
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
TM
Capgemini
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 1

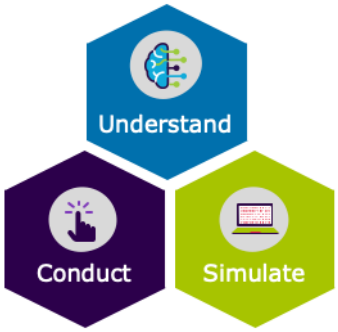
Module 3 – Malware and Analysis

Module Learning Objectives

Upon completion of this module, the student should be able to do the following:

Understand

- The different types of malware and how they are different.
- How file-less malware works.
- How malware can prevent its own detection.
- How malware can use common file types to infect network computers.
- What metadata is and how it can be used in forensics.
- What Yara is and how Yara rules can be used to identify malware.
- What an executable is and how to identify it.



Simulate

- The dynamic analysis of malware.

Conduct

- A static analysis of malware.

Content Source:

https://us.norton.com/internetsecurity-malware.html
https://libraryofhacks.blogspot.com/2017/01/types-of-keylogger.html
https://www.wired.com/2016/06/hacker-lexicon-password-hashing/
https://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation-33283
http://woshub.com/how-to-get-plain-text-passwords-of-windows-users/

Module Overview:

Attackers are constantly creating and evolving new methods and software to compromise target environments. Traditional malware is transferred to the host via many different methods, and once on the host, it will execute its instructions to begin the process of compromising the host, unless we can stop it first.

Attribution:

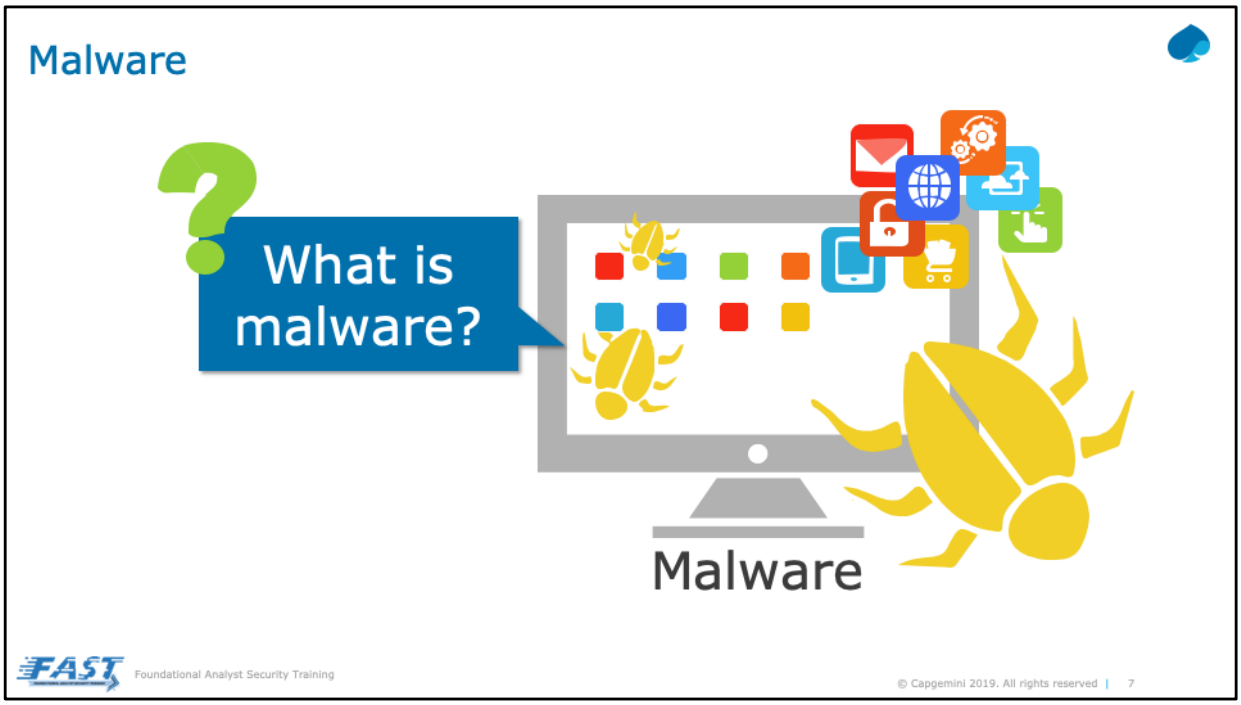
Malware and Analysis

- What is Malware?
- Escalating Privileges
- Types of Malware

Topic Learning Objectives

Upon completion of this topic, the student should be able to do the following:

- ***Understand how malicious code is constructed and how it interacts with the operating system of a targeted computer.***
- ***Describe how to analyze malware, determine its purpose and how it can provide intelligence.***



Instructor Notes:

What is Malware?

According to Norton's website… "Malware is an abbreviated form of "malicious software." This is software that is specifically designed to gain access to or damage a computer, usually without the knowledge of the owner. There are various types of malware, including spyware, ransomware, viruses, worms, Trojan horses, adware, or any type of malicious code that infiltrates a computer."

Generally, software is considered malware based on the intent of the creator rather than its actual features.

Malware (cont.)

The term "malware" was coined in the early 1990's by an Israeli researcher.

FAST Foundational Analyst Security Training

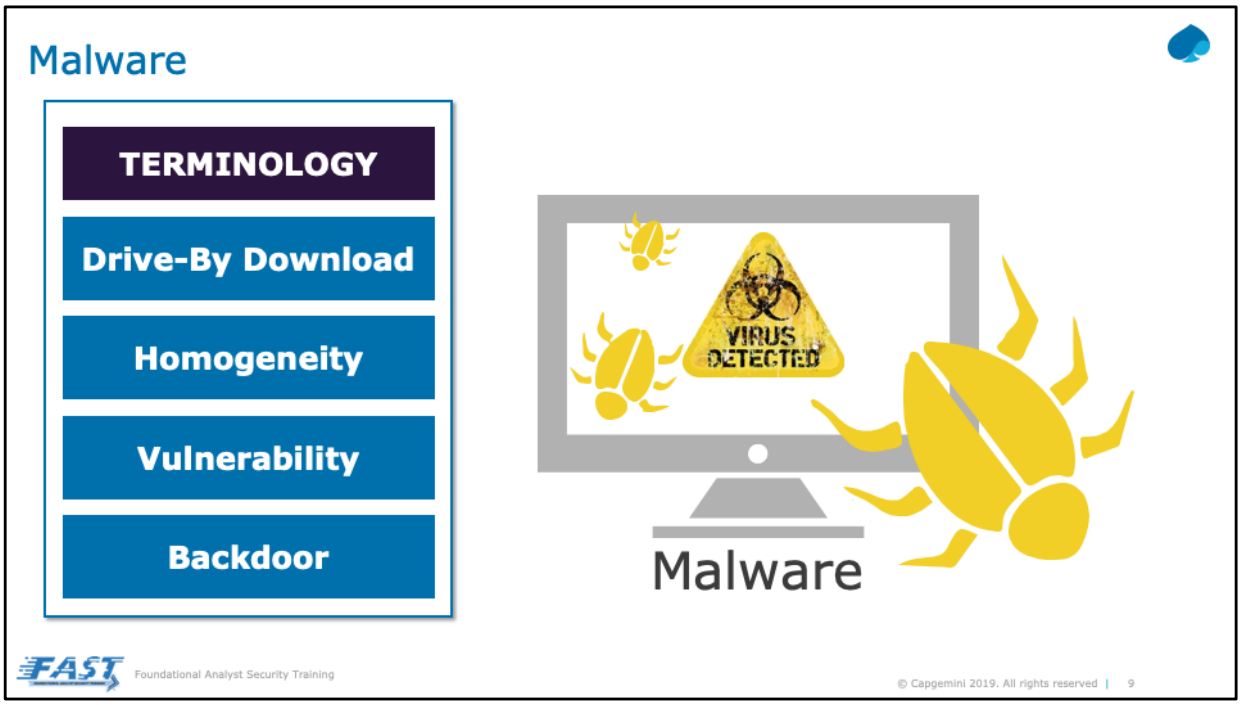
 8

Instructor Notes:

Malware creation is on the rise due to money that can be made through organized Internet crime. Originally malware was created for experiments and pranks, but eventually it was used for vandalism and destruction of targeted machines.

The term Malware was could have been introduced by Yisrael Rada in the 1990's, but the threats were already there. Radai was a prominent researcher in the field of computer viruses, he passed away in 2014.

Today, much of malware is created to make a profit from forced advertising (adware), stealing sensitive information (spyware), spreading email spam or child pornography (zombie computers), or extorting money (ransomware).



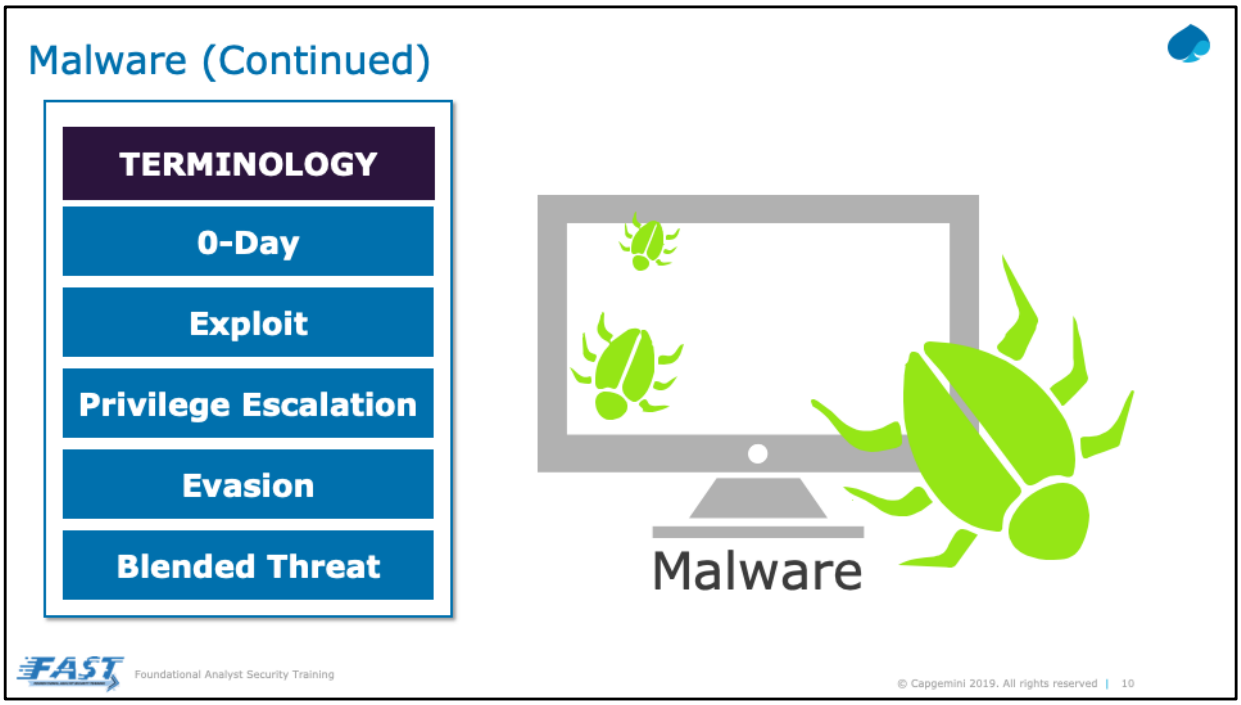
Instructor Notes:

Drive-by download: The unintended download of computer software from the Internet. It either refers to the download that happens without the knowledge of a user, or the download that a person authorizes but without the understanding of the consequences.

Homogeneity: A setup where all the systems are running on the same operating system and connected to the same network. This increases the chances of a worm in one computer to easily spread to others on that network.

Vulnerability: A security defect in software that can be attacked by a malware. It could be a design flaw, programming error, or some other kind of inherent weakness in a software implementation, application or operating system.

Backdoor: An opening or break left in a software, hardware, network or system security by design, usually for debugging purposes.



Instructor Notes:

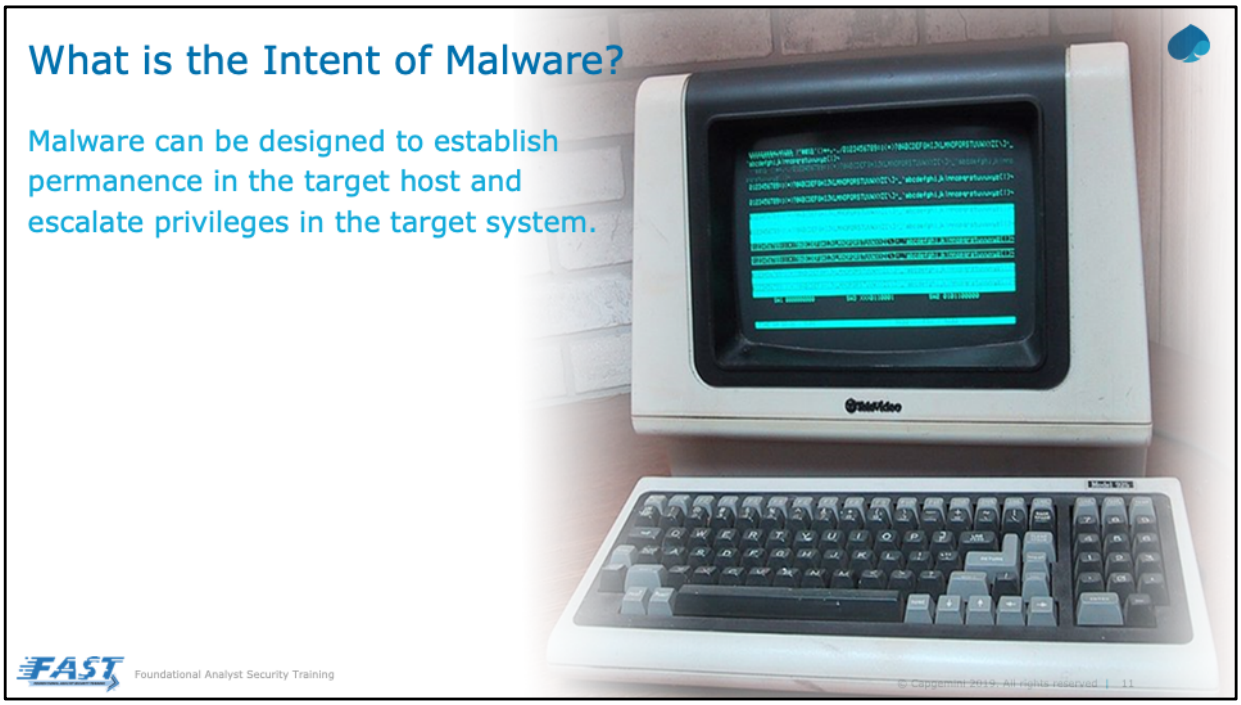
0-Day: A zero-day vulnerability is an undisclosed flaw that hackers can exploit. It's called 0-day because it is not publicly reported or announced before becoming active.

Exploit: A threat made real via a successful attack on an existing vulnerability. Also refers to software that is developed to target the loopholes on a particular device.

Privilege escalation: Situation where the attacker gets escalated access to restricted data that is on a higher level of security.

Evasion: The techniques malware maker design to avoid detection and analysis of their malware by security systems and software.

Blended threat: A malware package that combines the characteristics of multiple types of malware like Trojans, worms or viruses, seeking to exploit more than one system vulnerability.



Instructor Notes:

Attackers will always try to get the highest level privileges they can get on a host and then a network. A windows local admin account on the host will allow them to do anything the need on that host, and give them a path to getting access to a network admin account.

This is sometimes done using zero-day attacks that allow escalation, but more commonly this is done by leveraging misconfigurations of the systems services, group policy settings, preferences.

We can often find malware operating with escalated privileges by looking for SEDebugPrivilege()

This capability is only given to local admin accounts, and is used for sys level debugging, and provides access to all system level processes.

How is Privilege Escalation Accomplished?

One goal of malware is to gain access to passwords so that other accounts can be compromised.

FAST Foundational Analyst Security Training

 | 12

Instructor Notes:

One goal of malware is to gain access to passwords, so that other accounts can be compromised.

Password Hash Dumping – Allows an attacker to dump the LM and NTLM password hashes for local credentials from the Security Accounts Manager (SAM) which is partially encrypted.

Pass the Hash – Uses LM and NTLM hashes to authenticate to a remote system via NTLM authentication.

Clear Text Password Recovery – Can steal clear text passwords stored by Windows authentication packages.

Password Hash Dumping

Hashing is the act of converting passwords into unreadable strings of characters that are designed to be impossible to convert back, known as hashes.

Instructor Notes:

When an APT steals “hashed passwords” they aren’t getting something useable, they get hashed passwords that have to be decrypted.

Hash is both a noun and a verb. Hashing is the act of converting passwords into unreadable strings of characters that are designed to be impossible to convert back, known as hashes. Some hashing schemes are more easily cracked than others.

Password Hash Dumping (cont.)

- Hashing is easy to do, and difficult to undo, with a simple mathematical process.
- Some processes are easier to crack than others, depending on the complexity or number of operations associated with the process.

Instructor Notes:

Hashing is easy to do, and hard to undo with a simple mathematical process. Some processes are easier to crack than others, depending on the complexity or number of operations associated with the process.

The APT cant know what process was used to hash the passwords, they can however attempt to guess passwords, until they end up with an identical hash. This requires dedicated computer power to attempt to crack stolen passwords. However, once they can break one, they can reverse engineer them all, this is called pre-computing.

To prevent pre-computation, hashing schemes now use a trick called "salting," adding random data to a password before hashing it and then storing that "salt" value along with the hash.

Pass the Hash

In a pass-the-hash attack, the goal is to use the hash directly without cracking it, this makes time-consuming password attacks less needed.

Pass-the-hash technique itself is not new. It was first published in 1997 when Paul Ashton posted an exploit called "NT Pass the Hash" on Bugtraq.

However, the knowledge of this attack and its severity remains poor.

FAST Foundational Analyst Security Training

Instructor Notes:

In a pass-the-hash attack, the goal is to use the hash directly without cracking it, this makes time-consuming password attacks less needed.

Pass-the-hash technique itself is not new. It was first published in 1997 when Paul Ashton posted an exploit called "NT Pass the Hash" on Bugtraq.

However, the knowledge of this attack and its severity remains poor.

In earlier versions of Windows, the LM hash is typically stored and transmitted by default.

However, in Windows Vista and versions above, the LM hash is not stored by default, nor is it used by default during network authentication.

Instead, the newer versions use the NTLMv2 hash as the default authentication.

Pass the Hash (cont.)

Local Area Network Manager (LM) Hash

- 14 characters maximum
- Broken into 7-byte chunks
- Uses Data Encryption Standard (DES) encryption

NT Local Area Network Manager (NTLM) Hash

- Message Digest 4 (MD4) algorithm
- Password unbroken
- 127 characters maximum

FAST Foundational Analyst Security Training

Instructor Notes:

The process to create the LM hash is relatively complex. When a user creates a new password, this password is converted to all uppercase, then it's padded out to 14 characters. The password is then split into two 7-byte chunks. The two chunks then will be used as a key in a Data Encryption Standard (DES) encryption to encrypt a fixed value.

The values of the two DES operations are concatenated and the result is stored as the LM hash.

The NTLM hash algorithm is much simpler than the LM hash.

It takes the password, hashes it using the MD4 algorithm, then stores it.

It does not break up the password into chunks, the password is case-sensitive, and can support very long passwords (127 characters on Windows 2000 and later systems).

Pass the Hash (cont.)

LM/NTLM

- Used for Workgroup Authentication
- Domain Authentication
  - Clients
  - Non-Domain Members

FAST Foundational Analyst Security Training

Instructor Notes:

LM and NTLM Both LM and NTLM are very similar, but differ mainly in the hash used to compute the response. LM and NTLM are used for authentication in workgroups. They are also used in a domain environment if either the client, or the server is not a domain member, or if a resource within the domain is accessed by its IP address instead of its NetBIOS or DNS name.

All Windows OSs prior to Windows Server 2003 send both LM and NTLM responses by default. In Windows Server 2003 only the NTLM response is sent by default, while the LM response field is mostly unused.

Pass the Hash (cont.)

Passing the hash means that the Advanced Persistent Threat (APT) is able to use the passwords while they are hashed to authenticate to other computers on the network.

This method allows APTs to get on the network without having to decrypt the hashed passwords.

The use of hashed passwords is being phased out but is still common in older systems.

FAST Foundational Analyst Security Training

Instructor Notes:

Passing the hash means that the APT is able to use the passwords while they are hashed to authenticate to other computers on the network.

This method allows APTs to get on the network without having to decrypt the hashed passwords.

The use of hashed passwords is being phased out, but is still common in older systems.

Cleartext Password Recovery

Using tools, such as "Mimikatz," it is possible to extract passwords from Windows Memory.

FAST Foundational Analyst Security Training

Instructor Notes:

Mimikatz allows you to extract user passwords directly from the memory, from the memory dump of the PC or from the hibernation file. This is called Clear Text Password Recovery.

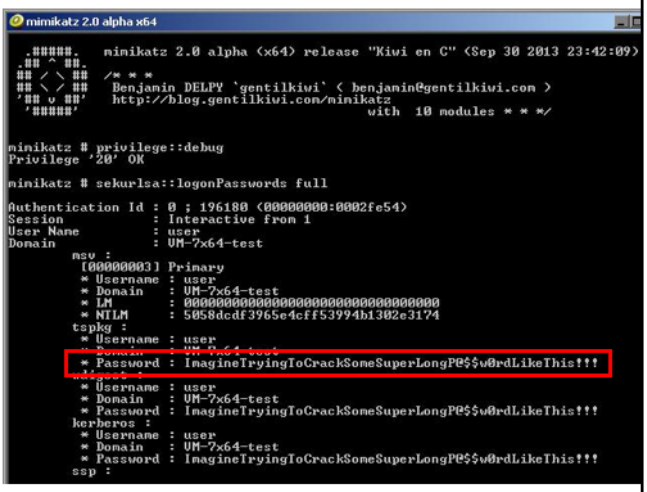
Most system administrators are sure that Windows does not store user passwords in plain text in its memory, but only in the form of a hash. Though today there are a lot of tools able to extract password hashes from the system, it is safe to say that using a quite complex password, not from a dictionary, makes it almost impossible for an attacker to get it by a brute force or with a base of already calculated hashes.

Cleartext Password Recovery (cont.)

The utility shows us the super-strong user's password in the cleartext!

Mimikatz also allows extracting passwords from the following:

- Windows Memory Dump
- Hiber.sys Files
- Virtual Machines



FAST Foundational Analyst Security Training

Instructor Notes:

As you can see, the utility shows us the super strong user's password in the clear text!

The command was successful because the Debug Mode is enabled on this computer, which allows you to set the **SeDebugPrivilege** flag for the desired process. In this mode, programs can receive low-level access to the memory of processes running on behalf of the system.

Imagine that this is a terminal (RDS) server on which many users work simultaneously, and on which there is the enterprise administrator's session. Those if you have administrator rights on a single server, you can even grab the domain administrator's password.

Preventing Cleartext Password Recovery

In Windows 8.1 and Server 2012 R2 (and newer), the ability to extract passwords from Local Security Authority Subsystem Service (LSASS) is limited.

The LM hashes and passwords are not stored in memory in these systems by default.

FAST Foundational Analyst Security Training

 | 21

Instructor Notes:

In Windows 8.1 and Server 2012 R2 (and newer), the ability to extract passwords from LSASS is limited. The LM hashes and passwords are not stored in memory in these systems by default.

The same functionality is backported to earlier versions of Windows (7/8/2008R2/2012), in which you need to install a special update **KB2871997** (the update provides other options to enhance the security of the system) and in the registry key **HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\Wdigest** set the DWORD parameter **UseLogonCredential** to **0** (WDigest is disabled). If you try to extract passwords from memory after installing this update and the UseLogonCredential key, you will see that mimikats using the creds_wdigest command cannot extract passwords and hashes.

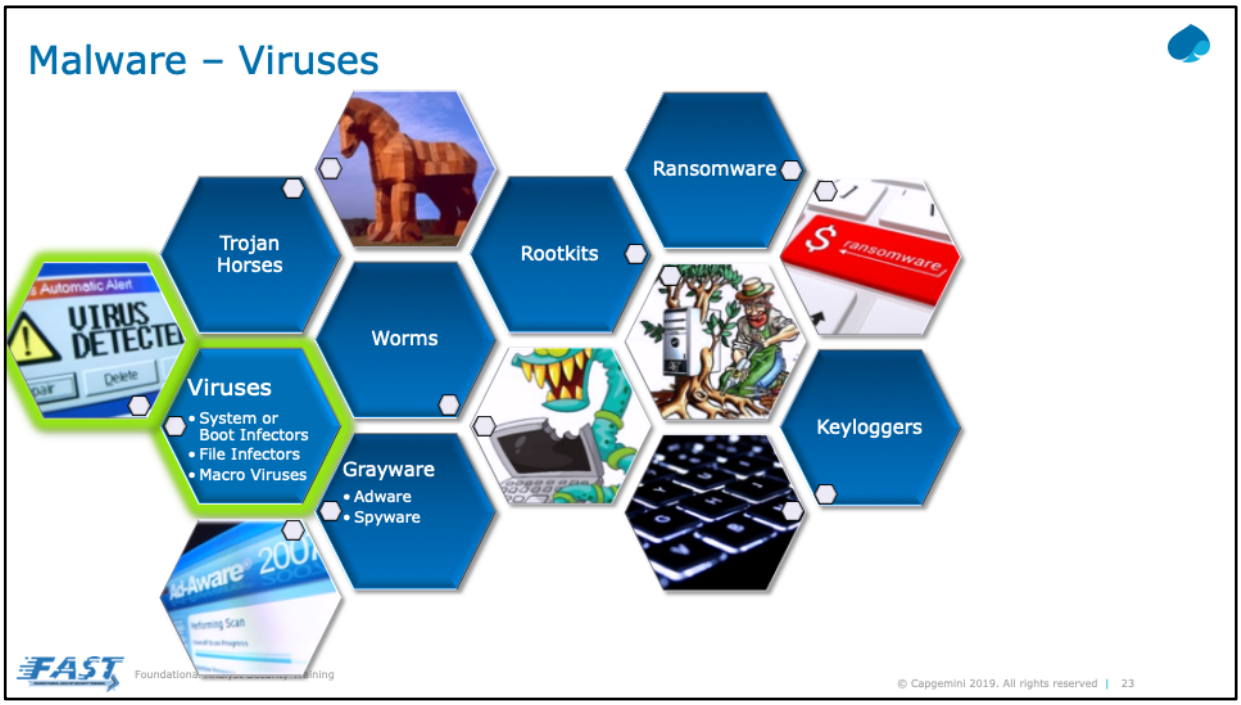
Malware Types

- Trojans and Worms are the most prevalent.
- It is estimated that almost 70 percent of malware are Trojans.

Instructor Notes:

Malware creation is on the rise due to money that can be made through organized Internet crime. Originally malware was created for experiments and pranks, but eventually it was used for vandalism and destruction of targeted machines.

Today, much of malware is created to make a profit from forced advertising (adware), stealing sensitive information (spyware), spreading email spam or child pornography (zombie computers), or extorting money (ransomware).



Instructor Notes:

Viruses

Viruses have been around since the dawn of time — speaking in computer terms, that is. In fact, computing luminary John von Neumann did the first academic work on the theory of self-replicating computer programs all the way back in 1949. The first examples of what can be classified as a virus have been detected since the 70s.

The primary characteristic that a piece of software must possess to qualify as a virus is an urge to reproduce that is programmed into it. This mechanism means that this type of malware will distribute copies of itself, using any means to spread. Another characteristic common to viruses is that they are covert, making it hard to detect their presence on a system, without dedicated security programs called antivirus.

Essentially, they arrive uninvited, hide in secrecy and usually work in obscurity. And that is what makes them so deadly.

They hide within computer files, and the computer must run that file (execute that

code, in other words) for a virus to do its dirty work. At its core, a virus is nothing but a contagious code or program that attaches itself to other software and usually requires human interaction to propagate. This is how viruses are further classified, depending on whether they reside in binary executables, data files, or in the boot sector of a hard drive of a particular system.

1a. System or boot infectors
A virus can infect a system as a resident virus by installing itself as part of the operating system, so that it remains in the RAM from the time a computer is booted up to when it is shutdown. These types of viruses are very rare these days, what with the advent of the Internet, and security procedures built into modern operating systems like Windows 10.
2a. File infectors
Many viruses sneak up into ordinary executable files like .EXE and .COM in order to up their chances of being run by a user. Any program that file type that Windows can call for execution is susceptible, including batch and script files like .BAT, .JS. .VB, and even screensaver files with the .SCR extension.
3a. Macro viruses
These types of viruses are the ones that run inside specific applications that allow macro programs in order to extend the capabilities of a given software. Viruses that targeted Microsoft Office were widespread a few years back, though the threat of macro viruses has also declined in recent times as unsigned macros are automatically disabled in Office and are not allowed to run.
READ
How to Detect Keyloggers?
Many users install antivirus software that can detect and eliminate known viruses, and also prevent infections when the computer attempts to download or run the executable files that are either downloaded from the Internet, or distributed as email attachments, or on USB flash drives. This means that the antivirus software needs to be regularly updated in order to recognize the latest threats, as cybercriminals continue to create new viruses.
And although their threat may have diminished in recent years, and other forms of malware may have taken the spotlight, viruses have been the cause of widespread destruction, as they replicate and perform activities like accessing sensitive information, stealing data, and most of all, consuming system resources like CPU and disk space, crippling the systems, often rendering them useless.
Some infamous examples of viruses over the years are the Concept virus, the Chernobyl virus (also known as CIH), the Anna Kournikova virus, Brain and RavMonE.exe.
2. Worms
The second of the two types of infectious malware. A worm is a standalone software that replicates without targeting and infecting specific files that are already present

on a computer. Think of worms as small programs that replicate themselves in a computer and destroy the files and data on it. They usually target the operating system files, and work until the drive they are in becomes empty.
Basically, whereas viruses add themselves inside existing files, worms carry themselves in their own containers.
Worms usually show up via email and instant messages, and often confine themselves their activities to what they can accomplish inside the application that moves them. They use a computer network to spread, relying on security failures on the target computer in order to access it, and delete data.
Many worms that have been created are designed only to spread, and do not attempt to change the systems that they pass through. But even these have unintended effects can cause major disruptions by increasing the network traffic.
Examples include Melissa, Morris, Mydoom, Sasser, Blaster, and Mylife.
3. Trojan Horses
A Trojan is a malicious program that misrepresents itself to appear useful. These are spread in the guise of routine software that persuade a victim to install it on their PC. The term is derived from the Ancient Greek story of the wooden horse that was used to invade the city of Troy by stealth — Trojan horses are just as deadly on computers. The payload can be anything, but is usually a form of a backdoor that allows attackers unauthorized access to the affected computer. Trojans also give cybercriminals access to the personal information of a user like IP addresses, passwords and banking details. They are often used to install keyloggers that can easily capture account names and passwords, or credit card data, and disclose it to cybercriminals. Most ransomware attacks are also usually carried out using a Trojan horse, by housing the harmful code inside an apparently harmless piece of data.
Trojans are now considered to be the most dangerous of all malware, particularly the ones that are designed to steal the financial information of a user. Some insidious types of Trojans actually claim to remove the viruses in the system, but instead introduce viruses.
Notable examples also include Trojan horses developed by governments and government agencies like the FBI, NSA, and GCHQ. Names like Magic Lantern, FinFisher, WARRIOR PRIDE, Netbus, Beast, Blackhole exploit kit, Gh0st RAT, Tiny Banker Trojan, Clickbot.A, and Zeus have been the cause of horror. While an Android malware discovered in 2015, called Shedun, is one of the many that target mobile devices.
4. Rootkits
A rootkit is a collection of software specifically designed to permit malware that gathers information, into your system. These work in the background so that a user may not notice anything suspicious. But in the background, a rootkit will permit several types of malware to get into the system.
These software work like a back door for malware to enter and wreak havoc, and are now being used extensively by hackers to infect systems. A rootkit installation can

either be automatic, or an attacker can install it once they have obtained administrator privileges.

READ

What is PUP Malware?

Root access in other words.

Detecting a rootkit is difficult, as this type of malware is often able to subvert the software that locates it. Removing a rootkit is equally complicated, or in some cases practically impossible — more so in cases where the rootkit resides inside the kernel of an operating system. Reinstalling the OS is often the only solution to completely get rid of such an advanced rootkit.

The first malicious rootkit to gain notoriety on Windows was NTRootkit in 1999, but the most popular is the Sony BMG copy protection rootkit scandal that rocked the company in the year 2005. Its discovery and media attention exposed users to even more serious vulnerabilities.

5. Ransomware

The most devastating type of malicious software, by some counts. Definitely one of the most advanced and constantly on the rise these days. Ransomware blocks access to the data of a victim, threating to either publish it or delete it until a ransom is paid. Worse yet, there is no guarantee that paying a ransom will return access to the data, or prevent it from deletion.

This type of malware basically infects the system from the inside, locking the computer and making it useless. Simpler ransomware may lock a system that may be difficult to reverse for most people, while the more advanced variety of ransomware encrypts the files of a victim, rendering them inaccessible, and demanding a ransom payment to decrypt the files.

Ransomware attacks initially gained popularity in Russia, but these types of scams have now grown in popularity internationally. They are typically carried out using a Trojan that comes with a payload that is disguised as a legitimate file.

Although this manner of digital extortion has been in play since late 80s, it returned to prominence in late 2013 with the advent of digital currency that is used to collect ransom money. Many security vendors classify ransomware to be the most dangerous cyber threat — its detection and removal is a complicated process. And though it is widespread on PC platforms, ransomware that target mobile operating systems has also seen a rise.

Major ransomware like Reveton, CryptoLocker, CryptoWall, and more recently, the 2017 WannaCry attack, have caused no small amount of destruction. While Fusob, one of the most widely used mobile ransomware families, has employed scare tactics to extort people to pay a ransom.

6. Keyloggers

Software that records all the information that is typed using a keyboard. Keyloggers usually are not capable of recording information that is entered using virtual keyboards and other input devices, but physical keyboards are at risk

with this type of malware.
Keyloggers store the gathered information and send it to the attacker, who can then extract sensitive information like username and passwords as well as credit card details.

7. Grayware

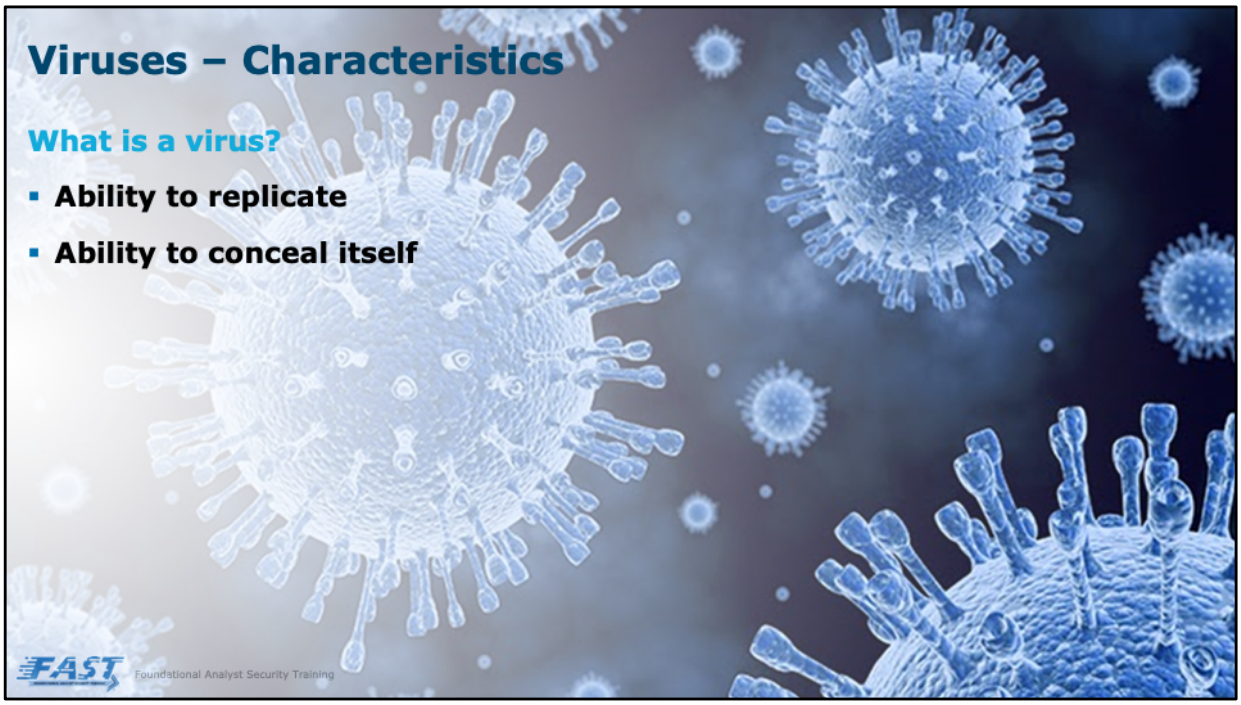
Grayware is a recently coined term that came into use around 2004. It is used to describe unwanted applications and files that though are not classified as malware, can worsen the performance of computers and lead to security risks. At the minimum, these programs behave in an annoying or undesirable manner, and at worst, they monitor a system and phone home with information.
Grayware alludes to both adware and spyware. Almost all commercially available antivirus software can detect these potentially unwanted programs, and offer separate modules to detect, quarantine and remove malware that displays advertisements.

7a. Adware

Although ad-supported software is now much more common, and known as adware in some circles, the word has been linked to malware for quite some time. While adware can refer to any program that is supported by advertising, malicious adware usually shows ads in the form of popups and windows that cannot be closed.
It is the perhaps the most lucrative and least harmful malware, designed with the specific purpose of displaying ads on your computer. Adware usage is on the rise on mobile, in particular, with some Chinese firms bundling in adware by default in certain low-cost Android smartphones.

7b. Spyware

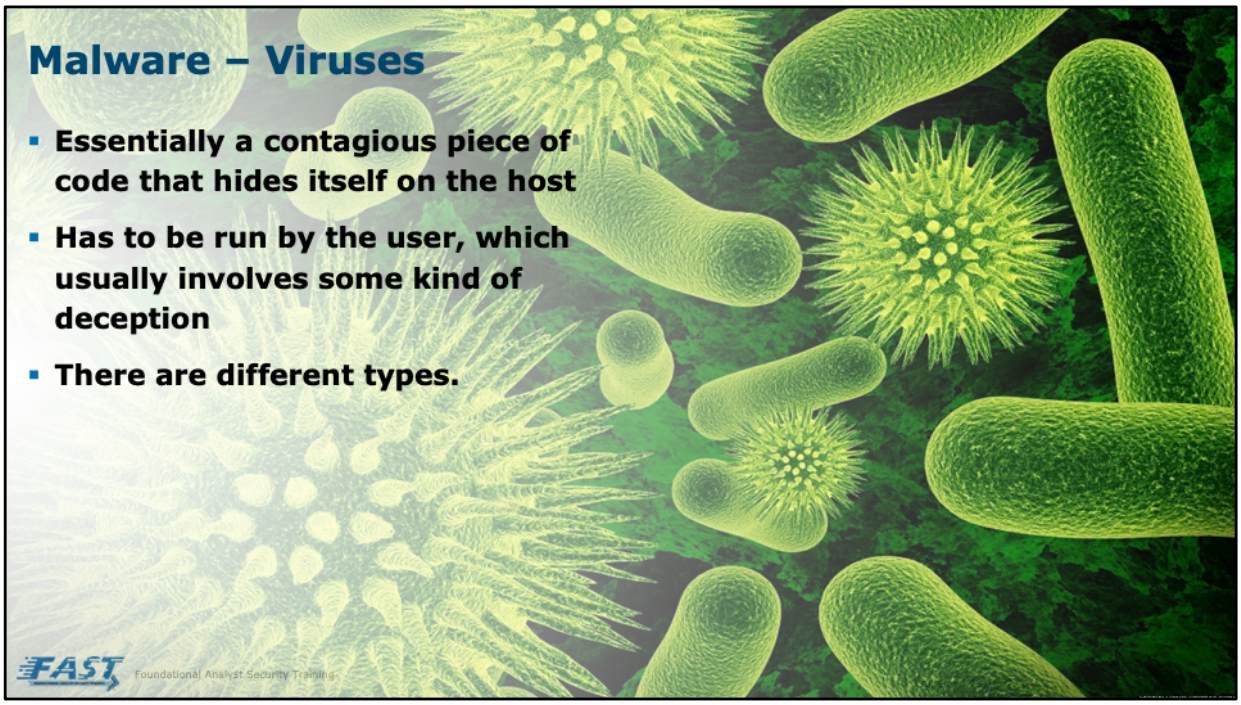
Spyware, as the name gives away, is software that constantly spies on you. Its main purpose is to keep track of your Internet activities in order to send adware. Spyware are also used to gather information about an organization without their knowledge, and send that information to another entity, without consent of the victim.



Instructor Notes:

The primary characteristic that a piece of software must possess to qualify as a virus is an urge to reproduce that is programmed into it. This mechanism means that this type of malware will distribute copies of itself, using any means to spread. Another characteristic common to viruses is that they are covert, making it hard to detect their presence on a system, without dedicated security programs called antivirus.

Essentially, they arrive uninvited, hide in secrecy and usually work in obscurity. And that is what makes them so deadly.



Instructor Notes:

They hide within computer files, and the computer must run that file (execute that code, in other words) for a virus to do its dirty work. At its core, a virus is nothing but a contagious code or program that attaches itself to other software and usually requires human interaction to propagate. This is how viruses are further classified, depending on whether they reside in binary executables, data files, or in the boot sector of a hard drive of a particular system.

Viruses – System Boot Injectors

By hiding in the Operating System (OS), the virus can load itself into memory anytime the computer is booted up.

FAST Foundational Analyst Security Training

Instructor Notes:

1a. System or boot infectors
A virus can infect a system as a resident virus by installing itself as part of the operating system, so that it remains in the RAM from the time a computer is booted up to when it is shutdown. These types of viruses are very rare these days, what with the advent of the Internet, and security procedures built into modern operating systems like Windows 10.

Instructor Notes:

2a. File infectors
Many viruses sneak up into ordinary executable files like .EXE and .COM in order to up their chances of being run by a user. Any program that file type that Windows can call for execution is susceptible, including batch and script files like .BAT, .JS. .VB, and even screensaver files with the .SCR extension.

Viruses – Macro Viruses

The first macro virus, called Concept, appeared in July 1995; and macro viruses (mostly infecting Word documents) subsequently became the dominant type of virus until the turn of the century.

FAST Foundational Analyst Security Training

 | 28

Instructor Notes:

Macro Viruses – Macro Viruses run inside other applications like word or pdf, using macros inside the capability of the other documents to interact with the user and allow them to operate in the host environment.

Unsigned Macros in more modern versions of these file suites are typically disabled, but these types of infectious programs are still out in the wild, though getting more rare they are a threat.

The first macro virus, called Concept, appeared in July 1995 and macro viruses (mostly infecting Word documents) subsequently became the dominant type of virus until the turn of the century, when Microsoft disabled macros by default in Office (versions since Office 2000): since then, cybercriminals have had to try and trick their victims into enabling macros before their infected macro is able to run.

JavaScript

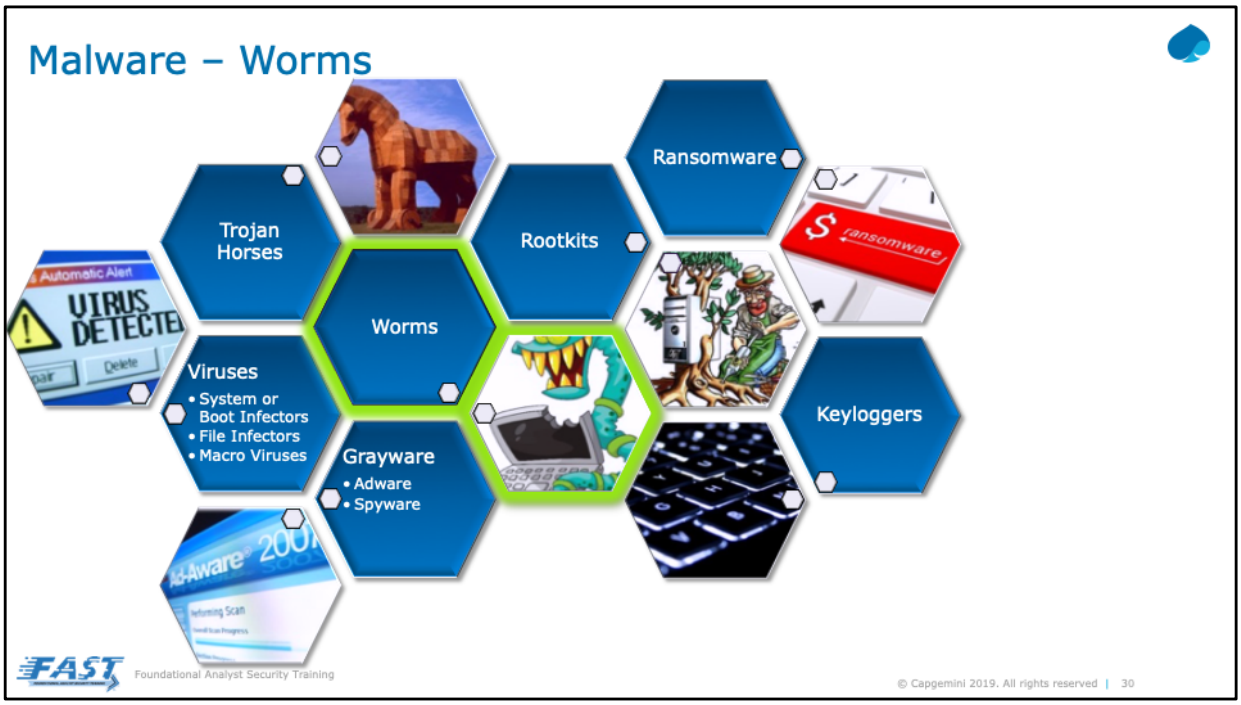
Versatile coding languages used to write exploits for websites, documents, and code downloaders

FAST Foundational Analyst Security Training

Instructor Notes:

In 2016 The Microsoft Malware Protection Center reported that there are several spam campaigns that use JavaScript (.js) to download malicious code. The .js file acted as a downloader.

JavaScript has even been used to actually write Malware code, which is traditionally done in other languages like C



Instructor Notes:

Worms

The second of the two types of infectious malware. A worm is a standalone software that replicates without targeting and infecting specific files that are already present on a computer. Think of worms as small programs that replicate themselves in a computer and destroy the files and data on it. They usually target the operating system files, and work until the drive they are in becomes empty.

Malware – Worms

Basically, whereas viruses add themselves inside existing files, worms carry themselves in their own containers.

FAST Foundational Analyst Security Training

Instructor Notes:

Basically, whereas viruses add themselves inside existing files, worms carry themselves in their own containers.

Malware – Worms (cont.)

Worms usually show up via email and instant messages and often confine their activities to what they can accomplish inside the application that moves them.

Instructor Notes:

Worms usually show up via email and instant messages, and often confine themselves their activities to what they can accomplish inside the application that moves them. They use a computer network to spread, relying on security failures on the target computer in order to access it, and delete data.

Malware – Worms (cont.)

Many worms that have been created are designed only to spread and do not attempt to change the systems through which they pass.

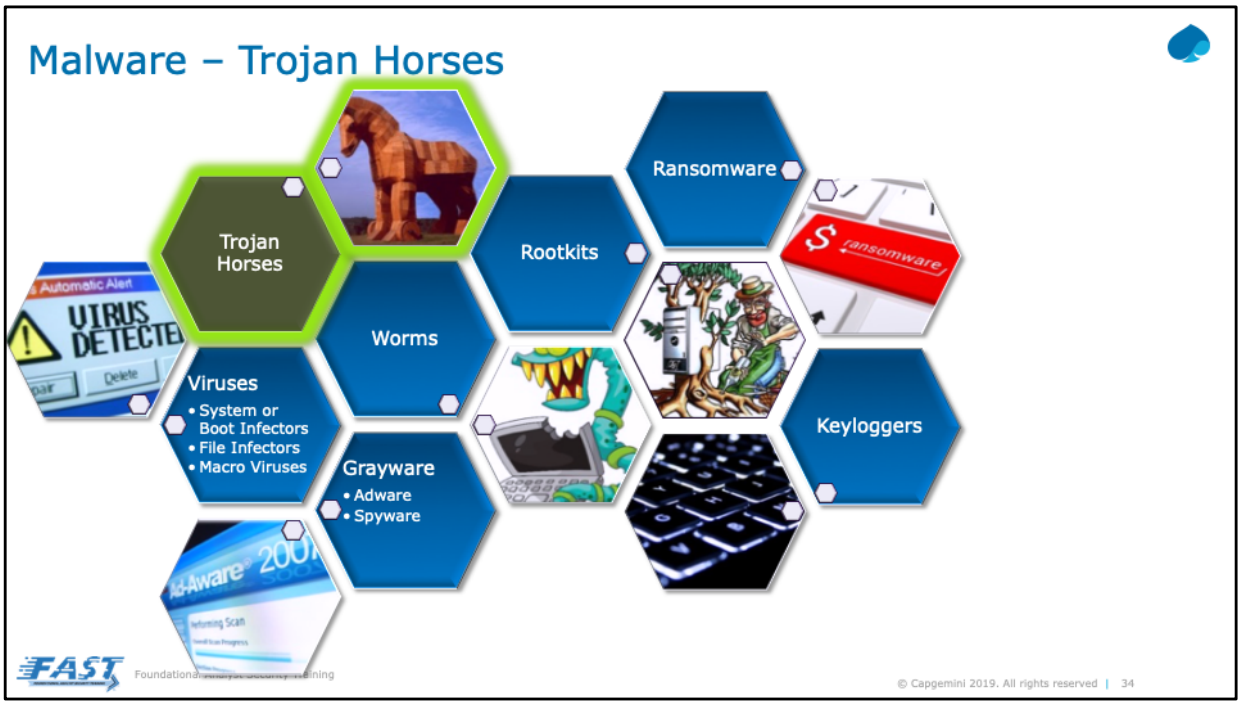
FAST Foundational Analyst Security Training

 | 33

Instructor Notes:

Many worms that have been created are designed only to spread, and do not attempt to change the systems that they pass through. But even these have unintended effects can cause major disruptions by increasing the network traffic.

Examples include Melissa, Morris, Mydoom, Sasser, Blaster, and Mylife.



Instructor Notes:

Trojan Horses

A Trojan is a malicious program that misrepresents itself to appear useful. These are spread in the guise of routine software that persuade a victim to install it on their PC. The term is derived from the Ancient Greek story of the wooden horse that was used to invade the city of Troy by stealth — Trojan horses are just as deadly on computers.

Malware – Trojan Horses (cont.)

The payload can be anything but is usually a form of a backdoor that allows attackers unauthorized access to the affected computer.

FAST Foundational Analyst Security Training

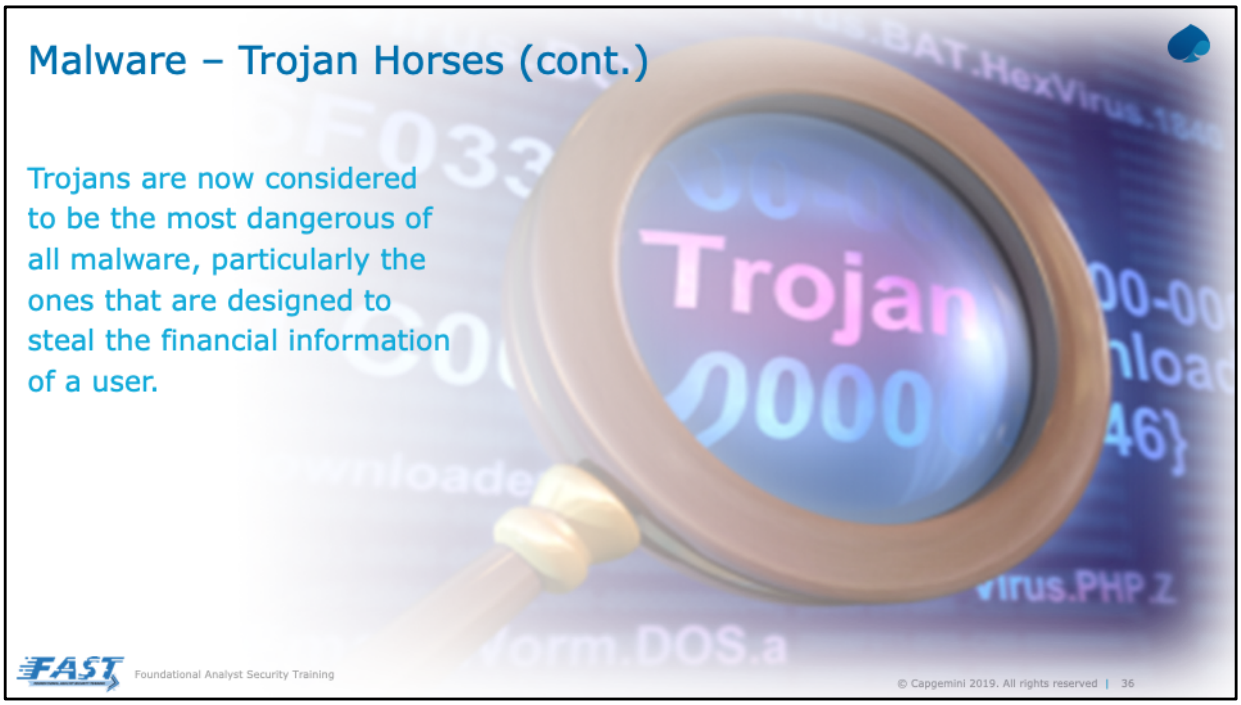
 | 35

Instructor Notes:

The payload can be anything, but is usually a form of a backdoor that allows attackers unauthorized access to the affected computer.

Trojans also give cybercriminals access to the personal information of a user like IP addresses, passwords and banking details. They are often used to install keyloggers that can easily capture account names and passwords, or credit card data, and disclose it to cybercriminals.

Most ransomware attacks are also usually carried out using a Trojan horse, by housing the harmful code inside an apparently harmless piece of data.



Instructor Notes:

Trojans are now considered to be the most dangerous of all malware, particularly the ones that are designed to steal the financial information of a user.

Some insidious types of Trojans actually claim to remove the viruses in the system, but instead introduce viruses.

Notable examples also include Trojan horses developed by governments and government agencies like the FBI, NSA, and GCHQ. Names like Magic Lantern, FinFisher, WARRIOR PRIDE, Netbus, Beast, Blackhole exploit kit, Gh0st RAT, Tiny Banker Trojan, Clickbot.A, and Zeus have been the cause of horror. While an Android malware discovered in 2015, called Shedun, is one of the many that target mobile devices.

Instructor Notes:

Rootkits

A rootkit is a collection of software specifically designed to permit malware that gathers information, into your system. These work in the background so that a user may not notice anything suspicious. But in the background, a rootkit will permit several types of malware to get into the system.

Malware – Rootkits (cont.)

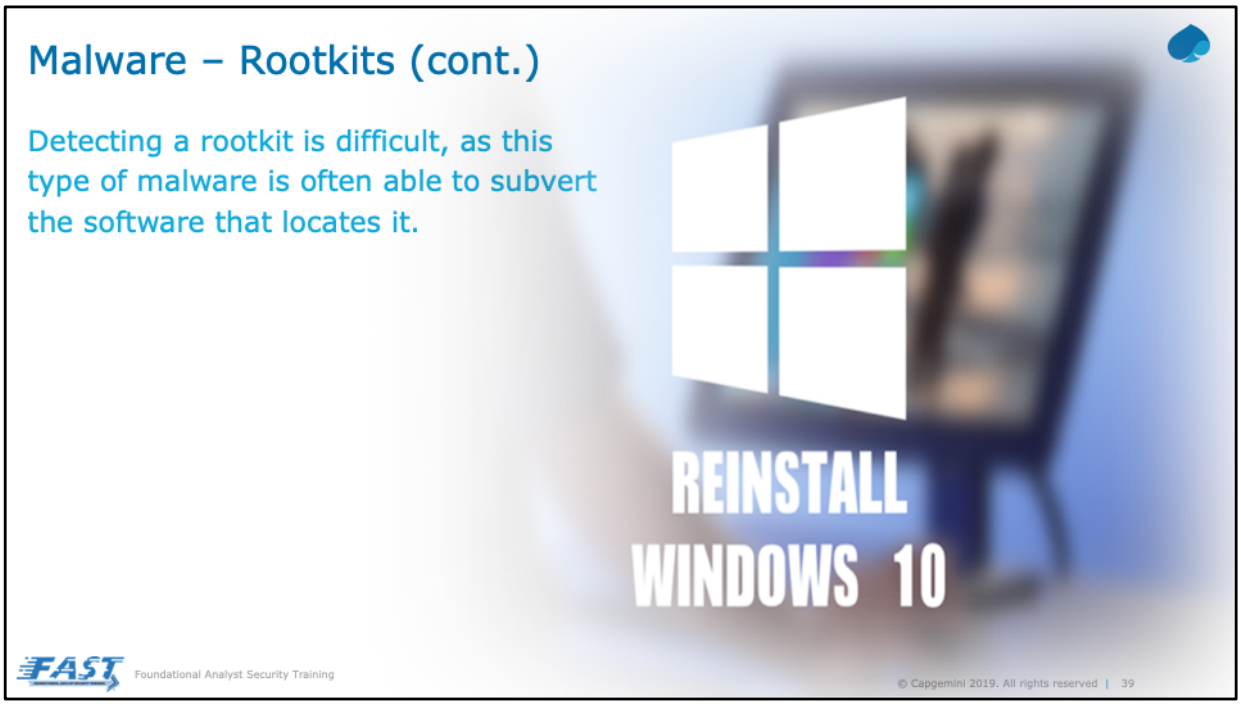
These software work like a backdoor for malware to enter and wreak havoc and are now being used extensively by hackers to infect systems.

FAST Foundational Analyst Security Training

 | 38

Instructor Notes:

These software work like a back door for malware to enter and wreak havoc, and are now being used extensively by hackers to infect systems. A rootkit installation can either be automatic, or an attacker can install it once they have obtained administrator privileges.
Root access in other words.



Instructor Notes:

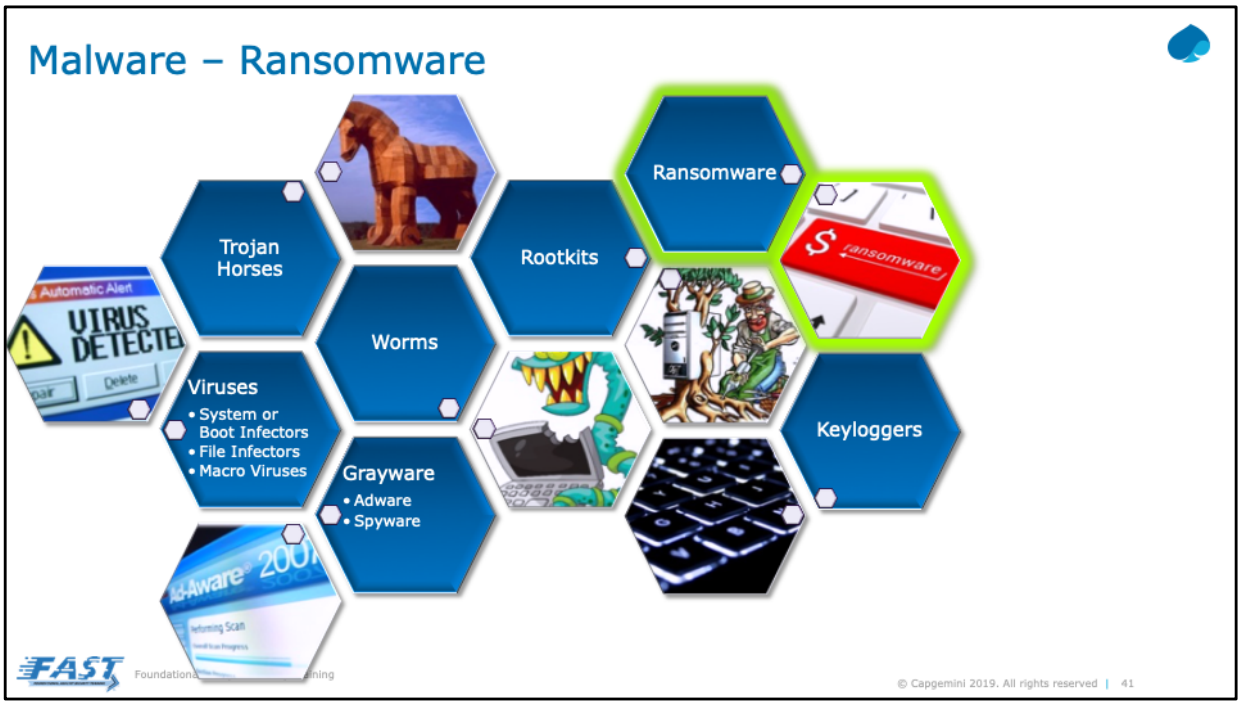
Detecting a rootkit is difficult, as this type of malware is often able to subvert the software that locates it. Removing a rootkit is equally complicated, or in some cases practically impossible — more so in cases where the rootkit resides inside the kernel of an operating system. Reinstalling the OS is often the only solution to completely get rid of such an advanced rootkit.

Malware – Rootkits (cont.)

The first malicious rootkit to gain notoriety on Windows was **NTRootkit in 1999**.

Instructor Notes:

The first malicious rootkit to gain notoriety on Windows was NTRootkit in 1999, but the most popular is the Sony BMG copyright protection rootkit scandal that rocked the company in the year 2005. Its discovery and media attention exposed users to even more serious vulnerabilities.



Instructor Notes:

Ransomware

The most devastating type of malicious software, by some counts. Definitely one of the most advanced and constantly on the rise these days. Ransomware blocks access to the data of a victim, threating to either publish it or delete it until a ransom is paid. Worse yet, there is no guarantee that paying a ransom will return access to the data, or prevent it from deletion.

Malware – Ransomware (cont.)

This type of malware basically infects the system from the inside, locking the computer and making it useless.

FAST Foundational Analyst Security Training

 | 42

Instructor Notes:

This type of malware basically infects the system from the inside, locking the computer and making it useless. Simpler ransomware may lock a system that may be difficult to reverse for most people, while the more advanced variety of ransomware encrypts the files of a victim, rendering them inaccessible, and demanding a ransom payment to decrypt the files.

Ransomware attacks initially gained popularity in Russia, but these types of scams have now grown in popularity internationally. They are typically carried out using a Trojan that comes with a payload that is disguised as a legitimate file.

Malware – Ransomware (cont.)

Although this manner of digital extortion has been in play since the **late 1980s** …

It returned to prominence in **late 2013** with the advent of digital currency that is used to collect ransom money.

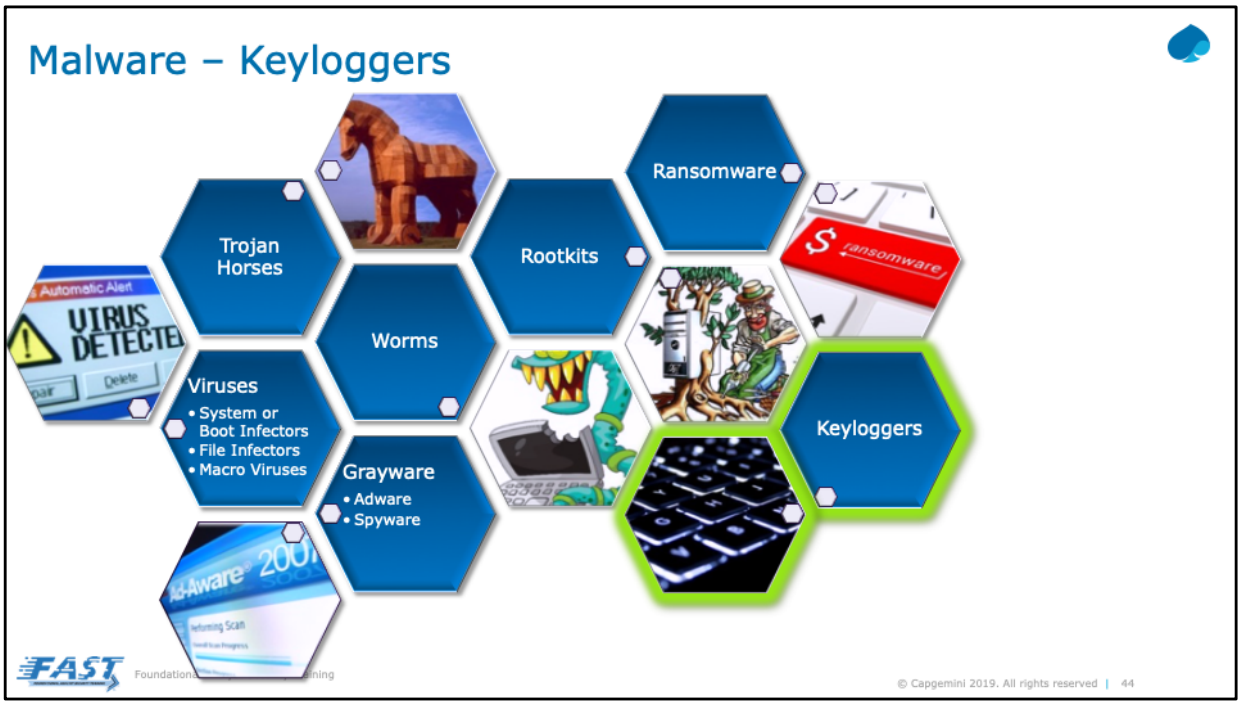
FAST Foundational Analyst Security Training

 | 43

Instructor Notes:

Although this manner of digital extortion has been in play since late 80s, it returned to prominence in late 2013 with the advent of digital currency that is used to collect ransom money. Many security vendors classify ransomware to be the most dangerous cyber threat — its detection and removal is a complicated process. And though it is widespread on PC platforms, ransomware that target mobile operating systems has also seen on the rise.

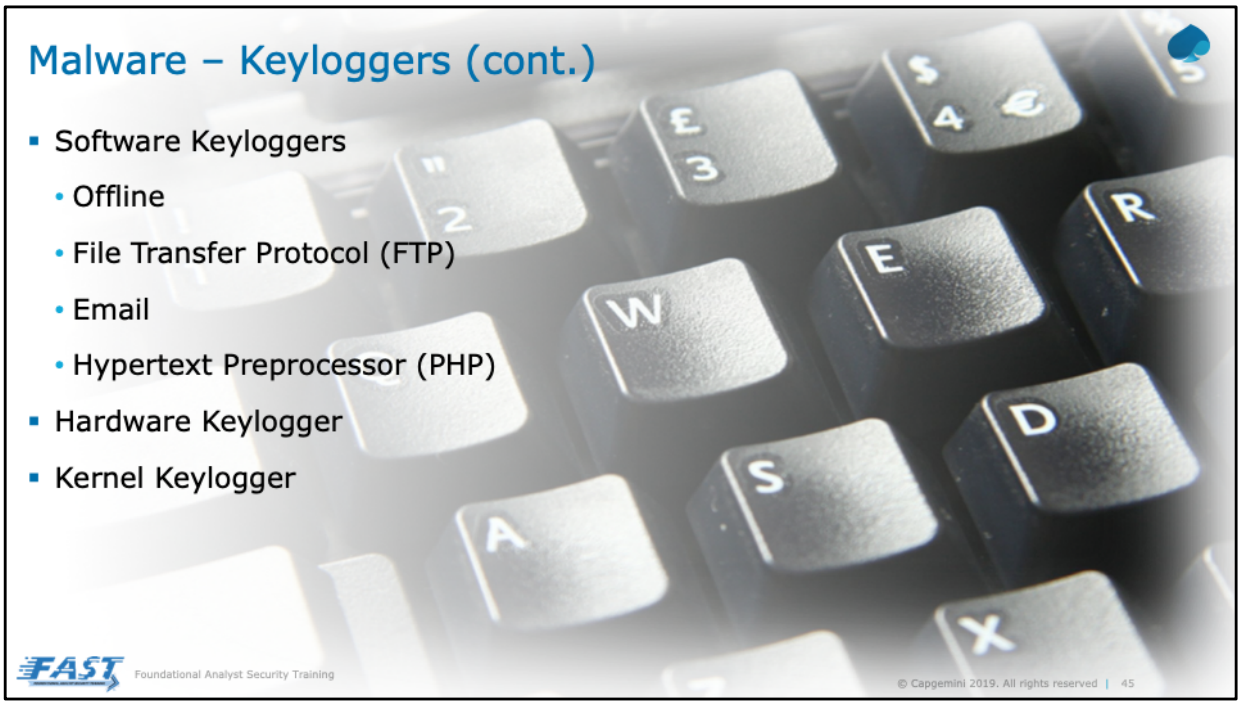
Major ransomware like Reveton, CryptoLocker, CryptoWall, and more recently, the 2017 WannaCry attack, have caused no small amount of destruction. While Fusob, one of the most widely used mobile ransomware families, has employed scare tactics to extort people to pay a ransom.



Instructor Notes:

Keyloggers

Software that records all the information that is typed using a keyboard. Keyloggers usually are not capable of recording information that is entered using virtual keyboards and other input devices, but physical keyboards are at risk with this type of malware.
Keyloggers store the gathered information and send it to the attacker, who can then extract sensitive information like username and passwords as well as credit card details.



Instructor Notes:

Software Key Loggers – Software Keyloggers are defined at the application level, and is accomplished using the SetWindowsHookEx(). This will monitor all keystrokes, the keylogger will come packaged as an .exe file and with a DLL that controls logging functions. Software Keyloggers will also work with autocomplete forms.

Offline Key Logger: Key strokes are stored on the targeted host, and the attacker must gain physical access to download the data.

FTP Key Logger: Similar to the offline key logger, the FTP key logger stores the files on the targeted host, then on a specified schedule, the logs are uploaded to an APT FTP site.

Email Key Logger: Similar to the FTP key logger, except the files are sent using the users email, and then typically deleted from the sent items queue.

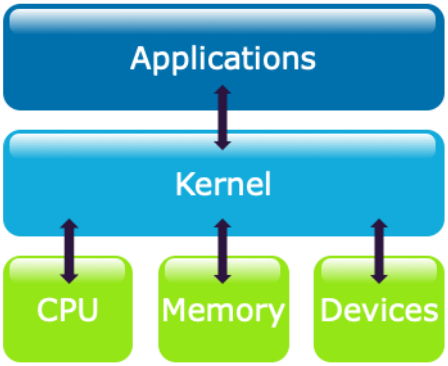
PHP Key Logger: Unlike the other software key loggers, a PHP key logger live streams the keystrokes back to the ATP's server. The downside to this type of key logger is

that any loss of connection and the keystrokes from the targeted host are lost.

Hardware Key Loggers – Typically small inline devices between the keyboard and the host. They are difficult to place, and are easily defeated by competent physical security measures.

Malware – Keyloggers (cont.)

Kernel keyloggers are neither hardware nor software based but are actually complex malware tools that operate in memory, usually from a concealed file on the targeted host's hard drive.



Instructor Notes:

Kernel Key Loggers – Kernel Keyloggers are neither hardware or software based, but are actually complex malware tools that operate in memory, usually from a concealed file on the targeted hosts hard drive. These type key loggers operate in the registry, as well, at the application layer, allowing the keystrokes to be captures almost undetectably. The drawback with this type of key logger, is that it will not capture autocomplete data at the application layer.

Malware – Keyloggers: Detection

Check Portable Executable (PE) Headers for indications of the following:

- SetWindowsHookEx()
- GetAsyncKeyState()
- GetForegroundWindow()

Look for the following strings:

- [Insert]
- [Right Arrow]
- [Left Arrow]

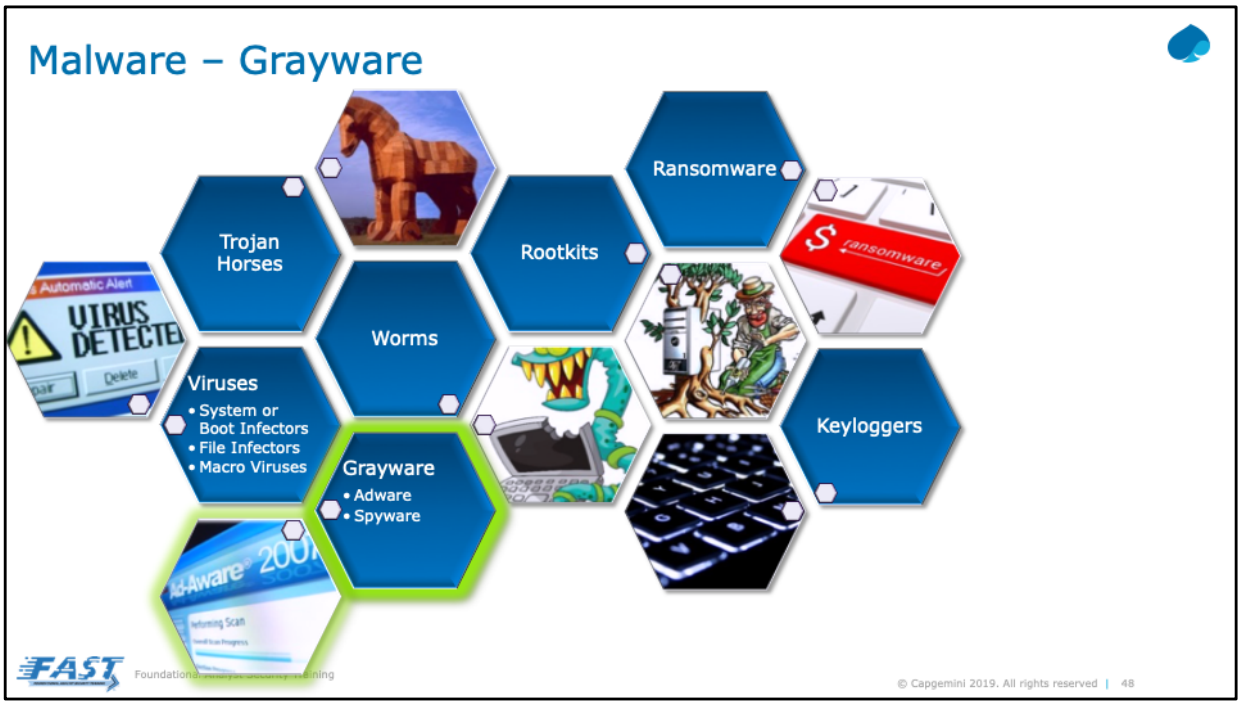
FAST Foundational Analyst Security Training

Instructor Notes:

Check the PE Headers for:

SetWindowsHookEx()
GetAsyncKeyState()
GetForegroundWindow()

Look for the following strings:
[Insert]
[Right Arrow]
[Left Arrow]
etc.



Instructor Notes:

Grayware

Grayware is a recently coined term that came into use around 2004. It is used to describe unwanted applications and files that though are not classified as malware, can worsen the performance of computers and lead to security risks. At the minimum, these programs behave in an annoying or undesirable manner, and at worst, they monitor a system and phone home with information.
Grayware alludes to both adware and spyware. Almost all commercially available antivirus software can detect these potentially unwanted programs, and offer separate modules to detect, quarantine and remove malware that displays advertisements.

Grayware – Adware

- Adware has been around for years.
- More ads are built in to applications and software to help offset cost of development.
- Adware has always been associated with malware.

FAST Foundational Analyst Security Training

Instructor Notes:

Adware

Although ad-supported software is now much more common, and known as adware in some circles, the word has been linked to malware for quite some time. While adware can refer to any program that is supported by advertising, malicious adware usually shows ads in the form of popups and windows that cannot be closed.
It is the perhaps the most lucrative and least harmful malware, designed with the specific purpose of displaying ads on your computer. Adware usage is on the rise on mobile, in particular, with some Chinese firms bundling in adware by default in certain low-cost Android smartphones.

Grayware – Spyware

Spyware A Classic Attacker Tool

Keeps an eye on Internet activity to target advertising.

Spyware Used for Nefarious Intent

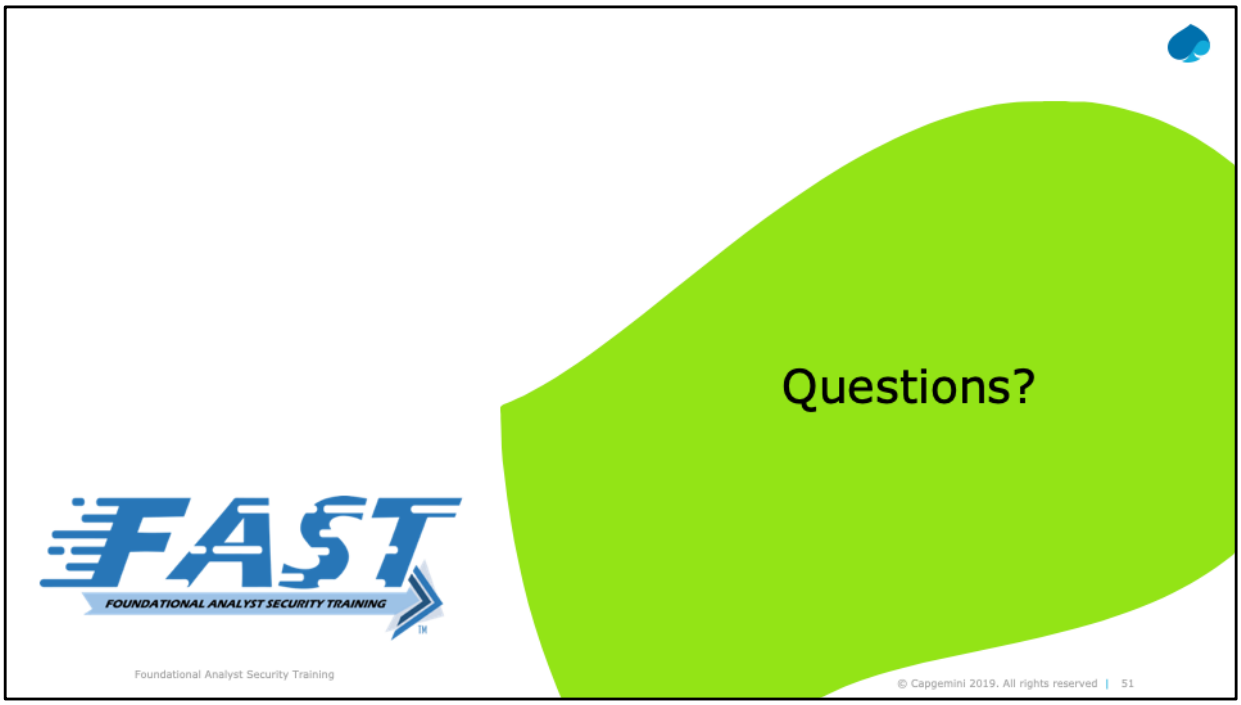
Tracks network usage by individuals and companies.

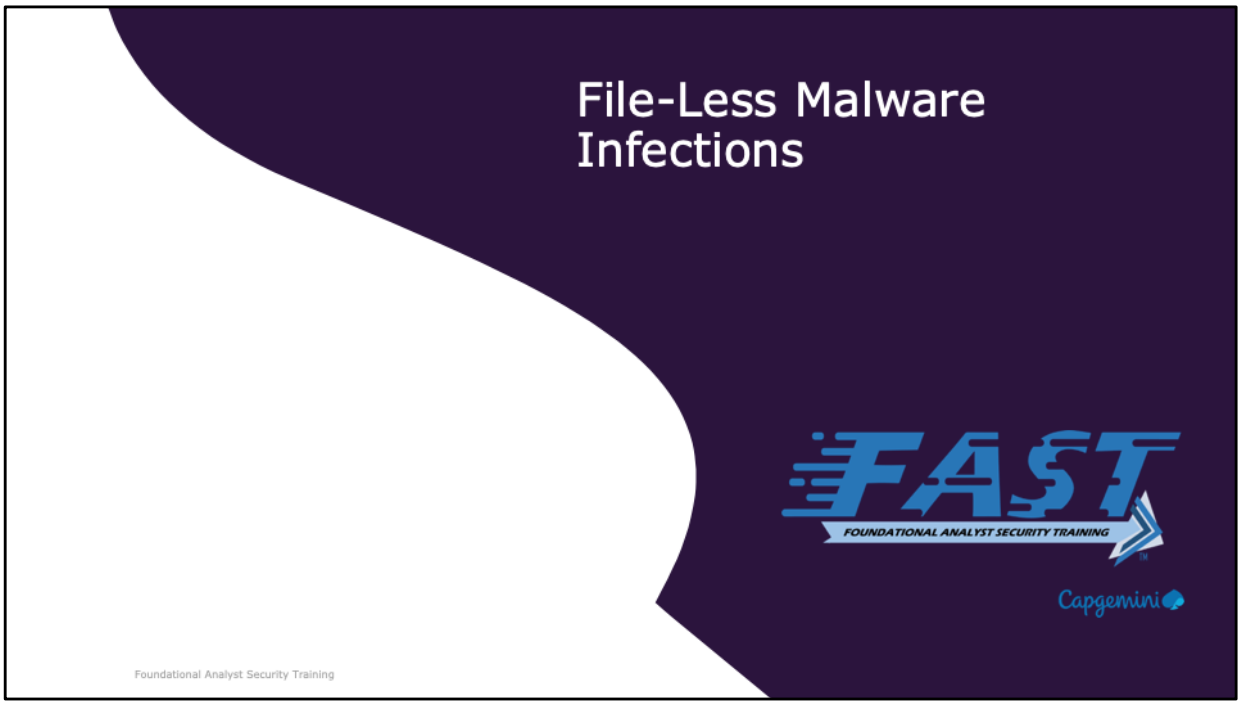
FAST Foundational Analyst Security Training

Instructor Notes:

Spyware

Spyware, as the name gives away, is software that constantly spies on you. Its main purpose is to keep track of your Internet activities in order to send adware. Spyware are also used to gather information about an organization without their knowledge, and send that information to another entity, without consent of the victim.


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 51



Content Source:

https://heimdalsecurity.com/blog/fileless-malware-infections-guide/
https://www.oreilly.com/library/view/digital-forensics-and/9781787288683/d66fdf77-50cd-4ef2-917f-b4dac1ff74dd.xhtml
https://www.hackingarticles.in/volatility-an-advanced-memory-forensics-framework/
http://blog.opensecurityresearch.com/2013/01/windows-dll-injection-basics.html
https://support.microsoft.com/en-us/help/815065/what-is-a-dll
https://www.malwarefox.com/malware-types/
https://us.norton.com/internetsecurity-malware.html
https://www.andreafortuna.org/cybersecurity/what-is-reflective-dll-injection-and-how-can-be-detected/

Module Cyber Kill Chain:

Technology is something that is persistent in our current society. The more complex our technology becomes, the more external threats to that technology evolve. Not all malware is downloaded and run from the hard drive of the computer. Some malware types are capable of running from system memory, never being resident on

the hard drive, making it difficult to detect.

Attribution:

Agenda

Dynamic Link Libraries (DLLs) | DLL Injection | Reflective DLL Injection

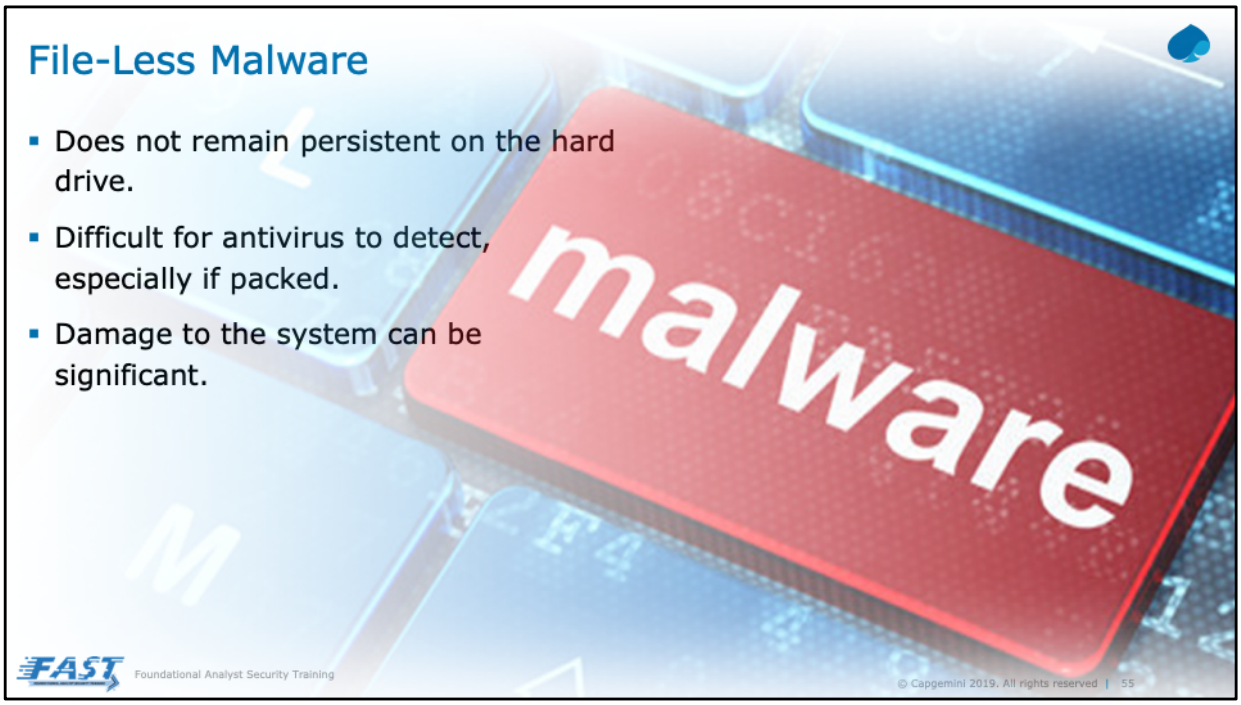
Topic Learning Objectives

Upon completion of this topic, the student should be able to do the following:

Understand what DLLs are and how they are used by system and malicious processes.

Understand the difference between file-less and traditional malware.

Document the differences between DLL Injection and reflective DLL Injection.



Instructor Notes:

So what is a file-less malware infection? It's exactly what you think it is, its malware that does not take up bits or bytes on the physical drive. It resides solely in the volatile system memory of the host computer.

Traditional Antivirus

Malware can be detected, in part, because it is stored somewhere on the hard drive, giving the antivirus something to analyze and detect.

This is not true for file-less malware.

FAST Foundational Analyst Security Training

 | 56

Instructor Notes:

Traditional malware can be stopped by anti-virus because it has a chance to analyze the file structure and content when it is passed on to the hard-drive by the infection. When a matching signature is detected, the file can be quarantined, or removed and the user notified.

Without a file on the host it is difficult for traditional anti-virus to help us protect the host.

File-Less Malware

APTs have four goals for any malicious software attack:

1. STEALTH
2. ESCALATE PRIVILEGES
3. GATHER INFORMATION
4. PERSISTENCE

FAST Foundational Analyst Security Training

Instructor Notes:

As we discussed, evolutions in technology, create corresponding evolutions and innovations by APT's.

File-Less Malware (cont.)

Attackers trade persistence for stealth with file-less malware.

This does not mean they give up on persistence though!

FAST Foundational Analyst Security Training

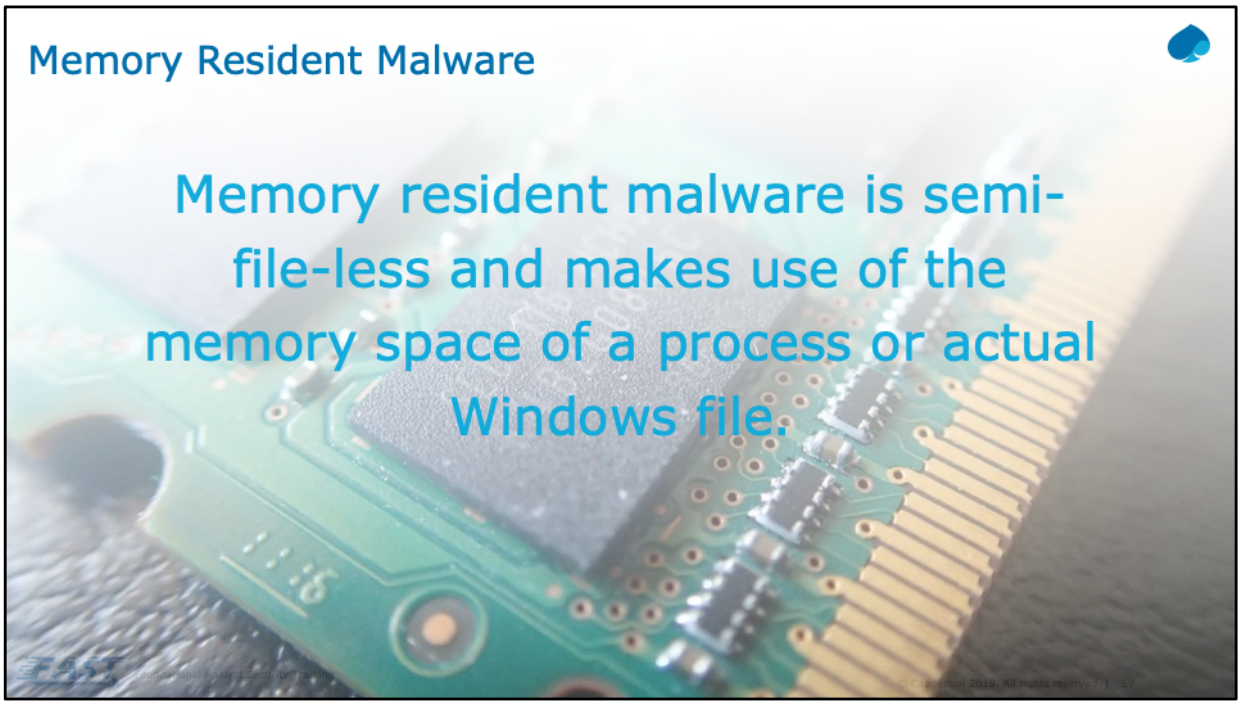
Instructor Notes:

What malware creators have done with file-less infections is **trade persistence for stealth**. Keeping the malware infection concealed while it triggers the intended actions is key here.

When the exploit kit carrying the file-less infection finds its way into the system (we will talk more about this), the malware can fulfill its purpose directly.

But that doesn't mean they give up on the idea of persistence. Once the malware is installed in memory or RAM, file-less malware can hide in places where traditional anti-virus scanning has difficulty.

Including: in Memory, Rootkits, Registry Keys,



Instructor Notes:

z

Dynamic Link Libraries (DLLs)

A DLL is a library that contains code and data that can be used by more than one program at the same time.

Instructor Notes:

For the Microsoft Windows operating systems that are listed in the "Applies to" section, much of the functionality of the operating system is provided by dynamic link libraries (DLL). Additionally, when you run a program on one of these Windows operating systems, much of the functionality of the program may be provided by DLLs. For example, some programs may contain many different modules, and each module of the program is contained and distributed in DLLs.

Dynamic Link Libraries (DLLs) (cont.)

Much of the functionality of the OS is provided by DLLs.

Some programs may contain many different modules, and each module of the program is contained and distributed in DLLs.

Instructor Notes:

Dynamic Link Libraries (DLLs) (cont.)

The use of DLLs helps promote modularization of code, code reuse, efficient memory usage, and reduced disk space.

FAST Foundational Analyst Security Training

 | 62

Instructor Notes:

The use of DLLs helps promote modularization of code, code reuse, efficient memory usage, and reduced disk space. Therefore, the operating system and the programs load faster, run faster, and take less disk space on the computer.

By allowing multiple programs, installed on the computer to use the same code from a shared library.

When a program uses a DLL, a dependency is created. If another program overwrites and breaks this dependency, the original program may not successfully run.

Dynamic Link Libraries (DLLs) (cont.)

Common Windows DLLs

- .ocx – Active X Controls
- .cpl – Control Panel Files
- .drv – Device Driver Files

Instructor Notes:

The use of DLLs helps promote modularization of code, code reuse, efficient memory usage, and reduced disk space. Therefore, the operating system and the programs load faster, run faster, and take less disk space on the computer.

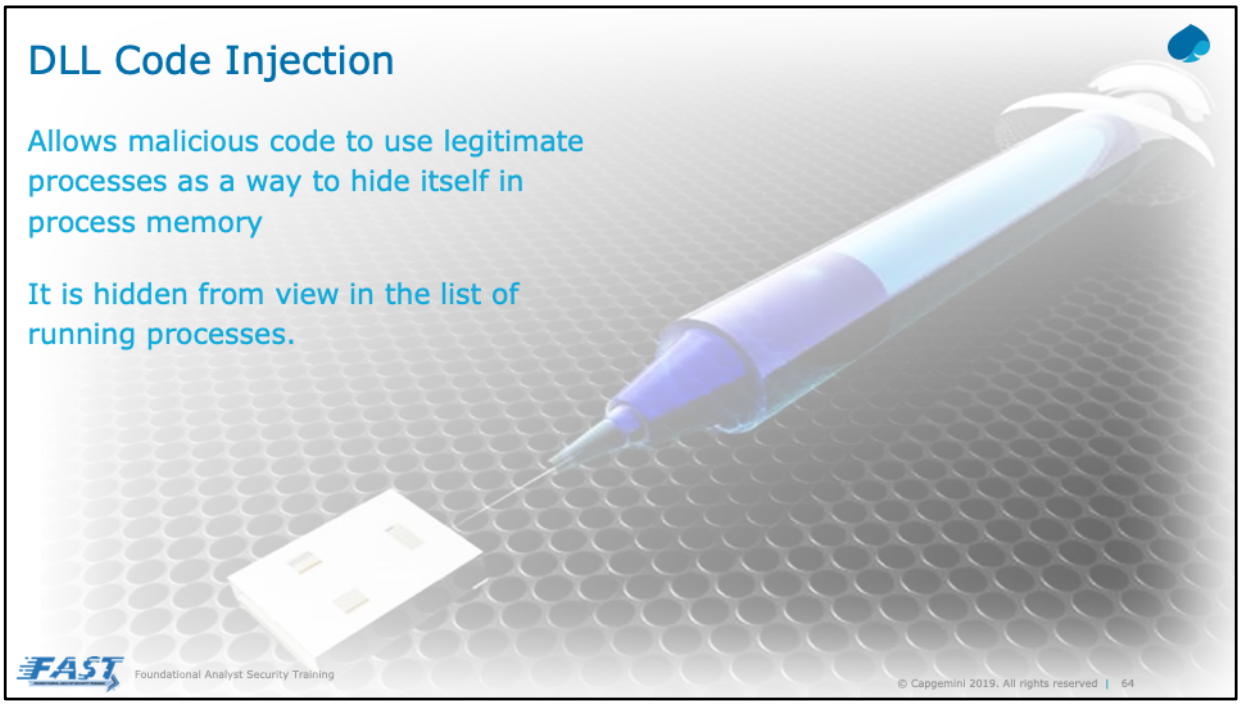
By allowing multiple programs, installed on the computer to use the same code from a shared library.

When a program uses a DLL, a dependency is created. If another program overwrites and breaks this dependency, the original program may not successfully run.

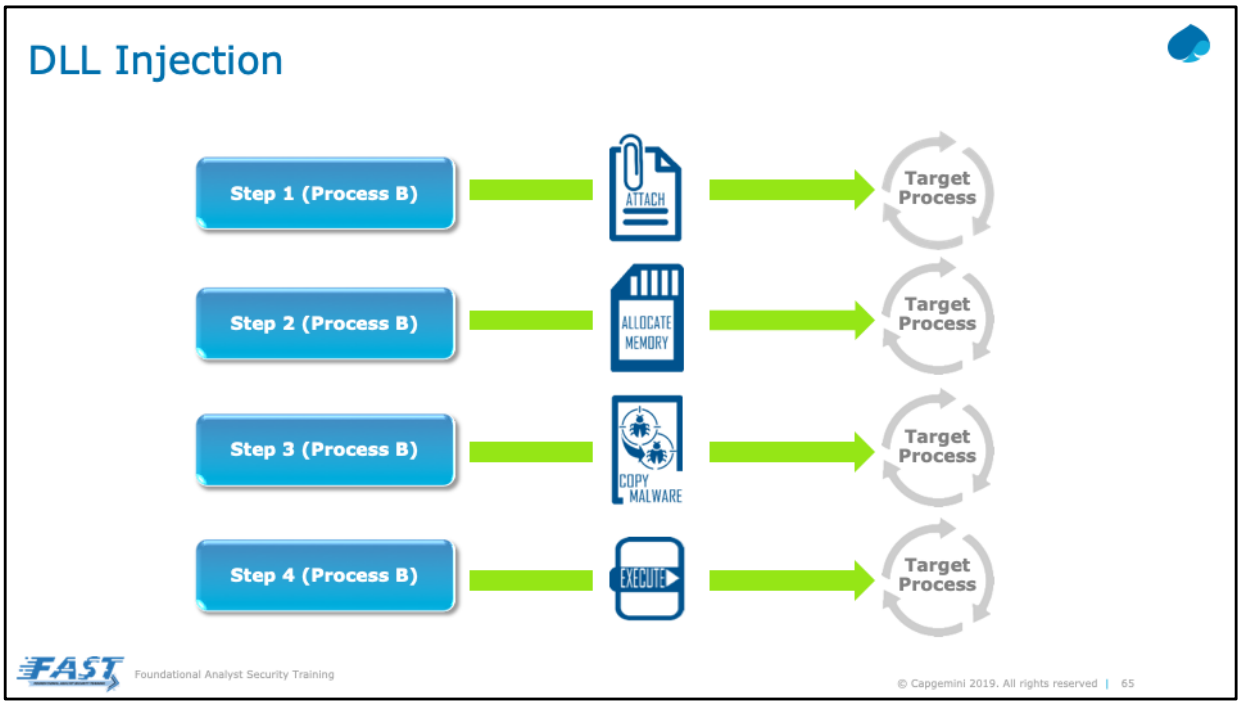
ActiveX Controls (.ocx) files
An example of an ActiveX control is a calendar control that lets you select a date from a calendar.

Control Panel (.cpl) files
An example of a .cpl file is an item that is located in Control Panel. Each item is a specialized DLL.

Device driver (.drv) files
An example of a device driver is a printer driver that controls the printing to a printer.

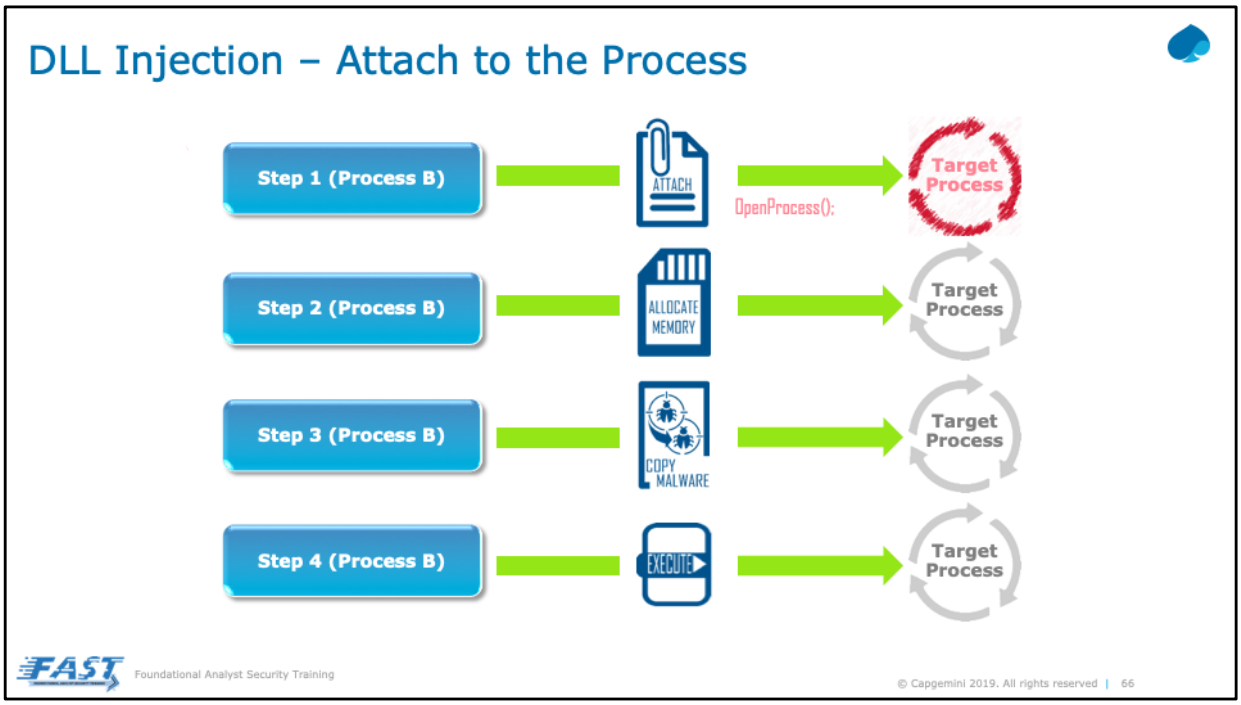


Instructor Notes:



Instructor Notes:

This part of the injection process is the same as a typical DLL Injection.



Instructor Notes:

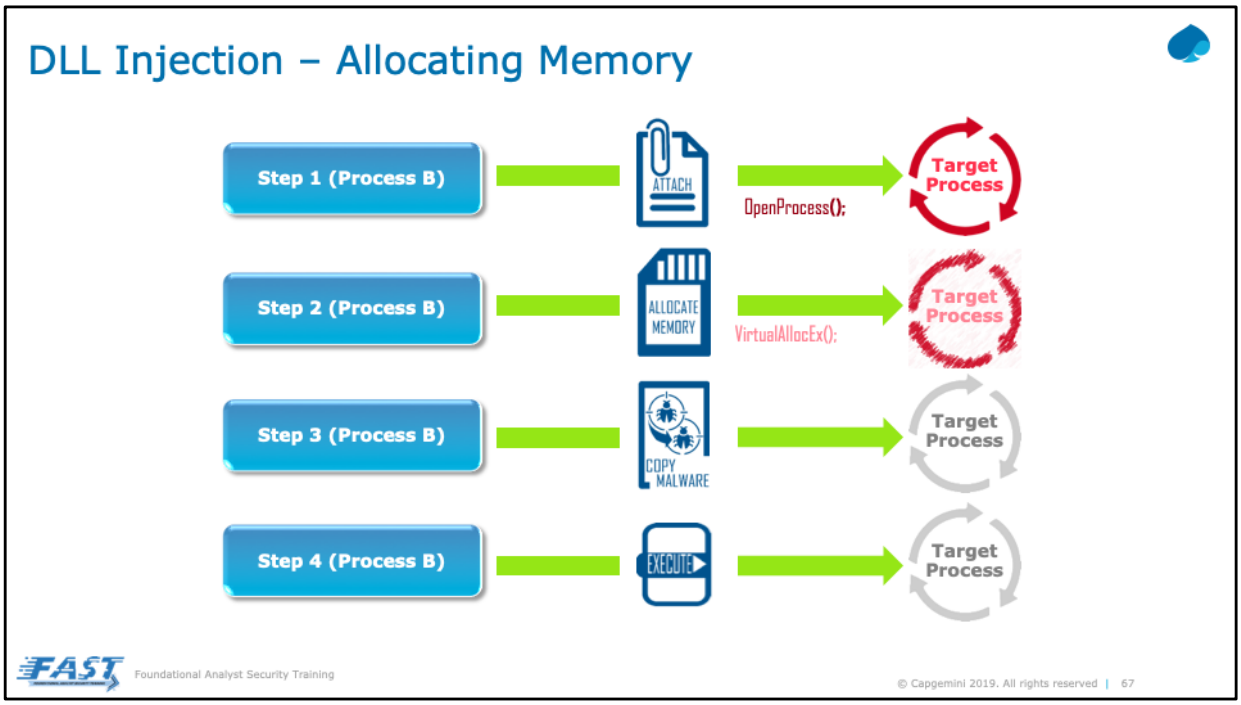
LoadLibraryA()

LoadLibraryA() is a kernel32.dll function used to load DLLs, executables, and other supporting libraries at run time. It takes a filename as its only parameter and magically makes everything work. This means that we just need to allocate some memory for the path to our DLL and set our execution starting point to the address of LoadLibraryA(), providing the memory address where the path lies as a parameter.

The major downside to LoadLibraryA() is that it registers the loaded DLL with the program and thus can be easily detected. Another slightly annoying caveat is that if a DLL has already been loaded once with LoadLibraryA(), it will not execute it. You can work around this issue but it's more code.

First the malware will need a handle to the process so that it can interact with it. This is done with the OpenProcess() function. The malware will need to request certain access rights in order for it to perform the follow on tasks.

The specific access rights it requests vary across Windows versions.



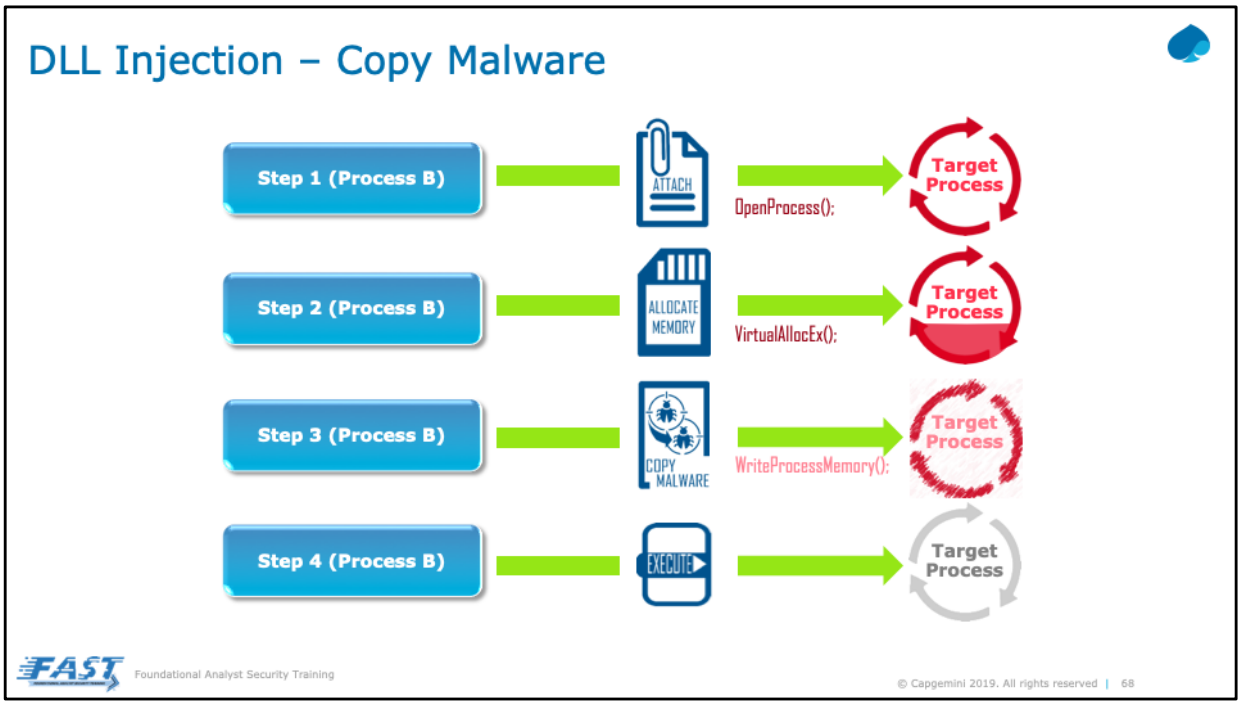
Instructor Notes:

Before the malware can inject anything into another process, it needs a place to put it. It will use the VirtualAllocEx() function to do so.

VirtualAllocEx() takes amount of memory to allocate as one of its parameters. If the malware is to use LoadLibraryA(), it will allocate space for the full path of the DLL and it will jump to the DllMain, and allocate space for the DLL's full contents.

DLL Path
Allocating space for just the DLL path slightly reduces the amount of code the APT needs to write but not by much. It also requires them to use the LoadLibraryA() method which has some downsides, this is a popular method of loading.

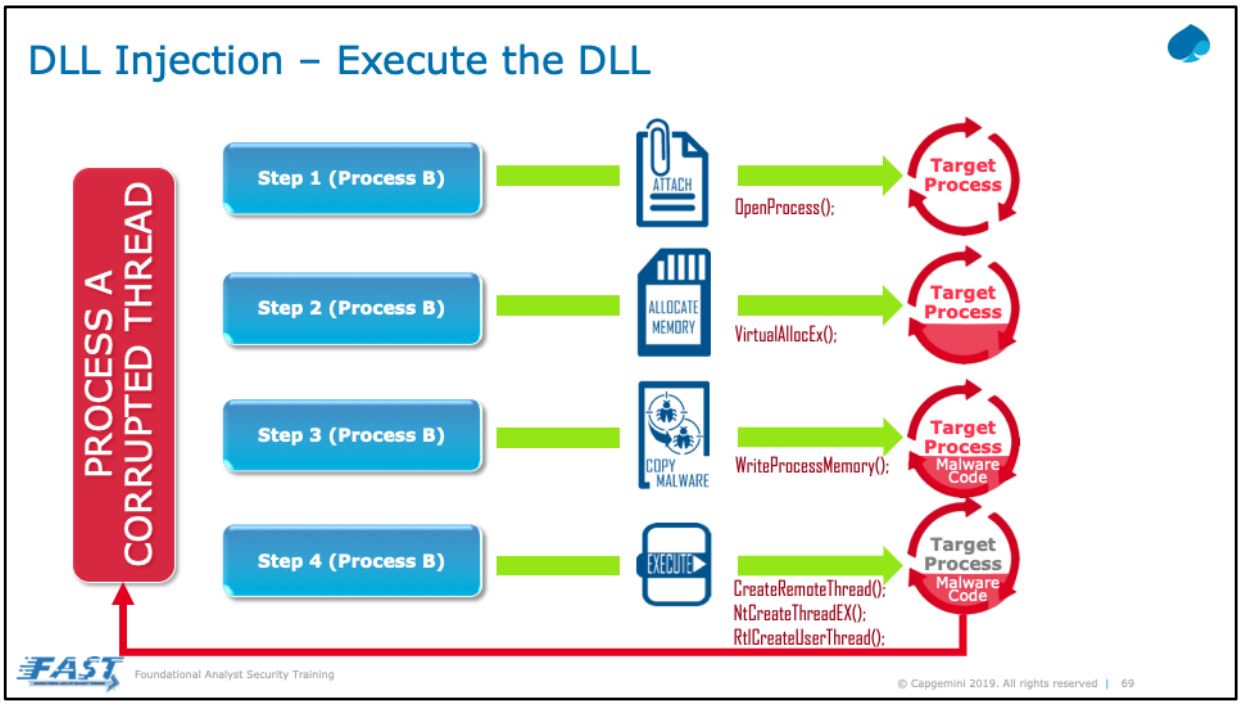
The malware will use the VirtualAllocEx() and allocate enough memory to support a string which contains the path to the DLL:



Instructor Notes:

Depending where the malware is stored, either in a location on the physical disk, or in another location in memory (we will discuss reflective DLL injection next), the code for the function is copied into the memory allocation created in the target process.

The malware will then determine the memory address where the execution will start when run.



Instructor Notes:

Now the malware is in memory, and we know where the memory address is to begin the execution, now the malware just has to execute when told.

The CreateRemoteThread() command is most commonly used, the code will execute and create a child process once the excute command is given. Another possibility is that the NtCreateThreadEx() could be used, this is an undocumented windows function, and may or may not exist on a particular host.

DLL Hijacking is similar to proxying but differs in that hijacking usually abuses Windows' DLL search order in order to compromise a system (or otherwise control the flow of the application). It doesn't usually require the attacker to have write permission to the application's installation directory but rather the directory where the application was launched. In the case that the application attempts to call a non-existent DLL or if an attacker was able to place a malicious DLL in the same directory as a file that launches a vulnerable application, the attacker's DLL would be loaded and code execution would be achieved. This is because Windows [used to] search for application DLLs in the current directory from which the application was

loaded before most other locations.

DLL Injection Pros and Cons

Downsides

- Malware must be self-contained, and the malware must use existing DLLs (no independent functionality).
- Antivirus detections could result from scans of process memory.
- Shows up with other running processes but can be disguised when properly named

FAST Foundational Analyst Security Training

 | 70

Instructor Notes:

DLL Injection Pros and Cons (cont.)

Upsides

- Easily disguised if named correctly
- Easy to execute

Instructor Notes:

Reflective DLL Injection

Typical DLL Injection involves loading malware from a file.

Reflective DLL Injection involves loading the malware from another place in memory.

FAST Foundational Analyst Security Training

Instructor Notes:

Stephen Fewer pioneered the process of reflective DLL Injection, which offers a greater level of stealth in comparison to existing methods

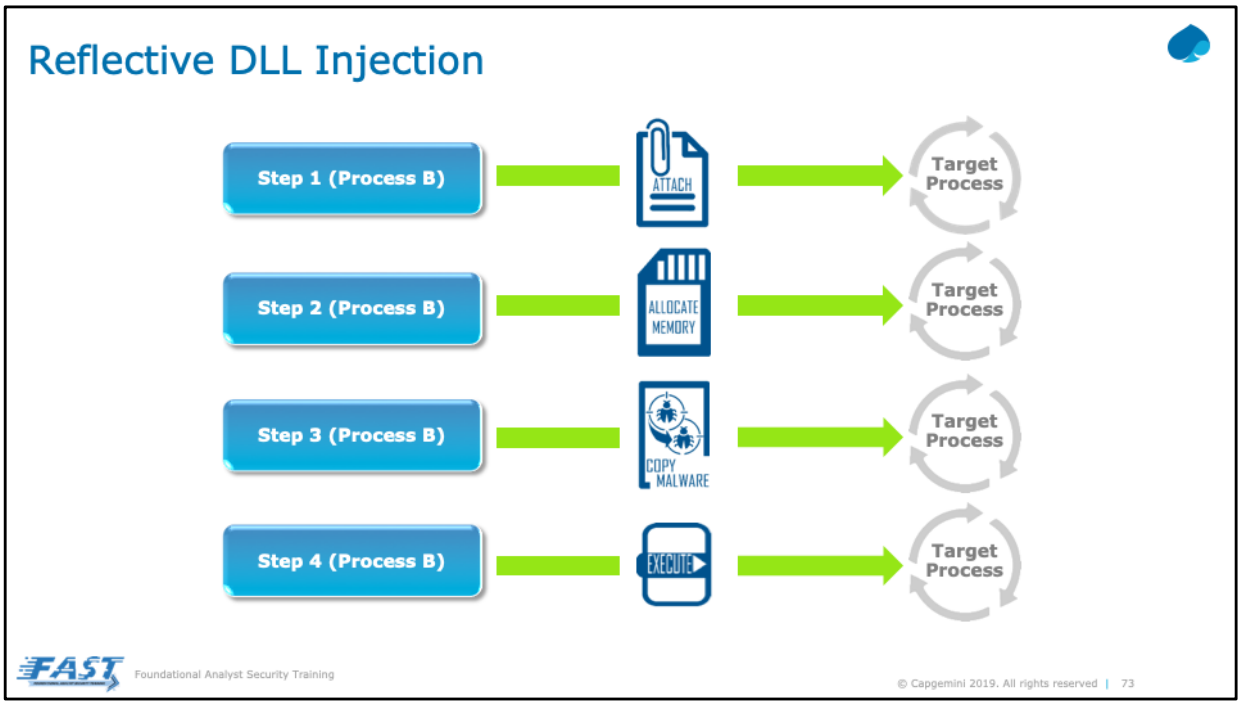
Unlike regular injection, Windows doesn't have a LoadLibrary function that supports reflective DLL Injection so to get the functionality APT's have to write their own code into the malware to accomplish it. This omits some of the things Windows normally does, such as registering the DLL as a loaded module in the process , potentially bypassing DLL load monitoring, all good for stealth.

Full DLL and Jump to DllMain

By copying the entire DLL into memory the malware can avoid registering itself with the process and more reliably inject. The somewhat difficult part of doing this is obtaining the entry point to the target process, when it's loaded in memory.

Luckily enough The LoadRemoteLibraryR() function included within fewers ReflectiveDLLInjection project implements this entirely, however it limits the

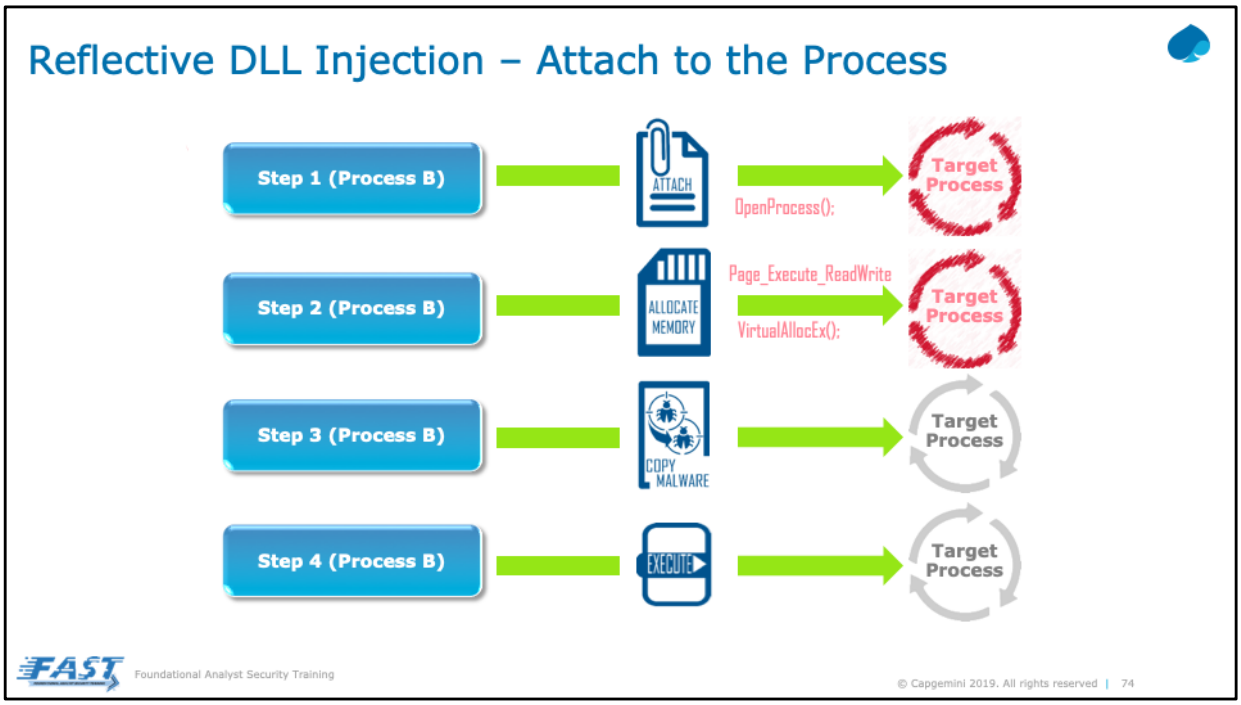
execution method to CreateRemoteThread().



Instructor Notes:

DLL injection is the process of inserting code into a running process. The code we usually insert is in the form of a dynamic link library (DLL), since DLLs are meant to be loaded as needed at run time. However this doesn't mean we cannot inject assembly in any other form (executables, handwritten, etc..). It's important to note that you'll need to have an appropriate level of privileges on the system to start playing with other program's memory.

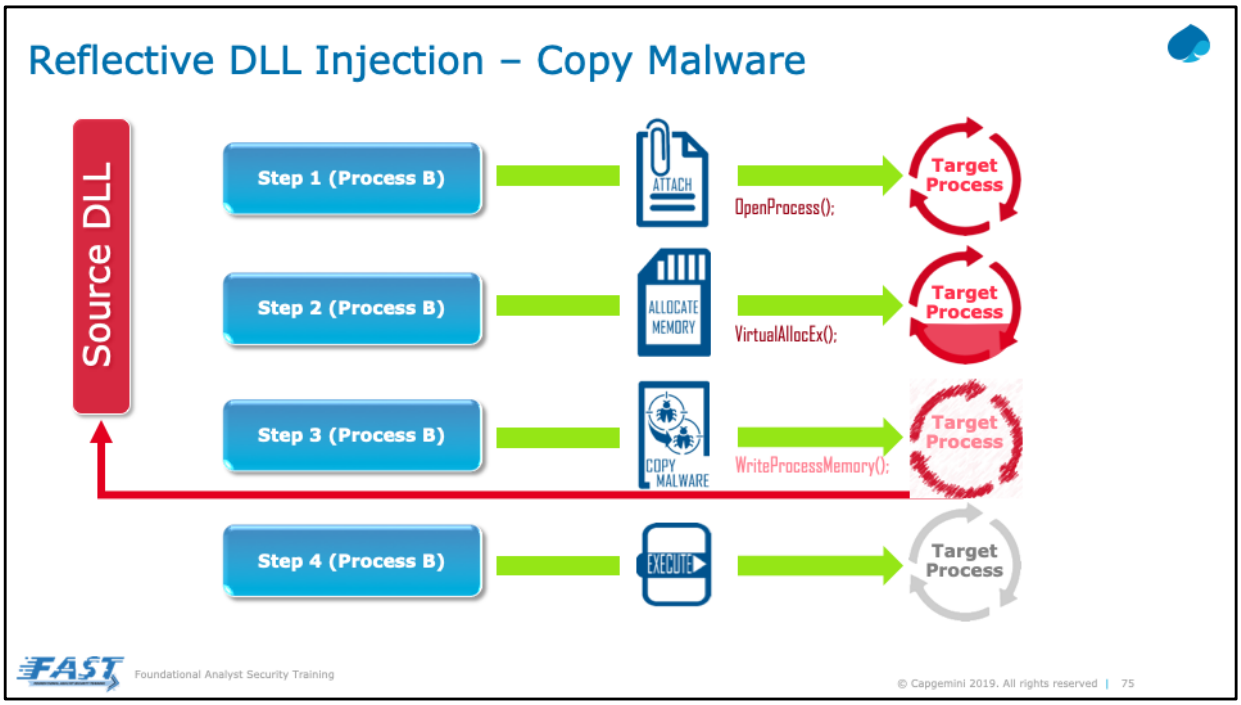
Malware can load itself into the Windows LoadLibrary() in the windows environment to allow it to be injected into legitimate processes running on the system.



Instructor Notes:

The malware allocates memory in the Target Process.

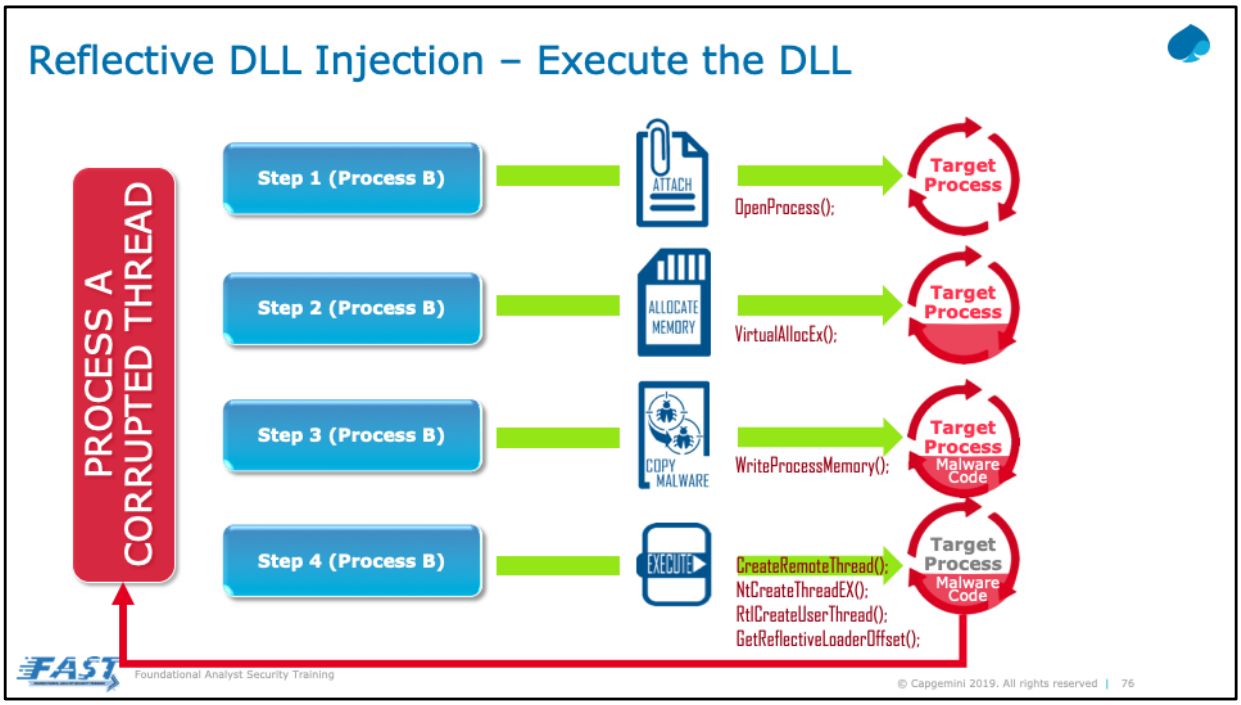
This is set by Sets PAGE_EXECUTE_READWRITE protection on allocated memory in the target process.



Instructor Notes:

The malware will then read the content of the source DLL, and then injects it into its own Memory.

The malware then then copies that information into the allocated memory in the target process.



Instructor Notes:

Since the malware is not relying on the LoadLibraryA(), it has to determine the entry point to the DLL when it's loaded in memory

The function written by Stephen Fewer "GetReflectiveLoaderOffset()" will allow the malware to do so.

The new corrupted thread can be created with the provided address that was allocated, and the offset can be determined.

Reflective DLL Injection Pros and Cons

Downsides

- The DLL has to be modified to increase functionality to allow it to utilize GetReflectiveLoaderOffset().
- Process memory permissions have to be modified (read, write, execute).
  - This will give permissions to private memory with no file mappings.
  - This could look suspicious to a savvy analyst.

FAST Foundational Analyst Security Training

 | 77

Instructor Notes:

Reflective DLL Injection Pros and Cons (cont.)

Upsides

- The LoadLibraryA() is not a part of the injected DLL, so it is never written to disk.
- The injected DLL can come straight from an off-host source and be injected.
- The injected DLL is not documented in any of the lists in the Process Execution Block (PEB).

Instructor Notes:

Detecting Remote DLL Injection

There are several Volatility plugins that can help detect Remote DLL Injections.

- Dlllist: Displays processes loaded into memory
- Ldrmodules: Detects DLLs that have not been linked
- Malfind: Volatility plugin used to find "unpacked" malware

FAST Foundational Analyst Security Training

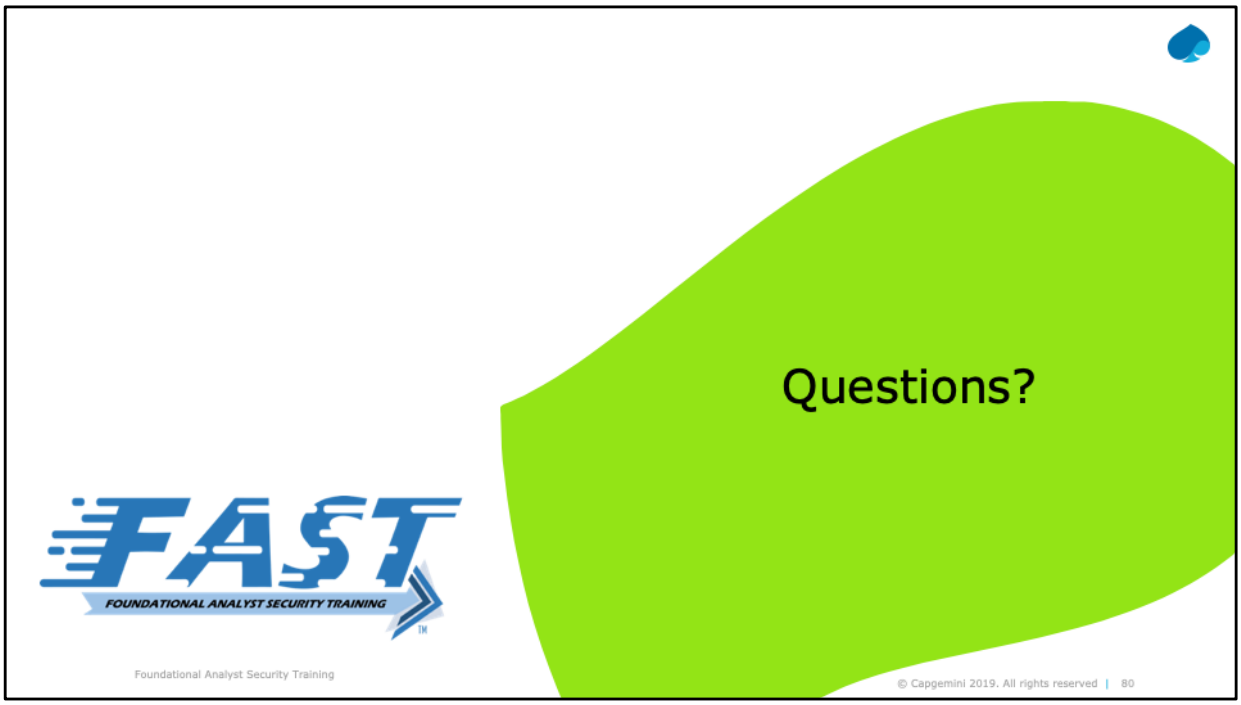
Instructor Notes:

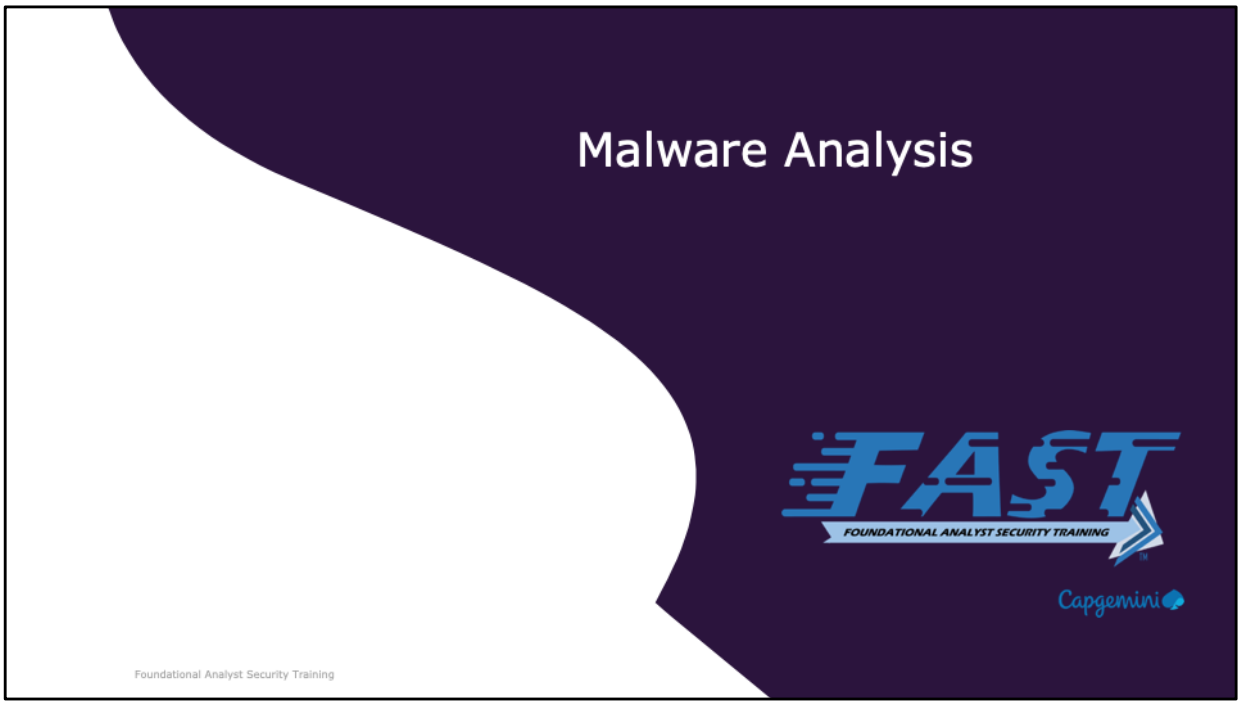
There are several Volatility plug-ins that can help detect Remote DLL Injections.

Dlllist: Displays processes loaded into memory

Ldrmodules: Detects DLL's that haven't been linked.

Malfind: Volitility plugin used to find "unpacked" malware, malfind can detect pages in process memory with PAGE_EXECUTE_READWRITE protection with no file mappings this is indicative of reflective DLL injection. The dump –dir command will give a list of suspect memory areas, and you can do string searches of that content. For example, searching for executable file headers MK, MZ, etc.


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 80



https://resources.infosecinstitute.com/malware-analysis-basics-static-analysis/

Agenda

Static Malware Analysis | Dynamic Malware Analysis

Topic Learning Objectives

Upon completion of this topic, the student should be able to do the following:

- ***Understand what malware analysis is.***
- ***Understand the dangers associated with working with malware.***
- ***Understand how static malware analysis can be used to reverse engineer malware.***
- ***Understand how dynamic malware analysis can be used to reverse engineer malware.***

Malware Analysis

- Malware analysis refers to the process by which the purpose and functionality of the given malware samples are analyzed and determined.
- The culled information from the malware analysis provides insights into developing an effective detection technique for the malicious codes.

Additionally, it is an essential aspect for developing the efficient removal tools that can definitely perform malware removal on an infected system.

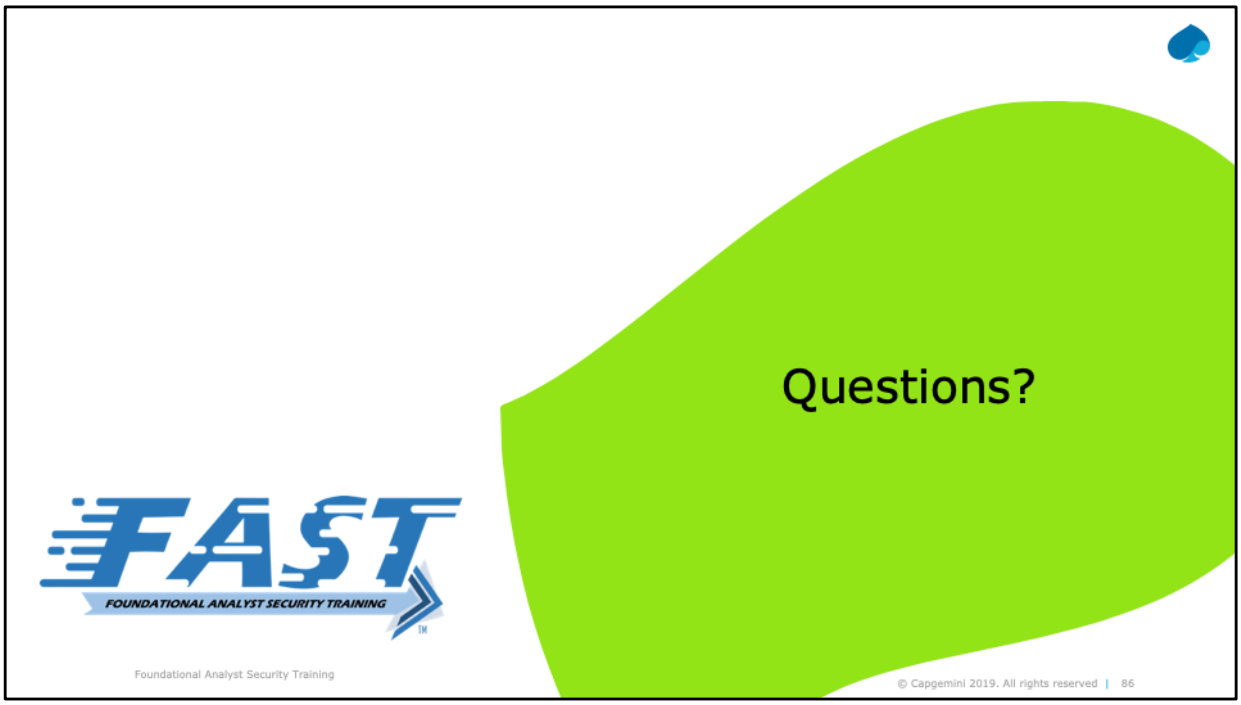
Static Analysis

Static analysis, also called static code analysis, is a process of software debugging without executing the code or program.

In other words, it examines the malware without examining the code or executing the program.

The techniques of static malware analysis can be implemented on various representations of a program.

- The techniques and tools instantaneously discover whether a file is of malicious intent or not.
- Then the information on its functionality and other technical indicators help create its simple signatures.
- The source code will help static analysis tools in finding memory corruption flaws and verify the accuracy of models of the given system.


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 86

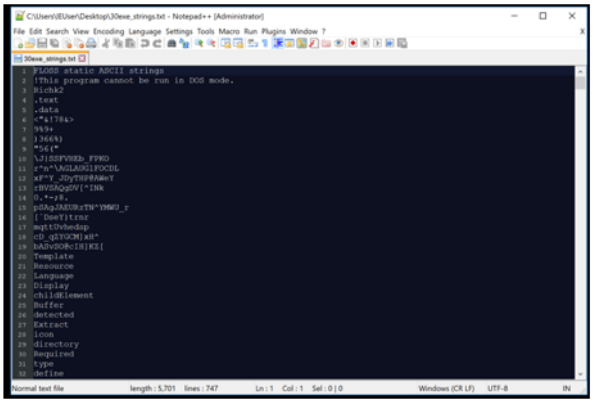
LAB001: Static Malware Analysis

 | 87

Results from Static Malware Analysis

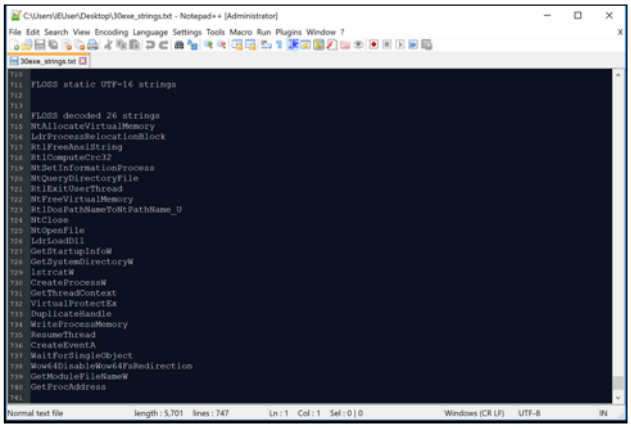
From the static analysis, we know the following:

- We can see that the strings utilized are calling some .dll files, as well as the steps through the program.
- One string to note is at the very beginning, Rich2k, and then .text and .data.



Results from Static Malware Analysis (cont.)

See what system calls are being made.



If you have a packet capture from an incident, this will help to distinguish the traffic generated by the malware from the traffic generated by the user to get a better timeline of the user actions causing the incident.

Always execute the malware with **Administrator** privileges so the full nature of the malware can be explored.

Results from Static Malware Analysis (cont.)

Finally, see the call to msiexec.exe.

```
741
742 FLOSS extracted 2 stackstrings
743 msiexec.exe
744 z8mq
745
746 Finished execution after 6.827000 seconds
747
```


If you have a packet capture from an incident, this will help to distinguish the traffic generated by the malware from the traffic generated by the user to get a better timeline of the user actions causing the incident.

Always execute the malware with **Administrator** privileges so the full nature of the malware can be explored.