

Malware Forensics

Module 11






Computer Hacking Forensic Investigator v9

Module 11: Malware Forensics

Exam 312-49

Module Objectives

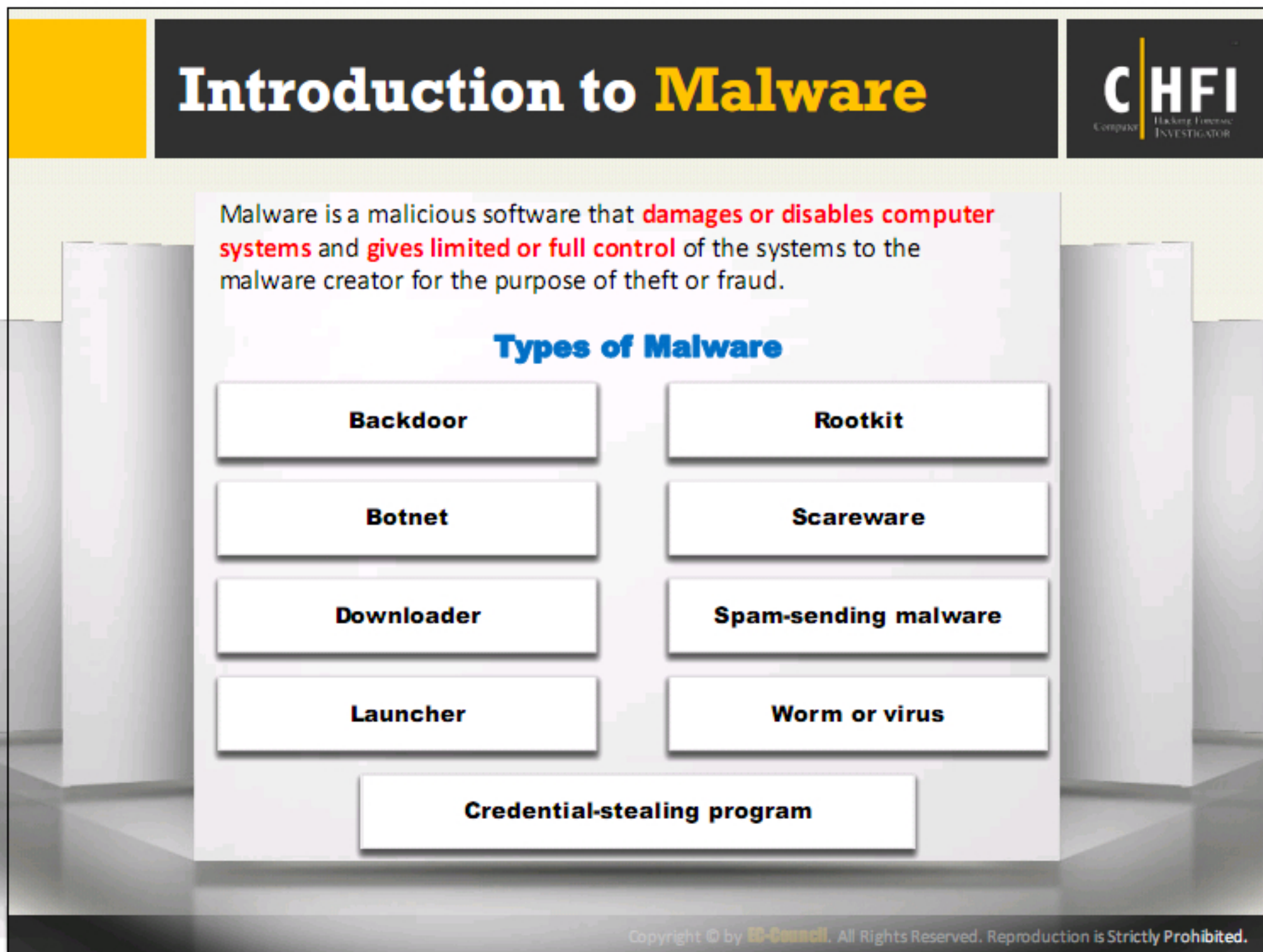


→ After successfully completing this module, you will be able to:

- 1 Define a malware and list the different ways a malware can get into a system
- 2 Discuss techniques attackers use to spread malware, and list the basic malware components
- 3 Apply malware forensics concepts, identify and extract malware from live and dead systems
- 4 Understand the prominence of setting up a controlled malware analysis lab
- 5 Prepare Testbed for malware analysis
- 6 Identify the general rules to perform malware analysis
- 7 Perform Static and Dynamic malware analysis and analyze malicious documents
- 8 Understand the challenges faced while performing malware analysis

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Currently, malicious software, commonly called malware, is the most efficient tool used in compromising security of the computer or any other electronic device connected to the internet. This has become a menace owing to the rapid progress in technologies such as easy encryption and data hiding techniques. Malware is the major source of various cyber-attacks and internet security threats, which is why computer forensic analysts need to have expertise in dealing with it. This module will elaborately discuss the different types of malware, their propagation methods, ways to detect them, etc.

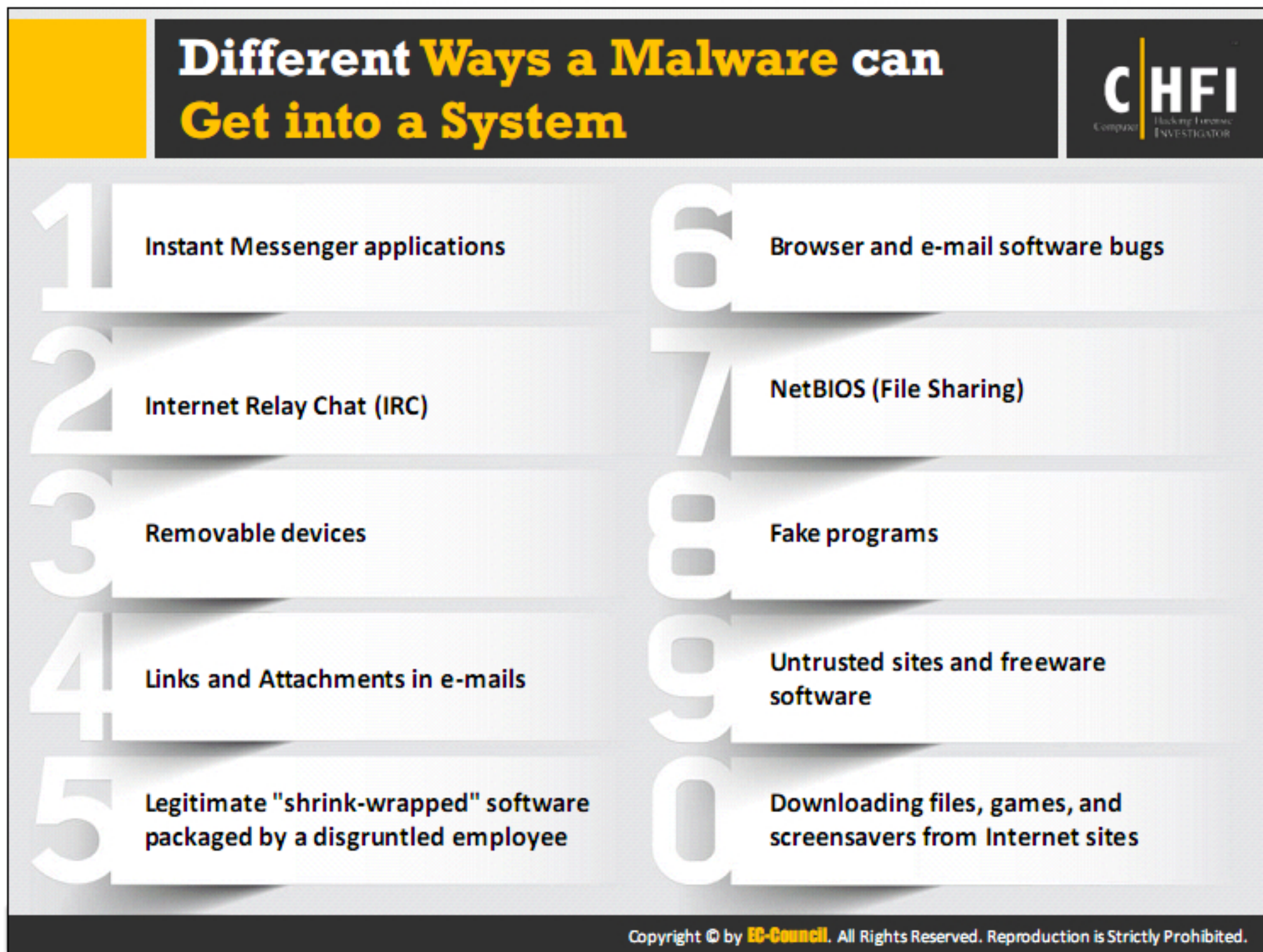


Malware, short for malicious software, is a program that is capable of altering the properties of a device or target application to provide limited or full control of the device to its creator. The malware is useful when an unauthorized person wants to access a locked or secure device illegally.

Malware programs include viruses, worms, Trojans, rootkits, adware, spyware, etc., that can delete files, slow down computers, steal personal information, send spam, and commit fraud. Malware can perform various malicious activities that range from simple email advertising to complex identity theft as well as password stealing. Malware programmers develop and use it to:

- Attack browsers and track websites visited.
- Alter system performance, making it very slow.
- Cause hardware failure, rendering computers inoperable.
- Steal personal information, including contacts.
- Erase important information, resulting in potentially huge data losses.
- Attack additional computer systems directly from a compromised system.
- Spam inboxes with advertising emails.

The attackers are using them for breaking down the cyber security. Therefore, it is crucial for the forensic analysts to have sound knowledge of different malware programs; their working, propagation, site of impact, output, as well as methods of detection and analysis.



Investigators need to know how malware can spread from one system to another, and should also be able to detect the mechanism used for getting into and corrupting a system. The most common ways an attacker can send a malware into a system are as follows:

Instant Messenger Applications

Instant messenger (IM) applications such as ICQ or Yahoo Messenger have the provision for transferring text messages and files. The malware can disperse into a system through files received during transfer using IM. The received files can contain highly malicious files or programs as the IM applications do not have proper scanning mechanism for the transferred files. The users can never be sure about the persons they are exchanging information with, as the IMs are vulnerable to identity theft attacks. For example, an attacker could have hacked someone's messenger ID and password, and used it to spread Trojans to the people in victim's friend list.

Internet Relay Chat

Internet Relay Chat (IRC) is a chatting service that allows multiple users to connect with each other and exchange data and files over the internet. Designed for group communication in discussion forums, the IRC allows communications through private messages, chats, and file sharing.

Malware such as Trojans uses IRC as means of propagation. The intruders rename Trojan files as something else to fool the victim and send it over IRC. When the IRC user downloads and clicks on the file, the Trojan executes and installs malicious program over the system.

Removable Devices

Malware can propagate through corrupted removable media such as pen drives, CD-ROM, etc. When a user connects corrupted media devices to a computer system, the malware automatically spreads to the system as well.

CDs, DVDs and USB storage devices, such as flash drives or external hard drives, come with Autorun support, which triggers certain predetermined actions in a system on connecting these devices. Attackers exploit this feature to run malware along with genuine programs by placing an Autorun.inf file with the malware in a CD/DVD or USB and trick people to insert or plug it into their systems.

E-mail and Attachments

Invaders adopt mass mailing technique to send out a large number of e-mail messages, with attached malware as file or embedded in the mail itself. When the user opens the e-mail, the embedded malware automatically installs onto the system and starts spreading. Whereas, the malware sent as attachment requires the user to download and open the attached file for the malware to become active and corrupt the system. Some email clients, such as Outlook Express, have bugs that automatically execute attached files.

The invaders also place links for malicious websites in the emails along with enticing messages that lure the victim into clicking the link. Most of the web clients detect such messages and sort them into harmful category. If the user clicks on such links, the browser will navigate to a harmful website, which is capable of downloading the malware on to the system without the user's consent.

Browser and Software Bugs

Users do not update the software and applications installed on their system. These elements of a system come with various vulnerabilities, which attackers capitalize to corrupt the system using a malware.

An outdated Web browser may support cannot be able to identify if a malicious user is visiting a malicious site and cannot stop the site from copying or installing programs onto the user's computer. Sometimes, a visit to a malicious site can automatically infect the machine without downloading or executing any program.

File Downloads

Attackers masquerade malicious files and applications with icons and names of costly or famous applications. They place these applications on websites and make them freely downloadable to attract victims. Further they create the websites in such a way that the free program claims to have features such as an address book, access to check several POP3 accounts, and other functions to attract many users.

If a user downloads, labels it as TRUSTED and executes such programs, the protection software may not scan the new software for malice or harmful content. Such malware can prompt e-mail, POP3 account passwords, cached passwords, and keystrokes to the attackers through email secretly.

Sometimes, disgruntled employees of a company create a seemingly legitimate shrink-wrapped software packages with malware and place them on the internal network of the company. When other employees access these files and try to download and execute them, the malware will compromise the system and may also cause intellectual and financial losses.

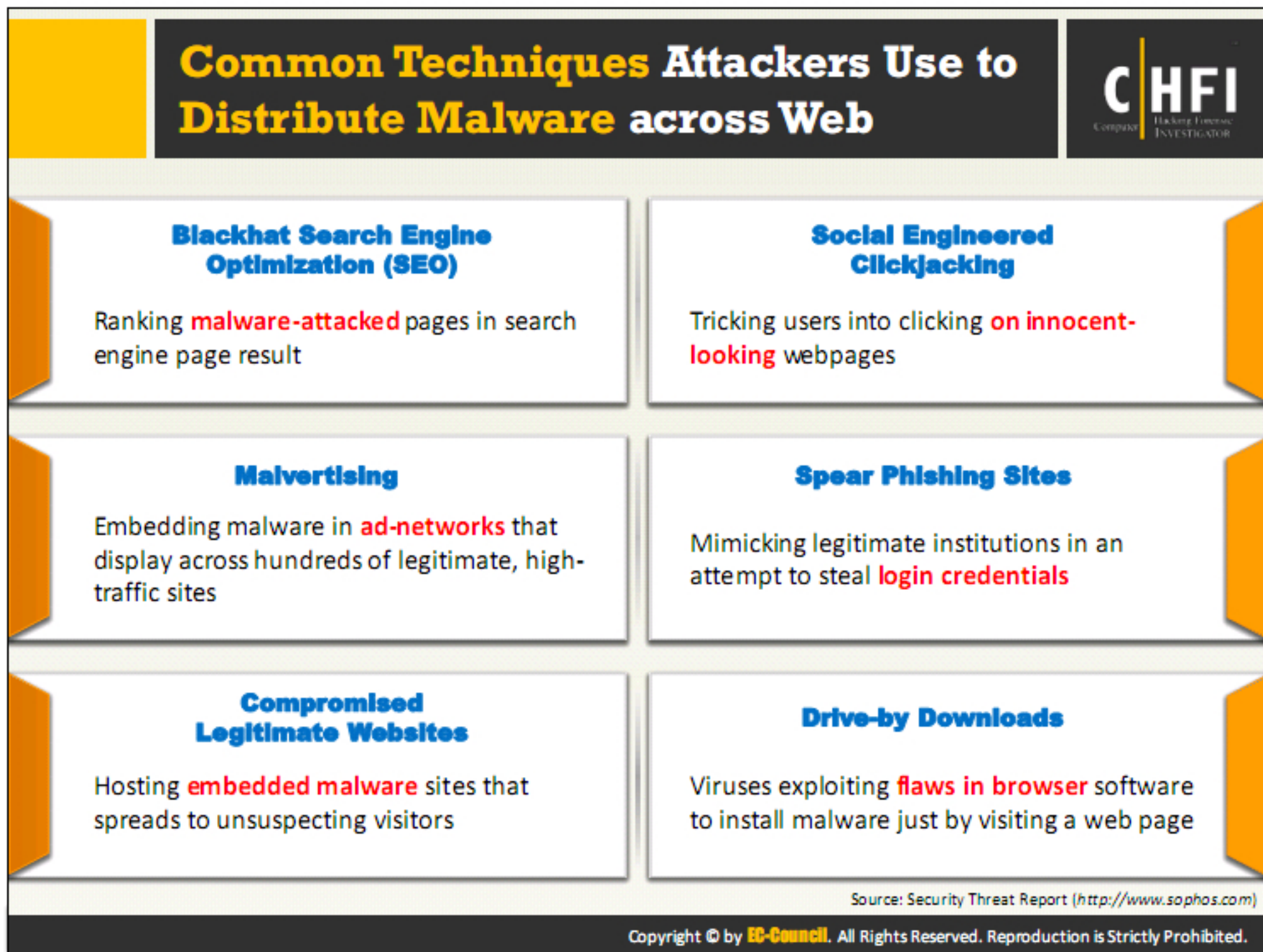
Beside fake software, the intruder can also construct other fake files such as music players, files, movies, games, greeting cards, screensavers, etc.

Network File Sharing (Using NetBIOS)

If the users share a common network with open ports, then the malware can propagate from corrupted system to other through shared files and folders.

Bluetooth and wireless networks

Attackers use open Bluetooth and Wi-Fi networks to attract users to connect to it. These open networks have software and hardware devices installed at the router level that could capture the network traffic, data packets and also find the account details including username and password.



Some of the common techniques used to distribute malware on the web:

- **Blackhat Search Engine Optimization (SEO):**
Blackhat SEO (also referred to as unethical SEO) uses aggressive SEO tactics such as keyword stuffing, doorway pages, page swapping, and adding unrelated keywords in an effort to get higher search engine ranking for their malware pages.
- **Social Engineered Click-jacking:**
Attackers inject malware into legitimate-looking websites to trick users into clicking them. When clicked, the malware embedded in the link executes without the knowledge or consent of the user.
- **Spearphishing Sites:**
The technique helps attacker in mimicking legitimate institutions, such as banks, in an attempt to steal passwords, credit card and bank account data, and other sensitive information.
- **Malvertising:**
Involves embedding malware-laden advertisements in authentic online advertising channels to spread malware onto the systems of unsuspecting users.

- **Compromised Legitimate Websites:**

Often, attackers use compromised websites to infect systems with malware. When an unsuspecting user visits the compromised website, the malware secretly installs itself on the user's system and thereafter carries out malicious activities.

- **Drive-by Downloads:**

The unintentional downloading of software via the Internet. Here, an attacker exploits flaws in browser software to install malware just merely by visiting a web site.

Source: *Security Threat Report* (<http://www.sophos.com>)

Components of Malware



Components of a malware software relies on the requirements of the **malware author** who designs it for a specific target to perform the intended tasks

Basic components of a malware:

Malware Component	Description
Crypter	Software that protects malware from undergoing reverse engineering or analysis, thus hardening the task of security mechanism its detection
Downloader	A type of Trojan that downloads other malware from the Internet on to the PC. Usually, attackers install downloader software when they first gain access to a system
Dropper	A type of Trojan that installs other malware files on to the system either from malware package or internet
Exploit	A malicious code that breaches the system security via software vulnerabilities to access information or install malware
Injector	A program that injects its code into other vulnerable running processes and changes the way of execution in order to hide or prevent its removal
Obfuscator	A program via various techniques that conceals its code and intended purpose, and thus, makes it hard for security mechanisms to detect or remove it
Packer	A program that allows to bundle all files together into a single executable file via compression in order to bypass security software detection
Payload	A piece of software that allows to control a computer system after it has been exploited
Malicious Code	A command that defines malware's basic functionalities such as stealing data and creating backdoor

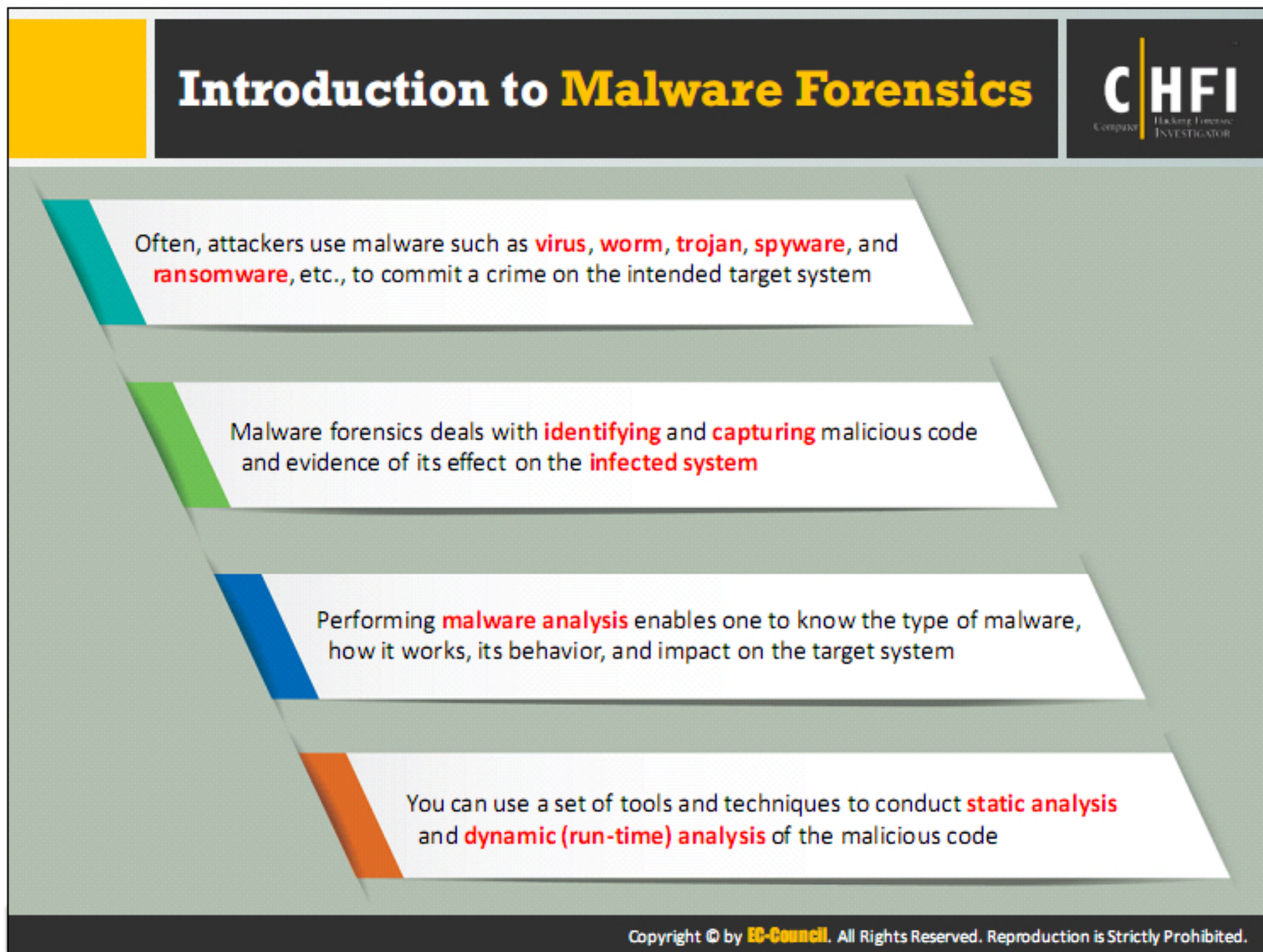
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Malware authors and attackers create malware using the components that can help them achieve their goals. They can use malware to steal the information, delete the data, change system settings, provide access or simply multiply and occupy the space. Malware are capable of propagating and functioning secretly.

Some the basic components of most malware programs are:

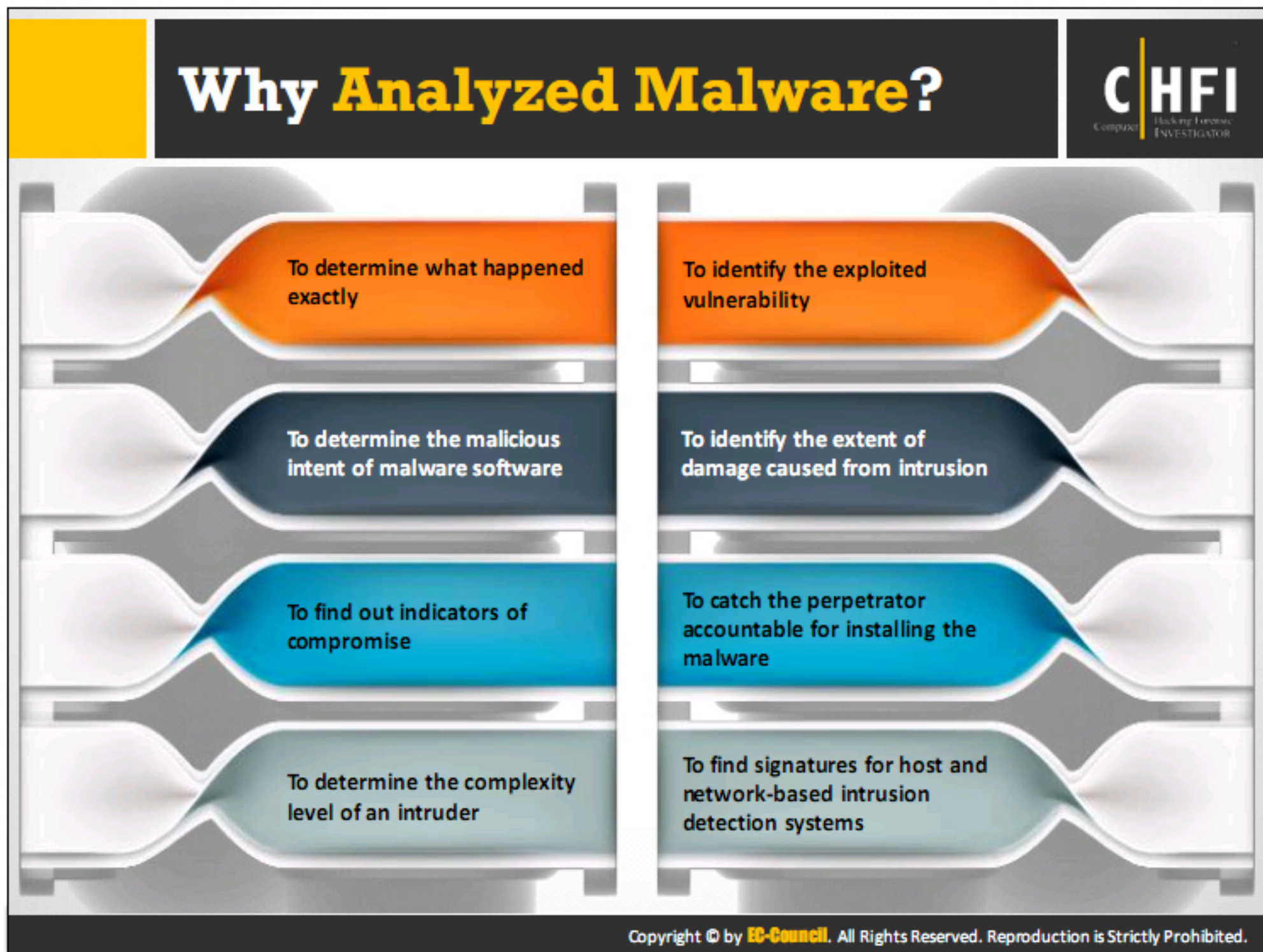
- **Crypter:** Refers to a software program that can conceal existence of malware. Attackers use this software to elude antivirus detection. The crypter encrypts the malicious file in a malware or the complete malware itself to avoid detection.
- **Downloader:** Type of Trojan that downloads other malware (or) malicious code and files from the Internet on to the PC. Usually, attackers install downloader when they first gain access to a system.
- **Dropper:** Attackers need to install the malware program or code on the system to make it run and this program can do the installation task covertly. The dropper can contain unidentifiable malware code that antivirus scanners cannot detect and is capable of downloading additional files needed to execute the malware on a target system.
- **Exploit:** Part of the malware that contains code or sequence of commands that can take advantage of a bug or vulnerability in a digital system or device. It is the code the attackers use to breach the system's security through software vulnerabilities to spy the information or to install malware. Based on the type of vulnerabilities they abuse, the exploits have different categories including local exploits and remote exploits.

- **Injector:** Program that injects the exploits or malicious code available in the malware into other vulnerable running processes and changes the way of execution to hide or prevent its removal.
- **Obfuscator:** A program to conceal the malicious code of a malware via various techniques. Thus, making it hard for security mechanisms to detect or remove it.
- **Packer:** It is software that compresses the malware file to convert the code and data of malware into an unreadable format. The packers use compression techniques to pack the malware.
- **Payload:** Part of the malware that performs desired activity when activated. Payload can have the tendency of deleting, modifying files, affecting the system performance, opening ports, changing settings, etc. as part of compromising the security.
- **Malicious Code:** It is a piece of code that defines basic functionality of the malware and comprises commands that result in security breaches. It can take forms like:
 - Java Applets
 - ActiveX Controls
 - Browser plug-ins
 - Pushed content



Attackers are using sophisticated malware techniques as cyber weapons to steal sensitive data. The malware can inflict intellectual and financial losses to the target, may it be an individual, a group of people or an organization. The worst part is that it spreads from one system to another with ease and stealth.

Malware forensics is the method of finding, analyzing and investigating various properties of malware to find the culprits and reason for the attack. The process also includes tasks such as finding out the malicious code, determining its entry, method of propagation, impact on the system, ports it tries to use, etc. Investigators conduct forensic investigation using different techniques and tools.




Some of the basic objectives behind analyzing a malicious program include:

- Evaluate harm from an intrusion
- List the indicators of compromise for different machines and different malware programs
- Find the system vulnerability malware has exploited
- Distinguish the gatecrasher or insider responsible for the malware entry

Some of the most common business questions answered by malware analysis are:

- What is the intention of the malware?
- How did it get through?
- Who are the perpetrators and how good are they?
- How to abolish it?
- What are the losses?
- How long the system has it infiltrate from?
- What is the medium of malware?
- What are the preventive measures?

Identifying and Extracting Malware



■ If a user has **reported about suspicious activity** on his/her system, you have to examine the following areas of the compromised system to find the traces of malware installation

● Installed programs	● Logs
● Suspicious executables	● User accounts and logon activities
● Auto-starting locations	● File system
● Scheduled jobs	● Registry entries
● Services	● Application traces
● Modules	● Restore points, etc.

■ You can use tools such as balbuzard, Cryptam Malware Document Detection Suite, etc. to extract patterns from malicious files for investigative purpose


■ You can perform static and dynamic analysis together in order to identify the intent and capabilities of the malware software


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

When the investigators obtain reports of suspicious activity from victims, they have to conduct a thorough examination of the suspect system, network, and other connected devices to find the traces of malware. Malware programs exhibit specific properties, which can help the investigators in identifying or distinguishing them from usual software programs. Investigators can use software and hardware tools as well as online tools and databases to identify the malware.

Investigators can use tools such as balbuzard, Cryptam Malware Document Detection Suite, etc. to extract patterns of investigative interest from malicious files. These tools offer automated scanning of the system for traces of malware that result in easy identification. Perform static and dynamic analysis together to identify the intent and capabilities of the malware. Static analysis is the process of looking for known traces and values that represent presence of malware. These traces include presence of malicious code, strings, executables, etc., in the software program. Dynamic analysis uses a different approach such as scanning the behavior of the software program while running it in a controlled environment.

Prominence of Setting up a Controlled Malware Analysis Lab



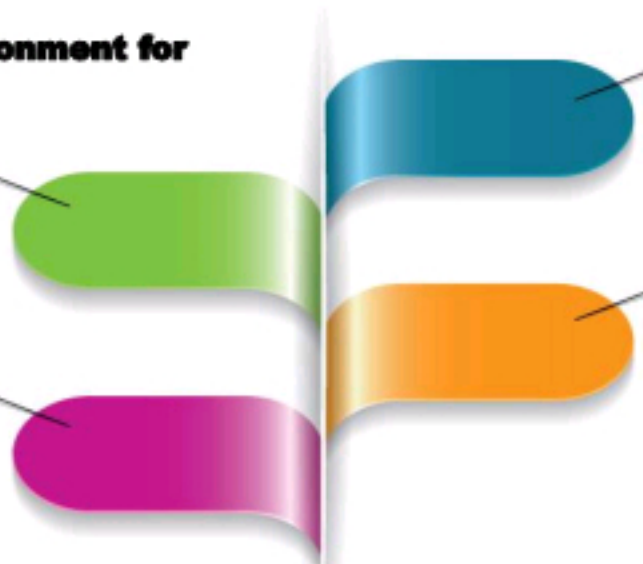


- Usually, malware analysis is carried out by infecting a system with the **malicious code** and then evaluating its behavior using a set of monitoring tools
- Thus, a **dedicated laboratory system** is required that can be infected keeping the production environment safe
- Best way to set up such lab system involves:
 - Using a physical system isolated from the production network to prevent the spread of the malware
 - Using **virtualization software** such as Virtualbox, VMware, Parallels, etc. (to set up single physical system with multiple VMS installed in it, each running different OSs)

Importance of virtual environment for malware analysis:

Protects real systems and network from being infected by the malware under analysis

Easy to analyze malware interaction with other systems



Allows capturing of screen during analysis

Ability to take snapshots of the laboratory system, which can be used to easily revert to a previous system state

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Malware analysis lab

A Controlled Malware Analysis Lab is instrumental in gauging the behavioral pattern of the malware, as the malware programs are dynamic in nature and would spread to various parts of the system as well as network when executed. Investigators should create an environment, which they can corrupt with the malware without disrupting or corrupting the other devices. This requires a laboratory system so that the production environment is safe. The most effective way to set up such lab involves use of virtualization software, which enables investigators to host multiple virtual systems running different operating systems on a single computer. Commonly used software to simulate real time systems in virtual environment include:

- VirtualBox
- VMware vSphere Hypervisor
- Microsoft Windows Server

Malware connect with networks and other systems, for stealing data on getting instructions from the attacker, or copying itself. Researchers can use multiple interconnected virtual machines on a single physical computer for analyzing malware behavior on connected systems and also learn about their propagation methods as well as various other characteristics.

Investigators must take precautions such as isolating the malware-analysis lab from the production network using firewall to inhibit malware propagation. Use removable media, mainly DVDs to install tools and malware. DVDs mostly support read only format of data

transfer and prevent malicious software from writing or copying itself onto the DVD. Investigators can also use a write-protected USB key.

Preparing Testbed for Malware Analysis

CHFI
Computer Hacking Forensic Investigator

Allocate a **physical system** for the analysis lab

Install **Virtual machine** (VMware, Hyper-V, etc.) on the system

Install **guest OSs** in the Virtual machine(s)

Isolate the system from the network by ensuring that the **NIC card** is in "**host only**" mode

Simulate internet services using tools such as **iNetSim**

Disable the '**shared folders**' and the '**guest isolation**'

Install **malware analysis tools**

Generate **hash value** of each OS and tool

Copy the **malware** over to the guest OS

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Analysis Procedure: Preparing Test bed

Malware analysis provides in-depth understanding of each individual sample and identifies emerging technical trends from the large collections of malware samples. The samples of malware are mostly compatible with the Windows binary executable. There are different goals behind performing a Malware analysis.

It is very hazardous to analyze malware on production devices connected to production networks. Therefore, one should always analyze malware samples on a test bed.

Given below is the procedure for preparing a test bed:

Requirements to build a test bed:

- An isolated test network to host your test bed and isolated network services, such as DNS
- A machine installed with a variety of operating systems and configuration states
- Virtualization snapshot and re-imaging tools to capture machine state
- Tools to wipe and rebuild the victim's machine quickly
- A number of tools are required for testing:

- **Imaging tool:** To get a clean image for forensics and prosecution purpose.
- **File/data analysis:** To perform static analysis of potential malware files.
- **Registry/configuration tools:** Malware infects the Windows registry and other configuration variables. These tools help to identify the last saved settings.
- **Sandbox:** To perform dynamic analysis manually.
- **Log analyzers:** The devices under attack record the activities of malware and generate log files. Log analyzers are the tools used to extract log files.
- **Network capture:** To understand how the malware leverages the network.

Supporting Tools for Malware Analysis



Virtual Machines Tools

- Virtual Box (<https://www.virtualbox.org>)
- Parallels Desktop 11 (<http://www.parallels.com>)
- Boot Camp (<https://www.apple.com>)
- VMware vSphere Hypervisor (<http://www.vmware.com>)

Screen Capture and Recording Tools

- Snagit (<https://www.techsmith.com>)
- Jing (<https://www.techsmith.com>)
- Camtasia (<https://www.techsmith.com>)
- Ezvid (<http://www.ezvid.com>)

Network and Internet Simulation Tools


- NetSim (http://tetcos.com/netsim_gen.html)
- ns-3 (<https://www.nsnam.org>)
- Riverbed Modeler (<http://www.riverbed.com>)
- QualNet (<http://web.scalable-networks.com>)

OS Backup and Imaging Tools

- Genie Backup Manager Pro (<http://www.genie9.com>)
- Macrium Reflect Server (<http://www.macrium.com>)
- R-Drive Image (<http://www.drive-image.com>)
- O&O DiskImage 10 (<https://www.oo-software.com>)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

General Rules for Malware Analysis



During malware analysis, pay attention to the key features instead of understanding each and every detail

Try different tools and approaches to analyze the malware, as single approach may not be helpful

Identify, understand, and defeat new malware analysis prevention techniques


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

During malware analysis, the investigators should pay great attention to key features of a malware and should not try to observe every detail as the malware are dynamic and may change properties. In difficult and complex sections, investigators should try to gather a general overview.

Investigators should try different tools and approaches as they yield different results in different situations. Even though various tools and techniques have similar functionalities, the approach or different angle may also provide a different result.

As investigators adopt new malware analysis techniques, malware authors and attackers also try to find new evasion techniques to thwart analysis. Investigators must be able to identify, understand, and defeat these aversion techniques.

Documentation Before Analysis




The following are some of the documentations that an investigator should prepare before performing an executable file analysis:

- 1 Full path and location of the file
- 2 MAC-timestamp
- 3 The system information where file was stored, e.g. OS and version, file system, user accounts, IP address
- 4 References to that file within the file system or registry
- 5 Who found the file and when
- 6 Details of forensics investigation tools

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Documentation involves the process of recording detailed information on the malware analysis. Investigators should be quick in making a note of the steps they follow, properties of the executable file they are analyzing, study results, and supporting material such as screenshots, etc. Investigators can also take note of system status, platform, operating system and tools used for the process.

Types of Malware Analysis



- **Static Malware Analysis:**
 - Also known as **code analysis**, involves going through the executable binary code without actually **executing** it to have a better understanding about the malware and its purpose
 - **Disassemblers** such as IDA Pro, can be used to disassemble the **binary file**
- **Dynamic Malware Analysis:**
 - Also known as **behavioral analysis**, involves executing the malware code to know how it interacts with the host system and its impact on it
 - This type of analysis requires **virtual machines** and **sandboxes** to deter the spreading of malware
 - **Debuggers** such as GDB, OllyDbg, WinDbg, etc., are used to debug malware at the time of execution to study its behavior
- Both techniques are intended to understand how the **malware works**, but differ in the tools used, and time and skills required for performing **analysis**
- It is recommended to perform both static and dynamic analysis to understand the functionality of malware to a large extent

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The two of malware analysis types based on the approach methodology include static analysis or dynamic analysis. Both the approaches demonstrate malware function process, however the tools, time and skills required for performing the analysis are altogether different.

Static analysis is a basic analysis of the binary code and comprehension of the malware that explains its functions. Behavioral analysis or dynamic analysis deals with the study of malware behavior during installation, on execution and while running.

The general static scrutiny involves analysis of malware without executing the code or instructions. The process includes usage of different tools and techniques to determine the malicious part of the program or a file. It also gathers the information about malware functionality and collects technical pointers or simple signatures it generates. Such pointers include file name, MD5 checksums or hashes, file type, and file size.

Dynamic analysis involves execution of malware to examine its conduct, operations and identifies technical signatures that confirm the malicious intent. It reveals information, such as domain names, file path locations, created registry keys, IP addresses, additional files, installation files, DLL and linked files located on the system or network.

Malware Analysis: Static

CHFI
Computer Hacking Forensic Investigator

- In **static analysis**, we are not running the malware code so there is no need of creating a safe environment
- Analyzing the **binary code** provides information such as data structures, function calls, call graphs, etc.
- Load the binary code on to the **test system** (preferably the OS on which the malware is not designed to run) to analyze its static properties - strings embedded into the file, header details, hashes, embedded resources, packer signatures, metadata, etc.

Some of the static malware analysis techniques:

- File **fingerprinting**
- Local and Online **malware scanning**
- Performing **strings search**
- Identifying **packing/obfuscation** methods
- Finding the **portable executables (PE)** information
- Identifying **file dependencies**
- Malware **disassembly**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Static analysis refers to the process of investigating an executable file without running or installing it. It is safe to conduct static analysis because the investigator does not install or execute the suspect file. However, some malware does not need installation for performing malicious activities, so it is better that the investigators perform static analysis in controlled environment.

It involves the process of accessing the source code or binary code to find the data structures, function calls, call graphs, etc. that can represent malice. Investigators can use various tools to analyze binary code to understand file architecture and impact on the system. Compiling the source code of a system into a binary executable will result in data losses, which makes the analysis of the code more difficult.

The procedure of examining a given binary without executing it is mostly manual and requires extraction of intriguing data such as data structures, utilized functions and call graphs from the malicious file. The investigators cannot see this data gets after the program compilation.


Different procedures utilized for static malware analysis are:

- **File fingerprinting:** It examines the evident elements of the binary code which includes processes on the document level. This process includes calculation of cryptographic hashes of the binary code to recognize its function and compare it to other binary codes and programs faces in the past scenarios.
- **Local and online malware scanning:** It calculates hash values of a suspect file and compare them to online and offline malware databases to find the existence of the

recognized malicious code. This process simplifies further investigation by offering better insight of the code, its functionality, and other important details.

- Performing strings search: Software programs include some strings that are commands for performing specific functions such as printing output. Various strings exist that could represent the malicious intent of a program, such as reading the internal memory or cookie data, etc. embedded in the compiled binary code. Investigators can search for such embedded strings to draw conclusions about the suspect file.
- Identifying Packing or obfuscation methods: The attackers use packing and obfuscation by using jumbled structure or a packer to avoid detection. Investigators should find if the file includes packed elements and also locate the tool or method used for packing it.
- Finding the portable executables (PE) information: The PE format stores the information a Windows system requires to manage the executable code. The PE stores metadata about the program, which helps in finding the additional details of the file which include the unique number on UNIX systems to find the file type and divide information of the file format. For instance, Windows binary is in PE format that consists of information, such as time of creation and modification, import and export functions, compilation time, DLLs, linked files, as well as strings, menus and symbols.
- Identifying file dependencies: Any software program depends on various inbuilt libraries of an operating system that help in performing specified actions in a system. Investigators need to find the libraries and file dependencies, as they contain information about the run-time requirements of an application.
- Malware Disassembly: The static analysis also includes dismantling of a given executable into binary format to study its functionalities and features. This process will help investigators find the language used for programming the malware, look for APIs that reveal its function, etc. The process uses debugging tools such as OllyDbg and IDAPro.

Static Malware Analysis: File Fingerprinting

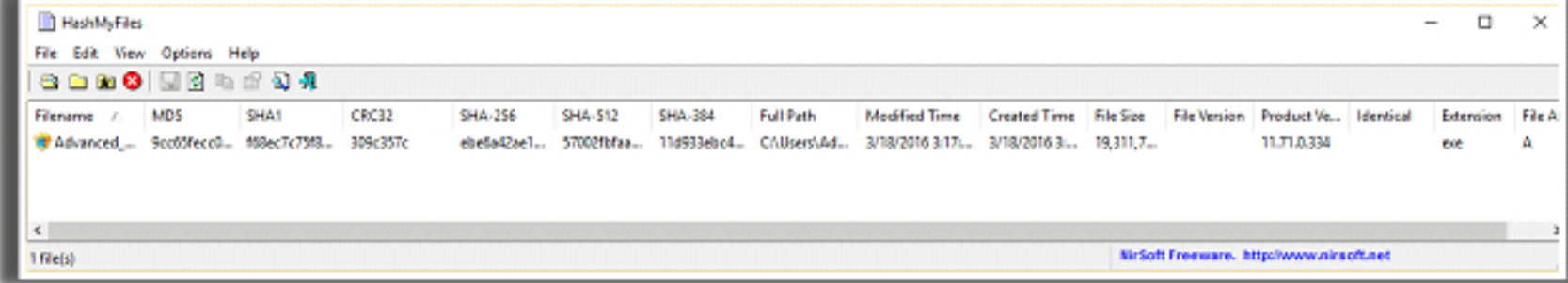


It is recommended to compute hash value for a given **binary code** before carrying out the investigation

Common **hash calculators** include HashTab, HashMyFiles, HashCalc, md5sum, md5deep, etc.

You can use the computed hash value to periodically verify if any change is made to the **binary code** during analysis

You can also compare the computed hash value with that of the identified malware stored in **databases**. Ex: VirusTotal - an online database



Filename	MD5	SHA1	CRC32	SHA-256	SHA-512	SHA-384	Full Path	Modified Time	Created Time	File Size	File Version	Product Ver...	Identical	Extension	File A
Advanced...	Sec09ec0...	990ec7c7993...	309c357c	e1e1fa42ae1...	570021bfaa...	11d9334be4...	C:\Users\Ad...	3/18/2016 3:17...	3/18/2016 3:...	18,311,7...	11.71.0.334			exe	A

1 file(s)

NirSoft Freeware, <http://www.nirsoft.net>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


File fingerprinting is data loss prevention method used for identifying and tracking data across a network. The process involves creating shorter text strings for the files called hash values. Unique hash values or fingerprints are developed using various cryptographic algorithms which utilize data such as strings, metadata, size and other information. .

These fingerprints help investigators recognize sensitive to track and identify similar programs from a database. Fingerprinting does not generally work for certain record sorts, including encrypted or password secured files, pictures, audio, and video, which have different content compared to the predefined fingerprint.

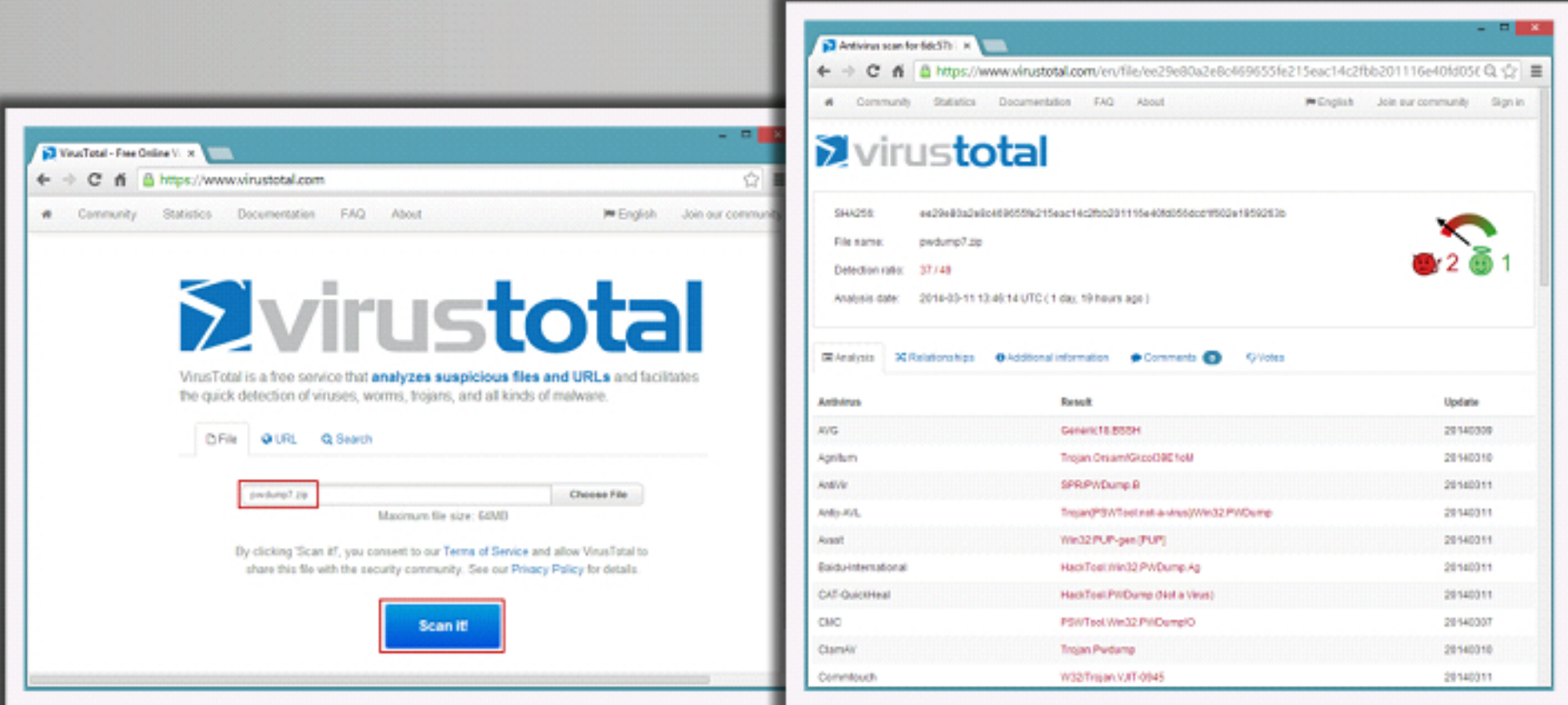
The Message-Digest Algorithm 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) are the most commonly used hash functions for malware analysis. Investigators can use tools such as HashMyFiles to create a fingerprint of the suspect file as part of the static analysis. It is a GUI-based tool that can calculate various hash values.

HashMyFiles produces hash value of a file using MD5, SHA1, CRC32, SHA-256, SHA-512 and SHA-384 algorithms. The program also provides information about the file such as full path of the file, date of creation, date of modification, file size, file attributes, file version, and extension. All this data will help investigators in searching for the similar files and comparing them.

Online Malware Testing: VirusTotal



■ VirusTotal is a free service that **analyzes suspicious files and URLs**, and facilitates the detection of viruses, worms, Trojans, etc.



The screenshot displays the VirusTotal website. On the left, the 'Free Online VirusTotal' interface shows a file upload area with a text input containing 'perdump7.zip' and a 'Scan It!' button. On the right, a detailed analysis report for the file 'perdump7.zip' is shown. The report includes the SHA256 hash, file name, detection ratio (37/48), and analysis date. Below this, a table lists the results from various antivirus engines.

Antivirus	Result	Update
AVG	Generic18.BSDH	20140309
Agribum	Trojan.Cream/Groco38C.told	20140310
AntVir	SPRUP/Dump.B	20140311
Anty-VUL	TrojanPSW/ToolKit-a-virus/Wo32.PW.Dump	20140311
Avast	Win32.PUP-gen (PUP)	20140311
BaiduInternational	HackTool.Win32.PW.Dump.Ag	20140311
CAE-QuickHeal	HackTool.PW.Dump (Not a Virus)	20140311
CMC	PSW/Tool.Win32.PW.Dump.O	20140307
ClamAV	Trojan.Perdump	20140310
Comodo	Win32/Trojan.VJT-0945	20140311


<http://www.virustotal.com>











Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

VirusTotal generates a report that provides the total number of engines that marked the file as malicious, the malware name, and, if available, additional information about the malware.

It also offers important details of the online file analysis such as target machine, compilation time stamp, type of file, compatible processors, entry point, PE sections, data link libraries (DLLs), used PE resources, different hash values, IP addresses accessed or contained in the file, program code, and type of connections established.

Online Malware Analysis Services



 Anubis: Analyzing Unknown Binaries http://anubis.iseclab.org	 Metascan Online http://www.metascan-online.com
 Payload Security https://www.hybrid-analysis.com	 Bitdefender QuickScan http://quickscan.bitdefender.com
 Malware Protection Center https://www.microsoft.com	 IObit Cloud http://cloud.iobit.com
 Malwr http://malwr.com	 Valkyrie https://valkyrie.comodo.com
 Dr. Web Online Scanners http://vms.drweb.com	 ThreatAnalyzer http://www.threattracksecurity.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Online Malware Analysis Services

Malware analysis helps in the understanding of its behavior and the potential severity of the damage it can and does cause. Below is a list of online malware analysis services that one can use to analyze various malware samples.

Anubis: Analyzing Unknown Binaries

Source: <http://anubis.iseclab.org>

Anubis is a tool for analyzing the behavior of Windows PE-executables, with a focus on malware analysis. It generates a report file that contains enough information about the purpose and the actions of the analyzed binary. The generated report includes detailed data about modifications made to the Windows registry or file system, about interactions with the Windows Service Manager or other processes, and of course it logs all generated network traffic.

Payload Security

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

This is an online malware analysis service powered by Payload Security that detects and analyzes unknown threats. The service is running VxStream Sandbox v5.50 in the backend that supports PE, Office, PDF, APK and more such files.

Malware Protection Center

Source: <https://www.microsoft.com>

The Malware Protection Center is a service provided to protect computers from malware.

Users submit the file containing malware or potentially unwanted software, and then Microsoft analyzes the file and generates a complete report of its findings.

Malwr

Source: <https://malwr.com>

Malwr is a free malware analysis service and community that allows users to submit files to it and receive the results of a dynamic analysis.

Dr. Web Online Scanners

Source: <http://vms.drweb.com>

Dr. Web Online Scanner is an online tool that needs a suspicious file or link to scan. This tool allows file scan, link scan, and virus database search. After the analysis of the suspicious file or links, the tool generates a detailed report of detected viruses, worms, and various kinds of adware, and sends it to the requester.

Metascan Online

Source: <http://www.metascan-online.com>

Metascan Online is an online file scanning service powered by OPSWAT's Metascan technology, a multiple-engine malware scanning solution.

Bitdefender QuickScan

Source: <http://quickscan.bitdefender.com>

Bitdefender QuickScan is an online virus scanner that detects hidden threats, malware, and keyloggers. It uses in-the-cloud scanning technology to detect active malware on a system.

IObit Cloud

Source: <http://cloud.iobit.com>

IObit Cloud is an automated threat analysis system that uses Cloud Computing technology and Heuristic Analyzing mechanic to analyze the behavior of spyware, adware, trojans, keyloggers, bots, worms, hijackers and other security-related risks.

Valkyrie

Source: <https://valkyrie.comodo.com>

Valkyrie is a signature based malware detection system that conducts analysis using run-time behavior and hundreds of features from a file. It can also warn users against malwares undetected by other Anti-Virus products.

ThreatAnalyzer

Source: <http://www.threattracksecurity.com>

ThreatAnalyzer is a malware analysis tool that provides defense against Advanced Persistent Threats (APTs), Zero-days, and custom-targeted attacks. This tool analyzes malware samples, generates report analyses to aid in the understanding of each threat, and improves response time to remediate threats.

Static Malware Analysis: Local and Online Malware Scanning




- Scan the **binary code** using renowned and up-to-date **anti-virus software**
- If the code under analysis is a component of a **well-known malware**, it may have been already discovered and documented by many anti-virus vendors
- Go through their documentation to recognize the code **capabilities, signatures**, etc.
- You can also upload the code to **websites** such as VirusTotal (<https://www.virustotal.com>) and Jotti (<https://virusscan.jotti.org>) to get it scanned by a wide-variety of different scan engines



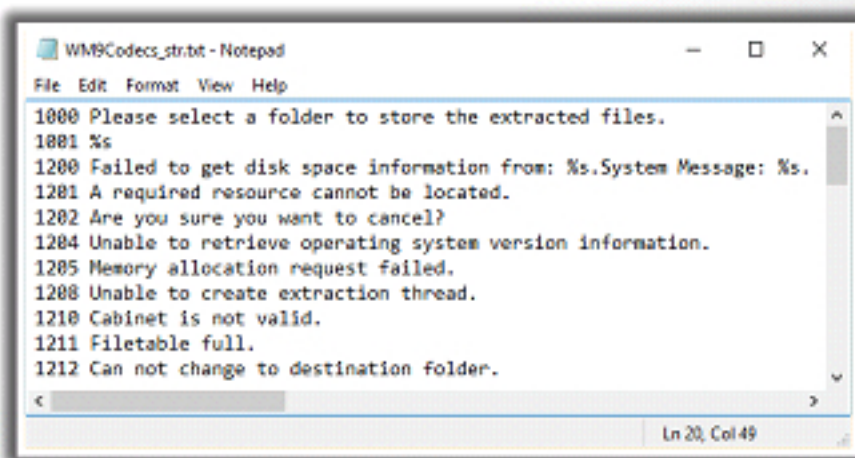
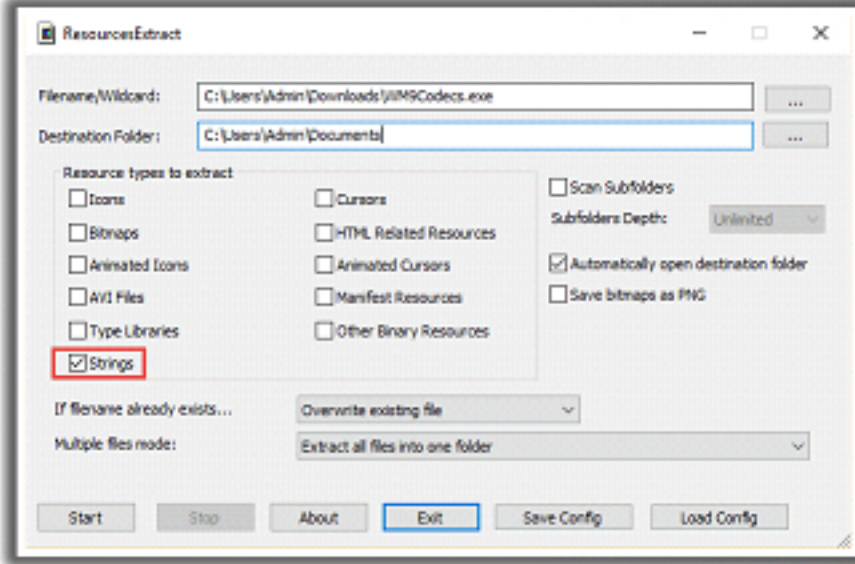
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigators can scan malware using online tools like Jotti for well-known malwares. Numerable anti-virus vendors would have analyzed and sorted the malware files. The documentation of such malwares would fetch important information such as code capabilities and modus operandi of the attacks it has performed. Jotti is one such tool which performs the above mentioned functionalities.

Static Malware Analysis: Performing Strings Search



- 1 **Strings** communicate information from the program to its user
- 2 Analyze **embedded strings** of the readable text within the program's executable file.
Ex: Status update strings and error strings
- 3 Use tools such as Strings, ResourcesExtract, Bintext, Hex Workshop, etc. to extract embedded strings from **executable files**
- 4 Ensure that the tool extract strings are represented in both **ASCII** and **Unicode** formats
- 5 On extracting, one can see the input of strings of interest in **search engine** for more information



<https://www.microsoft.com>

Note: Strings may be often misleading or cause you to activate a sort of reverse-honeypot


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Searching through the strings can provide information about the basic functionality of any program. During malware analysis, the investigators search for the common malicious string that could determine harmful actions that a program can perform. For instance, if the program accesses a URL, it will have that particular URL string stored in it. Investigators should be attentive while looking for strings and also search for the embedded and encrypted strings in the suspect file.

Use tools such as Strings, ResourcesExtract, Bintext, Hex Workshop, etc. to extract all types of strings from executable files. Ensure that the tool can scan and display ASCII and Unicode strings as well.

Some tools have the capability to extract all the strings and copy them to a text or document file. Use such tools and copy the strings to a text file for ease in searching the malicious strings.

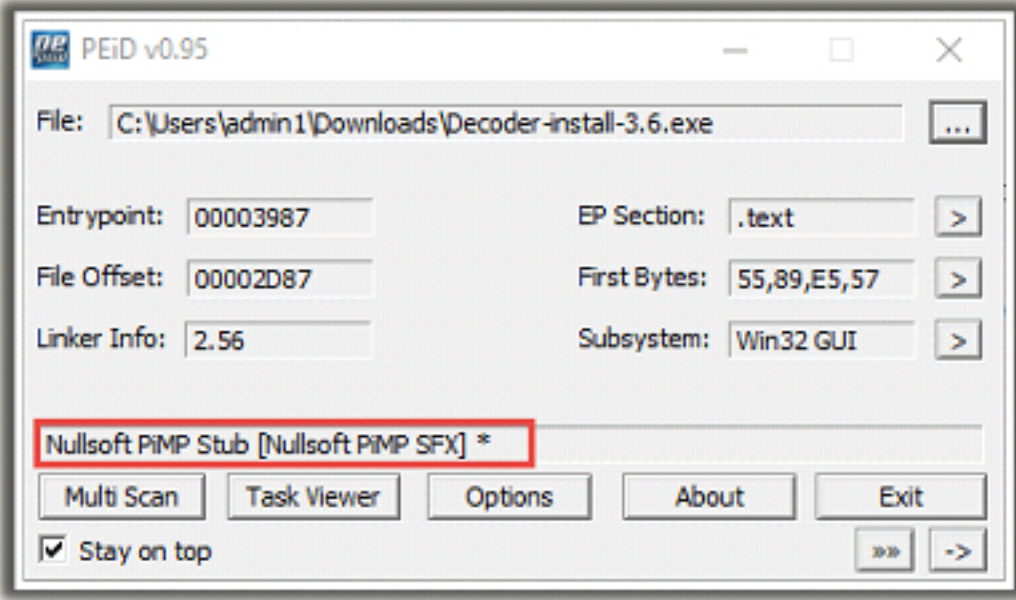
Static Malware Analysis: Identifying Packing/Obfuscation Methods



Attackers often use packers to compress, encrypt, or modify a **malware executable file**

It toughens the task of the **reverse engineers** in finding out the actual program logic and other metadata via static analysis

Use tools such as **PEiD**, which detects most common packers, cryptors and compilers for PE executable files



PEiD v0.95

File: C:\Users\admin1\Downloads\Decoder-install-3.6.exe

Entrypoint: 00003987 EP Section: .text

File Offset: 00002D87 First Bytes: 55,89,E5,57

Linker Info: 2.56 Subsystem: Win32 GUI

Nullsoft PIMP Stub [Nullsoft PIMP SFX] *

Multi Scan Task Viewer Options About Exit

☒ Stay on top


<http://www.softpedia.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

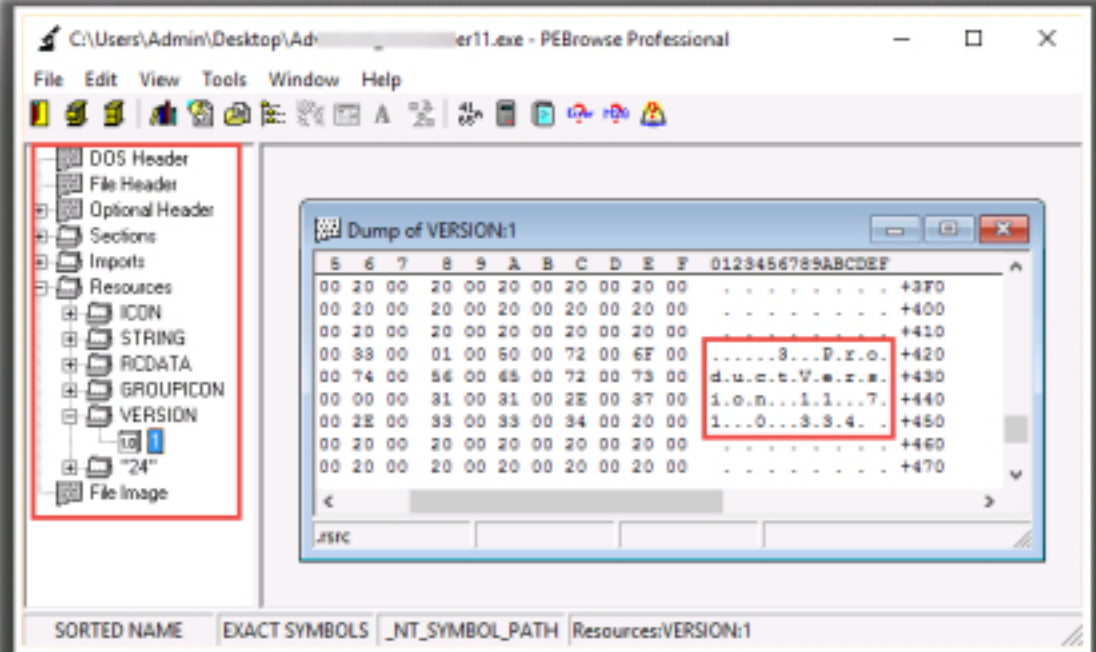
Malware creators use packing or obfuscation to deceive the investigators into thinking the file as normal or unanalyzable. Obfuscation also hides execution of the programs. When the user executes a packed program, it also runs a small wrapper program to decompress the packed file and then run the unpacked file.

Investigators can use tools like PEid to find if the file has packed programs or obfuscated code. This tool also displays the type of packers used in packing the program. Additional details it displays include entry point, file offset, EP Section, and subsystem used for packing. Finding the packer will ease the task of selecting a tool for unpacking the code.

Static Malware Analysis: Finding the Portable Executables (PE) Information



- PE format is the **executable file** format used on Windows operating systems
- Information available for examining the **metadata** of a PE file:
 - Time and date of compilation
 - Functions imported and exported by the program
 - Linked libraries
 - Icons, menus, version info, strings, etc. embedded in resources
- You can use tools such as PView, PE Explorer, Portable Executable Scanner (PEscan), PEBrowse Professional, Resource Hacker, Dependency Walker, etc. to extract the above mentioned information



<http://www.smidgeonsoft.prohosting.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Portable Executable (PE) format stores the information required to install and run any executable program on a Windows operating system. The PE format contains header and sections, which stores metadata about the file and code mapping in an operating system. Investigators can use the header information to gather additional details of a file or program, such as features.

PE of a file contains the sections:

- **.text:** Contains instructions and program codes that the CPU executes.
- **.rdata:** Contains the import and export information as well as other read-only data used by the program.
- **.data:** Contains the program's global data, which the system can access from anywhere.
- **.rsrc:** Comprises of the resources employed by the executable, such as icons, images, menus, and strings, as this section offers multi-lingual support.

Investigators can use PE analysis tools such as PView, PE Explorer or PEBrowse Professional to gather the following information:

- Imports: Functions from other libraries used by the malware
- Exports: Functions in the malware that other programs or libraries call while running
- Time Date Stamp: Time of program compilation

- Sections: Names of all the sections a file contains along with their sizes on disk and in memory
- Subsystem: Denotes if the program is a command-line or GUI application
- Resources: Includes strings, icons, menus, and other information stored in the file

CHFI
Computer Hacking Forensic Investigator

-
- Dependency Walker - [nti.exe]
- File Edit View Options Profile Window Help
- NTI.EXE
- API-MS-WIN-CORE-RTLSUPPORT
NTDLL.DLL
KERNELBASE.DLL
NTDLL.DLL
API-MS-WIN-CORE-APIQUKE
EXT-MS-WIN-ADVAPI32-REI
EXT-MS-WIN-KERNEL32-AP
EXT-MS-WIN-NTUSER-STRI
EXT-MS-WIN-KERNEL32-FIL
EXT-MS-WIN-KERNEL32-DL
EXT-MS-WIN-KERNEL32-CL
EXT-MS-WIN-KERNEL32-SIC
- | Name | Ordinal | Hint | Function | Entry Point |
|----------------|--------------|------|----------------|-------------|
| CreatePipe | 65 (0x0041) | | CreatePipe | Not Bound |
| CreateProcessA | 66 (0x0042) | | CreateProcessA | Not Bound |
| CreateThread | 72 (0x0048) | | CreateThread | Not Bound |
| GetVersionExA | 352 (0x0160) | | GetVersionExA | Not Bound |
| ReadFile | 509 (0x01FD) | | ReadFile | Not Bound |
| Sleep | 627 (0x0273) | | Sleep | Not Bound |
- | Name | Ordinal | Hint | Function | Entry Point |
|-------------------------|------------|------------|-------------------------|---------------------|
| AcquireSRWLockExclusive | 1 (0x0001) | 0 (0x0000) | AcquireSRWLockExclusive | NTDLL.RtlAcquireSRW |
| AcquireSRWLockShared | 2 (0x0002) | 1 (0x0001) | AcquireSRWLockShared | NTDLL.RtlAcquireSRW |
| ActivateActCtx | 3 (0x0003) | 2 (0x0002) | ActivateActCtx | 0x00003C50 |
| ActivateActCtxWorker | 4 (0x0004) | 3 (0x0003) | ActivateActCtxWorker | 0x00003B90 |
| AddAtomA | 5 (0x0005) | 4 (0x0004) | AddAtomA | 0x00003B90 |
| AdjustToken | 6 (0x0006) | 5 (0x0005) | AdjustToken | 0x00003B90 |
- | Module | File Time Stamp | Link Time Stamp | File Size | Attr. | Link Checksum | Real Checksum |
|-----------------------------------|------------------|------------------|-----------|-------|---------------|---------------|
| API-MS-WIN-CORE-BEML1-1-0.DLL | 08/22/2013 5:15p | 08/22/2013 5:15p | 2,560 | HA | 0x00002C80 | 0x00002C80 |
| API-MS-WIN-CORE-COMM1-1-0.DLL | 08/22/2013 5:15p | 08/22/2013 5:15p | 1,584 | HA | 0x00008D4A | 0x00008D4A |
| API-MS-WIN-CORE-CONSOLE1-1-0.DLL | 08/22/2013 5:15p | 08/22/2013 5:15p | 3,584 | HA | 0x00004598 | 0x00004598 |
| API-MS-WIN-CORE-CONSOLE12-1-0.DLL | 08/22/2013 5:15p | 08/22/2013 5:15p | 4,096 | HA | 0x00003D44 | 0x00003D44 |
| API-MS-WIN-CORE-CRT1-1-1-0.DLL | 08/22/2013 5:15p | 08/22/2013 5:15p | 4,608 | HA | 0x0000FBD5 | 0x0000FBD5 |
- Error: Modules with different CPU types were found.
- Warning: At least one delay-load dependency module was not found.
- For Help, press F1

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some of the standard dlls are:

dll	Description of contents
Kernel32.dll	Core functionality, such as access and manipulation of memory, files, and hardware
Advapi32.dll	Provides access to advanced core Windows components such as the Service Manager and Registry
User32.dll	User-interface components, such as buttons, scroll bars, and components for controlling and responding to user actions
Gdi32.dll	Functions for displaying and manipulating graphics
Ntdll.dll	Interface to the Windows kernel
WSock32.dll and Ws2_32.dll	Networking DLLs that help to connect to a network or perform network-related tasks
Wininet.dll	Supports higher-level networking functions

TABLE 11.1 Standard dlls

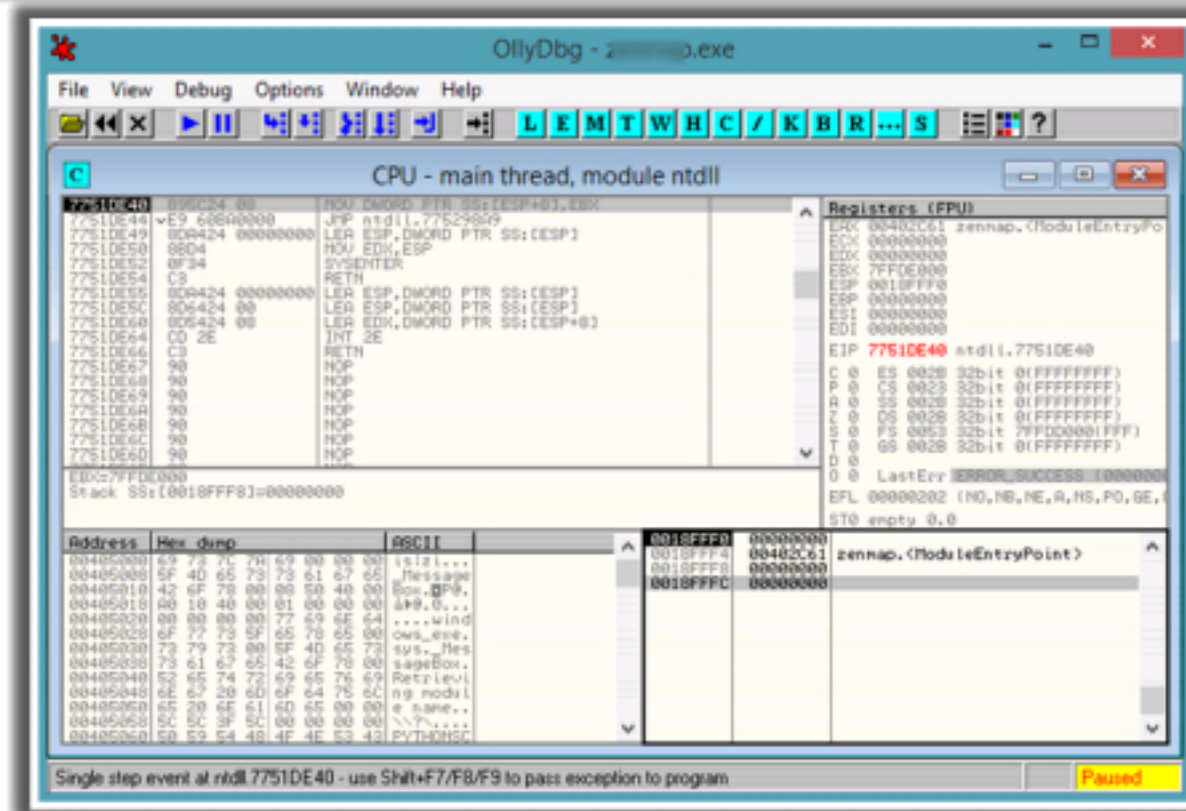
Investigators can use tools such as Dependency Walker that lists all the dependent modules and builds a hierarchical tree diagram. It also records all the functions each module exports and calls. The GUI tool can also detect many common application problems such as missing and invalid modules, import/export mismatches, circular dependency errors, mismatched machine modules, and module initialization failures.

Investigators should look for dlls with different names or misspelled dlls or functions of the dlls to identify malicious dlls.

Static Malware Analysis: Malware Disassembly



- Disassemble the **binary code** and analyze the assembly code instructions
- You can use tools such as **IDA Pro** that can reverse machine code to **assembly language**
- Based on the reconstructed assembly code, you can inspect the **program logic** and recognize its threat potential. This process is carried out by using debugging tools such as **OllyDbg**, **WinDbg**, etc.



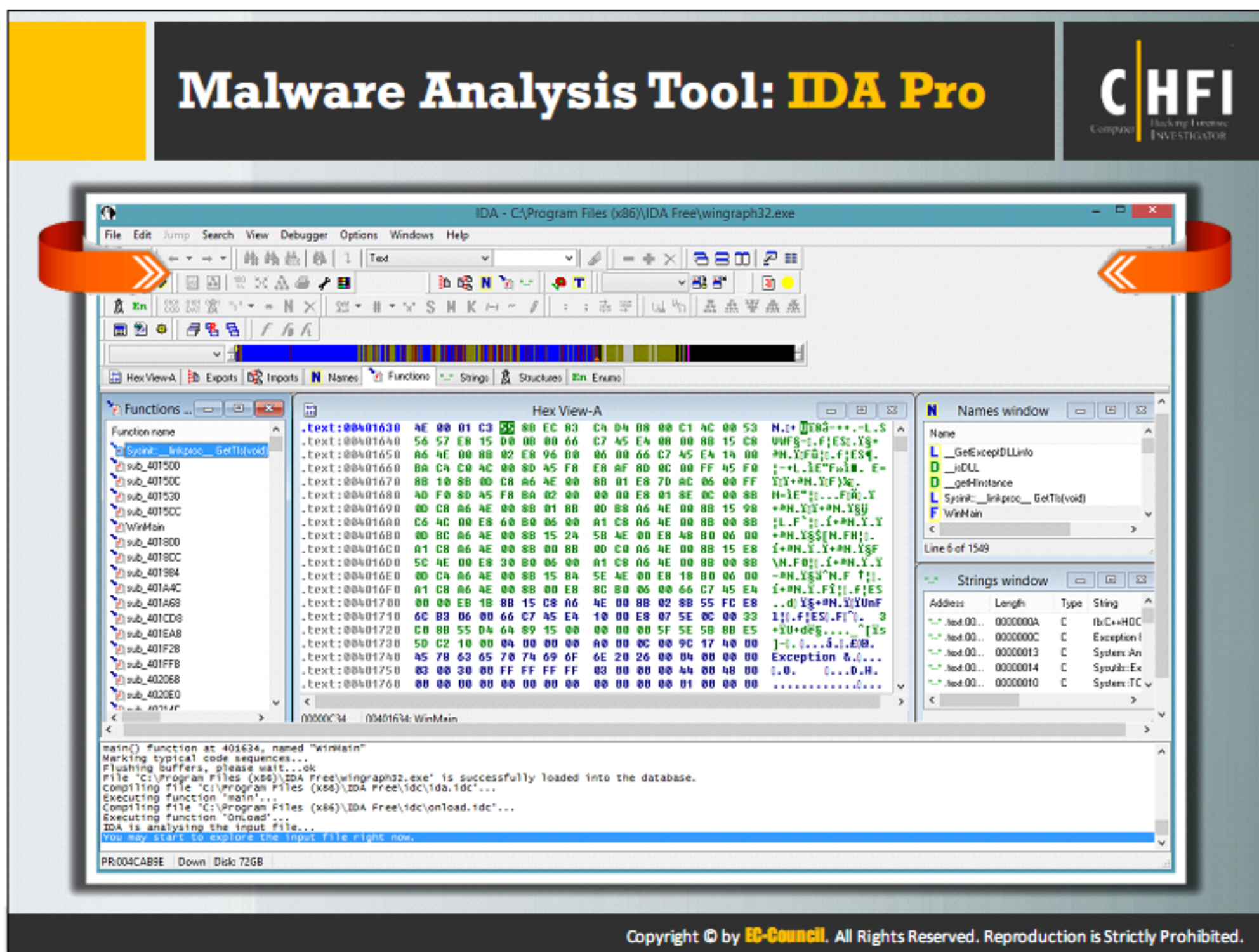
<http://www.ollydbg.de>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IDA Pro is a multi-platform disassembler and debugger that explores binary programs, for which source code isn't always available, to create maps of their execution. It shows the instructions in the same way as a processor executes them in a symbolic representation called assembly language. Thus, it is easy for the investigators to find the harmful or malicious processes.

For example, if a user installs a screensaver that is spying on e-banking session or logging e-mails, a disassembler can reveal it. IDA Pro makes assembly language and code more readable. The tool displays the internals of the file such as IDA view, hex view, enumerations, imports and exports, subroutines and their paths, functions that call a subroutine, etc.

Investigators can use all these values and data to find the functions and subroutines that perform harmful activities and confirm that the executable file contains malware.




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IDA is a Windows, Linux or Mac OS X hosted multi-processor disassembler and debugger that offers so many features it is hard to describe them all. Just grab an evaluation version if you want a test drive.

Source: <https://www.hex-rays.com>

Malware Analysis: **Dynamic**



System Baselining:

- Refers to taking **snapshot** of the system at the time the malware analysis begins
- Main purpose of system baselining is to identify significant changes from the **baseline state**
- System baseline includes details of file **system**, **registry**, **open ports**, **network activity**, etc.

Host Integrity Monitor:

- Host integrity monitoring involves taking a snapshot of the **system state** using the same tools before and after the analysis to detect **changes** made to the entities residing on the system.
- Host integrity monitoring includes:

Installation Monitor	DNS Monitoring/Resolution
Process Monitor	API Calls Monitor
Files and Folder Monitor	Device Drivers Monitor
Registry Analysis/Monitoring	Startup Programs Monitor
Network Traffic Monitoring/Analysis	Windows Services Monitor
Port Monitor	

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Dynamic malware analysis refers to the process of studying the behavior of the malware by running it in a monitored environment. The environment design should include the tools that can capture every movement of the malware in detail and give feedback to the investigator. Mostly virtual systems act as a base for conducting such experiments.

Investigators use the dynamic analysis to gather valuable information about malware activity including files and folders created, ports and URLs accessed, called functions and libraries, applications and tools accessed, information transferred, settings modified, processes and services the malware started, etc.

The investigator should design and setup the environment for performing dynamic analysis in such a way that the malware cannot propagate to the production network and the testing system is capable of recovering from an earlier set timeframe in case anything goes wrong during the test. To achieve this, the investigator needs to perform the following:

System Baselining

Baselining refers to the process of capturing system state that investigators can use to compare to the system's state after executing the malware file. This will help investigators understand the changes malware has made across the system. System baseline includes recording details of the file system, registry, open ports, network activity, etc.

An Investigator should baseline the system properties before executing the malware while ensuring that the baseline includes system properties, file system, registry, ports, network, firewall, etc.

Host Integrity Monitor

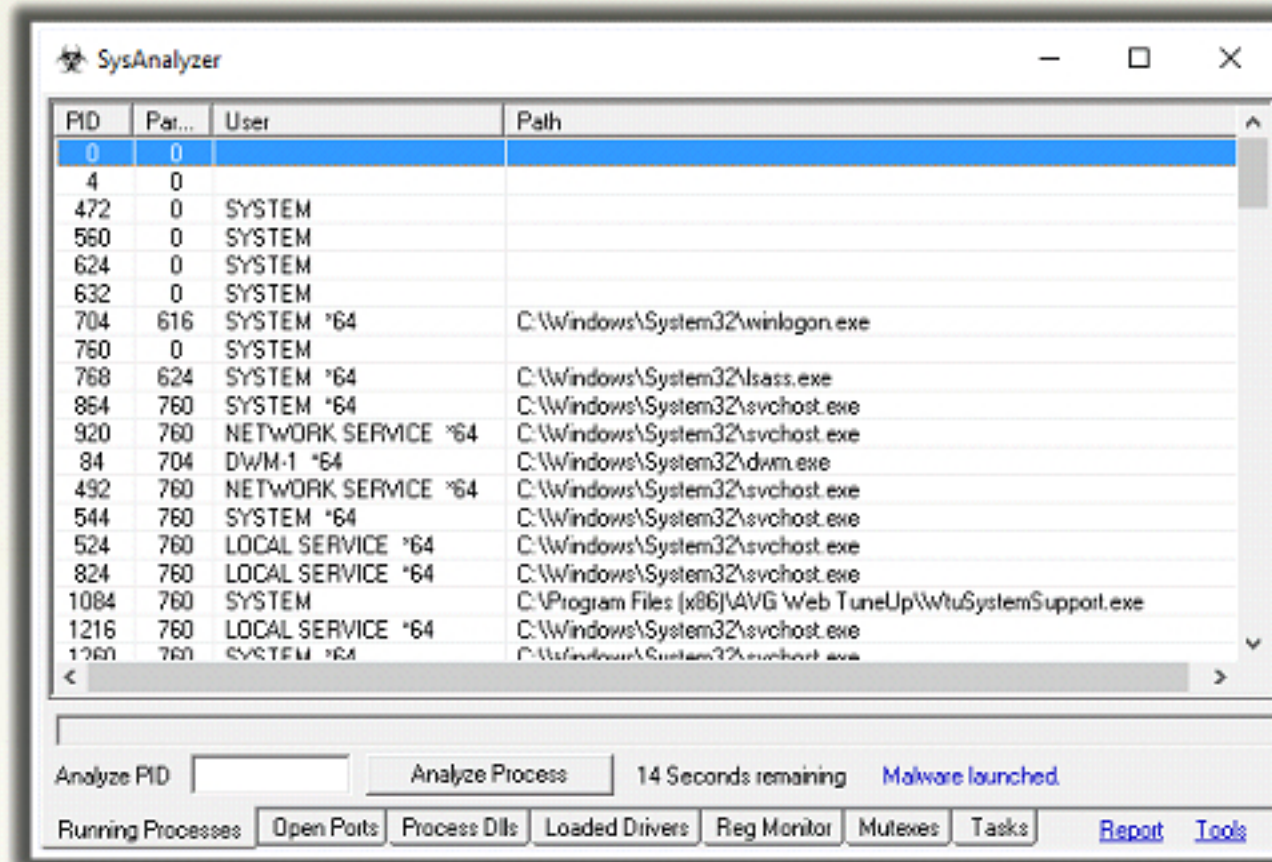
Host integrity monitoring is the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents. It involves taking a snapshot of the system before and after the incident or actions using the same tools and analyzing the changes to evaluate the impact on the system and its properties.

In malware analysis, host integrity monitoring will help investigators understand the runtime behavior of a malware file as well as its activities, propagation techniques, URLs accessed, downloads initiated, etc.

Dynamic Malware Analysis: Installation Monitor



- You can use tools such as Mirekrosoft Install Monitor, Advanced Uninstaller PRO, Epsilon Squared's InstallWatch, Revo Uninstaller Pro, Comodo Programs Manager, **SysAnalyzer**, etc. to detect changes made to a system on execution of an **unknown binary specimen**



<http://www.sysanalyser.com>


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

When the system or users try to install or uninstall an application, there is a chance that it leaves traces of the application data on the system. This data may include evidential information the investigators need. To find these traces, the investigators should know the folders modified or created during the installation process as well as the files and folders which has not been modified by the uninstalling process.

Installation monitor will help investigator in detecting hidden and background installations which the malware performs. Tools such as Mirekrosoft Install Monitor, Advanced Uninstaller PRO, Epsilon Squared's InstallWatch, Revo Uninstaller Pro, Comodo Programs Manager, SysAnalyzer, etc. help investigators to monitor installation process.

Using the SysAnalyzer for monitoring installation of an executable, the investigator can find installation information such as Process ID (PID), the path of storing the new files, open ports, process DLLs, loaded drivers, and tasks.

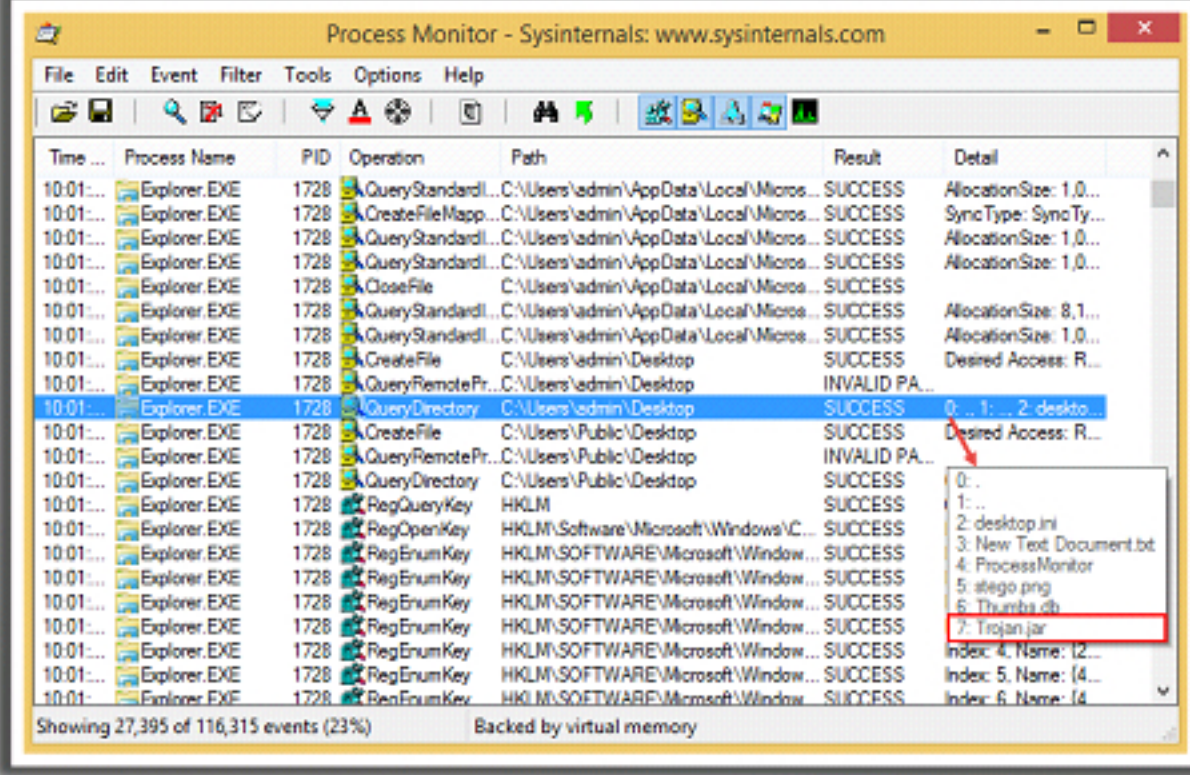
Dynamic Malware Analysis: Process Monitor



After executing the suspect program, you can use tools such as **Process Monitor**, **Perfmon**, etc. to gather the resulting process information (process name, process ID, associated handles, libraries loaded, related child processes, path of the program responsible for process creation, etc.)

Process Monitor Tool

Process Monitor is a monitoring tool for Windows that **shows file system, registry, and process/thread activity**



<http://technet.microsoft.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigators should perform the process monitoring as it will help them understand the processes a malware initiates and takes over after execution. They should also observe the child processes, associated handles, loaded libraries, and functions, to define the entire nature of a file or program, gather information about processes running before execution of the malware, and compare them to the processes running after execution. This method will reduce the time taken to analyze the processes and help in easy identification of all the processes malware starts.

Process Monitor Tool

Process Monitor is a monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two Sysinternals utilities, Filemon and Regmon, and adds enhancements including rich and non-destructive filtering, comprehensive event properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.


Process Monitor includes monitoring and filtering capabilities, which includes:

- More data captured for operation input and output parameters.
- Non-destructive filters allow you to set filters without losing data.

- Capture of thread stacks for each operation makes it possible in many cases to identify the root cause of an operation.
- Reliable capture of process details, including image path, command line, user and session ID.
- Configurable and moveable columns for any event property.
- Filters can be set for any data field, including fields not configured as columns.
- Advanced logging architecture scales to tens of millions of captured events and gigabytes of log data.
- Process tree tool shows relationship of all processes referenced in a trace.
- Native log format preserves all data for loading in a different Process Monitor instance.
- Process tooltip for easy viewing of process image information.
- Detail tooltip allows convenient access to formatted data that doesn't fit in the column.
- Cancellable search.
- Boot time logging of all operations.


Source: <https://technet.microsoft.com>

Process Monitoring Tool: What's Running

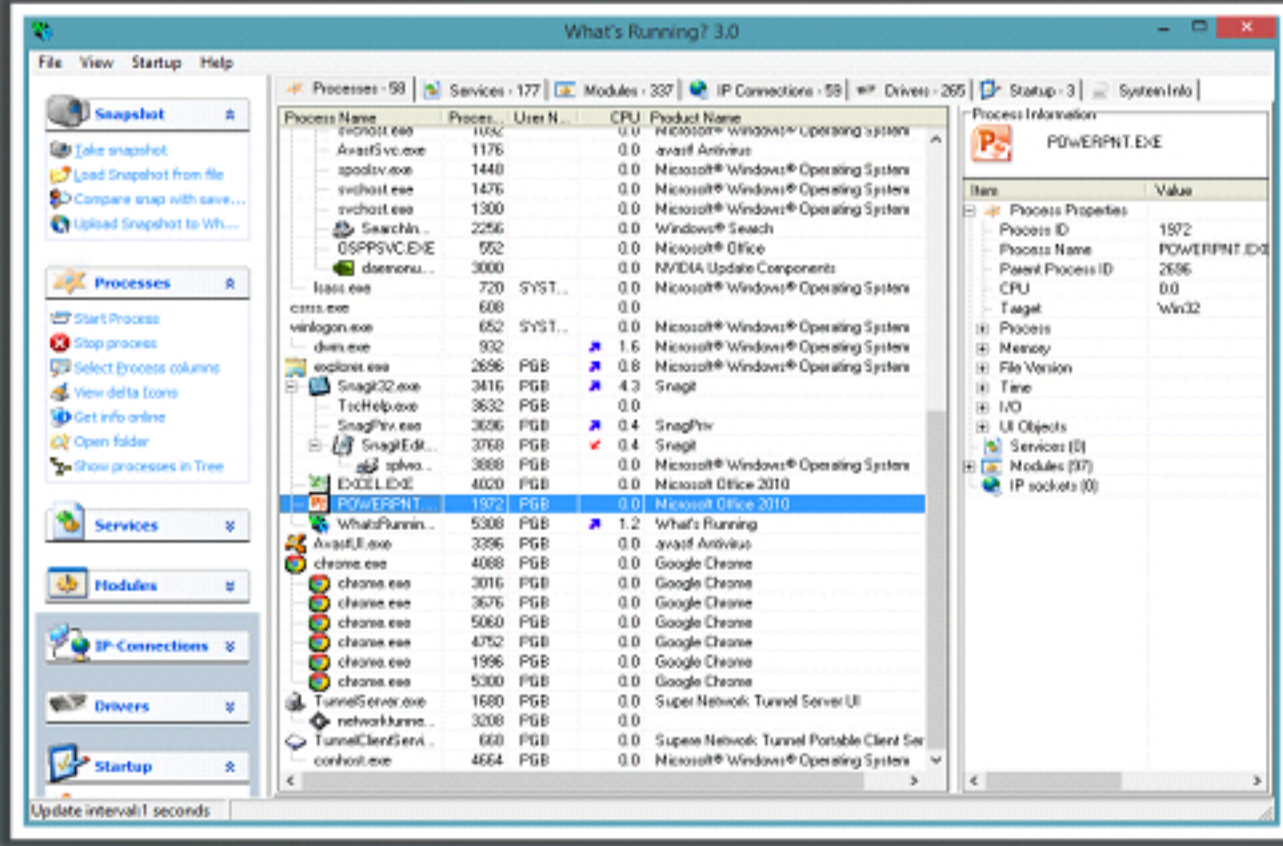


Features

- Inspect the **processes** and get performance along with **resource usage data** such as memory usage, processor usage, and handles
- Gather information about **dlls** loaded, **services** running within the process, and **IP-connections** associated with processes



What's Running is a monitoring tool that gives an **inside look** into your Windows operating systems



<http://www.whatsrunning.net>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Process Monitoring Tool: What's Running

A user can use What's Running to explore processes, services, modules, IP-connections, and drivers, among others. It finds relevant information such as what modules are involved in a particular process.

Features:

- **Processes:** It inspects the processes and gives performance and resource usage data, such as memory usage, processor usage, and handles. It gives all the details about dll's that are loaded, services that are running within the process, and the IP connections for each process.
- **IP connections:** Gives information about all active IP-connections in the system. Provides a list of what remote connections each program have and find out what applications are listening for connections.
- **Services:** Inspect services that are running and stopped, find the process for services and inspect its properties.
- **Modules:** Find information about all dll's and exe's in use in the system. For each module, one can find all processes that have loaded the module. Besides, one can find the full path and immediately open the folder where the file is located.
- **Drivers:** Finds information about all drivers, for running drivers one can inspect the file version for finding the supplier of the drive.

- **Startup:** Allows management of all startup programs, regardless of the source (registry or Startup folder).
- **System information:** Shows important system information about your computer, such as installed memory, processor, registered user, operating system type, and its version.

Source: <http://www.whatsrunning.net>



Process Explorer

Source: <http://technet.microsoft.com>

Process Explorer shows information about which handles and DLLs processes have opened or loaded. The unique capabilities of Process Explorer make it useful for tracking down DLL-version problems or handle leaks, and provide insight into the way Windows and applications work.

The Process Explorer display consists of two sub-windows. The top window always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode that Process Explorer is in:

- In handle mode, one can see the handles that the process selected in the top window has opened.
- In DLL mode, one can see the DLLs and memory-mapped files that the process has loaded.

System Explorer

Source: <http://systemexplorer.net>

System Explorer is software for exploration and management of system Internals. It includes many tools, which help to keep the system under control. With System Explorer, one can get fast access to file database, which helps to determine unwanted processes or threats.

Features:

- Gives information about tasks, processes, modules, startups, IE add-ons, uninstallers, windows, services, drivers, connections, and opened files
- Checks for suspicious files via file database or the virusTotal service
- Monitors processes activities and system changes

HijackThis

Source: <http://sourceforge.net>

HijackThis is a utility that generates an in depth report of registry and file settings from the computer. It makes no separation between safe and unsafe settings in its scan results giving the ability to selectively remove items from the machine. In addition, HijackThis comes with several tools useful in manually removing malware from a computer.

Autoruns for Windows

Source: <http://technet.microsoft.com>

Autoruns for Windows has the knowledge of auto-starting locations of any startup monitor, shows what programs are configured to run during system bootup or login, and shows the entries in the order Windows processes them. These programs include ones in the startup folder, Run, RunOnce, and other Registry keys. One can configure Autoruns to show other locations, including Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, and auto-start services.

KillProcess

Source: <http://orangelampsoftware.com>

KillProcess can terminate almost any process on a Windows machine, including any service and process running in the system. It can even terminate the protected Microsoft system processes. It can kill multiple processes, either by multi-select or by use of "kill lists." Using these techniques it is possible to batch-terminate processes. It can also scan the running processes on the computer, and kill them on sight, much like an anti-spyware application would.

Security Task Manager

Source: <http://www.neuber.com>

Security Task Manager shows comprehensible information about programs and processes running on the computer. For each Windows process, it improves on Windows Task Manager, providing:

- unique security risk rating
- full directory path and file name
- process description
- CPU usage graph

- embedded hidden functions (e.g., keyboard monitoring, browser supervision, or manipulation)
- process type (e.g., visible window, systray program, DLL, IE-plugin, startup service)

Yet Another (remote) Process Monitor

Source: <http://yaprocmon.sourceforge.net>

Yet Another (remote) Process Monitor (YAPM) is an application that allows to view and manage running tasks, processes, threads, and modules, and the services on a local or on a remote machine.

MONIT

Source: <http://mmonit.com>

Monit is an open source utility for managing and monitoring UNIX systems. It conducts automatic maintenance and repair and can execute meaningful causal actions in error situations. One can use Monit to:

- Monitor daemon processes or similar programs running on local host, Monit is particularly useful for monitoring daemon processes, such as those started at system boot time from /etc/init/
- Test programs or scripts at certain times, much like cron, but in addition, you can test the exit value of a program and perform an action or send an alert if the exit value indicates an error
- Monitor files, directories, and filesystems on localhost. Monit can monitor these items for changes, such as timestamps changes, checksum changes or size changes
- Monitor general system resources on localhost such as overall CPU usage, memory, and Load Average

ESET SysInspector

Source: <http://www.eset.com>

ESET SysInspector is a diagnostic tool that helps troubleshoot a wide range of system issues. It tracks down the presence of malicious code. ESET SysInspector resolves issues related to:

- Running processes and services
- Presence of suspicious and unsigned files
- Software issues
- Hardware incompatibility
- Outdated or malfunctioning drivers
- An unpatched operating system
- Broken registry entries
- Suspicious network connections

OpManager

Source: <http://www.manageengine.com>

ManageEngine OpManager is a network and data center infrastructure management software that helps large enterprises, service providers, and SMEs manage their data centers and IT infrastructure efficiently and cost-effectively. Automated workflows, intelligent alerting engines, configurable discovery rules, and extendable templates enable IT teams to setup a “24x7” monitoring system.

Do-it-yourself plug-ins extend the scope of management to include network change and configuration management and IP address management as well as monitoring of systems, applications, databases, virtualization, and NetFlow-based bandwidth.

Dynamic Malware Analysis:
File and Folder Monitor

CHFI
Computer Hacking Forensic Investigator

You can use files and folder integrity monitoring tools to examine real-time file system and folder activity on an infected system

SIGVERIF


- It checks integrity of critical files that have been digitally signed by Microsoft
- To launch SIGVERIF, go to **Start** → **Run**, type **sigverif** and press **Enter**

FCIV

- It is a command line utility that computes **MD5** or **SHA1 cryptographic hashes** for files
- You can download FCIV at <http://download.microsoft.com>

TRIPWIRE

- It is an enterprise class system integrity verifier that **scans** and **reports critical system files for changes**



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Malware can also modify the system files and folders to save some information on them. Investigators should be able to find the files and folders which malware creates and analyze them to collect any important information stored in them. These files and folders may also contain hidden program code or malicious strings that the malware would schedule for execution on specific timing.

File Signature Verification utility also called Sigverif is a Microsoft tool that comes inbuilt in Windows 10/8/7. This tool will help investigators find unsigned drivers.

FCIV

The File Checksum Integrity Verifier (FCIV) is a command prompt utility that generates and verifies hash values of files using MD5 or SHA-1 algorithms.

The FCIV utility has the following features:

- Supports MD5 or SHA1 hash algorithms (The default is MD5.)
- Can output hash values to the console or store the hash value and file name in an XML file
- Can recursively generate hash values for all files in a directory and in all subdirectories (for example, `fciv.exe c:\ -r`)
- Supplies an exception list to specify files or directories to hash
- Can store hash values for a file with or without the full path of the file


Tripwire

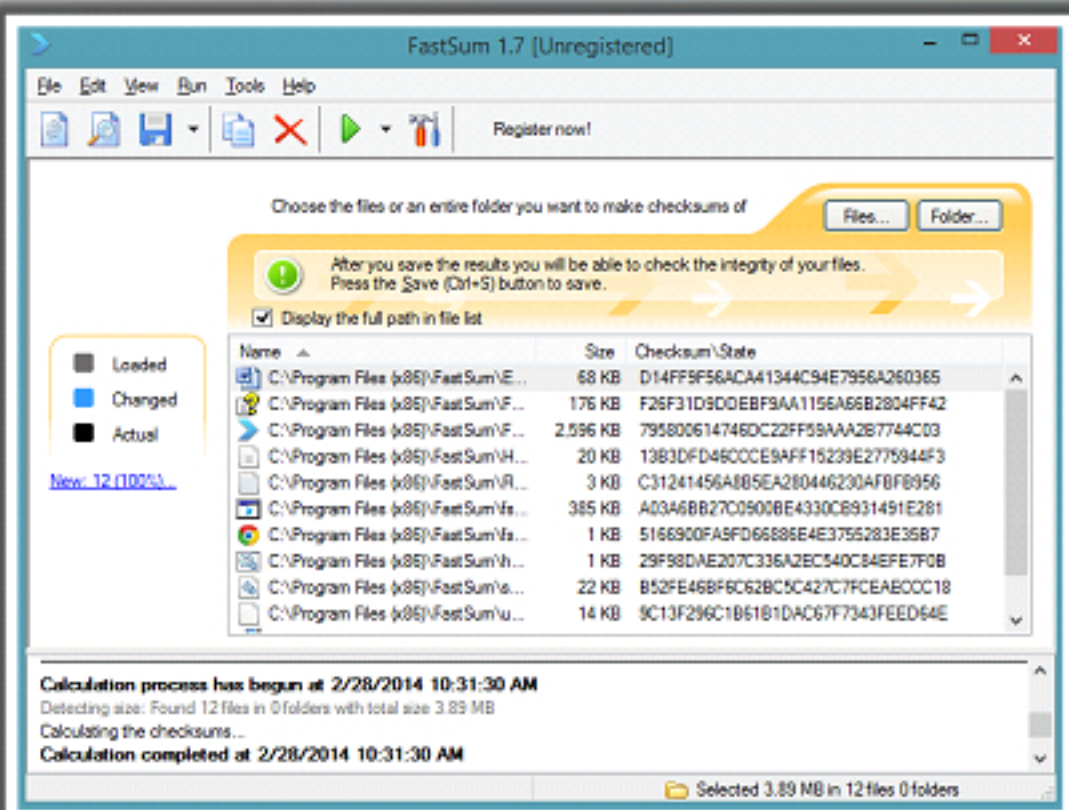
Tripwire Enterprise is a tool for assessing IT configurations and detecting, analyzing and reporting on change activity across IT infrastructure. Tripwire Enterprise can monitor servers, desktops, directory servers, hypervisors, databases, middleware applications and network devices.

Tripwire Enterprise captures a baseline of server file systems, desktop file systems, directory servers, databases, virtual systems, middleware applications and network device configurations in a known good state. Ongoing integrity checks and then compares the current states against these baselines to detect changes. While doing this, it collects information essential to the reconciliation of detected changes. It can crosscheck detected changes with either defined IT compliance policies (policy-based filtering), documented changes in tickets in a CCM system or a list of approved changes, automatically generated lists created by patch management and software provisioning tools, and against additional ChangeIQ™ capabilities. This enables it to recognize desired changes and expose undesired changes automatically.

Source: <https://www.tripwire.com>

File and Folder Integrity Checkers: FastSum and WinMD5





FastSum 1.7 (Unregistered)

Choose the files or an entire folder you want to make checksums of

After you save the results you will be able to check the integrity of your files. Press the Save (Ctrl+S) button to save.

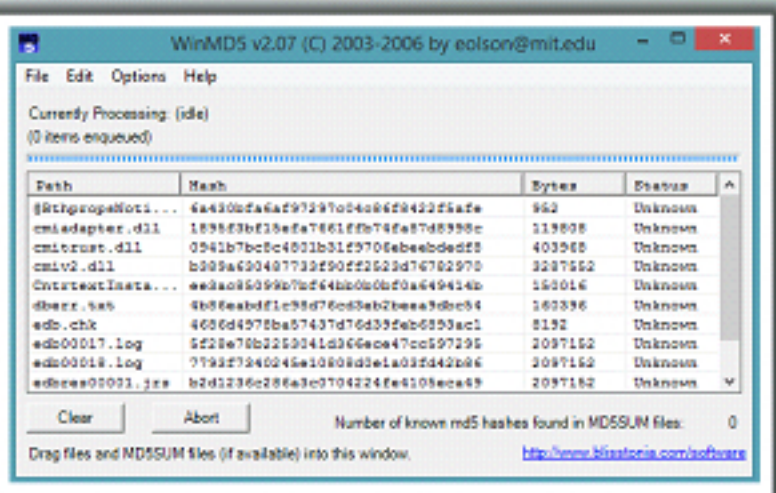
☒ Display the full path in file list

Name	Size	Checksum/State
C:\Program Files (x86)\FastSum\E...	68 KB	D14FF9F56ACA11344C94E7956A260365
C:\Program Files (x86)\FastSum\F...	176 KB	F26F31D9D0EBF9AA1156A66B2804FF42
C:\Program Files (x86)\FastSum\F...	2,596 KB	795800614746DC22FF59AA2B7744C03
C:\Program Files (x86)\FastSum\H...	20 KB	1383DFD46CCCE9AFF15239E2775944F3
C:\Program Files (x86)\FastSum\H...	3 KB	C31241456A885EA280446230A8F8956
C:\Program Files (x86)\FastSum\H...	385 KB	A03A6BB27C9008E4330C8931491E281
C:\Program Files (x86)\FastSum\H...	1 KB	5166900FA5FD66886E4E3755283E35B7
C:\Program Files (x86)\FastSum\H...	1 KB	29F98DAE207C336A2EC540C84EFE7F0B
C:\Program Files (x86)\FastSum\H...	22 KB	B52FE46BF6C62BC5C427C7FCEABCC18
C:\Program Files (x86)\FastSum\H...	14 KB	9C13F296C1B61B1DAC67F7343FEED64E

Calculation process has begun at 2/28/2014 10:31:30 AM
Detecting size: Found 12 files in 0 folders with total size 3.89 MB
Calculating the checksums...
Calculation completed at 2/28/2014 10:31:30 AM

Selected 3.89 MB in 12 files 0 folders

<http://www.fastsum.com>



WinMD5 v2.07 (C) 2003-2006 by eolson@mit.edu

Currently Processing: (idle)
(0 items enqueued)

Path	Hash	Bytes	Status
g:\cprogr\files...	6a430bfa62972970c4c64284222f4fe	962	Unknown
cmideptecr.d31	1898f3b135efa7861f8b74fa7d8998c	11908	Unknown
cmicrust.d31	0941b7b0c4001b31f9706ebebdeedf8	403968	Unknown
cmiv2.d31	b009a400407732f90f22523d76762970	3287562	Unknown
C:\text\Insta...	ee8a0609907a2f64b0b0b0a649414b	16016	Unknown
dberr.sab	4b8feabdf1c98d76d35eb2bee7dbec84	160396	Unknown
edb.chk	468d4977ba57437d76d35eb2bee7dbec84	8192	Unknown
edb00017.log	5228e70b2250341d366eae47cc597295	2097162	Unknown
edb00018.log	779327940046a10808d0e1a035d42a86	2097162	Unknown
edbeee050931.jre	b2d1236c286a3e0704224fe4108eca49	2097162	Unknown


Clear Abort

Number of known md5 hashes found in MD5SUM files: 0

Drag files and MD5SUM files (if available) into this window.

<http://www.winmd5.com>

- FastSum is used for **checking integrity** of the files
- It computes checksums according to the **MD5 checksum** algorithm



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

FastSum

Source: <http://www.fastsum.com>

FastSum, built upon the MD5 checksum algorithm, is a tool for checking the integrity of the files. FastSum computes checksums according to the MD5 checksum algorithm, which gives easy to compare and store outputs.

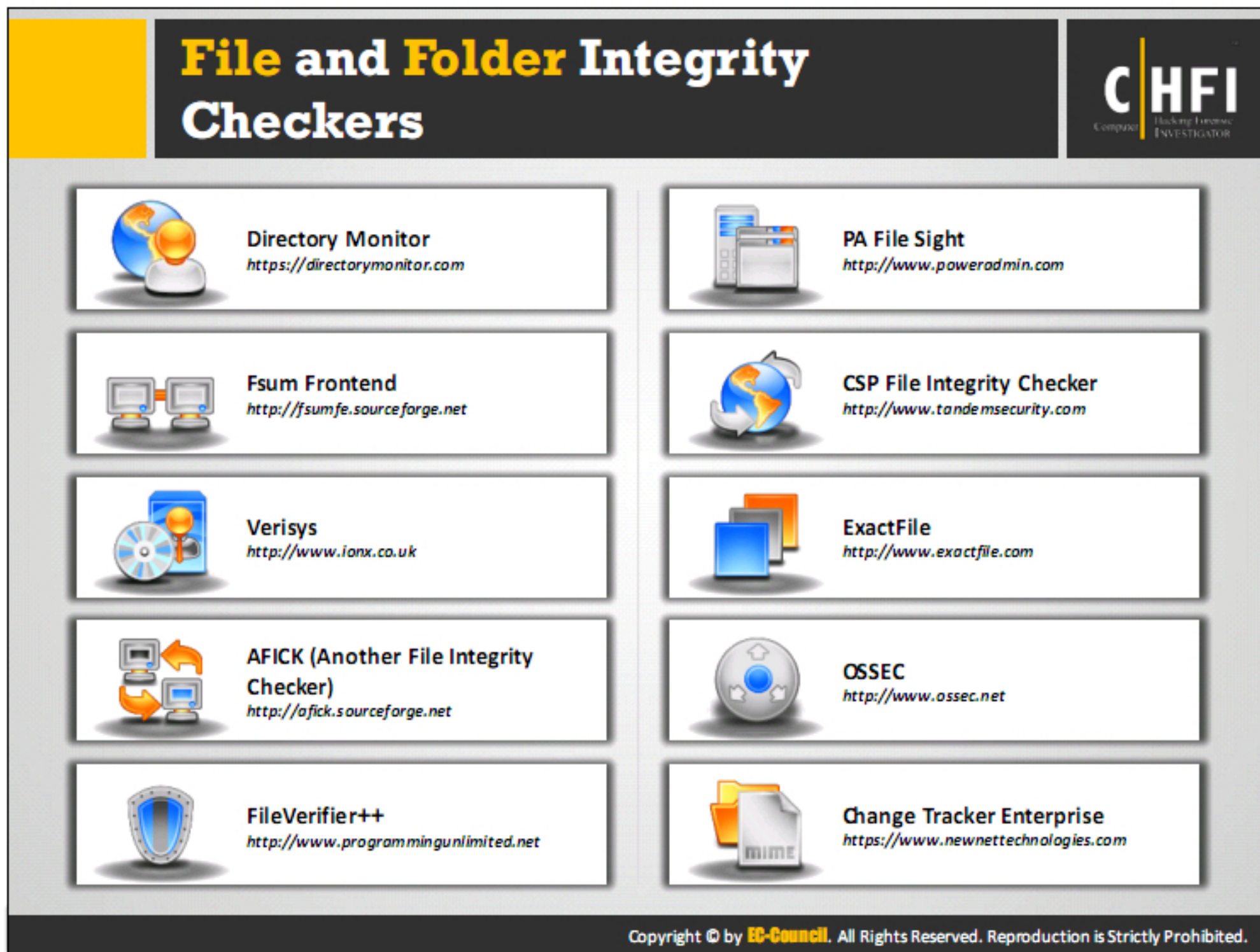
WinMD5

Source: <http://www.winmd5.com>

WinMD5Free is a utility to compute MD5 hash value for files. It works with Microsoft Windows 98, 2000, XP, 2003, Vista, 7 and later versions.

Few of its features are:

- Supports almost all Windows platforms including Microsoft Windows 95, 98, 2000, Me, XP, 2003, Vista and Windows 7
- Supports big files and low resource usage
- Supports "Drag & Drop"
- Supports verification of original MD5 value and current MD5 value
- Small size, an effective and tiny tool for data security



Directory Monitor

Source: <https://directorymonitor.com>

This tool helps in getting notified within milliseconds of file modifications, deletions, renames, new files and file access on your file system or network shares. It also helps to:

- Options to detect all files in subdirectories and changes to file attributes.
- Balloon notifications whenever an event is detected.
- Include and exclude filter patterns per directory.
- Monitor local directories or network shares including hidden/private shares.

FSUM Frontend

Source: <http://fsumfe.sourceforge.net>

Fsum Frontend is a free and easy-to-use tool that allows computing message digests checksums and HMACs for files and text strings. It supports drag-and-drop, and you can handle multiple files at once. The checksum generated can be used to verify the integrity of the files. Few of features enlisted below:

- Calculate the checksums, message digest and HMAC of files and text strings.
- Verify files using a SFV/MD5/SHA1/SHA2 file and notify you if a file is corrupted or missing.

- Verify a file containing a checksum in its name (Ex: readme[b7b9c51e].txt).
- Create a checksums file.
- Put a checksum in the file name.

Verisys

Source: <https://www.ionx.co.uk>

Verisys is file integrity monitoring solution for Windows and Linux that allows you to maintain the integrity of business critical files and data by detecting unauthorized changes. Verisys is configurable to suit your requirements using the interface and includes many templates for common systems and applications to help you get started quickly.

AFICK (Another File Integrity Checker)

Source: <http://afick.sourceforge.net>

Afick is a portable utility which acts as an aid in intrusion detection as well as helping to monitor the overall integrity of the system. It also monitors changes in the file system of your machine and reports them back to you, thereby letting you decide whether any given change was expected.

FileVerifier++

Source: <http://www.programmingunlimited.net>

FileVerifier++ is a Windows application for verifying the integrity of files. FileVerifier supports various algorithms using dynamically loadable hash libraries. It uses the Windows API and doesn't have any dependencies other than what comes with Windows (WinFVC excluded). Permanent installation is not required and may be burned to a CD or used from a flash drive. Some of its feature are listed below:

- Can load and save results to and from various formats
- Hash algorithms can be added through the dll interface
- Can load hash results and compare to what is actually on your disk
- Color coding of validity states
- Verification considers file size, file attributes, and modification date to be significant
- Drag and drop support
- Recursive directory processing
- Recursive processing using patterns
- Calculate hashes on strings
- Search and grep using regular expressions
- Selective verification

PA File Sight

Source: <https://www.poweradmin.com>

PA File Sight is a file monitoring software that will help you determine *who* is reading from and writing to important files. It can tell you when a new file or folder is created or renamed. And, with our file watcher, when a file or folder gets deleted, PA File Sight can tell you who did it and which computer they did it from (IP address and computer name).

CSP File Integrity Checker

Source: <https://www.cspsecurity.com>

CSP File Integrity Monitor provides granular monitoring of changes to specified disk files. By storing unique fingerprints for selected disk files based on particular attributes (contents, security settings etc.) and then monitoring for change, FIC enables strict compliance to security policies, including PCI-DSS regulations. Any detected changes are flagged in reports and can be used to generate alerts. Key Features:

- Monitors Guardian and OSS files.
- Meets PCI DSS regulation 11.5.
- Unique file fingerprint.
- GUI display for file management.
- Full audit reporting capability.
- Audit database of change history.
- Alerts for unauthorized change.
- Easily integrated with enterprise compliance tools.
- Easy setup and intuitive GUI.

ExactFile

Source: <http://www.exactfile.com>

ExactFile is checksum calculation that supports multiple files. ExactFile (both the console and GUI versions) fully support Unicode. ExactFile also supports extremely large files. ExactFile supports a one-step process for “stamping” a deployment folder with a checksum digest and GUI file scanner that can be burned to the CD along with the rest of your files. Run the scanner, and it will automatically start checking the integrity of the files on the CD, telling you once-and-for-all if the disc is damaged. This makes it easy for your customers and clients to find out if their disc has been damaged, or if there is some other problem that needs to be worked out.

OSSEC

Source: <http://ossec.github.io/>

OSSEC watches it all, actively monitoring all aspects of UNIX system activity with file integrity monitoring, log monitoring, root check, and process monitoring. With OSSEC you won't be in the dark about what is happening to your valuable computer system assets. When attacks


happen, OSSEC lets you know through alert logs and email alerts sent to you and your IT staff so you can take quick actions. OSSEC also exports alerts to any SIEM system via syslog so you can get real-time analytics and insights about your system security events.

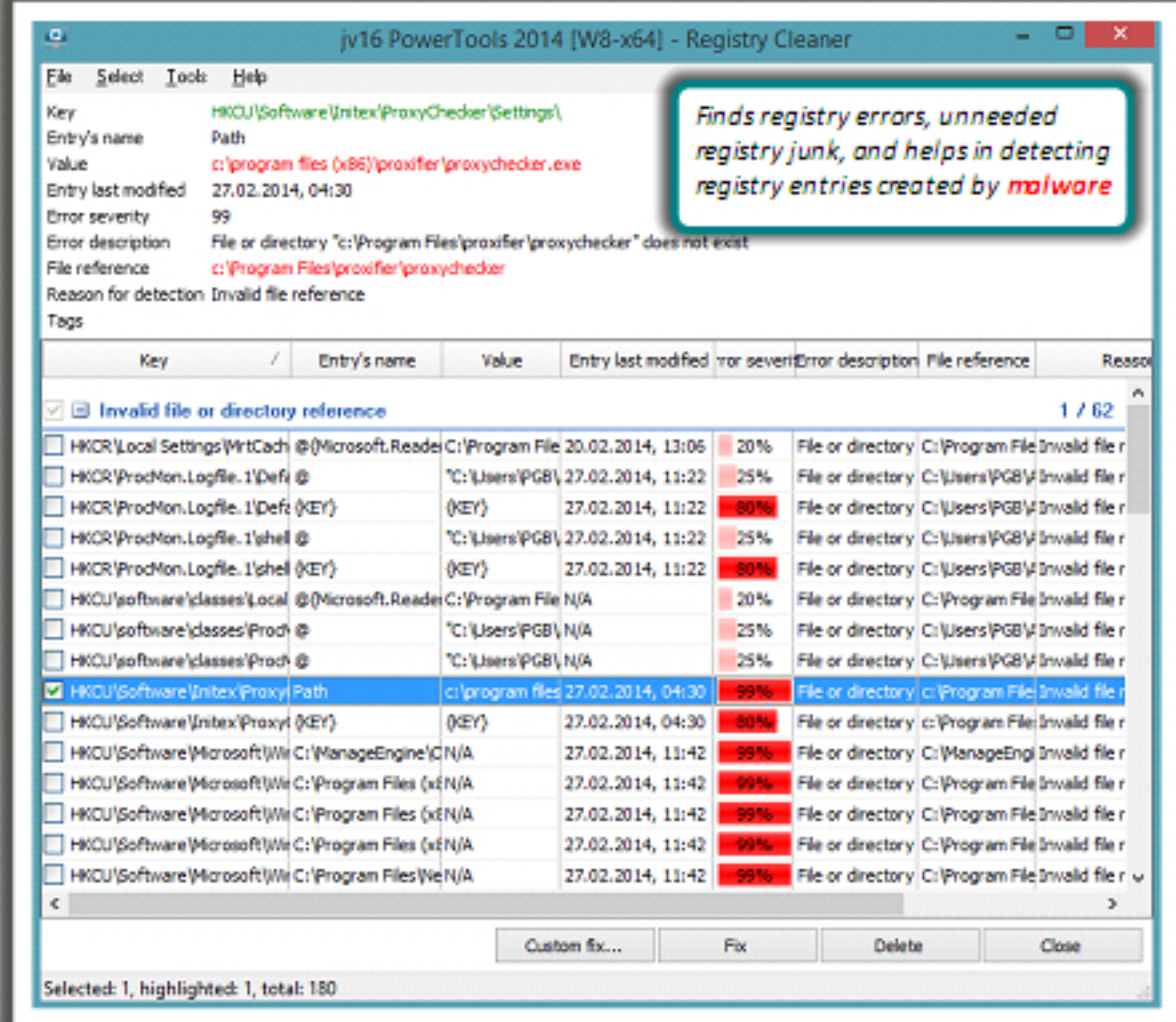
Change Tracker Enterprise

Source: <https://www.newnettechnologies.com>

Change Tracker is a system integrity monitoring tool used for real-time breach detection. Closed-Loop Intelligent Change Control (CLICC) reconciles the benefits of forensic-level change control with the hitherto onerous workload associated of reviewing and acknowledging reported changes. Change Tracker learns the difference between good and bad changes, automatically promoting legitimate changes to Planned Changes, leaving behind only potentially harmful, unplanned changes for review.

You can use registry entry monitoring tools to examine the changes made to the system's registry by suspect program





<http://www.macecraft.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows registry stores OS and program configuration details, such as settings and options. If the malware is a program, the registry stores its functionality. The malware uses the registry to perform harmful activity continuously by storing entries into the registry and ensuring that the malicious program run whenever computer or device boots automatically.

Investigators should have a fair knowledge of the Windows registry, its contents, and working to analyze the presence of malware. Registry contains:

Root keys: These are the predefined handles to specific keys at the root level of the hierarchical database and named by their Windows API definitions.

The registry contains the following root keys:

Root Key	Description of Contents
HKEY_LOCAL_MACHINE (HKLM)	Stores local machine's global settings
HKEY_CURRENT_USER (HKCU)	Contains current user's specific settings
HKEY_CLASSES_ROOT	Description for files including types and extensions
HKEY_CURRENT_CONFIG	Contains current hardware configuration
HKEY_USERS	Defines settings for the default users

TABLE 11.2: Root Keys

Note: Making changes to the registry would damage the OS and cease the working of a system.

Regedit

The Registry Editor (Regedit) is a built-in Windows tool that allows users to view and edit the registry. It displays the open subkeys and value entries in each subkey. Malware writes programs to the Run subkey of the registry to automatically run the code or launch the malware itself automatically.

Registry Functions


The malware uses registry functions to alter the registry configuration and run automatically when the system boots. Most commonly used registry functions include:


- **RegOpenKeyEx:** Opens a registry for editing and querying
- **RegSetValueEx:** Adds a new value to the registry
- **RegGetValue:** Returns the data for a value entry in the registry
- **RegDisablePredefinedCache:** Disables handle caching for the predefined registry handle for HKEY_CURRENT_USER for the current process
- **RegOpenKeyEx:** Opens the specified registry key

Investigators should use registry monitoring tools such as Registry Cleaner and RegScanner to identify and track changes to the registry entries. Some of the tools can also detect and display errors in the registry.

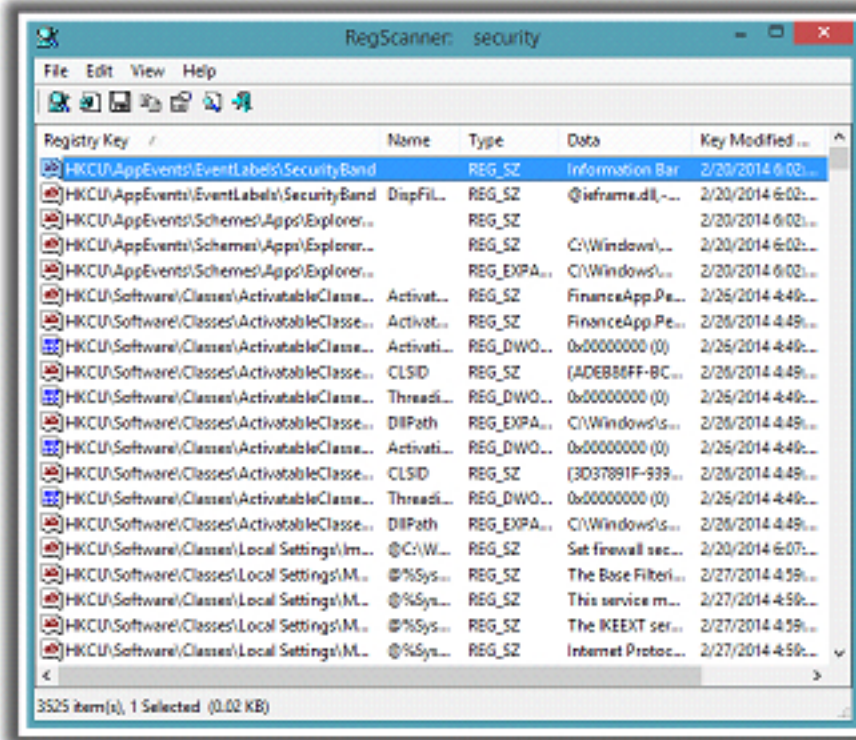
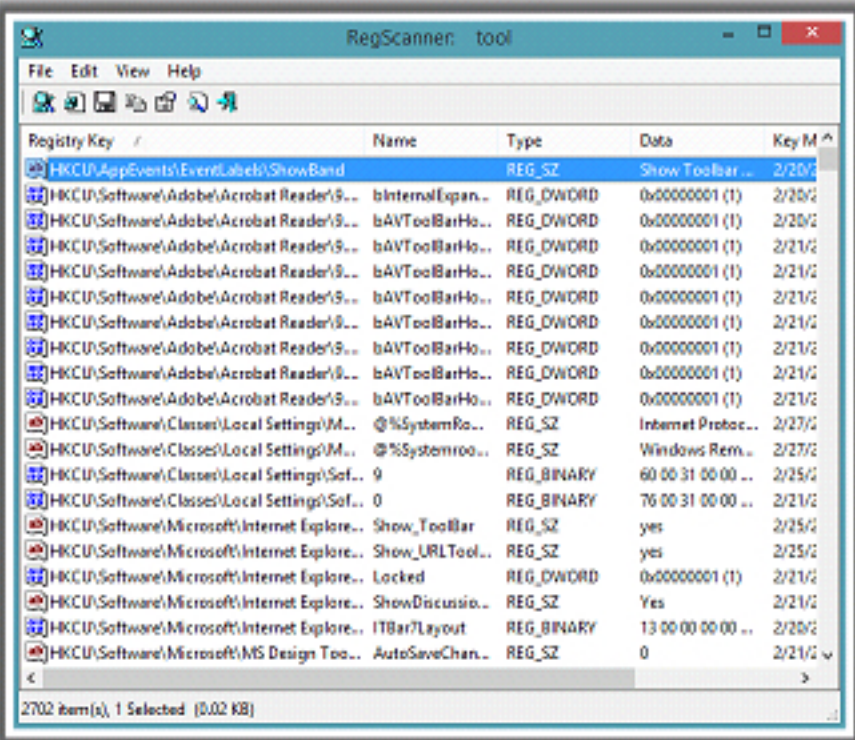
Registry Cleaner is part of the jv16 PowerTools, which detects errors and unneeded that can have a measurable adverse effect on general system performance.

Registry Entry Monitoring Tool: RegScanner





RegScanner allows you to scan the Registry, find the desired Registry values that match to the specified search criteria, and display them in one list



<http://www.nirsoft.net>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

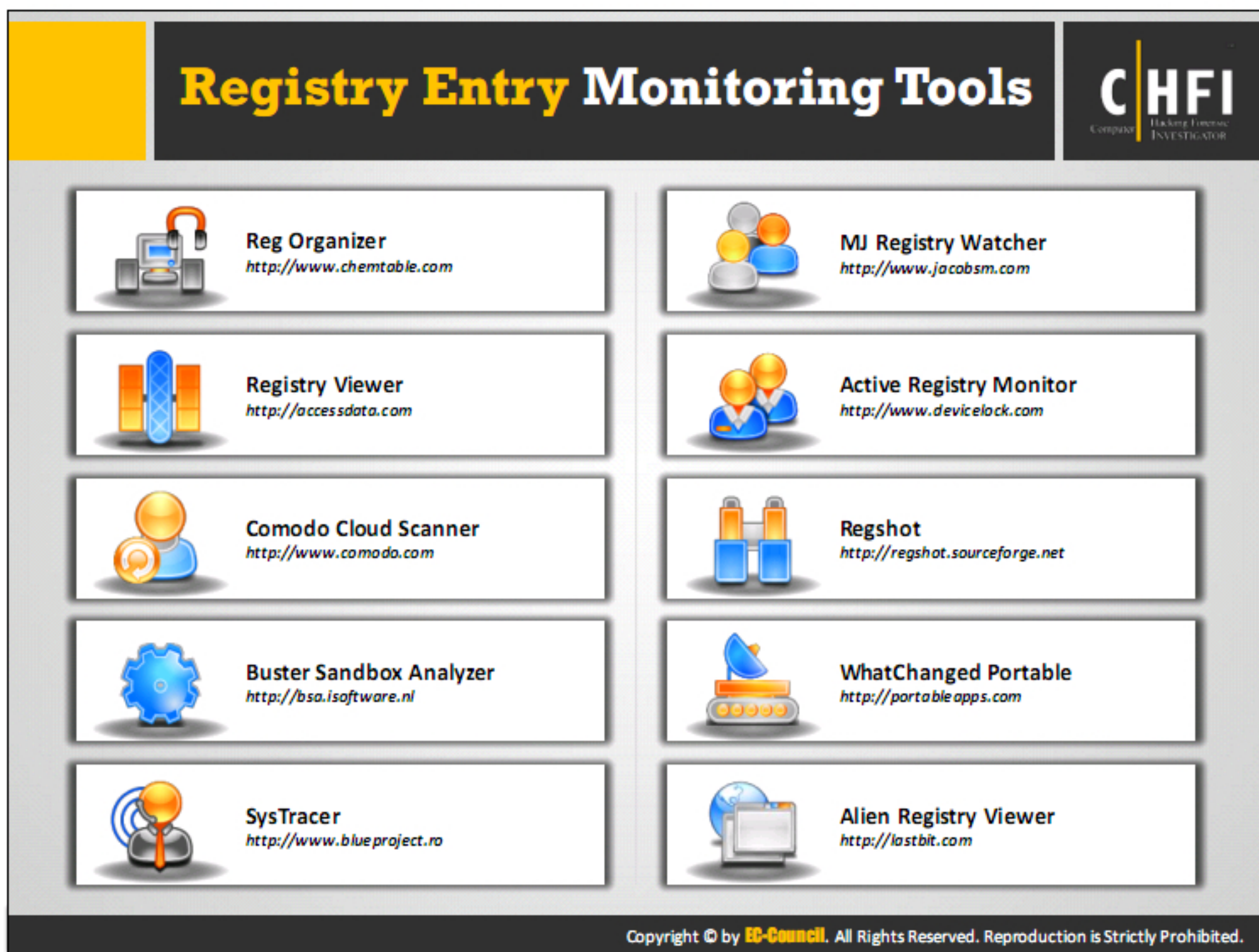
RegScanner

RegScanner is a utility that allows you to scan the Registry, find the desired Registry values that match the specified search criteria, and display them in one list. After finding the Registry values, you can jump to the right value in RegEdit by double-clicking the desired Registry item. You can also export the found Registry values into a .reg file that can be used in RegEdit.

Advantages over RegEdit find of Windows

- RegScanner allows you to make a case sensitive search
- While scanning the Registry, RegScanner displays the current scanned Registry key, as opposed to RegEdit, that simply display a boring "Searching the registry" dialog-box
- Standard string search (Like in RegEdit), RegScanner can also find Registry values by data length, value type (REG_SZ, REG_DWORD, and so on), and by modified date of the key
- RegScanner can find a unicode string

Source: <http://www.nirsoft.net>



Reg Organizer

Source: <http://www.chemtable.com/organizer.htm>

Reg Organizer is a set of tools to tweak, optimize, and clean Windows, designed to free up system resources and rev performance to the max. The set includes a visual autostart manager, an advanced uninstaller featuring search for leftovers of the uninstalled programs in the system, functions to purge unnecessary data, a powerful registry editor to quickly search and replace keys and data quickly, and much more – all to keep your system healthy.

Registry Viewer

Source: <http://www.gaijin.at/en/dlreqview.php>

Registry Viewer allows you to view the contents of Windows® operating system registries. Registry Viewer lets you view registry files from any computer. Registry Viewer gives you access to a registry's protected storage. The protected storage can contain passwords, usernames, and other information that is not accessible in Windows Registry Editor.

Comodo Cloud Scanner

Source: <https://www.comodo.com>

Comodo Cloud Scanner (CCS) is a system scanning tool that identifies malware, viruses, suspicious processes and other problems with your computer. Apart from identifying the viruses and malware, CCS also identifies other problems like Windows Registry errors that

cause system instability, issues that threaten your privacy and junk or garbage files that occupy your valuable disk space.

Buster Sandbox Analyzer

Source: <http://bsa.isoftware.nl>

Buster Sandbox Analyzer is a tool that has been designed to analyze the behavior of processes and the changes made to the system and then evaluate if they are malware suspicious.

SysTracer

Source: <http://www.blueproject.ro>

SysTracer is a system utility tool that can scan and analyze your computer to find changed (added, modified or deleted) data into registry and files. SysTracer can scan your system and record information about changed files and folders, modified registry entries, installed programs, etc.

MJ Registry Watcher

Source: <http://www.jacobsm.com>

MJ Registry Watcher is a registry, file and directory hooker that safeguards the most important startup files, registry keys and values, and other registry locations commonly attacked by trojans.

Active Registry Monitor

Source: <http://www.devicelock.com>

Active Registry Monitor (ARM) is a utility designed for analyzing the changes made to Windows registry - by making the "snapshots" of it and keeping them in the browsable database. You can compare any two snapshots and get the list of keys/data which are new, deleted or just changed. ARM can do comparing not only in the entire registry but also in any key of the registry.

Regshot

Source: <https://sourceforge.net>

Regshot is an open-source (LGPL) registry compare utility that allows you to take a snapshot of your registry quickly and then compare it with a second one - done after doing system changes or installing a new software product.

Whatchanged Portable

Source: <http://portableapps.com>

WhatChanged is a system utility that scans for modified files and registry entries. It is useful for checking program installations. There are two steps for using WhatChanged:

- First, take a snapshot to get the current state of the computer
- Second, run it again to check the differences since the previous snapshot

WhatChanged uses the 'brute force method' to check files and the registry.

Alien Registry Viewer

Source: <http://lastbit.com>

Alien Registry Viewer is similar to the RegEdit application included into Windows, but unlike RegEdit, it works with standalone registry files. While RegEdit shows the contents of the system registry, Alien Registry Viewer works with registry files copied from other computers. Alien Registry Viewer can be extremely useful for system administration and forensic computer examination purposes.

**Dynamic Malware Analysis:
Network Activity Monitor**

CHFI
Computer Hacking Forensic Investigator

01

You can use tools such as **Wireshark**, **Capsa Network Analyzer**, etc. to monitor and capture live network traffic to and from the victim system during execution of the suspect program

02

Analyzing network traffic reveals **network capabilities** of the suspect program and its requirements


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Malware depends on the network for various activities such as propagation, downloading malicious content, transmitting sensitive files and information, offering a remote control to attackers, etc. Therefore, investigators should adopt techniques that can detect the malware artifacts and usage across networks.

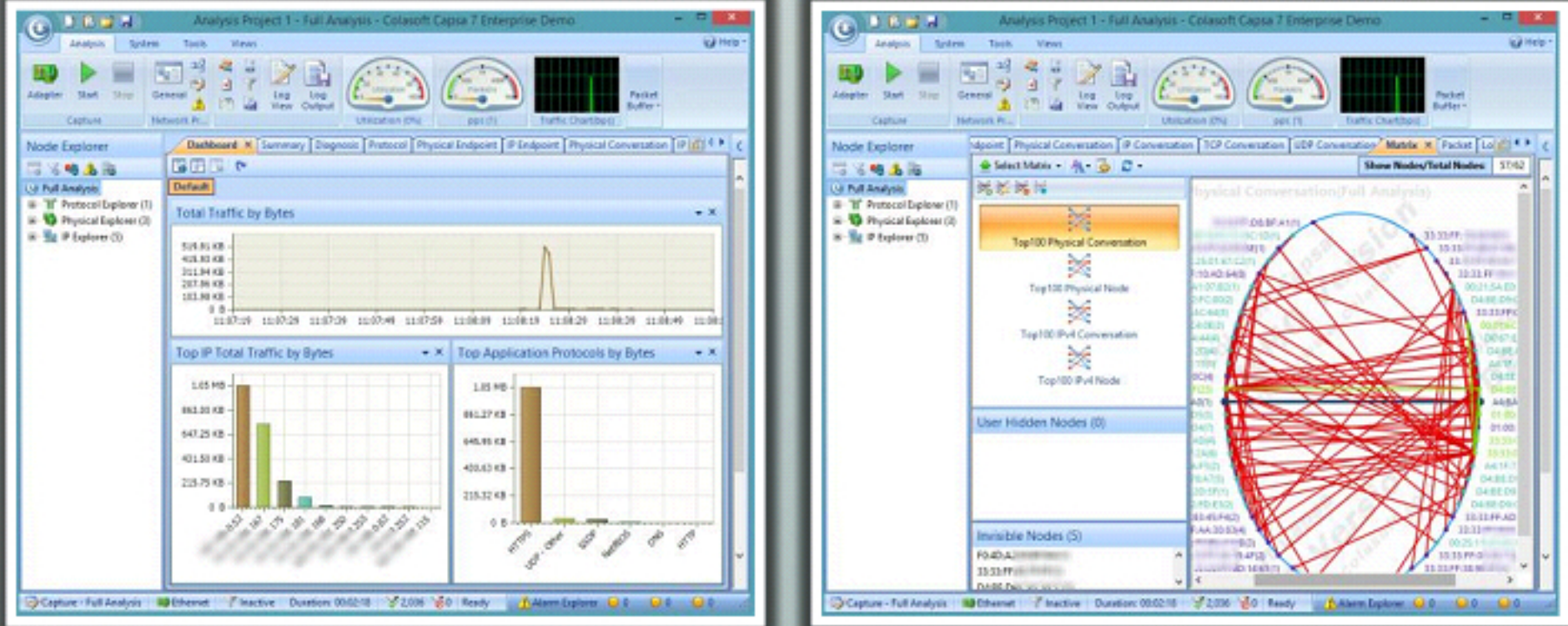
In dynamic analysis, the investigators run malware in a controlled environment installed with various network monitoring tools to trace all the networking activities of malware. Investigators use tools such as Wireshark, Capsa Network Analyzer, etc. to monitor and capture live network traffic to and from the victim system during execution of the suspect program. This will help investigators understand malware's network artifacts, signatures, functions and other elements.

Network analysis is the process of capturing the network traffic and investigating it carefully to determine the malware activity. It helps to find the type of traffic/network packets or data transmitted across the network.

Detecting Trojans and Worms with Capsa Network Analyzer



Capsa is an intuitive network analyzer, which provides detailed information to help check for any **Trojan** activities in a network



<http://www.colasoft.com>


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


Capsa Network Analyzer

Capsa is a portable network analyzer application for both LANs and WLANs, which performs real-time packet capturing capability, 24x7 network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis. Capsa's window view of the entire network gives quick insight to network administrators or network engineers allowing them to pinpoint and resolve application problems rapidly. Capsa performs network monitoring, troubleshooting, and analysis for both wired & wireless networks including 802.11a/b/g/n.


Source: <http://www.colasoft.com>

Dynamic Malware Analysis: Port Monitor






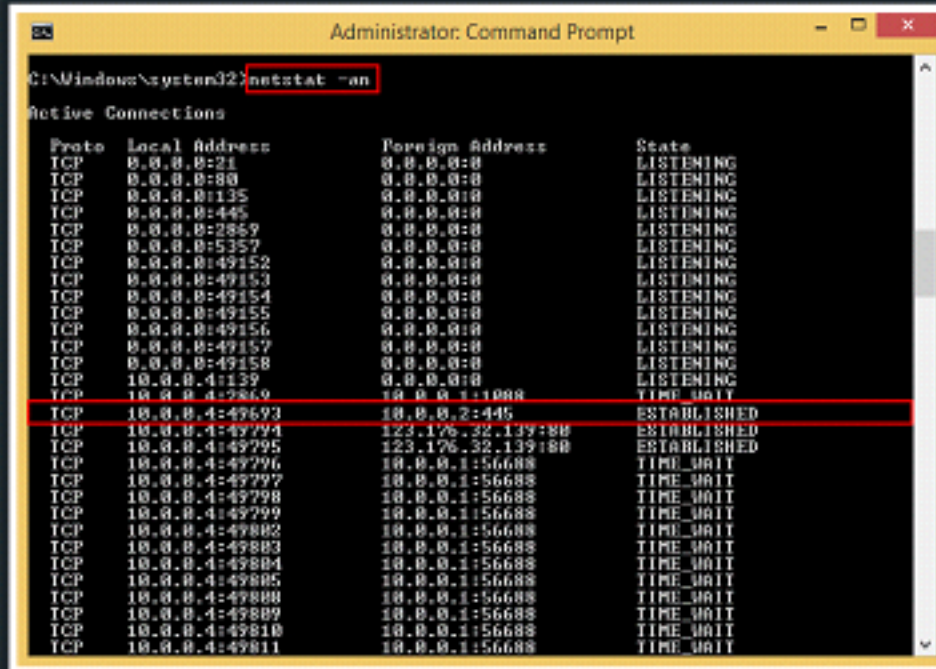
You can use tools such as CurrPorts, PortMon, SysAnalyzer, TCP View, etc., to monitor live open ports on the infected system and the remote system port numbers that are requested by the infected system while trying to connect to an email server



It reveals the network capabilities of the suspected program
Ex: Requesting remote system port number 25 implies Simple Mail Transfer Protocol



You can type 'netstat -an' in the command prompt to look for connection established to unknown or suspicious IP addresses



Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2869	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49157	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49158	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1139	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2869	0.0.0.0:13988	TIME_WAIT
TCP	0.0.0.0:49693	0.0.0.0:445	ESTABLISHED
TCP	0.0.0.0:49774	123.176.32.139:80	ESTABLISHED
TCP	0.0.0.0:49775	123.176.32.139:80	ESTABLISHED
TCP	0.0.0.0:49776	0.0.0.0:15668	TIME_WAIT
TCP	0.0.0.0:49777	0.0.0.0:15668	TIME_WAIT
TCP	0.0.0.0:49778	0.0.0.0:15668	TIME_WAIT
TCP	0.0.0.0:49779	0.0.0.0:15668	TIME_WAIT
TCP	0.0.0.0:49802	0.0.0.0:15668	TIME_WAIT
TCP	0.0.0.0:49803	0.0.0.0:15668	TIME_WAIT
TCP	0.0.0.0:49804	0.0.0.0:15668	TIME_WAIT
TCP	0.0.0.0:49805	0.0.0.0:15668	TIME_WAIT
TCP	0.0.0.0:49806	0.0.0.0:15668	TIME_WAIT
TCP	0.0.0.0:49807	0.0.0.0:15668	TIME_WAIT
TCP	0.0.0.0:49808	0.0.0.0:15668	TIME_WAIT
TCP	0.0.0.0:49809	0.0.0.0:15668	TIME_WAIT
TCP	0.0.0.0:49810	0.0.0.0:15668	TIME_WAIT
TCP	0.0.0.0:49811	0.0.0.0:15668	TIME_WAIT

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Malware programs corrupt the system and open system input/output ports to establish the connection with remote systems, networks or servers to accomplish various malicious tasks. These open ports can also form backdoor for other harmful malware and program.

Investigators can find if malware is trying to access particular port during dynamic analysis by installing port monitoring tools. Some such tools include CurrPorts, PortMon, SysAnalyzer, TCP View, etc., and command line utility called netstat.

The port monitoring tools will offer details such as the protocol used, local address, remote address and state of the connection. Additional features may include process name, process ID, remote connection protocol, etc.

Netstat

Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, netstat displays active TCP connections.

Syntax

```
netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
```


Parameters

- **-a:** Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
- **-e:** Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.
- **-n:** Displays active TCP connections, however, addresses and port numbers are expressed numerically, and no attempt is made to determine names.
- **-o:** Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.
- **-p Protocol:** Shows connections for the protocol specified by Protocol. In this case, the Protocol can be tcp, udp, tcpv6, or udpv6. If this parameter is used with -s to display statistics by protocol, Protocol can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6.
- **-s:** Displays statistics by the protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The -p parameter can be used to specify a set of protocols.
- **-r:** Displays the contents of the IP routing table. This is equivalent to the route print command.

In the image, the command netstat -an displays all the active TCP connections as well as the TCP and UDP ports on which the computer is listening along with addresses and port numbers.

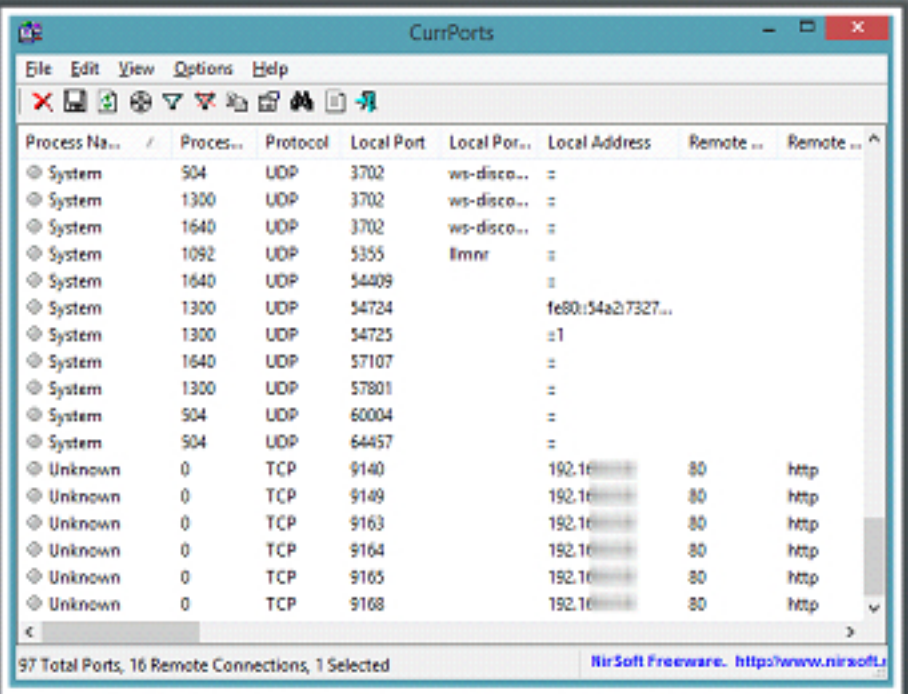
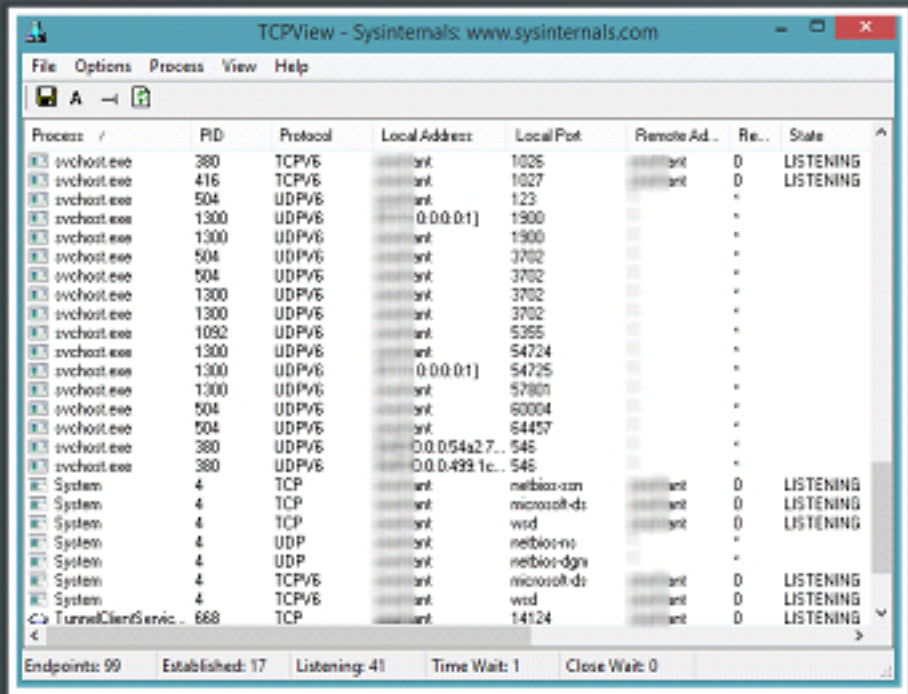
Port Monitoring Tools: TCPView and CurrPorts

TCPView

TCPView shows a detailed listings of all **TCP** and **UDP endpoints** on your system, including the local and remote addresses and state of **TCP connections**

CurrPorts

CurrPorts is a **network monitoring** software that displays the list of all currently opened **TCP/IP** and **UDP** ports on your local computer



<http://technet.microsoft.com>

<http://www.nirsoft.net>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

TCPView

Source: <https://technet.microsoft.com>

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ship with Windows. The TCPView download includes Tcpcvcon, a command-line version with the same functionality.

Currports

Source: <http://www.nirsoft.net>

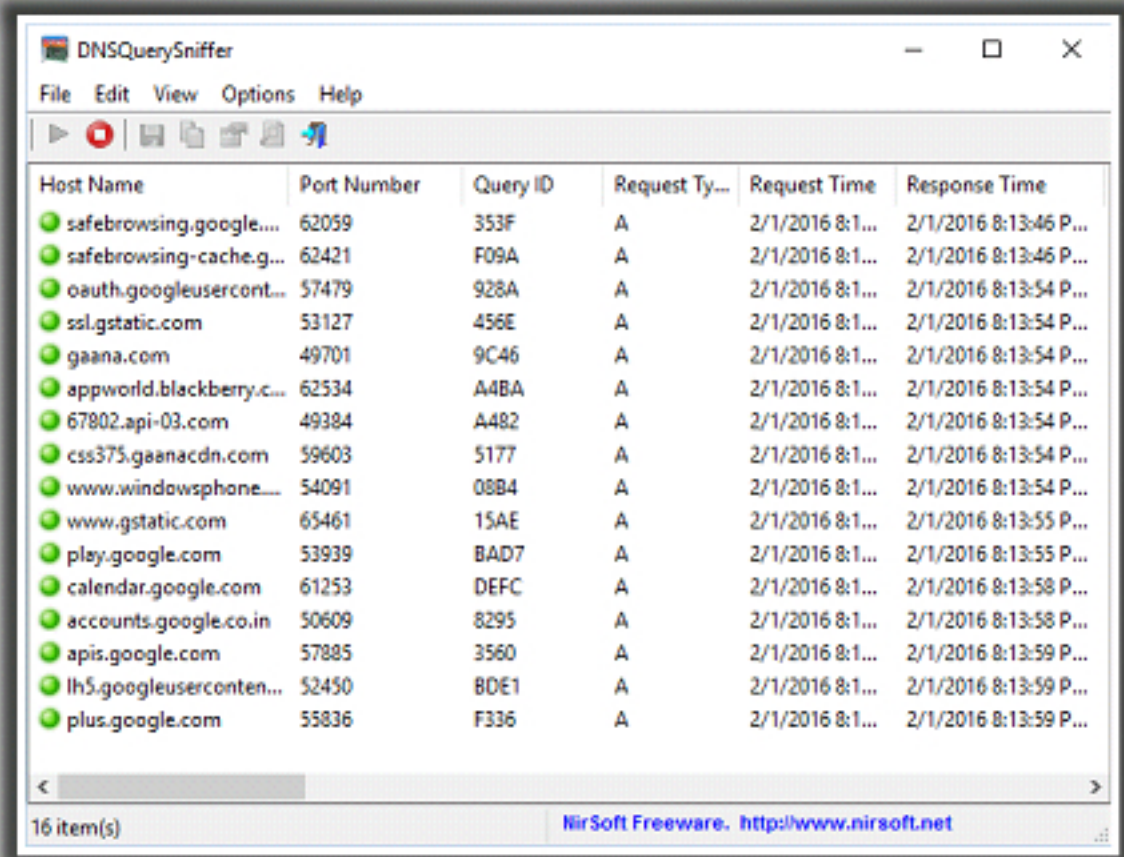
CurrPorts is network monitoring software that displays the list of all currently opened TCP/IP and UDP ports on your local computer. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, and so on), the time that the process was created, and the user that created it.

In addition, CurrPorts allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP ports information to HTML file, XML file, or to tab-delimited text file. CurrPorts also automatically mark with pink color suspicious TCP/UDP ports owned by unidentified applications (Applications without version information and icons)

**Dynamic Malware Analysis:
DNS Monitoring/Resolution**

CHFI
Computer Hacking Forensic Investigator

You can use tools such as **DNSstuff**, **DNSQuerySniffer**, etc. to verify the DNS servers malware try to connect and to identify the **type of connection**



The screenshot shows the DNSQuerySniffer application window. It has a menu bar (File, Edit, View, Options, Help) and a toolbar with icons for play, stop, save, print, and help. Below the toolbar is a table with the following columns: Host Name, Port Number, Query ID, Request Ty..., Request Time, and Response Time. The table contains 16 rows of data, all with a request type of 'A'. The status bar at the bottom indicates '16 item(s)' and provides the NirSoft Freeware website URL.

Host Name	Port Number	Query ID	Request Ty...	Request Time	Response Time
safebrowsing.google...	62059	353F	A	2/1/2016 8:1...	2/1/2016 8:13:46 P...
safebrowsing-cache.g...	62421	F09A	A	2/1/2016 8:1...	2/1/2016 8:13:46 P...
oauth.googleusercontent...	57479	928A	A	2/1/2016 8:1...	2/1/2016 8:13:54 P...
ssl.gstatic.com	53127	456E	A	2/1/2016 8:1...	2/1/2016 8:13:54 P...
gaana.com	49701	9C46	A	2/1/2016 8:1...	2/1/2016 8:13:54 P...
appworld.blackberry.c...	62534	A4BA	A	2/1/2016 8:1...	2/1/2016 8:13:54 P...
67802.api-03.com	49384	A482	A	2/1/2016 8:1...	2/1/2016 8:13:54 P...
css375.gaanacdn.com	59603	5177	A	2/1/2016 8:1...	2/1/2016 8:13:54 P...
www.windowsphone...	54091	08B4	A	2/1/2016 8:1...	2/1/2016 8:13:54 P...
www.gstatic.com	65461	15AE	A	2/1/2016 8:1...	2/1/2016 8:13:55 P...
play.google.com	53939	BAD7	A	2/1/2016 8:1...	2/1/2016 8:13:55 P...
calendar.google.com	61253	DEFC	A	2/1/2016 8:1...	2/1/2016 8:13:58 P...
accounts.google.co.in	50609	8295	A	2/1/2016 8:1...	2/1/2016 8:13:58 P...
apis.google.com	57885	3560	A	2/1/2016 8:1...	2/1/2016 8:13:59 P...
lh5.googleusercontent...	52450	BDE1	A	2/1/2016 8:1...	2/1/2016 8:13:59 P...
plus.google.com	55836	F336	A	2/1/2016 8:1...	2/1/2016 8:13:59 P...

16 item(s) NirSoft Freeware. <http://www.nirsoft.net>

<http://www.nirsoft.net>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Malicious software called DNSChanger is capable of changing the systems' DNS server settings and provides the attackers with control to the victims' DNS servers. Using this control, the attackers can control the sites user tries to connect to the Internet and also make the victim connect to a fraudulent website or interfere the online web browsing.

Therefore, investigators should check if the malware is capable of changing any DNS server settings while performing dynamic analysis. They can use tools such as DNSstuff, DNSQuerySniffer, etc. to verify the DNS servers' malware try to connect and to identify the type of connection.

DNSQuerySniffer

DNSQuerySniffer is a network sniffer utility that shows the DNS queries sent on your system. For every DNS query, the following information is displayed: Host Name, Port Number, Query ID, Request Type (A, AAAA, NS, MX, and so on), Request Time, Response Time, Duration, Response Code, Number of records, and the content of the returned DNS records.

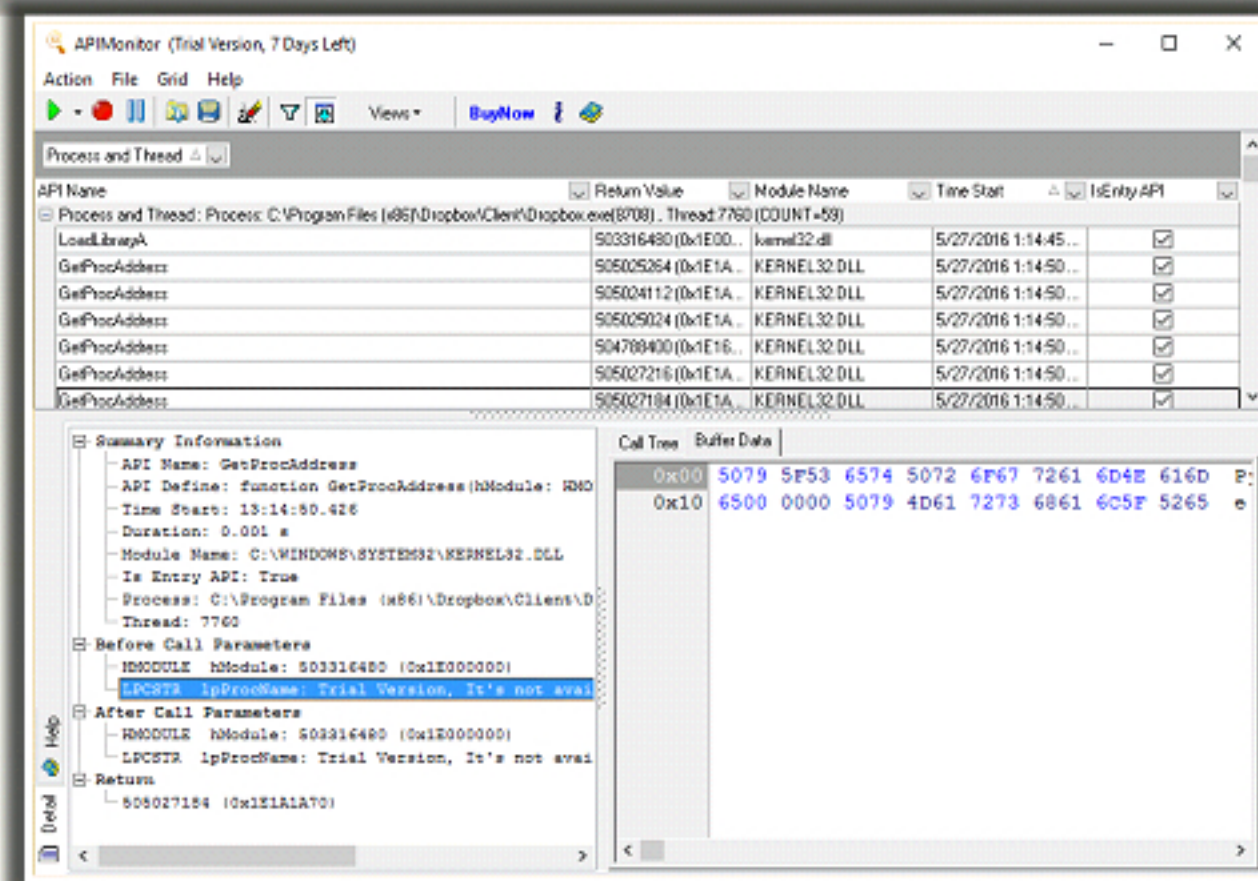
You can easily export the DNS queries information to csv/tab-delimited/xml/html file, or copy the DNS queries to the clipboard, and then paste them into Excel or other spreadsheet application.

Source: <http://www.nirsoft.net>

Dynamic Malware Analysis: API Calls Monitor



- You can use tools such as **API Monitor** to intercept the API calls from the suspected program to the OS
- Analyzing the API calls may reveal the suspected program's interaction with the OS, which is of investigative value (may provide correlative clues regarding system and network activity)



<http://www.apimonitor.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Application programming interfaces (APIs) are parts of the Windows OS that allow external applications to access operating system information such as file systems, threads, errors, registry, kernel, buttons, mouse pointer, network services, web, and the internet, etc. Malware programs also make use of these APIs to access the operating system information.

Investigators need to gather the APIs related to the malware programs and analyze them to reveal its interaction with the operating system as well as the activities it has been performing over the system. Use tools such as API monitor.

API Monitor

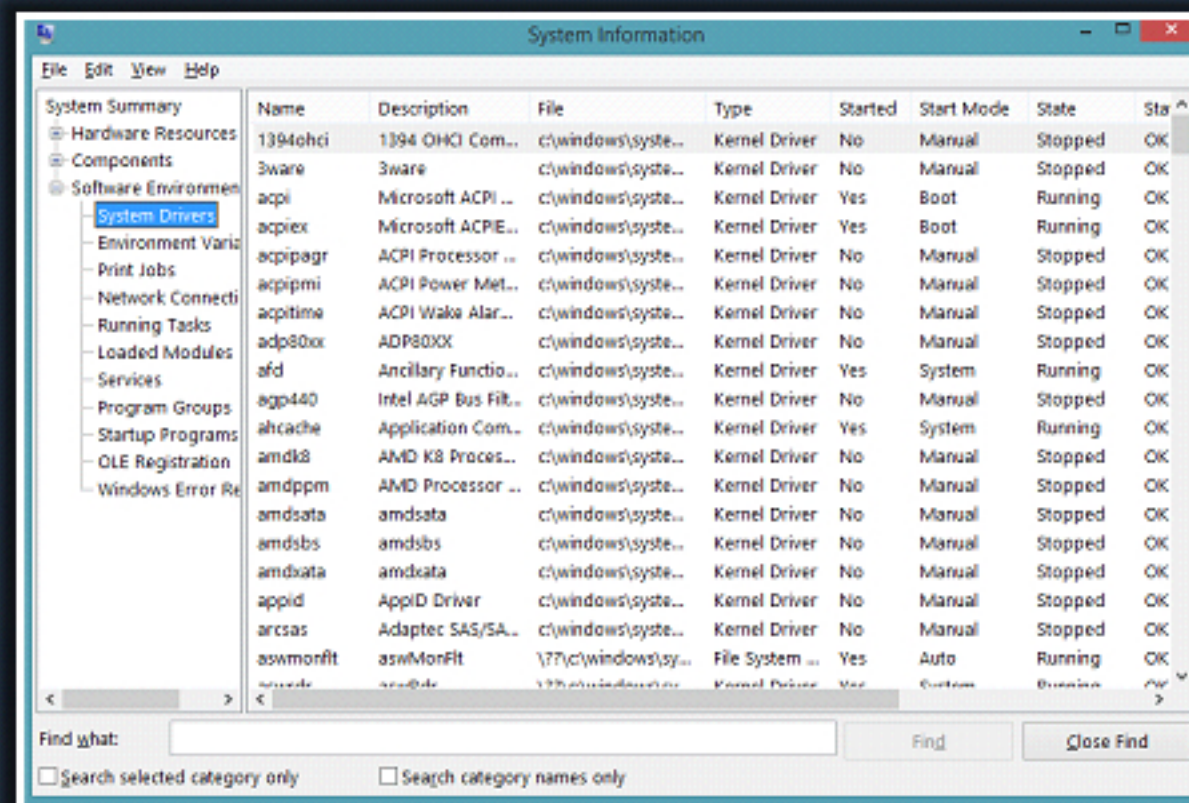
API Monitor is a software that allows you to spy and display Win32 API calls made by applications. It can trace any exported APIs and displays a wide range of information, including function name, call sequence, input and output parameters, function return value and more. It's a useful developer tool for seeing how win32 applications work and learn their tricks.

Source: <http://www.apimonitor.com>

Dynamic Malware Analysis: Device Drivers Monitor



- Malware gets installed along with device drivers **downloaded from untrusted sources** and use these as shield to avoid detection
- You have to scan for **suspicious device drivers** and verify if they are genuine and downloaded from the publisher's original site
- Go to **Run** → **Type msinfo32** → **Software Environment** → **System Drivers**

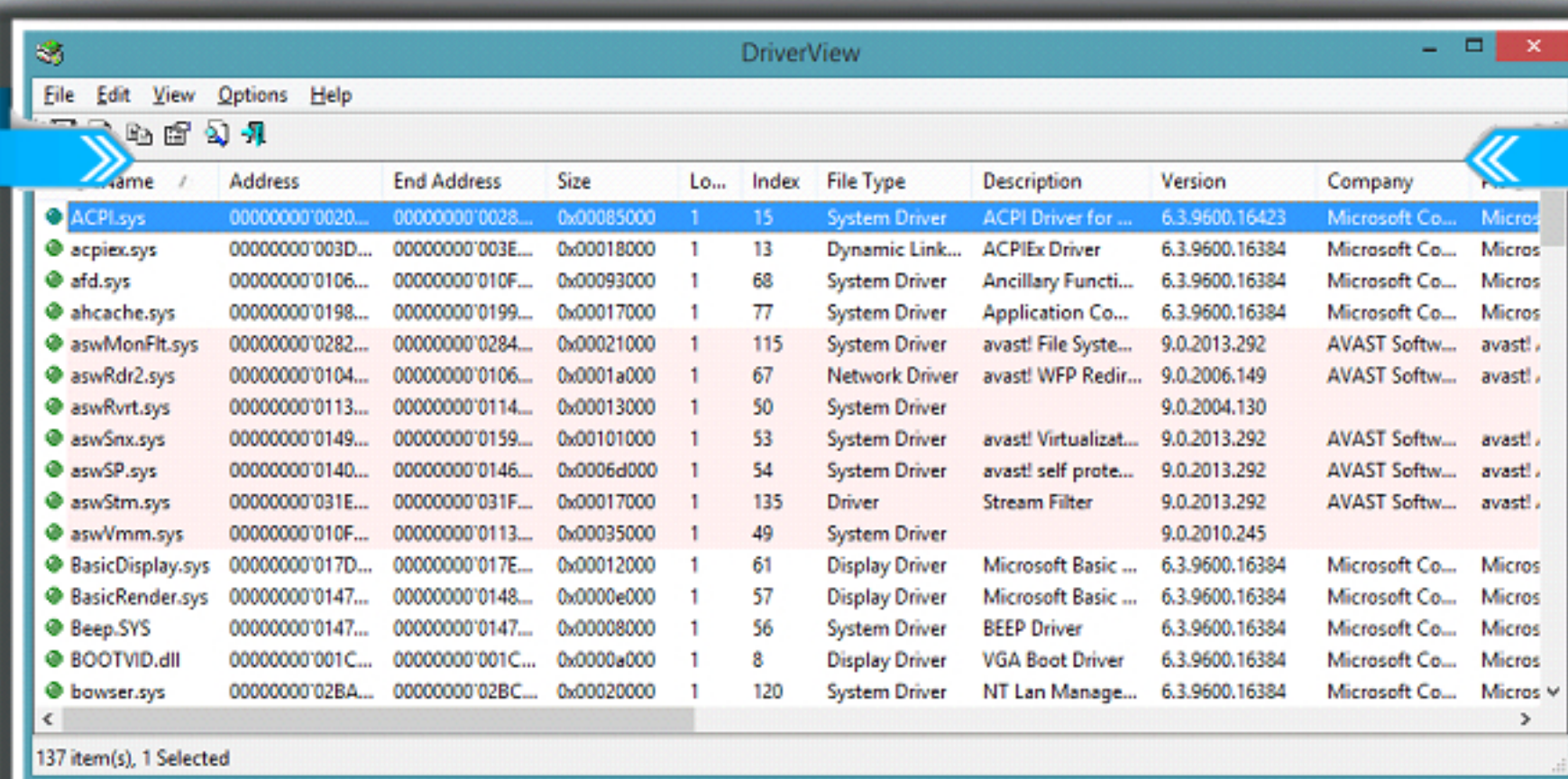


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Device Drivers Monitoring Tool: DriverView














DriverView utility displays a list of all **device drivers** currently loaded on the system. For each driver in the list, **additional information** is displayed such as load address of the driver, description, version, product name, and the company that created the driver, etc.

<http://www.nirsoft.net>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Device Drivers Monitoring Tools



 Driver Detective http://www.drivershq.com	 Driver Reviver http://www.reviversoft.com
 Unknown Device Identifier http://www.zhangduo.com	 ServiWin http://www.nirsoft.net
 DriverGuide Toolkit http://www.driverguidetoolkit.com	 Driver Fusion https://treexy.com
 InstalledDriversList http://www.nirsoft.net	 My Drivers http://www.zhangduo.com
 Driver Magician http://www.drivemagician.com	 DriverEasy http://www.drivereasy.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Driver Detective

Source: <http://www.drivershq.com>

Driver Detective removes guesswork in resolving driver problems by providing instant access to the most relevant content for your computer's hardware.

Features:

- Scans your PC to determine the manufacturer, family, model, and motherboard
- Easy Migrator will automatically scan your computer's hardware, download all of the latest drivers for any destination operating system that you choose, and then creates a device-driver migration CD
- Ensures that the downloads do not contain viruses
- Possess tools necessary to keep the computer running at its best
- Provides accurate recommendations for user's computer
- Has a built-in wizard that allows you to copy (backup) your downloaded drivers to a CD, network drive, or USB flash drive

Unknown Device Identifier

Source: <http://www.zhangduo.com>

Unknown Device Identifier enables one to identify the yellow question mark labeled “Unknown Devices in Device Manager.” It reports a detailed summary for the manufacturer name, OEM name, device type, device model and even the exact name of the unknown devices. With the collected information, one might contact the hardware manufacturer for support or search the Internet for the corresponding driver.

DriverGuide Toolkit

Source: <http://www.driverguidetoolkit.com>

DriverGuide Toolkit identifies and lists drivers installed on the computer and when connected to the Internet, allows one to search DriverGuide.com (and other sources) for driver updates and manufacturer sites. In addition, it allows to take a backup of currently installed drivers for safe keeping.

InstalledDriversList

Source: <http://www.nirsoft.net>

InstalledDriversList is a tool for Windows that lists all device drivers that exists on the system. For every device driver, it displays the following information: Driver Name, Display Name, Description, Startup Type, Driver type, Driver Group, Filename, File Size, Modified/Created Time of the driver file, and version information of the driver file.

If the driver is currently running on Windows kernel, it also displays the following information: Base Memory Address, End Address, Memory Size, and Load Count.

Driver Magician

Source: <http://www.drivermagician.com>

Driver Magician allows device drivers backup, restoration, update and removal in Windows operating system. It identifies all the hardware in the system, extracts their associated drivers from the hard disk and backs them up to a location of your choice. It has a built-in database of the latest drivers with the ability to go to the Internet to receive the driver updates. If there are unknown devices in the PC, Driver Magician helps to detect them with its built-in hardware identifier database.

Driver Reviver

Source: <http://www.reviversoft.com>

Driver Reviver restores maximum performance and functionality to the user PC's hardware and its components.

Features:

- Ensures that the user PC and its components are performing at their optimum levels
- It tracks down each driver for each single piece of hardware connected to the PC
- Scans for drivers downloads them and installs them correctly

- Prevents users from incorrectly using the wrong driver
- Eliminates the risk of downloading a faulty driver or even malware
- Ensures that if there are any problems with an update, the changes can be reversed to get the system back up and running

ServiWin

Source: <http://www.nirsoft.net>

ServiWin utility displays the list of installed drivers and services on the system. For some of them, it shows additional useful information: file description, version, product name, company that created the driver file, and so on. In addition, ServiWin allows one to stop, start, restart, pause, and continue service or driver, change the startup type of service or driver (automatic, manual, disabled, boot or system), save the list of services and drivers to file, or view HTML report of installed services/drivers in the default browser.

Driver Fusion

Source: <https://treexy.com>

Driver Fusion is the complete device and driver solution for your PC that can manage and monitor your devices and their drivers. You can install and uninstall drivers with Driver Fusion, including the ability to backup, restore and download drivers with ease. The effortless health check, including an automatic driver updater to update outdated drivers and install missing drivers, lets you scan and fix detected issues quickly. Furthermore, you can disable, enable and restart devices while Windows is running. With our cloud-powered removal engine, you can delete the driver entries that are left behind by the normal uninstallers, which is especially useful when you are updating a driver or changing a device.

My Drivers

Source: <http://www.zhangduo.com>

My Drivers enables to detect, backup and restore all hardware device drivers currently on the system. In addition, it allows finding the latest drivers for the hardware and installing them onto the computer. One can back up the list of all hardware devices extracted, into the desired folder and restore them after reinstalling or upgrading the system.

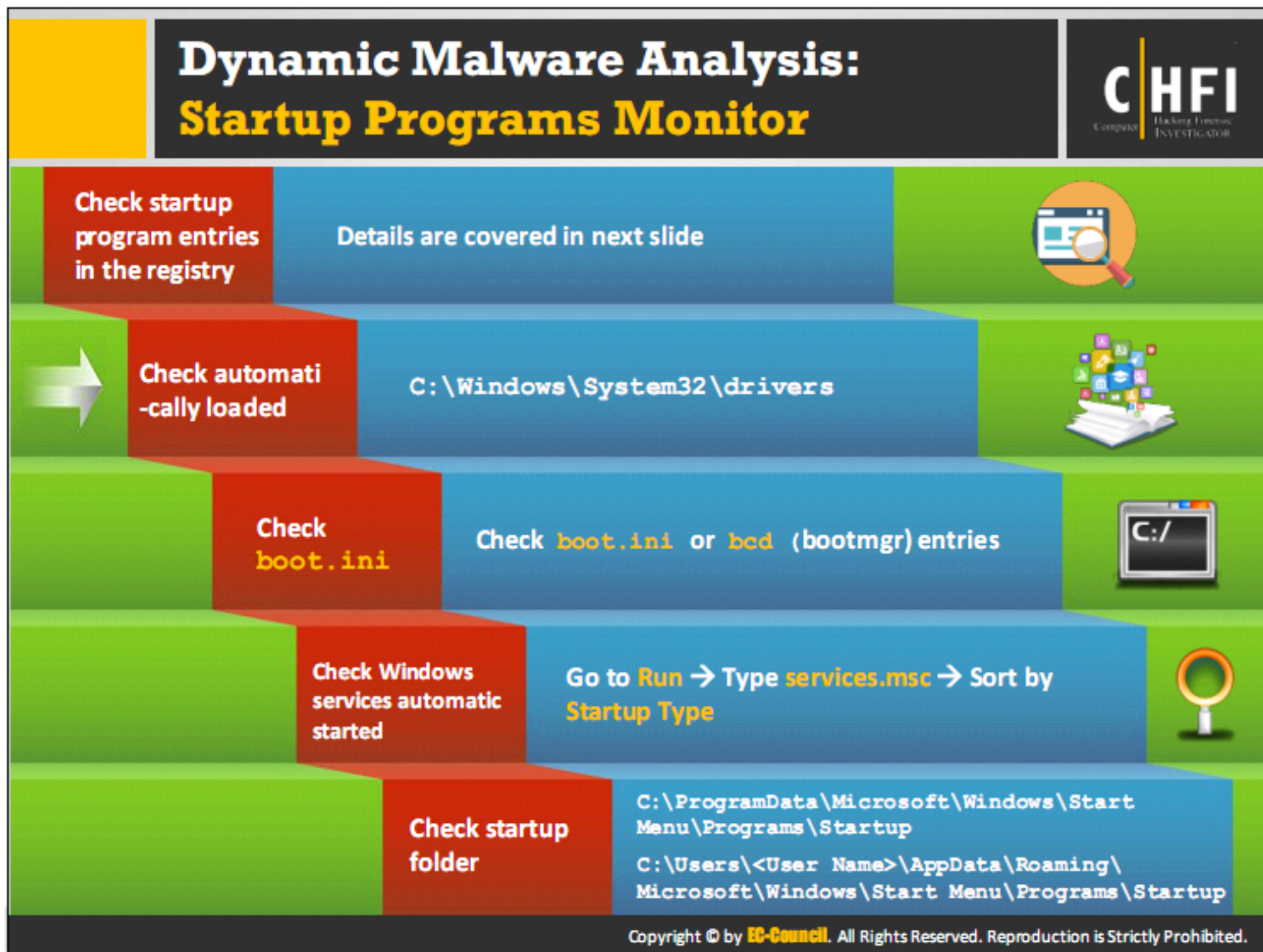
DriverEasy

Source: <http://www.drivereasy.com>

DriverEasy tool automatically scans and analyzes users' systems.

Features:

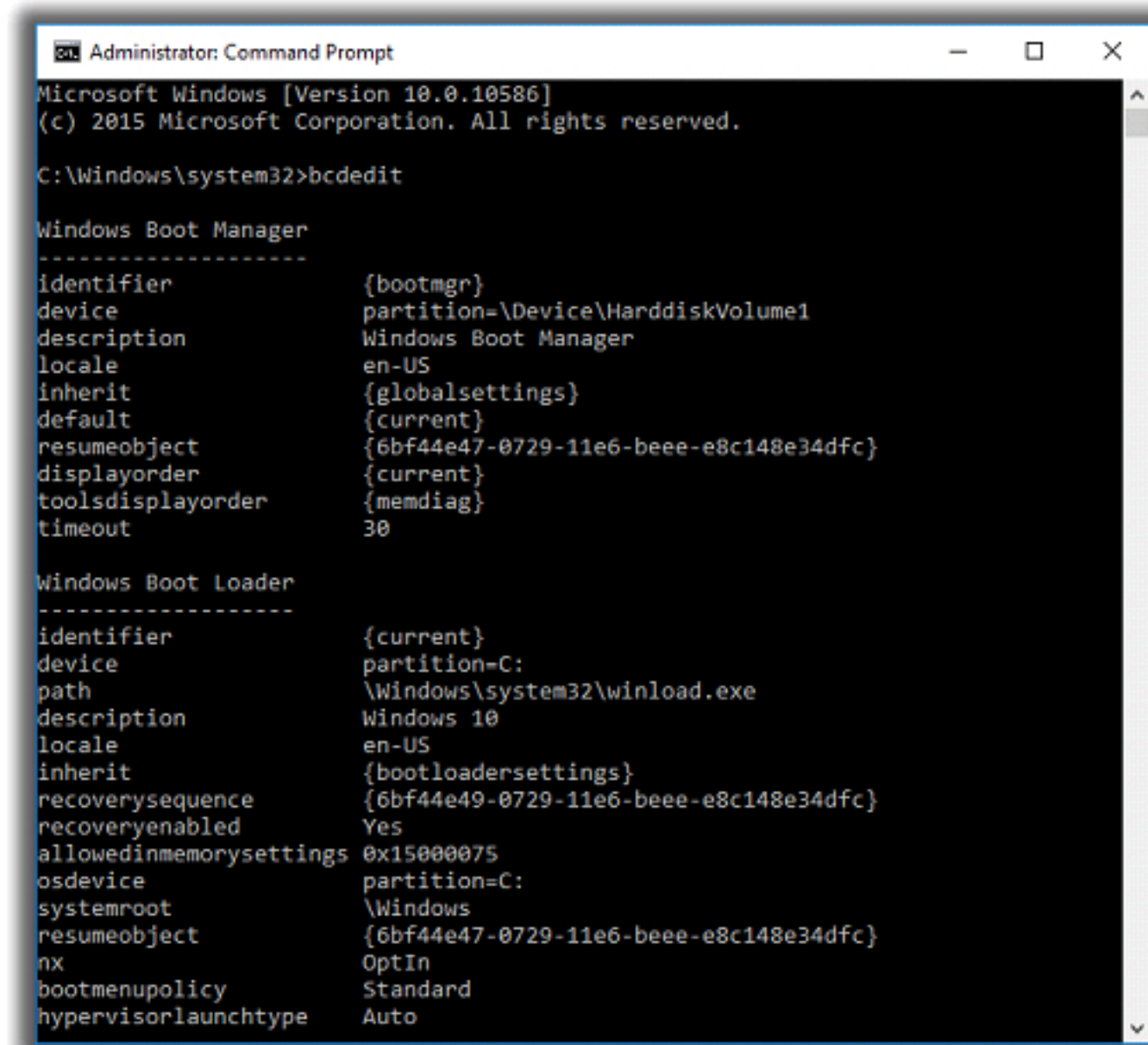
- Fixes driver issues
- Detects unknown device drivers
- Keeps drivers up-to-date with latest versions
- Secures user's system with backup of Installed drivers, easy to roll back or restore them
- Uninstalls removed device drivers to speed up booting



Various Trojans and malware can alter the system settings and add themselves to the startup menu to perform malicious activities continuously whenever the system starts. Therefore, scanning for suspicious startup programs is essential for detecting Trojans. Given below are steps to detect hidden Trojans:

Check boot.ini

Check **boot.ini** or **bcd** (bootmgr) entries using command prompt. Open **command prompt with administrator**, type **bcdedit** command and press enter button to view all the boot manager entries.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>bcdedit

Windows Boot Manager
-----
identifier          {bootmgr}
device              partition=\Device\HarddiskVolume1
description         Windows Boot Manager
locale              en-US
inherit             {globalsettings}
default             {current}
resumeobject        {6bf44e47-0729-11e6-beee-e8c148e34dfc}
displayorder        {current}
toolsdisplayorder   {memdiag}
timeout             30

Windows Boot Loader
-----
identifier          {current}
device              partition=C:
path               \Windows\system32\winload.exe
description         Windows 10
locale              en-US
inherit             {bootloadersettings}
recoverysequence    {6bf44e49-0729-11e6-beee-e8c148e34dfc}
recoveryenabled     Yes
allowedinmemorysettings 0x15000075
osdevice            partition=C:
systemroot          \Windows
resumeobject        {6bf44e47-0729-11e6-beee-e8c148e34dfc}
nx                  OptIn
bootmenupolicy       Standard
hypervisorlaunchtype Auto
```

FIGURE 11.1: Screenshot displaying the results for Windows Boot Manager Entries

Check the Windows services

To find the startup process, investigators can check the Windows services list for viewing services that start automatically when system boots:

1. Go to Run → Type **services.msc** → Sort by **Startup Type**.

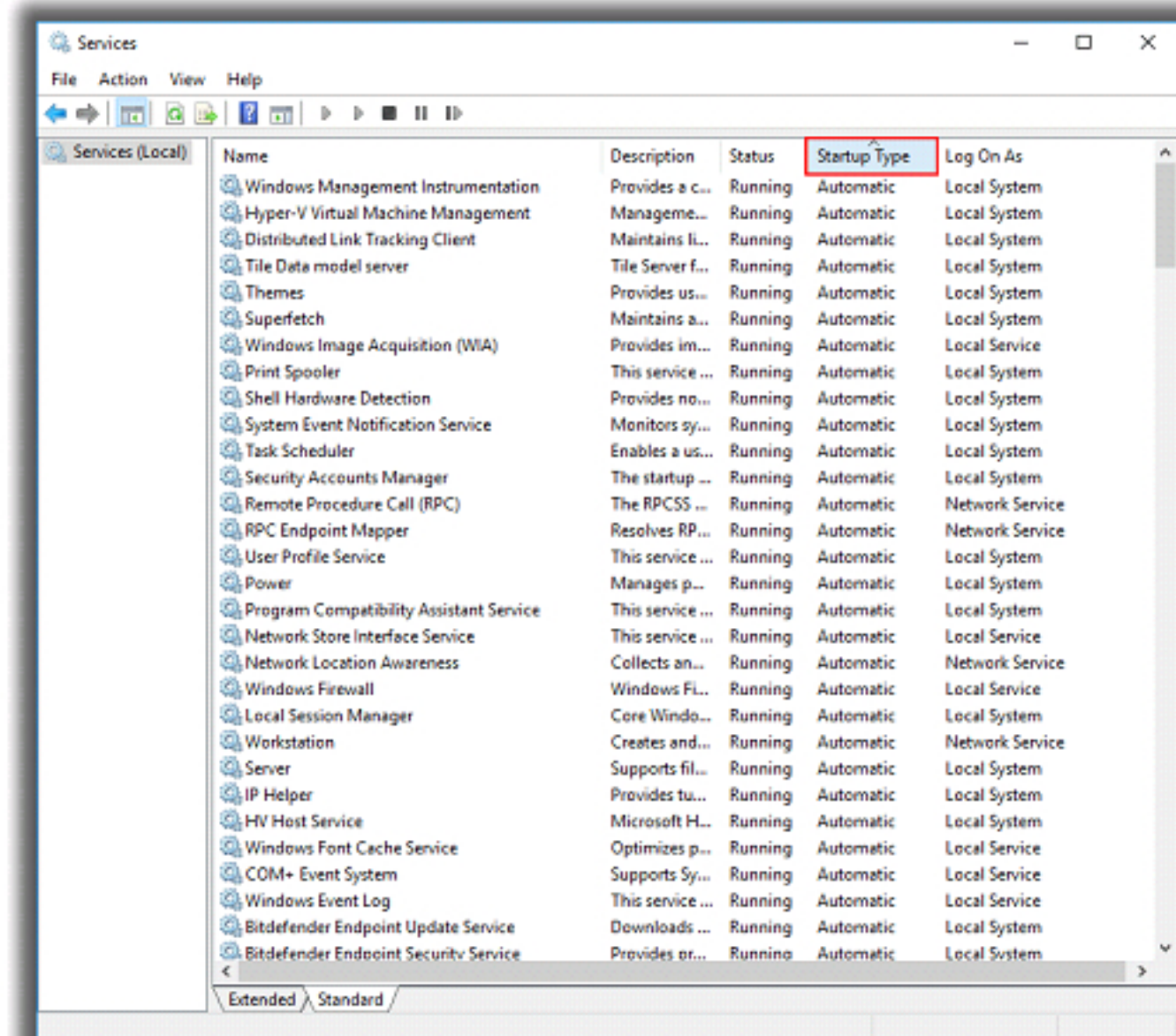


FIGURE 11.2: Screenshot showing the information about services on a local system

Check Startup folders

Startup folders store the applications or shortcuts of applications that auto-start when the system boots. To check the **Startup** applications search the following locations on Windows 10:

- **C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup**
- **C:\Users\(User-Name)\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup**

Another method to access startup folders is:

1. Press the Windows and r buttons simultaneously to open the **run** box
2. Type **shell:startup** in the box and click **OK** button to navigate to the startup folder

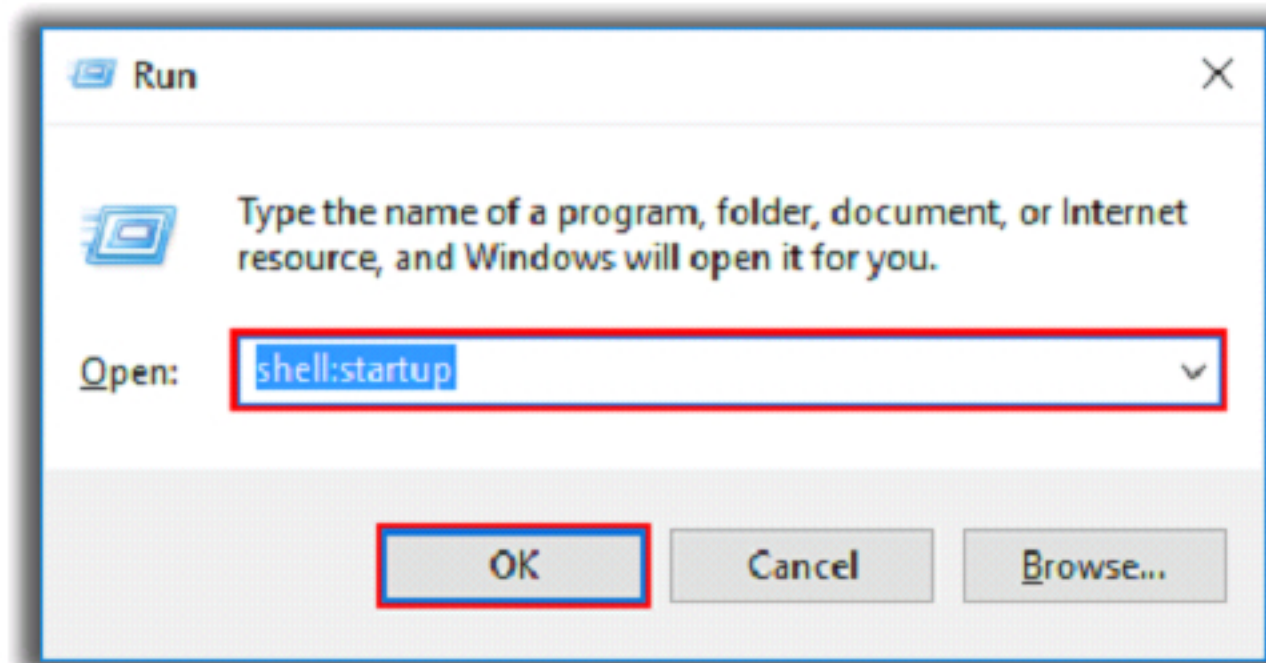




FIGURE 11.3: Screenshot showing shell: startup command in Run box

Windows 10 Startup Registry Entries




Windows Startup Setting




```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Runonce
```

Explorer Startup Setting



```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Common Startup
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Startup
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup
```

IE Startup Setting



```
HKCU\SOFTWARE\Microsoft\Internet Explorer\URLSearchHooks
HKLM\SOFTWARE\Microsoft\Internet Explorer\Toolbar
HKLM\SOFTWARE\Microsoft\Internet Explorer\Extensions
HKCU\SOFTWARE\Microsoft\Internet Explorer\MenuExt
```









Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Startup items such as programs, shortcuts, folders, and drivers run automatically at startup when users log into a Windows OS (e.g., Windows 8). The OS stores the startup items either as programs or drivers installed, or services in the assigned startup folders or collects them directly from the system using registry keys.

Investigators can find the programs that run on Windows startup in the registry entries, such as **IE Startup Setting**, **Windows Startup Setting**, and **Explorer Startup Setting**.

Startup Programs Monitoring Tools



 Autoruns for Windows http://technet.microsoft.com	 PCTuneUp Free Startup Manager http://www.pctuneupsuite.com
 WinTools.net 16.0.0 Premium http://www.wintools.net	 Ccleaner https://www.piriform.com
 StartEd Pro http://www.outertech.com	 WinPatrol http://www.winpatrol.com
 Startup Delayer http://www.r2.com.au	 Chameleon Startup Manager http://www.chameleon-managers.com
 WhatInStartup http://www.nirsoft.net	 Startup Booster http://www.smartpctools.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Autoruns for Windows

Source: <http://technet.microsoft.com>

This utility can auto-start the location of any startup monitor, display what programs are configured to run during system bootup or login, and show the entries in the order Windows processes them. As soon as this program includes in the startup folder, Run, RunOnce, and other Registry keys; users can configure Autoruns to show other locations, including Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, and auto-start services.

Autoruns' Hide Signed Microsoft Entries option helps the user to zoom in on third-party auto-starting images that add to the users' system, and it has support for looking at the auto-starting images configured for other accounts configured on a system.

WinTools.net 16.7.1 Premium

Source: <http://www.wintools.net>

It is a suite of tools for increasing MS Windows operating system performance. WinTools.net cleanly removes unwanted software from disk drives and dead references from the Windows registry. WinTools.net puts you in control of the Windows start up process, memory monitoring and gives you the power to customize desktop and system settings to fit your needs.

Adds more speed and stability for your connection. Ensures your privacy and keep sensitive information secure.

StartEd Pro

Source: <http://www.outertech.com>

StartEd is a utility that helps to manage the Windows startup procedure. It recognizes obsolete or memory-hogging startup programs and enables the option of disabling them to increase the quality of system performance.

Features:

- View, edit, delete, disable, and add entries to the Windows startup configuration
- Backup and Restore startup configurations
- Manage System Services with detailed notes and description
- Filter Service List with keywords
- See new startup items and services since last StartEd use
- Show detailed information about every startup entry
- Create shortcuts on desktop which is useful for temporarily disabled items
- Recognize Trojan Horses in startup configuration

Startup Delayer

Source: <http://www.r2.com.au>

Startup Delayer optimizes startup process by delaying applications from starting up as soon as a user logs into the computer. Because of the delay, the computer becomes usable a lot faster. Startup Delayer will then start launching the delayed applications when the computer is idle.

Features:

- Provides automatic delay engine
- Possess advanced launch options, which let to modify various launch options such as launching on a specific day.
- Monitors running tasks and services
- Creates backups of startup applications and restores them when required
- Recovers deleted applications

WhatInStartup

Source: <http://www.nirsoft.net>

This utility displays the list of all applications that are loaded automatically when Windows starts up. For each application, the following information is displayed: Startup Type (Registry/Startup Folder), Command-Line String, Product Name, File Version, Company Name, Location in the Registry or file system, and more. It allows you to easily disable or delete unwanted programs that run in your Windows startup. You can use it on your currently running instance of Windows, as well as you can use it on external instance of Windows in another drive.

PCTuneUp Free Startup Manager

Source: <http://www.pctuneupsuite.com>

PCTuneUp Free Startup Manager is a system startup entry monitor and management tool. It displays the configuration of applications and processes to run automatically during startup or login and helps to disable or enable startup items from system boot. It displays the detailed information of the exact applications such as the name, type, and arguments, and it makes possible to process some operations of each item in the activated registry editor, such as import/export, modification, renaming, and copy, as needed.

Features:

- Speeds up system boot and Windows login process
- Removes unneeded programs in the startup list
- Allows to set programs to launch at startup
- Allows to acquire more available memory, such as RAM and other system resources

Chameleon Startup Manager

Source: <http://www.chameleon-managers.com>

Chameleon Startup Manager can control the programs that run at Windows startup, which makes Windows start faster, operate with increased stability, and lower the HDD usage. It also offers program launch options with fixed or automatic delayed startup (each program is initiated in sequence after the previous one finishes starting), allowing the computer to be started as quickly and smoothly as possible.

Programs run according to various functions including startup order change, priority, consecutive program launch, and day selection. A user can create and select the configurations at Windows startup or applied without restarting Windows.

Ccleaner

Source: <https://www.piriform.com>

CCleaner is a utility for computers running Microsoft Windows that cleans out the 'junk' that accumulates over time: temporary files, broken shortcuts, and other problems. CCleaner protects your privacy. It cleans your browsing history and temporary internet files, allowing you to be a more confident Internet user and less susceptible to identity theft.

CCleaner can clean unneeded files from various programs saving you hard disk space, removes unnecessary entries in the Windows Registry, help you uninstall software and select which programs start with Windows.

WinPatrol

Source: <http://www.winpatrol.com>

WinPatrol is a system utility that helps users to monitor changes made to files and folders, startup programs, hidden files, scheduled tasks, and services.

Chameleon Startup Manager

Source: <http://www.chameleon-managers.com>

Chameleon Startup Manager can control programs that run at Windows startup, which makes Windows start faster and operate with increased stability. Programs can be run according to various functions including startup order change, startup delay, priority, consecutive program launch, day selection and much more.

Chameleon Startup Manager also offers program launch options with fixed or automatic delayed startup, allowing the computer to be started as quickly and smoothly as possible.

Startup Booster

Source: <http://www.smartpctools.com>

Startup Booster classifies all of the programs that are executed at startup as system programs, suspicious applications (such as viruses, etc.), and the unwanted programs for startup. This tool helps to remove programs from startup list or to add them when needed.

Features:

- Configures Windows to perform maximum by simple tweaks that suggest which options are to be activated and deactivated
- Cleans up the registry of outdated data or wrong values
- Instructs on how to configure the BIOS

Dynamic Malware Analysis: Windows Services Monitor

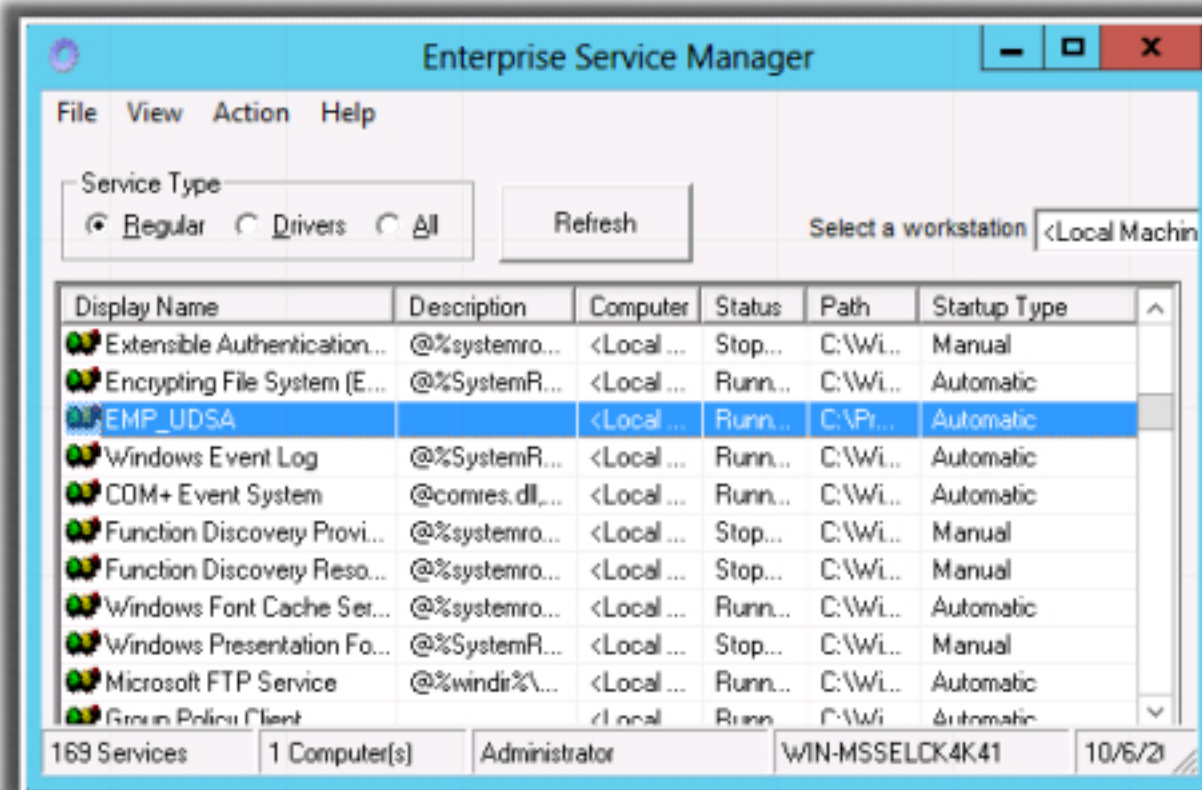


1

Malware may **rename their processes** to look like a genuine Windows service in order to avoid detection

2

You can use various tools to identify such suspicious Windows Services



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers design malware and other malicious code in such a way that they install and run on a computer device in the form of a service. As most of the services run in the background to support processes and applications, the malicious services are invisible even when are performing harmful activities on the system and can function even without intervention or input.

These malicious services run as SYSTEM account or other privileged accounts, which provides more access compared to the user accounts. Making them more dangerous compared to the common malware and executable code. Attackers also try to trick users and investigators alike by naming the malicious services with almost similar names like that of genuine Windows services to avoid detection.

Investigators need to trace the malicious services initiated by the suspect file during dynamic analysis by using the tools that can detect changes in services.

Windows Services Monitoring Tool: Windows Service Manager (SrvMan)

SrvMan has both GUI and Command-line modes. It can also be used to run arbitrary Win32 applications as services (when such service is stopped, the main application window is closed automatically). You can use SrvMan's Command Line interface to perform the following tasks:

- **Create services**

```
srvman.exe add <file.exe/file.sys> [service name] [display name] [/type:<service type>]  
[/start:<start mode>] [/interactive:no] [/overwrite:yes]
```


- **Delete services**

srvman.exe delete <service name>

- **Start/stop/restart services**

srvman.exe start <service name> [/nowait] [/delay:<delay in msec>]

srvman.exe stop <service name> [/nowait] [/delay:<delay in msec>]


srvman.exe restart <service name> [/delay:<delay in msec>]

- **Install and start a legacy driver with a single call**

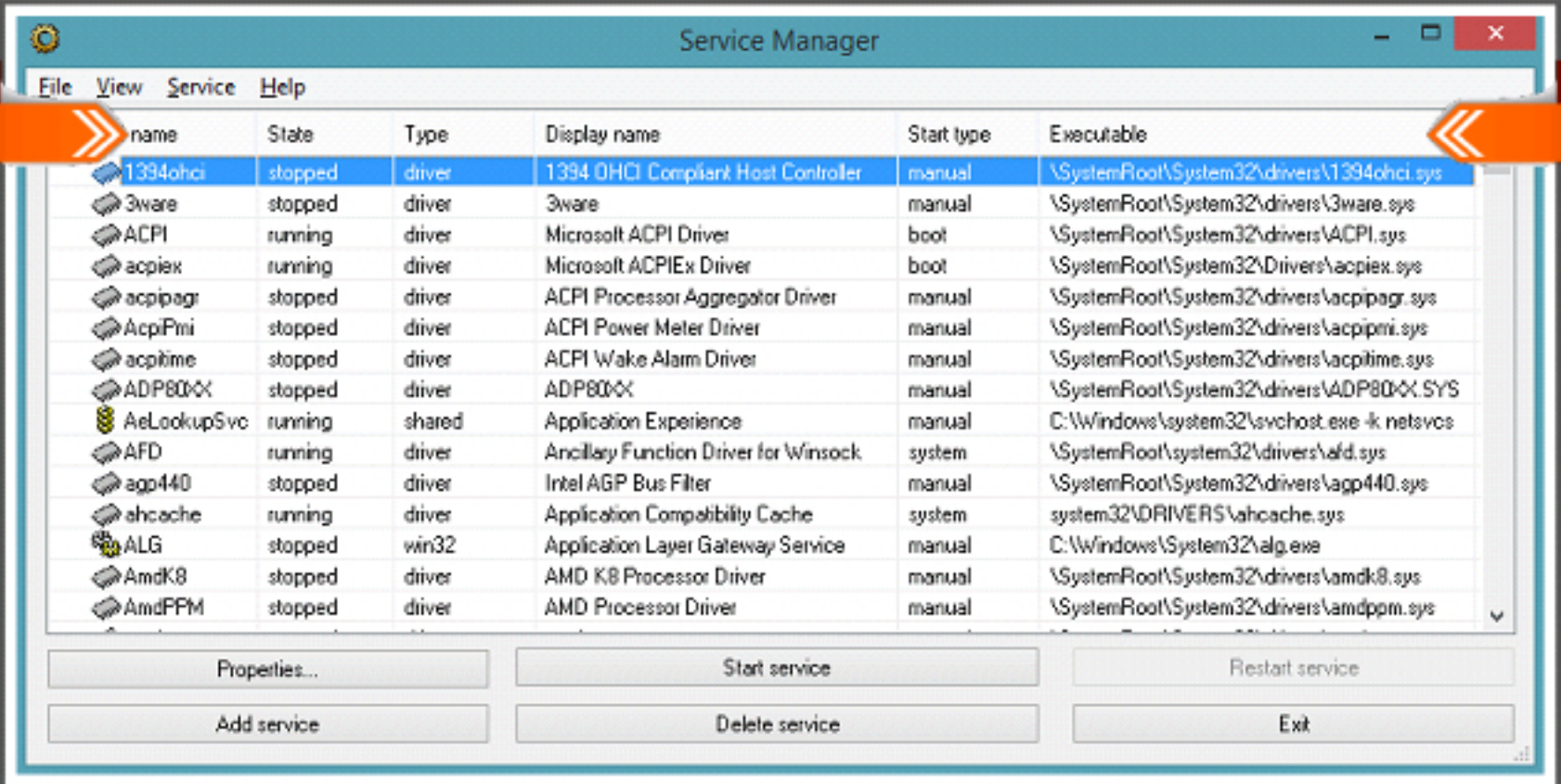
srvman.exe run <driver.sys> [service name] [/copy:yes] [/overwrite:no]
[/stopafter:<msec>]

Source: <http://tools.sysprogs.org>

Windows Services Monitoring Tool: Windows Service Manager (SrvMan)



Windows Service Manager (SrvMan) simplifies all common tasks related to Windows services. It can create services (both Win32 and Legacy Driver) without restarting Windows, delete existing services, and change the service configuration



<http://tools.sysprogs.org>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


Windows Service Manager is a small tool that simplifies all common tasks related to Windows services. It can create services (both Win32 and Legacy Driver) without restarting Windows, delete existing services and change service configuration. It has both GUI and Command-line modes. It can also be used to run arbitrary Win32 applications as services (when such service is stopped, the main application window is closed automatically).











Features:

- Allows creating driver and Win32 services without restarting
- Supports both GUI and Command Line
- Supports all modern 32-bit and 64-bit versions of Windows
- Allows running arbitrary Win32 applications as services
- Allows installing & running legacy driver services in a single command line call

Source: <http://tools.sysprogs.org>

Windows Services Monitoring Tools



 Advanced Win Service Manager http://securityxploded.com	 AnVir Task Manager http://www.anvir.com
 Netwrix Service Monitor http://www.netwrix.com	 Process Hacker http://processhacker.sourceforge.net
 PC Services Optimizer http://www.smartpcutilities.com	 Free Windows Service Monitor Tool http://www.manageengine.com
 ServiWin http://www.nirsoft.net	 Nagios XI http://www.nagios.com
 PRTG Network Monitor https://www.paessler.com	 Service+ http://www.activeplus.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Advanced Win Service Manager

Source: <http://securityxploded.com>

Advanced Win Service Manager is software for smarter analysis of Windows Services. It offers many features which set it apart from built-in Service Management Console as well as other similar software. Some of the features include Detection of Malicious/Rootkit Services, Automatic Threat Analysis, Service Filter mechanism, Integrated Online Virus/Malware Scan, Color based Threat Representation, and HTML/XML based Service Report, etc.

Netwrix Service Monitor

Source: <http://www.netwrix.com>

Netwrix Service Monitor is a tool to monitor critical Windows services and optionally restart them after failure. The tool tracks all automatic startup services on multiple servers at a time and sends e-mail alerts when one or more services stops unexpectedly. The optional automatic restart feature ensures that all monitored services are up and running without downtime.

PC Services Optimizer

Source: <http://www.smartpcutilities.com>

PC Services Optimizer is a tweaking solution that enables to optimize Windows Services automatically. It turns off unneeded Windows services without affecting the normal function, which will make PC to run faster and more securely.

Features:

- **Gaming Mode:** It gives users' systems an immediate performance boost.
- **Services Profiles:** It saves user services settings in profiles, enabling the user to apply different settings in seconds, saving time especially when dealing with multiple computers or users.
- **Services Manager:** It enables advanced users to master Windows services including third party services by providing several tools for performing advanced functions.

ServiWin

Source: <http://www.nirsoft.net>

ServiWin utility displays the list of installed drivers and services on the user's system. For some of them, it displays additional useful information such as file description, version, product name, and the company that created the driver file.

In addition, it allows users to stop, start, restart, pause, and continue service or driver, change the startup type of service or driver (automatic, manual, disabled, boot or system), save the list of services and drivers to file, or view HTML report of installed services/drivers in their default browser.

Windows Service Manager Tray

Source: <http://winservicemanager.codeplex.com>

Windows Service Manager Tray allows selecting the necessary services and controlling them from the tray. This tool also optimizes the default Windows service manager and permits to start, stop, or restart required services.

AnVir Task Manager

Source: <http://www.anvir.com>

AnVir Task Manager controls everything running on the user's computer. It offers all of its features in a single interface instead of releasing multiple packages to perform a family of related tasks.

Features:

- Monitors processes, services, startup programs, etc.
- Replaces Windows Task Manager
- Gets rid of spyware and viruses
- Speeds up the system and Windows startup

Process Hacker

Source: <http://processhacker.sourceforge.net>

Process Hacker is a multi-purpose tool that helps to monitor system resources, debug software, and detect malware. It is an open source alternative to programs such as Task Manager and Process Explorer.

Features:

- Provides a detailed overview of system activity with highlighting
- Offers graphs and statistics to track down resource hogs and runaway processes
- Allows discovery of which processes are using the file that cannot be edited or deleted
- Permits seeing what programs have active network connections, and close them if necessary
- Provides real-time information on disk access
- Allows viewing of detailed stack traces with kernel-mode, WOW64, and .NET support
- Permits going beyond services.msc: create, edit, and control services

Free Windows Service Monitor Tool

Source: <http://www.manageengine.com>

Free Windows Service Monitor helps to monitor Exchange Server, SharePoint services, MySQL services, MSSQL services, DHCP services, etc. It allows users to monitor up to five custom services simultaneously.

Features:

- Monitors the Windows services for up to three devices simultaneously
- Allows to know the status and startup type of the Windows services
- Configures the startup type and updates the status of Windows services
- Allows to fetch the status of Windows services by refreshing

Nagios XI

Source: <http://www.nagios.com>

Nagios XI monitors the state of any Microsoft Windows service such as IIS, Exchange, and DHCP, and alerts whenever the service stops or crashes.

Features:

- Increased server, services, and application availability
- Detects network outages and protocol failures
- Detects failed processes and batch jobs

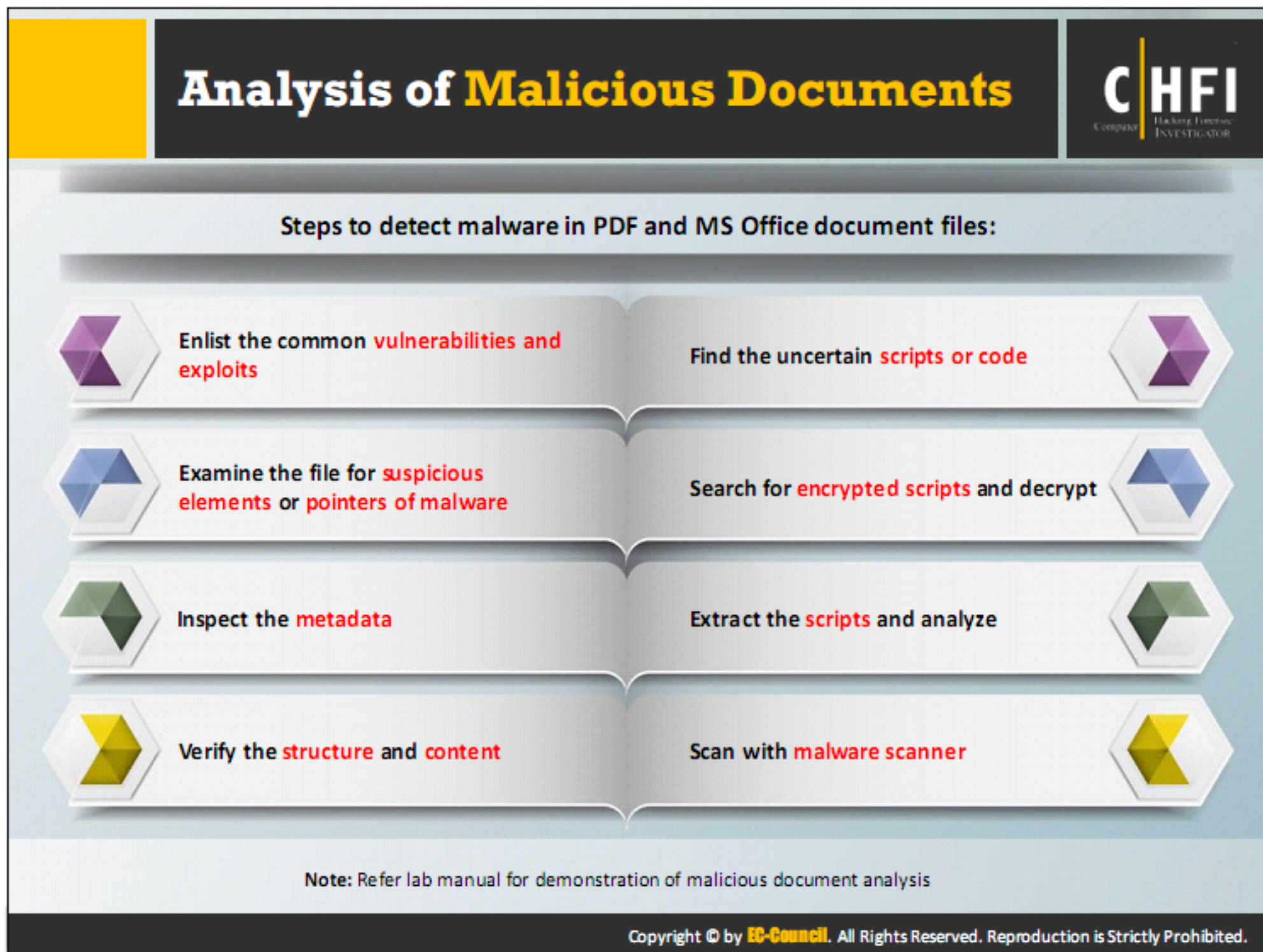
Service+

Source: <http://www.activeplus.com>

Service+ provides advanced features to manage Windows services (custom views, specific properties, monitoring, etc.).

Features:

- Implements multiple services such as startup, account, dependencies, name, and path simultaneously
- Monitors services installation and un-installation in real time
- Terminates un-responding services without any reboot
- Allows all authenticated users to start a service
- Prohibits all users, including administrators to stop critical services such as backup and critical applications
- Manages the services on a remote computer
- Sorts services by standard and advanced properties such as name, status, startup, and type
- Imports or exports the configuration of services as an XML file to duplicate them, to backup settings, or to mirror the same configuration on several computers



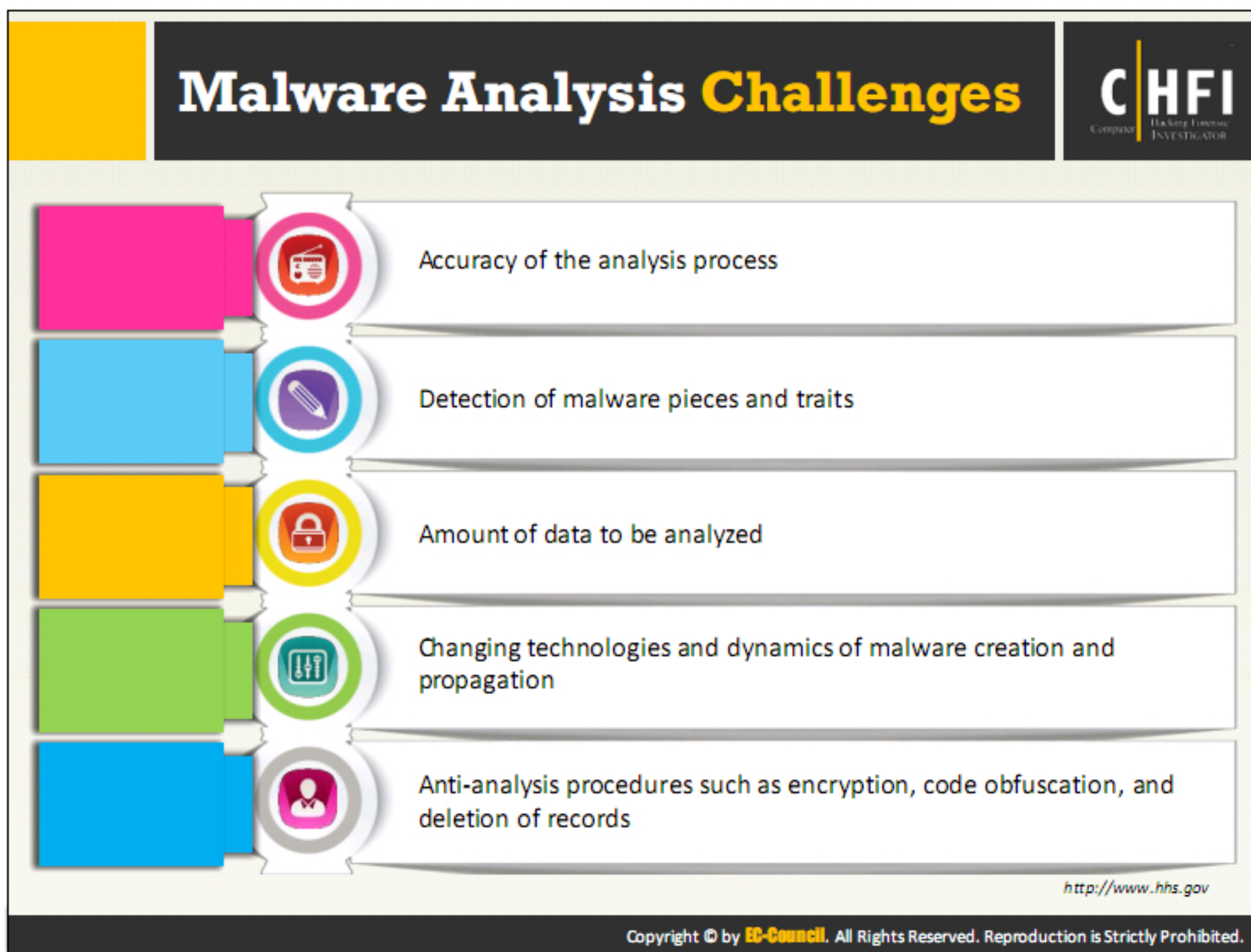
To find if a document either in the form of PDF or a MS-Word file, the investigators should at first understand the structure of the document. They should have knowledge on how the attackers could embed malicious code or program into the document and be aware of all the packing and obfuscation techniques prevailing.

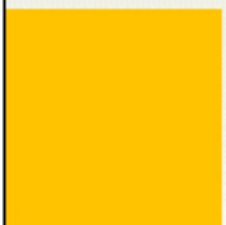
The investigators should know how to identify the malicious document file by using identification tools and comparing the document structure with the standard structure.

Steps to detect malware in PDF and MS Office document files


1. Enlist the common vulnerabilities and exploits: Study and list the common vulnerabilities and their impact on the document structure.
2. Examine the file for suspicious elements or pointers of malware: Using the common vulnerability, investigators should be able to scan the document for suspicious elements that can confirm presence of malicious code, strings, commands, etc.
3. Inspect the metadata: Metadata may include time of creation and modification, author and moderator names, an application used for creation, etc. Gather the metadata and inspect it for any mistakes.
4. Verify the structure and content: Analyze the structure and contents of the document for suspicious elements such as objects, streams, scripts, and shellcode.
5. Extract the uncertain scripts or code: Search and extract the suspicious scripts and code from the document.

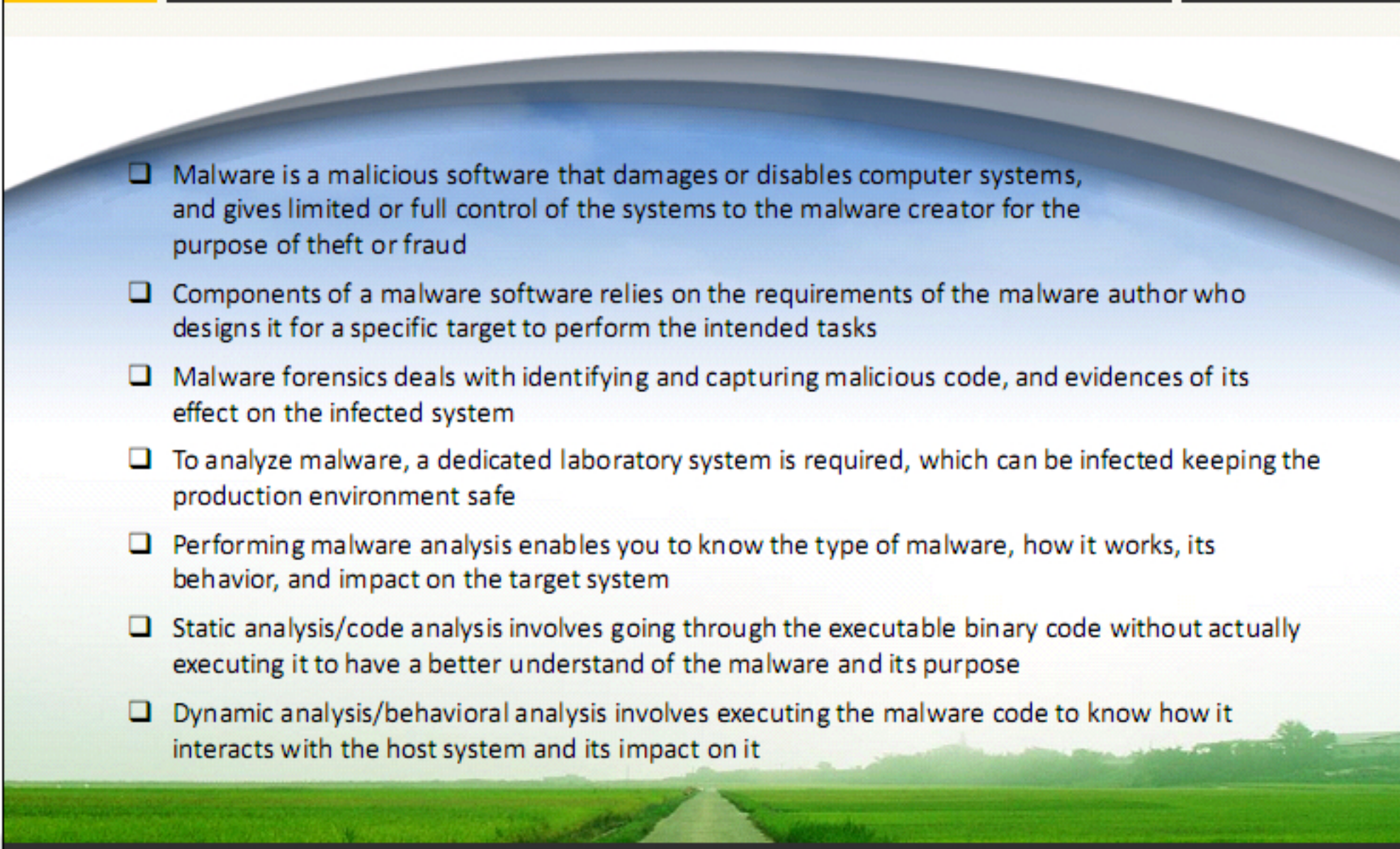
6. Search for encrypted scripts and decrypt: Find if the document contains any encrypted elements, as the attackers encode the malicious code, scripts, and objects to avert detection. Extract such elements and decrypt them.
7. Analyze the suspicious element: Evaluate the impact of the suspicious element by finding their course of action, propagation, and modification they make on the system.
8. Scan with malware scanner: Scan the suspicious documents with malware scanner or scan them using online and offline tools to find if they contain any malicious content.





Module Summary





- ☐ Malware is a malicious software that damages or disables computer systems, and gives limited or full control of the systems to the malware creator for the purpose of theft or fraud
- ☐ Components of a malware software relies on the requirements of the malware author who designs it for a specific target to perform the intended tasks
- ☐ Malware forensics deals with identifying and capturing malicious code, and evidences of its effect on the infected system
- ☐ To analyze malware, a dedicated laboratory system is required, which can be infected keeping the production environment safe
- ☐ Performing malware analysis enables you to know the type of malware, how it works, its behavior, and impact on the target system
- ☐ Static analysis/code analysis involves going through the executable binary code without actually executing it to have a better understand of the malware and its purpose
- ☐ Dynamic analysis/behavioral analysis involves executing the malware code to know how it interacts with the host system and its impact on it

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

This module has imparted knowledge about malware, its different types, methods of propagation and impact on various devices. In this module, you have learned the process of finding malware and differentiating it from the normal code, extracting it from a corrupted system, assessing its code and analyzing its impact on the victim system. This module has also divulged information on different methods for analyzing the malware from different files.

In the upcoming module, you will learn about various email crimes and the process of investigating them.