EXECUTIVE SUMMARY

MONTHLY HIGHLIGHTS

- DARKSIDE RANSOMWARE: COLONIAL PIPELINE INCIDENT
- UNC2529 GLOBAL PHISHING CAMPAIGN: A NEW TRIFECTA OF CUSTOM MALWARE
- RECORDED FUTURE REPORT ON CHINESE PLA PURCHASING FOREIGN AV PRODUCTS FOR SOFTWARE EXPLOITATION DEVELOPMENT
- JAPANESE AUTHORITIES ACCUSE CHINA OF CYBERATTACKS
- RANSOMWARE ATTACK AGAINST IRISH HEALTH SERVICES
- RUSSIAN FEDERAL AGENCIES BREACHED BY FOREIGN ‘CYBER MERCENARIES’

THREAT DATA HIGHLIGHTS

- FILE THREATS: TROJANS, RANSOMWARE AND EXPLOITS
- EMAIL THREATS: SPAM THEMES AND PREVALENT MALICIOUS ATTACHMENT EXTENSIONS

RESEARCH HIGHLIGHTS

- NEW SYSTEMBC Variant
- F-SECURE C3 FRAMEWORK AND DETECTIONS

DETECTION & RESPONSE HIGHLIGHTS

- EXPLOITING RICHFACES FRAMEWORK
MONTHLY HIGHLIGHTS

DARKSIDE RANSOMWARE: COLONIAL PIPELINE INCIDENT

SUMMARY

On Friday the 7th of May, Colonial Pipeline shut down its operations due to a ransomware attack. The pipeline shutdown led to panic buying and gasoline shortages in the South East US, as well as a state of emergency for 18 states affected by the ransomware incident. In the days following, US law enforcement made their attribution of the attack public, specifically naming ransomware group DarkSide. On May 11th, the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI published an advisory detailing the groups TTPs and providing mitigations to reduce the risk posed by ransomware attacks. On May 13th, Colonial Pipeline admitted to paying nearly $5 million in cryptocurrency to DarkSide. The US administration has since signed an executive order aimed at bolstering the federal government’s cyber defences and improving its resilience. This comes following a series of cyber-attacks against US infrastructure, spanning government, education and private industry.

DarkSide ransomware group launched as a RaaS (Ransomware-as-a-Service) gang in August 2020, and has since targeted nearly 100 organizations spanning several verticals in over 15 countries. DarkSide is a Russian-speaking ransomware threat actor assessed to almost certainly be operating out of Russia. The group runs an affiliate program, where the developers of the ransomware receive a share of the proceeds from the cybercriminal actors who deploy it.

DarkSide ransomware is written in C, designed to encrypt files on fixed or removable disks as well as network shares. The malware has persistence mechanisms built in, User Account Control bypass, PSExec, and file encryption which uses Salsa20 and RSA-1024 public key encryption. DarkSide actors have been observed gaining initial access to organizations through phishing (T1566) and exploiting remotely accessible accounts and systems, including Virtual Desktop Infrastructure (T1190 and T1133). They have also been observed using Remote Desktop Protocol to maintain persistence (TA0003). After gaining access, the threat actors deploy DarkSide ransomware to encrypt and steal sensitive data (T1486) before threatening to publicly release the data if the ransom is not paid. DarkSide primarily uses TOR for C2 communications, as well as Cobalt Strike (TA0011 and T1090.003).

The TTPs of DarkSide and their affiliates are summarized in the following graphic:

---

F-Secure.com | © F-Secure
DarkSide published a post on the 10th of May in response to the backlash stating:
“We are apolitical, we do not participate in geopolitics, do not need to tie us with a defined government and look for other our motives. Our goal is to make money, and not creating problems for society. From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future.”

F-SECURE’S INSIGHT

Shortly after the US administration’s announcement that they would pursue disruptive measures the operators lost control of its web servers and some of the funds it made from ransom payments, losing access to their blog, payment and content delivery network servers. DarkSide have since also announced that they will be closing their affiliate program and shutting down their servers.

We assess it is highly likely the threat actor behind the attack on Colonial Pipeline was an affiliate member of DarkSide given the above. Targeting a critical infrastructure company that is integral to the US economy goes directly against the group’s interests: ramifications of this incident resulted in federal action against the group and caused their operations to come to a halt. These groups are opportunistic in nature, seeking to profit and evade criminal conviction. They would unlikely take actions to deliberately attract national level investigations as this would be against the groups’ interests. As such, this supports the assessment that the attack on Colonial Pipeline was carried out by an affiliate partner whose miscalculated risk led to the DarkSide’s loss of infrastructure and intense national level scrutiny.

However, without evidence about the kind of data exfiltrated from Colonial Pipeline, there is not enough information to make a sound assessment on the intention of the DarkSide affiliated threat actor which carried out the attack. Nevertheless, given it was a ransomware attack, and the fact Colonial Pipeline paid the threat actor nearly $5 million, it suggests it was likely financial gain.

UNC2529 GLOBAL PHISHING CAMPAIGN: A NEW TRIFECTA OF CUSTOM MALWARE

SUMMARY

A report by FireEye details a widespread, global phishing campaign targeting multiple organizations across various verticals. The threat actor is assessed to be professional, capable, and well resourced, with a financial crime motivation. UNC2529 employed large amounts of infrastructure, tailored phishing lures and professionally coded, sophisticated malware. Throughout the campaign, three new malware families were identified, DOUBLEDRAG, DOUBLEDROP and DOUBLEBACK. The malware trifecta consisted of a downloader (DOUBLEDRAG), a dropper (DOUBLEDROP), and a backdoor (DOUBLEBACK).

The first wave of the phishing campaign occurred on the 2nd of December 2020, and the second wave between the 11th and 18th of December 2020. UNC2529 utilized nearly 50 different domains to conduct the campaign, including the hijacking of a legitimate third-party domain belonging to a U.S. heating and cooling services company. The group engaged in significant target research based on their selection of sender
email addresses and subject lines which were tailored to their intended victims. In one case, they created an account masquerading as an account executive for Californian electronics manufacturing company, sending out phishing emails targeting the medical industry, high-tech electronics, automotive and military equipment manufacturers, with subject lines specific to the products of the company.

The threat actors targeting was indiscriminate across industries and geographies, although due to FireEye’s telemetry, their collection bias shows a larger number of victims in the U.S. The following graphics show the 2 waves of phishing campaigns and the targeting breakdown.

The initial infection vector starts with phishing emails which contain a link to download an obfuscated JavaScript downloader payload – DOUBLEDRAG. Once executed, the malware reaches out to its C2 server and downloads a dropper – DOUBLEDROP – which exists in memory-only. This is similar functionality to the TEARDROP malware seen during the NOBELIUM campaign associated with the compromise of SolarWinds. DOUBLEDROP is a PowerShell script that contains instances of the backdoor DOUBLEBACK. The dropper works by setting up the initial connection with DOUBLEBACK to establish persistence, and proceeds to inject the backdoor into its own PowerShell process before executing it. Once this connection is established, DOUBLEBACK can begin taking commands directly from the attacker-controlled infrastructure. FireEye notes that only the downloader - DOUBLEDRAG – exists in the file system of the compromised host. The rest of the components are serialized in the registry database, making their detection more difficult for file-based antivirus engines.

FireEye’s article details IOCs and domains associated with this recent phishing campaign, including a MITRE ATT&CK mapping.

**F-SECURE’S INSIGHT**

The sophistication of UNC2529’s custom mostly fileless malware demonstrates the threat actor’s professional capabilities to carry out a successful phishing campaign. Their targets were well researched, their infrastructure was elaborate and their targeting, indiscriminate. Based on their wide-ranging targeting across geographies and verticals, FireEye’s assessment that UNC2529 is likely a financially motivated threat group is sound.

When financial crime is the motivation behind a cyber campaign, casting a wide net and establishing backdoor connections with multiple victims allows threat actors to engage in what is called, prepositioning. By prepositioning, threat actors facilitate further actions to compromise
victims and reduce the cost of losing access to a particular victim. Although there is currently no evidence of further actions carried out by UNC2529, they have put themselves in the position to carry out attacks which could take the form of ransomware, business email compromise, cryptocurrency mining, botnets, or others.

RECORDED FUTURE REPORT ON CHINESE PLA PURCHASING FOREIGN AV PRODUCTS FOR SOFTWARE EXPLOITATION DEVELOPMENT

SUMMARY

Recorded Future’s Insikt Group published a report on procurement documents from a Chinese People’s Liberation Army (PLA) website detailing the purchase of Western antivirus products. The procurement documents list a contact address associated with Unit 61419 of the PLA Strategic Support Force. The products listed included antivirus software by McAfee, Kaspersky, Norton, Avira, BitDefender, and Symantec. They also found purchase documents for telecommunications technology, including CISCO routers.

The report assesses PLA Unit 61419 is purchasing these products to build malware that can bypass detections and identify software vulnerabilities to exploit for initial access. Recorded Future notes China has demonstrated a pattern of software supply chain exploitation in multiple cyber intrusion campaigns in the past. This includes Avast CCleaner in 2017, Tick Group exploited zero-days in Trend Micro’s Apex One and OfficeScan XG in 2019, and this year HAFNIUM group exploited four zero-days in Microsoft Exchange, known as the ProxyLogon vulnerabilities.

Unit 61419 is a bureau under the PLA Strategic Support Force which is responsible for foreign SIGINT and other cyber operations with a regional focus on Korea and Japan. Recorded Future assesses the purchase of western cybersecurity products by the unit to be notable because they were for English-language products rather than Chinese-language products. The latter being more suitable for legitimate use or to test exposure of private and commercial end-users in China to vulnerabilities in foreign antivirus software. Furthermore, since August 2014, China’s Central Government Procurement Department has excluded Kaspersky and Symantec from a list of approved information security software providers.

F-Secure also notes that in 2019, the Chinese government removed all foreign computer equipment from its offices, adding strength to the argument these products were not for legitimate government use.

Recorded Future provides two scenarios in their assessment of how the PLA would be exploiting foreign antivirus software:

- For PLA affiliated APT groups to use this software as a testing environment for their own natively developed malware.
- For PLA cyber units to reverse engineer foreign AV products and identify previously undisclosed vulnerabilities.

They link this activity with past campaigns where China has successfully demonstrated the capability to exploit vulnerabilities in foreign antivirus software that appear on this list. Other western AV products compromised by the group include Avast CCleaner, Trend Micro’s Apex One and OfficeScan XG enterprise security products and McAfee Total Protection AV software. Reporting shows that threat actor Tick group which is associated with Unit 61419, took advantage of zero-days in Trend Micro’s Apex One and OfficeScan XG AV in attacks that took place just months after Unit 61419 purchase of these products.
Recorded Future recommends the brands and products identified in their report be monitored for future exploitation with a focus on adversarial simulations, penetration testing, patching known vulnerabilities, and monitoring anomalous traffic related to these products.

**F-SECURE’S INSIGHT**

Chinese APT groups have been increasingly leveraging software vulnerabilities as a vector for initial access. The recent HAFNIUM attacks that exploited zero-day vulnerabilities in Microsoft Exchange servers is the most recent demonstration of that. Recorded Future’s report provides context to the operational activity of Chinese PLA operations to develop capabilities that exploit software supply chain vulnerabilities as a vector.

**SUMMARY**

In an unusual step, a Japanese police chief officially identified China as being responsible for a cyberattack against Japan. Two days after this [announcement](https://www.recordedfuture.com/china-pla-unit-purchasing-antivirus-exploitation/) the Tokyo police department filed a case against a Chinese systems engineer and former Chinese Communist Party (CCP) member, for allegedly taking part in cyberattacks against the Japan Aerospace Exploration Agency (JAXA), Mitsubishi Electric and 200 other Japanese companies and research institutes in 2016 and 2017.

The police report attributes these attacks to Chinese threat actor Tick group (BRONZE BUTLER, REDBALDKNIGHT). This attribution is based on what they claim is credible evidence, including testimonies of the suspects and other parties involved.

The police discovered a suspicious server that they monitored and detected an attack against JAXA. The attacker was attempting to exploit a zero-day software vulnerability in JAXA’s security software. They
identified the man responsible for purchasing the server used in the attack and brought him in for questioning.

The suspect was an IT systems engineer and Chinese Communist Party (CCP) member and has since left the country. Separate reporting reveals he was working for a state-owned telecoms company and suspected of being involved in attacks against around 200 companies and research institutions and is linked to the Chinese threat actor Tick because he shared a server and other information used by the group.

**F-SECURE’S INSIGHT**

Evidence in this report demonstrates the Chinese threat actor - Tick group - is deploying CHIS (clandestine human intelligence sources) to purchase legitimate infrastructure under aliases in support of computer network exploitation (CNE) operations. They have the funding and capability to develop their own malware and have access to digital certificates to sign its own malware when needed. This demonstrates all the hallmarks of an advanced cyberespionage group.

This high-profile exposure of Tick group activity by Japanese authorities combined with Recorded Future’s reporting on Unit 61419 will likely result in these Chinese PLA linked groups shifting their TTPs and tradecraft to limit compromise of future operations. However, we recommend organizations within target sectors (Japanese government, biotechnology, electronics manufacturing, industrial chemistry, technology, media, and broadcasting industries) remain cognizant of the risk this threat actor pose to their networks.

**RANSOMWARE ATTACK AGAINST IRISH HEALTH SERVICES**

Earlier this month, a cyberattack against Ireland’s health system paralyzed the country’s health services for a week, cutting off access to patient records, delaying Covid-19 testing, and forcing cancellations of medical appointments.

A ransomware group deployed the use of Conti ransomware to encrypt data at Ireland’s publicly funded health care system, the Health Service Executive (HSE) and Department of Health (DoH). While the DoH was...
able to minimize damage caused to its operations, the attack forced the HSE to shut down its entire IT system. This caused cancellations of patients’ appointments for radiation treatments, MRIs, gynecological visits, endoscopies and other health services. Health authorities also said the attack caused delays in Covid-19 test results, but the vaccine appointment system was still working.

The Irish Prime Minister made it clear that they would not pay the $19,999,000 demand to prevent patient’s personal data being released. The threat actor then released a decryption tool free of charge to the HSE and warned they will still sell or publish the stolen private data if a ransom of $19,999,000 is not paid. Since then, patients have started to receive unsolicited phone calls from individuals with access to their personal data and pretending to be from medical organizations. The Financial Times located samples of patient data on the Dark Web and have since verified it is from the HSE breach.

Days after the attack, the FBI revealed the Conti ransomware gang had also attempted to breach network of over a dozen US healthcare and first responder organizations. Targets of these attacks included law enforcement agencies, emergency medical services, 911 dispatch centers and municipal governments. The report claimed the healthcare and first responder networks were among the more than 400 organizations worldwide victimized by Conti, over 290 of which are in the US.

Conti ransomware is a private Ransomware-as-a-Service (RaaS) operation believed to be controlled by a Russian-based cybercrime group known as WIZARD SPIDER. It is being deployed as part of WIZARD SPIDER’s Big Game Hunting (BGH) campaigns. Additional features, obfuscation techniques and code changes are added on a weekly basis:

- In August 2020, Conti’s technique shifted from fully encrypting files with AES-256 to a more strategic approach of selectively encrypting files with the ChaCha stream cipher.
- Conti’s host discovery and network share targeting functionality has also evolved and is comparable to that of Ryuk ransomware also deployed by WIZARD SPIDER and its affiliates.
- Portions of Conti’s source code are restructured or rewritten regularly with the intention of avoiding detection and disrupting automated malware analysis systems.
Ransomware groups such as WIZARD SPIDER continue to operate with relative immunity in Russia, where government officials rarely prosecute cybercriminals and refuse to extradite them. In response to the Colonial Pipeline episode last week, President Biden said Russia bore some responsibility for ransomware attacks because cybercriminals operate within its borders.

On the 12th May, the Whitehouse issued an executive order aimed at strengthening US cybersecurity defenses in response to a series of cyberattacks against private companies and federal government networks over the past year including the high profile SolarWinds incident that targeted US government organizations last year. An attack that has been attributed to the Russian SVR by CISA and the FBI.

**F-SECURE’S INSIGHT**

The attacks come on top of a similar ransomware attack on Colonial Pipeline, the American pipeline operation that shut down its pipeline operations because of a ransomware attack by DarkSide group. Colonial Pipeline agreed to pay its extortionists $5 million.

As with the Colonial Pipeline incident, the threat actors fell victim to their own success as the scale of impact escalated response and remediation to a national level investigation placing intense scrutiny on the threat actors involved.

Tightening of government policy and more concerted responses to cyber-attacks will not prevent ransomware attacks happening. However, they will result in further changes to the modus operandi of ransomware groups to evade detection and force them to shift their targeting as they try to avoid national level responses and investigation, as was the case with DarkSide and the Colonial Pipeline attack.

**SUMMARY**

A report from the National Coordination Center for Computer Incidents - NKTsKI- in Russia (the FSB’s CERT-like organization) was published, claiming that professional ‘cyber mercenaries pursuing the interests of a foreign state’ carried out a series of attacks against the federal executive authorities (FOIV) of the Russian Federation.

The attacks were identified in 2020 and formed the basis of the joint report between Rostelecom-Solar – a cybersecurity division of Russian telecom player Rostelecom – and NKTsKI, the CERT created by the Russian Federal Security Service (FSB) in 2018. The report did not directly attribute the attack to any foreign nation state, and neither of the organizations have made attribution public as of the writing of this report. Nevertheless, they assessed that the level of malware deployed, and the tactics observed suggested the group had significant professional experience and were operating in the interests of a nation state. This assessment is likely based on the kinds of information the attackers accessed and stole.

The report claims that the attackers’ objectives were to completely compromise the IT infrastructure of the federal agencies and to steal confidential information. This included documents from protected network segments and email correspondences of key federal executive authorities. The attackers managed to collect confidential information from all sources of interest, including mail servers, electronic document management servers, file servers and workstations of managers with seniority.
The three main attack vectors the attackers exploited were:

- Spearphishing
- Exploiting public vulnerabilities in web applications
- Compromising the infrastructure of key government contractors with trusted relationships to the Russian federal agencies.

Through the exploitation of these vectors, the attackers targeted administrator accounts with high privileges to infrastructure systems. They deployed fileless malware, legitimate utilities and demonstrated an intimate knowledge of the security tools present on Russian government systems.

Two novel malware strains were identified in the attacks, named *Mail-O* and *Webdav-O*, both stealthy backdoors used to execute commands and exfiltrate data. Both strains exfiltrated data to C2 infrastructure located in Russia, uploading data to Mail.ru cloud servers and Yandex.Disk cloud servers, respectively. Interestingly, both malware strains were designed to bypass Kaspersky antivirus software, which is commonly found on Russian federal networks.

**F-SECURE’S INSIGHT**

The assessment that the threat actor behind these series of attacks is an attacker operating in the interests of a foreign nation state aligns with the actions observed throughout the campaign. The actions on objectives included a wide array of cyberespionage tactics. By targeting mail servers, key figures in federal executive bodies and exfiltrating sensitive protected data, the attackers were able to collect intelligence on Russian federal activities.

Traditionally, when an attacker is observed to be gathering intelligence, and exfiltrating sensitive data directly from government networks, it tends to be a nation state threat actor. The primary reason for this, is that there is no direct financial gain or motive behind carrying out the attack.

Moreover, the threat actor demonstrated a desire to remain undetected for a prolonged period. Through disguising their network traffic as legitimate communications from Russian cloud applications, it makes it appear as normal activity. Not only that, but the malware the threat actor deployed was designed to bypass Kaspersky antivirus. Developing this capability to bypass a vendor’s commercial product takes significant resources and time. In all stages of this campaign, the threat actor’s *modus operandi* was to remain undetected. Increasing the time it takes for a cyberespionage operation to be detected allows the attacker more dwell time to collect and exfiltrate valuable intelligence.

The report was released with little fanfare on a Russian news site and gained little traction in the press until it was picked up by Recorded Future more than a week later. Some reporting has questioned the motivations for Russia in openness releasing details of this attack that exposes vulnerability in their government networks and native cybersecurity products. However, the release of this report comes a month after the U.S. and UK government formally attributed the SolarWinds attack to a cyberespionage operation carried out by the SVR. As such, it should be viewed in context of broader US-Russian posturing over cyberespionage activity. Although Russia made no attribution to a nation-state at this stage, we cannot rule such an announcement in the future.
Malware types
In May, out of the identified malware types, Ransomware, Worms and Exploits are the most prevalent in the wild malware.

Generic trojans contribute to the most noise on the internet.

Exploits
The top 3 observed CVEs remain the same with small variations in numbers. 2017-11882 and 2018-0798 are vulnerabilities in Microsoft office applications providing code execution for the attacker. 2018-8653 is a vulnerability affecting Internet Explorer versions 9, 10 and 11.

These three are commonly used in phishing attacks and malicious websites. Organizations should ensure their office applications and web browsers are patched with the latest security patches.
Spam Themes

In May 2021, cryptocurrencies saw two significant spam campaigns during the 13th and 24th which contributed to the dominance in crypto themes. The campaigns seem to be loosely tied to the cryptocurrency price where big trend reversals cause spam campaigns.

Apart from E-Commerce and Cryptocurrency, spam has been seen growth in May.

The majority of the financial related spam contain phishing documents and are themed as account statements from banks, luring users to open the attachments.

Cryptocurrency spam

Comparisons of BTC price and observed volumes of cryptocurrency related spam over May 2021 suggest loose connections between market trend reversals.

Most of the spam are advertisements for investing into cryptocurrencies.
This month, Callum Roxan and Sami Ruohonen published a blog post detailing findings from an incident where a new SystemBC remote access trojan variant was found. SystemBC is a remote access trojan used by ransomware operators to remotely control and operate in victim environments after gaining access to the network.

In the incident investigated, SystemBC was one of the remote access tools used by the actor along with PowerShellEmpire. The actor used benign tools and custom scripts to collect information and harvest credentials in the environment, based on the ongoing investigation and observed TTPs it was assessed that the actor is a ransomware operator preparing to deliver ransomware.

The SystemBC sample collected was protected by a wrapper utilizing process hollowing technique to execute the wrapped remote access trojan. This same wrapper is used commonly among threat actors to protect other malware payloads such as bazar loader. The sample had features distinct to previously discovered SystemBC samples but was lacking some such as the TOR capability and so was smaller in size.

The utilization of SystemBC further suggests a potential ransomware actor behind the breach based on observations from previous incidents.

F-Secure incident response was able to start the remediation of the breach and contain it before ransomware was deployed.

C3 is a Custom Command and Control platform for offensive security professionals that was first publicly released by F-Secure Labs in September 2019.

For some readers, the first time you may have heard of F-Secure’s C3 Framework was from recent news that FireEye reported. DarkSide, the ransomware syndicate had used C3 in their attack against the Colonial Pipeline earlier this month. According to FireEye, threat group dubbed “UNC2628” was employing the C3 framework to hide the origin of their network traffic, proxying Command and Control (C2) communications through the Slack API. FireEye said, “based on this actor’s other TTPs they were also likely using C3 to obfuscate Cobalt Strike BEACON traffic.”

Given media coverage of the tool we are covering what C3 is and detailing research on how to detect it.

C3 is a red team tool that enables security teams performing adversary simulation exercises and purple team engagements to demonstrate C2 or command and control capabilities that utilize ‘esoteric’ command and control channels. That is command and control channels through social media and other cloud services that are increasingly being used by threat actors to hide malicious activity within legitimate traffic. Examples of legitimate services that have been used in real world attacks include Outlook, Instagram, Google Drive, Photobucket, and Telegram.
C3 extends other red team tooling such as COTS Cobalt Strike product enabling red teams to concern themselves with only the C2 they want to implement and rely on C3 and CS tooling to take care of the rest.

The first proof of concept of C3 was presented at BlueHat v18 by William Knowles and Dave Hartley. Since then, it has been refactored and some aspects reimagined into what it is today by a team of developers heavily influenced by members of the MWR Red Team.

F-Secure Labs released detections for F-Secure C3 activity – that show it is possible to detect C3 activity if teams first baseline what ‘normal’ looks like within the chosen application or service.

In the example given, researchers discovered for ‘non-injected’ case study (where no memory injection has taken place) where C3 slack module was deployed there was a clear difference in the variation of DNS requests: C3 slack module heavily utilized the “slack.com” DNS query and occasional requests were also made to “files.slack.com”.

Alternatively, when analyzing legitimate slack executables there was a clear difference in the variation of queries. From a detection point of view the difference in DNS queries used by legitimate Slack executables and the C3 Slack module presents a method of detection.

In the ‘injected’ case study (where memory injection has taken place) the researchers discovered it is possible to identify differences in network connections made by a legitimate Slack process to the connections created by a Slack process that has been injected into by an attacker: legitimate process the connections originate from the main executable (slack.exe). Whereas when an attacker has injected into one of the Slack executables and has been using it to beacon out to a C2 server, they found the connections originate from the ntdll.dll module instead of the core Slack executable. There was also an elevated baseline count of the number of Slack executable packets transmitted by compromised endpoints.

Get C3: C3 is open-source software maintained by F-Secure, released under a 3-clause BSD license, and is available on Github: https://github.com/FSecureLABS/C3

Tutorial on getting started: https://labs.f-secure.com/tools/c3/

F-Secure are pleased to announce that C3 now supports C2 over LDAP, adding a much-needed internal channel to C3’s arsenal: https://labs.f-secure.com/blog/introducing-ldap-c2-for-c3/

Detections: https://labs.f-secure.com/blog/hunting-for-c3/

Blog on DarkSide use of C3: https://thestack.technology/from-c2-to-c3/amp/

FireEye https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html

BlueHat presentation: https://www.youtube.com/watch?v=2O-KKLIsDqM
F-SECURE DETECTION & RESPONSE HIGHLIGHTS

INCIDENT CORNER: EXPLOITING RICH FACES FRAMEWORK

Recently F-Secure provided support in an incident involving a server running an outdated version of JBoss. F-Secure incident response was called in to investigate when the target organization had detected the breach with their endpoint detection and response solution.

A suspicious GET request towards the vulnerable server was recovered from JBOSS application logs. Upon closer inspection, this request contained an exploit for the RichFaces framework exploiting a 9.8 base score remote code execution vulnerability CVE-2018-14667. The HTTP traffic and the exploit originated from a TOR exit node which was also known for SSH scanning and brute force attacks.

The payload delivered with the exploit contained a command for a bash reverse-shell which was used to call back to the attacker infrastructure to download further payloads. The C2 in the reverse-shell was different from the infrastructure utilized during the reconnaissance and exploitation phases of the attack.

Meterpreter is an interactive shell which allows attackers to interact with victim machines, and comes standard with the opensource tool, Metasploit. The attacker used the reverse shell connection to upload a meterpreter stage 1 “reverse_tcp” payload to the exploited server. This reverse_tcp calls back to the Metasploit C2 server and retrieves instructions in shellcode format.

Further investigation shows internal reconnaissance activity by the attacker but no activity reaching towards a potential objective in the network.

F-SECURE’S INSIGHT

It is likely that the exploitation of the JBoss server has been conducted by an automated scanning and exploitation infrastructure by an unknown adversary.

It is common for various adversaries to opportunistically breach vulnerable devices online for different purposes such as gaining infrastructure for proxy/C2 servers for future operations or for selling access to others in underground marketplaces.

Vulnerable 3rd party software is among the most common initial access vectors against linux based operating systems. It is of utmost importance that organizations are aware of their public facing infrastructure and have implemented a vulnerability management process.

Even with the best practices in place, with automated solutions there can be technological problems or configuration errors, F-Secure suggests assessing organizational exposure from third party software on a regular basis.

The associated malware was studied by F-Secure’s Tactical Defense Unit and the foothold in the environment was removed after understanding the full scope of attacker activity.
## MITRE ATT&CK

<table>
<thead>
<tr>
<th>Tactic</th>
<th>Technique</th>
<th>Technique ID</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reconnaissance</strong></td>
<td>Active Scanning</td>
<td>T1595.002</td>
</tr>
<tr>
<td><strong>Initial Access</strong></td>
<td>Exploit Public-Facing Application</td>
<td>T1190</td>
</tr>
<tr>
<td><strong>Execution</strong></td>
<td>Command and Scripting Interpreter</td>
<td>T1059.004</td>
</tr>
<tr>
<td></td>
<td>Exploitation for Client Execution</td>
<td>T1203</td>
</tr>
<tr>
<td><strong>Persistence</strong></td>
<td>Server Software Component</td>
<td>T1505</td>
</tr>
<tr>
<td><strong>Command and Control</strong></td>
<td>Application Layer Protocol</td>
<td>T1071.001</td>
</tr>
<tr>
<td></td>
<td>Multi-Stage Channels</td>
<td>T1104</td>
</tr>
</tbody>
</table>