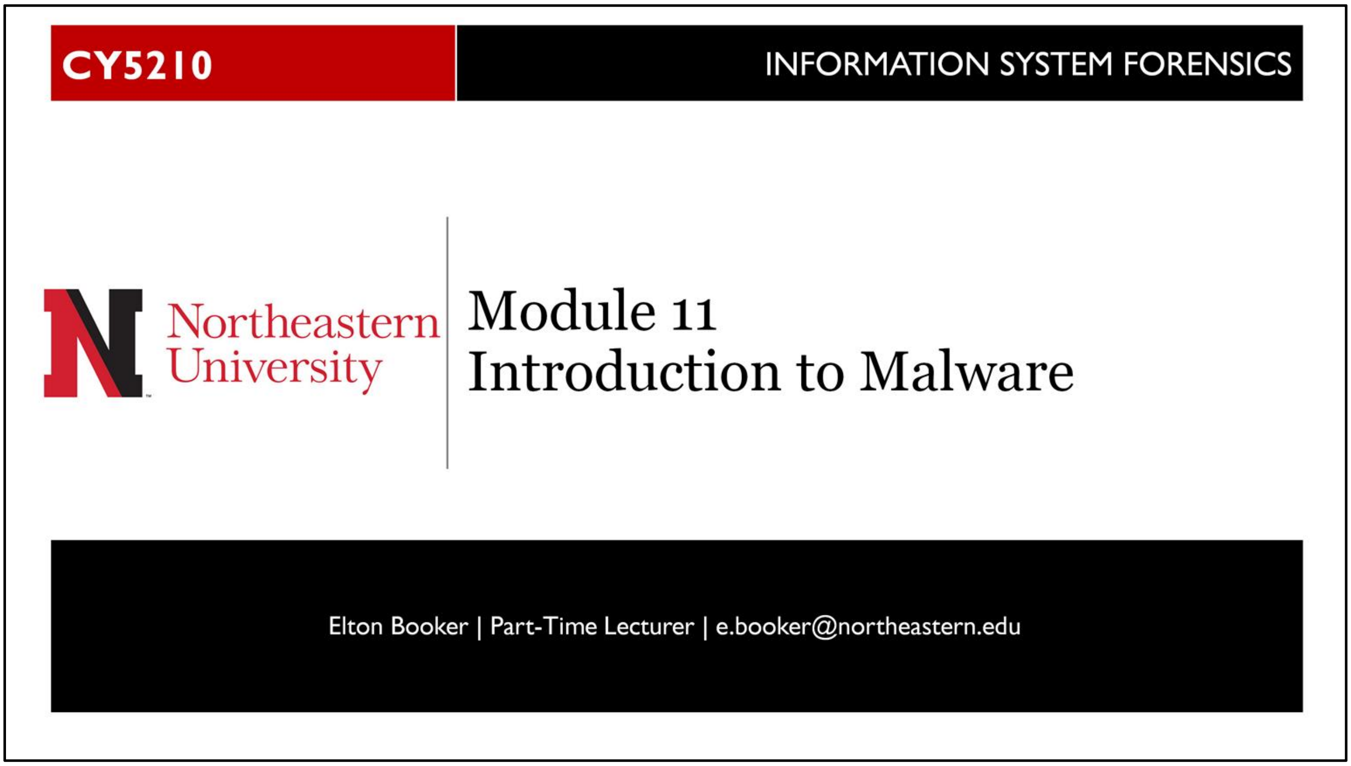


CY5210 INFORMATION SYSTEM FORENSICS

Northeastern University

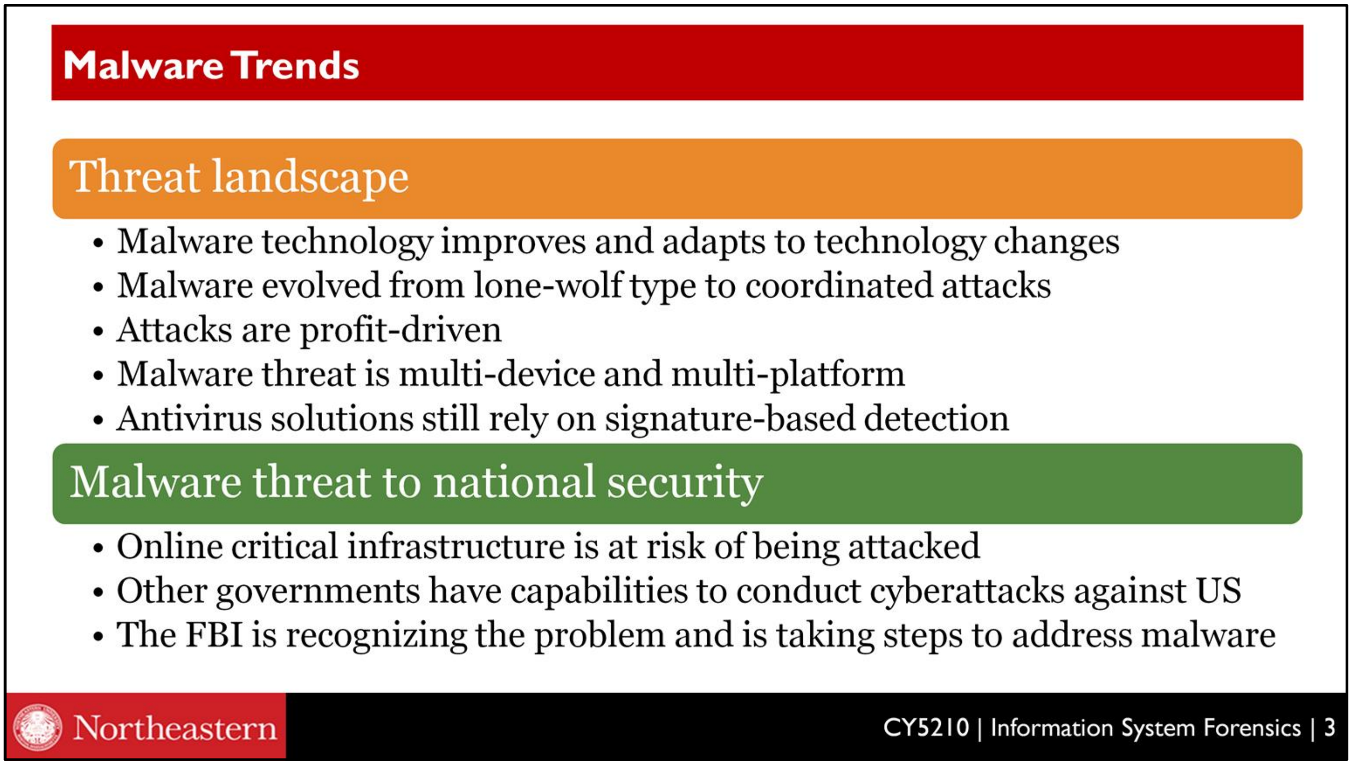
Module 11 Introduction to Malware

Elton Booker | Part-Time Lecturer | e.booker@northeastern.edu

This page intentionally left blank.

History of Malware

CY5210
Information System Forensics



Malware Trends

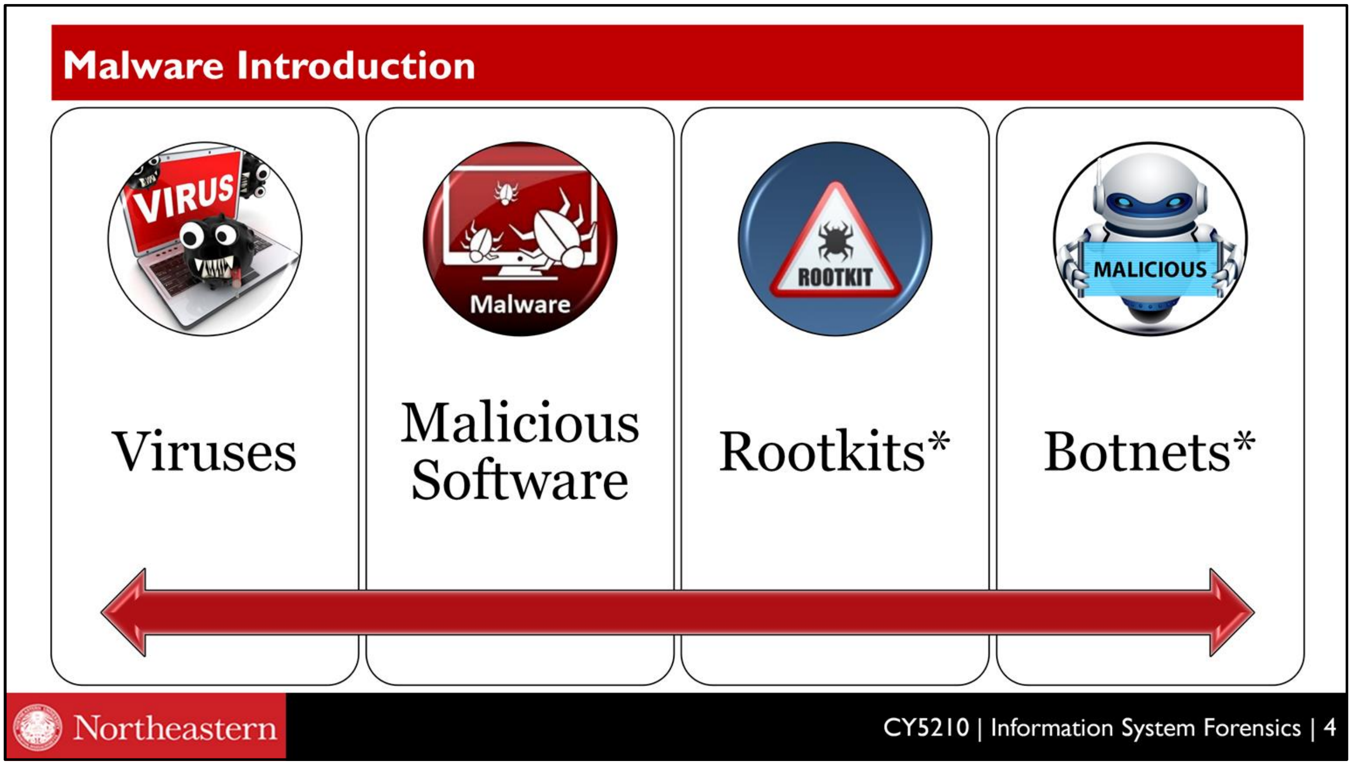
Threat landscape

- Malware technology improves and adapts to technology changes
- Malware evolved from lone-wolf type to coordinated attacks
- Attacks are profit-driven
- Malware threat is multi-device and multi-platform
- Antivirus solutions still rely on signature-based detection

Malware threat to national security

- Online critical infrastructure is at risk of being attacked
- Other governments have capabilities to conduct cyberattacks against US
- The FBI is recognizing the problem and is taking steps to address malware

When the first known computer virus (ELK Cloner) appeared in 1982, no one knew what to call it. In 1984, Dr. Frederick Cohen introduced the term “computer viruses” in a research paper, and malicious programs have been called computer viruses since. Early malicious programs were mostly file infectors and self-replicators, making the term “virus” appropriate for programs that spread by infection.



Malware Introduction

Viruses

Malicious Software

Rootkits*

Botnets*

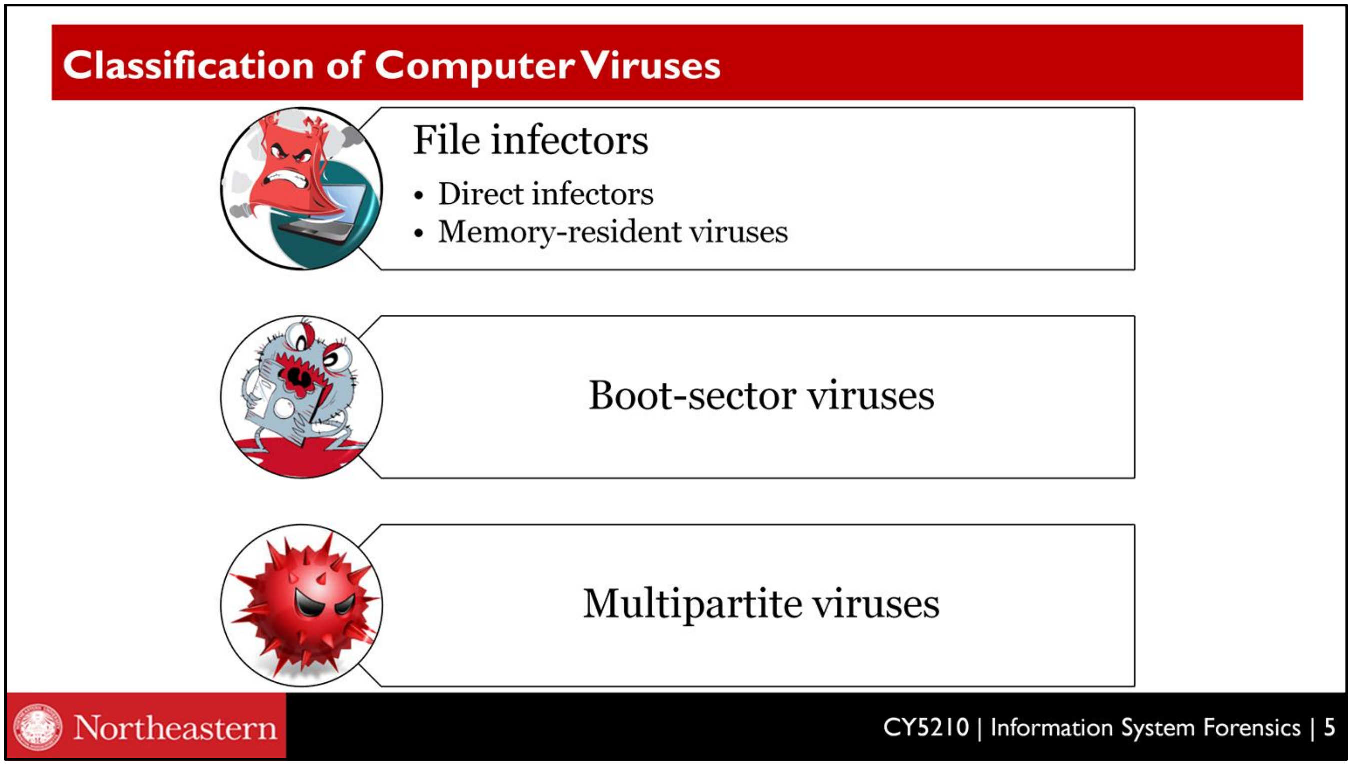
VIRUS
Malware
ROOTKIT
MALICIOUS

Northeastern

CY5210 | Information System Forensics | 4

This lecture will look at various types/classifications of malware and the history of malware, to some extent.

1. **Viruses** – Viruses are self-replicating programs that spread from one host to another. Viruses are typically based on the object they infect, such as files, boot-sectors, macros, etc.
2. **Malware** – malware, or malicious software, soon became the name for any malicious software, including viruses. Malware can be classified in many ways, including based on behavior, target platform, or even the attack directive.
3. **Rootkits** – a set of tools that enable root- or administrator-level access on a system.
4. **Botnets** – a network of robots that execute tasks without user intervention.



Classification of Computer Viruses

File infectors

- Direct infectors
- Memory-resident viruses

Boot-sector viruses

Multipartite viruses

Northeastern

CY5210 | Information System Forensics | 5

Computer viruses may be classified in several ways, which typically relate to what object the virus actually infects, but not always.

File infectors were the reason for the term computer virus, as they defined this era. There are two types of file infectors; direct infectors and memory-resident viruses.

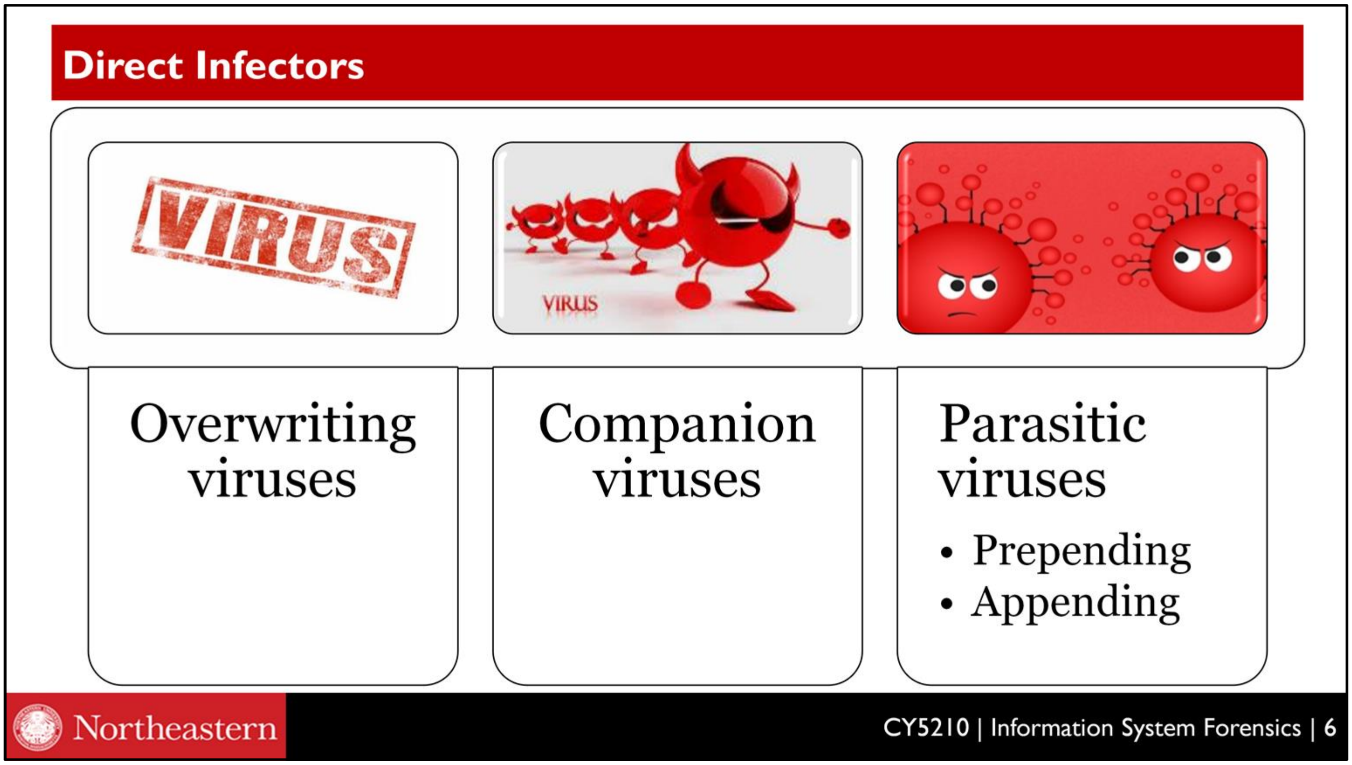
Direct infectors
Direct infectors are computer viruses that immediately infect files as soon as they are executed and actively search for files to infect. The search parameters for infection vary from files in the same folder or the entire disk.

Memory-resident viruses
Memory-resident viruses do not infect files directly upon execution, but rather hide and wait in memory until a host program is executed. The infection strategies are the same: overwrite a host program, be a companion virus, and they can use parasitic techniques to infect host programs.

Boot-sector viruses infect the boot sector of a disk to get control of the system's execution flow before the OS. A boot-sector virus works by hijacking the first instruction in the boot sector to point to itself, and then passes control back to the boot sector code after virus execution. These types of viruses typically spread via an infected floppy disk boot-sector. The risk of infection was higher if a floppy disk was not write-protected and was inserted in a system where a boot-sector virus was already active.

Recall that a boot sector is typically 512-bytes, therefore, the virus utilizes other sectors on the disk to hide its code. If a machine has a hard drive, a boot-sector virus might infect the drive's Master Boot Record (MBR) located at the first sector of the device and contains the boot code and partition table (identifying the bootable partition). The virus can hijack the boot code in the MBR or find the boot sector of the bootable partition instead.

Multipartite viruses are viruses that infect both boot sectors and files. These viruses are also capable of multiplatform infection. Multipartite is an adjective defined as having several or many parts or divisions. More specifically, in biology, a multipartite virus exist as two or more separate but incomplete particles. These viruses can infect both boot sectors and files, since it has both components and does not have to be in a particular order.



Direct Infectors

Overwriting viruses

Companion viruses

Parasitic viruses

- Prepending
- Appending

Northeastern

CY5210 | Information System Forensics | 6

Direct infectors can be divided into several types:

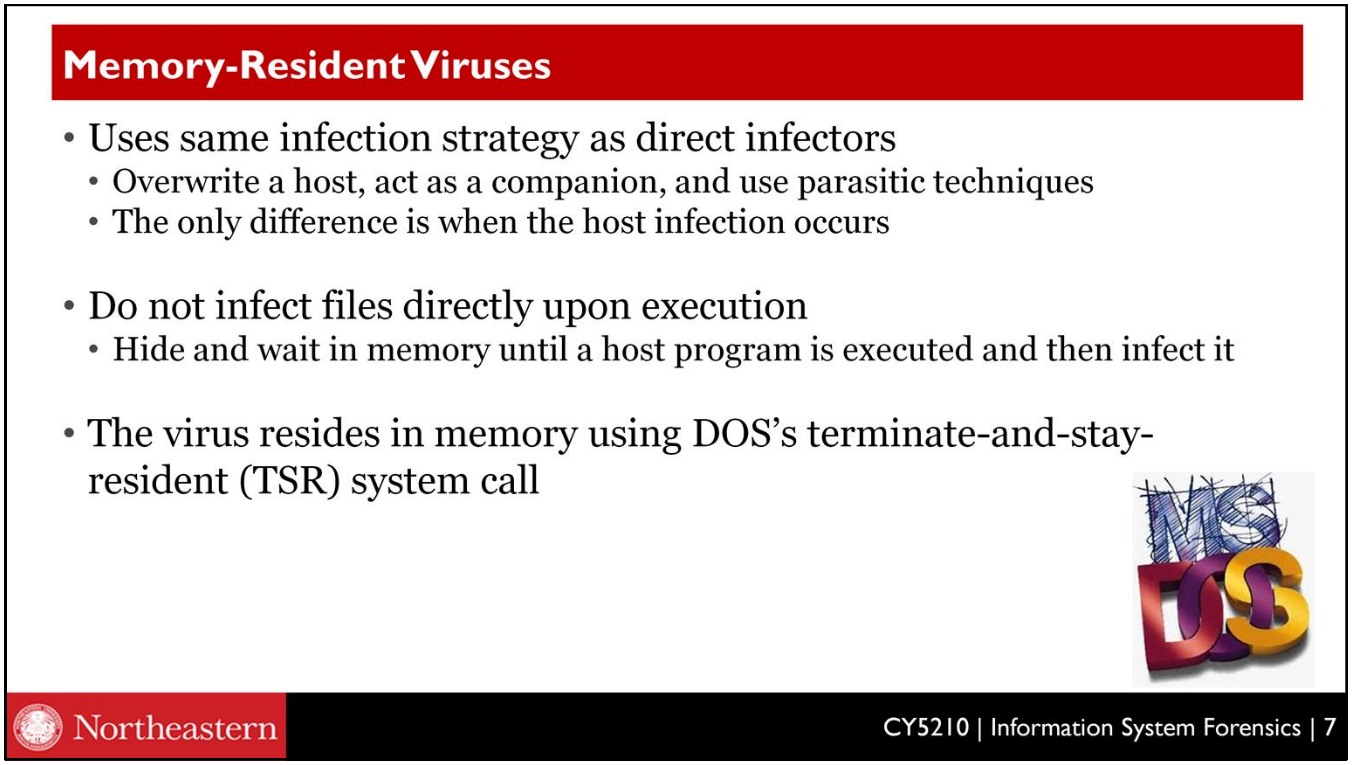
Overwriting viruses – overwrite the host files they infect with their own malware code. This type of infection results in the total destruction of the host file due to the original file's code being overwritten. Hence, these viruses were considered the first destructive computer virus. There is no way to recover from this infection. The original file may be completely or partially overwritten, depending on the source file and virus code size. The end result is often the overwriting virus code with the name of the now-overwritten host (target) file.

There are some overwriting viruses that simply replace the host file entirely with its own copy. This results in the resulting file being equivalent to the virus with the name of the host file, regardless of the original host file size. This method only needs a few lines of code and makes the malware smaller and faster. This makes detection easier by simply listing the files in a directory, which might result in all files being the same size, and depending on routines, the original timestamps of the host file may not be retained; therefore the timestamps will have the same date as the infection; these were telltale signs of infection and could detect malware upon visual inspection. Also, from a user perspective, the intended host file will not execute because the original file was overwritten.

Companion viruses – rename the host file's extension and then create a copy of itself with the name of the host file. The renamed host file is also given a hidden attribute so it cannot be easily viewed in directory listings. In DOS and Windows, there is an order of execution based on file extension (.BAT, .EXE, .COM for example). This is why it became best practice to type a complete filename at the command prompt, including the file extension. After the malware executes, control is passed to the host file, which is then executed. This order of execution, and redirection does not happen, if the entire filename is typed at the command prompt.

Parasitic viruses – attach themselves to the host file during infection, which is the classic form of file infection. These viruses take control of the host file's first instruction to point to the malicious code. Once the malicious code executes, control is returned to the host program. There are two types of parasitic viruses (prepending and appending).

A prepending parasitic virus attaches itself to the top of the host file, while an appending parasitic virus attaches itself to the end of the host file.



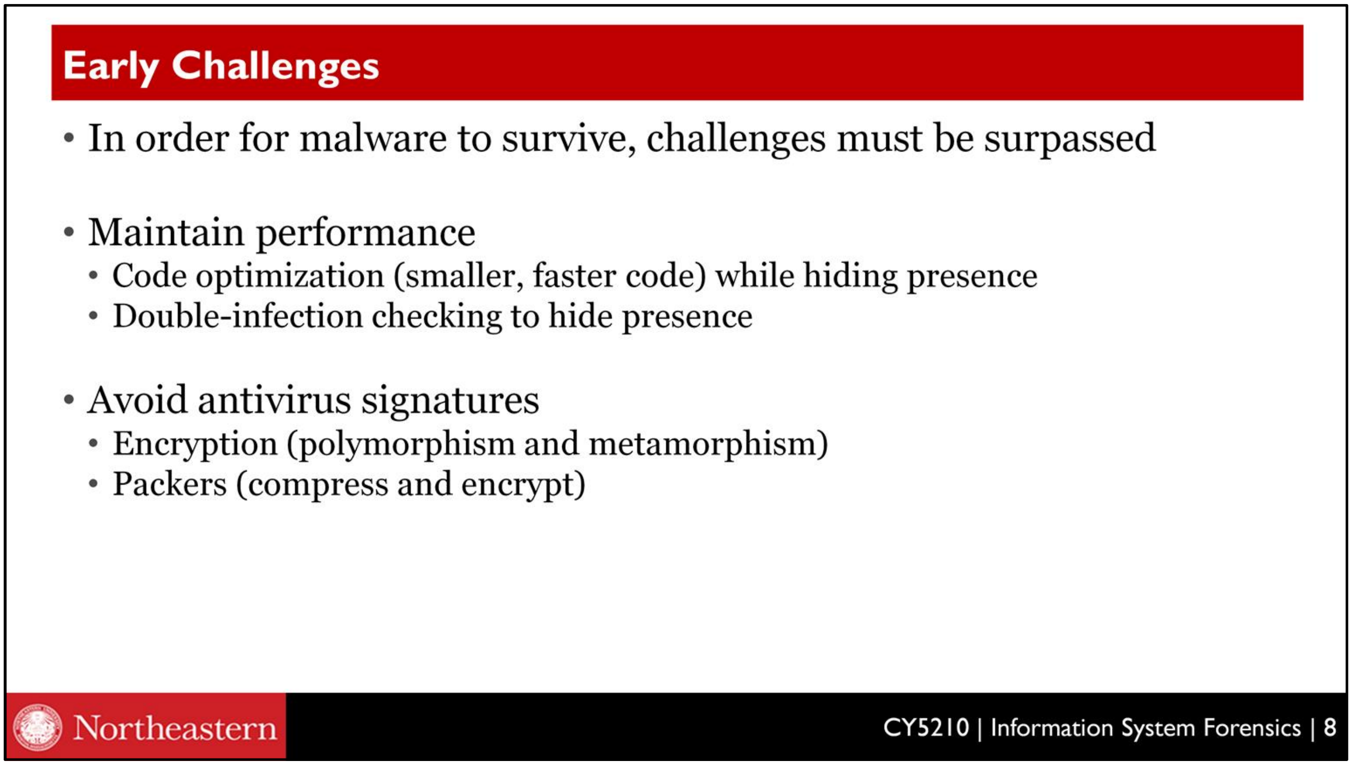
Memory-Resident Viruses

- Uses same infection strategy as direct infectors
  - Overwrite a host, act as a companion, and use parasitic techniques
  - The only difference is when the host infection occurs
- Do not infect files directly upon execution
  - Hide and wait in memory until a host program is executed and then infect it
- The virus resides in memory using DOS's terminate-and-stay-resident (TSR) system call

Memory-resident viruses - do not infect files directly upon execution, but rather hide and wait in memory until a host program is executed. The infection strategies are the same: overwrite a host program, be a companion virus, and they can use parasitic techniques to infect host programs.

Direct infectors infect host programs when the virus or an infected host is executed, whereas memory-resident viruses infect host programs when the host programs are executed.

[1] https://en.wikipedia.org/wiki/Terminate_and_stay_resident_program
[2] http://virus.wikidot.com/virus



Early Challenges

- In order for malware to survive, challenges must be surpassed

- Maintain performance
  - Code optimization (smaller, faster code) while hiding presence
  - Double-infection checking to hide presence

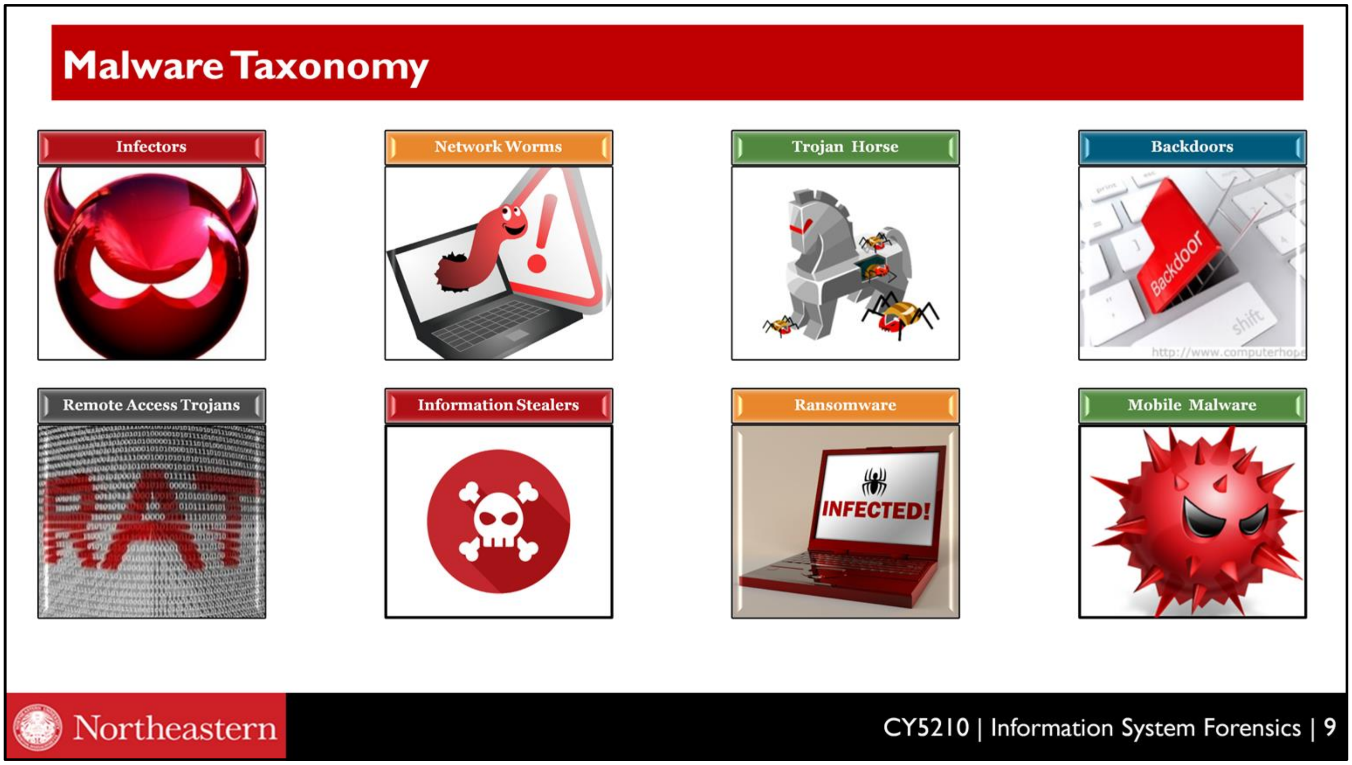
- Avoid antivirus signatures
  - Encryption (polymorphism and metamorphism)
  - Packers (compress and encrypt)

In order for malware authors to be successful with their malicious code, they have to plan for specific challenges. These challenges include maintaining performance and evading antivirus detection methods.

Performance challenges for malicious software authors include:

1. **Code optimization** – applications require system resources to function. It is imperative that code have a small footprint and reduce the number of required CPU cycles in order to avoid negatively impacting system performance. Optimization requires less code without reducing functionality by using assembly functions that require less CPU cycles.
2. **Double-infection checking** – a system can be infected many times, therefore if this does happen, system resources can be consumed and the malicious code has a greater chance of being detected. Malware authors have created a check for current infections to avoid infecting systems more than once. This double-checking, often called a mutex, prevents a system from being infected twice with the same malicious code. This does not prevent a system from being infected multiple times with different malicious code, however.

Malicious code authors must also continue to bypass antivirus protections, which continue to evolve. Initially, the malicious software authors would use packers to evade detection, but security monitoring tools quickly matured. Now malicious code may be packed, obfuscated, change in real-time, or even encrypted. These functions also allow for compression, in addition to encryption, to reduce the footprint of the malware.



Malware Taxonomy

Infectors

Network Worms

Trojan Horse

Backdoors

Remote Access Trojans

Information Stealers

Ransomware

Mobile Malware

Northeastern

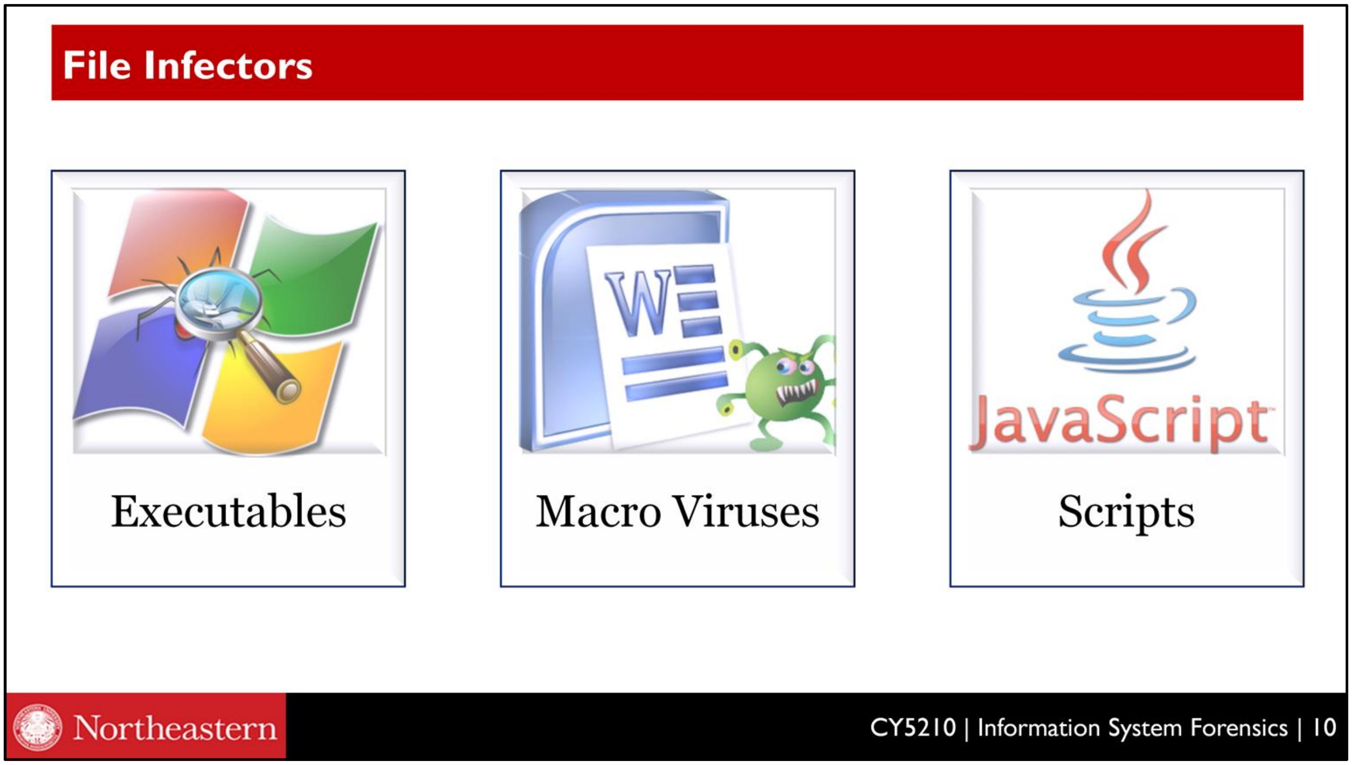
CY5210 | Information System Forensics | 9

Malware may be classified based on **behavior**, target platform, or on their attack directive. Other than mobile malware (a target platform), we will classify malware based on its behavior.

If a malware exhibits more than one behavior (e.g., file infector and network work) at the same time, the classification is made based on the hierarchy of behaviors. This order is typically infector, network worm, Trojan, and backdoor. If malware displays characteristics of a backdoor and an infector, ultimately the classification is infector.

Malware quickly became the term coined for any malicious software, including viruses.

1. **Infectors** – file infectors are computer viruses, which branched out into various types as software tools and various programming languages emerged.
2. **Network Worms** – malware that replicates itself to multiple systems in the network with little or no user intervention, typically using network services such as browsing, e-mail, and chat protocols. Network worms are often classified based on their network-propagating features.
3. **Trojans** – malware that disguises itself as a harmless program or tool, but actually aims to be destructive. The only recovery is a reinstallation of the OS.
4. **Backdoors** – allow an attacker to gain access to a compromised system without requiring authentication and allowing them to bypass security controls. The access may even be a shell with root access.
5. **Remote Access Trojans** – a malicious administrative tool with backdoor capabilities, enabling an attacker root access to a previously compromised system.
6. **Information Stealers** – programs used to steal information.
7. **Ransomware** – a malicious program that holds data or system access to systems or resources hostage until a ransom is paid.
8. **Mobile Malware** – any malicious program installed or made for a mobile device.



File Infectors

Executables

Macro Viruses

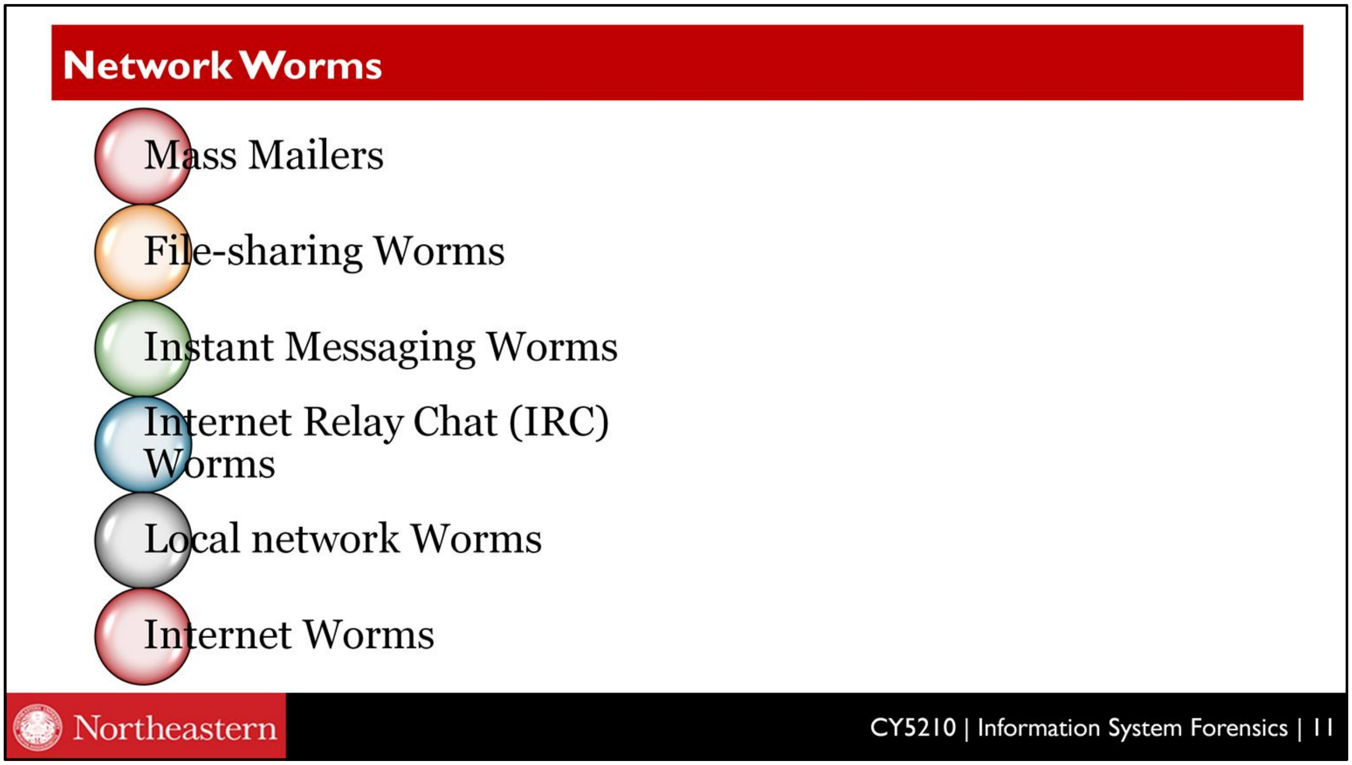
Scripts

Northeastern

CY5210 | Information System Forensics | 10

File Infectors are simply computer viruses that emerged as programming languages grew and changed over time; there are three classes:

1. **Executables** – executables went through several changes from DOS's old MZ format, the New Executable (NE) format, and the Portable Executable (PE) format introduced with Windows 95. Any file that can execute can potentially became infected with malicious code.
2. **Macro Viruses** – a macro is a set of instructions combined to perform s specific task or function automatically. There are many types of macro viruses and historically these have targeted Windows systems due to the use of specific macro languages such as Visual Basic for Applications (VBA) which is used across Office documents. Typically the default templates for Office documents were the most susceptible to being infected, which in turn infect any file created from that infected template. These are OS independent and infect the application-specific macro language instead of the actual OS. These macro types include several Office macro viruses:
   a) **Word macro viruses**
   b) **Excel macro viruses**
   c) **Access macro viruses**
   d) **PowerPoint macro viruses**
   e) **Cross-platform macro viruses** (Typically those used in Office products but for Windows and OS X systems)
3. **Scripts** – virus writers eventually made the transition to Visual Basic Script (VBS) or JavaScript to write viruses. JavaScript works as a part of an application such as a web browser or Portable Document File (PDF).



Network Worms

- Mass Mailers
- File-sharing Worms
- Instant Messaging Worms
- Internet Relay Chat (IRC) Worms
- Local network Worms
- Internet Worms

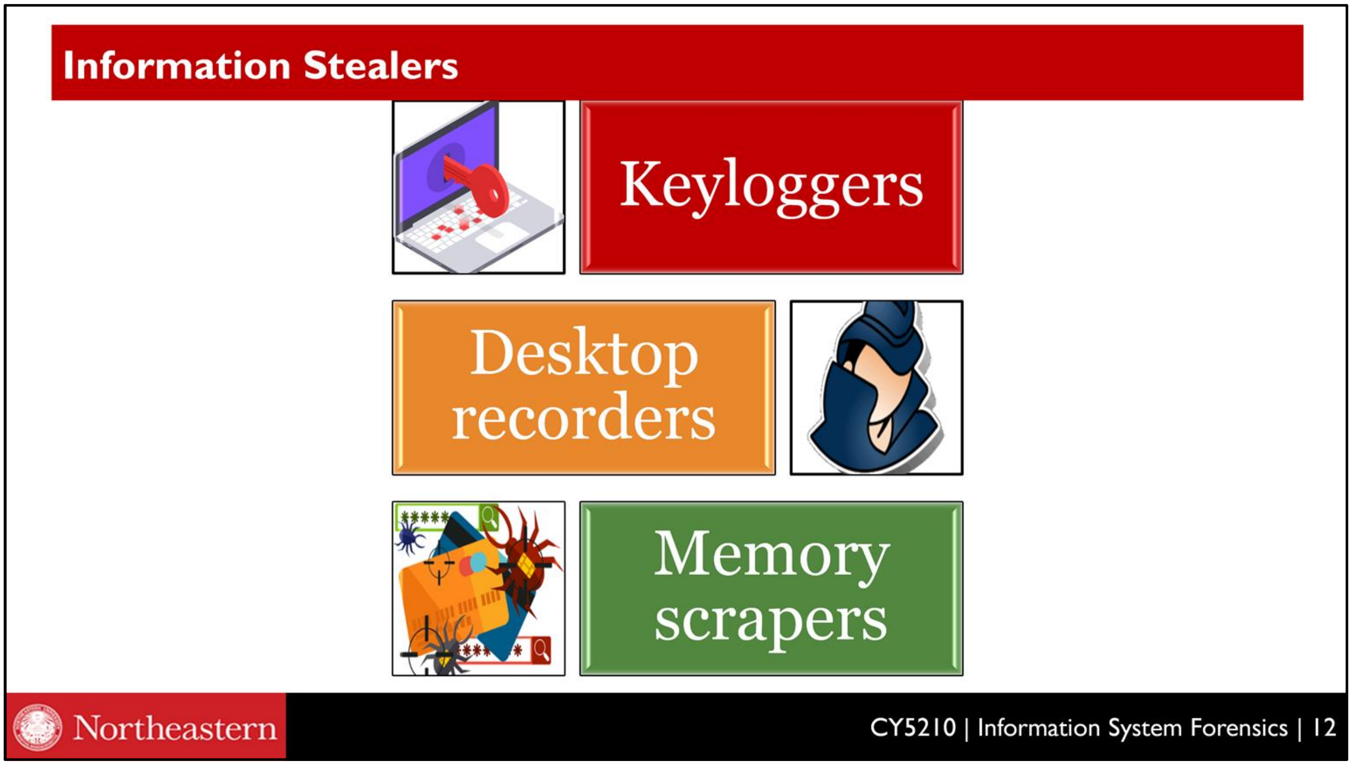
Northeastern

CY5210 | Information System Forensics | 11

Network worms are often classified based on their network-propagating features. These features include how the malicious software is spread, used, and potentially identified.

Examples of network worms include:

- **Mass mailers** – are worms that spread via e-mail and use the victim's address book to spread.
- **File-sharing worms** – spread by adding copies of themselves to publicly facing file share folders using enticing names.
- **Instant messaging worms** – IM worms use IM software as the main vector of infection. Infected machines send out IMs to the user's contact list containing malicious links.
- **Internet Relay Chat (IRC) worms** – spread through IRC channels by sending messages with malicious links or instructions to make changes to the system making infection easier.
- **Local network worms** – spread within a local area network (LAN) after scanning writeable shared folders connected to various hosts and copying itself.
- **Internet worms** – spread by scanning the Internet for vulnerable machines or use vulnerable browsers to spread.



Information Stealers

Keyloggers

Desktop recorders

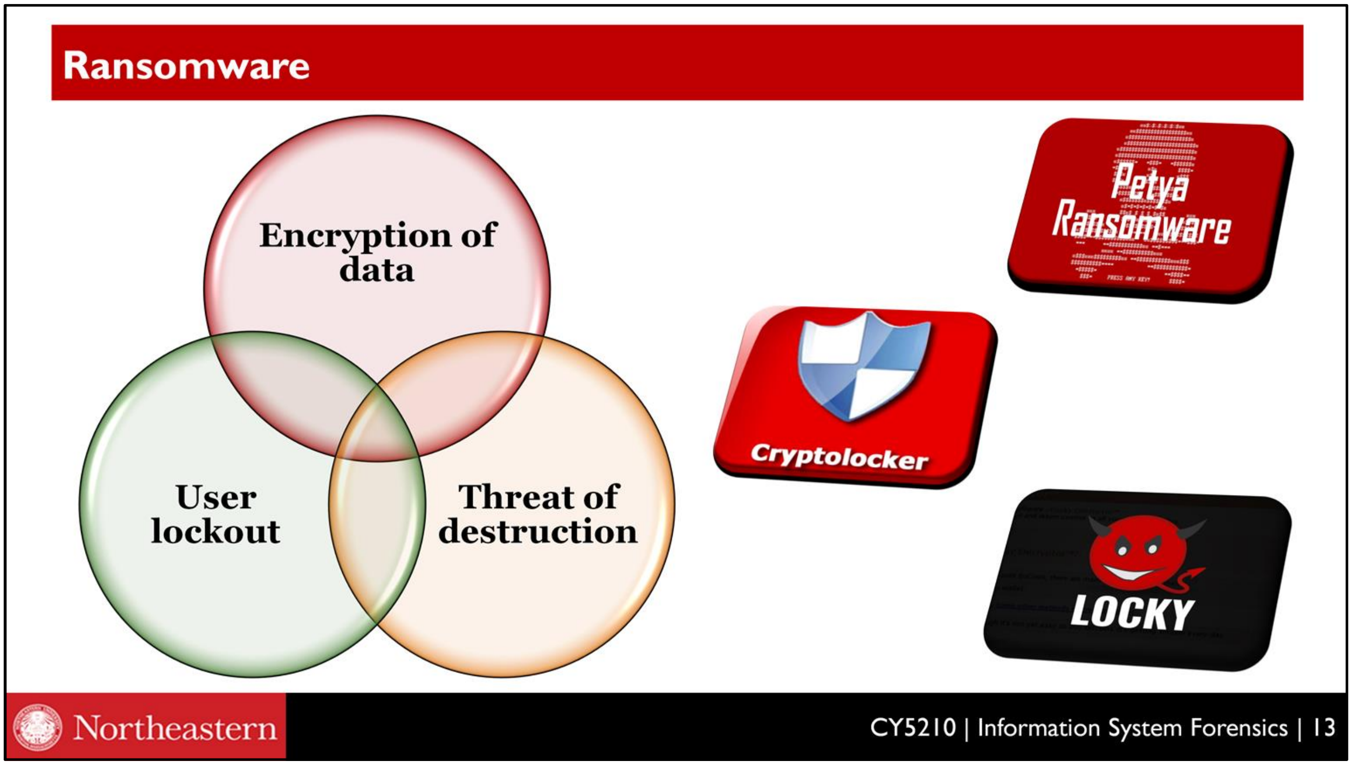
Memory scrapers

Northeastern

CY5210 | Information System Forensics | 12

Information Stealers

1. **Keyloggers** – capture keystrokes and log them; these keystrokes are stored and retrieved later or forwarded to a server.
2. **Desktop Recorders** – takes a screenshot of a desktop at predefined intervals or when triggered by an event.
3. **Memory/RAM Scrapers** – can grab information unencrypted in RAM.



Ransomware

Encryption of data

User lockout

Threat of destruction

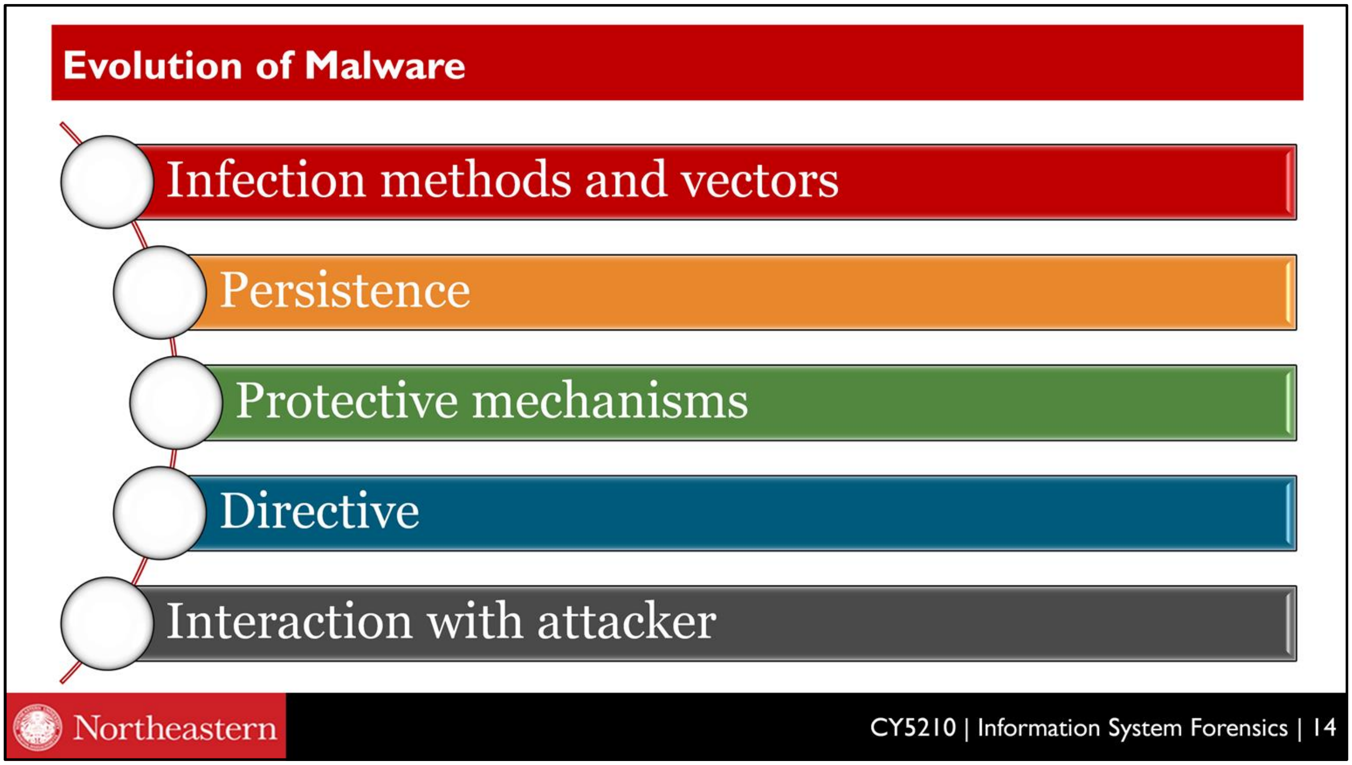
Northeastern

CY5210 | Information System Forensics | 13

Ransomware is a malicious program that holds data or access to systems or resources holding that data hostage unless a ransom is paid.

Ransomware is a virtual extortion, of sorts, which can be one of the following:

- **Encryption of data** – malware encrypts specific data (e.g., document files, picture files, or specific extensions), specific folders, or a disk partition. The main goal is to prevent access until some monetary amount is paid to the attacker/cyber criminal.
- **Threat of destruction** – threaten to pay in a specific time or lose data, refuse decryption, or reformat the drive.
- **User lockout** – the user is locked out until s/he pays the ransom amount.



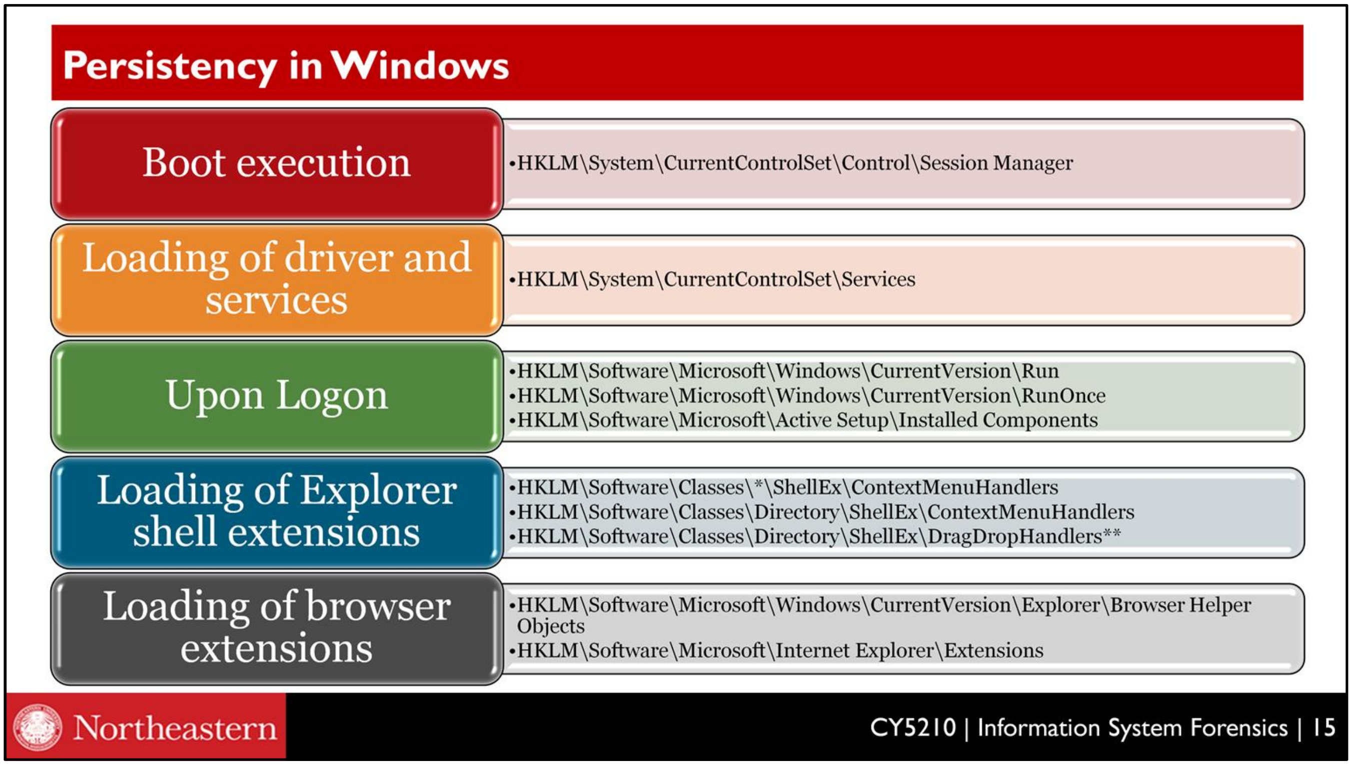
Evolution of Malware

- Infection methods and vectors
- Persistence
- Protective mechanisms
- Directive
- Interaction with attacker

Northeastern CY5210 | Information System Forensics | 14

There are several areas of malware evolution that are worth discussing.

1. **Infection methods and vectors** – malware infection methods and vectors continue to grow and change as the world becomes more interconnected. Malware used to be a single file whereas now it includes many files with various capabilities as malware has become more modular.
2. **Persistence** – malware must have a means for running and remaining persistent across reboots. This is where persistence mechanisms come into play and where OS-level techniques are used to make sure malware starts as intended. This might include hijacking the boot sector, adding itself to autoexec.bat, and infecting system files.
3. **Protective Mechanisms** – malware will often make several attempts to protect itself including attempting to conceal its presence and protect its code. Now compression, encryption, and polymorphism are some of the many protective mechanisms.
4. **Directives** – while the initial directive was to prove a proof-of-concept, this has now been replaced with information stealing, sabotage, and destruction.
5. **Interaction with Attacker** – early malware had no ability to interact with handlers. Now server-client malware allows constant communication between the handler and the malware sample.



Persistency in Windows

Boot execution

- HKLM\System\CurrentControlSet\Control\Session Manager

Loading of driver and services

- HKLM\System\CurrentControlSet\Services

Upon Logon

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKLM\Software\Microsoft\Active Setup\Installed Components

Loading of Explorer shell extensions

- HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers
- HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers
- HKLM\Software\Classes\Directory\ShellEx\DragDropHandlers**

Loading of browser extensions

- HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
- HKLM\Software\Microsoft\Internet Explorer\Extensions

Northeastern

CY5210 | Information System Forensics | 15

Persistence in Windows

Boot execution

HKLM\System\CurrentControlSet\Control\Session Manager

Loading of driver and services

HKLM\System\CurrentControlSet\Services

Upon Logon

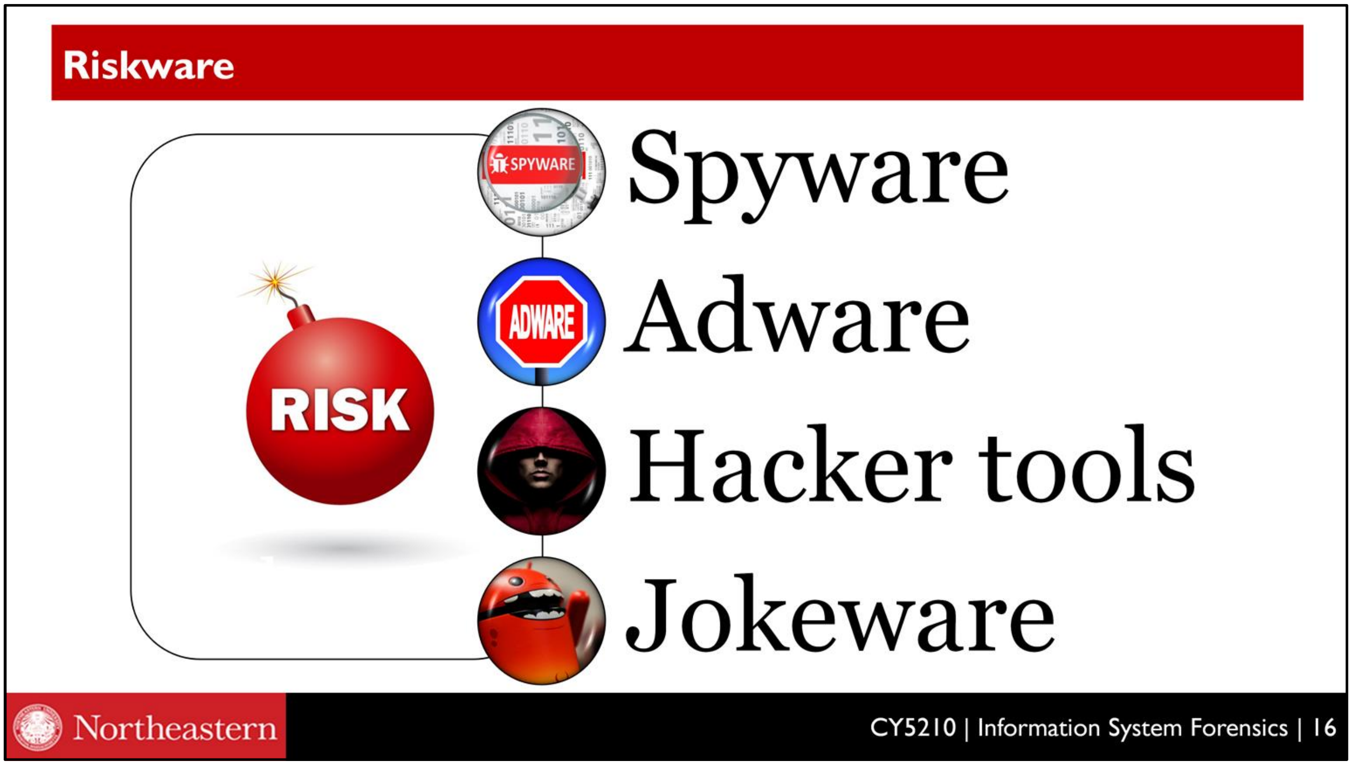
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\Software\Microsoft\Active Setup\Installed Components

Loading of Explorer shell extensions

HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers
HKLM\Software\Classes\Directory\ShellEx\DragDropHandlers
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers
HKLM\Software\Classes\Folder\ShellEx\DragDropHandlers

Loading of browser extensions

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
HKLM\Software\Microsoft\Internet Explorer\Extensions



Riskware

RISK
SPYWARE
ADWARE

- Spyware
- Adware
- Hacker tools
- Jokeware

Northeastern

CY5210 | Information System Forensics | 16

Riskware are computer programs that can be potentially dangerous, but not necessarily so. This is also known as greyware or “potentially unwanted programs (PUPs) or applications (PUAs).

1. **Spyware** – software that collects information without the user’s knowledge. It can be considered an information stealer, but may also be packaged as commercial software.
2. **Adware** – displays ads in the form of pop-ups. Some is preloaded and others track users’ online browsing behavior and displays ads based on their tracked behavior.
3. **Hacker Tools** – system administration tools in the wrong hands. These may include password cracking tools, vulnerability scanning tools, or other remote access programs.
4. **Jokeware** – Is not malicious, per se, but could trick the user into doing something destructive or harmful to a system or data.