EXECUTIVE SUMMARY

MONTHLY HIGHLIGHTS

- Pulse Secure VPN vulnerabilities actively exploited in the wild
- SonicWall email security product zero days under active exploitation
- US government attributes SolarWinds campaign to Russian SVR
- Codecov supply chain breach
- Lazarus Group: Vyveva backdoor
- Facebook and LinkedIn data leaks

THREAT DATA HIGHLIGHTS

- File threats: Trojans, ransomware and exploits
- Email threats: Spam themes and prevalent malicious attachment extensions

RESEARCH HIGHLIGHTS

- ML data poisoning and Cobalt Strike DNS research

DETECTION & RESPONSE HIGHLIGHTS

- Lockbit ransomware
MONTHLY HIGHLIGHTS

PULSE SECURE VPN VULNERABILITIES ACTIVELY EXPLOITED IN THE WILD

SUMMARY

On the April 20th, 2021, FireEye released a blog post detailing the active exploitation of a newly discovered vulnerability in Pulse Secure VPNs to target the US defense industry. In the days following, various outlets reported on further targeting, including EU and Japanese defense industries.

CyberScoop reported that 24 US government agencies are currently running Pulse Connect Secure devices, with the DHS issuing an emergency directive requiring all federal agencies to run the Pulse Connect Secure Integrity Tool. Despite no confirmation that US government agencies have been directly affected by the exploitation of this vulnerability, the emergency directive suggests it is likely that CISA has observed it being exploited in at least one federal agency.

Pulse Secure is addressing vulnerabilities in the Pulse Connect Secure VPN publicly reported by FireEye’s Mandiant unit. CISA has issued an Alert on the vulnerabilities, providing technical details and urging organizations to apply the mitigations Pulse Secure has provided. Pulse Secure says the vulnerability (CVE-2021-22893) “allows a remote unauthenticated attacker to execute arbitrary code via unspecified vectors.” The company says a patch will be available in early May, and in the meantime has outlined mitigations.

Based on the CISA Alert, the threat actor is leveraging multiple vulnerabilities in Pulse Secure VPN appliances to implant webshells for further access and persistence. The currently known impacts include authentication bypass, multi-factor authentication (MFA) bypass, password logging, and longer term persistence. The threat actor has also been observed proxying their connections through residential IPs, correlating with the country of the victim to allows actor activity to blend in with normal telework user activity.

(Source: https://www.pulsesecure.net/)

According to Reuters, FireEye have witnessed at least two activity groups exploiting Pulse Secure vulnerabilities, however, one of the activity groups they assess to be operating in the interests of China-based initiatives and collections.

The activity group UNC2630’s usage of infrastructure, tooling and hands-on-keyboard behavior appear to be unique. However, UNC2630 has similar TTPs to historic intrusions FireEye has tracked which align with APT5 activity. Nevertheless, there is not enough evidence to make a definitive statement about the correlation between the two as of the writing of this report.

The Chinese government dismisses FireEye's attribution as "irresponsible and ill-intentioned,” because Beijing “firmly opposes and cracks down on all forms of cyber-attacks.”
F-SECURE’S INSIGHT

The targeting of the US government and defense industry suggest that the assessment of the threat actor being a nation state is highly likely. Moreover, given the threat actor was observed to establish persistence and gain further access that is difficult to remediate, it is highly likely the objective is cyberespionage.

Although FireEye has assessed this recent campaign and the exploitation of the newest Pulse Secure vulnerability to be aligned with Chinese interests, NSA-CISA-FBI released a joint advisory earlier in the month stating that Russian Foreign Intelligence Service (SVR) were exploiting vulnerabilities in a number of internet facing devices, including Pulse Connect Secure, specifically citing CVE-2019-11510. This much older vulnerability is still seeing active exploitation from one of the most advanced threat actors targeting Western organizations.

Therefore, organizations should be cautious of attributing all exploitation of Pulse Connect Secure appliances to the actors identified by FireEye. It is highly likely that there may be multiple actors exploiting appliances at the same time and this may cause the conflation of activity clusters in reporting.

NCC Group published statistics showing that as of the 22nd of April 2021, there were still thousands of Pulse Secure VPN servers running versions affected by CVE-2019-11510, CVE-2020-8260, CVE-2020-8243 and, as the most recent CVE is still unpatched, CVE-2021-22893. Although your organization may not have been a target of this particular campaign, nation state threat actors around the world are actively exploiting these vulnerabilities in publicly facing internet appliances. As always, F-Secure recommends patching and following mitigation guidance for the vulnerabilities discussed here.

SONICWALL EMAIL SECURITY PRODUCT ZERO DAYS UNDER ACTIVE EXPLOITATION

SUMMARY

SonicWall has issued mitigations for three zero-days affecting its email security products. FireEye discovered that the vulnerabilities were under active exploitation and disclosed the security issues to SonicWall. Attribution is unclear, but FireEye’s Mandiant unit is tracking the activity as UNC2682. The threat actor’s goals are unknown, as the attacker was unable to carry out their actions on objectives.

The three vulnerabilities are being tracked as follows:

**CVE-2021-20021** — 9.8 rating — Pre-Authentication Administrative Account Creation: A vulnerability in the SonicWall Email Security product could allow an attacker to potentially create an administrative account by sending a crafted HTTP request to the remote host.

**CVE-2021-20022** — 7.2 rating — Post-Authentication Arbitrary File Creation: A vulnerability in the SonicWall Email Security product could allow a post-authenticated attacker to potentially upload an arbitrary file to the remote host.

**CVE-2021-20023** — TBD rating — Post-Authentication Arbitrary File Read: A vulnerability in the SonicWall Email Security product could allow a post-authenticated attacker to potentially read an arbitrary file from the remote host.

According to FireEye, “these vulnerabilities were executed in conjunction to obtain administrative access and code execution on a SonicWall ES device. The adversary leveraged these vulnerabilities, with intimate
knowledge of the SonicWall application, to install a backdoor, access files and emails, and move laterally into the victim organization’s network”.

Through exploiting the vulnerabilities above, the threat actor was able to deploy a webshell to the server which had unrestricted access as it had inherited permissions of the “NT AUTHORITY/SYSTEM” account. The attacker employed an anti-forensic technique by clearing the SonicWall application log file which tracked their activity. Then, through multiple living off the land techniques, the adversary was able to dump the process memory of the server to harvest credentials in preparation for lateral movement into the victim environment.

Before the threat actor was removed from the environment, they were observed to use the publicly available WMIEXEC.PY tool to access several internal hosts, which essentially enables remote command execution via Windows Management Instrumentation (WMI). This allowed the attacker to perform initial internal reconnaissance activity prior to being isolated and contained.

This threat actor is now being tracked under the activity group moniker, UNC2682. As the attacker was unable to carry out their actions on objectives, the goal of the attack remains unknown.

Organizations running vulnerable versions of the SonicWall ES product are strongly encouraged to upgrade to the latest versions found here.

F-SECURE’S INSIGHT

Organizations running vulnerable versions of the SonicWall ES product are strongly encouraged to upgrade to the latest versions found here. The level of access exploitation of this vulnerability provides to attackers is high, with sensitive email data being exposed to the threat actor.

This is one of a number of high severity vulnerabilities in external appliances exposed as being actively exploited this year by malicious threat actors. The observable success of this focus is something that F-Secure assess is highly likely to cultivate further attention and exploitation. Therefore, it is important that organizations factor in this threat to strategic architectural decisions of their network.

US GOVERNMENT ATTRIBUTES SOLARWINDS CAMPAIGN TO RUSSIAN SVR

SUMMARY

In a geopolitically significant move on April 15th 2021, the US government formally attributed the SolarWinds campaign to the Russian Foreign Intelligence Service (SVR), known in the industry as The Dukes, APT29, and Cozy Bear. The White House briefing stated that the “U.S. Intelligence Community has high confidence in its assessment of attribution to the SVR”.

On the same day, the US Administration announced a set of measures designed to impose costs on Russian threat actors for election influence operations, for the SolarWinds compromise, and for other cyberespionage incidents. The steps taken include sanctions, diplomatic expulsions, and naming and shaming.

The SVR’s compromise of the SolarWinds software supply chain gave them the ability to further compromise over 18,000 vulnerable machines worldwide. Whilst not every vulnerable machine was a target in this cyberespionage campaign, it highlights the risks posed by Russia’s efforts to target organizations through supply chain exploitation.

The National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the FBI jointly released a Cybersecurity
Advisory attributing the SolarWinds campaign to Russia’s SVR. The advisory titled, “Russian SVR Targets U.S. and Allied Networks,” provides specific details on software vulnerabilities the SVR uses to gain access to victim devices and networks. The advisory also provides specific steps that network defenders can take to identify and defend against the SVR’s malicious cyber activity.

Organizations are urged to patch against the following five vulnerabilities being exploited by Russia’s SVR:

- CVE-2018-13379 Fortinet FortiGate VPN
- CVE-2019-9670 Synacor Zimbra Collaboration Suite
- CVE-2019-11510 Pulse Secure Pulse Connect Secure VPN
- CVE-2019-19781 Citrix Application Delivery Controller and Gateway
- CVE-2020-4006 VMware Workspace ONE Access

Actions to take off the back of this advisory can be found [here](#). Furthermore, CISA have released in-depth details covering the TTPs they have observed the SVR to employ.

F-SECURE’S INSIGHT

This level of public attribution from the US government to foreign intelligence service activity is historically and geopolitically significant for multiple reasons. First, it is an international norm for nation states to keep intelligence on foreign services classified or shared in strict partnerships, like Five Eyes. For the current administration to publicly share this level of detail on the visibility they have into the SVR marks a significant deviation from this norm, and the previous Trump administration.

Second, this level of public attribution is part and parcel of the capacity building effort to define rules and international norms for cyberspace, where it appears the US is taking the stance that software supply chains are out of bounds and will result in public naming and shaming, diplomatic expulsions and sanctions. And third, it is incredibly rare for private cybersecurity organizations to get true attribution for malicious cyber activity they have been tracking under distinct monikers such as The Dukes or APT29.

Governments have significantly more telemetry and coverage of nation state cyber activity than private companies. Equipped with this understanding, organizations can now better defend their assets and networks with an understanding of the SVR’s targeting, objectives and TTPs.

Lastly, whilst the US government has connected The Dukes, APT29 and Cozy Bear to SVR, the private sector has been tracking this activity under the names NOBELIUM, UNC2452 and DarkHalo. This does not mean that the tracking of this campaign was incorrect, but rather, defines a very specific set of behaviors that are distinct from other activity that was previously attributed to APT29 or The Dukes.

This could be for a multitude of reasons, but the most likely explanation is that there are multiple operational teams operating within the SVR, all with different intelligence requirements and objectives. This would ultimately result in and reflect the differing *modus operandi*. Joe Slowik produced the following great diagram connecting private sector activity tracking to real world organization attribution.
CODECOV SUPPLY CHAIN BREACH

SUMMARY

Codecov, a company that builds software auditing tools for developers, was breached on April 1st. This breach has been described in press reports as a supply chain attack likened to that of SolarWinds because the incident gave attackers access to several Codecov clients.

According to Bleeping Computer, Codecov became aware of the problem on April 1 when customers notified them that they had spotted suspicious activity. The attackers seem to have been active since January, when they began stealing developers’ credentials.

Codecov has published a security update with remediation advice and a history of how the incident unfolded. The announcement stated that on April 1st, they discovered someone had gained unauthorized access to the Bash Uploader script and modified it without permission. The actor gained access due to an error in Codecov’s Docker image creation process that enabled them to extract the credential required to modify the Bash Uploader script.

The company says it has since secured and remediated the affected script and undertook an investigation with the support of a third-party company. Early results of these investigations found that there were periodic unauthorized alterations to the Bash Uploader script by a third party beginning in late January, which enabled the threat actor to potentially export information stored in users’ continuous integration environments. This information was then sent to a third-party server outside of Codecov’s infrastructure.

(Source: https://twitter.com/fslowik/status/138280679172411843/photo/1)


On the 29th April Codecov began informing maintainers of software repositories affected by the supply chain attack confirming they believe these repositories were downloaded by threat actors. The repositories listed under a user’s account that were impacted now show a security
warning. They also updated their security update to contain multiple IOCs related to the attack.

Codecov says three categories of data and services are potentially affected:

- Any credentials, tokens or keys that our customers were passing through their CI runner that would be accessible when the Bash Uploader script was executed
- Any services, data stores and application code that could be accessed with these credentials, tokens
- Or keys and the Git remote information to Codecov in CI

It is recommended all users reroll all their affected credentials, tokens and keys located in the environment variables in their CI processes that used one of Codecov’s Bash Uploaders.

**F-SECURE’S INSIGHT**

The Codecov incident reinforces the trend that supply chain attacks will grow in frequency as organizations become increasingly reliant on third party software vendors for specific functions. It serves as a reminder that organizations should weight the risk involved when using third party services such as Codecov.

F-Secure recommends organizations:

- Select third party vendors carefully, treat them as part of your organization when performing security audits and only grant necessary accesses and keep levels of access under regular review
- Ensure all configurations are verified, particularly when deploying anything over cloud applications or when making them publicly accessible to prevent unintentional leaks or exposing sensitive information
- Review or limit what is shared with third party software, especially if that contains credentials or otherwise sensitive data
- Do threat modelling exercise to consider third-party access and how it can be abused, then consider what measures you can put in place to limit the damage of an attack
- Have a planned response, organize simulations to practice all aspects of your response (technical, legal, communications)
- Have backups and response plan for when breaches such as this are discovered

**CISA Report: Defending Against Software Supply Chain Attacks**

For a more detailed assessment of the risk software supply chain risk, the US Cybersecurity and Infrastructure Security Agency (CISA) published a report this month advising organizations on how to defend against software supply chain attacks. The report provides an overview of software supply chain risks and recommendations on how to use the National Institute of Standards and Technology (NIST) framework, Cyber Supply Chain Risk Management (C-SCRM) framework and secure Software Development Frameworks to identify, assess and mitigate risks.

LAZARUS GROUP: VYVEVA BACKDOOR

**SUMMARY**

ESET researchers discovered a new backdoor they attribute with high confidence to the Lazarus Group. The new backdoor, they have called Vyveva, was identified during an investigation into an attack against a South African freight logistics company. ESET published a blog post containing technical analysis of Vyveva’s components. They assess Vyveva
shares multiple code similarities with older Lazarus samples detected by ESET such as NukeSped malware family. Other similarities include the use of fake TLS in network communication, command lines execution chains and use of encryption and Tor services all match with Lazarus TTPs.

**MalwareBytes** further identified new TTPs deployed by the Lazarus Group this month, in which the North Korean group used a technique to bypass security products by embedding one of its payloads as a BMP image.

**Group-IB** published an article on the 14th April that identified Lazarus group using JS sniffers for the first time that they have redesigned to steal crypto currency. This previously undocumented campaign marks the first time the group has used malicious JS-sniffers to steal cryptocurrency.

In July 2020, **Sansec** published an article about the attacks on US and European online shops with the use of JavaScript sniffers (JS-sniffers). These researchers attributed the “clientToken=” campaign to the North Korean APT group, Lazarus.

The Group-IB Threat Intelligence investigation further identified the Lazarus group using the same infrastructure as the “clientToken=” campaign and a modified version of the “clientToken=” JavaScript sniffer to attack online stores that accept cryptocurrency payments. Group-IB have called this new campaign BTC Changer and they attribute it to the Lazarus Group with a high level of confidence based on linking the activity to BTC addresses used by Lazarus and the group’s previous campaigns that have targeted cryptocurrency in the past.

Finally on 27 April, **Positive Technologies** published a report on Lazarus Group compromise of a large pharmaceutical company. On analysis of the threat actors TTPs the investigation team found similarities between this and other Lazarus campaigns. Of note, was the speed in which this compromise occurred, they gained partial foothold within four days. This demonstrates the high degree of preparedness of attackers and an individual approach to compromising each host on the infrastructure.

**F-SECURE’S INSIGHT**

The Lazarus Group has been active since 2009 and is an advanced North Korean Threat Actors reportedly responsible for the 2014 attack against Sony Pictures. The group is known to employ new techniques and custom toolsets in its operations to increase the effectiveness of its attacks.

In 2019, F-Secure **discovered** an ongoing global phishing campaign by the Lazarus group whilst investigating an attack against an organization in the cryptocurrency vertical. The phishing campaign associated with this attack was observed continuing into 2020 raising the need for awareness and ongoing vigilance amongst organizations in target verticals that includes cryptocurrency and potentially extending to their supply chain.
The Lazarus Group has shown a penchant for the use of a continuously evolving arsenal of custom malware in its attacks. This malware will commonly bypass more traditional signature based detections, highlighting the importance of behavioral based detection strategies to counter this threat.

F-Secure is aware of the Lazarus Group operating in South Africa historically, and therefore organizations in this country should take note of evolutions of this group’s TTPs.

FACEBOOK AND LINKEDIN DATA LEAKS

Both LinkedIn and Facebook user data was discovered by security researchers in April raising significant privacy concerns for users of these platforms. This comes at the same time as Mi5 announces widespread use by LinkedIn as a targeting platform for foreign intelligence agencies wanting to recruit UK officials and academics.

On the 3rd of April, Business Insider reported on exposed Facebook user data that was for sale on a low-level hacking forum. The leaked data included the phone numbers and personal data of over 533 million Facebook users. It included users’ phone numbers, Facebook IDs, full names, locations, birthdates, bios and, in some cases email addresses. Facebook told Insider that the data had been scraped because of a vulnerability that the company patched in 2019. This vulnerability had been widely exploited by hackers and investigators before it was patched in 2019 and so the availability of such a dataset was not big news for many within the InfoSec community.

Then just days after Facebook user’s data was discovered, Cyber News reported they discovered data from over 500 million LinkedIn users for sale on darknet forums to cybercriminals. This data included user IDs, full names, email addresses, phone numbers, professional titles and other work-related information. As with the Facebook dataset, it is not clear how old this dataset is but LinkedIn said in statement that, although the scraped data contains some “publicly viewable member profile data in it,” it is, “actually an aggregation of data from a number of websites and companies,” which suggests the threat actors compiled it with information from multiple services.

Many security researchers and privacy advocates have also dismissed the relevance of these leaks because Facebook and LinkedIn have both had user data breached in the past and many believe these datasets are reconstituted from these old scrapes or breaches. However, personal data such as this being sold to threat actors can have significant implications for victims.

As just a few days later, Mi5, UK domestic intelligence agency warned 450,000 civil servants and partners in academia and industry were the potential targets for agents of hostile states with alias profiles on social media and professional-networking sites. This just demonstrates the risk posed to individuals by data posted publicly, combined with passwords and selectors such as an email address or phone number, this information can easily be weaponized by cybercriminals or state actors targeting you or your organization.

Further, the threat actor behind the Microsoft Exchange Server exploitation earlier this year is reported to have leveraged large personal datasets during the reconnaissance stage of the breach. The theory is that the group relied on personal information that led them to the system
administrators’ email account names, either from previous hacks or scraped from publicly available social-media sites like LinkedIn.

F-SECURE’S INSIGHT

These recent events serve as a reminder that information posted in social media platforms such as job title, skills and experience, location as well as the email and phone numbers used to register these accounts and even our connections to other users can all be exploited by threat actors to conduct attacks such as SMS spam or advanced phishing campaigns.

The prevalence and availability of large datasets such as this further increase the scale and speed in which us as individuals or staff within your organizations can be identified and targeted by a threat actor looking to compromise company networks using social engineering and phishing techniques.

F-Secure has observed APT groups such as Lazarus Group using platforms like LinkedIn to target users in spearphishing campaigns in the past. The availability of data from these platforms for analysis will help this group and others to continue to leverage this platform for nefarious purposes.

Just as organizations are considering their suppliers as supply chain risks, third party platforms form another attack path for the employees of organizations; and therefore the organizations themselves. In a remote working world where the divide between corporate and personal spaces has blurred it is important that organizations look to implement controls that recognize the threat posed by these platforms.

Recommendations

- Check for affected LinkedIn or Facebook accounts by searching on an email address on Have I Been Pwned (HIBP) where both datasets have been uploaded
- Use strong passwords, do not reuse passwords and enable multi-factor-authentication where possible
- Research your own or your own online presence, what data is available that could be exploited by an adversary targeting you or your organization
- Block accessing of external third party platforms on corporate devices or networks to prevent the delivery of malicious documents to that environment
- Conduct security user awareness training and other exercises to educate employees on the use of these platforms to reduce the risk of social engineering

(Source: https://haveibeenpwned.com/)
**F-SECURE THREAT DATA HIGHLIGHTS**

**Malware types**
Comparisons to March 2020 reveal small shift in malware types. Detected ransomware families outperform worms and exploits yet are second to trojans. Generic trojans is malware that is not identified with other more specific detections such as Trojan droppers or Trojan Downloaders.

<table>
<thead>
<tr>
<th>Malware Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware</td>
<td>12%</td>
</tr>
<tr>
<td>Trojans</td>
<td>10%</td>
</tr>
<tr>
<td>Worm</td>
<td>9%</td>
</tr>
<tr>
<td>Exploit</td>
<td>7%</td>
</tr>
<tr>
<td>File Infector</td>
<td>5%</td>
</tr>
<tr>
<td>Backdoor/Bot/Infostealer</td>
<td>4%</td>
</tr>
<tr>
<td>Hacking Tool</td>
<td>4%</td>
</tr>
<tr>
<td>Trojan Downloader</td>
<td>4%</td>
</tr>
<tr>
<td>Banking Trojan</td>
<td>5%</td>
</tr>
<tr>
<td>Other</td>
<td>43%</td>
</tr>
</tbody>
</table>

**Exploits**
In April, the most prevalent exploit observed was targeting the vulnerability: **CVE-2017-11882** which is a code execution vulnerability in the MS Office family. Payloads targeting this vulnerability were consistent throughout April escalating in volume towards the end of the month.

The second most common was **CVE-2018-8653**, which is a remote code execution in Internet Explorer. This vulnerability is being exploited by malicious web sites in the wild. Third is **CVE-2013-0422**, which is another type of code execution vulnerability in MS Office.
Spam Themes
In April, the cryptocurrency theme remains strong, but the contrast is less than what it was back in March. E-Commerce is back on the leading spot for email themes. It might have been that the sharp rise in cryptocurrency prices caused quick big email campaigns, but that current peak has passed.

Malicious Email Attachments
.gz, .zip and .7z archives are the most common attachments in email. These archives contain malware of other file types and are often used to hide the actual malware from email scanning or attachment file type policies. Password encrypted archives can also be used to prevent email scanning services from unpacking the attachments. Surprisingly .rar files are not in the top 10 anymore.

Additionally, in April .doc has grown more prevalent and surpassed .xlsx files. MS Office documents are common delivery mechanism for malware in forms of additional download urls, macros or exploits.
Data Poisoning in Action

This month, Andrew Patel and Matti Aksela published a post on F-Secure LABS detailing data poisoning in machine learning applications, and how it is one of the most serious security threats facing machine learning applications. Data poisoning attacks compromise the integrity of machine learning models by injecting incorrect data in their training set. Optimal poisoning data points can be algorithmically generated by solving an optimization problem to reach both denial-of-service and backdoor goals. The article acknowledges that for this kind of attack to take place, the attacker must have sufficient knowledge about machine learning and optimization techniques, however, the authors note that several libraries are already publicly available to generate poisoning data with limited effort and knowledge.

The article goes into depth about how various machine learning models are vulnerable to attack regardless of their complexity, therefore concluding that there is no silver bullet to generically protect models against data poisoning attacks by design. The solution is to implement an additional line of defense during the training process of a model to efficiently mitigate these kinds of attacks.

For further detail and visual representation of how machine learning data models can be poisoned, read the article here.

Research to identify Cobalt Strike DNS servers or redirectors

This month, F-Secure LABS published research that focused on detections that can be used to fingerprint exposed Cobalt Strike servers that are using DNS as a communication channel. It shows many approaches that can be used to track Cobalt Strike servers exposed on the internet and can be used to enrich threat intelligence data to achieve better detections.

For red teamers and penetration testers that use either Cobalt Strike or any other C2 framework that supports DNS, this research provides an approach that can be used to build better and smarter DNS redirectors using open source tools.

A “redirector” can be used to harden the attack infrastructure and decouple what is exposed by the attacked component and the actual C2 servers. It grants the operator greater flexibility in case any of their internet-facing endpoints get “burned” during the attack.

The research showed that “redirector” setup can be validated by querying the hostname that was initially configured for DNS C2. If the setup is working properly, the DNS response will be the one configured in the dns_idle malleable profile option, and by default it’s equal to “0.0.0.0”
The Detection

The research that F-Secure conducted is based on the following:

“Cobalt Strike’s DNS listeners will reply using the value defined in the dns_idle field regardless of the query received, as long as it is not part of a C2 communication”

In fact, the dns_idle field is used by the beacon as a heartbeat to check in for new tasks. The “problem” is that the default DNS server will reply using that value to all the other queries for other domains as well.

The research confirmed the hypothesis that is that if a DNS server replies to all the queries with always the same IP address then it is possible to validate our hypothesis using a live Cobalt Strike serve.

This demonstrates one of the many approaches that can be used to track Cobalt Strike servers exposed on the internet.Whilst not perfect, this can certainly be used to enrich threat intelligence data to achieve better detections.

For red teamers and penetration testers that use either Cobalt Strike or any other C2 framework that supports DNS, we provided an approach that can be used to build better and smarter DNS redirectors using open source tools.

Visit F-Secure Labs webpage to read the full report.
INCIDENT CORNER: LOCKBIT RANSOMWARE

An F-Secure client was alerted to an event when several unresponsive servers were running at 100% CPU usage. These unresponsive servers had a production impact when staff could not access the information required from the servers.

Following an initial investigation, the client found a suspicious process running on each of the servers. After an attempt to kill the process, it automatically re-spawned. Anti-Virus (AV) and email alerts indicated the detection of password stealing software on a host connected to the primary back-office and production network. The same alert for password stealing was triggered on other servers and most of the client’s estate was encrypted by Lockbit ransomware. F-Secure’s Incident Response (IR) team were engaged to assist in the investigation.

The F-Secure IR team found a firewall misconfiguration led to an exposed virtual machine (VM) being compromised by a threat actor. This VM was the ransomware staging host and first host on which the attackers gained a foothold. They moved laterally from this host within the victim’s network before escalating their privileges to Domain Administrator and deploying Lockbit ransomware.

The investigation revealed artefacts that showed the threat actor accessed directories and files from a compromised host before the ransomware was deployed. F-Secure, however, found no conclusive evidence that any data was exfiltrated due to absence of endpoint artefacts and no evidence in firewall logs that signified the transfer of large data sets. Data exfil cannot be ruled out, however.

F-Secure Insight: Consider making using backup solution that can be isolated from your primary network, patch vulnerable software and take steps to replace or remove legacy software from your network, implement MFA for VPN users, and disable default accounts

The Lockbit ransomware attack resulted in the client loosing 4 months of data because the backup server was encrypted. This occurred because the backup server was not segregated from the primary network so it was not protected in the event of this widespread compromise. This is unfortunately a common observation in ransomware investigations, and one F-Secure highly recommends organizations look to action.

One affected server was running legacy operating system that was no longer supported creating significant security risk to the environment. The attacker further exploited a default ‘postmaster’ account during the incident, it was also possible to log into hosts using the built in Administrator account. These facts highlight the importance of ensuring basic cyber hygiene is actioned to patch systems and remove or alter default configurations and accounts that may be exploited by an attacker.
<table>
<thead>
<tr>
<th>Tactic</th>
<th>Technique</th>
<th>Technique ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnaissance</td>
<td>Active Scanning</td>
<td>T1595</td>
</tr>
<tr>
<td>Initial Access</td>
<td>External Remote Services</td>
<td>T1133</td>
</tr>
<tr>
<td></td>
<td>Valid Accounts: Default Accounts</td>
<td>T1078.001</td>
</tr>
<tr>
<td></td>
<td>Exploit Public-Facing Application</td>
<td>T1190</td>
</tr>
<tr>
<td>Execution</td>
<td>Command and Scripting Interpreter</td>
<td>T1059</td>
</tr>
<tr>
<td>Persistence</td>
<td>Create Account: Local Account</td>
<td>T1136.001</td>
</tr>
<tr>
<td>Privilege Escalation</td>
<td>Valid Accounts: Default Accounts</td>
<td>T1078.001</td>
</tr>
<tr>
<td>Credential Access</td>
<td>OS Credential Dumping</td>
<td>T1003</td>
</tr>
<tr>
<td>Lateral Movement</td>
<td>Lateral Tool Transfer</td>
<td>T1570</td>
</tr>
<tr>
<td></td>
<td>Remote Services</td>
<td>T1021</td>
</tr>
<tr>
<td>Command and Control</td>
<td>Application Layer Protocol</td>
<td>T1071</td>
</tr>
<tr>
<td>Impact</td>
<td>Data Destruction</td>
<td>T1485</td>
</tr>
</tbody>
</table>

Inhibit System Discovery: T1490