SolarWinds Attack

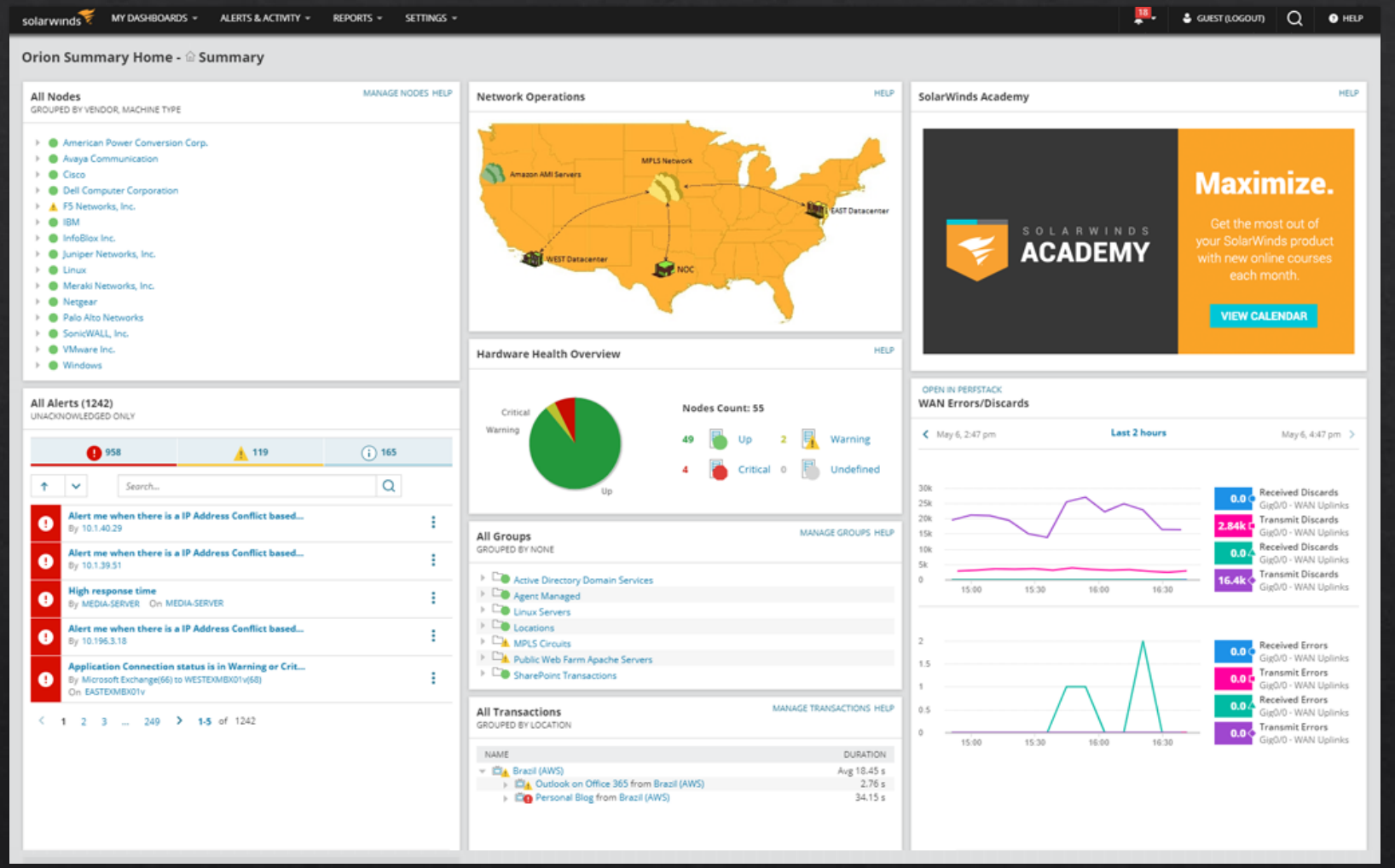
By Thomas Hamilton

Who is SolarWinds

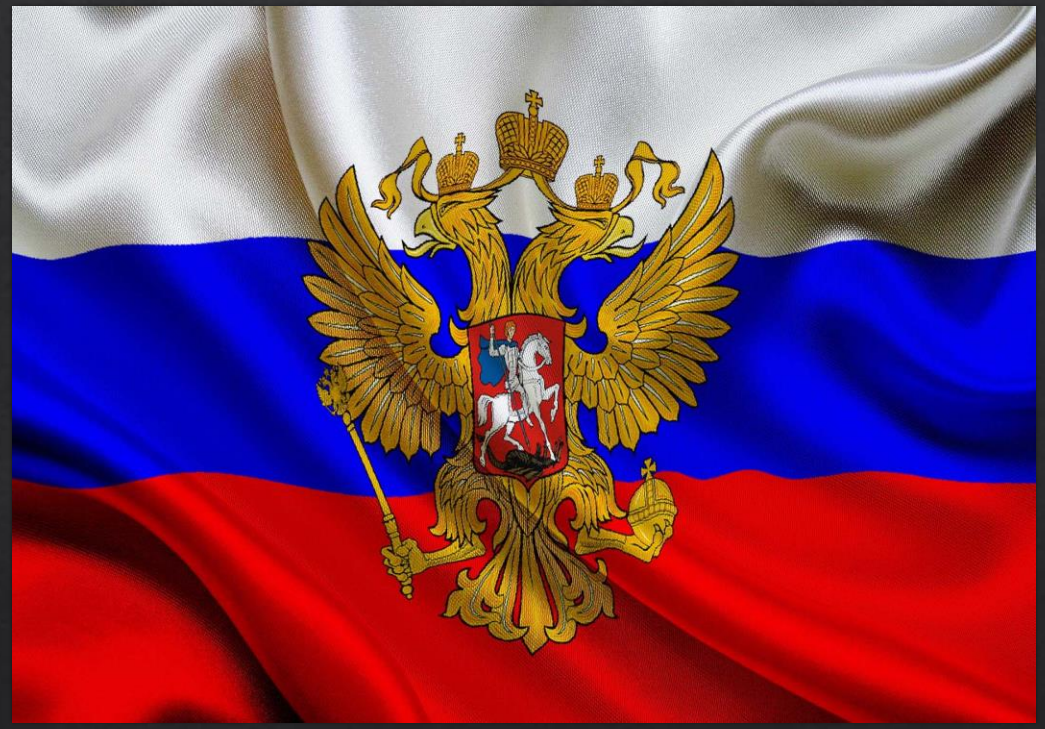
- IT management company out of Austin, Texas
- Provided network monitoring software
- At the time of the attack they did not have a director for cybersecurity nor a director for information security
- Flagship platform was Orion

What is Orion

- Flagship of SolarWinds and was used by many companies
- Orion is a platform for managing resources easily
- “Orion allows chief information officers (CIOs) to automate certain activities such as managing internet protocol (IP) addresses, monitoring devices, and deploying updates” (No Easy Fix, 2020)
- Office 365 Account had been breached previously, but they continued to push updates using it



Who Was Responsible



- The people that are the most likely to have caused this incident were the Russians
- Almost all experts agree that it was the Russian SVR or one of the groups that are working for it
- The most likely responsible is CozyBear, a group that works for the SVR
- Though the president at the time Donald Trump claimed it was the Chinese nation
  - Though he did not have any factual evidence

The Attack

- Supply Chain
- Initial breach was in September 2019
- First malicious code injected was in February 2019
  - This was coined Sunburst
- Discovered by FireEye

How Did They Gain Access and What Did They Do

- The most likely way was through a compromised Office 365 account
- The password to this account was SolarWinds123 set by an intern
- They then pushed code into the update that was then sent out to all networks using the Orion platform
- The affected versions are 2019.4 through 2020.2.1 HF1
- The tools used to get in were labeled SUNSPOT to match the theme of the sun
- The NSA apparently did not know of the attack

Who was Affected

- Those Affected include, Federal Agencies, but are not limited to
  - The NNSA or the National Nuclear Security Administration which monitors all of the nation's nuclear arsenal
  - Department of Agriculture, Department of Defense, Department of Energy, which the NNSA is a part of, Department of Health and Human Services, Department of Homeland Security, Department of Labor, Department of State, Department of Transportation, and the Administrative Office of the United States Courts
- Those affected include, private businesses, but are not limited to
  - Belkin, Cisco, Cox Communications, Equifax, Fidelis, FireEye themselves, Malwarebytes, Microsoft, Mimecast, Nvidia, Palo Alto Networks, Qualys, and Vmware
- "This wave of attacks targeted approximately 3,000 email accounts at more than 150 different organizations. While organizations in the United States received the largest share of attacks, targeted victims span at least 24 countries" (The Fly, 2021)

Damages

- Amount Unknown
- Estimates range from a few billion dollars to hundreds of billions of dollars
- The stock for SolarWinds dropped from $52 before the attack to only $8.38
- Their net income also dropped from $164.8 million to -$929 million

Conclusion

- You should always be ready to kill a software program no matter how needed it is
- Always be scanning with an IDS, Intrusion Detection System, and an IPS, Intrusion Prevention System
- Always stay up to date on all software unless it is known that the update is not as secure as the one running currently
- Always stay up to date on knowledge of what software has a vulnerability that might be discovered or not
- If something has been compromised kill it and go through an extensive check to see what the threat actor gained access to
- Always have password policies in place to help protect against weak passwords

References

- Baker, P. (2021, June 4). *The SolarWinds hack timeline: Who knew what, and when?* CSO Online. https://www.csoonline.com/article/3613571/the-solarwinds-hack-timeline-who-knew-what-and-when.html
- Microsoft warns about cyberattack from actor behind attacks on SolarWinds. (2021). The Fly.
- SolarWinds Attack -- No Easy Fix (IN11559). (2021).