Threat Highlight Report

April 2023

WITH secure

Contents

Foreword

WithSecure's monthly threat highlights report contains our own proprietary data, as well as other carefully curated sources from the wider cybersecurity industry. It is designed to serve as a single-source product, providing an overview of this month's cybersecurity news, the changing threat landscape and relevant advice.

This month we explore several new vulnerabilities exploited by a range of different threat actors related to Microsoft, Chrome, and Papercut. While less ransomware victims were posted to breach sites, Ransomware actors have still been very active, exploiting high profile vulnerabilities and targeting high profile organizations.

DDoS attacks originating from Pro-Russian hacktivists continue delivering some impact to victims, and we explore the conception that "Macs don't get Malware" by highlighting some recent threat actor malware development.

- Tim West, Head of Threat Intelligence

1 Monthly highlights

1.1 Papercut Vulnerability exploited by Ransomware Gangs

A critical vulnerability in Papercut's print management software could allow attackers to execute arbitrary code on vulnerable systems is being exploited in the wild. The vulnerability affects Papercut NG and MF versions 8.0 or 15.0, or later. The vulnerability is a remote code execution (RCE) vulnerability in the Papercut User Interface (UI). The vulnerability is caused by a failure to properly sanitize user input before it is passed to a command execution function. This allows an attacker to craft a malicious request that can be used to execute arbitrary code on a vulnerable system. It highlights how threat actors are capable and willing to target software and services that are less prevalent, seeking any possible opening. It's not just Windows, Office, VPN services and common enterprise software/services that are being targeted.

WithSecure™ Insight

At the time of writing this report, the vast majority of papercut services observable to WithSecure™ remain vulnerable. The vulnerability is under active exploitation by actors that researchers have linked to CLOP through the observed deployment of TrueBot. TrueBot deployments were also seen in the mass exploitation of the GoAnywhere vulnerability WithSecure™ reported on in February 2023. The use of legitimate RMM software has been increasingly observed by WithSecure™ in ransomware deployments, and in this case, Atera RMM has been observed in exploitation attack chains.

Other threats have been observed by researchers at Sophos, who note Bhuti ransomware, Coinminers and Mirai botnet herders have also attempted to exploit Papercut.

1.2 "Macs don't get Malware"

Lockbit are widely known as the most prolific ransomware variant, consistently posting the most victims and also demonstrating continual development of their toolkit. As part of this development, 2021 saw the first detection of the Linux variant of their ransomware and in April this year, a MacOS variant, identified as "locker_apple_M1_64", was discovered by researchers. Whilst in the developmental stages, as not only didn't this raise any red flags with antivirus or sandbox vendors, but it also used an invalid code signature which meant it isn't easily executed. While in its current state it does not present a significant threat, it does suggest a need for a change in perception around the safety of Apple devices as a default position.

This is now just one example of a shift towards targeting Apple systems. Jamf report BlueNoroff, believed to be a subgroup of the notorious Lazarus hacking group, have also developed the "RustBucket" malware. Deployed as an unsigned PDF application, it is designed to execute a payload masquerading as an Apple bundle which will in turn communicate with a C2 server to deploy another payload, a signed Rust trojan. This malware can then gather system information, processes, and allows attackers to perform various actions, as per common windows malware, thus demonstrating the capabilities of APT groups now being OS agnostic. Furthermore, it's believed that due to the nature of the initial dropper, fake domains and social engineering schemes were still the primary mechanism of ingress so despite being a novel MacOS malware, the initial ingress mechanisms remain consistent.

WithSecure™ Insight

Whilst Apple devices were never safe from viruses, these recent developments show an increased intent for capable groups to develop and evolve their tactics and software to ensure they encompassing the entire technology ecosystem. As with Windows systems, EPP, XDR, and other protection mechanisms are essential, as is user awareness training to ensure their users have the knowledge, they need to reduce the potential exposure and risk.

1.3 Pro-Russian Hactivism Continues

Russian domiciled hacktivist groups continue to launch disruptive attacks against Western and NATO organizations. Russian state provocation occurred when Finland announced intent on joining NATO, such as airspace incursions. On the date Finland officially joined NATO, several targets were posted for DDoS attacks by pro-Russian hactivist groups. 'NoName' and 'KillNet' launched DDoS attacks on government and civil organizations in Finland at the start of the month and some impact was observed. At around a similar time, a separate pro-Russian hacktivism group 'Anonymous Sudan' launched #opisrael, targeting Israeli organizations. Throughout the month other targets have been identified particularly around NATO, whereby reports arose that KillNet, in a minor fashion, disrupted a NATO web page.

WithSecure™ Insight

WithSecure™ do not assess it is likely that operational, sensitive NATO networks were impacted by DDoS attacks as some reports suggest, but in any case, the increasing reports of disruption (albeit still relatively minor) demonstrate that KillNet's capability has increased from this time last year. It is also likely that such groups are relying more on bootstrapped tooling and less upon rented 'stressor' services. It should also be noted that these DDoS attacks come along with claims and assessment that some pro-Russian hactivist groups retain links with the Russian state and retain ransomware/wiper capability. In April, KillNet has attempted to rebrand itself as a 'Private Military Contractor', likely to monetize its capability. KillNet has expressed willingness to work on behalf of the Russian state, and nobody hostile to Russia or CIS countries (it is unclear what their position is on Ukraine in this regard).

It is highly likely these groups are the subject of NCSC's and the UK Deputy Prime Minister warning against "Russia-aligned", "not state-sponsored" adversaries. NCSC has warned critical national infrastructure operators about the risk of destructive cyber-attacks from such actors. This is another indicator the threat has increased from pro-Russian hacktivist groups.

1.4 3CX Supply Chain Contd.

Following on from last month's 3CX supply chain attack against global organizations, it has come to light that they themselves were the victim of a supply chain attack which is being attributed to the North Korean APT group, LAZARUS. It is reported that trojanised 'X_Trader' software, delivering the VEILEDSIGNAL malware led to the 3CX breach, and is believed to be financially motived. However, the implications are that the earlier supply chain attack means that this attack is far wider ranging than initially believed as, according to recent findings, two critical infrastructure organizations within the Energy Sector in the US and Europe, and two financial organizations have also been compromised. The 'final' stage payload of the 3CX supply chain attack was revealed to be an info-stealer named ICONICSTEALER on which CISA have released a malware analysis report.

WithSecure™ Insight

The current tech ecosystem relies heavily on trust relationships and service providers, so supply chain attacks simply make a lot of sense if the opportunity is available to malicious actors. Infrastructure/Platform/Software providers must be trusted by their customers as they have access to, or even control over the information, network, and business functions of their customers. 3CX is a current example of a supply chain attack that was wrapped in a supply chain attack, and highlights difficulties and risks associated with improper application deployment controls and management. WithSecure™ telemetry detected that MacOS variants of trojanized 3CX software installers were distributed prior to Window's equivalents. Previous sections of this report provide further examples of prominent threat actors increasingly targeting Apple environments.

1.5 MSQM

CVE-2023-21554, nicknamed QueueJumper, one of three vulnerabilities addressed by a patch fix by Microsoft in April 11th's Patch Tuesday fixes, enables an attacker to execute code remotely on port 1801. The vulnerable Windows Message Queuing (MSMQ) is an optional middleware component which provides network communication between applications and potentially affects all Windows Server and Endpoint operating systems up to the latest 22H2 or Server 2022 releases.

Three vulnerabilities were found in MSMQ, CVE-2023-21554 (RCE), CVE-2023-21769 (Unauthenticated Remote App Level DoS), and CVE-2023-28302 (Unauthenticated Remote Kernel level DoS). The remote code execution, considered to be the most significant, can be exploited via maliciously crafted packets, exploiting the mqsvc.exe service on port 1801.

WithSecure™ Insight

More than 400,000 hosts have been detected exposing MSMQ services on TCP port 1801 to the internet. It was also noted that when installing an MS Exchange server, the setup wizard enables the MSMQ service by default if automatic roles and features are selected. Furthermore, as the component can simply be enabled via PowerShell ("Install-WindowsFeature MSMQ-Services") or via control panel on any windows OS, then it is likely there are a significant number of servers and workstations exposed unknowingly. Whilst no "in the wild" exploits have currently been recorded (at the time of writing this report), a proof of concept exploit is available on Github, it is likely only a matter of time before exploitation begins.

2 Ransomware: Trends and notable reports

The following data is limited to multi-point of extortion ransomware leak sites which are parsable and was captured between 29th March 2023 and 27th April 2023. March 2023 was the single busiest month for ransomware leak site (450) thanks to a lot of activity from CLOP, who posted 103 victims by the month end. While April's numbers do represent a drop to 326 (at the time of writing this report) the numbers represent an increase from the totals posted in April in 2022, and 2021. Many researchers speculated about the slight drop in ransomware victims and payments observed in 2022 compared to 2021, yet 2023 is on track to be the busiest year yet in terms of victims posted to leak sites. Typically, construction is the most affected sector, although throughout April, Hospitals and Health Care are the most impacted sector.

Clop, who posted 129 in last recording period, only posted two victims throughout this period. This is largely the cause between the disparity between March and April's numbers.

Group	Victims	Percentage	Change (from last period)
Lockbit	110	35.83%	-6%
Alphv	51	16.61%	19%
Royal	30	9.77%	11%
BianLian	20	6.51%	-17%
BlackBasta	19	6.19%	-24%
PLAY	14	4.56%	-44%
Medusa	11	3.58%	-50%
Karakurt	10	3.26%	900%
Stormous	10	3.26%	-41%
BlackByte	9	2.93%	125%
Akira	9	2.93%	-200%
Nokoyawa	8	2.61%	60%
Trigona	6	1.95%	50%
Other	19	6.19%	N/A

2.1 Capita

Capita, a large international business process outsourcing and professional services company, this month was affected by a cyber incident that ransomware group BLACKBASTA took credit for. Whilst an IT outage was confirmed by Capita, the incident and data leak were initially denied. Since BLACKBASTA started leaking data on their dark web shame site, they have since admitted that data was exfiltrated from the network.

Details of initial access are unknown, but BLACKBASTA are typically observed following a QAKBOT/QBOT infection. Proliferated over email, QBOT has been a prevalent malware family over April 2023 and serves as another reminder that even large organizations with a mature computer network defense (CND) is still vulnerable to a single user mishandling a malicious email.

2.2 Nokoyawa – CVE-2023-28252

A high severity zero-day vulnerability under active exploitation has been patched in April's Patch Tuesday release. CVE-2023-28252 is an elevation of privilege vulnerability in Common Log File System, found in a suite of Microsoft services with a base CVSS score of 7.8 – HIGH. Researchers for Kaspersky detected exploitation by a criminal grouping in February 2023 which had also been observed developing a number of other exploits into the Common Log File System (CLFS) driver. CVE-2023-28252 was observed by Kaspersky in an execution chain which ended in a Nokoyawa ransomware payload being deployed. Nokoywawa is a relatively new ransomware family, posting 13 victims to their leak site since it was initialized on March 20 2023.

2.3 Rorschach Ransomware discovered

Researchers at Checkpoint have discovered a sophisticated ransomware variant dubbed Roeschach. There were no discernable overlaps with known ransomware strains. The ransomware was part-auonomous, encrypts at a pace that exceeds known variants and is highly customizable. At the time of writing this report there is no breach site, or insight into the motivations or organization/affiliations of the actor(s) behind Rorschach, but it does serve as a reminder that some actors in the ransomware space do still operate outside of the now common affiliate model.

3 Other notable highlights in brief

3.1 DuckTail new update?

A new version of DuckTail has been detected in WithSecure™ telemetry. While the threat actor still relies on the usage of self-contained .NET Core bundle files to compile its primary information stealer malware, we have seen some notable changes. Some of these changes include:

- The threat actor has further incorporated the usage of cryptographic functions to encrypt and decrypt plaintext strings and data for further obscurity and exfiltration. For instance, almost all the strings used in the malware are now encrypted.
- While the core logic remains the same, the codebase has undergone major refactoring, which was observed since early April 2023
- The information stealer malware is now capable of performing screen captures, which is performed upon and during execution of the malware and on-demand via command issued from C&C. The screenshots are stored in the %TEMP% folder, using the following naming convention: tmp_cap_<DATETIME>.jpg
- Browser information stealing capabilities have expanded to include stored browser passwords, download and browsing histories
- General information stealing capabilities have also expanded to include information about the victim's machine, such as username, operating system name & version, and more. Some of these are done via WMI queries. WMI classes queried:
  - Win32_OperatingSystem
  - Win32_Processor
  - Win32_VideoController
  - Win32_ComputerSystemProduct
- Facebook information stealing capabilities have also expanded to include the ability to add members as employees (when admin is not possible), accept different type of business requests, and more.

The malware continues to save (and read from) its logs locally, however the file name is now different. The extension used is '*.tmp*'.

3.2 APT41 HOODOO

An(other) Open-Source red teaming Google Command and Control C2 (GC2) tool is being leveraged by APT41, a Chinese state sponsored hacking group also known as HOODOO, in attacks against a Taiwanese media agency and an Italian job search company during April 2023. This evidence of yet more attackers diverging from 'traditional' cracked Cobalt Strike post-exploitation services to tools such as GC2, Brute Ratel, and Sliver. The attack also utilized Google software for command and control instructions and exfiltration endpoints. Misuse of such a ubiquitous and legitimate service is difficult to detect through network traffic analysis without thorough baselining.

3.3 Service Location Protocol Vulnerability

Attackers could exploit CVE-2023-29552, a legacy Internet protocol vulnerability, to launch Denial-of-Service (DoS) attacks on an unprecedented scale. Research has shown over 54,000 SLP instances that could potentially be leveraged. Once exploited, the vulnerability allows for a DoS attack via a reflective amplification attack, which significantly increases the traffic sent to a client. A typical SLP packet size is 48-350 bytes, but by exploiting CVE-2023-29552 this can be amplified by a maximum of 2200x (compared to the usual 1.6-12x) which would have significant impact on the target network.

This comes at a time where pro-Russian hacktivist groups are launching DDoS flood attacks at significant levels, and there will almost certainly be operational groupings of actors with the objective of cultivating and improving DDoS capability and will take active interest in this. Cloudflare have also reported on an increase of malicious usage of VPS services to increase the 'power' of a DDoS capability over and above that of an IoT based botnet (a la Mirai). Whether hacktivist groups can successfully harness it into an offensive capability is yet to be determined.

3.4 Google Chrome Zero Day attacks

This month, two zero days in Chrome were patched in the tranche of updates delivered by Google. One such Zero-day was released out of bands in response to its active exploitation. CVE-2023-2033 is a vulnerability rated as HIGH, affecting Google Chrome for Windows, MacOS and Linux, "*a remote attacker could exploit this Chrome V8 type confusion vulnerability to cause heap corruption via a crafted HTML page, which could lead to arbitrary code execution.*" Details of the actors behind the exploitation are as yet unknown.

3.5 Continued targeting of Networking Devices

Throughout April stories have arisen relating to active compromises of networking equipment. Whilst critical to business function, these devices are often overlooked in terms of updates, and whilst endpoint software is often the focus of patch management, this plethora of attacks against edge devices, software, connected hardware and systems merely serves to highlight the need to patch firmware as well as software. These are summarised as follows:

- Routers being targeted in the wild as the Mirai botnet continues to actively exploit TP-Link devices via CVE-2023-1389, where a patch was delivered last month.
- Cisco routers are being targeted by APT28, FancyBear, via a 2017 CVE (CVE-2017-6742), coupled with an unpatched CVE-2022-20968 on their IP Phones, and a 0-day for the Prime Collaboration Deployment software, Cisco devices and software are highly likely to be targeted.

Whilst not yet observed being exploited in the wild, it is a realistic possibility that recently patched Fortiguard devices (and software) will be targeted, in line with this trend of targeting edge devices. Actors can wield equity on networking equipment several ways, including but not limited to DDoS attacks, and intelligence gathering purposes.

4 Threat data highlights

4.1 Exploits and Vulnerabilities

As highlighted earlier, an exploit was released publicly for PaperCut vulnerability (CVE-2023-27350 & CVE-2023-27351). This is a vulnerability in PaperCut a print management software and allows attackers to gain remote code execution on public facing PaperCut servers. It has already been exploited in the wild by multiple threat actors.

CISA’s known exploited vulnerabilities catalog

CISA’s known exploited vulnerabilities catalog

Since last month, CISA have added 17 new vulnerabilities to their catalog. 3 of which are rated as CRITICAL.43

CVE ID	Vendor / Product	CVSS Rating	What's the vulnerability?
CVE-2023-28432	MinIO	High	MinIO contains a vulnerability in a cluster deployment where MinIO returns all environment variables, which allows for information disclosure.
CVE-2023-27350	PaperCut MF/NG	Critical	PaperCut MF/NG contains an improper access control vulnerability within the SetupCompleted class that allows authentication bypass and code execution in the context of system.
CVE-2023-2136	Google Chrome	Critical	Google Chrome Skia contains an integer overflow vulnerability. Specific impacts from exploitation are not available at this time. This vulnerability resides in Skia which serves as the graphics engine for Google Chrome and ChromeOS, Android, Flutter, and other products.
CVE-2017-6742	Cisco IOS and IOS XE Software	High	The Simple Network Management Protocol (SNMP) subsystem of Cisco IOS and IOS XE contains a vulnerability that could allow an authenticated, remote attacker to remotely execute code on an affected system or cause an affected system to reload.
CVE-2019-8526	Apple macOS	High	Apple macOS contains a use-after-free vulnerability that could allow for privilege escalation.
CVE-2023-2033	Google Chromium V8 Engine	High	Google Chromium V8 contains a type confusion vulnerability. Specific impacts from exploitation are not available at this time.
CVE-2023-20963	Android Framework	High	Android Framework contains an unspecified vulnerability that allows for privilege escalation after updating an app to a higher Target SDK with no additional execution privileges needed.
CVE-2023-29492	Novi Survey Novi Survey	Critical	Novi Survey contains an insecure deserialization vulnerability that allows remote attackers to execute code on the server in the context of the service account.
CVE-2023-28252	Microsoft Windows	High	Microsoft Windows Common Log File System (CLFS) driver contains an unspecified vulnerability that allows for privilege escalation.
CVE-2023-28205	Apple Multiple Products	High	Apple iOS, iPadOS, macOS, and Safari WebKit contain a use-after-free vulnerability that leads to code execution when processing maliciously crafted web content.
CVE-2023-28206	Apple iOS, iPadOS, and macOS	High	Apple iOS, iPadOS, and macOS IOSurfaceAccelerator contain an out-of-bounds write vulnerability that allows an app to execute code with kernel privileges.
CVE-2021-27876	Veritas Backup Exec Agent	High	Veritas Backup Exec (BE) Agent contains a file access vulnerability that could allow an attacker to specially craft input parameters on a data management protocol command to access files on the BE Agent machine.
CVE-2021-27877	Veritas Backup Exec Agent	High	Veritas Backup Exec (BE) Agent contains an improper authentication vulnerability that could allow an attacker unauthorized access to the BE Agent via SHA authentication scheme.
CVE-2021-27878	Veritas Backup Exec Agent	High	Veritas Backup Exec (BE) Agent contains a command execution vulnerability that could allow an attacker to use a data management protocol command to execute a command on the BE Agent machine.
CVE-2019-1388	Microsoft Windows	High	Microsoft Windows Certificate Dialog contains a privilege escalation vulnerability, allowing attackers to run processes in an elevated context.
CVE-2023-26083	Arm Mali Graphics Processing Unit (GPU)	Low	Arm Mali GPU Kernel Driver contains an information disclosure vulnerability that allows a non-privileged user to make valid GPU processing operations that expose sensitive kernel metadata.
CVE-2022-27926	Zimbra Collaboration (ZCS)	Medium	Zimbra Collaboration Suite (ZCS) contains a cross-site scripting vulnerability by allowing an endpoint URL to accept parameters without sanitizing.

5 Research highlights

5.1 Ransomware Actors exploiting Veeam Servers

WithSecure™ Intelligence identified attacks which occurred in late March 2023 against internet-facing servers running Veeam Backup & Replication software. Our research indicates with high confidence that the intrusion set used in these attacks is consistent with activities attributed to the FIN7 activity group. It is likely that initial access & execution was achieved through a recently patched Veeam Backup & Replication vulnerability, CVE-2023-27532. FIN7 is a financially motivated cybercrime group with roots dating back to mid-2010s. The group has been involved in several high-profile, large-scale attacks over the years. The group's tradecraft and modus operandi have evolved over their multi-year history, developing new tools2 and expanding their operations.

- The affected servers had TCP open port 9401 exposed to the internet. This port is used for communication with the Veeam Backup Service over SSL. Network activity with an external IP address was observed over this port right before the shell command invocation by the SQL server instance process.
- CVE-2023-27532 was patched a few weeks prior to this campaign. Exploitation of this vulnerability requires communication over port 9401.
- The servers were running vulnerable versions of the software at the time of attack.
- A proof-of-concept6 (POC) exploit was made publicly available a few days prior to the campaign, on 23rd March 2023. The POC contains remote command execution functionality. The remote command execution, which is achieved through SQL shell commands, yields the same execution chain observed in this campaign. More details are available here.

Who We Are

WithSecure™, formerly F-Secure Business, 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 and response are 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™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

WITH secure