EXECUTIVE SUMMARY

MONTHLY HIGHLIGHTS

- Proxylogon Exploits Microsoft Exchange Zero-Day Vulnerabilities Crisis
- Unc2452/Nobelium New Second-Stage Malware Discovered
- Supernova WebsHELL: Spiral Threat Group Targeted SolarWinds
- Operation Dianxun: Mustang Panda’s Latest Campaign Targeting Telecommunications
- AcCellion FTA Vulnerability: Shell Energy Company, Qualys Cyber Security Firm and Flagstar Bank
- Indrik Spider: Changing TTPs in Response to Sanctions
- Red Echo Targeting Indian Critical Infrastructure: China-Indian Geopolitical Tensions
- APT10 Delivering Multi-Layered Loader Ecipekac In A41APT Campaign

THREAT DATA HIGHLIGHTS

- File Threats: Trojans, Ransomware and Exploits
- Email Threats: Spam Themes and Prevalent Malicious Attachment Extensions

RESEARCH HIGHLIGHTS

- Android Samsung Browser Vulnerability
- Samsung Notes Vulnerability

DETECTION & RESPONSE HIGHLIGHTS

- Ransomware Actor: PowershellEmpire & SystemBc
MONTHLY HIGHLIGHTS

PROXYLOGON EXPLOITS: MICROSOFT EXCHANGE ZERO-DAY VULNERABILITIES CRISIS

On the 2nd of March 2021, Microsoft released a security update detailing multiple vulnerabilities in Microsoft Exchange Server being actively exploited by a threat group they track as HAFNIUM. The threat actor exploited the vulnerabilities in Exchange, which gave them highly privileged access to the underlying servers. This could facilitate access to email accounts and the ability to install additional malware to facilitate long-term access to victims.

KrebsOnSecurity reported on March 5th that at least 30,000 organizations in the US had been hacked by the Chinese threat actor tracked by Microsoft as HAFNIUM. The threat actor exploited four (now-patched) zero-day vulnerabilities in Microsoft Exchange Server 2013, 2016 and 2019 to plant backdoors and exfiltrate emails. The flaws, which were discovered and reported by Volexity, are collectively dubbed "ProxyLogon" and tracked as CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. Following Microsoft’s issuance of emergency patches on March 2nd, Krebs said Hafnium "dramatically stepped up attacks on any vulnerable, unpatched Exchange servers,” gaining access to hundreds of thousands of servers worldwide.

ESET claimed at least four other APT groups besides Hafnium had exploited the vulnerabilities before they were publicly disclosed, and "many more threat actors" began scanning and compromising Exchange Servers after the disclosure. They include the espionage-focused groups Tick, LuckyMouse, Calypso, Tonto Team, Mikroceen, and Winnti Group, as well as the cryptojacking gang DLTMiner. The Record cited ESET and Kryptos Logic as saying that at least one of the threat actors was trying to log into and hijack other group’s web shells. The Record also noted that on the 10th March a Vietnamese security researcher published a working public exploit for the vulnerabilities. Palo Alto Networks’ Unit 42 claimed one of the criminal operators exploiting the ProxyLogon vulnerabilities is the operator of DearCry, a new ransomware variant.

Security firm Check Point reported that it observed attacks increase by an order of magnitude, from seven hundred on March 11th all the way up to seven thousand two hundred, on March 15th. The country most attacked has been the United States (17% of all exploit attempts), followed by Germany (6%), the United Kingdom (5%), The Netherlands (5%) and Russia (4%). The most targeted industry sector has been Government/Military (23% of all exploit attempts), followed by Manufacturing (15%), Banking & Financial Services (14%), Software vendors (7%) and Healthcare (6%).

By March 22nd, Microsoft Security Resource Center (MSRC) tweeted that 92% of worldwide Exchange IPs were now patched or mitigated, and it was a 43% improvement worldwide from the week prior.

F-SECURE’S INSIGHT

F-Secure observed widespread exploitation of the ProxyLogon vulnerabilities through our EPP, MDR and IR services. After publication, the time to exploitation of critical vulnerabilities such as ProxyLogon appears to have grown shorter in recent years. This stresses the
importance of organizations adapting their emergency patch processes to keep up with external actors. This also stresses the importance of defense in depth through other security technologies to protect organizations during this period of vulnerability.

**SUMMARY**

FireEye has identified a second-stage backdoor dubbed "SUNSHUTTLE" that the security firm thinks may be linked to the threat actor they track as UNC2452. UNC2452 has been associated with the SolarWinds supply chain exploitation, but FireEye stresses its researchers have not fully verified a connection with SUNSHUTTLE.

The backdoor was uploaded by a U.S. based entity to a public malware repository in August 2020, and the researchers say the malware was observed at an entity that had been compromised by UNC2452. SUNSHUTTLE is written in the GO language. It has the capability to read an embedded or local configuration file, communicate with a hard-coded command and control (C2) server over HTTPS, and supports commands including remote config upload, file upload and download, and arbitrary command execution. Notably, SUNSHUTTLE uses cookie headers to pass values to the C2, and when customized, can select referrers from a list of popular website URLs to help the network traffic blend in with usual activity.

The new SUNSHUTTLE backdoor is a sophisticated second-stage backdoor that demonstrates straightforward but elegant detection evasion techniques via its “blend-in” traffic capabilities for C2 communications. SUNSHUTTLE would function as second-stage backdoor in such a compromise for conducting network reconnaissance alongside other SUNBURST related tools.

Microsoft (which tracks the Solarigate threat actor as "NOBELIUM") has published its own analysis of the backdoor, along with two other tools called GoldFinder and Sibot. Reporting shows the malware was used from August to September 2020, though it may have been placed on systems in June 2020. These novel pieces of malware discovered are entirely unique to the threat actor. They are tailor-made for specific networks and are assessed to be introduced after the actor has gained access through compromised credentials or the SolarWinds binary and after moving laterally with TEARDROP and other hands-on-keyboard actions.

**F-SECURE’S INSIGHT**

These capabilities differ from previously known NOBELIUM tools, but are consistent with the capability and intent previously shown by the threat actor. In all stages of the attack, the actor demonstrated a deep knowledge of software tools, deployments, security software and techniques frequently used by incident response teams. This knowledge is reflected in the actor’s operational decisions, from the choice of command-and-control (C2) infrastructure to the naming of scheduled tasks used to maintain persistence. These tools suggest the actor has substantial capability to develop custom tooling for their intrusions and draws from a group of operatives who have advanced knowledge of information systems and their security.
SUPERNOVA WEBSHELL: SPIRAL THREAT GROUP
TARGETED SOLARWINDS

SUMMARY

Secureworks describes cyberespionage activity by a suspected Chinese actor dubbed "SPIRAL." The actor exploited a vulnerability (CVE-2020-10148) in SolarWinds’ Orion product to deploy its SUPERNOVA web shell. The researchers say this activity is unrelated to the Russian-linked Solorigate campaign that also made use of SolarWinds’ Orion Platform.

The SUPERNOVA web shell is a trojanized version of a legitimate Orion DLL. The threat actor first executed a reconnaissance script before deploying the web shell, then obtained credentials from Windows' Local Security Authority Subsystem Service (LSASS). After this, the actor mapped network shares on two hosts: a domain controller and a server that could provide access to sensitive business information.

Secureworks believes the group is based in China because the actor exposed a Chinese IP address when it downloaded an installer. In addition, a Secureworks Endpoint Detection and Response (EDR) agent checked in from a host that did not belong to the compromised organization and used an IP address geo-located to China. The naming convention of this host was the same as another host used by the threat actor to connect to the network via a VPN connection. This ‘<Username>-PC’ naming convention is the default hostname for a Windows 7 host, but it is not the victim’s standard naming convention for hosts.

Secureworks CTU analysis suggests the threat group likely downloaded the endpoint agent installer from the network and executed it on the attacker-managed infrastructure. The exposure of the IP address was likely unintentional, so its geolocation supports the hypothesis that the SPIRAL threat group operates out of China.

F-SECURE’S INSIGHT

The interest in a vendor’s EDR agent is a distinct piece of tradecraft that is usually associated with APT classified groups. F-Secure is aware of other groups in this region showing similar interest in our own agent, though the exposure of the IP address appears to be an embarrassing slip in operational security by the threat actor. EDR technology provides valuable insight for defenders, and F-Secure expects interest in this technology by more advanced threat actors to continue to rise in the future.

OPERATION DIANXUN: MUSTANG PANDA’S LATEST
CAMPAIGN TARGETING TELECOMMUNICATIONS

SUMMARY

McAfee has disclosed a cyberespionage campaign dubbed "Operation Diànxùn" that is targeting telecommunications companies. McAfee believes with a moderate level of confidence that this operation is run by the Chinese threat actor Mustang Panda, and that this is the same threat actor tracked by Recorded Future as RedDelta.

McAfee researchers discovered malware using similar tactics, techniques, and procedures (TTPs) to those observed in earlier campaigns publicly attributed to the threat actors RedDelta and Mustang Panda. While the initial vector for the infection is not entirely clear, McAfee suggests that victims were lured to a domain under control of the threat actor, from which they were infected with malware that the threat actor leveraged to perform additional discovery and data collection. McAfee assesses with a
medium level of confidence that the attackers used a phishing website masquerading as the Huawei company career page to target people working in the telecommunications industry.

The researchers believe the actor is trying to steal information related to 5G technology (and they stress that they have no evidence that Huawei itself had any involvement in this campaign).

McAfee’s telemetry revealed possible targets based in Southeast Asia, Europe, and the US were discovered in the telecommunication sector. They also identified a strong interest in German, Vietnamese, and Indian telecommunication companies. Combined with the use of the fake Huawei site, they assess with a high level of confidence that this campaign was targeting the telecommunication sector. They assess with a moderate level of confidence that the motivation behind this specific campaign has to do with the ban of Chinese technology in the global 5G roll-out.

**F-SECURE’S INSIGHT**

McAfee’s assessment of the crossover with RedDelta and MustangPanda appears to be sound based on the public technical indicators reviewed by F-Secure’s threat intelligence team. F-Secure is also aware of technical indicators suggesting additional companies beyond Huawei were impersonated by the threat actor behind this campaign.

F-Secure is aware from its own telemetry of Chinese nexus actors targeting the global telecommunication industry and so any organization in this vertical should take note of the indicators as a credible threat to their organization.

**SUMMARY**

Energy giant Shell, cyber security firm Qualys and US bank, Flagstar all announced this month that they were breached due to Accellion software vulnerabilities that were originally disclosed by Accellion late last year.

These three latest victims reported the Accellion platform was segmented from the rest of their operational networks limiting the extent of impact on customers. However, Shell have reported attackers accessed some personal data as well as data belonging to Shell stakeholders and subsidiaries.

Qualys have notified the limited number of customers affected but that there was no impact on its production environments, codebase or customer data hosted on the Qualys Cloud Platform. Initially Flagstar bank announced only staff data had been taken but have subsequently reached out to current and former customers whose personal identifiable information including social security numbers.

Earlier investigations into the Accellion compromise by FireEye revealed cybercrime group FIN11 had exploited multiple zero-day vulnerabilities in Accellion FTA servers, a 20 year old legacy software, to install a newly identified web shell tracked as “DEWMODE” by FireEye.

This web shell was used to steal private files and breached data of some victims was subsequently published on Clop ransomware leak site and, as such, related activity is being attributed to the Clop ransomware group.
PUBLIC

F-SECURE’S INSIGHT

At the time, Accellion said that of 300 FTA clients, less than 100 companies were victims of these attacks and only 25 suffered significant data loss and that all affected parties have been contacted. However, these recent announcements indicate some companies are still suffering fallout from exposed servers. FireEye and Accellion are due to issue a joint report on the details of the compromise and the most up to date information can be found on FireEye’s blog.

Data related extortion is a rising trend in cybercrime circles and exploitation of this vulnerability highlights the continued risk legacy applications can have to organizations if not patched. F-Secure is aware of threat actors who use this extortion technique using other vulnerabilities to exploit organizations in March 2021. This highlights the importance of ensuring vulnerabilities are patched and any risk exposed by exploitation remediated properly.

INDRIK SPIDER: CHANGING TTPS IN RESPONSE TO SANCTIONS

SUMMARY

CrowdStrike reported Russian cybercrime operation Indrik Spider (Evil Corps) has shifted TTPs in response to US Office of Foreign Assets Control (OFAC) sanctions against gang members. Importantly these sanctions prohibited significant payment of ransoms to the group by organizations under the relevant jurisdiction.

Sanctions were enforced in December 2019 when the group was charged for using Dridex banking trojan to cause over $100 million in financial damages. At the same time, the Department of Justice charged two members of the group with criminal infringements and a $5 million USD reward was put up for information leading to the capture of the Indrik Spider’s leader.

After the sanctions were announced Indrik Spider paused operations to reappear in January 2020 when they deployed BitPaymer against a conglomerate spanning multiple verticals. This was the first time the group was seen using a variant of Gozi ISFB instead of the Dridex banking trojan.

After another lull in activity, the group further shifted away from old tools and started to deploy WastedLocker – successor to BitPaymer – in May 2020. Other measures to further distance themselves from earlier operations and tooling included use of a variant of Gozi ISFB.

In June 2020, the group began to use fake browser updates to deliver Cobalt Strike, establish an initial foothold, and move laterally within the target networks. Once Command and Control (C2) was established, WastedLocker ransomware was executed in their big game hunting campaigns targeting organizations across multiple sectors in the US.

Then in December 2020, researchers first identified Hades ransomware, successor to WastedLocker. According to CrowdStrike, there is ‘significant code overlap’ between newly deployed ransomware variant Hades and WastedLocker, with Hades being a 64-bit compiled variant of WastedLocker. There were similarities in the ISFB static configuration, multi-staged persistence/installation process, file/directory enumeration and encryption functionality.

Changes include upgraded code obfuscation and a few minor changes that remove features characteristic of WastedLocker and BitPaymer. Beyond deploying a new ransomware strain, the group have also changed tactics to leaving a ransomware note directing victims to a Tor site as opposed to delivering ransom notes by email.
CrowdStrike concluded that the group’s development of tradecraft has been an attempt to bypass sanctions placed on Indrik Spider by OFAC and the Department of Justice (DoJ). The group has expended considerable resources and operational resilience to adapt and change demonstrating the significant impact sanctions have had on their operations.

**F-SECURE’S INSIGHT**

Ransomware actors have proved to be singularly focused on maximizing profit and willing to adapt to where needed to achieve this in recent years. F-Secure is aware of evidence that suggests these groups are well aware of sanctions, regulation and other factors that may influence a company’s ability to pay the ransoms demanded.

Disruption of cybercrime operations and sanctions have increased in frequency to respond to the damage caused by ransomware, but it is yet to be seen if this is an effective long term tactic for governments. The CrowdStrike report highlights pauses in activity as well as the additional time investment by the Indrik Spider threat actor to respond to these actions. This is a positive takeaway that the sanctions are having some effect on the threat actor and forcing them to adapt, even if this is not stopping the activity.

F-Secure assess that it is likely that governments will look at the most effective ways to influence these operations and take a more bellicose posture in the future.

**RED ECHO TARGETING INDIAN CRITICAL INFRASTRUCTURE: CHINA-INDIAN GEOPOLITICAL TENSIONS**

**SUMMARY**

Recorded Future released results of their investigation into targeted intrusion activity against Indian critical infrastructure they attribute to activity group RedEcho, a group that shares strong infrastructure and victimology overlaps with Chinese groups APT41/Barium and Tonto Team.

From mid-2020 onwards, Recorded Future’s collection revealed a steep rise in the use of infrastructure tracked as AXIOMATICASYMPTOTE, which encompasses ShadowPad command and control (C2) servers to target India’s power sector organizations. Targets of these attacks include 4 Regional Load Dispatch Centre (RLDC) responsible for operation of the power grid and 2 Indian seaports. A Chinese Ministry of Foreign Affairs spokesman later denied claims China was responsible for the attacks.

Recorded Future note the significant growing diplomatic tensions between the two countries, which forms a compelling backdrop to this activity. The report states that they expect this activity to further escalate in line with the real world strategic objectives, and expand beyond the targeting of the mentioned critical national infrastructure verticals.

(Source: [http://independentpress.cc/india-steps-up-vigil-for-cyber-attacks-from-china-after-military-standoff/2020/09/18/]())
F-SECURE’S INSIGHT

Since Recorded Future published its findings, some Indian press reports have claimed Chinese cyber operations caused Indian power industry blackouts that occurred in October last year. These claims remain unsubstantiated, and F-Secure has seen no evidence to suggest a link between these events. There is no clear economic espionage benefit to China as a result of these intrusions. This indicates other motivations for the attacks which come at a time of increased political tension between China and India.

Recorded Future raise significant concerns over potential pre-positioning of network access to support Chinese strategic objectives such as geostategic signaling, influence operations or precursors to kinetic operations. F-Secure’s own assessment supports the excellent work conducted by Recorded Future and notes this is consistent with other Chinese nexus operations F-Secure has visibility of.

KASPERSKY IDENTIFIES APT10 DELIVERING MULTI-LAYERED LOADER ECIEPKAC IN A41APT CAMPAIGN

SUMMARY

In 2019 Kaspersky identified an APT campaign they called A41APT – a name given to the group because it refers to a host name observed in the initial compromise with SSL-VPN products called “DESKTOP-A41UVJV”.

A41APT has been seen targeting Japanese companies since March 2019 across multiple industries with specific focus on automotive industry and companies involved in supplying parts to the motor industry. This recent report by Kaspersky covers new activity identified by Kaspersky in January 2021. During this period, the group used modified and updated payloads.

Other reporting on this campaign has been covered by Symantec Symantec and LAC. Symantec notably observed the threat actor deploying a tool capable of exploiting the critical ZeroLogon vulnerability. In addition, the JPCERT reports that the threat actors were exploiting SSL-VPN products, including Pulse Connect Secure.

This new report by Kaspersky covers the technical details of the multiple pieces of malware uncovered as linked to this campaign. In particular, there is analysis of Ecipekac, a sophisticated multi-layer loader. Ecipekac is named after a distinct string in the malware that is “Cake piece” in reverse (with a typo), but is also known as DESLoader, SigLoader, and HEAVYHAND by other vendors.

Ecipekac was observed delivering payloads such as SodaMaster (DelfsCake, dfls, and DARKTOWN), P8RAT (GreetCake, and HEAVYPOT) and FYAnti (DILLJUICE stage2) which loads QuasarRAT. It has also been seen delivering Cobalt Strike payloads.

Ecipekac uses a complicated loading schema that makes use of multiple stages and files before eventually loading the final payload in to memory. An example flow can be seen in the below image.

(Source: https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/)
According to Kaspersky, the most significant characteristic of Ecipekac, apart from the large number of layers, is that “encrypted shellcodes were being inserted into digitally signed DLLs without affecting the validity of the digital signature. When this technique is used, some security solutions cannot detect these implants”.

Based on the main features of P8RAT and SodaMaster backdoors, they believe that there is likely to be yet additional undiscovered malware that these backdoors are responsible for downloading. P8RAT was modified in December in 2020 in what Kaspersky believe was a direct response to the public analysis posted by Symantec and LAC.

Kaspersky provide their support of attribution to APT10 by detailing overlaps in the coding of crypto algorithms and hashing, DLL side-loading technique, their use of PowerShell scripts, using an exe to remove logs, modification of implants after public research is posted and their targeting of Japanese organizations. They note that two deviances from APT10 expected behaviors by the lack of inclusion of malware version numbers and lack of spearphishing related to this campaign.

**F-SECURE’S INSIGHT**

The main connection between victims of this campaign is that they are large well-known Japanese manufacturing and automotive organizations most of which are in Japan or have links to Japan. Based on attribution of this activity to APT10, a group linked to the Chinese government, F-Secure assess the motivation for these attacks is likely to be exfiltration of data for economic advantage.

Kaspersky’s attribution assessment that this is APT10 activity appears to be well supported, though there is significant analytical debt surrounding the APT10 group that may cloud this slightly. However, the assumptions have been detailed in the report to provide confidence to the analysis done.

The Symantec report details victims across a much broader spectrum than just Japan and the automotive vertical. Therefore, international organizations whose operations may be subject to interest from China due to alignment with the focus areas identified in China’s five year plan should also take note of the findings in these reports.
Threat Types
In March, the most prevalent threats observed in the wild were different trojans with varying capabilities such as banking trojans and spyware. Generic trojans take a big portion of the detected threats followed by different worms such as Njw0rm, trojan downloaders and ransomware. WannaCry still contributes to the ransomware statistics today as infections persist and spread across vulnerable systems.

Exploits
In March our EPP saw a variety of vulnerabilities exploited in the wild. The top 3 include: CVE-2017-11882 which is used by malicious RTF files for code execution; CVE-2018-8653 an Internet Explorer vulnerability exploited by exploit kits and CVE-2021-27065 the notorious ProxyLogon vulnerability exploited by attackers globally to deliver web shells in exchange servers.
Spam Themes
On the spam email front in March cryptocurrency significantly surpassed other themes due to few prevalent cryptocurrency related spam campaigns. The rest of the more traditional emails remained constant but lower in volume.

Malicious Email Attachments
Throughout different malicious email campaigns in March, the most prevalent attachments were different archives such as rar, gzip and zip. Archives are often used to hide payloads behind a password and change the attachment file type to avoid email malware scanning or email rules.

Archives were closely followed by executables and MS Office .xlsx files. The latter are commonly used for malware delivery as macro-enabled documents.
Vulnerability in Samsung Browser on Android Devices

This month, F-Secure LABS published research on an application security bypass vulnerability discovered in the Samsung Browser application on the Google Play Store.

As part of Tokyo Pwn2Own 2020, F-Secure began investigating how to exploit the new Samsung S20. An issue (CVE-2021-25354) was found that allowed a specific browsable intent in Samsung browser (com.sec.android.app.sbrowser) to either:

- Launch non-exported activities in the Samsung Browser application
- Launch an exported activity in any installed application

Whilst this issue was found on Samsung device, the Samsung Internet browser application is available for download on the Google Play Store, and can be accessed and downloaded by any device with access to Google Play. It was confirmed by Samsung that this issue could be exploited on any device with the application installed.

Samsung has now released Samsung Browser version 13.2.1.46 which fixes the issue outlined in this advisory. F-Secure recommends that users upgrade Samsung Browser to the latest available version.

Vulnerability in Samsung phones with Samsung Notes

Further research done as part of Tokyo Pwn2Own 2020 was published on F-Secure LABS, disclosing a storage security bypass vulnerability in Samsung Notes which allows a rogue application to access any file on the external storage partition without the “External Storage” Android permissions. This path traversal vulnerability can be found here – CVE-2021-25367.

Samsung Notes (com.samsung.android.app.notes) has an exported content provider called “clipdatacontentprovider” that can be used by other applications to download files from the external storage. Essentially this allows an unauthorized application to read and retrieve data stored on Samsung external storage.

As a result of this research, Samsung has released Samsung Notes version 4.2.00.22 which fixes the issue outlined in this advisory. F-Secure recommends that users upgrade Samsung Notes to the latest version.
F-SECURE DETECTION & RESPONSE HIGHLIGHTS

INCIDENT CORNER

Ransomware Actor – PowerShell Empire & SystemBC

The MDR Detection & Response Team (DRT) detected the execution of an encoded PowerShell command linked to the PowerShell Empire framework. This activity was quickly followed by the retrieval of another payload containing a new variant of the SystemBC malware from a legitimate file sharing platform. This malicious activity was quickly traced back to a Remote Desktop Protocol (RDP) session by a high privileged user account from a third party service provider.

The threat actor executed several PowerShell scripts to enumerate the host they were on, the wider network and to escalate privileges by dumping LSASS memory through the MiniDump function of comsvcs.dll. In one script the threat actor had failed to update a file path variable from a previous intrusion, and inadvertently revealed a previous victim to F-Secure. Engagement with the relevant CERT confirmed this organization had suffered a ransomware attack a week earlier, and that the threat actor had deployed the Ryuk ransomware.

Armed with this context of the threat, and the wider assessment of the F-Secure Threat Intelligence team, containment was swiftly planned and actioned with the victim organization to prevent the same outcome. The threat actor was observed trying to logon to the victim domain controller just as containment had finished, suggesting this happened just in time.

With the immediate situation resolved the team focused on reviewing the forensic evidence left by the threat actor for anything that may have been missed and future detection opportunities. In addition, F-Secure’s Incident Response (IR) team engaged with the third party to collaborate on an investigation into the root cause of the intrusion. The initial access vector was confirmed to be through exploitation of “CVE-2018-13379”, a vulnerability in a Fortinet VPN appliance used by this organization.

F-Secure Insight: The exploitation of this vulnerability has been seen across multiple organizations by F-Secure over the past month. F-Secure is aware of a historic “credential dump”, which may be linked to this activity.

F-Secure recommends that organizations patch any vulnerable devices, enable & enforce MFA for all VPN users and cycle any related credentials of VPN users.

Amusingly, the IR team also uncovered forensic artifacts that show the threat actor watching a “how to” YouTube video for a network enumeration tool while on the victim systems. This provides evidence of how even unskilled threat actors are being enabled to conduct damaging attacks on organizations through the cybercrime affiliation models.

The SystemBC malware sample was reverse engineered by the F-Secure Threat Intelligence team to aid further research and detection. The final SystemBC payload was encrypted within a wrapper that F-Secure identified is common across multiple crimeware trojans, including the increasingly prevalent BazarLoader. The wrapper uses a process hollowing technique to execute the final payload in memory to avoid many common detection techniques.

This incident was typical of many ransomware related intrusions. The full activity observed during the intrusion has been mapped to the MITRE ATT&CK framework below for reference.
## MITRE ATT&CK

<table>
<thead>
<tr>
<th>Tactic</th>
<th>Technique</th>
<th>Technique ID</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initial Access</strong></td>
<td>External Remote Services</td>
<td>T1133</td>
</tr>
<tr>
<td></td>
<td>Valid Accounts: Domain Accounts</td>
<td>T1078.002</td>
</tr>
<tr>
<td></td>
<td>Trusted Relationship</td>
<td>T1199</td>
</tr>
<tr>
<td><strong>Execution</strong></td>
<td>Command &amp; Scripting Interpreter: PowerShell</td>
<td>T1059.001</td>
</tr>
<tr>
<td></td>
<td>Command &amp; Scripting Interpreter: Windows Command Shell</td>
<td>T1059.003</td>
</tr>
<tr>
<td></td>
<td>Inter-Process Communication: Component Object Model</td>
<td>T1559.001</td>
</tr>
<tr>
<td></td>
<td>Native API</td>
<td>T1106</td>
</tr>
<tr>
<td><strong>Persistence</strong></td>
<td>Scheduled Task/Job: Scheduled Task</td>
<td>T1053.005</td>
</tr>
<tr>
<td><strong>Defense Evasion</strong></td>
<td>Obfuscated Files or Information: Software Packing</td>
<td>T1027.002</td>
</tr>
<tr>
<td></td>
<td>Process Injection: Portable Executable Injection</td>
<td>T1055.002</td>
</tr>
<tr>
<td></td>
<td>Process Injection: Process Hollowing</td>
<td>T1055.012</td>
</tr>
<tr>
<td></td>
<td>Deobfuscate/Decode Files or Information</td>
<td>T1140</td>
</tr>
<tr>
<td></td>
<td>Impair Defenses: Disable or Modify Tools</td>
<td>T1562.001</td>
</tr>
<tr>
<td><strong>Credential Access</strong></td>
<td>Exploitation for Credential Access</td>
<td>T1212</td>
</tr>
<tr>
<td></td>
<td>OS Credential Dumping: LSASS Memory</td>
<td>T1003.001</td>
</tr>
<tr>
<td></td>
<td>OS Credential Dumping: NTDS</td>
<td>T1003.003</td>
</tr>
<tr>
<td><strong>Discovery</strong></td>
<td>Account Discovery: Domain Account</td>
<td>T1087.002</td>
</tr>
<tr>
<td></td>
<td>Domain Trust Discovery</td>
<td>T1482</td>
</tr>
<tr>
<td></td>
<td>Network Service Scanning</td>
<td>T1046</td>
</tr>
<tr>
<td><strong>Lateral Movement</strong></td>
<td>Lateral Tool Transfer</td>
<td>T1570</td>
</tr>
<tr>
<td></td>
<td>Remote Services: Remote Desktop Protocol</td>
<td>T1021.001</td>
</tr>
<tr>
<td></td>
<td>Remote Services: SMB/Windows Admin Shares</td>
<td>T1021.002</td>
</tr>
<tr>
<td><strong>Command and Control</strong></td>
<td>Application Layer Protocol: Web Protocols</td>
<td>T1071.001</td>
</tr>
<tr>
<td></td>
<td>Non-Standard Port</td>
<td>T1571</td>
</tr>
</tbody>
</table>