Name: Tram Nguyen

**Take Home Midterm Exam**

1. (5 pts) An attacker has gained access to one of your organization’s systems. List 3 ways that they can use to move laterally within the organization & maintain that access. Your arguments **MUST** be supported by at least 3 news sources (must be provided in order to get points) from 2020 or later. *200-300 words.*   
   Sample Google query for pulling up news sources with relevant keywords[[1]](#footnote-1).  
   **Answer:**   
   **Rootkit**

- A group of Chinese-language hackers is believed to be involved in activities targeting Southeast Asian users since July 2020. The group's goal is to penetrate and deploy kernel-mode rootkits (kernel-mode) on Windows systems. - Kaspersky – the Russian cybersecurity company named the rootkit Demodex that “used to hide the user-mode malware's artifacts from investigators and security solutions” (Lakshmanan, 2021) and showed an undocumented downloader program called Cheat Engine that bypasses Microsoft's Driver Signature Enforcement mechanism.

**Spyware** (e.g Pegasus spyware)

- The attackers use Pegasus spyware to access the device of the organization. Pegasus spyware includes two vectors that are one-click and zero-click. - For a one-click vector, the attackers will send the single link in the email, text message, or SMS. If users open the link, it will permit to limited access the device. “The link sent by the Pegasus vector opens a malicious website called an Anonymizer, which communicates with the operator's server.” (Shrestha, 2019)

- The zero-click vector is more dangerous than the one-click one. This does not necessitate the user clicking or opening the link. The spyware code via an internet connection installs itself into devices when the phone rings even though users ignore it. You won't know if your phone has been compromised in the new assaults unless WhatsApp informs you via a message on the platform. (Shrestha, 2019)

**Ransomware**

- Ransomware is a type of malware that, after infecting a computer, encrypts or blocks access to data on a disk and then informs the victim of the possibility of recovering them. Of course, it is not free, and it is necessary to transfer funds to the specified account.

- According to the article “UK cyber head says Russia responsible for 'devastating' ransomware attacks,” “ransomware would continue to be attractive while organizations remained vulnerable and were willing to pay.” (Corera, 2021). Indeed, the attackers gain the capacity to go back in time, and they strive to retain it and leave a lasting impression. In the past, you could contact, and they would guide you through the process of reclaiming your data. They do not supply those services to businesses or government agencies. Even if you have already paid, you are unlikely to have your data returned.

1. (5 pts) Write a business-level summary about why the SolarWinds attack was a big deal, about how the attack unfolded, and provide 4-5 recommendations for the top leadership. You MUST refer to some US government materials (DoJ, CISA, GAO, and any other federal or state entity). The audience is your company’s executives, so avoid using technical jargon; put things in business context (i.e. how might this impact the organization?). Here are some resources[[2]](#footnote-2),[[3]](#footnote-3) you can use to base your answer on, but you are not limited to just those two. *300-400 words.***Answer:**

**Audience**

The alert is for the company’s executives

**Purpose**

An Alert is used to make people aware of a recently discovered cyber threat that may affect cyber data assets, as well as to give further detection and mitigation guidance to recipients.

**Overview**

- On December 13, 2020, SolarWinds, the information technology company in the US, became a victim of a hack that extended to its customers and remained unnoticed for months. The attacker used the spyware on the SolarWinds product’s update (Smith, 2021) to access private companies such as FireEye or even the US government.

**The Problem**

- In FireEye’s case, employees were alert something unusual happened when they logged in. Employees have two-factor authentication on their accounts that requires the code popping up on their phones to verify. However, one day, they notice that other people used their names to register the second device. The hackers posed as FireEye workers to take its unique tools, however, there was no indication of how they got in. (Smith, 2021)

**Why It Matters**

- This cyber-attack is extremely sophisticated and is still evolving. Security experts believe that because the attack was done so quietly and went unnoticed for months, some victims might never discover if they were compromised or not. Affected companies can expect a long and tough recovery process after the assault. (Isabella Jibilian. Katie Canales, 2021)

**Recommends**

- SolarWinds Orion, the monitoring software for IT systems, is discovered many vulnerabilities.

***Detection***

- Hence, according to CIS, there are updated recommendations:

* “2019.4 HF5 Update To 2019.4 HF6
* 2020.2 (with no hotfix installed) & 2020.2 HF 1 > Update To 2020.2.1 HF2
* If you are running 2019.2 HF 3, 2018.4 HF 3, or 2018.2 HF 6 and do not wish to update to one of the above versions, apply the security patch released by SolarWinds to address CVE-2020-10148.” (Multiple Vulnerabilities in SolarWinds Orion Could Allow for Arbitrary Code Execution, 2020)

- Users should be cautioned not to visit shady websites or click on links provided by unknown or shady sources. (Multiple Vulnerabilities in SolarWinds Orion Could Allow for Arbitrary Code Execution, 2020)

- Inform and educate individuals on the risks of hypertext links in emails or attachments, particularly those from unverified sources. (Multiple Vulnerabilities in SolarWinds Orion Could Allow for Arbitrary Code Execution, 2020)

***Mitigation***

According to CISA Alert, (Alert (AA20-352A), 2020), SolarWinds Orion specific mitigations:

* Step 1:

Evaluate archived network data for signs of compromise, such as new replacement DNS domains connected to a small number of administrative hosts (e.g., SolarWinds systems).

* Step 2:
* “Businesses affected should immediately unplug any network access (e.g., Ethernet cable or Wi-Fi) from the application running system(s) from SolarWinds.” (Multiple Vulnerabilities in SolarWinds Orion Could Allow for Arbitrary Code Execution, 2020)
* Stop all communications to and from servers outside the organization that have any version of the SolarWinds Orion software running, and all threat actor-controlled accounts should be identified and completely removed.
* Step 3:

After the threatened actor-controlled accounts are removed completely

- Rebuild hosts using trustworthy sources that are monitored by the SolarWinds Orion monitoring software.

- Resetting all corporate credentials (users, SNMP strings, SSH keys, certificates, and so forth).

- Using multi-factor authentication as a requirement

- Extra system and configuration protection is available

1. (5 pts) Using this article[[4]](#footnote-4) and at least another on the same topic (identity & authentication) that should be clearly cited, provide 4-6 recommendations for a small business to improve its cybersecurity posture. The business employs around 100 people but isn’t a tech-focused business (i.e. it doesn’t sell s/w or h/w). You MUST connect your answers with specific news pieces that you logged in your class journal (the Sep 28th file). Max of *200-300 words, not including any quotes of your own journal entries, which should be provided as a screenshot of one of your journal entries showing your journal header.***Answer:**   
   In the article “How weak passwords could put your organization at risk,” there is a lot of users uses the weak password to protect their accounts such as “1234”, “Hello123", or even “solarwinds123” to protect the security server in the SolarWinds attack example. (Whitney, 2021) The password manager NordPass provides the following suggestions to assist businesses and people in developing better password habits:

* Users should use strong passwords that include at least 12 characters, lower, upper case, and a special symbol. However, users should not use the same password for many accounts or many sites and update them on a regular schedule.
* Companies may use a password manager to create specific, high-strength, random passwords for their websites and applications and store them in a private, encrypted file vault accessible from any device. The password manager can keep companies’ information safe from the attacker and employers do not need to reset their passwords every month (Five key tips to better your business’s password security, 2021)
* Multi-factor authentication is very important in security and preventing compromise. For example, in my journal, the article “Stolen Credentials Led to Data Theft at United Nations” showed the consequence of not enabling multi-factor authentication to secure. “The attack highlights why simply using a username/password combination to secure entry into a system” Graphical user interface, text

  Description automatically generated
* Employees should not use their personal information to create the password. Hackers will be more likely to guess your password because of this. The company should request employees create strong and impersonal passwords as a means of enhancing their data security.

Other recommendations for improving the companies’ security:

* In my journal, according to “How APTs become long-term lurkers: Tools and techniques of a targeted attack,” the organizations’ security architectures should focus more on “Detection” (recognizing an attack as soon as it occurs) and “React” (obtain the best effect while minimizing needless losses) systems as the way they do on “Prevent” one

Text

Description automatically generated

A picture containing graphical user interface

Description automatically generated

1. (5 pts) Summarize, in your own words, the key warnings raised in this article[[5]](#footnote-5). How can the state of Minnesota and MSU bring about awareness and positive change of these issues? *200-400 words.***Answer:**   
   **Key Warning Raised:**

- People are increasingly unhappy and distrustful of their governments and society, and there is an increased need for government assistance

- People’s expectations do not meet that might lead to increased polarization, protest groups, and, in the most extreme situations, bloodshed, internal strife, or state breakdown.

- The present epidemic has hastened global transformation and cast doubt on official assumptions.

- Technology will be power. Extremists might grow more deadly by utilizing artificial intelligence and virtual reality.

- Economic systems never recovered after the Covid virus. and living in a worldwide system that is "directionless, chaotic, and unpredictable," as nations, companies, and other organizations disregard international laws and standards.

- In the competition between the US and China, whether one of them succeeds more than the other if they compete evenly, or whether they split the globe into distinct silos.

- In the early 2030s, the globe is in the middle of a worldwide disaster due to climate change, hunger, and instability.

**How can the state of Minnesota and MSU bring about awareness and positive change of these issues?**

- Minnesota State should develop and support capacities to contribute to peace as well as to predict and avoid violent conflict before it occurs.

- MSU students can share their thought by non-violent protest or writing letters to the school’s president or the leader of the state to expand awareness and positive change. Although they cannot be prevented from meeting to debate or oppose concerns by the govt, violent protest is against the law.

- The government or the state of Minnesota should devise a strategy to prevent the use of AI of terrorist organizations

- The governor in MN can promote the state's economy after the Covid pandemic, such as Invest in small companies to help the economy recover, make sure kids catch up on their education so they can achieve in the future, and help vital employees and middle-class families, and keep MN people safe.

- For the threat of climate change, the governor of Minnesota, as well as MSU, urges people to take part in the solution to the climate issue. The governor can set the goals to reduce carbon emissions, promote wind and solar sources.

1. (5 pts) In 2*00-400 words*, summarize what is known so far about how Facebook makes it easier for foreign adversaries to run campaigns of disinformation. What impact are such disinformation activities having on a global scale? Provide at least 2 sources from 2020 or later. Note: the recent news & testimony of a Facebook whistleblower are likely to be very useful to researching and writing about this development. **Answer:**

**How Facebook makes it easier for foreign adversaries to run campaigns of disinformation**

- Foreign countries, including China and Iran, were utilizing the platform to undertake spying activities, according to Frances Haugen, a former Facebook employee. (Reuters, 2021)

- According to Haugen, Facebook has constantly chosen to optimize its growth above implementing protections on its services. (Allyn, 2021)

- The fact that Facebook's counterespionage and counterterrorism teams are consistently understaffed is a national security concern. (Reuters, 2021)

- During the 2016 election, there were two different Russian efforts on Facebook. Russian military spy agencies established fictitious Facebook profiles and disseminated incorrect information, including fake news. After finding a Russian page that was sharing stolen emails, Facebook had no regulations prohibiting foreign organizations from using its platform to influence American sentiment. (Newston, 2021)

- When Facebook learned that DCLeaks - a Russian-operated page was sharing stolen Clinton’s emails and share them with journalists, Facebook chose to keep silent at first. DCLeaks was only removed by Facebook after a security expert discovered that the emails contained personal information. (Newston, 2021)

**What impact are such disinformation activities having on a global scale?**

- Proactive Disinformation efforts can have a real-world influence by effecting customer behavior.

- In 2016, Lisa – a Russian-German girl, claimed that two migrant males abducted and raped her, and that claim was proven to be wrong after that. However, Moscow attempted to exploit internal German political differences to inspire large demonstrations and politically harm the German government by using media and diplomatic resources to push a fake tale at a time when German anti-migrant sentiment was on the rise. (Mankoff, 2020)

- Far-right religious figures in India utilized messaging apps to propagate false information about religious minorities, resulting in communal bloodshed. (India: Government Policies, Actions Target Minorities, 2021)

- Political and religious leaders in Indonesia have condemned the proliferation of hate speech and misinformation on social media, which influenced the Jakarta mayoral race. (Social Media Disinformation, and Democracy in Asia, 2020)

- Ultranationalist Buddhist monks in Burma, for example, have exploited social media to rally followers and incite violence against the Rohingya, a persecuted Muslim minority community. (Wirathu: Myanmar military releases firebrand Buddhist monk, 2021)

1. (5 pts) You work as a security consultant at a company that is an upcoming competitor to Kaseya. Management has recognized your good analysis and writing skills and would like for you to write a summary of the key issues[[6]](#footnote-6) that plagued Kaseya and follow it up with 4-6 detailed recommendations to ensure the same thing doesn't happen to your employer. *300-400 words.* **Answer:**

* The ransomware assault against Kaseya Ltd, a Miami-based software manufacturer, was on July 2021.
* According to the article “Kaseya Failed to Address Security Before Hack, Ex-Employees Say.”, **Kaseya Problems are:**

- On July 2, REvil, a Russian-linked criminal group, claimed credit for one of the most extensive ransomware attacks ever, demanding $70 million in Bitcoin in exchange for a worldwide decryption key. (Kaseya Failed to Address Security Before Hack, Ex-Employees Say, 2021)

- Kaseya failed to fix its software and servers in early 2019, and several breaches of basic cybersecurity standards were found throughout Kaseya's products, making a hacker's work simple according to former workers who were dismissed. REvil utilized the company's VSA software as the vehicle for its assault. (Kaseya Failed to Address Security Before Hack, Ex-Employees Say, 2021)

- Employees quit that job because they were dissatisfied with the fact that new features and goods were emphasized before fixing problems. (Kaseya Failed to Address Security Before Hack, Ex-Employees Say, 2021)

- Marcus Murray, the creator of Truesec Inc., reviewed Kaseya VSA's code and uncovered many exploitable weaknesses in just a few hours. According to him, the code is made up of a variety of scripting languages, and some of it is “outdated and inappropriate for a modern remote information systems platform.” (Kaseya Failed to Address Security Before Hack, Ex-Employees Say, 2021)

* **Recommendations:**

- Implement MFA:

Install and perform multi-factor identity verification (MFA) on all accounts under the company's control and activate and execute MFA for all client services to the greatest degree practicable. (Install and implement multi-factor identity verification (MFA) on all accounts under the company's control, and activate and execute MFA for all client services to the greatest degree practicable., 2021)

- Evaluate your security stack regularly:

What works for the organization today must not stand up to tomorrow's onslaught. We should assess the technologies in our security stack regularly to ensure we are ready to cope with tomorrow's threats.

- Work with our vendors to ensure that our tools are correctly configured:

There is no one-size-fits-all answer for every firm. Work with each vendor we collaborate with to ensure that our tools are properly configured for the business. Even more than that, ensure that our vendors are up to speed on best practices and the most recent security warnings. (Huntress, 2021)

- Reexamine our incident response strategy:

Cyberattacks, like storms, are unavoidable. There is no surefire technique to avoid a cyberattack, and there never will be. Instead, cybersecurity professionals should concentrate their efforts on being prepared for the worst-case scenario. This fact is when an incident response strategy comes into play. Contingency planning cannot only provide us peace of mind about how to respond to worst-case circumstances, but it can also help us respond swiftly and get back on track faster. (Huntress, 2021)

# References

*Alert (AA20-352A)*. (2020, December 17). Retrieved from CISA: https://us-cert.cisa.gov/ncas/alerts/aa20-352a

Allyn, B. (2021, October 5). *Here are 4 key points from the Facebook whistleblower's testimony on Capitol Hill*. Retrieved from NPR: https://www.npr.org/2021/10/05/1043377310/facebook-whistleblower-frances-haugen-congress

Corera, G. (2021, October 11). *UK cyber head says Russia responsible for 'devastating' ransomware attacks*. Retrieved from BBC News: https://www.bbc.com/news/uk-58877433

*Five key tips to better your business’s password security*. (2021, July 1). Retrieved from Information Age: https://www.information-age.com/five-key-tips-to-better-your-businesss-password-security-123495881/

Huntress, T. (2021, July 28). *A Recap of Events and Lessons Learned During the Kaseya VSA Supply Chain Attack*. Retrieved from Huntress: https://www.huntress.com/blog/a-recap-of-events-and-lessons-learned-during-the-kaseya-vsa-supply-chain-attack

*India: Government Policies, Actions Target Minorities*. (2021, February 19). Retrieved from Human Right Watch: https://www.hrw.org/news/2021/02/19/india-government-policies-actions-target-minorities#

*Install and implement multi-factor identity verification (MFA) on all accounts under the company's control, and activate and execute MFA for all client services to the greatest degree practicable.* (2021, July 6). Retrieved from CISA: https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa

Isabella Jibilian. Katie Canales. (2021, April 15). *The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal*. Retrieved from INSIDER: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

*Kaseya Failed to Address Security Before Hack, Ex-Employees Say*. (2021, July 10). Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2021-07-10/kaseya-failed-to-address-security-before-hack-ex-employees-say

Lakshmanan, R. (2021, October 1). *Chinese Hackers Used a New Rootkit to Spy on Targeted Windows 10 Users*. Retrieved from The Hacker News Logo: https://thehackernews.com/2021/10/chinese-hackers-used-new-rootkit-to-spy.html?utm\_source=feedburner&utm\_medium=feed&utm\_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29

Mankoff, J. (2020). *With Friends Like These, Assessing Russian Influence In German.* CSIS.

*Multiple Vulnerabilities in SolarWinds Orion Could Allow for Arbitrary Code Execution*. (2020, December 14). Retrieved from Cisecurity: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-solarwinds-orion-could-allow-for-arbitrary-code-execution\_2020-166/

Newston, C. (2021, July 15). *WHAT A NEW BOOK REVEALS ABOUT FACEBOOK AND RUSSIAN INTERFERENCE*. Retrieved from The Verge: https://www.theverge.com/2021/7/15/22577939/facebook-an-ugly-truth-frankel-kang-stamos-russia-interference

Reuters. (2021, October 5). *Whistle-Blower Warns of Foreign Influence on Facebook*. Retrieved from New York Times: https://www.nytimes.com/video/us/100000008010157/whistle-blower-warns-of-foreign-influence-on-facebook.html

Shrestha, D. B. (2019, November 1). *Pegasus spyware: All you need to know*. Retrieved from DH Deccan Herald: https://www.deccanherald.com/specials/pegasus-spyware-all-you-need-to-know-772667.html

Smith, B. (2021, February 14). *SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy and Commerce Departments*. Retrieved from CBS News: https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/

*Social Media Disinformation, and Democracy in Asia.* (2020, October). Retrieved from https://www.defindia.org/wp-content/uploads/2021/01/Social-Media\_ADRN\_Sepcial-Report-Final-2.pdf

Whitney, L. (2021, March 10). *How weak passwords could put your organization at risk*. Retrieved from Tech Republic: https://www.techrepublic.com/article/how-weak-passwords-could-put-your-organization-at-risk/

*Wirathu: Myanmar military releases firebrand Buddhist monk*. (2021, September 7). Retrieved from BBC News: https://www.bbc.com/news/world-asia-58471535

1. Sample Google query for pulling up news sources with matching keywords <https://www.google.com/search?q=breach+attackers+%22moved+laterally%22&tbs=qdr:y&start=40&sa=N> [↑](#footnote-ref-1)
2. The hack by Russia is huge. Here’s why it matters | MPR News

   <https://www.mprnews.org/episode/2020/12/29/the-hack-by-russia-is-huge-heres-why-it-matters> [↑](#footnote-ref-2)
3. SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy and Commerce Departments - CBS News

   <https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/> [↑](#footnote-ref-3)
4. How weak passwords could put your organization at risk

   <https://www.techrepublic.com/article/how-weak-passwords-could-put-your-organization-at-risk/> [↑](#footnote-ref-4)
5. US spies peer into the future - and it doesn't look good. <https://www.bbc.co.uk/news/world-us-canada-56683852> [↑](#footnote-ref-5)
6. Kaseya Failed to Address Security Before Hack, Ex-Employees Say.

   <https://www.bloomberg.com/news/articles/2021-07-10/kaseya-failed-to-address-security-before-hack-ex-employees-say> [↑](#footnote-ref-6)