EXECUTIVE SUMMARY

“Those of you with a keen eye will have noticed that we, the MDR Threat Intelligence Team, have decided to change the name of these monthly reports to the Threat Highlights Report. This is to better reflect the purpose and contents of these reports.

These reports contain the most recent, up-to-date information from the wider threat landscape that we find are worth highlighting and sharing. It also includes some insights from the latest threat data that F-Secure collects. We hope that this monthly report contains useful information for our consumers and provides a clear picture of how the cyber threat landscape is continually developing and evolving.”

CALLUM ROXAN
Head of Threat Intelligence

FEBRUARY’S HIGHLIGHTS

- **Silver Sparrow**, a macOS malware compiled for Apple’s new M1 ARM64 chip architecture was identified infecting a large number of endpoints
- ANSSI disclosed a three-year campaign by the **Sandworm** threat actor targeting the IT monitoring software company Centreon
- A **water treatment facility was compromised** in the US and chemical levels in the water alerted after an actor gained access via TeamViewer
- CISA reported on activity by an **APT group linked to the DPRK** targeting organizations involved in the Cryptocurrency vertical
- Multiple vulnerabilities in **Accellion’s File Transfer Appliance (FTA)** exploited for data theft and extortion of victims
- **Operation NightScout**: A supply Chain compromise of gamers in Asia through BigNox’s NoxPlayer delivers surveillance related malware
- **Lazarus group targeting defense industry** with spearphishing and ThreatNeedle malware cluster to steal sensitive data
ANSSI SANDWORM INTRUSION

French agency ANSSI disclosed an intrusion campaign by the APT group Sandworm targeting users of an older, open-source version of Centreon IT monitoring software. ANSSI claims the campaign had been ongoing from late 2017 until 2020.

The threat actor had employed the use of P.A.S webshells, an open-source web shell that is widely available despite no longer being actively developed by its author. The threat actor also deployed Exaramel, a Linux backdoor believed to be used exclusively by Sandworm and relied on Command and Control (C2) infrastructure tied to Sandworm. Exaramel malware has similarities to Industroyer malware used by Sandworm in the cyber-sabotage of Ukraine’s power grid in 2016.

Despite there being concern when this attack first came to light of its supply chain implications, the company Centreon emphasized that the 15 entities that were targeted were all operating versions of the company’s software that were 5 years past EOL. Further, contrary to best practice, those targeted had their web interfaces publicly facing the internet.

SILVER SPARROW MACOS MALWARE

Red Canary discovered a new strain of macOS malware they are tracking as Silver Sparrow. The malware contains a binary compiled for Apple’s new M1 ARM64 chip architecture, which is one of the first reported for this new chip set. The malware currently lacks a feature which brings its purpose into question: a payload. There is some analysis in the industry suggesting the malware has ties to adware, but this is unconfirmed at this time.

According to Malwarebytes, Silver Sparrow had infected 29,139 macOS endpoints across 153 countries as of February 17, 2021, including high volumes of detections in the US, UK, Canada, France and Germany. In F-Secure’s own data we have been able to identify infections in the US, UK, Belgium, Canada, Germany, France, Netherlands, and Sweden.

Despite the lack of additional malicious payloads beyond the downloader, its targeting of the new M1 chip, global reach, relatively high infection rate and operational maturity suggests Silver Sparrow is a threat worth tracking due to its unique characteristics. The malware currently has capabilities to establish and maintain persistence, connect to AWS-based C2 servers and the ability to deliver a payload.
CISA ALERT AA21-042A: U.S. WATER TREATMENT FACILITY COMPROMISE

On the 11th February the Cybersecurity Infrastructure & Security Agency (CISA) released an alert (AA21-042A) after an unidentified threat actor gained access to a U.S. water treatment facility. The actor is reported to have gained access to a SCADA system through unsecured remote access software (TeamViewer).

The levels of Sodium Hydroxide (NaOH) were altered by the actor to a level that would have been dangerous to anyone who consumed that water. Fortunately, an employee at the facility noticed odd behaviour of the system in question and was able to reverse the changes made before any dangerous levels were reached. As noted by Dragos, it is likely the changes would have been also detected by the facility’s safeguards. Included in the alert are recommendations for securing remote access software, which is applicable to both corporate IT and OT environments.

The alert also contains details suggesting the exploitation of legacy (Windows 7) systems by the actor, specifically referencing vulnerabilities in Remote Desktop Protocol (RDP). There is no confirmation of the use of these techniques in this compromise, but the inclusion in this alert infers that this is likely.

CISA ALERT AA21-048A: NORTH KOREAN CRYPTOCURRENCY MALWARE APPLEJEUS

On February 17th 2021 CISA released an alert (AA21-048A) on Lazarus Group’s cryptocurrency theft campaigns ongoing since 2020. The Lazarus Group is reported to operate in the interests of the Democratic People’s Republic of Korea (DPRK). According to the advisory, Lazarus Group has targeted organizations in over 30 different countries in the past year alone using AppleJeus malware. The Lazarus Group has used AppleJeus malware posing as cryptocurrency trading platforms since at least 2018.

The malicious application has gone through various iterations, but it can operate on both Windows and Mac operating systems; appearing to be a legitimate cryptocurrency trading company, thus tricking victims into downloading it as a third-party application. In addition to infecting victims through malicious websites, Lazarus Group also uses phishing, social networks, and social engineering techniques to lure users into downloading the malware. Each variant of AppleJeus malware covered in the CISA alert essentially functions as backdoor, with RAT capabilities built into each malicious application connecting to C2 servers hosted by Lazarus Group.

This activity by Lazarus Group is consistent with activity F-Secure has observed and published on last year. Lazarus Group continues to steal and launder hundreds of millions of dollars in cryptocurrency, on a global scale to circumvent sanctions place on them by the international community.
Criminal Threats Exploiting Accellion FTA for Data Theft and Extortion

Threat actors have exploited the vulnerabilities in Accellion File Transfer Appliance (FTA), impacting organizations in Australia, New Zealand, Singapore, the UK and the US. The attackers have targeted multiple national government organizations, as well as private industry organizations across the medical, legal, telecommunications, finance, and energy sectors.

Starting in December 2020, malicious threat actors related to “CLOP^_LEAKS”.onion website have been exploiting multiple 0-day vulnerabilities in Accellion’s legacy FTA to install a novel web shell named DEWMODE. In January 2021, several organizations impacted by the web shell began receiving extortion threats from the actors threatening to publish stolen data on their website. This number continued to grow in February 2021 with organizations across the US, Canada, the Netherlands, and Singapore all recently outed on the onion site. Accellion FTA is a 20-year-old product nearing EOL. According to Accellion, 300 of their customers were running the FTA legacy servers, 100 were attacked and data was stolen from around 25.

On February 23rd, it was reported that airplane manufacturer Bombardier had their data posted on CLOP_LEAKS ransomware website following the FTA hack. Bombardier had their data shared in the leak, including design specifications for various Bombardier models and plane parts. Bombardier state that no personal data was stolen as the purpose-built FTA servers they were running were isolated from the main IT environment. They joined the cohort of other companies which had their data leaked on the website, including geo-spatial data company Fugro, tech firm Danaher, Singapore’s largest telco Singtel and US law firm Jones Day.

Operation Nightscout: Supply Chain Attack Targeting Online Gaming in Asia

Researchers at ESET have uncovered a cyberespionage supply chain attack that compromised the update mechanism of NoxPlayer. NoxPlayer is an Android emulator with more than 150 million users from the company BigNox. The research by ESET indicates that the BigNox update infrastructure was compromised and would deliver a malicious update when a user used the legitimate BigNox updater.

ESET report that the malicious update was only delivered to a very small percentage of users, suggesting the victims were specifically targeted by the threat actor. Over 100,000 of ESET’s customers have NoxPlayer installed on their computers, but only five of these were selected to receive the malicious update. The five victims were located in Taiwan, Hong Kong, and Sri Lanka. This suggests the threat actor is carefully targeting its victims.

The threat actor was observed deploying three different malware families to the victims, all with surveillance capabilities with the intent of collecting intelligence on the victims. The operation is of particular interest due to the targeting of specific online gamers for espionage motivations. The activity has been tracked since September 2020 and ESET believe is currently still ongoing.
LAZARUS GROUP TARGETING DEFENSE INDUSTRY WITH THREATNEEDLE MALWARE CLUSTER

Researchers at Kaspersky identified a campaign targeting the defense industry since mid-2020 using the ThreatNeedle malware cluster. The activity was identified targeting organizations in more than a dozen countries. The report notes that Kaspersky are “highly confident that this malware cluster is attributed only to the Lazarus group”, which is linked to the DPRK. Kaspersky were able to identify crossover between this cluster and others linked to the threat actor, notably the AppleJeus and DeathNote clusters.

The ThreatNeedle campaign used COVID-19 themed spearphishing emails to gain an initial foothold on their victims. Once the actor has a foothold they look to harvest credentials and move laterally across victim networks, targeting crucial assets in the environment. The group displayed high levels of capability and in one instance compromised an internal host in order to proxy traffic between the victim’s corporate and restricted networks. The actor used the compromised host, which had been serving as a router between the two networks, to host malware and eventually exfiltrate data from the restricted network. Kaspersky identified malware samples with the router’s address hardcoded in, suggesting that the actor was able to adapt their approach to the victim network to achieve their objectives.

Kaspersky noted that last month Google identified a cluster of activity targeting security researchers, which also used the same cluster of malware they track as ThreatNeedle.
F-SECURE THREAT DATA HIGHLIGHTS

Malware: Popular Families

- rycon
- lnkgen
- wannacry
- expkit
- downadup
- autorun
- voools
- kavala
- ippedo
- floxif
- other

Malware: Classification

- Trojan (gen)
- Worm
- Ransomware
- Exploit
- File Infector
- Trojan Downloader
- Hacker Tool
- Backdoor/Bot/Info stealer
- Trojan Dropper
- Banking Trojan
- Trojan Spy
- Phishing
**INCIDENT CORNER**

**Russian Ransomware Actor - QakBot & Cobalt Strike:** The MDR Detection & Response Team (DRT) detected the execution of QakBot malware on two endpoints as a result of users downloading a malicious excel file. The malicious excel file was accessed by the users from an internal ticketing system. A phishing email was sent to an email address that had been newly setup to enable automation for creating tickets from incoming external emails. The automation bypassed existing mail security controls and the attachments were not scanned prior to attaching. This highlights the importance of ensuring security considerations are built in to the provisioning process for new systems.

The excel file was impersonating a legitimate DocuSign file and required the user to enable macros to execute the payload. Once executed, it would download an additional malicious payload (QakBot) from an external URL to then execute with `rundll32.exe`. QakBot was then used to inject a Cobalt Strike payload into memory and establish additional C2 communication. The actor started performing network enumeration using the open source enumeration tool, Bloodhound.

The intrusion was contained before the actor could progress further, but this is linked to a cluster of activity F-Secure is tracking related to a Ransomware threat actor. F-Secure have observed this actor across multiple Incident Response engagements in recent months, indicating it is a prevalent threat.

**Ransomware Actor – Watering Hole & Cobalt Strike:** The DRT detected the execution of an in-memory Cobalt Strike payload on a single host along with other suspicious indicators. The device was quickly isolated, and the infection traced back to a malicious Zip file containing a JavaScript payload that would eventually execute a malicious PowerShell command. This command would result in the download and execution of the Cobalt Strike payload inside the memory of a legitimate process.

After the retrieval of forensic artifacts, the DRT were able to link this Zip file to a download through a web browser, and identified the site as being used as a watering hole to deliver malicious payloads to individuals interested in a particular geographic political issue.

The incident spread to a second host after the user logged in to a new machine and their roaming profile loaded a malicious persistence item that had been inserted during the initial infection. This highlights the need for the disabling of compromised user accounts during investigations and the provision of new, clean accounts, for the duration of the investigation to users. This is a common finding during many incident response engagements and a valuable lesson to build into incident response playbooks and response processes.
Phishing Prevalence: In addition to the incidents above the DRT and Incident Response (IR) teams handled several investigations this month where phishing was the root cause of the infection. These include:

- A banking Trojan installed after the interaction with a Zip archive containing a JavaScript payload
- A PDF containing a link to Google Drive that was hosting an unknown malicious payload
- A malicious .hta file bypassed email filters when compressed in a Zip archive impersonating a SWIFT update
- Various .rar files bypassed email filters and contained a heavily obfuscated .hta payload when reconstructed
- An Emotet payload delivered to a user after interacting with a malicious attachment

This highlights the continued threats delivered through this infection vector and the need for both technical security controls and user awareness of such issues.