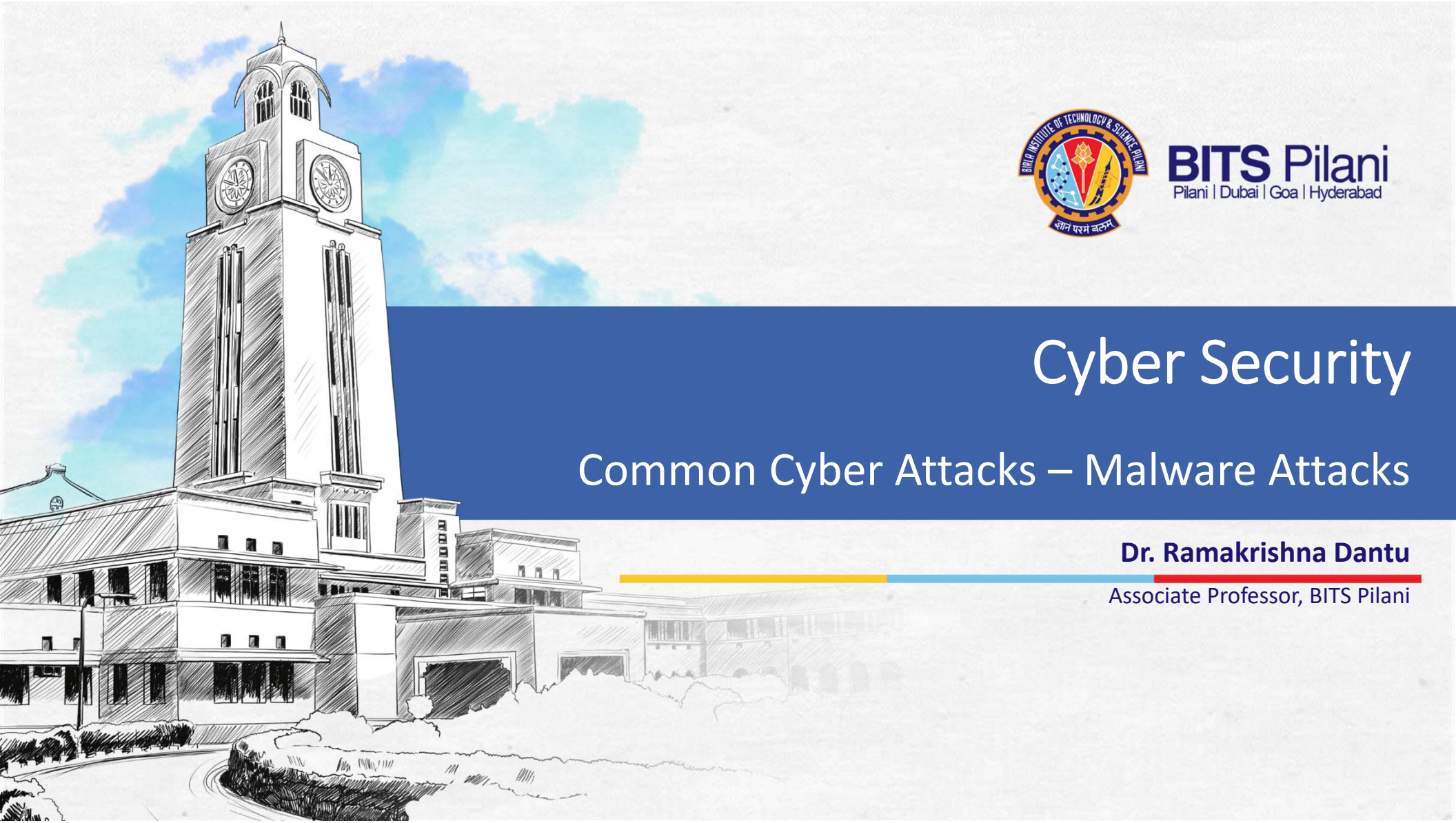


BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Common Cyber Attacks – Malware Attacks

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Common Cyber Attacks

Agenda

- Common Cyber Attacks – Practical Strategies for Identification, Containment and Mitigation:
  - Malware Attacks
    - E.g., Ransomware Attacks
  - Denial of Service Attacks
  - Session Hijacking and Man-in-the-Middle Attacks
  - Phishing and Spear Phishing Attacks
  - SQL Injection Attacks
  - Zero Day Exploits
  - DNS Tunneling Attacks

Types of Malicious Software

Types of Malicious Software

innovate achieve lead

Classification of Malware

- Malware software or malware is defined as
  - "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."
    - --- NIST SP 800-83 (*Guide to Malware Incident Prevention and Handling for Desktops and Laptops, July 2013*)
- Two broad classifications
  - 1) based on how the malware spreads or *propagates* to reach the desired target
  - 2) based on the actions or payloads it performs once the malware reaches a target
- Propagation mechanisms
  - includes those used by viruses, worms, and Trojans
- Payloads
  - In the world of malware, the term payload is used to describe what a virus, worm or Trojan is designed to do on a victim's computer.
  - For example, payload of malicious programs includes damage to data, theft of confidential information and damage to computer-based systems or processes

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Types of Malicious Software

A Broad Classification of Malware

- Based on Propagation Mechanisms:
  - Virus
    - Infection of existing executable or interpreted content that is subsequently spread to other systems
      - *Binary executables*: E.g., .exe or .com files
      - *Interpretable data files*: E.g., command scripts or a specific application's document files
  - Worms or drive-by-downloads
    - Exploiting software vulnerabilities either locally or over a network to allow the malware to replicate
  - Trojans and Spam Emails
    - Social engineering attacks that convince users to bypass security mechanisms to install Trojans, or to respond to phishing attacks

Types of Malicious Software

A Broad Classification of Malware

- Earlier Approaches to Classification of Malware:
  - Dependent Vs. Independent
    - those that need a host program (parasitic code)
      - E.g., viruses
    - those that are independent (self-contained programs run on the system)
      - E.g., worms, Trojans, and bots
  - Replicating Vs. Non-replicating
    - those that replicate themselves
      - E.g., viruses and worms
    - those that do not replicate
      - E.g., Trojans and spam e-mail

Types of Malicious Software

A Broad Classification of Malware

- Payload Actions performed by malware once it reaches a target system can include:
  - corruption of system
  - corruption of data files
  - theft of service
    - in order to make the system a zombie agent of attack as part of a botnet
  - theft of information from the system
    - especially of logins, passwords, or other personal details by keylogging or spyware programs
  - stealthing
    - where the malware hides its presence on the system from attempts to detect and block it

Types of Malicious Software

Terminology for Malicious Software

Name	Description
Advanced Persistent Threat (APT)	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 mechanism 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 first inserted 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.

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Types of Malicious Software

Terminology for Malicious Software

Name	Description
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, etc) 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.

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Types of Malicious Software

Terminology for Malicious Software

Name	Description
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 it.
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.

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Propagation – Infected Content – Viruses

Viruses

innovate achieve lead

Overview

- Computer viruses first appeared in the early 1980s
  - They constituted the majority of malware during the early personal computer era
- Viruses are like parasites
  - they attach themselves to some existing executable content
- They can infect some application, utility program, system program, or even the code to boot a computer system
- A virus can make copies of itself
  - Whenever the infected computer comes into contact with an uninfected piece of code
- The infection spreads from one computer to another when users exchange files, disks, or USB drives containing these viruses
- Viruses also manifest as scripting code that is used to support active content within data files
  - E.g., Microsoft Word, Excel Spreadsheets, or Adobe PDF documents

Viruses

innovate achieve lead

Nature of Viruses

- A virus that attaches to an executable program can do anything that the program is permitted to do
  - Typically, it can perform any function that is allowed by the privileges of the current user
    - E.g., erasing files and programs
- Viruses dominated the malware scene in the earlier years because of
  - lack of user authentication and access controls on PCs at that time
- Tighter access controls in modern computers significantly hinders the ease of infection by viruses
- This resulted in the development macro viruses that exploit active content supported by some document types
  - E.g., MS Word, Excel, or Adobe PDF documents

Viruses

Components of Virus

- Viruses and many malware types include one or more variants of these components:
  - Infection mechanism:
    - The means by which a virus spreads or propagates (replicates)
      - The mechanism is also referred to as the infection vector
  - Trigger:
    - The event or condition that determines when the payload is activated or delivered
      - Sometimes referred to as a logic bomb.
  - Payload:
    - What the virus does, besides spreading
      - May involve damage or benign but noticeable activity

Phases of a Virus

- A typical virus goes through the following four phases during its lifetime:
  - Dormant phase:
    - The virus is idle initially, but not all viruses have this stage
    - The virus is eventually activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit
  - Propagation phase:
    - The virus places a copy of itself into other programs or into certain system areas on the disk
    - The copy may not be identical to the propagating version; viruses often morph to evade detection
    - Each infected program will now contain a clone of the virus, which will itself enter a propagation phase
  - Triggering phase:
    - The virus is activated to perform the function for which it was intended
    - As with the dormant phase, the triggering phase can be caused by a variety of system events
      - E.g., a count of the number of times that this copy of the virus has made copies of itself.
  - Execution phase:
    - The action may be harmless (E.g., a message on the screen) or damaging (E.g., destruction of programs and data files)

Viruses

Macro and Scripting Viruses

- A macro virus is defined as
  - "*a virus that attaches itself to documents and uses the macro programming capabilities of the document's application to execute and propagate*"
- Reasons why macro viruses are more threatening
  - Platform independence
    - Macro viruses infect active content in applications such as MS Office or scripting code in Adobe PDF documents
    - Any hardware platform and OS that supports these applications can be infected
  - Macro viruses infect documents, not executable portions of the code
    - Most of the information introduced onto a computer system is in the form of documents rather than programs
  - Macro viruses are easily spread
    - Documents are shared by users in their normal use, via emails, for example
    - Documents are mostly opened automatically without prompting the user
  - Traditional file access controls cannot prevent their spread
    - Since macro viruses infect documents rather than system programs, users are expected to modify them
  - Macro viruses are much easier to write
    - Compared to traditional executable viruses

Viruses

Macro and Scripting Viruses

- Protecting from Macro Viruses
  - Microsoft offers optional Macro Virus Protection tool that detects suspicious Word files and alerts the user
  - Since the year 2000, MS Office products improved their macro security
    - They allow the authors to digitally sign their macros for authors to be listed as trusted
  - Users are warned if a document being opened contained unsigned or signed, but untrusted macros
    - Products give an option to disable macros
  - Various anti-virus products also have features that detect and remove micro viruses
  - Recent PDF viewers include measures to warn users when potentially harmful scripting code is run
    - However, the message the user is shown can be manipulated to trick the user into permitting its execution

Viruses

innovate achieve lead

Classification of Viruses

- There is no universally agreed-upon classification scheme for viruses
- One type of classification is along two orthogonal axes:
  - the type of target the virus tries to infect
  - the method the virus uses to conceal itself from detection
- Classification based on target:
  - Boot sector infector
  - File infector
  - Macro virus
  - Multipartite virus
- Classification by concealment strategy
  - Encrypted virus
  - Stealth virus
  - Polymorphic virus
  - Metamorphic virus

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Viruses

innovate achieve lead

Classification of Viruses

- Based on the target:
  - Boot sector infector:
    - Infects a master 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 consider to be executable
  - Macro virus:
    - Infects files with macro or scripting code that is interpreted by an application
  - Multipartite virus:
    - Capable of infecting multiple types of files, so that virus eradication must deal with all of the possible sites of infection

Viruses

innovate achieve lead

Classification of Viruses

- Based on the Concealment Strategy
  - Encrypted virus:
    - A form of virus that uses encryption to obscure it's content
    - A portion of the virus creates a random encryption key and encrypts the remainder of the virus
      - The key is stored with the virus
    - When an infected program is invoked, the virus uses the stored random key to decrypt the virus
    - When the virus replicates, a different random key is selected
    - Because the bulk of the virus is encrypted with a different key for each instance, there is no constant bit pattern to observe.
  - Stealth virus:
    - A form of virus explicitly designed to hide itself from detection by anti-virus software by using code mutation, compression, or rootkit techniques
    - Thus, the entire virus, not just a payload is hidden

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Viruses

Classification of Viruses

- Based on the Concealment Strategy
  - Polymorphic virus:
    - Creates copies that are functionally equivalent but have distinct bit patterns to defeat programs that scan for viruses
      - In this case, the "signature" of the virus will vary with each copy
      - To achieve this variation, the virus may randomly insert superfluous instructions or interchange the order of independent instructions
    - Virus may use encryption
      - The portion of the virus that is responsible for generating keys and performing encryption/decryption is referred to as the mutation engine. The mutation engine itself is altered with each use.
  - Metamorphic virus:
    - As with a polymorphic virus, a metamorphic virus mutates with every infection
    - The difference is that a metamorphic virus rewrites itself completely at each iteration, using multiple transformation techniques, increasing the difficulty of detection
    - Metamorphic viruses may change their behavior as well as their appearance

Propagation – Vulnerability Exploit – Worms

Worms

innovate achieve lead

Overview

- The concept of a computer worm was introduced in John Brunner's 1975 Science Fiction novel *The Shockwave Rider*
- The first known worm implementation was done in Xerox Palo Alto Labs in the early 1980s
  - It was non-malicious, searching for idle systems to use to run a computationally intensive task
- Worm programs exploit software vulnerabilities in client or server programs to gain access to each new system
- Machines infected by worms can act as a launch pad for attacks on other machines
- Worms can spread through
  - network connections from system to system, or
  - shared media, such as USB drives or CD and DVD data disks
  - macro or script code in documents attached to e-mail or to instant messenger file transfers
- Upon activation, the worm may replicate and propagate again
- In addition to propagation, the worm usually carries some form of payload

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Worms

How Worms Replicate?

- Electronic mail or instant messenger facility:
  - A worm e-mails a copy of itself to other systems, or sends itself as an attachment via an instant message service, so that its code is run when the e-mail or attachment is received or viewed
- File sharing:
  - A worm either creates a copy of itself or infects other suitable files as a virus on removable media such as a USB drive; it then executes
    - when the drive is connected to another system using the autorun mechanism by exploiting some software vulnerability, or
    - when a user opens the infected file on the target system
- Remote execution capability:
  - A worm executes a copy of itself on another system, either by using an explicit remote execution facility or by exploiting a program flaw in a network service to subvert its operations
- Remote file access or transfer capability:
  - A worm uses a remote file access or transfer service to another system to copy itself from one system to the other, where users on that system may then execute it.
- Remote login capability:
  - A worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other, where it then executes

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Worms

Phases of Worms

- A worm typically uses the same phases as a computer virus:
  - dormant, propagation, triggering, and execution
- In the propagation phase, a worm:
  - searches for appropriate access mechanisms to other systems
    - by examining host tables, address books, buddy lists, trusted peers, and other similar repositories of remote system access details
  - uses the access mechanisms found to transfer a copy of itself to the remote system, and cause the copy to be run
- The worm may also attempt to determine whether a system has previously been infected before copying itself to the system
- A worm can also disguise its presence by naming itself as a system process or using some other name that may not be noticed by a system operator
- Some worms can even inject their code into existing processes, and run using additional threads in that process, to further disguise their presence

Worms

innovate achieve lead

Target Discovery

- In the propagation phase, worms discover their target systems to infect through a process of scanning or fingerprinting
- Typically, worms use the following network address scanning strategies
  - Random:
    - Each compromised host probes random addresses in the IP address space.
    - This technique 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
    - This can be a slow process done over a long period to avoid detection that an attack is underway
    - 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
  - 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.

Worms

innovate achieve lead

Client-Side Vulnerabilities and Drive-by Downloads

- Exploiting software vulnerabilities involves the use of bugs in user applications to install malware
- A common technique exploits browser and plugin vulnerabilities
- Drive-by-download
  - When a user views a webpage controlled by the attacker, it contains the code that installs malware without user's knowledge or consent
- Attackers exploited multiple vulnerabilities in the Adobe Flash Player and Oracle Java plugins over many years
- In most cases, this malware does not actively propagate like a worm. Instead, it waits for the user to visit the infected webpage in order to spread to their systems
- In general, drive-by-download attacks are aimed at anyone who visits a compromised site

Worms

Client-Side Vulnerabilities and Drive-by Downloads

- Watering-hole attacks
  - These are a variant of drive-by-download attacks, used in highly targeted cases
  - The attacker researches their victims to identify websites they are likely to visit
  - Then, scans these sites to identify those with vulnerabilities that allow their compromise with a drive-by-download attack
  - The attacker then waits for one of the intended victims to visit these compromised sites
  - The attack code can be customized such that it will only infect systems belonging to the target organization
    - It takes no action for other visitors to the site
    - This increases the likelihood of the site compromise remaining undetected

Worms

Client-Side Vulnerabilities and Drive-by Downloads

- Malvertising
  - It is a technique used to place malware on websites without actually compromising them
  - The attacker pays for advertisements (containing malware) that are highly likely to be placed on their intended target websites
  - Using these malicious ads, attackers can infect visitors to these sites
  - The malware code may be dynamically generated to either reduce the chance of detection, or to only infect specific systems
  - Attackers can even place these ads for just a few hours when their intended victim is expected to browse the targeted website
  - Malvertising has grown rapidly as they are easy to place with few questions asked

Worms

Clickjacking (or user-interface (UI) redress attack)

- Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element
- This can cause users to
  - unknowingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online
- Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees
- The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.
- Thus, the attacker is hijacking clicks meant for one page and routing them to another page, most likely owned by another application, domain, or both
- Using a similar technique, keystrokes can also be hijacked
- With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account
  - instead, they are typing into an invisible frame controlled by the attacker

Worms

A Brief History of Worm Attacks

Year	Name	Exploited	Details
1998	Melissa	Email	Includes aspects of virus, worm, and Trojan. Embedded in the MS Word macro. Activated by opening the attachment
1999	More powerful version of Melissa	Email	Activated by opening an email that contains the virus, rather than by opening the attachment Propagates itself as soon as it is activated to all of the e-mail addresses known to the infected host The virus uses the Visual Basic scripting language supported by the email software Infected over 100,000 computers in 3 days
2001	Code Red	MS Internet Information Server	Exploits a security hole in MS Internet Information Server (IIS) to penetrate and spread Probes random IP addresses to spread to other hosts Can initiate a denial-of-service attack against a government Web site by flooding the site with packets from numerous hosts Code Red infected nearly 360,000 servers in 14 hours
2001	Code Red II	MS Internet Information Server	Targeted MS IIS It tried to infect systems on the same subnet as the infected system Also, this newer worm installs a backdoor, allowing a hacker to remotely execute commands on victim computers

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Worms

A Brief History of Worm Attacks

Year	Name	Exploited	Details
2001	Nimda	Email	It has worm, virus, and mobile code characteristics It spread using a variety of distribution methods: Email, Windows Shares, Web Servers, Web Clients, and Backdoors
2003	SQL Slammer	Buffer overflow in MS SQL Server	Extremely compact and spreads rapidly Infected 90% of vulnerable hosts in 10 minutes. This rapid spread caused significant congestion on the Internet
2003	Sobig.F	Open Proxy servers	Turns infected machines into spam engines At its peak, Sobig.F accounted for one in every 17 messages Produced more than 1Million copies of itself within the first 24 hours
2004	Mydoom	Email	This is a mass-mailing email work Installs backdoors in infected computers and enables hackers to gain remote access to access data such as passwords and credit card numbers Replicated up to 1,000 times per minute Flooded the Internet with 100 million infected messages in 36 hours

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Worms

A Brief History of Worm Attacks

Year	Name	Exploited	Details
2006	Warezov	Email	Creates several executables in system directories and sets itself to run every time Windows starts by creating a registry entry Scans several types of files for e-mail addresses and sends itself as an e-mail attachment Some variants are capable of downloading other malware, such as Trojan horses and adware Many variants disable security-related products and/or disable their updating capability.
2008	Conficker or Downadup	Windows buffer overflow	It spread initially by exploiting a Windows buffer overflow vulnerability Later versions could also spread via USB drives and network file shares Even though patches were available from Microsoft to close the main vulnerabilities it exploits
2010	Stuxnet	Industrial Control Systems	Targeted industrial control systems, mostly connected with Iranian nuclear program Supported a range of propagation mechanisms – USB drives, network file shares, and four zero-day vulnerability exploits First serious use of a cyberwarfare weapon against a nation's physical infrastructure Researchers who analyzed Stuxnet expected to find espionage, but never the malware with targeted sabotage as its aim
2011	Duqu		Uses code related to that in Stuxnet Its aim is cyber-espionage, to target Iranian nuclear program

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Worms

A Brief History of Worm Attacks

Year	Name	Exploited	Details
2012	Flame family		Its aim is cyber-espionage, appears to target Middle-Eastern countries Their infection strategies have been very successful that they were identified on computer systems in a very large number of countries
2017	WannaCry	SMB file sharing service on unpatched Windows systems	It's used in ransomeware attack Spread extremely rapidly over a period of hours to days Infected 100s of 1000s of systems from both public and private organizations in more than 150 countries Once installed on infected systems, it also encrypted files, demanding a ransom payment to recover them

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Propagation - Social Engineering – Spam Email, Trojans

Spam Email & Trojans

innovate achieve lead

Spam E-Mail

- Large volumes of email sent to 1000s of email IDs
- Imposes significant costs on two aspects:
  - the network infrastructure needed to relay this traffic, and
  - on users who need to filter their legitimate email out of this flood
- In response to this explosive growth, there has been equally rapid growth of the anti-spam industry
- There is an arms race between the spammers devising techniques to sneak their content through, and the defenders' effort to block them

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Spam Email & Trojans

innovate achieve lead

Spam E-Mail

- Some spam emails are sent from legitimate mail servers using stolen user credentials
- Most spam is sent by botnets using compromised user systems
- A significant portion of spam e-mail content is just advertising
- Spam is also a significant carrier of malware
- Spam may be used in a phishing attack, where it directs the user
  - either to a fake website that mirrors some legitimate service such as online banking site, where it attempts to capture the user's login credentials
  - or to complete some form with sufficient personal details to allow the attacker to impersonate the user in an identity theft
- Now a days, the criminal marketplace makes phishing campaigns easier by selling packages to scammers that largely automate the spam process

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Spam Email & Trojans

innovate achieve lead

Trojan Horses

- A Trojan horse is an "apparently" useful program containing hidden code, that when invoked, performs unwanted or harmful function
- Trojan horse programs can be used to accomplish functions indirectly that the attacker could not accomplish directly. For example:
  - A Trojan horse program can scan user's files and sends a copy of sensitive, personal information to the attacker
- Trojan horse programs can be incorporated into a game or useful utility program, and make it available via a known software distribution site or app store
  - E.g., Utility software that "claims" to be the latest anti-virus scanner, or security update, for systems, but are actually malicious Trojans
  - These Trojans often carry payloads such as spyware that search for banking credentials

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Spam Email & Trojans

innovate achieve lead

Trojan Horses

- Trojan horses fit into one the three models
- Model-1
  - Continuing to perform the function of the original program and additionally performing a separate malicious activity.
- Model-2
  - Continuing to perform the function of the original program but
    - Modifying the function to perform malicious activity
      - E.g., a Trojan horse version of a login program that collects passwords
    - Or to disguise other malicious activity
      - E.g., a Trojan horse version of a process listing program that does not display certain processes that are malicious
- Model-3
  - Performing a malicious function that completely replaces the function of the original program

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – System Corruption

Payload – System Corruption

innovate achieve lead

Overview

- Once a malware is active on the target system, the next question is what actions will it take on this system
  - That is, what payload does it carry?
- Different actions that malware can perform
  - Some malware has a nonexistent or nonfunctional payload
    - Its only purpose is to spread
  - Early payloads in a number of viruses and worms resulted in data destruction
  - Another variant of payload inflicts real-world damage on the system
    - Causes damage to physical equipment
- Usually, malware carries one or more payloads that perform covert actions
- Typically, payloads target the integrity of the computer system's software or other user data
  - These changes occur when specific trigger conditions are met

Payload – System Corruption

innovate achieve lead

Data Destruction and Ransomware

- Chernobyl Virus
  - First appeared in 1998
  - Example of a destructive parasitic memory-resident Windows-95 and 98 virus
  - It infects executable files when they are opened
  - When a trigger date is reached, it deletes data on the infected system by overwriting the first megabyte of the hard drive with zeroes
    - Results in massive corruption of the entire file system
    - This event first occurred on April 26, 1999
  - It is estimated that more than one million computers were affected

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – System Corruption

innovate achieve lead

Data Destruction and Ransomware

- Klez mass-mailing worm
  - First seen in October 2001
  - An early example of a destructive worm infecting Windows-95 to XP systems
  - Spreads by e-mailing copies of itself to addresses found in the address book and in files on the system
  - It can stop and delete some anti-virus programs running on the system
  - On trigger date, it causes files on the local hard drive to become empty

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – System Corruption

innovate achieve lead

Data Destruction and Ransomware

- Ransomware
  - Don't destroy data
  - Instead, encrypts the user's data and demands payment in order to access the key needed to recover the information
  - Ransomware is often spread via "drive-by-downloads" or via SPAM e-mails
- PC Cyborg Trojan
  - First seen in 1989 was an early example of ransomware
  - Around mid-2006, a number of worms and Trojans appeared, such as the Gpcode Trojan
    - They used public-key cryptography with increasingly larger key sizes to encrypt data
  - The user needed to pay a ransom, or to make a purchase from certain sites, in order to receive the key to decrypt this data.

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – System Corruption

innovate achieve lead

Data Destruction and Ransomware

- WannaCry Ransomware
  - Infected a large number of systems in many countries in May 2017
  - It encrypted a large number of files and then demanded a ransom payment in Bitcoins to recover them
  - Recovery of this information was only possible if the organization had
    - good backups and recovery plan, and
    - an appropriate incident response and disaster recovery plan
  - Generated a significant media attention because
    - a large number of organizations were affected and the significant costs they incurred in recovering from it
  - Following tactics were used to put pressure on the victim to pay up
    - threatening to publish sensitive personal information, or
    - threatening to permanently destroy the encryption key after a short period of time

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – System Corruption

innovate achieve lead

Real-World Damage

- A variant of system corruption payloads aims to cause damage to physical equipment
- Chernobyl Virus
  - The Chernobyl virus not only corrupts data, but attempts to rewrite the BIOS code used to initially boot the computer
  - If it is successful, the boot process fails, and the system is unusable until the BIOS chip is either re-programmed or replaced

Payload – System Corruption

innovate achieve lead

Real-World Damage

- Stuxnet worm
  - Targets some specific industrial control system software as its key payload
  - If control systems using certain Siemens industrial control software with a specific configuration of devices are infected
    - then the worm replaces the original control code with code that deliberately drives the controlled equipment outside its normal operating range
    - results in the failure of the attached equipment
  - Centrifuges used in the Iranian Uranium Enrichment program
    - During the time when this worm was active, these centrifuges experienced much higher than normal failure rates
    - These centrifuges were strongly suspected as the target of this attack
- The December 2015 attack that disrupted Ukranian power systems is another example of attack on infrastructure
- https://www.youtube.com/watch?v=_F3w911tgko
- https://www.youtube.com/watch?v=7g0pi4J8auQ

Payload – System Corruption

innovate achieve lead

Logic Bomb

- Code embedded in the malware that is set to "explode" when certain conditions are met
- Examples of triggering conditions:
  - Presence or absence of certain files or devices on the system
  - A particular day of the week or date
  - A particular version or configuration of some software
  - A particular user running the application
- Once triggered, a bomb may alter or delete data or entire files, cause a machine halt, or do some other damage

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – System Corruption

innovate achieve lead

Logic Bomb

- The case of Tim Lloyd
  - A striking example of how logic bombs can be employed
  - Lloyd worked at Omega for 11 years, had long been a trusted employee
  - He was convicted of setting a logic bomb that:
    - cost his employer, Omega Engineering, more than $10 million
    - derailed its corporate growth strategy, and
    - eventually led to the layoff of 80 workers
  - Ultimately, Lloyd was sentenced to 41 months in prison and ordered to pay $2 million in restitution
- References
  - https://www.computerworld.com/article/2596062/computer-sabotage-verdict-set-aside.html
  - https://edition.cnn.com/2000/TECH/computing/06/27/omega.files.idg/
  - https://www.cnet.com/tech/services-and-software/software-time-bomber-goes-to-prison/

Payload – Attack Agent – Zombie, Bots

Payload – Attack Agent – Zombie, Bots

Overview

- Takes over another Internet-attached computer and uses that computer to launch or manage attacks
  - attacks are difficult to trace back to the bot's creator
- Such a system is known as a bot (robot), zombie or drone
- A bot is typically planted on hundreds or thousands of computers belonging to unsuspecting third parties
- Botnet - collection of such bots capable of acting in a coordinated manner
- This type of payload attacks the integrity and availability of the infected system

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – Attack Agent – Zombie, Bots

Uses of Bots

- Distributed denial-of-service (DDoS) attacks:
  - A DDoS attack is an attack on a computer system or network that causes a loss of service to users
- Spamming:
  - With the help of a botnet consisting of thousands of bots, an attacker is able to send massive amounts of bulk e-mail (spam)
- Sniffing traffic:
  - Bots can also use a packet sniffer to watch for interesting clear-text data passing by a compromised machine
  - The sniffers are mostly used to retrieve sensitive information like usernames and passwords.
- Keylogging:
  - Bots can also be used as keyloggers
  - A keylogger can captures and sends keystrokes on the infected machine to the attacker

Payload – Attack Agent – Zombie, Bots

innovate achieve lead

Uses of Bots

- Spreading new malware:
  - Botnets are used to spread new bots
  - This is very easy since all bots implement mechanisms to download and execute a file via HTTP or FTP
  - A botnet with 10,000 hosts that acts as the start base for a worm or mail virus allows very fast spreading and thus causes more harm
- Installing advertisement add-ons and browser helper objects (BHOs):
  - Botnets can also be used to gain financial advantages
  - This works by setting up a fake Web site with some advertisements:
    - The operator of this Web site negotiates a deal with some hosting companies that pay for clicks on ads
    - With the help of a botnet, these clicks can be "automated" so that instantly a few thousand bots click on the pop-ups
    - This process can be further enhanced if the bot hijacks the start-page of a compromised machine so that the "clicks" are executed each time the victim uses the browser

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – Attack Agent – Zombie, Bots

innovate achieve lead

Uses of Bots

- Attacking Internet Relay Chat (IRC) networks:
  - Botnets are also used for attacks against chat networks
  - Popular among attackers is especially the so-called clone attack:
    - In this kind of attack, the controller orders each bot to connect a large number of clones to the victim IRC network
    - The victim is flooded by service requests from thousands of bots or thousands of channel-joins by these cloned bots
    - In this way, the victim IRC network is brought down, similar to a DDoS attack
- Manipulating online polls/games:
  - Online polls/games are getting more and more attention and it is rather easy to manipulate them with botnets
  - Since every bot has a distinct IP address, every vote will have the same credibility as a vote cast by a real person
  - Online games can be manipulated in a similar way.

innovate achieve lead

Payload – Information Theft
Keyloggers, Phishing, Spyware

Types of Malicious Software

innovate achieve lead

A Broad Classification of Malware

- So far, we have seen different classification of malware
- Based on Propagation Mechanisms:
  - Infected Content – Virus
  - Vulnerability Exploit – Worms or drive-by-downloads
  - Social Engineering – Trojans and Spam Emails
- Based on Payload (Action performed)
  - System Corruption
  - Attack Agent – Zombie, Bots
  - Information Theft – Keyloggers, Phishing, Spyware
  - Stealthing – Backdoors, Rootkits

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – Information Theft

innovate achieve lead

Overview

- In the next set of payloads, the malware gathers data stored on the infected system for use by the attacker
- A common target is the user's login credentials to banking, gaming, and related sites
  - The attacker uses these to impersonate the user to gain profit
- The payload may target documents or system configuration details for the purpose of reconnaissance or espionage
- These attacks target the confidentiality of this information

Payload – Information Theft

innovate achieve lead

Credential Theft, Keyloggers, and Spyware

- Typically, User ID & password are transmitted over encrypted communication channels (e.g., HTTPS or POP3S)
  - This protects them from capture by monitoring network packets
- To bypass this, an attacker can install a *keylogger*
  - A keylogger captures keystrokes from the user and sends data back to the attacker
  - The attacker receives a copy of all text entered on the compromised machine
- So, keyloggers use a filtering mechanism to only return information close to desired keywords
  - E.g., "login" or "password" or "paypal.com"

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – Information Theft

innovate achieve lead

Credential Theft, Keyloggers, and Spyware

- To counter keyloggers, some sites (E.g., banking) use a graphical applet to enter critical information, such as passwords
- Since these graphical applets do not use keyboard, traditional keyloggers are incapable of capturing this information
- In overcome this, attackers developed *spyware* payloads
- Spyware allows monitoring of a wide range of activity on the system:
  - Monitoring the history and content of browsing activity
  - Redirecting certain Web page requests to fake sites controlled by the attacker, and
  - Dynamically modifying data exchanged between the browser and certain Web sites of interest

Payload – Information Theft

innovate achieve lead

Credential Theft, Keyloggers, and Spyware

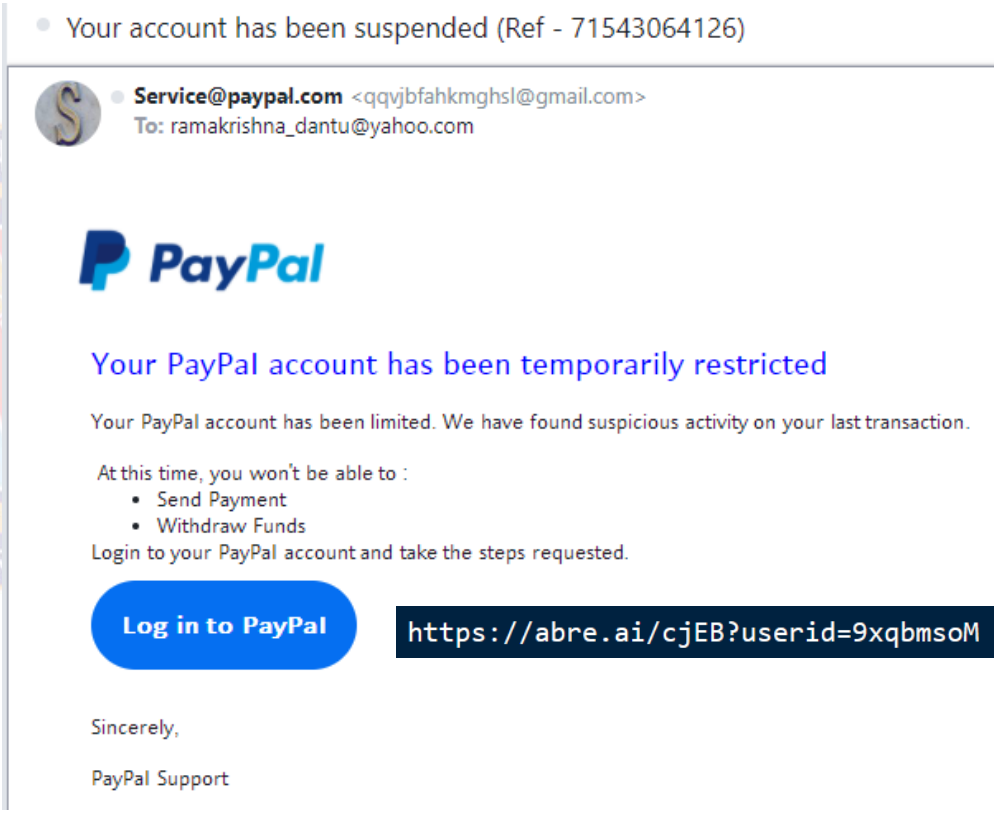
- Zeus banking Trojan
  - A prominent example of spyware
  - First identified in 2007 and became widespread by March 2009
  - Runs on versions of Microsoft Windows
  - Created using a crimeware toolkit
  - Used to steal banking information by
    - man-in-the-browser keystroke logging and
    - form grabbing
  - Zeus is spread mainly through:
    - drive-by downloads and
    - phishing schemes

Payload – Information Theft

innovate achieve lead

Phishing and Identity Theft

- Phishing
  - Involves capturing user login and password credentials using a spam email
  - This spam email includes some message suggesting that urgent action is required by the user to authenticate their account, to prevent it being locked
  - The technique includes a URL that links to
    - a fake Web site controlled by the attacker, or
      - This web site mimics the login page of some banking, gaming, or similar site
    - a form that that once filled and submitted goes to attacker's email
      - The form includes a range of personal information about the user
  - Such spam e-mails are typically widely distributed to very large numbers of users, often via a botnet



Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – Information Theft

innovate achieve lead

Phishing and Identity Theft

- Spear-Phishing
  - A more dangerous variant of general Phishing attack
  - This again is an e-mail claiming to be from a trusted source
  - However,
    - the recipients are carefully researched by the attacker
    - each e-mail is carefully crafted to suit its recipient specifically
    - often it quotes a range of information to convince them of its authenticity
  - This greatly increases the likelihood of the recipient responding as desired by the attacker
  - This type of attack is particularly used in industrial and other forms of espionage by well-resourced organizations

Payload – Stealthing – Backdoors, Rootkits

Payload – Stealthing

innovate achieve lead

Backdoor

- Also known as a trapdoor, a secret entry point into a program or System
- Allows someone to gain access without going through the usual security access procedures
- The backdoor is a code that recognizes some special sequence of input or is triggered by being run from a certain user ID
- Programmers used backdoors legitimately for many years to debug and test programs
  - Such a backdoor is called a *maintenance hook*
- This usually is done when the programmer is developing an application that has an authentication procedure, or a long setup, requiring the user to enter many different values to run the application
- To debug the program, the developer may wish to gain special privileges or to avoid all the necessary setup and authentication
- The WannaCry ransomware included such a backdoor

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – Stealthing

innovate achieve lead

Rootkit

- Originally, a rootkit was a collection of tools that enabled administrator-level access to a computer or network
  - Root refers to the Admin account on Unix and Linux systems
  - Kit refers to the software components that implement the tool
- Today rootkits are generally associated with malware – such as Trojans, worms, viruses – that conceal their existence and actions from users and other system processes
- A rootkit is a set of programs that allows covert (unauthorized) access to that system
- A rootkit allows someone to maintain command & control over a computer without the computer user/owner knowing about it
- A rootkit may contain a number of malicious tools such as keyloggers, banking credential stealers, password stealers, antivirus disablers, and bots for DDoS attacks

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – Stealthing

innovate achieve lead

Rootkit

- Once a rootkit has been installed, the controller of the rootkit has the ability to
  - remotely execute files and
  - change system configurations on the host machine
- Gives administrator (or root) privileges to attacker
  - can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand
- A rootkit can make many changes to a system to hide its existence
  - makes it difficult for the user to determine that the rootkit is present and to identify what changes have been made
- A rootkit can hide even from the mechanisms that monitor and report on the processes, files, and registries on a computer

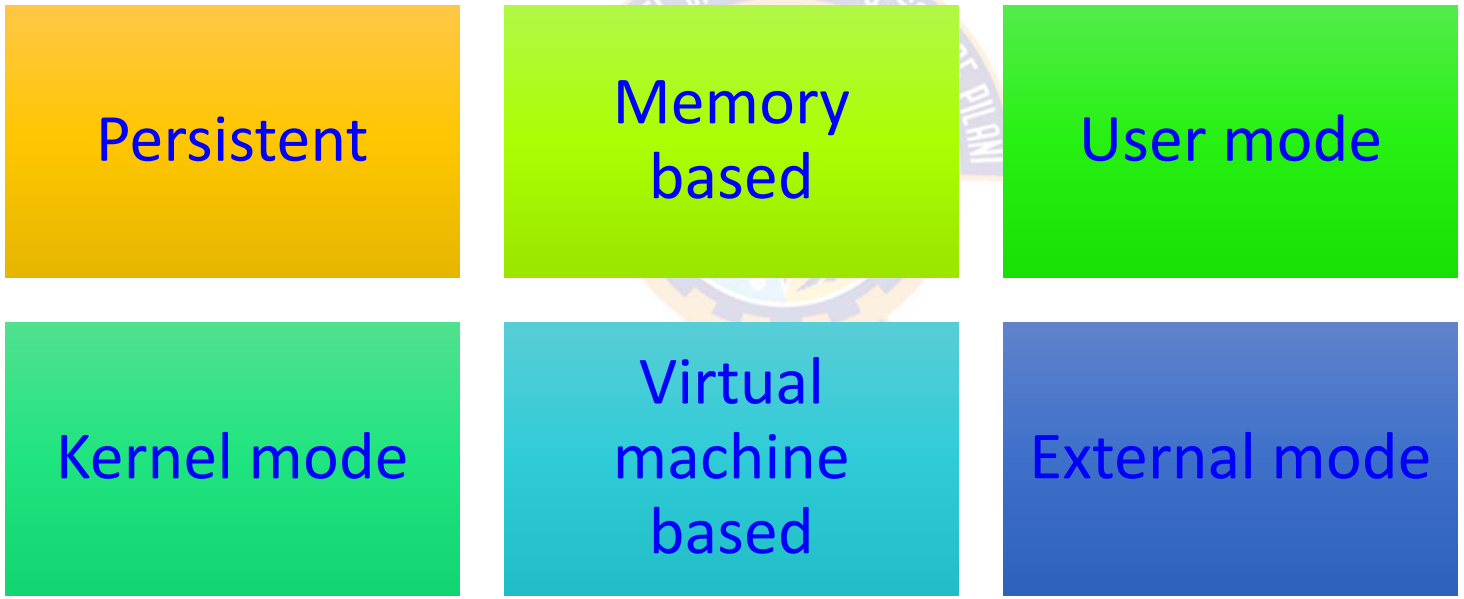
Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – Stealthing

innovate achieve lead

Rootkit

- Classification of rootkits based on certain characteristics



Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – Stealthing

innovate achieve lead

Rootkit

- Persistent:
  - Activates each time the system boots
  - The rootkit must store code in a persistent store, such as the registry or file system, and configure a method by which the code executes without user intervention
  - This means it is easier to detect, as the copy in persistent storage can potentially be scanned
- Memory based:
  - Has no persistent code and therefore cannot survive a reboot
  - However, because it is only in memory, it can be harder to detect
- User mode:
  - Intercepts calls to APIs (application program interfaces) and modifies returned results
  - For example, when an application performs a directory listing, the return results do not include entries identifying the files associated with the rootkit.

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – Stealthing

innovate achieve lead

Rootkit

- Kernel mode:
  - The kernel is a computer program at the core of a computer's operating system that has complete control over everything in the system
  - Rootkit can intercept calls to native APIs in kernel mode
  - The rootkit can also hide the presence of a malware process by removing it from the kernel's list of active processes.
- Virtual machine based:
  - This type of rootkit installs a lightweight virtual machine monitor, and then runs the operating system in a virtual machine above it
  - The rootkit can then transparently intercept and modify states and events occurring in the virtualized system
- External mode:
  - The malware is located outside the normal operation mode of the targeted system, in BIOS or system management mode, where it can directly access hardware

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!