EBOOK

Michael Andre Franiatte

Anti-Cheating Note and Solution

Being Competitive in Black Ops II Multiplayer

EBOOK

Anti-Cheating Note and Solution

Being Competitive in Black Ops II Multiplayer

Michael Franiatte

19/03/2021

It isn't obvious for new players to take pleasure in a game where other players have skills or hacks. It's impossible to enjoy a multiplayer game when you realize people cheats and so you want to do the same but your conscious won't be in harmony with your spirit and you would think about being banned while playing. Information about license, EULA and contract for using these following works can be found at https://michaelfraniatte.wordpress.com.

Anti-Cheating Note and Solution

Michael Franiatte*

Abstract

Cheaters are blatant in all multiplayer games, but for some games there is anti-cheat that kick and ban cheaters but in popular games the number of hackers and cheaters are such amazing that there is bypass or unban tool or file modifications, so cheaters are always in and destroy until ruin totally the game to be 80 per cent presents and only 20 per cent of players, the game becoming unplayable. When trying to do something if an anti-cheat is used, hackers makes new hacks and bypass the anti-cheat by hacking our computers for avoid the data sent and open hacked lobbies. When a game is incorporating a good anti-cheat, the address of memory that is written on our computers and read by the hack of the cheater, is randomly assignate each time the game is launched. The work of the hacker becomes impossible and expensive, when searching the address of memory to read to make his cheats. This book explain how to do this in all games, and for all processes running on our computers, and was never found by other authors or searchers knowing informatics. Before this universal solution for randomly assigns memory addresses by a transfer of all the memory, in all games and processes, other useless possibilities were accomplished. Such addresses are in numbers, 16 to power 8, but random memory usage is for 16 to power 7 addresses, so it becomes possible for a simple user to transfer memory in less than 10 minutes otherwise it takes 300 minutes for transferring memory in all possible addresses. The research leads to an append giving some tricks to increase performance and to resolve issues.

Keywords: *Anti-cheat, hacking, memory, addresses, transfer*

* Author correspondence: michael.franiatte@gmail.com

1. Introduction

Since the start of multiplayer games, the most popular cheats are wallhack (see square around players on all a map), aimbot (auto aim on the heads of players triggers when the cheater fire), autoshoot (auto fire when the enemy of the cheater is on his crossfire), lag switch (the aim of the enemy is deviate by a resolution screen hack or a mouse move event hack or a fake and pre firing hack), lag compensation (when the enemy fire the cheater, it's like he has god mod, fire has no effect), and lag event (when the enemy want to accomplish an action to kill the cheater, it doesn't happen or the enemy reload magically). Other cheats are like respawn kill while the cheater teleports him or the enemy in front of him) or the cheater becomes invisible or few others like the cheater kill you like a battering ram or if the cheater touch with one bullet one time the enemy, all other bullets touch the enemy.

The number of hacks grows with the imagination of hackers, and cheaters that use it are showing their gameplay like they have skill and are aggressive if you accuse them or without any reason, because hackers humanize their hacks and use propaganda on forums like saying lag compensation isn't a hidden god mod but a bad internet connection bug. Cheaters and hackers are from all countries like cheating for exams at school, it touch every layouts of society but not intellects.

This book concerns security, against hackers, on all Windows PC, and on games like Call of Duty, particularly Black Ops II, but also Modern Warfare 3, Ghosts, Advanced Warfare, and the game of the first developers of the Call of Duty series, known as Titanfall, but also Payday 2, Grand Theft Auto 5, The Division, DOOM, as well as Black Ops III, Rocket League, The Crew, Modern Warfare 2019, and Black Ops Cold War on PC. This book even concerns security on consoles with Battlefield 1, Battlefield V, Battlefield Hardline, Starwars Battlefront, Fifa 15, Garden Warfare 2, Titanfall 2, Need For Speed, but also Playerunknown's Battlegrounds (well known as PUBG), Fortnite Battle Royale, Apex

Legends, Destiny 1 and 2, Advanced Warfare, Black Ops III, Black Ops IV, Modern Warfare 2019, Vigor, and even Mixer and Netflix. The explanations can be extended to all multiplayer games. Searching to secure a PC leads to knowledge on how increase performance and to solve issues. An append gives information to give health to computers.

Because the support of Black Ops II on Activision site says to disable modem and Windows firewall, the problem with the hackers and cheaters in their games is entire, despite the developers ”priority to get rid of cheaters” in their own words. But apparently it’s filling by a lot of cheaters.

Hacked lobby is a PC side server using game files modify by an IDE tool well known by game hackers and crackers. It's like having the SDK of the game which can be modified as well. Servers use UDP protocol with IP of connection like every site on Internet browser but with the protocol TCP. The websites use the port 80, the secure websites use 443, the DNS servers use port 53, Steam use 27014-27050, BO2 authentication use 3074 and its servers use 13000-17000 but Titanfall use only 80, 443, 3075 and 30000-30010.

The school case of BO2 is interesting, because to people saying "few cheaters", "only official servers", "not like other Call of Duty" and "good anti-cheat", I can say, there is hacked lobbies, even players showing video proof of cheaters can say it also. My point of view, is that I've seen 5 lobbies for only 2 IP of servers connections. So 3 hacked lobbies and only 2 secure lobbies. Also, I've seen, at the same time, the same clan (FaiL) playing on the same lobby, where the server connection uses 2 different scales of ports (14100-14200 and 14400-14500). These people totally fail to argue, defending lies, to insult players, to continue to be few cheating, to take them as good players but using cheats. Playing a multiplayer game ask respect to others, totally different of cheating.

With perfect aimbot, aimboter whines "I'm just a pro", but aimboters are just noobs with no respect for developers and all the community around their work.

All chapters are made for information of explored solutions as purposes but almost all useless. In fact, hackers always find counter measures to give to cheaters a way to annoy gamers trying to enjoy and play the game they pay for it. There are always rotten people working in a factory that work in the reversed side of their co-workers and factory. These people enjoy destroying the works of other, even if they work on the same things, like it was for my files to resolve state equation, hydrogen coefficient diffusion, and Wiimote on PC and also can break expensive experimental and analytic tools.

The chapter 2 is made to understand what is possible to do with Windows firewall. The chapter 3 is made to give you information of useless solutions that was tested and explored, and it's not recommended to apply the things exposed in it. You can test on your computer the chapter 3, as purpose to disable virtual memory, and let the physical memory choose randomly which addresses will be used for values in your games. Also it explains like a summary how to make settings in Windows firewall. The chapter 4 extends to BO2 and all other games, the security methods to use, and the chapter 5 gives the programs tested in BO2 and AW. So you will find easy to apply security in your favourites games, and maybe you will see disappear cheaters in your games. But it's almost impossible on Call of Duty games because all servers aren't Valves Anti-Cheat (VAC) secure. Server owners of these games are full of money because they don't spend time for developing the game and don't want to spend time for banning all the cheaters. They let Fairfight, Punkbuster, VAC… look like noobs to ban cheaters. Developers of Call of Duty games use their own system of authentication into the game with Demonware.net, but cheaters banned can still playing with the help of servers owners. Each match, there is between 1 to 4 hackers, no more, no less from the launch with servers of gamerservers/clanservers. All the multiplayer games use a lot of servers of hackers like if you read the sentence I pick up on the forum of Gameservers.com (renting servers for BO1 and BO2) as following:

View topic - Battlefield3 Server Creation Questions - Game Servers Forum_php

[gs] Limp_bizkit* Posted: Sun Nov 04, 2012 9:37 am

GameServers Staff Joined: Tue Apr 05, 2005 12:19 pm

Posts: 1448 "Starxpilot is mostly correct. The only game servers we rent for Xbox 360 or PS3 are for a game called Section 8 Prejudice, because of the way their server hosting software is set up, we can rent out servers for those consoles even though the servers themselves are run on PCs. As for BF3, we host strictly for PC only."

http://forums.gameservers.com/viewtopic.php?f=4&t=49256

Also Malwarebytes Antimalwares sometimes block dangerous attacks of IP while playing at MW3 or BO2 associate with Call of Duty games process on the port 3074, normally reserved, like the IP 83.128.208.86:3074. So the servers of gameservers/clanservers are hacked lobbies insecure. Or maybe these servers on IP own by gameservers/clanservers are fake servers on IP own by cheaters having modified their computer IP. I saw Call of Duty Advanced Warfare being played using wallhack under official sportive competition organized by gameservers/clanservers but also fast XP lobby with connection IP corresponding to their servers IP.

2. Playing Black Ops II Multiplayer on Official Servers

2.1. Prerequist

BO2 scale servers IP are from 95.141.0.0/16, 195.122.0.0/16, 93.93.0.0/16, 189.1.0.0/16, 108.61.0.0/16, 197.80.0.0/16, 197.84.0.0/16, 173.199.0.0/16, 196.41.0.0/16, 152.111.0.0/16, 104.238.0.0/16, 177.54.0.0/16, 4.79.0.0/16. Most of IP from 195.122.134.0 to 195.122.135.255 disappear in resource monitor (tool in administration tool in control panel, or if you don't find resource monitor, the file is in Windows/System32 and is named perfmon.exe) when you create a IPsec strategy rule in Windows firewall. So, it must be IP of hacked servers, otherwise, these IP would not disappear. To play on official servers controlled

by editors, developers and retailers in your games, you can create strategy rules in Windows firewall like this…

2.2. Method to play on official servers of Call of Duty Black Ops II and Advanced Warfare

With this simple method you will be able to play on p2p servers host by a player or you and on official servers. It use Windows firewall and require you open a nat/pat rule with port 3074 in UDP for your computer on your modem/router. It takes 10 minutes for setting properly your Windows firewall and will resolve your problem of nat strict or moderate to be nat open.

P2p and official servers are more secure than fake of gameservers/clanservers server. Fake of gameservers/clanservers servers are allowing crack game, VAC banned and cheat owners to play like on BO2.

This guide explain how to have a connection to servers linked to the port 3074 in UDP own by developers without allowing the ports of any servers. The method is based on restricting outbound traffic connection with Windows firewall and allowing inbound traffic with a nat/pat rule for the port 3074 in UDP for connection to servers.

2.3. Creating a nat/pat rule for port 3074 in UDP

Create a nat/pat rule for port 3074 in UDP on your modem associate with your computer. There are lot of guides all over the net to do it. I let you search by yourself how to do it. It’s on your modem/router page. It's made for allowing inbound traffic on your computer.

2.4. Restricting traffic with Windows firewall

First thing to do is to set manually your IP of network connection as alternative configuration of ipv4 configuration properties of Ethernet in network properties (shown in details of your connection properties). Set ipv4 configurations from network card properties and disable all other features than ipv4. Add to optional DNS servers IP Norton ConnectSafe:

Preferred DNS: 199.85.126.30

Alternate DNS: 199.85.127.30

It’s same IP for DNS IP servers and WINS IP servers under the tab alternative configurations.

Disable the services server and workstation from services in administration tools from control panel. Also disable all services for distant assists.

From control panel, open Windows firewall from advanced parameters. In the middle tab you can open Windows firewall properties. In all combobox of the third first tabs set to block if no rules for outbound and inbound traffic.

Open outbound traffic connection tab from the left tab, it appear rules. Delete all rules.

Create a outbound traffic rule allowing with distant port 53 in UDP for the service client DNS (with distant IP your modem internal IP or DNS servers IP like Norton ConnectSafe primary DNS IP).

Create two outbound traffic rules allowing in TCP, local ports 1024-65535, distant ports 80, 443, 27000-27050 for Steam, Steamwebhelper and SteamGameOverlayUI.

Create two outbound traffic rules allowing in TCP, local ports 1024-65535, distant ports 80, 443, 3074 for BO2 and AW (distant IP 185.34.0.0/16, 209.170.0.0/16).

Create two outbound traffic rules allowing in UDP, local port 3074, distant ports 3074-3075 for BO2 and AW (distant IP 185.34.0.0/16, 209.170.0.0/16).

Create a outbound traffic rule allowing in UDP, local port 3074, distant port 40000 for AW (distant IP 108.61.0.0-108.61.255.255, 195.122.0.0-195.122.255.255, 173.199.0.0/16).

Open inbound traffic connection tab from the left tab, it appear rules. Delete all rules and don‘t let rules autocreate each time you install or update a game. When finished, you can export a .wfw file to not lose the settings.

Create two inbound traffic rules allowing with protocol UDP, local port 3074, and distant ports 3074-3075, and 13000-14000 for BO2 servers and 33000-34000 for AW servers

(distant IP 108.61.0.0-108.61.255.255, 195.122.0.0-195.122.255.255, 173.199.0.0/16, 192.168.1.0/24).

Create two inbound traffic rules allowing if secure with the second option with protocol UDP, local port 3074, and distant ports 3074-3075, and 13000-14000 for BO2 servers and 33000-34000 for AW servers (distant IP 108.61.0.0-108.61.255.255, 195.122.0.0-195.122.255.255, 173.199.0.0/16, 192.168.1.0/24). Under the tab distant users, deny the rule for group policy owner creator or this organization certificate.

Create two outbound and two inbound traffic rules allowing if secure in TCP and UDP, all local ports, all distant ports for all programs and services or your programs and services. Don't create a outbound traffic rule allowing if secure in UDP for BO2 and AW or deny the rule for the group policy TASK or other group policy in local security entity.

Open secure traffic connection rules from left tab. Add an IPsec rule with all protocols with authentication mode require authentication for inbound traffic and for outbound traffic with all IP for termination endpoints 1 and with IP 0.0.0.0 to 223.255.255.255 for termination endpoints 2. Termination endpoint 1 (server) corresponds to distant ports, and Termination endpoint 2 (client) corresponds to local ports. Open the properties of the rule and go on the tab advanced, open parameters of tunnelling IPsec options, then check the two first options and click apply. Set the parameters of IPsec tunnelling properties in Windows firewall properties. Add to deny all group policy for distant computers and users. Add a IP rule with all protocols with authentication mode ask authentication for inbound traffic and for outbound traffic with IP 0.0.0.0 to 223.255.255.255 for termination endpoints 1 and 2. Add a IP rule with all protocols with authentication mode require authentication for inbound traffic and for outbound traffic with all IP for terminaison endpoints 1 and 2.

Create outbound and inbound firewall rules blocking all distant IP and local IP 224.0.0.0 to 255.255.255.255.

Create outbound and inbound firewall rules blocking all local IP and distant IP 224.0.0.0 to 255.255.255.255.

Create outbound and inbound firewall rules blocking all services with all local IP and distant IP out of the range of your preferred DNS IP.

Create outbound and inbound firewall rules blocking local IP range out of your computer internal IP. It needs to be disable if it change. It's shown with the cmd dos prompt command ipconfig.

Create outbound and inbound firewall rules blocking distant IP range of your computer external IP like 90.6.0.0 to 90.6.255.255. Change it each time you restart your modem/router. It's shown with the website http://whatismyipaddress.com/ for example.

You can transform inbound rules to outbound rules and block all inbound traffic connection. But with inbound traffic connection rules, normally you will be nat open in BO2 and AW.

Open properties of Steam, BO2 and AW shortcut icons you created, type -tcp -secure -r -noproxy -disableSocks -connectToHost –RunAsService after the path showing where Steam is installed.

Apply this method for the service Windows update (set with recommended parameters), for the service Windows management infrastructure, and for iexplorer (ports 80 and 443) and your multiplayer games.

You can secure connection traffic by blocking all inbound traffic and block outbound traffic where you delete all rules. You will only create two rules in UDP and TCP allowing if secure with second option of authentication, and only create two rules in UDP and TCP allowing. Keep the IPsec rule with tunnelling IPsec and set to maximum security the properties of Windows firewall for IPsec parameters.

2.5. Secure your network

In Ethernet properties, for ipv4 properties, set manually your primary and auxiliary DNS server IP of your internet provider or of a secure DNS server listed: Level3 DNS 209.244.0.3, 209.244.0.4, 4.2.2.1, 4.2.2.2, 4.2.2.3 and 4.2.2.4, Comodo DNS 8.26.56.26 and 8.20.247.20, Norton DNS 199.85.126.30 and 199.85.127.30, Securly DNS 184.169.143.224 and 184.169.161.155, SafeDNS DNS 195.46.39.39 and 195.46.39.40, DNS.WATCH DNS 82.200.69.80 and 84.200.70.40, Opendns DNS 208.67.222.222 and 208.67.220.220, Dyn Internet Guide DNS 216.146.35.35 and 216.146.36.36, FoolDNS DNS 87.118.111.215 and 213.187.11.62, GreenTeam Internet DNS 81.218.119.11 and 209.88.198.133, DNS Advantage DNS 156.154.70.1 and 156.154.71.1, DNSResolvers DNS 205.210.42.205 and 64.68.200.200, Google Public DNS 8.8.8.8 and 8.8.4.4. You need to find only one DNS server, like with IP 127.0.0.1 (your local computer address) and 8.8.8.8 (primary google DNS server IP). Auxiliary DNS server is made to find connection if primary DNS server don't find it. For setting a new IPv4 configuration properly you can add 192.168.1.1 modem/router as primary DNS, and 127.0.0.1 localhost as secondary DNS that does not take account 'it's when your network have problem to be identify. Your modem doesn't need to have an allowing rule for port 53 if your DNS IP is your modem/router IP. With http://www.dnsqueries.com/en/ or http://www.webdnstools.com/ for IP of AW lobby connection 209.170.124.117 and domain name aw-pc-lobby.prod.demonware.net you have the results of DNS traversal and trace route servers. You can't DDos with LOIC (low orbit ion cannon) IP shown cause it's IP of Data Center. To find better DNS servers protected with Verisign, DNSmasq, and Microsoft look at these links:

http://h.root-servers.org/, http://public-dns.info/nameserver/us.html,

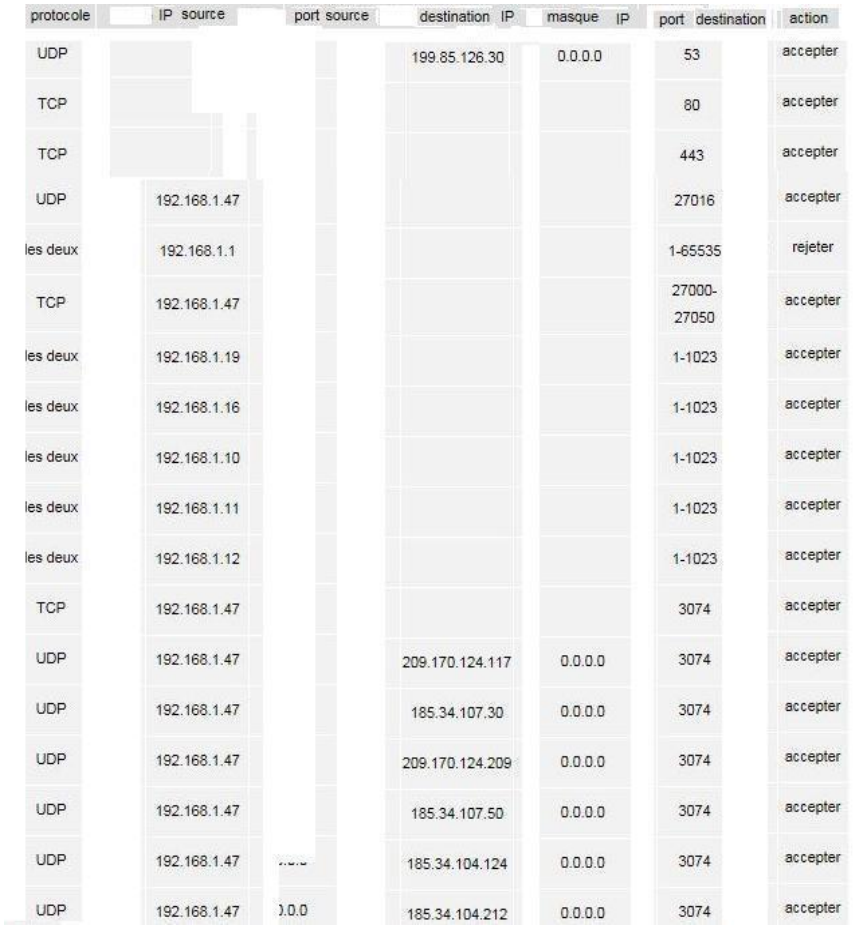
http://www.iana.org/domains/root/servers

If you want to download a game faster, it's better if you set a DNS server in your country.

In cmd dos command prompt you can type tracert 209.170.124.117 -d to watch IP of routers accross AW lobby server and your computer. If you type pathping 209.170.124.117 -n, you can watch a report of trace route IP, instead of -n, you can type -T and -R to identify IP with low quality of service and if some routers supports the resource reservation protocol (RSVP). You can block in your modem and Windows firewall IP of trace routers identified as bad and unsecure. For it, create a Windows firewall rule with ICMPv4 protocol and distant IP 209.170.124.117. Use the command ping 209.170.124.117 -n 1000000000000 -v 1 -a -f -S your internal IP -r 1. Use -? to display help and Ctrl+C to stop pinging. It's used to create a bridge helping connection in UDP for AW lobby.

It's important to use often the command dos ipconfig/flushdns and restart your modem to avoid noobs attacks on your computers in your network.

In your modem firewall allow only IP 209.170.124.117 for port 3074 in UDP corresponding to AW lobby connection. For BO2 lobby connection, the IP is 209.170.124.113. It's shown with the cmd dos prompt command ipconfig/displaydns. Allow ports 53, 80, 443, 3074, 27014-27050 in TCP and 53, 27000-27036, 4379-4380, 3478 in UDP. You can remove port 40000 in UDP from your modem firewall and Windows firewall rules for AW. Here a picture of my modem firewalls as example to help you:



protocole	IP source	port source	destination IP	masque IP	port destination	action
UDP			199.85.126.30	0.0.0.0	53	accepter
TCP					80	accepter
TCP					443	accepter
UDP	192.168.1.47				27016	accepter
les deux	192.168.1.1				1-65535	rejeter
TCP	192.168.1.47				27000-27050	accepter
les deux	192.168.1.19				1-1023	accepter
les deux	192.168.1.16				1-1023	accepter
les deux	192.168.1.10				1-1023	accepter
les deux	192.168.1.11				1-1023	accepter
les deux	192.168.1.12				1-1023	accepter
TCP	192.168.1.47				3074	accepter
UDP	192.168.1.47		209.170.124.117	0.0.0.0	3074	accepter
UDP	192.168.1.47		185.34.107.30	0.0.0.0	3074	accepter
UDP	192.168.1.47		209.170.124.209	0.0.0.0	3074	accepter
UDP	192.168.1.47		185.34.107.50	0.0.0.0	3074	accepter
UDP	192.168.1.47		185.34.104.124	0.0.0.0	3074	accepter
UDP	192.168.1.47	).0.0	185.34.104.212	0.0.0.0	3074	accepter

I searched to find a match while opening ports for Steam service and all programs in Steam folder, but it failed. I also searched to have connection with protocols TLS/SSL for secure TCP and DTLS for secure UDP, with no success. Steam show you if you have a network connection. The last advice is to have the recovery system CD of Microsoft bought legally in the market place and install your games under the disk D:\ instead of C:\ for restoring without losing your files.

If you encounter connection problem, you can change your computer internal IP with cmd dos command prompt, type ipconfig/renew or set a new configuration for ipv4 properties. To connect to BO3 use an internal IP finishing by a even number. Also try to restart your modem and your PC, set to automatic properties of IPv4 configuration settings, check game cache files from properties of the game in your Steam library.

With internet options in panel control, you can install the Geotrust CA certificate found in the folder game files of AW.

Set UAC to high security level from user account in panel control. Allow only execution of trusted programs.

2.6. Why to do it?

Since MW3, cheaters and hacked lobbies avoid gamers to enjoy playing. Fake of gameservers/clanservers server like on BO2 and AW is open to 400 000 members of cheat sites with their 44+ cheats and more to come as it was written on a cheat site calling fair players "the noobs".

99% of the time you play on AW is on fake of gameservers/clanservers, but players think it's p2p host server. Playing on p2p servers and official servers with a connection only linked to the port 3074 watched by developers, is the best way to not be the first to leave waiting the impossible cheaters clan to do it first.

On BO2, with this method, it's easy to find a connection to gameservers/clanservers server, because it's linked with port 3074 allowed as inbound traffic, so it's not fake of gameservers/clanservers server. On AW, with this method, it's hard to find a server, cause the game is only p2p and fake of gameservers/clanservers server has invade the matchmaking. Fake of gameservers/clanservers aren't linked to port 3074, and take all the player base fighting against cheaters that are banned and use crack game.

We have to wait an update of AW for this, because it's not normal that offenders destroy the fun of players that bought the game. It's almost impossible to find a p2p server, waiting 1 hour to fill the server, cause players ignore my works or take it as a joke. Even if players can understand, they prefer to leave the game or play against cheaters busting them with aimbot. It's a total fault of the community, too lazy or too ignorant to apply this simple method, and too stupid to forward this guide to all the community.

You don't have to disable your firewalls for allow all inbound traffic like it was written on Activision support site. Server not linked to port 3074 is totally infested with aimboters, because there is no control, no ban, no solution to stop cheats.

2.7. Conclusion on AW

I played AW being the host of the parties, there was, always in the opposite team, an obvious wallhacker and a less obvious aimboter that somtimes auto-aiming his allies (humanized aimbot) allowing to be sure to say it was a aimboter, but even if I was the host the aimboter never quitted. So developers allow people to cheat in their game. Nothing is done and never will in Call of Duty games against cheaters. Letting cheaters allowed to do everything they want by just changing values in address of codes, with the amazing killcam innovation, is made to make raging people. Cheaters are helping by Microsoft community to debug their cheat codes and probably by developers of this kind of game seeing the hack menu in BO2 on PS3. It's a shame. The Call of Duty games series is a part of crime industry and not game industry.

I also tried to open on my modem with nat/pat rules and in Windows firewall as inbound and outbound traffic listen ports (local ports) 3074, 27016 for AW and 27036 for Steam shown in perfmon.exe as allowed… But nothing stops and kick cheaters in AW.

I don't believe Steam needs same ports used by AW to communicate together. Certainly with Steam service. Steam giving no information on VAC as they replied to me when asking the Steam support, their fault is entire like the developers. Even if I've pointed to them I was working on this book. It didn't avoid them to give me a VAC banned on record on BO2 for searching a solution against cheaters.

2.8. VAC Secure Servers on Call of Duty

More and more cheats and cheaters in COD games, and so nothing will change but will be worst and worst. My Anti-Cheating solution is running on other games, but totally

don't run in COD games. They ban you if you try tools to counter cheats without using even a shadow of a cheat. They modify your PC if you find something interesting in order cheaters can still cheat.

Developers of COD games create it with in mind all possible cheats can be used, like cheaters can even change your own FOV, mouse move, gun recoil, position, spawn place, energy, be killed by half of a bullet, killcam duration and even servers forward with only prestige master or cheaters.

When software has not aslr, it's for accessing data, controlling data against cheats or controlling data for cheating. Payday 2 kicks when a cheater throws more grenades than he can or when he don't own a mask. In CoD games, I never see someone kicked for 50 hacks available.

2.9. But cracked and hacked lobbies are the problem

With VPN programs, cheaters can open hacked lobbies on any games cause their computers can take every IP existing even those reserved. So even banned or without buying the game cheaters invade your multiplayer games.

To block VPN users, you must have your network as private. If your network is set to public, click on resolve problem under network in control panel, then resolve residential group problem and apply the recommended Windows setting for a private network. Create Windows inbound and outbound blocking rules for all programs with domain and public profils (https://en.wikipedia.org/wiki/VPN_blocking). If you encounter problem for authentication of network, you need to restart your PC.

When you play a match on BO2 or BO3, the ping number of each player is displayed when you watch the leaderboard of scores. Often the best player has the lowest ping like when you play a private match against bots. It corresponding to a cheater that opened the hacked lobby where you playing. He uses a VPN to change his IP similar to IP of official servers. We

need a DPI (Deep Packet Inspection) firewall. This kind of firewall checks if the IP of the country has the latency corresponding to the country. I recommend using PeerBlock, it's a DPI firewall that can block p2p, hacked computer, VPN users IP connections with our computers. Check this link for information on peerblock:

https://github.com/PeerBlock/peerblock.

Also having the connection only linked to IP of Call of Duty lobby connection on port 3074 with inbound rule is the best way to not be forwarded on hacked lobbies full of cheaters. But instead of a nat/pat rule for port 3074, create a nat/pat rule with internal port 3074 and external port 27031 or 27016 or 4986. These ports correspond to listening ports for BO2, AW and BO3 shown in perfmon.exe under the tab network. The report button on steam profit of offenders is useful to have game session without them the day after you reported. The steam profiles on Steam game overlay are open from the game shown in recent players you played with when you ask a friend request on AW and on BO2.

2.10. Conclusion on gameservers/clanservers

Since BO1 gameservers/clanservers is allowing hacked lobbies and cheaters banned and using cracked games. You don’t find anymore matches on p2p servers on port 3074. If you are accused to lag the cheaters, the game allow to break your computer that will lagging even more than you lag cheaters computers. By removing the rule allowing if secure in UDP for BO2 and AW you can find matches with only inbound traffic (blocking lateral traverse) but if you don’t remove this rule or don’t deny the rule for group policy TASK or other group policy in local security entity, even if your game is nat open, you don’t find matches. For find matches with inbound traffic, you need to open all ports on your modem firewall and create a nat/pat rule for port 3074 in UDP. For outbound traffic, only local entity security is taking account but for inbound traffic, only distant users and distant computers is taking account considering rules allowing if secure. By creating rules allowing if secure with different group

policy, it's possible to increase security. For it you must put same distant ports for rules allowing and allowing if secure but local ports 1024-65535 for rules allowing and all local ports for rules allowing if secure. Also if you define a distant IP.

You can double rules allowing by same rules allowing if secure for your programs and services if you set rules with all distant IP, all local ports, distant port 53 in UDP for client DNS, distant ports 27000-27050 in TCP for Steam.exe, distant port 3074 in TCP for AW and BO2, distant ports 1024-65535 in UDP for AW and BO2. You can't do it for distant ports 80 and 443 for steamwebhelper.exe as example. For it, you need all ports open on your modem firewall.

The last attempt was to open the listen port shown in perfmon.exe for Black Ops III and Steam in Windows firewall and modem firewall as following:

application / service	protocole	adresse IP source	masque adresse IP	port source	adresse IP destination	masque adresse IP	port destination	action
80	TCP	192.168.1.23	0.0.0.0				80	accepter
88	UDP	192.168.1.23	0.0.0.0				88	accepter
443	TCP	192.168.1.23	0.0.0.0				443	accepter
3074	les deux	192.168.1.23	0.0.0.0				3074	accepter
4986	les deux	192.168.1.23	0.0.0.0				4986	accepter
27036	UDP	192.168.1.23	0.0.0.0				27036	accepter
steam	TCP	192.168.1.23	0.0.0.0				27000-27050	accepter
modem	les deux	192.168.1.1	0.0.0.0				1-65535	rejeter
VAIO	les deux	192.168.1.19	0.0.0.0				1-1023	accepter

application / service	port interne	port externe	protocole	appareil	activer
3074	3074	88	UDP	pc-michael	☑
4986	4986	4986	UDP	pc-michael	☑
27036	27036	27036	les deux	pc-michael	☑

3. Explored solutions

3.1. Services disabling

Take care to programs you install or use Windows Defender or Windows Security Essentials.

Take care about the user account control (UAC) settings in control panel. UAC must be set to the highest security.

All Windows services are safe and DEP (Data Execution Prevention) on Windows programs and services is enabling by default. Enabling for all other programs is a good way to avoid hackers to change something on our computers. It's important to do this for trigger an error if hackers try to change something. The services which can be stop and disable with services in administration tool in control panel are the services finishing by at distance, and with at distance in the description like WorkStation and user peripheral access.

To increase security on your computer, some uninstalls can be made as following

Uninstall all programs but let network, graphic and audio drivers, and Steam+games.

Uninstall all in Ethernet properties but let ipv4 and uncheck ipv6.

Disable lmhost and netbios in tcp/ip in the tab wins of ipv4 properties.

Disable Dcom in work station properties of components service in administration tools by unchecking Dcom in the tab default properties.

Stop and disable the services workstation and server, in services, in administration tool, in control panel.

You can stop http services by run as administrator cmd prompt and type net stop http.

Uncheck assistance at distance in the tab using at distance in system properties in system in panel control.

In order to test if services can involve security attacks, disable PC settings in System from control panel, disable Windows functionalities in program and functionalities but you

must let the functionalities executions of Microsoft framework 3.0, 4.0, 4.5, Internet Explorer 9, 10, you can uninstall all programs but let the audio card, graphic card, network card drivers, disable services in administrative tools but, in French, let services as Informations d'application, Service de profil utilisateur, Générateur de point de terminaison du service audio Windows, Audio Windows, Moteur de filtrage de base, Service de prise en charge bluetooth, Service de chiffrement, Client DHCP, Client DNS, Journal d'événement Windows, Service de stratégie de diagnostic, Service d'association de périphérique, Gestionnaire d'installation de periphérique, Détection materiel noyau, Plug-and-Play, Client de stratégie de groupe, Planificateur de classe multimédia, Windows installer, Netlogon, Connexions réseau, Service Interface du magasin réseau, Alimentation, Mappeur de point de terminaison, Planificateur de taches, Service client steam, Sauvegarde Windows, Service ouverture de session locale, Service de découverte automatique de Proxy Web pour les services HTTP Windows, Service de moteur de sauvegarde en mode bloc and other security services as Windows firewall. These services are very important and shall not be disabling. Other services than security and restore services shall be disabling. Security and restore services shall be enabling. The services in French Service Liste des réseaux and connaissance des emplacements réseau can be disable but for open Ethernet properties you must open properties of the network card used to have internet connection. You can enable services with safe mod computer start. Services to never disable in English are: Application Information, Background Tasks Infrastructure Service, Base Filtering Engine, Bluetooth Support Service, Cryptographic Services, DCOM Server Process Launcher, DHCP Client, Diagnostic Policy Service, Diagnostic System Host, Distributed Link Tracking Client, DNS Client, Function Discovery Resource Publication, Group Policy Client, IKE and AuthIP IPsec Keying Modules, IP Helper, Local Session Manager, Multimedia Class Scheduler, Network Connections, Network List Service, Network Location Awareness, Network Store Interface

Service, Power, Remote Procedure Call (RPC), RPC Endpoint Mapper, Security Accounts Manager, Security Center, Shell Hardware Detection, Task Scheduler, User Profile Service, Windows Audio, Windows Audio Endpoint Builder, Windows Connection Manager, Windows Error Reporting Service, Windows Event Log, Windows Firewall, Windows Management Instrumentation, WinHTTP Web Proxy Auto-Discovery Service. Normally it will kill the processes rundll32, dllhost, taskhost and taskhostex shown with task manager.

Put to read only BO2 files (after you have verified the game cache integrity of BO2) and put game launch options -secure 1 -VAC 1. But maybe, when you playing against a hacker or cheater, their hacks can modify configuration files, like on Modern Warfare 3, when FOV can have changed, even if it's not a game option. So it can change the matchmaking system where you can be forwarded in hacked lobbies. When you are in the leaderboard, and suddenly you are on another, quit the game, and delete these files: user_mp.cgp, user_common.cgp, hardware_mp.chp, bindings_mp.bdg, installscript.vdf. Also quit steam and delete these files: steamevents_123456789.pkv, SteamAppData.vdf, loginusers.vdf, libraryfolders.vdf, GameOverlayRenderer, DialogConfig.vdf, debug, coplay_123456789.vdf, confif.vdf, ClientRegistry.blob, appmanifest_202990.acf, appmanifest_202970.acf, find in Steam folder. Do it each time you finish to play BO2.

You can disable starting programs from task manager opened with ctrl+shift+esc under the tab starting. Also you can delete files in startup folder; it's where a file can be executed when your PC is starting. In

C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

and on the desktop where there is your program shortcuts... There are masked files like files named desktop with shell commands. It can cause to cut the sounds and the pictures when you are playing, and make appearing red pixels displayed on your screen. To delete these files,

you must show folder and files masked, and unmask protected files of the system, from folders options in the tab display, in control panel.

3.2. Using Punkbuster

To get rid of cheaters in MW3 and BO2, I have tried punkbuster. Put pbsvc.exe and pbsetup.exe in the folder of BO2 and md5tool before this folder, the files are found on the site of Punkbuster. To use md5tool, open cmd and type cd c:\program files (x86)\Steam\Steamapps\common, then push enter key, then md5tool.exe "call of duty black ops ii"\t6mp.exe 0 2048. It create a cfg file named pbsvuser, open it with notepad, then copy the number after SZ to the 0 of LEN to have SZxxxxxx to LENxxxxxx and copy this file in the folder of pb in BO2 folder after updating pbsetup, and after launch pbsvc that you rename pbsvc_t6mp.

3.3. Host forcing

This example is made for Black Ops II that use dedicated servers hosting by Gameservers of the domain name Choopa.net, official servers or some unknown servers associate with same IP but different ports. It seem that choopa.net servers are official but some IP closer or IP with same domain name seem to be owned by hackers cracking games and servers.

On Black Ops first opus, the list of servers shows the names of servers where Treyarch official servers (in orange) has IP corresponding to IP from Gameservers organization like for a lot of Secure servers of Modern Warfare 3 if you look in details in resources monitor and in the list of servers of Steam. Gameservers rents servers for a lot of games, the IP that this organization own are indicated on the site speedguide.net, and only these IP are indicated for connections to secure servers. Other servers with different IP own by Fragnet or Nuclearfallout or Bazaar... seems to be not fair, in particularly on Black Ops II where same

strange players pre-aims, reloads automatically, starts and stops firing as soon as you die or kills with half of bullets that you need to kill.

Setting Windows Firewall to play on secure servers is the best way to play with legit players and see cheaters kicked and never comes again.

The windows resources monitor will show you the IP addresses of servers. The cmd prompt command ipconfig/displaydns will show you the IP addresses of connections. It's difficult to understand why servers are hosting by Gameservers because the developers of the game, instead of pay servers, have their own servers. But the IP presented here to find servers corresponds to IP of Treyarch developers servers available on Black Ops I.

Hackers open prestige master lobbies like on the IP 108.61.237.153 ports 14300-14399 as I've seen in the game and read on a cheater site. Also there is multiple servers with the same IP 108.61.237.153 ports 14380-14419, 14420-14499, IP 195.122.134.237 ports 14330-14359, 14500-14539, IP 173.199.105.17 ports 15000-15099, 14000-14099, 14300-14399. Also they open booster lobbies like on the IP 108.61.237.150, because it open a fresh new lobby, where boosters can join themselves. Cheaters on these IP seem to be so sure to not get banned like if they play with a game crack. Maybe it's important to allow listen port 3074 shown in resource monitor. For it, you must create an inbound connection rule applied for public network if your network is set on public with local port 3074, and all local IP, distant ports 3074-3075, all distant IP. You can verify if the port 3074 is allowed with resource monitor in the tab listen ports. For allowing inbound traffic, you must open a nat/pat rule for port 3074 in TCP/UDP on the advanced options of your modem (internal IP in details of your network properties, with login name admin and password admin), and you must check the combobox block by default in the tab public network (if your network is set on public) in Windows firewall properties. Maybe VAC secure servers are find on ports 15000-15050 or

other scale ports, but nobody talked about that, and it's very difficult in time to test all ports to find if there is cheaters or not, if they are banned or not.

Go to panel control, then click on Windows firewall, then open advanced parameters, requiring administrative privilege, then click to the upper left to open the tab Security connection rules, then click to create a new rule, in the right tab, it open a window. In it, create a personalized IPsec rule (authentication inbound and outbound required), you can add in the tab distant computer in the box ending point 2, IP from 0.0.0.0 to 223.255.255.255. When it's created open the property of the rule in the middle tab, click right on the rule to open its property window. In the tab advanced, click on the button personalize for the last tab named IPsec tunnelling, in it check only the box, use tunnelling IPsec, then click ok to close. In the box ending point 1, for the tab distant computer, let all IP check box checked. In a second rule, you can add in the tab distant computer in the box ending point 1, IP from 0.0.0.0 to 223.255.255.255. In the box ending point 2, for the tab distant computer, let all IP check box checked. If you don't want to create a IPsec tunnelling, you can uncheck the box use tunnelling IPsec, and add in the boxes ending point 1 and ending point 2, the IP from 0.0.0.0 to 192.168.1.1 (or your computer internal IP minus 1) and IP 192.168.1.3 (or your computer internal IP plus 1) to 223.255.255.255. Then, create blocking rules for inbound and outbound traffic, you can add distant IP 224.0.0.0 to 255.255.255.255 and the internal IP of your computer like 192.168.1.2. Also you can add IPsec rules with ask authentication for inbound and outbound traffic with all distant IP. In any case, the IPsec rules can be associated, and the strongest security is applied, rather than a low level security.

Also for IPsec rules, you can use another certificate, and propagate in trust root the certificate of BO2 in the tab numeric signature of the window property of t6mp.exe. But also, you can edit the default settings of IPsec rules in the tab IPsec of Windows firewall properties,

with the first command button personalize. In it, you can add new IPsec authentication types with higher level of security.

Set manually your IP of network connection as alternative configuration of ipv4 configuration properties of Ethernet in network properties (shown in details of your connection properties). You need to know, the internal IP of your computer and your modem. Set the firewall properties to block (by default) for all texboxes of inbound and outbound connection in Windows firewall properties. Delete all rules, and then create blocking rules as following… For inbound and outbound traffic, create rules TCP and UDP for local ports 1-1023 and all distant ports. For inbound traffic, create a rule TCP for all local ports and all distant ports, also two other rules in UDP for local ports: traversal edge and discover PlayTo, with all distant ports. Then create allowing rules in outbound traffic, rule for the service client DNS, port 53 in UDP, distant IP, the internal IP of your modem, then create a rule for Steam.exe, ports 80, 443 and 27000-27050 in TCP, then create a rule for t6mp.exe, port 3074 in TCP, distant IP, 209.170.124.147 and 209.170.124.209, then create a rule for t6mp.exe, port 3074 in UDP, distant IP, 209.170.124.117 (in outbound connection rules). Then create a rule in inbound traffic, for t6mp.exe, local port 3074 or 3074-3075, and distant ports 1024-65535 or 14000-16000 in UDP, all distant IP, in inbound connection rules, for blocking server connections from a modem/router but allowing official server connections (with the default option block edge traversal to prevent NAT edge device connections) but to find a match, you will need to open a nat/pat rule for port 3074 in TCP/UDP, on the advanced settings of your modem (other servers rules are studied with IP that will be given from time to time in this book). Each time you will verify the game cache files of your games, and launch its, delete the new rules autocreate to let only the interesting IP of server connections in the rules you customized. To be able to connect in Steam, you need to add –tcp in the shortcut of Steam.exe, after the target where the exe is located. After authentication into BO2, before

searching a match, you can disable the client DNS rule and the rule for t6mp.exe, port 3074 in UDP, distant IP, 209.170.124.117. Also you can disable the nat/pat rule in your modem, after finding a match, and before connection to the match.

Also create allowing outbound traffic rules for steamwebhelper.exe and steamgameoverlayUI in the folder steam/bin and steam respectively (folder where you installed Steam), with distant ports 80, 443, in TCP.

If you don't want to open a nat/pat rule in your modem settings for your computer, do as following. Instead of creating the inbound connection rule for find a match in BO2, block all inbound traffic with the properties window of Windows firewall and create two outbound rules as following. Add the rules for t6mp.exe with local port 3074 or 3074-3075, and distant ports 1024-65535 or 14000-16000 in UDP with distant IP like 93.93.64.0/21, 108.61.0.0/18, 108.61.64.0/19, 173.199.62.0 to 173.199.63.255 and 173.199.67.0 to 173.199.67.255 and 173.199.83.0 to 173.199.83.255 and 173.199.104.0 to 173.199.104.255 and 173.199.106.0 to 173.199.107.255 and 173.199.112.0 to 173.199.122.255. You can copy this rule for the other rule, but instead of an allowing rule, it's an allowing if secure rule which you create. Click on the button personalize and check the box null encapsulation to allow connection only if the IP is authenticate. You can try to copy the other allowing rules explained in this chapter for change to if secure with null encapsulation but you will lose connections.

You can also create an outbound blocking rule with all protocols, all ports, all distant IP and local IP from 0.0.0.0 to 192.168.1.1 (or your computer internal IP minus 1) and IP 192.168.1.3 (or your computer internal IP plus 1) to 255.255.255.255.

As explained above, the best way, is to set properly Windows firewall but with more details, as for allowing rules with these advanced options: apply for public network only and for local access only. Also rules with block all services only and block all application packages only for inbound and outbound traffic connections can be added but the service

client DNS will be block, so you won’t be able for authentication in BO2. The UDP inbound rules can allow all distant IP creating a NAT/PAT rule on your modem/router, so block all inbound traffic. Also, you can add your internal computer IP for local IP in all inbound and outbound allowing rules, and you can add you as allowing user for allowing rules in the tab locales securities entities, you just have to check box allowed users, then add the user “local account“ with advanced options by clicking search. And in the tab locales securities entities, you can exempt the allowing rules for all users by adding it with click left+ctrl key or shift key, but not add in French Administrateur(s), Compte local (et membre du groupe administrateur), Interactif, Computer name, Ouverture de session de console, Tout le monde, "Utilisateurs", "Utilisateurs authentifiés".

The way is to set windows firewall. In windows firewall properties in all combo boxes, set to block (if no rules). Disable all inbound and outbound rules. Useless outbound rules in TCP to create but disable when playing is port 80 (http), 443 (https) and 27000-27050 to download games with the programs Steam.exe, SteamGameOverlay.exe. Create an outbound rule in TCP for Steam.exe (path in services and programs) with port 27017 (IP in ressources monitor) or 27030 for Steam connection. Create an outbound rule in TCP for t6mp.exe (...) with port 3074, with locale IP, your internal IP, and distant IP, 209.170.122.109, 209.170.124.209 and 209.170.124.216 or inbound rule with distant IP 209.170.124.209 and 209.170.124.216. Create a outbound rule in UDP for t6mp.exe (...) with port 3074, with locale IP, your internal IP, and distant IP, 209.170.124.113 or inbound rule. Create an outbound rule in UDP with port 53 for DNS client service (choose it in property in the tab services and programs) with locale IP, your internal IP, and distant IP, your dns server like 192.168.1.1 or the one you add as a manual dns server. Then lasting by create two outbound or inbound rules in UDP for t6mp.exe with locale port 3074 (take care to disable the other autocreate each time you verify game cache), one rule with locale IP, your internal IP,

and distant IP: 209.170.124.113, 209.170.124.114, 209.170.124.209, 209.170.124.216 (ports 3074-3075), and one rule with all ports, with locale IP, your internal IP, and distant IP: 173.199.64.0 to 173.199.66.255 and 173.199.68.0 to 173.199.82.255 and 173.199.84.0 to 173.199.103.255 and 173.199.105.0 to 173.199.105.255 and 173.199.108.0 to 173.199.111.255 and 208.167.232.0 to 208.167.232.255 and 208.167.234.0 to 208.167.235.255 and 208.167.240.0 to 208.167.240.255 and 208.167.242.0 to 208.167.251.255 (speedguide.net site information for IP corresponding to Gameservers organization and not choopa LLC organization). You can view it in resources monitor even you aren't open nat, but normally with these rules you are if you open a nat/pat rule for port 3074 in UDP on your modem. If you shutdown Steam and want to log again, open a outbound instant useless rule in TCP and UDP with all ports and distant IP open. You can replace the inbound rules to outbound rules but the nat state will be strict. Create an outbound rule for PnkBstrA.exe in TCP and another one in UDP, with local IP, your internal IP, and distant IP, all (Port indicated in resources monitor for the program PnkBstrA). Create an outbound rule for pbsetup.exe in TCP, with local IP, your internal IP, and distant IP, all (port 80).

Another solution explored:

After Windows updates and blocking all inbound traffic, allowing all outbound traffic, it’s possible to find a match without creating a nat/pat rule for the port 3074 in your router. I recommend this way because inbound traffic can warm your computer. To setting properly Windows firewall do as following by creating outbound rules:

TCP for the program Steam.exe with port 443 (facultative)

TCP for the program Steam.exe with ports 80, 27014-27050 (port and IP in resources monitor)

UDP for the program Steam.exe with ports 27000-27030

TCP for the program Steam GameOverlayUI.exe with port 80

TCP for the program t6mp.exe with port 3074 (209.170.124.209 and 209.170.124.216)

UDP for the program t6mp.exe with ports between 10000 and 16000 (173.199.64.0 to 173.199.66.255 and 173.199.68.0 to 173.199.82.255 and 173.199.84.0 to 173.199.103.255 and 173.199.105.0 to 173.199.105.255 and 173.199.108.0 to 173.199.111.255 and 208.167.232.0 to 208.167.232.255 and 208.167.234.0 to 208.167.235.255 and 208.167.240.0 to 208.167.240.255 and 208.167.242.0 to 208.167.251.255)

UDP for the program t6mp.exe with port 3074 (209.170.124.113)

UDP for the service ClientDNS with port 53 (192.168.1.1) (can be disable after connecting to the game)

TCP for the program malwarebytes antimalwares with port 80 (facultative)

TCP for the service Windows update with ports 80 and 443 (facultative)

Create an outbound traffic rule for blocking all ports, all protocols, and distant IP generate by predefined group of computers, add all options but not internet, then disable and enable it when connecting to Steam and the game. Create an outbound traffic rule for blocking all ports, all protocols, and add the shortcut of svchost.exe in Windows\system32 and Windows\SysWOW64, then disable and enable it when connecting to Steam and the game. Create an outbound traffic rule for blocking all ports, all protocols, and local IP from 0.0.0.0 to your internal IP minus 1 and from your internal IP plus 1 to 255.255.255.255 and let all distant IP to block.

Set a static IP for the protocol ipv4, with the properties of your connection, in Ethernet. Create rules to block ipv6 IP with all protocols, all ports (::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff).

In Windows Firewall again, create a custom ipsec strategy with the rule require authentification for inbound traffic and ask authentification for outbound traffic with the option advanced for authentification. After installation of Steam.exe certificates by clicking

right on this file, then choose properties, in the tab numeric signature, then install Valve and Symantec certificates in the folder that can be access when you will choose the strategy in the rule ipsec. For the first authentification choose the Valve certificate, and for the second authentification, choose Symantec. Its to apply to all ports, all IP.

Other solution more simple is blocking all traffic incoming, and setting traffic outcoming as: public rule, all ports, all protocols, for t6mp program, allowing all ports, TCP and UDP protocols, for t6mp program, distant IP between 173.199.64.0 to 173.199.66.255 and 173.199.68.0 to 173.199.82.255 and 173.199.84.0 to 173.199.103.255 and 173.199.105.0 to 173.199.105.255 and 173.199.108.0 to 173.199.111.255 and 208.167.232.0 to 208.167.232.255 and 208.167.234.0 to 208.167.235.255 and 208.167.240.0 to 208.167.240.255 and 208.167.242.0 to 208.167.251.255, 209.170.122.109, 209.170.124.113, 209.170.124.209, and 209.170.124.216. No lag comp and switch lag like on other servers than GameServers.com choopa.net domain with aimboters never banned, like with the scale IP 108.61.237.0 to 108.61.237.255 of fragnet.net choopa.net domain and choopa LLC organization (allowing friends to boosting in the game while opening only one IP enabling them to join together, but also allowing hackers to make cheats) and IP between 195.122.135.0-195.122.135.255 of fragnet.net too, just try it. Take care about what can learn to you the ressources monitor on IP when you forward with Windows Firewall only IP 209.170.124.113, 209.170.124.209, 209.170.124.216 and searching a game. In fact, some IP aren't show by order or without the dns domain name choopa.net, so it correspond to fake servers not protected by Valve and Treyarch Anti-Cheat. 99% of servers are fake and compromize your gameplay (in it, aimboters, wallhackers using lag comp as god mode and mouse deviation as lag switch). The rest of 1% have none of noob cheaters and noob lags, and nobody will insult you or complain, but only compliments as you fighting against soldiers training themselves. Also there is an IP 209.170.72.124 appearing in ressources monitor, that

I don’t know if it’s an IP in UDP or TCP, but it seem to be a security IP of demonware.net like close IP for connection. So you can add it as an allowing rule for outbound traffic in Windows Firewall.

Another method:

Block all incoming connections or delete all rules, and don’t add ports 3074-3076 in UDP and TCP, to not be open nat in black ops II.

Block if no rules outcoming connections. Delete all rules. You must create public rules only with your local IP of your PC connected to your modem; it’s your internal IP. Create an allowed rule in TCP with the ports 80, 443 and the service windows update. Create an allowed rule with the port 80 for the program gameoverlayUI.exe in Steam folder. Create an allowed rule in UDP for the port 3074 and distant IP 209.170.122.0 to 209.170.124.255. Create an allowed rule for ports 27014-27050, 3074 in TCP, and another one for ports 27000-27030, 3074, 4380, 3478, 4379, 4380, 1500, 3005, 3101, 28960, 53 in UDP. Create an allowed rule for t6mp.exe program, in UDP with all ports and distant IP as following: 173.199.64.0 to 173.199.66.255 and 173.199.68.0 to 173.199.82.255 and 173.199.84.0 to 173.199.103.255 and 173.199.105.0 to 173.199.105.255 and 173.199.108.0 to 173.199.111.255 and 208.167.232.0 to 208.167.232.255 and 208.167.234.0 to 208.167.235.255 and 208.167.240.0 to 208.167.240.255 and 208.167.242.0 to 208.167.251.255, with the good port to have Gameservers organization with choopa.net domain name indicated in resources monitor while you playing. It corresponds to ports between 10000 and 16000 or all other ports if you don’t find a match. Because the same public IP can be assign with different servers and different ports. For one of these IP forwarded with Windows firewall, 3 servers can be find while searching a game, with 2 that are not with choopa.net domain name indicated in resources monitor and obviously, you will not be on the good one. You should find the good ports to forward with these IP,

corresponding to ports between 10000 and 16000. So you will need to create an outbound rule in UDP for blocking ports 0-10000, 16000-65535 or 0-13000, 15000-65535 for example, with distant IP from 173.199.64.0 to 173.199.66.255 and 173.199.68.0 to 173.199.82.255 and 173.199.84.0 to 173.199.103.255 and 173.199.105.0 to 173.199.105.255 and 173.199.108.0 to 173.199.111.255 and 208.167.232.0 to 208.167.232.255 and 208.167.234.0 to 208.167.235.255 and 208.167.240.0 to 208.167.240.255 and 208.167.242.0 to 208.167.251.255. It correspond to Gameservers (choopa.net) of official dedicated servers IP of Treyarch official servers of BO1 and so BO2, protected by VAC and TAC and not choopa LLC fragnet unofficial servers, not protected by VAC and TAC (99% of servers where people are playing are unsecure servers). To ensure that rcon port is open between your pc and servers side security of the game, you can open all IP and TCP ports and all IP and UDP ports between 0-10000 and 16000- 65535 or maybe almost 0-14000 and 14500- 65535, for the program t6mp.exe, but take care with resources monitor if you are always connected of servers IP corresponding to Gameservers organization. The IP of servers from Gameservers organization and opening game ports are designate to be use for all other multiplayer Steam or Origin games to ensure to play on VAC or PunkBuster protected servers.

Another solution explored:

Set the firewall properties to block (by default) for public, to always or all block for domain and private in textboxes of inbound connection, and to block for all texboxes of outbound connection, then delete all rules for outbound and inbound connections.

Create custom IPsec strategy with the rule no authentication.

Create three inbound and outbound connection rules for all protocols, all ports (inbound), ports 27050-65535 (outbound) with the action check, allow the connection only if it’s secure, each time, with a different option.

Let the inbound connection rules UDP (distant IP: 173.199.64.0 to 173.199.66.255 and 173.199.68.0 to 173.199.82.255 and 173.199.84.0 to 173.199.103.255 and 173.199.105.0 to 173.199.105.255 and 173.199.108.0 to 173.199.111.255 and 208.167.232.0 to 208.167.232.255 and 208.167.234.0 to 208.167.235.255 and 208.167.240.0 to 208.167.240.255 and 208.167.242.0 to 208.167.251.255, all ports) and TCP (all distant IP, ports 3074-3076) autocreate each time you update or install your game, named with the game name corresponding, with the default option block edge traversal to prevent NAT edge device connections.

Create an inbound and outbound connection rule for the service Client DNS, with protocol UDP and port 53, with local IP, your internal IP, and distant IP, your DHCP and DNS server IP (shown in details of your connection properties for Ethernet).

Create an outbound connection rule with the protocol TCP for ports 80, 443, 27000-27050, 3074-3076 and for all programs and services.

Create an outbound connection rule with the protocol UDP for ports 3074-3076 and distant IP, 209.170.122.0 to 209.170.124.255, and all programs and services.

Create a rule for blocking and not allowing this time, for outbound connection, with all protocoles, and all ports, with distant IP: 95.141.0.0 to 95.141.255.255, 195.122.0.0 to 195.122.255.255, 93.93.0.0 to 93.93.255.255, 189.1.0.0 to 189.1.255.255, 108.61.0.0 to 108.61.255.255, 197.80.0.0 to 197.80.255.255, 197.84.0.0 to 197.84.255.255, 173.199.0.0 to 173.199.255.255.

Or set windows firewall as following:

In windows firewall properties in all combo boxes, set to block (or block all) for inbound connection and to block (if no rules) for outbound connection. Disable or delete all inbound and outbound connection rules.

Create an allowing outbound connection rule with protocol UDP with ports 3074, 27000-27030, 3478, 4379, 4380, 1500, 3005, 3101, 28960 and all distant IP for all programs or only port 3074 for t6mp.exe in the folder steamlibrary and other ports for steam.exe in the folder steam (Demonware.net authentication for MW3, BO2, Ghosts, and Steam ports).

Create an allowing outbound connection rule with protocol TCP with ports 3074, 27014-27050, 80, 443 and all distant IP for all programs or only port 3074 for t6mp.exe in the folder steamlibrary and other ports for steam.exe, also the port 80 for gameoverlayUI.exe in the folder steam (Demonware.net authentication for MW3, BO2, Ghosts, and Steam ports).

Create an allowing outbound connection rule with protocol UDP with port 14010 only or ports 14000-14010, and distant IP 108.61.230.0 to 108.61.237.255 for the program t6mp.exe (BO2 servers, of domain names constant.com or choopa.net).

Create an outbound connection rule for the service Client DNS, with protocol UDP and port 53, with local IP, your internal IP, and distant IP, your DHCP and DNS server IP (shown in details of your connection properties for Ethernet).

Create two allowing inbound connection rules with protocol UDP with ports 3074-3075, 27000-27030, 3478, 4379, 4380, 1500, 3005, 3101, 28960 and all distant IP for the programs Steam.exe and t6mp.exe (not necessary).

Create two allowing inbound connection rules with protocol TCP with ports 3074-3075, 27014-27050 and all distant IP for the programs Steam.exe and t6mp.exe (not necessary).

You can replace these rules with two blocking rules in UDP and TCP by choosing to let necessary ports, and two allowing rules in TCP and UDP, for all ports (1-65535).

Allowing rules and blocking rules:

In Window properties, block all connections for inbound traffic, and block if no rules for outbound traffic, in all combo boxes of all tabs.

For outbound traffic only...

Allowing rules:

All ports for protocol TCP.

All ports for protocol UDP.

Blocking rules:

Ports 1-79, 81-442, 444-3073, 3075-27013, 27051-65535 for protocol TCP.

Ports 1-52, 54-3073, 3075-14009, 14011-26999, 27031-65535 for protocol UDP.

But it corresponds probably to servers of fragnet.net, that are game servers rents by hackers and have nothing to do with official servers of Treyarch.

Or this method:

Block all inbound rules, and block if no rules outbound rules. Then delete all inbound rules. Create allowing outbound rules as following:

A rule for the service client DNS with port 53 in UDP.

Rules for the service Steam Client Service with all ports in UDP and TCP.

Rules for steam.exe and gameoverlayUI.exe (in Steam folder) with all ports in UDP and TCP.

A rule for t6mp.exe with port 3074 in TCP.

A rule for t6mp.exe with port 3074 in UDP.

A rule for t6mp.exe with all ports and distant IP of domain name constant.com 108.61.230.2 to 108.61.230.253 in UDP (hybrid servers of BO2).

Host forcing with Windows firewall isn't a good way to enable VAC and TAC, because with all these methods explored, cheaters are always here, even those reported on their Steam profiles.

To enable VAC and TAC use Windows firewall, modem firewall and the game launch option (-secure 1). To see in the kill feed of the game "player name cheat codes detected"

(like I’ve seen it on the server of IP 195.122.135.225) and to see cheaters kicked and never be in your game, apply the following settings.

First thing to do is to set manually your IP of network connection as alternative configuration of ipv4 configuration properties of Ethernet in network properties (shown in details of your connection properties). For this, you need to know it by opening TCP and UDP outbound connection rules with all ports and all IP authorized with Windows firewall.

Or set Windows firewall as following:

Delete all inbound and outbound traffics rules with the keys delete and enter. Set Windows firewall properties to block by default and block in all combo boxes for inbound and outbound traffics.

Rules as following… protocol, distant ports, programs or services.

Inbound rules:

UDP, all, t6mp.exe. TCP, all, t6mp.exe. UDP, all, steam.exe. TCP, all, steam.exe. UDP, all, steam client service. TCP, all, steam client service. UDP, all, all services only. TCP, all, all services only. UDP, all, all application packages only. TCP, all, all application packages only.

Outbound rules:

UDP, all, t6mp.exe. TCP, all, t6mp.exe. UDP, all, steam.exe. TCP, all, steam.exe. UDP, all, steam client service. TCP, all, steam client service. UDP, all, all services only. TCP, all, all services only. UDP, all, all application packages only. TCP, all, all application packages only.

UDP, 53, client DNS. TCP, 80, 443, 27000-27050, GameoverlayUI.exe.

For modem firewall, open all ports 1-65535 to allow connections. The last thing to do is to open a nat/pat rule for all ports (1-65535) in both UDP/TCP (ports for inbound traffic allowed shown in resource monitor in listen ports for your network associate with the program steam.exe and all Windows services).

Or set rules as following:

Set a DNS server on your computer like explain in the previous chapters (OpenDNS), then use Windows firewall as following (no need to open a nat/pat rule for port 3074):

To play on official servers controlled by editors, developers and retailers in your games, you can create an IPsec strategy rule in Windows firewall like this… Go to panel control, then click on Windows firewall, then open advanced parameters, requiring administrative privilege, then click to the upper left to open the tab Security connection rules, then click to create a new rule, in the right tab, it open a window. In it, create a personalized IPsec rule (authentication inbound and outbound required), you can add in the tab distant computer in the box ending point 2, IP from 0.0.0.0 to 223.255.255.255. When it's created open the property of the rule in the middle tab, click right on the rule to open its property window. In the tab advanced, click on the button personalize for the last tab named IPsec tunnelling, in it check only the box, use tunnelling IPsec, then click ok to close. In the box ending point 1, for the tab distant computer, let all IP check box checked. In a second rule, you can add in the tab distant computer in the box ending point 1, IP from 0.0.0.0 to 223.255.255.255. In the box ending point 2, for the tab distant computer, let all IP check box checked. If you want to add a secure IPsec rule or If you don't want to create a IPsec tunnelling, you can uncheck the box use tunnelling IPsec, and add in the boxes ending point 1 and ending point 2, the IP from 0.0.0.0 to 192.168.1.1 (or your computer internal IP minus 1) and IP 192.168.1.3 (or your computer internal IP plus 1) to 223.255.255.255.

Set manually your IP of connection in ipv4 properties (only checked in your network connection properties), shown in details, in network and share center in control panel.

Set to block all inbound traffic in all comboboxes and set to block (by default) outbound traffic in all comboboxes in properties of Windows firewall.

Disable all rules, but let the one for svchost.exe with port 53 named Base network manager - DNS (UDP outbound traffic). But create a rule for the service client DNS instead

of svchost.exe with distant port 53 in UDP, to have the store of Steam, and also steamwebhelper.exe with distant ports 80 and 443.

Create outbound traffic allowing rules for public network if it's set to public:

- for Steam.exe, local ports 1024-65535, distant ports 80, 443, 27000-27050 in TCP (browse the programs exe find in the drive C:/program files (x86)/steam),

- for BO2 (t6mp.exe), local ports 1024-65535, distant port 3074 in UDP (distant IP, 209.170.124.117) and in TCP (distant IP, 209.170.124.147 and 209.170.124.209) (browse the programs exe find in the drive C:/program files (x86)/steam/steamapps/common/call of duty black ops ii),

- for BO2 with local port 3074, distant port 14140 and distant IP 108.61.230.0-108.61.239.255,

- for SteamService.exe with same rules as previously (browse the programs exe find in the drive C:/program files (x86)/Common Files/Steam).

Create outbound traffic blocking rules:

- local IP from 0.0.0.0 to 192.168.1.1 (or your computer internal IP minus 1) and IP 192.168.1.3 (or your computer internal IP plus 1) to 255.255.255.255,

- distant IP 0.0.0.0-108.61.0.0, 108.61.255.255-146.66.0.0 (let Valves IP), 146.66.255.255-173.199.0.0, 173.199.255.255-192.168.1.0 (let your modem internal IP), 192.168.1.2-195.255.255.255, 224.0.0.0-255.255.255.255 (disable this rule to have the Steam store).

For allowing rules in advanced options tab, profile network applied to your network profile (add blocking rule for other profile) and interface type applied to local access (add blocking rule for other interface).

Last method:

If problem with Windows firewall after settings, you must initialize Windows Firewall and do again what it's explain in Chapter 2 or for abstract these settings as following. Go to control panel and click on Windows firewall.

Set manually your IP of connection in ipv4 properties (only checked in your network connection properties), shown in details, in network and share center in control panel.

Set to block all traffic in all comboboxes in properties of Windows firewall. Disable all rules.

Create outbound traffic allowing rules for public network if it's set to public:

- for client DNS service, distant port 53 in UDP, distant IP your modem internal IP and primary DNS IP (find in service),
- for Steam service (find in service), Steam.exe, SteamgameoverlayUI.exe, for steamwebhelper.exe, for iexplorer.exe, distant ports 80, 443, 27000-27050 in TCP (browse the programs exe find in the drive C:/program files (x86)/steam/(bin)/ and C:/program files (x86)/Internet Explorer),
- for BO2 (t6mp.exe), distant port 3074 in UDP (distant IP, 209.170.124.117) and in TCP (distant IP, 209.170.124.147 and 209.170.124.209) (browse the programs exe find in the drive C:/program files (x86)/steam/steamapps/common/call of duty black ops ii).

Set one of the inbound allowing rules always added after verify game cache files, for BO2 with local port 3074, all distant ports and distant IP 195.122.134.0 to 195.122.135.255 (not own by "Gameservers" on speedguide.net and on http://bgp.he.net/ but Level 3 communications), for public network only. Delete all other inbound allowing traffic rules, even those adds each time you verify game cache files or updates.

For find a match, you must set on your modem a nat/pat rule for port 3074 in UDP and in TCP.

The outbound traffic rule is for connection at an IP, and inbound traffic rule is for connection from a server. It prevents to be connected to a server own by a cheater on his computer. There is far less servers find with this method, so it must prevent to be connected to a hacked lobby.

If you have another computer to be on the page on your modem, you can disable the nat/pat rule for port 3074 in UDP, just before you connect to the match, after match was find.

SteamgameoverlayUI.exe is for report cheaters from their Steam profiles (also for block cheaters from your games).

Also create outbound rules for ports 80 and 443 in TCP in Windows firewall for Windows updates service, WinDefend service, the program mbam.exe…

Create outbound and inbound blocking rules:

For inbound and outbound traffic rules, block all services and block exe programs shown in task manager (open with ctrl+shift+esc) like audiodg, csrss, dllhost, dwm, explorer, lsass, msmpeng, ntoskrnl, services, smss, svchost, taskhostex, taskmgr, wininit, winlogon, wmiprvse, rundll32, mmc.exe, mbamgui, mbamservice (click right on the files in task manager to open the folder and see where the files are). Also, create blocking inbound and outbound rules for all programs, all services, all protocols, all ports, all local IP and distant IP 0.0.0.0 to 146.0.0.0.

Disable the blocking outbound traffic rules for all services and svchost only for authentication into BO2, before searching a match, and for downloads on Steam, and for report cheaters from their Steam profiles with SteamgameoverlayUI.exe (but on VAC secure servers it's not necessary normally), and for Steam updates. Then enable all these rules for playing. But after authentication into BO2, before searching a match, in chapter 2, it was possible to disable the allowing rule for t6mp.exe, port 3074 in UDP, distant IP,

209.170.124.117, for find a match, now it’s not, so let this rule. Navigate between windows with Alt+tab, Alt+F4 to close the windows, and Alt+enter to full screen your games.

For Windows Firewall again, add Local IP, your internal IP like 192.168.1.2 and allowing user "local account" in the tab security of local entity to all allowing rules.

Lasting by open connections on your modem for only ports 80, 443, 27000-27030 (TCP), 53 (TCP/UDP) and 27014-27050 (UDP), and for BO2, only IP 209.170.124.209, 209.170.124.216 (TCP) and 209.170.124.113 (UDP) for port 3074. And also open a nat/pat rule for all ports to allow inbound traffics for these connections.

The IP 209.170.124.113 (UDP) shall be closed on your modem after connection into the game and before searching a match, because this IP in the protocol UDP isn’t safe, and can be used more than a single time. It prevent to not be forwarded into hacked lobbies.

Maybe, you can create blocking inbound and outbound traffic rules for all the files named svchost.exe, in the folder Windows, with Windows firewall because malicious web site detected by malwarebytes antimalwares, attempt to enter your computer through this exe. To download files with Steam and update malwarebytes antimalwares on port 80, you must disable the rule for svchost.exe in the folder Windows/System32. But also block all inbound traffic (set the firewall properties to always or all block in textboxes of inbound connection, and to block (by default) for all texboxes of outbound connection in Windows firewall properties), and block services like SSDPSRV (PID in resource monitor, and name in task manager to open with keys ctrl+shift+esc), or programs like rundll, dllhost, csrss, dwm, lsass, winlogon, taskhost, explorer, ntoskrnl... Also create an IPsec rule with require authentication for inbound and ask authentication for outbound. It prevent hackers incomes like black screen freeze when you playing. Also, and it’s important, create blocking rules for all programs and all services, for distant IP between 195.0.0.0 to 195.255.255.255 because BO2 servers on these IP are full of cheaters, it correspond to public IP own by users like you and me, so it’s

servers of hacked lobbies with cheaters never banned or banned but still playing (you can know what IP you are connected with resource monitor in administration tool, from control panel, by watching in the tab network, in network activity, it correspond to the maximum of sending packets when you playing. You can know if an IP is owned by a user or by servers retailers when typing the IP and see the information in speedguide.net). The best thing to do is to create only specific allowing rules, in Windows firewall, for steam.exe, steamclientservice.exe, client DNS service and t6mp.exe in TCP and UDP, but for UDP you can add only distant IP shown in resource monitor like for t6mp.exe (BO2 authentication) 209.170.124.117, 209.170.124.147, 209.170.72.124 and only distant IP of BO2 servers like 93.93.64.0/21 or other IP shown in resource monitor for both ntoskrnl.exe (System) and BO2 (t6mp.exe), because when IP interacts with System, it's authentic IP. To browse windows, press Alt+Tab, close windows with Alt+F4, and full screen windows with Alt+Enter. Disable the blocking rules for svchost.exe in Windows/Sytem32 and all services for BO2 authentication. Create shortcuts for resource monitor, Windows firewall and BO2.

It's very important to create IPsec strategy rule (authentication inbound and outbound required) with all protocols, and all ports, with distant IP: 95.141.0.0 to 95.141.255.255, 195.122.0.0 to 195.122.255.255, 93.93.0.0 to 93.93.255.255, 189.1.0.0 to 189.1.255.255, 108.61.0.0 to 108.61.255.255, 197.80.0.0 to 197.80.255.255, 197.84.0.0 to 197.84.255.255, 173.199.0.0 to 173.199.255.255. To find servers you must create a tunnelling IPsec in the tab advanced, check boxes use tunnelling IPsec, apply authentication, and remove connections protected by IPsec, then click the button ok, and apply. For more security, when you create a personalized IPsec rule (authentication inbound and outbound required), you can add in the tab distant computer in the box ending point 2, IP from 0.0.0.0 to 223.255.255.255 and check only the box, in the tab advanced, use tunnelling IPsec. In the box ending point 1, let all IP check box checked. Normally, BO2 servers IP Between 195.122.0.0 to 195.122.255.255 will

not appear in resource monitor when you search a server. Maybe these IP forwards on hacked lobbies.

3.4. Against lag switching

First thing, is to allow Windows update automatically and have the license of the anti-virus with your computer. Then, let by default, the Windows firewall settings. Then checking Regedit entries and files suspicious like explained on the following page:

http://www.symantec.com/connect/articles/most-common-registry-key-check-while-dealing-virus-issue

“

1) StartUp

C:\windows\start menu\programs\startup

* [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders]

Startup="C:\windows\start menu\programs\startup"

* [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders]

Startup="C:\windows\start menu\programs\startup"

* [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\User Shell Folders]

"Common Startup"="C:\windows\start menu\programs\startup"

* [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Shell Folders]

"Common Startup"="C:\windows\start menu\programs\startup"

"Anything over here execute when you start up your computer"

2) Windows Scheduler:

Check for entries in the Scheduled Tasks, as well as via the AT command at a command prompt.

3) c:\windows\winstart.bat

'It basically behaves like a normal batch file, then only difference is that it can be used to delete files when you start up your computer

4) Registry :

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]

"Whatever"="c:\runfolder\program.exe"

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]

"Whatever"="c:\runfolder\program.exe"

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

"Whatever"="c:\runfolder\program.exe"

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]

"Whatever"="c:\runfolder\program.exe"

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

"Whatever"="c:\runfolder\program.exe"

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]

"Whatever"="c:\runfolder\program.exe"

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]

"Whatever"="c:\runfolder\program.exe"

5) "Autoexec.bat"

6) These reg keys will basically spawn your programs, as you can see this is very dangerous because these keys are very used by viruses and Trojans.

[HKEY_CLASSES_ROOT\exefile\shell\open\command] @="\"%1\" %*"

[HKEY_CLASSES_ROOT\comfile\shell\open\command] @="\"%1\" %*"

[HKEY_CLASSES_ROOT\batfile\shell\open\command] @="\"%1\" %*"

[HKEY_CLASSES_ROOT\htafile\Shell\Open\Command] @="\"%1\" %*"

[HKEY_CLASSES_ROOT\piffile\shell\open\command] @="\"%1\" %*"

[HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\command] @="\"%1\" %*"

[HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command] @="\"%1\" %*"

[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command] @="\"%1\" %*"

[HKEY_LOCAL_MACHINE\Software\CLASSES\htafile\Shell\Open\Command] @="\"%1\" %*"

[HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\command] @="\"%1\" %*"

The key should have a value of Value "%1 %*", if this is changed to "server.exe %1 %*", the server.exe will be executed EVERYTIME an exe/pif/com/bat/hta is executed.

7) Explorer start-up

The problem with these operating systems is that they look for a file called "explorer.exe" whenever you start up your computer, that file is basically the one that you see all the time but don’t realize it is there , if you go to your taskmanager you can see it, you can even kill it and you will see that everything in your computer that belongs to Microsoft will disappear, except for the extra windows that you open such as cmd, regedit, services.msc etc, but your desktop will be gone. As you can see this is dangerous because it also means that if somebody modify your explorer.exe file then your computer will be corrupted. In fact, to change the name of the

start bottom has to be done by modifying the explorer.exe file, so there is a clue of a small difference that can have an effect in your computer.

here is the key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

if a Trojan changes that to a path of another "infected explorer.exe file" your computer will start up the file the Trojan told it to and not the one used by Microsoft.

8)"Active-X Component"

[HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\KeyName]

StubPath=C:\PathToFile\Filename.exe

This key is great because it starts the program that it has in its path BEFORE the explorer.exe file and any other program starts in your computer, so if you can understand why your antivirus can't detect the virus when you boot up, it is maybe because your "virus" is taking care of it before it starts up. It could even kill your antivirus before your antivirus starts up.“

Because wallhackers and aimboters are so noobs, they lag switch the player aim in Black Ops 2. Lag switch is the worst hack made by hackers, because you totally can't fire wallhackers and aimboters. If these cheaters doesn't lag switch your aim, it's still easy to kill these big noobs. The solution is to set work station properties of port COM or disable it. To do it:

Open panel control, then go to admin tool, then open component services, in the left tab, double click on my computer, then click right on work station in the main tab, and click properties. It open a window named work station properties, In the tab options, set 0 to the transaction delay, in the tab, default properties, uncheck enable distributed COM, in the tab com security, click on each buttons to set allow local user and block distant user by checking boxes. WARNING: Take care to be able to open panel control again before close work station

properties window. Click apply, and not ok, and verify if you can open control panel and work station window, otherwise you must reboot fresh your entire PC. You can add users to block distant access by clicking on add, then advanced, then search, then by push shift and click left for add all users, after each user is set to allow local user and block distant user by checking boxes. This isn't recommended. If you have a problem with your computer, you can reset it by push shift key and click restart computer. It will open advanced start with refresh options.

Cheat programs of hackers can lag mouse events on your own computer like your mouse moves alone in a false direction, different of where you aim. For a counter measure, don't trust TrustInstaller, the owner of files that can do switch lag. The cheat programs use the files crypt32.dll, cryptnet.dll, psapi.dll, GDI32.dll, ole32.dll, shell32.dll, and shlwapi.dll in Windows\System32 and Windows\SysWOW64. Click right on these files, then click left property, then in the security tab, you can change owner TrustInstaller with Users by an advanced research, then uncheck all the controls for TrustInstaller, Administrators, Application Packages… and check all the controls for Users and apply changes.

To disable virtual memory, open the "Control Panel then open System and open the Advanced tab, then click on Performance Settings button to open the Performance Options window. In the Advanced tab, open Virtual Memory section. Click the Change button in order to launch the virtual memory settings window. Select No Paging File option and click on Set button, then apply and restart your computer.

Open launching options of Black Ops II in Steam library property options of the game, then type in the box of launch options -secure 1. If you can't connect to the game, create outbound rules in TCP and UDP for the port 3074 and all distant IP.

Use cmd.exe in c:/Windows/System32/ to allocate bytes for memory addresses. The following options with explanations comes from the site with this link:

http://msdn.microsoft.com/en-us/library/ff542202.aspx

“ nx [Optin |OptOut | AlwaysOn |AlwaysOff]

AlwaysOn

Enables DEP for the operating system and all processes, including the Windows kernel and drivers. All attempts to disable DEP are ignored.

bcdedit /set {current} nx AlwaysOn

xsavedisable [0 | 1]

When set to a value other than zero (0), disables XSAVE processor functionality in the kernel.

bcdedit /set {current} xsavedisable 1

tpmbootentropy [default | ForceEnable | ForceDisable]

Determines whether entropy is gathered from the trusted platform module (TPM) to help seed the random number generator in the operating system.

bcdedit /set {current} tpmbootentropy ForceEnable

truncatememory address

Limits the amount of physical memory available to Windows. When you use this option, Windows ignores all memory at or above the specified physical address. Specify the address in bytes.

For example, the following command sets the physical address limit at 1 GB. You can specify the address in decimal (1073741824) or hexadecimal (0x40000000).

bcdedit /set {current} truncatememory 0x80000000

nolowmem [on | off]

Controls the use of low memory. When nolowmem on is specified, this option loads the operating system, device drivers, and all applications into addresses above the 4 GB boundary

bcdedit /set {current} nolowmem on

groupaware [on | off]

The groupaware on setting ensures that processes are started in a group other than group 0

bcdedit /set {current} groupaware on

hypervisordhcp [yes | no]

Controls use of DHCP by the network debugger used with the hypervisor

bcdedit /set {current} hypervisordhcp no

hypervisorlaunchtype [Off | Auto]

Controls the hypervisor launch options

bcdedit /set {current} hypervisorlaunchtype Off

hypervisoruselargevtlb [yes | no]

Increases virtual Translation Lookaside Buffer (TLB) size.

bcdedit /set {current} hypervisoruselargevtlb no

hypervisoriommupolicy [default | enable | disable]

Controls whether the hypervisor uses an Input Output Memory Management Unit (IOMMU).

bcdedit /set {current} hypervisoriommupolicy disable

usefirmwarepcisettings [yes | no]

Enables or disables the use of BIOS-configured peripheral component interconnect (PCI) ressources

bcdedit /set {current} usefirmwarepcisettings no

uselegacyapicmode [yes | no]

Used to force legacy APIC mode, even if the processors and chipset support extended APIC mode.

bcdedit /set {current} uselegacyapicmode no

x2apicpolicy [enable | disable]

Enables or disables the use of extended APIC mode, if supported. The system defaults to using extended APIC mode if it is available.

bcdedit /set {current} x2apicpolicy disable

pciexpress [default | forcedisable]

Enables or disables PCI Express functionality

bcdedit /set {current} pciexpress forcedisable

pae [Default | ForceEnable | ForceDisable]

Enables or disables Physical Address Extension (PAE). When PAE is enabled, the system loads the PAE version of the Windows kernel.

bcdedit /set {current} pae ForceDisable

Enable Driver Signature Enforcement (DSE)

bcdedit.exe -set TESTSIGNING OFF

bcdedit.exe -set NOINTEGRITYCHECKS OFF

To delete a boot option value that you have set, use the /deletevalue option

To view the current boot entries and their settings, use the bcdedit /enum command

Open regedit with execute, then change these values but take care when changing values:

PagedPoolSize and NonPagedPoolSize

This registry key determines the number of bytes allocated to the paged pool

set the following registry value to 0x40000000:

Registry path

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PagedPoolSize

set the following registry value to 0x10000000:

Registry path

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\NonPagedPoolSize

AllocationPreference

To force allocations to allocate from higher addresses before lower addresses for testing purposes

set the following registry value to 0x100000:

Registry path

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\AllocationPreference

“

If you don't have sound anymore with the regedit value AllocationPreference, you shall initialize parameters options in BO2.

After it, is to enter the bios, in the bios, you can switch the primary display/video in advanced chipset features to PCIE graphic card, in order to disabling the virtual memory and access rights by users to physical memory. Also, you can disable memory remap features above 4 GB. After it, to disable virtual memory, go in System properties tab, through the panel control, click on the box performance, then in the tab advanced, click on the box virtual memory, then uncheck the box named automatically manage exchange files, then check the box no exchange file, and click the box define. You must restart your computer to apply the changes.

Finally, to add somes features for your computer, like enable ASLR, and enable the preferred allocation type for virtual memory management use these following regedit values:

Open regedit with execute tool and change

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

PhysicalAddressExtension 0x00000000

SessionPoolSize 0x00000000

SessionViewSize 0x00000000

MoveImages 0x00100000

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems

change Windows key:

%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,5120,2048 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16

The only thing to change is "SharedSection=1024,5120,2048" instead of "SharedSection=1024,20480,768".

Some regedit entries for t6mp are unjustified, so you can delete somes of entries with t6mp.exe as data within (you can save the regedit table with the button Export). Search the name t6mp in regedit and delete the values and the keys if necessary. Then to apply the change, you need to restart your computer. To open regedit, type regedit in the accessory run, and click ok. Other regedit entries for Windows firewall are unjustified too. Search the term Action=Allow| to find the entries and change Active=TRUE| by Active=FALSE| (with double clicks to replace the exact terms) or add Active=FALSE| for all values of keys but let the values you set in Windows firewall like those explained below. It's possible that these regedit entries are an open door to hackers to be able to throw you into their hacked lobbies where cheaters still can play even if they are VAC banned.

Put all regedit values of ServiceDllUnloadOnStop to 0. It avoid a dll to take account as a service.

To protect your computer to attacks,

set the EnableICMPRedirect DWORD value to 0 in the registry key

HKLM\System\CurrentControlSet\Services\AFD\Parameters

HKLM\System\ControlSet001\Services\AFD\Parameters

and set the AllowNetworkAccess value to 0 in the registry key

HKLM\System\CurrentControlSet\Services\RemoteAccess\Parameters\IP

HKLM\System\CurrentControlSet\Services\RemoteAccess\Parameters\Ipv6

HKLM\System\CurrentControlSet\Services\RemoteAccess\Parameters\Nbf

HKLM\System\ControlSet001\Services\RemoteAccess\Parameters\IP

HKLM\System\ControlSet001\Services\RemoteAccess\Parameters\Ipv6

HKLM\System\ControlSet001\Services\RemoteAccess\Parameters\Nbf

and clean the entries

HKLM \ System \ControlSet001\Services\Dnscache\Parameters\Probe

HKLM \System\CurrentControlSet\Services\Dnscache\Parameters\Probe

Execute regedit with the exe command, and add the line for

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session

Manager\Memory Management] "MoveImages"=dword:ffffffff. It's to enable Address Space Layout Randomization (ASLR).

To the registry key for enable ASLR in:

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\

When you add the DWORD 32 bits value "MoveImages" you can allocate a hex value of fffffffe instead of ffffffff, otherwise CoD AW will not start. But you must set 0 if you want to play CoD BO2, otherwise it will not start.

In the bios, you can switch the primary display/video in advanced chipset features to PCIE graphic card, in order to disabling the shared memory.

3.5. Modem security

Open a NAT/PAT rule in your modem for the port 3074 associate with your computer. If you don't want to open a NAT/PAT rule, you can open the ports between 10000 and 16000

in UDP on your modem firewall but you will be forwarded on fake servers with fake players already banned and cheating. Use the firewall of your modem with the following rules in this picture

Règles personnalisées

Application / Service	Protocole	Adresse de l'IP source	Adresse du masque IP	Port source (Saisir un numéro ou une plage de port (ex: 200-300))	Adresse de l'IP destination	Adresse du masque IP	Port destination (Saisir un numéro ou une plage de port (ex: 200-300))
HTTP	TCP			1024-6553			80
HTTPS	TCP			1024-6553			443
FTP	TCP			1024-6553			21
FTP-Data	TCP			1024-6553			20
DNS	Tous			1024-6553			53
Telnet	TCP			1024-6553			23
SSH	TCP			1024-6553			22
IMAP	TCP			1024-6553			143
IMAPS	TCP			1024-6553			993
POP3	TCP			1024-6553			110
POP3S	TCP			1024-6553			995
SMTP	TCP			1024-6553			25
SMTP-Auth	TCP			1024-6553			587
NNTP	TCP			1024-6553			119
NTP	UDP			1024-6553			123
Ping	Tous						
UNIK	Tous						
steam udp	UDP			1024-65535			27000-270
steam tcp	TCP			1024-65535			27014-270
steam1	UDP			1024-65535			4380
st2	UDP			1024-65535			3478
st3	UDP			1024-65535			4379
st4	UDP			1024-65535			28960
st5	UDP			1024-65535			1500
st6	UDP			1024-65535			3005
st7	UDP			1024-65535			3101
bo2a	TCP			1024-65535	209.170.122.109		3074
bo2b	TCP			1024-65535	209.170.124.113		3074
bo2c	TCP			1024-65535	209.170.124.209		3074
bo2d	TCP			1024-65535	209.170.124.216		3074
bo2e	TCP			1024-65535	209.170.124.147		3074

Also, you can add the IP of free Norton DNS server for primary and secondary DNS server on your modem and your computer, in the alternative configuration network of advanced properties ipv4 (without adding IP of WINS server, you just have to copy some of the details of your network connection) for increasing security and avoid phishing IP and information hacks. Also add the IP of DNS server manually. To the default list in the table above, you must open on your modem, the Steam forwarding ports as 27014-27050, 3074 (209.170.122.109, 209.170.124.113, 209.170.124.209, 209.170.124.216, 209.170.124.147), 80, 443 in TCP, and 27000-27030, 3074 (209.170.124.113) for authentication only (disable

for searching a match), 3478, 4379, 4380, 1500, 3005, 3101, 28960, 53 in UDP, then you must open a nat/pat rule on your modem for the port 3074 in TCP/UDP. But only ports 80, 443, 53 and 3074 (209.170.122.109, 209.170.124.113, 209.170.124.209, 209.170.124.216, 209.170.124.147) are required for your computer (internal IP shown in details in Ethernet properties of network panel control). You can add the distant subnet mask IP 255.0.0.0 for 3074 and 27000-27050 ports.

On the firewall of your modem, you need only ports 80 (http protocol), 443 (https protocol), 27014-27050, 3074 (external IP 209.170.124.209 and 209.170.124.216) in TCP, and ports 53 (DNS protocol, external IP of your modem address as 192.168.1.1), 3074 (209.170.124.113), in UDP for connection into the game that you shall disable both when searching a match (but it isn't necessary to disable). You must add the external subnet mask IP 255.0.0.0 for 3074 and 27014-27050 ports. With it, you will not be forwarded on unsecure hacked lobbies, if Steam, Activision and Treyarch do their works. But it isn't a good way because cheaters are always in the game even those reported.

3.6. Steam in secure mode

Some players meet issues when connecting to Counter-Strike secure servers. The game is disconnected from the servers and advertises that you are in insecure mode or VAC secure mode disabled. Some players have just to launch the game from Steam library, or delete the game launch options for the game, or disable steam community overlay with the options in the properties of the game in Steam Library. Players contacting steam support find the solution for being able to play on secure servers by doing this:

Download Steam on http://store.steampowered.com, uninstall Steam, and then install Steam by choosing to replace the installation on the root C:\Steam, instead of C:\Program Files\Steam. The files of your games library aren't lost when installing games in the folder

SteamLibrary on the root you choose, if you installed your games the first time by choosing the root, if you follow the steps of installation when you install again your games.

Specify the launch options by typing -secure 1 +sv_lan 1 -white 1 -VAC 1 -linux 0 -type d -noplayers 1 -proxy 1 -napp [202990] -sv_pure 2 +cl_restrict_server_commands 2, in the window of launch options in the property window of the game, when you click right on the game name in Steam library.

In the folder Steam/userdata/(number)/config for the file serverbrowser change “appid“ “202990“ and “secure“ “1“ and in the folder Steam/userdata/(number)/7/remote for the file sharedconfig change “cloudenabled“ “0“ “secure“ “1“, then click right on these files, click on properties, and check the box readonly, and apply.

The most important Steam and Game Launch Options put in the target shortcut of Steam.exe and t6mp.exe (BO2) are -secure 1 -VAC 1 –white -linux 0 -type d -noplayers 1 -proxy 1 -sv_pure 2. Define Game Launch Options as following Steam Library -> Right click on game name -> click left properties -> First tab -> Define game launch options. Game Launch Options are find on valves developper site and are used to :

-secure 1 (use in L4D to connect a VAC secure server)

+sv_lan 1 (Authentication required to connect to a server)

-white 1 (connection to a white listed server)

-VAC 1 (enable VAC for playing on secure servers)

-linux 0 (avoid connection on linux servers, as Bazaar servers)

-type d (playing on dedicated servers)

-noplayers 1 -empty 0 (multiply and open servers with an empty lobby)

-proxy 1 (enable spectators as pc_dev_assist)

-napp [202990] -tcp (steam launch options, the best way to)

-sv_pure 2 (all players with same game files)

+cl_restrict_server_commands 2 (restrict command consoles)

Maybe Activision uses linux servers, but the game launch options is a solution to explore.

On Steam support, you can read the following writes about enabling VAC:

"An issue with your computer is blocking the VAC system. You cannot play on secure servers

How do I fix this?

Enable DEP

Data Execution Prevention (DEP) must be enabled to play on VAC secured servers. To restore DEP settings to default please follow the steps below:

Exit Steam.

Click the Start button, then 'All Programs', and 'Accessories'

Right-click on Command Prompt and click "Run as administrator..."

- Please note if you are running Windows 8 you will need to press Windows Key + X and select Command Prompt (Admin)

In the command prompt, type the following command and press Enter:

bcdedit.exe /deletevalue nx

Restart your computer.

Launch Steam and test the issue again.

Restart your computer

If this is a problem for you on all servers then you can try fixing this problem by exiting Steam and restarting your computer.

Repair the Steam Service

This may also indicate a Steam Service failure. Please try repairing the Steam Service:

Exit Steam.

Click Start > Run (Windows Key + R)

Type the following command:

"C:\Program Files (x86)\Steam\bin\SteamService.exe" /repair

(If you have installed Steam to another path, please replace C:\Program Files (x86)\Steam with the correct path.)

This command requires administrator privileges and may take a few minutes.

Launch Steam and test the issue again.

Conflicting Software

This issue can be caused by third party software interfering with your game or Steam. Please restart your computer, and then launch Steam and the game without running any other third party software."

Source https://support.steampowered.com/kb_article.php?ref=2117-ILZV-2837

Open task manager, in detail tab, end the task for explorer.exe, then click on file in upper left, click new task, type explorer.exe and check the box run with administrative privilege, then click ok. It's used if your game blocks your access to VAC servers. Also it's important to update the Windows time if it's wrong.

To enable VAC in CoD AW do as following

Add or change in configuration file config_mp: seta cheats "0"seta net_noipx "1"seta net_notcp "1"seta net_secure "1"seta net_sv_private "0"seta net_sv_pure "1"seta net_svprivate "0"seta net_vac "1"seta notcp "1"seta secure "1"seta svprivate "0"seta svpure "1"seta vac "1"seta ui_joinGametype "0"seta ui_netGametype "0"seta ui_netGametypeName "dm"seta ui_netSource "1".

Your game configuration file of CoD AW must look like:

// generated by Sledgehammer Games - do not modifyseta cg_blood "1"seta cg_brass "1"seta cg_chatHeight "4"seta cg_chatTime "12000"seta cg_connectionIconSize "0"seta cg_cursorHints "4"seta cg_descriptiveText "1"seta cg_drawBreathHint "1"seta cg_drawBuildName "0"seta cg_drawDoubleTapDetonateHint "1"seta cg_drawFPSLabels "1"seta cg_drawMantleHint "1"seta cg_drawSnapshot "0"seta cg_drawStatsSource "0"seta cg_drawTurretCrosshair "1"seta cg_drawVarGrenadeHint "1"seta cg_drawViewpos "0"seta

cg_fov "65"seta cg_gameBoldMessageWidth "390"seta cg_gameMessageWidth "455"seta cg_headIconMinScreenRadius "0.025"seta cg_hintFadeTime "100"seta cg_hudChatIntermissionPosition "5 110"seta cg_hudChatPosition "5 200"seta cg_hudProneY "-160"seta cg_hudSayPosition "5 175"seta cg_hudVotePosition "5 220"seta cg_invalidCmdHintBlinkInterval "600"seta cg_invalidCmdHintDuration "1800"seta cg_mapLocationSelectionCursorSpeed "0.6"seta cg_marks_ents_player_only "0"seta cg_paintballFx "0"seta cg_scriptIconSize "0"seta cg_sprintMeterDisabledColor "0.8 0.1 0.1 0.2"seta cg_sprintMeterEmptyColor "0.7 0.5 0.2 0.8"seta cg_sprintMeterFullColor "0.8 0.8 0.8 0.8"seta cg_subtitleMinTime "3"seta cg_subtitleWidthStandard "520"seta cg_subtitleWidthWidescreen "520"seta cg_teamChatsOnly "0"seta cg_viewZSmoothingMax "16"seta cg_viewZSmoothingMin "1"
seta cg_viewZSmoothingTime "0.1"seta cg_voiceIconSize "0"seta cg_waterSheeting_distortionScaleFactor "0.021961 1 0 0"seta cg_waterSheeting_magnitude "0.0655388"seta cg_waterSheeting_radius "4.44051"seta cg_weaponCycleDelay "0"seta cg_youInKillCamSize "6"seta cl_freelook "1"seta cl_maxPing "800"seta cl_mouseAccel "0"seta cl_packetdup "2"seta cl_pitchspeed "140"seta cl_pushToTalk "0"seta cl_textChatEnabled "0"seta cl_voice "0"seta cl_yawspeed "140"seta com_recommendedSet "1"seta compassSize "1"seta con_gameMsgWindow0FadeInTime "0.25"seta con_gameMsgWindow0FadeOutTime "0.5"seta con_gameMsgWindow0Filter "gamenotify obituary"seta con_gameMsgWindow0LineCount "4"seta con_gameMsgWindow0MsgTime "5"seta con_gameMsgWindow0ScrollTime "0.25"seta con_gameMsgWindow1FadeInTime "0.25"seta con_gameMsgWindow1FadeOutTime "0.5"seta con_gameMsgWindow1Filter "boldgame"seta con_gameMsgWindow1LineCount "1"seta con_gameMsgWindow1MsgTime "3"seta con_gameMsgWindow1ScrollTime "0.25"seta con_gameMsgWindow2FadeInTime "0.75"seta con_gameMsgWindow2FadeOutTime "0.5"
seta con_gameMsgWindow2Filter "subtitle"seta con_gameMsgWindow2LineCount "7"seta con_gameMsgWindow2MsgTime "5"seta con_gameMsgWindow2ScrollTime "0.25"seta con_gameMsgWindow3FadeInTime "0.25"seta con_gameMsgWindow3FadeOutTime "0.5"seta con_gameMsgWindow3Filter ""seta con_gameMsgWindow3LineCount "5"seta con_gameMsgWindow3MsgTime "5"seta con_gameMsgWindow3ScrollTime "0.25"seta con_typewriterColorGlowCheckpoint "0.6 0.5 0.6 1"seta con_typewriterColorGlowCompleted "0 0.3 0.8 1"seta con_typewriterColorGlowFailed "0.8 0 0 1"seta con_typewriterColorGlowUpdated "0 0.6 0.18 1"seta con_typewriterDecayDuration "700"seta con_typewriterDecayStartTime "6000"seta con_typewriterPrintSpeed "50"seta dynEnt_active "1"seta fx_flare "1"seta fx_marks "0"seta fx_marks_ents "1"seta fx_marks_nearlimit "5"seta fx_marks_smodels "1"seta g_allowvote "1"seta g_banIPs ""seta g_clonePlayerMaxVelocity "80"seta g_deadChat "1"seta g_dropForwardSpeed "10"seta g_dropHorzSpeedRand "100"seta g_dropUpSpeedBase "10"seta g_dropUpSpeedRand "5"seta g_playerCollisionEjectSpeed "25"seta g_voiceChatTalkingDuration "500"seta gpad_menu_scroll_delay_first "420"seta gpad_menu_scroll_delay_rest_accel "2"seta gpad_menu_scroll_delay_rest_end "50"seta gpad_menu_scroll_delay_rest_start "210"seta hud_deathQuoteFadeTime "1000"seta hud_enable "1"seta hud_fade_ammodisplay "0"seta hud_fade_healthbar "2"seta hud_fade_offhand "0"seta hud_fade_sprint "1.7"seta hud_flash_period_offhand "0.5"seta hud_flash_time_offhand "2"seta hud_health_pulserate_critical "0.5"seta hud_health_pulserate_injured "1"seta hud_health_startpulse_critical "0.33"seta hud_health_startpulse_injured "1"seta in_mouse "1"seta intro "0"seta lui_hud_motion_enabled "1"seta m_filter "0"seta m_forward "0.25"seta m_pitch "0.022"seta m_side "0.25"seta m_yaw "0.022"seta monkeytoy "0"seta net_nomaster "1"seta net_noudp "0"seta net_secure "1"seta net_socksEnabled "1"seta net_socksPassword ""seta net_socksPort "3075"seta net_socksServer "209.170.124.117"seta net_socksUsername

""seta net_sv_private "0"seta net_sv_pure "2"seta net_sv_usedevshotsfile "1"seta net_vac "1"seta r_aaMaxQuality "0"seta r_aaSamples "1"seta r_adapter "NVIDIA GeForce GTX 750"seta r_aspectRatio "auto"seta r_autoPriority "0"seta r_blacklevel "0"seta r_debugLineWidth "1"seta r_depthPrepass "None"seta r_dlightForceLimit "8"seta r_dof_limit "0"seta r_drawWater "1"seta r_elevatedPriority "0"seta r_fill_texture_memory "0"seta r_floatZCopy "0"seta r_fullscreen "1"seta r_fullscreenWindow "0"seta r_glow_allowed "0"seta r_image_cache_copy_memory_budget "0"seta r_image_cache_copy_number_budget "0"seta r_image_cache_create_memory_budget "0"seta r_image_cache_delay_ms "5"seta r_image_cache_delete_until_available "0"seta r_image_cache_keep_lower_mips "0"seta r_image_cache_make_staging_texture "0"seta r_image_cache_mass_remove_threshold "67108864"seta r_image_cache_throttle_ms "50"seta r_imageQuality "0"seta r_inGameVideo "1"seta r_lodBiasRigid "0"seta r_lodBiasSkinned "0"seta r_lodScaleRigid "1"seta r_lodScaleSkinned "1"seta r_mdaoLimit "2"seta r_mode "1024x768"seta r_monitor " DTV "seta r_picmip "3"seta r_picmip_bump "3"seta r_picmip_spec "3"seta r_picmip_water "0"seta r_portalBevels "0.7"seta r_postAA "None"seta r_preloadShaders "0"seta r_preloadShadersELL "0"seta r_preloadShadersELLMLLT "-1"seta r_preloadShadersELLMSPT "-1"seta r_preloadShadersWNDTOO "1"seta r_refreshRate "60.00 Hz"seta r_ssaaSamples "1"seta r_ssaoLimit "0"seta r_sssLimit "1"seta r_texFilterAnisoMax "4"seta r_texFilterAnisoMin "1"seta r_uav_overlap "1"seta r_videoMemoryScale "1"seta r_vsync "0"seta ragdoll_enable "1"seta ragdoll_max_simulating "32"seta ragdoll_mp_limit "16"seta ragdoll_mp_resume_share_after_killcam "3000"seta rate "25000"seta secure "1"seta sensitivity "1.4"seta server1 ""seta server10 ""seta server11 ""seta server12 ""seta server13 ""seta server14 ""seta server15 ""seta server16 ""seta server2 ""seta server3 ""seta server4 ""seta server5 ""seta server6 ""seta server7 ""seta server8 ""seta server9 ""seta sm_cacheSpotShadows "Disabled"seta sm_cacheSunShadow "Disabled"seta sm_enable "0"seta sm_maxLightsWithShadows "4"seta sm_sunShadowScaleLocked "1"seta sm_tileResolution "Auto"seta snd_cinematicVolumeScale "0.6"seta snd_enableEq "1"seta snd_envFollowerBuffScale "1"seta snd_errorOnMissing "0"seta snd_speakerConfig "0"seta snd_touchStreamFilesOnLoad "0"seta snd_volume "1"seta sv_hostname "CoD4Host"seta sv_nomaster "1"seta sv_publicbuild "1"seta sv_usedevshotsfile "1"seta sys_configSum "254862036"seta sys_configureGHz "12.004"seta sys_gpu "NVIDIA GeForce GTX 750 (0x10de, 0x1381, 0x84c21043, 0xa2, 0x7c6cf000); Microsoft Basic Render Driver (0x1414, 0x8c, 0, 0, 0)"seta sys_sysMB "8145"seta ui_autodetectGamepad "1"seta ui_bigFont "0.4"seta ui_browserFriendlyfire "0"seta ui_browserKillcam "0"seta ui_browserMod "0"seta ui_browserShowDedicated "0"seta ui_browserShowEmpty "0"seta ui_browserShowFull "0"seta ui_browserShowPassword "0"seta ui_browserShowPure "1"seta ui_browserShowSecure "1"seta ui_browserShowVAC "1"seta ui_currentFeederMapIndex "0"seta ui_currentMap "0"seta ui_drawCrosshair "1"seta ui_extraBigFont "0.55"seta ui_joinGametype "0"seta ui_netGametype "0"seta ui_netGametypeName "dm"seta ui_netSource "1"seta ui_serverStatusTimeOut "7000"seta ui_smallFont "0.25"seta vid_height "741"seta vid_width "1020"seta vid_xpos "265"seta vid_ypos "1"seta winvoice_mic_mute "0"seta winvoice_mic_outTime "0.5"seta winvoice_mic_reclevel "65535"seta winvoice_mic_scaler "1"seta winvoice_mic_threshold "3276.8"seta winvoice_save_voice "0"

Type in cmd command prompt run as administrator lines:

bcdedit.exe /set {current} nx AlwaysOn

bcdedit /set {current} nointegritychecks off

bcdedit /deletevalue loadoptions.

Enable DEP in system in control panel, select advanced tab and click on settings under performance section, select the tab DEP and click on Turn on for all programs and services.

Run Steam as administrator. You can set it in properties of the shortcut icon.

Check if the services EAF and IPsec are enables and runing.

3.7. Network configuration

You can add free DNS server Comodo as primary DNS and free DNS server Norton as secondary DNS for more security. Port Reporter exe is a service made by Microsoft Technet as EMET mitigation tool. You must install the port-rptr setup in compatibility mode Windows server 2003 and start the service, put as automatic execution from the panel control in administration tool. You must open all protocols and all ports for this service Port Reporter in Windows firewall. The IP of BO2 servers can be reduces as 108.61.237.150 to 108.61.237.151 or like it, between 108.61.237.0 to 108.61.237.255 with ports 13000-17000 in UDP. Because the same public IP can be used a few times, you can edit the file named hosts, by copying it in the folder of your documents, and after the edit, replace it. The file is found in the folder windows/system32/drivers/etc. You must be in administrator mode to replace this file with this adding:

108.61.237.150 rhino.choopa.net

108.61.237.151 rhino.choopa.net

Between the IP and the domain name it's a TAB key to use. Also with lmhosts.sam file with this add:

108.61.237.150 rhino #PRE #DOM:networking

108.61.237.151 rhino #PRE #DOM:networking

209.170.124.113 rhino #PRE #DOM:networking

209.170.124.209 rhino #PRE #DOM:networking

209.170.124.216 rhino #PRE #DOM:networking

108.61.237.150 "c_hoopa.net \x1C" #PRE

108.61.237.151 "c_hoopa.net \x1C" #PRE

209.170.124.113 "_demonware.net \x1C" #PRE

209.170.124.209 "_demonware.net \x1C" #PRE

209.170.124.216 "_demonware.net \x1C" #PRE

In Ethernet properties, for TCP/ipv4, use advanced options to set DNS parameters, check the box add these DNS suffix and add 108.61.237.150.choopa.net and 108.61.237.151.choopa.net. Set WINS parameters, check the boxes enable LMHOSTS research and enable NetBios on TCP/IP. Also click on add LMHOSTS file to add the new LMHOSTS.sam file.

3.8. Changing memory pagination zone

To change memory pagination zone of an exe of a Steam game launcher, you can create a shortcut of the exe on the desktop, then copy/paste the exe on a different folder, than where the exe is by default, named with strong characters for more security. Go to the properties of the shortcut you created and change the name of the folder, where the exe is by default, by the folder you created for the path of the "target" or for the path of "start in", under the tab shortcut. In advanced option under this tab, check the boxes execute as administrator and execute in different memory zones. Launch your game from one or other shortcut icon. Change strong characters as often you can. Also you can change the name of the shortcut icon.

I have noticed that after uninstalling and installing another time AW, the matches are free of cheaters, but after playing more matches, I'm only finding matches full of cheaters. Their cheats can hack your game memory. To fresh the memory of the game like it's a first install, you can delete the exe of the game in your Steam library and check the integrity of game files with the steam property of the game. Then create a shortcut icon on the desktop

where you will launch the game. Change the name of the shortcut, and open properties of it to change shortcut advanced properties by checking the two boxes named run as administrator and run in different memory places. These will fresh the memory of the game if you have encountered cheaters that have modified the matchmaking system to forward you on their hacked lobbies.

In order to have a new installation cache for your game on Steam, you can copy the folder of the game in a path you will create like D:\SteamLibrary 2\steamapps\common, then change the name of the old folder like D:\SteamLibrary 1, then restart Steam and reinstall the game from the new folder, it will discover the files already here.

To allocate AW in a new memory section header, create registry information as following: https://support.microsoft.com/en-us/kb/310593

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx

Flags = dword:00000002

Create a key with the name of the section header you want like THENAMEOFSECTIONHEADER

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\THENAMEOFSECTIONHEADER

RunMyApp = "s1_mp64_ship.exe"

Create a key named Depend to load dll in this section header

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\THENAMEOFSECTIONHEADER\Depend

dll1 = "binkw32.dll"

dll2 = "steam_api.dll"

3.9. Network card settings

Some parameters can be set to secure your network from your network card properties.

Type in cmd dos prompt command run as administrator the following command:

netsh int tcp set heuristics enabled, netsh int tcp set global autotuninglevel=highlyrestricted, netsh int tcp set global chimney=automatic, netsh int tcp set global ecncapability=enabled, netsh int tcp set global rss=enabled, netsh int ipv4 set global multicastforwarding=disabled, netsh int ipv4 set dnsservers name="ethernet" source=dhcp, netsh int ipv4 set global sourceroutingbehavior=dontforward, netsh int ipv4 set global groupforwardedfragments=enabled, netsh advfirewall set allprofiles settings remotemanagement disable, netsh advfirewall set allprofiles state on, netsh rpc filter delete rule, netsh rpc filter delete filter filterkey=all, netsh ras delete link lcp, netsh ras delete link swc, netsh ras delete multilink multi, netsh http delete cache, netsh int teredo set state disable netsh int ipv4 delete arpcache, netsh int ipv4 delete destinationcache, netsh int ipv4 delete neighbors, netsh int ipv6 delete arpcache, netsh int ipv6 delete destinationcache, netsh int ipv6 delete neighbors, netsh int isatap set state disable, netsh advfirewall set icmpsetting all disable netsh winsock reset, netsh winsock set autotuning off, netsh interface tcp show global, netsh interface tcp set global autotuning=restricted, netsh int tcp show global, netsh int tcp set global congestionprovider=ctcp, set supplemental congestionprovider=ctcp, netsh interface tcp set global autotuning=normal, netsh interface tcp set global autotuning=highlyrestricted, netsh interface tcp set global rsc=enabled, netsh interface tcp set global dca=enabled, netsh interface tcp set global ecncapability=enabled, netsh interface tcp set global chimney=enabled, netsh interface tcp set global netdma=enabled, netsh interface tcp set global timestamps=enabled, netsh interface tcp show security, netsh interface tcp set security mpp=enabled, netsh interface tcp set security profiles=enabled, netsh interface tcp set security startport=1 numberofports=65535 mpp=enabled, netsh interface ipv4 install, netsh interface ipv4 show global, netsh interface ipv4 set global icmpredirects=disabled, netsh interface ipv4 set global sourceroutingbehavior=drop, netsh interface ipv4 set global taskoffload=disabled,

netsh interface ipv4 set global dhcpmediasense=disabled, netsh interface ipv4 set global mediasenseeventlog=enabled, netsh interface ipv4 set global mldlevel=sendonly, netsh interface ipv4 set global mldversion=version1, netsh interface ipv4 set global multicastforwarding=enabled, netsh interface ipv4 set global groupforwardedfragments=enabled, netsh interface ipv4 set global randomizeidentifiers=disabled, netsh interface ipv4 set global store=persistent, netsh interface ipv4 set global addressmaskreply=enabled, netsh interface ipv4 show interface, netsh interface ipv4 set interface "1" nud=enabled, netsh interface ipv4 set interface "1" weakhostsend=disabled, netsh interface ipv4 set interface "1" weakhostreceive=disabled, netsh interface ipv4 set interface "1" currenthoplimit=255, netsh interface ipv4 set interface "1" ecncapability=application, netsh interface teredo set state disabled, netsh interface isatap set router disabled, netsh interface ipv6 set privacy state=disabled, netsh interface ipv6 set teredo disabled, netsh p2p pnrp cloud flush global_, netsh wlan stop hostednetwork, netsh wfp set options netevent=off.

You can often disable/enable your network card from network card settings and change your computer internal IP from ipv4 properties from Ethernet state with manual settings. In it set your computer internal IP and your modem/router internal IP only, for DNS and WINS servers also.

Disable WLAN or LAN card for network connection that you don't use for internet from network card settings like Bluetooth network connection.

In properties of Ethernet state, under the tab authentication, near the tab network management, you can set more secure parameters for connection to a server.

UNINSTALL NETWORK PERIPHERAL (from peripheral manager in panel control) IF PROBLEMS OPENING IPV4 PROPERTIES.

In regedit open with a run command you can change these registry entries:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces values DhcpIPAddress with data 0.0.0.0 to replace with 192.168.1.1 or your modem internal IP and the values UseZeroBroadcast to 1.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes delete the string value 0.0.0.0,0.0.0.0,192.168.1.1,-1 and create one with value 192.168.1.1,192.168.1.1,192.168.1.1,192.168.1.1.

For HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList change string value named (by default) with data 192.228.79.201 by 192.168.1.1 and delete RootDnsIpv6Addr 2001:478:65::53.

KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet delete values ActiveDnsProbeContent 131.107.255.255 and ActiveDnsProbeContentV6 fd3e:4f5a:5b81::1.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPSEC,

add a new DWORD entry named NoDefaultExempt 3

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\IPSec

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPsec

add a new DWORD entry named AssumeUDPEncapsulationContextOnSendRule 2

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Defaults\FirewallPolicy

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy

add a new DWORD entry named IPSecExempt 3

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy

add a new DWORD entry named IPsecThroughNAT 2

3.10. Finding IP of servers

You can create blocking rules for remote IP shown with TCPview or cports/Currports with no hostname resolution option if these IP of matchmaking connection like in AW forward to lobby with cheaters. But the programs don't show UDP connection IP. You can use the cmd dos prompt command by typing:

netstat -n -a -o interval 10 (ctrl+C to stop)

ipconfig/displaydns

Also you can find IP of servers by searching with perfmon.exe when you are ingame or connecting to game and match in order to restrict traffic for your games using Windows firewall. Maybe I'm bitching on developers and on some servers which normally are very secure in fact cause the matchmaking system coupled with Windows firewall allow to play only on these servers and not all other open by cheaters with VPN modifying their game files with an IDE tool on which I was always forwarded myself testing different IP of servers by blocking IP. In fact if you deny all connection for BO3, perfmon display no IP but when you allow only IP of authentication and you search a match, the IP display must be secure and official servers only. I let you deduce what to do, as allowing IP of authentication and 224.0.0.0 to 255.255.255.255 only for BO3 in UDP, then add IP one by one of servers display with perfmon. You must do it each time you want to play cause IP disable can be used by VPN users. It's not fun to play a game when it's unplayable cause of the opponents are bugged and too strong. When you know they cheating in a broken game, even a basic 2 bits pacman is more fun to play.

3.11. Process Explorer

With processexplorer by technet, you can kill the process that are not ASLR enabled, but not system, interrupts and system idle process. You can see which DLL are not ASLR

enabled and the command line for a process like: /DisableUI, 0xa74, 0x4, 0, /Embedding, /RunAsService, -r, /V, PriorityLow, /Start, /min, /FORPCEE3 /connectToHost, /LOAD /SPLASH, SCODEF:5456 CREDAT:203009, /HIGHENTROPYVA, /DYNAMICBASE.

3.12.Other considerations

Some other important information can be found with this base of research like with trusted tools available with Windows OS. For example... By executing mmc (microsoft manager console) with run command mmc, you can add a strategy of ip security with IP Security (IPsec) configuration for all protocols. Create a basic task with TaskSchd.msc in C:\Windows\System32 for execute at session start the msc file you created with mmc. In TaskSchd.msc you can see a lot of tasks allowing different programs to be executed when you start your computer like in the folder start programs or under the tab start in task manager. You can disable or delete all of it. It can be viruses launchers. Making Windows updates is important too, but sometimes it can be hacked, and throw viruses.

3.13. About unsecure files

Empty folder temp from C:\Users\Your User Name\AppData\Local\Temp. Don't download and install game crack or other files with untrusted sources. Some anti-virus free brings viruses. If you want a PC dedicated to gaming take care of what you launch. Windows firewall is a good way to protect your PC without loses performances.

3.14. About reporting cheaters

Report studio videos of cheaters, took with shadowplay, on Steam forum and to pcdev on twiter. You can have unchangeable Steam link to profiles with steamidfinder website. You can upload video report on youtube faster using a video compressor like HandBrake. It can be hard to spot wallhackers cause of the UAV and they hide they wallhacking by dying stupidly but they can't hide it every time.

4. Firewalls and secure DNS servers

4.1. Base of the method

As example for using Windows firewall in CoD AW do as following... In Windows firewall properties, set to block all in inbound traffic comboboxes, and set to block in outbound traffic comboboxes. Delete all rules. Create outbound traffic allowing rules as following... Two Rules with distant ports 80, 443 in TCP for Windows update service, and for steamwebhelper. A rule with distant port 53 in UDP for DNS client service. Two rules with distant ports 80, 443, 27014-27050 in TCP, and with distant ports 27000-27036, 4379-4380, 3478 in UDP for Steam. 4 rules with distant ports 443, 3074 in TCP, with distant port 3074 with local port 3074 in UDP, with local port 27016 with all distant ports in UDP, with local port 3074 with distant ports 33000-34000, 40000 in UDP, for CoD AW. Create outbound traffic allowing if secure rules as following... A rule with all distant and local ports in TCP. A rule with all distant and local ports in UDP. Create blocking Windows firewall rules for all services and the program ntoskrnl in the folder c:\windows\system32\ in TCP with distant ports 1-79, 81-442, 444-65535, and in UDP with distant ports 1-52, 54-65535.

As example for using Windows firewall in CoD BO2 do as following... In outbound traffic, create rules for Steam.exe (distant ports 80, 443, 27000-27050 in TCP, add –TCP in the shortcut icon of Steam after the path), steamwebhelper.exe (distant ports 80, 443 in TCP), Steam Client Service (all distant ports), DNS client service (distant port 53 in UDP), Uplay.exe (all distant ports), and three rules for BO2 (t6mp.exe) as following:

Outbound traffic rules (allowing):

- local ports 40000-65535, distant port 3074 in TCP, distant IP: 209.170.124.147, 209.170.124.209, 209.170.124.117, 209.170.124.109, 209.170.124.216.

- local port 3074, distant port 3074 in UDP, distant IP: 209.170.124.147, 209.170.124.117, 209.170.124.209, 209.170.124.113, 209.170.124.109, 209.170.124.216.
- locale port 3074 in UDP, all distant ports, all distant IP (or BO2 servers IP like 108.61.237.2 to 108.61.237.255).

Outbound traffic rules (allowing if secure):

- all local ports, all distant ports, all local IP, all distant IP for the service Steam Client Service.
- all local ports, all distant ports, all local IP, all distant IP for all programs, all services.

Security connection rules (set in default ipsec parameters in properties of Windows firewall for allowing IPsec tunnel tab, with parameter button, advanced check box, computers allowed: creator group; computers denied: creator group, task, interactive, authenticate users; and users allowed: administrator; users denied: line, anonymous logon, authenticate users, terminal server user, iis_iusrs, distance manager users, administrator…):

- authentication require inbound and ask outbound, method default, no tunnelling IPsec, all IP for terminal points.
- authentication require inbound and require outbound, method default, tunnelling IPsec, IP from 0.0.0.0 to 223.255.255.255 for terminal points.

Add blocking outbound traffic rules for protocols ICMP, UDP Lite (136)…, and rule for IP between 0.0.0.0 to 108.61.237.0 and 224.0.0.0 to 255.255.255.255, and also rules for all services but not the service Client DNS.

Set manually your network ipv4 configuration in Ethernet in network center. Set to all block inbound connection traffic, set to block by default outbound connection traffic and set maximum securities in IPsec parameters for default behaviour in Windows firewall properties.

To enable IPsec connections, the method is explained on the website http://www.it.cornell.edu/services/managed_servers/howto/ipsec.cfm but for it do as following… Install the certificates of Steam.exe or the exe of games under the tab numeric signature when you display properties of the exe, create Windows firewall security connection rules ask authentication for inbound and outbound traffic with IP from 0.0.0.0 to 223.255.255.255 for both termination endpoints with ports 80, 443, 3074, 27014 to 27050 for termination endpoint 1 (server) and all ports for termination endpoint 2 in TCP, with ports 53, 3074, 27000 to 27036, 4379, 380, 3478 for termination endpoint 1 (server) and all ports for termination endpoint 2 in UDP, with all ports for termination endpoint 1 and port 3074, 27000 to 27036, 4379, 4380, 3478 for termination endpoint 2 (client) in UDP, and rules require authentication for inbound and outbound traffic with personalized certificates installed for authentication method in TCP and UDP, create inbound and outbound traffic rules allowing if secure in TCP and UDP (and rules allowing with TCP and UDP protocols, all locales and distant ports and IP, for all services and programs) with the second personalized option (or double these rules with TCP and UDP protocols, all locales and distant ports, with services or programs selected, for every allowing rules with services, programs, locales ports, distant ports, and IP selected). In Windows 10, you can add a proxy server for your network connection. The proxy can be the address 209.170.124.117 and port 3074 corresponding to AW lobby, and the address 209.170.124.209 and port 3074 corresponding to BO2 lobby (you see it with the cmd prompt command dos ipconfig/displaydns). Remove the proxy to have Steam store connection because http and https ports are replaced by xbox port with this kind of proxy. Demonware.net has locations in Vancouver, Dublin, and Shanghai supporting Activision Publishing, so your proxy server IP must have an address near these locations. Type in google search tool: speedguide IP Vancouver or Dublin or Shanghai, to find an IP closer for setting it in the parameters of proxy server for your network connection.

Use often the prompt command dos ipconfig/flushdns and restart your modem/router often to secure your network from attackers. Also use the prompt command dos net stop dnscache to reset your DNS, the prompt command dos net stop http to reset your network, and use to restart these services the prompt command dos net start dnscache, and the prompt command dos net start http. Change often your internal IP address in network Ethernet ipv4 properties. In Ethernet properties let only ipv4 network installed.

Finding ports of servers is the most important thing cause only some ports don't forward on hacked lobbies. These fake servers use more ports cause it's host by cheater computers, and we know that a computer need more than 3000 ports in a row to work with the global network.

Maybe it help or not, but in any case, these information settings are a working around well done. Steam and Microsoft will do the rest, normally, if they take care of their customers, because despite VAC and TAC, we are bored of cheaters/hackers and hacked lobbies full in all Call of Duty and incoming our computers we paid honestly.

From control panel, open Windows firewall from advanced parameters. In the middle tab you can open Windows firewall properties. In all combobox of the third first tabs set to block if no rules but to block all for inbound traffic if you play Advanced Warfare. Open outbound traffic connection tab from the left tab, it appear rules. Create two rules from right tab with protocols TCP and UDP. In it put distant ports 53, 80, 443, and 27000-27050 in TCP and UDP. You can add local ports 1024-65535. For CoD BO2 and AW, add a rule for distant ports 443, 3074 and local ports 1024-65535 in TCP and distant IP 185.34.0.0/16, 209.170.0.0/16 and a rule for distant port and local port 3074 in UDP. Let inbound traffic rules autocreate each time you update or install Black Ops II and Advanced Warfare. You will be open nat if you open a nat/pat rule for port 3074 in UDP and a inbound traffic Windows firewall rule with distant ports 3074-3075 and local port 3074 in UDP. You can choose your

server IP if you add IP in server rule with ports corresponding, IP like 108.61.0.0/16. For CoD AW, add a outbound traffic rule for distant ports 33200-34600, 40000 and local port 3074 in UDP and distant IP 108.61.0.0/16 for playing on servers (but server connection will not be linked to the port 3074). Instead of this last rule for CoD AW do as following… Open a nat/pat rule for port 3074 in UDP. Create a Windows firewall outbound traffic rule for distant port 40000, local port 3074 in UDP, create a Windows firewall inbound traffic rule for distant ports 3074-3075, 33000-34000, local port 3074 in UDP and all distant IP and for CoD BO2, create a Windows firewall inbound traffic rule for distant ports 3074-3075, 13000-14000, local port 3074 in UDP and all distant IP (you need to set in Windows firewall properties block if no rules for outbound and inbound traffic). Create a Windows firewall inbound traffic rule blocking lateral traverse as local port and all distant port for protocol UDP with lateral traverse allowed in advanced options of the rule. Create two Windows firewall inbound traffic rules allowing if secure, one with users of model COM distributed exception, the second with USER TERMINAL SERVER exception, in the tab distant users of the rules. Create a Windows firewall outbound traffic rule for distant port 40000, local port 3074 in UDP and all distant IP. It's to have server connection linked to port 3074 own by Activision. So with your firewall on your modem you can allow only IP 209.170.124.117, for port 3074 in TCP/UDP, only IP 185.34.104.124, 185.34.107.30 for port 3074 in TCP, all IP for ports 1-1023, 27000-27050 in TCP, and all IP for ports 1-1023, 40000 in UDP, and so to add a second internal IP of your computer number 209.170.124.117 in ipv4 properties in the tab IP settings, under first section named IP addresses (moreover in the tab DNS you can add some more secure DNS servers). Also you can set in your modem firewall for these IP and ports the subnet mask of class A addresses corresponding to 255.0.0.0 for big numbers of client in the servers group. And use CHMYIP.exe find at http://sourceforge.net/projects/changemyip/ to set your IP as 209.170.124.117 with subnet mask 255.0.0.0. Don't forget to set to block if no rules inbound

traffic and outbound traffic in Windows firewall properties. These rules can be applied and defined to Steam, steamwebhelper, CoD AW exe launcher, and service DNS client (see other chapters to understand how).

application / service	protocole	adresse IP source	masque adresse IP	port source	adresse IP destination	masque adresse IP	port destination
COD5	UDP	192.168.1.8	255.255.255.0	3074	209.170.124.117	255.255.255.255	3074
COD9	UDP	192.168.1.8	255.255.255.0	3074			40000
CODA	TCP				185.34.104.124	0.0.0.0	3074
CODB	TCP				185.34.107.30	0.0.0.0	3074
CODTCP	TCP				209.170.124.117	255.255.255.255	3074
STEAM	TCP	192.168.1.8	255.255.255.0				27000-27050
CODC	UDP			3074	185.34.107.30	255.255.255.255	3074

Also other settings of your modem firewall can run. In conjunction of Windows firewall you can set the egress filtering on your modem like in this following picture:

application / service	**port interne**	**port externe**	**protocole**	**appareil**
MIC	3074	3074	UDP	192.168.1.11

application / service	protocole	adresse IP source	masque adresse IP	port source	adresse IP destination	masque adresse IP	port destination	action
modem	les deux	192.168.1.1	0.0.0.0				1-65535	rejeter
allevery1	les deux						1-1023	accepter
TCP	TCP	192.168.1.11	255.255.255.0				1-65535	accepter
UDP	UDP	192.168.1.11					1-65535	rejeter

4.2. From Windows firewall

In regards of MW3 and Ghosts, only distant ports 3074 in UDP and TCP are required for find a match. Maybe it's important to open port 3074 with all IP, in BO2, at least to send a report with the report button.

In regards of Titanfall, the ports used by the game are 3075 (TCP/UDP) and 30000-30010 or 30000-30099 and/or 25000-25010 or 25000-25099 (137.0.0.0 to 137.255.255.255)

in UDP and 80, 443 in TCP. So you can set your modem firewall and Windows firewall with these ports only. Also, Origin must be connected, it use only ports 80 and 443 in TCP, for let the connection into the game (like for Uplay). Don't forget the ClientDNS firewall side.

Block all inbound traffic connections and set to block outbound traffic connections (you must set manually your properties of Ethernet connections in ipv4 properties. Create outbound allowing rules as following:

- For the service client DNS, distant port 53 in UDP, distant IP 192.168.1.1 or your modem internal IP or the IP of your primary DNS server.

- For Origin.exe, distant ports 80 and 443 in TCP.

- For Titanfall.exe, distant ports 80, 443 in TCP, distant IP 54.0.0.0-54.255.255.255 (corresponding to the IP range of Origin connection in TCP open, shown in perfmon.exe).

- For Titanfall.exe, distant port 3075 in TCP, distant IP 137.0.0.0-137.255.255.255.

- For Titanfall.exe, distant port 3075 in UDP, distant IP 137.0.0.0-137.255.255.255 (to disable after connection and before searching a match).

- For Titanfall.exe, locale ports 27005, 27015, 27040, distant ports 30000-30099 in UDP and distant IP 104.39.0.0-104.41.0.0.

Create outbound blocking rule as following:

- For Titanfall.exe, distant ports 25000-25099 and 30000-30099 in UDP, distant IP: 108.0.0.0-108.255.255.255, 195.0.0.0-195.255.255.255, 189.0.0.0-189.255.255.255, 197.0.0.0-197.255.255.255, 173.0.0.0-173.255.255.255, 207.0.0.0-209.255.255.255, 223.0.0.0-255.255.255.255, 95.0.0.0-95.255.255.255, 93.0.0.0-93.255.255.255, 0.0.0.0-100.0.0.0 (corresponding to IP range of gameservers/clanservers hackers/crackers servers).

So finally we can see that same IP are used with different ports changing with the time, like it's IP of user computers. By forcing these users IP to be also ours, it allows the connection to official servers of Treyarch from our computers. The method is to multiply our

internal IP on our network, in order to have a conflict between cheater IP opening cracked servers and ours. So the connection will be allowed only on official servers certified as more secure servers. On a PC you don't play BO2, open network internet protocol ipv4 properties, check the box use IP address as following, in IP address, type your internal IP, and your modem internal IP, in DNS server, type your modem internal IP and a free DNS auxiliary server like the one of OpenDNS: 208.67.222.222, then click on advanced button. In the tab IP parameters, add IP addresses in the first texboxes, as following, one by one: for example for BO2 servers IP from 195.122.135.5 to 195.122.135.239. Then click ok for each window.

In regards of Payday 2, the ports used by the game are 9899, 27000-27050 in TCP and UDP (to open in the modem firewall). But to join a public match, you shall open all ports (1-65535 in TCP and UDP) for steam.exe, steamservice.exe (in program files/common files/steam and program files/steam/bin) and Steam client service only (to open in Windows firewall, no need to open ports in Windows firewall for the game exe). So it's important for VAC to open ports for the Steam client service maybe for all other games too. After an update of steam, steamservice isn't used anymore for connection to a lobby in Payday 2. So create Windows firewall rules allowing and allowing if secure with all local ports and distant ports 3478, 4379, 4380 in UDP for steam.exe for connection to a lobby in Payday 2. You can see which connection with programs or services are used with perfmon.exe, when you have all connection allowed by creating Windows firewall rules allowing and allowing if secure with all local ports and distant ports 1024-65535 in TCP and UDP for all programs and services that you will disable after identification of connections with programs or services used.

In regards of Grand Theft Auto 5, the game use ports 80, 443 in TCP and 6672, 61455-61458 in UDP. You need to open ports 80, 443 in TCP for subprocess.exe in the folder C:\programmes\Rockstar\ and for GTA Launcher in the folder of the game. It's shown in perfmon.exe if you temporary open ports 80, 443 in TCP for all programs and services. The

path of subprocess.exe is shown when you open task manager with ctrl+shift+esc keys under the tab details.

In regards of The Division, you can create rules for the game as following: 4 rules allowing and allowing if secure with second option of authentication in TCP and UDP. For allowing if secure rules, deny the rule for local security entity group policy System. Create 2 rules in TCP and UDP for all programs and services. If you set ports for allowing rules, the allowing if secure rules in TCP and UDP for all programs and services will not take effect. It blocks VPN connections. The Division ports are 80, 443, 27015, 51000, 55000 in TCP and port 33500 in UDP. The ports are indicated in perfmon under network tab. So create two blocking rules in UDP and TCP for ports between.

In regards of DOOM, proceed as for The Division but ports used by the game are 443 in TCP and 27000-27030 in UDP. Perfmon show ports 443 in TCP and 27016 in UDP. Other ports were deduced from Steam ports for game client and matches, also by trying myself to join a match.

In regards of Rocket League, it uses port 443 in TCP to be authenticated in the game, ports 7000-7890 in TCP to contact servers and ports 7000-7890 in UDP to be connected in servers. You can block ports out of these ranges.

In regards of The Crew, game uses ports 80, 443, 3000-3004 in TCP and ports 3000-4000, 30000-33000 in UDP. Create outbound allowing rules and allowing if secure rules with distant IP 0.0.0.0 to 223.255.255.255 and local security entity for System to apply for the game exe in Windows firewall. Create blocking rules for outbound traffic with ports between the ports I've found searching on internet, with perfmon and trying to have connection while the game running.

In regards of Advanced Warfare, you can create NAT/PAT rules on your modem and Windows firewall rules as following:

Configuration NAT/PAT

Règles personnalisées

application / service	port interne	port externe	protocole	appareil	activer
Telnet	23	23	TCP	pc-salon	
cod	3074	3074	les deux	pc-salon	☑
COD1	26900-27050	26900-27050	les deux	pc-salon	☑
COD2	443	443	TCP	pc-salon	☑
COD3	3478	3478	les deux	pc-salon	☑
COD4	4379-4380	4379-4380	les deux	pc-salon	☑

Outbound allowing Windows firewall rules:

- Initialize Windows firewall with default settings. Set to block if no rules inbound traffic and to block if no rules outbound traffic in all comboboxes of Windows firewall properties. Let all default rules and inbound rules autocreate each time you install or update a game. Add –tcp at the end of the shortcut link for the icon launcher of Steam.
- Let only the DNS rule with distant port 53 in UDP associate with svchost.exe (you can disable Client DNS service after connection to network)
- For the services Windows Update, Windows Defender, Windows Defender Network controller, EMET service and the programs EMET GUI, EMET Agent, (to send information when notification of DEP offend occurs) distant port 80, 443 in TCP
- For steamwebhelper.exe, distant port 80, 443 in TCP
- For Steam.exe, Origin.exe, Uplay.exe, distant port 80, 443 in TCP
- For Steam.exe, distant port 27000-27050 in UDP and TCP
- For Steam client service in TCP and UDP
- For the exe of the game, distant ports and distant IP…
- Create a outbound traffic rule with local ports 1024-65535 and distant ports 80, 443, 3074, 27000-27050 in TCP.

- Create a outbound traffic rule with local ports 3074, 27000-27050 and distant ports 3074, 27000-27050 in UDP.
- Create a outbound traffic rule for the exe of the game, with local and distant ports 3074-3076, 27016, 40000 in UDP and distant IP 93.93.65.0/24, 95.141.40.0/24, 108.61.237.0/24, 108.61.230.0/24
- Open a nat/pat rule for ports 3074-3076, 27016, 40000 in TCP/UDP for enable connection to servers but not to computers.

The game use ports 3074 for authentication and p2p host, and 40000 for servers. Use Windows Update for security patch and enable all options in Windows Defender.

Other method to play on server of Call of Duty Advanced Warfare:

From control panel, open Windows firewall from advanced parameters. In the middle tab you can open Windows firewall properties. In all combobox of the third first tabs set to block if no rules for outbound traffic and to block all for inbound traffic.

Open outbound traffic connection tab from the left tab, it appear rules.

Create two rules from right tab with protocols TCP and UDP. In it put distant ports 53, 80, 443, 3074, and 27000-27050. You can add local ports 1024-65535.

Add a rule with ports 40000, 33000-34000 with protocol UDP to play on dedicated servers. Local port 3074. You can add distant IP 108.61.0.0/16.

Add a rule allowing if secure with all ports, all protocols.

Install the certificate available in the installation folder of CoD AW. In Windows firewall properties, under the tab default IPsec behaviour set advanced settings of authentication by adding the certificate Geotrust Global CA.

Open secure traffic connection rules from left tab. Add an IPsec rule ask authentication for inbound traffic and for outbound traffic with IP 223.255.255.255 for termination endpoints 1 and 2. Add a IPsec rule require authentication for inbound traffic and for outbound traffic.

In Ethernet properties, for ipv4 properties, set manually your primary and auxiliary DNS server IP of your internet provider or of a secure DNS server listed under.

Level3 DNS 209.244.0.3, 209.244.0.4, 4.2.2.1, 4.2.2.2, 4.2.2.3 and 4.2.2.4; Comodo DNS 8.26.56.26 and 8.20.247.20; Norton DNS 199.85.126.30 and 199.85.127.30

Securly DNS 184.169.143.224 and 184.169.161.155; SafeDNS DNS 195.46.39.39 and 195.46.39.40; DNS.WATCH DNS 82.200.69.80 and 84.200.70.40; Opendns DNS 208.67.222.222 and 208.67.220.220; Dyn Internet Guide DNS 216.146.35.35 and 216.146.36.36; FoolDNS DNS 87.118.111.215 and 213.187.11.62; GreenTeam Internet DNS 81.218.119.11 and 209.88.198.133; DNS Advantage DNS 156.154.70.1 and 156.154.71.1

DNSResolvers.com DNS 205.210.42.205 and 64.68.200.200; Google Public DNS 8.8.8.8 and 8.8.4.4

It’s better to enable a maximum of Windows services when the description talks of security like the service netlogon. You can set to automatic launch these services. To display more services you can add Windows functionalities in control panel in programs and functionalities. You can add secure DNS server like Norton secure DNS or Comodo DNS server in your connection properties of ipv4. Activate netbios in TCP/IP for server DNS as DHCP server (in the tab WINS), add DNS and WINS server IP with IP of Norton DNS or Comodo DNS server in advanced options of ipv4 properties (for Norton it corresponds to IP preferred DNS: 199.85.126.30 and alternate DNS: 199.85.127.30 and for Comodo 8.26.56.26, 8.20.247.20). Also it’s better if you set COM properties with more security in control panel in administration tools in components services (open computer and click right on workstation to open properties). In it, set in the tab default properties to maximum security by checking boxes and put the last options in comboboxes. Also add in the tab default protocols for DCOM protocols Tunnel TCP/IP and delete TCP/IP connection. Set the property of Tunnel TCP/IP by adding ports 53, 80, 443, 3074, 27000-27050, 40000.

Using cheat-engine or CFF file modifications for games aren't recommended, there is a risk of be banned, cause it's considered as hacking, and it's easy to cheat with cheat-engine. You can use NewB program with example codes given in this book, like a simple code of WriteProcessMemory() function with random values of variables. But it can be disable by hackers if you use anti-virus, or other programs. Setting rules with Windows firewall is a good way to have a computer secure without using anti-virus programs like MBAM. For gaming you can use only Steam, Uplay, Origin and iexplorer. Make Windows memory diagnosis and defrag your drives from administration tools in control panel.

You can have Steam connection with ports in TCP only if you add –TCP at the end of the shortcut for steam icon. You can create blocking rules for programs shown in task manager open with ctrl+shift+esc (open the folder to locate the file). Programs like: C:\Windows\System32\smss.exe, C:\Windows\System32\csrss.exe, C:\Windows\System32\wininit.exe, C:\Windows\System32\svchost.exe, C:\Windows\System32\services.exe, C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe, C:\Windows\System32\lsass.exe, C:\Program Files\Intel\iCLS Client\HeciServer.exe, C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL\Jhi_service.exe, C:\Program Files\Windows Defender\MsMpEng.exe, C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe, C:\Windows\System32\taskhostex.exe, C:\Windows\System32\Taskmgr.exe, C:\Windows\explorer.exe, C:\Windows\System32\ntoskrnl.exe, C:\Windows\System32\winlogon.exe, C:\Windows\System32\dllhost.exe, C:\Windows\System32\dwm.exe, C:\Windows\System32\wbem\WmiPrvSE.exe.

To set rules in Windows firewall is something recommended by Microsoft despite all ports are open in it by default. But on Activision (the editors of Call of Duty series) support

web sites, they say to open all ports in modem and Windows firewall. Also enable UPnP, and put the computer in a DMZ on the modem. So maybe, there is a RCon port to open in Windows firewall… Add ports and nat/pat rules for inbound and outbound traffic for t6mp.exe and steam.exe with all distant IP, and distant TCP ports 80, 3074-3075, 27000-27050, 3478, 4379, 4380 and UDP ports 3074-3075, 27000-27050, 3478, 4379, 4380, like it's recommended by Steam support.

Instead of disable services in control panel in administration tools, enable a maximum of services with starting type set to automatic in the properties of the services, because a lot of services are for Windows securities. Also open ports 80 and 443 in TCP in Windows firewall for Windows updates service and steam gameoverlayUI.exe in Steam folder for report cheaters from their Steam profiles (also for block cheaters from your games) and for the program steamwebhelper.exe in the folder Steam/bin/ and maybe for services only when you click on services in the property window of the rule in the tab program and services but there is automatic Windows firewall rules for svchost.exe. Don't forget to set in recommended mode the Windows Updates in control panel.

From programs and functionalities in control panel, enable Windows functionalities like RIP Listener, Internet Explorer 11, Microsoft .NET Frameworks, API RDC (Remote Differential Compression), Protocol SNMP, SNMP WMI, all in MSMQ, all in activation service of Windows process, localisation Windows service, all in service world wild web in internet services (IIS), Simplified TCP/IP services, Windows Identity Foundation. It's for more securities and report tools of errors and malwares.

For playing modern warfare 2019 and black ops cold war on PC, you need allowing inbound rules for battle.net.exe, battle.net launcher, in program files, and battle.net agent in programdata, and allowing inbound rules for games exe, one rule in TCP with local ports 1024-65535 and distant ports 1-49151, a second rule in UDP with local ports 1024-65535 and

distant port 3074 with distant IP 185.34.107.128, and a third rule for servers in UDP with local ports 1024-65535 and distant ports 1024-49151 with distant IP 24.105.0.1-24.105.62.254.

4.3. From OpenDNS firewall

Create an account on OpenDNS.com and follow their instructions to use their DNS servers, Add primary and secondary DNS IP of OpenDNS in advanced settings of your IPv4 configuration properties in Ethernet network properties. In dashboard of OpenDNS, make a custom setting, blocking all categories, and allowing store.steampowered.com, steampowered.com, steamcommunity.com, and blocking 108.61.77.210.choopa.net, choopa.com, choopa.net, choopadns.com, colocrossing.com, dedicatedgaming.com.au, DELTTTSERVER.COM, dnsadm.choopa.com, domain.com, edgegameservers.net, fragnet.net, gameservers.com, iinet.net.au, in-addr.arpa, localhost.net, multiplay.co.uk, multiplaygameservers.com, nfoservers.com, nuclearfallout.net, vilayer.com, whois.domain.com, ZoneNetworks.com.au, seflow.it.

More research have been made with servers connections on Call of Duty Advanced Warfare using OpenDNS and the cmd prompt command typing ipconfig/displaydns to see domain name to block and to allow in OpenDNS. The IP of connections are used by hackers using the same IP of Call of Duty authentications, but domain names are registered differently and can't be used by hackers normally. Here the settings for CoD AW in OpenDNS:

ALWAYS BLOCK: ar, au, ch, de, eu, fi, fr, hu, jp, kz, net, nl, org, ro, uk, us.

NEVER BLOCK: 192.168.1.1.NET, 192.168.1.8.net, 208.67.220.220.net, 208.67.222.222.net, akamai.net, akamaihd.net, akamaitechnologies.com, aw-pc-auth1.prod.demonware.net, aw-pc-auth2.prod.demonware.net, aw-pc-auth3.prod.demonware.net, aw-pc-lobby.prod.demonware.net, myamoto708.net, s1-

stun.au.demonware.net, s1-stun.eu.demonware.net, s1-stun.jp.demonware.net, s1-stun.us.demonware.net, steamcommunity.com, steampowered.com, valve.net.

Delete .net blocking rule to have a normal display of Steam store. You must add DNS suffix for your connection in ipv4 properties (it correspond here to myamoto708.net). Also change my modem and computer internal IP by your modem and computer internal IP in OpenDNS configuration of domain allowing rules.

Moreover you can use Comodo firewall and configure it to have a maximum of security. Unlike Norton firewall, Comodo firewall don't disable Windows firewall.

4.4. From modem/router firewall

In regards of security on consoles you can restrict ports with the firewall on your modem/router. XBox live needs ports to be open, it's given on XBox support website:

Port 88 (UDP)

Port 3074 (UDP et TCP)

Port 53 (UDP et TCP)

Port 80 (TCP)

Port 500 (UDP)

Port 3544 (UDP)

Port 4500 (UDP)

XBox support website gives additional ports that may need to be opened:

Star Wars Battlefront (Xbox One):

TCP: 53, 80, 3074, 3659, 42100-42200

UDP: 53, 88, 500, 3074, 3544, 3659, 4500

Star Wars Battlefront (PC):

TCP: 3569, 9946, 9988, 10000-29999, 42100-42200

UDP: 3659, 9565, 9570, 9000-9999

Call of Duty: Black Ops III (Xbox One):

TCP: 3075

UDP: 3075

Call of Duty: Advanced Warfare (Xbox One):

TCP: 3075, 3076

UDP: 3075, 3076

Battlefield One (Xbox One):

TCP: 53, 80, 500, 1863, 3544, 3659, 4500, 10000-29999, 42100-42200

UDP: 53, 88, 500, 1863, 3544, 3659, 4500, 9565, 9570, 10000-10080

Destiny (Xbox One):

TCP: 53, 80, 3074, 7500-17899, 30000-40399

UDP: 53, 88, 500, 3074, 3544, 4500, 1200, 1001

Destiny 2 (Xbox One):

TCP: 53, 80, 443, 3074, 7500-7509, 30000-30009

UDP: 53, 88, 500, 3074, 3544, 4500, 1200-1299, 1001

Also check EA website https://help.ea.com/uk/help/faq/opening-tcp-or-udp-ports-for-connection-issues and other websites. Otherwise, search to have connections by finding TCP and UDP ports which need to be open. Your game can freeze on XBox one always starting/quiting. To close the game, push the XBox button and then push the button Select, it opens a menu where you can close the game. After updates of games and consoles, you can encounter problems of connection. Shut down your console and your modem/router. Unwire electricity of both, wire again both, and then start your modem/router, wait it's totally on, finally start your console. Connection will be established. If you encounter problems to update your Xbox One games for new DLC as example, restart your modem and console and when both are shut down, unwire electricity.

5. Program to walling cheats

5.1. NewB

Activate DEP (Data Execution Prevention) on your PC, checking the box to enable it for all programs. If you encounter problem, verify the game cache integrity in property of the game on Steam library. Create a C++ visual studio 2010 empty project and add a cpp sheet named main in the folder source files. Add the following code and debug the project, then launch the exe in the debug folder to start playing. To validate the namespace System, you must debug with the Common Language Runtime Support /clr. Rigth click on the name of the solution in explorer solution, then left click on configuration properties, then in the tab general, select /clr in front of Common Language Runtime Support. In the folder, you need to put the dll files named msvcp110, msvcp110d, msvcp110_clr0400, msvcp100, msvcp100d, msvcr100d. Launch this exe when the game is open. You can replace the process window name by NULL or other names. Feel free to transform the source code for adapting it for your games. It's made for transfer memory on random addresses and avoid hackers to read in the process memories. The program to change memory allocations with this code:

```
#include <windows.h>
#include <stdio.h>
#include <Aclapi.h>
#pragma comment(lib, "advapi32.lib")
#pragma comment(lib, "Kernel32.lib")
#define  _WIN32_WINNT 0x0602;
#define GAMENAME "Call of Duty®: Black Ops II - Multiplayer"
#define GAMENAME1 "Call of Duty® Ghosts Multiplayer"
#define GAMENAME2 "Titanfall"
HANDLE hProcHandle;
DWORD dwProcId;
HWND hWnd;
BOOL SetPrivilege(HANDLE hToken, LPCTSTR lpszPrivilege, BOOL bEnablePrivilege)
      {
    TOKEN_PRIVILEGES tp;
    LUID luid;
    if ( !LookupPrivilegeValue(
            NULL,            // lookup privilege on local system
            lpszPrivilege,   // privilege to lookup
            &luid ) )        // receives LUID of privilege
    {
        printf("LookupPrivilegeValue error: %u\n", GetLastError() );
        return FALSE;
    }
    tp.PrivilegeCount = 1;
```

```
    tp.Privileges[0].Luid = luid;
    if (bEnablePrivilege)
        tp.Privileges[0].Attributes = SE_PRIVILEGE_ENABLED;
    else
        tp.Privileges[0].Attributes = 0;
    // Enable the privilege or disable all privileges.
    return TRUE;
}
void main ()
{
       hWnd = FindWindow(NULL, GAMENAME2);
       GetWindowThreadProcessId(hWnd, &dwProcId);
       hProcHandle = OpenProcess(PROCESS_VM_OPERATION, FALSE, dwProcId);
       if (hProcHandle == NULL)
       {
       hWnd = FindWindow(0, GAMENAME);
       GetWindowThreadProcessId( hWnd, &dwProcId );
       hProcHandle = OpenProcess( PROCESS_ALL_ACCESS, FALSE, dwProcId );
       }
       if (hProcHandle == NULL)
       {
       hWnd = FindWindow(0, GAMENAME1);
       GetWindowThreadProcessId( hWnd, &dwProcId );
       hProcHandle = OpenProcess( PROCESS_ALL_ACCESS, FALSE, dwProcId );
       }
       PHANDLE hToken = NULL;
       LPVOID alloc;
       OpenProcessToken(hProcHandle, TOKEN_ADJUST_PRIVILEGES, hToken);
                     SetPrivilege(hToken, SE_ASSIGNPRIMARYTOKEN_NAME, true);

                     CloseHandle(hToken);
       HMODULE hK = GetModuleHandleW(L"KERNEL32.DLL");
                     BOOL (WINAPI *pfnSetDEP)(DWORD);
                     *(FARPROC *) &pfnSetDEP = GetProcAddress(hK,
"SetProcessDEPPolicy");
                     (*pfnSetDEP)(NULL);
       while (hProcHandle != NULL)
              {
                     SetProcessWorkingSetSizeEx(hProcHandle, (SIZE_T)(1000000),
(SIZE_T)(rand()%1800000000+1700000000), QUOTA_LIMITS_HARDWS_MAX_DISABLE |
QUOTA_LIMITS_HARDWS_MIN_DISABLE);
                     SetProcessWorkingSetSizeEx(hProcHandle, (SIZE_T)(-1), (SIZE_T)(-
1), QUOTA_LIMITS_HARDWS_MAX_DISABLE | QUOTA_LIMITS_HARDWS_MIN_DISABLE);
                     alloc = VirtualAllocEx(hProcHandle, (LPVOID)(rand()%4293967296),
1000000, MEM_RELEASE, PAGE_EXECUTE);
                     VirtualProtectEx(hProcHandle, alloc, 1000000, PAGE_NOACCESS,
(PDWORD)PAGE_EXECUTE);
                     VirtualFreeEx(hProcHandle, alloc, 1000000, MEM_RELEASE);
                     alloc = VirtualAllocEx(hProcHandle, (LPVOID)(rand()%4293967296),
1000000, MEM_RELEASE, PAGE_EXECUTE_READ);
                     VirtualProtectEx(hProcHandle, alloc, 1000000, PAGE_NOACCESS,
(PDWORD)PAGE_EXECUTE_READ);
                     VirtualFreeEx(hProcHandle, alloc, 1000000, MEM_RELEASE);
                     alloc = VirtualAllocEx(hProcHandle, (LPVOID)(rand()%4293967296),
1000000, MEM_RELEASE, PAGE_EXECUTE_READWRITE);
                     VirtualProtectEx(hProcHandle, alloc, 1000000, PAGE_NOACCESS,
(PDWORD)PAGE_EXECUTE_READWRITE);
                     VirtualFreeEx(hProcHandle, alloc, 1000000, MEM_RELEASE);
                     alloc = VirtualAllocEx(hProcHandle, (LPVOID)(rand()%4293967296),
1000000, MEM_RELEASE, PAGE_EXECUTE_WRITECOPY);
                     VirtualProtectEx(hProcHandle, alloc, 1000000, PAGE_NOACCESS,
(PDWORD)PAGE_EXECUTE_WRITECOPY);
```

```
                    VirtualFreeEx(hProcHandle, alloc, 1000000, MEM_RELEASE);
                    alloc = VirtualAllocEx(hProcHandle, (LPVOID)(rand()%4293967296),
1000000, MEM_RELEASE, PAGE_NOACCESS);
                    VirtualProtectEx(hProcHandle, alloc, 1000000, PAGE_NOACCESS,
(PDWORD)PAGE_NOACCESS);
                    VirtualFreeEx(hProcHandle, alloc, 1000000, MEM_RELEASE);
                    alloc = VirtualAllocEx(hProcHandle, (LPVOID)(rand()%4293967296),
1000000, MEM_RELEASE, PAGE_READONLY);
                    VirtualProtectEx(hProcHandle, alloc, 1000000, PAGE_NOACCESS,
(PDWORD)PAGE_READONLY);
                    VirtualFreeEx(hProcHandle, alloc, 1000000, MEM_RELEASE);
                    alloc = VirtualAllocEx(hProcHandle, (LPVOID)(rand()%4293967296),
1000000, MEM_RELEASE, PAGE_READWRITE);
                    VirtualProtectEx(hProcHandle, alloc, 1000000, PAGE_NOACCESS,
(PDWORD)PAGE_READWRITE);
                    VirtualFreeEx(hProcHandle, alloc, 1000000, MEM_RELEASE);
                    alloc = VirtualAllocEx(hProcHandle, (LPVOID)(rand()%4293967296),
1000000, MEM_RELEASE, PAGE_WRITECOPY);
                    VirtualProtectEx(hProcHandle, alloc, 1000000, PAGE_NOACCESS,
(PDWORD)PAGE_WRITECOPY);
                    VirtualFreeEx(hProcHandle, alloc, 1000000, MEM_RELEASE);
                    SetProcessWorkingSetSize(NULL, (SIZE_T)(1000000),
(SIZE_T)(3500000000));
                    SetProcessWorkingSetSize(NULL, (SIZE_T)(-1), (SIZE_T)(-1));
                    alloc = VirtualAlloc((LPVOID)(rand()%4293967296), 1000000,
MEM_RELEASE, PAGE_EXECUTE);
                    VirtualProtect(alloc, 1000000, PAGE_NOACCESS,
(PDWORD)PAGE_EXECUTE);
                    VirtualFree(alloc, 1000000, MEM_RELEASE);
                    alloc = VirtualAlloc((LPVOID)(rand()%4293967296), 1000000,
MEM_RELEASE, PAGE_EXECUTE_READ);
                    VirtualProtect(alloc, 1000000, PAGE_NOACCESS,
(PDWORD)PAGE_EXECUTE_READ);
                    VirtualFree(alloc, 1000000, MEM_RELEASE);
                    alloc = VirtualAlloc((LPVOID)(rand()%4293967296), 1000000,
MEM_RELEASE, PAGE_EXECUTE_READWRITE);
                    VirtualProtect(alloc, 1000000, PAGE_NOACCESS,
(PDWORD)PAGE_EXECUTE_READWRITE);
                    VirtualFree(alloc, 1000000, MEM_RELEASE);
                    alloc = VirtualAlloc((LPVOID)(rand()%4293967296), 1000000,
MEM_RELEASE, PAGE_EXECUTE_WRITECOPY);
                    VirtualProtect(alloc, 1000000, PAGE_NOACCESS,
(PDWORD)PAGE_EXECUTE_WRITECOPY);
                    VirtualFree(alloc, 1000000, MEM_RELEASE);
                    alloc = VirtualAlloc((LPVOID)(rand()%4293967296), 1000000,
MEM_RELEASE, PAGE_NOACCESS);
                    VirtualProtect(alloc, 1000000, PAGE_NOACCESS,
(PDWORD)PAGE_NOACCESS);
                    VirtualFree(alloc, 1000000, MEM_RELEASE);
                    alloc = VirtualAlloc((LPVOID)(rand()%4293967296), 1000000,
MEM_RELEASE, PAGE_READONLY);
                    VirtualProtect(alloc, 1000000, PAGE_NOACCESS,
(PDWORD)PAGE_READONLY);
                    VirtualFree(alloc, 1000000, MEM_RELEASE);
                    alloc = VirtualAlloc((LPVOID)(rand()%4293967296), 1000000,
MEM_RELEASE, PAGE_READWRITE);
                    VirtualProtect(alloc, 1000000, PAGE_NOACCESS,
(PDWORD)PAGE_READWRITE);
                    VirtualFree(alloc, 1000000, MEM_RELEASE);
                    alloc = VirtualAlloc((LPVOID)(rand()%4293967296), 1000000,
MEM_RELEASE, PAGE_WRITECOPY);
```

```
                    VirtualProtect(alloc, 1000000, PAGE_NOACCESS,
(PDWORD)PAGE_WRITECOPY);
                    VirtualFree(alloc, 1000000, MEM_RELEASE);
                    Sleep(1);
                    hProcHandle = OpenProcess( PROCESS_QUERY_LIMITED_INFORMATION,
FALSE, dwProcId );
                    SetSecurityInfo(hProcHandle,SE_UNKNOWN_OBJECT_TYPE,
PROTECTED_SACL_SECURITY_INFORMATION | PROTECTED_DACL_SECURITY_INFORMATION, NULL,
NULL,NULL, NULL);
                    Sleep(1);

            }
}
```

Close the program with Alt+F4 of your keyboard. Push Alt and press Tab to navigate between windows. Alt+Enter is used to have the game in full screen. The program presented here isn't perfect but better programs exist to enable mitigation and ASLR (like EMET 4.1 to add BO2 enabling all mitigation but not EAF and SimExecFlow). For the program in C++ with the codes above, you must disable DEP in control panel with the window System or with the cmd prompt command "bcdedit.exe /set nx alwaysoff" but it's not safe if you use your computer on Internet Explorer.

If you want more features, you can use Visual Studio 2013 Desktop Edition and make some programs that you will apply for the game process of your choice (the name of the process is specifying above the window when your game is in windowed mode). In C++, the following code can transferring memories on physical memory and free virtual memory, so the numbers of addresses allocating are randomized on the physical memory each time you start your computer, hoping it do the same think with cheaters game. Insert this code in a main.cpp sheet:

```
#include <windows.h>
#define _WIN32_WINNT _WIN32_WINNT_WIN8
#define GAMENAME "Call of Duty®: Black Ops II - Multiplayer"
#define GAMENAME1 "Call of Duty® Ghosts Multiplayer"
#define GAMENAME2 "Titanfall"
#define GAMENAME3 "Call of Duty®: Black Ops II - Zombies"
#define GAMENAME4 "PAYDAY 2"
HANDLE hProcHandle;
DWORD dwProcId;
HWND hWnd;
int i;
int k;
HANDLE hProcHandle4;
```

```
int m;
int p;
HANDLE hProcHandleP;
LPVOID mem;
LPVOID memi;
LPVOID mem4;
LPVOID mem4i;
LPVOID memP;
LPVOID memPi;
void main()
{
	while (true)
	{
		if (hProcHandle == NULL)
		{
			hWnd = FindWindow(NULL, GAMENAME2);
			GetWindowThreadProcessId(hWnd, &dwProcId);
			hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
			if (hProcHandle == NULL)
			{
				hWnd = FindWindow(0, GAMENAME);
				GetWindowThreadProcessId(hWnd, &dwProcId);
				hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
			}
			if (hProcHandle == NULL)
			{
				hWnd = FindWindow(0, GAMENAME1);
				GetWindowThreadProcessId(hWnd, &dwProcId);
				hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
			}
			if (hProcHandle == NULL)
			{
				hWnd = FindWindow(0, GAMENAME3);
				GetWindowThreadProcessId(hWnd, &dwProcId);
				hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
			}
			if (hProcHandle == NULL)
			{
				hWnd = FindWindow(0, GAMENAME4);
				GetWindowThreadProcessId(hWnd, &dwProcId);
				hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
			}
			hProcHandle4 = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, 4);
			Sleep(1);
		}
		else
		{
			PrefetchVirtualMemory(hProcHandle, 2,
(PWIN32_MEMORY_RANGE_ENTRY)((PVOID)1, (SIZE_T)999999999999), 0);
			VirtualFreeEx(hProcHandle, (PVOID)1,
(SIZE_T)999999999999, MEM_DECOMMIT);
			VirtualProtectEx(hProcHandle, (PVOID)1,
(SIZE_T)999999999999, PAGE_NOACCESS, 0);
```

```
                PrefetchVirtualMemory(hProcHandle, 2,
(PWIN32_MEMORY_RANGE_ENTRY)((PVOID)(i = rand() % 999999999999),
(SIZE_T)64), 0);
                VirtualFreeEx(hProcHandle, (PVOID)i, (SIZE_T)64,
MEM_DECOMMIT);
                VirtualProtectEx(hProcHandle, (PVOID)i, (SIZE_T)64,
PAGE_NOACCESS, 0);
                PrefetchVirtualMemory(hProcHandle4, 2,
(PWIN32_MEMORY_RANGE_ENTRY)((PVOID)1, (SIZE_T)999999999999), 0);
                VirtualFreeEx(hProcHandle4, (PVOID)1,
(SIZE_T)999999999999, MEM_DECOMMIT);
                VirtualProtectEx(hProcHandle4, (PVOID)1,
(SIZE_T)999999999999, PAGE_NOACCESS, 0);
                PrefetchVirtualMemory(hProcHandle4, 2,
(PWIN32_MEMORY_RANGE_ENTRY)((PVOID)(i), (SIZE_T)64), 0);
                VirtualFreeEx(hProcHandle4, (PVOID)i, (SIZE_T)64,
MEM_DECOMMIT);
                VirtualProtectEx(hProcHandle4, (PVOID)i, (SIZE_T)64,
PAGE_NOACCESS, 0);
                if (m > 100000)
                {
                      m = 0;
                }
                if (p > 10000)
                {
                      p = 0;
                }
                if (m == 1)
                {
                      hProcHandleP = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, p);
                      p = p + 1;
                }
                if (hProcHandleP == NULL | dwProcId == p | p == 4)
                {
                      m = 0;
                }
                if (hProcHandleP != NULL)
                {
                      PrefetchVirtualMemory(hProcHandleP, 2,
(PWIN32_MEMORY_RANGE_ENTRY)((PVOID)1, (SIZE_T)999999999999), 0);
                      VirtualFreeEx(hProcHandleP, (PVOID)1,
(SIZE_T)999999999999, MEM_DECOMMIT);
                      VirtualProtectEx(hProcHandleP, (PVOID)1,
(SIZE_T)999999999999, PAGE_NOACCESS, 0);
                      PrefetchVirtualMemory(hProcHandleP, 2,
(PWIN32_MEMORY_RANGE_ENTRY)((PVOID)(i), (SIZE_T)64), 0);
                      VirtualFreeEx(hProcHandleP, (PVOID)i, (SIZE_T)64,
MEM_DECOMMIT);
                      VirtualProtectEx(hProcHandleP, (PVOID)i,
(SIZE_T)64, PAGE_NOACCESS, 0);
                }
                m = m + 1;
                if (m == 2)
                {
                      k = rand() % 4 - 1;
                }
                mem = VirtualAllocExNuma(hProcHandle, (PVOID)1,
(SIZE_T)999999999999, MEM_DECOMMIT, 0, (DWORD)k);
                mem4 = VirtualAllocExNuma(hProcHandle4, (PVOID)1,
(SIZE_T)999999999999, MEM_DECOMMIT, 0, (DWORD)k);
```

```
                    memP = VirtualAllocExNuma(hProcHandleP, (PVOID)1,
(SIZE_T)999999999999, MEM_DECOMMIT, 0, (DWORD)k);
                    memi = VirtualAllocExNuma(hProcHandle, (PVOID)i,
(SIZE_T)64, MEM_DECOMMIT, 0, (DWORD)k);
                    mem4i = VirtualAllocExNuma(hProcHandle4, (PVOID)i,
(SIZE_T)64, MEM_DECOMMIT, 0, (DWORD)k);
                    memPi = VirtualAllocExNuma(hProcHandleP, (PVOID)i,
(SIZE_T)64, MEM_DECOMMIT, 0, (DWORD)k);
                    FlushInstructionCache(hProcHandle, (PVOID)1,
(SIZE_T)999999999999);
                    FlushInstructionCache(hProcHandle4, (PVOID)1,
(SIZE_T)999999999999);
                    FlushInstructionCache(hProcHandleP, (PVOID)1,
(SIZE_T)999999999999);
                    FlushInstructionCache(hProcHandle, (PVOID)i, (SIZE_T)64);
                    FlushInstructionCache(hProcHandle4, (PVOID)i,
(SIZE_T)64);
                    FlushInstructionCache(hProcHandleP, (PVOID)i,
(SIZE_T)64);
                    FreeUserPhysicalPages(hProcHandle, (PULONG_PTR)1,
(PULONG_PTR)999999999999);
                    FreeUserPhysicalPages(hProcHandle4, (PULONG_PTR)1,
(PULONG_PTR)999999999999);
                    FreeUserPhysicalPages(hProcHandleP, (PULONG_PTR)1,
(PULONG_PTR)999999999999);
                    FreeUserPhysicalPages(hProcHandle, (PULONG_PTR)i,
(PULONG_PTR)64);
                    FreeUserPhysicalPages(hProcHandle4, (PULONG_PTR)i,
(PULONG_PTR)64);
                    FreeUserPhysicalPages(hProcHandleP, (PULONG_PTR)i,
(PULONG_PTR)64);
                    free(mem);
                    free(mem4);
                    free(memP);
                    free(memi);
                    free(mem4i);
                    free(memPi);
                    SetSystemFileCacheSize(0, 0, FILE_CACHE_MAX_HARD_ENABLE);
                    InitNetworkAddressControl();
                    Sleep(1);
            }
      }
}
```

Another exemple for codes of NewB anti-cheating tool as following

```
#define _WIN32_WINNT 0x0501
#include <string>
#include <stdio.h>
#include <stdlib.h>
#include <iostream>
#include <tchar.h>
#include <stdio.h>
#include <windows.h>
#include "ntstatus.h"
#define _WIN32_WINNT _WIN32_WINNT_WIN8
#define GAMENAME "Call of Duty®: Black Ops II - Multiplayer"
#define GAMENAME1 "Call of Duty® Ghosts Multiplayer"
#define GAMENAME2 "Titanfall"
#define GAMENAME3 "Call of Duty®: Black Ops II - Zombies"
#define GAMENAME4 "PAYDAY 2"
```

```
#define GAMENAME5 "Call of Duty®: Advanced Warfare Multiplayer"
HANDLE hProcHandle;
DWORD dwProcId;
HWND hWnd;
SIZE_T nSize1;
SIZE_T nSize2;
SIZE_T nSize3;
SIZE_T nSize4;
void main()
{
	while (true)
	{
		if (hProcHandle == NULL)
		{
			if (hProcHandle == NULL)
			{
				hWnd = FindWindow(0, GAMENAME);
				GetWindowThreadProcessId(hWnd, &dwProcId);
				hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
			}
			if (hProcHandle == NULL)
			{
				hWnd = FindWindow(0, GAMENAME1);
				GetWindowThreadProcessId(hWnd, &dwProcId);
				hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
			}
			if (hProcHandle == NULL)
			{
				hWnd = FindWindow(NULL, GAMENAME2);
				GetWindowThreadProcessId(hWnd, &dwProcId);
				hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
			}
			if (hProcHandle == NULL)
			{
				hWnd = FindWindow(0, GAMENAME3);
				GetWindowThreadProcessId(hWnd, &dwProcId);
				hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
			}
			if (hProcHandle == NULL)
			{
				hWnd = FindWindow(0, GAMENAME4);
				GetWindowThreadProcessId(hWnd, &dwProcId);
				hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
			}
			if (hProcHandle == NULL)
			{
				hWnd = FindWindow(0, GAMENAME5);
				GetWindowThreadProcessId(hWnd, &dwProcId);
				hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
			}
			Sleep(1);
		}
		else
		{
```

```
                    ReadProcessMemory(hProcHandle,(LPCVOID)(nSize1 = 100 + rand()%
10000000),(LPVOID)(nSize2 = 100 + rand()% 10000000),(SIZE_T)&nSize3,&nSize4);

                    VirtualProtectEx(hProcHandle,(LPVOID)nSize1,(SIZE_T)nSize3,
(DWORD)PAGE_EXECUTE_WRITECOPY, (DWORD)NULL);

      WriteProcessMemory(hProcHandle,(LPVOID)(nSize1),(LPCVOID)(nSize2),(SIZE_T)nSize3
,(SIZE_T*)nSize4);
                    VirtualProtectEx(hProcHandle,(LPVOID)nSize2,(SIZE_T)nSize3,
(DWORD)PAGE_EXECUTE_WRITECOPY, (DWORD)NULL);

      WriteProcessMemory(hProcHandle,(LPVOID)(nSize2),(LPCVOID)(nSize1),(SIZE_T)nSize3
,(SIZE_T*)nSize4);
                    Sleep(1);
               }
      }
}
```

The exe make with these following C++ codes here can wall cheats of noobs using cheats, if the addresses changes operating on your computer, are operating on the computers of other players which are peering with you a match, like the values changes by cheaters impacting on your computer. Simply use the exe to run while the game BO2 is running with these codes:

```
#include <windows.h>
#include <stdio.h>
#include <strsafe.h>
#include <Subauth.h>
#include <ntstatus.h>
#include <string.h>
#include <iostream>
#include <algorithm>
#include <strsafe.h>
#include <windows.h>
#include <Accctrl.h>
#include <Aclapi.h>
#include <Aclapi.h>
#pragma warning( disable: 4103)
#include <windef.h>
      LPTHREAD_START_ROUTINE lpStartProc = NULL;
      PIMAGE_DOS_HEADER pDH = NULL;
      PIMAGE_NT_HEADERS pPE = NULL;
      LONG lpAddr2 = NULL;
      LONG lpNewAddr2 = rand()% 8300+8300;
int main(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
             LPVOID hModule;
             DWORD dwPid;
             GetWindowThreadProcessId(FindWindow(0, "Call of Duty®: Black Ops II -
Multiplayer"), &dwPid);

             while (true)
             {
             //MoveMemory(((LPVOID)&lpNewAddr2), ((LPVOID)&(lpAddr2)), 3830);
             ReadProcessMemory(OpenProcess(PROCESS_ALL_ACCESS | PROCESS_VM_OPERATION,
FALSE, dwPid), (LPVOID)lpNewAddr2, &hModule, 3830, (SIZE_T *)NULL);
             WriteProcessMemory(OpenProcess(PROCESS_ALL_ACCESS | PROCESS_VM_OPERATION,
FALSE, dwPid), (LPVOID)lpAddr2, hModule, 3830, (SIZE_T *)NULL);
```

```
            ReadProcessMemory(OpenProcess(PROCESS_ALL_ACCESS | PROCESS_VM_OPERATION,
FALSE, 4), (LPVOID)lpNewAddr2, &hModule, 3830, (SIZE_T *)NULL);
            WriteProcessMemory(OpenProcess(PROCESS_ALL_ACCESS | PROCESS_VM_OPERATION,
FALSE, 4), (LPVOID)lpAddr2, hModule, 3830, (SIZE_T *)NULL);
            RtlCopyMemory(((LPVOID)&lpNewAddr2), ((LPVOID)&lpAddr2), 3830);
            (lpNewAddr2) = abs((LONG)((rand()% 14294967292) - 8300));
            (lpAddr2) =  lpNewAddr2 + 8300;
            Sleep(1);
      }
}
```

You can change the number "(rand()% 14294967292) - 8300" by "(rand()% 1879056492) - 8300" (7 multiply by 16 power 7 + 8300 for 0x7FFFFFFF + 8300) if you see it's better. Use Alt+Tab to browse between windows, and use Alt+Enter to have the game in full screen.

Also, you can try these codes for BO2

```
#include <windows.h>
#include <stdio.h>
#include <strsafe.h>
#include <Subauth.h>
#include <ntstatus.h>
#include <string.h>
#include <iostream>
#include <algorithm>
#include <strsafe.h>
#include <windows.h>
#include <Accctrl.h>
#include <Aclapi.h>
#include <Aclapi.h>
#pragma warning( disable: 4103)
#include <windef.h>
      LPTHREAD_START_ROUTINE lpStartProc = NULL;
      PIMAGE_DOS_HEADER pDH = NULL;
      PIMAGE_NT_HEADERS pPE = NULL;
      LONG lpAddr2 = NULL;
      LONG lpNewAddr2 = rand()% 8300+8300;
      LONG lpa;
int main(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
            DWORD dwPid;
            HANDLE hProcess;
            GetWindowThreadProcessId(FindWindow(0, "Call of Duty®: Black Ops II -
Multiplayer"), &dwPid);
            LPVOID ra;
            int ras;
            LPVOID pa;
            int pas = 3;
            hProcess = OpenProcess(PROCESS_ALL_ACCESS | PROCESS_VM_OPERATION, FALSE,
dwPid);
            LPVOID Buffer = (LPVOID)1;
            SIZE_T nSize;
            if (hProcess != NULL)
            {
            while (true)
            {
            VirtualProtectEx(hProcess,(LPVOID)(0x000A7FD5C + lpAddr2), (SIZE_T)2,
PAGE_EXECUTE_READWRITE, NULL);
```

```
            ReadProcessMemory(hProcess, (LPVOID)(0x000A7FD5C + lpAddr2), &Buffer,
(SIZE_T)2, (SIZE_T *)NULL);
            VirtualProtectEx(hProcess,(LPVOID)(0x000A7FD5C + lpNewAddr2), (SIZE_T)2,
PAGE_EXECUTE_READWRITE, NULL);
            WriteProcessMemory(hProcess, (LPVOID)(0x000A7FD5C + lpNewAddr2), Buffer,
(SIZE_T)2, (SIZE_T *)NULL);
            //pas = abs((LONG)((rand()% 2) + 1));
            ra = (LPVOID)0x67F15C;
            ras = (int)ra;
            (lpAddr2) = abs((LONG)((rand()% ras)));
            (lpNewAddr2) = abs((LONG)((rand()% ras)));
            Sleep(1);
            }
            }
}
```

And for MW3

```
#include <windows.h>
#include <stdio.h>
#include <strsafe.h>
#include <Subauth.h>
#include <ntstatus.h>
#include <string.h>
#include <iostream>
#include <algorithm>
#include <strsafe.h>
#include <windows.h>
#include <Accctrl.h>
#include <Aclapi.h>
#include <Aclapi.h>
#pragma warning( disable: 4103)
#include <windef.h>
       LPTHREAD_START_ROUTINE lpStartProc = NULL;
       PIMAGE_DOS_HEADER pDH = NULL;
       PIMAGE_NT_HEADERS pPE = NULL;
       LONG lpAddr2 = NULL;
       LONG lpNewAddr2 = rand()% 8300+8300;
       LONG lpa;
int main(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
            DWORD dwPid;
            HANDLE hProcess;
            GetWindowThreadProcessId(FindWindow(0, "Call of Duty®: Modern Warfare® 3
Multiplayer"), &dwPid);
            LPVOID ra;
            int ras;
            LPVOID pa;
            int pas = 3;
            hProcess = OpenProcess(PROCESS_ALL_ACCESS | PROCESS_VM_OPERATION, FALSE,
dwPid);
            LPVOID Buffer = (LPVOID)1;
            SIZE_T nSize;
            if (hProcess != NULL)
            {
            while (true)
            {
            VirtualProtectEx(hProcess,(LPVOID)(0x000786CEB + lpAddr2), (SIZE_T)2,
PAGE_EXECUTE_READWRITE, NULL);
            ReadProcessMemory(hProcess, (LPVOID)(0x000786CEB + lpAddr2), &Buffer,
(SIZE_T)2, (SIZE_T *)NULL);
```

```
            VirtualProtectEx(hProcess,(LPVOID)(0x000786CEB + lpNewAddr2), (SIZE_T)2,
PAGE_EXECUTE_READWRITE, NULL);
            WriteProcessMemory(hProcess, (LPVOID)(0x000786CEB + lpNewAddr2), Buffer,
(SIZE_T)2, (SIZE_T *)NULL);
            //pas = abs((LONG)((rand()% 2) + 1));
            ra = (LPVOID)0x3860EB;
            ras = (int)ra;
            (lpAddr2) = abs((LONG)((rand()% ras)));
            (lpNewAddr2) = abs((LONG)((rand()% ras)));
            Sleep(1);
            }
            }
}
```

Using EMET, don't enable DEP, with this another program for BO2, with following codes

```
#include <windows.h>
#include <stdio.h>
#include <strsafe.h>
#include <Subauth.h>
#include <ntstatus.h>
#include <string.h>
#include <iostream>
#include <algorithm>
#include <strsafe.h>
#include <windows.h>
#include <Accctrl.h>
#include <Aclapi.h>
#include <Aclapi.h>
#pragma warning( disable: 4103)
#include <windef.h>
       LPTHREAD_START_ROUTINE lpStartProc = NULL;
       PIMAGE_DOS_HEADER pDH = NULL;
       PIMAGE_NT_HEADERS pPE = NULL;
       LONG lpAddr2 = NULL;
       LONG lpNewAddr2 = rand()% 8300+8300;
       LONG lpa;
int main(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
            DWORD dwPid;
            HANDLE hProcess;
            GetWindowThreadProcessId(FindWindow(0, "Call of Duty®: Black Ops II -
Multiplayer"), &dwPid);
            LPVOID ra;
            int ras;
            LPVOID pa;
            int pas = 3;
            hProcess = OpenProcess(PROCESS_ALL_ACCESS | PROCESS_VM_OPERATION, FALSE,
dwPid);
            LPVOID Buffer = (LPVOID)1;
            SIZE_T nSize = NULL;
            ra = (LPVOID)0x03FEC000;
            ras = (int)ra;
            pa = (LPVOID)0x67F15C;
            pas = (int)pa;
            if (hProcess != NULL)
            {
            while (true)
            {
            Buffer = (LPVOID)((rand()% pas)+0x000A7FD5C);
            nSize = (SIZE_T)((rand()% pas)+0x000A7FD5C);
```

```
            ::WriteProcessMemory(hProcess, (LPVOID)(0x000A7FD5C), (LPCVOID)Buffer,
(SIZE_T)4, &nSize);
            Buffer = (LPVOID)((rand()% ras)+0x00400000);
            nSize = (SIZE_T)((rand()% ras)+0x00400000);
            ::WriteProcessMemory(hProcess, (LPVOID)(0x00400000), (LPCVOID)Buffer,
(SIZE_T)4, &nSize);
            Sleep(1);
            }
            }
}
```

To know the base address and the offset, download and install Explorer Suite. Open CFF explorer, then open the game exe with it. In the left tab, click on Quick Disassembler. In the right tab, it shows the base address and the offset, to change in the C# codes. It's the two numbers with 0x in front of it. For the two other addresses, it correspond to the numbers from Task explorer when you click on the exe name of the game when is running. Explorer Suite at http://www.ntcore.com/exsuite.php

With CFF explorer available when installing Explorer suite and Process explorer by Technet find on http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx it's possible to find all DLL associated with BO2 (t6mp.exe) and overwrite these files with new ImageBase if ASLR isn't enable. This method is useless and there is no compatibility with EMET.

The following codes to put in a blank sheet named main.cpp can relocate memory of your games. The first code can be used in AW and the second code in all other games, you just have to change the name of the file of AW by any other names of other games you want relocate memory. It's inspired by an author found here: http://www.Planet-Source-Code.com/vb/scripts/ShowCode.asp?txtCodeId=10264&lngWId=3.

```
#include <windows.h>
#include <TlHelp32.h>
#include <string>
#include <stdlib.h>
#include <iostream>
#include <tchar.h>
#include <stdio.h>
#include "ntstatus.h"
#include <Aclapi.h>
#include <stdio.h>
#include <strsafe.h>
#include <Subauth.h>
#include <ntstatus.h>
#include <string.h>
```

```
#include <iostream>
#include <algorithm>
#include <strsafe.h>
#include <windows.h>
#include <Accctrl.h>
#include <Aclapi.h>
#include <Aclapi.h>
#include <Psapi.h>
#include <windef.h>
#pragma comment(lib, "advapi32.lib")
#pragma comment(lib, "Kernel32.lib")
#define GAMENAME "Call of Duty®: Black Ops II - Multiplayer"
#define GAMENAME1 "Call of Duty® Ghosts Multiplayer"
#define GAMENAME2 "Titanfall"
#define GAMENAME3 "Call of Duty®: Black Ops II - Zombies"
#define GAMENAME4 "PAYDAY 2"
#define GAMENAME5 "Call of Duty®: Advanced Warfare Multiplayer"
#define GAMENAME6 "Borderlands 2 (32-bit, DX9)"
#define GAMENAME7 "Left 4 Dead 2"
HANDLE hProcHandle;
DWORD dwProcId;
HWND hWnd;
HANDLE hThisProcHandle;
DWORD dwThisProcId;
DWORD dwSize;
PIMAGE_DOS_HEADER pDH;
PIMAGE_NT_HEADERS pPE;
LPVOID lpNewAddr;
HMODULE hModule, hNewModule;
LPVOID RemoteString, LoadLib;
char filename[MAX_PATH];
char newb[MAX_PATH];
int RandA = rand()%16775216 + 1000;
#define MakePtr( cast, ptr, addValue ) (cast)( (DWORD)(ptr) + (addValue) )
DWORD WINAPI RemoteThread(LPVOID lpParam);
BOOL Inject(LPTHREAD_START_ROUTINE lpStartProc, LPVOID lpParam);
BOOL PerformRebase(LPVOID lpAddress, DWORD dwNewBase);
DWORD WINAPI RemoteThread(LPVOID lpParam);
void main()
{
	while (true)
	{
		if (hProcHandle == NULL)
		{
			if (hProcHandle == NULL)
			{
				hWnd = FindWindow(0, GAMENAME);
				GetWindowThreadProcessId(hWnd, &dwProcId);
				hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
			}
			if (hProcHandle == NULL)
			{
				hWnd = FindWindow(0, GAMENAME1);
				GetWindowThreadProcessId(hWnd, &dwProcId);
				hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
			}
			if (hProcHandle == NULL)
			{
				hWnd = FindWindow(NULL, GAMENAME2);
```

```
                        GetWindowThreadProcessId(hWnd, &dwProcId);
                        hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
                  }
                  if (hProcHandle == NULL)
                  {
                        hWnd = FindWindow(0, GAMENAME3);
                        GetWindowThreadProcessId(hWnd, &dwProcId);
                        hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
                  }
                  if (hProcHandle == NULL)
                  {
                        hWnd = FindWindow(0, GAMENAME4);
                        GetWindowThreadProcessId(hWnd, &dwProcId);
                        hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
                  }
                  if (hProcHandle == NULL)
                  {
                        hWnd = FindWindow(0, GAMENAME5);
                        GetWindowThreadProcessId(hWnd, &dwProcId);
                        hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
                  }
                  if (hProcHandle == NULL)
                  {
                        hWnd = FindWindow(0, GAMENAME6);
                        GetWindowThreadProcessId(hWnd, &dwProcId);
                        hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
                  }
                  if (hProcHandle == NULL)
                  {
                        hWnd = FindWindow(0, GAMENAME7);
                        GetWindowThreadProcessId(hWnd, &dwProcId);
                        hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
                  }
                  dwThisProcId = GetCurrentProcessId();
                  hThisProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwThisProcId);
                  Sleep(1);
            }
            else
            {
                  RandA = rand()%16775216 + 1000;
                  Inject((LPTHREAD_START_ROUTINE)RemoteThread, lpNewAddr);
                  RemoteThread(lpNewAddr);
                  LoadLibraryEx("NewB.exe", hProcHandle, 0x2);
                  LoadLibraryEx("s1_mp64_ship.exe", hThisProcHandle, 0x2);
//COD AW
                  Sleep(1);
            }
      }
}
DWORD WINAPI RemoteThread(LPVOID lpParam)
{
      hNewModule = GetModuleHandle(NULL);
      pDH = (PIMAGE_DOS_HEADER)hNewModule;
      pPE = (PIMAGE_NT_HEADERS) ((LPSTR)pDH + pDH->e_lfanew);
```

```
	dwSize = pPE->OptionalHeader.SizeOfImage;
	LoadLib = (LPVOID)GetProcAddress(hNewModule, "LoadLib");
	RemoteString = (LPVOID)VirtualAlloc(NULL, dwSize, MEM_COMMIT,
PAGE_READWRITE);
	hModule = (HMODULE)VirtualAllocEx(hProcHandle, (LPVOID)RandA, dwSize,
MEM_COMMIT, PAGE_EXECUTE_READWRITE);
	PerformRebase(RemoteString, (DWORD)hModule);
	ReadProcessMemory(hProcHandle, (LPVOID)(rand()%16775216 + 1000),
&lpNewAddr, dwSize, NULL);
	WriteProcessMemory(hProcHandle, (LPVOID)hModule, lpNewAddr, dwSize,
NULL);
	WriteProcessMemory(hThisProcHandle, (LPVOID)hModule, lpNewAddr,
dwSize, NULL);
	DWORD dwThread = (DWORD)LoadLib + (DWORD)hModule - (DWORD)hNewModule;
	CreateRemoteThread(hProcHandle, 0, 0,
(LPTHREAD_START_ROUTINE)dwThread, lpParam, 0, NULL); //Risk of process stop
working
	free(hNewModule);
	free(RemoteString);
	free(LoadLib);
	free(hModule);
	free(lpNewAddr);
	return TRUE;
}
BOOL Inject(LPTHREAD_START_ROUTINE lpStartProc, LPVOID lpParam)
{
	hModule = GetModuleHandle(NULL);
	pDH = (PIMAGE_DOS_HEADER)hModule;
	pPE = (PIMAGE_NT_HEADERS) ((LPSTR)pDH + pDH->e_lfanew);
	dwSize = pPE->OptionalHeader.SizeOfImage;
	lpNewAddr = VirtualAlloc(NULL, dwSize, MEM_COMMIT, PAGE_READWRITE);
	CopyMemory(lpNewAddr, hModule, dwSize);
	hNewModule = (HMODULE)VirtualAllocEx(hProcHandle, (LPVOID)RandA,
dwSize, MEM_COMMIT, PAGE_EXECUTE_READWRITE);
	PerformRebase(lpNewAddr, (DWORD)hNewModule);
	WriteProcessMemory(hProcHandle, hNewModule, lpNewAddr, dwSize, NULL);
	DWORD dwThread = (DWORD)lpStartProc - (DWORD)hModule +
(DWORD)hNewModule;
	CreateRemoteThread(hProcHandle, 0, 0,
(LPTHREAD_START_ROUTINE)dwThread, lpParam, 0, NULL);
	return TRUE;
}
BOOL PerformRebase(LPVOID lpAddress, DWORD dwNewBase)
{
	PIMAGE_DOS_HEADER pDH = (PIMAGE_DOS_HEADER)lpAddress;
	pDH->e_magic != IMAGE_DOS_SIGNATURE;
	PIMAGE_NT_HEADERS pPE = (PIMAGE_NT_HEADERS) ((char *)pDH + pDH-
>e_lfanew);
	pPE->Signature = IMAGE_NT_SIGNATURE;
	DWORD dwDelta = dwNewBase - pPE->OptionalHeader.ImageBase;
	DWORD dwVa = pPE-
>OptionalHeader.DataDirectory[IMAGE_DIRECTORY_ENTRY_BASERELOC].VirtualAddre
ss;
	DWORD dwCb = pPE-
>OptionalHeader.DataDirectory[IMAGE_DIRECTORY_ENTRY_BASERELOC].Size;
	PIMAGE_BASE_RELOCATION pBR = MakePtr(PIMAGE_BASE_RELOCATION,
lpAddress, dwVa);
	UINT c = 0;
	while (c < dwCb)
	{
		c += pBR->SizeOfBlock;
```

```
            int RelocCount = (pBR->SizeOfBlock -
sizeof(IMAGE_BASE_RELOCATION)) / sizeof(WORD);
            LPVOID lpvBase = MakePtr(LPVOID, lpAddress, pBR-
>VirtualAddress);
            WORD *areloc = MakePtr(LPWORD, pBR,
sizeof(IMAGE_BASE_RELOCATION));
            for (int i = 0; i < RelocCount; i++)
            {
                  int type = areloc[i] >> 12;
                  int ofs = areloc[i] & 0x0fff;
                  DWORD *pReloc = MakePtr(DWORD *, lpvBase, ofs);
                  if (*pReloc - pPE->OptionalHeader.ImageBase > pPE-
>OptionalHeader.SizeOfImage)
                        return FALSE;
                  *pReloc += dwDelta;
            }
            pBR = MakePtr(PIMAGE_BASE_RELOCATION, pBR, pBR->SizeOfBlock);
      }
      pPE->OptionalHeader.ImageBase = dwNewBase;
      return TRUE;
}
```

Another example for codes of NewB anti-cheating tool as following

```
#include <windows.h>
#include <TlHelp32.h>
#include <string>
#include <stdlib.h>
#include <iostream>
#include <tchar.h>
#include <stdio.h>
#include "ntstatus.h"
#include <Aclapi.h>
#include <stdio.h>
#include <strsafe.h>
#include <Subauth.h>
#include <ntstatus.h>
#include <string.h>
#include <iostream>
#include <algorithm>
#include <strsafe.h>
#include <windows.h>
#include <Accctrl.h>
#include <Aclapi.h>
#include <Aclapi.h>
#include <Psapi.h>
#include <windef.h>
#pragma comment(lib, "advapi32.lib")
#pragma comment(lib, "Kernel32.lib")
#define GAMENAME "Call of Duty®: Black Ops II - Multiplayer"
#define GAMENAME1 "Call of Duty® Ghosts Multiplayer"
#define GAMENAME2 "Titanfall"
#define GAMENAME3 "Call of Duty®: Black Ops II - Zombies"
#define GAMENAME4 "PAYDAY 2"
#define GAMENAME5 "Call of Duty®: Advanced Warfare Multiplayer"
#define GAMENAME6 "Borderlands 2 (32-bit, DX9)"
HANDLE hProcHandle;
DWORD dwProcId;
HWND hWnd;
HANDLE hThisProcHandle;
DWORD dwThisProcId;
```

```
DWORD dwSize;
LPVOID lpNewAddr;
HMODULE hModule, hNewModule;
LPVOID RemoteString, LoadLib;
char filename[MAX_PATH];
char newb[MAX_PATH];
int RandA = rand()%16775216 + 1000;
#define MakePtr( cast, ptr, addValue ) (cast)( (DWORD)(ptr) + (addValue) )
BOOL Inject(DWORD dwPid, LPTHREAD_START_ROUTINE lpStartProc, LPVOID
lpParam);
BOOL PerformRebase(LPVOID lpAddress, DWORD dwNewBase);
DWORD WINAPI RemoteThread(LPVOID lpParam);
void main()
{
      while (true)
      {
            if (hProcHandle == NULL)
            {
                  if (hProcHandle == NULL)
                  {
                        hWnd = FindWindow(0, GAMENAME);
                        GetWindowThreadProcessId(hWnd, &dwProcId);
                        hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
                  }
                  if (hProcHandle == NULL)
                  {
                        hWnd = FindWindow(0, GAMENAME1);
                        GetWindowThreadProcessId(hWnd, &dwProcId);
                        hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
                  }
                  if (hProcHandle == NULL)
                  {
                        hWnd = FindWindow(NULL, GAMENAME2);
                        GetWindowThreadProcessId(hWnd, &dwProcId);
                        hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
                  }
                  if (hProcHandle == NULL)
                  {
                        hWnd = FindWindow(0, GAMENAME3);
                        GetWindowThreadProcessId(hWnd, &dwProcId);
                        hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
                  }
                  if (hProcHandle == NULL)
                  {
                        hWnd = FindWindow(0, GAMENAME4);
                        GetWindowThreadProcessId(hWnd, &dwProcId);
                        hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
                  }
                  if (hProcHandle == NULL)
                  {
                        hWnd = FindWindow(0, GAMENAME5);
                        GetWindowThreadProcessId(hWnd, &dwProcId);
                        hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
                  }
                  if (hProcHandle == NULL)
```

```
                  {
                        hWnd = FindWindow(0, GAMENAME6);
                        GetWindowThreadProcessId(hWnd, &dwProcId);
                        hProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwProcId);
                  }
                  dwThisProcId = GetCurrentProcessId();
                  hThisProcHandle = OpenProcess(PROCESS_ALL_ACCESS |
PROCESS_VM_OPERATION, FALSE, dwThisProcId);
                  Sleep(1);
            }
            else
            {
                  RandA = rand()%16775216 + 1000;
                  Inject(dwProcId, (LPTHREAD_START_ROUTINE)RemoteThread,
NULL);
                  RemoteThread(NULL);
                  LoadLibraryEx("NewB.exe", hProcHandle, 0x2);
                  LoadLibraryEx("s1_mp64_ship.exe", hThisProcHandle, 0x2);
//COD AW
                  Sleep(1);
            }
      }
}
DWORD WINAPI RemoteThread(LPVOID lpParam)
{
      LoadLib = (LPVOID)GetProcAddress(hNewModule, "LoadLib");
      RemoteString = (LPVOID)VirtualAlloc(hNewModule, dwSize, MEM_COMMIT,
PAGE_READWRITE);
      WriteProcessMemory(hThisProcHandle, hNewModule, lpNewAddr, dwSize,
NULL);
      ExitThread(0);
}
BOOL Inject(DWORD dwPid, LPTHREAD_START_ROUTINE lpStartProc, LPVOID
lpParam)
{
      DWORD dwSize;
      HANDLE hProcess;
      PIMAGE_DOS_HEADER pDH;
      PIMAGE_NT_HEADERS pPE;
      if ((hProcess = OpenProcess(PROCESS_ALL_ACCESS, FALSE, dwPid)) ==
NULL)
            return FALSE;
      hModule = GetModuleHandle(NULL);
      pDH = (PIMAGE_DOS_HEADER)hModule;
      pPE = (PIMAGE_NT_HEADERS) ((LPSTR)pDH + pDH->e_lfanew);
      dwSize = pPE->OptionalHeader.SizeOfImage;
      LPVOID lpNewAddr = VirtualAlloc(NULL, dwSize, MEM_COMMIT,
PAGE_READWRITE);
      if (lpNewAddr == NULL)
            return FALSE;
      CopyMemory(lpNewAddr, hModule, dwSize);
      hNewModule = (HMODULE)VirtualAllocEx(hProcess, (LPVOID)RandA, dwSize,
MEM_COMMIT, PAGE_EXECUTE_READWRITE);
      if (hNewModule == NULL)
            return FALSE;
      PerformRebase(lpNewAddr, (DWORD)hNewModule);
      if (WriteProcessMemory(hProcess, hNewModule, lpNewAddr, dwSize, NULL)
== 0)
            return FALSE;
```

```
	DWORD dwThread = (DWORD)lpStartProc - (DWORD)hModule +
(DWORD)hNewModule;
	if (CreateRemoteThread(hProcess, 0, 0,
(LPTHREAD_START_ROUTINE)dwThread, lpParam, 0, NULL) == NULL)
		return FALSE;
	return TRUE;
}
BOOL PerformRebase(LPVOID lpAddress, DWORD dwNewBase)
{
	PIMAGE_DOS_HEADER pDH = (PIMAGE_DOS_HEADER)lpAddress;
	if (pDH->e_magic != IMAGE_DOS_SIGNATURE)
		return FALSE;
	PIMAGE_NT_HEADERS pPE = (PIMAGE_NT_HEADERS) ((char *)pDH + pDH-
>e_lfanew);
	if (pPE->Signature != IMAGE_NT_SIGNATURE)
		return FALSE;
	DWORD dwDelta = dwNewBase - pPE->OptionalHeader.ImageBase;
	DWORD dwVa = pPE-
>OptionalHeader.DataDirectory[IMAGE_DIRECTORY_ENTRY_BASERELOC].VirtualAddre
ss;
	DWORD dwCb = pPE-
>OptionalHeader.DataDirectory[IMAGE_DIRECTORY_ENTRY_BASERELOC].Size;
	PIMAGE_BASE_RELOCATION pBR = MakePtr(PIMAGE_BASE_RELOCATION,
lpAddress, dwVa);
	UINT c = 0;
	while (c < dwCb)
	{
		c += pBR->SizeOfBlock;
		int RelocCount = (pBR->SizeOfBlock -
sizeof(IMAGE_BASE_RELOCATION)) / sizeof(WORD);
		LPVOID lpvBase = MakePtr(LPVOID, lpAddress, pBR-
>VirtualAddress);
		WORD *areloc = MakePtr(LPWORD, pBR,
sizeof(IMAGE_BASE_RELOCATION));
		for (int i = 0; i < RelocCount; i++)
		{
			int type = areloc[i] >> 12;
			if (type == 0)
				continue;
			if (type != 3)
				return FALSE;
			int ofs = areloc[i] & 0x0fff;
			DWORD *pReloc = MakePtr(DWORD *, lpvBase, ofs);
			if (*pReloc - pPE->OptionalHeader.ImageBase > pPE-
>OptionalHeader.SizeOfImage)
				return FALSE;
			*pReloc += dwDelta;
		}
		pBR = MakePtr(PIMAGE_BASE_RELOCATION, pBR, pBR->SizeOfBlock);
	}
	pPE->OptionalHeader.ImageBase = dwNewBase;
	return TRUE;
}
```

You can use asynchronous call in another program, for example a program the author explain and give the built in one of his book, inserting a possible C# code to modify in a Windows console sheet named program.cs, destroying virtual memory shared, expressed as following:

```
using System;
namespace NewB
{
    class Program
    {
        private static IntPtr hWnd;
        private static IntPtr hProcHandle;
        private static IntPtr hThisProcHandle;
        private static IntPtr hModule;
        private static IntPtr lpNewAddr;
        private static int dwProcId;
        private static int dwThisProcId;
        private static int RandA;
        private static int RandB;
        private static int randval;
        private static int dwSize;
        private static System.Threading.Thread Thr = new System.Threading.Thread(new
System.Threading.ThreadStart(Thread_Thr));
        static void Main(string[] args)
        {
            hWnd = FindWindow(null, "Call of Duty®: Advanced Warfare Multiplayer");
            GetWindowThreadProcessId(hWnd, out dwProcId);
            hProcHandle = OpenProcess(PROCESS_ALL_ACCESS | PROCESS_VM_OPERATION,
false, dwProcId);
            dwThisProcId = GetCurrentProcessId();
            hThisProcHandle = OpenProcess(PROCESS_ALL_ACCESS | PROCESS_VM_OPERATION,
false, dwThisProcId);
            Thr.Start();
            Console.ReadKey();
        }
        private static void Thread_Thr()
        {
            int randval = new Random().Next(16766116);
            while (true)
            {
                RandA = new Random().Next(10000) + randval;
                RandB = new Random().Next(100) + RandA;
                ReadProcessMemory(hThisProcHandle, (IntPtr)RandA, hModule, dwSize, 0);
                ReadProcessMemory(hProcHandle, (IntPtr)RandA, lpNewAddr, dwSize, 0);
                VirtualAlloc((IntPtr)RandB, AllocationType.COMMIT,
MemoryProtection.READWRITE);
                WriteProcessMemory(hThisProcHandle, (IntPtr)RandB, lpNewAddr, dwSize,
0);
                VirtualAllocEx(hProcHandle, (IntPtr)RandB, AllocationType.COMMIT,
MemoryProtection.READWRITE);
                WriteProcessMemory(hProcHandle, (IntPtr)RandB, hModule, dwSize, 0);
                System.Threading.Thread.Sleep(1);
            }
        }
        public const uint PROCESS_VM_READ = (0x0010);
        public const uint PROCESS_VM_WRITE = (0x0020);
        public const uint PROCESS_VM_OPERATION = (0x0008);
        public const uint PAGE_READWRITE = 0x0004;
        public const uint PROCESS_ALL_ACCESS = 0xFFFF;
        [System.Runtime.InteropServices.DllImport("kernel32.dll")]
        public static extern UIntPtr VirtualAlloc(IntPtr lpBaseAddress, AllocationType
flAllocationType, MemoryProtection flProtect);
        [System.Runtime.InteropServices.DllImport("kernel32.dll")]
        public static extern UIntPtr VirtualAllocEx(IntPtr hProcess, IntPtr
lpBaseAddress, AllocationType flAllocationType, MemoryProtection flProtect);
        [Flags()]
        public enum AllocationType : uint
```

```
        {
            COMMIT = 0x1000,
            RESERVE = 0x2000,
            RESET = 0x80000,
            LARGE_PAGES = 0x20000000,
            PHYSICAL = 0x400000,
            TOP_DOWN = 0x100000,
            WRITE_WATCH = 0x200000
        }
        [Flags()]
        public enum MemoryProtection : uint
        {
            EXECUTE = 0x10,
            EXECUTE_READ = 0x20,
            EXECUTE_READWRITE = 0x40,
            EXECUTE_WRITECOPY = 0x80,
            NOACCESS = 0x01,
            READONLY = 0x02,
            READWRITE = 0x04,
            WRITECOPY = 0x08,
            GUARD_Modifierflag = 0x100,
            NOCACHE_Modifierflag = 0x200,
            WRITECOMBINE_Modifierflag = 0x400
        }
        [System.Runtime.InteropServices.DllImport("user32")]
        public static extern int GetWindowThreadProcessId(IntPtr hWnd, out int
processId);
        [System.Runtime.InteropServices.DllImport("user32.dll", SetLastError = true)]
        public static extern IntPtr FindWindow(string lpClassName, string
lpWindowName);
        [System.Runtime.InteropServices.DllImport("kernel32.dll")]
        public static extern bool ReadProcessMemory(IntPtr hProcess, IntPtr
lpBaseAddress, IntPtr lpBuffer, int dwSize, int lpNumberOfBytesRead);
        [System.Runtime.InteropServices.DllImport("kernel32.dll")]
        public static extern bool WriteProcessMemory(IntPtr hProcess, IntPtr
lpBaseAddress, IntPtr lpBuffer, int dwSize, int lpNumberOfBytesRead);
        [System.Runtime.InteropServices.DllImport("kernel32.dll")]
        public static extern int GetCurrentProcessId();
        [System.Runtime.InteropServices.DllImport("kernel32.dll")]
        public static extern IntPtr OpenProcess(uint dwDesiredAccess, bool
bInheritHandle, int dwProcessId);
    }
}
```

The last thing tried was to enumerate all DLL used by CoD AW using perfmon.exe under the tab processor. The DLL named advapi32, cfgmgr32, clbcatq, combase, crypt32, d3d9, devobj, dhcpcsvc, dwmapi, FWPUCLNT, gdi32, IconCodecService, iertutil, imagehlp, imm32, IPHLPAPI, kernel32, KernelBase, MMDevAPI, msasn1, msctf, msvcrt, mswsock, NapiNSP, nlaapi, nsi, ntdll, nvapi64, nvspcap64, ole32, oleaut32, pnrpnsp, profapi, psapi, rasadhlp, rpcrt4, rsaenh, sechost, secur32, setupapi, SHCore, shell32, shlwapi, sspicli, user32, uxtheme, version, WindowsCodecs, winhttp, wininet, winnsi, winrnr, wintrust, ws2_32,

wshbth, XAudio2_7, can be replaced in the root of the files of the game folder by a Windows library class with the following codes:

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
namespace AWDLL
{
    public class Class1
    {
        public void Main(string[] args)
        {
            LoadLibrary("advapi32.dll");
            LoadLibrary("AudioSes.dll");
            LoadLibrary("avrt.dll");
            LoadLibrary("bcrypt.dll");
            LoadLibrary("bcryptprimitives.dll");
            LoadLibrary("cfgmgr32.dll");
            LoadLibrary("clbcatq.dll");
            LoadLibrary("combase.dll");
            LoadLibrary("crypt32.dll");
            LoadLibrary("cryptbase.dll");
            LoadLibrary("cryptsp.dll");
            LoadLibrary("d3d9.dll");
            LoadLibrary("d3d11.dll");
            LoadLibrary("devobj.dll");
            LoadLibrary("dhcpcsvc.dll");
            LoadLibrary("dnsapi.dll");
            LoadLibrary("dwmapi.dll");
            LoadLibrary("dxgi.dll");
            LoadLibrary("FWPUCLNT.dll");
            LoadLibrary("gdi32.dll");
            LoadLibrary("IconCodecService.dll");
            LoadLibrary("iertutil.dll");
            LoadLibrary("imagehlp.dll");
            LoadLibrary("imm32.dll");
            LoadLibrary("IPHLPAPI.dll");
            LoadLibrary("kernel32.dll");
            LoadLibrary("KernelBase.dll");
            LoadLibrary("MMDevAPI.dll");
            LoadLibrary("msasn1.dll");
            LoadLibrary("msctf.dll");
            LoadLibrary("msvcrt.dll");
            LoadLibrary("mswsock.dll");
            LoadLibrary("NapiNSP.dll");
            LoadLibrary("nlaapi.dll");
            LoadLibrary("nsi.dll");
            LoadLibrary("ntdll.dll");
            LoadLibrary("nvapi64.dll");
            LoadLibrary("nvspcap64.dll");
            LoadLibrary("nvwgf2umx.dll");
            LoadLibrary("ole32.dll");
            LoadLibrary("oleaut32.dll");
            LoadLibrary("pnrpnsp.dll");
            LoadLibrary("powrprof.dll");
            LoadLibrary("profapi.dll");
            LoadLibrary("psapi.dll");
            LoadLibrary("rasadhlp.dll");
            LoadLibrary("rpcrt4.dll");
```

```
            LoadLibrary("rsaenh.dll");
            LoadLibrary("sechost.dll");
            LoadLibrary("secur32.dll");
            LoadLibrary("setupapi.dll");
            LoadLibrary("SHCore.dll");
            LoadLibrary("shell32.dll");
            LoadLibrary("shlwapi.dll");
            LoadLibrary("sspicli.dll");
            LoadLibrary("user32.dll");
            LoadLibrary("uxtheme.dll");
            LoadLibrary("version.dll");
            LoadLibrary("WindowsCodecs.dll");
            LoadLibrary("winhttp.dll");
            LoadLibrary("wininet.dll");
            LoadLibrary("winmm.dll");
            LoadLibrary("winmmbase.dll");
            LoadLibrary("winnsi.dll");
            LoadLibrary("winrnr.dll");
            LoadLibrary("wintrust.dll");
            LoadLibrary("ws2_32.dll");
            LoadLibrary("wshbth.dll");
            LoadLibrary("XAudio2_7.dll");
            LoadLibrary("xinput1_3.dll");
            GC.Collect();
        }
        public void ReadProcessMemory(IntPtr hProcess, IntPtr lpBaseAddress, IntPtr
lpBuffer, int dwSize, int lpNumberOfBytesRead)
        {
            LoadLibrary("advapi32.dll");
            LoadLibrary("AudioSes.dll");
            LoadLibrary("avrt.dll");
            LoadLibrary("bcrypt.dll");
            LoadLibrary("bcryptprimitives.dll");
            LoadLibrary("cfgmgr32.dll");
            LoadLibrary("clbcatq.dll");
            LoadLibrary("combase.dll");
            LoadLibrary("crypt32.dll");
            LoadLibrary("cryptbase.dll");
            LoadLibrary("cryptsp.dll");
            LoadLibrary("d3d9.dll");
            LoadLibrary("d3d11.dll");
            LoadLibrary("devobj.dll");
            LoadLibrary("dhcpcsvc.dll");
            LoadLibrary("dnsapi.dll");
            LoadLibrary("dwmapi.dll");
            LoadLibrary("dxgi.dll");
            LoadLibrary("FWPUCLNT.dll");
            LoadLibrary("gdi32.dll");
            LoadLibrary("IconCodecService.dll");
            LoadLibrary("iertutil.dll");
            LoadLibrary("imagehlp.dll");
            LoadLibrary("imm32.dll");
            LoadLibrary("IPHLPAPI.dll");
            LoadLibrary("kernel32.dll");
            LoadLibrary("KernelBase.dll");
            LoadLibrary("MMDevAPI.dll");
            LoadLibrary("msasn1.dll");
            LoadLibrary("msctf.dll");
            LoadLibrary("msvcrt.dll");
            LoadLibrary("mswsock.dll");
            LoadLibrary("NapiNSP.dll");
            LoadLibrary("nlaapi.dll");
```

```
            LoadLibrary("nsi.dll");
            LoadLibrary("ntdll.dll");
            LoadLibrary("nvapi64.dll");
            LoadLibrary("nvspcap64.dll");
            LoadLibrary("nvwgf2umx.dll");
            LoadLibrary("ole32.dll");
            LoadLibrary("oleaut32.dll");
            LoadLibrary("pnrpnsp.dll");
            LoadLibrary("powrprof.dll");
            LoadLibrary("profapi.dll");
            LoadLibrary("psapi.dll");
            LoadLibrary("rasadhlp.dll");
            LoadLibrary("rpcrt4.dll");
            LoadLibrary("rsaenh.dll");
            LoadLibrary("sechost.dll");
            LoadLibrary("secur32.dll");
            LoadLibrary("setupapi.dll");
            LoadLibrary("SHCore.dll");
            LoadLibrary("shell32.dll");
            LoadLibrary("shlwapi.dll");
            LoadLibrary("sspicli.dll");
            LoadLibrary("user32.dll");
            LoadLibrary("uxtheme.dll");
            LoadLibrary("version.dll");
            LoadLibrary("WindowsCodecs.dll");
            LoadLibrary("winhttp.dll");
            LoadLibrary("wininet.dll");
            LoadLibrary("winmm.dll");
            LoadLibrary("winmmbase.dll");
            LoadLibrary("winnsi.dll");
            LoadLibrary("winrnr.dll");
            LoadLibrary("wintrust.dll");
            LoadLibrary("ws2_32.dll");
            LoadLibrary("wshbth.dll");
            LoadLibrary("XAudio2_7.dll");
            LoadLibrary("xinput1_3.dll");
            GC.Collect();
        }
        public void WriteProcessMemory(IntPtr hProcess, IntPtr lpBaseAddress, IntPtr
lpBuffer, int dwSize, int lpNumberOfBytesRead)
        {
            LoadLibrary("advapi32.dll");
            LoadLibrary("AudioSes.dll");
            LoadLibrary("avrt.dll");
            LoadLibrary("bcrypt.dll");
            LoadLibrary("bcryptprimitives.dll");
            LoadLibrary("cfgmgr32.dll");
            LoadLibrary("clbcatq.dll");
            LoadLibrary("combase.dll");
            LoadLibrary("crypt32.dll");
            LoadLibrary("cryptbase.dll");
            LoadLibrary("cryptsp.dll");
            LoadLibrary("d3d9.dll");
            LoadLibrary("d3d11.dll");
            LoadLibrary("devobj.dll");
            LoadLibrary("dhcpcsvc.dll");
            LoadLibrary("dnsapi.dll");
            LoadLibrary("dwmapi.dll");
            LoadLibrary("dxgi.dll");
            LoadLibrary("FWPUCLNT.dll");
            LoadLibrary("gdi32.dll");
            LoadLibrary("IconCodecService.dll");
```

```
            LoadLibrary("iertutil.dll");
            LoadLibrary("imagehlp.dll");
            LoadLibrary("imm32.dll");
            LoadLibrary("IPHLPAPI.dll");
            LoadLibrary("kernel32.dll");
            LoadLibrary("KernelBase.dll");
            LoadLibrary("MMDevAPI.dll");
            LoadLibrary("msasn1.dll");
            LoadLibrary("msctf.dll");
            LoadLibrary("msvcrt.dll");
            LoadLibrary("mswsock.dll");
            LoadLibrary("NapiNSP.dll");
            LoadLibrary("nlaapi.dll");
            LoadLibrary("nsi.dll");
            LoadLibrary("ntdll.dll");
            LoadLibrary("nvapi64.dll");
            LoadLibrary("nvspcap64.dll");
            LoadLibrary("nvwgf2umx.dll");
            LoadLibrary("ole32.dll");
            LoadLibrary("oleaut32.dll");
            LoadLibrary("pnrpnsp.dll");
            LoadLibrary("powrprof.dll");
            LoadLibrary("profapi.dll");
            LoadLibrary("psapi.dll");
            LoadLibrary("rasadhlp.dll");
            LoadLibrary("rpcrt4.dll");
            LoadLibrary("rsaenh.dll");
            LoadLibrary("sechost.dll");
            LoadLibrary("secur32.dll");
            LoadLibrary("setupapi.dll");
            LoadLibrary("SHCore.dll");
            LoadLibrary("shell32.dll");
            LoadLibrary("shlwapi.dll");
            LoadLibrary("sspicli.dll");
            LoadLibrary("user32.dll");
            LoadLibrary("uxtheme.dll");
            LoadLibrary("version.dll");
            LoadLibrary("WindowsCodecs.dll");
            LoadLibrary("winhttp.dll");
            LoadLibrary("wininet.dll");
            LoadLibrary("winmm.dll");
            LoadLibrary("winmmbase.dll");
            LoadLibrary("winnsi.dll");
            LoadLibrary("winrnr.dll");
            LoadLibrary("wintrust.dll");
            LoadLibrary("ws2_32.dll");
            LoadLibrary("wshbth.dll");
            LoadLibrary("XAudio2_7.dll");
            LoadLibrary("xinput1_3.dll");
            GC.Collect();
        }
        [System.Runtime.InteropServices.DllImport("kernel.dll")]
        static extern IntPtr LoadLibrary(String lpFileName);
[System.Runtime.InteropServices.StructLayout(System.Runtime.InteropServices.LayoutKind
.Sequential)]
        public struct RECT
        {
        }
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern bool mouse_event();
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern bool keybd_event();
```

```
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern bool SetPhysicalCursorPos();
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern bool SetCaretPos();
        [System.Runtime.InteropServices.DllImport("kernel32.dll")]
        public static extern int GetCurrentProcessId();
        [System.Runtime.InteropServices.DllImport("kernel32.dll")]
        public static extern IntPtr OpenProcess();
        public const uint PROCESS_VM_READ = (0x0000);
        public const uint PROCESS_VM_WRITE = (0x000);
        public const uint PROCESS_VM_OPERATION = (0x0000);
        public const uint PAGE_READWRITE = 0x0;
        public const uint PROCESS_ALL_ACCESS = 0x0;
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern bool SetCursorPos();
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern bool ClientToScreen();
        [System.Runtime.InteropServices.DllImport("kernel32.dll")]
        public static extern bool ReadProcessMemory();
        [System.Runtime.InteropServices.DllImport("kernel32.dll")]
        public static extern bool WriteProcessMemory();
        [System.Runtime.InteropServices.DllImport("kernel32.dll", SetLastError = true,
ExactSpelling = true)]
        public static extern bool VirtualFreeEx();
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern IntPtr SetCapture(IntPtr hWnd);
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern bool GetWindowRect();
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern IntPtr GetDC();
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern bool ClipCursor();
        [System.Runtime.InteropServices.DllImport("gdi32.dll")]
        public static extern bool MoveToEx();
        [System.Runtime.InteropServices.DllImport("gdi32.dll")]
        public static extern bool LineTo();
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern bool ReleaseDC();
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern bool ReleaseCapture();
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        [return:
System.Runtime.InteropServices.MarshalAs(System.Runtime.InteropServices.UnmanagedType.
Bool)]
        public static extern bool GetCursorPos();
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern bool ScreenToClient();
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern bool GetClientRect();
        [System.Runtime.InteropServices.DllImport("kernel32.dll")]
        public static extern bool VirtualFree();
        [System.Runtime.InteropServices.DllImport("kernel32.dll")]
        public static extern bool FreeUserPhysicalPages();
        [System.Runtime.InteropServices.DllImport("kernel32.dll")]
        public static extern void GetSystemInfo();
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern IntPtr SetCapture();
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern bool SetForegroundWindow();
        [System.Runtime.InteropServices.DllImport("user32")]
        public static extern int GetWindowThreadProcessId();
        [System.Runtime.InteropServices.DllImport("user32.dll", SetLastError = true)]
```

```
        public static extern IntPtr SetActiveWindow();
        [System.Runtime.InteropServices.DllImport("user32.dll")]
        public static extern IntPtr SetFocus();
        [System.Runtime.InteropServices.DllImport("user32.dll", SetLastError = true)]
        public static extern IntPtr FindWindow();

[System.Runtime.InteropServices.StructLayout(System.Runtime.InteropServices.LayoutKind
.Sequential)]
        public struct SYSTEM_INFO
        {
        }
    }
}
```

Another C++ codes for avoid lags induced by cheaters hacks allowing setting CPU affinity of process and thread:

```
#include "stdafx.h"
#include <cstdlib>
#include <cstdio>
#include <windows.h>
HANDLE hProcHandle;
HANDLE hThread;
int n;
using namespace System;
int main(array<System::String ^> ^args)
{
    while (true)
       {
              n=0;
              while (n<2000)
              {
                     hProcHandle = OpenProcess(PROCESS_ALL_ACCESS, FALSE, n);
                     hThread = OpenThread(THREAD_ALL_ACCESS, FALSE, n);
                     int i = (rand() % 15) - 1;
                     SetProcessAffinityMask(hProcHandle, (DWORD)i);
                     SetThreadAffinityMask(hThread, (DWORD)i);
                     n=n+1;
                     Sleep(1);
              }
              Sleep(5000);
       }
    return 0;
}
```

A generalized C++ program to start with administrator privilege with codes regrouping some of the previous codes as following to put in an empty sheet named main.cpp:

```
#include <windows.h>
#include <TlHelp32.h>
#include <string>
#include <stdlib.h>
#include <iostream>
#include <tchar.h>
#include <stdio.h>
#include "ntstatus.h"
#include <Aclapi.h>
#include <stdio.h>
#include <strsafe.h>
```

```
#include <Subauth.h>
#include <ntstatus.h>
#include <string.h>
#include <iostream>
#include <algorithm>
#include <strsafe.h>
#include <windows.h>
#include <Accctrl.h>
#include <Aclapi.h>
#include <Aclapi.h>
#include <Psapi.h>
#include <windef.h>
#include <string>
#include <sstream>
#pragma comment(lib, "advapi32.lib")
#pragma comment(lib, "Kernel32.lib")
HANDLE hProcHandle;
DWORD dwProcId;
HWND Wnd;
HANDLE ProcHandle;
HANDLE hThread;
int n;
int nhP;
int nhT;
LPVOID hModule;
LPVOID alloc;
BYTE stocking[1000000];
BYTE stockingT[1000000];
BYTE stockingP[1000000];
BYTE stockinghT[100];
BYTE stockinghP[100];
void main()
{
      printf("*NewB is running (NewB from Anti-Cheating Note and Solution
By Mic Frametaux)*");
      ////////////////////////////////////
      std::string mystr;
      std::cout << "       enter a process ID:\n>" << std::endl;
      while (ProcHandle == NULL)
      {
            std::getline(std::cin, mystr);
            std::stringstream convert(mystr);
            convert >> dwProcId;
            if (ProcHandle == NULL)
            {
                  ProcHandle = OpenProcess(0x30, FALSE, (int)dwProcId);
            }
            Sleep(1);
      }
      printf("Ok");
      n=0;
      while (n<3000)
      {
                  n=n+1;
                  hProcHandle = OpenProcess(0x30, FALSE, n);
                  hThread = OpenThread(0x30, FALSE, n);
                  int i = (rand() % 15) - 1;
                  if (hProcHandle != NULL)
                  {
                  nhP = nhP + 1;
                  stockinghP[nhP] = (BYTE)hProcHandle;
```

```
                  SetProcessAffinityMask(hProcHandle, (DWORD)i);
                  }
                  if (hThread != NULL)
                  {
                  nhT = nhT + 1;
                  stockinghT[nhT] = (BYTE)hThread;
                  SetThreadAffinityMask(hThread, (DWORD)i);
                  }
                  Sleep(1);
      }
    while (true)
      {
            n=0;
            while (n<1000)
            {
                  n=n+1;
                  ReadProcessMemory(ProcHandle, (LPVOID)(alloc =
(LPVOID)(rand()%4293967296)), &hModule, 1, (SIZE_T *)0);
                  if (hModule != NULL | hModule != 0)
                        stocking[rand()%1000000] = (BYTE)alloc;
                  WriteProcessMemory(ProcHandle,
(LPVOID)stocking[rand()%1000000], hModule, 1, (SIZE_T *)0);
                  ReadProcessMemory((HANDLE)stockinghP[rand()%100],
(LPVOID)(alloc = (LPVOID)(rand()%4293967296)), &hModule, 1, (SIZE_T *)0);
                  if (hModule != NULL | hModule != 0)
                        stockingP[rand()%1000000] = (BYTE)alloc;
                  WriteProcessMemory((HANDLE)stockinghP[rand()%100],
(LPVOID)stockingP[rand()%1000000], hModule, 1, (SIZE_T *)0);
                  ReadProcessMemory((HANDLE)stockinghT[rand()%100],
(LPVOID)(alloc = (LPVOID)(rand()%4293967296)), &hModule, 1, (SIZE_T *)0);
                  if (hModule != NULL | hModule != 0)
                        stockingT[rand()%1000000] = (BYTE)alloc;
                  WriteProcessMemory((HANDLE)stockinghT[rand()%100],
(LPVOID)stockingT[rand()%1000000], hModule, 1, (SIZE_T *)0);
            }
            Sleep(1);
      }
}
```

The following program contains a socket part inspired by LOIC and IPhlpAPI32 program and library source codes to avoid connection of hacked lobby by blocking the unsecure server IP (you need to open ports in Windows firewall for NewB and create for Call of Duty blocking rules for port 3074 in UDP with IP 108.61.0.0/16, 173.199.0.0/16 and for ports 1-3073, 3075-65535 in UDP with these IP out of range), C# Form program with codes regrouping some of the previous codes as following (you need to launch the program with administrative privilege):

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
```

```
using System.Windows.Forms;
using System.Linq;
using System.Text;
using System.Diagnostics;
using System.Threading;
using System.Runtime.InteropServices;
using System.Net;
using System.Net.Sockets;
using NetFwTypeLib;
namespace NewB
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
        }
        public static BackgroundWorker backgroundWorker0 = new BackgroundWorker(),
backgroundWorkerflood = new BackgroundWorker();
        private static System.Threading.Thread Thrf;
        private static System.Threading.Thread Thrl;
        private void NewB_thrf()
        {
            string port = textBox21.Text;
            Int64 iPort = Int64.Parse(port.ToString().Replace("Port: ", ""));
            string path = richTextBox1.Text;
            string iPath = path.ToString().Replace("Path of the program: ", "");
            string pname = textBox1.Text;
            string iPName = pname.ToString();
            string rIP0 = "0.0.0.0";
            string rIP1 = "0.0.0.0";
            string IPs = "0.0.0.0";
            INetFwRule2 newRule;
            INetFwPolicy2 firewallpolicy;
            string RemoteAdrr = "0.0.0.0";
            int RemotePort = 0;
            string LocalAdrr = "0.0.0.0";
            int LocalPort = 0;
            IPAddress[] addresslist;
            byte[] macAddr = new byte[6];
            uint macAddrLen = (uint)macAddr.Length;
            Stopwatch timer = new Stopwatch();
            timer.Start();
            Socket server = null;
            string elapsed = string.Empty;
            string IPS1 = textBoxS1.Text;
            string IPE1 = textBoxE1.Text;
            string IPS2 = textBoxS2.Text;
            string IPS3 = textBoxS3.Text;
            string IPS4 = textBoxS4.Text;
            string IPE4 = textBoxE4.Text;
            string IPE3 = textBoxE3.Text;
            string IPE2 = textBoxE2.Text;
            Int64 iIPS1 = Int64.Parse(IPS1.ToString().Replace(".", ""));
            Int64 iIPE1 = Int64.Parse(IPE1.ToString().Replace(".", ""));
            Int64 iIPS2 = Int64.Parse(IPS2.ToString().Replace(".", ""));
            Int64 iIPS3 = Int64.Parse(IPS3.ToString().Replace(".", ""));
            Int64 iIPS4 = Int64.Parse(IPS4.ToString().Replace(".", ""));
            Int64 iIPE4 = Int64.Parse(IPE4.ToString().Replace(".", ""));
            Int64 iIPE3 = Int64.Parse(IPE3.ToString().Replace(".", ""));
            Int64 iIPE2 = Int64.Parse(IPE2.ToString().Replace(".", ""));
            while (true)
            {
                if (!checkBox1.Checked)
                {
                    byte[] buffer = new byte[20000];
```

```
                    int pdwSize = 20000;
                    int res = GetTcpTable(buffer, out pdwSize, true);
                    if (res != 0)
                    {
                        buffer = new byte[pdwSize];
                        res = GetTcpTable(buffer, out pdwSize, true);
                        if (res != 0)
                            return;
                    }
                    TcpConnexion = new MIB_TCPTABLE();
                    int nOffset = 0;
                    TcpConnexion.dwNumEntries = Convert.ToInt32(buffer[nOffset]);
                    nOffset += 4;
                    TcpConnexion.table = new MIB_TCPROW[TcpConnexion.dwNumEntries];
                    for (int n = 0; n < TcpConnexion.dwNumEntries; n++)
                    {
                        int st = Convert.ToInt32(buffer[nOffset]);
                        ((TcpConnexion.table[n])).StrgState = convert_state(st);
                        ((TcpConnexion.table[n])).iState = st;
                        nOffset += 4;
                        LocalAdrr = buffer[nOffset].ToString() + "." + buffer[nOffset +
1].ToString() + "." + buffer[nOffset + 2].ToString() + "." + buffer[nOffset +
3].ToString();
                        nOffset += 4;
                        LocalPort = (((int)buffer[nOffset]) << 8) + (((int)buffer[nOffset +
1])) +
                            (((int)buffer[nOffset + 2]) << 24) + (((int)buffer[nOffset +
3]) << 16);
                        nOffset += 4;
                        ((TcpConnexion.table[n])).Local = new
IPEndPoint(IPAddress.Parse(LocalAdrr), LocalPort);
                        RemoteAdrr = buffer[nOffset].ToString() + "." + buffer[nOffset +
1].ToString() + "." + buffer[nOffset + 2].ToString() + "." + buffer[nOffset +
3].ToString();
                        nOffset += 4;
                        if (RemoteAdrr == "0.0.0.0")
                        {
                            RemotePort = 0;
                        }
                        else
                        {
                            RemotePort = (((int)buffer[nOffset]) << 8) +
(((int)buffer[nOffset + 1])) +
                                (((int)buffer[nOffset + 2]) << 24) + (((int)buffer[nOffset
+ 3]) << 16);
                        }
                        nOffset += 4;
                        ((TcpConnexion.table[n])).Remote = new
IPEndPoint(IPAddress.Parse(RemoteAdrr), RemotePort);
                        try
                        {
                            addresslist = Dns.GetHostAddresses(RemoteAdrr);
                            foreach (IPAddress theaddress in addresslist)
                            {
                                rIP0 = theaddress.ToString();
                                if (rIP0 != "0")
                                {
                                    file.Write(rIP0);
                                    file.Write(file.NewLine);
                                    newRule =
(INetFwRule2)Activator.CreateInstance(Type.GetTypeFromProgID("HNetCfg.FWRule"));
                                    if (iPName == "Process Name")
                                        newRule.Name = rIP0;
                                    else
                                        newRule.Name = iPName + ", " + rIP0;
```

```
                                    if (comboBox1.Text.EndsWith("UDP") &
comboBox1.Text.StartsWith("UDP"))
                                        newRule.Protocol =
(int)NET_FW_IP_PROTOCOL_.NET_FW_IP_PROTOCOL_UDP;
                                    if (comboBox1.Text.EndsWith("TCP") &
comboBox1.Text.StartsWith("TCP"))
                                        newRule.Protocol =
(int)NET_FW_IP_PROTOCOL_.NET_FW_IP_PROTOCOL_TCP;
                                    if (comboBox1.Text.EndsWith("Both") &
comboBox1.Text.StartsWith("Both"))
                                        newRule.Protocol =
(int)NET_FW_IP_PROTOCOL_.NET_FW_IP_PROTOCOL_ANY;
                                    if (iPath != "")
                                        newRule.ApplicationName = iPath;
                                    newRule.RemoteAddresses = rIP0;
                                    if (comboBox2.Text.EndsWith("Outbound") &
comboBox2.Text.StartsWith("Outbound"))
                                        newRule.Direction =
NET_FW_RULE_DIRECTION_.NET_FW_RULE_DIR_OUT;
                                    if (comboBox2.Text.EndsWith("Inbound") &
comboBox2.Text.StartsWith("Inbound"))
                                        newRule.Direction =
NET_FW_RULE_DIRECTION_.NET_FW_RULE_DIR_IN;
                                    if (comboBox2.Text.EndsWith("Both") &
comboBox2.Text.StartsWith("Both"))
                                        newRule.Direction =
NET_FW_RULE_DIRECTION_.NET_FW_RULE_DIR_MAX;
                                    newRule.Enabled = true;
                                    newRule.InterfaceTypes = "All";
                                    newRule.Action = NET_FW_ACTION_.NET_FW_ACTION_BLOCK;
                                    newRule.EdgeTraversal = false;
                                    firewallpolicy =
(INetFwPolicy2)Activator.CreateInstance(Type.GetTypeFromProgID("HNetCfg.FwPolicy2"));
                                    firewallpolicy.Rules.Remove(rIP0);
                                    firewallpolicy.Rules.Add(newRule);
                                }
                                new System.Threading.ManualResetEvent(false).WaitOne(10);
                            }
                        }
                        catch { }
                        if (!this.Visible)
                        {
                            this.Close();
                            break;
                        }
                        new System.Threading.ManualResetEvent(false).WaitOne(10);
                    }
                    buffer = new byte[20000];
                    pdwSize = 20000;
                    res = GetUdpTable(buffer, out pdwSize, true);
                    if (res != NO_ERROR)
                    {
                        buffer = new byte[pdwSize];
                        res = GetUdpTable(buffer, out pdwSize, true);
                        if (res != 0)
                            return;
                    }
                    UdpConnexion = new MIB_UDPTABLE();
                    nOffset = 0;
                    UdpConnexion.dwNumEntries = Convert.ToInt32(buffer[nOffset]);
                    nOffset += 4;
                    UdpConnexion.table = new MIB_UDPROW[UdpConnexion.dwNumEntries];
                    for (int n = 0; n < UdpConnexion.dwNumEntries; n++)
                    {
```

```
                        LocalAdrr = buffer[nOffset].ToString() + "." + buffer[nOffset +
1].ToString() + "." + buffer[nOffset + 2].ToString() + "." + buffer[nOffset +
3].ToString();
                        nOffset += 4;

                        LocalPort = (((int)buffer[nOffset]) << 8) + (((int)buffer[nOffset +
1])) +
                            (((int)buffer[nOffset + 2]) << 24) + (((int)buffer[nOffset +
3]) << 16);
                        nOffset += 4;
                        ((UdpConnexion.table[n])).Local = new
IPEndPoint(IPAddress.Parse(LocalAdrr), LocalPort);
                        try
                        {
                            addresslist = Dns.GetHostAddresses(LocalAdrr);
                            foreach (IPAddress theaddress in addresslist)
                            {
                                rIP0 = theaddress.ToString();
                                if (rIP0 != "0")
                                {
                                    file.Write(rIP0);
                                    file.Write(file.NewLine);
                                    newRule =
(INetFwRule2)Activator.CreateInstance(Type.GetTypeFromProgID("HNetCfg.FWRule"));
                                    if (iPName == "Process Name")
                                        newRule.Name = rIP0;
                                    else
                                        newRule.Name = iPName + ", " + rIP0;
                                    if (comboBox1.Text.EndsWith("UDP") &
comboBox1.Text.StartsWith("UDP"))
                                        newRule.Protocol =
(int)NET_FW_IP_PROTOCOL_.NET_FW_IP_PROTOCOL_UDP;
                                    if (comboBox1.Text.EndsWith("TCP") &
comboBox1.Text.StartsWith("TCP"))
                                        newRule.Protocol =
(int)NET_FW_IP_PROTOCOL_.NET_FW_IP_PROTOCOL_TCP;
                                    if (comboBox1.Text.EndsWith("Both") &
comboBox1.Text.StartsWith("Both"))
                                        newRule.Protocol =
(int)NET_FW_IP_PROTOCOL_.NET_FW_IP_PROTOCOL_ANY;
                                    if (iPath != "")
                                        newRule.ApplicationName = iPath;
                                    newRule.RemoteAddresses = rIP0;
                                    if (comboBox2.Text.EndsWith("Outbound") &
comboBox2.Text.StartsWith("Outbound"))
                                        newRule.Direction =
NET_FW_RULE_DIRECTION_.NET_FW_RULE_DIR_OUT;
                                    if (comboBox2.Text.EndsWith("Inbound") &
comboBox2.Text.StartsWith("Inbound"))
                                        newRule.Direction =
NET_FW_RULE_DIRECTION_.NET_FW_RULE_DIR_IN;
                                    if (comboBox2.Text.EndsWith("Both") &
comboBox2.Text.StartsWith("Both"))
                                        newRule.Direction =
NET_FW_RULE_DIRECTION_.NET_FW_RULE_DIR_MAX;
                                    newRule.Enabled = true;
                                    newRule.InterfaceTypes = "All";
                                    newRule.Action = NET_FW_ACTION_.NET_FW_ACTION_BLOCK;
                                    newRule.EdgeTraversal = false;
                                    firewallpolicy =
(INetFwPolicy2)Activator.CreateInstance(Type.GetTypeFromProgID("HNetCfg.FwPolicy2"));
                                    firewallpolicy.Rules.Remove(rIP0);
                                    firewallpolicy.Rules.Add(newRule);
                                }
                                new System.Threading.ManualResetEvent(false).WaitOne(10);
                            }
```

```
                        }
                        catch { }
                        if (!this.Visible)
                        {
                            this.Close();
                            break;
                        }
                        new System.Threading.ManualResetEvent(false).WaitOne(10);
                    }
                    if (!this.Visible)
                    {
                        this.Close();
                        break;
                    }
                }
                else
                {
                    if (iIPS1 <= iIPE1 & iIPS2 <= iIPE2 & iIPS3 <= iIPE3 & iIPS4 <= iIPE4)
                    {
                        IPs = iIPS1.ToString() + "." + iIPS2.ToString() + "." +
iIPS3.ToString() + "." + iIPS4.ToString();
                        timer = new Stopwatch();
                        timer.Start();
                        server = null;
                        elapsed = string.Empty;
                        try
                        {
                            IPHostEntry hostEntry =
Dns.GetHostEntry(System.Net.IPAddress.Parse(IPs));
                            IPAddress ipAddress = hostEntry.AddressList[0];
                            IPEndPoint ip = new IPEndPoint(ipAddress,
Convert.ToInt32(iPort));
                            server = new Socket(AddressFamily.InterNetwork,
SocketType.Dgram, ProtocolType.Udp) { Blocking = false, UseOnlyOverlappedIO = true,
DontFragment = false, EnableBroadcast = true };
                            IAsyncResult result = server.BeginConnect(ip, null, null);
                            result.AsyncWaitHandle.WaitOne(2000, true);
                            elapsed = timer.ElapsedMilliseconds.ToString();
                            timer.Stop();
                            if (!server.Connected)
                            {
                                //server.Close();
                            }
                            else
                            {
                                /*addresslist = Dns.GetHostAddresses(IPs);
                                foreach (IPAddress theaddress in addresslist)
                                {
                                    new
System.Threading.ManualResetEvent(false).WaitOne(10);
                                }*/
                                rIP1 = IPs.ToString() + "-" + iIPS1.ToString() + "." +
iIPS2.ToString() + "." + iIPS3.ToString() + ".255";
                                file.Write(rIP1);
                                file.Write(file.NewLine);
                                newRule =
(INetFwRule2)Activator.CreateInstance(Type.GetTypeFromProgID("HNetCfg.FWRule"));
                                if (iPName == "Process Name")
                                    newRule.Name = rIP1;
                                else
                                    newRule.Name = iPName + ", " + rIP1;
                                if (comboBox1.Text.EndsWith("UDP") &
comboBox1.Text.StartsWith("UDP"))
                                    newRule.Protocol =
(int)NET_FW_IP_PROTOCOL_.NET_FW_IP_PROTOCOL_UDP;
```

```
                                if (comboBox1.Text.EndsWith("TCP") &
comboBox1.Text.StartsWith("TCP"))
                                    newRule.Protocol =
(int)NET_FW_IP_PROTOCOL_.NET_FW_IP_PROTOCOL_TCP;
                                if (comboBox1.Text.EndsWith("Both") &
comboBox1.Text.StartsWith("Both"))
                                    newRule.Protocol =
(int)NET_FW_IP_PROTOCOL_.NET_FW_IP_PROTOCOL_ANY;
                                if (iPath != "")
                                    newRule.ApplicationName = iPath;
                                newRule.RemoteAddresses = rIP1;
                                if (comboBox2.Text.EndsWith("Outbound") &
comboBox2.Text.StartsWith("Outbound"))
                                    newRule.Direction =
NET_FW_RULE_DIRECTION_.NET_FW_RULE_DIR_OUT;
                                if (comboBox2.Text.EndsWith("Inbound") &
comboBox2.Text.StartsWith("Inbound"))
                                    newRule.Direction =
NET_FW_RULE_DIRECTION_.NET_FW_RULE_DIR_IN;
                                if (comboBox2.Text.EndsWith("Both") &
comboBox2.Text.StartsWith("Both"))
                                    newRule.Direction =
NET_FW_RULE_DIRECTION_.NET_FW_RULE_DIR_MAX;
                                newRule.Enabled = true;
                                newRule.InterfaceTypes = "All";
                                newRule.Action = NET_FW_ACTION_.NET_FW_ACTION_BLOCK;
                                newRule.EdgeTraversal = false;
                                firewallpolicy =
(INetFwPolicy2)Activator.CreateInstance(Type.GetTypeFromProgID("HNetCfg.FwPolicy2"));
                                if (iPName == "Process Name")
                                    firewallpolicy.Rules.Remove(rIP1);
                                else
                                    firewallpolicy.Rules.Remove(iPName + ", " + rIP1);
                                firewallpolicy.Rules.Add(newRule);
                                iIPS4 = Int64.Parse(IPS4.ToString().Replace(".", ""));
                                iIPS3 = iIPS3 + 1;
                                //server.Shutdown(SocketShutdown.Both);
                                //server.Close();
                            }
                        }
                        catch { }
                        iIPS4 = iIPS4 + 1;
                        if (iIPS4 > iIPE4)
                        {
                            iIPS4 = Int64.Parse(IPS4.ToString().Replace(".", ""));
                            iIPS3 = iIPS3 + 1;
                        }
                        if (iIPS3 > iIPE3)
                        {
                            iIPS3 = Int64.Parse(IPS3.ToString().Replace(".", ""));
                            iIPS2 = iIPS2 + 1;
                        }
                        if (iIPS2 > iIPE2)
                        {
                            iIPS2 = Int64.Parse(IPS2.ToString().Replace(".", ""));
                            iIPS1 = iIPS1 + 1;
                        }
                        if (iIPS1 > iIPE1)
                        {
                            iIPS1 = Int64.Parse(IPS1.ToString().Replace(".", ""));
                        }
                        new System.Threading.ManualResetEvent(false).WaitOne(10);
                    }
                }
                if (!this.Visible)
                {
```

```
                this.Close();
                break;
            }
            new System.Threading.ManualResetEvent(false).WaitOne(10);
        }
    }
    private static void Receive(Socket client)
    {
        try
        {
            StateObject state = new StateObject();
            state.workSocket = client;
            client.BeginReceive(state.buffer, 0, StateObject.BufferSize, 0, new
AsyncCallback(ReceiveCallback), state);
        }
        catch { }
    }
    private static void ReceiveCallback(IAsyncResult ar)
    {
        try
        {
            StateObject state = (StateObject)ar.AsyncState;
            Socket client = state.workSocket;
            int bytesRead = client.EndReceive(ar);
            if (bytesRead > 0)
            {
                state.sb.Append(Encoding.ASCII.GetString(state.buffer, 0, bytesRead));
                client.BeginReceive(state.buffer, 0, StateObject.BufferSize, 0,
                    new AsyncCallback(ReceiveCallback), state);
            }
            else
            {
                if (state.sb.Length > 1)
                {
                    response = state.sb.ToString();
                }
                receiveDone.Set();
            }
        }
        catch { }
    }
    private static ManualResetEvent receiveDone = new ManualResetEvent(false);
    private static String response = String.Empty;
    private static ManualResetEvent sendDone = new ManualResetEvent(false);
    private static void SendCallback(IAsyncResult ar)
    {
        try
        {
            Socket client = (Socket)ar.AsyncState;
            int bytesSent = client.EndSend(ar);
            sendDone.Set();
        }
        catch { }
    }
    private static void Send(Socket client, String data)
    {
        byte[] byteData = Encoding.ASCII.GetBytes(data);
        client.BeginSend(byteData, 0, byteData.Length, 0,
        new AsyncCallback(SendCallback), client);
    }
    private static void ConnectCallback(IAsyncResult ar)
    {
        try
        {
            Socket client = (Socket)ar.AsyncState;
            client.EndConnect(ar);
```

```
            Console.WriteLine("Socket connected to {0}",
                client.RemoteEndPoint.ToString());
            connectDone.Set();
        }
        catch (Exception e)
        {
            Console.WriteLine(e.ToString());
        }
    }
    private static ManualResetEvent connectDone = new ManualResetEvent(false);
    private string convert_state(int state)
    {
        string strg_state = "";
        switch (state)
        {
            case MIB_TCP_STATE_CLOSED: strg_state = "CLOSED"; break;
            case MIB_TCP_STATE_LISTEN: strg_state = "LISTEN"; break;
            case MIB_TCP_STATE_SYN_SENT: strg_state = "SYN_SENT"; break;
            case MIB_TCP_STATE_SYN_RCVD: strg_state = "SYN_RCVD"; break;
            case MIB_TCP_STATE_ESTAB: strg_state = "ESTAB"; break;
            case MIB_TCP_STATE_FIN_WAIT1: strg_state = "FIN_WAIT1"; break;
            case MIB_TCP_STATE_FIN_WAIT2: strg_state = "FIN_WAIT2"; break;
            case MIB_TCP_STATE_CLOSE_WAIT: strg_state = "CLOSE_WAIT"; break;
            case MIB_TCP_STATE_CLOSING: strg_state = "CLOSING"; break;
            case MIB_TCP_STATE_LAST_ACK: strg_state = "LAST_ACK"; break;
            case MIB_TCP_STATE_TIME_WAIT: strg_state = "TIME_WAIT"; break;
            case MIB_TCP_STATE_DELETE_TCB: strg_state = "DELETE_TCB"; break;
        }
        return strg_state;
    }
    private const int NO_ERROR = 0;
    private const int MIB_TCP_STATE_CLOSED = 1;
    private const int MIB_TCP_STATE_LISTEN = 2;
    private const int MIB_TCP_STATE_SYN_SENT = 3;
    private const int MIB_TCP_STATE_SYN_RCVD = 4;
    private const int MIB_TCP_STATE_ESTAB = 5;
    private const int MIB_TCP_STATE_FIN_WAIT1 = 6;
    private const int MIB_TCP_STATE_FIN_WAIT2 = 7;
    private const int MIB_TCP_STATE_CLOSE_WAIT = 8;
    private const int MIB_TCP_STATE_CLOSING = 9;
    private const int MIB_TCP_STATE_LAST_ACK = 10;
    private const int MIB_TCP_STATE_TIME_WAIT = 11;
    private const int MIB_TCP_STATE_DELETE_TCB = 12;
    public struct MIB_UDPTABLE
    {
        public int dwNumEntries;
        public MIB_UDPROW[] table;
    }
    public struct MIB_UDPROW
    {
        public IPEndPoint Local;
    }
    public MIB_UDPTABLE UdpConnexion;
    public MIB_TCPTABLE TcpConnexion;
    public struct MIB_TCPTABLE
    {
        public int dwNumEntries;
        public MIB_TCPROW[] table;
    }
    public struct MIB_TCPROW
    {
        public string StrgState;
        public int iState;
        public IPEndPoint Local;
        public IPEndPoint Remote;
    }
```

```
        public struct MIB_EXTCPROW
        {
            public string StrgState;
            public int iState;
            public IPEndPoint Local;
            public IPEndPoint Remote;
            public int dwProcessId;
            public string ProcessName;
        }
        [DllImport("iphlpapi.dll", SetLastError = true)]
        public static extern int GetTcpTable(byte[] pTcpTable, out int pdwSize, bool
bOrder);
        [DllImport("iphlpapi.dll", SetLastError = true)]
        public static extern int GetUdpTable(byte[] UcpTable, out int pdwSize, bool
bOrder);
        [DllImport("iphlpapi.dll", ExactSpelling = true)]
        public static extern int SendARP(IPAddress DestIP, int SrcIP, byte[] pMacAddr, ref
uint PhyAddrLen);
        private static bool Start = false;
        private static uint CurrentResolution = 0;
        private static double nbmemoryflooded = 0;
        private static IntPtr processPointer;
        private static Int64 baseAddress;
        private static Int64 lastAddress;
        private static DateTime basedate = new DateTime(1970, 1, 1);
        private static TimeSpan diff = DateTime.Now - basedate;
        private static double watch1, watch2;
        private static Process proc;
        private static string input;
        private static bool Closinggetstate;
        private static int wd = 2;
        private static int wu = 2;
        private static int timeout = 0;
        private static Random rnd = new Random();
        public static List<byte[]> bufferm = new List<byte[]>();
        public static byte[] buffertrue = new byte[1], bufferfalse = new byte[1];
        public static List<int> sizem = new List<int>();
        public static int size;
        public static byte[] buffer;
        public static int index = 0;
        private static IntPtr bytesReader;
        [DllImport("user32.dll")]
        public static extern bool GetAsyncKeyState(System.Windows.Forms.Keys vKey);
        [DllImport("kernel32.dll")]
        private static extern IntPtr OpenProcess(UInt32 dwDesiredAccess, bool
bInheritHandle, UInt32 dwProcessId);
        [DllImport("kernel32.dll")]
        private static extern Int32 ReadProcessMemory(IntPtr hProcess, IntPtr
lpBaseAddress, [In, Out] byte[] buffer, UInt64 size, out IntPtr lpNumberOfBytesRead);
        [DllImport("kernel32.dll")]
        static extern void GetSystemInfo(out SYSTEM_INFO lpSystemInfo);
        [DllImport("kernel32.dll", SetLastError = true)]
        static extern int VirtualQueryEx(IntPtr hProcess, IntPtr lpAddress, out
MEMORY_BASIC_INFORMATION lpBuffer, uint dwLength);
        [DllImport("kernel32.dll")]
        private static extern bool WriteProcessMemory(IntPtr hProcess, IntPtr
lpBaseAddress, byte[] buffer, IntPtr size, ref int lpNumberOfBytesRead);
        [DllImport("kernel32.dll")]
        private static extern bool VirtualAllocEx(IntPtr hProcess, IntPtr lpBaseAddress,
IntPtr size, uint flAllocationType, uint lpflOldProtect);
        [DllImport("kernel32.dll")]
        static extern bool VirtualProtectEx(IntPtr hProcess, IntPtr lpAddress, IntPtr size,
uint flNewProtect, out uint lpflOldProtect);
        [DllImport("winmm.dll", EntryPoint = "timeBeginPeriod")]
        public static extern uint TimeBeginPeriod(uint ms);
        [DllImport("winmm.dll", EntryPoint = "timeEndPeriod")]
```

```
        public static extern uint TimeEndPeriod(uint ms);
        [DllImport("ntdll.dll", EntryPoint = "NtSetTimerResolution")]
        public static extern void NtSetTimerResolution(uint DesiredResolution, bool
SetResolution, ref uint CurrentResolution);
        public struct MEMORY_BASIC_INFORMATION
        {
            public IntPtr BaseAddress;
            public IntPtr AllocationBase;
            public uint AllocationProtect;
            public IntPtr RegionSize;
            public uint State;
            public uint Protect;
            public uint lType;
        }
        public struct SYSTEM_INFO
        {
            public ushort processorArchitecture;
            ushort reserved;
            public uint pageSize;
            public IntPtr minimumApplicationAddress;
            public IntPtr maximumApplicationAddress;
            public IntPtr activeProcessorMask;
            public uint numberOfProcessors;
            public uint processorType;
            public uint allocationGranularity;
            public ushort processorLevel;
            public ushort processorRevision;
        }
        public enum AllocationProtectEnum : uint
        {
            PAGE_EXECUTE = 0x00000010,
            PAGE_EXECUTE_READ = 0x00000020,
            PAGE_EXECUTE_READWRITE = 0x00000040,
            PAGE_EXECUTE_WRITECOPY = 0x00000080,
            PAGE_NOACCESS = 0x00000001,
            PAGE_READONLY = 0x00000002,
            PAGE_READWRITE = 0x00000004,
            PAGE_WRITECOPY = 0x00000008,
            PAGE_GUARD = 0x00000100,
            PAGE_NOCACHE = 0x00000200,
            PAGE_WRITECOMBINE = 0x00000400
        }
        public enum ProcessAccess : int
        {
            VM_Operation = 0x8,
            VM_Write = 0x20,
            VM_Read = 0x10
        }
        public enum AllocationType : int
        {
            commit = 0x1000
        }
        private void NewB_thrfloodstart(uint dwdesiredaccess)
        {
            if (textBox2.Text == "4")
            {
                processPointer = OpenProcess(dwdesiredaccess, false, (uint)4);
                textBox1.Text = "System";
                baseAddress = 0;
                lastAddress = Convert.ToInt32("0x1FFFFFFF", 16) * 2;
            }
            else
            {
                try
                {
                    proc = null;
```

```
                    new System.Threading.ManualResetEvent(false).WaitOne(100);
                    input = textBox2.Text;
                    if (input != "PID" & input != "")
                        proc = Process.GetProcessById(Int32.Parse(input));
                    if (proc == null)
                    {
                        input = textBox1.Text;
                        proc = Process.GetProcessesByName(input).FirstOrDefault();
                        textBox2.Text = proc.Id.ToString();
                        processPointer = OpenProcess(dwdesiredaccess, false,
(uint)proc.Id);
                    }
                    else
                    {
                        textBox1.Text = proc.ProcessName.ToString();
                        processPointer = OpenProcess(dwdesiredaccess, false,
UInt32.Parse(input));
                    }
                }
                catch
                {
                    proc = null;
                    new System.Threading.ManualResetEvent(false).WaitOne(100);
                    input = textBox1.Text;
                    proc = Process.GetProcessesByName(input).FirstOrDefault();
                    textBox2.Text = proc.Id.ToString();
                    processPointer = OpenProcess(dwdesiredaccess, false, (uint)proc.Id);
                }
                baseAddress = proc.MainModule.BaseAddress.ToInt64();
                lastAddress = baseAddress + proc.MainModule.ModuleMemorySize;
            }
        }
        private void NewB_thrflood(object sender, DoWorkEventArgs e)
        {
            SYSTEM_INFO sys_info = new SYSTEM_INFO();
            GetSystemInfo(out sys_info);
            IntPtr proc_min_address = new IntPtr(0);
            long proc_address_1;
            long proc_address_2;
            int bytesRead = 0;
            byte[] valfalseBuffer = BitConverter.GetBytes(false);
            byte[] valtrueBuffer = BitConverter.GetBytes(true);
            int booleanfalsesize = BitConverter.GetBytes(false).Length;
            int booleantruesize = BitConverter.GetBytes(true).Length;
            int m1 = 0, m2 = 0;
            List<long> proc_address_m1 = new List<long>(), proc_address_m2 = new
List<long>();
            List<byte[]> buffertruem1 = new List<byte[]>(), buffertruem2 = new
List<byte[]>();
            List<byte[]> bufferfalsem1 = new List<byte[]>(), bufferfalsem2 = new
List<byte[]>();
            List<long> proc_address_m12 = new List<long>();
            List<byte[]> buffertruem12 = new List<byte[]>();
            List<byte[]> bufferfalsem12 = new List<byte[]>();
            bool waitbool = true;
            index = 0;
            button1.BackColor = Color.Green;
            for (; ; )
            {
                if (!Start)
                    return;
                do
                {
                    proc_address_1 = baseAddress + m1;
                    ReadProcessMemory(processPointer, (IntPtr)(proc_address_1), buffertrue,
(uint)buffertrue.Length, out bytesReader);
```

```
                    ReadProcessMemory(processPointer, (IntPtr)(proc_address_2 =
proc_address_1 + booleantruesize), bufferfalse, (uint)bufferfalse.Length, out bytesReader);
                    if (buffertrue != valtrueBuffer & bufferfalse != valtrueBuffer &
buffertrue != valfalseBuffer & bufferfalse != valfalseBuffer)
                    {
                        proc_address_m1.Add(proc_address_1);
                        buffertruem1.Add(buffertrue);
                        bufferfalsem1.Add(bufferfalse);
                    }
                    m1 += booleantruesize;
                } while (proc_address_2 + booleanfalsesize <= lastAddress);
                if (waitbool)
                    System.Threading.Thread.Sleep(6000);
                do
                {
                    proc_address_1 = baseAddress + m2;
                    ReadProcessMemory(processPointer, (IntPtr)(proc_address_1), buffertrue,
(uint)buffertrue.Length, out bytesReader);
                    ReadProcessMemory(processPointer, (IntPtr)(proc_address_2 =
proc_address_1 + booleantruesize), bufferfalse, (uint)bufferfalse.Length, out bytesReader);
                    if (buffertrue != valtrueBuffer & bufferfalse != valtrueBuffer &
buffertrue != valfalseBuffer & bufferfalse != valfalseBuffer)
                    {
                        proc_address_m2.Add(proc_address_1);
                        buffertruem2.Add(buffertrue);
                        bufferfalsem2.Add(bufferfalse);
                    }
                    m2 += booleantruesize;
                } while (proc_address_2 + booleanfalsesize <= lastAddress);
                if (waitbool)
                {
                    for (int i = 0; i < proc_address_m2.Count; i++)
                    {
                        if (buffertruem1[i] != buffertruem2[i])
                        {
                            proc_address_m12.Add(proc_address_m2[i]);
                            buffertruem12.Add(buffertruem1[i]);
                            bufferfalsem12.Add(bufferfalsem1[i]);
                        }
                        else
                        {
                            proc_address_m12.Add(proc_address_m2[i]);
                            buffertruem12.Add(BitConverter.GetBytes(0));
                            bufferfalsem12.Add(BitConverter.GetBytes(0));
                        }
                    }
                    button1.BackColor = Color.Red;
                }
                waitbool = false;
                index = rnd.Next(proc_address_m12.Count);
                proc_address_1 = proc_address_m12[index];
                proc_address_2 = proc_address_1 + booleantruesize;
                WriteProcessMemory(processPointer, (IntPtr)proc_address_1,
bufferfalsem12[index], (IntPtr)booleanfalsesize, ref bytesRead);
                WriteProcessMemory(processPointer, (IntPtr)proc_address_2,
buffertruem12[index], (IntPtr)booleantruesize, ref bytesRead);
                nbmemoryflooded++;
            }
        }
        private void button1_Click(object sender, EventArgs e) //flood
        {
            start();
        }
        private void start()
        {
            if (!Start)
```

```
            {
                Start = true;
                nbmemoryflooded = 0;
                NewB_thrfloodstart((uint)(ProcessAccess.VM_Operation |
ProcessAccess.VM_Write | ProcessAccess.VM_Read));
                backgroundWorkerflood.DoWork += new DoWorkEventHandler(NewB_thrflood);
                backgroundWorkerflood.RunWorkerAsync();
                button1.BackColor = Color.Red;
                diff = DateTime.Now - basedate;
                watch1 = diff.TotalMinutes;
            }
            else
            {
                Start = false;
                backgroundWorkerflood.DoWork -= new DoWorkEventHandler(NewB_thrflood);
                button1.BackColor = Color.Black;
                diff = DateTime.Now - basedate;
                watch2 = diff.TotalMinutes;
                textBox5.Text = ((int)(watch2 - watch1)).ToString();
                textBox4.Text = Convert.ToString(index);
                textBox3.Text = Convert.ToString((int)((nbmemoryflooded * 2) / index));
            }
        }
        private void NewB_thr0(object sender, DoWorkEventArgs e)
        {
            for (; ; )
            {
                if (Closinggetstate)
                    return;
                if (GetAsyncKeyState(System.Windows.Forms.Keys.NumPad0))
                {
                    timeout = timeout + 1;
                    if (wd <= 1)
                        wd = wd + 1;
                    wu = 0;
                }
                else
                {
                    if (wu <= 1)
                        wu = wu + 1;
                    wd = 0;
                }
                if (wd == 1)
                    timeout = 0;
                if (wu == 1 & timeout < 10 & !Start)
                    start();
                if (wu == 1 & timeout >= 10 & Start)
                    start();
                new System.Threading.ManualResetEvent(false).WaitOne(100);
            }
        }
        [DllImport("kernel32.dll")]
        static extern bool VirtualProtectEx(IntPtr hProcess, IntPtr lpAddress, UIntPtr
dwSize, uint flNewProtect, out uint lpflOldProtect);
        public enum AllocationProtect : uint
        {
            PAGE_EXECUTE = 0x00000010,
            PAGE_EXECUTE_READ = 0x00000020,
            PAGE_EXECUTE_READWRITE = 0x00000040,
            PAGE_EXECUTE_WRITECOPY = 0x00000080,
            PAGE_NOACCESS = 0x00000001,
            PAGE_READONLY = 0x00000002,
            PAGE_READWRITE = 0x00000004,
            PAGE_WRITECOPY = 0x00000008,
            PAGE_GUARD = 0x00000100,
            PAGE_NOCACHE = 0x00000200,
```

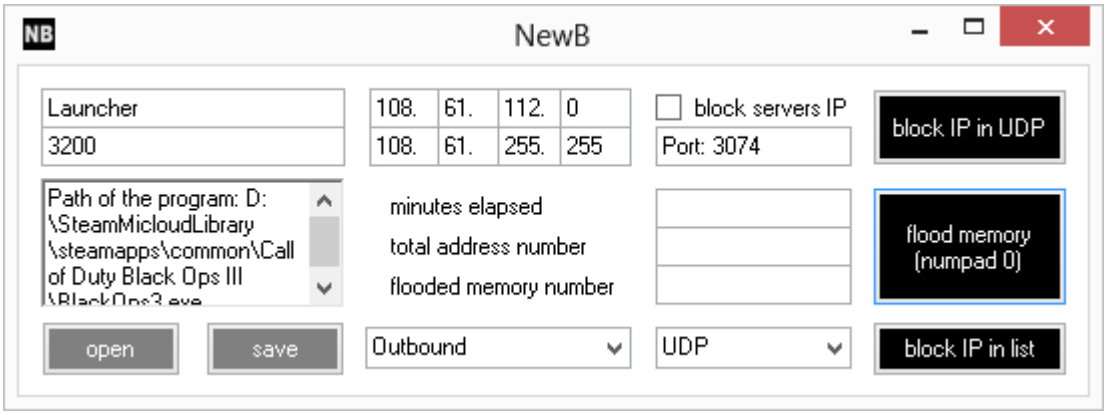
```
            PAGE_WRITECOMBINE = 0x00000400
        }
        [DllImport("kernel32.dll")]
        private static extern IntPtr OpenProcess(UInt32 dwDesiredAccess, Int32
bInheritHandle, int dwProcessId);
        [DllImport("kernel32.dll")]
        private static extern Int32 CloseHandle(IntPtr hObject);
        [DllImport("kernel32", SetLastError = true, CharSet = CharSet.Ansi)]
        private static extern IntPtr LoadLibrary([MarshalAs(UnmanagedType.LPStr)]string
lpFileName);
        [DllImport("kernel32.dll", SetLastError = true)]
        private static extern IntPtr LoadLibraryEx(string lpFileName, IntPtr hReservedNull,
LoadLibraryFlags dwFlags);
        [DllImport("user32.dll", SetLastError = true)]
        private static extern UInt32 GetWindowThreadProcessId(IntPtr hWnd, out UInt32
lpdwProcessId);
        [System.Flags]
        private enum LoadLibraryFlags : uint
        {
            DONT_RESOLVE_DLL_REFERENCES = 0x00000001,
            LOAD_IGNORE_CODE_AUTHZ_LEVEL = 0x00000010,
            LOAD_LIBRARY_AS_DATAFILE = 0x00000002,
            LOAD_LIBRARY_AS_IMAGE_RESOURCE = 0x00000020,
            LOAD_LIBRARY = 0x00000800,
            LOAD_LIBRARY_AS_DATAFILE_EXCLUSIVE = 0x00000040,
            LOAD_WITH_ALTERED_SEARCH_PATH = 0x00000008
        }
        [DllImport("kernel32.dll")]
        private static extern Int32 WSADuplicateSocketW(Socket s, int dwProcessId,
LPWSAPROTOCOLINFO lpProtocolInfo);
        private enum LPWSAPROTOCOLINFO : uint
        {
            lpProtocolInfo = 0x00000001
        }
        [DllImport("ws2_32.dll", CharSet = CharSet.Unicode, SetLastError = true,
CallingConvention = CallingConvention.StdCall)]
        private static extern IntPtr WSASocket(ADDRESS_FAMILIES af, SOCKET_TYPE
socket_type, PROTOCOL protocol,
             LPWSAPROTOCOLINFO lpProtocolInfo, Int32 group, OPTION_FLAGS_PER_SOCKET
dwFlags);
        private enum ADDRESS_FAMILIES : short
        {
            AF_UNSPEC = 0
        }
        private enum SOCKET_TYPE : short
        {
            SOCK_DGRAM = 2
        }
        private enum PROTOCOL : short
        {
            IPPROTO_UDP = 17
        }
        private enum OPTION_FLAGS_PER_SOCKET : short
        {
            SO_DONTROUTE = 0x0010,
            SO_BROADCAST = 0x0020,
            SO_USELOOPBACK = 0x0040
        }
        private void button2_Click(object sender, EventArgs e) //save
        {
            String charstore;
            System.Windows.Forms.SaveFileDialog saveFileDialog1 = new
System.Windows.Forms.SaveFileDialog();
            saveFileDialog1.Filter = "txt files (*.txt)|*.txt|All files (*.*)|*.*";
            saveFileDialog1.FilterIndex = 2;
            saveFileDialog1.RestoreDirectory = true;
```

```
            if (saveFileDialog1.ShowDialog() == System.Windows.Forms.DialogResult.OK)
            {
                charstore = saveFileDialog1.FileName;
                System.IO.StreamWriter file = new System.IO.StreamWriter(charstore);
                file.WriteLine(textBox1.Text);
                file.WriteLine(textBox2.Text);
                file.WriteLine(textBoxS1.Text);
                file.WriteLine(textBoxE1.Text);
                file.WriteLine(textBoxS2.Text);
                file.WriteLine(textBoxS3.Text);
                file.WriteLine(textBoxS4.Text);
                file.WriteLine(textBoxE4.Text);
                file.WriteLine(textBoxE3.Text);
                file.WriteLine(textBoxE2.Text);
                file.WriteLine(textBox21.Text);
                file.WriteLine(richTextBox1.Text);
                file.WriteLine(checkBox1.Checked);
                file.WriteLine(comboBox1.Text);
                file.WriteLine(comboBox2.Text);
                file.Close();
            }
        }
        private void button3_Click(object sender, EventArgs e) //open
        {
            String myRead;
            System.Windows.Forms.OpenFileDialog openFileDialog1 = new
System.Windows.Forms.OpenFileDialog();
            openFileDialog1.Filter = "txt files (*.txt)|*.txt|All files (*.*)|*.*";
            openFileDialog1.FilterIndex = 2;
            openFileDialog1.RestoreDirectory = true;
            if (openFileDialog1.ShowDialog() == System.Windows.Forms.DialogResult.OK)
            {
                myRead = openFileDialog1.FileName;
                System.IO.StreamReader file = new System.IO.StreamReader(myRead);
                textBox1.Text = file.ReadLine();
                textBox2.Text = file.ReadLine();
                textBoxS1.Text = file.ReadLine();
                textBoxE1.Text = file.ReadLine();
                textBoxS2.Text = file.ReadLine();
                textBoxS3.Text = file.ReadLine();
                textBoxS4.Text = file.ReadLine();
                textBoxE4.Text = file.ReadLine();
                textBoxE3.Text = file.ReadLine();
                textBoxE2.Text = file.ReadLine();
                textBox21.Text = file.ReadLine();
                richTextBox1.Text = file.ReadLine();
                checkBox1.Checked = bool.Parse(file.ReadLine());
                comboBox1.SelectedItem = file.ReadLine();
                comboBox2.SelectedItem = file.ReadLine();
                file.Close();
            }
        }
        private static System.IO.StreamWriter file = null;
        private bool StartRec = false;
        private void button4_Click(object sender, EventArgs e) //block IP
        {
            if (!StartRec)
            {
                StartRec = true;
                String charstore;
                System.Windows.Forms.SaveFileDialog saveFileDialog1 = new
System.Windows.Forms.SaveFileDialog();
                saveFileDialog1.Filter = "txt files (*.txt)|*.txt|All files (*.*)|*.*";
                saveFileDialog1.FilterIndex = 2;
                saveFileDialog1.RestoreDirectory = true;
                if (saveFileDialog1.ShowDialog() == System.Windows.Forms.DialogResult.OK)
```

```
                {
                    charstore = saveFileDialog1.FileName;
                    file = new System.IO.StreamWriter(charstore);
                }
                Thrf = new System.Threading.Thread(new
System.Threading.ThreadStart(NewB_thrf));
                Thrf.Start();
            }
        }
        private static bool StartList = false;
        private static string myReadl = null;
        private static string IPl = null;
        private static System.IO.StreamReader filel;
        private void button5_Click(object sender, EventArgs e) //block IP in list
        {
            if (!StartList)
            {
                StartList = true;
                System.Windows.Forms.OpenFileDialog openFileDialog1 = new
System.Windows.Forms.OpenFileDialog();
                openFileDialog1.Filter = "txt files (*.txt)|*.txt|All files (*.*)|*.*";
                openFileDialog1.FilterIndex = 2;
                openFileDialog1.RestoreDirectory = true;
                if (openFileDialog1.ShowDialog() == System.Windows.Forms.DialogResult.OK)
                {
                    myReadl = openFileDialog1.FileName;
                    filel = new System.IO.StreamReader(myReadl);
                }
                Thrl = new System.Threading.Thread(new
System.Threading.ThreadStart(NewB_thrl));
                Thrl.Start();
            }
        }
        private void NewB_thrl()
        {
            string path = richTextBox1.Text;
            string iPath = path.ToString().Replace("Path of the program: ", "");
            string pname = textBox1.Text;
            string iPName = pname.ToString();
            INetFwRule2 newRule;
            INetFwPolicy2 firewallpolicy;
            while (true)
            {
                IPl = filel.ReadLine();
                newRule =
(INetFwRule2)Activator.CreateInstance(Type.GetTypeFromProgID("HNetCfg.FWRule"));
                if (iPName == "Process Name")
                    newRule.Name = IPl;
                else
                    newRule.Name = iPName + ", " + IPl;
                if (comboBox1.Text.EndsWith("UDP") & comboBox1.Text.StartsWith("UDP"))
                    newRule.Protocol = (int)NET_FW_IP_PROTOCOL_.NET_FW_IP_PROTOCOL_UDP;
                if (comboBox1.Text.EndsWith("TCP") & comboBox1.Text.StartsWith("TCP"))
                    newRule.Protocol = (int)NET_FW_IP_PROTOCOL_.NET_FW_IP_PROTOCOL_TCP;
                if (comboBox1.Text.EndsWith("Both") & comboBox1.Text.StartsWith("Both"))
                    newRule.Protocol = (int)NET_FW_IP_PROTOCOL_.NET_FW_IP_PROTOCOL_ANY;
                if (iPath != "")
                    newRule.ApplicationName = iPath;
                newRule.RemoteAddresses = IPl;
                if (comboBox2.Text.EndsWith("Outbound") &
comboBox2.Text.StartsWith("Outbound"))
                    newRule.Direction = NET_FW_RULE_DIRECTION_.NET_FW_RULE_DIR_OUT;
                if (comboBox2.Text.EndsWith("Inbound") &
comboBox2.Text.StartsWith("Inbound"))
                    newRule.Direction = NET_FW_RULE_DIRECTION_.NET_FW_RULE_DIR_IN;
                if (comboBox2.Text.EndsWith("Both") & comboBox2.Text.StartsWith("Both"))
```

```
                    newRule.Direction = NET_FW_RULE_DIRECTION_.NET_FW_RULE_DIR_MAX;
                newRule.Enabled = true;
                newRule.InterfaceTypes = "All";
                newRule.Action = NET_FW_ACTION_.NET_FW_ACTION_BLOCK;
                newRule.EdgeTraversal = false;
                firewallpolicy =
(INetFwPolicy2)Activator.CreateInstance(Type.GetTypeFromProgID("HNetCfg.FwPolicy2"));
                if (iPName == "Process Name")
                    firewallpolicy.Rules.Remove(IPl);
                else
                    firewallpolicy.Rules.Remove(iPName + ", " + IPl);
                firewallpolicy.Rules.Add(newRule);
                new System.Threading.ManualResetEvent(false).WaitOne(10);
                if (!this.Visible)
                {
                    file1.Close();
                    this.Close();
                    break;
                }
            }
        }
        private void Form1_FormClosed(object sender, FormClosedEventArgs e)
        {
            savePathInitFile();
            Start = false;
            Closinggetstate = true;
            TimeEndPeriod(1);
        }
        public void savePathInitFile()
        {
            System.IO.StreamWriter initfile = new System.IO.StreamWriter("initexe.txt");
            initfile.WriteLine(textBox1.Text);
            initfile.WriteLine(textBox2.Text);
            initfile.Close();
        }
        private void Form1_Shown(object sender, EventArgs e)
        {
            System.Diagnostics.Process process =
System.Diagnostics.Process.GetCurrentProcess();
            process.PriorityClass = System.Diagnostics.ProcessPriorityClass.RealTime;
            try
            {
                System.IO.StreamReader file = new System.IO.StreamReader("initexe.txt");
                textBox1.Text = file.ReadLine();
                textBox2.Text = file.ReadLine();
                file.Close();
            }
            catch
            {
                using (System.IO.StreamWriter createdfile =
System.IO.File.AppendText("initexe.txt"))
                {
                    createdfile.WriteLine("Process Name");
                    createdfile.WriteLine("PID");
                    createdfile.Close();
                }
            }
            TimeBeginPeriod(1);
            NtSetTimerResolution(1, true, ref CurrentResolution);
            backgroundWorker0.DoWork += new DoWorkEventHandler(NewB_thr0);
            backgroundWorker0.RunWorkerAsync();
        }
    }
    public class StateObject
    {
        public Socket workSocket = null;
```

```
        public const int BufferSize = 256;
        public byte[] buffer = new byte[BufferSize];
        public StringBuilder sb = new StringBuilder();
    }
}
```



5.2. Cheat Engine

The program most used by hackers and cheaters is cheat engine (version 6.3.), because with it, you can find address of memory where values can be changed in order to hack a game with god mode, energy remain, infinite ammo, speed hack, change impacts, penetration impacts, fire rate, invisible hack… The study in this book, imply to be interesting in hacking codes like wallhack, aimbot, autoshoot, in order to know if there is a solution to counter hacks. For an aimbot, knowing if the victim can be fire, if still alive, is important, and a value in addresses indicating if the victim is still alive, named "isingame" by hackers must be different of 0. In private match, against bots in BO2, you can try to change your ammo, by using cheat engine. Open cheat engine, and with it the process t6mp.exe, and make a first scan with the exact value of your amount ammo, then a next scan after firing with the new amount number of ammo. In windowed mode, it's easy the find the address where the value of ammo change when firing in the game. Add the address to the table under, and you can change the value. It's just an example for you to try to learn how to use cheat engine to counter hacks. If you play against cheaters or a clan cheating, always loosing each game, you can deploy an energy remain hack trainer, freezing your amount of energy, plus or less like a god mode with the freezing intervals in milliseconds, in cheat engine with the tool generate a trainer. You can

set/edit a toggle keypress. When you play against bots in private match in BO2, when you are alive, search the exact values 100 with a first scan, when you are die search the values 0 with a next scan, you will find 3 or 4 addresses, with the values 100 to 0 when you are fired. Change the values to 0, 2 or 3 values will stay to 0 when you are alive and the bots will not see you, and don't kill you anymore. Add these addresses the table under, and then set/edit a toggle keypress, like the key F for respawn and to remove the killcam. Add F as hotkey for set the value to 0, and add F to freeze the value with a 0 millisecond of freezing interval when you make your exe trainer. Make the same in your favourite public match. Also you can search addresses when it's the exact value 0 for the first scan when you are die, and when it's above 1 value for the next scans when you are alive. Add the addresses to the table under with shift key and clicks, and then cut the addresses with values 87, when you have the knife as a secondary weapon, for removing to the table. Set/edit toggle keypress each address (almost 30) with key F for set value to 0 and toggle freeze. Generate your trainer with the option freeze the values with a 0 millisecond of freezing interval. Don't be scary to use cheat engine if you don't play, this method doesn't imply you cheating, it's just repairing the errors of the old game engine that is used to make Call of Duty games. If your trainer doesn't appear, it run, when you launch it with BO2 executed in full screen (Alt+Tab or Alt+Esc to change window, Alt+Enter for full screen). When you finish to play, open task manager with ctrl+shift+esc, for ending the task named Cheat Engine for your trainer. Don't create a shortcut of your trainer, because the icon is invisible and your process explorer.exe will turn in loop, with 100 percent of a processor used. You can be banned for using this method, so it's useless.

5.3. Explorer Suite

The program coming with Explorer Suite named CFF Explorer (Explorer Suite at http://www.ntcore.com/exsuite.php) can allocate memory with random values of base of code

and base of data, find in optional header. Even change the Image Base of DLL find in rebuilder. You can overwrite the files exe and DLL. In optional header, you can change the values of size of code, size of initialized data, size of headers, check sum, dllcharacteristics like dll can move, and null the values of size of stack reserve; size of stack commit, size of heap reserve, and size of heap commit. In Data Directories, you can change, Relocation Directory Size and null the values of Debug Directory Size.

When changing baseofcode with CFF, avira antivir detected virus in the files of CoD AW named tier0_s, vstdlib_s, UpdateDLLWrapper, so delete it. The files tier0_s, vstdlib_s, UpdateDLLWrapper, d3dcompiler_46, Steam.dll, steam_api.dll, steamclient.dll are useless, you can delete it. The list of exe and dll files in CoD AW folder are: tier0_s, vstdlib_s, UpdateDLLWrapper, d3dcompiler_46, Steam.dll, steam_api.dll, steamclient.dll, s1_mp64_ship, bink2w64, ControllerManager, nvToolsExt64_1, steam_api64, SteamAPIUpdater, vcomp110, XGamepad.

With Stud_PE, you can change for CoD AW exe in DOS Header: Pages in file, Relocations, File address of relocation table. You can change for CoD AW files in Headers, Entry Point, address image base with CFF in rebuilder (with options rebuild PE header, remove base relocation, bind import table, new image base), sectionalignement, and BaseOfCode: s1_mp64_ship (no, no, no, and yes), bink2w64 (no, no, no and yes), steam_api64 (no, no, no and yes), ControllerManager (yes, yes, yes and yes), nvToolsExt64_1 (yes, yes, yes and yes), SteamAPIUpdater (yes, yes, yes and yes), vcomp110 (yes, yes, yes and yes), XGamepad (yes, yes, yes and yes) and all other dll in APEX folder.

The method is to fresh files of steam and the game. For it delete all dll and exe in steam folder and in the game folder, rename your steam games library folder, then make a new install of steam and check integrity of game files, then change all base of code with CFF,

and put all these files in the folder of the game. But it's useless, even for not encounter hacked lobbies.

This is applied to Titanfall but can be applied to all other games respectful, not like Call of Duty games. Make a copy of titanfall.exe in case you have a problem, then change the original file, open with CFF, enable when you install explorersuite.exe, as following:

- Change New Image Base and Rebuild with the button in Rebuilder. Save change, overwrite file.

- Change BaseofCode in Optional Header. Save change, overwrite file.

- Replace original file Titanfall.exe.

Also what you can change and not change as following:

In Data Directories:

- Relocation Directory Size (ok)
- null the values of ...

  Debug Directory Size (ok)

  Import Address Table Directory Size (no)

In Rebuilder:

- Rebuild PE Header (ok)
- Update Checksum (ok)
- Realign File (no)
- Remove Base Relocation (no)
- New Image Base (ok)

In Optional Header:

- AddressofEntryPoint (no)
- BaseofCode (ok)
- size of code (?)

- size of initialized data (?)
- check sum (?)
- dllcharacteristics like...

  dll can move (ok)

Code Integrity Image (no)

- null the values of ...

  size of headers (no)

  size of stack reserve (no)

  size of stack commit (ok)

  size of heap reserve (ok)

  size of heap commit (ok)

dos header

  e_maxalloc (ok)

nt headers

  signature (no)

file header

  number of sections (no)

optional header

  base of code (ok)

data directories

  relocation directory rva (ok)

section headers

  reloc address (ok)

Also you can see all the DLL used by games with perfmon.exe under the tab processor, so it's possible to replace, by copy/paste, all the DLL under the folder where games files are installed, in order to change the base of code and image base address of these DLL with CFF.

To avoid cheat programs of cheaters, when you fight against it, modifying your game, you can use Stud_PE to change memory information of the exe of your game before playing. Instead of overwriting the exe, you can use the button test it. Overwriting the exe can cause problem of integrity to launch your game. More information on Stud_PE can be known on the website http://forum.cgsoftlabs.ro/.

With Stud_PE you can change the following memory information:

EXE and DLL, Rva<=>Raw ok, Headers: ImageBase ok (not AW exe, bink2w64 dll, steam_api64 dll, and for Titanfall not GFSDK_SSAO.win64 dll and GFSDK_TXAA.win64 dll), PE Characteristics Flags: relocations stripped ok, executable image, line numbers stripped ok, locale symbols stripped ok, aggressive WS trime ok, large address aware ok, bytes reversed low ok, 32 bit machine expected ok, debug information stripped ok, run from swap removeable ok, run from swap net ok, file system ok, dll no, no multiprocessor systems no, bytes reversed hygh ok, Dos: EntryPoint, Initial CS ok, Initial IP ok.

With CFF explorer from Explorer suite you can change the following memory information:

EXE and DLL, ImageBase ok (for Titanfall not bink2w64 dll, datacache dll, engine dll, filesystem_stdio dll, inputsystem dll, launcher dll, localize dll, materialsystem_dx11 dll, studiorender dll, tier0 dll, valve_avi dll, vgui2 dll, vguimatsurface dll, vphysics dll, vstdlib dll, GDFBinary_fr_FR_64 dll, GFSDK_SSAO.win64 dll, GFSDK_TXAA.win64 dll, client.dll, Activation64 dll, not dll in core folder).

Hacking programs connected online can hack your computer. It's realized with DLL used by the game that editors don't redistribute. You can see which DLL are used by

programs. For it, open resource monitor (perfmon.exe) from control panel in administration tool, check AW processes when it's running, and under associate modules under processor tab, you can see which DLL are used. From the link here: https://app.box.com/s/deqrumpo2hd0g3v3ap9pw843e1w40nev you can download DLL I have copy from my computer and process explorer for using CFF to modify BaseOfCode number under Optional Header for all DLL, but not for bcryptprimitives.DLL. For this DLL, you can modify the number ImageBase under Rebuilder (you must rebuild). Overwrite files with CFF and place all DLL in the root where AW is installed. The folder can be open with the properties of AW in your Steam library under the tab local files.

I think it's not necessary to change memory informations with CFF for EXE and DLL with ASLR enabled. Use ProcessExplorer by Technet to know it.

5.4. EMET 5.2

To add processes running to EMET running, configure each process under the EMET tab. EMET will ask to disable EAF for some programs. EMET by Technet can be used with Advanced Warfare disabling only EAF and Stack Pivot but all other mitigations can be enable. In EAF+, you can prevent modules to be loaded like:

a*.dll;b*.dll;c*.dll;d*.dll;e*.dll;f*.dll;g*.dll;h*.dll;i*.dll;j*.dll;k*.dll;l*.dll;m*.dll;n*.dll;o*.dll;p*.dll;q*.dll;r*.dll;s*.dll;t*.dll;u*.dll;v*.dll;w*.dll;x*.dll;y*.dll;z*.dll;user32.dll;npjpi*.dll;jp2iexp.dll;vgx.dll;msxml4*.dll;wshom.ocx;scrrun.dll;vbscript.dll;dwmapi.dll;kernel32.dll;dnsrslvr.dll;dnsapi.dll;flash*.ocx;wow64win.dll;wow64cpu.dll;kernelbase.dll;apphelp.dll;EMET.dll;msvcrt.dll;wtsapi32.dll;steam_api.dll;winmm.dll;wsock32.dll;faultrep.dll;dxgi.dll;dsound.dll;gdi32.dll;advapi32.dll;shell32.dll;ole32.dll;oleaut32.dll;wintrust.dll;wininet.dll;xinput1_32.dll;psapi.dll;binkw32.dll;d3d11.dll;winmmbase.dll;rpcrt4.dll;powrprof.dll;sechost.dll;combase.dll;shlwapi.dll;crypt32.dll;msasn1.dll;iertutil.dll;setupapi.dll;ntdll.dll;nsi.dll;sspicli.dll;cfgmgr32.dll;devobj.dll;cryptbase.dll;bcryptprimitives.dll;imm32.dll;msctf.dll;dbghelp.dll;shcore.dll;

winsta.dll;gameoverlayrenderer.dll;cryptsp.dll;rsaenh.dll;uxtheme.dll;napinsp.dll;pnrpnsp.dll;nlaapi.dll;mswsock.dll;winrnr.dll;wshbth.dll;iphlpapi.dll;winnsi.dll;fwpuclnt.dll;rasadhlp.dll;steamclient.dll;imagehlp.dll;version.dll;tier0_s.dll;vstdlib_s.dll;pdh.dll;secur32.dll;steam.dll;cserhelper.dll;dhcpcsvc.dll;clbcatq.dll;quartz.dll;qcap.dll;msvfw32.dll;comctl32.dll;devenum.dll;ntmarta.dll;msdmo.dll;profapi.dll;nvapi.dll;nvwgf2um.dll;ddraw.dll;dciman32.dll;xaudio2_7.dll;mmdevapi.dll;audioses.dll;avrt.dll;wdmaud.drv;ksuser.dll;msacm32.drv;msacm32.dll;midimap.dll;d3dcompiler_43.dll;steam_api64.dll;bink2w64.dll;SteamAPIUpdater.dll;steamclient.dll;Steam.dll;steam_api.dll;nvToolsExt64_1.dll;WININET.dll;PSAPI.DLL;WINMM.dll;KERNEL32.DLL;ADVAPI32.dll;SHELL32.dll;USER32.dll;GDI32.dll;ole32.dll;d3d11.dll;dxgi.dll;DSOUND.dll;POWRPROF.dll;WS2_32.dll;XINPUT1_3.dll;*.dll

Other modules to add in this mitigation can be seen with Process Explorer by Technet too or with CFF installing ExplorerSuite. With CFF you can see address base and base of code to add in Heap Spray Protection like:

0x0;0x1;0x2;0x3;0x4;05;0x6;0x7;0x8;0x9;0x0a040a04;0x0a0a0a0a;0x0b0b0b0b;0x0c0c0c0c;0x0d0d0d0d;0x0e0e0e0e;0x04040404;0x05050505;0x06060606;0x07070707;0x08080808;0x09090909;0x20202020;0x14141414;0x0;0x10000000;0x20000000;0x30000000;0x40000000;0x50000000;0x60000000;0x70000000;0x80000000;0x90000000;0xA0000000;0xB0000000;0xC0000000;0xD0000000;0xE0000000;0xF0000000;0x91000000;0x92000000;0x93000000;0x94000000;0x95000000;0x96000000;0x97000000;0x98000000;0x99000000;0x9A000000;0x9B000000;0x9C000000;0x9D000000;0x9E000000;0x9F000000.

You can enable for all programs EAF mitigation but not for AW. Also add EMET and iexplore.exe, Steam.exe, t6mp.exe, s1_mp64_ship.exe, SteamService.exe, steamwebhelper.exe, steamerrorreporter.exe from program files folder and add exe from folders sysWOW64 and system32 for mitigation. Apply mitigations settings to these programs also. Add ASR for these exe with modules typed as *.dll or same modules as

previously for EAF+. If a EMET notification appears, you can use Alt+Enter to full screen your game, and Alt+Tab to change of window. Alt+F4 is used to close window. You can add all .exe in EMET. Open regedit, change the key in

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EMET

to the registry value “EnableUnsafeSettings" add

1 instead of 0 but probably your game will not launch

to the registry value “EMET_CE" add

iexplore.exe;Steam.exe;t6mp.exe;s1_mp64_ship.exe;SteamService.exe;steamwebhelper.exe;

steamerrorreporter.exe

You can install the certificate GeoTrust Global CA find in the folder of CoD AW installation files and add this to rules in EMET for Trust websites as GameServers.com, demonware.net, choopa.net, steamcommunity, steampowered.com and ?. To avoid the alerts and steam crash by the what, change the base of code with CFF of your game exe and dll. Also, it can disable hacks use by noobs if values they use are contains in it.

Add all .exe in EMET 5.2 with all mitigations enable but not ASR. With CoD BO2, it will run. But with CoD AW, with EAF mitigation you will not be able to connect, and with stack pivot mitigation it will not start.

If you encounter problems to start your computer session with EMET you must let push the button F8 at computer start, then select hard drive, and let push again F8 to start your computer in safe mode and uninstall EMET or change configurations in it. Also you can use shift key press when you click on restart to open advanced start. From it, you can choose a restore point. It’s created when you uninstall multi-language frameworks, or Nvidia audio driver or when you install or repair DIRECTX driver found in common redist folders of your games. You can also create a restore point in control panel in System under the tab System protection.

If hackers has modified your game, you can change the name of the steam library folder where game is installed, then you need to click install and specify the new folder. All Games files will be automatically detected but you must check integrity of it. Don't forget to change in EMET and Windows firewall the path of the exe of the game (you can add all exe in EMET).

5.5. Flush Memory

You can flush memory by creating a new shortcut icon on your desktop and add in the target browser:

%windir%\system32\rundll32.exe advapi32.dll,ProcessIdleTasks for Windows 32 bits

%windir%\SysWOW64\rundll32.exe advapi32.dll,ProcessIdleTasks for Windows 64 bits

The other solution is to create a C++ program with these codes:

```
#pragma once
#include <windows.h>
namespace start {

	using namespace System;
	using namespace System::ComponentModel;
	using namespace System::Collections;
	using namespace System::Windows::Forms;
	using namespace System::Data;
	using namespace System::Drawing;
	/// <summary>
	/// Summary for Form1
	/// </summary>
	public ref class Form1 : public System::Windows::Forms::Form
	{
	public:

		Form1(void)
		{
			InitializeComponent();
			while (true)
			{
	System::Diagnostics::Process::Start("rundll32.exe",
"advapi32.dll,ProcessIdleTasks");
			Sleep(2000);
			}
		}

	protected:
		/// <summary>
		/// Clean up any resources being used.
		/// </summary>
		~Form1()
		{
			if (components)
```

```
                {
                        delete components;
                }
        }

    private:
        /// <summary>
        /// Required designer variable.
        /// </summary>
        System::ComponentModel::Container ^components;

#pragma region Windows Form Designer generated code
        /// <summary>
        /// Required method for Designer support - do not modify
        /// the contents of this method with the code editor.
        /// </summary>
        void InitializeComponent(void)
        {
                this->SuspendLayout();
                //
                // Form1
                //
                this->AutoScaleDimensions = System::Drawing::SizeF(6, 13);
                this->AutoScaleMode = System::Windows::Forms::AutoScaleMode::Font;
                this->ClientSize = System::Drawing::Size(284, 264);
                this->Name = L"Form1";
                this->Text = L"start";
                this->ResumeLayout(false);
        }
#pragma endregion
    };
}
```

5.6. Netcat

Netcat (nc111nt.zip) is a networking tool allowing transforming TCP to UDP to connect with server, computer or user. You can use it to connect your PC from your network to listen to a port in UDP on another PC. IP of demonware.net 209.170.124.117 can forward to AW lobby. Using the following command dos in cmd.exe

cd C:\Users\Michael\Downloads\nc111nt

C:\Users\Michael\Downloads\nc111nt >nc -L -p 3074 | nc -u 209.170.124.117 3074

nc -L -p 1-65535 | nc -l -p 1-65535 & nc -L -p 3074 | nc -u 209.170.124.117 3074 & nc -L -p 1-65535 | nc -u 8.8.4.4 1-65535 & nc -L -p 1-65535 | nc -u 8.8.8.8 1-65535

would secure the connection to AW lobby. Netcat can be downloaded here http://joncraton.org/files/nc111nt.zip.

5.7. ESL Wire Anti-Cheat

I strongly recommend to use ESL Wire Anti-Cheat cause it check if someone is using lags to have an unfair advantage, and cause lot of games are supported. Some games on Steam incorporate ESL. It help you to be connected on Steam secure servers protected by VAC, and maybe send information to Steam support in order cheaters be banned. Download of ESL Wire and more information are available on the official website of ESL. UAC for Universal Anti-Cheat is less efficient, but for using it with a community of friends using UAC, it do the job also.

5.8. WTFast server GPN

I strongly recommend using WTFast GPN (Game Private Network) to be forwarded on secure official servers for BO3 in conjunction of Windows firewall. For it you need to create outbound traffic rules in Windows firewall for WTFast in the folder WTFast in program files in UDP and TCP. Open all TCP and UDP ports on your modem for your computer without nat/pat rule for port 3074 in UDP. You can choose which WTFast server will control your game connection and so task as a VPN for relocalization. It runs better than with privatetunnel VPN program. You need Windows firewall rules for BO3, as outbound rules in TCP for distant ports 80, 443, 3074, 4986, in UDP for local and distant port 3074 with distant IP 185.34.104.124, 185.34.107.50, 185.34.107.52, in UDP local ports 3074, 4986 and distant ports 33040, 33050, 33060, 33070, 33080, 33090, 33100, 33110, 33120, 33130, 33140. It will establish connection to servers through WTFast.

5.9. VPN programs and proxy

For securely and annonymously use internet for your online activity, there is VPN programs: https://www.privatetunnel.com/home/#, http://www.hotspotshield.com/fr, https://switchvpn.net/, https://openvpn.net/, https://hide.me/en/software/windows, https://www.softether.org, https://openvpn.net/index.php/open-source/downloads.html,

https://www.goldenfrog.com/vyprvpn/usa-vpn, https://fra.privateinternetaccess.com/, https://www.mudfish.com, https://www.hotspotshield.com/vpn-for-windows/. It's programs used my moders for open hacked lobbies, cause it's easy to have any IP even reserved IP. Here you can find proxy and vpn servers list:

http://www.proxy4free.com/list/webproxy_country4.html,

http://www.gatherproxy.com/sockslist

These other programs allow to not play in a region full of cheaters: hidemyip, FreeHideIP... Check if your external IP changed, for it look in network options in AW. You must adapt the maximum ping allowed; look in configuration file of AW. Using vpntunnel from https://www.privatetunnel.com isn't the best way to secure your identity and to play on secure servers. It have no effect on forwarding or not on hacked lobbies. I don't recommend using VPN programs. I tested premium version of hide-my-ip 6 but what it pretend to do isn't running. It don't hide my IP in advanced warfare as shown in system information and for using hyde-my-ip, it require to open allowing rules with all protocols for services, Steam, Uplay, Games, also starting Steam without TCP command. It's harmful for my computer. You can't use DNS protection option otherwise DNS client will not run. SSL and TLS connection options have no effect.

In Windows 10, you can add a proxy server for your network connection. The proxy can be the address 209.170.124.117 and port 3074 corresponding to AW lobby, and the address 209.170.124.209 and port 3074 corresponding to BO2 lobby (you see it with the cmd prompt command dos ipconfig/displaydns). Remove the proxy to have Steam store connection because http and https ports are replaced by xbox port with this kind of proxy. Demonware has locations in Vancouver, Dublin, and Shanghai supporting Activision Publishing, so your proxy server IP must have an address near these locations. Type in google search tool: speedguide IP Vancouver or Dublin or Shanghai, to find an IP closer for setting it

in the parameters of proxy server for your network connection. As proxy IP and port, I recommend to set it with the IP of DNS server you choose with the port 53 (client DNS). You can add as proxy server the IP and port corresponding to a hidden steam proxy server with IP and port shown in steamwebhelper.exe with perfmon.exe when you notice the change when you set another IP and port before disabling proxy server for your network. You should have Steam store connection using the IP and port shown but not access to world wild web.

5.10. Putty sponsored by Microsoft for Telnet connections

I tried the network SSH tool PuTTY with a rule for port 53 in TCP, to enable SSH and Telnet connections with my modem and other IP. Also repairing the driver of my network card with official driver on Realtek site. Connection to servers changed from Europeans to Russians. Even worst.

5.11. Other firewalls

On http://www.zonealarm.com/security/en-us/fza-install-steps.htm you can download a good firewall allowing to secure your identity and connection to servers. Also there is a game mod to enable when playing very smart, but enable deny all new rules just before finding a match. Accept BO3 to have internet connection. In settings let allowing secure and public servers, otherwise put settings with higher security. Take care to enable again Windows firewall after first installation or restart of your computer. But I don't recommend zone alarm firewall like other unofficial firewall: Norton internet security, Sygate PSPF, http://www.arcai.com/ Netcut, CHX-I, LnS, http://www.8signs.com/ 8Signs, JPF2 Jetico Personal Firewall, Outpost pro. It don't do better than Windows firewall. Avast, Norton, comodo, bitdefender are useless to avoid fighting against cheaters on every match of BO3. Also their firewalls disable Windows firewall. Like ESL Wire and WTFast useless.

6. Conclusion

In regards of people that don't mind there is hacked lobbies, I've seen that opening ports between 14000 and 14599 in UDP, and only two IP (108.61.237.150 and 108.61.237.151) in Windows firewall for find a match, 5 lobbies are available to be connected in. So there is 3 hacked lobbies and only 2 secure lobbies protected by VAC and TAC. Also, I've seen the same lobby with the same clan (FaiL) at the same time with the same IP on two different scales of ports (14100-14200 and 14400-14500). It corresponds to a PC connection to a hacked lobby but not to a server connection. So people defending that there isn't cheaters or they have only seen three cheaters, totally fail. I've seen the site of the game DayZ reporting a server own and hosted by gameservers.com with the IP 93.93.65.200, but it's probably a fake name to make believe gameservers.com own the server, however, it's a cheater that create this server on his computer, because the IP is own by iberbit (Innovasoft, they are official servidores of MOH Warfighter and worked with Infinity Ward for MW3. 93.93.64.0/21 are good IP to play with on BO2). So BO2 must encounter this kind of hacked lobby. Gameservers worked with 3arc (Treyarch) for BO1, so on BO2, they must worked together also. Fighting hackers and cheaters isn't easy, and their doing are very annoying for everyone. Maybe the solution exposed here is or isn't good, but it's a good basis to further research. For the experience in my case, I was able to enjoy playing the best multiplayer game of this day, but before it was very annoying to fight and play with a lot of cheaters because the game is very popular, and a lot of players stop playing it because of lags introduced by hackers and cheaters, moreover they wanted that we believe they have skill and starting to insult players because cheaters has no intellect and conscious while invaded the game leting only one chance for them to enjoy the game. Cheaters open hacked lobbies with their computers like on IP 195.122.134.0 to 195.122.135.255 where it's impossible to find a match by forwarding only one port with Windows firewall, but not when forwarding an entire scale

of ports like 14000-14099. A server is associate with one port and one IP only. These IP was also used for servers available, when other servers was all in maintenance and so not available, at the same time. The IP of gamemservers/clanservers are good IP (108.61.230.0-108.61.239.255) if you choose the good port like 14140 or one like 14000, 14030, 14060, 14090, 14100, 14130, 14140, 14150, 14160, 14180, 14190, 14200, 14210, 14220, 14250, 14290, but if you don't find a match on one of the port, it was probably a bad port forwarding to hacked lobbies. IP 195.122.134.0 to 195.122.135.255 is because servers were always here when others were not here after game update, a german banned after playing against him on a server corresponding IP, one time in the killfeed it appeared a name followed by cheat codes detected. Also, I was banned from BO2 forum cause explaining that for some server IP you can't get banned, and for these server IP, there is bans occurring. People said I was explaining how to not get banned. IP 108.61.0.0/16 is because it's shown in Steam display servers for secure servers of games like Killing Floor 2, when it's written Gameservers.com Official Server… You can add the tab server IP. But for different IP and ports tested, there was always cheaters in each match on BO2.

Each time I tried and arrived to something, the next day all my works were undo on BO2. Wallhackers and aimboters again and again, every match. For finally been VAC banned without using any hacks, even if I asked steam support to help me to know IP and port of servers. They said, "we don't give any information on VAC".

For finishing, here my table of search ports and IP on BO2 and AW as following… Here my report on ports and IP for CoD BO2:

14030, match..., (Aimboter/wallhacker)..., lags ?, ..., (108.61.237.151) (TDM), match (108.61.237.151) (FAO), no more match (TDM), 14090, no cheaters (2 days), then clan of cheaters + lot of cheaters (wallhackers/aimboters/bulletkillers), w/f=0, k/d=0.2 (TDM), match (108.61.237.155) (FAO), match (108.61.237.155) (TDM), match (108.61.237.155) (D),

14140, Lot of cheaters (wallhackers/aimboters/bulletkillers) k/d=0.2, (2 IP) (TDM), no match (FAO), 14150, Lot of cheaters (wallhackers/aimboters/bulletkillers), come, go, then come again after, w/f = 0.3, k/d = 0.9, 6th place (TDM), match (108.61.237.153) (FAO), match (TDM) (108.61.237.153), match (108.61.237.153) (D), 14210, match..., (Aimboter/wallhacker)..., lags ?, ..., long to get into match, ... (TDM), no match (FAO), 14220, match 2/3 full (prestige masters), long to get into match, big lags, big lag comp, aimboters/wallhackers, clan of cheaters, cheater here hosting its shit (TDM), match (108.61.237.169) (FAO), no more match (TDM), 14290, match..., Cheater Adren, lags, nuketown, cheaters gone, noobs, ... (Wallhackers/aimboters), can't get a kill (TDM), no match (FAO), 14300, match (TDM), match (108.61.237.162) (FAO), no more match (TDM), 14310, match 9/10 full, (108.61.237.153), only newbies (TDM), match (108.61.237.153), (FAO), match (108.61.237.153) (TDM), match (108.61.237.153) (DEM), 14330, match (108.61.237.155), very hard to fill with players, only newbies (TDM), no match (FAO), 14340, match (108.61.237.153), very hard to fill with players, only newbies, then clan of master prestiges (3 of clan RioT), end then sounds, (player Kami) (TDM), no match (FAO)
14360, sounds, match (108.61.237.153), long to get into match, easy to fill with players, lot of level 55 1st prestige, (player Kami), lags on tactic insertion, (TDM), no match (FAO)
14370, match started (108.61.237.155), long to get into match, A Big Cheatard In, fill with newbies, (TDM), match (108.61.237.162) (FAO), 14380, match started (108.61.237.155), easy to get into match, (TDM), match (108.61.237.153) (FAO), 14370 & 14380, full of cheaters and clan of big cheaters (half cheating), unplayable, big aimboters/bulletkillers with emblem "get skill please" saying "spawn trap faggot"...

Here my report on ports and IP for CoD AW: Ports 33000-33099: IP 195.122.135.231 big aimboter gone after one match, IP 173.199.105.17 aimboters and wallhackers gone after one match, IP 195.122.134.185 no cheater, no more match. Ports 33100-33199: no more

match. Ports 33200-33299: IP 173.199.110.95 big cheatards with aimbot, wallhack, lag switch and god mode, ever gone but very noob. Ports 33200-33230: no more match. Ports 33230-33240: IP 173.199.110.95 noobs and two big cheatards that opened their hacked lobbies with them and only noobs, being good disconnect us, IP 173.199.105.91 noobs and two big cheatards that opened their hacked lobbies with them and only noobs, being good disconnect us. Ports 33240-33250: no more match. Ports 33250-33260: IP 173.199.105.20 only noobs cheatards. Ports 33260-33270: IP 173.199.105.18 only newbies, hacked lobby of a big noob believing his hacked lobby isn't a cheat where we are disconnected, IP 173.199.105.18 only newbies, hacked lobby of a big noob believing his hacked lobby isn't a cheat where we are disconnected, IP 173.199.105.27 only newbies, hacked lobby of a big noob believing his hacked lobby isn't a cheat where we are disconnected. Ports 33270-33280: IP 173.199.105.27 always loosing against same cheatards. Ports 33280-33290: IP 173.199.105.20 only fill by trigger aimboters and wallhackers looking at left or right on a wall before killing, IP 195.122.134.188 only fill by trigger aimboters and wallhackers looking at left or right on a wall before killing, IP 173.199.105.20 only fill by trigger aimboters and wallhackers looking at left or right on a wall before killing, IP 173.199.105.86 only fill by trigger aimboters and wallhackers looking at left or right on a wall before killing. Ports 33290-33299: IP 195.122.135.235 all cheatards in same team. Ports 33300-33399: IP 173.199.105.20 full of cheatards never gone. Ports 33300-33310: IP 108.61.116.130 full of cheatards never gone, IP 173.199.105.30 full of cheatards never gone, IP 195.122.135.235 full of cheatards never gone, IP 173.199.105.15 full of cheatards never gone. Ports 33330-33340: IP 173.199.105.15 full of aimboters never gone, IP 173.199.105.27 full of aimboters never gone, IP 173.199.105.27 full of aimboters never gone. Ports 33341-33399, 33400-33499, 33500-33599, 33600-33699, 33700-33799, 33800-33899, 33900-33999: no more match.

As partial conclusion, people prefers cheating instead of understand how to set properly Windows firewall and work to find good server ports using perfmon and Windows firewall. Same IP used on different ports forward to hacked lobbies, so the different ports where there is these same IP are ports of hacked lobbies open by cheater computers. I've seen that same lobby with same cheaters changed of IP and ports between two matches. When letting all IP of connections to server, it almost only forward to hacked lobbies. Also I have encountered hacked lobby with fast XP on IP 195.122.135.56 (after forwarded on the fast XP lobby sledgehammer rested my progress), and a lobby with this IP range on port 3074, on AW. For the server IP of BO3, I've tried to allow only IP shown in System when searching a match because IP normally shown in System are normally only secure IP. These IP are: 185.34.0.0/16, 209.170.0.0/16, 192.168.1.255, 95.141.40.105, 196.41.143.15, 152.111.192.242, 189.1.169.47, 104.238.166.202, 189.1.171.237, 189.1.172.27, 177.54.146.166, … The IP in the range 4.79.0.0/16 was free of cheaters during 10 matches, then after 20 matches there were only cheaters. All matches on BO3 are filled with cheaters even if there is Valve Anti Cheat and Treyarch Anti-Cheat, and even on consoles. Developers are cheaters that need more and more money so they banned only cheaters after they can buy again the game to cheat another time. If it's too soon, they unbanned, saying it was a false banned. The cheaters don't play cheating enough time to buy the game, so it complains on the forums screaming like cry babies banned for no reason. They offer a free copy to cheaters.

On hacked lobbies cheaters can't be banned because cheaters are blocking all traffic that can make ban them, like VAC checking. I've tried to set port 33000 for the server port in the Windows firewall rule allowing servers connection instead of distant ports 1024-65535 because hacked lobbies open by cheaters computers and hacks use more than one port. To control only one port to be used, control the distant IP range like 0.0.0.0-184.255.255.255 for the rule with port 33000 and 185.0.0.0-255.255.255.255 for the rule with port 3074. I also

tried to create two rules allowing if secure in TCP and UDP with local and distant ports 1024-65535 and with all local and distant IP, for all programs and services, applied for all group policy in local security entity, activate at last. Rule in UDP allow connection but the same rule in TCP don't allow connection. I tried to create nat/pat rules on my modem and inbound allowing rule for BO3 in Windows firewall for ports 33000-33150 in UDP but no match was found. I also tried to have connection only with inbound traffic but it fail to connect to Steam and DNS.

For last attempt, I've tried to peer a wireless connection to network for my gaming computer with a network wire. From the host computer you just have to open properties of the network card used to have the network, under the tab sharing you can allow local connection to be peered with other computers connected to this computer host. The only usefull rule in Windows firewall of the host is an inbound rule in UDP with local port 53, all distant ports for the service distant access connection manager. A server DNS only resolve domain names, so it's useless to secure a PC with a DNS server. I've tried to put a wrong DNS server IP, I still have connection to Steam. So you can add on your gaming PC the UDP allowing if secure rule with local and distant ports 1024-65535 as explained in the section above. It's better if you set in IPv4 properties an IP of a server DNS near IP of Demonware.net from Irland shown with the dos command ipconfig/displaydns or perfmon.exe. You can find the IP of primary DNS on the website http://public-dns.info/, the IP of auxiliary DNS can be 127.0.0.1 (localhost). You need to allow IP of servers with a domain name like 108.61.230.117.constant.com in the Windows firewall rule for the game with local port 3074 in UDP. When you set IPv4 properties from network parameters it's better to set advanced settings with DNS and WINS servers Norton DNS server IP (199.85.126.30) and disable the peer network mod with computers of your network called NetBios on TCP/IP.

The conclusion is if a game use more than only one port in UDP for connection to lobbies, it allows cheaters to open hacked lobbies... So you should consider it to take your time in a multiplayer game. Call of Duty support said to open only port 3074 but there isn't one match on this port, and you must open a lot of ports like with the port 3074 that allow all ports if you create a nat/pat rule for port 3074 in UDP. There aren't any other ports that allow this. Take care when you open port 3074 with a na/pat rule because it will open all ports, even if your modem firewall doesn't allow all other ports. It's like you open a nat/pat rule for each port allowing all inbound traffic very harmful for security. To choose a multiplayer game you will lose time take care of information given and how the game uses really UDP ports, otherwise you will encounter a lot of cheaters destroying your PC. The first information you will take is from the support of developers and then from the community less accurate.

Payday 2 requires you open ports in UDP for steam.exe, so it can't be hacked like BO3 because Steam is a secure platform that don't allow hackers to change the way it run. It's both the platform to connect to your account and to connect people together in Payday 2. In this game cheaters are detected by the engine and kicked, never was and will be in call of duty hack fest games. I saw that in official competition of AW, they were using wallhacks with a game file modification. There will be always cheaters in call of duty games, but it was a school case very interesting to find some methods to secure our computers and the truth about lying developers. These games are only a big hack made by cheaters for cheaters using cheaters servers. Not everyone are cheaters, with my information you will find good multiplayer games without these big retards with no respect for others.

In abstract you need these outbound traffic Windows firewall rules for BO3 as example... Allowing rules, with all local ports, for client DNS distant port 53 in UDP distant IP your DNS server IP like 192.168.1.1, for Steam distant ports 80, 443, 27000-27050 in TCP, 3478 and 4379-4380 in UDP, for the game distant ports 80, 443, 3074 in TCP, for

Steamwebhelper, Uplay and Origin distant ports 80, 443 in TCP, with local port 3074 for the game distant ports 3074, 33040, 33050, 33060, 33070, 33080, 33090, 33100, 33110, 33120, 33130, 33140 in UDP (all these allowing rules with at least IP 0.0.0.0-223.255.255.255 or all IP cause it's better otherwise rules allowing if secure with group policy for programs and the two others in TCP and UDP for all programs would not be effective). Double the allowing rules with allowing if secure rules with second option of security; deny the rules for the group policy local service or system (more secure) under the tab local security entity. Multiply rules allowing if secure for each local security entity for ports in UDP for BO3. You can't do it for DNS client service. Create allowing if secure rules, with all local ports, all distant ports, all programs and services in TCP and UDP. All rules allowing if secure with second option of authentication. Deny the allowing if secure rules for the group policy local service or system (more secure) in local security entity if you have not set IP range like explained for allowing rules but normally it’s not necessary even if you have not set distant IP in allowing rules. Blocking rules, local IP out of your computer internal IP range, distant IP 224.0.0.0-255.255.255.255, public and domain profiles, in UDP with distant IP 0.0.0.0-108.61.122.0, 108.61.122.255-185.34.104.0, 185.34.107.255-192.168.1.0, 192.168.1.2-255.255.255.255. 3 blocking rules in UDP, one with distant port 3074 with distant IP 0.0.0.0-185.34.104.123, 185.34.104.125-185.34.107.149, 185.34.107.51, 185.34.107.53-255.255.255.255, one with distant ports 0-52, 54-3073, 3075-65535 with distant IP 0.0.0.0-108.61.122.0, 108.61.122.255-108.61.237.0, 108.61.237.255-255.255.255.255, the last one with all distant ports with distant IP 0.0.0.0-108.61.122.0, 108.61.122.255-108.61.237.0, 108.61.237.255-185.34.104.123, 185.34.104.125-185.34.107.49, 185.34.107.51, 185.34.107.53-192.168.1.0, 192.168.1.2-255.255.255.255 (choose the IP of servers you find more accurate with the lowest ping you have when playing). A Security traffic connection rule IPsec tunnel with terminal endpoint 1 IP 0.0.0.0-223.255.255.255 and all terminal endpoint 2 IP. Security traffic

connection rule for tunnel IPsec with authentication required for inbound and outbound traffic. Create isolation rules in rule of connection security, one with require authentication with user authentication method, one with ask authentication with computer authentication method. Let all IP in terminal endpoints 1 and 2. IPsec properties in Windows firewall properties set to maximum security, denying all users and all computers for tunnel. Between same rules allowing and allowing if secure, the last rule activate is the one taking effect on the other. Activate rules allowing if secure after rules allowing. Ports UDP/TCP and IP for AW are the same for BO3, but there aren't any p2p servers... Sometimes there are problems of connections when you set Windows firewall. Set it to default for have connection with BO3, then import strategy before find a match. Set properties of Windows firewall and your network card to not accept monodiffusion traffic.

Ports used by BO3 for official servers seems to be 33000, 33010, 33020, 33030, 33040, 33050, 33060, 33070, 33080, 33090, 33100, 33110, 33120, 33130, 33140, 33150 in UDP and IP 108.61.99.0 to 108.61.239.255, 173.199.64.0 to 173.199.111.255 corresponding to almost 50 matches found. Fake of these IP with these ports seems to unexist. But servers can be crashed by hacks of cheaters like for official ARK game servers. When you get out of servers if the server don't respond anymore, a message say you've been disconnected from the server or the server don't respond and not the host don't respond or connection to host lost. Other ports and IP used by BO3 are 80, 443, 3074 and 185.34.0.0/16, 209.170.0.0/16. After port 28808, ports registered must finish by a 0. You can have information on ports on the website speedguide.net but it's not updated often and only few are available. Opening a nat/pat rule for port 3074 seem to be dangerous cause it allow all inbound and outbound traffic with all ports (1-65535). I tried to disable and stop the services netbios, DHCP client and DNS client after authentication in BO3 but without success... The rules I used when searching a match in BO3 are local ports 1024-65535 distant ports 80, 443, 3074, 4986, all

distant IP in TCP, and local and distant port 3074, distant IP 185.34.104.124, 185.34.107.50 and 185.34.107.52 in UDP, and after searching with perfmon.exe which IP of servers, I deduced distant IP 108.61.237.151 to 108.61.237.233 with local port 3074 and distant ports 33040, 33050, 33060, 33070, 33080, 33090, 33100, 33110, 33120, 33130, 33140 in UDP. The results shown in the following picture are a proof that the IP not in the order classified by perfmon and probably some other are DNS addresses used by VPN users opening hacked lobbies (they hide their IP changed with openVPN behind a DNS address but can be a little the same as true IP, so cheaters are everywhere in the world). The addresses shown don't correspond to the IP of connection and can be totally different like the last IP in the picture.

Adresse	Adresse
108.61.102.21	108.61.237.204
108.61.102.40	108.61.237.206
108.61.112.23	108.61.237.207
108.61.116.60	108.61.237.208
108.61.116.99	108.61.237.209
108.61.122.103	108.61.237.210
108.61.122.110	108.61.237.211
108.61.122.206	108.61.237.212
108.61.122.21	108.61.237.214
108.61.122.222	108.61.237.215
108.61.122.227	108.61.237.216
108.61.122.230.choopa.net	108.61.237.217
108.61.122.231	108.61.237.219
108.61.122.234	108.61.237.220
108.61.122.235	108.61.237.221
108.61.122.237	108.61.237.222
108.61.122.238	108.61.237.223
108.61.122.24	108.61.237.224
108.61.122.242	108.61.237.225
108.61.122.26	108.61.237.226
108.61.122.42	108.61.237.227
108.61.122.44	108.61.237.228
108.61.122.46	108.61.237.230
108.61.122.63	108.61.237.232
108.61.122.75	108.61.237.233
108.61.122.76	108.61.97.14
108.61.122.79	108.61.98.19
108.61.237.151	162.254.197.41
108.61.237.156	185.34.104.124
108.61.237.163	185.34.107.50
108.61.237.165	185.34.107.52
108.61.237.166	189.1.169.47
108.61.237.183	189.1.172.27
108.61.237.185	196.41.143.15
108.61.237.188	199.85.126.30
108.61.237.190	95.141.40.105

Gameservers.com from http://bgp.he.net is corresponding to IP 108.61.230.0 to 108.61.239.255. It was written on a cheat site, that there was 400 000 members of cheat sites ready to cheat when BO2 launched. I really think that gameservers/clanservers and call of duty developers allow cheaters and crackers to play on their servers dispatching on every match these noobs. Also they open hacked lobbies like the one I've seen on AW after 10 hours of using this game on one of the IP in the range 195.122.135.0/24. They make propaganda on Steam forum to make believe there aren't any cheaters and we are noobs, insulting us of all bird names moreover. VAC never banned cheaters I reported. They never went. For Black Ops III, instead of the IP of servers 93.93.0.0/16 or 108.61.230.0 to 108.61.239.255, define the IP 4.79.0.0/16 in Windows firewall because you find a lot of matches with same IP and port with less cheaters. The IP corresponds to Level 3 communications but they are host by Choopa, LLC as shown on http://bgp.he.net/. IP before 4.255.255.255 included are private IP and can't be used by VPN users and hosts. You can export/import the Windows firewall strategy from right tab. Block IP of gameservers/clanservers servers with server side hacks as: 95.141.0.0/16, 195.122.0.0/16, 93.93.0.0/16, 189.1.0.0/16, 108.61.0.0/16, 197.80.0.0/16, 197.84.0.0/16, 173.199.0.0/16, 45.63.80.0/20, 45.63.124.0/22, 45.63.0.0/16, 107.191.0.0/16, 4.79.0.0/16, 152.111.0.0/16, 104.238.0.0/16, 196.41.0.0/16, 208.167.0.0/16, 68.232.0.0/16, 63.208.0.0/16, 62.67.0.0/16, 177.54.0.0/16... Other IP of gameservers can be found with call of duty games searching a match. It's important to block IP from Choopa, LLC and all organizations that they host cause it hack your computer. Use information on http://bgp.he.net to know which organizations own IP. On a server with IP 152.111.192.242, I had only IP associated of BO3 authentication like shown on the following picture of perfmon but there was still server side hacks.

Processus	PID	Adresse
BlackOps3.exe	3796	152.111.192.242
BlackOps3.exe	3796	185.34.107.52
BlackOps3.exe	3796	185.34.107.50
BlackOps3.exe	3796	185.34.104.124
BlackOps3.exe	3796	pc-salon

It's better if you block ports/IP instead of setting local and distant ports/IP for each allowing rules cause group policy setting for allowing if secure rules and the two allowing if secure rules for all programs and services in TCP and UDP would not be effective. On servers not officials of gameservers/clanservers cheaters don't need hacks running on their computers cause these servers corresponds to hacked lobbies with lag switch, lag compensation, grenade disabler, respawn kill… So like for The Division create rules allowing and allowing if secure denying the rule for group policy System in TCP and UDP with all local and distant ports for each program. Create the two allowing if secure rules for all programs and services in TCP and UDP. And create blocking rules for ports/IP between ports/IP of connections for each program. It blocks VPN connections. Add two security connection rules one with users authentication required for inbound and outbound traffic, one with computers authentication required for inbound traffic and asked for outbound traffic. Block all distant IP in the range of your network computers but not the IP corresponding to your modem address or DNS server. Block modem internal distant IP or DNS server IP in the range out of port 53 in UDP, and block all distant IP out of modem internal IP or DNS server IP for port 53 in UDP. Also block all distant IP suspicious. Block for all programs and services UDP ports out of the range of server ports of the game you play. To take on allowing rules, it's better if you put the range of IP 223.255.255.255 for allowing if secure rules with security entity set for System. IANA ports can be blocked. local ports in UDP and TCP from 1 to 1023, distant ports 1-79, 81-442, 444-1023 in TCP and 1-52, 54-1023 in UDP. You can create different Windows firewall strategy and export/import it. You can watch and determine IP using perfmon.exe and a google research in order to block it with Windows firewall. I saw IP of connection to match

don't corresponding to IP shown in perfmon but closer. So take care and use NewB to block these IP unwanted. The best solution to avoid hacked lobbies connection is to create blocking rules for IP range (corresponding to IP of internet provider range used by unofficial servers) from IP shown with perfmon when playing and seeing cheaters and cheats like the IP range I report here: 195.122.0.0/16, 108.61.237.0/24, 108.61.116.0/24, 173.199.105.0/24. But using NewB, you just have to scan IP of VPN servers to block it and then block one by one each IP of users having an IP closer of official servers, using Windows firewall. It's important to block IP in TCP and UDP of servers corresponding to a modem/router network. NewB detects and blocks these IP. The method is useless for call of duty games where matches are hosted by gameservers cracking servers and opening hacked lobbies maybe. Developers of the series pay gameservers for hosting match. It doesn't deserve to be played maybe. All games of the series are full of cheaters aimboting or wallhacking? If you speak with these noobs they will insult you of noob and lot of nazi comments, also they will threaten you. But it's good to protect your PC using Windows firewall for your programs creating UDP and TCP allowing rules and for client DNS UDP allowing rule, in conjunction with blocking rules for ports between range of connections and suspicious IP. You can use NewB to block IP in a list find on these sites:

http://www.nirsoft.net/countryip/index.html, http://cyber-defense.sans.org/blog/2011/10/25/windows-firewall-script-block-addresses-network-ranges, http://cyber-defense.sans.org/blog/2010/08/31/windows-dns-server-blackhole-blacklist, http://www.ipdeny.com/ipblocks/, http://www.okean.com/thegoods.html, http://www.countryipblocks.net/, http://www.wizcrafts.net/iptables-blocklists.html, http://www.iblocklist.com, http://lite.ip2location.com.

In order to have a compatible blocking IP list file for use with NewB, you can use Excel to separate rows with characters (using converter with selection or opening a text file), to delete

unwanted rows, then you can use wordpad to replace tabulations by empty strings (copy/paste tabulations and replace it with the replace tool in wordpad).

Maybe if people were using NewB, we will see lot of cheaters banned, but alone as creator and people not interested, it's hard to populate official servers, people believing there isn't any hacked lobbies, cause of cheaters propaganda and humanized aimbots. Lot of IP is used by unofficial servers. Pc master race is transformed in PC cheater race. The majority of people stopped playing the hack fest land is call of duty. Lot of people doesn't find any match on Advanced Warfare because cheaters made go players. The problem is real but who knows if developers are concerned or gameservers implicated?

I tried to disable network services to deny connections of VPN, users and unsecure servers, but no effect overcame on the hackfest happening on Gamservers owners of servers. Humanized aimbot users never kicked, never banned, banned but still in the game, always lying they don't cheat even if it's obvious with killcams. The humanized aimbot aims automatically enemies but also allies even if allies are behind. Cheaters hiding the cheats they use are so sure to not be banned that they ask us to report them like if we haven't thought of this. Even on consoles Call of Duty games encounter lot of aimboters. They even don't need to watch the game to kill like I've seen in a Stream of someone. Strange things happen like properties of Windows firewall changing alone, installed Microsoft update while Windows update service disabled, like Windows defender enabled alone, lot of services disabled enabled alone, Microsoft Visual frameworks installed alone without installing games, lot of IP appearing in perfmon without opening one program. The hackfest is real and on the entire PC. Let a brand new PC connected to network working alone, I'm sure all regedit entries and all I talked previously will strangely happen. Also when you try to update your PC with Windows update, the PC is dying. It's due to multiplayer games and online services and programs used by hackers modifying it for hacking your PC when it's connected through it. Like on

consoles, using IP blocking in NewB, you can have some legit matches on Call of Duty games otherwise people populate mainly hacked lobbies open with VPN servers detected with NewB. It stays hacked lobbies when users have closer IP as official servers, but you can block each IP one by one in Windows firewall.

I recommend setting a DNS server like Norton ConnectSafe with IP as following: preferred DNS: 199.85.126.30, alternate DNS: 199.85.127.30. I don't think peering network from a computer with console or gaming PC is a good idea but you can try to do it using a secure VPN server installed on the host computer. I recommend the VPN program Hotspot Shield which can be found on https://www.hotspotshield.com/vpn-for-windows/. It doesn't change your external IP as shown by System information of Advanced Warfare.

7. Append

7.1. Connection problems

To know which programs and services use connections, you can restore Windows firewall settings to default after exporting your configurations of Windows firewall. Connections are shown with perfmon, opened from administrative tools in control panel, under the tab network. You can know the path of the programs and services by opening task manager with keystroke control+shift+escape. From the list you can open the folder where the programs and services are. It's useful to know the path to use with rules in Windows firewall. Sometimes games need connections to run, even if there isn't a multiplayer feature, because it can have scoreboard or authentication. For games with denuvo verification you can simply allow distant ports 80 and 443 and local ports 1024-65535 in TCP with a rule in Windows firewall and let rule allowing if secure with all distant and local ports in TCP. Hacked programs like can be Steam owned by your friends can retrieve your external IP and so your connection can be ddos and have a malicious traceroute. To avoid this, you can launch Steam without the option to connect to friends at Steam start.

Now connection to Uplay needs to open Windows firewall rules for Uplay.exe, UplayWebCore.exe and UPC.exe, for ports 80 and 443 in TCP. Sometimes games needs to open ports 80 and 443 in TCP when there is scoreboard, otherwise the game will not be display, but running in background. Even if you are offline, the game will be display, opening the ports 80 and 443 in TCP with rules in Windows firewall. To have better download speed on Steam you can change download region in Steam parameters to United Arab Emirates or whatever is convenient for you but when you restart Steam few times, the download region can be automatically assign. An option can resolve download problems; called empty the cache of downloads. If you want to upload artworks on Steam and see the servers in server browser you must open a rule with all protocols for Steam.exe. I tried to open with NAT/PAT rules Steam ports to see if it will kick cheaters out of servers but without success (ports TCP 27014-27050 and UDP 3478, 4379-4380, 27000-27036). Only peer to peer programs, pornographic websites and Call of Duty games bring mbam to block IP. There is a conflict between VAC and TAC on black ops 2 as hackers deduced because cheaters were not banned, so for black ops 3 don't expect a dedicated server tool appearing as promised on the steam store page of the game before launch, because it would reveal the problem. But people are not blind, they can recognize in each match who cheat. I recommend not rent servers to gameservers/clanservers and blocking their IP as I recommend playing on dedicated servers VAC enable and creating your own servers with tools and information available on Steam. Only games where you can create servers VAC enable and not only a game with VAC banhammer. In fact VAC on servers can be disabling. Cheaters on Steam forums and their profiles are such sure to not be banned that they insult people of noobs, claim they are not banned, so they can't cheating. They are so sure that they can't be banned, is because they pay their hacks to developers and editors of call of duty games. On AW consoles official competition organized each year, competitors were using wallhacks where enemies and allies

were marked everywhere, every time. Mod like playing only against noobs on BO3 reversed from mod on Payday 2 to play only with good players is undetectable. On BO2 cheaters with cracked games after be banned replacing their game files by skidrow and 4dead1 files, 4Dead1 claiming for MW2 they made a new MW2 game exe against cheaters, are allowed to play on gameservers/clanservers servers. About hacked lobbies where cheaters and cracked games owners can play, like lobbies with fast XP to win, it's possible when the offenders modified the original game files. A friend of mine played PayDay 2 on a lobby of a cheater allowing to prestige two times in one hour, he goes from Level 0-70 to II-40. In my experience, after 10 hours playing CoD AW, there was a lobby with fast XP to win on a server with IP 195.122.134.17 corresponding normally to official servers of gameservers/clanservers (Sledgehammer initialized my level two days later). Call of Duty Developers like Sledgehammer only want your ass be kicked by cheaters like on AW where it kick you out of the match if you don't let you killed, like when you suicide you 20 times with your own semtex. I advice to let all IP in allowing rules, deny a certain group policy in local security entity for allowing if secure rules, to create a blocking rule for the game with IP out of the range of servers you choose and of authentication, and to create a UDP allowing if secure rule for all ports, all IP, all programs and services, all group policy (this one in TCP don't allow TCP connection). Block suspicious distant IP in Windows firewall like your computer internal IP and IP 192.168.1.255 from your own network corresponding to an attack of an unresolved computer presents. Block IP from 0:: to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. Set port source range, with cmd prompt running as administrator: netsh int ipv4 set dynamicportrange tcp startport=1025 numberofports=255 store=persistent, netsh int ipv4 set dynamicportrange udp startport=1025 numberofports=255 store=persistent. Before setting it, you can see default port source range: netsh int ipv4 show dynamicportrange tcp (start=49152, num=16384), netsh int ipv4 show dynamicportrange udp (start=49152,

num=16384). You don't need to restart your computer. Change it often. The goal is to deny connection of whole VPN users, and to find IP of servers where IP near in same locations encounter less people decreasing the bad chance to fall on a hacked lobby open by a cheater that don’t need to go through a VPN. If you encounter same cheaters that use a fake of lag compensation freezing their energy and energy of other players, it corresponds for sure to hacked lobbies. The servers are located in a big town. The cheaters will not give up. The ping of the cheaters is 30 ms. Block these IP to not play on these lobbies.

Open run command with Windows key + R then type MMC, from here you can set security adding snaps. Name the file dsa.msc, domain.msc and dssite.msc, and then copy it in the folder C:\Windows\System32 and C:\Windows\SySWow64.

7.2. Hardware problems

For Flushing memory of GPU and CPU cause of cheaters filling the cache memory of your computer, it exist official tools... From control panel, in administrative tool, you can make a memory diagnosis, helping to remove error in your computer memory. From NVIDIA website: https://developer.nvidia.com/cuda-downloads you can download CUDA toolkit in order to deploy optimization of your graphic card. It's toolkit for visual studio game developers but with it, your computer can access to game features added by developers like GPU cleaning needing the frameworks installed when you install CUDA. Also when you install CUDA, it install automatically the good driver for any NVIDIA graphic cards. Disable GPU from peripherals manager before installing NVIDIA GPU drivers. Use oldest NVIDIA GPU drivers because newest add only graphic features but not performance features. If you changed graphic card you can uninstall old peripheral shown in masked peripherals, also all masked peripherals because they aren't used anymore and so can induce conflicts and latency. NVIDIA Ti drivers for graphic cards are more optimized cause it's made for Virtual Reality. It can be downloaded on NVIDIA website if you specify your graphic card ending with Ti. On

https://gaming.msi.com/fr/features/afterburner you find a program that can optimize performances of your GPU but the program can crash it. Take care to follow and apply my advices in this append. Tool like Afterburner for optimize GPU and CPU is available on Steam. It's named EVGA PrecisionX 16. I don’t advice to overclock your GPU and CPU because there’s a risk of breaks it. Prefer to lower graphic settings in game options. Also available on Steam, there is a tool to update your peripheral drivers named Driver Booster 3.3. Also it remove drivers of peripherals not connected and can help you to resolve some errors of drivers. A firewall useless and expensive compare to Windows firewall is available on Steam named GlassWire recommended by a website with malwares known as Lifehacker.com. You can't block IP by IP like it pretends you can do. Magix PC check & tunning 2016 is better than Driver Booster 3 cause it update your PC for secure it, clean registry, delete internet trace and optimization for visible gain of performance, but it's not free. Unlike Driver Booster 3 for 3 computers, Magix tool is a time life license, so even if you reboot fresh your PC, you keep Magix tool. From peripherals manager in control panel for system peripherals you can uninstall redirector bus of remote desktop peripherals. For Controllers IDE ATA/ATAPI channels ATA in properties under the tab advanced settings, you can disable DMA (Direct Memory Access) but if you do it you can encounter big latency on your computer. Always in peripheral manager set higher security for properties of communications port (com1). I tried to install different drivers from peripheral manager for network card and system, but without success.

After uninstalling masked peripherals, if your network card isn't identifying and recognizing TCP/IP you can uninstall the network driver from the properties tab under driver of your network card when where configure it (but let driver files), then restart your PC, it will install automatically the driver or use the network card driver found on official site of the network card provider.

To flush computer components, a method is too shut down your PC, then unwires electricity, then pushes the button to start. When you buy a brand new PC, for first using, during one week or two weeks, it's better to not warm components too much, because of thermal expansion. Shut down often your PC to let it cold. It's important every year to remove dust from fans with a timbre pincer. Also to blow dry air in the inner of your PC. Take care to programs making fans running too much due to processor and memory leakage. Open task manager with ctrl+shift+esc keystroke and stop tasks taking too much resources. Don't be scary to reboot fresh your computer if you encounter issues. It's better to do it than stay with issues that will become worst with time.

7.3. Softwares problems

You can remove lot of hack exploits with programs from https://fr.malwarebytes.org/. Malwarebytes antimalwares is important to block harmful IP and programs, furthermore if you use peer to peer programs and cracks of games. But again, with any anti-virus and firewalls, nothing avoids fighting against cheaters in call of duty games, even after fresh installation of OS and games. It's better if you run Steam with administrative privilege because sometimes games must run as administrator to avoid bugs in Steam achievements (also try to start a fresh game). Create a desktop shortcut, open properties of it, under the tab shortcut, click on the button advanced, in the window, and check the box to run the program with administrative privilege, apply change. Use the cmd dos prompt command run with administrator privilege sc delete BEService to remove service Battleye for example... Use sc delete the name of service you want to delete like for the service coming with ZoneAlarm. To check the integrity and repair files of your computer system use the command dos in cmd run with administrator privilege as following sfc /scannow. Games can crash giving as main reasons bad DLL loads when you launch it from the root folder. Advanced Warfare had a known issue for a DIRECTX error, unable to find supported monitor. The reason is when you

update your graphic card, driver doesn’t replace all DLL. You can see which DLL are loaded with a game using perfmon. The issue was caused by a old version of a nvidia driver DLL called nvwgf2umx.dll presents in a folder rooting with Advanced Warfare installation files. Sometimes your game doesn’t start because it needs to be root with a DLL from the folder Sys64 or System32. When you launch the game from the exe file directly it can indicate which DLL is lacking. Some applications require to be launched with administrative privilege. To avoid BO3 crashing, you must launch Steam and BO3 with administrative privilege and also set BO3 property with Windows 7 compatibility. If you encounter problem of connection in BO3, restart your modem and computer, change your computer internal IP, uninstall driver of your network card but let driver files and set Windows firewall to default settings then you can import strategy. Don’t forget to adapt your modem firewall. Disable Steam and origin game overlay because it disable streaming where you can be hacked. Set your Steam profile to private or put you offline in order cheaters can't join your game from your Steam profile. Take care to people you add as friends. A method to change memory pagination and clear memory with fresh files is to make a copy of library folder of your games after first installation, rename old folder and then restart Steam, then specify the new folder after a new copy from fresh files. It needs a new copy of fresh files each time you do it. Copy files of BO3 on a hard drive after downloaded it. You can use these files to replace it after uninstallation. Copy of the game files is required for your multiplayer games. Put to masked and readonly games files installed, used to play the games, also Steam and Origin installation files in C:\program files (x64)\ (in order BO3 check files to connect you have to not put installation files to read only and masked, or try to change the hard drive where BO3 is installed and disable Steam library properties of the game for Synchronization with the cloud). The masked files can be shown with folder options (that can be open from the folder shortcuts above the window). Because when you play online, cheaters modify your game

files. Also, like tool of memory diagnosis in administrative tool, you can use the defrag tool to optimize you disks. From peripherals manager for system peripherals you can uninstall redirector bus of remote desktop peripherals. Also from peripherals manager remove or disable drivers and peripherals for debug and debugging tools, also teredo tunnelling and distant access (display masked peripherals). Add drivers of old peripherals. From C:\Windows\System32 open Taskschd.msc and delete all tasks, it can be virus autostart... Also to optimize drivers like for graphic card, network... even games, Origin and Steam, also services, copy DLL in System32 in the root of folders where there is exe files. Increase size of exchange files under the tab virtual memory from performance options in System in control panel. Start run window, type regedit, in HKLM\SYSTEM\\CurrentControlSet\Control\SessionManager\Memory Management create a DWORD value named MoveImages with value ffffffff or fffffffe, or 1. Disable Virtualization of user account control from task manager or with the following registry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System with DWORD value 0 for key EnableVirtualization. Disable remote assistance from the registry keys in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Remote Assistance. It can reduce lags induced by Call of Duty Games cheaters impacting your computer performances. Other regedit entries that can be changed are Computer\HKLM\SOFTWARE\Microsoft\FTH, Fault Tolerant Heap, remove values for Key ExclusionList for better security, and also this regedit entry Computer\HKLM\SYSTEM\ControlSet001\Services\mouhid\Parameters, change values to 1 for keys TreatAbsolutePointerAsAbsolute and TreatAbsoluteAsRelative for better mouse control. Regedit can be open with the Start program typing regedit then clicking on run.

To remove crash and lags like in PayDay 2 where community is angry about micro transactions and so hackers making cheats and mods incorporating hacks to destroy the game,

you can set from task manager (open with ctrl+shift+esc) under the tab details affinity and priority level of all process. For example set all Steam process to affinity processor 1, Payday 2 to processor 2 and 3, and all other process like svchost, dwm, lsass to processor 0. Set Payday 2 with real time priority. Hacks from other computers induce lag and crash cause same memory address are cover by few process, so setting affinity is a way to not be infested. If your game is crashing randomly, you can set all process with a normal priority, and the process of your game to real time priority because it will flush memory and avoid other process to use all the CPU clock. Enable DEP in system in control panel, select advanced tab and click on settings under performance section, select the tab DEP and click on Turn on for all programs and services. Disable remote assistance. Set user account control to high priority from user account in control panel. Also enable Windows Updates to have security updates. With some updates (SQL, codec, Silverlight, updates for Microsoft Windows) of Windows Updates you can encounter lags while playing. You can remove some updates from installed updates in Windows Updates and Programs and Functionalities in control panel. Let only Security updates, Frameworks and Redistributables. Take care to Windows updates if your PC has been infected. Only install security updates.

Setting compatibility modes in properties of the game exe can resolve crash and lags issues. You need to start Steam with administrative privilege. Go to properties of Steam launcher shortcut, then under the tab shortcut, click on advanced, then check the box run as administrator, and apply change. Take care where you install your games. It’s better to install games on the other hard drives than master drive where the OS is installed. Check integrity of game cache files in properties of the game from your game libraries if you encounter issues, and check if DLL aren’t missing by launching the game exe from the folder where the game is installed.

You can increase of Steam levels to show some of your favorite games, screenshots, artworks, guides, reviews, achievements, PC configurations or stylish texts by winning Steam cards of games you playing. You can sell some cards to buy cards for completing pinner in order to win 100 XP each time you create a pinner when you have all cards. Buying cards is very expensive and take a long time. To sell fast cards, put a price one cent under the recommended price but you need also consider the two cents Steam takes on the transaction. Enable Steam guard to secure your Steam account from Steam parameters. For use Steam, I recommend to take the mail address given to you with your internet connection by your internet provider.

7.4. Security problems

To run correctly EMET some services are required like in French biométrie Windows and ouverture de session secondaire. Use EMET 5.5 and add BlackOPs3.exe and Steam.exe to mitigation but disable Mandatory ASLR for BO3 and enable ASR with the same modules as iexplorer. Add to registry in HKLM/SOFTWARE/Microsoft/EMET for the value EMET_CE the following string:

iexplorer.exe;BlackOps3.exe;Steam.exe;svchost.exe;thedivision.exe;Uplay.exe;DOOMx64.exe. From EMET create trust rules and websites with allowed pin rule with certificates the more secure like with certificates SHA2 for ?.?.?.?.choopa.net, ?.?.?.?.constant.com, ?.?.?.?.demonware.net and ?.?.?.?.vultr.com but create blocked rule with no certificates for ?.?.?.?, choopa.net, constant.com, demonware.net and vultr.com. Also you can block fake IP of servers and authentication (185.34.104.124, 184.34.107.50 and 185.34.107.52) and your DNS/modem/router IP with blocked pin rule with no certificates. You can export/import the EMET configuration. With EMET when you enable for a game the mitigation mandatory ASLR normally the game doesn't crash because the game is ASLR enable. Call of Duty games, even BO3 made with new game engine, isn’t ASLR enable. Moreover there isn't any

IP and ports of servers forwarding in a match free of cheaters. Developers of these games are implied in hacks without any doubt. Moreover I only encounter mbam blocking harmful IP of websites on p2p programs of cracked files, porn sites and Call of Duty games. In term of network security in applications, Java is important to be installed on a PC because it allows setting of secure configurations. You need to install Java and configure it for secure activities on your PC.

7.5. Network problems

To avoid fake or disrouting connections, I strongly recommend to never wiring television channels to your screens connected to your computers or consoles. It's something strange but it's totally possible knowing the illuminati behaviour of television channels workers. HDMI wires allow network traffics and screens are connected peripherals with low security. I advice to don't trust even radio frequencies. With wave radio for TV connected with antenna wire, I encounter disconnection of my controller at moment I'm annoying cheaters. Disable wifi as more as you can. If you don't choose the good canal of your wifi, you can encounter cuts of downloads, even on your computers or consoles connected with Ethernet wire. Change canal of your wifi as soon as you detect fake or disrouting connections. Uncheck the box reply to ping under the tab of modem firewall. If the box is autochecked, you have a peripheral with a virus. Use malwarebytes antimalwares to remove it. To set security in your network from modem/router, it's recommended to not enable inbound traffic by opening NAT/PAT rules and by enabling UPnP, to only allow outbound traffic for ports 1-65535 in UDP/TCP, to enable MAC address filtering (achieved with a PC connected with RJ45 wire), to change often modem internal IP and range of internal IP of computers in the network corresponding, to change often external IP by restarting the modem. Set computers and consoles names with confuse words like XboxOne and macbook-admins respectively, thinking to reuse names of different devices connected. You can do it from advanced

parameters of system tab. Also, you can set a computer in demilitarized zone (DMZ) for secure all other computers cause the computer in DMZ will be the only one attacked by hackers. This computer needs to be firewalled with Windows firewall to a high degree because all ports will be forwarded by the modem. Even if the computer in DMZ is offline, all other computers will have internet access and modem firewall activate. Set a static IP to this computer under DHCP tab and add it to DMZ under DMZ tab. You can add your gaming computer or console in No-IP service using the internal IP as host name because it allow to safeguard against DDos attacks like if it's a server. No-IP service is used to have a static external IP for owning a website or self game server. Use the e-mail address given by your internet provider with password you use for connecting to your e-mail box. Alternatively you can secure your network and have more privacy on internet by using the DynDNS service from the website https://desec.io/#!/en/product/dyndns. Follow their instructions sent by e-mail. You need to choose a domain name, an e-mail, and a password to enter in your modem settings. But I advice more the DynDNS service from https://www.dynu.com, updating your external IP and denying network distant access with the Windows tool found at the address https://www.dynu.com/en-US/Support/Download. If a problem occurs, the modem can be initialized manually for fresh start. The following picture explain configuration of how to set a DMZ, No-IP and internal static IP:

configuration DMZ

DMZ		
nom	**adresse IP**	**adresse MAC**
PC4	192.168.1.14	

configuration DynDNS

service	nom d'hôte complet	nom d'utilisateur email	mot de passe	dernière mise à jour
No-IP	192.168.1.130	@orange.fr	********	27/12/16 15:39:18

configuration DHCP

adresse IP statique			
nom	adresse IP	adresse MAC	
XboxOne	192.168.1.130		
PC4	192.168.1.14		

You must change the password to login your modem web page because it's through it you update the modem firmware. Reset from fresh the modem, but you need the identity parameters and to synchronize again modem accessories, if each time you play multiplayer games it's unplayable. Custom firmware can do deviation of connection traffic like if it incorporates VPN or proxy servers. Multiplayer games don’t use security certificates to identify connection, so it's possible to only play on fake servers. Do connection problem test or contact by tchat your internet provider from main web page of your internet provider to show you aren't forwarded on official servers saying there is a routing connection problem. It's better to not enable static IP for internal IP of your devices under DHCP tab of your modem, and so to change often internal IP under network settings of your devices. If you don’t set a server DNS under network settings of your computers, you just need port 80 and 443 in TCP allowed on your modem firewall, but if you use outlook you need to allow ports 80, 443, 995, 110, 20-22, 587, 25 in TCP and 53 in UDP. Create rules for static internal IP of your computers with these ports adding computers under DHCP tab with static IP. Let ports 80 and 443 in TCP for all computers without setting internal IP under modem firewall. So you

can peer secure connections. To set MAC filter, you need to connect your PC to your modem with an Ethernet wire. Change the default password of your modem with a strong password. Sometimes you can make mistakes adding rules in your modem, like adding a computer for static internal IP in DHCP or adding a firewall rule, so next rules can't be add. To avoid the bug, you must restart your modem. When you want to add a phone after a fresh reboot of your modem, for authentication of the phone, you must place the phone on its basis and push the button on your modem to have it in synchronization mode.

7.6. Security with console problems

The only platform you will take pleasure for playing multiplayer games is XBox (no lags, no cheaters). Ports to open in modem/router firewall are only 88 (UDP), 3074-3076 (UDP and TCP), 53 (UDP and TCP), 80 (TCP), 500 (UDP), 3544 (UDP), 4500 (UDP) (don't create any NAT/PAT rules and disable UPnP). Use firewall of your modem/router like shown in the following picture:

application / service	protocole	adresse IP source	masque adresse IP	port source	adresse IP destination	masque adresse IP	port destination	action
88	UDP						88	accepter
500	UDP						500	accepter
3074	les deux						3074	accepter
3075	les deux						3075	accepter
3075	les deux						3075	accepter
3544	UDP						3544	accepter
HTTP	TCP						80	accepter
HTTPS	TCP						443	accepter
POP3	TCP						110	accepter
POP3S	TCP						995	accepter
SMTPAuth	TCP						587	accepter
SMTP	TCP						25	accepter
FTP	les deux						20-21	accepter
SSH	TCP						22	accepter
NTP	UDP						123	accepter
NNTP	TCP						119	accepter
NNTPS	TCP						563	accepter
DNS	les deux						53	accepter
IMAP	TCP						143	accepter
IRC	TCP						6666-6667	rejeter
IMAPS	TCP						993	accepter
ISAKMP	UDP						500	accepter
STUN	UDP						3478	accepter
IPSEC-NAT-T	UDP						4500	accepter
DNSb	les deux				192.168.168.1	0.0.0.0	1-65535	rejeter

You can block gameservers/clanservers IP and block ports as following:

TCP: 0-52, 54-79, 81-3073, 3077-65535,

UDP: 0-52, 54-87, 89-499, 501-3073, 3077-3543, 3545-4499, 4501-65535.

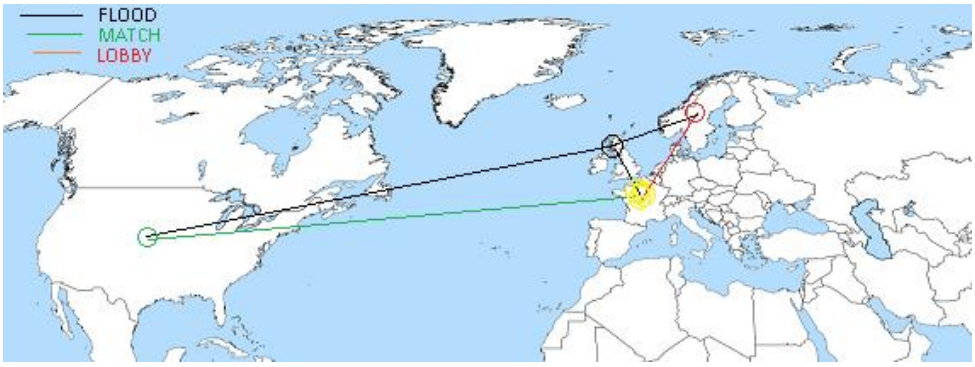
application / service	protocole	adresse IP source	masque adresse IP	port source	adresse IP destination	masque adresse IP	port destination	action
TCP1	TCP	192.168.168.11	0.0.0.0				1-52	rejeter
TCP2	TCP	192.168.168.11	0.0.0.0				54-79	rejeter
TCP3	TCP	192.168.168.11	0.0.0.0				81-3073	rejeter
TCP4	TCP	192.168.168.11	0.0.0.0				3077-65535	rejeter
UDP1	UDP	192.168.168.11	0.0.0.0				1-52	rejeter
UDP2	UDP	192.168.168.11	0.0.0.0				54-87	rejeter
UDP3	UDP	192.168.168.11	0.0.0.0				89-499	rejeter
UDP4	UDP	192.168.168.11	0.0.0.0				501-3073	rejeter
UDP5	UDP	192.168.168.11	0.0.0.0				3077-3543	reieter
UDP7	UDP	192.168.168.11	0.0.0.0				3545-4499	rejeter
UDP8	UDP	192.168.168.11	0.0.0.0				4501-65535	rejeter
DNSc	les deux				192.168.0.0	255.255.0.0		rejeter
GIP	les deux	192.168.168.11	0.0.0.0		108.61.0.0	255.255.0.0		rejeter
GIP2	les deux	192.168.168.11	0.0.0.0		195.122.0.0	255.255.0.0		rejeter
GIP1	les deux	192.168.168.11	0.0.0.0		173.199.0.0	255.255.0.0		rejeter
GIP3	les deux	192.168.168.11	0.0.0.0		104.238.0.0	255.255.0.0		rejeter
GIP4	les deux	192.168.168.11	0.0.0.0		93.93.0.0	255.255.0.0		reieter
GIP5	les deux	192.168.168.11	0.0.0.0		95.141.0.0	255.255.0.0		rejeter
GP6	les deux	192.168.168.11	0.0.0.0		189.1.0.0	255.255.0.0		rejeter
GP7	les deux	192.168.168.11	0.0.0.0		197.80.0.0	255.255.0.0		rejeter
GIP8	les deux	192.168.168.11	0.0.0.0		197.84.0.0	255.255.0.0		rejeter
GIP9	les deux	192.168.168.11	0.0.0.0		196.41.0.0	255.255.0.0		rejeter
GIP10	les deux	192.168.168.11	0.0.0.0		152.111.0.0	255.255.0.0		rejeter
GIP11	les deux	192.168.168.11	0.0.0.0		104.238.0.0	255.255.0.0		rejeter
GP12	les deux	192.168.168.11	0.0.0.0		177.54.0.0	255.255.0.0		rejeter
GIP13	les deux	192.168.168.11	0.0.0.0		4.79.0.0	255.255.0.0		rejeter

Consoles and games need to be updated to connect and authenticate for multiplayer. I tried to change of DNS server IP different times with different locations found on http://public-dns.info/nameserver/fr.html, http://public-dns.info/nameserver/it.html, http://public-dns.info/nameserver/nz.html, http://public-dns.info/nameserver/us.html, http://public-dns.info/nameserver/ca.html, http://public-dns.info/nameserver/ru.html, for playing battlefield 1. Strangely, I noticed the playerbase names were corresponding to the location of the DNS server IP. I met far less cheaters when the DNS server IP locations I was setting are corresponding to Baton Rouge (US), Redwood (US), Coquitlam (Canada), towns of EA public network, found on http://google.com, http://www.tcpiputils.com/browse/ip-address/159.153.229.89, http://bgp.he.net/report/multi-origin-routes. Maybe, well known DNS servers like Norton ConectSafe or OpenDNS are misrouted by hackers. Maybe, routing the connections through satellites is safer using a far distant DNS server or having the

network connections through satellites. Maybe, using a router between your computer and your modem is better. Maybe, changing of DNS server IP often with different locations found on http://public-dns.info/ is a cheap method to not be hacked. Is it the way to adopt?

There is less risk to be forwarded on hacked lobbies when DNS server is on the way of servers you playing. DNS server is more efficient; to control the flow of connections, if less distance there is to browse, between the server and your place. Particularly for a game where the ping is important and having a better connection is required. You can choose to play on 5 different servers place around the world in battlefield 1. The following picture is explaining why there is less distance to browse when DNS server is near servers hosting a match:

The following picture is explaining how a hacker can flood your network to redirect the connection of a match to the connection of a hacked lobby:



After searching Windows firewall and modem firewall restriction, taking account paying a game 70 Euros but it's unplayable every time, forced to reboot fresh my computer and console every day, worried to buy online some sales, finding it's strange to have same

match with same hackers on one IP with different ports and one port with different IP, I contacted my internet provider to enable the flow connection control, I explained one IP is used more than once, and I want connection to servers and not users like me because it's hackers. They replied to restart often my modem to change IP, but wait some minutes in order the IP be used by another user. They replied they asked to support to enable flow connection control. I tried two times to explain this for it. The first time they said I must ask to a specialist. I was very angry because I searched 5 years making this book. But the second time they said they will forward my problem to their experts cell. It seems that the problem with hackers was resolved for me contacting my internet provider. But 3 days after, the game I was playing, Battlefield 1 on Xbox One, became again unplayable. All multiplayer games are infested by cheaters and worst on consoles. Youtube is full of videos full of likes explaining how to cheat and where find cheats. Each year more and more cheaters and cheats. To have access to most of online games on consoles and offline games on PC without changing anything on your modem/router you can set your modem firewall as following:

application / service	protocole	adresse IP source	masque adresse IP	port source	adresse IP destination	masque adresse IP	port destination	action
HTTP	TCP						80	accepter
HTTPS	TCP						443	accepter
POP3	TCP						110	accepter
POP3S	TCP						995	accepter
SMTPAuth	TCP						587	accepter
SMTP	TCP						25	accepter
FTP	TCP						20-21	accepter
DNS	UDP				192.168.1.1	0.0.0.0	53	accepter
IMAP	TCP						143	accepter
FTPS	TCP						22	accepter
IMAPS	TCP						993	accepter
STEAM	TCP	192.168.1.32	0.0.0.0				27000-27050	accepter
TA2	les deux	192.168.1.4	0.0.0.0				7001-26999	accepter
TA3	les deux	192.168.1.4	0.0.0.0				27051-42200	accepter
TA1	les deux	192.168.1.4	0.0.0.0				3000-5999	accepter
NDNS	UDP	192.168.1.4	0.0.0.0		199.85.126.30	0.0.0.0	53	accepter
SDNS	UDP	192.168.1.4	0.0.0.0		192.168.1.1	0.0.0.0	53	rejeter
TD	les deux	192.168.1.4	0.0.0.0		192.168.1.1	255.255.0.0		rejeter

But restriction of traffic over modem firewall for consoles games should remove connection to hacked lobby. I searched to restrict ports for call of duty games but it's always unplayable. Also I searched for battlefield 1 with less ports allowed from what I found earlier with the beta version, ports wrote in a previous chapter. The modem firewalls I have set for battlefield 1 on Xbox One is as following considering to deny ports which are unsafe shown on http://speedguide.net:

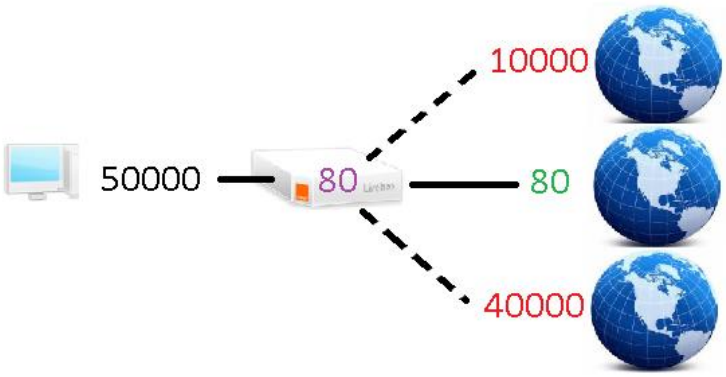
application / service	protocole	adresse IP source	masque adresse IP	port source	adresse IP destination	masque adresse IP	port destination	action
HTTP	TCP						80	accepter
HTTPS	TCP						443	accepter
POP3	TCP						110	accepter
POP3S	TCP						995	accepter
SMTPAuth	TCP						587	accepter
SMTP	TCP						25	accepter
FTP	TCP						20-21	accepter
SSH	TCP						22	accepter
DNS	UDP				192.168.1.1	0.0.0.0	53	accepter
IMAP	TCP						143	accepter
IMAPS	TCP						993	accepter
FTPS	TCP						22	accepter
SDNS	UDP	192.168.1.36	0.0.0.0		192.168.1.1	0.0.0.0	53	rejeter
NDNS	UDP	192.168.1.36	0.0.0.0		199.85.126.30	0.0.0.0	53	accepter
TD	les deux	192.168.1.36	0.0.0.0		192.168.1.1	255.255.0.0	1-65535	rejeter
TB1	les deux	192.168.1.36	0.0.0.0				1-52	rejeter
TB2	les deux	192.168.1.36	0.0.0.0				54-79	rejeter
TB3	les deux	192.168.1.36	0.0.0.0				81-442	rejeter
TB4	les deux	192.168.1.36	0.0.0.0				444-1023	rejeter
10000	les deux	192.168.1.36	0.0.0.0				10001	accepter
10010	les deux	192.168.1.36	0.0.0.0				10003-10004	accepter
10020	les deux	192.168.1.36	0.0.0.0				10006-10007	accepter
10030	les deux	192.168.1.36	0.0.0.0				10009-10011	accepter
10040	les deux	192.168.1.36	0.0.0.0				10014-10026	accepter
10050	les deux	192.168.1.36	0.0.0.0				10028-10066	accepter
10060	les deux	192.168.1.36	0.0.0.0				10068-10069	accepter
10070	les deux	192.168.1.36	0.0.0.0				10081	accepter
10080	les deux	192.168.1.36	0.0.0.0				10083	accepter
10090	les deux	192.168.1.36	0.0.0.0				10088	accepter
10100	les deux	192.168.1.36	0.0.0.0				10090-10098	accepter
42100	TCP	192.168.1.36	0.0.0.0				42100-42200	accepter

It's important to block IP you find very unwanted, like IP of gameservers/clanservers, Level 3 communication and GMBH appearing to be used by hackers and hacks, cheaters and

cheats. To know which IP to block, it's based on experience by playing, looking with ipconfig/displaydns, perfmon, and correlating IP with websites like http://bgp.he.net/report/multi-origin-routes. The following picture show the settings I have add to the modem firewall for blocking unwanted IP but rules allowing take over on blocking rules, so it would ask to allow IP between instead:

GS1	les deux				108.0.0.0	255.0.0.0	1-65535	rejeter
GS2	les deux				195.0.0.0	255.0.0.0	1-65535	rejeter
GS3	les deux				173.0.0.0	255.0.0.0	1-65535	rejeter
GS4	les deux				104.0.0.0	255.0.0.0	1-65535	rejeter
GS5	les deux				93.0.0.0	255.0.0.0	1-65535	rejeter
GS6	les deux				95.0.0.0	255.0.0.0	1-65535	rejeter
GS7	les deux				189.0.0.0	255.0.0.0	1-65535	rejeter
GS8	les deux				197.0.0.0	255.0.0.0	1-65535	rejeter
GS9	les deux				196.0.0.0	255.0.0.0	1-65535	rejeter
GS10	les deux				152.0.0.0	255.0.0.0	1-65535	rejeter
GS11	les deux				104.0.0.0	255.0.0.0	1-65535	rejeter
GS12	les deux				177.0.0.0	255.0.0.0	1-65535	rejeter
GS13	les deux				4.0.0.0	255.0.0.0	1-65535	rejeter
GS14	les deux				208.0.0.0	255.0.0.0	1-65535	rejeter
GS15	les deux				209.0.0.0	255.0.0.0	1-65535	reieter
GS16	les deux				185.0.0.0	255.0.0.0	1-65535	rejeter
GS17	les deux				207.0.0.0	255.0.0.0	1-65535	rejeter
GS18	les deux				162.0.0.0	255.0.0.0	1-65535	rejeter
GS19	les deux				155.0.0.0	255.0.0.0	1-65535	rejeter
GS20	les deux				68.0.0.0	255.0.0.0	1-65535	rejeter
GS21	les deux				8.0.0.0	255.0.0.0	1-65535	rejeter
GS22	les deux				109.0.0.0	255.0.0.0	1-65535	rejeter
GS23	les deux				176.0.0.0	255.0.0.0	1-65535	rejeter
GS24	les deux				64.0.0.0	255.0.0.0	1-65535	rejeter
GS25	les deux				67.0.0.0	255.0.0.0	1-65535	rejeter
GS26	les deux				91.0.0.0	255.0.0.0	1-65535	rejeter
GS27	les deux				113.0.0.0	255.0.0.0	1-65535	rejeter
GS28	les deux				172.0.0.0	255.0.0.0	1-65535	rejeter
GS29	les deux				159.0.0.0	255.0.0.0	1-65535	rejeter
GS30	les deux				168.0.0.0	255.0.0.0	1-65535	rejeter
GS31	les deux				190.0.0.0	255.0.0.0	1-65535	rejeter
GS32	les deux				193.0.0.0	255.0.0.0	1-65535	rejeter
GS33	les deux				194.0.0.0	255.0.0.0	1-65535	rejeter
GS34	les deux				198.0.0.0	255.0.0.0	1-65535	reieter
GS35	les deux				200.0.0.0	255.0.0.0	1-65535	rejeter
GS36	les deux				201.0.0.0	255.0.0.0	1-65535	rejeter
GS37	les deux				204.0.0.0	255.0.0.0	1-65535	rejeter
GS38	les deux				206.0.0.0	255.0.0.0	1-65535	rejeter
GS39	les deux				199.76.0.0	255.255.0.0	1-65535	rejeter
GS40	les deux				199.77.0.0	255.255.0.0	1-65535	reieter
GS41	les deux	192.168.1.36	0.0.0.0		146.0.0.0	255.0.0.0	1-65535	rejeter
GS42	les deux	192.168.1.36	0.0.0.0		192.0.0.0	255.0.0.0	1-65535	rejeter
GS43	les deux				80.0.0.0	255.0.0.0	1-65535	rejeter
GS44	les deux				2.0.0.0	255.0.0.0	1-65535	rejeter
GS45	les deux				5.0.0.0	255.0.0.0	1-65535	rejeter
GS46	les deux				62.0.0.0	255.0.0.0	1-65535	rejeter
GS47	les deux				77.0.0.0	255.0.0.0	1-65535	rejeter
GS48	les deux				78.0.0.0	255.0.0.0	1-65535	rejeter
GS49	les deux				79.0.0.0	255.0.0.0	1-65535	reieter
GS50	les deux				85.0.0.0	255.0.0.0	1-65535	rejeter
GS51	les deux				89.0.0.0	255.0.0.0	1-65535	reieter
GS52	les deux				92.0.0.0	255.0.0.0	1-65535	rejeter
GS53	les deux				94.0.0.0	255.0.0.0	1-65535	rejeter
GS54	les deux				178.0.0.0	255.0.0.0	1-65535	reieter
GS55	les deux				212.0.0.0	255.0.0.0	1-65535	reieter
GS56	les deux				213.0.0.0	255.0.0.0	1-65535	rejeter
GS57	les deux				217.0.0.0	255.0.0.0	1-65535	rejeter

In fact, blocking ports is important even if you don't set allowing ports, because it block unwanted traffic incoming. This following picture is explaining why:



Finally the rules on my modem firewall I have set to play battlefield 1 on Xbox One looks like this:

NDNS	UDP	192.168.1.36	0.0.0.0		199.85.126.30	0.0.0.0	53	accepter
10000	les deux	192.168.1.36	0.0.0.0				10001	accepter
10010	les deux	192.168.1.36	0.0.0.0				10003-10004	accepter
10020	les deux	192.168.1.36	0.0.0.0				10006-10007	accepter
10030	les deux	192.168.1.36	0.0.0.0				10009-10011	accepter
10040	les deux	192.168.1.36	0.0.0.0				10014-10026	accepter
10050	les deux	192.168.1.36	0.0.0.0				10028-10066	accepter
10060	les deux	192.168.1.36	0.0.0.0				10068-10069	accepter
10070	les deux	192.168.1.36	0.0.0.0				10081	accepter
10080	les deux	192.168.1.36	0.0.0.0				10083	accepter
10090	les deux	192.168.1.36	0.0.0.0				10088	accepter
10100	les deux	192.168.1.36	0.0.0.0				10090-10098	accepter
ALLREJECT	les deux	192.168.1.36					1-65535	reieter
42100tcp	TCP	192.168.1.36	0.0.0.0				42100-42200	accepter
80	TCP	192.168.1.36					80	accepter
443	TCP	192.168.1.36					443	accepter

After changing of internal IP, for first connection to EA server on battlefield 1, you need to remove the rule all reject. Here my last firewall settings attempt for battlefield 1:

application / service	protocole	adresse IP source	masque adresse IP	port source	adresse IP destination	masque adresse IP	port destination	action
HTTP	TCP						80	accepter
HTTPS	TCP						443	accepter
POP3	TCP	192.168.1.0	255.255.255.128				110	accepter
POP3S	TCP	192.168.1.0	255.255.255.128				995	accepter
SMTPAuth	TCP	192.168.1.0	255.255.255.128				587	accepter
SMTP	TCP	192.168.1.0	255.255.255.128				25	accepter
FTP	TCP	192.168.1.0	255.255.255.128				20-21	accepter
SSH	TCP	192.168.1.0	255.255.255.128				22	accepter
DNS	UDP						53	accepter
IMAP	TCP	192.168.1.0	255.255.255.128				143	accepter
STEAM	TCP	192.168.1.32	0.0.0.0				27000-27050	accepter
FTPS	TCP	192.168.1.0	255.255.255.128				22	accepter
IMAPS	TCP	192.168.1.0	255.255.255.128				993	accepter
42100tcp	TCP	192.168.1.130	0.0.0.0				42100-42200	accepter
10000	les deux	192.168.1.130	0.0.0.0		255.255.255.0	128.0.0.0	10001-10098	accepter
ALLREJECT	les deux	192.168.1.130	0.0.0.0				1-65535	rejeter

In abstract for securing to higher degree your network, considering you will enjoy playing battlefield 1 on Xbox One, you only need to open ports for each internal IP of your computers, ports TCP/UDP: 1-1023 (iana) and ports TCP: 27000-27050 (Steam), and for each consoles internal IP, ports TCP/UDP: 10001-10098, with distant IP 255.255.255.254 and mask 128.0.0.0, ports TCP: 443, with distant IP 127.255.255.255 and masks 255.128.0.0 and 128.0.0.0, and 80, 443, 42100-42200, with distant IP 255.255.255.254 and mask 128.0.0.0, ports UDP: 53, with distant IP 80.10.246.5 and 81.253.149.13 (Orange DNS) and mask 0.0.0.0, but I advice more the DNS server of Norton named ConnectSafe (IP: 199.85.126.30, 199.85.127.30) or the DNS server OpenDNS (208.67.222.222, 208.67.220.220). Also you need to refuse ports and IP for each consoles internal IP, ports TCP/UDP: 1-65535, port TCP:

443, with distant IP 128.0.0.0 and mask 128.0.0.0, ports TCP/UDP: 1-65535, with distant IP 255.255.255.254 and mask 0.0.0.0. The following picture explains the configuration of modem firewall to play battlefield 1 and to isolate computers without setting a DMZ:

adresse IP statique								
application / service	protocole	adresse IP source	masque adresse IP	port source	adresse IP destination	masque adresse IP	port destination	action
80	TCP	192.168.1.130	0.0.0.0		255.255.255.254	128.0.0.0	80	accepter
443	TCP	192.168.1.130	0.0.0.0		255.255.255.254	128.0.0.0	443	accepter
10000	les deux	192.168.1.130	0.0.0.0		255.255.255.254	128.0.0.0	10001-10098	accepter
42100	TCP	192.168.1.130	0.0.0.0		255.255.255.254	128.0.0.0	42100-42200	accepter
HTTPS128	TCP	192.168.1.130	0.0.0.0		128.0.0.0	128.0.0.0	443	rejeter
HTTPS127	TCP	192.168.1.130	0.0.0.0		127.255.255.255	128.0.0.0	443	accepter
ALL255	les deux	192.168.1.130	0.0.0.0		255.255.255.254	0.0.0.0	1-65535	rejeter
DNSA	UDP	192.168.1.130	0.0.0.0		199.85.127.30	0.0.0.0	53	accepter
DNS	UDP	192.168.1.130	0.0.0.0		208.67.220.220	0.0.0.0	53	accepter
PC4DNS	UDP	192.168.1.14	0.0.0.0		192.168.1.1	0.0.0.0	53	accepter
PC41	TCP	192.168.1.14	0.0.0.0		1.0.0.0	128.0.0.0	1-1023	accepter
PC463	TCP	192.168.1.14	0.0.0.0		63.0.0.0	128.0.0.0	1-1023	accepter
PC4193	TCP	192.168.1.14	0.0.0.0		193.0.0.0	128.0.0.0	1-1023	accepter

You can pick a DNS server IP of OpenDNS for primary DNS and of Norton for secondary DNS for mixing security in network settings for DNS server on your consoles. Sometimes it's hard to be connected to EA authentication service, to resolve this issue, close and restart battlefield 1 with ports 80, 443 in TCP all open. Also to update games or download games you need to allow ports TCP: 80, 443 and remove the rules refusing ports and IP. It's not necessary to allow IP of your modem with port 53 in UDP in your modem firewall, when you set as DNS server the default server DNS or the DNS server is set automatically (corresponding to your modem) on your router, computers and consoles. For basic connection with web applications like Chrome, Internet Explorer, outlook, Skype... you just need to allow ports 1-1023 in TCP with distant IP 1.0.0.0, 63.0.0.0, 193.0.0.0 and masks 128.0.0.0 on your modem firewall.

Check if EA services don't encounter issue on their own with the websites http://touteslespannes.fr/statut/ea, or http://downdetector.com/status/ea. You can set a bunch of first internal IP of computers connected or which would be connected allowing iana ports,

and choose internal IP of your consoles with a high end IP number to allow specific ports. Set manually internal IP, modem IP, DNS servers IP of connection in network options of your consoles and computers where you play games. Other computers take automatically first internal IP available to connect to your modem. Sometimes newest computers connected can take same internal IP of your consoles or computers, so it's important to set manually internal IP of your favourite consoles and computers to have connection. To set properly a router behind your modem, you need to set to default modem firewall and Windows firewall of the computer you will use for installation of the router and set to automatic the configuration of network connection for your consoles and computers. Use the router as an access point like it's recommended by Netgear routers. These kinds of routers allow DMZ for secure gaming by isolating devices you connect through it and allow parental control like with OpenDNS, but also to have better connectivity. You can disable SSID diffusion in order to disable Wi-Fi connection for better security. Your modem will task as usual. You just need to enable again static IP settings on your modem under DHCP, for your devices connected a new time to the modem but through the router. Set a static internal IP, modem IP, DNS servers IP like IP of Norton ConnectSafe and OpenDNS, for the router configuration. You can proceed with modem firewall for each computers and consoles like explained in the section above. It doesn't need to allow ports and IP for the router internal IP on your modem firewall, but maybe, you need to disable refusing rules for ports TCP/UDP: 1-65535 and for port TCP: 443, with distant IP 128.0.0.0 and mask 128.0.0.0. These both refusing rules can be replaced by two refusing rules: ports 1-52, 54-65535 in TCP/UDP (if you block port 53 in TCP on your modem firewall, you will lose connection after restarting your modem). Create allowing rules for ports TCP: 80, 443 all open for very first authentication of EA servers for battlefield 1 on Xbox One (like when you change of internal IP), and then you can disable these rules. Check if you are connected to Xbox live before. With the Netgear routers you can set security

features like anti-ddos, proxy, blocking websites by keywords... When you use it as a router instead of access point tasking as a simple antenna. When you choose to set the router like a router, it's like you have another modem behind your modem connected to internet. For setting properly the router to task as a server DHCP follow these instructions. Set to default modem and Windows firewall. Enable automatic configuration of network settings on your computers and consoles. Set a static IP for your router under your router settings. Then set modem firewall with internal local IP, the IP of your router shown under the page of configuration of your modem or the IP of your router you have set as static under the page of configuration of your router. The distant ports and IP are the same as explained in the section above but for distant port UDP: 53, the distant IP corresponds to the DHCP server of your router shown in network settings of your computers and consoles, or to the IP of the DNS nameservers you can set under your router settings for more security (like with OpenDNS: 208.67.222.222, 208.67.220.220). Follow these instructions for setting OpenDNS under the opendns.com internet dashboard: enable all security features, set custom blocking filtering websites categories by checking all categories and apply changes, and then add domain names as following:

- ALWAYS BLOCK: AMAZONAWS.COM, bandiwdth.co.uk, bandiwdth.com, choopa.net, core-backbone.com, eudedicated.com, fragnet.net, gtt.net, i3d.net, link11.de, mcbone.net, mpgh.com, myloc.de, nl-ix.net, ntt.net, ociris.com, optinet.net Pnap.net, rudedicated.com, tele2.de, telia.net, unitymedia.de, usdedicated.com, versatel.de, your-server.de.
- NEVER BLOCK: opendns.com, vrsn.net.

After restarting your modem, the external IP of your network will change, so it needs to enable again settings on OpenDNS for your network. In conjunction with DNS nameservers you can set under configuration of your router, you can set another DNS nameservers under

the network configuration of your computers and consoles like DNS nameservers of Verisign (64.6.64.6, 64.6.65.6). Don't forget to allow distant IP of DNS nameservers under modem firewall with the local internal IP of your router. On www.alexa.com/ and http://www.trafficestimate.com/ you can find keywords for knowing which words to add for blocking websites by keywords under your router security settings, like: x22, mpgh, bf1cheats, unknowncheats, elitepvpers, iwantcheats, se7ensins, leakforums, cheat, hack, cheating, hacking, aimbot, wallhack, autoshoot, godmod, ddos, lagswitch, hacks, cheats, servers, lobby, server, lobbies, LiteSpeed, megaupload, urlmegaupload, maga, gameservers, clanservers, gameserver, clanserver, de, me, net, com, itz, yolo, elite, faze, tnt, millenium, stg, mrlev12, torr, noob, noobs, file, files, free, demonware, DICE, electronicarts, ea, xbox, server, dedicated, official, battlefield, battlefield1, www, http, https, 255.255.255.254, 192.168.1.1, 192.168.1.255, ?, ... (with NETGEAR WNR2000v5, the ? corresponds to all websites). Also you can add domain names: 1und1.de, akamai.com, akamaitechnologies.com, amazon.com, AMAZONAWS.COM, choopa.com, choopa.net, clanservers.com, congstar.de, constant.com, dsl.1und1.de, dsl.o2online.de, gameservers.com, hetzner.de, level3.net, mpgh.com, o2online.de, orange.com, tele2.de, telekom.de, telko.check24.de, unitymedia.de, versatel.de, vodafone.de, bandiwdth.co.uk, bandiwdth.com, core-backbone.com, eudedicated.com, fragnet.net, gtt.net, i3d.net, link11.de, mcbone.net, myloc.de, nl-ix.net, ntt.net, ociris.com, optinet.net, Pnap.net, rudedicated.com, telia.net, usdedicated.com, your-server.de. And also you can add all generic domains: aero, arpa, asia, biz, cat, com, coop, edu, eu, gov, gouv, info, int, jobs, mil, mobi, museum, name, net, org, post, pro, tel, travel, xxx, ac, ad, ae, af, ag, ai, al, am, an, ao, aq, ar, as, at, au, aw, ax, az, ba, bb, bd, be, bf, bg, bh, bi, bj, bm, bn, bo, br, bs, bt, bv, bw, by, bz, ca, cc, cd, cf, cg, ch, ci, ck, cl, cm, cn, co, cr, cs, cu, cx, cy, cz, dd, de, dj, dk, dm, do, dz, ec, ee, eg, eh, er, es, et, fi, fj, fk, fm, fo, fr, ga, gb, gd, ge, gf, gg, gh, gi, gl, gm, gn, gp, gq, gr, gs, gt, gu, gw, gy, hk, hm, hn, hr, ht, hu, id, ie, il, im, in, io, iq, ir, is, it, je, jm, jo,

jp, ke, kg, kh, ki, km, kn, kp, kr, kw, ky, kz, la, lb, lc, li, lk, lr, ls, lt, lu, lv, ly, ma, mc, md, me, mg, mh, mk, ml, mm, mn, mo, mp, mq, mr, ms, mt, mu, mv, mw, mx, my, mz, na, nc, ne, nf, ng, ni, nl, no, np, nr, nu, nz, om, pa, pe, pf, pg, ph, pk, pl, pm, pn, pr, ps, pt, pw, py, qa, re, ro, rs, ru, rw, sa, sb, sc, sd, se, sg, sh, si, sj, sk, sl, sm, sn, so, sr, st, su, sv, sy, sz, tc, td, tf, tg, th, tj, tk, tl, tm, tn, to, tp, tr, tt, tv, tw, tz, ua, ug, uk, um, us, uy, uz, va, vc, ve, vg, vi, vn, vu, wf, ws, ye, yt, yu, za, zm, zr, zw. Check with traceroute websites like http://ping.eu/traceroute/, your external IP, and other IP like 255.255.255.254, 8.8.4.4, 8.8.8.8, 199.85.126.10, and IP of game servers found with gametracker websites, to block domain names (like hetzner.de, your-server.de, level3.net) found routing the destinations, under OpenDNS and router firewall. Under your router firewall, block ports TCP: 1-79, 81-442, 444-10000, 10099-42099, and 42201-65535, and ports UDP: 1-52, 54-10000 and 10099-65535. Make enough attempts to connect to EA servers, but normally it run under 8 attempts without router and under 4 with router. Enable QoS (Quality of Service) for better authentication under your router settings. It's better to disable Wi-Fi and use Ethernet connection. Enable RIP (Routing Information Protocol) under DHCP tab of your router, for having direct connection to servers with less distance instead of higher internet speed to servers with more distance. Also it's a good way for secure your computers and consoles against attacks, to set the IP of an auxiliary DNS server for your DHCP server of your router. The mask for the IP you choose can be found when you set manually your computer internal IP under properties of TCP/IPv4 in Ethernet properties. You can set IP of DHCP server of your router to an IP of a DNS server and internal IP of your computers and consoles to an IP of the same DNS server like it's possible with DNS server of ConnectSafe by Norton (199.85.126.10-20-30, 199.85.127.10-20-30). But when you assign internal IP of your computers and consoles to an IP of a DNS server, you can't use this IP as DNS server furthermore. It's possible, for increase security, to disable ports 42100-42200 in TCP and 10001-10098 in TCP/UDP, just after authentication and for

searching a server. Then, when entering a server, enable ports 10001-10098 in UDP, and then disable it when you entered a server. All your game session will be secure and you can play different matches awhile the same server. When only ports 53 and 443 are enabled for searching a server, you can add servers to the list of your favourite's servers. Take care to information on the server like the user owner because he can rents a server to not be banned and his friends. Apparently, server owner renting a server shall himself ban cheaters or choose to enable or not automatic ban of cheaters. Prefer a server when there isn't any owner. Disable on your router the security feature blocking websites by keywords, and enable ports 80 and 443 in TCP with all distant IP on your modem firewall, when you want to download games on your Xbox One and update your Xbox One. Disable automatic update of Xbox One and games, otherwise it bugs. In abstract, for playing battlefield 1 on Xbox One, you need only 4 rules on your modem firewall: distant ports 443, 42100-42200 in TCP, ports 10000-10060 in UDP/TCP, with distant IP 255.255.255.254 and masks 128.0.0.0, and port 443 in TCP with distant IP 0.0.0.1 and mask 128.0.0.0. When browsing server list to add server to favourites, disable the second and third rules, and when you are playing on a server, disable the three last rules. The ports for connecting to quick match are 17490-17510 in TCP/UDP with distant IP 255.255.255.254 and mask 128.0.0.0. On your modem you can allow ports 1-1023 in TCP and other ports for battlefield 1, and on your router you can block websites by keywords and block services as ports in TCP: 1-442, 444-9999, 10061-17489, 17511-42099, 42201-65535, in UDP: 1-52, 54-9999, 10061-17489, 17511-65535. Use router firewall blocking ports outside ports for battlefield 1 associated with modem firewall with a rule for all ports in TCP/UDP with second part of IP (255.255.255.254 and mask 128.0.0.0), to disable when entered server, letting only port 443 in TCP. Values of memory addresses through port 443 in TCP are encrypted. When browsing server list, you can use the filter option name of server by typing [dice] or official. Some servers are privates and unranked like with UDP ports 10060-

10070. If it doesn't want to authenticate, it's more due to the modem and router firewall blocking ports 80 in TCP. You need restarting the game sometimes. As someone says on this forum: http://battlelog.battlefield.com/bf4/forum/threadview/2955065218227920951/, it's better to join with quick match as following: 2013-11-06 00:34, by BigShottt: “I run an official server for BF4. Official marked servers are severely capped in what settings they can change...mostly the settings stay at what DICE set the defaults to be so it's played as Dice intended. Also Official servers are the only servers that "Play Now" will connect you to. Ranked marked servers have a lot more options that are allowed to be changed and they are NOT used for "Play Now" connections. Unranked servers can pretty much do whatever they want...and can even unlock all weapons & attachments for all players, but while playing on these types of servers you will not earn points and will not rank up or unlock any of your own weapons.” Choose quick match from multiplayer screen. It's written official on the screen it search a match. Matches under server browser aren't official ones. For playing Starwars Battlefront on Xbox One, you can allow port 443 in TCP and ports 1-65535 in TCP/UDP with distant IP 255.255.255.254 and mask 128.0.0.0. You can open these ports for all internal IP without setting a static IP for your console, and you can open ports 1-1023 in TCP for each internal IP of your computers with setting static IP for your computers. Also, create refusing rules for ports 1-52 and 54-65535 in TCP/UDP (disable/enable both rules after restarting your modem if you encounter connection problems). Remove the two refusing rules for having allowing rules created after to take effect, then add it again. Opening a NAT/PAT rule for port 3074 or other ports for Xbox One don't task as on PC, where it allow to find servers for Call of Duty games without allowing other ports in modem firewall. It can be better to not use a router behind your modem and to not use a public DNS server, and to only use your modem with the firewall well set because you can trust only your internet provider. Do not apply automatic updates of games and console because you can play without a rule for port 80 in

TCP, but it need it to update. But you need port 80 in TCP with distant IP 255.255.255.254 and mask 128.0.0.0 for block and report cheaters on Xbox One. In fact, the mask 128.0.0.0 in the modem firewall rules implies for IP under 127.255.255.255, it corresponds to the IP scale 0.0.0.1 to 127.255.255.255 and for IP above 128.0.0.0, it corresponds to the IP scale 128.0.0.1 to 223.255.255.255. So, to not have possible UDP traffic coalescent with TCP traffic, you can do as following to set modem firewall. Create a rule for port 443 in TCP, create rules for ports 1-65535 in UDP and for ports 17490-17510 in TCP/UDP with distant IP 127.255.255.255 and mask 128.0.0.0, create a rule for ports 1-65535 in TCP with distant IP 255.255.255.254 and mask 128.0.0.0. But you can't join a match from server browser; however you can join a match from quick match. To join a match from server browser or quick match, set modem firewall as following. Create a rule for port 443 in TCP, create rules for ports 17490-17510 in UDP/TCP and for ports 10000-10100 in UDP with distant IP 127.255.255.255 and mask 128.0.0.0, create rules for ports 10020-10100 in UDP and for ports 10000-10019 in TCP and for ports 42100-42200 in TCP with distant IP 255.255.255.254 and mask 128.0.0.0. To play on American servers, reverse the TCP and UDP rules for ports 10000-10019 and 10020-10100 to UDP and TCP. But maybe, a router behind your modem is better to secure your gaming experience, because you can add to your router the security blocking websites by keywords, with your external IP and address (found on what's my IP websites and your DNS found with websites https://db-ip.com/all or https://ru.myip.ms/view/ip_addresses or http://bgp.he.net/ searching your external IP, for me it's abo.wanadoo.fr), your router internal IP, your console internal IP. Allow only second part of IP with mask 128.0.0.0 on your modem firewall for battlefield ports. If cheaters take the same external IP of you, you will not be allowed to connect to them, and then you will not be connected to their hacked servers available worldwide if they put their servers in DynDNS for example. Port 443 in TCP and all other ports will be secure in this case, if you have your external IP and address, your router

internal IP, your console internal IP, in the first part of IP. You can search which scale of IP what battlefield 1 needs for connection to a server like with ports. To know which scale of IP with mask 255.0.0.0 you need to have in modem firewall to connect to a server, you have to restart your game each time you test the IP. Check your ping on scoreboard of the match when playing. In conclusion, on your router disable the feature blocking websites by keywords, enable blocking services with ports in TCP: 1-442, 444-9999, 10061-17489, 17511-42099, 42201-65535, in UDP: 1-52, 54-9999, 10061-17489, 17511-65535, and on your modem allow port 443 in TCP with all distant IP (add port 80 in TCP with all distant IP if you encounter too much problems for connection), port 80 in TCP with distant IP 159.153.128.0 and mask 255.255.128.0, ports 10000-10100, 42100-42200 in TCP with distant IP 159.153.0.0 and mask 255.255.0.0, ports 10000-10100 in TCP with distant IP 134.213.128.0 and mask 255.255.128.0, ports 10000-10100 in UDP, 17490-17510 in UDP/TCP with distant IP 159.153.0.0 and mask 255.255.128.0. You can find IP by incrementing IP with masks 128.0.0.0, 255.0.0.0, 255.128.0.0 and 255.255.0.0 and with websites like http://bgp.he.net/report/multi-origin-routes and http://google.com using search tools for words Electronic Arts, Microsoft Corporation, Xbox, myip, IP start number... Because all IP aren't own by Electronic Arts as shown by the website https://bgpview.io/, for more security, instead of rules for ports 80 in TCP, 10000-10100 in TCP, 42100-42200 in TCP, 10000-10100 in UDP and 17490-17510 in TCP/UDP with distant IP 159.153.128.0 and 159.153.0.0, add rules with the following distant IP with mask 255.255.255.0 for ports 1-65535 in TCP/UDP: 159.153.40.0/23, 159.153.40.0/21, 159.153.42.0/24, 159.153.64.0/22, 159.153.92.0/22, 159.153.108.0/24, 159.153.112.0/21, 159.153.119.0/24, 159.153.152.0/22, 159.153.227.0/24, 159.153.234.0/24, 159.153.235.0/24, 159.153.238.0/24, 159.153.240.0/24, 159.153.242.0/24, 159.153.244.0/24 (with mask /20 -> 16 ranges, mask /21 -> 8 ranges, mask /22 -> 4 ranges, mask /23 -> 2 ranges, mask /24 -> 1 range). Also you can replace the distant

IP 134.213.128.0 and mask 255.255.128.0 for ports 10000-10100 in TCP by distant IP 134.213.244.128 and mask 255.255.255.128 (or /24 -> 1 range). Information on the IP can be found with the website http://ipindex.dihe.de/. Within IP for ports 1-65535 in TCP/UDP, the IP to keep shown by http://ping.eu/traceroute/ are (akamaitechnologies.com hosting official website and authentication) 159.153.42.0/24, 159.153.108.0/24, 159.153.227.0/24, 159.153.234.0/24, 159.153.235.0/24, 159.153.238.0/24, 159.153.240.0/24, 159.153.242.0/24, 159.153.244.0/24, (zayo.com hosting official servers) 159.153.43.0/24, 159.153.44.0/24, 159.153.45.0/24, 159.153.46.0/24, 159.153.47.0/24, 159.153.64.0/24, 159.153.65.0/24, 159.153.66.0/24, 159.153.67.0/24, 159.153.92.0/24, 159.153.93.0/24, 159.153.94.0/24, 159.153.95.0/24, 159.153.112.0/24, 159.153.113.0/24, 159.153.114.0/24, 159.153.115.0/24, 159.153.116.0/24, 159.153.117.0/24, 159.153.118.0/24, 159.153.152.0/24, 159.153.153.0/24, 159.153.154.0/24, 159.153.155.0/24. In definitive, for connections to quick match in battlefield 1 on Xbox One you need the following rules in your modem firewall: for ports 80 and 443 in TCP all distant IP, for ports 1-65535 in UDP distant IP 159.153.42.0 with mask 255.255.255.128, for ports 1-65535 in UDP distant IP 159.153.114.0 and 159.153.115.0 with mask 255.255.255.0, for ports 1-65535 in TCP distant IP 134.213.244.128 and 159.153.244.128 and 159.153.42.0 with mask 255.255.255.128. The IP 159.153.42.73 is used by hackers, even lot of IP above 159.153.42.67 because it's detected by Newb as a modem behind but for quick match it need IP from 159.153.42.0 to 159.153.42.83. The problem can be solve by disable rule for ports 1-65535 in UDP distant IP 159.153.42.0 with mask 255.255.255.128 before entering quick match. Otherwise enable this rule for ports 17490-17510. Also set ports 10000-10100 in UDP for distant IP 159.153.114.0 and 159.153.115.0 with mask 255.255.255.0. Consequently you need to open in your modem firewall for local IP of your console or your computer host if you share the connection, ports 80 and 443 in TCP with all distant IP, ports 10000-42200 in TCP with distant IP 159.153.244.128 and

134.213.244.128 with masks 255.255.255.128, ports 10000-10100 in UDP with distant IP 159.153.115.0 with mask 255.255.255.0, ports 17490-17510 in TCP/UDP with distant IP 159.153.42.0 with mask 255.255.255.128. In order to be able to report cheaters, you need to load the recent players tab under main menu of Xbox, once to do when you started it. Sometimes you can't access quick match, for access it, you need to set to default modem firewall or open all ports in TCP/UDP with second part of IP and to disable router firewall. Access once quick match, then enable again modem and router firewalls. Accessing quick match forwarded me on Asian servers with a higher ping and no one in the server, every time. I know it was Asian servers because when I restored to default server browser filter, Asian country location was checked every time. To resolve this issue I restored my Xbox to US language and country; I deleted my historic on my Google account linked with my e-mail from Microsoft account. Then I restored my Xbox to my country language and place. Also I changed settings on my Xbox as following: In my account parameters, from application confidentiality, I disabled all features but not for e-mail application access. Take time to report all cheaters when you are forwarded in a hacked lobby to show you aren't forwarded on official servers. If you are sure, you've been forwarded on a hacked lobby, report everyone with a positive ratio. All reports are reviewed by Microsoft; they received only 1000 reports per day because people don't know a developer console owned by hackers is like a PC for them. If you follow all these network instructions, normally you can play without encounter too much cheater in battlefield 1 on Xbox One. For set security streaming with Mixer on Xbox One, on your modem firewall, allow ports 8000-8999 in TCP/UDP with distant IP 169.50.0.0 and mask 255.255.128.0. Netflix requires local ports 49152-65535, for distant port 443 in TCP and distant port 80 in TCP for IP 34.192.0.0 to 34.255.0.0 with masks 255.255.0.0. This range of IP is found by opening netflix website under a PC internet navigator and looking TCP connexion with perfmon.exe under network tab, and also the

website https://bgpview.io/. Like all Electronic Arts Games, battlefield 1 or star wars battlefront or fifa 15 or garden warfare 2 or titanfall 2 or need for speed, on Xbox One, for playing on official servers, you can create on your modem firewall, allowing rules for ports 1-65535 in TCP all distant IP and for ports 1-65535 in UDP distant IP 159.153.0.0 with mask 255.255.0.0. Like for battlefield 1, in starwars battlefront or titanfall 2 or garden warfare 2 or need for speed or fifa 15, you can play only with port 443 in TCP after finding a match. Concerning titanfall 2 on XBox One, the ports are only 1-1023 in TCP (protected iana ports) and 37000-39999 in UDP. It's possible to play a match with only port 443 in TCP, but after each match these ports must be enable because the game forward you automatically on another match. It's a server side matchmaking and not a p2p one. It's possible to find the range of IP in UDP for the servers. To do it, you must start by knowing if it's the first or second part of IP range with IP 0.0.0.1 or 128.0.0.1 and mask 128.0.0.0. And then setting different IP like 128.0.0.0, 129.0.0.0, ... with mask 255.0.0.0, etc... The IP don't correspond to IP found with perfmon in titanfall on PC. Also I searched IP but lot of IP scales are necessary. Although, it's possible to play with only port 443 in TCP if you entered once a match and if you choose only one matchmaking or the same like for battlefield 1. For playing PUBG ports required are 80 and 443 in TCP, and ports 5000-21000 in TCP/UDP for distant IP 34.128.0.0 and 19.128.0.0 with masks 255.128.0.0 for both IP. It allows connecting under European servers. I searched to restrict ports and IP but it doesn't allow connection. Playing Fortnite requires ports 443 in TCP, and 5222-9222 in UDP for IP 14.0.0.0 to 34.0.0.0 with masks 255.0.0.0. The distant IP for PUBG and Fortnite corresponds to Azure cloud services and servers of Microsoft. Destiny 1 and 2 use only ports 80, 443, 3074, 7500-7509, 30000-30009 in TCP and 3074 in UDP. Darwin project normally should require ports 80 and 443 in TCP and ports 5000-21000 in TCP/UDP with distant IP between 14.0.0.0 and 34.0.0.0 with masks 255.0.0.0. But it's not the case even if it's write Xbox live servers under its store page. For PUBG and Fortnite, you can

set local IP corresponding to internal IP of your console with mask 255.255.255.255 and local port 49152-65535. Normally games edited by Microsoft use Azure servers, like games edited by Electronic Arts use their own servers. IP are corresponding. For playing Fortnite, it requires to allow visibility and download of user creation, under settings of Xbox One, in game content, in online privacy and safety, in Xbox Live privacy. Vigor needs port 443 in TCP and ports 5001-49151 in TCP/UDP with local ports 49152-65535. For display true names of battlefield 1 servers, under server browser, this setting is required. The games of EA battlefield V and battlefield hardline use almost same IP and ports as battlefield 1. See chapters 7.20 and 7.26 for more details. It's easy to find IP and ports, even if you don't have a router showing network activity. This chapter explained how to achieve this. For enable connection to north American servers and quick match, battlefield V needs to allow local IP your internal IP with mask 255.255.255.255, local ports 49152-65535, distant IP 9.0.0.0 with mask 224.0.0.0, distant ports 25200-25300 in UDP (see chapter 7.28 for the mask) and distant IP 9.0.0.0 to 22.0.0.0 with masks 255.0.0.0 and your external IP with mask 255.255.255.255, distant ports 1024-49151 in TCP/UDP. You can find you external IP and internet provider IP range on the website https://bgp.he.net/, check and change it on your modem firewall, each time you want to play and your modem restarted. For the game apex legends the following modem firewall rules allow connection to servers (similar to battlefield V and battlefield 1):

Application/Service	Protocole	Adresse IP source	Masque sous réseau	Port source	Adresse IP destination	Masque sous réseau	Port destination	Action
ea1	Les deux	192.168.1.209	255.255.255.255	49152-65535	159.153.0.0	255.255.0.0	1024-49151	accepter
EA2	TCP	192.168.1.209	255.255.255.255	49152-65535	134.213.244.0	255.255.255.0	1024-49151	accepter
Ea3	UDP	192.168.1.209	255.255.255.255	49152-65535	9.0.0.0	192.0.0.0	1024-49151	accepter

With the following modem firewall rules securing your consoles, it's possible to play securely a lot of games without changing these rules when you change of games you playing because UDP and TCP traffics aren't coalescent, only for few IP own by official game developers.

Application/Service	Protocole	Adresse IP source	Masque sous réseau	Port source	Adresse IP destination	Masque sous réseau	Port destination	Action
bf1	Les deux	192.168.1.209	255.255.255.255	49152-65535	159.153.0.0	255.255.0.0	1024-49151	accepter
bf2	TCP	192.168.1.209	255.255.255.255	49152-65535	134.213.244.0	255.255.255.0	1024-49151	accepter
codbf	UDP	192.168.1.209	255.255.255.255	1024-65535	151.0.0.0	248.0.0.0	1024-49151	accepter
cod2	Les deux	192.168.1.209	255.255.255.255	1024-65535	185.34.0.0	255.255.0.0	3074-3076	accepter
cod1	Les deux	192.168.1.209	255.255.255.255	1024-65535	209.170.0.0	255.255.0.0	3074-3076	accepter
codbf0	UDP	192.168.1.209	255.255.255.255	1024-65535	128.0.0.0	252.0.0.0	1024-49151	accepter
codbf1	UDP	192.168.1.209	255.255.255.255	1024-65535	132.0.0.0	254.0.0.0	1024-49151	accepter
codbf2	UDP	192.168.1.209	255.255.255.255	1024-65535	135.0.0.0	240.0.0.0	1024-49151	accepter
codbf6	UDP	192.168.1.209	255.255.255.255	1024-65535	186.0.0.0	240.0.0.0	1024-49151	accepter
codbf3	UDP	192.168.1.209	255.255.255.255	1024-65535	160.0.0.0	240.0.0.0	1024-49151	accepter
fortnite	UDP	192.168.1.209	255.255.255.255	1024-65535	0.0.0.1	128.0.0.0	1024-49151	accepter
codbf4	UDP	192.168.1.209	255.255.255.255	1024-65535	202.0.0.0	252.0.0.0	1024-49151	accepter
codbf5	UDP	192.168.1.209	255.255.255.255	1024-65535	205.0.0.0	252.0.0.0	1024-49151	accepter
codbf7	UDP	192.168.1.209	255.255.255.255	1024-65535	210.0.0.0	248.0.0.0	1024-49151	accepter
codbf8	UDP	192.168.1.209	255.255.255.255	1024-65535	215.0.0.0	248.0.0.0	1024-49151	accepter

Black ops 3 and black ops 4 on Xbox One seem to be fairer when setting on your modem firewall these following rules (IP for port 53 in UDP corresponds to IP of Norton DNS server to set under Xbox One network settings) and a nat/pat rule associated with the static IP of your console (it allows to be the host of a match but not be forwarded on hacked lobbies open by gameservers/clanservers fill by cheaters unbannable).

Application/Service	Protocole	Adresse IP source	Masque sous réseau	Port source	Adresse IP destination	Masque sous réseau	Port destination	Action
cod3	UDP	192.168.1.209	255.255.255.255	49152-65535	199.85.127.30	255.255.255.255	53	accepter
cod4	TCP	192.168.1.209	255.255.255.255	49152-65535			443	accepter
cod5	TCP	192.168.1.209	255.255.255.255	49152-65535			80	accepter
all1	UDP	192.168.1.0	255.255.255.128	1024-65535			53	accepter
all2	TCP	192.168.1.0	255.255.255.128	1024-65535			1-1023	accepter
cod1	UDP	192.168.1.209	255.255.255.255	49152-65535			3075	accepter
cod2	Les deux	192.168.1.209	255.255.255.255	49152-65535			3074	accepter
cod6	UDP	192.168.1.209	255.255.255.255	3075			3075	accepter

Application/Service	Port interne	Port externe	Protocole	Équipement
cod2	3075	3075	UDP	PC-7

The following modem firewall rules allow having connection for outlook on one PC, and for fortnite on one console from a computer host (both DNS IP correspond to IP set under a computer host ipv4 properties and under console network settings if you share connection, see chapters 7.17 and 7.31).

Application/Service	Protocole	Adresse IP source	Masque sous réseau	Port source	Adresse IP destination	Masque sous réseau	Port destination
p1	TCP	192.168.1.10	255.255.255.255	49152-65535			80
p2	TCP	192.168.1.10	255.255.255.255	49152-65535			443
p3	TCP	192.168.1.10	255.255.255.255	49152-65535			110
p4	TCP	192.168.1.10	255.255.255.255	49152-65535			995
p5	TCP	192.168.1.10	255.255.255.255	49152-65535			20-22
p6	UDP	192.168.1.10	255.255.255.255	49152-65535	64.6.64.6	255.255.255.255	53
p7	TCP	192.168.1.10	255.255.255.255	49152-65535			587
p8	TCP	192.168.1.10	255.255.255.255	49152-65535			25
x1	UDP	192.168.1.23	255.255.255.255	49152-65535	64.6.64.6	255.255.255.255	53
x2	TCP	192.168.1.23	255.255.255.255	49152-65535			80
x3	TCP	192.168.1.23	255.255.255.255	49152-65535			443
x5	UDP	192.168.1.23	255.255.255.255	49152-65535	8.26.56.10	255.255.255.255	53
x4	UDP	192.168.1.23	255.255.255.255	49152-65535	16.0.0.0	240.0.0.0	5001-49151

Playing Modern Warfare 2019 requires larger ranges of IP and ports than Black Ops IV. It needs local ports 49152-65535 with distant ports 80 and 443 in TCP, local ports 49152-65535 with distant IP 209.170.124.0 with mask 255.255.255.0 and distant port 3074 in TCP/UDP, local ports 1024-65535 with distant IP 185.34.105.0 with mask 255.255.248.0 and distant ports 3074-3076 in TCP/UDP, local ports 1024-65535 with distant IP 24.105.0.0 with mask 255.255.192.0 and distant ports 1024-49151 in TCP/UDP.

7.7. EA server problems

If you want to play Electronic Arts games, you can find useful the report of traceroute on http://ping.eu/traceroute/ for all IP normally own by Electronic Arts to find IP of servers. Here the following report:

159.153.0.0 (as6453.net) secure, 159.153.1.0 (as6453.net) modem, 159.153.2.0 (as6453.net) secure, 159.153.3.0 (as6453.net) modem, 159.153.4.0 (as6453.net) modem, 159.153.5.0 (as6453.net) modem, 159.153.6.0 (as6453.net) modem, 159.153.7.0 (as6453.net) secure, 159.153.8.0 (as6453.net) secure, 159.153.9.0 (as6453.net) modem, 159.153.10.0 (as6453.net) secure, 159.153.11.0 (as6453.net) secure, 159.153.12.0 (as6453.net) secure, 159.153.13.0 (as6453.net) secure, 159.153.14.0 (as6453.net) secure, 159.153.15.0 (as6453.net) secure, 159.153.16.0 (zayo.com) modem, 159.153.17.0 (zayo.com) secure, 159.153.18.0 (zayo.com) secure, 159.153.19.0 (zayo.com) modem, 159.153.20.0 (zayo.com) modem, 159.153.21.0 (zayo.com) modem, 159.153.22.0 (zayo.com) modem, 159.153.23.0 (zayo.com) modem, 159.153.24.0 (zayo.com) secure, 159.153.25.0 (zayo.com) modem, 159.153.26.0 (zayo.com) modem, 159.153.27.0 (zayo.com) modem, 159.153.28.0 (zayo.com) modem, 159.153.29.0 (zayo.com) modem, 159.153.30.0 (zayo.com) modem, 159.153.31.0 (zayo.com) modem, 159.153.32.0 (telia.net), 159.153.33.0 (telia.net), 159.153.34.0 (telia.net), 159.153.35.0 (telia.net), 159.153.36.0 (telia.net), 159.153.37.0 (telia.net), 159.153.38.0 (telia.net), 159.153.39.0 (telia.net), 159.153.40.0 (Level3.net), 159.153.41.0 (Level3.net), 159.153.42.0 (akamaitechnologies.com) modem, 159.153.43.0 (zayo.com) modem, 159.153.44.0 (zayo.com) modem, 159.153.45.0 (zayo.com) modem, 159.153.46.0 (zayo.com) modem, 159.153.47.0 (zayo.com) secure, 159.153.48.0 (zayo.com) secure, 159.153.49.0 (zayo.com) secure, 159.153.50.0 (zayo.com) modem, 159.153.51.0 (zayo.com) secure, 159.153.52.0 (zayo.com) secure, 159.153.53.0 (zayo.com) secure, 159.153.54.0 (zayo.com) secure, 159.153.55.0 (zayo.com) secure, 159.153.56.0 (as6453.net) modem, 159.153.57.0 (as6453.net) secure, 159.153.58.0 (telia.net), 159.153.59.0 (telia.net), 159.153.60.0 (as6453.net) modem, 159.153.61.0 (as6453.net) modem, 159.153.62.0 (hetzner.com), 159.153.63.0 (hetzner.com), 159.153.64.0 (zayo.com) modem, 159.153.65.0 (zayo.com) modem, 159.153.66.0 (zayo.com) secure, 159.153.67.0 (zayo.com) modem, 159.153.68.0 (zayo.com) modem, 159.153.69.0 (zayo.com) secure, 159.153.70.0 (zayo.com) modem, 159.153.71.0 (zayo.com) secure, 159.153.72.0 (telia.net), 159.153.73.0 (telia.net), 159.153.74.0 (telia.net), 159.153.75.0 (Level3.net), 159.153.76.0 (telia.net), 159.153.77.0 (telia.net), 159.153.78.0 (telia.net), 159.153.79.0 (telia.net), 159.153.80.0 (telia.net), 159.153.81.0 (telia.net), 159.153.82.0 (telia.net), 159.153.83.0 (telia.net), 159.153.84.0 (zayo.com) modem, 159.153.85.0 (zayo.com) modem, 159.153.86.0 (zayo.com) modem, 159.153.87.0 (zayo.com) modem, 159.153.88.0 (as6453.net) modem, 159.153.89.0 (as6453.net) modem, 159.153.90.0 (hetzner.com), 159.153.91.0 (your-server.de), 159.153.92.0 (zayo.com) modem, 159.153.93.0 (zayo.com) modem, 159.153.94.0 (zayo.com) secure, 159.153.95.0 (zayo.com) modem, 159.153.96.0 (zayo.com) modem, 159.153.97.0 (zayo.com) modem, 159.153.98.0 (zayo.com) modem, 159.153.99.0 (zayo.com) modem, 159.153.100.0 (zayo.com) modem, 159.153.101.0 (zayo.com) modem, 159.153.102.0 (zayo.com) modem, 159.153.103.0 (zayo.com) modem, 159.153.104.0 (zayo.com) modem 159.153.105.0 (zayo.com) modem, 159.153.106.0 (zayo.com) modem, 159.153.107.0 (zayo.com) modem, 159.153.108.0 (akamaitechnologies.com) modem, 159.153.109.0 (zayo.com) modem, 159.153.110.0 (zayo.com) modem, 159.153.111.0 (zayo.com) secure

159.153.112.0 (zayo.com) modem, 159.153.113.0 (zayo.com) secure, 159.153.114.0 (zayo.com) secure, 159.153.115.0 (zayo.com) secure, 159.153.116.0 (zayo.com) secure, 159.153.117.0 (zayo.com) modem, 159.153.118.0 (zayo.com) modem, 159.153.119.0 (Level3.net), 159.153.120.0 (gtt.net), 159.153.121.0 (gtt.net), 159.153.122.0 (gtt.net) 159.153.123.0 (gtt.net), 159.153.124.0 (zayo.com) modem, 159.153.125.0 (zayo.com) modem 159.153.126.0 (zayo.com) modem, 159.153.127.0 (zayo.com) secure, 159.153.128.0 (Level3.net), 159.153.129.0 (Level3.net), 159.153.130.0 (Level3.net), 159.153.131.0 (integra.net), 159.153.132.0 (zayo.com) modem, 159.153.133.0 (zayo.com) secure, 159.153.134.0 (zayo.com) modem, 159.153.135.0 (zayo.com) secure, 159.153.136.0 (Level3.net), 159.153.137.0 (Level3.net), 159.153.138.0 (as6453.net), 159.153.139.0 (hetzner.com), 159.153.140.0 (Level3.net), 159.153.141.0 (Level3.net), 159.153.142.0 (outernet.net), 159.153.143.0 (shawcable.net), 159.153.144.0 (outernet.net), 159.153.145.0 (Level3.net), 159.153.146.0 (twtelecom.net), 159.153.147.0 (hetzner.com), 159.153.148.0 (Level3.net), 159.153.149.0 (eastlink.ca), 159.153.150.0 (telia.net), 159.153.151.0 (DTAG.DE), 159.153.152.0 (zayo.com) modem, 159.153.153.0 (zayo.com) modem, 159.153.154.0 (zayo.com) modem, 159.153.155.0 (zayo.com) modem, 159.153.156.0 (Level3.net), 159.153.157.0 (Level3.net), 159.153.158.0 (Level3.net), 159.153.159.0 (Level3.net), 159.153.160.0 (zayo.com) modem, 159.153.161.0 (zayo.com) modem, 159.153.162.0 (zayo.com) modem, 159.153.163.0 (zayo.com) modem, 159.153.164.0 (zayo.com) modem, 159.153.165.0 (zayo.com) modem, 159.153.166.0 (Level3.net) 159.153.167.0 (zayo.com), 159.153.168.0 (as6453.net) secure, 159.153.169.0 (as6453.net) secure, 159.153.170.0 (as6453.net) secure, 159.153.171.0 (as6453.net) secure, 159.153.172.0 (as6453.net) modem, 159.153.173.0 (as6453.net) secure, 159.153.174.0 (as6453.net) modem, 159.153.175.0 (as6453.net) secure, 159.153.176.0 (Level3.net), 159.153.177.0 (Level3.net), 159.153.178.0 (Level3.net), 159.153.179.0 (Level3.net), 159.153.180.0 (Level3.net), 159.153.181.0 (Level3.net), 159.153.182.0 (Level3.net), 159.153.183.0 (as6453.net), 159.153.184.0 (as6453.net) modem, 159.153.185.0 (as6453.net) modem, 159.153.186.0 (as6453.net) modem, 159.153.187.0 (as6453.net) secure, 159.153.188.0 (zayo.com) modem, 159.153.189.0 (zayo.com) modem, 159.153.190.0 (Level3.net), 159.153.191.0 (Level3.net), 159.153.192.0 (as6453.net) secure, 159.153.193.0 (hetzner.com), 159.153.194.0 (your-server.de), 159.153.195.0 (hetzner.com), 159.153.196.0 (hetzner.com), 159.153.197.0 (your-server.de), 159.153.198.0 (your-server.de), 159.153.199.0 (your-server.de), 159.153.200.0 (hetzner.com), 159.153.201.0 (hetzner.com), 159.153.202.0 (hetzner.com), 159.153.203.0 (hetzner.com), 159.153.204.0 (as6453.net) modem, 159.153.205.0 (as6453.net) modem, 159.153.206.0 (your-server.de), 159.153.207.0 (your-server.de), 159.153.208.0 (hetzner.com), 159.153.209.0 (hetzner.com), 159.153.210.0 (hetzner.com), 159.153.211.0 (VOCUS.net.au), 159.153.212.0 (hetzner.com), 159.153.213.0 (hetzner.com), 159.153.214.0 (hetzner.com), 159.153.215.0 (hetzner.com), 159.153.216.0 (VOCUS.net.au), 159.153.217.0 (airtel.in), 159.153.218.0 (core-backbone.com), 159.153.219.0 (hetzner.com), 159.153.220.0 (your-server.de), 159.153.221.0 (hetzner.com), 159.153.222.0 (as6453.net) modem, 159.153.223.0 (as6453.net) secure, 159.153.224.0 (zayo.com) modem, 159.153.225.0 (zayo.com) modem, 159.153.226.0 (zayo.com) modem, 159.153.227.0 (akamaitechnologies.com) modem, 159.153.228.0 (akamaitechnologies.com) modem, 159.153.229.0 (zayo.com) modem, 159.153.230.0 (zayo.com) modem, 159.153.231.0 (zayo.com) modem, 159.153.232.0 (zayo.com) modem, 159.153.233.0 (zayo.com) modem, 159.153.234.0 (akamaitechnologies.com) modem, 159.153.235.0 (akamaitechnologies.com) modem, 159.153.236.0 (zayo.com) modem, 159.153.237.0 (zayo.com) modem, 159.153.238.0 (akamaitechnologies.com) modem, 159.153.239.0 (akamaitechnologies.com) modem, 159.153.240.0 (akamaitechnologies.com) modem, 159.153.241.0 (zayo.com) modem, 159.153.242.0 (akamaitechnologies.com) modem, 159.153.243.0 (zayo.com) modem,

159.153.244.0 (akamaitechnologies.com) modem, 159.153.245.0 (zayo.com) modem, 159.153.246.0 (zayo.com) modem, 159.153.247.0 (zayo.com) modem, 159.153.248.0 (zayo.com) modem, 159.153.249.0 (zayo.com) modem, 159.153.250.0 (zayo.com) modem, 159.153.251.0 (zayo.com) modem, 159.153.252.0 (zayo.com) modem, 159.153.253.0 (zayo.com) modem, 159.153.254.0 (core-backbone.com) modem, 159.153.255.0 (zayo.com) modem.

7.8. Public DNS server problems

The DNS server of your internet provider isn't secure because sometimes it implements redirects. The website you ask to go can be another website. A DNS secure server can be unrestricted to avoid this. The primary DNS server is anycast so it's from all locations, but the auxiliary DNS server is unicast so it's from the location of retailer. In fact, using only auxiliary DNS server is more secure. You can set DNS servers under your router and under the network configuration of your computers and consoles. The following results show my opinions on DNS servers for finding servers in battlefield 1 on Xbox One (one star implies hacked lobbies, and five stars imply official servers): Public Secure DNS server List: Level3: 209.244.0.3, 209.244.0.4(*), Verisign: 64.6.64.6, 64.6.65.6(*****), Google: 8.8.8.8, 8.8.4.4(*), Comodo Secure DNS: 8.26.56.26, 8.20.247.20(*), OpenDNS Home: 208.67.222.222, 208.67.220.220(*), DNS Advantage: 156.154.70.1, 156.154.71.1(*****), Norton ConnectSafe: 199.85.126.10, 199.85.127.10(*), GreenTeamDNS: 81.218.119.11, 209.88.198.133(*), SafeDNS: 195.46.39.39, 195.46.39.40(*), Dyn: 216.146.35.35, 216.146.36.36(*), Alternate DNS: 198.101.242.72, 23.253.163.53(*), OpenNIC: 96.90.175.167, 193.183.98.154(*), SmartViper: 208.76.50.50, 208.76.51.51(*). Public DNS server found on http://public-dns.info/: DNS server near where I live, with DNSsec: 89.234.141.66(*). Public DNS server found on http://www.dns-lg.com/ (sponsored by Akamai Technolgies, partner of DICE for hosting https://www.battlefield.com/ as shown on http://ping.eu/traceroute/): freedns.zone: 37.235.1.174, 37.235.1.177(*****), DNS.WATCH: 84.200.69.80, 84.200.70.40(*), CZ NIC Labs: 217.31.204.130, 193.29.206.206(*****), UncensoredDNS: 91.239.100.100, 89.233.43.71(*). The best, so far, DNS public server I have

found for playing battlefield 1 on Xbox One is the DNS public server of Verisign. It ensures stability and security with your connection traffic when you set the DNS server under your router or modem and PC and consoles. But you can't disable allowing rules for playing only with ports 53 in UDP and 443 in TCP. When choosing a DNS check if the server can be reached without firewall using the website tool: https://ping.eu/traceroute/ because otherwise nothing ensure if the server would be the one intended. For example here some results: 209.244.0.3 us reach, 8.8.8.8 us reach, 64.6.64.6 se before firewall reach, 4.4.4.4 us before firewall reach, 114.114.114.114 us before firewall reach, 1.1.1.1 fake dns, 199.85.126.30 fake dns.

7.9. DHCP server problems

On your modem or your router, you can set an IP for the DHCP server corresponding to the server IP of your modem or router. Choosing an IP used by a server of a sensitive website can be a method to counter DDos attacks. DDos attacks avoid finding official servers and so it forwards you on hacked lobbies. For example, you can search with NewB the server corresponding to the website https://home.cern. The IP corresponds to 188.184.37.205 found with http://ping.eu/nslookup/. NewB find a server with IP 188.184.37.1 between 188.184.37.0 and 188.184.37.255 (like 10.0.0.1 and 192.168.1.1). The mask is 255.255.0.0 from network settings of IPv4 manual configuration on a computer. Set this server IP as DHCP server on your router. And use the website IP as internal IP of your computer or console through your router. Also, you can set IP of EA or Activsion (Demonware), to make believes to cheaters when you play against them, they are watch by developers.

7.10. Server problems

People don't believe there is cheaters, particularly on consoles, thinking you can't launch cheats on it. It's due to a lack of knowledge and experience in video-games. People don't report and block in mass cheaters, so only few cheaters are banned, even those using fast

aimbot. The main problem is fake servers allowing cheaters already banned and with cracked game to invade badly multiplayer games. Battlefield 1 encounter fake servers full of cheaters, but true servers are free of cheaters. Gameservers/clanservers open fake servers on all platforms even if they work with game developers. It's easy to cheat, to play with cheats, to insult people of noobs hide behind a screen. Cheaters are worst noobs and will never be good players without cheating. It's easy to know if the server is fake, if game developers support cheats, if someone is cheating. If you find a fair game made by fair developers, enjoy the game and the following games, but don't play games where it's unfair, where you find strange behaviour of everything. Try to find IP of servers, and notice if it isn't fake servers, if it's always unfair, even changing IP of connections, so game developers like those of call of duty games, supports cheats. Always block and report everybody you suspecting are cheaters. These following websites explain how to report cheaters in battlefield games: https://help.ea.com/fr-fr/help/faq/how-to-report-cheating/,
https://www.battlefield.com/companion/career,
https://battlelog.battlefield.com/bf3/news/view/2832654789222476703/.

7.11. Windows firewall problems

To secure your game connection, using Windows firewall, you can do as following. A first step is to create a outbound allowing rule for the service client DNS with distant port 53 and distant IP the IP of your primary DNS server. Also an outbound blocking rule with distant IP 224.0.0.0 to 255.255.255.255. A second step is to create two outbound allowing if secure rules with second option of authentication in TCP and UDP. A third step is to create outbound allowing if secure rules in TCP with locale security entity System and in UDP, with distant IP 0.0.0.0 to 223.255.255.255, for Steam, Uplay, games and all services associate shown with task manager opened with keystrokes ctrl+shift+esc. A fourth step is to create outbound blocking rules in TCP and UDP with distant ports between ports to allow, for Steam, Uplay,

games and all services associate. A last step is to create outbound allowing rules in TCP and UDP, for Steam, Uplay, games and all services associate. Using Windows firewall like explained makes Steam opening hard, but by forcing the online connection to Steam, it finishes by open. Consequently, properties of Windows firewall must be set to all block for inbound traffic and to block for outbound traffic.

7.12. NewB problems

NewB can help to avoid cheaters to hack because it change memory addresses fills by values and also avoid to be connected on hacked lobby by blocking the unsecure server IP. It needs to be run with administrative privilege. Cheats of noobs can be impacted if game developers don't support cheaters. Enter the name of the process or PID to flood memory. Flood memory of NewB can be composed of 24-30 threads maximum. You can block traffic for remote IP in TCP and local IP in UDP, creating automatically blocking Windows firewall rules for connection traffic. When you check "block servers IP", you can block traffic for servers IP found between IP you enter. It asks a file for record IP found. When an IP is found, each IP is recorded in a new line. You can block IP in a text file list which will be added in Windows firewall. One IP by line. Every IP must correspond to IP with the format shown with Windows firewall. If you set a word in process name, the rules created will be named the word, IP, otherwise only IP. If you remove the path of the program, the rules created will be for all programs. By default the rules created is for UDP protocol for outbound traffic, but you can set differently. Run as admin NewB. To do it, create a shortcut and open properties. Under the tab shortcut, click on the button advanced and check the box run with administrative privilege. Apply change.

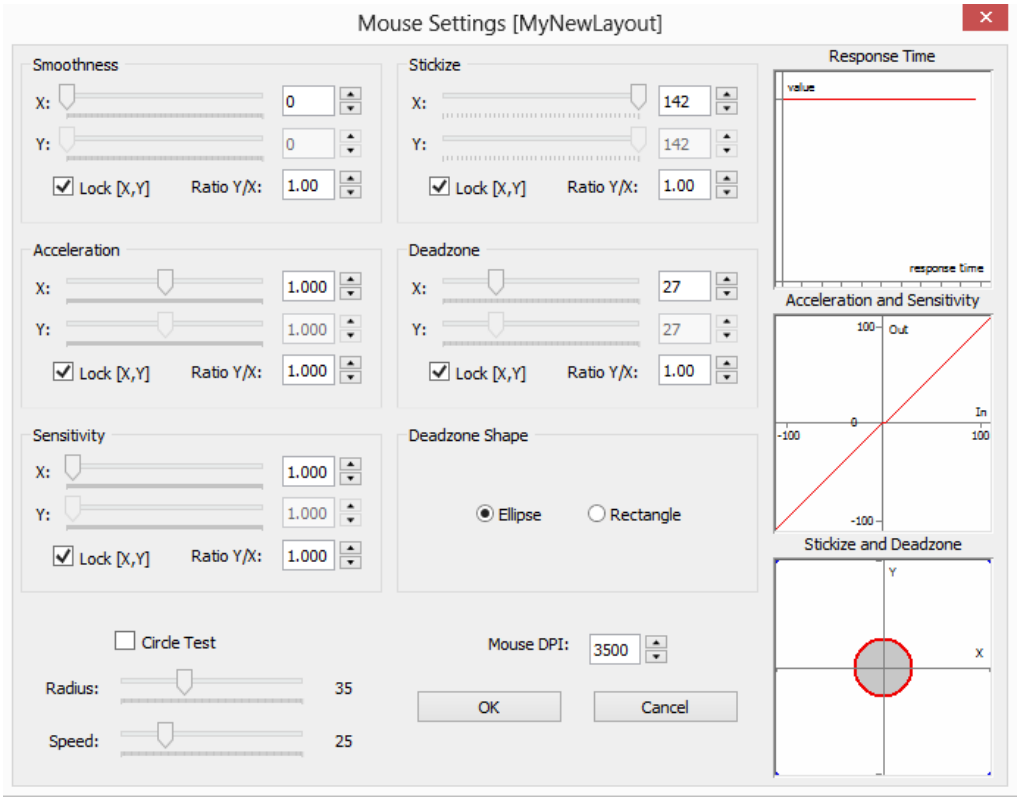
7.13. Playing on console problems

With Xbox live gold subscription, it's possible to own permanently for free older games when you download it from the subscription store, not when it's free game day,

removed after reboot fresh of Xbox. You can undo your subscription to Xbox live if you want to sell your console or cancel the renew automatic of your subscription to have offer on a new subscription. Information on subscription can be found here: https://account.microsoft.com/services/xboxlive/billing. You must login on your Microsoft account from Google chrome. But lot of games, with solo campaign, doesn't need an Xbox live gold subscription, unlike multiplayer games. However Battlefield and call of duty games need it, but I really don't know why how it's full of cheaters. You can set higher privacy for Xbox Live and applications from settings of Xbox One. There is an Xbox One Microsoft store online access from a PC on https://www.xbox.com/fr-FR/games/xbox-one for keep yourself informed on new games and sales. There are often time sales, like winter, summer, holiday, christmas, black friday, halloween... You can have free games with xbox live gold subscription. To have these games at first hour the day it's given, instead of waiting the page update of subscription gold gifts, go on the store page of the game. You can know which games are given in advance by watching the videos of Xbox channel about games with gold for the month. When games are bad optimized, to have your games running smoothly, I recommend setting output video quality to 720p instead of 1080p under display settings of Xbox One. Shrink games if possible, under system, under storage. It doesn't ask downloading the rescue disk space and protect against modification. To play keyboard and mouse on consoles, there is hardware like cronusmax, xim and venom x. It's possible to play very well keyboard/mouse using cronusmax device on Xbox and Playstation platforms. Cronusmax is the best to play keyboard/mouse on consoles. For better control, I strongly recommend to not update firmware of cronusmax device or reset to the factory firmware the cronusmax device (it run with Xbox One). Also for more security, I recommend to use the installer of cronusmax pro application, with the inside plugin X-Aim, directly found on the official cronusmax website. I don't recommend community updates and scripts, for low quality and

security. Also, online updates from cronusmax pro application aren’t secure. When using plugin X-Aim for playing Xbox One with keyboard/mouse, you can flood memory of Cronus process with NewB. Disable option ignore CM controller input in plugin x-aim, and also connect the controller to the rear. For playing on consoles using keyboard/mouse, you can use cronusmax device and cronusmax pro application (must be run with administrative privilege, to run it with administrative privilege, create a shortcut, then under properties, under the tab shortcut, click on the button advanced and check the box run with administrative privilege) with updates of both. You need to insert cronusmax device in the console like a controller, then behind the cronusmax device you need to insert the controller with a Samsung phone micro USB wire for authentication (wire allowing charge/data/synchronisation), lasting by connecting cronusmax device from the side to PC using the wire coming with. Use the plugin X-AIM of cronusmax pro application. Make the reverse for closing. For remove the problem of disguard authentication, you can move up/down the left stick just after connecting the controller into cronusmax device. For don't have to authenticate few times the controller, set the console time of automatic shut down to 6 hours or never instead of 1 hour. Disable rumbles in game options and from parameters in ergonomic settings, because your controller can fall on the floor (it can break wire and controller). You need 2 HDMI inputs on your HDMI screen for switch between your PC and console, and so you need 2 HDMI wires. When you encounter a disconnection of gamepad on Xbox One, you must shut down cronusmax application, then unwire the device from PC, then unwire gamepad of the device, then the device from console, and then connect directly the gamepad to console. Do the reverse for connecting cronusmax device. It's better to unwire from PC the cronusmax device if you don't play cause with time the device is overheated. Close the cronusmax application before. You can let the device connected to the console. To stop the inputs to be sent in plugin X-Aim, press first ctrl then esc keys while ctrl is pressed. For next generation consoles, you

can still use outdated cronusmax device by using a custom special accessory found on http://www.brookaccessory.com/detail/07484504/. Here mouse settings for cronusmax application as following:



Push the key ctrl first then esc, while you let pushed ctrl, for stopping data input to be sent in plugin X-AIM. If you play on consoles using the cronusmax device, I advice to remove your payment method after each bought because you can make mistakes buying stuff without you take care. Or you can set a passkey for buying games under settings of your account, under online privacy and safety under billing and payment, and under settings, security, passkey, under barrier, under customize by deleting passkey and create passkey. From a cheat website, it's writing "Xbox One SDK has been leaked". Probably cronuxmax application and firmware SDK has been leaked too, so Steam takes control of your console network. I strongly recommend to not using cronusmax with the same PC where you use Steam, even just installed once. I noticed when I don't flood memory of cronus process with NewB, I fall on match fill by cheaters I already reported. Games under CD on consoles are very cheaper after

released compare to games under Steam where you must wait discount. Stop the game each time you finish to play it, by pressing the Xbox button, then press the menu button under shortcut of the game you played and press stop. It's better if you reset from fresh your Xbox sometimes, keeping installed games. Put in standby installation of games when you play, because of your ping and use of harddrive, also before shut down your console. For setting properly your Xbox for playing like on PC, do as following: It's better to set a content restriction under account for content access set to 18 and plus and web filtering to websites allowed only, under system for update check if there is update available sometimes and uncheck boxes keep console up to date and keep up to date my games and applications, under clock uncheck the box for updating summer clock, under storage remove residual expansions, from display and sound for video output set colour intensity to 36 bits per pixel (12 bits) and set colour space to PC RVB, under advanced video setting check boxes allow rate 50 Hz and allow rate 24 Hz, under kinect and peripherals for peripherals and accessories in peripheral information check for gamepad update, under power and start choose a power mode to green (economize) energy and disable start ring sound, under preference disable notification, disable streaming and options, disable comment with send notification, disable options of activity flow, under TV and OneGuide for OneGuide in comboboxes for HDMI and USB choose masks duplicates in SD and erase OneGuide and historic, under audio and video choose rates of 50 Hz for comboboxes for HDMI and USB, under disk and blu-ray disable automatic start of reading, under options and ergonomic disable narrator and subtitles. After reset or update of the console, these options must be set again. For a better rendering of graphics for your console, there are unlocked picture options of your TV screen when you are on the channel of your console. Change these options for better graphics. It's important to let default brightness in game options and well set brightness on your TV screen for not be disturbed by dark zone. For more privacy, subscribers can be blocked through their Xbox profile on your Xbox One.

Remove all shortcuts for better performance also. If you uninstalled a game and you reinstalled it, DLC you bought aren't installed automatically, click the button menu under the shortcut of the game and click on manage, and then under the tab you can enable DLC. Sometimes the available updates aren’t displayed and you must launch the game to know if there is an update. Also, available updates are only displayed when you check the game manager page. If you encounter problem of download or connection you can shut down your modem and console, and then unwire electricity of both, and then restart together it. You can personalize the community tab to not have annoying posts of the community or from nowhere. Change region of your XBox like Arab United Emirates or Israel or Pakistan if you live in a European country to increase the download speed. The region can be changed from parameters in System, language and region. Sometimes games will take region for set the language of the region in the games. If you have a problem of language you can choose the region South Africa or India or Turkey. It's possible to have satellite connection to US servers of BF1 choosing the right region. In scoreboard your ping will not display bad variation due to saturation of data. I advice to set the region in United States when playing on Electronic Arts servers because Microsoft claims XBox One servers are secure and if you live far from United States there isn't any vault the connection may be disrouted with fake servers own by gameservers/clanservers. The connection will be secure until United States country. Check if there is free stuff in XBox live store. I had for free all Starwars Battlefront DLC. Don't forget to go in the manager page of your games to install DLC. Take care to let 10 percent of free space on hard drive of your consoles like on PC. When you insert a DVD into your consoles, take care to not have something on it. Always put DVD into their boxes after each use. Don't trust any other website than xbox.com for showing publically your profile. The address is https://live.xbox.com/en-US/Profile?Gamertag=Daddy+Kiefer for the gamertag Daddy Kiefer. If you want to do it, I recommend to enable full ASLR with the regedit key

MoveImages and if you use a screen without secure HDMI wire, allowing radio TV channel, disable radio waves by using a wire which makes a short circuit with the radio plug joining sides of metal parts. I also recommend to not use Steam, and even any network with your computer. Also disable a maximum of services like explained in chapter 3.1. Make a fresh reboot of your PC before installing application for it, like explained in chapter 7.15. Also, I recommend adding to EMET running, cronusmax application. Also you can enable DEP using cmd dos command: bcdedit /set {current} nx AlwaysOn. For better control with the plugin X-Aim, check for the default mouse configuration and acceleration, change otherwise, if the Windows Registry Keys are like this:

[HKEY_CURRENT_USER\Control Panel\Mouse]

"SmoothMouseXCurve"=hex:

00,00,00,00,00,00,00,00,

15,6e,00,00,00,00,00,00,

00,40,01,00,00,00,00,00,

29,dc,03,00,00,00,00,00,

00,00,28,00,00,00,00,00

"SmoothMouseYCurve"=hex:

00,00,00,00,00,00,00,00,

b8,5e,01,00,00,00,00,00,

cd,4c,05,00,00,00,00,00,

cd,4c,18,00,00,00,00,00,

00,00,38,02,00,00,00,00

When you use cronusmax device to play multiplayer games, I advice to set the cronusmax operational mode (from tools in cronusmax software) of your device to tournament (letter t display on device). It disable GPC scripting, but it turn your match parties to several

advantages, like avoiding controller disconnection, avoiding to fight against other using no recoil or aim abuse scripts, and having better control. If you don’t set this operational mode, think to use script abuses like others you will fight against.

7.14. Steam games problems

In panel control with language options you can switch keyboard QWERTY/AZERTY, when games don't allow rebinding keys. Add an entry method, and then remove the first entry method. To increase your Steam statistics you can choose to play some games like ZupZup or Super Duper Genocide Simulator 2017 for having lot of achievements like shown on this website: http://astats.astats.nl/astats/Steam_Games.php?DisplayType=Achievements. For win levels on Steam and show some screenshots or your favourite games or artworks or achievements or items, you can sell cards you win when playing and buy some to create badges. Exchanging cards for gems is very expensive and so you will not win levels. Also, there are Steam guides and Youtube videos explaining how to win achievements in your games. With these helps, sometimes it's easy to have 100% achievements for your games, increasing your Steam stats. For enable the counter of your achievements won in your games, you must go on the page of the games in your Steam library loading the achievements on your profile if you have set an achievement showcase. Also, obviously you need to be online. There is game with only one achievement to win the game to 100%. You can find it with http://astats.astats.nl/astats/Steam_Games.php?DisplayType=Achievements at last pages. When you play offline but want to win achievements, you must load the page of the game to show achievement to unlock, then close Steam once, unfortunately you must do it just before be offline. It's like for games protected by Denuvo because you must launch the game just before be offline. Check game files integrity of games from properties of your games from games library and start at least once your games with online connection after fresh reboot of your PC. There are free DLC on store pages of your games. To install/uninstall them you

must go on the page of the game in your Steam games library and check/uncheck box of the DLC you added. You must restart Steam to apply change. You can save money by buying games with bundle even if you already own one of it. There is nice discount price on games when you wait good sales like christmas sales. You can create wishlist on Steam for knowing which games you are interested will be in discount price, and you can manage which games you will be really interested after studying it when you have money for buying it. You can access your Steam account on http://store.steampowered.com/ for keep yourself informed on new games and sales. There are often time sales, like winter, summer, holiday, christmas, black friday, halloween... Use offline mode to unlock Steam achievements if it don't run in online mode of Steam. Steam can freeze, to remove this issue; you must uninstall few games until freeze disappears. Often Steam games which are cheap are hard to finish because they aren't tested and developers are scary of hardcore gamers from their hates on Steam forums. Even with the game Cuphead known as a hard game, there are haters insulting people when they ask to have the full game in simple mode difficulty. To avoid cuts of download, set a download region adapted, the one you will see better speed of download. I prefer to set the regions United Arab Emirates or Egypt or Turkey. When Steam game download is lowest, remember to restart your modem for change of IP and remove saturation of data. If download slower, you can change country in Steam download settings to increase download, like changing from Egypt to Turkey or Pakistan or United Arab Emirates. Take care with Steam client beta because after game updates, your game can crash at launch. Disable Steam beta in parameters and delete launch options of Steam and your games. Choose a server from the tab display servers, and choose servers VAC protected with IP you will check with https://bgpview.io/. Take care if it's own by gameservers/clanservers. Take care to IP of connection when you playing shown in perfmon.exe under network tab also. With Windows firewall, block IP of gameservers/clanservers for ports 1-65535 in TCP/UDP. If all servers are

only own by gameservers/clanservers, it's not a fair game. I don't recommend spending money on Steam, but instead on Origin for PC and Xbox, because I've seen a big cheater playing, the 25th June 2017, Half Life 3 closed alpha developed by Valves, creator of Steam. They say, they don't like cheaters but with servers' retail by Gameservers/Clanservers, it's a platform full of cheaters. There is nothing to do and nothing good with Steam. When a cheater asks the support to remove his ban, they say to contact them later for finishing removing the ban one year later. The Steam profile picture of the cheater show an illuminati alliance: http://steamidfinder.com/lookup/spinyB/, http://steamcommunity.com/profiles/76561197983836905. No doubt he's a cheater and closer to Steam creators. Even if the cheater wanted to prank his friends with notepad added to non-Steam games and renamed to HL3 closed alpha, he cheated in lot of VAC protected multiplayer games without being banned at least once. I wrote on his profile: cheater playing HL3 closed alpha, I was sure about steam, he replied without denying he doesn't cheat but this: always nice to play HL3 closed alpha as non-steam game! God, give ppl some brain pls. Another insults coming from cheaters. They can insult you 10 times in 3 posts like I was massively insulted in call of duty forums. It's to developers to ban cheaters. If a multiplayer game uses exclusively gameservers/clanservers servers, it's not a descent or fair game, it's infested by cheaters and developers will do nothing against. You can remove your credit card numbers from account parameters leaving this hack fest platform. I removed my credit card numbers, then one hour later, on the e-mail box of my internet provider, I use to login on Steam, I received an e-mail of g2a saying I bought a Steam gift card but I never bought on this hack site of stolen keys.

7.15. Installing Windows problems

After installing bootable Windows, you can uninstall programs installed from control panel in programs and functionalities, but let graphic, audio, and network drivers and let

frameworks. From programs and functionalities in functionalities, you can disable all features but let .NET framework 3.5 and Internet Explorer 10. In System, open performance tab and disable features for better performance, enable DEP for all programs, disable remote assistance in System and disable NetBIOS in network settings, delete fax and printer in peripherals and printers. In User account, enable highest level of UAC. From energy manager open when you personalize desktop screen, enable highest performance. In administrative tool, open services and disable some services but you shall let services explained in chapter 3.1 (take care if you can still open another services tab before closing the first). Set your network configurations and enable specific rules in Windows firewall like explained in chapter 7.10, set Windows firewall correctly by blocking all inbound traffic and all outbound traffic if no rules. You can import/export strategy rules. Under network configuration, if TCP/IP isn't recognized, uninstall driver of network card, then reboot your PC. Take care if your network is set to public or private. If it's set to public you can check resolve problems for residential group and apply fix for changing to private network. Set a static internal IP under network settings for TCP/IP parameters (if it asks to install it, disable driver of network card and then restart your PC). Add to your modem under DHCP tab, your computer with static IP and create modem firewall rules. Disable tasks from tasks scheduler in Windows/System32. Disable start programs from task manager open with keystrokes ctrl+shift+escape. Under desktop click right and then under the tab click personalize, open standby screen option and check the box at the resumption request the logon, under power option for system parameters enable require password after quitting the standby mode. In ergonomic settings, from control panel, enable return to open session page when computer is put in standby, and enable high performance. Only download and install drivers from trusted sources like https://www.microsoft.com/, http://www.nvidia.com... It's better to install Steam, Origin, Uplay games on a hard drive where Windows isn't installed. The game files can be easily

recovered when you reinstall Steam. Make a copy of game save files folders present in the folder "My Documents" to your hard drive. When you install Steam games, specify the folder of installation. Game files are auto-detected and game save files are restored from the folder "My Documents". If your PC miss files, install vcredist and framework found on microsoft official website instead of using DLL found on unsecure websites because it can hide virus. I don't recommend uninstalling vcredist and framework packages because files can miss after.

7.16. FPS multiplayer gameplay problems

Here my advices for be competitive in FPS and for improve your skill: look everywhere as long as you can, walk with caution if you know there is someone waiting you or searching you, run if you know there isn't someone else and you want rush a physical or killing objective, learn to aim perfectly, don't miss the chance to kill someone in your sight, learn to imagine where can be someone to kill or where camper is use to stay (use your memory), stay with your team if you aren't hot to rush, use your teammates to be a shell or a chill or a bait, stay in setback if the adversary team is rushing you, infiltrating enemy lines by circumventing them, try to cover your body with decorative element if you take an objective, use wall, head glitch, crouch to protect yourself from someone, for rushing you must take someone from front, give up the match if it's unplayable because rage quitting doesn't exist but cheaters are real, play with guns corresponding more to your gameplay and pleasure, try hard because cheaters are insane, play a lot of different games in solo campaigns or with friends or make pause as you want because you learn more instead of persisting with rage and playing a lot of different games is training your brain, try to never have stress, if you stressing you need to camp awhile a moment, no need to enjoy playing, quit the match if you rage so hard, enjoy aiming and killing, enjoy learning your tactic and skill, enjoy win a duel, reload if you are sure there is anybody else, footstep, explosion and rifle sounds indicate where there is someone to kill, privilege one kill one die for your accessories and movement as tactical

behaviour, if someone can't be reached throw a grenade, the movement of grenade someone throw at you give you the direction of the someone, throw grenade or camp or wait someone if you think it will protect you, throw grenade if you think they are numerous or finishing to kill knowing you will die, throw grenade to kill a camper or a team, be curious to look around, don't be scary to play because everyone have a first start or is learning, only newbie, no one is a noob, lot of cheaters everywhere but not everytime, learn from your mistakes, play fair, never cheat because you will always need cheat a moment or another, never offence people, never be a racist otherwise nobody will help you, be proud to always learn, be always careful and concentrate, prefer playing anything else instead of be tired doing nothing or watching TV. Better to choose defending an area instead of attacking a new area. Choose to rush an enemy hides instead of him choosing to rush you. Take care to enemy hide possibly everywhere when you enter a house, in an edge for example, you can throw a grenade for see if there is someone else in. Stay cover and safe as possible. Stay concentrate and imagine strategies while playing. Wait before entering a room by a door because enemies can be in the room or enter also the room like you. Your allies can help you or not to know if there is enemies ready to shoot you. Use allies and vehicles of your team as cover. The scoreboard gives you knowledge if rage quit is necessary when the members of adversary team have a K/D ratio positive while the members of your team have a K/D ratio negative. Don't accept this kind of match. Use video settings and use brightness of your TV to have better visual of enemies. Use mines where you think vehicles will go through, for example like just in front of an available vehicle. Allies shoot by enemies indicate where they are. Don't run across a large expanse if there aren’t any rocks or trees or walls to avoid enemies to see you. Always look left or right to detect potential enemies or to check if there isn't any enemy. When you run or climb stairs, always place the cursor where enemies can arrive. Try to cover your back with rocks, trees, walls, vehicles... Attack enemies being own body cover or hide or by surprise or

with allies often as possible. Always search enemies zone by zone, house by house, looks left and right, walk everywhere into, find a scope to focus enemies would go through. If you see someone in your team with bad aim, follow him and shoot enemies for him. Enable highest FOV (Field Of View) if the game allows it and let default luminosity but prefer change it under settings of your screen.

7.17. Sharing connection problems

It can be useful to share connection with your PC or consoles because you can use a VPN or flood memory with NewB for the service distant connection access manager. For flooding memory with NewB you need .NET Microsoft Framework 4.5 and you need to know the PID of the service distant connection access manager with task manager (open with keystrokes ctrl+shift+esc). In order flood memory can be achieved you must disable DEP, particularly for Windows services, to do it, launch with administrative privilege cmd.exe and type: bcdedit.exe /set {current} nx AlwaysOff, and then restart your computer. For prevent attacks, UAC must be set to maximum security. Also remove virus like DLL or EXE from unwanted folders with shut down of what is using it like explorer.exe, retry to delete files while shut down. You must run as admin NewB, for it create a shortcut on desktop, and then with its properties, under shortcut tab, click on advanced button, and then check the box run with administrative privilege, apply change. For sharing connection with your PC or consoles, you don’t need to create rules on your modem firewall for distant port 53 in UDP, but you need rules for distant ports and IP you found for having connection into games for the computer host. If you use DNS servers IP like Norton ConnectSafe, you need to create rules on your modem firewall with distant IP, the IP of DNS servers and distant port 53 in UDP. The host must have Wi-Fi and Ethernet cards. The TCP/IP properties of your network Wi-Fi card must be set as usually but under property of the network Wi-Fi card, under the tab share, check the box allow sharing this connection and set the combobox to local network

(Ethernet). You can set DNS servers IP under manual configuration of TCP/IP ipv4 properties of the Wi-Fi card. The TCP/IP properties of your network Ethernet card must be configuring manually, with ipv4 address 192.168.137.1, mask 255.255.255.0, without default bridge IP, and primary server DNS 192.168.1.1 or DNS servers IP. The connection for your PC and consoles should be established through a RJ45 wire from the host connected to the modem through Wi-Fi. For secure your console you can set manually DNS servers IP under its network settings and create Windows firewall rules on the computer host. For inbound traffic, an allowing rule with local port 53 and distant ports 49152-65535 in UDP with local IP the IP corresponding to the computer host internal IP tasking as a modem (like 192.168.137.1) and distant IP the IP corresponding to your console internal IP (like 192.168.137.9 shown in the network configuration of your console) for the service distant access connection manager. For outbound traffic, an allowing rule with local ports 49152-65535 and distant port 53 in UDP with distant IP the IP of your modem (192.168.1.1) or DNS servers IP and the internal IP of the computer host tasking as a modem (192.168.137.1) for the service DNS client, an allowing rule with local ports 49152-65535 and distant port 53 in UDP with distant IP the IP of your modem (192.168.1.1) or DNS servers IP for the service distant access connection manager, add allowing rules for the programs you use for browsing internet on your computer host with all local ports and distant ports 80 and 443 in TCP, for secure connection traffic create rules with authentication mod require authentication for inbound and outbound traffics with protocols UDP with port 53 in terminal endpoint 1 and all ports in terminal endpoint 2 and with all ports in terminal endpoint 1 and port 53 in terminal endpoint 2. Consequently, setting Windows firewall options for inbound and outbound traffic with blocked if no rules. Set manually network configuration under parameters of your console, it will remember the configuration after restart. The secure connection traffic rules must be enabling after connection to a match and be disabling for report cheaters. Take care with these last two rules,

because you must allow inbound and outbound traffic on port 53 in UDP and outbound traffic on ports 80 and 443 in TCP to report cheaters and browse pages on your console. Block IP and ports under your modem firewall like explained in chapter 7.6. To update a game or repair connection you need to unwire/wire the Ethernet wire connecting your computer host to your console or restart your console, because letting only traffic through port 53 in UDP will stop update or sometimes connection fails. Obviously you need to enable peer connection services for the computer host from administrative tools in control panel. In order the service distant access connection manager run, the service telephony must run. There are services and programs sending data from your computer to worldwide computers like service layer application that provides protocols for third parties in internet connection sharing named alg.exe and user notification service from Intel name UNS.exe. Disable services and remove exe like it found from task manager (open with ctrl+shift+esc, open file place, stop task, watch names...) and under network tab under listen ports tab in perfmon.exe in administrative tools in control panel. Also uninstall programs, in programs and functionalities in control panel, using connection traffic like explained in chapter 3.1. These services or other unwanted programs on your computer send data through Windows firewall unable to stop it. After restarting your computer host, you must delete Windows firewall rules for sharing connection automatically create. In conjunction, on your computer host, use the cmd prompt commands explained in chapter 3.9. Also, you can use DNScrypt by OpenDNS available here: https://www.opendns.com/about/innovations/dnscrypt/, https://github.com/opendns/dnscrypt-win-client, https://dnscrypt.org/, https://github.com/Noxwizard/dnscrypt-winclient, https://download.dnscrypt.org/dnscrypt-proxy/. You need to set Windows firewall to default settings on your computer host and to allow on your modem firewall port 53 in UDP/TCP and IP 208.67.220.220 with ports 1-65535 in UDP/TCP. Launch dnscrypt-winclient.exe and choose to apply proxy on both network cards. It needs to have dnscrypt-resolvers.csv and

dnscrypt-proxy.exe under the same folder as dnscrypt-winclient.exe. Choose Cisco OpenDNS as provider and start proxying. Open the GUI with administrative privilege. If the console window can't be open, you need to stop the service internet connection sharing (ICS) then start proxying, and then restart the service SharedAccess (from task manager under service tab). It's due to port 53 already in uses by this service as listening port. To restart the service, you need administrator privilege in task manager. After you open it with keystroke ctrl+shift+esc, under the tab process, click on the button open process for all users. If you encounter problem with sharing connection after restarting your computer host, like your console doesn't have connection anymore, I advice to unwire the wire RJ45 connected to your console, and then disable sharing connection for your Wi-Fi card under network settings of your computer host, and then enable it again, and finally wire with the RJ45 your console. Also, check or set manually network settings under your console when you use Windows firewall for the computer host. For better connection, under share tab of wireless card properties, open settings and allow services for ports 80, 443 in TCP and 3074 in TCP/UDP. Normally, sharing connection with a computer host having Windows 10 OS, set automatically a rule for connection sharing service named dacm for distance access connection manager under Windows firewall settings.

7.18. Port 3074 problems

For avoid hackers to use your connection through your modem and games using port 3074 because port 3074 allow all ports by inbound traffic with nat/pat rule, you must allow only ports out of port 3074. if games use port 3074, don't mind to play these games free of cheaters but these games like all call of duty games or even Destiny games (edited by hacktivision) are cheaters infested lying they don't cheat and we are noobs. When you create rules on your modem firewall like for steam, create rules as following: local port is your computer internal IP, distant ports are 80, 443 and 27000-27050 in TCP, or 1-3073, 3075-

65535 in TCP/UDP. On your modem, never allow Upnp and any nat/pat rule for port 3074 for your computers or consoles. It allows unwanted inbound traffic for all ports and IP even if you don't allow these ports and IP. Even if your computers or your consoles have a strong firewall, the games you have on your computers and consoles go through the firewall. The traffic coming from internet can't, but the traffic send by your computers and consoles can go forward internet. The games you have will do both. Cracked game owners and banned cheaters can play the game when port 3074 is used. Multiplayer games using port 3074 don’t deserve to be played.

7.19. Call of duty games problems

Call of Duty games on PC through Steam, even with VAC enable, are really a hack fest. On XBox One, it's less a problem because you can secure your connection through sharing connection with a computer host. Also there is a strong firewall denying inbound traffic. Inbound traffic from a nat/pat rule for port 3074 and malicious IP can be blocked easily using Windows firewall of the computer host. You can block IP with a list using NewB as explained in the chapter 6. I tested to secure connection on a PC through a computer host sharing connection but it doesn't seem to run like on XBox One. It's really hard to understand why Steam claims VAC secure servers in multiplayer PC games while the connection itself isn't secure. Call of Duty games on PC through Steam is edited by hacktivision. Until call of duty servers are own by gameservers/clanservers, all these games will be infested by cheaters. You shall not trust the developers working with gameservers/clanservers whitout having their own servers for their games.

7.20. Multiplayer games problems

If you want the best experience in multiplayer games, XBox One delivers it. You can play very well with keyboard and mouse or any controllers using cronusmax device. You need to set security by searching IP and ports with your modem firewall for playing your

favourite multiplayer game like explained in chapter 7.6. Also for better connection, you need to be NAT open by just allowing in your modem firewall ports 88, 500, 3544, 4500 in UDP, 80, 443 in TCP, 53, 3074 in TCP/UDP. When servers are locating in United States like for battlefield 1, set the language to French (Canada) or any language you want in available country and set the region to United States. Also use the DNS servers IP of Verisign (64.6.64.6, 64.6.65.6) but don't flood memory of services using NewB. Sharing connection from a computer host can be more a problem than a solution. Verisign delivers integrity certificates for games (it's shown under properties of call of duty exe on your PC) allowing secure connection between trusted users connected together in the same network interface where trusted users are those who don't modify the interface from read/write process memory or files. But the game I meet less cheaters is battlefield 1 on Xbox One just setting Verisign DNS servers IP and confidentiality letting my e-mail and information in access for games under Xbox One parameters, and allowing on my modem firewall:

TCP: all local IP, distant IP 134.213.244.128, mask 255.255.255.128, distant ports 1-65535

TCP: all local IP, distant IP 159.153.0.0, mask 255.255.0.0, distant ports 1-65535

UDP: all local IP, distant IP 159.153.115.0, mask 255.255.255.0, distant ports 10000-10100

UDP: all local IP, distant IP 159.153.42.0, mask 255.255.255.128, distant ports 17490-17510

TCP/UDP: all local IP, distant IP 64.6.65.6, mask 255.255.255.255, distant ports 1-65535

TCP/UDP: all local IP, distant IP 64.6.64.6, mask 255.255.255.255, distant ports 1-65535

TCP: all local IP, all distant IP, distant port 443

TCP: all local IP, all distant IP, distant port 80

TCP: local IP internal IP of my computers, all distant IP, distant ports 1-1023

With it, the connection will be established on secure servers with trusted users, deploying features to kick cheaters and to show you are not that one. If it's still not it, try to use the auxiliary DNS server IP of your internet provider, shown under your modem page. Set this

distant IP under DNS settings of your console and your modem firewall for distant port 53 in UDP. When you are in a match, disable all rules under your modem firewall, even the rule DNS. Let rules for your computers associated with their internal IP. Don't forget to have set your computer’s internal IP to static IP. Use the internal IP above 192.168.1.128 for your console, so you can have your computers connected using the internal IP 192.168.1.2 and mask 255.255.255.128 allowing distant ports 1-1023 in TCP under your modem firewall. There are modems starting at IP 159.153.42.68 which use badly similar IP of Electronic Arts (found by NewB). Instead of IP 159.153.42.0 with mask 255.255.255.128, it would be better setting under your modem firewall IP 159.153.42.1 to 159.153.42.67 with masks 255.255.255.255 and ports 17490-17510 in TCP/UDP. IP free of modems are (to set under your modem firewall): 159.153.0.0, 159.153.2.0, 159.153.7.0, 159.153.8.0, 159.153.10.0, 159.153.11.0, 159.153.12.0, 159.153.13.0, 159.153.14.0, 159.153.15.0, 159.153.17.0, 159.153.24.0, 159.153.40.0, 159.153.41.0, 159.153.47.0, 159.153.48.0, 159.153.49.0, 159.153.51.0, 159.153.52.0, 159.153.53.0, 159.153.54.0, 159.153.55.0, 159.153.57.0, 159.153.62.0, 159.153.63.0, 159.153.66.0, 159.153.69.0, 159.153.71.0, 159.153.78.0, 159.153.90.0, 159.153.91.0, 159.153.94.0, 159.153.111.0, 159.153.112.0, 159.153.113.0, 159.153.114.0, 159.153.115.0, 159.153.116.0, 159.153.119.0, 159.153.120.0, 159.153.121.0, 159.153.122.0, 159.153.123.0, 159.153.127.0, 159.153.129.0, 159.153.131.0, 159.153.133.0, 159.153.135.0, 159.153.136.0, 159.153.137.0, 159.153.138.0, 159.153.141.0, 159.153.142.0, 159.153.145.0, 159.153.147.0, 159.153.148.0, 159.153.149.0, 159.153.151.0, 159.153.167.0, 159.153.168.0, 159.153.169.0, 159.153.170.0, 159.153.171.0, 159.153.173.0, 159.153.175.0, 159.153.181.0, 159.153.182.0, 159.153.187.0, 159.153.192.0, 159.153.195.0, 159.153.201.0, 159.153.209.0, 159.153.210.0, 159.153.212.0, 159.153.213.0, 159.153.214.0, 159.153.215.0, 159.153.216.0, 159.153.220.0, 159.153.223.0 with masks 255.255.255.0 and ports 10000-10100 in UDP, and 159.153.16.0, 159.153.19.0, 159.153.25.0, 159.153.35.0, 159.153.61.0,

159.153.68.0, 159.153.70.0, 159.153.72.0, 159.153.92.0, 159.153.132.0, 159.153.163.0, 159.153.191.0, 159.153.219.0, 159.153.233.0 with masks 255.255.255.128 and ports 10000-10100 in UDP. Otherwise, allow all distant IP and distant ports 1-65535 in TCP/UDP associated with your console internal IP under your modem firewall and when you are connected into a match disable the rule. Don't forget to set a DNS server under your console setting like Verisign auxiliary DNS server IP, or auxiliary DNS server IP of Norton Connectsafe. Another solution tested and simplest to put in place, but not satisfying, is to allow on your modem firewall all distant IP for ports 1-65535 in TCP, and distant IP 159.153.0.0 with mask 255.255.0.0 for ports 1-65535 in UDP, and distant IP an auxiliary DNS server with mask 255.255.255.255 for port 53 in UDP. Due to connection to servers be disrouting to hacked servers by allowing ports 1-65535 even only in TCP, the exact and only rules to allow are for IP 159.153.244.128 for ports 42000-42200 in TCP, 134.213.244.128 for ports 10000-10100 in TCP, with masks 255.255.255.128, for IP from 159.153.42.71 until 159.153.42.85 for ports 17490-17510 in TCP/UDP with masks 255.255.255.255 (to avoid hacker servers behind a router), and for IP 159.153.113.0, 159.153.114.0, 159.153.115.0, 159.153.116.0, for ports 10000-10100 in UDP, with masks 255.255.255.0. Also ports 80, 443 in TCP and IP of primary and auxiliary DNS server you choose for port 53 in UDP. For all of these rules, set on your modem firewall for your consoles you playing, local IP higher than 192.168.1.128 with mask 255.255.255.255, allowing your other computers to be connected with first part of IP with masks 255.255.255.128, and also set on your modem firewall for your consoles you playing, local ports 49152-65535, avoiding port stealing, otherwise it allows hackers to use your MAC address and so spoofing server IP, by denying authentication of servers with some local ports from MAC table. But some multiplayer games like call of duty advanced warfare ask you set under your modem firewall local ports 49152-65535 but also local ports 3074-3076 with distant ports 3074-3076 in TCP/UDP and it need to create a

NAT/PAT rule for ports 3074-3076 to be the host with NAT open (more precisely, advanced warfare need rules with local ports 49152-65535 and distant ports 3074-3076 for distant IP 185.34.0.0 and 209.170.0.0 with masks 255.255.0.0 and a rule with local port 3074 and distant ports 3074-3075). The game black ops 3 use same ports and IP than advanced warfare. Hackers can set their modem IP everywhere for have their computers on 253 IP maximum. Their computers can't use same IP of IP already in use. Their modem can use IP in first part and their computers IP in second part of the scale IP with mask 255.255.255.128. If there are modems on first part and second part, all the first part of IP isn't used by computers of hackers but all the second part is used. If you still encounter very annoying cheaters, I advice to reboot from fresh your console and uninstall/reinstall battlefield 1, because hacks of cheaters can modify your game and console to allow IP spoofing causing fake servers connection with same IP of official servers. Annoying cheater corresponds to someone always killing you because he knows exactly where you are all over the map, he uses recoil hack (switch lag) because he's so noob that he needs you can't shoot him, he uses aimbot because he's a very bad person and not a gamer or a FPS lover. When there is someone like this against you, the teams aren't in equilibrium of forces, the match becoming unplayable. Report the cheater and leave the match. Fake servers of gameservers/clanservers are full of lags and cheaters. Don't let you destroy by adversary team, happily in battlefield 1, you can change of team as you want. Use Anti-spoofing DNS server like the one found on https://github.com/puxxustc/sans. The IP of DNS server you must use is 114.114.114.114. To test different DNS servers, allow all distant IP and port 53 in TCP/UDP under your modem firewall and you can set only one DNS server IP under your console letting empty cells or 0.0.0.0 for auxiliary DNS server. Try DNS server IP 1.1.1.1 as primary DNS IP and 0.0.0.0 as auxiliary DNS IP. If on your computers you don't set a DNS server with IP different than your modem IP, you don't have to create a modem firewall rule for port 53 in UDP. Just add it for your console you play with

DNS server IP you choose. Check DNS servers on https://public-dns.info/ corresponding to California location, near where Electronic Arts are, with DNS sec enable like the DNS server on IP 72.13.94.130 or 72.13.94.132 or 72.13.94.155 or 72.13.94.133 in San Jose. In this case it's better to set both DNS server IP under DNS setting of your console. In US, as DNS server with DNS sec enable, there is Google DNS with IP 8.8.8.8. But if you live far from US, prefer a DNS server with DNS sec enable from your country. If the server DNS and server to play are far, the IP can be spoofing. I recommend using the DNS server IP with DNS sec enable shown first in the list of your country from the website https://public-dns.info. Download the CSV file to open with Excel. Gameservers/clanservers rent servers for players but open hacked lobbies and allow crack game owners to play with fair players. They are cheaters, hackers and lagers. Their cracked, hacked, cheater infested and full lagging servers use IP spoofing and they also spoof IP of the DNS server you choose. Don't play call of duty because their servers are only own by gameservers/clanservers. But battlefield 1 has EA official servers if not spoof by gameservers/clanservers. Also, always delete save files of your multiplayer games before playing it. If you want to use battlefield 1 server browser, use the following rules under your modem firewall. With local ports 49152-65535, distant port 443 in TCP, distant IP 134.213.244.128 with masks 255.255.255.128 for ports 80 and 10000-10100 in TCP, distant IP 159.153.0.0 with masks 255.255.0.0 for ports 80, 42000-42200 in TCP and ports 10000-10100 in UDP. Use the same game content option as fortnite to show the true names of servers.

7.21. IP spoofing and port stealing problems

Gameservers/clanservers owning lot of servers for playing games doesn't need IP spoofing in order to forward fair players against cheaters in call of duty games, but in battlefield where there are EA official servers, they use IP spoofing. For playing on EA official servers in battlefield or other editor’s official servers in other games, you need to find

distant IP and ports like explained in previous chapters. Set local ports 49152-65535 in your Windows or modem firewalls to avoid port stealing. Also when servers IP are spoofing, it uses your network device MAC address. Under network properties of your consoles and computers, configure manually MAC address. On PC change MAC address under properties of network card, for the value network address by typing the value with 12 numbers between 0-9 and A-F without dots or bars. The two first numbers of MAC address correspond to constructor of network card. When you have a doubt you playing against cheaters on fake servers, change your MAC address. The DNS server you choose must not ne behind a firewall like explained in the previous chapter. Check it with the website https://ping.eu/traceroute/. Create your firewall rules closer as possible to IP and ports of connections. Sometimes you need to restart the game when you search these connections. There are advanced router showing states of IP and ports used, but on PC you can use resource monitor. When you change your MAC address, if you use a wireless network, take care with MAC filtering set on your modem, but prefer to use a wired connection if possible. Have a PC wired to your modem to add new MAC address you changed to the MAC address filtering of your modem for having your consoles or PC you playing connected to network from wireless connection. Take care if you have set static IP to your computers or consoles under DHCP page of your modem, because when you change MAC address, it no more belong and you can't have the same IP. Add again static IP with new MAC address. Maybe you will need to restart your modem. So change firewall rules consequently or don't use static IP (local IP 192.168.1.1 with mask 255.255.255.128 and ports 49152-65535, distant ports 80, 443 in TCP on your modem firewall for your consoles and computers, and local IP 192.168.1.128 with mask 255.255.255.128 and ports 49152-65535, distant ports found playing for your consoles you playing. On your computers, to avoid hackers forward you on fake servers stealing MAC address of the console you playing, I recommend to block distant IP 192.168.1.1 with all ports

in TCP using Windows firewall. Disable it for configure your modem firewall. When you set manually network configuration under your PC and consoles parameters for have internet access, use the sub-network mask 255.255.255.255 instead of the default mask 255.255.255.0. It becomes easier for everyone even kids to hack someone. If one of these kids hates you, he can forward on your devices fake packets you download, like game files, avoiding launch of your game. In order to resolve this problem of game crashing, a DNS sec server is required on your devices. Set manually a DNS server like from Verisign on your devices, and under your modem firewall set for local IP internal IP of your devices with mask 255.255.255.255 and with local port 49152-65535 and distant IP the DNS server IP you choose, with mask 255.255.255.255 and with distant port 53 in TCP/UDP. A DNS sec server will check integrity of network packets you receive and send. If you encounter this problem of game crashing after downloading game files or updates, a full factory reset (without letting installed games and applications) is required to remove this problem. All free games you added through Xbox live gold should be shown under your library. Always let ports 80, 443 in TCP, and port 53 in UDP/TCP, but also IP and ports of Microsoft Azure servers under your modem firewall for a better network connectivity. To avoid computers in your network snitch MAC addresses of your consoles and computers you play, add secure and privacy respectful Verisign DNS server on settings of all your computers, consoles and devices. In regards of MAC addresses change under network settings of your computers and consoles to avoid forward on fake servers of gameservers/clanservers, you can use same MAC addresses on several devices in your network, but take care with MAC filtering security under settings of your modem, prefer to use Ethernet connection instead of Wi-Fi and also you can't use your modem MAC address on your devices (to retrieve modem MAC address use cmd dos prompt command arp –a –v). Only official servers will detect this trick if your devices are online at same time, and fake servers will be duped. Also, under your modem firewall set refusing distant ports 1-65535 in

TCP/UDP for internal IP 192.168.1.128 with mask 255.255.255.128 protecting your consoles against unwanted traffic.

7.22. PC file privacy problems

If you want your files stay private and own rights on it, but you want to play games, you can do the following events. When you aren't connected through internet by unwiring Ethernet and not allowing Wi-Fi connection on your PC, move your sensitive files under a USB hard drive. In System from control panel under the tab system protection, disable drive protection and configure it to remove the saving used. In administrative tool from control panel, use the tool clean drive for removing temp, garbage, internet... files. When you connect to network, don't forget to disconnect your USB hard drive. For having rights on your sensitive files and you don't want it will be lose, if it's for publish later, you have access to DRM (Digital Right Management) with google books publishing with your google account. Change and use a strong password, if you have used this account on unofficial platforms of google. You can disable preview of the books you will create, publishing it by set a date purchase of 2 years after the actual date. It's possible to update books as numerous times as you want with google books publishing. It's well protected and the support is very nice. Sometimes update can bug, but check it and try another time. Put a EULA (End User Licence Agreement) in description. The name of the PDF book file you upload must correspond to the google key given when you add a new book like this: GGKEY(number).

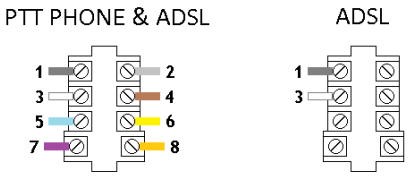
7.23. Playing on PC problems

The most known platform for download and play games is Steam. There are lot of games available but most of games are simple and ugly. All games appearing on the platform aren't reviewed, everyone can publish a game, and a lot of them contain virus not in agreement with your privacy. It destroys your PC slowly and even if you use a firewall, your files can be hacked and corrupted, even transferred through worldwide web. Games can return

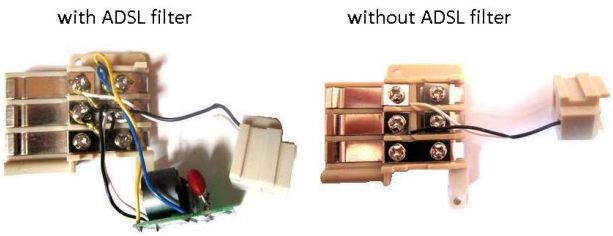
against you the difficulty, freezing the data, using bugs, to make you rage, against your privacy, it adapt the mood of the gameplay if people behind hate you and jealous you. PC is an open platform. Prefer play with Sony, Nintendo and Microsoft instead of Steam because it's all true. If you want to publish a game with Steam, it will do but you will win nothing, only hates of people on the Steam forums. You can publish your game with Xbox game creator from here: https://developer.microsoft.com/fr-fr/games/xbox. There are much more cheaters on games with Steam than on consoles. Also flood memory with NewB doesn't run with games on Steam.

7.24. Internet rate of flow problems

When you want to download games faster, you can remove the capacitors of the internet sockets of your home. Also only two wires are needed to use ADSL (Asymmetric Digital Subscriber Line) like explained with the following picture:



Also, remove ADSL filter from your ADSL socket rewelding the wires or using electric domino like shown by the following picture:



If you encounter disconnections while playing, use a brand new adaptator without removing condensators and also use DNS servers with both primary and auxiliary IP in TCP/UDP for port 53. Otherwise, it’s done (worth it). Also, for better rate of flow connection, the new modems allow 2.4 and 5 GHz Wi-Fi with their own antenna. When you choose a different

SSID for your modem for both Wi-Fi, the security is divided in two parts allowing hiding SSID and with a different WPA2 authentication key. I advice separating your devices with it.

7.25. Xbox One problems

Xbox One has some issues but with its troubleshooting. Games edited by Microsoft and EA have its own servers. IP of azure servers and Microsoft Corporation are listed in the glossary chapter (chapter 8). It's easy to find IP of EA games. Setting under your modem firewall other IP is an issue. Anyone now can hack any device and Xbox One in first place. Hackers can use any computers they hacked to use its IP in order to hack other computers, and so it's easy for them to hack any device. When this is accomplished on your Xbox One, when you download a game or update a game it kept to returning to menu, crashing everytime. It's very annoying to have to always download again the game. The troubleshooting is as following. Use a wired connection. Disable all rules in your modem firewall. Reset to factory your Xbox One without letting games installed. Set under network setting of your Xbox One internal IP above 192.168.1.128, mask 255.255.255.255 if your modem gateway is 192.168.1.1, primary DNS 64.6.64.6, secondary DNS 64.6.65.6. Change MAC address of your Xbox One. Add the following rules to your modem firewall. Internal IP 192.168.1.128, mask 255.255.255.128, local ports 49152-65535, distant ports 80 and 443 in TCP, and Internal IP 192.168.1.128, mask 255.255.255.128, local ports 49152-65535, distant IP 64.6.65.6, distant mask 255.255.255.255, distant ports 53 in UDP (add same rules with local ports its distant ports). Add static internal IP for your Xbox One under DHCP properties of your modem. Then for your other devices create modem firewall rule. Internal IP 192.168.1.1, mask 255.255.255.128, distant ports 1-1023 in TCP. You can add under your modem firewall specific IP and ports of game connections and servers when this is in place. Another issue is time of download when it always cut connections. For this, create three NAT/PAT rules associated with internal IP of your console, for port 80, 443 in TCP and port

53 in UDP. But take care to have local ports 49152-65535 in rules under your modem firewall for internal IP of your Xbox One. With Android devices, local ports don't allow internet connection. To add to troubleshooting, when you reset your Xbox One, set your language to English and region to United State because language pack to download if you change language will be modified by hackers, and region other than origin of your Xbox One don't ensure privacy and safety claimed by Xbox One constructor. You can buy with your Microsoft account by loading it with money from Microsoft website here: https://www.microsoft.com/fr-fr/store/b/gift-cards?rtc=1, buying a gift card, or add an option for paying here:

https://account.microsoft.com/billing/payments?refd=account.microsoft.com#/?state=add,

with your country billing information, or buy games directly from here: https://www.xbox.com/fr-FR/games/xbox-one, if you are logged with your Xbox account. You can let language set to English (US) and change region set to your region only when buying a game under your console, otherwise the language package can destroy it. If you encounter problem with loading map or problem with unable to connect to servers, instead of quitting game, you can disconnect the RJ45 wire and reconnect it from your Xbox, but if you use wireless network, you can temporary disable your console from MAC filtering under your modem. Also it's quicker and easier to reset Xbox than a PC.

7.26. Free of cheaters and low latency problems

Developers of BO3 claims free of cheaters but even bots are cheated and cheating. They use the port 3074 allowing all inbound traffic with all ports if you create a NAT/PAT rule whereas this port is required for playing with outbound traffic forwarding to hacked lobbies in their game. The inbound traffic can be useful to check if you don't cheat and so server you will play would be free of cheaters. Use firewall rules by adding local ports 53, 80, 443 for distant ports 53, 80, 443 and local ports 49152-65535 for distant ports 53, 80, 443.

Use NAT/PAT rules by adding internal port 10000 and external ports 10000-10100 for example. The following pictures illustrate how to do for BF1 and Fortnite:

application / service	port interne	port externe	protocole	appareil
53	53	53	UDP	PC42
10000	10000-10100	10000-10100	les deux	PC42
42000	42000-42200	42000-42200	TCP	PC42
Secure Web Server (HTTPS)	443	443	TCP	PC42
Web Server (HTTP)	80	80	TCP	PC42
5000	5222-9222	5222-9222	UDP	PC42

application / service	protocole	adresse IP source	masque adresse IP	port source	adresse IP destination	masque adresse IP	port destination
HTTP	TCP	192.168.1.128	255.255.255.128	49152-65535			80
HTTPS	TCP	192.168.1.128	255.255.255.128	49152-65535			443
DNS	UDP	192.168.1.128	255.255.255.128	49152-65535	64.6.65.6	255.255.255.255	53
1-1023	TCP	192.168.1.16	255.255.255.255				1-1023
steam	TCP	192.168.1.13	255.255.255.255	49152-65535			1-1023
3544	TCP	192.168.1.23	255.255.255.255	49152-65535			1-1023
3074	UDP	192.168.1.128	255.255.255.128	5222-9222			5222-9222
ms	UDP	192.168.1.128	255.255.255.128	49152-65535			5222-9222
bf7	UDP	192.168.1.128	255.255.255.128	53	64.6.65.6	255.255.255.255	53
bf1	TCP	192.168.1.128	255.255.255.128	80			80
bf3	TCP	192.168.1.128	255.255.255.128	49152-65535	159.153.0.0	255.255.0.0	42000-42200
bf4	UDP	192.168.1.128	255.255.255.128	49152-65535	159.153.0.0	255.255.0.0	10000-10100
bf6	TCP	192.168.1.128	255.255.255.128	42000-42200	159.153.0.0	255.255.0.0	42000-42200
bf8	TCP	192.168.1.128	255.255.255.128	49152-65535	134.213.244.128	255.255.255.128	10000-10100
bf9	TCP	192.168.1.128	255.255.255.128	10000-10100	134.213.244.128	255.255.255.128	10000-10100
bf5	UDP	192.168.1.128	255.255.255.128	10000-10100	159.153.0.0	255.255.0.0	10000-10100
bf2	TCP	192.168.1.128	255.255.255.128	443			443

Even if call of duty games aren't anymore on steam platform, it's still gameservers/clanservers servers full of cheaters. If you don't cheat or use script on battlefield 1 on Xbox, you will not encounter any cheaters. The game call of duty black ops 2 is full of cheaters even on Xbox with game compatibility. Developers have their responsibility against cheaters. If they like cheating, game is infested with cheaters, but if they don't like cheating, the game is free of cheaters, but it needs to play on official servers. You can play on official

servers of battlefield 1 free of cheaters and low latency with the following few rules (it allows to browse internet and use outlook on every platforms). Test the two methods to see the difference and make mixing rules between them if you don't see any difference. Allowing ports 1-1023 increase latency. The following rules normally are the best to play. If games need to allow all IP for a port scale, it's not a decent game which deserves to be played.

application / service	protocole	adresse IP source	masque adresse IP	port source	adresse IP destination	masque adresse IP	port destination
HTTP	TCP			1024-65535			80
HTTPS	TCP			1024-65535			443
POP3	TCP			1024-65535			110
POP3S	TCP			1024-65535			995
SMTPAuth	TCP			1024-65535			587
SMTP	TCP			1024-65535			25
FTP	TCP			1024-65535			20-22
NTP	TCP			1024-65535			123
NNTP	TCP			1024-65535			119
WINS	TCP			1024-65535			42
IMAP	TCP			1024-65535			143
IMAPS	TCP			1024-65535			993
ISAKMP	TCP			1024-65535			500
IPSEC-NAT-T	TCP			1024-65535			4500
bf6	les deux			49152-65535	159.153.0.0	255.255.0.0	1024-49151
bf8	TCP			49152-65535	134.213.244.0	255.255.255.0	1024-49151
bf4	les deux			1024-65535	64.6.65.6	255.255.255.255	53
bf1	les deux			1024-65535	64.6.64.6	255.255.255.255	53

7.27. Windows 10 problems

Disable Cortana completely: Win+R, type cmd, Ctrl + Shift + Enter, and the command will run elevated, but if it doesn't run, you can open task manager with ctrl+shift+esc, for open location of cmd, click right on the file, and then choose to run it with administrative privilege. In CMD prompt command, type cd .., and then press Enter, it will show C:/Windows, then type cd systemapps, it will show C:/Windows/SystemApps, and then copy this: REN Microsoft.Windows.Cortana_cw5n1h2txyewy Microsoft.Windows.Cortana_cw5n1h2txyewy.bak, and then in task manager stop the task SearchUi.exe, as soon as you did it, press enter for the command in CMD. Disable Windows Defender: Open the Run command with Win+R, type regedit, create the following key DisableAntiSpyware 1 (DWORD 32 bits) in, HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender. Disable fast start by typing in run (Windows + R) %windir%\system32\control.exe /name Microsoft.PowerOptions /page pageGlobalSettings, then click on modify unavailable settings. For browsing web with Microsoft Edge on Windows 10 with last updates, you have to create a Windows firewall rule for application packages.

7.28. USB store device in read only mode problems

Follow the following steps if your USB store device is in read only mode after the problem occurred. On windows choose analyse and repair device when you plug it, and then after eject it. It's dangerous for a store device plugged in a PC starting.

7.29. Finding server IP problems

You can use the following subnet masks for find IP of connection under a modem testing to have connection. Proceed by dichotomy. Sometimes it needs to restart the game.

CIDR	Subnet Mask	Total IPs	Usable IPs
/32	255.255.255.255	1	1
/31	255.255.255.254	2	0
/30	255.255.255.252	4	2
/29	255.255.255.248	8	6

/28	255.255.255.240	16	14
/27	255.255.255.224	32	30
/26	255.255.255.192	64	62
/25	255.255.255.128	128	126
/24	255.255.255.0	256	254
/23	255.255.254.0	512	510
/22	255.255.252.0	1024	1022
/21	255.255.248.0	2048	2046
/20	255.255.240.0	4096	4094
/19	255.255.224.0	8192	8190
/18	255.255.192.0	16,384	16,382
/17	255.255.128.0	32,768	32,766
/16	255.255.0.0	65,536	65,534
/15	255.254.0.0	131,072	131,070
/14	255.252.0.0	262,144	262,142
/13	255.248.0.0	524,288	524,286
/12	255.240.0.0	1,048,576	1,048,574
/11	255.224.0.0	2,097,152	2,097,150
/10	255.192.0.0	4,194,304	4,194,302
/9	255.128.0.0	8,388,608	8,388,606
/8	255.0.0.0	16,777,216	16,777,214
/7	254.0.0.0	33,554,432	33,554,430
/6	252.0.0.0	67,108,864	67,108,862
/5	248.0.0.0	134,217,728	134,217,726
/4	240.0.0.0	268,435,456	268,435,454
/3	224.0.0.0	536,870,912	536,870,910
/2	192.0.0.0	1,073,741,824	1,073,741,822
/1	128.0.0.0	2,147,483,648	2,147,483,646
/0	0.0.0.0	4,294,967,296	4,294,967,294

If you have an IPv6 connection use websites like

https://www.subnetonline.com/pages/subnet-calculators/ipv4-to-ipv6-converter.php to convert

IPv4 IP to IPv6 IP. The subnet mask for IPv6 are corresponding like following :

IPv6 CIDR Subnet	Number of IPs
/128	1
/127	2
/126	4
/125	8
/124	16
/123	32
/122	64
/121	128
/120	256
/119	512
/118	1,024
117	2,048
116	4,096
/115	8,192
/114	16,384
/113	32,768
/112	65,536
/111	131,072
/110	262,144
/109	524,288
/108	1,048,576
/107	2,097,152
/106	4,194,304
/105	8,388,608
/104	16,777,216
/103	33,554,432
/102	67,108,864
/101	134,217,728

/100	268,435,456
/99	536,870,912
/98	1,073,741,824
/97	2,147,483,648
/96	4,294,967,296
/95	8,589,934,592
/94	17,179,869,184
/93	34,359,738,368
/92	68,719,476,736
/91	137,438,953,472
/90	274,877,906,944
/89	549,755,813,888
/88	1,099,511,627,776
/87	2,199,023,255,552
/86	4,398,046,511,104
/85	8,796,093,022,208
/84	17,592,186,044,416
/83	35,184,372,088,832
/82	70,368,744,177,664
/81	140,737,488,355,328
/80	281,474,976,710,656
/79	562,949,953,421,312
/78	1,125,899,906,842,624
/77	2,251,799,813,685,248
/76	4,503,599,627,370,496
/75	9,007,199,254,740,992
/74	18,014,398,509,481,985
/73	36,028,797,018,963,968
/72	72,057,594,037,927,936
/71	144,115,188,075,855,872
/70	288,230,376,151,711,744
/69	576,460,752,303,423,488
/68	1,152,921,504,606,846,976
/67	2,305,843,009,213,693,952
/66	4,611,686,018,427,387,904
/65	9,223,372,036,854,775,808
/64	18,446,744,073,709,551,616
/63	36,893,488,147,419,103,232
/62	73,786,976,294,838,206,464
/61	147,573,952,589,676,412,928
/60	295,147,905,179,352,825,856
/59	590,295,810,358,705,651,712
/58	1,180,591,620,717,411,303,424
/57	2,361,183,241,434,822,606,848
/56	4,722,366,482,869,645,213,696
/55	9,444,732,965,739,290,427,392
/54	18,889,465,931,478,580,854,784
/53	37,778,931,862,957,161,709,568
/52	75,557,863,725,914,323,419,136
/51	151,115,727,451,828,646,838,272
/50	302,231,454,903,657,293,676,544
/49	604,462,909,807,314,587,353,088
/48	1,208,925,819,614,629,174,706,176
/47	2,417,851,639,229,258,349,412,352
/46	4,835,703,278,458,516,698,824,704
/45	9,671,406,556,917,033,397,649,408
/44	19,342,813,113,834,066,795,298,816
/43	38,685,626,227,668,133,590,597,632
/42	77,371,252,455,336,267,181,195,264
/41	154,742,504,910,672,534,362,390,528
/40	309,485,009,821,345,068,724,781,056
/39	618,970,019,642,690,137,449,562,112
/38	1,237,940,039,285,380,274,899,124,224
/37	2,475,880,078,570,760,549,798,248,448
/36	4,951,760,157,141,521,099,596,496,896
/35	9,903,520,314,283,042,199,192,993,792
/34	19,807,040,628,566,084,398,385,987,584

/33	39,614,081,257,132,168,796,771,975,168
/32	79,228,162,514,264,337,593,543,950,336
/31	158,456,325,028,528,675,187,087,900,672
/30	316,912,650,057,057,350,374,175,801,344
/29	633,825,300,114,114,700,748,351,602,688
/28	1,267,650,600,228,229,401,496,703,205,376
/27	2,535,301,200,456,458,802,993,406,410,752
/26	5,070,602,400,912,917,605,986,812,821,504
/25	10,141,204,801,825,835,211,973,625,643,008
/24	20,282,409,603,651,670,423,947,251,286,016
/23	40,564,819,207,303,340,847,894,502,572,032
/22	81,129,638,414,606,681,695,789,005,144,064
/21	162,259,276,829,213,363,391,578,010,288,128
/20	324,518,553,658,426,726,783,156,020,576,256
/19	649,037,107,316,853,453,566,312,041,152,512
/18	1,298,074,214,633,706,907,132,624,082,305,024
/17	2,596,148,429,267,413,814,265,248,164,610,048
/16	5,192,296,858,534,827,628,530,496,329,220,096
/15	10,384,593,717,069,655,257,060,992,658,440,192
/14	20,769,187,434,139,310,514,121,985,316,880,384
/13	41,538,374,868,278,621,028,243,970,633,760,768
/12	83,076,749,736,557,242,056,487,941,267,521,536
/11	166,153,499,473,114,484,112,975,882,535,043,072
/10	332,306,998,946,228,968,225,951,765,070,086,144
/9	664,613,997,892,457,936,451,903,530,140,172,288
/8	1,329,227,995,784,915,872,903,807,060,280,344,576

7.30. Internet browser problems

With internet, you can use specific Windows firewall rules, ports 80 and 443 in TCP and port 53 or 433 in UDP for the client DNS service, setting the internal IP of your computer and DNS server IP under network settings. Use Adblock plugin for firefox under firefox, but not Adblock plus too invasive for your privacy and not under chrome by google because google don't like you block their sources of money. Adblock can block lot of annoying things like youtube publicities. If you open a hacker web site, often there a window popping when you must click to make disappear the window, it's often a hack. So don't click but use task manager to end all tasks in relation with your web browser you using opening the hacker web site. It will close your internet browser without danger.

7.31. Being competitive in black ops II multiplayer problems

Playing on PC with black ops I, II, III isn't enjoyable because of big noobs cheating under steam platform with the help of gameservers/clanservers opening hacked lobbies. Flooding the game memory, with the codes presented in this book, while playing isn't a solution for being competitive. But now black ops IV edited by activsion and developed

always by treyarch is on blizzard platform, and use their servers. Games like fortnite, pubg or battlefield still use or now use p2p servers and so everyone can open hacked lobbies, so these games don't deserve to be played. On Xbox One you can use these following rules under your modem firewall for playing on official servers of black ops IV.

Application/Service	Protocole	Adresse IP source	Masque sous réseau	Port source	Adresse IP destination	Masque sous réseau	Port destination	Action
all1	UDP	192.168.1.0	255.255.255.128	1024-65535			53	accepter
all2	TCP	192.168.1.0	255.255.255.128	1024-65535			1-1023	accepter
cod1	Les deux	192.168.1.209	255.255.255.255	1024-65535	209.170.124.0	255.255.255.0	1024-49151	accepter
cod6	Les deux	192.168.1.209	255.255.255.255	1024-65535	24.105.0.0	255.255.192.0	1024-49151	accepter
cod2	Les deux	192.168.1.209	255.255.255.255	1024-65535	185.34.104.0	255.255.252.0	1024-49151	accepter
cod3	UDP	192.168.1.209	255.255.255.255	49152-65535	208.67.222.222	255.255.255.255	53	accepter
cod4	TCP	192.168.1.209	255.255.255.255	49152-65535			443	accepter
cod5	TCP	192.168.1.209	255.255.255.255	49152-65535			80	accepter

But instead of Norton doing nothing against IP spoofing use the DNS of OpenDNS (see chapter 4.3 for setting OpenDNS). In abstract block all categories, set maximum security features, and add the following rules under your OpenDNS dashboard.

ALWAYS BLOCK:

amazonaws.com, amazontrust.com, atwola.com, crl3.digicert.com, crl4.digicert.com, de, dns.msftncsi.com, globalsign.com, goog, mixer.com, ms, msftconnecttest.com, msftncsi.com, net, ocsp.digicert.com, ocsp.msocsp.com, rapidssl.com, s-microsoft.com, twimg.com, us, xboxab.com.

NEVER BLOCK:

cloudfront.net, demonware.net, login.live.com, microsoft.com, storage.live.com, xboxlive.com.

Add to block rules if it's not a domain name finishing by net. Also, if it's not already added to categories. Add to allow rules if domain name finish by net. Also, if it's added to categories.

Don't forget to reload new IP of your network under OpenDNS dashboard if your modem restarts. Delete save files under game management of your consoles if you encounter problems, and change DNS IP under your modem firewall with the rule for port 53 in UDP and under network settings of your consoles. You can find information on domain names you need to block or allow with the cmd dos prompt command as example nslookup netflix.com for retrieve netflix.com.Broadcom.net. OpenDNS dashboard can retrieve stats and logs on domain name requests. If you want to update or download games, add firewall rules for port 80 and 443 in TCP and port 53 in UDP, and change network settings under your consoles with DNS IP 64.6.64.6. Don’t forget to check if your SSID of your Wifi connection is hidden if you have 2 types of Wifi (see chapter 7.24). If you don’t have connection when starting your consoles, make a connection test under network settings, and then you will be connected. But if you encounter too much problems with DNS server of OpenDNS, delete save files and use the following settings with both secure DNS servers of Verisign and Google.

Application/Service	Protocole	Adresse IP source	Masque sous réseau	Port source	Adresse IP destination	Masque sous réseau	Port destination	Action
all1	UDP	192.168.1.0	255.255.255.128	1024-65535			53	accepter
all2	TCP	192.168.1.0	255.255.255.128	1024-65535			1-1023	accepter
cod1	Les deux	192.168.1.209	255.255.255.255	1024-65535	209.170.124.0	255.255.255.0	1024-49151	accepter
cod6	Les deux	192.168.1.209	255.255.255.255	1024-65535	24.105.0.0	255.255.192.0	1024-49151	accepter
cod2	Les deux	192.168.1.209	255.255.255.255	1024-65535	185.34.104.0	255.255.252.0	1024-49151	accepter
cod4	TCP	192.168.1.209	255.255.255.255	49152-65535			443	accepter
cod3	Les deux	192.168.1.209	255.255.255.255	49152-65535	64.6.64.6	255.255.255.255	53	accepter
cod5	Les deux	192.168.1.209	255.255.255.255	49152-65535	8.8.8.8	255.255.255.255	53	accepter

Or maybe set the default DNS server (IP 192.168.1.1 for me) corresponding to your internet provider and see with them why you are forwarded on hacked lobbies full lagging and bugged, in a broken game full of cheaters making your anti-virus alerting every time malware IP intrusions, using only the following rules.

Application/Service	Protocole	Adresse IP source	Masque sous réseau	Port source	Adresse IP destination	Masque sous réseau	Port destination	Action
cod1	Les deux	192.168.1.209	255.255.255.255	1024-65535	209.170.124.0	255.255.255.0	1024-49151	accepter
cod6	Les deux	192.168.1.209	255.255.255.255	1024-65535	24.105.0.0	255.255.192.0	1024-49151	accepter
cod2	Les deux	192.168.1.209	255.255.255.255	1024-65535	185.34.104.0	255.255.252.0	1024-49151	accepter
cod4	TCP	192.168.1.209	255.255.255.255	49152-65535			443	accepter
DNS	Les deux						53	accepter
all	TCP	192.168.1.0	255.255.255.128	1024-65535			1-1023	accepter

Like OpenDNS, Comodo Dome Shield, can block domains. There is a whitelist and an option to block all domains but not domains in white list. What you can do, is set to maximum security the policy security rules, and when you search a match, you can enable the mode for domain accepted in only white list. It's because there are cheaters forwarding you on hacked lobbies after the first match. Enable only one category and only one domain you choose in white list, be imaginative, you can set a domain which not exist. It's because the free account is limited in term of requests. Disable the mode after playing. Comodo DNS IP for Dome Shield: 8.26.56.10 – 8.20.247.10, https://shield.dome.comodo.com. But the only convenient solution is using the following rules and delete both rules with ports 80 and 443 in TCP after authentication into the game.

Application/Service	Protocole	Adresse IP source	Masque sous réseau	Port source	Adresse IP destination	Masque sous réseau	Port destination	Action
cod1	Les deux	192.168.1.209	255.255.255.255	1024-65535	209.170.124.0	255.255.255.0	1024-49151	accepter
cod6	Les deux	192.168.1.209	255.255.255.255	1024-65535	24.105.0.0	255.255.192.0	1024-49151	accepter
cod2	Les deux	192.168.1.209	255.255.255.255	1024-65535	185.34.104.0	255.255.252.0	1024-49151	accepter
all	TCP	192.168.1.0	255.255.255.128	1024-65535			1-1023	accepter
dns	UDP	192.168.1.0	255.255.255.128	1024-65535			53	accepter
cod3	UDP	192.168.1.209	255.255.255.255	49152-65535	192.168.1.1	255.255.255.255	443	accepter
HTTP	TCP						80	accepter
HTTPS	TCP						443	accepter

From https://eu.battle.net/support/en/article/7870 and https://bgpview.io/, other IP of Blizzard servers are 185.60.112.0/255.255.252.0, 103.4.114.0/255.255.254.0, 137.221.64.0/255.255.224.0, 137.221.96.0/255.255.248.0, 137.221.104.0/255.255.252.0. But the exact IP for playing black ops 4 on Xbox One are 24.105.52.0 to 24.105.54.255. So three

ranges of IP with masks 255.255.255.0. If you divide these ranges with masks 255.255.255.128, no match is found. But with each range, you find a match. If you still encounter cheaters, each time you see they invade your matches, after have enabled once Xbox home main console under your Xbox One, under console personalization, you can use a new brand account with a new brand Microsoft account under hotmail, creating a new email address. You can create new accounts directly from your Xbox One. Your main account will share Xbox Live Gold, with your new accounts. Set again maximum of online security under online privacy and safety, but allow join multiplayer game and user creation content. Set again your black ops 4 view and ADS sensitivity and other parameters you prefer, like gamepad vibration off for example. The last solution is to block IP above 209.170.124.179 because this IP is detected by NewB as an IP of server behind a modem/router allowing spoofing official servers IP. Use the following rules under your modem firewall.

Application/Service	Protocole	Adresse IP source	Masque sous réseau	Port source	Adresse IP destination	Masque sous réseau	Port destination
all	TCP	192.168.1.0	255.255.255.128	1024-65535			1-1023
dns	UDP	192.168.1.0	255.255.255.128	1024-65535			53
ea5	TCP	192.168.1.209	255.255.255.255	49152-65535			443
cod2	Les deux	192.168.1.209	255.255.255.255	1024-65535	24.105.52.0	255.255.255.0	1024-49151
dns6	UDP	192.168.1.209	255.255.255.255	49152-65535	8.26.56.10	255.255.255.255	53
dns7	UDP	192.168.1.209	255.255.255.255	49152-65535	8.20.247.10	255.255.255.255	53
cod3	Les deux	192.168.1.209	255.255.255.255	1024-65535	185.34.104.0	255.255.252.0	1024-49151
cod4	Les deux	192.168.1.209	255.255.255.255	1024-65535	209.170.124.0	255.255.255.128	1024-49151
cod5	Les deux	192.168.1.209	255.255.255.255	1024-65535	209.170.124.128	255.255.255.224	1024-49151
cod6	Les deux	192.168.1.209	255.255.255.255	1024-65535	209.170.124.160	255.255.255.240	1024-49151
cod7	Les deux	192.168.1.209	255.255.255.255	1024-65535	209.170.124.176	255.255.255.254	1024-49151
cod8	Les deux	192.168.1.209	255.255.255.255	1024-65535	209.170.124.178	255.255.255.255	1024-49151

But deeply there are these following rules because NewB can’t detect all IP spoofed.

Application/Service	Protocole	Adresse IP source	Masque sous réseau	Port source	Adresse IP destination	Masque sous réseau	Port destination
all	TCP	192.168.1.0	255.255.255.128	1024-65535			1-1023
dns	UDP	192.168.1.0	255.255.255.128	1024-65535			53
cod1	Les deux	192.168.1.209	255.255.255.255	49152-65535	209.170.124.117	255.255.255.255	3074
cod3	TCP	192.168.1.209	255.255.255.255	49152-65535			443
cod2	UDP	192.168.1.209	255.255.255.255	3074-3076	24.105.52.0	255.255.255.0	5001-49151
cod5	Les deux	192.168.1.209	255.255.255.255	3074-3076	185.34.107.238	255.255.255.255	3074-3076
cod7	Les deux	192.168.1.209	255.255.255.255	3074-3076	185.34.107.237	255.255.255.255	3074-3076
cod8	TCP	192.168.1.209	255.255.255.255	49152-65535	185.34.107.238	255.255.255.255	3074-3076
cod9	TCP	192.168.1.209	255.255.255.255	49152-65535	185.34.107.237	255.255.255.255	3074-3076
cod10	Les deux	192.168.1.209	255.255.255.255	3074-3076	185.34.107.128	255.255.255.255	3074-3076
cod11	TCP	192.168.1.209	255.255.255.255	49152-65535	185.34.107.128	255.255.255.255	3074-3076

7.32. A DNS server against spoofed servers IP problems

The previous chapter presenting only few IP for playing black ops 4 don't ensure completely to not be forwarded on hacked lobbies opened by gameservers/clanservers, because with a bad internet provider like Orange or a bad DNS server, IP of servers can be spoofed. I tried intensively OpenDNS, Comodo, and Orange DNS but I was always fighting against cheaters in the game. The DNS of Quad9 with IP 9.9.9.9 seems to achieve what I wanted to do, i.e. to not be forwarded on fake servers using same IP of official servers. Check their website for more information about this organization and like me, make donations. I let you by yourself discover why they have a good DNS server.

7.33. Cut of download problems

To prevent cut of download on Xbox One, because it happens when one of your computer under your network is hacked with remote connection, wire your consoles and use invite Wi-Fi for your other devices, and also take example with the following modem firewall rules (DNS server IP used is 1.0.0.1 from Cloudflare, here).

Application/Service	Protocole	Adresse IP source	Masque sous réseau	Port source	Adresse IP destination	Masque sous réseau	Port destination
x2	TCP	192.168.1.23	255.255.255.255	49152-65535			443
x1	TCP	192.168.1.23	255.255.255.255	49152-65535			80
p1	TCP	192.168.1.10	255.255.255.255	49152-65535			80
p2	TCP	192.168.1.10	255.255.255.255	49152-65535			443
p3	TCP	192.168.1.10	255.255.255.255	49152-65535			110
p4	TCP	192.168.1.10	255.255.255.255	49152-65535			995
p5	TCP	192.168.1.10	255.255.255.255	49152-65535			20-22
p6	UDP	192.168.1.10	255.255.255.255	49152-65535	64.6.64.6	255.255.255.255	53
p7	TCP	192.168.1.10	255.255.255.255	49152-65535			587
p8	TCP	192.168.1.10	255.255.255.255	49152-65535			25
x5	Les deux	192.168.1.23	255.255.255.255	3074-3076	185.34.107.237	255.255.255.254	3074-3076
x7	Les deux	192.168.1.23	255.255.255.255	3074-3076	185.34.107.128	255.255.255.255	3074-3076
x9	TCP	192.168.1.23	255.255.255.255	49152-65535	185.34.107.0	255.255.255.0	3074-3076
x13	Les deux	192.168.1.23	255.255.255.255	49152-65535	209.170.124.117	255.255.255.255	3074
x11	UDP	192.168.1.23	255.255.255.255	3075	24.105.54.0	255.255.255.0	30000-40000
x3	Les deux	192.168.1.23	255.255.255.255	1-65535	1.0.0.1	255.255.255.255	1-65535

And if you share connection, take also example on the following rules for the computer host (chapter 7.17). Also, if you flood a process memory under host computer for anti-cheating, I advice the process wlanext or lsass or system or the process with the PID associate to the service distance access connection manager (svchost) or associate to the service client DNS or ICS (Internet Connection Sharing). Take care, because there is a service with almost similar name but containing the word automatic (the service to flood is a service host: local system shown in task manager). Don't forget to disable data execution prevention on your computer host with the cmd dos prompt command: bcdedit.exe /set nx AlwaysOff, and restart your computer. Launch NewB flood when you enter your first match for flooding more pertinent memory addresses.

Application/Service	Protocole	Adresse IP source	Masque sous réseau	Port source	Adresse IP destination	Masque sous réseau	Port destination
x2	TCP	192.168.1.23	255.255.255.255	49152-65535			443
x1	TCP	192.168.1.23	255.255.255.255	49152-65535			80
p1	TCP	192.168.1.10	255.255.255.255	49152-65535			80
p2	TCP	192.168.1.10	255.255.255.255	49152-65535			443
p3	TCP	192.168.1.10	255.255.255.255	49152-65535			110
p4	TCP	192.168.1.10	255.255.255.255	49152-65535			995
p5	TCP	192.168.1.10	255.255.255.255	49152-65535			20-22
p6	UDP	192.168.1.10	255.255.255.255	49152-65535	64.6.64.6	255.255.255.255	53
p7	TCP	192.168.1.10	255.255.255.255	49152-65535			587
p8	TCP	192.168.1.10	255.255.255.255	49152-65535			25
x3	UDP	192.168.1.23	255.255.255.255	49152-65535	1.0.0.1	255.255.255.255	53
x6	Les deux	192.168.1.23	255.255.255.255	3074-3076	185.34.107.0	255.255.255.0	3074-3076
x5	Les deux	192.168.1.23	255.255.255.255	49152-65535	209.170.124.0	255.255.255.0	3074
x4	Les deux	192.168.1.23	255.255.255.255	49152-65535	185.34.107.0	255.255.255.0	3074-3076
x7	UDP	192.168.1.23	255.255.255.255	49152-65535	24.105.0.0	255.255.192.0	5001-49151

Sometimes games won't download, so it's recommended by Microsoft when you click on the game update stopping downloaded to reboot from refresh your Xbox One. You need to cancel download and download again entirely the game.

7.34. Hacked lobbies problems

Firstly is to play on XBox One, and use connection sharing from a secure computer host only allowing IP of DNS server for the service client DNS and protocols HTTP and HTTPS for your favourite web browser under Windows firewall. Normally the service dacm will go through firewall as shown under properties of Windows firewall if your computer host is up to date. Secondly, to avoid any cut of download and hacked lobbies in black ops 4 playing MME, use the following rules as example.

Application/Service	Protocole	Adresse IP source	Masque sous réseau	Port source	Adresse IP destination	Masque sous réseau	Port destination
p1	TCP	192.168.1.10	255.255.255.255	49152-65535			80
p2	TCP	192.168.1.10	255.255.255.255	49152-65535			443
p3	TCP	192.168.1.10	255.255.255.255	49152-65535			110
p4	TCP	192.168.1.10	255.255.255.255	49152-65535			995
p5	TCP	192.168.1.10	255.255.255.255	49152-65535			20-22
p6	UDP	192.168.1.10	255.255.255.255	49152-65535	64.6.64.6	255.255.255.255	53
p7	TCP	192.168.1.10	255.255.255.255	49152-65535			587
p8	TCP	192.168.1.10	255.255.255.255	49152-65535			25
x9	UDP	192.168.1.23	255.255.255.255	49152-65535	185.34.107.128	255.255.255.255	3074-3076
x6	UDP	192.168.1.23	255.255.255.255	3074-3076	185.34.107.128	255.255.255.255	3074-3076
x8	TCP	192.168.1.23	255.255.255.255	3074-3076	185.34.107.0	255.255.255.0	3074-3076
x4	TCP	192.168.1.23	255.255.255.255	49152-65535	185.34.107.0	255.255.255.0	3074-3076
x2	TCP	192.168.1.23	255.255.255.255	49152-65535			443
x7	UDP	192.168.1.23	255.255.255.255	49152-65535	24.105.54.0	255.255.255.0	5001-49151
x5	UDP	192.168.1.23	255.255.255.255	49152-65535	64.6.64.6	255.255.255.255	53
x1	TCP	192.168.1.23	255.255.255.255	49152-65535			80

Normally when you block a cheater, you will not meet it a second time. See how to share connection set a DNS server and set Windows firewall properties with above chapters. Also flush DNS with following website

https://www.verisign.com/en_GB/security-services/public-dns/dns-cache/index.xhtml

for domain names cloudfront.net, demonware.net, login.live.com, microsoft.com, storage.live.com, xboxlive.com.

7.35. VPN on Xbox One problems

In the chapter 7.17. I explain how to share connection from a host computer for the Xbox One. If you have a W10 OS computer, it's possible to use a VPN server to make a secure connection for your Xbox One. Under Parameters of your computer host, under VPN

you can set information for VPN server (a proxy server doesn't secure your Xbox One but VPN do it). Try the last information from this list (but before you need to allow all protocols for all Windows services for outbound traffic under Windows firewall, whereas no additional rules are needed under your modem firewall compared to above chapter's explanations):

https://freevpn.eu/accounts/

PPTP

IP: server7-nl.freevpn.eu

Username: freevpn.eu

Password: 7FAopyCIe1oA

L2TP/IPSec (PSK)

IP: server7-nl.freevpn.eu

Username: freevpn.eu

Password: 7FAopyCIe1oA

Shared Secret (PSK): freevpn.eu

OpenVPN

Username: freevpn.eu

Password: 7FAopyCIe1oA

TCP 80, 443

UDP 53, 40000

Unlimited Bandwidth

Torrents Allowed

No Logging

https://www.vpnbook.com/freevpn

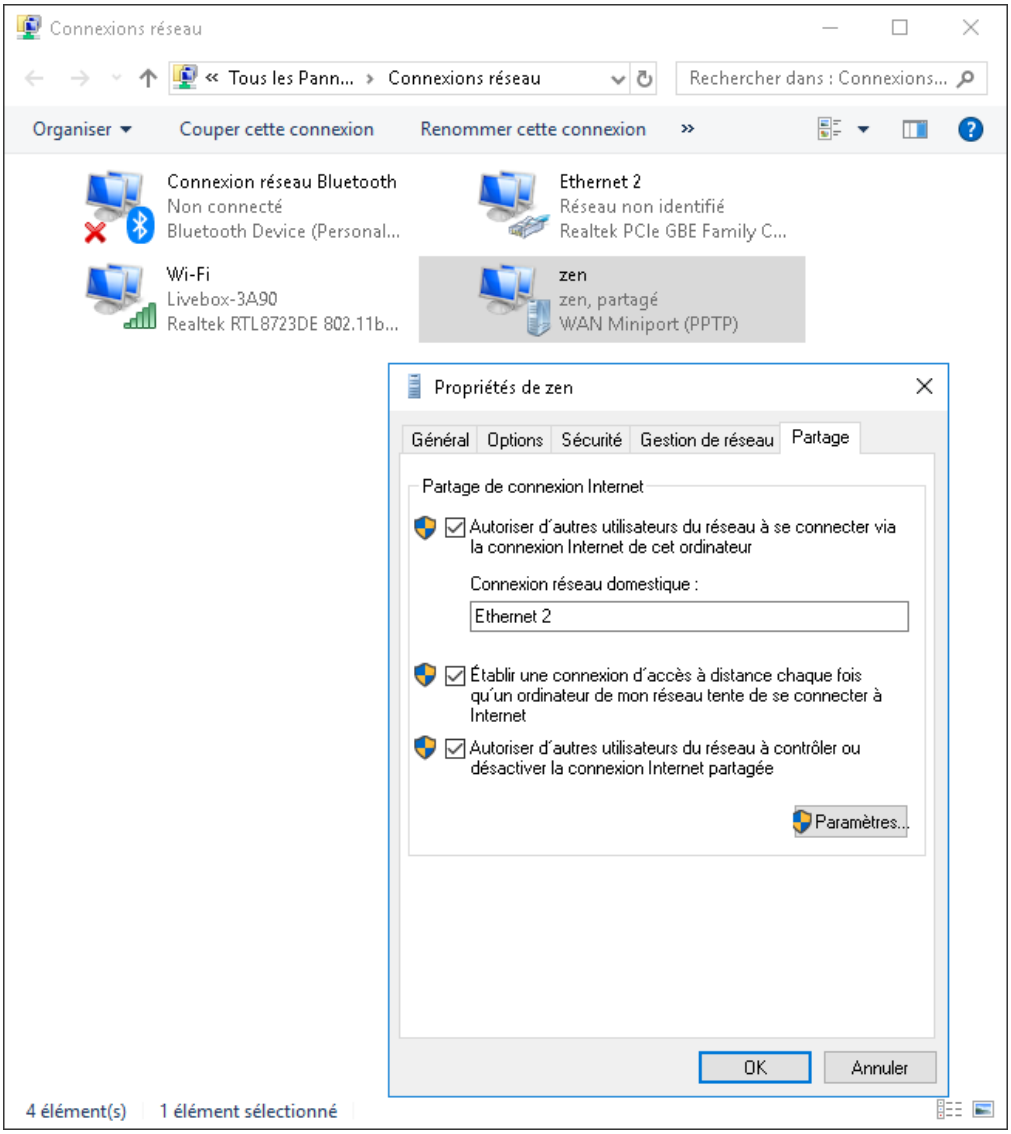
PL226.vpnbook.com

DE4.vpnbook.com

Username: vpnbook

Password: 9zszrs8 (the password change sometimes)

Normally you can browse internet with your favourite web browser after connection to the VPN you created with these information. Then, you can share connection with same settings than with normal connection sharing under Xbox One network settings, but you need to allow connection sharing with the network VPN adapter from network connection page of your computer host. If you don’t set a DNS server like Verisign (64.6.64.6, 64.6.65.6) instead of your ISP DNS server, you can encounter problem of disconnection. Set DNS server under ipv4 properties of your Wi-Fi card and of your Ethernet card under your computer host. Also change DNS server under network properties of your console. Also, to avoid disconnection, set options of VPN under parameters, like it's a PPTP network type and detect automatically settings of the VPN connection. And also, change advanced options under control panel (Windows + R), like under battery options, don't shut down hard drive, or under screensaver, don't shut down screen with restart lock screen, because it shut down network cards. If you encounter problem to have connection after restarting your computer host, enable VPN each time under parameters of your computer host, and change the allow connection sharing from Wi-Fi card properties to VPN card properties like shown in the following picture.



When using this method with VPNbook, it doesn't need any rules under your modem firewall to have connection from your computer host to your console. And it protects against fake servers spoofing IP of official servers in multiplayer games. Not really, it doesn't need any rules, because for connecting to VPN with this method and if you set a DNS server like verisign, you need a rule on your modem firewall for local IP the internal IP of your computer host with mask 255.255.255.255, local ports 49152-65535, distant IP 64.6.64.6 with mask 255.255.255.255, and distant port 53 in UDP. But that's all.

7.36. Fake servers behind routers problems

For playing modern warfare 2019 in good conditions, denying connection to fake servers, the following rules have been found because NewB detects routers behind IP 209.170.124.179, 185.34.108.2, and 24.105.63.70.

local ports	distant IP	distant subnet mask	distant port(s)
49152-65535	0.0.0.1	0.0.0.0	80
49152-65535	0.0.0.1	0.0.0.0	443
1024-65535	24.105.0.0	255.255.224.0	1024-49151
1024-65535	24.105.32.0	255.255.240.0	1024-49151
1024-65535	24.105.48.0	255.255.248.0	1024-49151
1024-65535	24.105.56.0	255.255.252.0	1024-49151
1024-65535	24.105.60.0	255.255.254.0	1024-49151
1024-65535	24.105.62.0	255.255.255.0	1024-49151
1024-65535	209.170.124.0	255.255.255.128	3074-3076
1024-65535	209.170.124.128	255.255.255.224	3074-3076
1024-65535	209.170.124.147	255.255.255.224	3074-3076
1024-65535	185.34.109.0	255.255.252.0	3074-3076
1024-65535	185.34.108.0	255.255.255.254	3074-3076
1024-65535	185.34.104.0	255.255.252.0	3074-3076

Also allow to reply to ping request, normally under firewall of your modem, because it can ensure to devs that you play under their official servers. But hackers are strongest than that, so try these following rules and change your network settings often like internal IP (192.168.1.2/255.255.252.0) and DNS server among the following list but maybe it’s risky more than letting your internet provider DNS. Increase the size of your LAN network, like with the mask 255.255.252.0, with starting IP 192.168.1.2 and ending IP 192.168.3.254 under

your modem settings for DHCP. Also it doesn't take too much time to reset fresh your Xbox One often.

Modem firewall rules:

local ports	distant IP	distant subnet mask	distant port(s)	protocoles
49152-65535	0.0.0.1	0.0.0.0	53	UDP
49152-65535	0.0.0.1	0.0.0.0	80	TCP
49152-65535	0.0.0.1	0.0.0.0	443	TCP
3074-3076	24.105.54.0	255.255.255.0	5001-49151	TCP/UDP
1024-65535	185.34.106.0	255.255.254.0	3074-3076	TCP
1024-65535	185.34.107.128	255.255.255.255	3074-3076	UDP

DNS server list against IP hijacking:

ISP DNS

quad9 9.9.9.9, 149.112.112.112

cloudflare 1.1.1.1, 1.0.0.1

Verisign DNS 64.6.64.6, 64.6.65.6

Google DNS 8.8.8.8, 8.8.4.4

Norton DNS 199.85.126.30, 199.85.127.30

Comodo Shield https://shield.dome.comodo.com 8.26.56.10, 8.20.247.10

Comodo Secure DNS 8.26.56.26, 8.20.247.20

OpenDNS https://www.opendns.com 208.67.222.222, 208.67.220.220

OpenNIC https://www.opennic.org

DNSWatch 84.200.69.80, 84.200.70.40

Alternate DNS 23.253.163.53, 198.101.242.72

AdGuard DNS 176.103.130.130, 176.103.130.131

Dyn Internet Guide 216.146.35.35, 216.146.36.36

DNSReactor 104.236.210.29, 45.55.155.25

FDN 80.67.169.12, 80.67.169.40

FoolDNS 87.118.111.215, 213.187.11.67

Freenom World 80.80.80.80, 80.80.81.81

FreeDNS 37.235.1.174, 37.235.1.177

GreenTeamDNS 81.218.119.11, 209.88.198.133

Neustar DNS service 156.154.70.4, 156.154.71.4

puntCAT 109.69.8.51

SafeDNS 195.46.39.39, 195.46.39.40

SmartViper Public DNS 208.76.50.50, 208.76.51.51

UncensoredDNS 91.239.100.100, 89.233.43.71

YandexDNS 77.88.8.7, 77.88.8.3

Lightning Wire Labs 74.113.60.185, 81.3.27.54

Chaos Computer Club 194.150.168.168

Xiala 77.109.148.136, 77.109.148.137

censurfridns.dk 91.239.100.100, 89.233.43.71

dnswarden 88.198.161.8, 116.203.35.255

blahdns 159.69.198.101

faelix 195.30.94.28

nextdns https://my.nextdns.io 45.90.28.31, 45.90.30.31

securedns 146.185.167.43

oszx DNS 51.38.83.141

CleanBrowsing 185.228.168.9, 185.228.169.9

CenturyLink (Level3) 4.2.2.1, 4.2.2.2, 4.2.2.3, 4.2.2.4

Hurricane Electric 74.82.42.42

https://public-dns.info

7.37. Playing several multiplayer games problems

It’s easy and fast to change internal IP address on your console or PC you use for connection to multiplayer games. Set on your modem firewall different internal IP for each multiplayer game you play and for download. Having a thin definition of IP, ports and protocols for a multiplayer game avoid to be forwarded on hacked lobbies. Change under ipv4 properties internal IP of your PC, or under network properties of your console, in function of the game you play corresponding to the definition of your modem firewall rules you have set. Here an exemple of modem firewall rules for outlook, advanced warfare, fortnite, download, modern warfare 2019.

Application/Service	Protocole	Adresse IP source	Masque sous réseau	Port source	Adresse IP destination	Masque sous réseau	Port destination
p1	TCP	192.168.1.10	255.255.255.255	49152-65535			80
p2	TCP	192.168.1.10	255.255.255.255	49152-65535			443
p3	TCP	192.168.1.10	255.255.255.255	49152-65535			110
p4	TCP	192.168.1.10	255.255.255.255	49152-65535			995
p5	TCP	192.168.1.10	255.255.255.255	49152-65535			20-22
p6	UDP	192.168.1.10	255.255.255.255	49152-65535	64.6.64.6	255.255.255.255	53
p7	TCP	192.168.1.10	255.255.255.255	49152-65535			587
p8	TCP	192.168.1.10	255.255.255.255	49152-65535			25
x2	TCP	192.168.1.23	255.255.255.255	49152-65535			443
x3	Les deux	192.168.1.23	255.255.255.255	49152-65535			3074-3076
x4	Les deux	192.168.1.23	255.255.255.255	3074-3075			5001-49151
x5	Les deux	192.168.1.23	255.255.255.255	3074-3075			3074-3075
x1	TCP	192.168.1.23	255.255.255.255	49152-65535			80
c1	TCP	192.168.1.26	255.255.255.255	49152-65535			443
c2	UDP	192.168.1.26	255.255.255.255	49152-65535	0.0.0.1	128.0.0.0	5001-49151
t1	TCP	192.168.1.36	255.255.255.255	49152-65535			80
t2	TCP	192.168.1.36	255.255.255.255	49152-65535			443
m1	TCP	192.168.1.33	255.255.255.255	49152-65535			80
m2	TCP	192.168.1.33	255.255.255.255	49152-65535			443
m3	Les deux	192.168.1.33	255.255.255.255	49152-65535	209.170.124.0	255.255.255.0	3074
m4	Les deux	192.168.1.33	255.255.255.255	1024-65535	185.34.105.0	255.255.248.0	3074-3076
m5	Les deux	192.168.1.33	255.255.255.255	1024-65535	24.105.0.0	255.255.192.0	1024-49151

7.38. Xbox support on Twitter problems

You can not hacking like cheaters to solve the problem with it, it can"t solve problem playing on fake servers. NewB flooding isn’t a true solution, and it can forward you to full cheaters lobbies. I solved my problem of ever fake servers forwarding by writing on Twitter

to Xbox support with some private messages but limited because they don’t follow me. Here my wrotes.

Hi, I have a problem with cheaters, I can't play any match on call of duty games without fighting against cheaters, even on blizzard servers. I restricted IP removing IP behind routers and allowing only demonware and blizzard IP around. I scaned IP by IP, there are routers spoofing IP of official servers behind 185.34.108.2, 209.170.124.179, and 24.105.63.70. I can give the source codes. It's worst than it was with Steam before I left my 350 games for it. I search since several years to get ride of cheaters. Please help, I'm hill now with that.

Jan 10, 2020, 8:27 PM

I restrict distant IP under my modem firewall with subnet masks, and change internal IP for playing different multiplayer games. Did I'm playing on official servers of call of duty modern warfare ? If yes, why there are so much cheaters ? I know thay are, I played all call of duty, I've seen tons of cheaters with crazy cheats. Will you make Something ?

Jan 10, 2020, 9:46 PM

I think you never banned any one cheating.

Jan 10, 2020, 9:51 PM

start with this one ghostiidrogon please.

Jan 10, 2020, 10:13 PM

I'm fighting against him again, still cheating actually. Other cheats than wallhacks. It's like Im fired when I fire an enemy.

Jan 10, 2020, 10:41 PM

...and I can't so.

Jan 10, 2020, 10:47 PM

good bye, thanks.

Jan 10, 2020, 11:05 PM

hey sorry, but modern warfare is full of cheaters. As soon as I spawn they forward on me. Please fix it.

I have only few IP on my modem firewall

Sun 1:07 AM

255 IP with 185.34.106..0/24, 255 IP with 24.105.54.0/24, and all IP with port 443. Please...

Sun 1:09 AM

I don't understand why it seems I have 2 seconds of ping only seeing it in killcam, because I don't have any problem of latency during playing, like bullet penetration. Is my internet provider joking me. My father pay them 70 euros each month for 5 mb/s only, and 2 hour of phone. Nothing more.

Sun 1:14 AM

What's the problem with the servers full of cheaters ? I Don't think it's official servers. Even if I allow only these few IP

I don't understand.

Sun 1:19 AM

After modern warfare updates, during 2 or 3 days, there isn't these kids, but I don't think hackers need all these days for update their cheats. Maybe fake servers renters need more days.

Sun 1:24 AM

Excuse-me to have been rude. Do you have a solution ?

Sun 1:27 AM

I can't change the MAC address of my modem, and it's hard to me to change my console MAC address everytime. Against IP spoofing.

Can you create Something around this ?

Sun 1:31 AM

thanks in advance.

Sun 1:32 AM

now someone with a god mode, "BCFC RYAN15"

Sun 2:34 AM

7.39. Which one DNS server problems

I found that the DNS server nextDNS is the best. You can set under https://my.nextdns.io black list, white list, no data as returned response to not answer several times to DNS queries when blocking it, protections, tld names blocking... You can use rewrites rules like your modem IP -> bantool.xboxlive.com, your external IP -> secure-team.epicgames.com, your internal IP -> your external IP. You can change of configurations when you change of games. See as following my white list for playing fortnite on Xbox One.

*.crl.rootg2.amazontrust.com

*.ocsp.sca1b.amazontrust.com

*.ocsp.rootg2.amazontrust.com

*.eulatracking-public-service-prod.ol.epicgames.com

*.fortnite-matchmaking-public-service-live-eu.ol.epicgames.com

*.events-public-service-live.ol.epicgames.com

*.presence-public-service-prod.ol.epicgames.com

*.party-service-prod.ol.epicgames.com

*.social-ban-public-service-prod.ol.epicgames.com

*.friends-public-service-prod.ol.epicgames.com

*.lightswitch-public-service-prod.ol.epicgames.com

*.fortnite-public-service-prod11.ol.epicgames.com

*.channels-public-service-prod.ol.epicgames.com

*.datarouter.ol.epicgames.com

*.account-public-service-prod.ol.epicgames.com

*.fortnitewaitingroom-public-service-prod.ol.epicgames.com

*.ctldl.windowsupdate.com

*.www.msftconnecttest.com

*.gamepass.com

*.windows.com

*.c.s-microsoft.com

*.xboxlive.com

*.microsoft.com

*.login.live.com

For The Division 2:

*.ubisoft.com

*.ubi.com

*.ctldl.windowsupdate.com

*.www.msftconnecttest.com

*.gamepass.com

*.windows.com

*.c.s-microsoft.com

*.xboxlive.com

*.microsoft.com

*.login.live.com

For AW:

*.aw-xboxone-lobby.prod.demonware.net

*.s1-stun.au.demonware.net

*.s1-stun.jp.demonware.net

*.s1-stun.eu.demonware.net

*.s1-stun.us.demonware.net

*.aw-xboxone-auth3.prod.demonware.net

*.ctldl.windowsupdate.com

*.www.msftconnecttest.com

*.gamepass.com

*.windows.com

*.c.s-microsoft.com

*.xboxlive.com

*.microsoft.com

*.login.live.com

For modern warfare 2019:

*.prod.uno.demonware.net

*.mw-lobby-1.prod.demonware.net

*.prod.umbrella.demonware.net

*.iw8-xb1-loginqueue.prod.demonware.net

*.genesis.stun.eu.demonware.net

*.iw8-xb1-auth3.prod.demonware.net

*.genesis.stun.us.demonware.net

*.d3ovluux6b7f2q.cloudfront.net

*.status.rapidssl.com

*.ctldl.windowsupdate.com

*.www.msftconnecttest.com

*.gamepass.com

*.windows.com

*.c.s-microsoft.com

*.xboxlive.com

*.microsoft.com

*.login.live.com

7.40. DNS over HTTPS problems

With nextdns you can use their official application to secure your PC and so your consoles by sharing WiFi with Ethernet 2 card through a RJ-45 wire. It's like a simple sharing connection not like when you use a VPN (chapter 7.17). Like explained in the chapters for peering connection and above chapter you can have a secure network to not be forwarded on fake servers where cheaters full of cheats are on their PC and you on your console even if you deny crossplateform in game options and console settings. Add to the rules above in white list api.nextdns.io and my.nextdns.io (chapter 7.39). Then install the application like explained by nextdns on their setup page. The rules on your modern firewall for servers can be different like more local and distant port ranges like it's for modern warfare 2019 connected on Blizzard servers for playing (see the corresponding chapters giving ports and IP for modern warfare 2019, e.g. 7.6 and 7.36). In abstract, I found a way to secure my console better than using my modem firewall. I use DoH (DNS over HTTPS) protocole sharing my PC connection with my console and using a free application found on internet for enable DoH on my PC and so on my console. To share my PC connection with my console I open network and share center from control panel, click left on modify network card parameters at left border, then click right on WiFi card (wireless network card) and choose properties, then under sharing tab, check the box allow users to connect to internet with this connection, and then choose Ethernet local connection in the combobox under. Wire my console to my PC

with a RJ-45 wire. The proof it secure my console is that I was forced to change of ports and IP on my modem firewall to find a match in call of duty modern warfare 2019. It’s better to play with people of same level, than in a match of 2 cheaters and 10 noobs. Here my white list for modern warfare 2019 and youtube as following.

*.ggpht.com

*.google.com

*.googletagservices.com

*.google.fr

*.googleusercontent.com

*.doubleclick.net

*.gstatic.com

*.googleadservices.com

*.ytimg.com

*.googlevideo.com

*.youtube.com

*.my.nextdns.io

*.api.nextdns.io

*.prod.uno.demonware.net

*.mw-lobby-1.prod.demonware.net

*.prod.umbrella.demonware.net

*.iw8-xb1-loginqueue.prod.demonware.net

*.genesis.stun.eu.demonware.net

*.iw8-xb1-auth3.prod.demonware.net

*.genesis.stun.us.demonware.net

*.d3ovluux6b7f2q.cloudfront.net

*.status.rapidssl.com

*.ctldl.windowsupdate.com

*.www.msftconnecttest.com

*.gamepass.com

*.windows.com

*.c.s-microsoft.com

*.xboxlive.com

*.microsoft.com

*.login.live.com

7.41. DNS SEC problems

Nextdns doesn't request and validate signatures with DNS SEC. But there's a tool to do it called YogaDNS and it's better than Nextdns because it enable to request and validate signatures of domains with DNS SEC and it uses DoH. From IP and domain names spoofed shown by YogaDNS, i.e., IP 0.0.0.0, 127.0.0.1, 192.168.1.1/24, the distant IP and masks to allow in modem firewall for ports 80 and 443 in TCP are: 1.0.0.0 / 192.0.0.0, 63.0.0.0 / 192.0.0.0, 128.0.0.0 / 192.0.0.0, 193.0.0.0 / 224.0.0.0, but not all 80 and 443 in TCP finally. The list to process signatures checking with a DoH server like cloudflare or google in YogaDNS and connection sharing, for modern warfare 2019 on Xbox, are as following. *.demonware.net;d3ovluux6b7f2q.cloudfront.net;ctldl.windowsupdate.com;*.microsoft.com; www.msftconnecttest.com;*.windows.com;*.s-microsoft.com;*.xboxlive.com;login.live.com;dns.msftncsi.com; And the list to block, i.e., all, as following : *. Otherwise it's impossible to play correctly in modern warfare 2019 because it's only cheaters on their PC full cheated. Also you can create pool of servers to hide your ingame status. Take care to not add att, cisco, libredns, quad9-nofilter DoH in the pool because it doesn't allow checking signatures. But Cloudflare and Google DoH in a pool are

enough, and also process with signatures checking for all domains (*) as default rule is enough.

7.42. Network card problems

The PC you use for sharing connection have a network card with low security. Like explained in chapter 3.9 you can set security of your network card. Use the following cmd dos prompt commands.

netsh int tcp set heuristics wsh=enabled forcews=enabled

netsh int tcp set global autotuninglevel=highlyrestricted

netsh int tcp set global ecncapability=enabled

netsh int tcp set global rss=enabled

netsh int ipv4 set global multicastforwarding=enabled

netsh int ipv4 set global sourceroutingbehavior=forward

netsh int ipv4 set global groupforwardedfragments=enabled

netsh advfirewall set allprofiles settings remotemanagement disable

netsh advfirewall set allprofiles state on

netsh rpc filter delete filter filterkey=all

netsh ras delete link lcp

netsh ras delete link swc

netsh ras delete multilink multi

netsh http delete cache

netsh int teredo set state default

netsh int ipv4 delete destinationcache

netsh int ipv4 delete neighbors

netsh int ipv6 delete destinationcache

netsh int ipv6 delete neighbors

```
netsh int isatap set state default

netsh winsock reset

netsh winsock set autotuning on

netsh interface tcp set global autotuning=highlyrestricted

netsh interface tcp set global rsc=enabled

netsh interface tcp set global dca=enabled

netsh interface tcp set global ecncapability=enabled

netsh interface tcp set global netdma=enabled

netsh interface tcp set global timestamps=enabled

netsh interface tcp set security mpp=enabled

netsh interface tcp set security profiles=enabled

netsh interface tcp set security startport=1 numberofports=65535 mpp=enabled

netsh interface ipv4 set global icmpredirects=enabled

netsh interface ipv4 set global sourceroutingbehavior=forward

netsh interface ipv4 set global taskoffload=enabled

netsh interface ipv4 set global dhcpmediasense=enabled

netsh interface ipv4 set global mediasenseeventlog=enabled

netsh interface ipv4 set global mldlevel=all

netsh interface ipv4 set global mldversion=version3

netsh interface ipv4 set global multicastforwarding=enabled

netsh interface ipv4 set global groupforwardedfragments=enabled

netsh interface ipv4 set global randomizeidentifiers=enabled

netsh interface ipv4 set global addressmaskreply=enabled

netsh interface ipv4 set global sourcebasedecmp=enabled

netsh interface ipv4 set global minmtu=576
```

```
netsh interface ipv4 set global loopbacklargemtu=enabled

netsh interface ipv4 set global loopbackworkercount=16

netsh interface ipv4 set global loopbackexecutionmode=inline

netsh interface ipv4 set global reassemblyoutoforderlimit=0

netsh interface ipv4 set global store=persistent

netsh interface ipv4 set interface "1" nud=enabled

netsh interface ipv4 set interface "1" weakhostsend=disabled

netsh interface ipv4 set interface "1" weakhostreceive=disabled

netsh interface ipv4 set interface "1" currenthoplimit=255

netsh interface ipv4 set interface "1" ecncapability=application

netsh interface teredo set state default

netsh interface isatap set router enabled

netsh interface ipv6 set privacy state=enabled

netsh interface ipv6 set teredo default

netsh p2p pnrp peer set machinename publish=start autopublish=enable

netsh wfp set options netevent=on

netsh bridge set adapter "1" forcecompatmode=enable

netsh bridge set adapter "2" forcecompatmode=enable

netsh bridge set adapter "3" forcecompatmode=enable

netsh ipsec dynamic add mmp name=mmp qmpermm=10 mmlifetime=300 softsa=20
mmsec="3DES-SHA1-3 DES-SHA1-2 3DES-MD5-3"

netsh trace start scenario=internetclient

netsh mbn disconnect wwansvc

netsh interface ip delete arpcache

netsh interface ip show addresses
```

netsh interface ip set dnsservers name="Ethernet 2" source=dhcp register=both validate=yes

netsh interface ip set dnsservers name="Connexion au réseau local* 2" source=dhcp register=both validate=yes

netsh interface ip set dnsservers name="Connexion au réseau local* 3" source=dhcp register=both validate=yes

netsh interface ip set dnsservers name="Wi-Fi" source=dhcp register=both validate=yes

netsh interface ip set dnsservers name="Loopback Pseudo-Interface 1" source=dhcp register=both validate=yes

netsh interface ip set dnsservers name="Ethernet 2" source=static 64.6.64.6 primary validate=yes

netsh interface ip set dnsservers name="Connexion au réseau local* 2" source=static 64.6.64.6 primary validate=yes

netsh interface ip set dnsservers name="Connexion au réseau local* 3" source=static 64.6.64.6 primary validate=yes

netsh interface ip set dnsservers name="Wi-Fi" source=static 64.6.64.6 primary validate=yes

netsh interface ip set dnsservers name="Loopback Pseudo-Interface 1" source=static 64.6.64.6 primary validate=yes

netsh int ipv4 set compartment 0 255 store=persistent

netsh int ipv4 set compartment 1 255 store=persistent

netsh int tcp set global ecncapability=enabled

netsh int tcp set global timestamps=enabled

netsh int tcp set global initialrto=300

netsh int tcp set global rsc=enabled

netsh int tcp set global maxsynretransmissions=8

netsh int tcp set global fastopen=enabled

netsh int tcp set global hystart=enabled

netsh int tcp set global pacingprofile=always

netsh int tcp set supplemental template=internet

For enable TLS on your network, execute Run and start regedit. Add the following keys

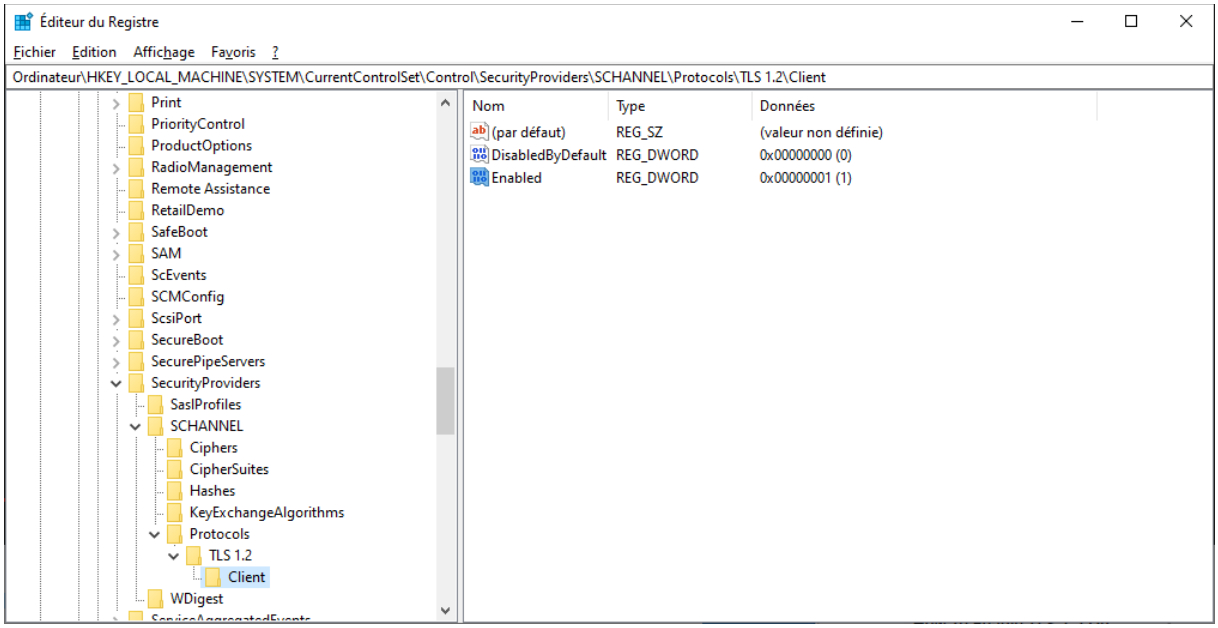
Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi

ders\SCHANNEL\Protocols\TLS 1.2\Client

with 32 bits dword values

DisabledByDefault 0

Enabled 1



Other regedit entries found on websites

https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings

https://docs.microsoft.com/fr-fr/windows-server/identity/ad-fs/operations/manage-ssl-protocols-in-ad-fs

https://support.microsoft.com/fr-fr/help/245030/how-to-restrict-the-use-of-certain-cryptographic-algorithms-and-protoc

are as following.

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi
ders\SCHANNEL

CertificateMappingMethods = 1

ClientCacheTime = 0

EnableOcspStaplingForSni = 1

EventLogging = 1

FIPSAlgorithmPolicy = 0

IssuerCacheSize = 100

IssuerCacheTime = 600000

MaximumCacheSize = 20000

SendTrustedIssuerList = 1

ServerCacheTime = 0

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi
ders\SCHANNEL\Ciphers\RC4 128\128

Enabled = 1

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi
ders\SCHANNEL\Ciphers\RC4 40\128

Enabled = 1

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi
ders\SCHANNEL\Ciphers\RC4 56\128

Enabled = 1

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168

Enabled = 1

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5

Enabled = 1

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman

ClientMinKeyBitLength = 1024

Enabled = 1

ServerMinKeyBitLength = 2048

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\PKCS

ClientMinKeyBitLength = 1024

Enabled = 1

ServerMinKeyBitLength = 2048

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Messaging

MessageLimitClient = 0x8000

MessageLimitServer = 0x4000

MessageLimitServerClientAuth = 0x8000

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi
ders\SCHANNEL\Protocols\DTLS 1.2\Client

DisabledByDefault = 0

Enabled = 1

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi
ders\SCHANNEL\Protocols\DTLS 1.2\Server

DisabledByDefault = 0

Enabled = 1

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi
ders\SCHANNEL\Protocols\SSL 3.0\Client

DisabledByDefault = 0

Enabled = 1

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi
ders\SCHANNEL\Protocols\SSL 3.0\Server

DisabledByDefault = 0

Enabled = 1

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi
ders\SCHANNEL\Protocols\TLS 1.2\Client

DisabledByDefault = 0

Enabled = 1

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvi
ders\SCHANNEL\Protocols\TLS 1.2\Server

DisabledByDefault = 0

Enabled = 1

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

MaxAsyncWorkerThreadsPerCpu = 2

FIPSAlgorithmPolicy = 1

restrictanonymous = 1

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\
Configuration\Local\SSL\00010002

functions = TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P521 (add to entry)

Ordinateur\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.5072
7

SchUseStrongCrypto = 1

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\Memory Management

MoveImages = 0xffffffff

7.43. Server of cheaters problems

Server renters like gameservers/clanservers allow cheaters to invade all games all

plateforms. Netcat spoofing IP is allowing fake servers by transforming UDP to TCP from server to client traffic. So IP on port 80 and port 443 must be set for modern warfare 2019 as following. IP with subnet masks: 25.0.0.0 /128.0.0.0, 128.0.0.0 /192.0.0.0, 193.0.0.0 /224.0.0.0. Because blizzard servers are on IP with subnet masks 24.105.0.0 /255.255.192.0, and internal IP of your network are dangerous. Also for IP of these servers, you must set local ports 3074-3076 and distant ports 37500-38500 in UDP because there are vulnerability ports on consoles. If you use cronusmax device, don't turn off controller under device monitor, don't ignore CM input and CM rumble under options of plugin X-Aim. Also under game options, enable streamer mode, under the tab account. The rules under your modem firewall are as following finally.

protocoles	local ports	distant IP	distant masks	distant ports
UDP	3074-3076	24.105.0.0	255.255.192.0	3074-3076
UDP	49152-65535	24.105.0.0	255.255.192.0	30000-40000
UDP	3074-3076	185.34.107.128	255.255.255.255	3074-3076
UDP	49152-65535	185.34.107.128	255.255.255.255	3074-3076
TCP	3074-3076	185.34.106.0	255.255.254.0	3074-3076
TCP	49152-65535	185.34.106.0	255.255.254.0	3074-3076
TCP	49152-65535	0.0.0.1	0.0.0.0	443

7.44. Port 443 problems

When you use DoH or even a free DNS server, you can't connect to online games without port 80 allowed on your modem firewall for your Xbox. Call of duty seems to refuse more and more to not been allowing port 80. I doubt of the honesty of all these people behind allowing hackers and cheaters in every matches. Using DoH for playing call of duty makes me forwarded in only matches with big teams of 3-4 cheaters I fighted against. They only banned less than 100 000 cheaters for a player base 1000 times greater. Since the last update

of Xbox it was impossible to connect to network on Xbox with only port 443, so from registering of NextDNS I search with cmd command prompt the IP associate with domain names to have conncetion on Xbox. Here some examples as following.

13.77.161.179 nslookup windows.com

13.77.161.179 nslookup microsoft.com

13.77.161.179 nslookup xboxlive.com

40.90.23.206 nslookup login.live.com

13.107.4.52 nslookup www.msftconnecttest.com

So I tried these distant IP allowed under my modem firewall as following.

13.70.0.0 /255.248.0.0

40.112.0.0 /255.254.0.0

40.76.0.0 /255.255.0.0

104.215.0.0 /255.255.0.0

13.107.0.0 /255.255.0.0

But only the following IP is needed for port 80 in TCP.

13.107.4.52 /255.255.255.255

So the modem firewall rules for playing fortnite on Xbox are as following.

protocoles	local ports	distant IP	distant masks	distant ports
TCP	49152-65535	0.0.0.1	0.0.0.0	443
UDP	49152-65535	0.0.0.1	128.0.0.0	5000-49151
UDP	49152-65535	64.6.64.6	255.255.255.255	53
TCP	49152-65535	13.107.4.52	255.255.255.255	80

7.45. Unfair multiplayer games problems

Reddit moderators won't let you scream on cheaters because they ban your topics, they ban my topics on explainations of solutions I tried. We must search multiplayer games fair

enough to be playable, games where devs are honests, even a console or plateform of games where devs are honests, not like Steam.

7.46. Fair games tool problems

Lot of multiplayer games like call of duty, are incorporating back doors for hackers to make cheats. Fake servers created by these hackers push good players in hacked lobbies fighting against cheaters unbannable. It's due to incoming ports like port 3074. Not allowing these ports and using a DOH client with connection sharing ensure good players to play in official servers. Port 80 and port 443 in TCP with local ports 49152-65535 are safe. Matchmaking with these ports only under your modem firewall and set security to maximum blocking all top levels, and all features enable, with NextDNS is a tool to get cheaters banned. You get rid of cheaters with the following settings for fortnite on Xbox as example.

fortnite NextDNS white list :

*.fortnite-public-service-prod11.ol.epicgames.com

*.fortnite-matchmaking-public-service-live-eu.ol.epicgames.com

*.lightswitch-public-service-prod.ol.epicgames.com

*.fortnitewaitingroom-public-service-prod.ol.epicgames.com

*.account-public-service-prod.ol.epicgames.com

*.my.nextdns.io

*.api.nextdns.io

*.ctldl.windowsupdate.com

*.www.msftconnecttest.com

*.windows.com

*.c.s-microsoft.com

*.xboxlive.com

*.microsoft.com

*.login.live.com

fortnite modem firewall rules :

Rule name : x1

Protocole : TCP

Local IP : 192.168.1.66

Subnet Mask : 255.255.255.255

Local ports : 49152-65535

distant IP : 13.107.4.52

Subnet mask : 255.255.255.255

distant port : 80

Rule name : x2

Protocole : TCP

Local IP : 192.168.1.66

Subnet Mask : 255.255.255.255

Local ports : 49152-65535

distant IP : 0.0.0.1

Subnet mask : 0.0.0.0

distant port : 443

Rule name : x3

Protocole : TCP

Local IP : 192.168.1.66

Subnet Mask : 255.255.255.255

Local ports : 49152-65535

distant IP : 0.0.0.1

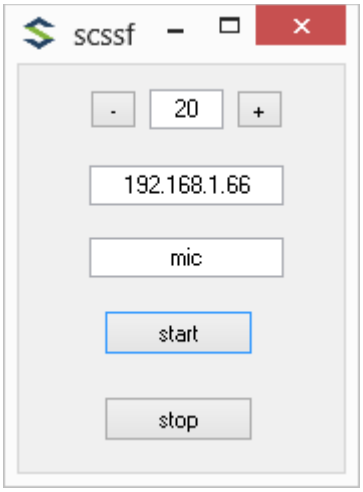
Subnet Mask : 128.0.0.0

distant ports : 5001-49151

Update network cards and let configurations for only TCP/ipv4 and use MBAM to remove viruses on computer host. Don't forget to set IP of DNS to 192.168.137.1 under network parameters of your console.

7.47. Secure connection problems

The tool on github SSF of the author securesockettunneling from the website securesockettunneling.github.io can secure TCP and UDP traffics. I made a C# form program to use it on a single PC for secure a console connected to internet sharing connection with. The code is as following.




```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using System.Runtime.InteropServices;
using System.Diagnostics;
namespace scssf
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
        }
        private int plus, minus, remoteport, localport;
        private Task task;
        private Random rnd = new Random();
        private bool finish;
        private void button3_Click(object sender, EventArgs e)
        {
            if (Int32.Parse(textBox1.Text) > 0)
```

```
            {
                minus = Int32.Parse(textBox1.Text);
                minus--;
                textBox1.Text = minus.ToString();
            }
        }
        private void button4_Click(object sender, EventArgs e)
        {
            plus = Int32.Parse(textBox1.Text);
            plus++;
            textBox1.Text = plus.ToString();
        }
        private void button1_Click(object sender, EventArgs e)
        {
            finish = false;
            task = new Task(ssfcmd);
            task.Start();
        }
        private void button2_Click(object sender, EventArgs e)
        {
            closeCmd();
            finish = true;
        }
        private void initCmd()
        {
            remoteport = rnd.Next(65535 - 54) + 54;
            using (System.IO.StreamWriter createdfile = new
System.IO.StreamWriter("config.json"))
            {
                createdfile.WriteLine("{");
                createdfile.WriteLine("\"ssf\": {");
                createdfile.WriteLine("\"circuit\": [");
                createdfile.WriteLine("{\"host\": \"192.168.137.1\", \"port\":\"" +
remoteport + "\"}");
                createdfile.WriteLine("]");
                createdfile.WriteLine("}");
                createdfile.WriteLine("}");
                createdfile.Close();
            }
            using (System.IO.StreamWriter createdfile = new
System.IO.StreamWriter("server.cmd"))
            {
                createdfile.WriteLine("cd /");
                createdfile.WriteLine("cd users/" + textBox3.Text + "/documents/ssf");
                createdfile.WriteLine("ssfd -p " + remoteport);
                createdfile.Close();
            }
            localport = rnd.Next(65535 - 54) + 54;
            using (System.IO.StreamWriter createdfile = new
System.IO.StreamWriter("client.cmd"))
            {
                createdfile.WriteLine("cd /");
                createdfile.WriteLine("cd users/" + textBox3.Text + "/documents/ssf");
                createdfile.WriteLine("ssf -c config.json -D " + localport + " -U
53:64.6.64.6:53 -p " + remoteport + " " + textBox2.Text);
                createdfile.Close();
            }
        }
        private void ssfcmd()
        {
            try { initCmd(); }
            catch
            {
                remoteport = rnd.Next(65535 - 54) + 54;
                using (System.IO.StreamWriter createdfile =
System.IO.File.AppendText("config.json"))
```

```
                {
                    createdfile.WriteLine("{");
                    createdfile.WriteLine("\"ssf\": {");
                    createdfile.WriteLine("\"circuit\": [");
                    createdfile.WriteLine("{\"host\": \"192.168.137.1\", \"port\":\"" +
remoteport + "\"}");
                    createdfile.WriteLine("]");
                    createdfile.WriteLine("}");
                    createdfile.WriteLine("}");
                    createdfile.Close();
                }
                using (System.IO.StreamWriter createdfile =
System.IO.File.AppendText("server.cmd"))
                {
                    createdfile.WriteLine("cd /");
                    createdfile.WriteLine("cd users/" + textBox3.Text + "/documents/ssf");
                    createdfile.WriteLine("ssfd -p " + remoteport);
                    createdfile.Close();
                }
                localport = rnd.Next(65535 - 54) + 54;
                using (System.IO.StreamWriter createdfile =
System.IO.File.AppendText("client.cmd"))
                {
                    createdfile.WriteLine("cd /");
                    createdfile.WriteLine("cd users/" + textBox3.Text + "/documents/ssf");
                    createdfile.WriteLine("ssf -c config.json -D " + localport + " -U
53:64.6.64.6:53 -p " + remoteport + " " + textBox2.Text);
                    createdfile.Close();
                }
                initCmd();
            }
            for (; ; )
            {
                System.Threading.Thread.Sleep(1000);
                System.Diagnostics.Process.Start("server.cmd");
                System.Threading.Thread.Sleep(5000);
                System.Diagnostics.Process.Start("client.cmd");
                int wait = Int32.Parse(textBox1.Text) * 1000 * 60;
                System.Threading.Thread.Sleep(wait);
                initCmd();
                closeCmd();
                if (finish)
                    return;
            }
        }
        private void Form1_Load(object sender, EventArgs e)
        {
            try { initConfig(); }
            catch
            {
                using (System.IO.StreamWriter createdfile =
System.IO.File.AppendText("initconfig.txt"))
                {
                    createdfile.WriteLine(textBox1.Text);
                    createdfile.WriteLine(textBox2.Text);
                    createdfile.WriteLine(textBox3.Text);
                    createdfile.Close();
                }
                initConfig();
            }
        }
        private void Form1_FormClosed(object sender, FormClosedEventArgs e)
        {
            using (System.IO.StreamWriter createdfile = new
System.IO.StreamWriter("initconfig.txt"))
            {
```

```
                createdfile.WriteLine(textBox1.Text);
                createdfile.WriteLine(textBox2.Text);
                createdfile.WriteLine(textBox3.Text);
                createdfile.Close();
            }
            finish = true;
        }
        private void initConfig()
        {
            using (System.IO.StreamReader createdfile = new
System.IO.StreamReader("initconfig.txt"))
            {
                textBox1.Text = createdfile.ReadLine();
                textBox2.Text = createdfile.ReadLine();
                textBox3.Text = createdfile.ReadLine();
                createdfile.Close();
            }
        }
        public void closeCmd()
        {
            Process[] bProcess = Process.GetProcessesByName("ssfd");
            foreach (Process process in bProcess)
            {
                process.Kill();
            }
            Process[] aProcess = Process.GetProcessesByName("cmd");
            foreach (Process process in aProcess)
            {
                process.Kill();
            }
        }
    }
}
```

7.48. Connections to official servers problems

On chapter 7.35, it's explained how to use a VPN on Xbox One. You can use AVG secure VPN for a low price subscription to be almost sure to connect to official servers choosing the location of VPN near the official servers. For call of duty black ops 4 and modern warfare 2019, you can use the location Los Angeles in North America and for fortnite Glasgow in England. You need to set your modem firewall to medium security allowing all ports in case of modern warfare 2019 but in case of fortnite only port 443 in TCP is required. You can use cmd dos prompt command to know where are the servers with tracert 24.105.54.12 and the website https://www.iplocation.net/. It's for set the closest location for official servers to change in the VPN. For my part I found Amsterdam. An example as following.

C:\WINDOWS\system32>tracert 24.105.54.12

Détermination de l’itinéraire vers 24.105.54.12 avec un maximum de 30 sauts.

1 1 ms 1 ms 1 ms lan.home [192.168.1.1]

2 98 ms 62 ms 52 ms 80.10.253.61

3 37 ms 41 ms 44 ms 193.251.109.214

4 141 ms 83 ms 65 ms ae42-0.nistr201.Schiltigheim.francetelecom.net [193.252.163.170]

5 20 ms 24 ms 25 ms 193.252.137.82

6 49 ms 44 ms 44 ms blizzard-2.gw.opentransit.net [81.52.179.220]

7 29 ms 31 ms 27 ms 137.221.80.35

8 32 ms 27 ms 32 ms et-0-0-2-br01-eqpa4.as57976.net [137.221.65.26]

9 30 ms 31 ms 27 ms be1-pe1-eqpa4.as57976.net [137.221.77.67]

10 30 ms 32 ms 33 ms 137.221.66.33

11 27 ms 26 ms 32 ms 185.60.115.147

12 * * * Délai d’attente de la demande dépassé.

13 * * * Délai d’attente de la demande dépassé.

14 * * * Délai d’attente de la demande dépassé.

15 * * * Délai d’attente de la demande dépassé.

16 * * * Délai d’attente de la demande dépassé.

17 * * * Délai d’attente de la demande dépassé.

18 * ^C

C:\WINDOWS\system32>

7.49. Low connection problems

Disable IPv6 under your modem settings and network cards settings. Change regedit following key. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\

DisabledComponents : 0xffffffff. Change WiFi network for choose WiFi-Invite because it's more secure separate from other devices connected to network and rules like UPnP aren't applied. When choosing a VPN like AVG Secure VPN, it open more ports than what are set under your modem with WiFi-Invite. Before I also tried to forward ports but useless (port 88 in UDP, 3074 in UDP and TCP, 53 in UDP and TCP, 80 in TCP, 500 in UDP, 3544 in UDP, 4500 in UDP), and also change WiFi canal and check each time with website https://speedtest.com your connection, but useless too. Low connection can be due to invisible devices owned by an ISP employe or his friend connected to your network. In order to rescue your network, apply the following recommandation. Add internal IP of your PC as static IP under your modem. Then create rules to disallow all distant ports and IP for all local ports and IP around the internal IP of your PC using the following subnet masks as abstract found from the chapter 7.29. Finally reboot your modem. It will avoid all other PC to connect after reboot. Share connection with your console and use a secure VPN with the computer host to play.

mask	nIP
255	1
254	2
252	4
248	8
240	16
224	32
192	64
128	128
0	255

7.50. Get rid of cheaters problems

With a VPN you can't set accurate firewall rules but you can escape cheaters incoming after you kicked noobs because you can change VPN location letting the time of bans. Also the ping is better and the connection with less lags. But there's download issue and it's possible a VPN is low of security. In the opposite, allowing all ports and forwarding ports recommended by devs can make gone cheaters and can send proofs to devs that you aren't cheating and cheaters are there. I've tested the VPN method and DoH method, I can say it varies between full cheaters and free of cheaters. The method of forwarding ports implies you can't share connection from a computer host, but you don't have to find IP and ports or even domains like with a DoH. Games like fortnite allow changing location of servers if you don't find any matches. Finally, prefer to forward ports and here it goes.

7.51. Steam problems

The only games where you enjoy playing and you don't see cheaters in every matches, if you are strong, not dying easy, so you can see aimboters, are solo games on Steam, for sure, but it's probably not better. Create a shortcut from options when you click right on desktop and type in location area C:\Windows\System32\cmd.exe /c start "Steam.exe" /high "C:\Program Files (x86)\Steam\steam.exe" –tcp for launching Steam. Open distant ports 80, 443, 27000-27050 with local ports 49152-65535 in TCP. Create Nat-Pat rules for these ports under your modem firewall. Create appropriate rules under Windows firewall for these ports, adding a rule for distant port 53 with local ports 49152-65535 in UDP. Set to block inbound and outbound traffics. You will download games faster and secure to maximum your PC meanwhile.

7.52. Epic Games Launcher problems

To avoid cut of downloads with Epic Games Launcher, there are some requirements. Create a shortcut from options when you click right on desktop and type in location area

cmd.exe /c start "EpicGamesLauncher" /High "C:\Program Files (x86)\Epic Games\Launcher\Portal\Binaries\Win64\EpicGamesLauncher.exe" for starting with high priority Epic Games Launcher. In the folder “C:\Program Files (x86)\Epic Games\Launcher\Portal\Config”, there is a file DefaultEngine.ini, where you set the following lines:

```
[HTTP]
HttpTimeout=40
HttpConnectionTimeout=40
HttpReceiveTimeout=40
HttpSendTimeout=40
bUseNullHttp=false
HttpMaxConnectionsPerServer=4

[Portal.BuildPatch]
ChunkDownloads=3
ChunkRetries=5
RetryTime=1
```

Under your modem, under network tab for DHCP configurations, set the IP of your PC as static, under network tab for DMZ, put your PC, and enable UPnP. And also under network tab for Nat/Pat rules, create rules for internal and external ports 53, 80, 443 for your PC. Under network configuration of your PC, set IPv4 properties, with internal IP of your PC, network mask, IP of your modem, and IP of your DNS. Under Windows firewall, create allowing inbound and outbound traffic rules with IP of DNS, and rules for Epic Games Launcher processes you see under task manager (ctrl+shift+esc). Also under Windows firewall properties set to block inbound and outbound traffic.

7.53. Refreshing or initializing a desktop PC problems

When refreshing a PC or booting for the first time a PC, it's important to proceed some optimization. Installing the new version of Microsoft Edge, blocking all inbound trafic and blocking outboud trafic if no rules with Windows firewall. Rules for your favorite game launcher and multiplayer games, rules for client DNS service and Microsoft Edge. Disabling services from administrative tool and functionalities from programs and functionnalities,

uninstalling programs, letting only the essentials. Uninstalling all VC redistributable and installing VC redistributable 2019 from Microsoft official website. Uninstall and delete of Nvidia containers and drivers, letting only both Nvidia audio and graphic drivers. Editing registry keys like MoveImages or even DisableAntiSpyware. Also using minimum of programs you need for playing, no anti-virus, no noob programs uncheckable inside codes. Only the necessaries. Cleaning the disk from administrative tools in control panel. Deleting contents of folder %temp%. Deleting anything related to useless programs from folders %programfiles(x86)%, %programdata%, %localappdata%, %appdata% (for it, you need to allow display masked elements from upper right menu named display). Opening and launching repair tool when restarting pressing shift key with click on restart. Checking application in backgroud tasks with task manager for stoping it and create extension .bak in order to free memory usage. In order to achieve unintallation of WindowsApp, you need to set under security tab in properties of folder, acces for users of your PC, instead of trustinstaller, in order to rename the folders where applications are. But create your shortcuts before like under task bar for acces control panel, programs and functionnalities, Windows firewall. Setting DEP for all programs and services under system properties, and changing to better performance, disabling remote access, and setting more RAM. Managing your modem firewall and IPv4 properties under network and maintenance center. Having a static internal IP for your PC. Using an Ethernet wire. Disabling Bluetooth and WiFi cards if using Ethernet card from card parameters under network settings. Changing MAC address often, letting the two first numbers, from configuration of network card under network center and maintenance under control panel. Enabling Planified QoS packets and RMCAST protocol and other services to install for security, from network properties under control panel and changing configurations of network card, enabling everything under the tab advanced. Using the DNS quad9, IP 9.9.9.9, because some ISP are stupids and bads. Deleting often cache of navigation

with Microsolt Edge or when something goes wrong with web sites. Checking memory under administrative tool. Updating drivers from peripheral manager under control panel and from Nvidia control panel with Game Ready Drivers, updating OS with Windows Update from parameters, updating your programs. Disabling all features when initializing your PC and in Windows 10 parameters like xbox games, capture, notifications, VPN, proxy, applications at start, Windows Defender scanning... but let security features in Windows 10 parameters like for using exploit protection security. Enabling exploit protection for your multiplayer games. Disabling restore points recorder security and all restore points for all your disks from advanced system parameters under control panel. Uninstall noob programs under starting menu and remove programs from start folder and start shown under task manager. Disabling notifications and alerts. Using a proxy with address and port found under internet googling a proxy for california if you are playing under blizzard servers, it doesn''t need any firewall rule but it run only with battle.net, not with epic games launcher where you can't connect. Not trying everything everytime, not going everywhere. Managing screensaver and alimentation for having better performance and not energy safe. Energy safe is when you do all I explained here, with all information in this book for optimizing your PC, not a shut down automatic. Not using a SSD drive with a USB-C wire but instead a USB-3.1 wire, and wiring SSD drive to the rear of your PC. Cleaning drives from administartive tool under control panel. Disabling all features from network settings under network and share center under control panel, but letting only TCP/IP IPv4, and in TCP/IP IPv4 properties under advanced settings, under tab WINS, disabling LMHOSTS and NetBIOS on TCP/IP. Uninstalling all intel products because there are security falls, from programs and functionnalities under control panel. Enable high resolution assists under Battle.net properties. Disabling services with open conncetion shown in ressource monitor (like the service IP assistance), from administrative tools under control panel. Setting IP configuration manually, in network properties, from

network center and maintenance, under control panel. Deleting all tasks from planified tasks under administrative tools under control panel. Setting User Account Control (UAC) to highest level. Exploit protection same for epic games launcher, eac, be. Exploit protection, new feature, it needs Windows update. Windows update for peripheral drivers and exploit protection sup. Reporting dates for Windows update after it. Disk manager under administrative tools from control panel, removing second disk you don't need if you have a ssd external drive for better performance. Removing all programs automatically starting at PC launch from task manager. FreePlay for blocking IP automatically playing Fortnite free of cheaters (exported firewall rules). Choosing the auto region of matchmaking (less latency) in Fortnite for avoid IP spoofing of fake servers. Checking if screensaver is running otherwise someone is hacking your computer. Not installing several game launcher, prefer Epic or Battle.net instead of Steam virus launcher. Setting game options for graphisms, like fullscreen, highest FoV (Field of View), privilege for textures and view quality instead of shoot impacts or shadows, or cinema render, or particules effects for explosion, or grain quality, because the game should be more fluid. Disabling all functionnalities, from program and functionnality under control panel, but not frameworks redist. Windows firewall to default if problem of authentication. Typing -aslr as command line argument for your games under battle.net game parameters. Updating often your graphic card driver with GeForce Experience. Finding and installing a maximum of Windows security updates known as KB, under Microsoft official website. Adding no access to all folders by applications under security from Windows Defender, but let access to Battle.net and Battle.Net Agent, and also call of duty games. Uninstalling all webbrowsers. Setting be and eac services to always running. Downloading graphic card driver from official source with internet explorer. Entering Bios for setting optimized and secure boot. Disabling LMHosts and NetBios TCP/IP under network card properties. Deleting useless files and system files from administartive

tools under control panel with the tool clean drive disks. Using nextdns or comodo secure shield with all secure features or simply Quad9 DNS with DNS IP of seconcondary DNS. Enabling services which are describing optimization for more framerate in games, i.e., more rigidity of control, better to be competitive. Disabling services allowing fake network connections, even IPSec service or Netlogon because of vunerabilities. Uninstalling useless webbrowsers and associated files. Uninstalling print peripherals. Setting Windows defender to maximum securities, like denying access to all folders but not folder documents. Setting Windows defender for cutting execution of wmic, powershell, conhost, ShellExperienceHost, dllhost, and wlanext, with exploit protection to maximum securities (remove it to be able to change properties like network and restarting your PC after, but also remove it to be able to reboot from fresh). Setting all files and subfolders of every folders and files, but not folder documents and folder desktop, to readonly and masked elements, and not folder program files (x86) or not folder battle.net in, to masked elements, with the button properties when you click right checking appropriate options under main tab. You can see it again with display button at top bar of folder tab. Setting property of your disks with properties when you click right on it, to not allow indexing contents under main tab. There's also tool to check disk and trim, and also clean disk, in other tabs of disk properties. Finding a multiplayer game fair not like call of duty games, but a game you like to play, instead of trying noob games, deserving the hates you put in it playing, more those in basis from developers and more in hand with cheaters. Playing a multiplayer game where you can choose your region of matchmaking because European servers are fill with only cheaters. You don't want lags, you don't want cheaters, you don't want to be a hater. You want to take pleasure for what you pay, for what you want to take time in. This chapter and all information linked to it in this book explain everything you need to know for playing in good place.

7.54. Eploit protection problems

I was able to set security for modern warfare 2019 for warzone and make more kills. In security settings for Windows Defender, from exploit protection, you can set the following parameters (but all applications can't be added, in particular Windows ones). In French, for call of duty games:

- Protection arbitraire du code -> Désactivé; Autoriser la désinscription du thread -> Désactivé

- Bloquer les images de faible intégrité -> Activé

- Bloques des images distantes -> Activé

- Bloquer les polices non approuvées -> Activé

- Protection de l'intégrité du code -> Désactivé; Autoriser aussi le chargement d'images signées par le Microsoft Store -> Désactivé

- Protection du flux de contrôle -> Désactivé; Utilisez une protection stricte du flux de contrôle -> Désactivé

- Prévention de l'éxécution des données (PED) -> Activé; Activer l'émulation thunk ATL -> Activé

- Désactiver les points d'extension -> Activé

- Désactiver les appels système Win32k -> Désactivé

- Ne pas autoriser les processus enfants -> Activé

- Exporter le filtrage d'adresses -> Désactivé; Valider l'accès à des modules qui sont couramment attaqués -> Désactivé

- Forcer la randomisation des images -> Activé; Ne pas autoriser les images rayées -> Activé

- Protection des piles appliquée par le matériel -> Activé; Applicable à tous les modules -> Activé

- Importer le filtrage d'adresses -> Désactivé

- Allocations de mémoire aléatoires -> Activé; N'utilisez pas l'entropie élevée -> Désactivé

- Simuler l'éxécution -> Activé

- Valider l'invocation de l'API -> Activé

- Valider les chaînes d''exception -> Activé

- Valider l'utilisation de la poignée -> Désactivé

- Valider l'intégrité du tas -> Activé

- Valider l'intégrité des dépendances d'images -> Activé

- Valider l'intégrité de la pile -> Désactivé

In French, for fortnite but « Valider l'utilisation de la poignée » to disable when easy anti cheat is starting:

- Protection arbitraire du code -> Désactivé; Autoriser la désinscription du thread -> Désactivé

- Bloquer les images de faible intégrité -> Activé

- Bloques des images distantes -> Activé

- Bloquer les polices non approuvées -> Activé

- Protection de l'intégrité du code -> Désactivé; Autoriser aussi le chargement d'images signées par le Microsoft Store -> Désactivé

- Protection du flux de contrôle -> Activé; Utilisez une protection stricte du flux de contrôle -> Désactivé

- Prévention de l'éxécution des données (PED) -> Activé; Activer l'émulation thunk ATL -> Activé

- Désactiver les points d'extension -> Activé

- Désactiver les appels système Win32k -> Désactivé

- Ne pas autoriser les processus enfants -> Activé

- Exporter le filtrage d'adresses -> Désactivé; Valider l'accès à des modules qui sont couramment attaqués -> Désactivé

- Forcer la randomisation des images -> Activé; Ne pas autoriser les images rayées -> Activé

- Protection des piles appliquée par le matériel -> Activé; Applicable à tous les modules -> Activé

- Importer le filtrage d'adresses -> Désactivé

- Allocations de mémoire aléatoires -> Activé; N'utilisez pas l'entropie élevée -> Désactivé

- Simuler l'éxécution -> Activé

- Valider l'invocation de l'API -> Activé

- Valider les chaînes d''exception -> Activé

- Valider l'utilisation de la poignée -> Activé

- Valider l'intégrité du tas -> Activé

- Valider l'intégrité des dépendances d'images -> Activé

- Valider l'intégrité de la pile -> Désactivé

In French, for easy anti cheat:

- Protection arbitraire du code -> Désactivé; Autoriser la désinscription du thread -> Désactivé

- Bloquer les images de faible intégrité -> Activé

- Bloques des images distantes -> Activé

- Bloquer les polices non approuvées -> Activé

- Protection de l'intégrité du code -> Désactivé; Autoriser aussi le chargement d'images signées par le Microsoft Store -> Désactivé

- Protection du flux de contrôle -> Activé; Utilisez une protection stricte du flux de contrôle -> Désactivé

- Prévention de l'éxécution des données (PED) -> Activé; Activer l'émulation thunk ATL -> Activé

- Désactiver les points d'extension -> Activé

- Désactiver les appels système Win32k -> Désactivé

- Ne pas autoriser les processus enfants -> Désactivé

- Exporter le filtrage d'adresses -> Désactivé; Valider l'accès à des modules qui sont couramment attaqués -> Désactivé

- Forcer la randomisation des images -> Activé; Ne pas autoriser les images rayées -> Activé

- Protection des piles appliquée par le matériel -> Activé; Applicable à tous les modules -> Activé

- Importer le filtrage d'adresses -> Activé

- Allocations de mémoire aléatoires -> Activé; N'utilisez pas l'entropie élevée -> Désactivé

- Simuler l'éxécution -> Activé

- Valider l'invocation de l'API -> Désactivé

- Valider les chaînes d''exception -> Activé

- Valider l'utilisation de la poignée -> Activé

- Valider l'intégrité du tas -> Activé

- Valider l'intégrité des dépendances d'images -> Activé

- Valider l'intégrité de la pile -> Activé

Exploit protection for svchost and everything shown in task manager as following :

- Prévention de l'éxécution des données (PED) -> Activé*; Activer l'émulation thunk ATL -> Activé*

- Forcer la randomisation des images -> Activé*; Ne pas autoriser les images rayées -> Activé*

- Protection des piles appliquée par le matériel -> Activé*; Applicable à tous les modules -> Activé*

- Allocations de mémoire aléatoires -> Activé*; N'utilisez pas l'entropie élevée -> Désactivé*

7.55. Services enable problems

There are lot of services useless using memory, CPU and GPU. A lot of services running can be disabling. The services running to never disable on W10 OS are as following. In French:

- Infrastructure de gestion Windows
- Service antivirus Microsoft Defender
- Gestion de niveaux de stockage
- SysMain
- Détection matériel noyau
- Planificateurs de tâches
- Gestionnaire de compte de sécurité
- Realtek Audio Universal Service
- Appel de procédure distante (RPC)
- Mappeur de point de terminaison RPC
- Service de profil utilisateur
- Alimentation
- Service Interface du magasin réseau
- Connaissance des emplacements réseau
- Service Liste des réseaux
- Pare-Feu Windows Defender
- Gestionnaire de session locale
- Journal d'événement Windows

- Service de stratégie de diagnostic
- Client DHCP
- Lanceur de processus DCOM
- Services de chiffrement
- CoreMessaging
- Service d'infrastructure des tâches en arrière-plan
- Moteur de filtrage de base
- Audio Windows
- Générateur de points de terminaison du service Audio Windows
- Centre de sécurité
- Service de transfert intelligent en arrière plan
- Protection logicielle
- Service Broker du moniteur d'exécution System Guard
- Gestionnaire des utilisateurs
- Service Broker des événements système
- Service de stockage
- Modules de génération des clés IKE et AuthIP
- Client DNS
- Service de découverte automatique de Proxy Web pour les services HTTP Windows
- Service d'inspection réseau de l'antivirus Microsoft Defender
- Service State Repository (State Repository)
- Service Sécurité Windows
- Connexions réseau
- Service Broker pour les événements horaires

- Optimisation de livraison

- Service d'association de périphérique

- Service de prise en charge Bluetooth

- Information d'application

Uninstall these services with cmd prompt commands running with administrator privilege:

sc delete beservice

sc delete easyanticheat

sc delete remoteregistry

sc delete termservice (it needs you restart your computer)

sc delete vmicrdv

sc delete winrm

sc delete lanmanserver

sc delete lanmanworkstation

sc delete remoteaccess

7.56. Network driver problems

For eliminate unwanted changes on your network, it's better checking and changing hosts file in windows/system32/drivers/etc as following :

127.0.0.1 localhost

::1 localhost

And checking and changing protocol file in windows/system32/drivers/etc as following :

tcp 6 TCP # Transmission control protocol

udp 17 UDP # User datagram protocol

Remember, all other files in in windows/system32/drivers/etc shall be empty.

7.57. Why developers would not do this against hackzone problems

It's easy to get ride of cheaters when it's your game. You can use screenshots of cheater gameplay and compare pictures with screenshots at same place of cheater position (the library AForge.NET is a fantastic tool to compare pictures). You can create invisible bots like other players but not counting in scores, for annoy cheaters wallhacking and aimboting. You can use ASLR for the game process in term of memory space allocations. When a cheater do DLL injection, it's easy to get modules information and see the memory size. You can make lawsuit against cheaters. You can check the speed of cheaters when running or paralyzed, even check the energy remains after taking headshots like if noobs cheating are using god mod. You can temporary banning cheaters. It's easy to make in place all of it, and so get ride of all cheaters. When applying Windows firewall or modem firewall, DNS flush, memory flush, normally more you are playing, less cheaters would be there, not like fortnite or pubg with amazon servers everywhere, with IP of fake servers unblockable. Devs for these games can't do nothing and so do nothing obviously with all garbage IP in UDP. The problem is also with IP location of blizzard servers for modern warfare 2019 where it's England or United States for same IP, and this even if changing of region in battle.net (information from

a bgp view search). As example, I've just set firewall to default, used a brand new PC, applied my methods in the previous chapter, never using other programs than battle.net and played only modern warfare 2019, I had the worst TROJAN named bifrost, with the folder of same name in program files (or can be in %temp%, %programdata%, %localappdata%, %appdata%), which control and watch your PC. I recommend to not using battle.net, steam, and xbox, because when you buy a game and enter your credit card numbers in these game launchers, the secure key is visible. So bifrost send your credit card information to hackers because hackers through bifrost can watch everything you doing. Repair epic games launcher when you can't login but they don't want you play on, so it was a temporary fix to connect until they saw it, but if you are lucky to connect on, they install this trojan bifrost and useless services for hack fest games breaking your PC. So? Which platforms for which games? Which enjoyable gameplay? Who deserve to have your money? Even if platform and games on aren't perfect? I think Battle.net on a PC applying essential information in this book.

7.58. Shadowban cheater hack problems

It's not possible to always fight against cheaters and losing all matches in every games of call of duty. It's probably a hack. Cheater programs are hacking players through the network to accomplish such bad things. I recommend using the following methods:

- Check/Repair files often with launcher.

- Use FreeWar and Windows firewall rules in exported files with blocked ip and without, launch game, wait error of authentication, export with blocked ip, import without, authenticate, import with blocked ip.

- Instead of FreeWar, an outage rule for blocking outside ip of ip necessary for playing, is more secure and convenient, using only imports of rules with two files explained above.

- Set Windows Defender to maximum security, like folder access (adding all your folders and creating application exceptions), exploit protection (for games and game launchers), ...

- Set run with administrative privilege games and game launchers.

- Don't cheat like big noobs.

- Delete files with strange dates of modification and then repair games with battle.net tool (it increases performances).

- Set battle.net to close after starting games.

- Use combination of Windows firewall and modem firewall (255.255.255.128).

7.59. Connection to call of duty problems

If you encounter connection problem for authentication into call of duty games, there is a method here to follow :

- Change MAC address of your network card under configuration of network card.
- Uninstall driver TCP/IPv4 from network properties then reinstalling.
- Change internal IP and change consequently it in Windows firewall.
- Reboot your PC and your modem.

Allow, just for connecting once, all ports and all protocols for outbound traffic, under Windows firewall.

7.60. Keep safe a PC problems

For being competitive in call of duty, there's lot of things to setup before coming online. There's lot of things to respect to not break a PC. The advices to setup a PC, I giving, are tested, and going futher isn't recommended. I listed important tools to use for unhacking a PC in my github repository. It must be adapted for other PC. But like I already said, going futher is dangerous, and unecessary, so much times I searched the issue with cheaters. I contacted blizzard and my ISP lot of times for the problem of hacked lobbies due to

redirection. The issue seems coming from the softwares on a PC. Following my guides is necessary for not be forwarded against only cheaters, always losing and fighting against.

8. Glossary

8.1. Azure Servers Public IP

```
<?xml version="1.0" encoding="utf-8"?>
<AzurePublicIpAddresses xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Region Name="australiac2">
    20.36.64.0/19
    20.36.112.0/21
    20.39.72.0/21
    20.39.96.0/19
    40.82.12.0/22
    40.82.244.0/22
    40.90.130.32/28
    40.90.142.64/27
    40.90.149.32/27
    40.126.128.0/18
    52.143.218.0/24
    52.239.218.0/23
  </Region>
  <Region Name="australiac">
    20.36.32.0/19
    20.36.104.0/21
    20.37.0.0/18
    20.38.184.0/22
    20.39.64.0/21
    40.82.8.0/22
    40.82.240.0/22
    40.90.130.48/28
    40.90.142.96/27
    40.90.149.64/27
    52.143.219.0/24
    52.239.216.0/23
  </Region>
  <Region Name="australiaeast">
    13.70.64.0/18
    13.72.224.0/19
    13.73.192.0/20
    13.75.128.0/17
    20.37.192.0/19
    20.38.112.0/23
    20.40.64.0/20
    20.40.80.0/21
    20.40.120.0/21
    20.40.176.0/20
    20.42.192.0/19
    20.188.128.0/17
    20.190.142.0/25
    20.191.192.0/18
    23.101.208.0/20
    40.79.160.0/20
    40.79.211.0/24
    40.82.32.0/22
    40.82.192.0/19
    40.87.208.0/22
    40.90.130.80/28
    40.90.130.208/28
    40.90.140.32/27
```

40.90.142.160/27
40.90.147.64/27
40.90.150.0/27
40.112.37.128/26
40.126.14.0/25
40.126.224.0/19
52.108.40.0/23
52.109.112.0/22
52.114.16.0/22
52.143.199.0/24
52.143.200.0/23
52.147.0.0/19
52.156.160.0/19
52.187.192.0/18
52.232.136.0/21
52.232.154.0/24
52.237.192.0/18
52.239.130.0/23
52.239.226.0/24
52.245.16.0/22
104.44.90.64/26
104.44.93.96/27
104.44.95.48/28
104.46.29.0/24
104.46.30.0/23
104.46.240.0/20
104.209.80.0/20
104.210.64.0/18
191.238.66.0/23
191.239.64.0/19
</Region>
<Region Name="australiasoutheast">
13.70.128.0/18
13.73.96.0/19
13.77.0.0/18
20.40.160.0/20
20.42.224.0/19
20.190.96.0/19
20.190.142.128/25
23.101.224.0/19
40.79.212.0/24
40.81.48.0/20
40.87.212.0/22
40.90.138.128/27
40.112.37.192/26
40.115.64.0/19
40.117.0.0/19
40.126.14.128/25
40.127.64.0/19
52.108.234.0/23
52.109.116.0/22
52.114.20.0/22
52.136.25.0/24
52.147.32.0/19
52.158.128.0/19
52.189.192.0/18
52.239.132.0/23
52.239.225.0/24
52.243.64.0/18
52.245.20.0/22
52.255.32.0/19
104.44.90.32/27
104.44.93.128/27
104.44.95.64/28
104.46.28.0/24
104.209.64.0/20
191.239.160.0/19

191.239.192.0/22
</Region>
<Region Name="brazilsouth">
20.40.16.0/20
20.40.32.0/21
20.40.112.0/21
20.190.145.0/25
23.97.96.0/19
40.90.133.32/27
40.90.141.64/27
40.90.144.224/27
40.126.17.0/25
52.108.36.0/22
52.109.108.0/22
104.41.0.0/18
191.232.32.0/19
191.232.160.0/19
191.232.192.0/18
191.233.0.0/21
191.233.24.0/21
191.233.128.0/24
191.233.130.0/23
191.233.132.0/22
191.233.136.0/21
191.233.192.0/18
191.234.160.0/19
191.235.32.0/19
191.235.64.0/18
191.235.196.0/22
191.235.200.0/21
191.235.224.0/20
191.235.240.0/21
191.235.248.0/24
191.237.195.0/24
191.237.200.0/21
191.237.248.0/21
191.238.128.0/21
191.238.192.0/19
191.239.112.0/20
191.239.204.0/22
191.239.240.0/20
</Region>
<Region Name="canadacentral">
13.71.160.0/19
13.88.224.0/19
20.39.128.0/20
20.43.0.0/19
20.190.139.0/25
40.79.216.0/24
40.80.44.0/22
40.82.160.0/19
40.85.192.0/18
40.90.128.0/28
40.90.138.32/27
40.90.143.160/27
40.90.151.96/27
40.126.11.0/25
52.108.42.0/23
52.109.92.0/22
52.114.160.0/22
52.136.23.0/24
52.138.0.0/18
52.139.0.0/18
52.156.0.0/19
52.228.0.0/17
52.233.0.0/18
52.237.0.0/18

52.239.148.64/26
52.239.189.0/24
52.245.28.0/22
104.44.93.32/27
104.44.95.16/28
</Region>
<Region Name="canadaeast">
20.190.139.128/25
40.69.96.0/19
40.79.217.0/24
40.80.40.0/22
40.80.240.0/20
40.86.192.0/18
40.89.0.0/19
40.90.130.192/28
40.90.138.64/27
40.90.140.0/27
40.90.147.32/27
40.126.11.128/25
52.108.232.0/23
52.109.96.0/22
52.114.164.0/22
52.136.22.0/24
52.139.64.0/18
52.155.0.0/19
52.229.64.0/18
52.232.128.0/21
52.235.0.0/18
52.239.164.128/26
52.239.190.0/25
52.242.0.0/18
52.245.32.0/22
104.44.93.64/27
104.44.95.32/28
</Region>
<Region Name="indiacentral">
13.71.0.0/18
20.40.40.0/21
20.40.48.0/20
20.43.120.0/21
20.190.146.0/25
40.79.214.0/24
40.81.224.0/19
40.87.224.0/22
40.90.137.128/27
40.112.39.0/25
40.112.39.128/26
40.126.18.0/25
52.108.44.0/23
52.109.56.0/22
52.114.40.0/22
52.136.24.0/24
52.140.64.0/18
52.159.64.0/19
52.172.128.0/17
52.239.135.64/26
52.239.202.0/24
52.245.96.0/22
104.44.92.128/27
104.44.94.192/28
104.47.210.0/23
104.211.64.0/18
</Region>
<Region Name="uscentraleuap">
13.67.153.16/28
13.67.154.0/24
20.190.138.128/25

40.78.200.0/21
40.78.208.16/28
40.82.0.0/22
40.83.24.96/27
40.89.32.0/19
40.90.132.80/28
40.90.142.32/27
40.90.149.0/27
40.122.0.0/20
40.126.10.128/25
52.109.140.0/22
52.141.224.0/20
52.143.198.0/24
52.158.176.0/20
52.165.104.128/26
52.176.225.0/24
52.176.232.0/21
52.176.240.0/20
52.180.160.0/20
52.180.176.0/21
52.185.56.112/28
52.185.112.64/27
52.239.177.0/27
52.239.238.0/24
52.245.69.0/27
52.253.156.0/22
52.253.232.0/21
104.208.48.0/20
168.61.136.0/21
</Region>
<Region Name="uscentral">
13.67.128.0/20
13.67.144.0/21
13.67.152.0/24
13.67.153.0/28
13.67.153.32/27
13.67.153.64/26
13.67.153.128/25
13.67.155.0/24
13.67.156.0/22
13.67.160.0/19
13.67.192.0/18
13.86.0.0/17
13.89.0.0/16
20.37.128.0/18
20.38.96.0/23
20.40.192.0/18
20.184.64.0/18
20.186.192.0/18
20.190.134.0/24
23.99.128.0/17
23.100.80.0/21
23.100.240.0/20
23.101.112.0/20
23.102.202.0/24
40.67.160.0/19
40.69.128.0/18
40.77.0.0/17
40.77.161.64/26
40.77.166.192/26
40.77.175.192/27
40.77.175.240/28
40.77.182.16/28
40.77.182.192/26
40.77.184.128/25
40.78.128.0/18
40.78.221.0/24

40.82.16.0/22
40.83.0.0/20
40.83.16.0/21
40.83.24.0/26
40.83.24.64/27
40.83.24.128/25
40.83.25.0/24
40.83.26.0/23
40.83.28.0/22
40.83.32.0/19
40.86.0.0/17
40.87.180.0/22
40.89.224.0/19
40.90.16.0/27
40.90.128.16/28
40.90.129.224/27
40.90.130.64/28
40.90.132.192/26
40.90.137.224/27
40.90.140.96/27
40.90.140.224/27
40.90.141.0/27
40.90.142.128/27
40.90.142.240/28
40.90.144.0/27
40.90.144.128/26
40.90.148.176/28
40.90.149.96/27
40.90.151.160/27
40.113.192.0/18
40.122.16.0/20
40.122.32.0/19
40.122.64.0/18
40.122.128.0/17
40.126.6.0/24
52.108.208.0/21
52.109.8.0/22
52.114.128.0/22
52.125.128.0/22
52.136.30.0/24
52.141.192.0/19
52.141.240.0/20
52.143.193.0/24
52.143.224.0/19
52.154.0.0/18
52.154.128.0/17
52.158.160.0/20
52.158.192.0/19
52.165.0.0/19
52.165.32.0/20
52.165.48.0/28
52.165.49.0/24
52.165.56.0/21
52.165.64.0/19
52.165.96.0/21
52.165.104.0/25
52.165.128.0/17
52.173.0.0/16
52.176.0.0/17
52.176.128.0/19
52.176.160.0/21
52.176.176.0/20
52.176.192.0/19
52.176.224.0/26
52.176.224.64/27
52.176.224.96/28
52.180.128.0/19

52.180.184.0/27
52.180.184.32/28
52.180.185.0/24
52.182.128.0/17
52.185.0.0/19
52.185.32.0/20
52.185.48.0/21
52.185.56.0/26
52.185.56.64/27
52.185.56.96/28
52.185.56.128/27
52.185.56.160/28
52.185.64.0/20
52.185.80.0/26
52.185.81.0/24
52.185.88.0/21
52.185.96.0/20
52.185.112.0/26
52.185.112.96/27
52.185.120.0/21
52.189.0.0/17
52.228.128.0/17
52.230.128.0/17
52.232.157.0/24
52.238.192.0/18
52.239.150.0/23
52.239.177.32/27
52.239.177.64/26
52.239.177.128/25
52.239.195.0/24
52.239.234.0/23
52.242.128.0/17
52.245.68.0/24
52.245.69.32/27
52.245.69.64/27
52.245.69.96/28
52.245.69.144/28
52.245.69.160/27
52.245.69.192/26
52.245.70.0/23
52.255.0.0/19
65.55.144.0/23
65.55.146.0/24
104.43.128.0/17
104.44.88.160/27
104.44.91.160/27
104.44.92.224/27
104.44.94.80/28
104.208.0.0/19
104.208.32.0/20
131.253.36.224/27
157.55.108.0/23
168.61.128.0/24
168.61.129.0/25
168.61.129.128/26
168.61.129.208/28
168.61.129.224/27
168.61.130.64/26
168.61.130.128/25
168.61.131.0/26
168.61.131.128/25
168.61.132.0/26
168.61.144.0/20
168.61.160.0/19
168.61.208.0/20
193.149.72.0/21
</Region>

<Region Name="asiaeast">
13.70.0.0/18
13.72.192.0/19
13.75.0.0/17
13.88.208.0/20
13.94.0.0/18
20.187.64.0/18
20.189.64.0/18
20.190.140.128/25
23.97.64.0/19
23.98.32.0/21
23.98.40.0/22
23.98.44.0/24
23.99.96.0/19
23.100.88.0/21
23.101.0.0/20
23.102.200.0/23
23.102.224.0/19
40.77.134.0/24
40.77.136.16/28
40.77.160.32/27
40.77.160.64/26
40.77.160.128/25
40.77.161.0/26
40.77.161.128/25
40.77.175.128/27
40.77.192.0/22
40.77.226.0/25
40.77.234.128/27
40.77.252.0/23
40.79.210.0/24
40.81.16.0/20
40.83.64.0/18
40.87.192.0/22
40.126.12.128/25
52.108.32.0/22
52.109.120.0/22
52.114.0.0/21
52.114.52.0/23
52.115.40.0/22
52.115.44.0/23
52.139.128.0/18
52.175.0.0/17
52.184.0.0/17
52.229.128.0/17
52.232.153.0/24
52.239.128.0/24
52.239.224.0/24
52.245.56.0/22
52.246.128.0/20
65.52.160.0/19
104.44.88.192/27
104.44.90.224/27
104.44.91.192/27
104.44.94.96/28
104.46.24.0/22
104.46.160.0/19
104.208.64.0/18
104.214.160.0/19
111.221.29.0/24
111.221.30.0/23
111.221.78.0/23
131.253.13.100/30
131.253.13.104/30
131.253.35.192/26
134.170.192.0/21
137.116.160.0/20

168.63.128.0/24
168.63.129.0/28
168.63.129.32/27
168.63.129.64/26
168.63.129.128/25
168.63.130.0/23
168.63.132.0/22
168.63.136.0/21
168.63.144.0/20
168.63.192.0/19
191.232.140.0/24
191.234.2.0/23
191.234.16.0/20
191.237.238.0/24
204.231.197.0/24
207.46.67.160/27
207.46.67.192/27
207.46.72.0/27
207.46.77.224/28
207.46.87.0/24
207.46.89.16/28
207.46.95.32/27
207.46.126.0/24
207.46.128.0/19
</Region>
<Region Name="europeeast">
40.78.213.0/24
40.80.28.0/22
52.109.84.0/22
</Region>
<Region Name="useast2euap">
20.39.0.0/19
20.190.138.0/25
40.70.88.0/28
40.74.144.0/20
40.75.32.0/21
40.78.208.0/28
40.79.88.0/27
40.79.88.32/28
40.79.89.0/24
40.79.96.0/19
40.89.64.0/18
40.90.137.32/27
40.90.146.192/27
40.91.12.0/28
40.91.12.32/28
40.91.13.0/28
40.126.10.0/25
52.138.64.0/20
52.138.88.0/21
52.143.212.0/23
52.147.128.0/19
52.184.168.16/28
52.184.168.32/28
52.225.136.48/28
52.225.144.0/20
52.225.160.0/19
52.232.150.0/24
52.239.157.224/27
52.239.165.192/26
52.239.184.128/27
52.239.184.176/28
52.239.184.224/27
52.239.185.0/28
52.239.192.128/27
52.239.198.128/27
52.239.230.0/24

52.239.239.0/24
52.245.45.144/28
52.245.46.32/28
52.245.46.80/28
52.245.46.96/28
52.245.47.0/24
52.253.150.0/23
52.253.152.0/23
52.253.224.0/21
52.254.120.0/21
104.44.95.208/28
</Region>
<Region Name="useast2">
13.68.0.0/17
13.77.64.0/18
20.36.128.0/17
20.38.100.0/23
20.41.0.0/18
20.186.0.0/17
20.186.128.0/18
20.190.131.0/24
20.190.192.0/18
23.100.64.0/21
23.101.32.0/20
23.101.80.0/20
23.101.144.0/20
23.102.96.0/19
23.102.204.0/22
23.102.208.0/20
40.65.192.0/18
40.67.128.0/19
40.70.0.0/18
40.70.64.0/20
40.70.80.0/21
40.70.128.0/17
40.75.0.0/19
40.75.64.0/18
40.77.128.128/25
40.77.129.0/24
40.77.130.0/25
40.77.132.0/24
40.77.136.48/28
40.77.163.0/24
40.77.166.160/27
40.77.167.0/24
40.77.168.0/24
40.77.170.0/24
40.77.175.96/27
40.77.177.0/24
40.77.178.0/23
40.77.182.0/28
40.77.182.32/27
40.77.184.0/25
40.77.224.128/25
40.77.228.0/24
40.77.233.0/24
40.77.234.192/27
40.77.240.0/25
40.77.245.0/24
40.77.248.0/25
40.77.251.0/24
40.78.208.48/28
40.78.220.0/24
40.79.0.0/21
40.79.8.0/27
40.79.8.32/28
40.79.8.64/27

40.79.8.96/28
40.79.9.0/24
40.79.16.0/20
40.79.32.0/20
40.79.48.0/27
40.79.48.32/28
40.79.49.0/24
40.79.56.0/21
40.79.64.0/20
40.79.80.0/21
40.79.90.0/24
40.79.91.0/28
40.79.92.0/24
40.79.93.0/28
40.79.94.0/24
40.79.95.0/28
40.82.4.0/22
40.84.0.0/17
40.87.168.0/22
40.90.130.160/27
40.90.132.128/26
40.90.136.0/28
40.90.138.160/27
40.90.140.160/27
40.90.140.192/27
40.90.143.192/26
40.90.144.64/26
40.90.145.32/27
40.90.145.64/27
40.90.148.96/27
40.91.12.16/28
40.91.12.48/28
40.91.12.64/26
40.91.12.128/28
40.91.12.160/27
40.91.12.208/28
40.91.12.240/28
40.91.13.64/27
40.91.13.96/28
40.91.13.128/27
40.91.13.240/28
40.91.14.0/24
40.123.0.0/17
40.126.3.0/24
52.109.4.0/22
52.114.136.0/21
52.114.180.0/23
52.115.48.0/22
52.115.52.0/23
52.125.136.0/24
52.136.29.0/24
52.138.80.0/21
52.138.96.0/19
52.143.192.0/24
52.147.160.0/19
52.167.0.0/16
52.177.0.0/16
52.179.128.0/17
52.184.128.0/19
52.184.160.0/21
52.184.168.0/28
52.184.168.80/28
52.184.168.96/27
52.184.168.128/28
52.184.169.0/24
52.184.170.0/24
52.184.176.0/20

52.184.192.0/18
52.225.128.0/21
52.225.136.0/27
52.225.136.32/28
52.225.136.64/28
52.225.137.0/24
52.225.192.0/18
52.232.151.0/24
52.232.160.0/19
52.232.192.0/18
52.239.156.0/24
52.239.157.0/25
52.239.157.128/26
52.239.157.192/27
52.239.172.0/22
52.239.184.0/25
52.239.184.160/28
52.239.184.192/27
52.239.185.32/27
52.239.185.64/27
52.239.192.0/25
52.239.192.160/27
52.239.192.192/26
52.239.198.0/25
52.239.198.160/27
52.239.198.192/26
52.239.206.0/24
52.239.207.0/27
52.239.207.32/28
52.239.207.64/26
52.239.207.128/26
52.239.222.0/23
52.242.64.0/18
52.245.44.0/24
52.245.45.0/25
52.245.45.128/28
52.245.45.160/27
52.245.45.192/26
52.245.46.0/27
52.245.46.48/28
52.245.46.64/28
52.245.46.112/28
52.245.46.128/28
52.245.46.160/27
52.245.46.192/27
52.245.46.224/28
52.247.0.0/17
52.250.128.0/18
52.251.0.0/17
52.252.0.0/17
52.253.64.0/20
52.253.148.0/23
52.253.154.0/23
52.254.0.0/18
52.254.64.0/19
52.254.96.0/20
52.254.112.0/21
65.52.108.0/23
65.52.110.0/24
65.55.44.16/28
65.55.44.32/27
65.55.44.64/27
65.55.44.96/28
65.55.44.128/27
65.55.60.188/30
65.55.105.0/26
65.55.105.96/27

65.55.105.224/27
65.55.106.0/26
65.55.106.64/27
65.55.106.128/26
65.55.107.48/28
65.55.107.64/27
65.55.108.0/24
65.55.209.128/26
65.55.211.32/27
65.55.213.64/26
65.55.213.128/26
65.55.217.0/24
65.55.219.32/27
65.55.219.128/25
104.44.88.32/27
104.44.88.96/27
104.44.91.96/27
104.44.93.160/27
104.44.94.48/28
104.46.0.0/21
104.46.96.0/19
104.46.192.0/20
104.47.200.0/21
104.208.128.0/17
104.209.128.0/17
104.210.0.0/20
131.253.12.208/28
131.253.12.224/30
131.253.13.16/29
131.253.13.48/28
131.253.13.72/29
131.253.13.80/29
131.253.13.96/30
131.253.14.16/28
131.253.14.208/28
131.253.14.224/28
131.253.15.8/29
131.253.15.16/28
131.253.24.0/28
131.253.24.192/26
131.253.34.224/27
131.253.38.0/27
131.253.38.128/26
134.170.221.0/24
137.116.0.0/18
137.116.64.0/19
137.116.96.0/22
157.55.7.128/26
157.55.10.192/26
157.55.11.128/25
157.55.37.0/24
157.55.38.0/24
157.55.48.0/24
157.55.50.0/25
157.55.55.100/30
157.55.55.104/29
157.55.55.136/29
157.55.55.144/29
157.55.55.160/29
157.56.2.128/25
157.56.3.0/25
191.236.192.0/18
191.237.128.0/18
191.239.224.0/20
193.149.64.0/21
199.30.18.0/23
199.30.20.0/24

199.30.22.0/24
199.30.28.64/26
199.30.28.128/25
199.30.29.0/24
</Region>
<Region Name="useast">
13.68.128.0/17
13.72.64.0/18
13.82.0.0/16
13.90.0.0/16
13.92.0.0/16
20.38.98.0/24
20.39.32.0/19
20.42.0.0/17
20.185.0.0/16
20.190.130.0/24
23.96.0.0/17
23.98.45.0/24
23.100.16.0/20
23.101.128.0/20
40.64.0.0/16
40.71.0.0/16
40.76.0.0/16
40.78.219.0/24
40.78.224.0/21
40.79.152.0/21
40.80.144.0/21
40.82.24.0/22
40.85.160.0/19
40.87.0.0/17
40.87.164.0/22
40.88.0.0/16
40.90.130.96/28
40.90.131.224/27
40.90.136.16/28
40.90.136.32/27
40.90.137.96/27
40.90.139.224/27
40.90.143.0/27
40.90.146.64/26
40.90.147.0/27
40.90.148.64/27
40.90.150.32/27
40.90.224.0/19
40.91.4.0/22
40.112.48.0/20
40.114.0.0/17
40.117.32.0/19
40.117.64.0/18
40.117.128.0/17
40.121.0.0/16
40.126.2.0/24
52.108.16.0/21
52.109.12.0/22
52.114.132.0/22
52.125.132.0/22
52.136.64.0/18
52.142.0.0/18
52.146.0.0/17
52.147.192.0/18
52.149.128.0/17
52.150.0.0/17
52.151.128.0/17
52.152.128.0/17
52.154.64.0/18
52.159.96.0/19
52.168.0.0/16

52.170.0.0/16
52.179.0.0/17
52.186.0.0/16
52.188.0.0/16
52.190.0.0/17
52.191.0.0/18
52.191.64.0/19
52.191.96.0/21
52.191.104.0/27
52.191.105.0/24
52.191.106.0/24
52.191.112.0/20
52.191.192.0/18
52.224.0.0/16
52.226.0.0/16
52.232.146.0/24
52.234.128.0/17
52.239.152.0/22
52.239.168.0/22
52.239.207.192/26
52.239.214.0/23
52.239.220.0/23
52.239.246.0/23
52.239.252.0/24
52.240.0.0/17
52.245.8.0/22
52.245.104.0/22
52.249.128.0/17
52.255.128.0/17
65.54.19.128/27
104.41.128.0/19
104.44.91.32/27
104.44.94.16/28
104.44.95.160/27
104.44.95.240/28
104.45.128.0/18
104.45.192.0/20
104.211.0.0/18
137.116.112.0/20
137.117.32.0/19
137.117.64.0/18
137.135.64.0/18
138.91.96.0/19
157.56.176.0/21
168.61.32.0/20
168.61.48.0/21
168.62.32.0/19
168.62.160.0/19
191.233.16.0/21
191.234.32.0/19
191.236.0.0/18
191.237.0.0/17
191.238.0.0/18
</Region>
<Region Name="francec">
20.39.232.0/21
20.39.240.0/20
20.40.128.0/19
20.43.32.0/19
20.188.32.0/19
20.190.147.0/25
40.66.32.0/19
40.79.128.0/20
40.79.144.0/21
40.79.222.0/24
40.80.24.0/22
40.89.128.0/18

40.90.130.240/28
40.90.132.0/27
40.90.136.64/26
40.90.136.128/27
40.90.147.128/26
40.90.147.192/27
40.126.19.0/25
52.108.52.0/23
52.109.68.0/22
52.114.104.0/22
52.143.128.0/18
52.143.215.0/24
52.143.216.0/23
52.239.134.0/24
52.239.194.0/24
52.239.241.0/24
52.245.116.0/22
</Region>
<Region Name="frances">
20.38.188.0/22
20.39.80.0/20
20.190.147.128/25
40.79.176.0/21
40.79.223.0/24
40.80.20.0/22
40.82.224.0/20
40.90.132.32/28
40.90.136.192/27
40.90.147.224/27
40.126.19.128/25
52.108.222.0/23
52.109.72.0/22
52.114.108.0/22
52.136.28.0/24
52.136.128.0/18
52.239.135.0/26
52.239.196.0/24
52.245.120.0/22
</Region>
<Region Name="japaneast">
13.71.128.0/19
13.73.0.0/19
13.78.0.0/17
20.37.96.0/19
20.40.88.0/21
20.40.96.0/21
20.43.64.0/19
20.188.0.0/19
20.190.141.128/25
23.98.57.0/24
23.100.96.0/21
23.102.64.0/19
40.79.184.0/21
40.79.192.0/21
40.79.208.0/24
40.81.192.0/19
40.87.200.0/22
40.90.132.64/28
40.90.142.0/27
40.90.142.192/28
40.90.148.224/27
40.115.128.0/17
40.126.13.128/25
52.108.228.0/23
52.109.52.0/22
52.114.32.0/22
52.140.192.0/18

52.155.96.0/19
52.156.32.0/19
52.185.128.0/18
52.232.155.0/24
52.239.144.0/23
52.243.32.0/19
52.245.36.0/22
52.246.160.0/19
52.253.96.0/19
104.41.160.0/19
104.44.88.224/27
104.44.91.224/27
104.44.94.112/28
104.46.208.0/20
138.91.0.0/20
191.234.138.0/23
191.237.240.0/23
191.239.128.0/19
</Region>
<Region Name="japanwest">
13.73.232.0/21
20.39.176.0/21
20.189.192.0/18
20.190.141.0/25
23.98.56.0/24
23.100.104.0/21
40.74.64.0/18
40.74.128.0/20
40.79.209.0/24
40.81.176.0/20
40.87.204.0/22
40.90.137.0/27
40.90.142.208/28
40.126.13.0/25
52.108.46.0/23
52.109.132.0/22
52.114.36.0/22
52.147.64.0/19
52.175.128.0/18
52.232.158.0/24
52.239.146.0/23
52.245.92.0/22
104.44.92.0/27
104.44.94.128/28
104.46.224.0/20
104.214.128.0/19
104.215.0.0/18
138.91.16.0/20
191.233.32.0/19
191.237.236.0/24
191.238.68.0/24
191.238.80.0/21
191.238.88.0/22
191.238.92.0/23
191.239.96.0/20
</Region>
<Region Name="koreacentral">
20.39.184.0/21
20.39.192.0/20
20.41.64.0/18
20.190.144.128/25
20.190.148.128/25
40.79.221.0/24
40.80.36.0/22
40.82.128.0/19
40.90.131.128/27
40.90.139.128/27

40.126.16.128/25
40.126.20.128/25
52.108.48.0/23
52.109.44.0/22
52.114.44.0/22
52.141.0.0/18
52.231.0.0/17
52.232.145.0/24
52.239.148.0/27
52.239.164.192/26
52.239.190.128/26
52.245.112.0/22
104.44.90.160/27
</Region>
<Region Name="koreasouth">
20.39.168.0/21
20.190.148.0/25
40.79.220.0/24
40.80.32.0/22
40.80.224.0/20
40.89.192.0/19
40.90.131.160/27
40.90.139.160/27
40.126.20.0/25
52.108.226.0/23
52.109.48.0/22
52.114.48.0/22
52.147.96.0/19
52.231.128.0/17
52.232.144.0/24
52.239.165.0/26
52.239.165.160/27
52.239.190.192/26
52.245.100.0/22
104.44.94.224/27
</Region>
<Region Name="usnorth">
20.36.96.0/21
20.41.128.0/18
20.190.135.0/24
23.96.128.0/17
23.98.48.0/21
23.100.72.0/21
23.100.224.0/20
23.101.160.0/20
40.77.131.224/28
40.77.136.96/28
40.77.165.0/24
40.77.175.0/27
40.77.176.0/24
40.77.182.128/27
40.77.183.0/24
40.77.188.0/22
40.77.224.0/28
40.77.224.32/27
40.77.231.0/24
40.77.234.0/25
40.77.236.32/27
40.77.248.128/25
40.78.208.64/28
40.78.222.0/24
40.81.32.0/20
40.87.172.0/22
40.90.132.96/27
40.90.140.128/27
40.90.144.32/27
40.91.24.0/22

40.116.0.0/16
40.126.7.0/24
52.109.16.0/22
52.114.168.0/22
52.141.128.0/18
52.162.0.0/16
52.232.156.0/24
52.237.128.0/18
52.239.149.0/24
52.239.186.0/24
52.240.128.0/17
52.245.72.0/22
52.251.128.0/17
52.252.128.0/17
65.52.0.0/19
65.52.48.0/20
65.52.106.16/28
65.52.106.32/27
65.52.106.64/26
65.52.106.128/27
65.52.192.0/19
65.52.232.0/21
65.52.240.0/21
65.55.25.128/25
65.55.54.128/25
65.55.60.176/29
65.55.105.64/27
65.55.105.192/27
65.55.106.208/28
65.55.106.224/28
65.55.109.0/24
65.55.208.0/24
65.55.211.0/27
65.55.211.192/26
65.55.212.0/27
65.55.212.64/26
65.55.212.128/25
65.55.213.0/27
65.55.218.0/24
65.55.219.0/27
104.44.88.128/27
104.44.91.128/27
104.44.94.64/28
104.47.220.0/22
131.253.12.16/28
131.253.12.40/29
131.253.12.48/29
131.253.12.176/28
131.253.12.192/28
131.253.12.248/29
131.253.13.0/28
131.253.13.32/28
131.253.13.160/28
131.253.14.32/27
131.253.14.64/28
131.253.14.160/27
131.253.14.248/29
131.253.15.32/27
131.253.15.64/26
131.253.15.160/27
131.253.15.208/28
131.253.15.224/27
131.253.24.128/27
131.253.25.0/24
131.253.26.128/25
131.253.27.0/24
131.253.36.128/26

131.253.36.192/27
131.253.38.32/27
131.253.38.192/26
131.253.40.0/24
134.170.220.0/24
157.55.24.0/21
157.55.55.0/27
157.55.55.32/28
157.55.55.112/28
157.55.55.152/29
157.55.55.168/29
157.55.55.176/29
157.55.55.200/29
157.55.55.216/29
157.55.60.208/28
157.55.60.224/27
157.55.64.0/20
157.55.106.128/25
157.55.110.0/23
157.55.115.0/25
157.55.136.0/21
157.55.151.0/28
157.55.160.0/20
157.55.208.0/21
157.55.248.0/21
157.56.0.0/24
157.56.8.0/21
157.56.24.160/27
157.56.24.192/28
157.56.28.0/22
157.56.216.0/26
168.62.96.0/19
168.62.224.0/19
191.233.144.0/24
191.233.145.0/28
191.233.152.0/21
191.233.160.0/20
191.233.176.0/21
191.236.128.0/18
199.30.17.0/24
199.30.23.0/24
207.46.193.192/28
207.46.193.224/27
207.46.198.128/25
207.46.200.96/27
207.46.200.176/28
207.46.202.128/28
207.46.205.0/24
207.68.174.24/29
207.68.174.40/29
207.68.174.48/29
207.68.174.112/28
207.68.174.184/29
207.68.174.192/27
</Region>
<Region Name="europenorth2">
40.78.212.0/24
40.80.4.0/22
52.109.80.0/22
</Region>
<Region Name="europenorth">
13.69.128.0/17
13.70.192.0/18
13.74.0.0/16
13.79.0.0/16
13.94.64.0/18
20.38.64.0/19

20.38.102.0/23
20.190.129.0/24
20.191.0.0/18
23.100.48.0/20
23.100.128.0/18
23.101.48.0/20
23.102.0.0/18
40.67.224.0/19
40.69.0.0/18
40.69.64.0/19
40.69.192.0/19
40.77.133.0/24
40.77.136.32/28
40.77.136.80/28
40.77.162.0/24
40.77.174.0/24
40.77.175.160/27
40.77.182.96/27
40.77.226.128/25
40.77.229.0/24
40.77.234.160/27
40.77.236.0/27
40.78.211.0/24
40.85.0.0/17
40.85.128.0/20
40.87.128.0/19
40.87.188.0/22
40.90.129.192/27
40.90.133.64/27
40.90.136.176/28
40.90.137.192/27
40.90.141.96/27
40.90.141.128/27
40.90.145.0/27
40.90.145.224/27
40.90.148.160/28
40.90.149.128/25
40.91.20.0/22
40.91.32.0/22
40.112.0.0/19
40.112.36.0/25
40.112.37.64/26
40.112.64.0/19
40.113.0.0/18
40.113.64.0/19
40.115.96.0/19
40.126.1.0/24
40.127.96.0/20
40.127.128.0/17
51.104.64.0/18
51.104.128.0/17
52.108.240.0/21
52.109.76.0/22
52.114.76.0/22
52.114.96.0/21
52.114.120.0/22
52.115.16.0/21
52.115.24.0/22
52.125.138.0/23
52.138.128.0/17
52.142.64.0/18
52.143.195.0/24
52.143.209.0/24
52.146.128.0/17
52.155.64.0/19
52.155.128.0/17
52.156.192.0/18

52.158.0.0/17
52.164.0.0/16
52.169.0.0/16
52.178.128.0/17
52.232.148.0/24
52.236.0.0/17
52.239.136.0/22
52.239.205.0/24
52.239.248.0/24
52.245.40.0/22
52.245.88.0/22
64.4.22.128/25
64.4.50.128/25
65.52.64.0/20
65.52.224.0/21
65.55.4.0/24
65.55.60.160/29
65.55.60.168/30
65.55.211.128/26
65.55.216.0/24
94.245.88.0/21
94.245.104.0/21
94.245.114.1/32
94.245.114.2/31
94.245.114.4/32
94.245.114.33/32
94.245.114.34/31
94.245.114.36/32
94.245.117.96/27
94.245.118.0/27
94.245.118.65/32
94.245.118.66/31
94.245.118.68/32
94.245.118.97/32
94.245.118.98/31
94.245.118.100/32
94.245.118.129/32
94.245.118.130/31
94.245.118.132/32
94.245.120.128/28
94.245.122.0/24
94.245.123.144/28
94.245.123.176/28
104.41.64.0/18
104.41.192.0/18
104.44.88.64/27
104.44.91.64/27
104.44.92.192/27
104.44.94.32/28
104.45.80.0/20
104.45.96.0/19
104.46.8.0/21
104.46.64.0/19
104.47.218.0/23
131.253.12.72/29
131.253.13.108/30
131.253.15.144/28
131.253.37.0/24
131.253.38.104/29
137.116.224.0/19
137.135.128.0/17
138.91.48.0/20
157.55.3.0/24
157.55.10.160/29
157.55.10.176/28
157.55.13.128/26
157.55.55.64/27

157.55.55.192/29
157.55.106.64/26
157.55.107.0/24
157.55.204.128/25
157.55.230.160/27
168.61.80.0/20
168.61.96.0/19
168.63.32.0/19
168.63.64.0/20
168.63.80.0/21
168.63.92.0/22
191.232.138.0/23
191.235.128.0/18
191.235.192.0/22
191.235.208.0/20
191.235.255.0/24
191.237.192.0/23
191.237.194.0/24
191.237.196.0/24
191.237.208.0/20
191.238.96.0/19
191.239.208.0/20
193.149.88.0/21
199.30.21.0/24
199.30.28.0/26
207.46.194.0/24
207.68.174.32/29
207.68.174.80/28
207.68.174.136/29
207.68.174.152/29
207.68.174.248/29
213.199.168.0/23
</Region>
<Region Name="ussouth">
13.65.0.0/16
13.66.0.0/17
13.73.240.0/20
13.84.0.0/15
20.38.104.0/23
20.188.64.0/19
20.189.0.0/18
20.190.128.0/24
23.98.128.0/17
23.100.120.0/21
23.100.192.0/19
23.101.176.0/20
23.102.128.0/18
40.74.160.0/19
40.74.192.0/18
40.77.130.192/26
40.77.131.0/25
40.77.131.128/26
40.77.172.0/24
40.77.175.224/28
40.77.225.0/24
40.78.214.0/24
40.80.192.0/19
40.84.128.0/17
40.86.128.0/19
40.87.176.0/22
40.90.133.96/27
40.90.136.160/28
40.90.141.192/27
40.90.145.96/27
40.90.145.160/27
40.90.148.0/26
40.91.16.0/22

40.119.0.0/18
40.124.0.0/16
40.126.0.0/24
52.108.248.0/21
52.109.20.0/22
52.114.144.0/22
52.125.137.0/24
52.141.64.0/18
52.152.0.0/17
52.153.64.0/18
52.153.192.0/18
52.171.0.0/16
52.183.192.0/18
52.185.192.0/18
52.189.128.0/18
52.232.159.0/24
52.239.158.0/23
52.239.178.0/23
52.239.180.0/22
52.239.199.0/24
52.239.200.0/23
52.239.203.0/24
52.239.204.0/24
52.239.208.0/23
52.245.24.0/22
52.248.0.0/17
52.249.0.0/18
52.253.0.0/18
52.255.64.0/18
65.52.32.0/21
65.54.55.160/27
65.54.55.224/27
70.37.48.0/20
70.37.64.0/18
70.37.160.0/21
104.44.89.0/27
104.44.89.64/27
104.44.92.64/27
104.44.94.160/27
104.44.128.0/18
104.47.208.0/23
104.210.128.0/19
104.210.176.0/20
104.210.192.0/19
104.214.0.0/17
104.215.64.0/18
157.55.51.224/28
157.55.80.0/21
157.55.103.32/27
157.55.153.224/28
157.55.176.0/20
157.55.192.0/21
157.55.200.0/22
157.55.204.0/27
157.55.204.32/28
168.62.128.0/19
191.238.136.0/21
191.238.144.0/20
191.238.160.0/19
191.238.224.0/19
</Region>
<Region Name="indiasouth">
13.71.64.0/18
20.40.0.0/21
20.41.192.0/18
20.190.145.128/25
40.78.192.0/21

40.79.213.0/24
40.81.64.0/20
40.87.216.0/22
40.90.130.224/28
40.90.137.160/27
40.90.140.64/27
40.90.147.96/27
40.126.17.128/25
52.108.230.0/23
52.109.60.0/22
52.114.24.0/22
52.136.17.0/24
52.140.0.0/18
52.172.0.0/17
52.239.135.128/26
52.239.188.0/24
52.245.84.0/22
104.44.92.160/27
104.44.94.208/28
104.47.214.0/23
104.211.192.0/18
</Region>
<Region Name="asiasoutheast">
13.67.0.0/17
13.76.0.0/16
20.43.128.0/18
20.184.0.0/18
20.188.96.0/19
20.190.64.0/19
20.190.140.0/25
20.191.128.0/19
23.97.48.0/20
23.98.64.0/18
23.100.112.0/21
23.101.16.0/20
40.65.128.0/18
40.78.223.0/24
40.78.232.0/21
40.82.28.0/22
40.87.196.0/22
40.90.133.128/27
40.90.137.64/27
40.90.138.96/27
40.90.141.224/27
40.90.145.128/27
40.90.146.160/27
40.90.146.224/27
40.90.160.0/19
40.119.192.0/18
40.126.12.0/25
52.108.236.0/22
52.109.124.0/22
52.114.8.0/21
52.114.56.0/23
52.115.32.0/22
52.115.36.0/23
52.136.26.0/24
52.139.192.0/18
52.143.196.0/24
52.143.210.0/24
52.148.64.0/18
52.163.0.0/16
52.187.0.0/17
52.187.128.0/18
52.230.0.0/17
52.237.64.0/18
52.239.129.0/24

52.239.197.0/24
52.239.227.0/24
52.239.249.0/24
52.245.80.0/22
52.253.80.0/20
65.55.106.96/27
65.55.214.0/24
104.43.0.0/17
104.44.89.32/27
104.44.90.128/27
104.44.92.32/27
104.44.94.144/28
104.44.95.192/28
104.44.95.224/28
104.46.128.0/19
104.215.128.0/17
111.221.80.0/20
111.221.96.0/20
131.253.12.96/27
131.253.12.128/27
131.253.13.64/29
131.253.34.0/25
131.253.38.112/29
137.116.128.0/19
138.91.32.0/20
168.63.90.0/24
168.63.91.0/26
168.63.160.0/19
168.63.224.0/19
191.238.64.0/23
207.46.50.128/28
207.46.59.64/27
207.46.63.64/27
207.46.63.128/25
207.46.224.0/20
207.68.174.128/29
207.68.174.144/29
207.68.174.160/29
</Region>
<Region Name="uknorth">
13.87.64.0/18
20.39.144.0/20
20.190.143.128/25
40.79.202.0/24
40.80.16.0/22
40.81.96.0/20
40.90.130.112/28
40.90.143.32/27
40.90.150.64/27
40.126.15.128/25
51.141.129.32/27
51.141.133.0/24
51.141.152.0/22
51.142.128.0/17
52.109.36.0/22
52.136.19.0/24
</Region>
<Region Name="uksouth2">
13.87.0.0/18
40.79.201.0/24
40.80.12.0/22
40.81.160.0/20
40.90.130.128/28
40.90.143.64/27
40.90.150.96/27
51.141.129.0/27
51.141.129.192/26

51.141.132.0/24
51.141.156.0/22
51.142.0.0/17
51.143.192.0/18
52.109.40.0/22
52.136.18.0/24
</Region>
<Region Name="uksouth">
20.38.106.0/23
20.39.208.0/20
20.39.224.0/21
20.190.143.0/25
40.79.215.0/24
40.80.0.0/22
40.81.128.0/19
40.90.131.64/27
40.90.139.64/27
40.126.15.0/25
51.104.0.0/19
51.105.0.0/18
51.140.0.0/17
51.140.128.0/18
51.141.128.32/27
51.141.129.64/26
51.141.130.0/25
51.141.135.0/24
51.141.144.0/22
51.141.192.0/18
51.143.128.0/18
51.145.0.0/17
52.108.50.0/23
52.109.28.0/22
52.114.80.0/22
52.114.88.0/22
52.136.21.0/24
52.151.64.0/18
52.239.187.0/25
52.239.231.0/24
52.245.64.0/22
104.44.89.224/27
</Region>
<Region Name="ukwest">
20.39.160.0/21
20.40.104.0/21
20.190.144.0/25
40.79.218.0/24
40.81.112.0/20
40.87.228.0/22
40.90.131.96/27
40.90.139.96/27
40.126.16.0/25
51.104.32.0/19
51.137.128.0/18
51.140.192.0/18
51.141.0.0/17
51.141.128.0/27
51.141.128.64/26
51.141.128.128/25
51.141.129.128/26
51.141.134.0/24
51.141.136.0/23
51.141.148.0/22
52.108.224.0/23
52.109.32.0/22
52.114.84.0/22
52.114.92.0/22
52.136.20.0/24

52.142.128.0/18
52.239.240.0/24
104.44.90.0/27
</Region>
<Region Name="uswestcentral">
13.71.192.0/18
13.77.192.0/19
13.78.128.0/17
20.190.136.0/24
40.77.128.0/25
40.77.131.192/27
40.77.131.240/28
40.77.135.0/24
40.77.166.0/25
40.77.166.128/28
40.77.173.0/24
40.77.175.32/27
40.77.182.160/27
40.77.185.0/25
40.77.224.16/28
40.77.224.64/27
40.77.227.0/24
40.77.232.0/25
40.77.235.0/24
40.77.236.96/27
40.77.246.0/24
40.78.218.0/24
40.90.131.0/27
40.90.138.192/28
40.90.139.0/27
40.90.143.96/27
40.90.151.0/26
40.90.151.128/28
40.126.8.0/24
52.109.136.0/22
52.136.4.0/22
52.143.214.0/24
52.148.0.0/18
52.150.128.0/17
52.153.128.0/18
52.159.0.0/18
52.161.0.0/16
52.239.164.0/25
52.239.167.0/24
52.239.244.0/23
52.245.60.0/22
52.253.128.0/20
64.4.8.0/24
64.4.54.0/24
65.55.209.192/26
104.44.89.96/27
104.47.224.0/20
131.253.24.160/27
157.55.12.128/26
157.55.103.128/25
</Region>
<Region Name="europewest">
13.69.0.0/17
13.73.128.0/18
13.73.224.0/21
13.80.0.0/15
13.88.200.0/21
13.93.0.0/17
13.94.128.0/17
13.95.0.0/16
20.38.108.0/23
20.190.137.0/24

23.97.128.0/17
23.98.46.0/24
23.100.0.0/20
23.101.64.0/20
40.67.192.0/19
40.68.0.0/16
40.74.0.0/18
40.78.210.0/24
40.87.184.0/22
40.90.130.0/27
40.90.133.0/27
40.90.138.0/27
40.90.141.32/27
40.90.141.160/27
40.90.142.224/28
40.90.144.192/27
40.90.145.192/27
40.90.146.16/28
40.90.146.128/27
40.90.150.128/25
40.91.28.0/22
40.91.192.0/18
40.112.36.128/25
40.112.37.0/26
40.112.38.192/26
40.112.96.0/19
40.113.96.0/19
40.113.128.0/18
40.114.128.0/17
40.115.0.0/18
40.118.0.0/17
40.119.128.0/19
40.126.9.0/24
51.105.128.0/17
51.136.0.0/16
51.137.0.0/17
51.137.192.0/18
51.144.0.0/16
51.145.128.0/17
52.108.24.0/21
52.108.56.0/21
52.109.88.0/22
52.114.64.0/21
52.114.72.0/22
52.114.116.0/22
52.115.0.0/21
52.115.8.0/22
52.125.140.0/23
52.136.192.0/18
52.137.0.0/18
52.142.192.0/18
52.143.0.0/18
52.143.194.0/24
52.143.208.0/24
52.148.192.0/18
52.149.64.0/18
52.157.64.0/18
52.157.128.0/17
52.166.0.0/16
52.174.0.0/16
52.178.0.0/17
52.232.0.0/17
52.232.147.0/24
52.233.128.0/17
52.236.128.0/17
52.239.140.0/22
52.239.212.0/23

52.239.242.0/23
52.245.48.0/22
52.245.124.0/22
65.52.128.0/19
104.40.128.0/17
104.44.89.160/27
104.44.90.192/27
104.44.93.0/27
104.44.93.192/27
104.44.95.80/28
104.44.95.96/28
104.45.0.0/18
104.45.64.0/20
104.46.16.0/21
104.46.32.0/19
104.47.128.0/18
104.47.216.64/26
104.214.192.0/18
137.116.192.0/19
137.117.128.0/17
157.55.8.64/26
157.55.8.144/28
157.56.117.64/27
168.61.56.0/21
168.63.0.0/19
168.63.96.0/19
191.233.64.0/18
191.237.232.0/22
191.239.200.0/22
193.149.80.0/21
213.199.128.0/20
213.199.180.32/28
213.199.180.96/27
213.199.180.192/27
213.199.183.0/24
</Region>
<Region Name="indiawest">
20.40.8.0/21
20.190.146.128/25
40.79.219.0/24
40.81.80.0/20
40.87.220.0/22
40.90.138.224/27
40.126.18.128/25
52.109.64.0/22
52.114.28.0/22
52.136.16.0/24
52.136.32.0/19
52.140.128.0/18
52.183.128.0/18
52.239.135.192/26
52.239.187.128/25
52.245.76.0/22
52.249.64.0/19
104.44.93.224/27
104.44.95.112/28
104.47.212.0/23
104.211.128.0/18
</Region>
<Region Name="uswest2">
13.66.128.0/17
13.77.128.0/18
20.36.0.0/19
20.38.99.0/24
20.42.128.0/18
20.187.0.0/18
20.190.0.0/18

20.190.133.0/24
20.191.64.0/18
20.191.160.0/19
23.98.47.0/24
23.102.192.0/21
23.102.203.0/24
23.103.64.32/27
23.103.64.64/27
23.103.66.0/23
40.65.64.0/18
40.77.136.0/28
40.77.136.64/28
40.77.160.0/27
40.77.164.0/24
40.77.166.144/32
40.77.169.0/24
40.77.171.0/24
40.77.175.64/27
40.77.180.0/23
40.77.182.64/27
40.77.185.128/25
40.77.186.0/26
40.77.186.128/25
40.77.187.0/24
40.77.224.96/27
40.77.230.0/24
40.77.232.128/25
40.77.234.224/27
40.77.236.64/29
40.77.236.128/27
40.77.240.128/25
40.77.241.0/24
40.77.242.0/23
40.77.244.0/24
40.77.247.0/24
40.77.249.0/24
40.77.250.0/24
40.78.208.32/30
40.78.217.0/24
40.78.240.0/20
40.80.160.0/24
40.82.36.0/22
40.87.232.0/21
40.90.131.32/27
40.90.132.48/28
40.90.136.224/27
40.90.138.208/28
40.90.139.32/27
40.90.146.32/27
40.90.148.192/27
40.90.192.0/19
40.91.0.0/22
40.91.64.0/18
40.91.128.0/18
40.125.64.0/18
40.126.5.0/24
51.141.160.0/19
51.143.0.0/17
52.96.11.0/24
52.109.24.0/22
52.114.148.0/22
52.136.0.0/22
52.137.64.0/18
52.143.64.0/18
52.143.197.0/24
52.143.211.0/24
52.148.128.0/18

52.149.0.0/18
52.151.0.0/18
52.156.64.0/18
52.156.128.0/19
52.158.224.0/19
52.175.192.0/18
52.183.0.0/17
52.191.128.0/18
52.229.0.0/18
52.232.152.0/24
52.233.64.0/18
52.235.64.0/18
52.239.148.128/25
52.239.176.128/25
52.239.193.0/24
52.239.210.0/23
52.239.236.0/23
52.245.52.0/22
52.246.192.0/18
52.247.192.0/18
52.250.0.0/17
65.52.104.0/24
65.52.111.0/24
65.54.247.128/25
65.55.2.0/24
65.55.32.128/27
65.55.32.192/27
65.55.32.224/28
65.55.33.176/28
65.55.33.192/28
65.55.35.192/27
65.55.44.8/29
65.55.44.112/28
65.55.51.0/24
65.55.60.128/27
65.55.105.128/26
65.55.106.192/28
65.55.106.240/28
65.55.107.0/27
65.55.107.32/28
65.55.107.96/27
65.55.107.128/25
65.55.110.0/24
65.55.120.0/24
65.55.189.128/25
65.55.207.0/24
65.55.209.0/25
65.55.210.0/24
65.55.211.64/26
65.55.212.32/27
65.55.213.32/27
65.55.213.192/26
65.55.215.0/24
65.55.219.64/26
65.55.250.0/24
65.55.252.0/24
70.37.0.0/21
70.37.8.0/22
70.37.16.0/20
70.37.32.0/20
104.44.89.128/27
104.44.89.192/27
104.44.95.0/28
131.253.12.8/29
131.253.12.36/30
131.253.12.56/29
131.253.12.64/29

131.253.12.160/28
131.253.12.228/30
131.253.13.24/29
131.253.13.88/30
131.253.13.112/28
131.253.13.128/27
131.253.13.176/28
131.253.13.192/26
131.253.14.4/30
131.253.14.8/31
131.253.14.80/28
131.253.14.96/27
131.253.14.128/27
131.253.14.192/29
131.253.15.128/28
131.253.15.192/28
131.253.24.16/28
131.253.24.32/27
131.253.24.64/26
131.253.26.0/25
131.253.34.128/26
131.253.35.0/25
131.253.35.128/26
131.253.38.64/27
131.253.38.96/29
131.253.41.0/24
134.170.222.0/23
137.116.176.0/21
157.55.2.128/26
157.55.12.64/26
157.55.13.64/26
157.55.39.0/24
157.55.55.128/29
157.55.55.184/29
157.55.55.228/30
157.55.55.232/29
157.55.55.240/28
157.55.106.0/26
157.55.154.128/25
157.56.1.0/24
157.56.2.0/25
157.56.3.128/25
157.56.19.224/27
157.56.21.32/27
157.56.21.64/26
157.56.21.128/26
157.56.21.192/27
157.56.80.0/25
168.62.64.0/19
191.232.137.0/24
191.237.224.0/21
191.237.244.0/22
191.239.196.0/24
191.239.197.0/28
199.30.16.0/24
199.30.24.0/23
199.30.26.0/24
199.30.27.0/25
199.30.27.144/28
199.30.27.160/27
199.30.27.192/26
199.30.30.0/23
207.46.13.0/24
207.68.174.0/29
207.68.174.56/29
207.68.174.64/29
207.68.174.96/28

207.68.174.168/29
207.68.174.176/29
209.240.212.0/23
</Region>
<Region Name="uswest">
13.64.0.0/16
13.73.32.0/19
13.83.0.0/16
13.86.128.0/17
13.87.128.0/17
13.88.0.0/17
13.88.128.0/18
13.88.192.0/23
13.91.0.0/16
13.93.128.0/17
20.43.192.0/18
20.184.128.0/17
20.187.128.0/17
20.189.128.0/18
20.190.132.0/24
23.99.0.0/18
23.99.64.0/19
23.100.32.0/20
23.101.192.0/20
40.65.0.0/18
40.75.128.0/17
40.78.0.0/17
40.78.216.0/24
40.80.152.0/21
40.81.0.0/20
40.83.128.0/17
40.85.144.0/20
40.86.160.0/19
40.87.160.0/22
40.90.131.192/27
40.90.139.192/27
40.90.146.0/28
40.90.148.128/27
40.112.128.0/17
40.118.128.0/17
40.126.4.0/24
52.108.0.0/21
52.109.0.0/22
52.114.152.0/21
52.114.184.0/23
52.115.56.0/22
52.115.60.0/23
52.137.128.0/17
52.153.0.0/18
52.155.32.0/19
52.157.0.0/18
52.159.128.0/17
52.160.0.0/16
52.180.0.0/17
52.190.128.0/17
52.225.0.0/17
52.232.149.0/24
52.234.0.0/17
52.238.0.0/18
52.239.0.0/17
52.239.160.0/22
52.239.228.0/23
52.239.254.0/23
52.241.0.0/16
52.245.12.0/22
52.245.108.0/22
52.246.0.0/17

52.248.128.0/17
52.250.192.0/18
52.254.128.0/17
65.52.112.0/20
104.40.0.0/17
104.42.0.0/16
104.44.88.0/27
104.44.91.0/27
104.44.92.96/27
104.44.94.0/28
104.44.95.128/27
104.45.208.0/20
104.45.224.0/19
104.209.0.0/18
104.210.32.0/19
137.116.184.0/21
137.117.0.0/19
137.135.0.0/18
138.91.64.0/19
138.91.128.0/17
157.56.160.0/21
168.61.0.0/19
168.61.64.0/20
168.62.0.0/19
168.62.192.0/19
168.63.88.0/23
191.233.8.0/21
191.236.64.0/18
191.238.70.0/23
191.239.0.0/18
</Region>
</AzurePublicIpAddresses>

8.2. Microsoft Corporation Public IP

Prefix,Type
13.64.0.0/11
13.96.0.0/13
13.104.0.0/14
20.36.0.0/14
20.40.0.0/13
20.128.0.0/16
20.140.0.0/15
20.144.0.0/14
20.160.0.0/12
20.176.0.0/14
20.180.0.0/14
20.184.0.0/13
23.96.0.0/13
40.64.0.0/10
42.159.0.0/16
51.4.0.0/15
51.8.0.0/16
51.10.0.0/15
51.12.0.0/15
51.18.0.0/16
51.51.0.0/16
51.53.0.0/16
51.103.0.0/16
51.104.0.0/15
51.107.0.0/16
51.116.0.0/16
51.120.0.0/16
51.124.0.0/16
51.132.0.0/16
51.136.0.0/15

51.138.0.0/16
51.140.0.0/14
51.144.0.0/15
52.96.0.0/12
52.112.0.0/14
52.120.0.0/14
52.125.0.0/16
52.126.0.0/15
52.130.0.0/15
52.132.0.0/14
52.136.0.0/13
52.145.0.0/16
52.146.0.0/15
52.148.0.0/14
52.152.0.0/13
52.160.0.0/11
52.224.0.0/11
64.4.0.0/18
65.52.0.0/14
66.119.144.0/20
70.37.0.0/17
70.37.128.0/18
91.190.216.0/21
94.245.64.0/18
103.9.8.0/22
103.25.156.0/24
103.25.157.0/24
103.25.158.0/23
103.36.96.0/22
103.255.140.0/22
104.40.0.0/13
104.146.0.0/15
104.208.0.0/13
111.221.16.0/20
111.221.64.0/18
129.75.0.0/16
131.253.1.0/24
131.253.3.0/24
131.253.5.0/24
131.253.6.0/24
131.253.8.0/24
131.253.12.0/22
131.253.16.0/23
131.253.18.0/24
131.253.21.0/24
131.253.22.0/23
131.253.24.0/21
131.253.32.0/20
131.253.61.0/24
131.253.62.0/23
131.253.64.0/18
131.253.128.0/17
132.245.0.0/16
134.170.0.0/16
134.177.0.0/16
137.116.0.0/15
137.135.0.0/16
138.91.0.0/16
138.196.0.0/16
139.217.0.0/16
139.219.0.0/16
141.251.0.0/16
146.147.0.0/16
147.243.0.0/16
150.171.0.0/16
150.242.48.0/22
157.54.0.0/15

157.56.0.0/14
157.60.0.0/16
167.220.0.0/16
168.61.0.0/16
168.62.0.0/15
191.232.0.0/13
192.32.0.0/16
192.48.225.0/24
192.84.159.0/24
192.84.160.0/23
192.100.102.0/24
192.100.103.0/24
192.197.157.0/24
193.149.64.0/19
193.221.113.0/24
194.69.96.0/19
194.110.197.0/24
198.49.8.0/24
198.105.232.0/22
198.200.130.0/24
198.206.164.0/24
199.60.28.0/24
199.74.210.0/24
199.103.90.0/23
199.103.122.0/24
199.242.32.0/20
199.242.48.0/21
202.89.224.0/20
204.13.120.0/21
204.14.180.0/22
204.79.135.0/24
204.79.179.0/24
204.79.181.0/24
204.79.188.0/24
204.79.195.0/24
204.79.196.0/23
204.79.252.0/24
204.152.18.0/23
204.152.140.0/23
204.231.192.0/24
204.231.194.0/23
204.231.197.0/24
204.231.198.0/23
204.231.200.0/21
204.231.208.0/20
204.231.236.0/24
205.174.224.0/20
206.138.168.0/21
206.191.224.0/19
207.46.0.0/16
207.68.128.0/18
208.68.136.0/21
208.76.44.0/22
208.84.0.0/21
209.240.192.0/19
213.199.128.0/18
216.32.180.0/22
216.220.208.0/20
2001:67c:1020::/48
2001:df0:7::/48
2001:df0:d7::/48
2001:df0:d8::/48
2001:df0:d9::/48
2001:4898::/32
2001:489a:2000::/35
2404:f801::/32
2603:1000::/24

2620:0:30::/45
2620:10c:5000::/44
2620:1ec::/36
2801:80:1d0::/48
2a01:110::/32
2a01:111::/32
2a01:4180::/32

9. Use and Agreement Contract

Owner: Michael Andre Franiatte.

Contact: michael.franiatte@gmail.com.

Owning: All works from scratch of the owner.

Proof of Owning: Works published, and writings/speakings all over.

Requirements of Use: Pay the owner, quote the owner, agreement of the owner.

Availability of Works: Only under the shapes of the owner built, only for personal use.

Subjects of Claims: Works published by the owner on Google Play and Google Books.

Concerning Author Rights: Equations and codes from scratch of the owner, softwares built from it, all things of people arising from it.

End User License Agreement: A commercial license is required to use in personal manner. Do not redistributing in any manner, including by computer media, a file server, an email attachment, etc. Do not embedding in or linking it to another programs, source codes and assistances including internal applications, scripts, batch files, etc. Do not use for any kind of technical support including on customer or retailer computer, hardware or software development, research, discovery, teachery, talk, speech, write, etc. Do not use for win money or for commercialisation of any products arising from my programs, source codes and assistances. Do not use and do not copy the way it run in other programs, source codes and assistances. Do not use without pay me, quote me and my agreement. Do not steal or copy or reproduce or modify or peer or share. Do not use in other manner than personal. It stand for my programs, source codes and assistances or programs, source codes and assistances stealing or copying or reproducing or modifying or peering or sharing my programs, source codes, and assistances. If you aren't agree you shall not use.

Terms of License and Price: The present contract acceptance is required to use works of the owner and built from it in all kind of manner. The price for each user shall be defined with the owner by contacting him and this for each subject of works the owner claims. Each user shall contact the owner for asking his agreement. It can be refused by the owner depending who asking and the price defined. People don’t respecting the present contract shall not use the works of the owner.