Macintosh HD:Users:fukayli:Documents:Ltd - Dragon Advance Tech:admin:name cards:DAT-ID-Pack:Logo Files:DAT-Logo-Name-CMYK.ai

Weekly Intelligence Summary

Dec 18, 2020 (TLP: WHITE)

In the spotlight this week:

* According to sources, among those was a flaw in software virtualization platform VMware, which the U.S. National Security Agency (NSA) warned on Dec. 7 was being used by Russian hackers to impersonate authorized users on victim networks. On Dec. 7, 2020, the NSA said, “Russian state-sponsored malicious cyber actors are exploiting a vulnerability in VMware Access and VMware Identity Manager products, allowing the actors access to protected data and abusing federated authentication.”
* Microsoft was hacked as part of the suspected Russian campaign that has hit multiple U.S. government agencies by taking advantage of the widespread use of software from SolarWinds Corp, according to people familiar with the matter.
* ESET researchers uncovered this new supply-chain attack in early December 2020 and notified the compromised organization and the VNCERT.
* FireEye has uncovered a widespread campaign, that we are tracking as UNC2452. The actors behind this campaign gained access to numerous public and private organizations around the world. They gained access to victims via trojanized updates to SolarWind’s Orion IT monitoring and management software.
* In November, Intezer uncovered COVID-19 phishing lures that were used to deliver the Go version of Zebrocy. Zebrocy is mainly used against governments and commercial organizations engaged in foreign affairs.
* Volexity worked three separate incidents involving Dark Halo. In the initial incident, Volexity found multiple tools, backdoors, and malware implants that had allowed the attacker to remain undetected for several years. After being extricated from the network, Dark Halo then returned a second time, exploiting a vulnerability in the organization’s Microsoft Exchange Control Panel.

(cisp-id:9757) Dec 18, 2020

VMware Flaw a Vector in SolarWinds Breach?

U.S. government cybersecurity agencies warned this week that the attackers behind the widespread hacking spree stemming from the compromise at network software firm SolarWinds used weaknesses in other, non-SolarWinds products to attack high-value targets. According to sources, among those was a flaw in software virtualization platform VMware, which the U.S. National Security Agency (NSA) warned on Dec. 7 was being used by Russian hackers to impersonate authorized users on victim networks. On Dec. 7, 2020, the NSA said, “Russian state-sponsored malicious cyber actors are exploiting a vulnerability in VMware Access and VMware Identity Manager products, allowing the actors access to protected data and abusing federated authentication.” In response to questions from KrebsOnSecurity, VMware said it has “received no notification or indication that the CVE 2020-4006 was used in conjunction with the SolarWinds supply chain compromise.”

<https://krebsonsecurity.com/2020/12/vmware-flaw-a-vector-in-solarwinds-breach/>

(cisp-id:9756) Dec 18, 2020

Exclusive: Microsoft breached in suspected Russian hack using SolarWinds -sources.

Microsoft was hacked as part of the suspected Russian campaign that has hit multiple U.S. government agencies by taking advantage of the widespread use of software from SolarWinds Corp, according to people familiar with the matter. It was not immediately clear how many Microsoft users were affected by the tainted products. The Department of Homeland Security, which said earlier Thursday that the hackers used multiple methods of entry, is continuing to investigate. Reuter said. Later Microsoft said: “Like other SolarWinds customers, we have been actively looking for indicators of this actor and can confirm that we detected malicious SolarWinds binaries in our environment, which we isolated and removed. We have not found evidence of access to production services or customer data. Our investigations, which are ongoing, have found absolutely no indications that our systems were used to attack others.”

<https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/>

(cisp-id:9736) Dec 17, 2020

Supply chain attack against a certification authority in Southeast Asia.

ESET researchers uncovered this new supply-chain attack in early December 2020 and notified the compromised organization and the VNCERT. We believe that the website has not been delivering compromised software installers as of the end of August 2020 and ESET telemetry data does not indicate the compromised installers being distributed anywhere else. The Vietnam Government Certification Authority confirmed that they were aware of the attack before our notification and that they notified the users who downloaded the trojanized software.

<https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/>

(cisp-id:9736) Dec 17, 2020

Credential Stealer Targets US, Canadian Bank Customers.

In mid-December, we discovered a campaign that distributed a credential stealer. We also learned that the main code components of this campaign is written in AHK. By tracking the campaign components, we found out that its activity has been occurring since early 2020. The malware infection consists of multiple stages that start with a malicious Excel file. In turn, this file contains an AHK script compiler executable, a malicious AHK script file, and a Visual Basic for Applications (VBA) AutoOpen macro. The full attack chain is depicted in Figure 1. Our telemetry tracked the malware’s command-and-control (C&C) servers and determined that these come from the US, the Netherlands, and Sweden. We also learned that the malware has been targeting financial institutions in the US and Canada.

<https://www.trendmicro.com/en_us/research/20/l/stealth-credential-stealer-targets-us-canadian-bank-customers.html>

(cisp-id:9743) Dec 14, 2020

SEC filings: SolarWinds says 18,000 customers were impacted by recent hack

In SEC documents filed today, SolarWinds said it notified 33,000 customers of its recent hack, but that only 18,000 used a trojanized version of its Orion platform. SolarWinds disclosed on Sunday that a nation-state hacker group breached its network and inserted malware in updates for Orion, a software application for IT inventory management and monitoring. Orion app versions 2019.4 through 2020.2.1, released between March 2020 and June 2020, were tainted with malware, SolarWinds said in a security advisory. The trojanized Orion update allowed attackers to deploy additional and highly stealthy malware on the networks of SolarWinds customers.

<https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/>

(cisp-id:9696) Dec 14, 2020

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor.

FireEye has uncovered a widespread campaign, that we are tracking as UNC2452. The actors behind this campaign gained access to numerous public and private organizations around the world. They gained access to victims via trojanized updates to SolarWind’s Orion IT monitoring and management software. This campaign may have begun as early as Spring 2020 and is currently ongoing. Post compromise activity following this supply chain compromise has included lateral movement and data theft. The campaign is the work of a highly skilled actor and the operation was conducted with significant operational security.

<https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>

(cisp-id:9710) Dec 14, 2020

Dark Halo Leverages SolarWinds Compromise to Breach Organizations.

At one particular think tank, Volexity worked three separate incidents involving Dark Halo. In the initial incident, Volexity found multiple tools, backdoors, and malware implants that had allowed the attacker to remain undetected for several years. After being extricated from the network, Dark Halo then returned a second time, exploiting a vulnerability in the organization’s Microsoft Exchange Control Panel. Near the end of this incident, Volexity observed the threat actor using a novel technique to bypass Duo multi-factor authentication (MFA) to access the mailbox of a user via the organization’s Outlook Web App (OWA) service. Finally, in a third incident, Dark Halo breached the organization by way of its SolarWinds Orion software in June and July 2020. Volexity also confirm that the attacker had presented cookie tied to a Duo MFA session named duo-sid.

<https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/>

(cisp-id:9744) Dec 13, 2020

Customer Guidance on Recent Nation-State Cyber Attacks.

An intrusion through malicious code in the SolarWinds Orion product. This results in the attacker gaining a foothold in the network, which the attacker can use to gain elevated credentials. Microsoft Defender now has detections for these files. Also, see SolarWinds Security Advisory.

Once in the network, the intruder then uses the administrative permissions acquired through the on-premises compromise to gain access to the organization’s global administrator account and/or trusted SAML token signing certificate. This enables the actor to forge SAML tokens that impersonate any of the organization’s existing users and accounts, including highly privileged accounts.

Anomalous logins using the SAML tokens created by the compromised token signing certificate can then be made against any on-premises resources (regardless of identity system or vendor) as well as to any cloud environment (regardless of vendor) because they have been configured to trust the certificate. Because the SAML tokens are signed with their own trusted certificate, the anomalies might be missed by the organization.

Using the global administrator account and/or the trusted certificate to impersonate highly privileged accounts, the actor may add their own credentials to existing applications or service principals, enabling them to call APIs with the permission assigned to that application.

Due to the critical nature of this activity, Microsoft is sharing the following information to help detect, protect, and respond to this threat.

<https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/>

(cisp-id:9709) Dec 09, 2020

Russian APT28 Uses COVID-19 Lures to Deliver Zebrocy.

In November, Intezer uncovered COVID-19 phishing lures that were used to deliver the Go version of Zebrocy. Zebrocy is mainly used against governments and commercial organizations engaged in foreign affairs. The lures consisted of documents about Sinopharm International Corporation--a pharmaceutical company that COVID-19 vaccine is currently going through phase three clinical trials--and an impersonated evacuation letter from Directorate General of Civil Aviation. The lure was delivered as part of a Virtual Hard Drive (VHD) file that requires victims to use Windows 10 to access the files.

<https://www.intezer.com/blog/research/russian-apt-uses-covid-19-lures-to-deliver-zebrocy/>

***Graphical user interface, application

Description automatically generatedOur Threat Intelligence Platform (***[***http://dashboard.cisp.org.hk/***](http://dashboard.cisp.org.hk/)***) is ready for public access.***

***Get access? please send an email to:*** [***admin@dragonadvancetech.com***](mailto:admin@dragonadvancetech.com)