F-SECURE THREAT HIGHLIGHTS REPORT

JUNE 2021
EXECUTIVE SUMMARY

CONTENTS

MONTHLY HIGHLIGHTS
- Siloscape: A cloud native attack targeting windows containers
- GESEMIUM: Operation NightScout supply chain attack
- ATM Jackpotting: Exploiting NFC vulnerability
- SITA: Data breach effecting Air India linked to APT41
- Data Breaches: McDonalds SK and Volkswagen

F-SECURE THREAT DATA HIGHLIGHTS
- Statistics on threat types, exploits, spam themes & malicious attachments

F-SECURE RESEARCH HIGHLIGHTS
- Vulnerability in Apple’s macOS Gatekeeper

F-SECURE DETECTION & RESPONSE HIGHLIGHTS
- Incident Corner: “FakeUpdates” cybercrime activity

FOREWORD

It is the end of June 2021, and just like that half of the year has gone. If you are like us, it has been a year of continued evolution, brought about to a backdrop of a changeable 18 months worldwide. The immediately notable change for this month’s report is the launch of the new design. We thank our fellows for their hard work to make this happen and hope you, the reader, enjoy the new cleaner design.

On to business, this month we have highlights across cloud, supply chain and ATM attacks. The researchers behind the cloud attacks claim they have identified the first malware to specifically target windows containers. As the adoption of these technologies grows, along with the move of critical data to cloud environments. This is a trend F-Secure expects will grow substantially.

In threat data this month we see the continued exploitation of Microsoft Office related vulnerabilities as well as trojans and ransomware continuing to top detection statistics. Phishing has seen a focus on pharmaceutical themes this month, whilst malicious attachments are dominated by .xlsx and archives.

In research we highlight a vulnerability our researchers found in macOS’ Gatekeeper that allows the bypass of security checks through a specially crafted archive file. Lastly, in our incident corner this month we highlight a watering hole attack against an MDR customer that we have linked to the FakeUpdates campaign previously reported on publicly.

We hope you enjoy this month’s report, and as always, we welcome any feedback you may have.

- Callum Roxan, Head of Threat Intelligence
MONTHLY HIGHLIGHTS

SILOSCAPE: A CLOUD NATIVE ATTACK

SUMMARY

On the 7th June Daniel Prizmant of Paolo Alto’s Unit42 published a report on his discovery of a malware targeting Windows Containers dubbed as Siloscape. The malware is designed to open a backdoor into poorly configured Kubernetes clusters to run malicious containers.

Organizations are increasingly using containers in the cloud in recent years particularly since the COVID-19 pandemic has led many to find faster ways to deploy cloud workloads more efficiently. Kubernetes is an open-source container platform. A Kubernetes cluster is a set of machines or nodes that run containerized applications. It was originally designed by Google and is now maintained by the Cloud Native Computing Foundation. It aims to provide a “platform for automating deployment, scaling, and operations of application containers across clusters of hosts”.

Prizmant of Unit42 first uncovered vulnerability CVE-2020-8558 in July 2020. The vulnerability enables a technique for escaping from a Windows container node in Kubernetes in order to spread in the cluster that Microsoft later recognized as a vulnerability.

Siloscape was discovered by Prizmart in the course of his research and is the first known malware targeting Windows containers. It opens a backdoor to a Kubernetes cluster which gives an attacker access to run any code, anywhere on a victim’s cluster. This could enable a variety of attacks against a victim including: ransomware, crypto jacking, DDoS and data exfiltration. It therefore has the potential to be highly damaging to a Windows cloud environment.

Recommendations made by Palo Alto Networks include:

- Follow Microsoft’s guidance recommending users not run anything in a Windows container that they wouldn’t be willing to run as an admin on the host.
- Limit the privilege of each node by using the Kubernetes Authorization modules, such as role-based access control (RBAC).
- Make sure all of your deployments are using the latest version of all of their applications and frequently scan for security releases with a Cloud Native Security Platform (CNSP) such as Prisma Cloud.
F-SECURE’S INSIGHT

This is the first known malware targeting windows containers. Its emergence is not surprising given the rapid increase in cloud adoption over the past few years. As operating practices and the platforms used by organizations change, so too will resourceful threat actors adapt to look for vulnerabilities to exploit in the changing operating environment.

It is F-Secure’s view that these types of attacks and techniques will proliferate over time as organizations increasingly move critical business functions and sensitive data in to their cloud environments. The movement of these will draw the attention of threat actors who see the disruption and compromise of these as key aims to achieve their overall objectives. The recent NOBELIUM campaign is a good signal of this intent, where reporting suggested there was key focus on data in cloud environments to achieve the objectives of their threat actor.

GELSEMIUM: OPERATION NIGHTSCOUT SUPPLY CHAIN ATTACKS AGAINST NOXPLAYER ANDROID EMULATORS

SUMMARY

In February, ESET discovered a supply chain attack targeting a vulnerability in NoxPlayer Android emulators. At the time they identified a very limited number of victims in Taiwan, Hong Kong and Sri Lanka. This was a campaign targeting online-gaming communities and “electronics manufacturers” in Asia. The attack (dubbed Operation NightScout) compromised NoxPlayer’s update API mechanism to deliver malware to selected users.

This month they published a White Paper, which is an update on their findings and attributes Operation NightScout to the Gelsemium group. In the white paper they have identified new targets that include governments, universities, electronics manufacturers and religious organizations in East Asia and the Middle East.

NoxPlayer is an Android emulator for PCs and Macs. The product user base is predominantly gamers who use the emulator to play mobile games from their PCs. It is made by BigNox, a Hong Kong company with over 150 million users worldwide, but most users are based in Asia.

In this campaign identified by ESET, initial access is gained through malicious software updates installed onto users’ machines. Victims of this supply chain attack were later targeted with a new version of Gelsemium, which is a complex and modular malware, later referred to as Gelsemine (the dropper), Gelsenicine (the loader) and Gelsevirine (the main plug-in).

The malware delivered possessed surveillance capabilities suggesting the motivation of the attack was to collect intelligence on the targets operating in the gaming community. Some victims had a PowerShell version of Mimikatz installed onto their machines which was downloaded from a remote server.

ESET’s attribution to the threat actor Gelsemium is based on connections to campaigns by the threat actor that date back as early as 2014 in a cyberespionage campaign dubbed Operation TooHash. This assessment is based on similarities in malware samples linked to other campaigns in which the Gelsemium group targeted governments, religious organizations, electronics manufacturers and universities in East Asia and the Middle East.

Cyclonis also note that Gelsemium group has been relatively difficult to track because the group has targeted a very small number of victims, despite having been in the field for over seven years. Meaning most related activity has flown under the radar.

Analysis of their implants and infrastructure shows some overlap with other known APT groups operating in Eastern Asia and the Middle East. However,
there are not enough similarities to determine whether the Gelsemium APT is a sub-group of a more popular threat actor.

Gelsemium has deployed a range of malware delivery techniques since 2014 including: documents exploiting Microsoft Office vulnerabilities and watering holes to a remote code execution flaw in Microsoft Exchange Server likely to be CVE-2020-0688, 2014 and 2016 spearphishing documents using exploits targeting a Microsoft office vulnerability CVE-2012-0158. ESET also link Gelsemium to a recent campaign against victims in government, education, and religious groups as well as electronics manufacturers. A victimology which indicates cyberespionage motives.

BigNox initially denied customers had been affected by this compromise but since updated their position and taken several steps to improve security for their users including:

- Use of HTTPS only to deliver software updates mitigating the risk of domain hijacking and man-in-the-middle attacks.
- Implemented file integrity verification using MD5 hashing and file signature checks.
- Adopted additional measures including encryption of sensitive data to protect personal information.
- They have also pushed the latest files to the update server for NoxPlayer and, on startup, NoxPlayer will run a check of application files previously installed on the users’ machines.

**F-SECURE’S INSIGHT**

F-Secure notes that this recent Gelsemium campaign was specifically targeted the gaming community and electronic industry in Asia and Middle East. Gelsemium’s attack on NoxPlayer stands out since not many threat actors target gaming community who are more commonly motivated by financial and criminal objectives.

There has been an increase in criminal groups targeting the gaming industry over the past two years, particularly during the pandemic when gaming has grown in popularity: the most high profile of which are cases such as the Ubisoft, supply chain attack against the gaming industry that infected several massive multiplayer online (MMO) game developers, and a recent attack against Electronic Arts that had source code stolen when they were compromised earlier this month.
Android emulators are used by developers, security professionals as well as gamers to create what is considered a ‘sandboxed’ environment on a user’s host machine enabling the user to replicate mobile applications on their computer. Because emulators isolate the Android environment from the host it is unlikely viruses on the emulator will affect the main operating system.

However, F-Secure advises that introducing any piece of software brings some risks: the remote execution bug CVE-2019-12936 was identified in BlueStacks Android emulator in 2019 which allowed BlueStack’s IPC mechanism to be tampered with that could lead to remote execution of code, information leaks, and the theft of data backups in the emulator.

Recommendations

- NoxPlayer users should remain cautious and follow the recommendations below for users to assess whether or not they have been exposed to this compromise: Refer to the ESET report and Github repository for IoCs relating to this campaign.

- If you identify an intrusion, you should take the necessary steps to investigate with a trained professional and remediate the intrusion though reinstalling NoxPlayer from a clean source.

- Users of Android emulators are recommended to only install trusted programs for Android, use emulators from reputable sources, and keep up to date with the latest security updates.

- Recent reports suggest Windows 11 will be able to run Android apps natively reducing or removing any need for an Android emulator running on Windows.

ATM JACKPOTTING VIA NFC

Security researcher, Josep Rodriguez at security firm IOActive has spent the last year researching vulnerabilities in near-field communications (NFC) reader chips that are used in millions of ATMs and point-of-sales systems globally.

NFC systems enable you to make a payment or withdraw money a cash machine by waving your card over a reader rather than inserting or swiping it. This research shows that it is possible to build an Android app that imitates credit card radio communications and exploits flaws in NFC firmware.

Exploiting this vulnerability, he has shown it is possible to exploit other bugs that may also be present on the device to crash point-of-sale devices, hack them to collect and transmit credit card data, change the value of transactions, and lock the devices whilst displaying a ransomware message.

He claims to have also successfully conducted a ‘jackpotting’ hack against at least one brand of ATM – that is, he has forced the machine to dispense money. This is only possible when other bugs are present on the machine’s software as a compromised NFC reader would only be able to steal mag-stripe credit card data and not the victim’s PIN or the data from the EMV chips. The ATM jackpotting requires an additional and distinct vulnerability in a target ATM’s code.
The technique exploits a vulnerability in ATM NFC readers that did not validate the size of the data packet sent via NFC from a credit card to the reader or application protocol data (APDU). By sending an ADPU much larger than the reader expects from his Android app, Rodriguez was able to trigger a buffer overflow, which is a vulnerability that allows an attacker to corrupt the memory of a target device and run their own code.

Vendors affected by this flaw include ID Tech, Igenico, Verifone, Crane Payment Innovations, BBPOS, Nexgo and another unnamed vendor. They have all been informed of the flaw in their machines. Most failed to respond to questions from a Wired journalist investigating the report findings. Those that did respond downplayed the impact on customers or said they have patched fixed the point-of-sale vulnerabilities to mitigate the problem. However, Rodriguez argues that the lack of consistent patching in the company’s devices means he has still identified vulnerable devices currently in use.

F-SECURE’S INSIGHT

This is far the first example of ATM hacking. The devices have been prone to hacking and jackpot attacks for years. It is possible to exploit ATM systems via a network attack but due to network segmentation this is much more challenging and requires greater technical expertise of the threat actor making it less common than physical attacks.

Based on F-Secure experience responding to these attacks F-Secure has found jackpotting potentially still has appeal to traditional criminal gangs with low level cyber skills and identifies a number of factors that leave them vulnerable to criminals and thieves with a minimal level of cyber expertise:

- Many ATM devices have multiple vulnerabilities that have remained unpatched for years. Some run on operating systems that are no longer supported: the vast majority of ATMs still use a version of Windows XP which stopped receiving updates from Microsoft in April 2014. As a result, many 0-day vulnerabilities for this system will remain unpatched and can be exploited. Engineers servicing ATMs often do not update the software, and so for example some ATMs still have the unpatched critical vulnerability MS08-067 that allows remote code execution.

- The task to secure thousands of ATMs is beyond the capacity of many ATM manufacturers for whom there is no pressing incentive to invest heavily in maintaining old devices. Many of which have expired warranties and are still used by banks around the world. These manufacturers are often more interested in selling new products than patching existing systems, and banks lack the necessary skills to cope with the problems on their own.
An ATM is basically a construction kit that is not too challenging to criminals with the right tools to physically access and compromise. Depending on the brand, it is possible to purchase a key online that opens the front panel, this exposes the workings of the machine. Again, depending on the manufacturer, a criminal can access network cables or plug in a USB drive to drop malware that prompts a machine to dispense cash. This malware is openly available online making this a relatively low sophistication attack.

Impact of these types of attacks over the past few years has in some cases cost banks billions of dollars. Threat actors known to have compromised ATM systems include Lazarus Group that deployed 10 different malware samples in the FASTCash cyber-attacks that compromised “switch application servers“ to facilitate fraudulent transactions causing ATMs to spit out large sums of cash without informing the bank.

Rodriguez’s research identifies a vulnerability in NFC systems which further increases the attack surface of ATMs. However, as the report suggests, there are other vulnerabilities or bugs to be present on the device. It also requires a higher degree of technical expertise to be able to exploit potentially making NFC less accessible as a vector to criminals with lower level of technical expertise. With the current attacks remaining effective, there is not much incentive currently for attackers to shift to more complex NFC attacks.

Patching and ensuring software is up to date and not vulnerable is recommended. Also, because the attacks more often require physical access to the machines, the physical security such as securing the panel of the device and ensuring CCTV coverage exists can be effective deterrents. As F-Secure notes geographical location of a device can determine the likelihood of an attack: remote locations and poor CCTV coverage can slow response by local law enforcement and be a factor increasing the chances of an attack. Therefore, banks and vendors responsible for maintaining ATMs should focus efforts to secure them on machines in more remote locations where physical security is poor.

AIR INDIA COMPROMISE ATTRIBUTED TO APT41 AND LINKED TO SITA ATTACK

A huge cyberattack on global IT provider for 90 percent of the world’s airline industry has revealed the largest supply chain attack on the airline industry in history.

Early assessment suggested that the breach impacted 4.5 million passengers and has potentially been traced back to the Chinese state-sponsored threat actor APT41. Analysts were warning airlines to hunt their networks for any traces of APT41 in their networks as a result of this intrusion.

The attack was originally reported by SITA in early March. Shortly after this announcement, Singapore and Malaysia Airlines as well as Air India announced their customers’ personal data had been exposed.

Group-IB responded to an Air India breach that it traced back to SITA and assess the Air India attack persisted for nearly three months. It took the threat actors only 24 hours to establish Cobalt Strike beacons on the victim’s network. Customer data thought to be exfiltrated from Air India has since been identified for sale on the dark web.

Group-IB identified a C2 server communicating with a SITA data processing server and found the threat actor began moving laterally in the network. The attackers, “exfiltrated NTLM hashes and plain-text passwords from local workstations using hashdump and Mimikatz”. They then attempted to escalate privileges using BadPotato malware. Investigators believe at least 20
devices were compromised during the lateral movement phase and that they used DNS-txt requests to connect to the C2 server.

Group-IB have attributed the Air India attack to APT41, the same threat actor responsible for the SITA breach with ‘moderate confidence’ based on:

- Linking to an APT41-controlled IP address used in the Air India attack.
- Other similarities in TTPs of the SITA breach and other attacks carried out by APT41.

APT41 (described in the industry as having crossover with groups tracked as Wicked Panda, Wicked Spider, Winnti and Barium) has been active since 2007 and specializes in supply-chain attacks. The group is reportedly motivated by financial gain as well as cyberespionage activity that is consistent with the sale of exfiltrated data in this case.

They have been known to “facilitate the theft of source code, software code-signing certificates, customer account data and business information”. In 2020 the DoJ charged five suspects linked to the group with hacking over 100 US victims across targets aligned with the interests of the Chinese state – such as computer hardware manufacturers, telecom providers, social-media companies, video game companies, nonprofit organizations, universities, think tanks and foreign governments as well as pro-democracy politicians and activists in Hong Kong.

(Source: https://blog.group-ib.com/column/tk_apt41)
F-SECURE’S INSIGHT

Group-IB have been measured in their attribution of this activity, they have shared details of attribution and assessed with ‘moderate confidence’ APT41 was responsible for the Air India attack. Although the compromise was originally defined as a ‘breach’, Group-IB’ technical reporting on compromise details that indicate a campaign linked to a targeted attack against SITA and post compromise actions on objectives indicate the threat actor was highly likely an APT operating with cyberespionage and financial objectives.

Data exfiltrated in the Air India and SITA attacks is extremely valuable to a threat actor operating in the interests of intelligence agencies. Foreign intelligence agencies can integrate this kind of bulk data that includes customer PII and travel manifests into proprietary data collections to be exploited in intelligence investigations and targeting activity against individuals.

The data exfiltrated did also appear for sale on the dark web suggesting either a financially motivated angle or that the group sought to profit on the side from this operation. This is consistent with APT41 profile as a group that operates under both cyberespionage remit for the Chinese state as well as also conducting financially motivated cybercriminal activity on the side.

In cases such as this where the data appears for sale on the dark web can also be beneficial to a state backed group trying to confuse attribution. Further, there has been an uptick in Chinese state backed APT activity against Indian targets over the past year, which the targeting of Air India would align with amongst the broader trend of increased border tensions between the two countries.

Initial access in this compromise is yet to be established and the extent of impact to customers and affected airlines we expect to be felt for the coming months to years. For technical report including IOCs refer to the Group-IB write up: Big airline heist: APT41 likely behind massive supply chain attack (group-ib.com)

DATA BREACHES: MCDONALDS AND VOLKSWAGEN

Other businesses affected by data breaches over June include McDonald’s who reported a data breach that exposed personal information of customers in South Korea and Taiwan. The company responded to “unauthorized activity” on its network that revealed a “small number of files were accessed, some of which contained personal data”.

Additional steps were taken to secure files that contained information about its employees. The breached data includes email, delivery addresses and phone numbers but not payment details. The breach was first identified during an external investigation and was first reported by the Wall Street Journal. McDonald’s said that they would be conducting an investigation and leveraging findings to further enhance security measures.

Volkswagen also announced sensitive information of 90,000 customers including driver’s license and social security numbers were left unsecured for two years. They recently discovered an, “unauthorized third party” obtained personal information about customers and interested buyers from a vendor that Audi, Volkswagen and some authorized dealers in the US and Canada that was used for sales and marketing activity. They are contacting approximately 90,000 customers directly for whom sensitive information was involved.

McDonald’s data breach: What customers need to know...

Other business affected over June include McDonald's who reported a data breach that exposed personal information of customers in South Korea and Taiwan. The company responded to “unauthorized activity” on its network that revealed a “small number of files were accessed, some of which contained personal data”.

Additional steps were taken to secure files that contained information about its employees. The breached data includes email, delivery addresses and phone numbers but not payment details. The breach was first identified during an external investigation and was first reported by the Wall Street Journal. McDonald’s said that they would be conducting an investigation and leveraging findings to further enhance security measures.

Volkswagen also announced sensitive information of 90,000 customers including driver’s license and social security numbers were left unsecured for two years. They recently discovered an, “unauthorized third party” obtained personal information about customers and interested buyers from a vendor that Audi, Volkswagen and some authorized dealers in the US and Canada that was used for sales and marketing activity. They are contacting approximately 90,000 customers directly for whom sensitive information was involved.

DATA BREACHES: MCDONALDS AND VOLKSWAGEN

Other businesses affected by data breaches over June include McDonald’s who reported a data breach that exposed personal information of customers in South Korea and Taiwan. The company responded to “unauthorized activity” on its network that revealed a “small number of files were accessed, some of which contained personal data”.

Additional steps were taken to secure files that contained information about its employees. The breached data includes email, delivery addresses and phone numbers but not payment details. The breach was first identified during an external investigation and was first reported by the Wall Street Journal. McDonald’s said that they would be conducting an investigation and leveraging findings to further enhance security measures.

Volkswagen also announced sensitive information of 90,000 customers including driver’s license and social security numbers were left unsecured for two years. They recently discovered an, “unauthorized third party” obtained personal information about customers and interested buyers from a vendor that Audi, Volkswagen and some authorized dealers in the US and Canada that was used for sales and marketing activity. They are contacting approximately 90,000 customers directly for whom sensitive information was involved.
F-SECURE’S INSIGHT

Based on the announcements by McDonald’s and Volkswagen (VW), objectives of the threat actors in these cases appear to have been access to PII. The access to the data is likely to be opportunistic given the acknowledgement by both parties that the data had been left exposed online.

PII of this kind, particularly in the level of personal information compromised in the VW breach has significant market value if sold on to other cyber threat actors and criminal groups looking to exploit this data in cases of online fraud and activity such as phishing and social engineering campaigns.

Organizations and individuals impacted by these breaches should review the data exposed and review how this may be used to target them. The cycling of credentials due to password re-use, the changing of security questions and the enabling of MFA on high risk platforms are all things that should be considered.

Recommendations

- VW customers whose sensitive data was exposed have been offered free credit monitoring and a help hub has been setup by IDX for anyone concerned they have been impacted by the breach.

- Communications claiming to be from Audi or Volkswagen should be treated with caution and extra suspicion due to actors potentially trying to target victims of the breach. Special attention should be given to email or SMS text messages.

- Anyone potentially affected by data breaches of this kind are advised to stay alert for phishing emails or spam based on any of the basic information leaked.

(Source: https://nypost.com/2021/06/11/mcdonalds-hit-by-data-breach/)
F-SECURE THREAT DATA HIGHLIGHTS

THREAT TYPES
Generic trojans continue to be the most prevalent malware in the wild followed by ransomware and exploits.

EXPLOITS
In June, the threat landscape for exploits was mostly dominated by CVE-2017-11882 which is an MS Office memory corruption vulnerability. This vulnerability continues to be the most exploited in the wild. The most commonly exploited software remains MS Office family.
SPAM EMAIL THEMES

Interestingly in June the spam email themes have seen some shift. Cryptocurrency spam has dropped significantly and in the middle of June we saw significant activity around Pharmaceutical spam which revolve around advertisement for drugs. The pharmaceutical theme seems to have died down towards the end of June.

MALICIOUS EMAIL ATTACHMENTS

In June, nearly 5th of the emails containing malicious attachments contain MS Office .xlsx documents. Over half of the malicious attachments are different types of archives. Often used to avoid detection and hide the actual payload which commonly are executables, shortcut files or other documents with malware or exploits.
F-SECURE RESEARCH HIGHLIGHTS

EXPLOITABLE VULNERABILITY IN APPLE’S MAC OS GATEKEEPER DISCOVERED BY F-SECURE R&D

Apple released patches in March for a vulnerability in macOS’ Gatekeeper that was discovered by F-Secure R&D late last year. F-Secure researchers found it was possible to exploit the vulnerability by tricking users to download a crafted .zip file allowing them to bypass the macOS Gatekeeper’s code signature and notarization checks.

Gatekeeper is a feature of the macOS operating system that is designed to protect the users of Mac computers from malware by preventing execution of software from untrusted sources, or more specifically applications that aren’t signed with an Apple-issued certificate (Developer ID) and approved by Apple’s notarization service.

R&D found any software distributed as a .zip file could contain an exploit for this vulnerability. There are a few exceptions such as applications downloaded from Apple’s App Store, which are not affected by this issue. Similarly, applications delivered as macOS packages (.pkg, .mpkg) contain an installer certificate which is verified independently of Gatekeeper.

The vulnerability, CVE-2021-1810, was originally discovered in late 2020. Apple released patches for this issue in both Big Sur and Catalina earlier this week. F-Secure has seen no evidence of this vulnerability being exploited in the wild, nor is it aware of any reports from third parties. However, there are other vulnerabilities addressed by the updates, so it’s important for users to patch as soon as possible.

F-Secure R&D will publish detailed write-up once users have had more time to update their devices. It is important to note that at the core of the exploit is a specially crafted zip file.

- F-Secure has developed detections to prevent these files from running on machines using our endpoint protection products.
- In addition, advanced users can manually inspect the code signature of any downloaded application using “codesign -v” and “codesign -dv” in Terminal.
- Users should regularly update their software to ensure they are safe from this and other threats.

Disclosure timeline:

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-12-09</td>
<td>Vulnerability discovered by F-Secure R&amp;D</td>
</tr>
<tr>
<td>2020-12-11</td>
<td>Vulnerability disclosed to Apple Product Security</td>
</tr>
<tr>
<td>2021-01-14</td>
<td>Detection released to F-Secure endpoint protection products (F-Secure SAFE, F-Secure Computer Protection, F-Secure Client Security)</td>
</tr>
<tr>
<td>2021-04-22</td>
<td>Apple acknowledges report will be credited in next update cycle</td>
</tr>
<tr>
<td>2021-04-26</td>
<td>Apple releases Security Update 2021-002 Catalina and macOS Big Sur 11.3</td>
</tr>
</tbody>
</table>
F-SECURE DETECTION & RESPONSE HIGHLIGHTS

INCIDENT CORNER: “FAKEUPDATES” INCIDENT

The MDR Detection & Response Team (DRT) detected the execution of malicious JavaScript (.js) and PowerShell commands on an endpoint. The source of these executions appeared to be an archive (.zip) titled “Chrome Update” opened by the user of the host.

In addition, there were numerous detections relating to the injection of a malicious payload into memory, suspicious module loads, enumeration commands, and anomalous network communication.

Whilst DRT had linked this activity to the malicious archive, it was not immediately clear how this file had been created on the host or why the user had opened it. Investigation of the network telemetry around the time of the creation of the archive highlighted a number of anomalous domains that the user had visited through their browser.

F-Secure were able to identify that the user had visited a legitimate website that had been compromised in order to deliver this malicious Chrome update. The website in question was navigated to after the user Googled a common phrased associated with their job function.

The threat actor’s access was contained and removed by the DRT within 45 minutes of the first detection. The customer was informed, and advised to cycle the credentials of the user as well as other post-incident related recommendations.

Combining the DRT’s analysis from the investigation and the broader investigation by the Threat Intelligence team F-Secure linked this activity to a campaign dubbed as “FakeUpdates” by FireEye. The initial activity observed by F-Secure was very similar to that reported in this campaign, though the post exploitation activity has evolved since this was initially reported on.

In addition to those details noted already, F-Secure observed the threat actor executing a number of .NET commands associated with SeatBelt, as well as other similar enumeration commands from open source PowerShell scripts. Specifically, SharpWeb, SharpChromium, SessionGopher and a version of Invoke-PrivescCheck were all executed in quick succession on the host before the threat actor was contained.

F-SECURE’S INSIGHT

The use of “watering holes” to compromise organizations is not a new technique, but is one that F-Secure’s MDR service has seen across a few incidents in recent months.

This initial access avenue is often a difficult one to completely prevent due to the requirement for user’s to be able to access the internet for their roles. These attacks can be broadly targeted against individuals or organizations who operate with certain interests, but are more commonly un-targeted in nature and reliant on opportunistic compromise of both the legitimate website and user visiting this.

F-Secure recommends that organizations focus on educating users about the risks of installing unknown applications from the internet and common examples of malicious downloads from these sites. In addition, controls that prevent the execution of untrusted content can reduce the success of such attacks.
<table>
<thead>
<tr>
<th>Tactic</th>
<th>Technique</th>
<th>Technique ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Access</td>
<td>Drive-by Compromise</td>
<td>T1189</td>
</tr>
<tr>
<td>Execution</td>
<td>Command and Scripting Interpreter: PowerShell</td>
<td>T1059.001</td>
</tr>
<tr>
<td></td>
<td>Command and Scripting Interpreter: Windows Command Shell</td>
<td>T1059.003</td>
</tr>
<tr>
<td></td>
<td>Command and Scripting Interpreter: JavaScript</td>
<td>T1059.007</td>
</tr>
<tr>
<td></td>
<td>Native API</td>
<td>T1106</td>
</tr>
<tr>
<td></td>
<td>User Execution: Malicious File</td>
<td>T1204.002</td>
</tr>
<tr>
<td>Evasion</td>
<td>Deobfuscate/Decode Files or Information</td>
<td>T1140</td>
</tr>
<tr>
<td></td>
<td>Process Injection: Dynamic-link Library Injection</td>
<td>T1055.001</td>
</tr>
<tr>
<td>Credential Access</td>
<td>Credentials from Password Stores:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Credentials from Web Browsers</td>
<td>T1555.003</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tactic</th>
<th>Technique</th>
<th>Technique ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery</td>
<td>Domain Trust Discovery</td>
<td>T1482</td>
</tr>
<tr>
<td></td>
<td>Permission Groups Discovery: Local Groups</td>
<td>T1069.001</td>
</tr>
<tr>
<td></td>
<td>Permission Groups Discovery: Domain Groups</td>
<td>T1069.002</td>
</tr>
<tr>
<td></td>
<td>System Information Discovery</td>
<td>T1082</td>
</tr>
<tr>
<td></td>
<td>Account Discovery: Local Account</td>
<td>T1087.001</td>
</tr>
<tr>
<td></td>
<td>Account Discovery: Domain Account</td>
<td>T1087.002</td>
</tr>
<tr>
<td>Command and Control</td>
<td>Application Layer Protocol: Web Protocols</td>
<td>T1071.001</td>
</tr>
</tbody>
</table>