UNC2452

Brought to you by:
Denis & Mark

(Your friendly neighborhood researchers)

Motivations

- Not fully known motives
- Most likely to be espionage

Affiliation

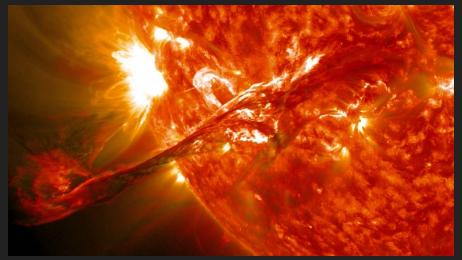
- Suspected to be Russian state-sponsored
- Yttrium, The Dukes, Cozy Bear, Cozy Dukes.(apt 29)
- Solarigate, StellarParticle, Dark hallo

Historical Events

Solar Winds

- Discovered by FireEye in december 13’th 2020
- Still under investigation
- Large Known victims of the breach:
  Multiple branches of the United States Federal Government
  U.S Treasury Department
  The National Telecommunication and information administration (NTIA)
  Part of the U.S Department of Commerce
- Victims outside of the US:
  North Atlantic Treaty Organization (NATO)
  United Kingdom government
  European Parlament

  And the list goes on ....



What happened?

- The attackers used certain exploits in software and credentials , which they discovered in 3 different companies known as: Microsoft ,SolarWinds and VMware.
- the attackers managed to access private and vulnerable information of clients of these said companies using a supply chain attack .

Supply Chain Attack

- Definition:

  “A supply chain attack is a cyber-attack that seeks to damage an organization by targeting less-secure elements in the supply chain. A supply chain attack can occur in any industry, from the financial sector, oil industry or government sector. Cybercriminals typically tamper with the manufacturing process of a product by installing a rootkit or hardware-based spying components.”

  -Wikipedia

Consequences / Damages

- Hard to estimate (Still under investigation).
- 18,000 (+) Companies suffered.
- The world is still recovering from the attack and is estimated to take years to fully recover.

FIN

Thank you for listening!

Sources

- https://attack.mitre.org/groups/G0016/
- https://attack.mitre.org/groups/G0118/
- https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
- https://www.scmp.com/tech/policy/article/3115216/russian-hackers-motive-solarwinds-cyberattack-baffle-us-mere-espionage
- https://www.fireeye.com/current-threats/sunburst-malware.html
- https://www.bitlyft.com/solarwinds-cybersecurity-breach-what-happened-who-it-affects-and-what-to-do-next/
- https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach
- https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach#Microsoft_exploits
- https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html
- https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12