

Lec – 2a

Malware:

Assignment Project Exam Help

Viruses & Worms

<https://powcoder.com>

Add WeChat powcoder

Overview

- What is malware?
- Classification
- Attacks kits and surfaces
- Advanced Persistent Threats (APTs)
- Virus
 - Virus components
 - Virus phases
 - Macro and scripting viruses
 - Classifications
- Worms
 - Worms replication
 - Target discovery
 - Morris worm
 - Wana Cry

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Malware

NIST 800-83 defines malware as:

Assignment Project Exam Help

“a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim.”

<https://powcoder.com>

Add WeChat, powcoder

Name	Description
Advanced persistent threat	Cybercrime directed at business and political targets, using a wide variety of intrusion technologies and malware, applied persistently and effectively to specific targets over an extended period, often attributed to state-sponsored organizations.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.
Attack Kit	Set of tools for generating new malware automatically using a variety of supplied propagation and payload mechanisms.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Backdoor (trapdoor)	Any mechanisms that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system.
Downloaders	Code that installs other items on a machine that is under attack. It is normally included in the malware code just in order on to a compromised system to then import a larger malware package.
Drive-by download	An attack using code in a compromised web site that exploits a browser vulnerability to attack a client system when the site is viewed.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Flooders (DoS client)	Used to generate a large volume of data to attack networked computer systems, by carrying out some form of denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Logic bomb	Code inserted into malware by an intruder. A logic bomb lies dormant until a predefined condition is met; the code then triggers an unauthorized act.
Macro Virus	A type of virus that uses macro or scripting code, typically embedded in a document, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.
Mobile Code	Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Spammer Programs	Used to send large volumes of unwanted e-mail.
Spyware	Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data and/or network traffic; or by scanning files on the system for sensitive information.

Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program.
Virus	Malware that, when executed, tries to replicate itself into other executable machine or script code; when it succeeds the code is said to be infected. When the infected code is executed, the virus also executes.
Worm	A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network, usually by exploiting software vulnerabilities in the target system.
Zombie, bot	Program activated on an infected machine that is activated to launch attacks on other machines.

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Classification of Malware

Classified into two broad categories:

Based first on how it spreads or propagates to reach the desired target

Then on the actions or payloads it performs once a target is reached

Also classified by:

Those that need a host program (parasitic code such as viruses)

Those that are independent, self-contained programs (worms, trojans, and bots)

Malware that does not replicate (trojans and spam e-mail)

Malware that does replicate (viruses and worms)

Assignment Project Exam Help
<https://powcoder.com>

Add WeChat powcoder

Types of Malicious Software (Malware)

Propagation mechanisms include:

- Infection of existing content by viruses that is subsequently spread to other systems
- Exploit of software vulnerabilities by worms or drive-by-downloads to allow the malware to replicate
- Social engineering attacks that convince users to bypass security mechanisms to install Trojans or to respond to phishing attacks

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder



Payload actions performed by malware once it reaches a target system can include:

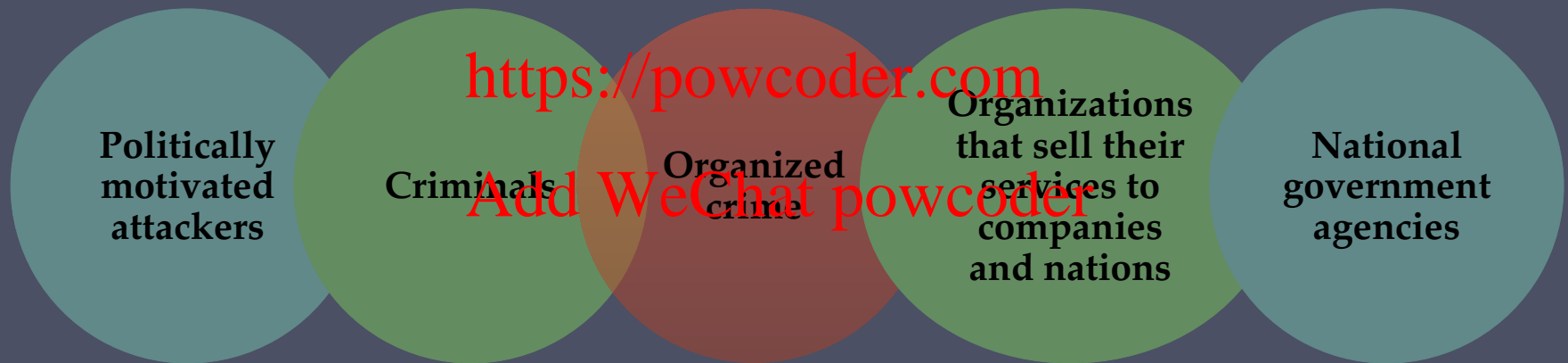
- Corruption of system or data files
- Theft of service/make the system a zombie agent of attack as part of a botnet
- Theft of information from the system/keylogging
- Stealthing/hiding its presence on the system

Attack Kits

- Initially the development and deployment of malware required considerable technical skill by software authors
 - The development of virus-creation toolkits in the early 1990s and then more general attack kits in the 2000s greatly assisted in the development and deployment of malware
- Toolkits are often known as “crimeware”
 - Include a variety of propagation mechanisms and payload modules that even novices can deploy
 - Variants that can be generated by attackers using these toolkits creates a significant problem for those defending systems against them
- Examples are:
 - Zeus
 - Angler

Attack Sources

- Another significant malware development is the change from attackers being individuals often motivated to demonstrate their technical competence to their peers to more organized and dangerous attack sources such as:



- This has significantly changed the resources available and motivation behind the rise of malware and has led to development of a large underground economy involving the sale of attack kits, access to compromised hosts, and to stolen information

Advanced Persistent Threats (APTs)

- Well-resourced, persistent application of a wide variety of intrusion technologies and malware to selected targets (usually business or political)
- Typically attributed to state-sponsored organizations and criminal enterprises
- Differ from other types of attack by their careful target selection and stealthy intrusion efforts over extended periods
- High profile attacks include Aurora, RSA, APT1, and Stuxnet

APT Characteristics

Advanced

- Used by the attackers of a wide variety of intrusion technologies and malware including the development of custom malware if required
- The individual components may not necessarily be technically advanced but are carefully selected to suit the chosen target

Persistent

- Determined application of the attacks over an extended period against the chosen target in order to maximize the chance of success
- A variety of attacks may be progressively applied until the target is compromised

Threats

- Threats to the selected targets as a result of the organized, capable, and well-funded attackers intent to compromise the specifically chosen targets
- The active involvement of people in the process greatly raises the threat level from that due to automated attacks tools, and also the likelihood of successful attacks

APT Attacks

- Aim:
 - Varies from theft of intellectual property or security and infrastructure related data to the physical disruption of infrastructure
- Techniques used:
 - Social engineering
 - Spear-phishing email
 - Drive-by-downloads from selected compromised websites likely to be visited by personnel in the target organization
- Intent:
 - To infect the target with sophisticated malware with multiple propagation mechanisms and payloads
 - Once they have gained initial access to systems in the target organization a further range of attack tools are used to maintain and extend their access

Viruses

- Piece of software that infects programs
 - Modifies them to include a copy of the virus
 - Replicates and goes on to infect other content
 - Easily spread through network environments
- When attached to an executable program a virus can do anything that the program is permitted to do
 - Executes secretly when the host program is run
- Specific to operating system and hardware
 - Takes advantage of their details and weaknesses

Virus Components

Infection mechanism

- Means by which a virus spreads or propagates
 - Also referred to as the *infection vector*
- <https://powcoder.com>

Trigger

- Event or condition that determines when the payload is activated or delivered
- Sometimes known as a *logic bomb*

Payload

- What the virus does (besides spreading)
- May involve damage or benign but noticeable activity

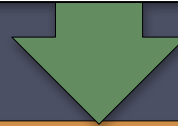
Virus Phases

Dormant phase

Virus is idle

Will eventually be activated
by some event

Not all viruses have this
stage



Assignment Project Exam Help

Triggering phase

Virus is activated to perform the function for
which it was intended

Can be caused by a variety of system events

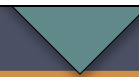
Add WeChat powcoder

Propagation phase

Virus places a copy of itself into
other programs or into certain
system areas on the disk

May not be identical to the
propagating version

Each infected program will now
contain a clone of the virus
which will itself enter a
propagation phase



Execution phase

Function is performed

May be harmless or damaging

Macro and Scripting Viruses

- NISTIR 7298 defines a macro virus as:
“a virus that attaches itself to documents and uses the macro programming capabilities of the document’s application to execute and propagate”
- Macro viruses infect scripting code used to support active content in a variety of user document types
- Are threatening for a number of reasons:
 - Is platform independent
 - Infect documents, not executable portions of code
 - Are easily spread
 - Because they infect user documents rather than system programs, traditional file system access controls are of limited use in preventing their spread, since users are expected to modify them
 - Are much easier to write or to modify than traditional executable viruses

```

macro Document_Open
  disable Macro menu and some macro security features
  if called from a user document
    copy macro code into Normal template file
  else
    copy macro code into user document being opened
  end if
  if registry key "Melissa" not present
    if Outlook is email client
      for first 50 addresses in address book
        send email to that address
        with currently infected document attached
      end for
    end if
    create registry key "Melissa"
  end if
  if minute in hour equals day of month
    insert text into document being opened
  end if
end macro

```

Figure 6.1 Melissa Macro Virus Pseudocode

Virus Classifications

Classification by target

- **Boot sector infector**
 - Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus
- **File infector**
 - Infects files that the operating system or shell considers to be executable
- **Macro virus**
 - Infects files with macro or scripting code that is interpreted by an application
- **Multipartite virus**
 - Infects files in multiple ways

Classification by concealment strategy

- **Encrypted virus**
 - A portion of the virus creates a random encryption key and encrypts the remainder of the virus
- **Stealth virus**
 - A form of virus explicitly designed to hide itself from detection by anti-virus software
- **Polymorphic virus**
 - A virus that mutates with every infection
- **Metamorphic virus**
 - A virus that mutates and rewrites itself completely at each iteration and may change behavior as well as appearance

Worms

- Program that actively seeks out more machines to infect and each infected machine serves as an automated launching pad for attacks on other machines
- Exploits software vulnerabilities in client or server programs
- Can use network connections to spread from system to system
- Spreads through shared media (USB drives, CD, DVD data disks)
- E-mail worms spread in macro or script code included in attachments and instant messenger file transfers
- Upon activation the worm may replicate and propagate again
- Usually carries some form of payload
- First known implementation was done in Xerox Palo Alto Labs in the early 1980s

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Worm Replication

Electronic mail or
instant messenger
facility

File sharing

Remote execution
capability

Remote file access or
transfer capability

Remote login capability

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Target Discovery

- Scanning (or fingerprinting)
 - First function in the propagation phase for a network worm
 - Searches for other systems to infect
- Random
 - Each compromised host probes random addresses in the IP address space using a different seed
 - This produces a high volume of Internet traffic which may cause generalized disruption even before the actual attack is launched
- Hit-list
 - The attacker first compiles a long list of potential vulnerable machines
 - Once the list is compiled the attacker begins infecting machines on the list
 - Each infected machine is provided with a portion of the list to scan
 - This results in a very short scanning period which may make it difficult to detect that infection is taking place
- Topological
 - This method uses information contained on an infected victim machine to find more hosts to scan
- Local subnet
 - If a host can be infected behind a firewall that host then looks for targets in its own local network
 - The host uses the subnet address structure to find other hosts that would otherwise be protected by the firewall

Morris Worm

- Earliest significant worm infection
- Released by Robert Morris in 1988
- Designed to spread on UNIX systems
 - Attempted to crack local password file to use login/password to logon to other systems
 - Exploited a bug in the finger protocol which reports the whereabouts of a remote user
 - Exploited a trapdoor in the debug option of the remote process that receives and sends mail
- Successful attacks achieved communication with the operating system command interpreter
 - Sent interpreter a bootstrap program to copy worm over

Recent Worm Attacks

Melissa	1998	E-mail worm First to include virus, worm and Trojan in one package
Code Red	July 2001	Exploited Microsoft IIS bug Probes random IP addresses Consumes significant Internet capacity when active
Code Red II	August 2001	Also targeted Microsoft IIS Installs a backdoor for access
Nimda	September 2001	Had worm, virus and mobile code characteristics Spread using e-mail, Windows shares, Web servers, Web clients, backdoors
SQL Slammer	Early 2003	Exploited a buffer overflow vulnerability in SQL server compact and spread rapidly
Sobig.F	Late 2003	Exploited open proxy servers to turn infected machines into spam engines
Mydoom	2004	Mass-mailing e-mail worm Installed a backdoor in infected machines
Warezov	2006	Creates executables in system directories Sends itself as an e-mail attachment Can disable security related products
Conficker (Downadup)	November 2008	Exploits a Windows buffer overflow vulnerability Most widespread infection since SQL Slammer
Stuxnet	2010	Restricted rate of spread to reduce chance of detection Targeted industrial control systems

WannaCry

Ransomware attack in May 2017 that spread extremely fast over a period of hours to days, infecting hundreds of thousands of systems belonging to both public and private organizations in more than 150 countries

It spread as a worm by aggressively scanning both local and remote networks, attempting to exploit a vulnerability in the SMB file sharing service on unpatched Windows systems

This rapid spread was only slowed by the accidental activation of a "kill-switch" domain by a UK security researcher

Once installed on infected systems, it also encrypted files, demanding a ransom payment to recover them

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Multiplatform

Assignment Project Exam Help
Metamorphic

Multi-exploit

<https://powcoder.com>

Add WeChat powcoder

**Worm
Technology**

Polymorphic

**Ultrafast
spreading**