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://www.mcafee.com/threat-intelligence/malware/latest.aspx

trendmicro.com :
http://about-threats.trendmicro.com/us/threatencyclopedia#malware

symantec.com :
http://www.symantec.com/security_response/landing/threats.jsp

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!D060AFD525EF

The risk analysis of the threat:

The W32 Expiro is a virus that affects the systems running on w32 machines. These include Windows Xp, Vista and 7. The Virus steals personal sensitive information, allows backdoor access and control over the computer. If the infected computer has Firefox, it redirects websites and also lowers Internet Explorer security.

What type of threat it is:

- Malware Type: Trojan
- Alert level: Severe
- Discovery Date: 2014-02-06

How it works.

The virus infects exe files on all drives rendering them unwriteable. It targets all shortcuts on your PC as well.

“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 infected file is then removed.” Their extension is changed to. exe. The file infection and the service run occur on the next system boot.
Win32/Expiro collects sensitive information on the PC

How you can remove it:

- Run a full scan of your computer using the Antivirus program with the updated definition database.
- Do not run executable files and do not reboot the computer until you run a full scan of your computer using the Antivirus program.
- Delete the original malware file (its file name and location depends on the way the malware originally penetrated a user’s computer).
- 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 of the user's computer. This means it could include the installation of additional malware or malware components to an affected computer.

What type of threat it is:

- Malware Type: Trojan
- Alert level: Severe
- Discovery Date: 2014-02-06

How it works:

When it runs, the virus 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

Note there wasn't a huge amount of information on the virus.
The virus itself tries to contact a remote host.
This connection is used for the following reasons.

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

How you can remove it:

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

Malware Name:

W32/Sality.gen!3C7E6D03F981

The risk analysis of the threat:

The virus spreads by infecting windows executable files and copying itself to removable and remote drivers. It terminates various security products on the computer.

What type of threat it is:

- Malware Type: Trojan
- 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 the extension ".EXE". The virus seeks other target files by reading file names found in the registry subkeys.
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

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

How you can remove it:

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

Malware Name:

Downloader.gen.a!9EBFC68C6A2A

The risk analysis of the threat:

Downloader.gen.a!9EBFC68C6A2A is a trojan downloader that is dropped and executed by Downloader.gen.a!9EBFC68C6A2A. It terminates certain processes and services related to antivirus programs, and connects to a certain website, possibly to download other malware.

What type of threat it is:

- Malware Type: Trojan
- Alert level: Severe
- Discovery Date: 2014-02-04

How it works:

It 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

Downloader. Gen. a! 9EBFC68C6A2A checks if Internet connection is available by attempting to connect to the following web sites:
http://www.google.cn

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

How you can remove it:

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

Malware Name:

RDN/Sdbot.bfr!d!44C970AD5ECA

The risk analysis of the threat:

RDN/Sdbot.bfr!d!44C970AD5ECA is a member of RDN/Sdbot.bfr!d!44C970AD5ECA - a broad family of backdoor Trojans that allows unauthorised access and control of an affected computer by a remote attacker via IRC.

What type of threat it is:

- Malware Type: Virus
- Discovery Date: 2014-02-04
- Alert level: Severe

How it Works :

The virus 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.
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:

- Disable Windows System Restore.
- Run a full system scan.
- 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:

It’s a Trojan which downloads other types of virus.

What type of threat it is:

- Malware Type: Trojan
- Discovery Date: 2014-02-09
- Alert level: Severe

How it works:

The RDN/Downloader contacts a remote host at 82.146.49.70 using port 80. Most of time this type of malware/Trojan:

- Reports a new infection to its author
- Receives configuration or other data
- Downloads and runs files, including updates or other malware
- Receives instructions from a remote hacker
- Uploads data taken from your PC

How you can remove it

- Disable Windows System Restore.
- Run a full system scan.
- 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:

This type of malware is a trojan and it is used to download additional types of malware to a device.

What type of threat it is:

- Malware Type: Trojan
- 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 by itself. It may perform a number of actions of an attacker's choice on an affected computer.

How it works :

When installed it modifies the registry entries to ensure that its copy executes at each Windows start.

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

- Disable Windows System Restore.
- Run a full system scan.
- 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 connects to a remote server and accept commands from an attacker.

What type of threat it is:

- Malware Type: Virus
- Alert level: Severe
- Discovery Date: 2014-02-09

How it works :

When running, 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.

It creates a log file "duel.log" in the Windows folder, and verifies Internet connectivity by testing connection attempts 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

- Disable Windows System Restore.
- Run a full system scan.
- 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 be installed onto users' computers.

The Rogue-Antivirus purports to execute a scan and presents the user with a false report, claiming that their device is overrun with malware and suffering from serious errors which they must pay to have corrected.

A website may, for example, display a fictitious warning dialogue saying that someone's machine is infected with a computer virus, and encourage them through manipulation to download or purchase shareware in the belief that they are getting 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 to a 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.
- Claiming to give a portion of their sales to a charitable cause.

A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. The greater the number of computers linked together on the botnet, the stronger the botnet’s capacity for generating attacks will be. Going back to the 2010 - 2012 period when activist groups like Lulzsec and anonymous used botnets like this to achieve the power to take down a website. Some of these methods relied on the installation of malware. In 2012, for example a Linux-based OS, endorsed by Anonymous was released following much anticipation (http://en.wikipedia.org/wiki/Anonymous-OS) however, the system was riddled with malware and Botnet software, which allowed Anonymous to greatly increase the potential strength of their DOS attacks.

In conclusion, the Fake Anti-Virus method is used widely by hackers to steal information, strengthen botnets and to gain control over the user’s computer.