Threat Highlight Report

March 2023

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 look at the exploitation of softphone application 3CX, we deliver some updates on "hacktivist" groups, examine some recently released cyber security strategies, and look at some dangers associated with ChatGPT.

We look at the ransomware landscape, including the most prevalent hack/leak actors from March, CISAs pre-ransomware notification initiative, the real world impacts of ransomware, the rise of Royal, and we highlight some newcomers to the ransomware landscape.

We also discuss some cyber best practices, a new threat actor called Hydrochasma, MacOS crypto-mining malware, and the downfall of Breach Forums.

- Ziggy Davies, Threat Intelligence Analyst

1 Monthly highlights

1.1 The exploitation of 3CX

3CX, a popular business communication platform, has recently fallen victim to a cyber compromise involving the delivery of a malicious installer file. At the time of writing, investigations into the exploitation of 3CX are ongoing, but initial reports from Sophos, CrowdStrike, and SentinelOne reveal a targeted attack against the company's customers, suggesting a desire to target the 3CX supply chain.

Attacks involve tainted (DLL sideloading) files, that appear legitimate and are fully functional, suggesting the attacker made efforts to hide their activity, not wishing to disrupt the legitimate usage of the base files. Once compromised, follow-up activity includes beaconing, second-stage infostealer payloads and finally, in some rare cases, hands-on-keyboard activity.

WithSecure™ Insight

Working with other researchers in the industry, WithSecure™ are currently investigating instances of attempted 3CX compromise that match the activity reported by Sophos, CrowdStrike and SentinelOne. WithSecure™ telemetry first detected this attack in early Feb 2023, although analysis of infrastructure suggests this could have begun as early as December 2022. At the time of writing, open-source indicators suggest that this threat actor is DPRK-backed, and that this was a concerted effort to target the 3CX supply chain. This campaign certainly seems very similar to the SolarWinds supply chain attacks of 2020, which caused widespread problems and a rethink of how organizations deal with third party software.

What can you do?

This serves as yet another reminder into the risk organisations face through the supply chain . To this end, WithSecure™ have produced an upcoming report that delves into the threat posed through the supply chain.

While waiting on further information, you can:

- Make use of security solutions, especially endpoint detection and response.
- WithSecure™ Elements Endpoint Detection and Response and WithSecure™ Countercept Managed Detection and Response detect the trojanized versions of the application and subsequent DLLs, and it will generate detections which the security administrator can act on
- Uninstall the following affected version(s) of the 3CX Desktop App
  - 18.12.407 – Windows
  - 18.12.416 – Windows
  - 18.11.1213 – MAC
  - 18.12.416 – MAC
- Assess vendor security: Evaluate the security posture of vendors and partners, ensuring they follow industry-standard security practices and guidelines.
- Regularly update software: Keep all software and operating systems up-to-date to minimize the risk of exploitation via known vulnerabilities.
- Implement strong access controls: Limit user access to sensitive data and resources, and enforce the principle of least privilege.
- Monitor network traffic and cloud services: Regularly review network traffic and cloud services for signs of unusual activity that may indicate a security breach or compromise.

1.2 Updates on “Hacktivist” groups

The activity of the pro-Russian group **Killnet** has been analyzed by Microsoft and their report focuses on the risk the group presents to healthcare institutions. Microsoft found that **Killnet** are utilizing a botnet in their DDoS attacks, but the packets per second (PPS) generated were relatively low and could be successfully mitigated using DDoS protections.

Anonymous Sudan, whom we discussed last month has continued their campaign and attacked hospitals in Denmark and airports, hospitals and schools in France, and have responded to an article by Truesec, by calling the company founder an “idiot” and announcing a switch to DDoS that uses botnets instead of abusing paid services.

The use of botnets by so-called hacktivist groups is a growing issue and Radware is reporting a campaign by the **Zarya**, a splinter group of **Killnet** who are deploying **Mirai** variants, a botnet that has been adapted and leveraged by many different threat actors since its origins in 2016.

New to the scene are the groups **Usersec** and **Mistsec** which have announced their desire to target NATO nations, and in one post on Telegram provided a list of targets in the UK, namely government organizations and hospitals.

The UK National Crime Agency (NCA) has taken proactive steps as part of an international operation called “Power-Off”, to deter and detect individuals seeking to use DDoS as a weapon. The NCA has set up honey traps, imitating DDoS-for-hire services, commonly sold on the cyber underground, capturing the registration information of users seeking the service. Those people caught in the UK will be issued warnings by UK law enforcement, while those abroad will be dealt with by their respective national law enforcement agencies.

WithSecure™ Insight

So-called hacktivist groups are a growing problem. They now more frequently targeting organizations in Europe and the United States, especially those considered critical national infrastructure such as airports and hospitals. Thankfully, DDoS attacks, as Microsoft pointed out in their report, can be mitigated, and many of the attacks aren’t generating the volumes of traffic that other major DDoS attacks have in the past, suggesting a limit in the infrastructure and personnel being deployed.

The NCA’s action in deploying honey traps to target individuals seeking to access DDoS services is welcomed but is not likely to impact hacktivist groups, who often rely on their own, or more established, tooling and infrastructure, such as the one being developed by **Zarya/Killnet**.

What can you do?

DDoS protections are reliant upon the use of specially configured network equipment or cloud-based protection services, offered by DDoS specialists. These protections will typically filter traffic and/or employ load balancing / caching servies.

As with all security incidents, the creation of incident response plans, and the delivery of related training to personnel is paramount. Including details on whom to contact if you are targeted, and what actions need to be taken.

Monitoring of these groups is also useful as many of their attacks are discussed and advertised ahead of time (albeit at short notice) via their public Telegram channels, giving defenders the opportunity to pre-empt potential attacks.

1.3 National cyber strategies

This month has included a lot of movement by governments and national institutions on the issue of national cyber security and the supply chain.

The White House has released the National Cybersecurity Strategy 2023, outlining the US government's approach to tackling cyber threats. The strategy focuses on five initiatives:

- Defend critical infrastructure
- Disrupt and dismantle threat actors
- Shape market forces to drive security and resilience
- Invest in a resilient future
- Forge international partnerships to pursue shared goals.

The plan also includes specific measures such as investing in cybersecurity research and development, increasing collaboration between the public and private sectors, and promoting a strong cybersecurity workforce. The strategy also highlights the need for continuous assessment and adaptation to changing cyber threats to maintain the safety and security of the nation's digital infrastructure.

Similarly, the Australian government has released a new strategy to enhance the country's resilience against cyber threats targeting critical infrastructure. The Critical Infrastructure Resilience Strategy 2023 outlines four key priorities, which include:

- Developing a national critical infrastructure resilience plan
- Improving threat intelligence sharing and incident response capabilities
- Enhancing the security of supply chains, and
- Strengthening partnerships between government and industry.

Likewise, the UK government has released a new cyber security strategy aimed at building a resilient health and adult social care system in England by 2030. The strategy identifies three key priorities:

- Protect sensitive data and critical systems
- Prevent cyber-attacks, and
- Respond effectively to incidents.

In addition to the strategy the UK government has also established a new organization, called the Joint Centre for Security Science (JCSS), to strengthen the UK's capabilities to combat national security threats. The JCSS will bring together experts from different fields to enhance the UK's understanding of threats and their potential impacts. It will collaborate with other government agencies, universities, and private sector partners to develop advanced technologies and strategies for counter-terrorism, counter-espionage, and cyber security. The new body will also provide training and guidance to enhance the skills and knowledge of professionals working in the national security sector.

WithSecure™ Insight

These strategies and responses come as the world appreciates the growing risk to what is a heavily cyber-dependent critical national infrastructure, by both nation-state threats and financially motivated cyber-criminals.

The strategies focus on increasing cyber resilience, improving coordination and information-sharing between agencies, investing in research and development of new technologies, and enhancing public-private partnerships. Clearly accepting and appreciating the complex way that critical national infrastructure has evolved, and involves entities from both the public and private sectors.

What can you do?

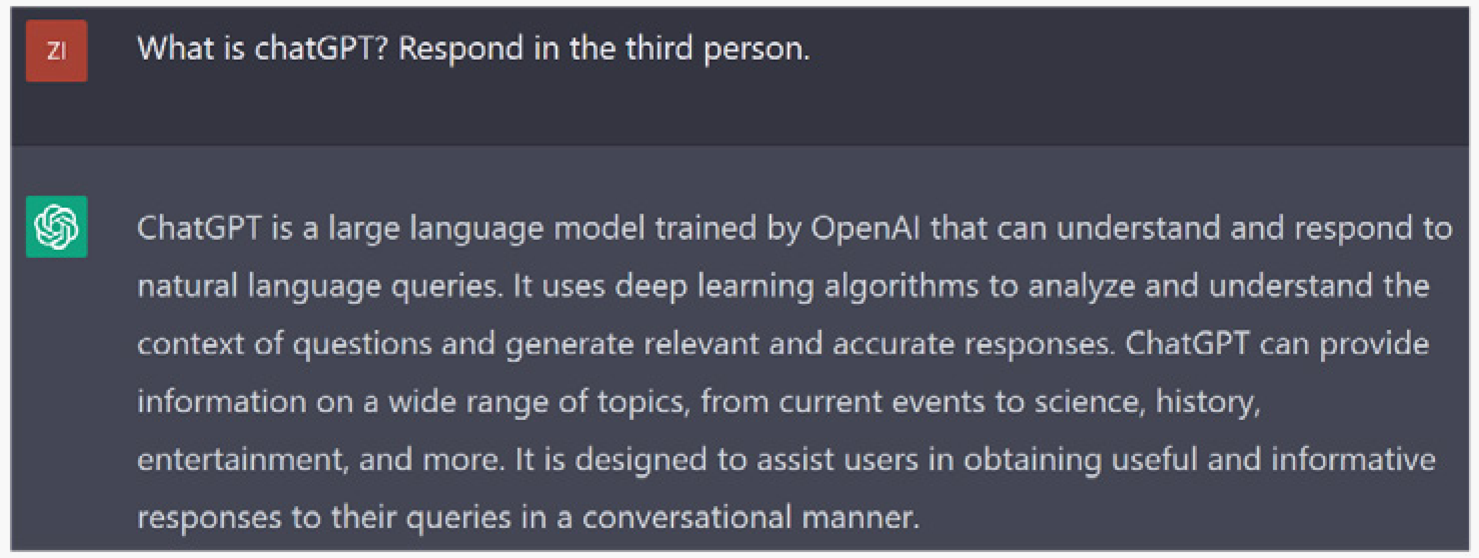
Every organization has a responsibility to consider the state of its cyber security posture, especially if other people, organizations, or infrastructure rely upon the services they provide, or would be impacted by the loss of data they hold.

It’s important to consider how these national strategies may relate to your organization, as you may have to meet certain requirements. They may also present an opportunity to join intelligence-sharing platforms/co-operatives and provide opportunities for training.

One of the common themes is the importance of securing the supply chain and considering the relationships you have with trusted parties, and creating incident plans that consider and involve them. WithSecure™ is producing a report on the Supply Chain which will be published soon.

1.4 ChatGPT dangers

In case you've been living under a rock...perhaps it is best to let ChatGPT explain itself...

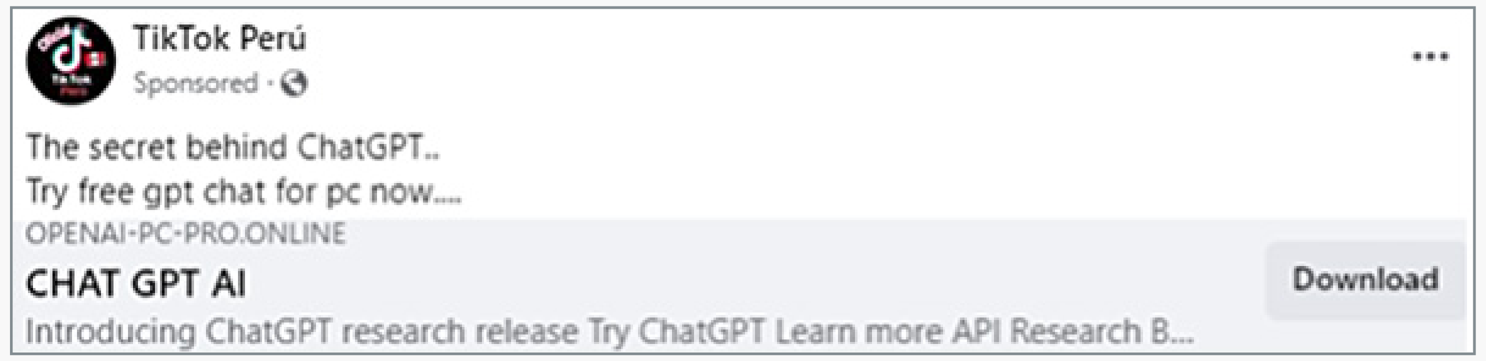


ZI What is chatGPT? Respond in the third person.

ChatGPT is a large language model trained by OpenAI that can understand and respond to natural language queries. It uses deep learning algorithms to analyze and understand the context of questions and generate relevant and accurate responses. ChatGPT can provide information on a wide range of topics, from current events to science, history, entertainment, and more. It is designed to assist users in obtaining useful and informative responses to their queries in a conversational manner.

You'll have likely heard lots about ChatGPT on the news lately, especially with regard to how it might take your job, or about students using it to their advantage. Unfortunately, discussion and interest in the topic of ChatGPT and artificial intelligence is being used as a way to distribute malware by threat actors.

Nexusguard has detected an ongoing campaign that is abusing Facebook advertisements to distribute stealer malware, with the adverts using ChatGPT as a pretext to drive user interaction.



TikTok Perú
Sponsored ·
The secret behind ChatGPT..
Try free gpt chat for pc now....
OPENAI-PC-PRO.ONLINE
CHAT GPT AI
Introducing ChatGPT research release Try ChatGPT Learn more API Research B...

Unfortunately, the threat actors are imitating the genuine OpenAI website design, which will further drive user interaction, but the file download `ChatGPT-OpenAI-Pro-Full-134676745403[.]exe` is stealer malware, and shows similarities to the commodity malware **Redline**, and has the ability to exfiltrate credentials and cookies used within browsers.

In unrelated news, ChatGPT experienced some downtime on March 20th. This was due to a bug in one of the third-party libraries used by openAI, called redis-py. OpenAI reported:

"*We took ChatGPT offline earlier this week due to a bug in an open-source library which allowed some users to see titles from another active user's chat history. It's also possible that the first message of a newly-created conversation was visible in someone else's chat history if both users were active around the same time...we also discovered that the same bug may have caused the unintentional visibility of payment-related information of 1.2% of the ChatGPT Plus subscribers who were active during a specific nine-hour window.*"

WithSecure™ Insight

Current affairs and topics of public interest have always been a driver for threat actors, tax season always brings tax-themed phishing emails, the pandemic brought healthcare-related pretexts, and any zeitgeist can become a point of abuse, and this includes new technologies like ChatGPT.

Stealer malware is a common first-stage infection, and malvertisements and SEO poisoning are common distribution methods, with **Redline**, **Raccoon**, and **VIDAR** all being common variants right now. The data exfiltrated by stealers are often sold on the cyber underground and used by initial access brokers (IABs) to sell initial access to other threat actors like ransomware groups. You can see how something as simple as a malicious ChatGPT advert, can turn into ransomware and WithSecure's incident response team has investigated a case of **Alphv** gaining initial access via Citrix following credentials being captured by **Redline**.

The OpenAI data leak associated with the third-party library redis-py is an example of the dangers associated with the supply chain, and demonstrates the importance of trust relationships, on the topic OpenAI said:

"*The Redis open-source maintainers have been fantastic collaborators, swiftly addressing the bug and rolling out a patch. Redis, along with other open-source software, plays a crucial role in our research efforts.*"

The quick fix and joint approach taken by openAI and the maintainers of Redis demonstrate the importance of maintaining good relationships with your software supply chain, as when the wheels inevitably fall off, you can quickly put things right together.

What can you do?

Language models, virtual assistants, and AI are going to be a talking point for a long time, especially with the dramatic improvements and new use cases we are seeing at the moment. It is obvious that people are going to be curious, and may be tempted to explore articles, adverts, and emails that purport to discuss ChatGPT and similar technologies. It's therefore important to inform, educate and train users about the dangers of phishing, malvertising, and SEO poisoning and how these are used to distribute malware. Security solutions including EDR are also vital and can detect the activity of stealer malware, such as the access/abuse of databases related to browsers.

The data leak potentially exposed the following information:

- Chat titles and the first message from chats
- Users' first and last names
- Email addresses
- Payment addresses
- The last 4 digits of payment card numbers

OpenAI says they are identifying impacted users and contacting them directly. While data has been exposed, it seems to have been done sporadically and to other random users, and will probably not have been scraped or harvested for later abuse by threat actors. Best practices though, assume a breach and be aware of the potential for an increase in phishing emails due to the leak of email addresses.

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 22nd February 2023 and 28th March 2023.

There has been a 103% increase in activity since last month, mostly attributable to the huge number of victims Clop have posted top their leak site following their exploitation of vulnerable GoAnywhere instances last month.

This month's data includes newcomers* **Vendetta** and **Abyss**, Vendetta appear to be connected to the ransomware group **Cuba**, which hasn't been active since December 2022, suggesting a rebrand. Information on **Abyss** is scant, but the group was first discussed on March 21st and they have since published data relating to 7 victims so far, with their victimology being limited to the United States, and involving organizations in the Manufacturing, Construction, and Healthcare sectors, with one victim being a chain of Colorado Cannabis dispensaries.

Group	Victims	Percentage
Clop	129	25.50%
LockBit	116	23.00%
Alphv	43	8.50%
Royal	27	5.30%
Play	25	4.90%
BlackBasta	25	4.90%
BianLian	24	4.80%
Medusa	22	4.40%
RansomHouse	12	2.40%
Abyss*	7	1.40%
Vice Society	7	1.40%
Monti	6	1.20%
Mallox	5	1.00%
Snatch	4	0.80%
BlackByte	4	0.80%
Vendetta*	3	0.60%
RagnarLocker	2	0.40%
RansomExx	2	0.40%
Lorenz	2	0.40%
Everest	2	0.40%
Qilin	2	0.40%
Karakurt	1	0.20%

2.1 CISAs pre-ransomware notification initiative

CISA has set up an intelligence-sharing collaborative, that relies upon tips from the wider intelligence and cyber security community, to warn organizations that they may have been compromised by a threat actor, and that they are likely to experience a ransomware attack.

This initiative relies on something called dwell time, CISA say:

"*We know that ransomware actors often take some time after gaining initial access to a target before encrypting or stealing information, a window of time that often lasts from hours to days. This window gives us time to warn organizations that ransomware actors have gained initial access to their networks. These early warnings can enable victims to safely evict the ransomware actors from their networks before the actors have a chance to encrypt and hold critical data and systems at ransom.*"

In order to provide CISA with relevant tips, information and intelligence, they have created the email address report@cisa.dhs.gov.

2.2 Dole attack shows real world impact

A currently unattributed ransomware attack has impacted the food production company Dole. The attack has reportedly caused a shutdown of the companies systems across North America and has led to some shortages of food products on supermarket shelves. Unfortunately it also appears that employee data has been compromised, and this incident demonstrates the potential real world impact of cyber-attacks.

2.3 Rise of Royal

Royal, have been active since November 2022 and have struck at least 136 organizations since then and are thought to be an off-shoot of the former ransomware titan **Conti**. CISA has produced an advisory on the group, of specific interest are stats on how the group gains initial access:

- Phishing, which was used in 66.7% of attacks
- Abuse of Remote Desktop Protocol (RDP) in 13.3% of attacks
- The exploitation of public facing applications in an unspecified amount of attacks
- The purchase of initial access from IABs in an unspecified amount of attacks

The advisory also discusses the use of (semi) legitimate tools by **Royal**, such as the tunneling tool **Chisel**, and remote access software like **AnyDesk** and **LogMeIn**. Something which is very common amongst all ransomware groups and threat actors.

2.4 Nevada is Nokoyawa

A report by ZScaler has linked a new ransomware variant called **Nevada** to **Nokoyawa**, an older variant. The variants have been linked due to an overlap in code, and this is not the first instance, with older variants of Nokoyawa existing, called **Karma** and **Nemty**.

This is a good example of the fluid state of ransomware, and how many current variants have branched off from a common source code.

2.5 Magniber’s SmartScreen bypass

Microsoft SmartScreen is a feature of Microsoft Defender that helps protect users from phishing attacks and malicious downloads. It works by analyzing websites and downloads for suspicious activity and potential threats.

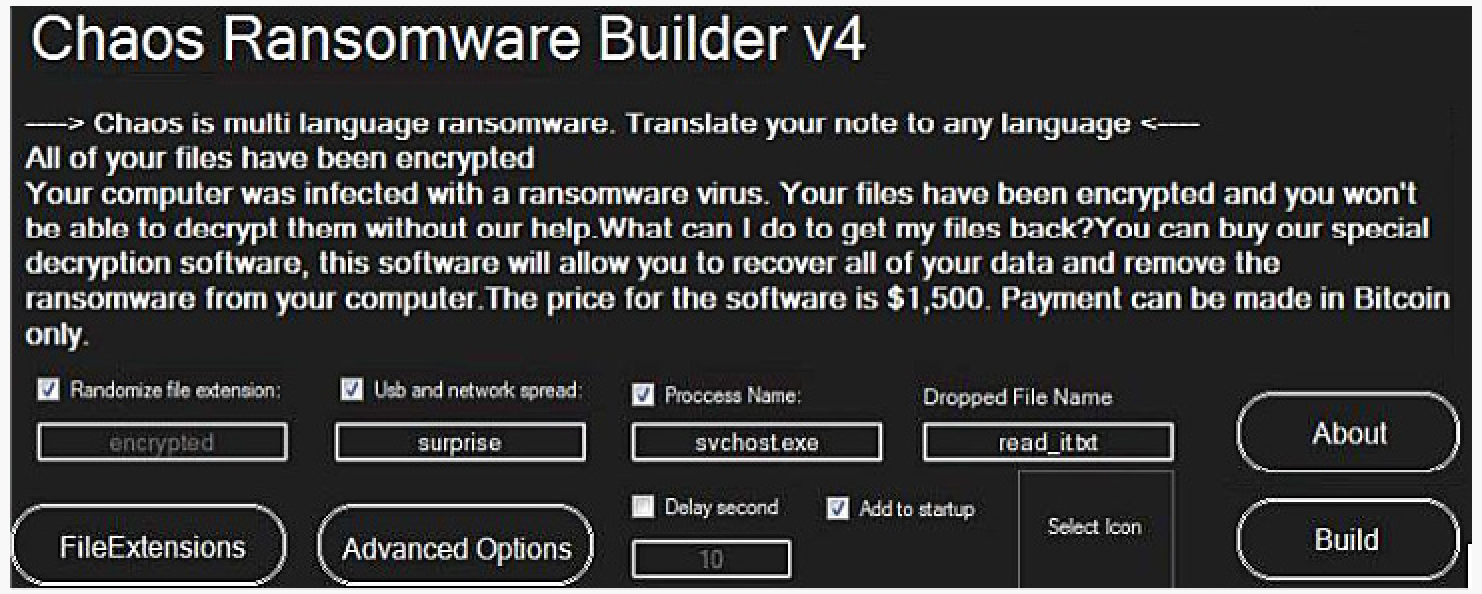
When a user visits a website or downloads a file, SmartScreen checks to see if it is a known threat or if it exhibits suspicious behavior. If it is deemed safe, the user can proceed with the action. If SmartScreen detects a potential threat, it will block the user from accessing the site or downloading the file, and will provide a warning message.

The ransomware group **Magnibar** had previously exploited a vulnerability in SmartScreen (CVE-2022-44698), which was patched, but Google’s Threat Analysis Group (TAG) has detected a new campaign by **Magnibar**, which appears to have found a workaround and is once again exploiting SmartScreen.

Magnibar is doing this by delivering MSI files signed with an invalid but specially crafted Authenticode signature. The malformed signature causes SmartScreen to return an error that results in bypassing the security warning dialog displayed to users when an untrusted file contains a Mark-of-the-Web (MotW), which indicates a potentially malicious file has been downloaded from the internet. This new vulnerability has been patched by Microsoft (CVE-2023-24880)

2.6 Ransomware newcomers

Sirattacker is a new ransomware variant reportedly created using the infamous **Chaos** ransomware builder. **Chaos**, which is available on the cyber underground is a ransomware builder which can create lockers based on the user’s desired settings, making it possible for a non-technical attacker to kickstart their own ransomware variant. **Sirattacker** is being distributed as a fake crypto-mining application, but when launched it encrypts the victim’s files and thanks to **Chaos’** features, displays a custom ransom note and changes the victim’s desktop background.



Chaos Ransomware Builder v4

——> Chaos is multi language ransomware. Translate your note to any language <——
All of your files have been encrypted
Your computer was infected with a ransomware virus. Your files have been encrypted and you won't be able to decrypt them without our help.What can I do to get my files back?You can buy our special decryption software, this software will allow you to recover all of your data and remove the ransomware from your computer.The price for the software is $1,500. Payment can be made in Bitcoin only.

☑ Randomize file extension: encrypted
☑ Usb and network spread: surprise
☑ Proccess Name: svchost.exe
Dropped File Name: read_it.txt
☐ Delay second: 10
☑ Add to startup

Fortinet is also reporting on another ransomware newcomer called **ALC**, who appear to be politically motivated, with their ransomware note stating “*our targets are Russia and its counterparts*”. Strangely though, **ALC** is not at current able to encrypt files, which either means it is being used as scareware, or is still under development.

A bulletin by Broadcom has discussed a new single point of extortion ransomware variant called **CMLocker**, which is very simple in comparison to many other ransomare variants, lacking any exfiltration ability or ability to be laterally spread across a network/estate.

Trellix have analyzed newcomer Dark Power, who are operating a double extortion ransomware group. The group don’t appear to have a specific victimology, but are acting opportunistically and demanding ransom in Monero (XMR).

3 Other notable highlights in brief

3.1 Best practices in cyber

There have been 3 very useful documents produced this month, all of which outline and discuss best practices across various cybersecurity topics.

The US National Security Agency (NSA) has created an information sheet titled "*Best practices for securing your home network*". While many of the suggestions are basic, they are still vital and form the foundation for a safe home and working environment. Some interesting suggestions include:

- Covering webcams when not in use
- Do not have sensitive conversations near to home assistants and mute their microphones when they are not in use
- Use WPA3 rather than WPA2 on your home network
- Schedule frequent device reboots, including on home routers

The NSA have also produced another information sheet titled "*Guidance on advancing zero trust maturity throughout the user pillar*", the first paragraph is indicative of the need for such guidance, stating:

"*...at least two-thirds of cyberattacks are now focused on impersonating trusted users and systems to access vital data or critical systems.*"

And on a similar topic, the NSA and CISA have produced a joint product titled "*Recommended best practices for administrators: Identity and access management.*" The key points include:

- Maintaining strict access controls based on the principle of least privilege
- Implementing multi-factor authentication
- Regularly reviewing access permissions
- Closely monitoring privileged user activities, and
- Administrators should also establish clear incident response plans and invest in security awareness training for their teams.

3.2 Hydrochasma gathering intelligence

A report by Symantec has identified a threat actor called **Hydrochasma** who have been infiltrating organizations in the shipping and medical sectors, with the motivation of gathering intelligence.

The attack chain is believed to begin with a phishing email, but interestingly doesn't make use of any custom tools or malware, and instead relies on off-the-shelf open source tools. The tools used include:

- **Meterpreter:** A tool included in the Metasploit framework.
- **Gogo scanning tool:** An automated scanning engine originally designed for use by red teams.
- **Process Dumper (lsass.exe):** A tool that allows attackers to dump domain passwords.
- **Cobalt Strike Beacon:** An off-the-shelf tool that can be used to execute commands, inject other processes, elevate current processes, or impersonate other processes, and upload and download files.
- **AlliN scanning tool:** A pentesting scan tool that can be used for lateral penetration of the intranet.
- **Fscan:** A publicly available hacktool that can scan for open ports and more.
- **Dogz proxy tool:** A free VPN proxy tool.
- **SoftEtherVPN:** The presence of this tool was what first prompted Symantec researchers to investigate this activity. It is free, open-source, and cross-platform VPN software.
- **Procdump:** Microsoft Sysinternals tool for monitoring an application for CPU spikes and generating crash dumps, but which can also be used as a general process dump utility.
- **BrowserGhost:** A publicly available tool that can grab passwords from an internet browser.
- **Gost proxy:** A tunneling tool.
- **Ntlmrelay:** An NTLM relay attack allows an attacker to intercept validated authentication requests in order to access network services.
- **Task Scheduler:** Allows tasks to be automated on a computer.
- **Go-strip:** Used to make a Go binary smaller in size.
- **HackBrowserData:** An open-source tool that can decrypt browser data.

3.3 I2PMiner targeting MacOS

A new crypto-mining malware targeting macOS systems has been identified by Jamf Threat Labs and CrowdStrike.

I2PMiner is an **XMRig** crypto mining malware, that has been embedded in malicious MacOS versions of common software, such as Logic Pro, Final Cut, Traktor and Adobe products. **I2PMiner** employs a combination of obfuscation techniques and persistence mechanisms to evade detection and maintain its presence on the infected systems. It utilizes the Invisible Internet Project (I2P) network for command and control, making it difficult to trace the threat actors and adding a layer of anonymity to their activities.

3.4 Lumma Stealer targets content creators

A new stealer malware is doing the rounds and is reportedly being used to target YouTube content creators through carefully crafted spear-phishing emails, which attempt to trick recipients into downloading and executing the malicious payload.

Once installed, Lumma Stealer can exfiltrate sensitive data, including login credentials, cookies, and cryptocurrency wallet keys, from the victim's computer. The malware is designed to be stealthy and persistent, allowing the threat actors to conduct long-term surveillance and data theft.

The Lumma Stealer campaign underscores the need for increased vigilance and robust security measures for content creators, as they are attractive targets for cybercriminals due to their reach and potential to serve as a launchpad for further attacks.

3.5 T-Mobile constantly targeted by SIM-swappers

T-Mobile has reportedly been compromised numerous times, with hackers claiming to have breached the company more than 100 times in 2022, predominantly for SIM-swapping attacks.

The frequent breaches of T-Mobile for SIM-swapping attacks highlight the importance and vulnerability of telecommunications providers to cyber threats. These attacks allow cybercriminals to take over victims' phone numbers, leading to potential account takeovers and unauthorized access to sensitive data. It appears all too easy to gain access to these organizations, likely due to the sheer size of the company, and vast amounts of personnel who have access. SIM-swapping is the reason why we suggest other forms of MFA such as hardware key solutions or the use of number/pattern matching challenges.

3.6 Android banking trojan tracker

Will (@BushidoToken) Thomas has created a tracker for Android banking trojan malware. The tracker currently has 59 entries, and includes the following data:

- The name of the trojan
- Alternative names for the trojan
- Code similarities with other malware
- Threat actors associated with the malware
- A last reported date
- References

3.7 Breach Forums down!

The recent arrest of Thomas Fitzpatrick aka Pompompurin, as documented in United States v. Fitzpatrick, signifies a noteworthy development in combating cybercrime. Fitzpatrick was allegedly an administrator of the underground cyber marketplace/community Breach Forums, which is known for facilitating criminal activities, including the trading of stolen data, hacking tools, and other illicit services.

Fitzpatrick's apprehension highlights the continuous efforts of law enforcement agencies in identifying and dismantling the infrastructure that supports cybercriminal operations. The arrest underscores the importance of international cooperation in tracking and apprehending individuals who enable and participate in cybercrime.

The future of Breach Forums was initially uncertain, but it has quickly closed down, after another admin raised fears due to the potential of law enforcement compromising the website. This is not the first time the hacker community has had to abandon ship, as Breach Forums was created following the demise of its predecessor Raid Forums, a new hive of villainy will undoubtedly appear in the coming weeks/months.

3.8 Ultrasonic attacks

Researchers at the University of Texas at San Antonio (UTSA) have discovered a novel technique for exploiting voice assistant devices, posing potential security risks for users.

The newly discovered technique reveals that voice assistant devices can be manipulated through inaudible near ultrasonic waves. This method enables attackers to issue voice commands to the device without the knowledge or consent of the device owner, examples include the unlocking of doors or activation/deactivation of IOT devices.

4 Threat data highlights

4.1 Exploits and Vulnerabilities

This month, we have seen third party reports based on the top and most common exploitations and vulnerabilities from 2022.

A report from Tenable believes the following to be the top 5 vulnerabilities exploited in 2022:

1. Previously known vulnerabilities from 2017-2021
2. Log4Shell (Log4j) CVE-2021-44228
3. Follina (Microsoft Office) CVE-2022-30190
4. Atlassian Confluence Server and Data Center CVE-2022-26134
5. ProxyShell (Microsoft Exchange) CVE-2021-34473

Rapid7 have a similar report out, one of the most interesting findings is:

"Attackers are still developing and deploying exploits faster than ever. 56% of the vulnerabilities in this report were exploited within seven days of public disclosure — a 12% rise over 2021 and an 87% rise over 2020."

Mandiant have released a blog post with the firm tracking 55 different 0-day vulnerabilities being exploited in 2022, which represents a 32% decline from last year, but a huge increase compared to the pre-2021 figures. Mandiant assess that nearly a quarter of 2022's 0-days were developed/exploited first by state-backed cyber espionage groups. This makes sense, as those groups are the ones with the expertise, infrastructure and assets to pursue exploit development.

CISA’s known exploited vulnerabilities catalog

Since last month CISA have added 9 new exploited vulnerabilities to their catalog. 3 of which are rated as CRITICAL.

CVE ID	Vendor / Product	CVSS Rating	What's the vulnerability?
CVE-2023-26360	Adobe ColdFusion	Critical	Adobe ColdFusion contains an improper access control vulnerability that allows for remote code execution.
CVE-2023-23397	Microsoft Office	Critical	Microsoft Office Outlook contains a privilege escalation vulnerability that allows for a NTLM Relay attack against another service to authenticate as the user.
CVE-2023-24880	Microsoft Windows	Medium	Microsoft Windows SmartScreen contains a security feature bypass vulnerability that could allow an attacker to evade Mark of the Web (MOTW) defenses via a specially crafted malicious file.
CVE-2022-41328	Fortinet FortiOS	High	Fortinet FortiOS contains a path traversal vulnerability that may allow a local privileged attacker to read and write files via crafted CLI commands.
CVE-2021-39144	XStream	High	XStream contains a remote code execution vulnerability that allows an attacker to manipulate the processed input stream and replace or inject objects that result in the execution of a local command on the server. This vulnerability can affect multiple products, including but not limited to VMware Cloud Foundation.
CVE-2020-5741	Plex	High	Plex Media Server contains a remote code execution vulnerability that allows an attacker with access to the server administrator's Plex account to upload a malicious file via the Camera Upload feature and have the media server execute it.
CVE-2022-28810	Zoho ManageEngine	Medium	Multiple Zoho ManageEngine ADSelfService Plus contains an unspecified vulnerability allowing for remote code execution when performing a password change or reset.
CVE-2022-33891	Apache Spark	High	Apache Spark contains a command injection vulnerability via Spark User Interface (UI) when Access Control Lists (ACLs) are enabled.
CVE-2022-35914	Teclib GLPI	Critical	Teclib GLPI contains a remote code execution vulnerability in the third-party library, htmlawed.

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.