Threat Highlights Report

June 2022

WITH secure

Contents

Foreword

This month's threat highlights report contains a look at several high-profile vulnerabilities in popular applications that are being actively exploited. These attacks and ongoing campaigns serve as a reminder of the expansive attack surface that applications can offer and the resourcefulness of threat actors to exploit them, whilst further substantiating the need for both a vulnerability patching process and sound detection capability.

Also included is a look at the shutdown of the prolific mobile malware Flubot, and our usual look at the ever-changing ransomware landscape.

The threat data section outlines the continued popularity of targeting vulnerabilities within the Microsoft Office suite given the ubiquity of MS office applications on corporate machines. Given the applications' importance in essential business tasks it is likely this trend will continue. Whilst the detection and response highlights section discusses how Citrix servers can be used to launch attacks.

1 Monthly highlights

1.1 Follina, an exploited vulnerability in MSDT

A vulnerability within Microsoft Windows Support Diagnostic Tool (MSDT) was recently found. It can be exploited via Microsoft Office and has been named “Follina” with the CVE number CVE-2022-30190.

Follina is being exploited by multiple threat actors as it allows Remote Code Execution (RCE), therefore facilitating system compromise. Malicious documents utilizing the exploit were first detected on the 12th of April, and has become widely adopted as an effective payload by both state-backed threat actors and cyber-criminals. The exploit has been used to deploy various malware types, including QBot, ASyncRat, and Cobalt Strike, but could easily be adapted to download and detonate any payload.

Microsoft has acknowledged the issue and has since released security updates for their products and are strongly recommending that all users install the updates.

WithSecure™ Insight

Follina is a 0-day vulnerability with the potential to cause severe consequences and allow attackers to take over a system with relative ease. While the vulnerability technically exists within MSDT (a diagnostic troubleshooting tool), it is currently being exploited through specially crafted MS Office documents. At this time examples are limited to MS Word documents (both .docx and .rtf).

Follina is easy to configure and deploy, as such it has been adapted and used by both state-backed threat actors and cyber criminals alike, with examples including its use against media organizations within Ukraine, China attacking Tibet, and the cyber-crime group TA570 using it to deploy QBot. There are numerous Follina proofs-of-concept (POC) examples available online, and the development of payloads is trivial, therefore it is highly likely that examples of Follina will persist and be used to target a wide range of targets across all sectors.

The vulnerability within MSDT allows a threat actor to abuse the remote template feature of MS Word and retrieve code, which is then executed under the same privileges as the user running MS Word. The retrieved code can run any command but is likely to be malware such as remote-access-trojans (RAT) or back doors, providing the attacker with access to the machine from which they can escalate privileges, enumerate the wider network and launch further attacks.

Microsoft released security updates for their products addressing Follina on the 30th of May, therefore there is a chance that Follina was used with some success prior to those patches being installed. It is also noteworthy that many of the payloads launched by Follina would likely be detected by endpoint detection tools, for instance, the launching of PowerShell or running of scripts.

1.2 State-backed actors target Confluence vulnerability

The team workspace and collaboration platform Confluence contains a critical vulnerability which is tracked as CVE-2022-26134 and was initially detected by the cyber-security company Volexity. On the 2nd of June Atlassian released an advisory relating to the vulnerability, which is contained within its Confluence Server and Confluence Data Center products. The advisory explains that they have released updated versions for those products which resolve the issue, but warn that the vulnerability is being actively exploited to achieve remote code execution on Confluence instances.

The Microsoft Security Intelligence team also reported that threat actors it tracks as DEV-0401 and DEV-0234 have been exploiting this vulnerability, and have detected instances of web shells, Cobalt Strike, botnets, coin miners and ransomware being deployed via vulnerable Confluence servers.

WithSecure™ Insight

This is a critical vulnerability and should be patched immediately. In cases where unpatched instances are found, those should be investigated for a breach.

The vulnerability within Confluence is an Object-Graph Navigation Language (OGNL) injection attack, an expression language for Java and the language Confluence is written in. This vulnerability allows an unauthenticated user the ability to execute arbitrary code on the Confluence instance, allowing the delivery of multiple payload types and detonation of malware.

Multiple POC exploits were released on platforms like Github and Exploit-DB at the beginning of June, and because this vulnerability may be detected through mass scanning activity using tools such as Shodan and Censys, it has become widely exploited by a variety of threat actors and used to deploy numerous types of malware, with coin miners and botnets being prevalent, but ransomware being deployed in some instances.

The presence of POC exploits has made this vulnerability trivial to exploit, and because exposed Confluence instances can be detected through scanning it has become widely exploited. The attacker sends a crafted OGNL request, which executes embedded arbitrary code. This could be used to create new users, view/delete information, or more commonly deploy web shells or malware.

Atlassian has released updates to their products that resolve the issue and recommend all users of Confluence patch their systems. This campaign has also highlighted the importance of ensuring web platforms like Confluence are not exposed to the internet and hidden behind a secure VPN.

1.3 Law enforcement takes down Flubot

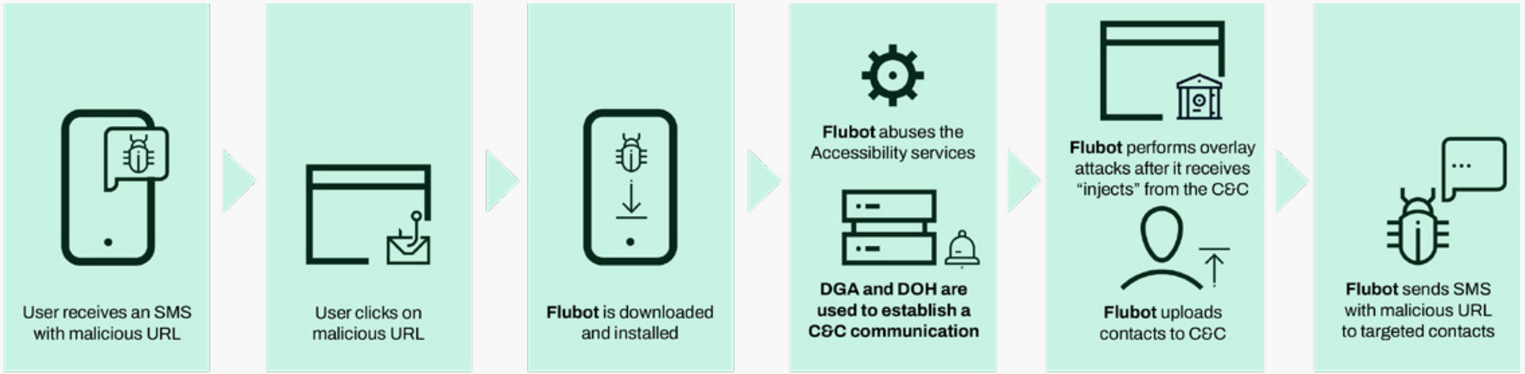
The European Union law enforcement organization Europol has headed a joint operation, along with 11 nations to take down the prolific Android malware Flubot. The mobile malware variant had become widespread throughout Europe, and was capable of stealing passwords, banking credentials and other sensitive data from victims Android devices, as well as spreading to their contacts via SMS. The infrastructure used by Flubot has been seized and is under the control of Dutch police, putting an end to Flubot and disrupting the operators' criminal campaign.

WithSecure™ Insight

Flubot is an Android malware variant that has previously been reported on and analyzed by WithSecure™, and had spread rapidly, becoming a prominent issue across Europe and has had some activity elsewhere, such as Australia.

The operators of Flubot appeared to be financially motivated, which is inferred from the data stolen by the malware, including personal data and banking credentials, as well as monitoring specific applications. The application was spread in a worm like way, with SMS phishing being the method of delivery.

Flubot follows the below attack pattern:



Injects: HTML code used in the overlay attacks to impersonate legitimate apps

DGA: Domain Generation Algorithm

DOH: DNS over HTTPS

This action by Europol and wider law enforcement is welcomed and an example of increased efforts to disrupt criminal networks. However, Flubot is just a single example of mobile malware and there are many other similar examples likely to fill the same space. The best way to avoid infection is improving user education surrounding SMS phishing and the installation of mobile anti-virus solutions.

2 Ransomware: Trends and notable reports

2.1 A look at the ransomware ecosystem

Cybersecurity company Tenable have released an excellent whitepaper on the ransomware ecosystem. The report contains insights into ransomware operators, including who those groups are, what they do and how they operate. Notably, there is a comprehensive list of commonly exploited vulnerabilities provided by Tenable, which serves as a reminder of the toolkit available to threat actors, their preferred TTPs and the importance of patch management.

2.2 LockBit is updated to 3.0

Lockbit, a nefarious ransomware group have released statements regarding an update to their locker dubbing it “LockBit 3.0”.

This includes an invitation to “*all security researchers, ethical and unethical hackers on the planet to participate in our bug bounty program*”. They are offering to pay affiliates up to $1 million in the cryptocurrency of their choice to find information to further their ransomware campaigns, including unreported vulnerabilities. This step is undoubtedly an effort by the group to generate initial access and avenues of exploitation for new targets and widen their already expansive foothold in the ransomware landscape.

2.3 An advisory on Karakurt

The US Cybersecurity and Infrastructure Security Agency (CISA) have released an advisory on the Karakurt data extortion group, a cybercrime threat actor associated with data theft and subsequent extortion. The group are a known off-shoot/partner of the now-defunct Conti and have attacked a variety of targets, with tactics, techniques and procedures (TTPs) which overlap with ransomware actors. A distinct difference is their goal of stealing a victim's data and threatening to leak it, rather than encrypting it.

The advisory includes a technical breakdown of the common vectors used by Karakurt, including vulnerabilities they are known to target, as well as tools used by the group, which include Mimikatz, Cobalt Strike, AnyDesk and Filezilla.

2.4 "Ransomware" targeting Elasticsearch

Secureworks Counter Threat Unit (CTU) have identified an unusual attack targeting unsecured internet-facing Elasticsearch hosts. The attackers appear to have targeted about 1200 vulnerable databases, wiping the data and replacing it with a ransom note, providing details on how to recover the missing data. However, as noted by Secureworks, it is highly unlikely that the attacker has retained the data, as storage would be very costly. This campaign does highlight the danger of exposing databases to the internet, and the importance of restricting access to authenticated users and how the enforcement of MFA can prevent such attacks.

2.5 The costs of ransomware to businesses

Research by Cybereason has highlighted the real-world cost of ransomware attacks on businesses, with their findings including:

- 31% of businesses were forced to suspend operations
- 40% of organizations laid off staff following a ransomware attack
- 35% of companies suffered c-level resignations following attacks

The report shows how the effect of ransomware goes beyond disruption or monetary loss and has caused substantial harm to people's livelihoods.

3 Other notable highlights in brief

3.1 Microsoft disrupts Bohrium

An Iranian threat actor tracked by Microsoft as BOHRIUM, have had legal action launched against them by Microsoft. This is an effort to disrupt BOHRIUM, who are a group linked to spear phishing and complex social engineering attacks designed to spread malware and gain initial access into victim environments.

3.2 Russia hack Ukrainian TV

It has been confirmed that Russia hacked a Ukrainian TV channel during a football world cup qualifying game between Ukraine and Wales. The attack resulted in the channel playing Russian propaganda. It serves as another example of the lengths Russia is willing to go to influence the population of Ukraine with disinformation.

3.3 PACMAN attack against M1 Macs

Researchers at the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) have released research on a novel attack technique targeting Apple devices with M1 ARM CPUs. The attack seeks to bypass pointer authentication (PAC), a security process to detect and guard against unexpected changes to pointers in memory. And has the potential to introduce a whole host of attacks to the M1 ARM architecture.

3.4 Multiple vulnerabilities in Trendnet

The NCC Group have released a technical advisory surrounding multiple vulnerabilities within Trendnet routers. Routers are often a target for threat actors seeking to create botnets and vulnerabilities such as this offer that opportunity and highlight why their firmware should be updated whenever possible.

3.5 A vulnerability in NinjaForms

A popular plugin “NinjaForms” for WordPress reportedly contains a critical vulnerability which can lead to the compromise of vulnerable websites. The developers have released patched updates for the plugin that resolve the issue.

3.6 MiVoice vulnerability exploited for initial access

A researcher from Crowdstrike has identified a threat actor exploiting a vulnerability in VOIP appliance Mitel MiVoice, which has subsequently been patched. The attacker used the exploit to gain initial access to the victim environment and attempt to deploy ransomware.

3.7 Racoon stealer is back

A popular stealer malware called “Racoon Stealer” has reportedly been updated and is being sold on dark web criminal marketplaces and forums. The operators of the malware had suspended operations due to the war in Ukraine, but have now resumed their operations.

4 Threat data highlights

4.1 Exploits

CVE-2017-11882 is a vulnerability in MS office products and provides remote code execution for the attacker, it is exploited by malicious office documents.

CVE-2017-0199 is a remote code execution vulnerability in MS Office and Wordpad exploited by a specially crafted RTF document.

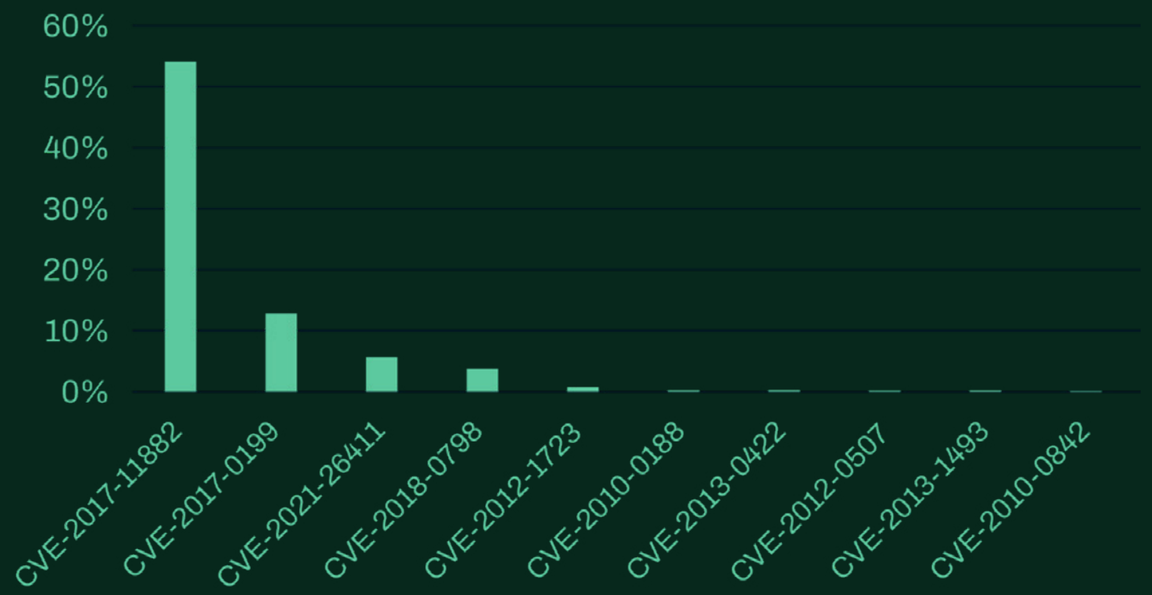
CVE-2021-26411 an internet explorer memory corruption vulnerability follows in third place. This vulnerability is exploited by malicious websites.

In June, CISA added 49 vulnerabilities into the catalog of vulnerabilities exploited in the wild. These entries are across systems and platforms such as MS Word, Adobe Acrobat, Google Chromium engine, multiple Apple products and more.

On 2nd June, an advisory on a zero-day remote code execution vulnerability in Confluence (CVE-2022-26134) was published. This vulnerability allows threat actors to remotely gain access to and execute code on a confluence server. This is a critical vulnerability which is being actively exploited in the wild.

WithSecure™ has observed this RCE to be used for delivering threats such as coinminers to vulnerable systems. This can be exploited by actors of varying capability to deliver various payloads.

Exploits in the wild



WithSecure™ endpoint protection

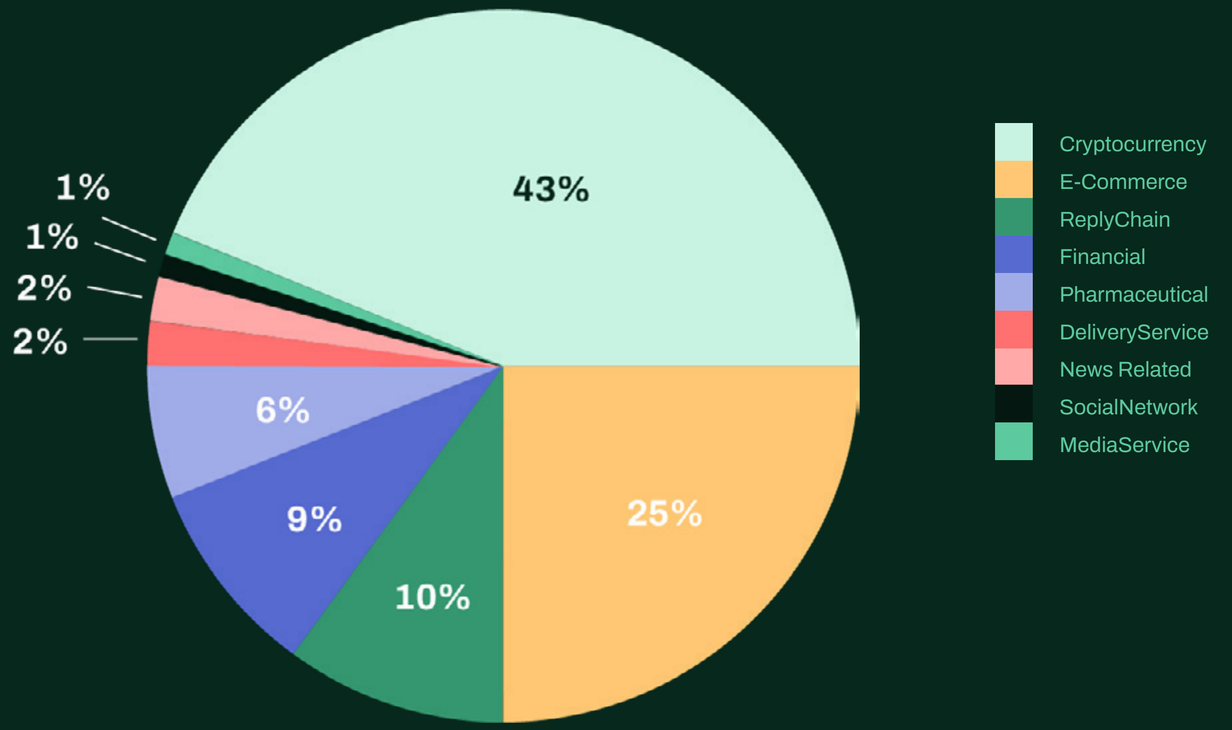
4.2 Email threats

During June cryptocurrency themed messages dominated the spam landscape. This is likely attributable to the recent big shifts in cryptocurrency prices.

E-Commerce and ‘reply-chain’ (where attackers insert themselves into legitimate conversation with stolen credentials) style email threats also scored highly.

There are no significant changes in the Ukraine email landscape. The volume of Ukraine themed spam and phishing emails remain low.

Spam Email themes



WithSecure™ spam data collection

5 Research highlights

5.1 WithSecure™ ransomware threat update

Ransomware is a type of malware that's plagued people and organizations for the last decade. From its origins as a floppy disc release demanding rather insubstantial sums of money via snail mail, the ransomware threat has grown in sophistication and scale. Increasingly large ransoms have turned ransomware into a problem with the potential to paralyze multinational corporations or critical national infrastructure relied on by millions of people.

In this report, WithSecure™ offers a brief overview of relevant observations from 2021 with the aim of providing defenders with an update on trends and developments regarding ransomware. It covers multi-year evolution of ransomware as a threat and trends in 2021 as well as an updated ransomware tube map.

Some of the key findings include declining number of new ransomware families annually since 2017 and the most popular initial access vector being malicious office documents.

Threat Update Ransomware

Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

WITH secure