solarwinds

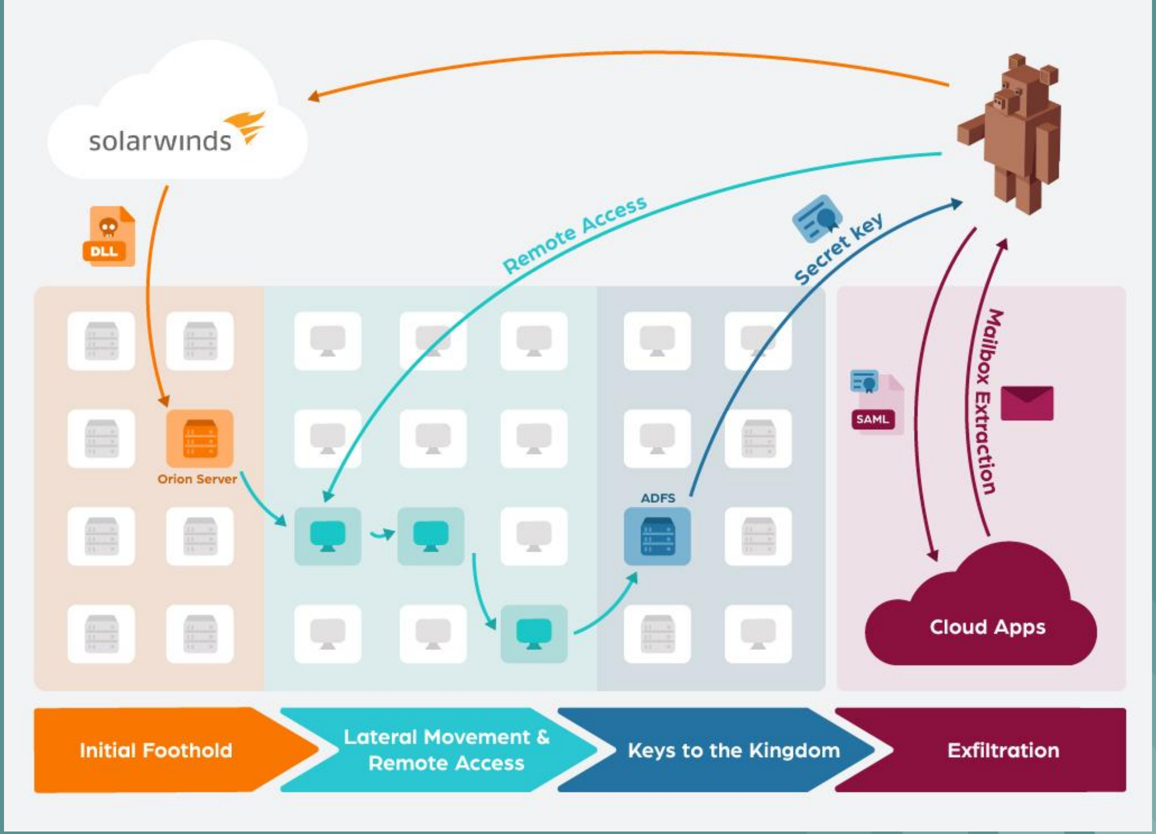
Hack Explained

Group 2
Rohini Shrivastava
Chileen Duncan
Jeffrey Thomson
Seshu Miriyala

The Issue:

- Created a backdoor to access and impersonate users and accounts, access system files
- The attackers, Nobelium, installed the malicious code, “Sunburst”, into a batch of software distributed by SolarWinds as an update
- More than 18,000 SolarWinds customers installed the malicious updates
- First access in September 2019, not publicly discovered or reported until December 2020

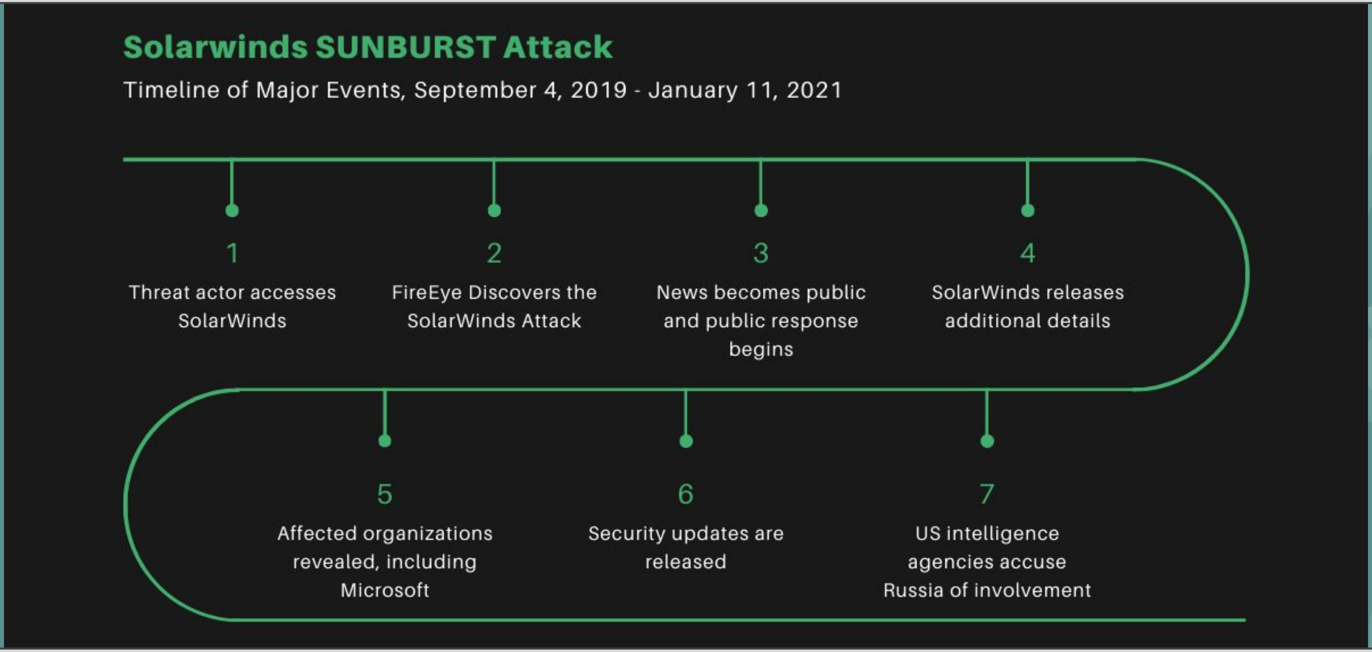
(https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know)



https://zeronetworks.com/blog/examining_solarwinds_supply_chain_attack_summary/

Was this a technical/people/process issue?

- The attackers modified sealed software code, creating a system that used domain names to select targets and mimicked Orion software communication protocols so they could hide in plain sight.
- The attack began with a tiny strip of code. The code fragment was a proof of concept



Solarwinds SUNBURST Attack

Timeline of Major Events, September 4, 2019 - January 11, 2021

1 Threat actor accesses SolarWinds

2 FireEye Discovers the SolarWinds Attack

3 News becomes public and public response begins

4 SolarWinds releases additional details

5 Affected organizations revealed, including Microsoft

6 Security updates are released

7 US intelligence agencies accuse Russia of involvement

https://www.kiuwan.com/solarwinds-hack-timeline/

- They designed an implant that delivered a backdoor that went into the software before it was published.
- They began by implanting code that told them any time someone on the SolarWinds development team was getting ready to build new software

- Created a temporary update file with the malicious code inside while the SolarWinds code was compiling

- They made sure that the switch to the temporary file happened at the last possible second, when the updates went from source code (readable by people) to executable code (which the computer reads) to the software that goes out to customers.

- The hackers also reverse-engineered the way Orion communicated with servers, built their own coding instructions mimicking Orion's syntax and formats

- This backdoor would wait up to two weeks before it went active on the host

- None of the tripwires put in place by private companies or the government seems to have seen the attack coming.”This was a previously unidentified technique." -Christopher Krebs

- DHS' current system, known as Einstein, doesn't scan software updates."What the SVR was able to do was make the transition from wherever they were operating from into the U.S. networks. -Krebs

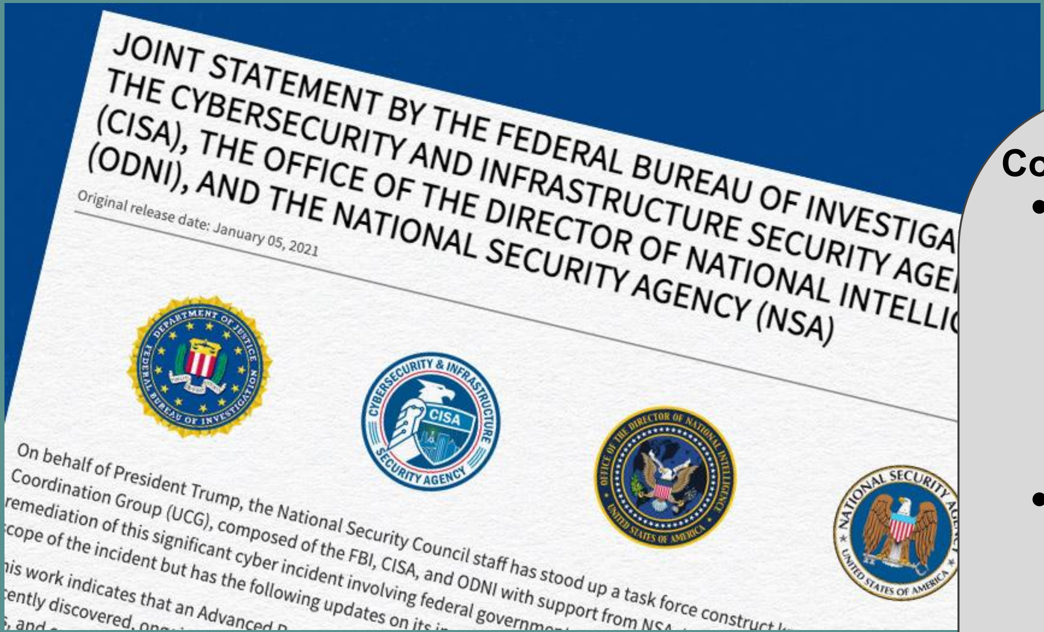
- The hackers rented servers from Amazon and GoDaddy to obtain the domestic footprint

(https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack)

What was the business impact?

- More than 18,000 SolarWinds customers installed the malicious updates
- Through this code, hackers accessed SolarWinds' customer information technology systems, which they could then use to install even more malware to spy on other companies and organizations.
- Figures estimate that the Russians successfully compromised about 100 companies.
- Government departments such as Homeland Security, the Pentagon, State, Commerce and Treasury, with evidence of emails missing from their systems.
- Private companies such as FireEye, Microsoft, Intel, Cisco and Deloitte
- The malware had access to entire networks; many government and enterprise networks and systems face the risk of significant breaches.
- The hack could also be the catalyst for rapid, broad change in the cybersecurity industry.
- The hackers also found their way into the Cybersecurity and Infrastructure Security Agency(CISA)
- "When there's cyber-espionage conducted by nations, FireEye is on the target list," Kevin Mandia, CEO of the cybersecurity firm FireEye, told NPR, but he believes there are other less obvious targets that now might need more protecting. "I think utilities might be on that list. I think health care might be on that list. And you don't necessarily want to be on the list of fair game for the most capable offense to target you."

(https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack)



JOINT STATEMENT BY THE FEDERAL BUREAU OF INVESTIGA
THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGE
(CISA), THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLI
(ODNI), AND THE NATIONAL SECURITY AGENCY (NSA)

Original release date: January 05, 2021

On behalf of President Trump, the National Security Council staff has stood up a task force construct k
Coordination Group (UCG), composed of the FBI, CISA, and ODNI with support from NSA
remediation of this significant cyber incident involving federal governm
cope of the incident but has the following updates on its i
is work indicates that an Advanced P
ently discovered, ong

https://www.bankinfosecurity.com/solarwinds-hit-was-likely-russian-espionage-us-says-a-15709

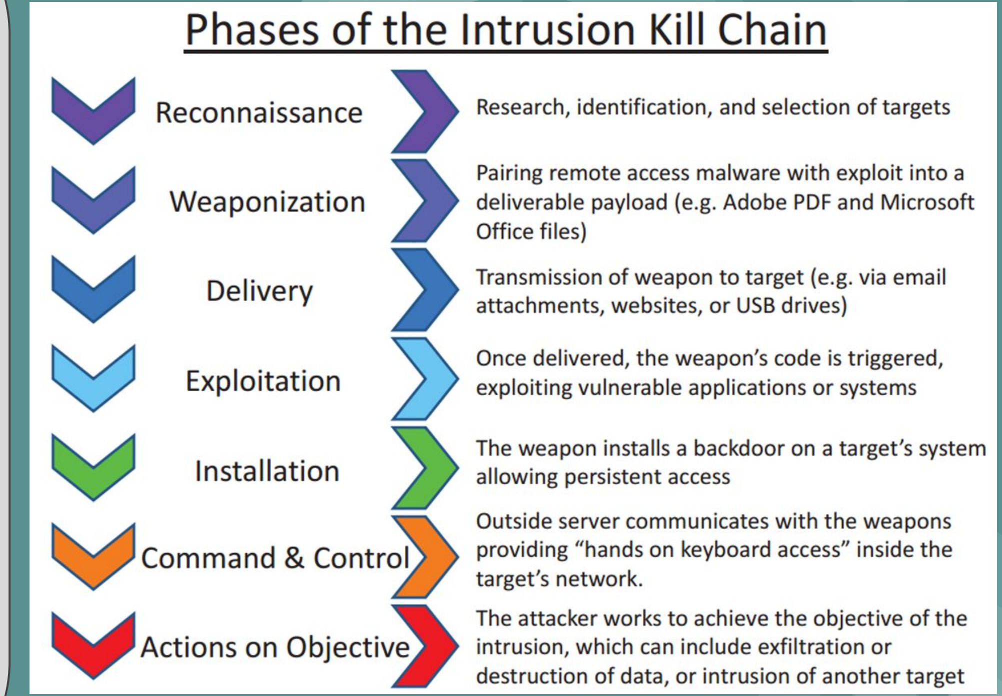
Continued business impact:

- “Since the malicious actor was already launching precision attacks on customers whose information was compromised, this indicates that attacking support agents were likely part of the campaign with a larger mission.” - Om Moolchandani, CISO of Accurics
- Targeting IT companies reflects that attackers want to gain access to their end targets using supply chain mechanisms. Most IT companies provide backbone services to large enterprises, businesses, governments, and industries.
- “As part of the intrusion set, Microsoft witnessed both password spray and brute-force attacks on accounts and customers. We must embrace the idea that identity is the new perimeter. We know that a compromised employee played a role in this most recent incident,” -Ralph Pisani, president of Exabeam

https://www.technewsworld.com/story/solarwinds-hackers-still-targeting-microsoft-focus-on-support-staff-87188.html

Cyber Kill Chain:

- A military concept, modified by Lockheed Martin for cyber security.
- A series of steps that trace stages of a cyberattack from the early reconnaissance stages to the exfiltration of data.
- The model identifies what the hackers must complete in order to achieve their objective.
- It has defined how organisations map out their security controls but also determines how they measure their cyber resilience



Phases of the Intrusion Kill Chain

Reconnaissance

Research, identification, and selection of targets

Weaponization

Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)

Delivery

Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)

Exploitation

Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems

Installation

The weapon installs a backdoor on a target's system allowing persistent access

Command & Control

Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.

Actions on Objective

The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

Cyber Kill Chain:

- Solarwinds is a highly trusted vendor, so most of their clients welcomed any updates with open arms.
- Companies need to adopt a cyber kill chain for supply chain companies in order to mitigate damage.

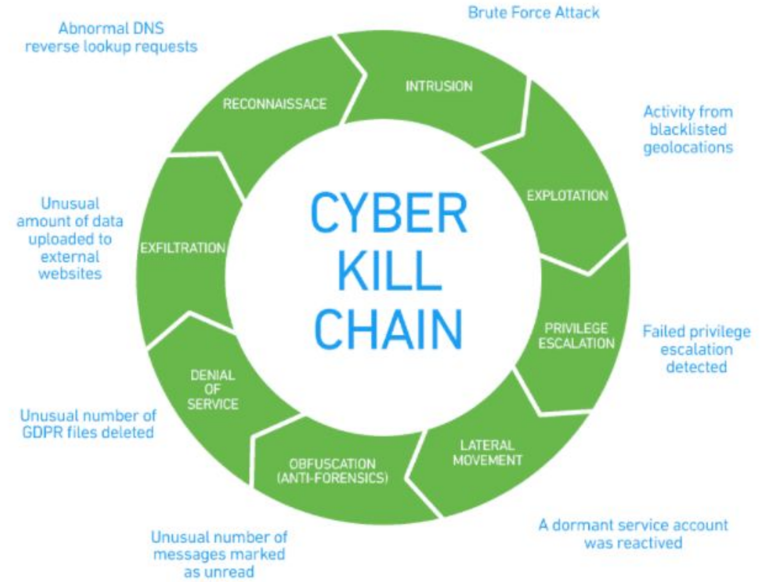

CYBER KILL CHAIN
RECONNAISSACE
INTRUSION
EXPLOTATION
PRIVILEGE ESCALATION
LATERAL MOVEMENT
OBFUSCATION (ANTI-FORENSICS)
DENIAL OF SERVICE
EXFILTRATION
Abnormal DNS reverse lookup requests
Brute Force Attack
Activity from blacklisted geolocations
Failed privilege escalation detected
A dormant service account was reactived
Unusual number of messages marked as unread
Unusual number of GDPR files deleted
Unusual amount of data uploaded to external websites

Figure 1 – Cyber kill chain with examples

Prevention Opportunities:

Zero trust architecture:

- Zero Trust - Eliminating the concept of trust from an organization's network architecture. Zero Trust is not about making a system trusted, but instead about eliminating trust.

- Once the malware was inside the Solarwinds Orion servers, it would send outgoing signals to the attackers server to receive commands.

- Outbound communication is allowed but only known bad destinations are blocked.

- With zero trust, only known and authenticated communication would have been allowed. This would have blocked communication to the attackers servers. Customers that disabled any outbound communication were not compromised in the attack.

Prevention Opportunities:

Limit access rights for suppliers

- Many organizations give full access rights to suppliers because it’s easy.
- This is part of the reason the malware was able to cause such widespread issues, but the update software didn’t need full access rights.
- Had privileges been limited, damages would have been less.

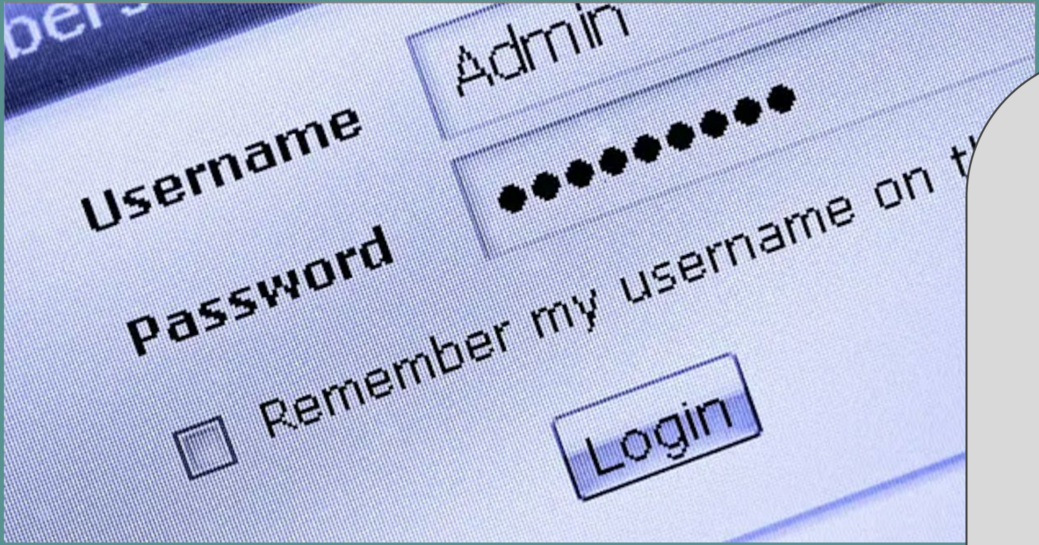
Prevention Opportunities:

Secure Code Signing:

- Once software is developed, it’s moved to an offline environment where a trusted person signs the software or updates using a non-extractable key. The software is then moved back to the release environment.
- Benefits: A trusted person has to sign any software updates.
- Problems: Takes longer for software to be deployed.

Detection Opportunities:

- Attacker Hostnames Match Victim Environment:
  - The attacker set the hostnames on their command infrastructure to match real ones found within the victim's environment.
  - How to detect this: Querying and cross-referencing internet-wide scan data sources for an organization’s hostnames can uncover malicious IP addresses.
- IP Addresses located in Victim’s Country:
  - The attacker primarily used only IP addresses originating from the same country as the victim.
  - How to detect this:Geolocating IP addresses used for remote access may show an impossible rate of travel if a compromised account is being used by the legitimate user and the attacker from disparate IP addresses



https://securityintelligence.com/administrator-credentials-a-security-breach-waiting-to-happen/

Detection Opportunities:

- Lateral Movement Using Different Credentials:
  - Once the attacker gained access, they moved laterally using multiple different credentials. The credentials used for lateral movement were always different from those used for remote access.
  - How to detect this: Organizations can attempt to track all logon activity and review systems displaying a one-to-many relationship between source systems and accounts.

Business impact - internet-wide scanning

- Takes long time to scan about 45 minutes to scan all IPV4 address over internet.

- Service providers defensive mechanisms block these scans.

- Log transfer from client machines and perform scheduled scan. Resembles same attack.

Business impact - Lateral movement using different credentials

- Organizations already use Security Information and Event Management (SIEM) tools to identify security incidents

- These legacy SIEMs alerts based on some correlation rules for each event, but without context.Because of this sometimes analysts are left with no clue on how to tie the things together.

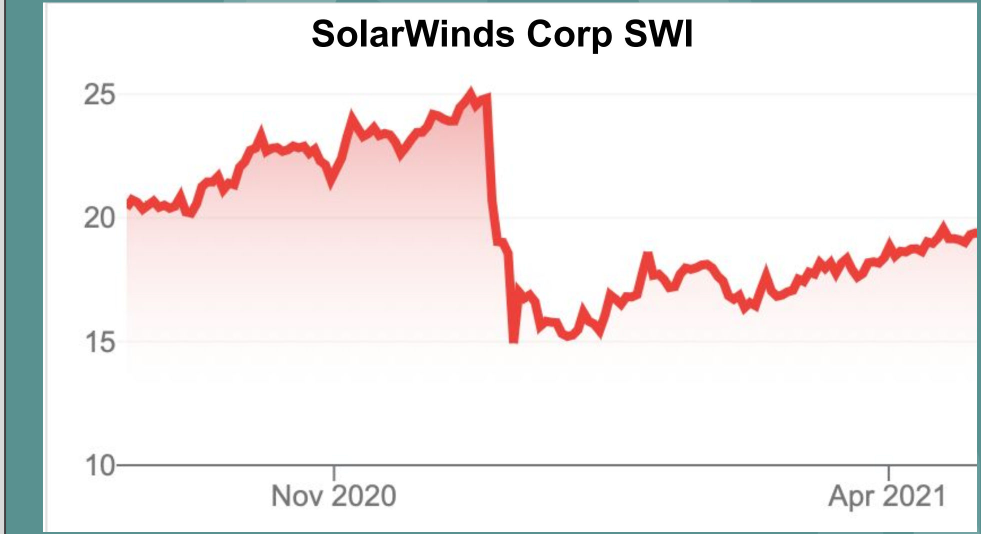
Business impact - Lateral movement using different credentials

- To bridge the gap we need tools with machine learning and AI capabilities.
- FireEye's HX's logon tracker, Exabeam's Advanced Analytics platform
- These tools are costly

Why Should the Business Care?

- At least 18,000 clients were exposed
  - Most Fortune 500 companies used SolarWinds for security
  - Data taken can be used for ransom or even Identity theft

- Around 19 Million Spent in the first Quarter of 2021
  - Class Action Lawsuit
  - Market shares fell 30%



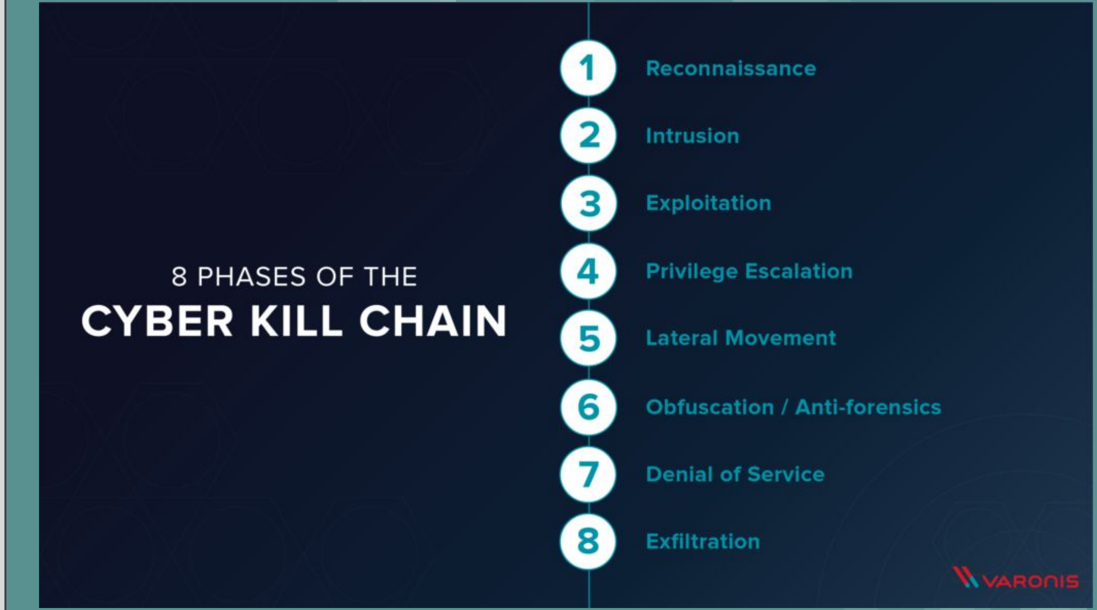
Lessons Learned- Company:

- Every suspicious activity is important and should be reviewed immediately
  - "None of us could pinpoint a supply chain attack at that point," Ramakrishna told NPR. "The ticket got closed as a result of that. If we had the benefit of hindsight, we could have traced it back"
- Decompiling the code after it compiles
  - If not decompiling code, then more guard rails
- Continuous security threats and assessments
- A firewall blocking all outgoing connections to the internet

https://identitymanagementinstitute.org/lessons-learned-from-the-solarwinds-hack/

Lessons Learned- Consumer:

- Add more logging
- Check the active directory to see any anomalies
  - NPR article hack was discovered because two phones were registered under one employee
- Cyber Kill Chain
  - 8 steps
  - Can neutralize most attacks



8 PHASES OF THE
CYBER KILL CHAIN

1. Reconnaissance
2. Intrusion
3. Exploitation
4. Privilege Escalation
5. Lateral Movement
6. Obfuscation / Anti-forensics
7. Denial of Service
8. Exfiltration

Sources:

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

https://www.upguard.com/blog/cyber-kill-chain

https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

https://searchsecurity.techtarget.com/feature/5-cybersecurity-lessons-from-the-SolarWinds-breach

https://www.crn.com/slide-shows/security/12-lessons-learned-from-the-solarwinds-breach-rsa-conference

https://www.illumio.com/blog/zero-trust-cyber-kill-chain