Cyber Conflict Part II

Nishant Jain
2/14/18
CPSC 610: Topics in Computer Science and Law

Topics and Themes

Outline:

1. Sony Hack (2015)
2. Stuxnet Cyber Weapon (2009-10)
3. Estonia Cyber Attack (2007)

How do the traditional laws of war apply to conflict in the cyber domain?

- Difficulty of Attribution
- Proportional Response
- Governmental Involvement

Sony Hack

-Overview: in 2015, Sony Pictures was preparing to release a movie (comedy) about the assassination of North Korean leader Kim Jong Un

-Sony was targeted by a devastating cyber attack that compromised a vast amount of its data and destroyed its technical infrastructure

-Terabytes of data were stolen

Confidential Data was made public (Emails, unreleased movies, employee info such as SSN, Banking Statements, Financial reports)

Source: https://seeklogo.com/images/S/Sony_Pictures_Entertainment-logo-693A80FF27-seeklogo.com.png

The Interview

-Comedy film starring Seth Rogen and James Franco

-Movie centers around plot to assassinate North Korean Leader

-Promotional materials provoked North Korean response

-NK Spokesman declared the movie "the most blatant act of terrorism and war" - NK has been known to employ hacking in the past

FROM THE WESTERN CAPITALIST PIGS WHO BROUGHT YOU
NEIGHBORS AND THIS IS THE END
JAMES FRANCO
THE
INTERVIEW
SETH ROGEN

The Interview. Source: https://www.rottentomatoes.com/m/the_interview_2014/

Inadequate Security Measures

-Sony had very lax practices related to information security

-No Two-factor authentication for accessing the network/email accounts

-Lax Email Retention Policy: up to 7 years of unencrypted emails were stored on the server

-IT Admin Usernames and Passwords were kept in spreadsheets

-Hardware/Infrastructure was not monitored:
"In the fall of 2013, while transferring studio security monitoring from an outside vendor to a corporate Sony team, one firewall and 148 routers, switches, and web servers were left unwatched for months"

The Beginning of the Hack

-FBI believes that Sony's network was first breached in September 2015 through "spear phishing—duping an employee into clicking on an email attachment or a web link" (Fortune)

-In security, it is critical to detect breaches ASAP: the Sony hackers had 2 months of undetected access!!

Breach

-Once the network had been breached, there were not many safeguards for protecting access to data

-Sony didn't employ intrusion-detection tools to detect abnormal file transfers and behaviors. Hackers were also careful to move data gradually over a number of weeks

-After stealing terabytes of data, the hackers unleashed malware (igfxtrayex.exe) that deleted contents of hard drives and left computers unbootable

Interview and Threats

-After posting several threatening messages to members of Sony, the Hackers began demanding that the Interview not be released

-Hackers said "stop immediately showing the movie of terrorism" (Fortune)

-The movie continued to be promoted and was scheduled for a Christmas release

-Hackers made physical threats of terrorism against movie theaters, referencing 9/11

Sony Response

Big Movie chains refused to show the movie.

Sony cancelled the Christmas release. Also pulled TV advertising, cancelled press screenings, and stopped promoting it on social media

This move, also resulted in criticism:

President Obama: "We cannot have a society in which some dictator someplace can start imposing censorship here in the United States."

Eventually, released it in 300 smaller theaters and on select Video-On-Demand Platforms (Youtube, Google Play, and Xbox Video) with enhanced security measures

Determining the Culprit

FBI concluded on Dec 19th that North Korea was behind the cyber attack

Stated that they had "evidence" but refused to disclose it. Discussed similarities to the DarkSeoul incident

-Others remained unconvinced:

-Could have been ex-Sony employees or hacker groups that don't like Sony because of its stance on Intellectual Property issues

-Confident attribution is difficult

Sony's New Cyber Security Response

-Created new "white network" that is completely segregated from old compromised network

-Emails will be archived after a few weeks (vs 7 years, before)

-Admins will only have privileges related to their job

-Employees will be unable to install unapproved applications

-Two-factor authentication

-Reduced amount of data will be available on network. Rest will be encrypted and archived and cut off from Internet access

U.S. Response?

According to Article 51 of UN charter: if this incident had been a "use of force" at the level of an "armed attack," then the U.S. would be allowed to respond forcefully, either by cyber or conventional means

-Sony hack is deemed to not have met this threshold

-However, could be considered a "violation of sovereignty," if attribution could be made to North Korea, since infrastructure was in the U.S. If this is true, U.S. would be legally allowed to "hack back"

-However, attribution is difficult to prove

Questions (Political)

How should nations respond when private corporations are targeted by foreign governments? Should there be diplomatic repercussions?

Whose responsibility is it to guard against such attacks? Should there be mandatory governmental regulations on security measures?

How prepared is the government itself for such attacks?

Should the government be compelled to release the evidence it gathered on determining the culprit?

Should journalists have accessed Sony's stolen data?

Questions (Sony)

How might have Sony handled the attack better? Both in terms of preparation and its response?

Was Sony's response to the hacking in terms of security measures adequate?

Was it justified for Sony to censor its content based on potential for a NK cyber retaliation?

Who should be financially responsible and liable for the damages caused to employees?

Stuxnet Cyber Weapon

Stuxnet was a computer worm that infected centrifuges in the Iranian Nuclear Program. First discovered in 2010.

Impact: One of the first demonstrations of a "Cyber Weapon"

Context:

Iran had old designs for a European IR-1 centrifuge from the 1970's that were stolen by Pakistani nuclear physicist A. Q. Khan. These were being used as part of an enrichment effort to develop nuclear weapons.

Stuxnet: Goal

The Stuxnet weapon was not meant to catastrophically destroy the Iranian nuclear program in an overt display of force

-This would only be a temporary setback of less than 2 years

-Iran possessed many replacements

Was meant to be more of a stealth weapon that gradually wore down the centrifuges by changing speeds and pressure

-Goal was to demotivate the Iranian engineers and scientists

Stuxnet: Operation

Stuxnet hijacks the Siemens s7-417 controllers

-industrial controller that manages the valves and pressure sensors of close to 1000 centrifuges

-When the attack is not taking place, the centrifuge functions as normal - legitimate code has access to true data inputs and output

-Implements a man-in-the middle attack: periodically attack is activated

Stuxnet: Operation (Part 2)

-21 seconds of process input signals are recorded and looped during the attack

-The engineers monitoring the system will see these values and think everything is normal. Software monitoring systems will not trigger any alarms since the data values seem normal

-Legitimate code keeps executing but receives fake input values

Stuxnet: Operation (Part 3)

-The attack code causes the pressure in the centrifuges to increase greatly by closing valves. Meanwhile the controllers and other monitoring systems are fed fake data so that no corrections are applied

-Attack continues for some time. Does not go indefinitely, because that would blow cover by damaging too many centrifuges

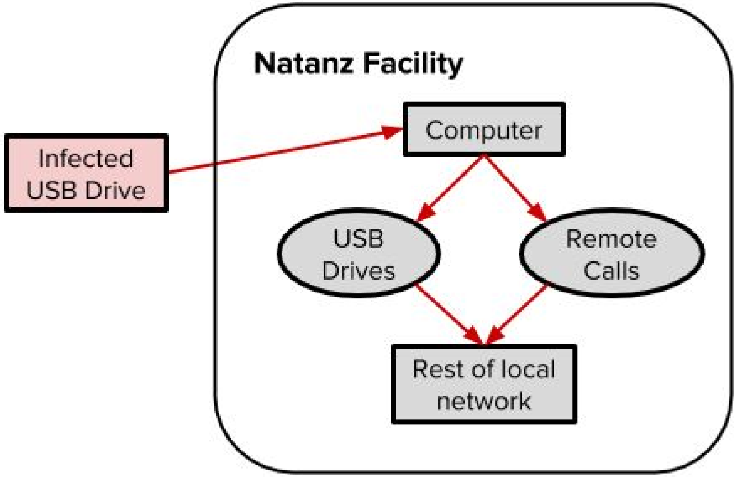
-Intent of this overpressure attack is to cause excess stress, making centrifuge rotors break earlier than they would

Stuxnet: Transmission

-Stuxnet had to be installed physically because the Iranian infrastructure was disconnected from the Internet

-Could be spread via USB sticks or by remote procedure calls to computers on the local network

-Was either first installed accidentally by Iranian scientists or by malicious agents



Source: http://people.carleton.edu/~grossea/spread.html

Stuxnet: A Targeted Weapon

Employs FOUR zero-day exploits in Windows!!

Stuxnet is very specific in its targeting: only causes damage on Windows systems that had the specific Siemens controller (Programmable Logic Controller - PLC) software installed

Can spread greatly, but does NOT really do anything on systems that do not have these specific modules installed

Clearly a finely-targeted weapon

Stuxnet: A Stealth Weapon

-Stuxnet's Overpressure Attack was designed to not be noticeable

-Centrifuges generally worked as normal

-Periodically, attack would be activated, causing stress to the centrifuges and wearing them down. They would break more frequently (but not necessarily during the attack)

-System would appear to be working normally to monitors, but in actuality damage was occurring

-Goal: to slow down the program and demotivate the Iranian engineers

Stuxnet: A Stealth Weapon

-Has code to spread to only three other computers from each machine

-Also deletes itself after 2012

-Clearly there was a focus on not being detected

-People believe that the U.S. and Israel jointly created this weapon, but this has not been confirmed

Stuxnet: Impact

Stuxnet is the first true cyberweapon

Demonstrates that industrial production machinery can be the target of cyber attacks

Terrifying because of how clandestine it is

Attackers clearly spent a lot of effort to engineer it (4 Zero-day exploits, stealth tactics, and targeted implementation)

Stuxnet Questions

What does the creation of Stuxnet entail for the domain of cyber warfare?

How could weapons like Stuxnet (its successors) affect the way that we secure our industrial infrastructure?

Would Iran be justified in considering the Stuxnet virus as an act of war?

Once again, we see that attribution is difficult in issues of cyber conflict. How should nations respond to the deployment of cyber weapons?

Estonia Cyber Attack (2007)

Estonia's entire digital infrastructure was targeted by waves of botnet attacks for 3 weeks

A DDOS Attack hit

-commercial banks

-telephone companies

-media outlets

-name servers

-government communications

https://upw.liuping.win/wikipedia/commons/thumb/a/a2/EU-Estonia.svg/250px-EU-Estonia.svg.png

DDOS: Distributed Denial of Service Attack

Type of attack that works by "flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled"

Distributed Denial of Service attack (DDoS attack): the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

https://en.wikipedia.org/wiki/Denial-of-service_attack

Estonia Cyber Attack (2007)

The Russian government was upset about a Soviet Statue commemorating the end of WWII being removed in Estonia, a former Soviet state

-Russia threatened disastrous consequences for this

-The statue was removed 3 days before the anniversary of the Soviet Victory in WWII

Bronze Soldier of Tallinn
Source: https://www.atlasobscura.com/places/the-bronze-soldier-of-tallinn

Estonia Cyber Attack (2007)

DDOS: Distributed Denial of Service

All of a sudden, Estonian sites started receiving tons of requests from international countries such as Peru, Egypt, and Vietnam

The traffic was so large that it caused the sites to go down

Estonian Internet administrators had to disable all international traffic

As a result, Estonian websites and news outlets got cut off from the outside world

Appears to have been a crudely coordinated attack from non-state actors (with potential state assistance)

Script Kiddies

"relatively unsophisticated troublemakers who copied programs line for line off hacker Web sites"

"primary weapon was the ping attack, a simple request for a response from a Web server, repeated hundreds of times per second. When deployed by masses of attackers, the pings could overwhelm a server."

Recruited off of forums. Many russian nationalists.

https://www.wired.com/2007/08/ff-estonia/

Botnets

Definition (according to Google): "a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g., to send spam messages."

Botnet of computers in the U.S. and other countries used to launch a DDOS attack on Estonian websites

1 million computers were employed in this botnet attack

Estonian Response

At first, the Estonians simply cut off all international traffic.

Then they started trying to determine and block malicious machines by identifying their IP addresses and calling on world ISP to block traffic originating from the machines

This allowed the Estonian authorities to block hundreds of thousands of malicious attacking computers

Interesting Points

The Russian government denies that it was involved in the attack. It is difficult to prove who is responsible, since many computers were hijacked as part of botnets. Yet, this seems to be a very well-funded/resourced attack.

Seem to be many non-state actors (Hacker Networks) coordinating the Estonian cyber attack (through forums).

This represented the first true total "cyber-takedown" of a country's infrastructure. Sets a dangerous precedent/preview of what could be to come

Was clearly just a demonstration of force, rather than a military attack

Compared to the precision of stuxnet, this was crude and brute force.

Questions (Estonia Cyber Attack)

How can countries be better prepared to withstand cyber-assaults on key infrastructure?

How should countries respond to coordinated cyber attacks that involve decentralized individual non-state actors (such as "script kiddies")? Should the governments that these citizens hail from be held accountable?

Would Estonia have been justified in invoking its defensive alliance with NATO? At what point does an attack warrant a NATO response on the basis that an attack on one is an attack on all?

Does this type of cyber attack justify a physical response? Or only a cyber one?

What differentiates cyberwar from cyberterrorism?

Sources: (Sony Hack)

https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/

http://fortune.com/sony-hack-part-1/

http://fortune.com/sony-hack-part-two/

http://fortune.com/sony-hack-final-part/

https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/

CPSC 457: Sensitive Information in a Connected World: Ewa Syta, Spring 2016. Yale University.

Sources (Stuxnet)

https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

https://www.tofinosecurity.com/blog/summing-stuxnet-4-easy-sections-plus-handy-presentation

https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html

http://people.carleton.edu/~grossea/spread.html

Sources (Estonia Cyber Attack)

https://www.wired.com/2007/08/ff-estonia/

https://en.wikipedia.org/wiki/Denial-of-service_attack

http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia

https://www.upi.com/Analysis-Who-cyber-smacked-Estonia/26831181580439/