LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Beyond Orion: Other Vectors in the SolarWinds Hack

01/07/2021

Report #: 202101071030

Agenda

- BLUF: The hack goes beyond Orion
- SolarWinds Orion
- The SolarWinds Hack
- What is VMWare?
- December 7th National Security Agency (NSA) Alert
- December 17th NSA Advisory
- KrebsonSecurity and VMWare's Response
- Multi-Factor Authentication (MFA) Compromise
- Danger to the HPH Sector
- Mitigations
- References

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Bottom Line Upfront

- The SolarWinds hack involved more than just Orion, and will affect more than just Orion users and customers
- Since the original reporting on the SolarWinds Orion hack, further details have emerged tying other software and vulnerabilities to this breach
- VMWare, Duo, other multi-factor authenticators (MFA)

"I think that number [of compromised vendors] is going to grow. I think we're going to find, as we untangle the knot behind this, that SolarWinds was not the only victim, and that FireEye was not the only victim in its space." - Greg Touhill, former US federal CISO

Source: Shutterstock

SolarWinds and Orion

- Some time in Spring 2020, threat actors compromised the Texas-based software company SolarWinds
  - SolarWinds' products allow organizations to manage their networks, systems, and IT resources
  - One SolarWinds product, Orion, is an IT monitoring and management platform
  - These tools provide extremely deep administrative access to a network's core functions
  - Orion was used by approximately 33,000 organizations across the public and private sector
- In November 2019, a security researcher reported to SolarWinds that their File Transfer Protocol (FTP) server was accessible using the password "solarwinds123"
  - Because of this, "any hacker could upload malicious files"
  - These files would then be distributed due to the FTP server's trusted certificate
- Separately, "internal emails shared with *The New York Times* showed that employees' passwords were leaking out on GitHub last year"

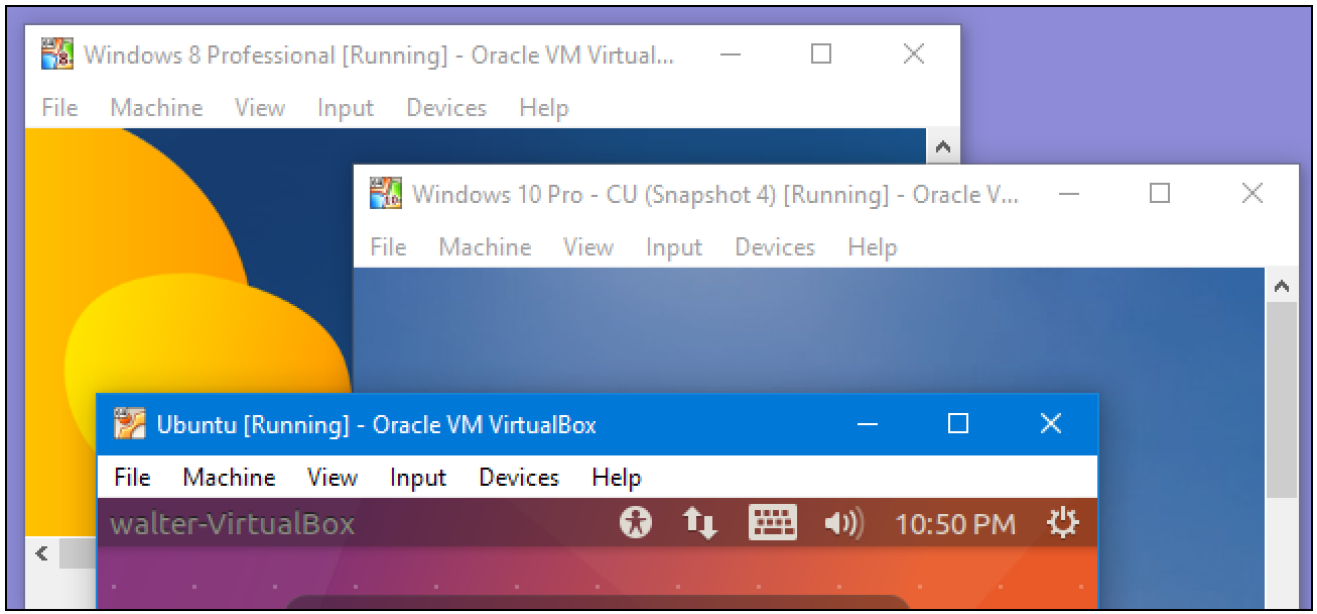
Source: Csaba Gyulai

The SolarWinds Hack

- On December 13th, *The Washington Post* reported that multiple government agencies and Fortune500 companies were breached due to a vulnerability in SolarWinds' Orion
  - Affected approximately 18,000 customers using versions 2019.4 through 2020.2.1
  - Hackers acquired superuser status and access to Security Assertion Markup Language (SAML) token-signing certificates
  - The SAML certificate could then be used to forge new tokens to allow hackers trusted and highly privileged access to networks
  - Hackers used this access to distribute malware
  - According to *The Washington Post*, "any time a customer checked in to request an update, the [actors] could hitch a ride on the weaponized update to get into a victim's system"
- The Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 21-01 in response to the hack
- Some reporting has tied this hack to APT29, also known as "Cozy Bear"
  - This group is tied to the Russian Foreign Intelligence Service (SVR)
  - Previously targeted the State Department and the White House email servers during the Obama administration
  - Russia denies the allegations
- Former Attorney General William Barr tied the hack to Russia in a statement on December 21st
- The list of affected organizations and software goes beyond SolarWinds and Orion
  - VMWare and Duo

What is VMWare?

- Publicly traded software company based in California
- Provides virtualization software
  - Allows users to divide a single computer into multiple virtual computers, commonly called “virtual machines”
  - These computers can run different operating systems and operate independently from each other
  - One piece of hardware can support multiple machines



Source: HowToGeek

December 7th NSA Alert

- On December 7th, the NSA released an alert titled “Russian State-Sponsored Actors Exploiting Vulnerability in VMware® Workspace ONE Access Using Compromised Credentials”
- In a related infographic, the NSA stated that nation state-level exploitation of the VMWare vulnerability had been observed in the wild
- Successful exploitation gave the actors access to protected data through the generation of SAML authentication tokens
- Threat actors must gain access to the victim account using valid credentials (no default credentials exist) and have access to the VMWare management interface
  - Using a strong and unique password lowers the risk of exploitation
  - The risk is lowered further if the web-based management interface is not accessible from Internet
- The vulnerability affects the following products:
  - VMware Access® 20.01 and 20.10 on Linux®
  - VMware vIDM® 3.3.1, 3.3.2, and 3.3.3 on Linux
  - VMware vIDM Connector 3.3.1, 3.3.2, 3.3.3, 19.03
  - VMware Cloud Foundation® 4.x
  - VMware vRealize Suite Lifecycle Manager® 8.x
- VMware released a patch for the Command Injection Vulnerability captured in CVE-2020-4006 on December 3rd

December 17th NSA Cybersecurity Advisory

- On December 17th, the NSA released an advisory titled “Detecting Abuse of Authentication Mechanisms”
- Once a threat actor gains access to a victim’s on-premises network (using any number of methods), they can leverage their “privileged access in the on-premises environment to subvert the mechanisms that the organization uses to grant access to cloud and on-premises resources and/or to compromise administrator credentials with the ability to manage cloud resources”
- The alert outlines two sets of tactics, techniques, and procedures (TTP) actors were observed using to gain access to cloud resources:
  - In the first method, actors steal the credential or private key that is used to sign SAML tokens and then forge trusted authentication tokens to access cloud resources
    - The VMWare vulnerability on the previous slide can be used to accomplish this
  - In the second, the actors leverage a compromised global administrator account to assign credentials to cloud application service principals, and then use the application’s credentials for automated access to cloud resources
    - This could be accomplished by spear phishing a global admin account
- **Neither of these methods constitute a vulnerability**
  - Trust is an integral part of security procedures
  - Corrupted trust corrupts security procedures

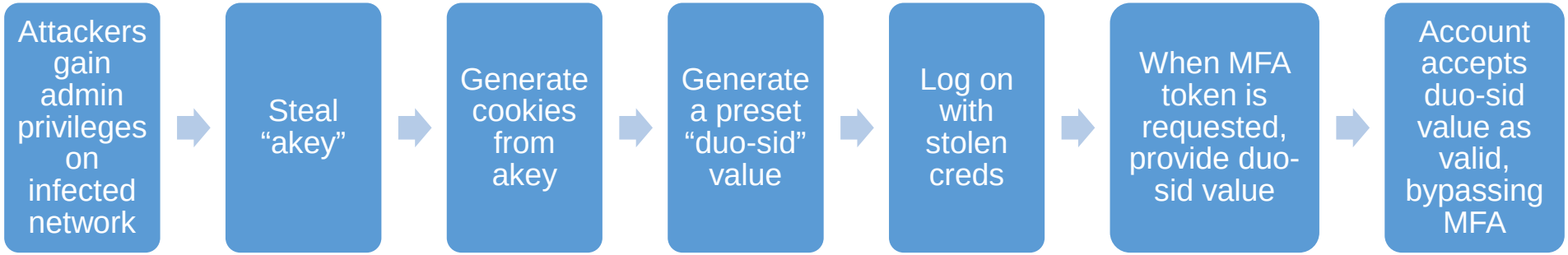
Source: FrostBrownTodd.com

KrebsonSecurity and VMWare's Response

- On December 18th, Brian Krebs at KrebsOnSecurity published an article tying CVE-2020-4006 to the SolarWinds supply chain compromise
- In his analysis, Krebs notes:
  - To exploit this particular VMWare vulnerability, hackers would already need to have access to a vulnerable VMware device's management interface
  - Unless the vulnerable interface was accessible from the internet, they would need to be on the target's internal network
  - This access could have been provided by the SolarWinds compromise
- The same day, VMWare issued a statement claiming to be unaware of any connection between CVE-2020-4006 and SolarWinds
- VMWare also claims that while they have identified "limited instances of the vulnerable SolarWinds Orion software in [their] own internal environment, [their] own internal investigation has not revealed any indication of exploitation."
- Regardless, these incidents are connected by a common thread of corrupted trust in security procedures

MFA Compromise

- Multi-factor Authentication (MFA) is an authentication method that requires users to provide two or more verification factors to gain access to an account or resource
  - Common MFA methods include One Time Passwords (OTPs) delivered to phones, other accounts, or physical devices
- Security researchers at Volexity identified a new technique used to bypass MFA in the SolarWinds hack



- An Ars Technica article noted: "MFA threat modeling generally doesn't include a complete system compromise of a [Microsoft Outlook Web App] server. The level of access the hacker achieved was enough to neuter just about any defense."
- This technique is not specific to Duo MFA, and could be effective against any MFA method

Danger to the HPH Sector

- Multiple federal agencies potentially affected
- Even HPH organizations that did not use SolarWinds may use vendors who did
  - o According to reporting by DataCenterKnowledge, these vendors could include Microsoft, Intel, Cisco, Nvidia, VMware, Belkin, and FireEye
  - o Organizations that did not use SolarWinds or Orion cannot assume they will be completely unaffected
- Effects of the hack will be wide-reaching and take time to discover

Source: FoodSafetyNews

Mitigations and Best Practices – SolarWinds Orion

CISA released Alert (AA20-352A) on December 17 and updated it on December 23. This alert recommends potentially affected organizations follow three steps:

- Step 1:
  - Forensically image system memory and/or host operating systems hosting all instances of affected versions of SolarWinds Orion.
  - Analyze for new user or service accounts, privileged or otherwise. Analyze stored network traffic for indications of compromise, including new external DNS domains to which a small number of agency hosts (e.g., SolarWinds systems) have had connections.
- Step 2:
  - Affected organizations should immediately disconnect or power down affected all instances of affected versions of SolarWinds Orion from their network.
  - Additionally: Block all traffic to and from hosts, external to the enterprise, where any version of SolarWinds Orion software has been installed. Identify and remove all threat actor-controlled accounts and identified persistence mechanisms.
- Step 3: Only after all known threat actor-controlled accounts and persistence mechanisms have been removed:
  - Treat all hosts monitored by the SolarWinds Orion monitoring software as compromised by threat actors and assume that the threat actor has deployed further persistence mechanisms.
  - Rebuild hosts monitored by the SolarWinds Orion monitoring software using trusted sources.
  - Reset all credentials used by or stored in SolarWinds software. Such credentials should be considered compromised.
  - Take actions to remediate kerberoasting, including—as necessary or appropriate—engaging with a third party with experience eradicating APTs from enterprise networks. Require use of multi-factor authentication. If not possible, use long and complex passwords (greater than 25 characters) for service principal accounts, and implement a good rotation policy for these passwords.
- **For a full list of mitigations, see CISA Alert (AA20-352A)**
- **Await updated guidance as research into this incident continues**

VMWare:

- The NSA recommends updating affected systems to the latest version as soon as possible according to VMware's instructions, available at their website, as well as reviewing and hardening configurations and monitoring of federated authentication providers
- Patching may not be sufficient if an organization is compromised and full mitigation may require a rebuild

MFA:

- Because this compromise did not involve exploiting a vulnerability, there is no mitigation available at this time
- However, officials at DUO state: "In order to reduce the likelihood of such an event, it is critical to protect integration secrets from exposure within an organization and to rotate secrets if compromise is suspected"

Reference Materials

References

- Cybersecurity and Infrastructure Security Agency. “CISA Emergency Directive 21-01” December 13, 2020. https://cyber.dhs.gov/ed/21-01/
- Nakashima, Ellen and Craig Timburg. “Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce,” The Washington Post. December 14, 2020. https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html
- Krebs, Brian. “VMware Flaw a Vector in SolarWinds Breach?,” KrebsOnSecurity. December 18, 2020. https://krebsonsecurity.com/2020/12/vmware-flaw-a-vector-in-solarwinds-breach/
- Grimes, Roger, “Solarwinds MFA Bypass Attack Pushes Limits.” KnowBe4. December 16, 2020. https://blog.knowbe4.com/solarwinds-mfa-bypass-attack-pushes-limits
- Goodin, Dan. “SolarWinds hackers have a clever way to bypass multi-factor authentication.” Ars Technica. December 14, 2020. https://arstechnica.com/information-technology/2020/12/solarwinds-hackers-have-a-clever-way-to-bypass-multi-factor-authentication/
- Hardcastle, Jessica Lyons. “VMware Denies Its Software Used in SolarWinds Hack.” SDXCentral. December 21, 2020. https://www.sdxcentral.com/articles/news/vmware-denies-its-software-used-in-solarwinds-hack/2020/12/
- “VMware Issues Statement on SolarWinds Supply Chain Compromise and CVE 2020-4006.” VMWare. December 18, 2020. https://www.vmware.com/company/news/updates/2020/vmware-statement-solarwinds-supply-chain-compromise.html
- Sanger, David E., Nicole Perlroth, and Julian E. Barnes. “Billions Spent on U.S. Defenses Failed to Detect Giant Russian Hack” New York Times. December 18, 2020. https://www.nytimes.com/2020/12/16/us/politics/russia-hack-putin-trump-biden.html

References (Continued)

- “Russian State-Sponsored Actors Exploiting Vulnerability in VMware® Workspace ONE Access Using Compromised Credentials” National Security Agency. December 7, 2020. https://media.defense.gov/2020/Dec/07/2002547071/-1/-1/0/CSA_VMWARE%20ACCESS_U_OO_195076_20.PDF
- “HW-128524: CVE-2020-4006 for Workspace ONE Access, Identity Manager and Connector (81754)” VMWare. December 12, 2020. https://kb.vmware.com/s/article/81754
- Gatlan, Sergiu. “VMware latest to confirm breach in SolarWinds hacking campaign.” Bleeping Computer. December 21, 2020. https://www.bleepingcomputer.com/news/security/vmware-latest-to-confirm-breach-in-solarwinds-hacking-campaign/

Questions

Upcoming Briefs

- HPH Distributed Attack Vectors - How supply chain attacks and managed service provider compromises impact healthcare (01/14)
- Basic Cyber Hygiene for the HPH (01/21)

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

HC3 Customer Feedback

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.
Visit us at: www.HHS.Gov/HC3

Contact

www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV