



Intro to Cybersecurity

Foundations and Threats

1.2.1 - Malicious Code Part 1

How does malicious software impact computer systems?

Overview

The student will be able to:

- Identify the types of malicious software that exist and how they can be layered to increase the security threat
- Examine how malware has a negative impact on a computer system and also on a person

Grade Level(s)

6, 7, 8, 9, 10, 11, 12

Cyber Connections

- Threat Actors
- Threats and Vulnerabilities

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Teacher Notes:

Malicious Code Part 1

Materials

Power Point: Malicious Code - Part 1

Instructions/rubric for Project: History Malware Research

Slide 1 - Intro Slide

Slide 2 - Back to the Beginning

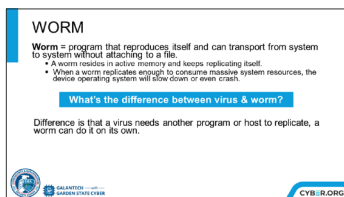
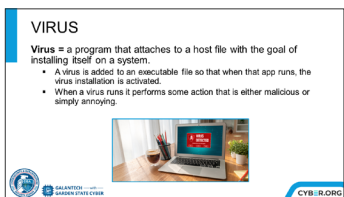
- Ted Talk video about the very first known virus, Brain. Video = 4:39 min
- Video is an edited version to extract just the story of the very first virus - the Brain Virus. The speaker, Mikko Hypponen, tracks down the authors of the virus and asks them “why did you do this?”. Edited video = 4:39 min on Vimeo: <https://vimeo.com/523531811>
- The original Ted Talk can be found here: https://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net

Slide 3 - Virus

- Define Virus

Slide 4 - Worm


- Define worm
 - Make sure the students understand that “replicates” = the ability to modify programs to include a version of the original virus.
 - KEY POINT: Difference is that a virus needs another program or host to replicate, a worm can do it on its own.
 - In real life, there are very few actual viruses that need a host file anymore, it is mostly worms and trojans out there. But it is important to use terminology properly. As the student presentations cover the evolution of malware, it becomes more obvious how we transitioned from viruses to worms.



Teacher Notes:

WannaCry:


- In 2017 the WannaCry ransomware hit over 200,000 computers in 150 countries in just one day.
- Here's the story of how it was stopped. ...



GALANTECH GARDEN STATE CYBER CYBER.ORG

TROJAN

- **Definition:** files that appear to be legitimate programs, but really contain malicious code.
- Usually, will do that one nice thing – play a game, or song, etc. AND it has hidden program.
- The main difference between a Trojan and a virus/worm is that a Trojan does not replicate itself.
- **RAT = Remote Access Trojan**
Definition: Trojan that installs a backdoor for administrative control over the victim PC.




CYBER.ORG

BACKDOOR

- **Definition:** programs that create a mechanism for gaining access to a computer.
 - leave a port open
 - create a bogus user with privileges
- Usually delivered through a Trojan horse

netbus
BackOffice
Subseven
TDRkit } examples of malicious backdoors.

VNC
PC Anywhere } examples of legitimate backdoors.



CYBER.ORG

Slide 5 - WannaCry

- Video about the WannaCry Worm which, at the time in 2017, held the title for most widely spread malware. Video = 9:39. Note, that this video is a bit long but the story is a good model for what students will be asked to report on in the upcoming Historic Malware Research project on YouTube, start at 0:23. https://www.youtube.com/watch?v=PWh4UaODijU&t=23s&ab_channel=TomorrowUnlocked
- Note that in many malware stories we don't have all the details. In some cases, we know who created it, in others we may only know what damage was done and in the case of WannaCry, we know who was able to stop it. Each iconic malware has an interesting story that shows how it played an important part in what cybersecurity practices were developed in response to those threats.

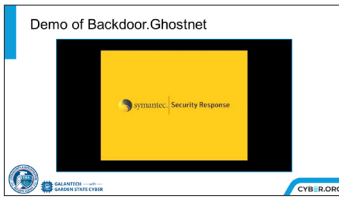
Slide 6 - Trojan

- Define Trojan (including RATs).
- The legitimate program of a Trojan usually DOES work - you actually get to play that game, song or movie. That was the person who has the Trojan doesn't suspect anything unless it's poorly made. LOTS of Internet free games are actually Trojans for malware. You happily download the free software and install it on your device, it happily installs some extra malware code in the background.
- The most dangerous type of Trojan is the RAT - Remote Access Trojan, which is essentially a backdoor packed inside a Trojan. The Trojan delivers code onto your machine that makes it possible for the hacker to remotely access your system and try to control it.

Slide 7 - Backdoor

- Identify specific known backdoor programs and on next slide watch video that demonstrates one version of a backdoor in action.
- A backdoor exists to provide a means of going in and out of a computer. Two popular methods to accomplish this are to leave a port open or to create a user with privileges. The "payload" of a Trojan horse is often a backdoor.
- Listed are a few well-known malicious backdoor programs BUT there are reasons why a legitimate user would want to be able to access their computer when they are away from home or the office. VNC = Virtual Network Computer and PC Anywhere are 2 popular legitimate programs to access your computer remotely. And they work by leaving a port open that can be accessed specifically by that program.

Teacher Notes:



From Backdoors to BOTNETS

1. Trojans or other malware are used to deliver a Backdoor program onto your computer or IoT device.
2. The Backdoor program is used to communicate back to the "Command and Control server" - aka C2C server.
3. The C2C server sends your PC program code to perform an action such as sending out spam or stealing information or participating in a Distributed Denial of Service attack.

Your device is now in a botnet - and it's likely you don't know it!

LOGIC BOMB

- **Definition:** small program that is timed to perform an operation on a system.
- It can also be triggered by an external event.
- A programmer might install a logic bomb on a system, timing it to go off long after he or she has left the company.

ROOTKIT

- **Definition:** a group of programs installed by an attacker to gain complete control of a computer.
- Changes how the operating system functions
- Can hide its processes and actions so that it is not detected by antimaware or the user.
- **How to STOP IT -** you don't. It is too difficult to be sure all of the rootkit is removed. Solution is to wipe the hard drive and reinstall the Operating System and files.

Slide 8 - Demo, Backdoor Ghostnet

- Video by Symantec Security Response = demonstrates one version of a backdoor in action = 4:36 min <https://vimeo.com/523592151>

Slide 9 - BOTNETS

- So, the sequence goes like this: virus, worm, or trojan infects your computer - it puts a backdoor program on your computer - the backdoor activates and communicates with the botmaster - and you computer is now part of a botnet of other computer computers that can be multiplied into a very powerful mass attack.
- Compromised computers, unknown to their innocent owners, are being used by hackers to send out large volumes of spam, launching distributed denial-of-service attacks, or stealing confidential information. Typically, they are home users who are not properly protected with up-to-date anti-virus software, firewalls and security patches.
- Video = 3:09, <https://www.youtube.com/watch?v=6V5BeXypd6U&t=86s&ab>. Channel = IDGTECHtalk

Slide 10 - Logic Bombs

- A logic bomb is often the tool of a disgruntled insider like an employee who has been terminated or someone who is in the pay of a competitor
- It is malicious code that delivers its payload based on some trigger event. Logic Bombs are also called "Time Bombs" when the trigger for a logic bomb is time or date based.


Slide 11 - Root Kit

- Usually, a malicious actor will use a Backdoor to install a Root Kit. With the two of these together, he will have unlimited access to and control over your PC.
- It may seem like all of this malware is essentially the same thing - but they each have their unique task to perform:
 - Trojan - deliver backdoor to the victim system
 - Backdoor - allow access to the victim system
 - Rootkit - take over control of the victim system
- Worms and Viruses and Logic Bombs are not often part of this chain. They usually are single task oriented.

Teacher Notes:

ZERO DAY

- Zero Day – an attack that takes advantage of code flaws that have VERY recently been discovered.
- Key to a Zero Day Attack is that there is a time period where the flaw is not known to exist so there are no defenses or signatures against it.
- Vulnerability window = time between start of attacks and the time a solution is released. (Usually, a software or OS update!)



The diagram shows a horizontal timeline with four stages: 1. Software is Developed, 2. Attacker Detects Vulnerability, 3. Malware is Released, and 4. Detection & Patching. A red arrow labeled 'Zero Day Vulnerability Timeline' points to the start of the second stage.

GALANTECH —with— GARDEN STATE CYBER


CYBER.ORG

Slide 12 - Zero Day

- Zero Days are worth including here as they are part of the larger picture of system attacks. However, they are NOT actually malware - instead, a Zero Day is a flaw that exists in the code of an application or OS. Of course, most programs have some sort of flaws, but the ones we care about are the areas in which the programmer made the code work but didn't think through the security of the application. This means that there is a vulnerability and once that vulnerability is discovered it can be exploited. NOTE: Zero Day exploits can be sold for a LOT of money depending on what type of application is vulnerable. (\$1,000 to \$100,000)
- Timeline details.
 1. Software is developed - software is developed but unbeknownst to the developers, it contains a security vulnerability.
 2. Attacker detects vulnerability - a bad actor finds a vulnerability either before the developer or exploits it before a developer having an opportunity to release an update or patch.
 3. Malware is released - attackers release malware to exploit software while the vulnerability is still open and unpatched.
 4. Detection & Patching after hackers release the exploit, either the public detects identity or data theft or the developer uncovers, and creates a patch.

APT - Advanced Persistent Threat

- Definition: an attack that uses sophisticated methods to establish a presence on a system or network for an extended period of time. Maintains multiple ways in and out, often used to exfiltrate data
- Signs of an APT Attack
 - Off-hours activity showing up in logs
 - Large unknown files or strange data flows
 - Multiple RATs found by security scans
 - Spear-phishing emails
 - Pass the hash tools



A bracket groups the last three items in the list: Spear-phishing emails, Pass the hash tools, and tools for initial entry.

GALANTECH —with— GARDEN STATE CYBER

CYBER.ORG

Slide 13 - APT

- Define APT (Advanced Persistent Threat)
- The APT is a corporate cybersecurity department's nightmare. An APT is a sophisticated attack with multiple components. It is typically used for a targeted attack, not an attack of opportunity. In other words, the attacker wants specifically a thing from an entity. Might be intelligence from a government agency or it might be the plans for a new drug from a pharmaceutical company. An APT will be installed so that there can be a continuous infiltration of this entity over a long period of time in order to "exfiltrate" the desired data.
- Exfiltrate - use stealthy methods to perform unauthorized transfer of data.
- It can be very difficult to identify an APT on a system or network, but most companies know that its not "whether" you have an APT, its "when" - because everyone will eventually have one if they have a healthy, profitmaking entity. The best bet is to either notice attempts to get in OR notice the extra activity.

