Intro to Cybersecurity

1.2.1 - Malicious Code Part 1

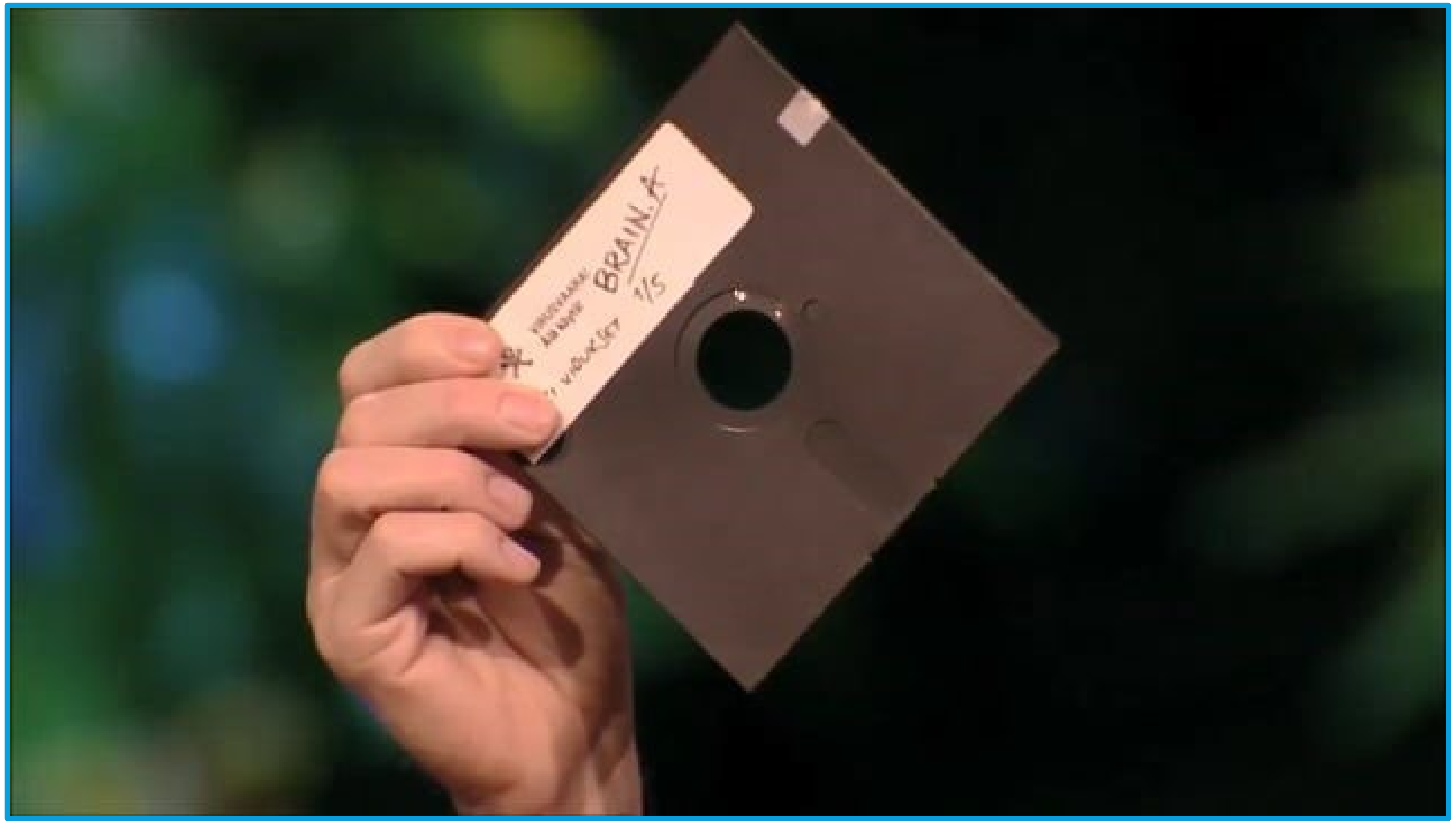
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

GALANTECH —with— GARDEN STATE CYBER

CYBER.ORG

Let’s go back to the very beginning

- What was the very FIRST piece of malware?



VIRUS

Virus = a program that attaches to a host file with the goal of installing itself on a system.

- A virus is added to an executable file so that when that app runs, the virus installation is activated.
- When a virus runs it performs some action that is either malicious or simply annoying.

WORM

Worm = program that reproduces itself and can transport from system to system without attaching to a file.

- A worm resides in active memory and keeps replicating itself.
- When a worm replicates enough to consume massive system resources, the device operating system will slow down or even crash.

What’s the difference between virus & worm?

Difference is that a virus needs another program or host to replicate, a worm can do it on its own.

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 . . .

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.

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
BackOrifice
SubSeven
T0rnkit

examples of malicious backdoors.

VNC
PC Anywhere

examples of legitimate backdoors.

Demo of Backdoor.Ghostnet

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

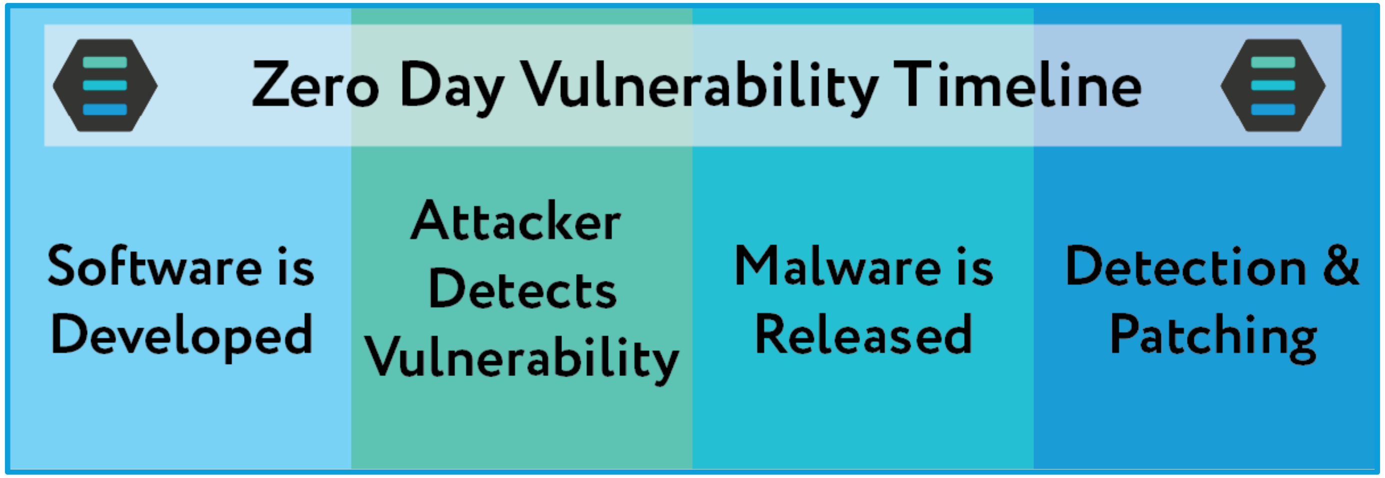
- **Definition:** a group of programs installed by an attacker to gain complete control of a computer.
- Changes how the operating system functions
- Can hide its processes and actions so that it is not detected by antimalware or the user.
- **How to STOP IT** - you don't. It is too difficult to be sure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

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!!)



Zero Day Vulnerability Timeline

Software is Developed

Attacker Detects Vulnerability

Malware is Released

Detection & Patching

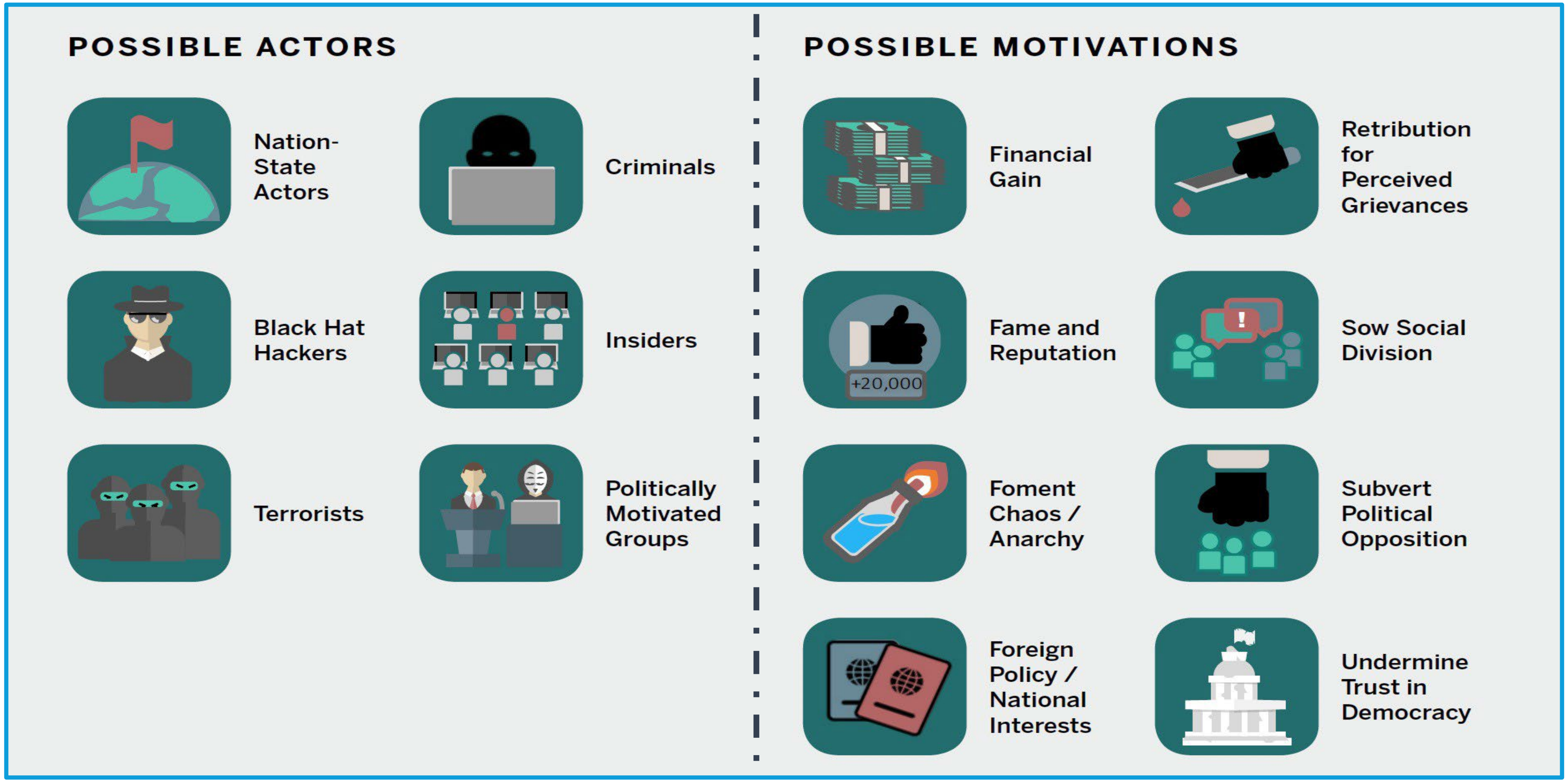
APT - Advanced Persistent Threat

- **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

tools for initial entry

The Who and the Why of Cyber Threats



POSSIBLE ACTORS

- Nation-State Actors
- Criminals
- Black Hat Hackers
- Insiders
- Terrorists
- Politically Motivated Groups

POSSIBLE MOTIVATIONS

- Financial Gain
- Retribution for Perceived Grievances
- Fame and Reputation
- Sow Social Division
- Foment Chaos / Anarchy
- Subvert Political Opposition
- Foreign Policy / National Interests
- Undermine Trust in Democracy

Source: https://www.belfercenter.org/sites/default/files/2018-02/cyberactorsmotivations.jpg

Intro to Cybersecurity

Activity – Historic Malware

GALANTECH —with— GARDEN STATE CYBER

CYBER.ORG