Pc Security

Lab 1

Robert Gabriel

# Task 1:Identify at least four websites where you can get details of the most current malware threats.

[mcafee.com](http://mcafee.com) : <http://www.mcafee.com/threat-intelligence/malware/latest.aspx>

[trendmicro.com](http://trendmicro.com) : [http://about-threats.trendmicro.com/us/threatencyclopedia#malware](http://about-threats.trendmicro.com/us/threatencyclopedia%23malware)

[symantec.com](http://symantec.com) : <http://www.symantec.com/security_response/landing/threats.jsp>

[microsoft.com](http://microsoft.com) : <http://www.microsoft.com/security/portal/threat/threats.aspx>

# Task 2 :Compile a list of eight of the most recent threats, including the following information

**Malware Name:**  W32/Expiro!D060AFD525​EF

**The risk analysis of the threat:** The W32 Expiro is a virus that affects the systems running on w32. These include Windows Xp, Vista and 7. What the Virus does it allows Steals personal sensitive information, allows backdoor access and control over the computer. If the infected computer has Firefox, it redirects websites also as petitioned before it Lowers Internet Explorer security.

**What type of threat it is:**

* Malware Type: Trojan
* Malware Sub-type: Generic
* Alert level: Severe
* Discovery Date: 2014-02-06

**How it works .**

The virus infects exe files on all local and network drives avaaible to write to . It targets all shortcuts on your pc as well.

Its starts by looking at the following locations

* %USERPROFILE%\Start Menu\Programs

Content of the infected file is copied with a .vir extension to the file with the same name. This file is saved to the parent folder of the infected file. The virus then adds a section with the "PACK" name to the end of the vir-file. This section contains a virus body. The code of corresponding file entry point address is modified to allow a virus body to control it. The infected file is then removed. The .vir extension is changed to .exe. The file infection and the service run occur on the next system boot. To infect protected files, the virus disables Windows File Protection (WFP).

Win32/Expiro collects the following sensitive information:

Installed certificates.Credentials stored by FileZilla.Credentials stored by Windows Protected Storage.Credentials entered by users in different windows, for example, in Internet Explorer

**How you can remove it**

If you have not used any antivirus program to protect your computer from viruses and it gets infected with this malicious program, follow the steps listed below to remove it:

1. Run a full scan of your computer using the Antivirus program with the updated definition database .
2. Do not run executable files and do not reboot the computer until you run a full scan of your computer using the Antivirus program.
3. Delete the original malware file (its file name and location depends on the way the malware originally penetrated a user’s computer).
4. Clean the Temporary Internet Files folder, which contains infected files.

**Malware Name:** TrojanDownloader:Win32/Kuluo.D

**The risk analysis of the threat:** TrojanDownloader:Win32/Kuluo.D is a Trojan that downloads , installs other programs without consent on the users computer. This means it could include the installation of additional malware or malware components to an affected computer. It is low to medium effts leader.

**What type of threat it is**

* Malware Type: Trojan
* Malware Sub-type: Generic
* Alert level: Severe
* Discovery Date: 2014-02-06

**How it works .**

When it runs, TrojanDownloader:Win32/Kuluo.D copies itself to c:\documents and settings\administrator\local settings\application data\pcnjbjhf.exe.

The malware creates the following files on your computer:

* *<current folder>\<malware file>.txt*

The virus itself trys and contacts a remote host. This comply used for the following reasons.

* To confirm Internet connectivity
* To report a new infection to its author
* To receive configuration or other data
* To download and execute files.
* To upload data taken from the affected computer

**How you can remove it**

1. Disable Windows System Restore.
2. Run a full system scan.
3. Reboot, as soon as it is convenient, to ensure all malicious components are removed.

**Malware Name:** W32/Sality.gen!3C7E6D​03F981

**The risk analysis of the threat:** The alert level is Severe ,the virus spreads by infecting windows executable files and copying itself to removable and remote drivers. It terminates lots of various security products on the computer.

**What type of threat it is**

* Malware Type: Trojan
* Malware Sub-type: Generic
* Alert level: Severe
* Discovery Date: 2014-02-04

**How it works :**

The virus injects code into all running processes to load and run the virus and infect Windows executable files with extension ".EXE" or ".SCR". The virus seeks other target files by reading file names found in the registry subkeys.

Deletes security-related files

This virus deletes security data files including security software detection database files or signatures that have the following file extensions found in all drives and network shares:

* *.AVC*
* *.VDB*

Terminates security-related processes

It attempts to terminate the following security-related processes:

Modifies Windows settings

* Disables Windows Registry Editor:
* From the reguistory.

Downloads arbitrary files It attempts to download files from remote servers to the local drive.

**How you can remove it**

1. Disable Windows System Restore.
2. Run a full system scan.
3. Reboot, as soon as it is convenient, to ensure all malicious components are removed.

**Malware Name:** Downloader.gen.a!9EBF​C68C6A2A

**The risk analysis of the threat:** Downloader.gen.a!9EBF​C68C6A2A is a trojan downloader that is dropped and executed by Downloader.gen.a!9EBF​C68C6A2A. It terminates certain processes and services related to antivirus programs, and connect to a certain website, possibly to download other malware.

**What type of threat it is**

* Malware Type: Trojan
* Malware Sub-type: Generic
* Alert level: Severe
* Discovery Date: 2014-02-04

**How it works .**

Terminates Running Processes and Disables Services

TrojanDownloader:Win32/Dogrobot.gen!J queries the system registry for the following keys and entries, which are associated with the ESET antivirus program:

Entry: InstallDir  
Subkey: HKLM\SOFTWARE\Eset\Nod\CurrentVersion\Info

If these exist, the trojan creates the batch file *sin.bat* to terminate the following ESET-related processes:

It uses the same batch file to disable the following services:

* NOD32krn
* ekrn

It also temrinates the following process:

* 360TRAY.EXE

Downloads Files

TrojanDownloader:Win32/Dogrobot.gen!J checks if Internet connection is available by attempting to connect to the following web sites:

* http://www.google.cn
* http://www.baidu.com

If successful, it then downloads the file *down.txt* from the site *cao.caonima01.com*.

How you can remove it

1. Disable Windows System Restore.
2. Run a full system scan.
3. Reboot, as soon as it is convenient, to ensure all malicious components are removed.

**Malware Name:** RDN/Sdbot.bfr!d!44C97​0AD5ECA

**The risk analysis of the threat:**

RDN/Sdbot.bfr!d!44C97​0AD5ECA is a member of RDN/Sdbot.bfr!d!44C97​0AD5ECA - a broad family of backdoor trojans that allows unauthorized access and control of an affected computer by a remote attacker via IRC.

**What type of threat it is:**

* Malware Type: Virus
* Malware Sub-type: N/a
* Discovery Date: 2014-02-04
* Alert level: Severe

**How it Works :**

RDN/Sdbot.bfr!d!44C97​0AD5ECA creates the following files on an affected computer:

* *c:\documents and settings\administrator\local settings\temp\i1385411986.bat*

Which allows back door access to more malware and virus.

it ttys and attempts to connect to an IRC server at *irc.whhcd.info*via TCP port 6667, join a channel and wait for commands.

Using this backdoor, an attacker can perform a number of actions on an affected computer. For example, an attacker may be able to perform the following actions:

* Download and execute arbitrary files
* Upload files
* Spread to other computers using various methods of propagation
* Log keystrokes or steal sensitive data
* Modify system settings
* Run or terminate applications
* Delete files

How you can remove it

1. Disable Windows System Restore.
2. Run a full system scan.
3. Reboot, as soon as it is convenient, to ensure all malicious components are removed.

**Malware Name:** RDN/Downloader.gen.a!​BF91297E36DC

**The risk analysis of the threat:**

* Malware Type: Trojan
* Malware Sub-type: Generic
* Discovery Date: 2014-02-09
* Alert level: Severe

**What type of threat it is :**tojron

**How it works .**

The RDN/Downloader contacts remote host at contact a remote host at 82.146.49.70 using port 80. Most times this type of malware/Tojan does this :

* Report a new infection to its author
* Receive configuration or other data
* Download and run files, including updates or other malware
* Receive instructions from a remote hacker
* Upload data taken from your PC

**How you can remove it**

1. Disable Windows System Restore.
2. Run a full system scan.
3. Reboot, as soon as it is convenient, to ensure all malicious components are removed.

**Malware Name:** Trojan:Win32/Loktrom.M

**The risk analysis of the threat:**

Malware Type: Trojan

Malware Sub-type: N/A

Discovery Date: 2014-02-09

Alert level: Severe

**What type of threat it is :**

Trojan:Win32/Loktrom.M is a malicious program that is unable to spread of its own accord. It may perform a number of actions of an attacker's choice on an affected computer.

**How it works :**

When installed the Trojan:Win32/Loktrom.M modifies the following registry entries to ensure that its copy executes at each Windows start:

Adds value: “Shell" With data: "<malware file>.exe”,to subkey: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Trojan:Win32/Loktrom.M terminates the following processes should they be running on an affected computer:

* explorer.exe

The malware may contact a remote host at google.com using port 80. Commonly, malware may contact a remote host for the following purposes:

* To report a new infection to its author
* To receive configuration or other data
* To download and execute arbitrary files (including updates or additional malware)
* To receive instruction from a remote attacker
* To upload data taken from the affected computer

How you can remove it

1. Disable Windows System Restore.
2. Run a full system scan.
3. Reboot, as soon as it is convenient, to ensure all malicious components are removed.

**Malware Name:** Backdoor:Win32/Luder.A

**The risk analysis of the threat:** Backdoor:Win32/Luder.A is a virus that spreads by infecting executable files, by inserting itself into .RAR archive files, and by sending a copy of itself as an attachment to e-mail addresses found on the infected computer. This virus has a date-activated, file damaging payload, and may connect to a remote server and accept commands from an attacker.

**What type of threat it is:** Malware Type: Virus

Malware Sub-type: Win32

Alert level: Severe

Discovery Date: 2014-02-09

## How it works :

## When run, Backdoor:Win32/Luder.A drops a copy of itself as 'duel\_v2.exe' into the Windows system folder. The virus then registers itself to run at Windows start by adding a registry value.Win32\_Duel\_v2 with data: <system folder>\duel\_v2.exe

In subkey: HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

It creates a log file "duel.log" in the Windows folder, and verifies Internet connectivity by testing connection attemtps to the domain 'google.com' using TCP port 80.

Win32/Luder.A will search within data files with file extensions .HTM, .TXT and .HTA, and collect e-mail addresses from them.

**How you can remove it**

1. Disable Windows System Restore.
2. Run a full system scan.
3. Reboot, as soon as it is convenient, to ensure all malicious components are removed.

# Task 3: Write a short report on the use of Fake Diagnostic/Anti-Virus tools in online attacks.

Rogue security software mainly relies on social engineering (fraud) to defeat the security built into modern operating systems and browser software and install it onto victims' computers.

Evidently, the Rogue-Antivirus does not execute an actual scan, and then the computer can be absolutely clean. Once it has reported the presence of these hypothetical malware, the Rogue-AV usually proposes for the user to buy a theoretical paid version to clean the computer.

A website may, for example, display a fictitious warning dialog saying that someone's machine is infected with a computer virus, and encourage them through manipulation to establish or purchase shareware in the belief that they are purchasing genuine antivirus software.

Once installed, the rogue security software may then try to entice the user into buying a service or additional software by:

* Alerting the user with the fake or simulated detection of malware or pornography.
* Displaying an animation simulating a system crash and reboot.
* Selectively disabling parts of the system to prevent the user from uninstalling the malware.
* Altering system registries and security settings, then "alerting" the user.
* A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks.
* Developers of rogue security software may also entice people into purchasing their product by claiming to give a portion of their sales to a charitable cause.

As mentioned in point Five, A botnet with the more it has the greater the power the bonnet it has. If pictured and going back to the 2010 -2012 where activist groups like losses and anonymous used boat nets like this to achieve the power to take down the website. Some methods where that's from installing malware. Example of this is the Highest Hyped but faked Anonymous Linux based OS (http://en.wikipedia.org/wiki/Anonymous-OS). Which was riddled with malware and Botnets? In short, it is used widely in terms of the methods for hackers, to steal information, strength botnets and to gain control over the user’s computer.