Solar Winds Hack

* Brad Smith, President, Microsoft: Hack put malware into legitimate software of a network management company, when updates were distributed, malware went to 18,000 customers all around the world.
  + Could pick and choose which to go in and disrupt further
  + More than 40 organizations around the world identified by Microsoft, 80% in the US, including number of critical parts of the Federal government
* Undetected for 6 months
  + Extraordinarily sophisticated attack
* Microsoft detected a few instances of the software on its computers, but network is built in such a way that no products or services were compromised
* Cannot afford to allow these kinds of attacks to go undetected in the future
* New approach needed to the sharing of threat intelligence data between government, security, and tech
  + Build on greater threat intel capability with
    - Stronger laws
    - Multilateral action between US and allies

CNN Biden Pressure

* Linked to Russia
* Hit multiple Fed agencies and the private sector
* Russian “hackers put malicious code into a tool published by SolarWinds, a software vendor used by countless government agencies and Fortune 500 businesses”
* Sen Rob Portman, OH, “This SolarWinds massive breach concerns all of us, and frankly, is not that surprising, given what we have been finding, which is that the federal government is not well prepared to deal with these kinds of breaches.”
* Acted to hasten Alejandro Mayorkas’ confirmation as Secretary of the Department of Homeland Security
* Hackers may have spent one month selecting their targets and developing custom code designed to stealthily compromise each victim.
* Used other mechanisms to gain access to network and compromise information, not just SolarWinds
* “qualified as a highly sophisticated foreign intelligence operation and falls short of an act of cyber warfare” – US official
* Gen. Keith Alexander, former direction of the NSA – “Congress must pass legislation to enable the public and private sectors to share threat information more easily, and to **provide legal immunity to companies that share that data.**
* Mayorkas promised that if confirmed, he’s review two CISA cybersecurity programs – Continuous Diagnostics and Mitigation (CDM) and EINSTEIN- to find out if they are sufficient to stop a threat like SolarWinds, and to explore additional defenses if necessary
* CISA suggestions to Biden Admin: funding for CISA to hunt for adversary activity on federal networks; the deployment of new sensors inside federal agencies to detect anomalous activity; and improvements to visibility of the cloud environment, like Office 365.

The Intercept – SolarWinds Hack infected critical infrastructure, including power industry

* Hack involved companies in electric, oil, and manufacturing industries
* SW software also infected three firms that provide services for such companies
* Service companies known as OEMs (original equipment manufacturers)
  + Sometimes have access to critical parts of customer networks
  + Also privileges that let them make changes to those networks, install new software, or control critical operations
  + Allowed hackers to control critical customer processes
* Compromising one OEM could lead to access to thousands of organizations
* SW compromised in March
  + Modified with a backdoor to provide access
  + Linked to Russia
  + Backdoor, dubbed SUNBURST by cybersec company FireEye
    - Gathers info about infected network
    - Waits approx. two weeks to send beacon to a server owned by hackers
      * Includes info about network
      * Signaled the infected system is open for them to enter
    - Use this info to determine who they wanted to “burrow into” further
    - Once inside, could download tools and steal credentials to gain access to more critical parts of the network
* Kevin Mandia, FireEye CEO: attackers only entered 50 of the thousands infected
  + Not just on IT networks, but sometimes on industrial control system networks
  + Critical infrastructure entities usually don’t log or monitor their control networks
    - May not be possible to know if hackers accessed 15 electric, oil, gas, and manufacturing entities infected with software
* Investigators in the security community have seen nothing to attribute the hack to any particular group or nation, but US government says it’s Russia, Russia denies
* Hacked agencies:
  + Homeland Security, Commerce, Treasury
    - Hackers were able to read and steal emails of some top off’s at Treasury Department
  + Two laboratories
  + Federal Energy Regulatory Commission
  + National Nuclear Safety Agency
* Tech Hacks:
  + Microsoft
  + Cisco
  + Intel