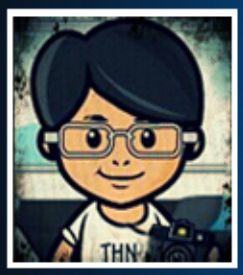
The Hacker News

August 2012 , Issue 13

Botnets



From Founder's Desk...

Hello faithful readers and new comers to our magazine! We are very sorry to have missed publishing the July issue, however, we were busy at work putting on the **THE HACKERS CONFERENCE** in Delhi, India. We had a fantastic turn out and professional, informative speakers.

We plan to have another conference on Internet Security in September next year and hope to see you there!

For now, enjoy all the good information on Botnets in our August edition and thank you again for your continued support.

Mohit Kumar
Founder, The Hacker News

Are You Part of the Zombie Army ?

Author : Mohit Kumar (THN)

If you have been hearing about the massive cyber attacks and assaults of supposed "bots and zombies" you might be wondering how our vast computer system has been invaded by aliens or worse; how "The Walking Dead" have taken command of the internet. Well, rest assured in reality, "bots' and zombies" are a computer or network security threat, or a collection of ordinary home and office computers that have been compromised by rogue software. At the present time, botnets are considered to pose the biggest threat to the Internet; not spam, not viruses, not worms.

A 'bot' is a category of malware which will allow an attacker to secure complete control over the affected computer. Simply, botnets are a grouping of Internet computers that have been assembled to broadcast transmissions including spam and viruses to other computers on the Internet and unfortunately their owners are unaware of it. The idiom "bot" is short for "robot" and the designated computers are referred to as "robots" or "bots" and in turn these designated computers are referred to as a zombie because for all intent and purposes a computer "robot" unknowingly carries out the requests of a master spam or virus initiator. It is through an Internet port that, unfortunately, has been left open that these "zombie" or "bots" are regularly fashioned and through which a smallTrojan horse program can be deposited for future potential release. At a designated time the individual that has assembled the "Zombie Army" can release the "Zombie Army" by merely dispatching a single directive most likely coming from an Internet Relay Channel site. When this action takes place, your computer will be capable of performing programmed duties over the Internet, exclusive of your knowledge . The majority of computers that have been elected to serve in these so called "Zombie Armies" are computers that have owners that have dramatically fallen down in providing effective firewalls and other protection for their computer.

Cyber criminals characteristically utilize “bots” or “Zombie Armies” to contaminate significant numbers of computers at one time. In unison, these computers will form a network, or a botnet. Cyber criminals will employ botnets to dispatch and spread viruses, attack computers and servers and to send out spam email messages, and to commit additional types of crime and fraud. If a computer is co-opted and becomes part of a botnet the computer may possibly slow down and the computers owner may unintentionally be assisting a cyber criminal. Bots can also be utilized to serve as a vehicle for mass identity theft. This can happen through phishing emails that look as if they are dispatched by a legitimate company in order to induce the user to submit personal information and passwords. Computers users should be especially suspicious of emails claiming to be from Paypal, eBay, banks and the government. Never ever click on any email links to access these sites; be sure to always use your bookmark or simply key it in directly.

The perpetrators of damaging malware such as “bots” are continuously updating, improving and revising their attacks to elude detection and circumvent measures like anti-virus and anti-spyware utilities. A computer owner can mount a good defense against threats like “bots “if the computers owner will run anti-virus and anti-spyware software on their computer. And it is also extremely wise to make certain that you keep your operating system and applications patched against known vulnerabilities. It is very important that you update the software frequently and use a personal firewall program of some sort; to safeguard your computer from any unauthorized access. Fortunately, for unsuspecting internet users, in the past two years, law enforcement and computer securitycompanies are having more than a modicum of success in pursuing, tracking, defusing and neutralizing some of the most infamous botnets. Back in March of 2010, the FBI helped by the Spanish government brought down theMariposa botnet, comprising more than 12 million computers and arrested the individuals behind it. And in 2011, Microsoft and Kaspersky united to deactivate the Rustock and Kelihos botnets, but unfortunately were unable to ascertain who the perpetrators were. And most recently the US and Estonia police made arrests of the cyber criminals running the Esthost botnet.

Recently, in the United States the White House has been underscoring the importance of tighter internet privacylaws. The White House has aggressively pushed to further their “Online Safety Agenda” with a new anti-botnet initiative for combating botnets. They recently revealed a pilot program for fighting viruses, referring to the massive infection worldwide of five million PCs this year alone. This newly announced White House program will use principles defined by the Industry Botnet Group. The main goal of this newly announced program will be to being to educate internet users on the hazards and many dangers of cyberspace while preventing botnets from spreading by sharing data about infected computers.

The White House is also working diligently with the Information Sharing and Analysis Center to develop and implement their "botnet pilot," presumably to enact those anti-virus principles.Numerous companies, along with the cooperation of the Department Homeland Security and the Federal Trade Commission, make public an educational campaign labeled 'Keep a Clean Machine' which is targeted to teach consumers how to prevent their computers from being hacked.

So it is evident that unscrupulous cyber criminals may be using your computer as you read this article. You now know that botnets do not come from an outer space invasion, they are cyber criminals that do invade your computer surreptitiously and hide software to get access to the information on your computer, including your email program. It is a fact that once these cyber criminals infect your computer, they can spy on your Internet surfing, easily pilfers your personal information and then uses your computer to send spam to other computers without your knowledge. And if your computer is taken over this way it is a good bet that your computer will become part of a robot network and you will without volunteering becomes part of at the “Zombie Army”. It is more than evident that botnets continue to increase the price of doing business online and place companies at a competitive disadvantage, while direly affecting and continuously threatening individual privacy,

The Dynamic Evolution of the Botnet

A botnet can be defined as a collection of compromised, individual computers operating on a common network protocol. The way that a botnet traditionally controls each infected machine is to send instructions from a central command and control Server. The largest of these botnets function over long periods of time by utilizing an aggregate of multiple command and control servers that are physically located in more than one country. This has been an effective method of staying alive and operational, as it relies on the lack of cooperation that exists between governing authorities in the international community.

The newest botnets are designed in such a way to make discovering and eliminating the source of control even more difficult. Instead of using the traditional command and control, server-centric model, they utilize the peer to peer protocol that has been popularized on the internets in file sharing applications. Using peer to peer, or p2p, it is no longer necessary to send commands from a physical server location. The internet protocol address, or IP, is dynamic (meaning constantly changing). The benefit of this is that it is much more difficult to trace back to the source. There is a trade-off of some security and functionality with this protocol as well. Using the p2p method requires more time for the commands to reach each individual node on the botnet. It also opens a new security risk. Since the instruction set is not coming directly from a command and control server, there is a greater possibility that another hacker or agency might hijack the compromised machines on the network. This risk is mitigated by employing encryption keys, but it is still more of a risk than a direct line of control.

Creating a botnet requires planning, coordination and technical skill. A good, functional botnet can be characterized as a professionally designed and built tool, intended to be rented or sold for use by anyone with a novice skill set, on up. A botnet can be leveraged in many different ways. Anyone can rent botnet resources, and harness the power of many individual machines on the network; for the purposes of DDOS (distributed denial of service attacks), mass spamming, page rank and advertising revenue manipulation, mining bitcoins, or for any combination of these and countless other possible exploits. For a relatively small amount of money, a single individual can level the playing field in competition with larger organizations. This is the appeal of the botnet, in the minds of many hackers globally. In the minds of most everyday network users, a botnet is nothing more than a high tech extension of common, organized crime. In the mind of anyone who is paying attention, they raise some serious security concerns.

The top three active botnets (responsible for the vast majority of internet spam) are Lethic, Cutwail and Grum, all three operating on the traditional command and control server model. As of today, even as I write this article, Grum is under attack. Two of Grums Servers (both in The Netherlands) have been shut down, leaving its zombies (compromised computers on the network) without a connection for new spamming instructions. The path of information can be characterized simply; the command and control server feeds the job instruction server(s), the job instruction server(s) feed into the proxy server(s), then the proxy serves the zombies. Without the job instruction servers, Grums current instruction sets will time out. Without new instructions from the bot herders (operators of the botnet), the zombies will become dormant. Botnets are profitable, so the bot herders will probably not allow Grums to terminate operations. They control other servers (one in Russia and one in Panama that have been identified) that can be re-tasked to serve instructions to the zombies under their control. What events like the Groms server take down indicate is that the command and control structure is becoming more vulnerable. From that, we can conclude that we will likely see a fast and dramatic rise in newer p2p botnets market share of internet spam delivery services.

Alureon is an example of the new generation of botnets, and is a good barometer of the overall climate of malware in the wild. Alureon is a p2p botnet that is designed from the ground up to not only be more difficult to track, but also to more effectively utilize its zombie network. The malware infecting the zombie on this botnet removes other rootkits as part of its normal installation routine, which, if anything, will improve system performance on the user side. This is a strong indicator that it is already operating from a position of technical superiority over a lot of commercial malware removal and antiviral packages available. It installs to the master boot record, so it is in memory before the operating system loads.

The code execution has already taken place by the time anti-malware applications load, and the network traffic is encrypted. While a power user may take the time to analyze system processes and network traffic to find and eliminate oddities, the typical user may not have the information or knowledge to do so. The zombie is then instructed from within the node based, dynamic p2p network. Every zombie is now a node on the system, capable of two way communications with all other nodes.

After looking at recent events in the botnet world, even with the limited success security researchers have had in disrupting traditional command and control structured networks, it appears unlikely that they will have any similar success with the newer p2p systems, in the immediate future. As long as the hacker community continues to find ways to work together and optimize their use of network technology, they will have an advantage over the dissociative, squabbling international community of researchers and law enforcement agencies. In a more perfect world, everyone would work together to find a way to harmoniously share information with one another. In the world we live in, botnets and other malware seem to be continuing to evolve, and are settling in for a long stay.

For The Lulz Of It,I Apologize To Lulzsec

Author : Ann Smith, Executive Editor Thn

Shame on me. When someone mentioned Lulzsec I would slightly bristle and turn a mighty heel towards the "real" movement. You know, the Anons that are taking down corruption and terror, targeting the real enemies of the world. If you were doing it for the LULZ of it, well, you were playing in the proverbial sand box and I thought you were hindering, instead of helping. I even wrote an editorial spanking them for releasing the emails of servicemen who had signed up for a porn site.

Then, I read the book, **WE ARE ANONYMOUS** by ***Parmy Olson***. Every person who considers themselves Anonymous or who sympathizes and rallies for the cause, must read this book. You will not only get a good education from this history of the movement but also get to know the people behind the masks and what drives them to hack.

You may see yourself in the stories of their lives or have a gut wrenching feeling of sadness when they are arrested. I know I did. I was right there, hanging on the hope that the authorities would be thrown off the track, get lost in cyber space, or go fuck themselves.

But alas, as in the ying and yang of life, it wouldn't be so. Still, you will be turning the pages in earnest as you read the story of why people came together and what behaviors they exhibited. You will discover people ended up tolerating all sorts of sordid and undefinable actions but then, as you will discover, it really was all for the Lulz of it.

But that wasn't what impressed me and made me stop to understand my own feelings about Lulzsec. It was in the pages of this story that human rights, passion, justice, injustice, personal struggles from childhood scars, ambitions, and the need to be right that I came to respect the Lulzsec movement, its pleasures, its goals and painfully the demise of the key players. Although Sabu may be the most hated man on the Anonymous planet, Olson takes an objective and supportive role in portraying the beast of the cyber world and even I was seeing the situation in a new light. After reading this book you will find other subjects to hate that brought down the group in what I describe as third grade politics and ego egg salad. Uggggh. Some of the people I just deplored, and unfortunately, in a group setting there will always be "those" kinds.

What I am really trying to say is that even though you can sew a thread of doing hacking for the Lulz of it, behind their actions was a real commitment to human rights. The drive and passion these people had for bringing justice to the people. I will always admire that in any form it takes place. I can excuse the nonsense and the immaturity because in the end, it really wasn't just for the Lulz of it. It really came down to being for you and me.

I hope Lulzsec forgives me. I hope the group continues with new and energized men and women who unite globally for the common good and have a few laughs while they are at.

After all, in the end, we are Anonymous, we are Legion, We do not forgive, We do not forget, Expect us.

Author : Ann Smith
Facebook Profile : http://www.facebook.com/ann.smith.92102
Email : Ann@thehackernews.com

Botnet around Us
Are we nodes of the Matrix?

Author : Pierluigi Paganini

Introduction: The nightmare of millions of infected computers synchronized to conduct an attack on a specific target finds materialization in the concept of botnet.

In the classic architecture each machine, named bot, executes orders sent by a master unit called botmaster, which can instruct the various components of the malicious network to perform an attack rather than exchange communication messages. The model of botnet could be used for various scopes, in military as cyber weapon, in industry for cyber espionage, in cybercrime to steal sensible information such as banking credentials.

As we will analyze in the article, other factors are helping the development of this kind of cyber threat, the evolution of the mobile scenario and also the diffusion of agents specialized for social network platforms. The phenomenon of the botnet is worrying due its rapid growth and due to the evolution of the model and the continuous improvement we are assisting.

But let's start from the beginning, the infection phase that represents the recruiting of the machines due the diffusion of different types of malware developed with specific and profoundly different characteristics. The most common way to build a botnet is to send the victims infected mails, containing a link to a compromised web site or that have attacked the malware agent that once executed on the machine it transforms it in a bot.

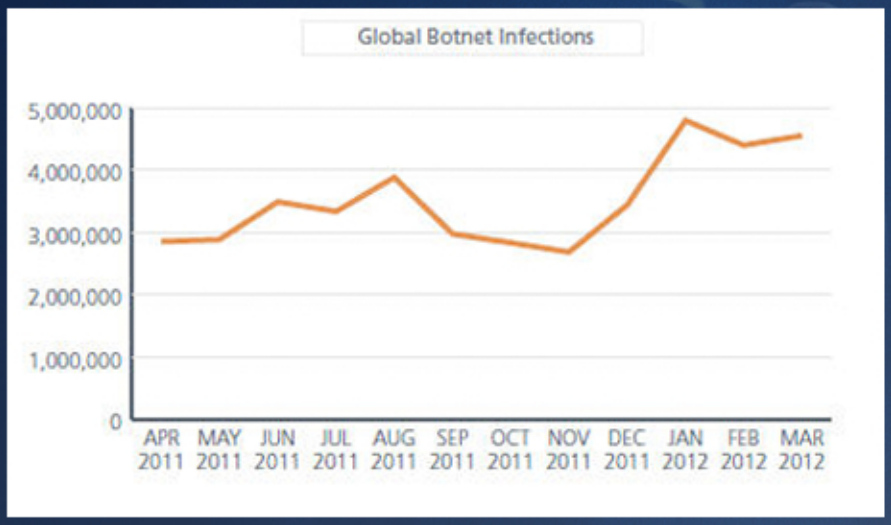
Usually the infected machines try to contact the C&C (Command & Control) server to receive operative instructions. Botnets are created for various purposes such as denial-of-service attacks, creation of SMTP mail relays for targeted spam campaigns, implementation of various fraud schemas (e.g. banking information gathering).

Botnets represent one of the most dangerous cyber threats due their adaptive capabilities and the massive diffusion, recent events have demonstrated that every platform could be attacked. One of the most aggressive of all the malware is Flashback Trojan, a malware created to conduct click fraud scam by hijacking people's search engine results inside their web browsers, stealing banking or login credential.

Of course once infected the system could be used as part of a botnet, causing bigger damages. The botnet related to the Flashback Trojan is called Flashfake, also designed by cyber criminals to conduct a click fraud scam, taking advantage of pay-per-click campaigns by advertising companies. Flashback was created in September 2011 to disguise itself as an Adobe Flash Player installer, using Flash player layout. Once installed the malware searches for user names and passwords stored on the victims machine.

Which is the status of botnet diffusion?

According to the data proposed by McAfee Labs in its McAfee Threats Report – First Quarter 2012, the cyber threat botnet is growing, creating great concern between security experts due their diffusion, millions of compromised computers connected to the Internet are, in fact, used daily to realize scams and cyber attacks. Observing the volume of messages exchanged between bots and command server is possible, to have an indicator on the level of the threat and its diffusion. Overall messaging botnet growth jumped up sharply from last quarter, mainly in Colombia, Japan, Poland, Spain, and the United States.



Many of the leading messaging botnets (Bobax, Cutwail, Grum, Lethic and Maazben) showed a minor growth or a decline with the exception of Cutwail botnet, which increased significantly.

Behind the principal botnets there is the cybercrime industry that is pushing on the diffusion of malware to infect an increasing number of machines, but also proposing new models of business, such as botnet rental or the commerce of the agents for botnet creation. The business is reaching important figures, in a short time, mainly due to the opportunities provided by the Deep Web.

Considerable is the discovery made by a group of experts of the AlienVault, led by Alberto Ortega, on a new service that offers cyber-attack tools and hosting as part of malware-as-a-service.

Once again cybercrime operates as enterprise, the products proposed are tools for the organization of cyber-attacks such as spam of malware, malware hosting, and a to build up a complete command and control infrastructure (C&C) for the arrangement of botnets.

The service is called Capfire4 and it's a good example of C2C (Cybercrime to Cybercrime), it provides technological support to criminals who haven't necessary knowledge to conduct a cyber attack or to arrange a cyber scam.

In the simplest way, users can access a Web portal that offers the possibility to create customized versions of malware, to access a management console to control bot, of the infected networks.

Few steps for criminal that need to create a botnet without having particular knowledge.

The most popular malware on the portal are RAT (Remote administration tool), software created to let the attacker spy on the victims with actions like key-logging, password stealing, command execution and remote access and controlling and screen capturing.

These tools are continually updated and improved to meet customer requirements, an excellent work made by specialists. The platform also offer hosting services for the malware. Once logged in the client can choose a destination for the agent from a list of fake domains that appear like legitimate ones.

Criminal models such as the one introduced make affordable the production of malware, also contribute to the diversification of the agents making complex their detection due to subsequent processing and improving. These groups are led by professionals that are familiar with the mechanisms of antivirus detection of the manufacturers of security products. The spread of malware in this way could be used by terrorists or other groups wishing to conduct cyber-attacks providing new and powerful weapons at low cost and without any special risks associated with their acquirement and detention.

Botnets and cyber warfare

The creation of botnets is also considered in cyber warfare scenario as a military option for offensive purposes or cyber espionage.

Through the establishment of a botnet is possible to attack the nerve centers of a country, isolated attacks can target its critical infrastructures, create serious problems in areas like finance, communications and transport. That is cyber warfare, no matter if behind the attack there is a foreign government or ruthless criminals, the risk is high and face the threat has high priority.

The US government is taking in serious consideration the cyber threat related to the botnet, recently administrative officials belonging to U.S. President Barack Obama's team declared that the government had started IBG (Industry Botnet Group) a coordinated project that involves private enterprises and trade units.

One of the key features of the program is the increasing level of awareness in the botnet world, through the cooperation of government and private sector.

White House Cybersecurity Coordinator Howard Schmidt has deep knowledge of the problem. For this reason, he's convening federal agencies, law enforcers and private companies to define a common strategy to deal with the threat.

The components of the botnets could be located everywhere in the world involving several countries, different social contexts and different laws and regulations, for this reason is quite difficult to arrange a unique front to face with the threat.

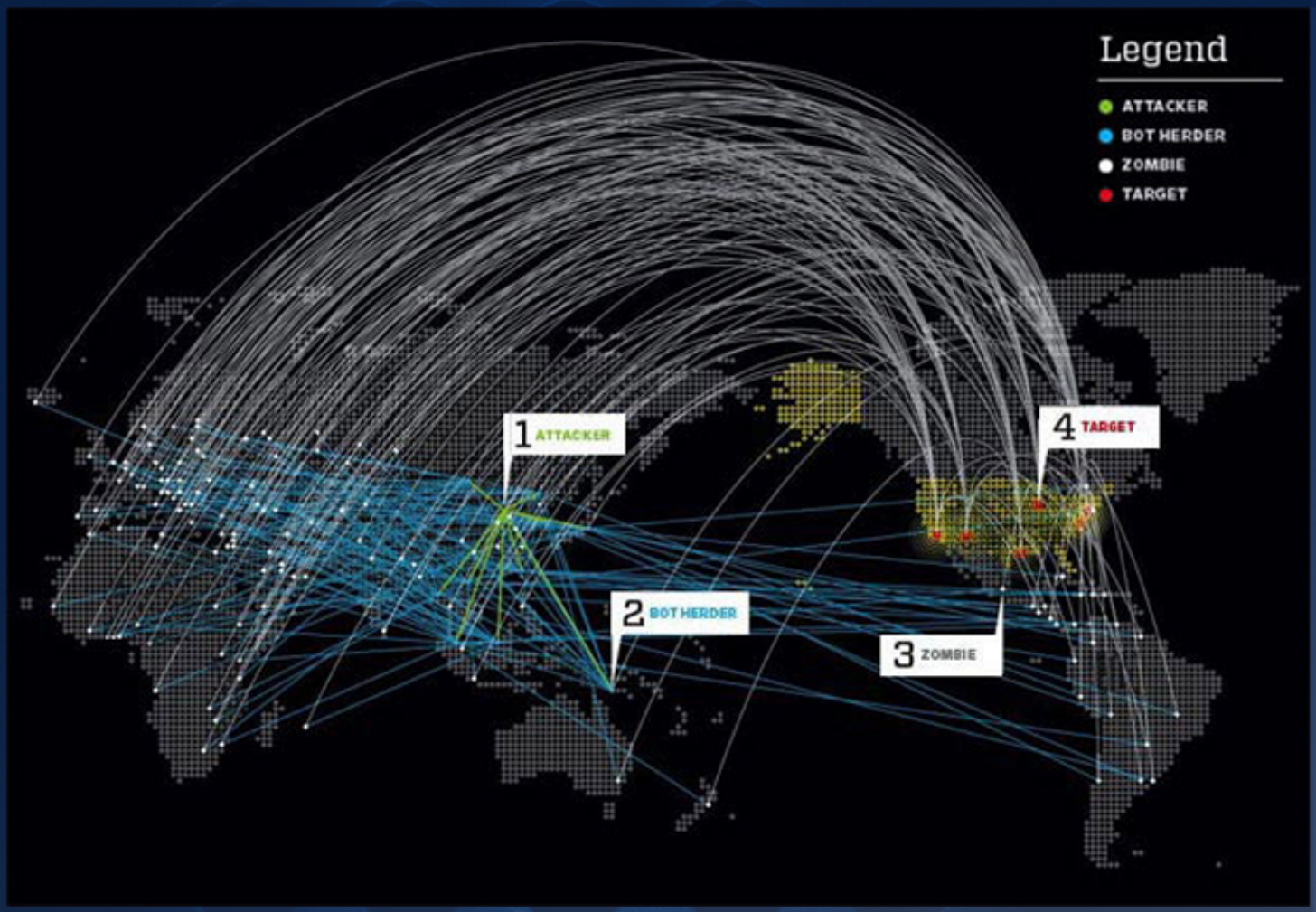
During the McAfee Public Sector summit in Arlington, Va, on April 11th, Schmidt declared:

"*There's been a lot of discussion about botnets…trying to identify how many are out there, what they're doing, what they could do and what the impact could be. I've asked my office to engage in a private-public partnership to enhance the nation's cyber security by fighting against bot networks,*" "*We're teaming U.S. internet service providers, search engines, internet vendors, privacy rights advocates and groups and trade associations to tackle this on all fronts. We're working on developing best practices and an industry code of conduct within the next 90 days.*"

The work group, led by Schmidt, is spending a sensible effort in the battle, working to reach the following four main goals:

1. To develop principles for addressing the botnets.
2. To establish high-level strategies to increase public awareness on the botnets.
3. Leverage available consumer-focused information tools and resources to prevent the botnets from the beginning.
4. Identify ways of measuring progress.

The fundamental aspect is a deep analysis of the current situation and the definition of methods to measure the extent of spread of the threat, elaborating a set of indicators, globally recognized, that can provide a status on the evolution of the phenomenon. Another key to fighting the proliferation of botnets is able to increase the level of awareness of the threat in each sector while also providing the tools necessary to tackle the problem.



According to Schmidt, it is necessary to act immediately due to the diffused offensive of botnet chat represents a serious threat for both military and private sectors, threatening the security of the nations. What most worries the U.S. government is the high rate of spread of malware in the private sector, not easy to contrast the phenomenon. That it has-been estimated one in ten Americans has some kind of malicious software on their devices.

"We're looking at what [botnets] might do to a business's infrastructure, to personally identifiable information – identity theft, credit card fraud, et cetera – but it goes beyond that. What we're beginning to see is about 4 million new botnet infections every month…it's a moving target,"

"One of the clear issues we won't be doing anymore is to just sit back and admire the problem. We've done that for too long. We've written strategy after strategy…it's time to move beyond the strategies and actually move into an environment where we're executing on these strategies,"

Botnet, a model in continuous evolution

Meantime, worldwide security expert are searching for a common strategy to decapitate the botnets, the cybercrime industry is providing new, efficient solutions to avoid any type of detection and mitigation.

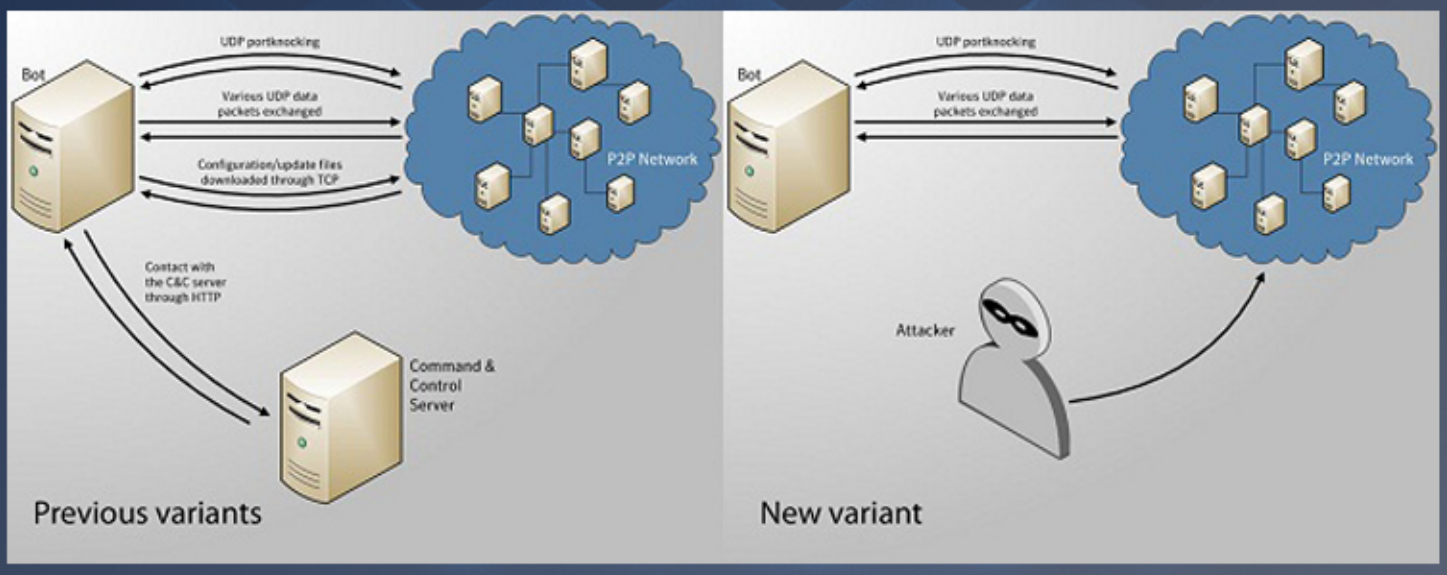
The real innovation in the last months is represented by the creation of botnet based on the P2P (peer to peer) communication protocol that does not rely on command and control (C&C) servers for receiving commands. The new variant is based on a new instance of the Zeus, a malware used mainly to steal information, such as bank credentials, from an infected pc. At the end of 2011, has been identified a new Zeus variant that uses P2P communication to transfer commands from compromised hosts in a botnet. Symantec experts have discovered as spread a mechanism of the distribu tion of fake antivirus programs.

The interesting feature is that P2P communication is used as a backup system in case the C&C servers are not reachable, creating an autonomous peer network in which each node can operate as a slave or as master giving orders to the other PC, operating and exchanging information acquired illegally from the victims.

The Symantec experts Andrea Lelli declared:
"Every peer in the botnet can act as a C&C server, while none of them really are one,"

"Bots are now capable of downloading commands, configuration files, and executable from other bots — every compromised computer is capable of providing data to the other bots,"

In similar botnet, each bot works as a Web server thanks to the presence of nGinx that equips the malware. The communications between the nodes in the network are based on HTTP protocol. The new type of botnet is really worrisome, because it hard to fight due the absence of point of failure represented in a classic botnet architecture by the C&C servers, distributed peer networks are so very difficult to identify. Tracking systems such as ZeusTracker are not able to track this variant due the impossibility to add the complete list of components of a P2P network, instead only the IP ad dresses of C&C servers.



To avoid tracking and dump of traffic, the communications mainly use UDP protocol, because TCP is easily detectable. The bot does not perform any authentication on the packets exchanged, so anyone can impersonate a bot and successfully communicate with other bots, downloading stuff like configuration data, this feature could be used to exploit the network.

The handshake phase between bots is possible using a homemade UDP and after successful connection the nodes start to exchange TCP data (e.g. configuration files, list of other peers, etc).

What is still a mystery is how the information is received by the botmaster, that's why analysis is still ongoing. It has been hypothesized that specific conditions can trigger the communication with a specific server to transfer, for example, stolen information. Preliminary research suggests that stolen information is still transmitted back to botmasters using classic methods, rather than relayed through the P2P network.

The Zeus case is not isolated, recently Kaspersky Lab, in collaboration with CrowdStrike Intelligence Team, Dell SecureWorks and members of the Honeynet Project, dismantled the second Hlux botnet (aka Kelihos).

This botnet had scary size, it has been estimated it was three times larger than the first botnet Hlux / Kelihos dismantled in September 2011. After only 5 days from the transaction, Kaspersky Lab had already neutralized more than 109,000 infected hosts. It is estimated that the first botnet Hlux / Kelihos had only 40,000 infected systems.

The event has demonstrated that it is becoming hard to tackle the new generation of botnets, due to the usage of the peer-to-peer technology, also implemented in Kelihos. The new variant of malware incorporates P2P technology to eliminate the need for a C&C server, avoiding detection and the immunization campaigns to decapitate the malicious networks.

To provide another example of botnets we can think of the Alureon / TLD4 botnet that can survive indefinitely in absence of its C&C servers, making difficult their detection. The new trend in the development of botnet is to provide them the capability to be "independent" from control servers, surviving and becoming anonymous for long periods, infecting many machines.

The battle is difficult, changes observed in the botnet scenario are the result of a developmental model of malware that has nothing to envy to the development of products of the legal industry.

The mobile scenario, business opportunity and related cyber threats

One of the IT sector that is interested by the major growth is without doubt the mobile, an increasing number of platforms and related applications have been developed in the last month, consolidating the trend. Of course with growth has been observed a sensible increasing of cyber attacks on the mobile sector, today still vulnerable from the security perspective. To an impressive growth in the demand does not corresponded with awareness of the threat, the user ignores most of the time the potential of its smartphone and threats which it is exposed.

To remain on topic, a mobile botnet is a botnet that targets mobile devices such as smartphones, attempting to gain complete control of the mobile. Mobile botnets take advantage of unpatched exploits to provide hackers with root permissions over the compromised mobile device, enabling hackers to send e-mail or text messages, make phone calls, spy on users, access contacts and photos, and more. The main problem is that botnets go undetected and this makes it really difficult to tackle. The malware spreads itself by sending the agents to other devices via e-mail messages or text messages.

Examples of mobile botnets are DreamDroid and TigerBot (SMS Controlled Android Malware) malware that compromises Google Android devices, Zitmo (zeus varian) that targeted The Blackberry platform and CommWarrior which affected Symbian devices. The last in order of time is TigerBot, a new form of Android malware controlled via SMS messages that can record phone calls, upload the device's GPS location, and reboot the phone, among other operations executable in the command, preventing the message from being seen by the user. TigerBot tries to hide itself from the user by not showing any icon on the home screen and by using legitimate sounding app names (like System) or by copying names from trusted vendors like Google or Adobe. "TigerBot", differs from "traditional" malware in that it is controlled via SMS rather than from a command & control (C&C) server on the Internet. The polymorphism of the threats and the genesis of new variants are the issues of most concern, these hacks and malware would essentially turn the phones into "zombies" in order to respond to external orders.

The rapid spread of botnets based on mobile devices is favored by the almost total absence of protection mechanisms, so they are difficult to tackle and it is difficult to trace the agents composing the network. This cyber threats must alert private industry, but especially institutional environments, the risk of data exposure is really high and due the the young growth of the sector, we are still too vulnerable. Cyber criminals and government agencies are aware of the importance of information gained from our mobiles and, therefore, are showing high interest in the field.

In particular it has been observed that an exponential growth of malware designed to attack mobile systems and steal sensitive information, useful for the accomplishments of frauds, very much impressed the banking sector.

The scenario of a mobile attack is always the same, the App stores, that is the sites for software download, and the mobile apps serve as programs users download onto our mobile devices. Users who download from app stores may download compromised apps infected by malware. The number of application available on the store is increasing day by day, especially for the open platforms like android. Let's consider also that there are also third-party stores that provide alternative apps for users, but downloading from these unofficial channels it's very dangerous for final users. The main problem related to alternative app stores are that they are not sufficiently controlled or that they can be managed by cyber criminals to provide a fake copy of legitimate applications, modified to realize the fraud. Due to the different malware targeting the Android OS, several companies have tried to categorize them depending on the fraud and attack schema implemented. The following is the categorization proposed by Trend Micro.

Types	Technique	User Implication
Data Stealer	Steals information stored in the mobile device and sends it to a remote user	Stolen information maybe used for malicious purposes
Premium Service Abuser	Subscribes the infected phone to premium services without user consent	Unnecessary charges for services not authorized by user
Click Fraudster	Mobile devices are abused via clicking online ads without users' knowledge (pay-per-click)	Cybercriminals gain profit from these clicks
Malicious Downloader	Downloads other malicious files and apps	Mobile device is vulnerable to more infection
Spying Tools	Tracks user's location via monitoring GPS data and sends this to third party	Cybercriimnals track down location of users
Rooter	Gains complete control of the phone, including their functions	Users' mobile devices are exposed to more threats

As previously mentioned, The Android Market has few restrictions when it comes to registering as a developer. The strategy is implemented to encourage app developers to adopt the platform, of course this also makes it is easier for cybercriminals to upload their malicious apps or their Trojanized counterparts. The following are some noteworthy incidents, listed by Trend Micro, that leveraged this loophole:

We analyzed several Trojanized applications found in The Android Market, detected as ANDROIDOS_LOTOOR.A. One of these apps is the game Falling Down, which renders similar to the clean version. Once installed, the Trojanized version asks for more access permissions. It also gathers device information like IMEI and IMSI numbers and roots affected devices.

One of the malware variants found in the Android Market is the notorious DroidDreamLight variant. Trend Micro researchers found an app that promotes itself as an .APK file management tool. However, instead of helping users, this app (detected as ANDROIDOS_DORDRAE.M) collects device-related information and uploads it to remote servers. It was immediately taken off the Android Market.

Google released the Android Market Security Tool in The Android Market. Cybercriminals, on the other hand, were not deterred by this tool and even released a Trojanized version. Detected as ANDROIDOS_BGSERV.A, it acts as a backdoor that gathers information from the device and sends these to a remote URL.

Cybercriminals have also created and distributed malware using the names of popular apps that are not yet available on the Android Market. Android users anticipating these games are the likely victims of this ruse. A recent example is a fake version of Temple Run we found in the Android Market. The reports alert mobile users regarding the extension of common threat to mobile environments like advanced persistent threats (APTs). For the implicit nature of the attacks they are considered “campaigns” rather than singular “incidents,”.

The introduction of mobile devices has considerably incremented the attack surface making this attacks most frequent. Mobiles are simple to infect through any infected media.

Present projects for future threats

The US government is financing several activities to investigate and hack into the technology spread in every device that ordinary surround us. This is the next step of the warfare, spy and attacks foreign enemy simply accessing to the devices that are presents in their offices, in their houses and in their cars.

Every device connected to internet could be target of a possible attack, the intelligence which is fitted can be used for numerous purposes, exploiting the lack of awareness in the cyber threat.

The U.S. government recently promoted a project to hack into video game consoles requesting for the "Development of Tools for Extracting Information from Video Game Systems."

The idea is as simple as it is efficient. Today, consoles are totally equivalent to a computer, they are connected to The Internet in the same way and they provide many services to the final customer. Last generation of gaming consoles have pushed on the communication aspect. Using the devices, users are able to communicate to every other player connected to the gaming platform. Well, those communications and any other sensible information stored in the console are an object of interest to US intelligence agencies.

The U.S. Navy has reported that the scope of the project is to hack into used consoles to access any sensitive information exchanged through their messaging services. It has also guaranteed that the spying technology will be used only on nations overseas, due the internal law restrictions that don't allow these practices on US citizens.

But let's think for a moment about the power of these networks and to the possibility to create a large botnet to attack every type of target. We are faced with an incredible war machine that could destroy an enemy computer system, coordinating a cyber-attack of unimaginable dimensions, or to arrange a large scale infiltration for cyber espionage purposes. Well, this is cyber war and an implementation of a botnet using a gaming platform is an option examined by the most advanced and technological countries.

Regarding the specific project the official U.S. Navy statement is:
"This project involves furnishing video game systems, both new and used, and creating prototype rigs for capturing data from the video game systems."

The description from the actual contract from the Federal Business Opportunities website, posted on March 26 is:

"R & D effort for the development and delivery of computer forensic tools for analyzing network traffic and stored data created during the use of video game systems."
The project has been assigned to the California-based company Obscure Technologies, signing a contract of $177,237.50 for the job.

Will we see the future botnet composed by gaming console?
Of course, yes … but don't' ask me about consequences!

Conclusions

The fight against the proliferation of botnets, in my judgment, goes through some key factors such as:

- The promotion of joint operations that involve government agencies and the major private industry players. In this sense, some large companies have already embarked on a close collaboration with governments, as in the case of Microsoft.
- Fundamental, is a timely and methodical study on evolution of technological so lutions on which botnets are based. It's important to define, a universally recog nized set of indicators to deterministically qualify the threat and its evolution.
- Awareness on the cyber threats and divulgation of best practices for the contain ment of the infection.
- Approval of regulations and penalties, recognized globally, for those who de velop or contribute to the spread of botnets. Unfortunately today, different legis lative frameworks represent an advantage for those who intend to commit a crime using these tools.

Despite the good intentions we are still far from global agreement of the definition of the proper action against botnet diffusion, both on legislative and operative perspec-tives.

We need to hurry!

Botnet

Recruitment of unintended robots (attackers / blags)

Author : Himanshu Chaudhary

Daily, you receive lots of emails. Out of them some are always advertising emails, such as, about jobs, you won a lottery or prizes, or some threatening message about unwanted transaction history from your bank account. In these emails you always get a link claiming to be for your prize, or some document or pdf file for getting more information. As soon as you click on that link or document, BANG. Now you are a recruited employee (Bot) under an attacker (Bot Master), you will lose all control of your machine, and it will start working any assigned task automatically.

Arghhh..Bit Scary right, but it's a truth. Now let's take a deeper dive into this, for understanding how exactly this whole black universe of botnet works.

What is Botnet : Botnet is a network of all compromised machines(Victim machine) which follows tasks assigned by a Bot Master (Attacker Machine). So you can take this situation as a quite similar situation of medieval times, where there used to be a king which used to control a huge army (innocent people), and that army used to follow an assigned task by that king. So that army used to attack on other side army, used to give their money to king for king's treasure or whatever assigned task by a king. Similarly it works in a botnet situation. There is an attacker (Bot master) controlling lot's of compromised machines (Victim's machine), and then those machines follows a command of bot master, either bot master can ask those machines to attack other machines, send an email to other users or can simply ask it to provide its users confidential information.

How Botnet works : There is an attacker (Bot Master) who send lots of emails to victims containing malicious code in itself, and as soon as users respond to that email that malicious code will get installed automatically in a user machine and then their machine gets compromised and then user machine will become a slave of an attacker. That malicious code can be capable of updating or deleting itself as per the instruction of an attacker, and the user will not be able to sense it ever, because it will do everything in a backend. That malicious code can perform several tasks on an basis of the nature of that code or on the basis of instruction of a bot master

The whole life cycle of Botnet can be divided into four steps :

- Creation
- Configuration
- Infection
- Control

In creation stage, attacker creates a malicious code, either he can write its own code or can do some manipulation in already available scratch code. Effectiveness of a botnet always depends on attacker skills and requirement. Either he can code a very malicious and untraceable botnet or simply can make some changes in old code, which generally script kiddies do.

In configuration stage, attacker implements his botnet code at some victim machine and serves it as a server. In this stage, he configures a server and channel information by defining the target and attack method, and makes it stealth and protected against detection or intrusion, into the botnet network by using a unique encryption scheme. After that, it restricts access to the bots by providing a list of authorized users, by which only allowed users will be able to control botnet.

In infection stage, attacker gives a command to C&C Server (Command & Control Server) to start infecting other hosts and for increasing a range of botnet network. There are various ways for infecting other users, such as either attacker can target vulnerabilities in browser or operating system, and then launch an attack on the basis of vulnerability, or it can send emails to users containing malicious code, and as soon as user will respond to that email code will get installed automatically on a victims machine. That malicious code can delete or update itself with the help of communication between bots and C&C Server. There will be a communication channel in between bots and C&C Server, which user will not able to identify.

In control stage, attacker controls all bots with the help of C&C Server and commands them to do assigned tasks. Either it can command it to attack other machines or can command it to provide all confidential information of user such as passwords, card details etc.

Types of attacks :

- **Email Spam :** Bot master will use victim's machine for sending spam emails to others, which is basically for advertisement purposes, or maybe it can contain some malicious code as well.
- **Denial-of-service attack :** Bot master will use victims resources for performing a DOS attack either on some other peoples machines or maybe on the same machine.
- **Adware :** In this, bot master will use victim's machine for advertisement purpose without victims permission and awareness, such as , by replacing ads on web pages with content of owner of website.
- **Spyware :** Spyware is malicious code, which will send all confidential informa tion of victim to the hacker. It will send all passwords, credit card details, stored files, documents etc.

How to detect botnet :

- If machine is working slowly then it may be an indication of botnet, as botnet uses victims machine resources.
- By passive OS fingerprinting you can detect a botnet attack.
- Network intrusion detection system can be best approach.

Preventive measures :

- Best preventive measure is use rate based intrusion prevention system.
- Configure your firewall, best way to do is just close all the ports and then open only required ones.
- Use updated antivirus.
- Avoid clicking on spam emails.

Some past research for stopping a botnet.

BotHunter: BotHunter is a type of bot application that looks for other bots by tracking two-way communication flows between active software inside a private network and external entities. BotHunters main purpose is to identify known or suspected malicious external entities and to mitigate the threats that bot infections can pose. BotHunter focuses on the communications dialog that occurs between internal network nodes and external entities in the form of a series of data exchanges. Two custom BotHunter plugins are, SCADE (a snort preprocessor plugin with two modules, one for inbound scan detection and another for detecting outbound attack propagations.) & SLADE (It is an anomaly-based engine for payload exploit detection. It examines the payload of every request packet sent to monitored services and outputs an alert if it's lossy n-gram frequency deviates from an established normal profile. SLADE makes the n-gram scheme practical by using a lossy structure while still maintaining approximately the same accuracy as the original full n-gram version.) To declare that local host is infected, BotHunter must complete a sufficient and minimum threshold of evidence within its pruning interval. BotHunter considers two potential criteria required for bot declaration:

1) An incoming infection warning(E2) followed by outbound local host coordination or exploit propagation warnings(E3-E5).
2) A minimum of, at least, two forms of outbound bot dialog warnings(E3-E5). While performance checking, in an In Situ Virtual Network, BotHunter successfully detected all bot infections, while in Honeynet experiment, most infection attempts did not succeed. After a 3-week period, working more on configurations, each test for finding a malware infection succeed. In SR1 Honeynet, 95.1% of test cases succeed and 4.9% didn't succeed because of three reasons; infection failures, honeynet setup and policy failures and data corruption failures.

Limitations for BotHunter are as follows; if the communication between the bot and C&C server is encrypted or they are performing a covert scanning technique, then it is very difficult to detect the potential botnets. Also, the bot infected model is based on certain bots and if the model is modified, then the efficiency of BotHunter may be affected. After having some pitfalls, it is not suggested for using it at a bigger level and has big room for modifications.

BotMiner: A botnet detection framework doesn't depend on C&C structure and protocol, and doesn't require the pre-knowledge of botnet signatures and C&C server addresses/name. A botnet works by using an IRC protocol to get the commands from the bot-master. But these days, bot-masters are using P2P communication because if this IRC channel is taken down then bots activities will not work. Structure of the botnets can be centralized or P2P and bots receive command from bot-master, using push and pull mechanism. The bots within the same botnet will have the same communication pattern for both the structures. BotMiner detects the group of machines in a network that are part of botnets. The architecture of BotMiner consist of five main components C-plane monitor, A-plane monitor, C-plane clustering module, A-plane clustering module and cross-panel correlator. A-plane monitor and C-plane monitor will be further classified as A-plane clustering and C-plane clustering, and after that we will get Cross-Plane Correlation.

A-plane monitor is able to detect the exploits, scanning, download and spams, and records the log as "who is doing what". A-plane is built on the basis of Snort, on open source intrusion detection tool, and is capable of record malicious activities that may be performed by internal host with the help of SCADE for scan detection in A-plane. C-plane monitor plans, which captures the log of network flows in a way that can be efficiently stored for analysis and both of them are referred to as Traffic Monitors. The C-plane monitor records the information on "who is talking to whom", and contains these details; time, duration, source IP, source port, destination IP, destination port and the number of packets.

The information from A-plane monitor is passed to the A-plane clustering and from C-plane monitor to the C-plane clustering. In both the cases, clustering algorithm is applied to find the similar pattern and communication by group of machines. In C-plane clustering, certain steps are taken to filter out the traffic load such as filtering out the traffic which is not from internal host to the external host, and flows that established completely i.e. flows with one way traffic. It also filters out traffic whose destination is for well-known servers. This will help in removing the unnecessary traffic for rescuing from any unnecessary confusion. In A-plane clustering, it clusters clients to their specific activities such as same port number, same subnet, same destinations, etc.

And finally Cross-plane correlation combines the result of both the Plane clustering and makes the decision if the machines are a member of botnet or not. limitations with the BotMiner framework is, as we filter the traffic flow on the basis of some points, such as if traffic destination is legitimate server such as Google, so it may be possible the botnet may use these legitimate websites for their C&C communication. Botnet can divert C-plane by changing the number of packets per flow or number of bytes per flow or having the same communication pattern of the normal host. Botnet can divert a-plane monitors by sending the spam very slow, which will divert not only the monitor sensors but the Cross-plane Analysis too.

BotGrep: BotGrep is an peer-to-peer communication based algorithm, it decides which node should communicate with which node following a communication graph. It partitions their communication graph into fast-mixing and slow-mixing pattern. BotGrep algorithm is not affected by the ports, encryption or other content based security measurements. But, it should be linked with some malware detection scheme, eg. anomaly or misuse detection. BotGrep architecture approach starts with a communication graph, where nodes are internet hosts and edges represent communication between them. So, actual requirement for building a BotGrep is building a scalable botnet detection algorithm, to operate on such an infrastructure. BotGrep algorithm works on a communication graph G = (V,E) with V representing the set of hosts recognized in traffic traces and undirected edges. BotGrep algorithm follows an approach consisting of three key steps. First, it applies a prefiltering step to extract a smaller set of candidate, peer-to-peer nodes. This set contains peer-to-peer nodes with false positives and then after that in second step, it follows, clustering technique for clustering with only peer-to-peer nodes and remove false positives. The final step involves validating the result of algorithm based on fast-mixing characteristics. In pre-filtering step, it simply does short random walks, while in clustering part, it looks at peer-to-peer and non peer-to-peer nodes, and then cluster P2P nodes, by using the sybilinfer framework. In this it follows a modified Sybil infer algorithm which will detect P2P nodes in three steps. 1) Generation of traces (It is a mechanism of clustering a set of random walks on the input graph.) 2) A probabilistic model for P2P nodes (It assigns a probability to each subset of nodes of being a P2P nodes.) 3) Metropolis-Hastings Sampling (to compute a set of samples, by which we can calculate marginal probabilities of nodes being P2P nodes.). Modified Sybil infer based clustering approach only partitions the graph into two sub graphs. So, for this, it will be using multiple iteration of the modified Sybil infer based clustering algorithm. In this we perform certain tests and, if all tests get satisfied, means iteration is true. Graph Conductance test (to formalize the notion of a small cut, as they should not have a small cut because of fast-mixing), entropy comparison test and degree-homogeneity test. In a performance wise it is quite efficient, but still it takes some amount of time because of large data sizes.

botNets

How to defeat the zombie army

Author : Peter Kipp, Security Specialist at AVG

A botnet (or as it is often known in security circles, a zombie army), is a collection of personal or business computers or devices that have been compromised by malware or hackers. Unbeknownst to their gentle users, these computers (or 'bots'), are then amassed into vast techno-armies for the purposes of forwarding further viruses or spam to other users, or to conduct large-scale cyber-terrorist attacks such as distributed denial of service (DDoS) or industrial click-fraud.

Botnets use a mixture of conventional malware attack vectors (drive-by-exploits, cracked or illegal software, 'free' pornography, etc) and social engineering to gather fresh recruits. Botnet techniques are particularly insidious in that individual computers often continue to transmit data to its botnet commanders long after the user has detected and 'removed' the initial malware. Once established, they will use well known and trusted internet protocols such as HTTP (World Wide Web) and IRC (Internet Relay Chat) to keep in touch with their victims, and will employ a range of techniques to thwart conventional anti-virus software. AVG's malware researchers have worked with the wider security population to uncover botnets numbering as few as a couple of hundred zombies to botnets of up to several million!

So, how do you know if you've been compromised, and how do you prevent it?

How to spot a bot

Beware of sudden, unexpected changes to your online experience:

- If your computer begins to behave erratically or run particularly slowly
- If your friends and family begin to complain that you are sending them spam or malware, or if you have messages in your sent items that you didn't send
- If your security software detects threats when you aren't even online
- If your internet usage spikes unexpectedly or your ISP detects strange behavior from your machine.

All of these can be indicators that your computer has been compromised. If you think you are compromised, then we recommend that you run a fully featured Internet Security scan through your machine, or seek professional assistance. In many cases it is easier and more cost-effective to reinstall your operating system than it is to continue using a computer that is being controlled by a shady third party.
Apart from this, the old adage holds true – prevention is better than a cure:

Update your operating system

Botnets almost exclusively target the Microsoft Windows operating system, primarily because Windows has the lion's share of the home and business computer market and represents the biggest financial return for the bad guys. Microsoft works as hard as anyone to prevent its customers from being infected, so it is absolutely critical that you download the latest updates, including security patches, when and as they are available. Don't click the "remind me later" button every four hours (that's just lazy), and don't refuse to update your system because you are "happy with what you've got" (that's just naive and foolish).

Use a full internet security suite with behavioral analysis

Conventional anti-virus, whilst it may or may not be successful in fighting off the initial malware attack, is not sufficient to detect or prevent botnet behaviour once the computer has been compromised. Rather than having a piece of software which just scans your hard-drive for known virus signatures, you need software which also scans active processes and launched software based on what it is trying to do. So, if a harmless and trusted web browser (such as Internet Explorer or Google Chrome) is behaving in a way that is not congruent with normal web behavior, a full security suite can flag and prevent the communication as malicious. AVG's unique Identity Protection software, available in AVG Internet Security, is one such behavioral analysis solution.

Use both a hardware and software firewall

Firewalls are another critical level of protection in the fight against the zombie army. Open ports are a botnet's best friend – Trojans and other malware left on compromised machines will keep specific ports open for the purposes of command and control. Unfortunately, the Windows Firewall is often not sufficient protection – you need a flexible, two-way firewall that can block both application based and system based communication on the way out as well as on the way in. If you're a home user, you should also use a hardware firewall, which are included as a standard feature with most of today's modems and routers. If you are directly connected to the internet, with no hardware or software firewall between you and the bad guys, you are effectively at their mercy regardless of any other security software you run.

Control your behavior

Finally, it is critical that you don't lose sight of the fact that the online world, with all its bright lights and apparent anonymity, is just as dangerous as any other (if not more so). It only takes one visit to a dodgy site or one piece of illegally downloaded software to become part of a botnet, and the consequences will usually far outweigh the advantages. Treat the internet with respect, don't expect that it will be able to do the impossible for you, and you and it should get along fine.

Until next time, stay safe out there!

Support Your Local InfoSec Professional

Author : John Shinaberry

I'm typing along last night and I realize, spellcheck is loading at an extremely slow rate. I go to check my processes; they all appear to be normal, save for the fact that svchost is using an extraordinary amount of resources. I now have to stop what I'm doing, save my work and boot into safe mode to look closer. For me this is a major inconvenience, because my thought process isn't like the process tree of an application, I can't necessarily just pick up where I left off later on (unstable long term storage). This is a problem that many people face, every single day. The system becomes unresponsive, the system simply fails, they lose the power of their interface due to unknown forces.

A lot of times, what they find (or worse yet, they don't find), is that their system has fallen victim to an attack in the form of malware.

The term “malware” can mean a lot of different things to the people who understand it, but the one definition that is clear to everyone is the theft of productivity. Time is money, and malware costs a lot of time. To go a step further, time is the measure of available cycles for productivity and creativity, life itself is restricted by time. With the stakes so high, it is more than a trivial thing to lose so much time to malware. Taken on an individual basis, malware is an inconvenience (ranging from mild to epic rage), but on the worldwide scale it is more than that. How many brilliant ideas have been hampered due to completely unnecessary system failure? That is a cost that cannot be quantified.

The modern world has become a tapestry of thought, people are well connected. I can introduce my plans to drink coffee on Twitter, announce my status as single on Facebook and request help with any problem I might have on an appropriate forum, all before breakfast. With such a powerful tool available, it is only natural that I will become at least somewhat dependent on it.

My computer (desktop, laptop, handheld device, any programmable interface at my disposal) becomes an integral part of my mind. What is even more profound is that I now have access to so many other human minds, input from all over the world. Since an increasing percentage of the input and output that guides my reasoning about the world around me comes from my connection through a software interface, when that system is attacked, so am I. My whole thought process, everything going in and coming out has become infected by rogue input.

When I look at it from this point of view, I think of malware as being much more than just an inconvenience. Just as a contagion in the biological ecosystem that keeps my body alive could be an eminent threat to my survival, a malware infection might be a similar threat to the congruence of my thoughts and ideas. While my ideas may not be the ones to change the world, what if the next Albert Einstein solves an incredibly complex problem, elsewhere on the network, and as he reaches critical mass on his breakthrough, his system crashes and he loses the bridge of thought that led to his discovery.

What if the next Mother Theresa loses faith in humanity, because she finds herself under what she perceives as a personal attack, as she tries to formulate a plan to help feed the poor. Emotional health is just as important to the world as physical health, and intentional attacks on the process of thought can be just as destructive as an attacking, physical army. It is so destructive because the incarnation of life that we perceive as human beings is internal, we see and feel everything from the minds eye.

Graffiti and pointless destruction are certainly not new concepts in the internet age, but the effects can certainly be more intrusive to the individual than ever before. The people who research and try to combat malware are becoming more significant, because they are defending more than just our computers, they are defending our minds. They deserve the support, respect and cooperation of all of us who incorporate an electronic device into our creative and productive processes. We can easily support them by providing feedback on our personal experiences with mal ware, on sites like The Hacker News. We can provide them with financial support, because information security is an emerging field of study, and it requires resources to properly evaluate and counter threats. We are all under attack in the cyber landscape, but thanks to the same framework that allows malware to spread, we also have the ability to work together against it. Supporting one another is what networked communications is all about, and the security professionals that are defending our networks need our support more than ever before.

The Rapid Rise Of The Botnet

Author : Lee Ives

If you are reading this article then you likely already know just how great an innovation the internet has been. Just about anyone can hop onto the World Wide Web and find a huge amount of information about almost any topic in minutes. The sheer volume of data stored on the web is astounding and not even the best libraries in the world can come close to competing in terms of the amount of information they store. But the one big disadvantage to all that information on the internet is the fact that you cannot always be sure that what you are reading is true. And the really curious thing is that false information will often spread faster and further afield than accurate data ever will. Much like a virus (the human kind), false data will often spread unchecked at breakneck speed and stopping the flow can often prove difficult.

Thats where the bad guys come in. Hackers and other online criminals learned long ago that news - be it good, bad or completely made up - will have the potential to spread like wildfire. And that serves their purposes very well indeed.

Any news will do

One of the popular ways for online criminals to make money is through the use of botnets. Once a botnet is set up they can use it in many different ways, such as for sending huge amounts of spam email or for orchestrating DDOS attacks, both of which they would receive handsome payment for. But the thing is, how do they grow a large botnet in the first place?

Well, one way is to leverage the news. As I said above, news travels very quickly across the web, even if it isn't true. So when a hacker wants to increase the size of their botnet they may very well tap into this area in order to achieve it. Of course the angle that they use has to be interesting - even your average web surfer who has little thought of security will be unlikely to click on links that sound like they go someplace boring. Therefore the news is a good way for the hackers to entice their victims.

Sometimes true stories will work for them as there is a huge interest there already. More often, fake news and enticing headlines are required though - you know, the "click here to see so-and-so naked" type links that can be found all across the net, or "celebrity x dies in car crash" type headlines that we've all seen on the web and received via email.

Hopefully some of you will already know better than to click through those sorts of links, even though it is human nature to be tempted. Alas, a large number of people are easily duped though and that is a real problem.

Botnet +1

Getting people to click on suspect links on the web or in emails is exactly what the bad guys are hoping to achieve. If you do click on something you shouldn't then you will have fallen into their trap. An infected piece of code will be downloaded onto your computer and, should it be installed, then you will now be another member of their botnet.

You may not realise that straight away, or ever, but your machine could now be used to help spread spam around the internet or to help bring networks down with a DDOS attack. In a way you will have become an attacker yourself and will be partly responsible for some of the issues that the web suffers from these days.

Good news, bad news, celebrity gossip and nude pictures are all highly interesting topics (even if we may wish they weren't) and the average surfer will often be tempted to find out more about any or all of them. Just make sure that your own curiosity doesn't take you to places where your computer would rather you didn't visit or else you may just be the reason why botnets are able to grow so quickly.

The Top 50 #911Truth #WTFacts Campaign

50 Days of Crazy Facts, Rumors and Questions

Author : John Shinaberry

It's been almost 11 years since the September 11th attacks on the United States, more specifically 50 days until this iteration. Today, we are launching our "Top 50 #911Truth WTFacts" campaign, culminating with number 1 on this year's anniversary. Specifically, we'll be breaking down the inconsistencies in the 9/11 Commission Report. Some of you reading this may be rolling your eyes for various reasons. Which category do you fall in?

Are you the patriotic "I'm sick of truthers" type that refuses to logically parse any evidence and excoriate anyone does, for argument's sake, like Bill Maher? For those that may defend Bill Maher for various reasons, see the more deliberate example of Tucker Carlson's disinfo.
That may be too much alternative media jargon for some of our readers, so let's back up.

Maybe you don't know what a truther is but are too patriotic to consider that high ranking US government officials have obsfucated and outright lied about the events of that day. If that's a stretch to you, then you definitely have a hard time considering the notion that people within the government had prior knowledge of the attacks, or worse, participated in them.

Are you simply a pragmatic person on the fence? You are the type to attempt to logically evalu-ate things before coming to a final conclusion, already "looked into it" and remain unconvinced.

Some consider themselves reasonable individuals but a concept or theory like the government being involved in the horrific attacks is unreasonable to suggest.

Some trust the government enough that the thought doesn't cross their mind.

Other contingents of people don't care if that was the case, they are resigned to the fact that nothing can be done about it.

The central problem in all of this is that the information necessary to form a logical, fact based theory is scattered, distorted, or concealed.

If one did want to do this research, where can one go to get accurate information? Beyond that, what about the concerns of government spying or others branding you as crazy?

These are some of the reasons that "conspiracy theories" are not evaluated by more people and more to the point, the reason that a stigma is attached to efforts to investigate large crimes.

It is because of the disinformation, peer pressure and watchful eye of the government that it is taboo to even discuss, and part of why the term "conspiracy theory" takes a negative connota-tion. It has basically become a four-letter word and destroys the possibility of reasonable, mean-ingful discussion.

Do not read this as us saying the blame is squarely on "Big Brother" government, there is another element to consider. The reckless nature of (for the sake of brevity) some "conspiracy theorists" gives the detractors ammunition for the argument that people who consider these things are crazy.

The incomplete vetting of information and faulty conclusions that some theorists draw is a big problem. It leads to more disinformation and distortion of reality.

The problems of having open and purposeful debate are not just limited to the conspirators or the unknowing people who aide these crimes and that is something to bear in mind for those that wish to engage in this sort of debate.

Consequently, the nexus of this article and campaign is the need to apply these standards and intense scrutiny to the events on and contributing to the September 11th attacks. Since then, the world has been irrevocably changed, it cannot go back to the way it was and respectfully to the lives lost as a result, it shouldn't. Simply taking a "go back to what used to be" approach is part of what allowed those attacks and up to now, what has been a clean getaway for the perpetra-tors.

The system of vilifying those that dare to ask questions of those who hold themselves out as above suspicion must end or we will find ourselves in the same vice of criminality with no respite.

To solve this problem and have a better functioning society, we must all take part in the debate, learn what we have to correct as individuals, appropriately evaluate the problem at hand and con-tribute our best ideas without selfish agendas or toxic rhetoric.

Even if intensified analysis doesn't produce enough evidence to warrant convictions, just having more people be aware of the head-scratching irregularities is enough to turn the tide against the New World Order and it's largely occultist membership. The September 11th attacks will be investigated from every angle, from the apparent and concrete to the esoteric and obscure such as the signs that 9/11 was a widescale occult human sacrifice.

The entire world can be part of the stage for these "people".

So without further delay, presenting #911Truth WTFact #50.