F-SECURE THREAT HIGHLIGHTS REPORT

October 2021

F-Secure

EXECUTIVE SUMMARY

CONTENTS

FOREWORD

It is the end of October 2021, and it has been a very busy month for the publication of reports, research, and insights across the industry. We start off with our monthly highlights looking at the use of a Zero day to escalate privileges by a Chinese state-backed threat actor, before diving deep on the use of a UEFI bootkit by an unknown but highly capable threat actor linked to a long running cluster of threat activity.

As always ransomware plays a prominent role in our consciousness with this month's highlights including some eye watering statistics on the financial impact of ransomware and the prevalence of different ransomware families in the wild. We share two reports related to the prominent BlackMatter ransomware group before looking more broadly at tradecraft evolutions by different ransomware groups this month.

Lastly, we finish our highlights section by providing a brief overview of nine other notable reports encompassing vulnerabilities, state-backed threat actors and the common misconfiguration of a popular workflow management solution.

In research we highlight a privilege escalation vulnerability an F-Secure researcher found in a prominent VPN client.

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

- Callum Roxan, Head of Threat Intelligence

MONTHLY HIGHLIGHTS

MYSTERYSNAIL: EXPLOITS WINDOWS ZERO DAY

SUMMARY

Kaspersky identified exploitation of a windows privilege escalation zero day when investigating a cluster of activity they track under the moniker MysterySnail. The vulnerability was *"discovered that it was using a previously unknown vulnerability in the Win32k driver and exploitation relies heavily on a technique to leak the base addresses of kernel modules".*[1] The vulnerability was reported to Microsoft and assigned CVE-2021-40449. The exploit used by MysterySnail had debug strings from an open source exploit for a much older vulnerability, CVE-2016-3309.

The exploit was specifically written to support the following versions of Windows:

- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows 10 (build 14393)
- Microsoft Windows Server 2016 (build 14393)
- Microsoft Windows 10 (build 17763)
- Microsoft Windows Server 2019 (build 17763)

Kaspersky state that they believe the explicit identification of server OS's and their detection of the use of this exploit only on servers suggests that this exploit was developed and advertised for use exclusively on servers.

Once the exploit executed successfully it was designed to execute the "MysterySnail RAT" malware, which is described by Kaspersky as a "remote shell-type Trojan". The RAT has twenty commands implemented, providing a wide range of capability to perform execution and Command and Control (C2) functionality. The malware is quite large and has redundant data, functions and string obfuscation in order evade detection by AV static analysis engines and make manual analysis more difficult.

Kaspersky were able to link this activity to an actor they track under the IronHusky moniker, as well as other clusters of Chinese state-backed activity dating back to 2012. These links were due to code and C2 server re-use with other Chinese state backed campaigns. Within the victims Kaspersky identified IT companies, military/defence contractors, and diplomatic entities. They suggest all this activity was linked to espionage related motivations.

F-SECURE'S INSIGHT

There has been a notable amount of high-profile vulnerability exploitation in 2021 that has been attributed to Chinese nexus threat activity. MysterySnail is another good example of the amount of exploit development being employed by actors from this region. F-Secure assesses that it is likely that Kaspersky's assessment of a Chinese state backed actor being responsible for this activity is accurate based on the targeting, capability and wider intrusion motivations described.

[1] https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/

F-Secure identified additional samples (1, 2, 3) of the MysterySnail RAT on VirusTotal that have been uploaded since the Kaspersky report was released. In addition, in F-Secure's own telemetry we note that there are detections for the RAT in Malaysia, China and Korea – though some of these are likely researchers investigating these samples after the public reporting.

ESPECTER: A REAL WORLD UEFI BOOTKIT

SUMMARY

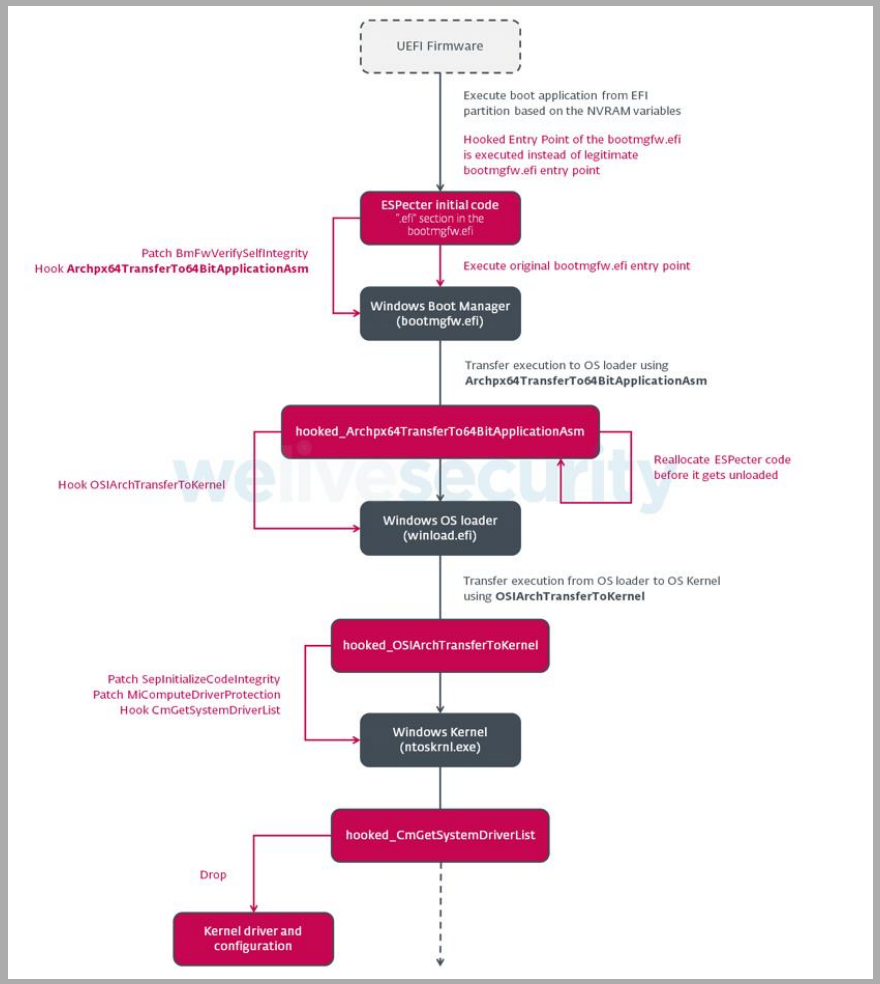
ESET have released a report detailing a previously unidentified Unified Extensible Firmware Interface (UEFI) bootkit that persists on the EFI System Partition (ESP). The bootkit, coined as ESPecter, can bypass Windows Driver Signature Enforcement to load its own unsigned driver and provide the actor with highly privileged access to the system.

As discussed by F-Secure's Connor Morley, at DEFCON 28 and in the Outerhaven Whitepaper, UEFI is an attractive attack surface for threat actors for "a number of reasons, ranging from obscurity to robust staying power. The most lucrative reason is that once on a system, the payload is largely undetectable by current systems." UEFI detection is definitely a hole for many existing security solutions, but one that vendors are starting to plug with the development of new detection capability.

ESET were able to trace the origins of ESPecter back to 2012, linking it to other bootkits for legacy BIOS systems. Kaspersky did report on another ESP based bootkit recently that they track as FinSpy, but ESET's analysis suggests that ESPecter is unique and not related to FinSpy.

ESPecter persistence is established through the modification of the Windows Boot Manager (bootmgfw.efi) and the fallback bootloader (bootx64.efi). Both these files are located on the EFI partition and the modification of these files adds a new section called ".efi" and changes the executable's entry point address to the beginning of this new section.

The new modified execution flow can be seen in the below image.

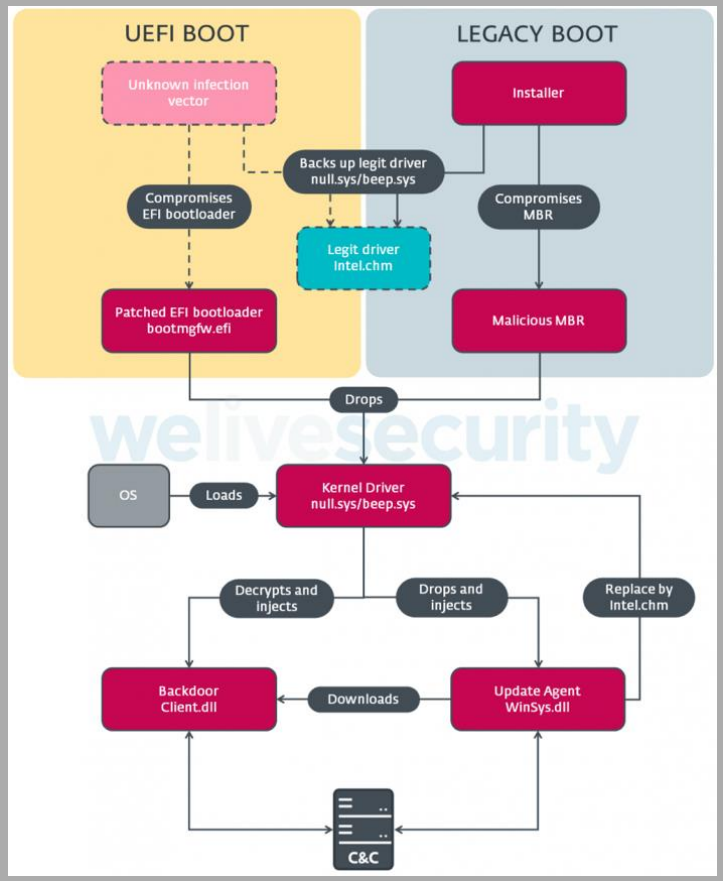


The ESET report provides detailed technical analysis of how this is all achieved to bypass operating systems checks and other security controls. F-Secure highly recommends reading the full ESET report for anyone interested in the full technical details for how this is achieved.

ESET identified multiple components related to ESPecter:

- Installers for the legacy MBR bootkit
- Boot code for the UEFI and MBR based bootkits
- Kernel-mode driver used that would enable the injection of malicious user-mode payloads into specific system processes
- User-mode payloads responsible for C2 interactions

The below image shows how these different components may interact during a compromise.



The kernel-mode driver driver's purpose is to load user-mode payloads, set up a keylogger and then delete itself to avoid detection. The keylogger is setup so that any process can then start to log intercepted keystrokes by interacting with a specific IOCTL (Input/Output Control) code.

The two user mode payloads loaded by default are "WinSys.dll" and "Client.dll". "WinSys.dll" is embedded in the driver in an encrypted form, whilst "Client.dll" is downloaded by "WinSys.dll" in an encrypted form. Both files are decrypted and written to the System32 folder by the driver. They are then injected into the memory of the system processes "winlogon.exe" and "svchost.exe" respectively.

ESET classify "WinSys.dll" as the base update agent, but both payloads have the ability to check-in with C2 servers to download or execute additional payloads and commands. In addition, "Client.dll" supports a richer range of commands that include accessing the previously described keylogging functionality, automatic document stealing and screenshots capability, execution of various commands, and the exfiltration of data to the C2 server.

Whilst "WinSys.dll" uses HTTPS communication, "Client.dll" uses TCP with single-byte XOR encryption applied to non-null message bytes that differ from the key (0x66 for the campaign ESET analysed). ESET note that each successful C2 command the result is reported back with a message that contains the wide string "WBKP" at offset 0x04, which provides a valuable detection opportunity for defenders at the network level.

F-SECURE'S INSIGHT

UEFI bootkits have been known about in theory, but there has been little evidence of real-world adoption by threat actors. This understanding appears to now be changing, as visibility in the industry improves of this attack surface, we are seeing that some actors have been operating in this space for a long time undetected. F-Secure assesses that it is likely we will see the growth of public knowledge of bootkit usage by threat actors, this may be tempered as a

valid attack surface long term with the adoption of cloud computing mediums and other mitigations for firmware level attacks.

The capabilities described heavily suggest that implants such as ESPecter are developed by state-backed threat actors due to the range of expertise required to develop the multiple components used in these attacks. In addition, the steps taken to remain undetected and preserve the kernel and bootkit capabilities from being linked to the user mode components suggest a level of operational security not commonly seen outside of state-backed threat actors. F-Secure assesses that it is likely that these types of attacks will largely remain the purview of state-based threat actors in the near future.

ESET note in their report that the user-mode client contained debug strings in Chinese but were unable to link this activity to any known threat actor. It is F-Secure's view that there is insufficient evidence to draw further conclusions from this fact as any threat actor with this level of capability and shown interest in operational security could feasibly leave false flags in their tooling.

RANSOMWARE: TRENDS AND NOTABLE REPORTS

SUMMARY

October has been a busy month for notable reporting on ransomware. We have seen the US government release trend analysis and advisories, VirusTotal release their first report on ransomware trends, and some interesting individual reports of evolutions in operational tradecraft of ransomware groups.

US Treasury Financial Trends Report

The US Treasury released a financial trend analysis report this month that concluded that there had been $5.2 billion worth of transactions tied to ransomware payments. This was the result of analysis of payments to the top 10 most popular variants of ransomware, though the report did not name these variants there are some identifying features that allow them to be de-anonymized.

In H1 of 2021 alone, which is where this report focused, the US treasury identified $590 million worth of ransomware payments. This value exceeded the entirety of the value reported for 2020 ($416 million). The report did note that these numbers should not be considered complete due to the challenges of having visibility of ransomware payments globally.

Overall, the report calculated that on average $66.4 million worth of ransomware payments are made each month and that this appears to be trending up. These figures start to put real financial values to the cost of ransomware globally and highlight why it has become the de facto pursuit for cyber-criminal groups.

VirusTotal Global Ransomware Context Report

VirusTotal released a report on analysis of ransomware samples that had been uploaded to its platform since the start of 2020. Without filtering they identified 80 million samples, but they focused their analysis on a representative 1 million samples that were reliably confirmed as ransomware. VirusTotal's analysis contained out a few interesting statistics:

- 130 different ransomware families were identified
- Israel, South Korea, Vietnam, China, Singapore, India, Kazakhstan, Philippines, Iran, and the UK are the 10 most affected territories based on the number of submissions to VirusTotal
- GANDCRAB, BABUK, CERBER, MATSNU, and WANNACRY were the five most common ransomware families by number of samples
- 95% of ransomware samples targeted Windows operating systems

The broader analysis in the report noted that whilst high profile ransomware families may come and go in waves, there is a consistent and persistent level of activity from a wide range of ransomware families ongoing. This report, like the US Treasury report, is useful for helping gain visibility into the true scale and nature of the threat posed by ransomware globally.

BlackMatter Ransomware

Cyber security and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) released an alert (AA21-291A) on BlackMatter ransomware. The alert is prompted after the ransomware was used in attacks against critical infrastructure entities in the US.

The report notes that BlackMatter uses compromised credentials to *"leverages the Lightweight Directory Access Protocol (LDAP) and Server Message Block (SMB) protocol to access the Active Directory (AD) to discover all hosts on the network. BlackMatter then remotely encrypts the hosts and shared drives as they are found."* The alert also notes that BlackMatter is a possible rebrand of DarkSide, which was a group that became notorious after the hacking of the Colonial Pipeline in the US.

The report contains other technical details, signatures, MITRE ATT&CK mapping and mitigations advice. The mitigations include common advice such as using strong passwords, Multi-Factor Authentication (MFA), keeping systems patched against the latest security vulnerabilities, and implementing controls to limit attackers' ability to spread and escalate privileges.

In another report this month related to BlackMatter, Emsisoft announce that earlier this year they discovered a critical flaw in BlackMatter ransomware. The Emsisoft researchers note that BlackMatter ransomware was almost identical to DarkSide. The flaw allowed for the decryption of any files encrypted by the applicable BlackMatter ransomware versions, and have been silently assisting victims in recovering their files without paying ransoms. Unfortunately, the BlackMatter developers have since identified and patched the flaw so that newer versions of the ransomware are not susceptible to decryption.

The blog does provide a link to contacting Emsisoft for anyone who still has encrypted files from historic BlackMatter or DarkSide intrusions, which also contained a flaw briefly.

Ransomware Tradecraft Evolutions

In three different reports this month there we noted evolutions of different ransomware groups tradecraft. First, the AvosLocker ransomware group announced they were going to auction off the data of any company that refuses to pay the ransom. This is not the first time this tactic has been used, as REvil announced the intention to do the same in June 2020, but this could inspire other groups to pursue this avenue to guarantee some financial payout from any data stolen during these intrusions.

The second report, by NCC Group, provides insight in to a threat actor they track under the moniker "SnapMC". The report describes how this threat actor operates with their entire focus on stealing data for extortion and does not deploy ransomware to encrypt victims' hosts. Notably, NCC Group detail how the group will generally have completed their attack on the victim in under 30 minutes. The report also identifies that for initial access they have observed this group scanning for multiple vulnerabilities in webserver applications and VPN solutions. These types of initial access can commonly grant highly privileged access to the threat actor and place them in a location where data may be easily accessible, enabling these types of attacks.

The third report, by KrebsonSecurity, discusses a recent announcement by the CONTI ransomware group that in addition to naming, shaming and leaking data from victims that they will also sell on access to victims to other threat actors for any organization that does not negotiate a ransom. The message itself reads as: *"We are looking for a buyer to access the network of this organization and sell data from their network"*.

The sale of access to organizations is common practice in cyber-criminal circles, with a group of actors coined as Initial Access Brokers (IABs) performing this role. However, this is the first time a ransomware actor has reported to be involved in such activity. The hosting of leak sites does provide an attack surface that ransomware groups must manage, as evidenced in the REvil case recently, so it is possible that CONTI is looking to reduce their risk and

outsource this part of their operations. The exact motivations cannot be clear, but what is clear is that any organization breached by a ransomware actor should be aware of the future risks posed by this activity and ensure proper post breach remediation is carried out to mitigate future risks of compromise.

F-SECURE'S INSIGHT

Ransomware continues to be a prevalent threat, and whilst this has been broadly known by organizations who are dealing with the aftermaths of attacks each day with victims, the true scale is now starting to be quantified. Reports, such as the US Treasury's, that start to put a financial value to these attacks do more than just grab headlines, they provide tangible evidence for policymakers to use as justification to support more active response from governments and industry.

We have started to see attitudes change and momentum begin for action and changes to be made. The recent REvil takedown and other recent law enforcement activity to bring individuals behind this activity to justice shows that it is possible to actively prevent these attacks and potentially deter others from future activity. This is not to say that the problem is solved, far from it, but the first steps are being observed to be taken to reduce the risks of ransomware for legitimate organizations.

The tradecraft evolutions highlight the continued innovation amongst ransomware threat actors to maximize their profits they get from their operations. Data extortion and monetization being a key theme broadly in 2021 for nearly all threat actors operating in this space. The focus exclusively on data exfiltration and extortion by SnapMC should be another sign to organizations that controls should not focus on ransomware detonation and instead incorporate the wider risks posed by intrusions into organization's networks. Lastly, the speed at which this group reportedly operates should be a key takeaway for any organization with regards to how this matches up against their playbooks and response capabilities.

OTHER NOTABLE HIGHLIGHTS IN BRIEF

SUMMARY

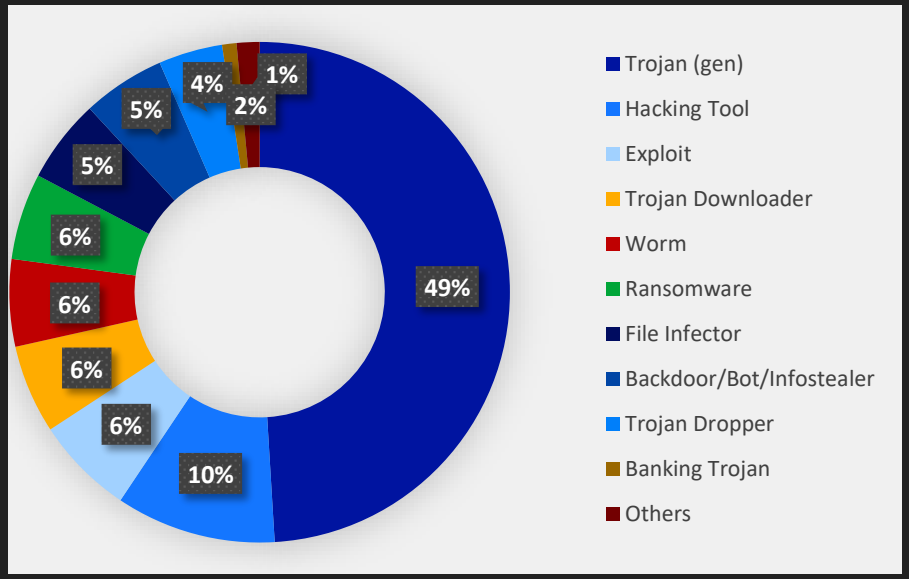
October was a busy month for interesting reporting and insights being published. While we cannot cover all these highlights in depth, we have included a brief listing of other interesting highlights from this month below:

- Google reportedly sent14,000 Gmail users notification that they had been targeted by an APT28 phishing campaign
- Syniverse, an organization responsible for routing text messages in the US has revealed a threat actor has had access to its network for five years
- The NSA revealed the dangers of using wildcard TLS certificates and how the ALPACA technique could be used to access sensitive data from organizations
- Apache revealed a critical path traversal and potential RCE vulnerability (CVE-2021-41773) that was being actively scanned for prior to public release
- Intezer identified common misconfigurations in Apache Airflow exposed sensitive credentials of many prominent organizations
- Microsoft reported the targeting of defense, GIS and maritime sectors by an Iran-linked threat actor they track as DEV-0343
- Google reported on an Iranian actor (APT35) who has been targeting high-value individuals in the UK and elsewhere to gather credentials and sensitive data
- Microsoft released another report on the NOBELIUM threat actor who has been targeting cloud, managed, and IT service providers to gain access to downstream victims
- CrowdStrike released a report on a threat actor (LightBasin) targeting organizations globally in the telecommunications industry since 2016

F-SECURE THREAT DATA HIGHLIGHTS

THREAT TYPES

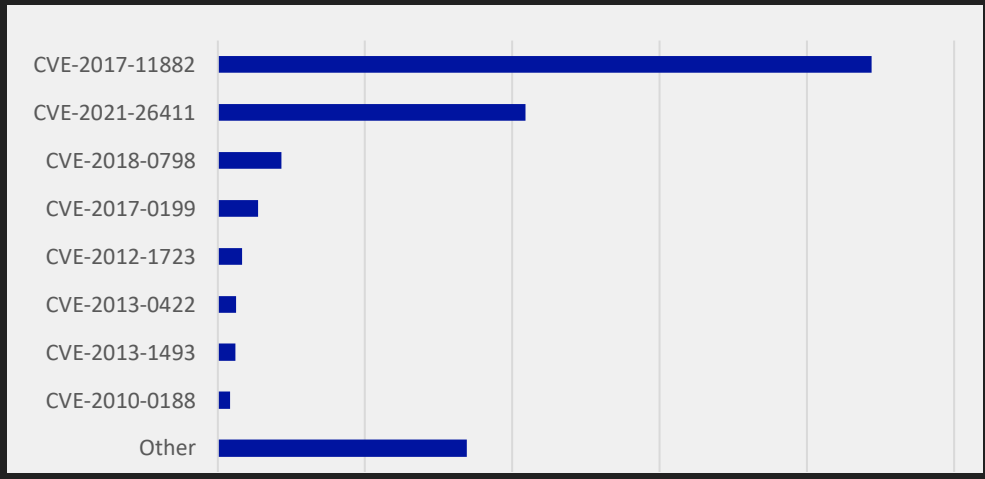
In October, out of the identified threats hacking tools, exploits and downloaders were the most common ones. Ransomware has slightly declined but remains a prevalent threat globally.



EXPLOITS

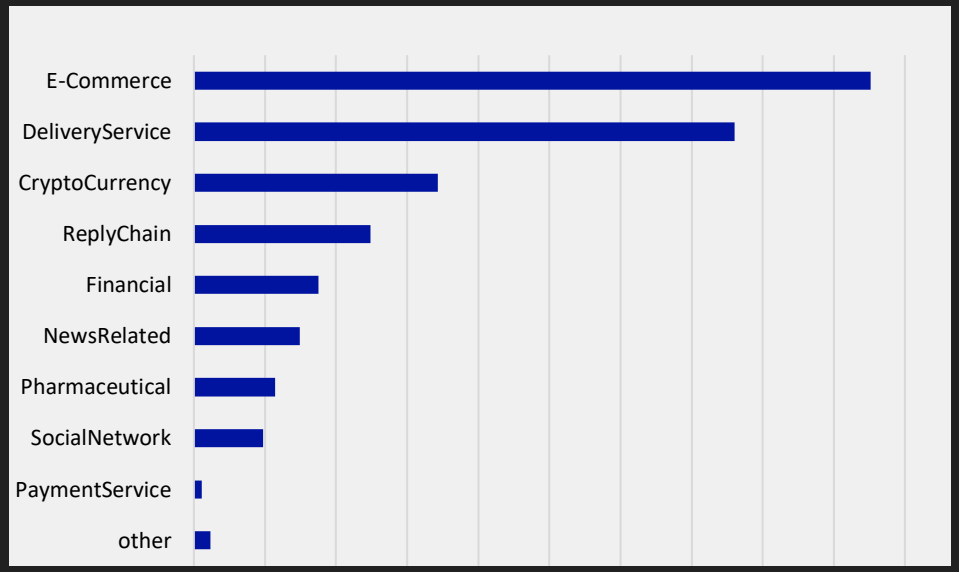
CVE-2017-11882 remains the most prevalent exploit used in the wild as detected by our endpoint protection. The exploit is most commonly detected in files such as .xlsx, .eml and .doc files. CVE-2017-11882 exploits vulnerability in MS office products and provides remote code execution for the attacker.

CVE-2021-26411 is a critical memory corruption vulnerability in the Internet explorer has gained significant popularity in since September. This vulnerability can be exploited via malicious websites and is used in the wild.



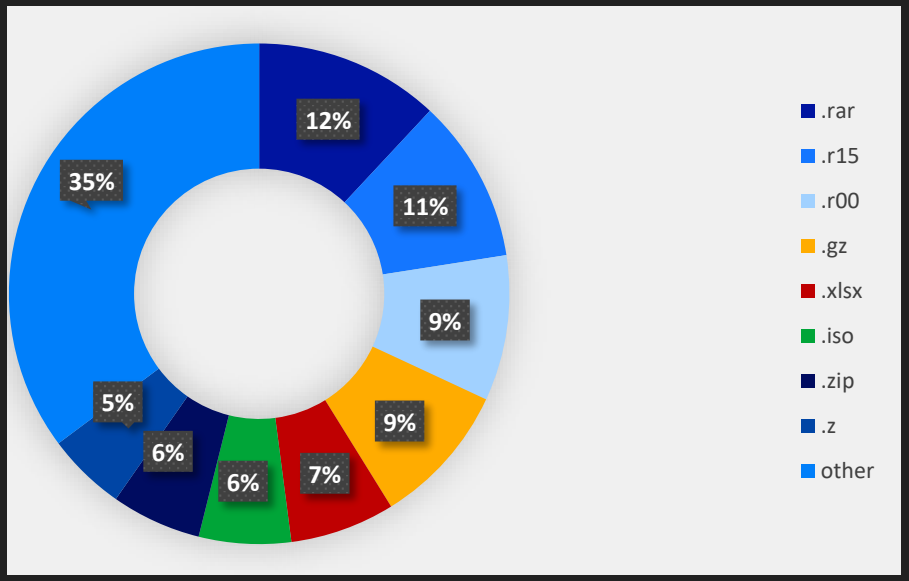
SPAM EMAIL THEMES

E-Commerce continues to dominate the spam landscape as the most popular theme. Delivery service has gained popularity while financial and cryptocurrency related spam have dropped.



MALICIOUS EMAIL ATTACHMENTS

Various archive formats are the most prevalent attachments in malicious emails. These archives contain other filetypes such as executables and document files. The following most prevalent types of attachments are various office documents which contain MS Office exploits or malicious macros.



F-Secure

F-SECURE RESEARCH HIGHLIGHTS

PALO ALTO NETWORKS GLOBALPROTECT BUFFER OVERFLOW

F-Secure's Tomas Rzepka uncovered a buffer overflow vulnerability in the GlobalProtect VPN client for Windows. The vulnerability exists in the service PANGPS that runs as SYSTEM and F-Secure confirmed its presence in versions 5.2.6 and 5.2.7, but it may have existed in earlier versions as well. Linux clients (5.3.0 and earlier) are also affected according to Palo Alto Networks.

The GlobalProtect client contains both a privileged system service (PANGPS) and a non-privileged user interface component (PANGPA). The vulnerability exists in one of the functions of the privileged component (PANGPS) that is reachable from the non-privileged component (PANGPA). When exploited it would enable a low privileged user to escalate their privileges to SYSTEM.

The most straightforward way of exploiting the vulnerability is to send the "portal" command to the PANGPS service to create a new portal configuration. Details of the communication between PANGPS and PANGPA have previously been publicly disclosed[2].

Using this information, a tool was developed that implements the custom protocol used in this communication as well as the encryption/decryption mechanisms used by GlobalProtect.

The tool is injected into the PANGPA executable (userland/GUI binary) to be able to use the existing PANGPS service communication channel. "Portal"-commands can be sent through this channel even if the client is limited by policy to add new portals. This policy only removes the specific user interface options but does not prevent the requests from being accepted by PANGPS.

By sending "portal"-command with an arbitrary portal address, PANGPS responds that the user/PANGPA needs to perform an HTTPS request to the portal address and "prelogin" authenticate to the portal. A successful prelogin request can then be forged and sent back to the service.

```
<?xml version="1.0" encoding="UTF-8" ?>
<prelogin-response>
<status>Success</status>
<ccusername>user@pwn.local</ccusername>
<autosubmit>true</autosubmit>
<msg></msg>
<newmsg></newmsg>
<authentication-message>Enter login
credentials</authentication-message>
<username-label>Username</username-label>
<password-label>Password</password-label>
<panos-version>1</panos-version>
<region>10.0.0.0-10.255.255.255</region>
</prelogin-response>
```

The XML message above is encrypted and embedded in a response to PANGPS service. PANGPS responds that the client needs to perform "getconfig" from the portal. An existing portal configuration can then be modified, here the "entry"-tag is used to demonstrate the vulnerability and 1023 "A"-characters are sent in the name property.

[2] https://www.crowdstrike.com/blog/exploiting-escalation-of-privileges-via-globalprotect-part-1/

```
<?xml version="1.0" encoding="UTF-8" ?>
<policy>
       <portal-name>PWN GP Portal</portal-name>
       <portal-config-version>4100</portal-config-version>
       <version>
                     </version>
       <client-role>global-protect-full</client-role>
       <agent-user-override-key>****</agent-user-override-
key>
       <connect-method>user-logon</connect-method>
       <on-demand>no</on-demand>
       <refresh-config>yes</refresh-config>
       <refresh-config-interval>1</refresh-config-interval>
       <authentication-modifier>
              <none/>
       </authentication-modifier>
       <authentication-override>
              <accept-cookie>yes</accept-cookie>
              <generate-cookie>yes</generate-cookie>
              <cookie-lifetime><lifetime-in-
hours>24</lifetime-in-hours></cookie-lifetime>
              <cookie-encrypt-decrypt-
cert>vpn.pwn.local</cookie-encrypt-decrypt-cert>
       </authentication-override>
       <use-sso>yes</use-sso>
              <ip-address></ip-address>
              <host></host>
       <gateways>
              <cutoff-time>5</cutoff-time>
              <external>
                     <list>
                            <entry name="vpn.pwn.local">
                                   <priority-rule>
                                          <entry
name="AAAAAAAAAAAAAAAAAAAA.....
---- snip ----
```

After sending the above response message, PANGPS crashes. When attached to WingDbg it is possible to see the stack security cookie is overwritten, which causes an exception, and the RBP (Stack Base Pointer) register is overwritten with A's. By introducing strings in the configuration that are longer than what PANGPS expects, it was possible to overflow data into the stack of the application. Developing a working exploit that uses this vulnerability to elevate privileges should be possible.

F-Secure recommends all users update Palo Alto GlobalProtect to at least version 5.2.8 to remediate this issue.

Disclosure Timeline

Date	Summary
2021-03-31	Notified Palo Alto Networks about the identified vulnerability
2021-04-08	Vendor acknowledged issue
2021-08-16	Patch released in version 5.2.8
2021-10-13	Palo Alto publishes advisory
2021-10-14	F-Secure publishes advisory

Read the full advisory here.

F-Secure®

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