DR. SARAH ABRAHAM

CS349

CYBERWARFARE

WHAT IS THE MORRIS WORM?

- Morris Worm created in 1988 by Cornell graduate student, Robert Morris, supposedly to gauge the size of the Internet
- Worm spread to Internet-connected machines running BSD (Unix flavor)
- Designed to be undetectable but bug led it to create more copies of itself that intended leading systems to become over-taxed
- Morris first individual to be charged under the then new Computer Fraud and Abuse Act of 1986
- After completing sentence three years of probation, 400 hours of community service and a $10,050 fine, Morris now is tenured professor at MIT

WHAT DOES THIS HAVE TO DO WITH CYBERWARFARE?

FIRST, LET'S DEFINE "CYBER"

- Norbert Wiener titled 1948 book "Cybernetics"
  - From Greek κυβερνήτης or "steersman, pilot, navigator, governor"
  - Book's subtitle was "control and communication in the animal and machine"
- So what then is cyberwarfare?

JUS AD BELLUM (RIGHT TO WAR)

- Article 2(4) of the UN Charter prohibits every nation from using "the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."
- Conceptual muddle: what constitutes a threat or use of force?

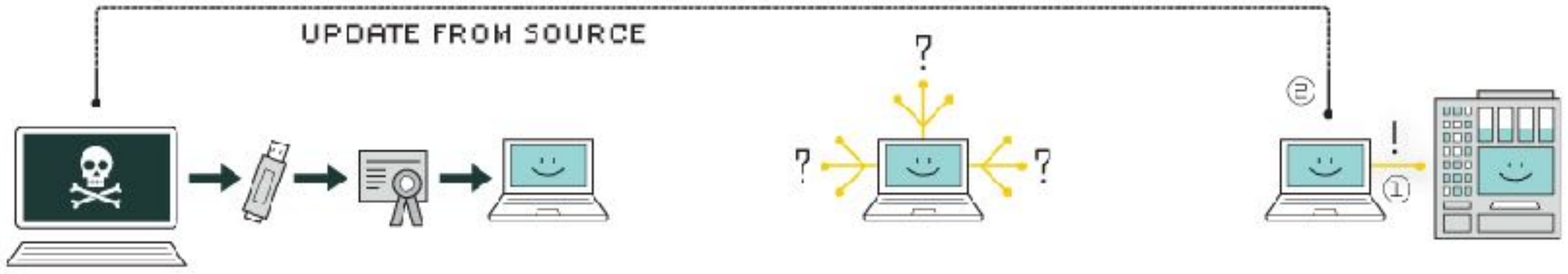
OPERATION AURORA

- In 2009, Google, Adobe, and 32 other high-profile companies targeted by a highly sophisticated virus originating from China
  - Companies in technology, finance, and defense sectors
  - IP stolen and accounts of human rights activists targeted
- Attackers used dozens of pieces of malware and multiple levels of encryption to hide on company networks
  - Attack entered system after employees visited malicious websites
  - Exploited flaw in Internet Explorer that was known by Microsoft internally but not patched till after the attack

STUXNET

- In January 2010, Iranians discovered Natanz Nuclear Facility had been targeted by worm for the past two years
- Stuxnet targeted plant's control systems of centrifuges, causing them to fail at an unusually high rate
- Uranium must be processed to increase concentration of active isotope, U-235, which in is only 0.7% of natural uranium
- Small difference in weight allows the U-235 isotope to be separated from the predominant U-238 isotope
- Centrifuges spin at over 60,000 RPM to separate isotopes and enrich the uranium

HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities - software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

STUXNET AFTERMATH

- First version of worm caused failures in centrifuges, second version caused OSes to repeatedly crash and reboot
  - Belarusian malware-detection firm called to investigate
  - Four zero-day (previously unknown) exploits used to break into Microsoft operating system
- In 2012 Chevron first US corporation to publicly confirm that Stuxnet had spread across its machines
  - Siemens systems have no direct connection to Internet, so five outside companies believed to be connected with nuclear program were infected
- Authors of Stuxnet never confirmed but leaks to press from US and Israel suggest nations worked in collaboration to create it

WHAT MAKES STUXNET DIFFERENT?

- Worm caused physical damage rather than just stealing or modifying information
- Sophistication and levels of attack suggest virus took around two to three years to author
- Likely US operation targeted software created by US corporations
- Connections discovered between Stuxnet and Flame discovered
  - Used for cyber espionage in the Middle East
  - Could exchange data with any Bluetooth-enabled device
  - Entered systems disguised as a legitimate Windows 7 update

WHAT DOES THIS MEAN FOR THE FUTURE OF CYBERSECURITY?

TRITON

- In December 2017, an industrial plant of undisclosed nature and location was targeted by hackers
  - Plant believed to be in Middle East
  - Hackers believed to be associated with a nation-state
- Malware, nicknamed Triton, hijacked workstation using Schneider Electric's Triconex, which is used in power plants
  - Tried to modify controllers to identify safety problems
  - When controllers entered a failsafe state, operators conducted investigation that revealed malicious code

WHAT DOES THIS MEAN FOR THE FUTURE OF WAR?

SOUTH OSSETIA AND ABKHAZIA

RUSSO-GEORGIAN WAR

- In 2006, Georgian province of South Ossetia held referendum of independence
  - Referendum declared illegal by Georgian government
  - South Ossetia backed by Russia
- Early in 2008, Russia deployed “peace-keeping” forces within South Ossetia and Abkhazia
- In August, Georgian troops began artillery attack on South Ossetia capital of Tskhinvali
- Russia responded by moving tanks and soldiers through South Ossetia to attack Georgia
  - Russian-backed troops conducted ethnic cleansing, rape, looting, and hostage-taking of Georgian villagers
- EU investigation deemed both sides in violation of international law

INITIAL CYBERWARFARE

- Attacks against Georgia's Internet infrastructure began as early as July
  - Coordinated distributed denial of service (DDoS) attack that overloaded Georgian servers
  - Command and control server directing the attack was based in US
  - Likely a test run before actual invasion of Georgia

COORDINATED CYBERWARFARE

- During conflict in August, Georgian banking and government websites defaced by hackers while undergoing DDoS
  - Outside agencies and services temporarily took over hosting of bank and government websites
- Days later, Russian news agency, RIA Novosti, hit with DDoS attack
- Russia's attacks likely coordinated by criminal organization, Russian Business Network (RBN)
  - Linked to other illegal activities such as child pornography, phishing, spam, malware and identity theft
  - Ran the then operational Storm botnet
  - Attack on South Ossetia likely connected to Russian government

THE CYBERATTACK ON ESTONIA

- In 2007, Estonia was first known nation to be subject to a cyberattack after moving monument to Soviet Red Army
- Looting and rioting erupted in capital of Tallinn
- DDoS attacks hit Estonian banks, media outlets, and government bodies

NO NATO RESPONSE?

- Article Five of Nato guarantees allies will defend each other even from cyberattacks
  - But only if cyberattack results in loss of life equivalent to military action
- In response, Estonian government established the voluntary Cyber Defense Unit
  - IT experts train for attacks against major utilities and/or service providers

REFERENCES

- <https://limn.it/the-morris-worm/>
- <http://pangaro.com/definition-cybernetics.html>
- <www.globalization101.org/law-of-armed-conflict/>
- <https://www.wired.com/2010/01/operation-aurora/>
- <http://www.zdnet.com/article/microsoft-knew-of-ie-zero-day-flaw-since-last-september/>
- <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>
- <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>

REFERENCES

- <https://fas.org/issues/nonproliferation-counterproliferation/nuclear-fuel-cycle/uranium-enrichment-gas-centrifuge-technology/centrifuge-works/>
- <https://www.engadget.com/2017/12/17/hackers-shut-down-plant-by-targeting-safety-system/>
- <https://www.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict/index.html>
- <https://www.theguardian.com/world/2009/sep/30/georgia-attacks-unjustifiable-eu>
- <http://www.nytimes.com/2008/08/13/technology/13cyber.html>
- <http://www.bbc.com/news/39655415>