CSCI 405 PRESENTATION: THE 2020 US GOVERNMENT BREACH

PRESENTED BY: JOSHUA INGALLS

OUTLINE

- Key Actors: SolarWinds, FireEye
- How the hack occurred
- Who was affected and what data was stolen
- Who was responsible for the hack
- Response to the hack
- Concluding thoughts

KEY ACTORS: SOLARWINDS CORP.

- An Austin, Texas based that develops technology for the management of network, system, and information technology infrastructure. (solarwinds.com)
- Their software is used by 96% of Fortune 500 companies, won 31 awards in 2022, service 300K+ customers worldwide, and partners with Google, Amazon, Apple, Walmart, McDonalds, etc.
- Software is used by Treasury Department, Army, Navy, Energy Department, Commerce Department, DISA.

KEY ACTORS: FIREEYE

- “FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting.” (https://fireeye.dev/docs/about/fireeye/)
- Provides cybersecurity resources to US Government

HOW THE HACK OCCURRED

- SolarWinds Orion's software allows IT staff to remotely access computers on corporate networks. (Tidy)
- “In a so-called "supply-chain attack", hackers gained access to SolarWinds Orion and then had access to all of its customers' networks.” (Tidy)
- Hackers manipulated Orion’s software updates to include malware which allowed monitoring of customers systems. (Tidy)
- FireEye, who discovered the hack, also had their hacking tools stolen by the hackers and used in attacks over 19 countries. (Tidy)

WHO WAS AFFECTED AND WHAT DATA WAS STOLEN

- Six government agencies: Energy, Commerce, Treasury, State, Homeland Security, and National nuclear Security Administration (Paul and Beckett)
- 18,000 organizations with 50 suffering major breaches.
- Government Email systems were compromised (Paul)
- “Treasury still does not know all of the actions taken by hackers, or precisely what information was stolen,” – Senator Ron Wyden (AP)

WHO WAS RESPONSIBLE FOR THE HACK

- The US Government has narrowed down to Russia as the hackers, specifically a joint operation between SVR and FSB. (Paul and Beckett)
- President Trump suggested that China was responsible for the attack, but this stance was not corroborated by any government agencies. (Paul and Beckett)
- Russia has denied any involvement in the attack.
- Supply-chain attack is the same method used by Russia military leaders in 2016 attack on Ukraine with NotPetya virus. (Paul and Beckett)

RESPONSE TO THE HACK

- SolarWinds urged users to update Orion immediately to remove the malware (Tidy)
- “FireEye has **now released** more than 300 countermeasures to detect the use of its stolen tools and to minimise the potential impact if they are used.” (Tidy)
- President Trump downplayed the severity of the hack and questioned the legitimacy of Russia orchestrating the attack. (Paul and Beckett)
- President-Elect Biden talked about how we need to increase our cyber defense, but he offered no plan on how to move forward. (Paul and Beckett)

CONCLUDING THOUGHTS

- The hack has left the US and Russia at a very tense relationship because of this hack and world events.
- The digital age has proven the importance of dedicated work to keep our cyber tools updated.
- Cyber experts need to be regularly checking for flaws or malware that may have infected the system.

REFERENCES

- Associated Press. (2020, December 22). *US government hack compromised dozens of treasury email accounts, senator says*. The Guardian. https://www.theguardian.com/us-news/2020/dec/21/us-government-hack-treasury-department-email
- BBC. (2020, December 20). *US cyber-attack: Around 50 firms "genuinely impacted" by massive breach*. BBC News. https://www.bbc.com/news/world-us-canada-55386947

REFERENCES

- FireEye. (n.d.). *About Fireeye*. https://fireeye.dev/docs/about/fireeye/
- Paul, K. (2021, January 6). *DOJ confirms email accounts breached by Solarwinds hackers*. The Guardian. https://www.theguardian.com/technology/2021/jan/06/doj-email-systems-solarwinds-hackers
- Paul, K., & Beckett, L. (2020, December 19). *What we know – and still don't – about the worst-ever US government cyber-attack*. The Guardian. https://www.theguardian.com/technology/2020/dec/18/orion-hack-solarwinds-explainer-us-government

REFERENCES

- SolarWinds. (2023, November 14). *Observability and IT management platform: SolarWinds*. IT Management Software and Observability Platform. https://www.solarwinds.com/
- Tidy, J. (2020, December 15). *SolarWinds Orion: More US government agencies hacked*. BBC News. https://www.bbc.co.uk/news/technology-55318815