CEH SeoCheatSheet

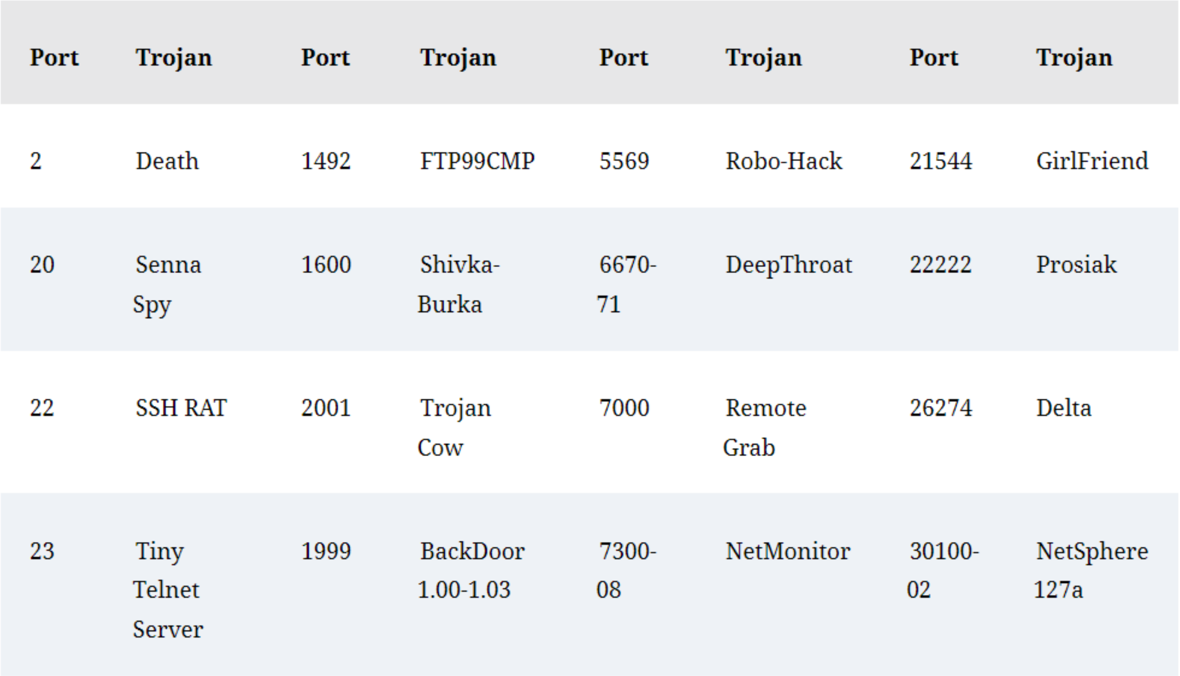
Contents

Chapter 4: Malware

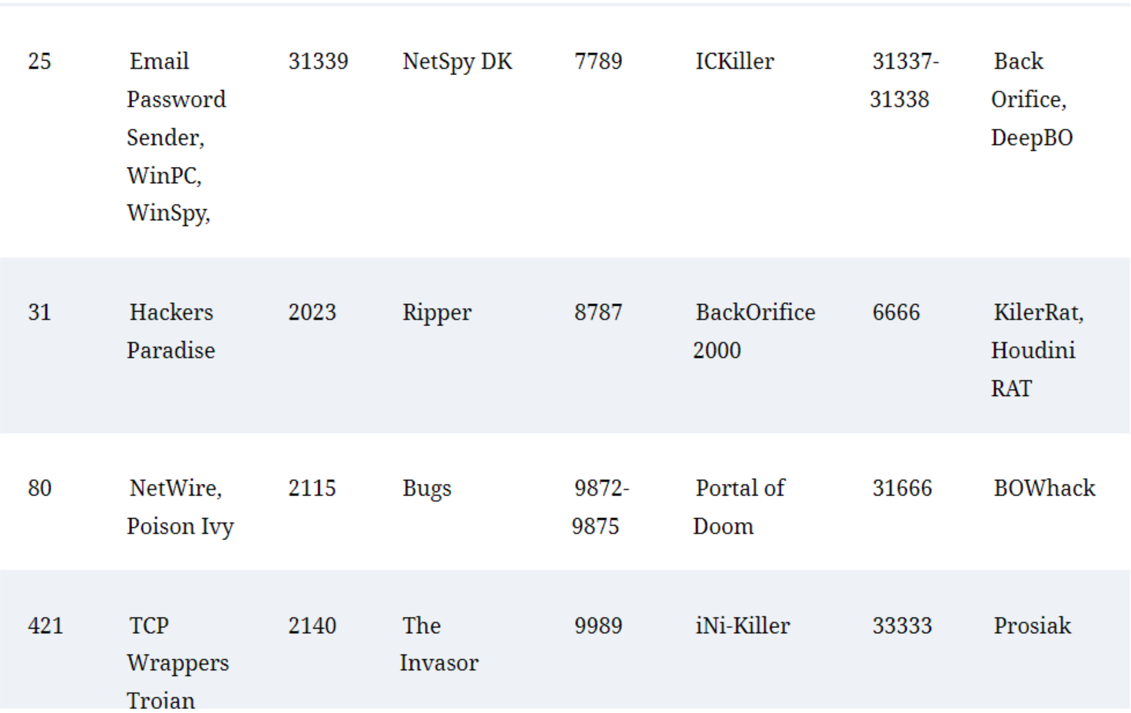
Malware Types

Trojan horses

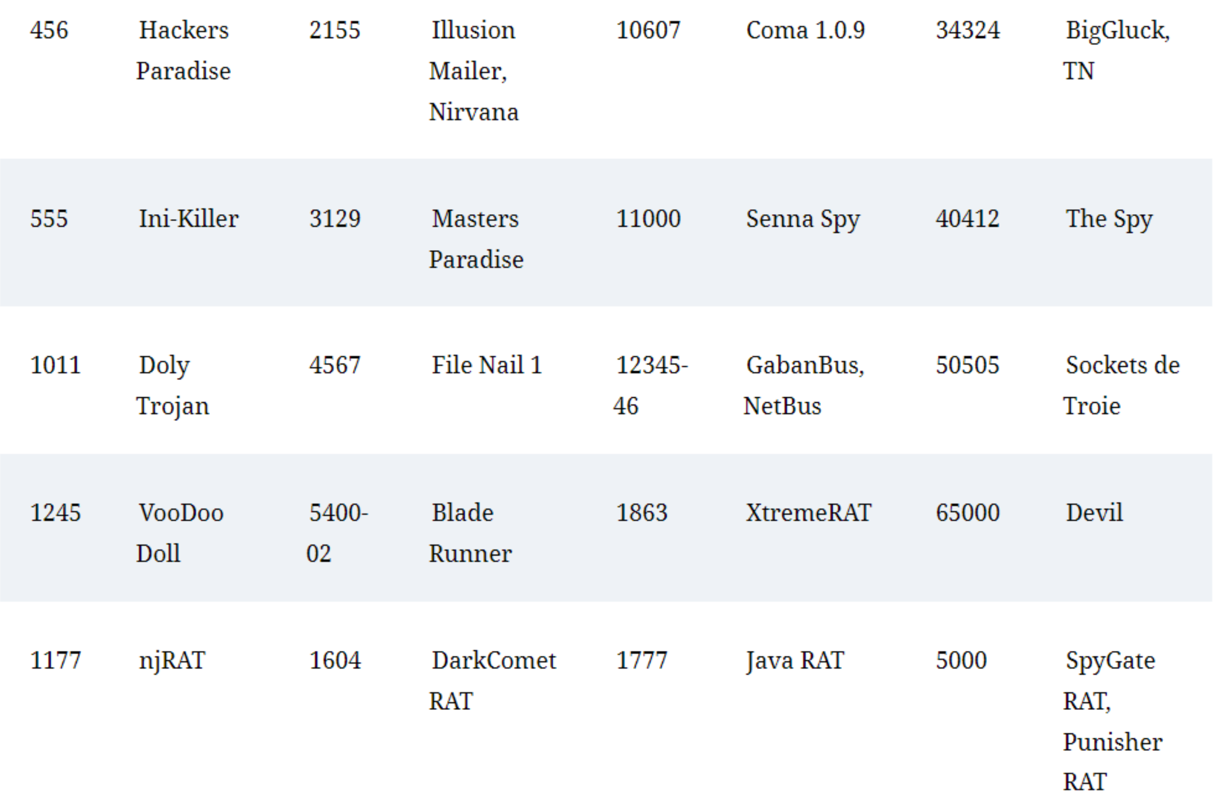
TABLE 4.1 Some Known Trojan Horses and Their Specific TCP Ports



Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP	5569	Robo-Hack	21544	GirlFriend
20	Senna Spy	1600	Shivka-Burka	6670-71	DeepThroat	22222	Prosiak
22	SSH RAT	2001	Trojan Cow	7000	Remote Grab	26274	Delta
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7300-08	NetMonitor	30100-02	NetSphere 127a



25	Email Password Sender, WinPC, WinSpy,	31339	NetSpy DK	7789	ICKiller	31337-31338	Back Orifice, DeepBO
31	Hackers Paradise	2023	Ripper	8787	BackOrifice 2000	6666	KilerRat, Houdini RAT
80	NetWire, Poison Ivy	2115	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers Trojan	2140	The Invasor	9989	iNi-Killer	33333	Prosiak



456	Hackers Paradise	2155	Illusion Mailer, Nirvana	10607	Coma 1.0.9	34324	BigGluck, TN
555	Ini-Killer	3129	Masters Paradise	11000	Senna Spy	40412	The Spy
1011	Doly Trojan	4567	File Nail 1	12345-46	GabanBus, NetBus	50505	Sockets de Troie
1245	VooDoo Doll	5400-02	Blade Runner	1863	XtremeRAT	65000	Devil
1177	njRAT	1604	DarkComet RAT	1777	Java RAT	5000	SpyGate RAT, Punisher RAT

While the term ***Trojan horse*** is used to describe any software that is designed to deliver a malicious payload, there are specialized Trojan horses, including:

Remote access Trojan: This type of Trojan is specifically designed to deliver remote access utilities to the target system.

Proxy Trojan: This type of Trojan essentially turns the target system into a proxy server, so the attacker can use that system as a base to attack other systems.

FTP Trojan: This type of Trojan initiates an FTP server on the target machine so the attacker can upload or download files.

Data stealing Trojan: As the name suggests, this type of Trojan is designed to deliver spyware and steal data. A subset of this type, called a banking Trojan, specifically targets financial data on the target system.

Destructive Trojans: As the name indicates, this type of Trojan delivers malware that will cause damage to the target system. It might delete system files, interfere with system operations, or conduct other types of destructive activities.

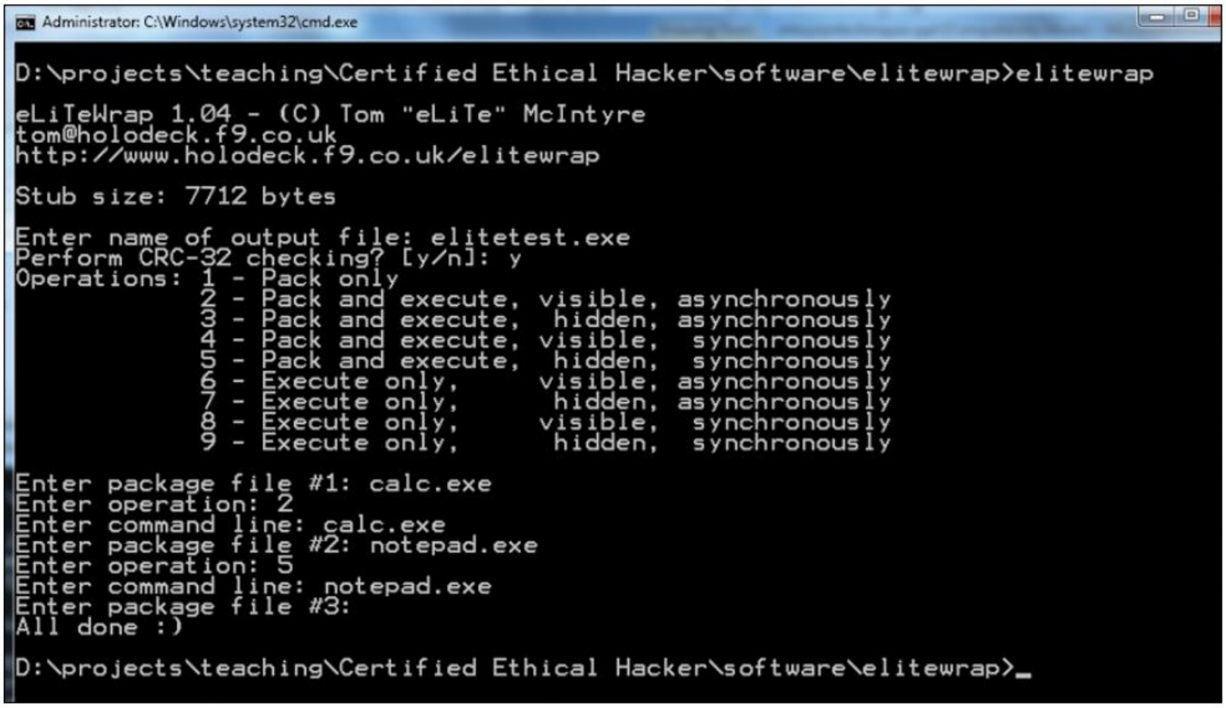
Command shell Trojan: This type of Trojan delivers some sort of command line remote access tool. For example, **netcat** is often used by network administrators to communicate between machines. A command shell Trojan might deliver **netcat** and have it listen on a machine while users connect and execute commands.

Covert channel tunneling tool (CCTT) Trojan: This type of Trojan creates arbitrary data transfer channels in the data streams authorized by a network access control system.

Defacement Trojan: This type of Trojan is used to deface either a website or an application. It is possible to find on the internet defacement Trojans that can deface standard Windows applications such as the Calculator app.

eLiTeWrap is a common Trojan horse tool that is easily found on and downloaded from the internet

Figure 4-1: eLiteWrap

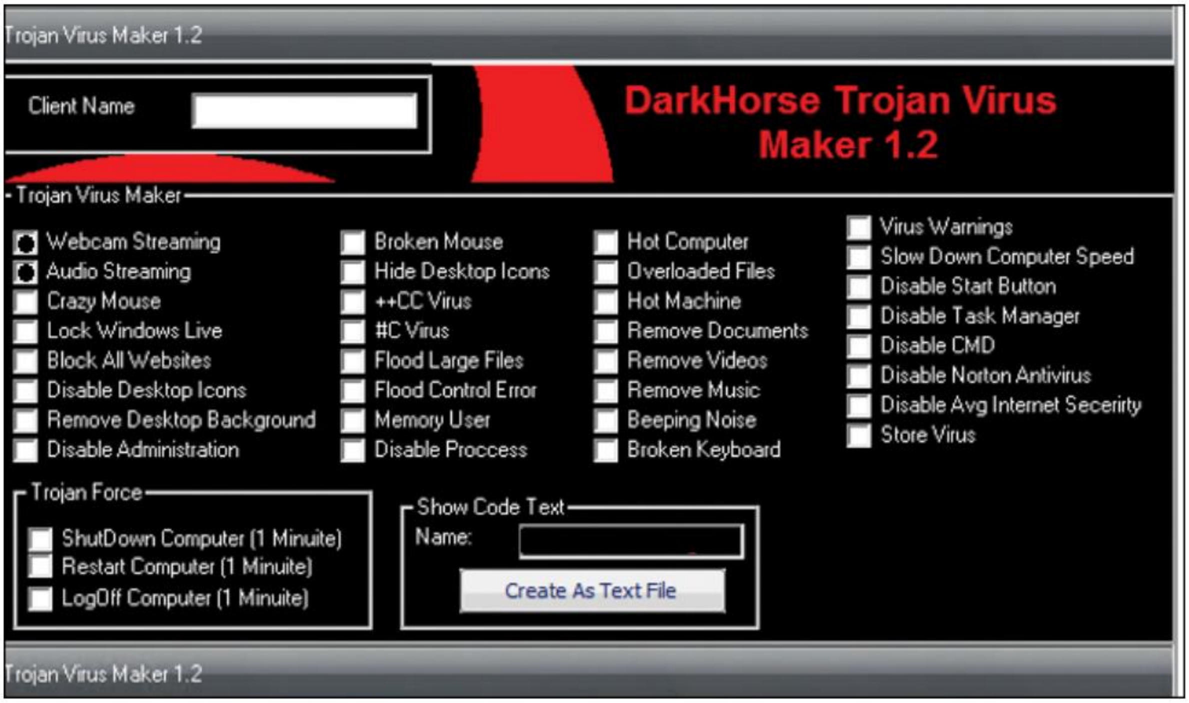


```
D:\projects\teaching\Certified Ethical Hacker\software\elitewrap>elitewrap

eLiTeWrap 1.04 - (C) Tom "eLiTe" McIntyre
tom@holodeck.f9.co.uk
http://www.holodeck.f9.co.uk/elitewrap

Stub size: 7712 bytes

Enter name of output file: elitetest.exe
Perform CRC-32 checking? [y/n]: y
Operations: 1 - Pack only
            2 - Pack and execute, visible, asynchronously
            3 - Pack and execute,  hidden, asynchronously
            4 - Pack and execute, visible,  synchronously
            5 - Pack and execute,  hidden,  synchronously
            6 - Execute only,     visible, asynchronously
            7 - Execute only,      hidden, asynchronously
            8 - Execute only,     visible,  synchronously
            9 - Execute only,      hidden,  synchronously

Enter package file #1: calc.exe
Enter operation: 2
Enter command line: calc.exe
Enter package file #2: notepad.exe
Enter operation: 5
Enter command line: notepad.exe
Enter package file #3:
All done :)

D:\projects\teaching\Certified Ethical Hacker\software\elitewrap>_
```

FIGURE 4.1 **eLiTeWrap**

DarkHorse Trojan Virus Maker is another tool for wrapping programs. It has a nice GUI interface that makes it even easier to work with than eLiTeWrap.

Figure 4-2: Trojan Virus Maker 1.2



Client Name

Trojan Virus Maker

☑ Webcam Streaming
☑ Audio Streaming
☐ Crazy Mouse
☐ Lock Windows Live
☐ Block All Websites
☐ Disable Desktop Icons
☐ Remove Desktop Background
☐ Disable Administration
☐ Broken Mouse
☐ Hide Desktop Icons
☐ ++CC Virus
☐ #C Virus
☐ Flood Large Files
☐ Flood Control Error
☐ Memory User
☐ Disable Proccess
☐ Hot Computer
☐ Overloaded Files
☐ Hot Machine
☐ Remove Documents
☐ Remove Videos
☐ Remove Music
☐ Beeping Noise
☐ Broken Keyboard
☐ Virus Warnings
☐ Slow Down Computer Speed
☐ Disable Start Button
☐ Disable Task Manager
☐ Disable CMD
☐ Disable Norton Antivirus
☐ Disable Avg Internet Secerity
☐ Store Virus

Trojan Force

☐ ShutDown Computer (1 Minuite)
☐ Restart Computer (1 Minuite)
☐ LogOff Computer (1 Minuite)

Show Code Text

Name:

FIGURE 4.2 DarkHorse Trojan Maker

There are many more tools for wrapping programs. A few are listed here:

1. Advanced File Joiner https://download.cnet.com/Advanced-File-Joiner/3000-2094_4-169639.html
2. Hidden Cry https://pentesttools.net/hidden-cry-windows-crypter-decrypter-generator-with-aes-256-bits-key/
3. Exe2vbs https://github.com/rapid7/metasploit-framework/blob/master/tools/exploit/exe2vbs.rb
4. IExpress Wizard https://docs.microsoft.com/en-us/internet-explorer/ie11-ieak/iexpress-wizard-for-win-server

In addition to these wrappers, there are a number of **crypters** available, as well:

1. SwayzCryptor https://guidedhacking.com/threads/swayzcrypter.5778/
2. Cypherx https://cypherx-crypter.updatestar.com/en
3. Java Crypter https://www.secrethackersociety.com/product/java-crypter/
4. BetaCrypt https://www.secrethackersociety.com/product/betacrypt/

5. Spartan Crypter https://www.silentexploits.com/spartan-crypter/
6. BitCrypter https://www.crypter.com/

Remember that a Trojan horse can be used to deliver anything. So sometimes Trojan horses are categorized by what they deliver. The following are some of the many types of Trojan horses:

Backdoor

Spyware

The following tools fall into this category:

1. AntiVIrus Gold
2. MacSweeper
3. Spy Wiper
4. Spysheriff
5. Windows Police Pro

The antivirus company Kaspersky defines four types or categories of spyware:

Trojan spyware: This type of spyware enters devices via Trojan malware, which delivers the spyware program.

Adware: This type of spyware may monitor you to sell data to advertisers or serve deceptive malicious ads.

Tracking cookie files: This type of spyware can be implanted by a website to follow you across the internet.

System monitors: This type of spyware can track any activity on a computer, capturing sensitive data such as keystrokes, sites visited, email addresses, and more. Keyloggers typically fall into this group.

Ransomware

You can learn more about Ryuk at https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/.

Rootkits

A rootkit is malware that is used to gain administrative-level privileges.

There are actually several types of rootkits. The major types are listed here:

Bootloader rootkit: This type of rootkit replaces the original boot loader with one that is controlled by the attacker.

Kernel rootkit: This type of root kit either adds malicious code or replaces the original OS kernel or device drivers.

Library rootkit: This type of root replaces certain libraries with fake libraries controlled by the attacker.

Hypervisor rootkit: This type of rootkit functions as a hypervisor and modifies the boot sequence of the computer system to load the host operating system as a virtual machine.

Hardware/firmware rootkit: This type of rootkit is much less common than the others. It is a rootkit in hardware devices or platform firmware.

Application rootkit: This type of rootkit replaces normal application binaries with malicious code. Such a rootkit can also work by modifying the behavior of existing applications by injecting malicious code.

Fileless Malware

This type of malware does not require the installation of a file on the target system. Instead, it uses existing system programs—legitimate programs—to attack the target system.

PowerShell Command to stop a service

```
service Stop-Service -displayname "Antimalware Service Executable"
get-process antivirus.exe| StopProcess
```

It is also possible to use the Windows Management Interface (WMI) to perform similar tasks. WMI has a number of classes that can be used in scripts to gather information and perform tasks. A few of these classes are listed here:

Win32_ApplicationService: This WMI class represents any installed or advertised component or application available on the system.

Win32_Account: This abstract WMI class contains information about user accounts and group accounts known to the Windows system.

Win32_ComputerSystem: This WMI class represents a computer system operating in a Windows environment.

Win32_LogicalDisk: This WMI class represents a data source that resolves to an actual local storage device on a Windows system.

You can get more information on WMI from the following sources:

WMI Samples: https://www.activexperts.com/admin/scripts/wmi/

Example: Getting WMI Data from the Local Computer: https://docs.microsoft.com/en-us/windows/win32/wmisdk/example--getting-wmi-data-from-the-local-computer

The net command in Windows

It is a standard command line tool that has many variations and that can also be used for fileless malware. The following are some examples:

net use: This command connects/disconnects the computer from a shared resource or allows the user to view information about the current computer connections.

net view: This command displays the computers in the local domain.

net view \\ComputerName: This command shows the shares on the specified computer.

net file: This command displays all the open shared files on a server and the lock ID.

net session\\ComputerName: This command lists the sessions on the specified machine.

net session: This command lists all sessions on the current machine.

net share sharename: This command displays the local share name.

net start service

net stop service

Common services

1. browser
2. alerter
3. messenger
4. “routing and remote access”
5. schedule
6. spooler

PowerShell, WMI, and the net command were all designed for legitimate uses by Windows administrators. Fileless malware simply exploits these tools.

Bonet

A botnet is a network of computers. One computer is the command and control node, and the others are zombie machines that are not willing participants in the activity.

Advanced Persistent Threats

Exploit Kits

Exploit kits, sometimes called crimeware toolkits, are platforms for delivering exploits and payloads to a target.

1. Terror
2. Sundown

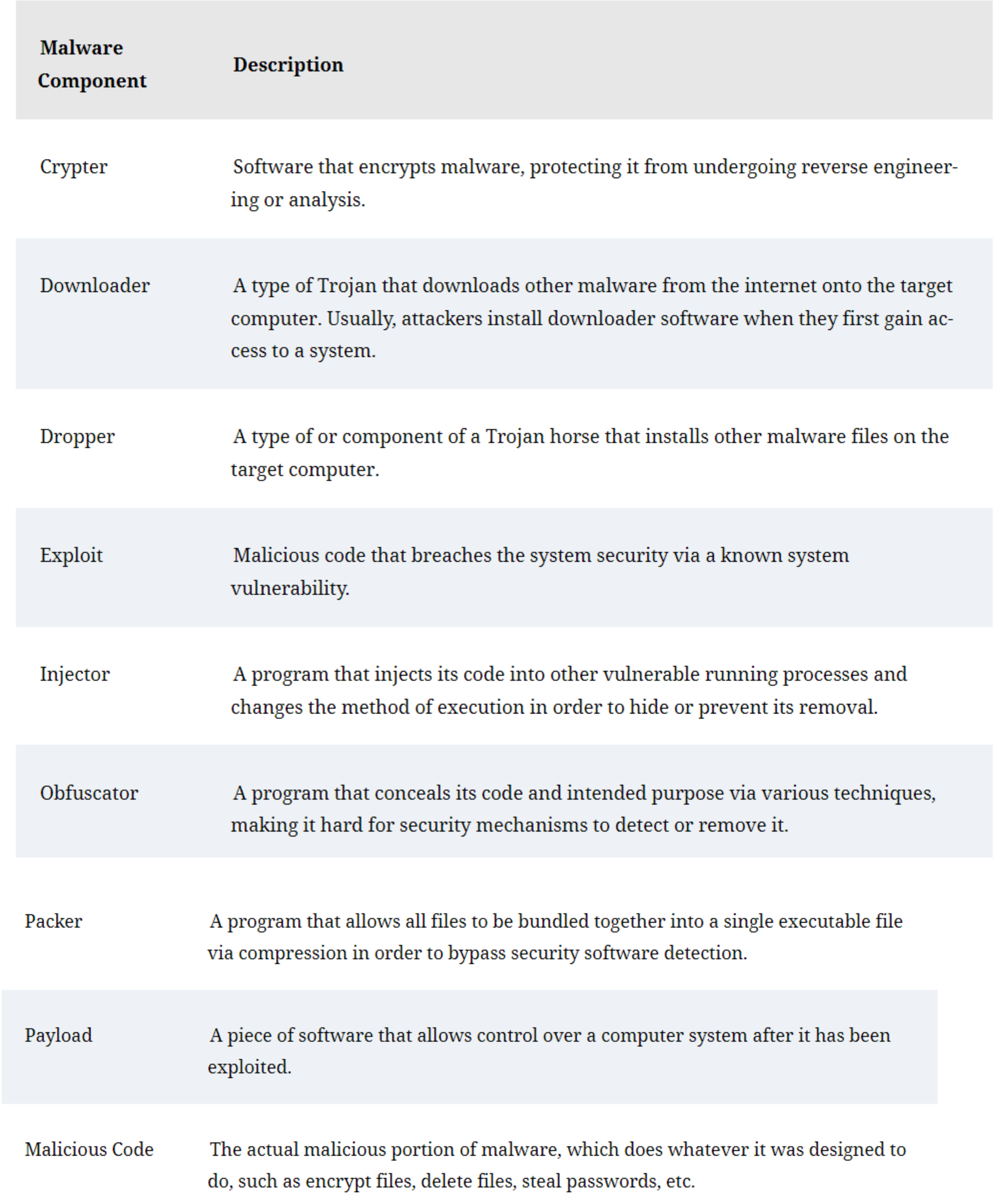
3. Neutrino
4. Angler
5. RIG Exploit Kit

How Malware Spreads

1. Email attachments
2. Instant messaging attachments
3. Websites that are infected
4. Portable media
5. Any download from the internet
6. File sharing services
7. Direct installation over wireless networking

Malware Components

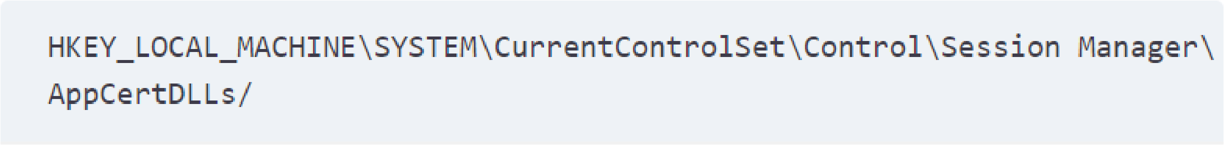
TABLE 4.2 Some Components of Malware



Malware Component	Description
Crypter	Software that encrypts malware, protecting it from undergoing reverse engineering or analysis.
Downloader	A type of Trojan that downloads other malware from the internet onto the target computer. Usually, attackers install downloader software when they first gain access to a system.
Dropper	A type of or component of a Trojan horse that installs other malware files on the target computer.
Exploit	Malicious code that breaches the system security via a known system vulnerability.
Injector	A program that injects its code into other vulnerable running processes and changes the method of execution in order to hide or prevent its removal.
Obfuscator	A program that conceals its code and intended purpose via various techniques, making it hard for security mechanisms to detect or remove it.
Packer	A program that allows all files to be bundled together into a single executable file via compression in order to bypass security software detection.
Payload	A piece of software that allows control over a computer system after it has been exploited.
Malicious Code	The actual malicious portion of malware, which does whatever it was designed to do, such as encrypt files, delete files, steal passwords, etc.

Malware evasion techniques

DLL injection involves causing code to execute within the address space of some other process. This is accomplished by forcing the targeted program to load a DLL (dynamic linked library). Multiple techniques can be used to accomplish this.



```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\
AppCertDLLs/
```

https://learning.oreilly.com/library/view/certified-ethical-hacker/9780137513697/ch04_images.xhtml#p106pro02a

Process hollowing is another technical method for hiding malware. In this technique, malware masquerades as a genuine system process that poses no threat of crashing the process.

Viruses

Types of Viruses

There are many different types of viruses. In this section we briefly look at some of the major virus types.

Viruses can be classified by either the method they use for propagation or their activities on the target computers:

File virus: A file virus is executed like any other executable on a system. It is a common type of virus.

System virus: A system virus attempts to compromise some portion of a system. For example, a boot sector virus attempts to infect the boot process of the target system.

Macro virus: A macro virus infects the macros in Microsoft Office documents. Microsoft Office products such as Word and Excel allow users to write mini programs called macros to automate tasks. A macro virus can be written into a macro in some business applications. For example, Microsoft Outlook is designed to allow a programmer to write scripts using a subset of the Visual Basic programming language called **Visual Basic for Applications** (VBA). This scripting language is, in fact, built into all Microsoft Office products.

Programmers can also use the closely related VBScript language. Both languages are quite easy to learn. If a macro virus script is attached to an email and the recipient is using Outlook, then the script can execute and do any number of things, including scan the address book, look for addresses, send out email, or delete email.

Multipartite virus: A multipartite virus can attack a computer in multiple ways, such as by infecting the boot sector of the hard disk and one or more files.

Cluster virus: A cluster virus modifies some directory table so that it points users to the virus rather than to the actual program. For example, it might alter the file that maintains information for the file system (MFT in Windows).

Memory-resident virus: A memory-resident virus installs itself and then remains in RAM from the time the computer is booted up to when it is shut down.

Armored virus: An armored virus uses techniques that make it hard to analyze. Code confusion is one such method. The code is written such that if the virus is disassembled, the code won't be easily followed. Compressed code is another method for armoring a virus.

Sparse infector virus: A sparse infector virus attempts to elude detection by performing its malicious activities only sporadically. With a sparse infector virus, the user sees symptoms for a short period and then sees no symptoms for a time. In some cases, a sparse infector virus targets a specific program but executes only every 10th time or 20th time that the target program executes. Or a sparse infector virus may have a burst of activity and then lie dormant for a period of time. There are a number of variations on the theme, but the basic principle is the same: This type of virus reduces the frequency of attack and thus reduces the chances for detection.

Polymorphic virus: A polymorphic virus literally changes its form from time to time to avoid detection by antivirus software.

Metamorphic virus: This is a special case of a polymorphic virus that completely rewrites itself periodically. This type of virus is very rare.

Boot sector virus: Some sources list boot sector viruses separately from system and file viruses. As the name suggests, this type of virus infects the boot sector of the drive. It can be difficult to find antivirus software for this type of virus, because most antivirus software runs within the operating system, not in the boot sector.

Overwriting/cavity virus: This type of virus embeds itself in a host file and overwrites part of the host file so that it does not increase the length of the file.

File extension virus: This type of virus changes the extension of a file. So, for example, such a virus might make a .vbs (Visual Basic script) file appear to be a .txt (text) file.

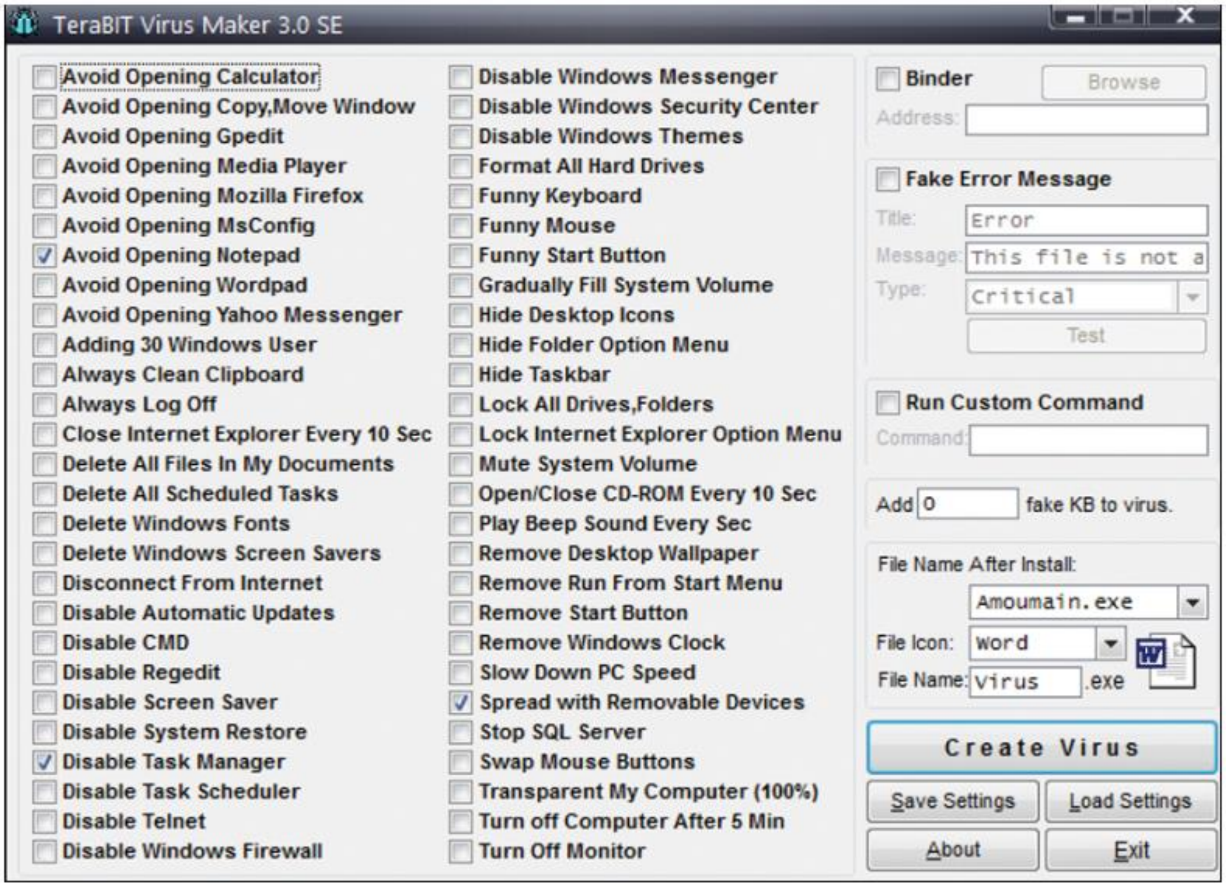
Terminate and stay resident (TSR) virus: This type of virus remains permanently in the memory during an entire work session, even after the target host's program is executed and terminated. In some cases, it can be removed by rebooting the system; in other cases, even a reboot will not remove the virus.

Companion virus: This type of virus creates a companion file for each executable file, so it might be associated with a legitimate program.

Creating a Virus

One well-known tool is TeraBIT Virus Maker.

FIGURE 4.3 TeraBIT Virus Maker



□ Avoid Opening Calculator
□ Avoid Opening Copy,Move Window
□ Avoid Opening Gpedit
□ Avoid Opening Media Player
□ Avoid Opening Mozilla Firefox
□ Avoid Opening MsConfig
☑ Avoid Opening Notepad
□ Avoid Opening Wordpad
□ Avoid Opening Yahoo Messenger
□ Adding 30 Windows User
□ Always Clean Clipboard
□ Always Log Off
□ Close Internet Explorer Every 10 Sec
□ Delete All Files In My Documents
□ Delete All Scheduled Tasks
□ Delete Windows Fonts
□ Delete Windows Screen Savers
□ Disconnect From Internet
□ Disable Automatic Updates
□ Disable CMD
□ Disable Regedit
□ Disable Screen Saver
□ Disable System Restore
☑ Disable Task Manager
□ Disable Task Scheduler
□ Disable Telnet
□ Disable Windows Firewall

□ Disable Windows Messenger
□ Disable Windows Security Center
□ Disable Windows Themes
□ Format All Hard Drives
□ Funny Keyboard
□ Funny Mouse
□ Funny Start Button
□ Gradually Fill System Volume
□ Hide Desktop Icons
□ Hide Folder Option Menu
□ Hide Taskbar
□ Lock All Drives,Folders
□ Lock Internet Explorer Option Menu
□ Mute System Volume
□ Open/Close CD-ROM Every 10 Sec
□ Play Beep Sound Every Sec
□ Remove Desktop Wallpaper
□ Remove Run From Start Menu
□ Remove Start Button
□ Remove Windows Clock
□ Slow Down PC Speed
☑ Spread with Removable Devices
□ Stop SQL Server
□ Swap Mouse Buttons
□ Transparent My Computer (100%)
□ Turn off Computer After 5 Min
□ Turn Off Monitor

□ Binder
Address:

□ Fake Error Message
Title: Error
Message: This file is not a
Type: Critical

□ Run Custom Command
Command:

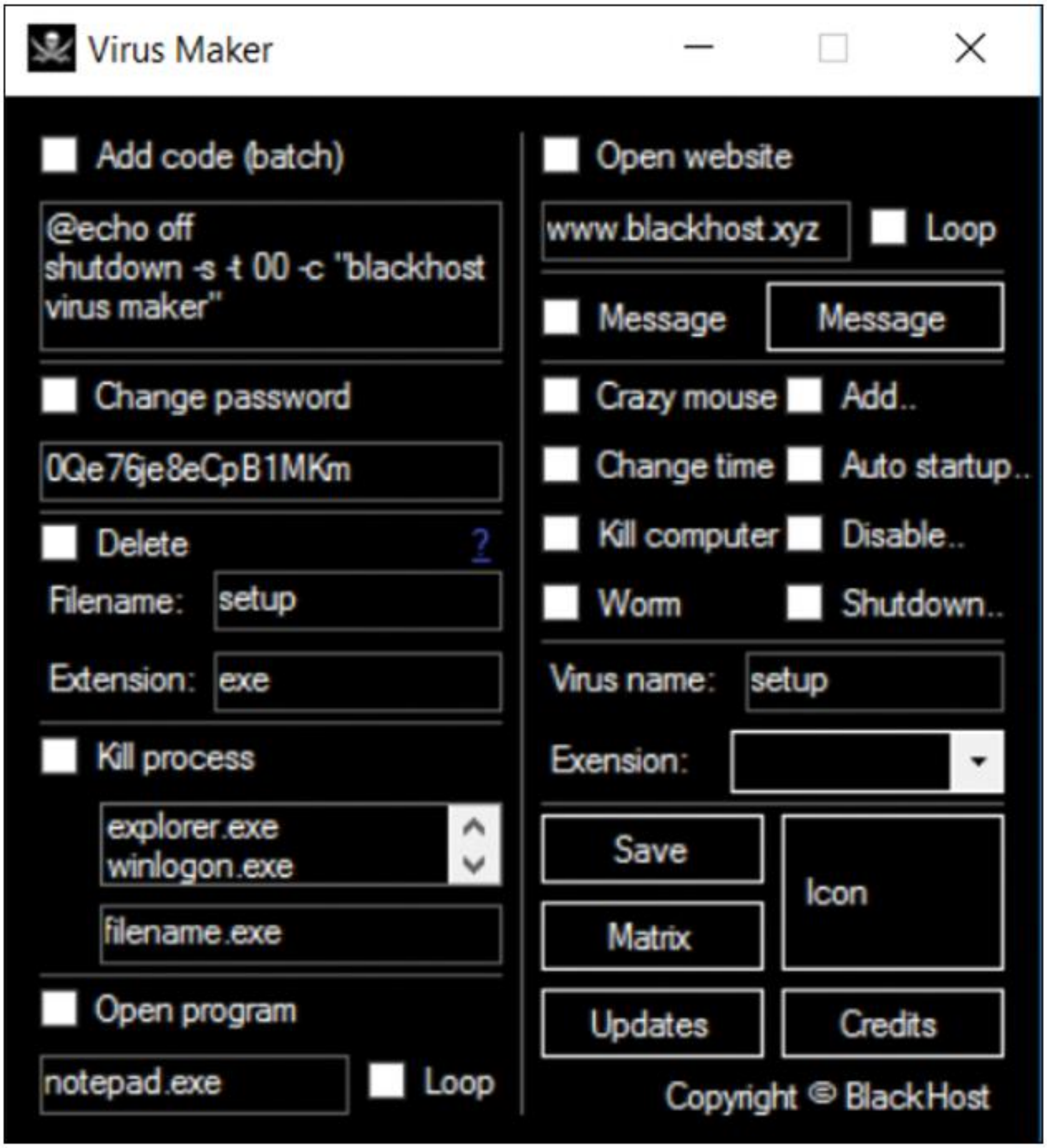
Add 0 fake KB to virus.

File Name After Install: Amoumain.exe
File Icon: Word
File Name: virus .exe

Some of the actions you can select are merely annoying, such as avoiding opening Notepad. Others are quite malicious, such as formatting all hard drives. Notice that there is also an option to spread a virus with removable devices.

Another interesting GUI virus maker is **Virus Maker** from BlackHost (http://www.blackhost.xyz).

FIGURE 4.4 BlackHost Virus Maker



Virus Maker

☐ Add code (batch)

```
@echo off
shutdown -s -t 00 -c "blackhost
virus maker"
```

☐ Change password

0Qe76je8eCpB1MKm

☐ Delete ?

Filename: setup

Extension: exe

☐ Kill process

explorer.exe
winlogon.exe

filename.exe

☐ Open program

notepad.exe ☐ Loop

☐ Open website

www.blackhost.xyz ☐ Loop

☐ Message

☐ Crazy mouse ☐ Add..

☐ Change time ☐ Auto startup..

☐ Kill computer ☐ Disable..

☐ Worm ☐ Shutdown..

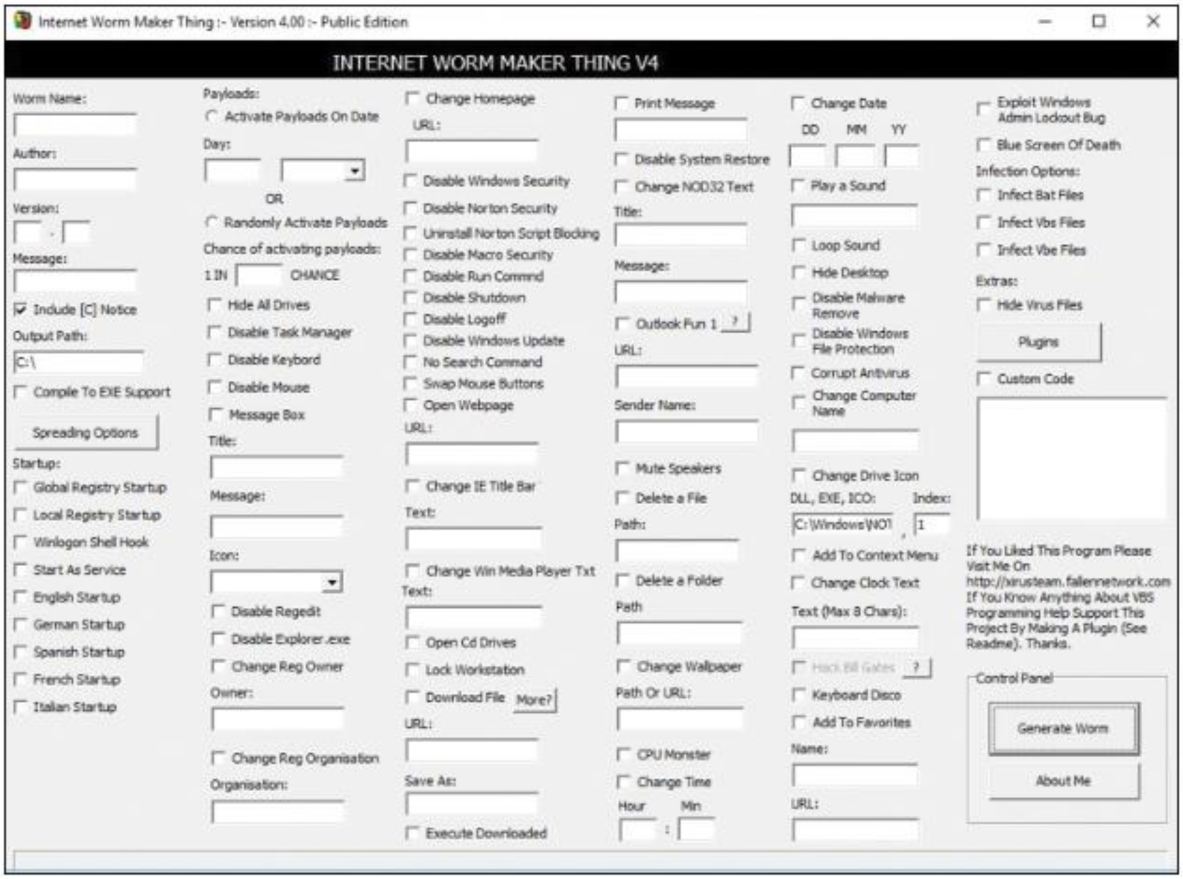
Virus name: setup

Exension:

FIGURE 4.4 **BlackHost Virus Maker**

One of the most well-known worm makers is the Internet **Worm Maker Thing**.

FIGURE 4.5 Internet Worm Maker Thing



☑ Include [C] Notice

Output Path: C:\

DLL, EXE, ICO: C:\Windows\WOT Index: 1

If You Liked This Program Please Visit Me On http://virusteam.fallennetwork.com If You Know Anything About VBS Programming Help Support This Project By Making A Plugin (See Readme). Thanks.

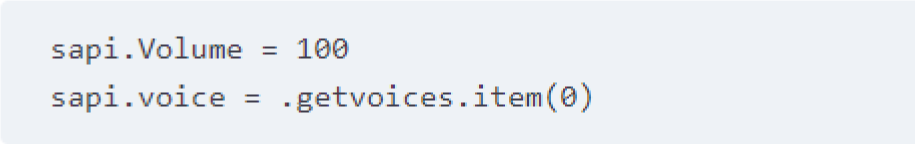
FIGURE 4.5 Internet Worm Maker Thing

In addition to using tools to write viruses, you can write them by using scripts or batch files.

For example, here is a simple **VBScript virus**:

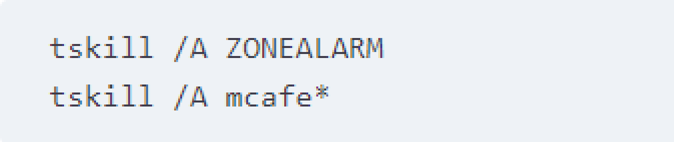
```
Dim msg, sapi
msg="You have violated security policies"
Set sapi=CreateObject("sapi.spvoice")
sapi.Speak msg
```

This is a VBScript script, so you should save it as a .vbs file. This script allows you to test whether users will click on an attachment, particularly one that is a script.



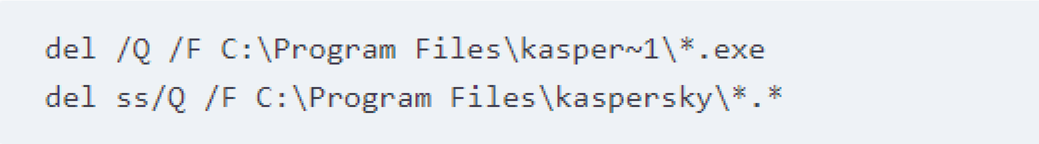
```
sapi.Volume = 100
sapi.voice = .getvoices.item(0)
```

The following batch file, if executed by someone with administrative privileges, will kill antivirus processes:



```
tskill /A ZONEALARM
tskill /A mcafe*
```

This can be followed with del to delete the files for that antivirus:



```
del /Q /F C:\Program Files\kasper~1\*.exe
del ss/Q /F C:\Program Files\kaspersky\*.*
```

/Q specifies quiet mode, which means the user does not get a prompt before the file is deleted.

/F indicates to ignore read-only setting and delete the file anyway.

More recent versions of Windows don’t support **tskill** but do support the related command **taskkill**.

Taskkill is actually more powerful than tskill.

Logic Bombs

In 2019, a contract employee for Siemens, David Tinley, pleaded guilty to charges of creating a logic bomb. The purpose of his logic bomb was to, after a period of time, cause the software he had developed for the company to malfunction. He planned for the logic bomb to cause Siemens to have to call him back to fix it so he could make more money.

Protecting Against Malware

Indicators of Malware

- Processes take more resources and time.
- Files and folders are missing.
- The system suddenly runs out of storage space.

- The computer freezes frequently.

- The computer crashes frequently (on Windows giving a BSOD [blue screen of death]).
- Unexplained popup windows appear.
- Files or folders are in places where they should not be.

Sheep Dipping

When sheep ranchers purchase a new sheep, they first dip the sheep in a liquid designed to kill any parasites before introducing the sheep to the rest of the flock.

In technology, a similar process can be accomplished with software. You can set up an isolated machine, or even a virtual machine, and install suspect software on it.

Then you can run a range of process monitors to find out precisely what this software does before it is authorized for use on the network.

This process, like the process sheep ranchers use, is called **sheep dipping**.

Sandboxing refers to putting something into an isolated environment in order to test it. Virtual machines are often used for this purpose. You can use a physical machine, but virtual machines are used more often for this purpose.

Backup

Before backing up, you need to do a complete virus scan on the system you are backing up. Then, once the backup is complete, disconnect from the network.

That way, a virus cannot move to your backup media. This is referred to as **air gapping**, as in there is nothing but air between your backup and the network—no wired or wireless connections, no Bluetooth, no connection of any kind.

Malware Analysis

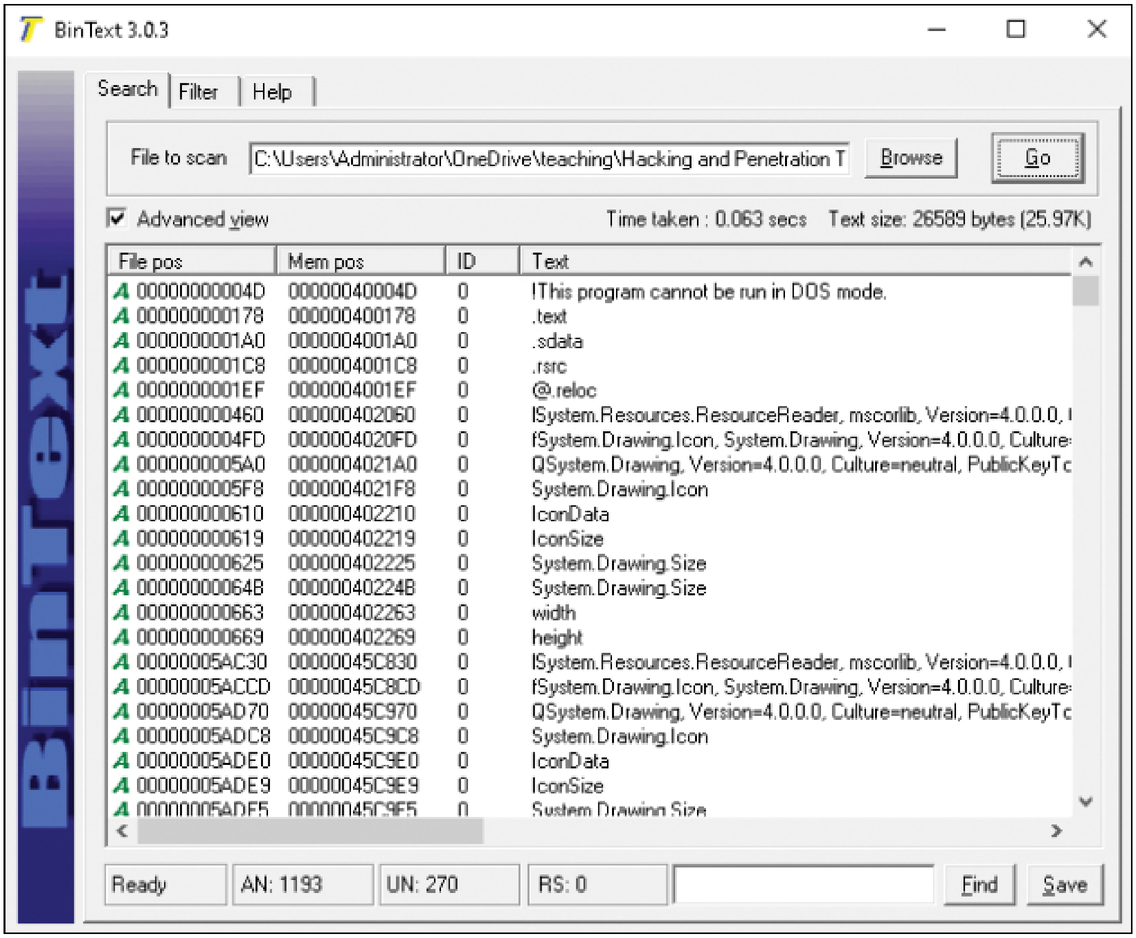
There are primarily two types of analysis:

Static analysis: This analysis involves going through the executable binary code without actually executing it to get a better understanding of the malware and its purpose.

Dynamic analysis: This analysis involves actually executing the malware code so you can learn how it interacts with the host system and its impact on the system after it has been infected. Obviously, this should be done on an isolated machine.

BinText is a text extractor available from https://www.aldeid.com/wiki/BinText that can extract text from any kind of file. It allows you to find plain ASCII text, Unicode text, and resource strings, all of which provide useful information.

Figure 4.6: BinText 3.0.3



File to scan: C:\Users\Administrator\OneDrive\teaching\Hacking and Penetration T

☑ Advanced view

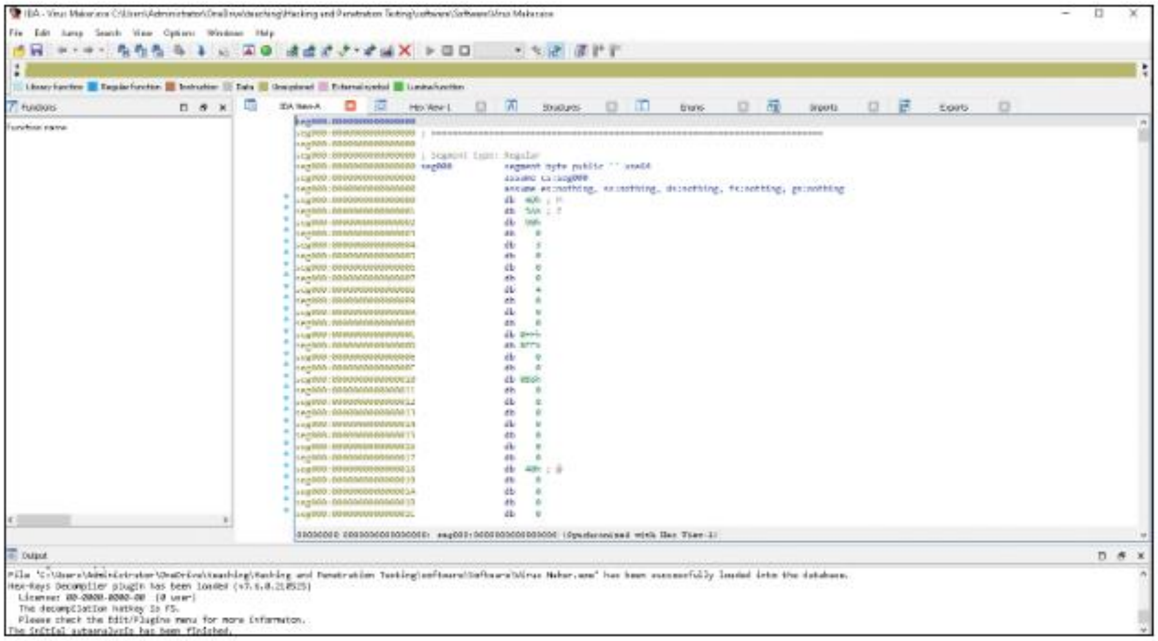
Time taken : 0.063 secs Text size: 26589 bytes (25.97K)

File pos	Mem pos	ID	Text
A 00000000004D	00000040004D	0	!This program cannot be run in DOS mode.
A 000000000178	000000400178	0	.text
A 0000000001A0	0000004001A0	0	.sdata
A 0000000001C8	0000004001C8	0	.rsrc
A 0000000001EF	0000004001EF	0	@.reloc
A 000000000460	000000402060	0	lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0,
A 0000000004FD	0000004020FD	0	fSystem.Drawing.Icon, System.Drawing, Version=4.0.0.0, Culture
A 0000000005A0	0000004021A0	0	QSystem.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyTc
A 0000000005F8	0000004021F8	0	System.Drawing.Icon
A 000000000610	000000402210	0	IconData
A 000000000619	000000402219	0	IconSize
A 000000000625	000000402225	0	System.Drawing.Size
A 00000000064B	00000040224B	0	System.Drawing.Size
A 000000000663	000000402263	0	width
A 000000000669	000000402269	0	height
A 00000005AC30	00000045C830	0	lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0,
A 00000005ACCD	00000045C8CD	0	fSystem.Drawing.Icon, System.Drawing, Version=4.0.0.0, Culture
A 00000005AD70	00000045C970	0	QSystem.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyTc
A 00000005ADC8	00000045C9C8	0	System.Drawing.Icon
A 00000005ADE0	00000045C9E0	0	IconData
A 00000005ADE9	00000045C9E9	0	IconSize
A 00000005ADF5	00000045C9F5	0	System.Drawing.Size

Ready AN: 1193 UN: 270 RS: 0

FIGURE 4.6 **BinText**

IDA is another popular tool for malware reverse engineering. This tool, available at https://hex-rays.com/ida-pro/, comes in a free version and a pro version. It allows you to decompile a file and see the source code, Shown in Figure 4.7.



```
File 'C:\Users\Administrator\OneDrive\teaching\Hacking and Penetration Testing\software\Software\Virus Maker.exe' has been successfully loaded into the database.
Hex-Rays Decompiler plugin has been loaded (v7.6.0.210525)
  License: [illegible] (0 user)
  The decompilation hotkey is F5.
  Please check the Edit/Plugins menu for more information.
The initial autoanalysis has been finished.
```

FIGURE 4.7 **IDA Decompiler**

There are tools for both static and dynamic analysis.

Static analysis tools include:

- **Portable Executable Scanner (pescan):** https://tzworks.com/prototype_page.php?proto_id=15
- **Resource Hacker:** http://www.angusj.com/resourcehacker/
- **PEView:** https://www.aldeid.com
- **UPX:** https://upx.github.io
- **Exeinfo PE:** http://exeinfo.atwebpages.com
- **ASPack:** http://www.aspack.com
- **Dependency-check:** https://jeremylong.github.io
- **Snyk:** https://snyk.io
- **Hakiri:** https://hakiri.io
- **RetireJS:** https://retirejs.github.io
- **WinDbg:** http://www.windbg.org
- **odjdump:** https://sourceware.org
- **ProcDump:** https://docs.microsoft.com

Dynamic analysis tools include:

CurrPorts: http://www.nirsoft.net

PortExpert: http://www.kcsoftwares.com

PRTG's Port sensor: https://kb.paessler.com

Nagios Port Monitor: https://exchange.nagios.org

Process Explorer: https://docs.microsoft.com

Registry Viewer: http://accessdata.com

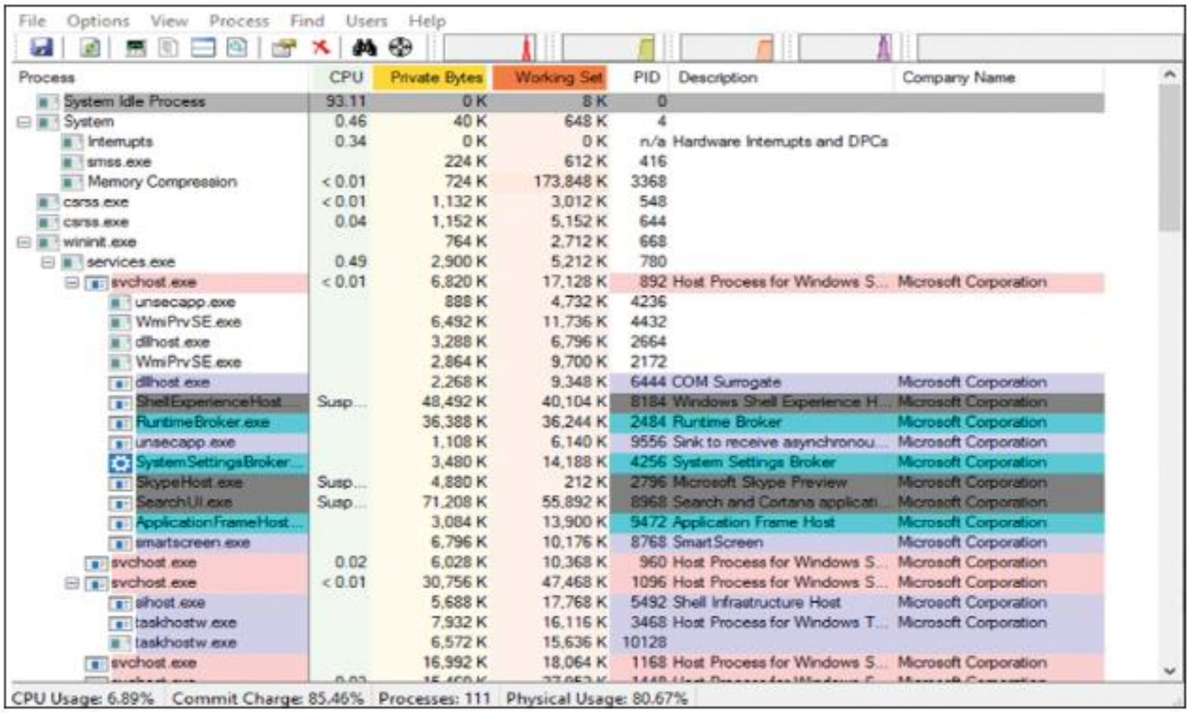
RegScanner: http://www.nirsoft.net

Process Hacker: http://processhacker.sourceforge.net

For Windows malware, the Sysinternals tool suite is very popular in dynamic analysis.

There are several tools in this suite that allow you to view processes, handles, memory allocation, and more. You can see the

Sysinternals Process Explorer in Figure 4.8.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	93.11	0 K	8 K	0		
System	0.46	40 K	648 K	4		
Interrupts	0.34	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		224 K	612 K	416		
Memory Compression	< 0.01	724 K	173,848 K	3368		
csrss.exe	< 0.01	1,132 K	3,012 K	548		
csrss.exe	0.04	1,152 K	5,152 K	644		
wininit.exe		764 K	2,712 K	668		
services.exe	0.49	2,900 K	5,212 K	780		
svchost.exe	< 0.01	6,820 K	17,128 K	892	Host Process for Windows S...	Microsoft Corporation
unsecapp.exe		888 K	4,732 K	4236		
WmiPrvSE.exe		6,492 K	11,736 K	4432		
dllhost.exe		3,288 K	6,796 K	2664		
WmiPrvSE.exe		2,864 K	9,700 K	2172		
dllhost.exe		2,268 K	9,348 K	6444	COM Surrogate	Microsoft Corporation
ShellExperienceHost...	Susp...	48,492 K	40,104 K	8184	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		36,388 K	36,244 K	2484	Runtime Broker	Microsoft Corporation
unsecapp.exe		1,108 K	6,140 K	9556	Sink to receive asynchronou...	Microsoft Corporation
SystemSettingsBroker...		3,480 K	14,188 K	4256	System Settings Broker	Microsoft Corporation
SkypeHost.exe	Susp...	4,880 K	212 K	2796	Microsoft Skype Preview	Microsoft Corporation
SearchUI.exe	Susp...	71,208 K	55,892 K	8968	Search and Cortana applicati...	Microsoft Corporation
ApplicationFrameHost...		3,084 K	13,900 K	9472	Application Frame Host	Microsoft Corporation
smartscreen.exe		6,796 K	10,176 K	8768	SmartScreen	Microsoft Corporation
svchost.exe	0.02	6,028 K	10,368 K	960	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	30,756 K	47,468 K	1096	Host Process for Windows S...	Microsoft Corporation
sihost.exe		5,688 K	17,768 K	5492	Shell Infrastructure Host	Microsoft Corporation
taskhostw.exe		7,932 K	16,116 K	3468	Host Process for Windows T...	Microsoft Corporation
taskhostw.exe		6,572 K	15,636 K	10128		
svchost.exe		16,992 K	18,064 K	1168	Host Process for Windows S...	Microsoft Corporation

CPU Usage: 6.89% Commit Charge: 85.46% Processes: 111 Physical Usage: 80.67%

FIGURE 4.8 **Sysinternals Process Explorer**

You can get the Sysinternals tools for free and learn more about them at https://docs.microsoft.com/en-us/sysinternals/.

Antivirus

Email and attachment scanning: Since a very common transmission method for a virus is email, email and attachment scanning is the most important function of any virus scanner. Some virus scanners actually examine your email on the email server before downloading it to your machine. Other virus scanners work by scanning your emails and attachments on your computer before passing them to your email program. And some even do both. The important point is that the email and its attachments should be scanned prior to the user having any chance to open them and release the virus on the system.

Download scanning: Any time a user downloads any file from the internet, there is a chance of downloading an infected file. Download scanning works much like email and attachment scanning but operates on files you select for downloading. When you click on a link on a web page, the target file is scanned before it is downloaded.

File scanning: This is the type of scanning in which files on the system are checked to see whether they match any known virus. File scanning can be done on a scheduled basis, on demand, or both. It is a good idea to schedule your virus scanner to do a complete scan of the system periodically.

Heuristic scanning: This type of scanning uses rules to determine whether a file or program is behaving like a virus. It looks at behavior, rather than at a list of known viruses. A new virus will not be on a virus definition list, so antivirus software must examine behavior to determine whether something is a virus. However, this process is not foolproof. Some actual virus infections will be missed, and some nonvirus files might be suspected of being viruses.

Sandbox: Another approach is the sandbox approach. This basically means that you have a separate area, isolated from the operating system, in which a download or attachment is run. Then, if it is infected, it won't infect the operating system.

It should be noted that many antimalware systems advertise that they incorporate some level of machine learning in their malware detection. However, at this point, the most the CEH exam might ask you is whether there is such a thing as machine learning antimalware. You won't need to know details. If you wish to learn more, see the following resources:

Machine Learning for Malware Detection: https://media.kaspersky.com/en/enterprise-security/Kaspersky-Lab-Whitepaper-Machine-Learning.pdf

Machine Learning & Artificial Intelligence: https://www.mcafee.com/enterprise/en-us/solutions/machine-learning.html

References

https://learning.oreilly.com/library/view/certified-ethical-hacker/9780137513697/bk01-toc.xhtml

https://learning.oreilly.com/library/view/certified-ethical-hacker/9780137513697/ch04_images.xhtml#p106pro02a

Glossary

https://learning.oreilly.com/library/view/certified-ethical-hacker/9780137513697/gloss01.xhtml