W / T H®
secure

The Cyber Security Black Book

VOL. I

WITH secure

Exposing the tactics and techniques of online criminals.

VOL. I

What makes us stand out

I

Our product

Elements Cloud™ connects technologies, human expertise and co-security services into a modular set of capabilities across endpoint protection, threat detection & response and exposure management.

II

Our standard

We play the European way. That means a higher standard across tech integrity, trusted partnerships, sustainability and Europe's regulative approach.

II•

Our customer

We're here for the mid-market. As the engines of European economic growth, they are susceptible to the same threats as enterprises but often lack the resources to keep themselves safe. That's where we come in.

III.

Our partnership

This is the superpower that sets us apart and makes the most of our human and AI capabilities.

SPHERE

Co-security unconference

MAY 28-29, 2024 HELSINKI, FINLAND

SPHERE.WITHSECURE.COM

Index

Foreword

A few years ago, my neighbor was on a train headed for the Finnish city of Tampere. During his journey, a young woman approached him and asked if she could borrow some money. Her credit card wasn't working, and she wanted to buy a cup of coffee and a snack from the train's restaurant.

Although hesitant to lend money to a stranger, my neighbor sensed an air of trustworthiness about her. She had been working on her laptop throughout the journey, and seemed like a good person – good enough for my neighbor to extend a helping hand.

This story got me thinking about the element of trust and how it really is the true essence of companies working in cyber security. This is not an industry of selling products or services: it's about offering expertise, experience and trustworthiness.

When our phone rings, it's often someone in the middle of a crisis. They are not just seeking a solution, but guidance, assistance and reassurance from those who have been there before and who know what they are doing.

As a European company with roots dating back to the 1980s, trustworthiness and experience are the cornerstones of our existence. With each interaction, we strive to exemplify our unwavering commitment to our clients, drawing upon decades of experience to provide steadfast solutions.

So, what of my neighbor? Well, the next day he received an online bank payment and got his money back. A couple of years later, the lady who borrowed the money for a cup of coffee and a croissant became the Prime Minister of Finland.

Mikko Hyppönen,
Chief Research Officer, WithSecure

Paolo Points Out

The following research has been conducted by our WithSecure Intelligence team throughout the past 12 months. Following each article, Paolo offers a summation and his expert opinion on how it impacts the mid-market.

Paolo Palumbo
Vice President, WithSecure Intelligence

2023 in Brief

December 2023 Threat Report, p.9

1. Numbers of victims posted to leak sites have almost doubled from 2022 to 2023. From 2,635 to 5,079.

2. Each month in 2023 saw higher numbers of victims from its respective month in 2022.

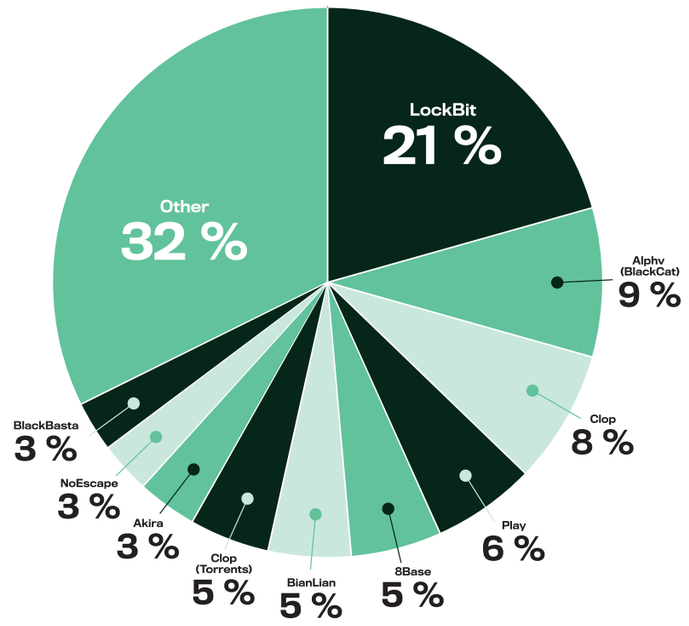
3. Lockbit were responsible for 1,046 victims. This is greater than 1 in every 5 victims posted to leak sites (20.6%).

4. 68 'brands' of multipoint extortion methods were observed in throughout 2023.

5. WithSecure observed 35 new Ransomware brands over 2023.

6. There remains no evidence to suggest that typical ransomware operators target specific industries in a discriminatory manner.

2023 Breakdown



Paolo Points Out

This article is confirmation that ransomware is going nowhere. It is a lucrative model and easy to pull off as an attack, meaning businesses will have to deal with this issue for many years to come.

The recent LockBit takedown during early 2024 is proof that we're dealing with a major societal problem, to the point that law enforcement agencies around the world must front up to the threat, as ransomware could also expand to other domains. For example, deepfakes could result in damaging photos, audio, and videos of victims, further damaging their image. A ransom could then be demanded, in order to avoid this material being published.

Hacktivist Landscape

November 2023 Threat Report, p.5-7

Hamas-linked group employ SysJoker malware

Researchers at Check Point[1] have identified a Hamas-affiliated APT group deploying the SysJoker backdoor against entities in Israel.

In December 2021, security experts at Intezer[2] initially uncovered the SysJoker backdoor capable of infecting Windows, MacOS, and Linux systems.

The version utilized in the attacks on Israel is coded in the Rust language, indicating a complete rewrite of the malware. Despite this, the malicious code maintains consistent functionalities with previous iterations. Notably, the threat actor transitioned from Google Drive to OneDrive for storing dynamic C2 (Command and Control) URLs. Intezer has provided an in-depth report[3] on the evolution of SysJoker and its attribution to a group it tracks as WildCard. The backdoor systematically gathers information about the infected system, including Windows version, username, and MAC address. This data is subsequently transmitted to the /api/attach API endpoint on the C2 server. Check Point also identified behavioral parallels with the Operation Electric Powder campaign, which targeted Israel in 2016-2017. This campaign was attributed to the Gaza Cybergang (aka Molerats), a threat actor with purported ties to the Palestinian organization Hamas.

The Gaza Cybergang exhibits a politically motivated profile and has been operational since at least 2012 and has intensified its activities since then, so it's important to note the group has been active well before the current conflict.

[1] Check Point Research. 2023. ISRAEL-HAMAS WAR SPOTLIGHT: SHAKING THE RUST OFF SYSJOKER.

[2] Mechtinger, A. et al. 2022. New SysJoker Backdoor Targets Windows, Linux, and macOS.

[3] Fishbein, N. 2023. WildCard: The APT Behind SysJoker Targets Critical Sectors in Israel.

" The Gaza Cybergang exhibits a politically motivated profile and has been operational since at least 2012. "

BiBi-Linux Wiper

Research[4] by Security Joes reveals that an anti-Israel hacktivist group, Karma, is likely responsible for attacks utilizing a wiper malware named BiBi-Linux. The malware's name plays on the nickname of Israel's Prime Minister, Benjamin Netanyahu.

In-depth analysis[5] of BiBi-Linux by Security Joes has been published, and ESET researchers have corroborated[6] these findings, identifying a Windows variant of the wiper. This malicious campaign has resulted in the destruction of data at various Israeli organizations, including a data-hosting center and a defense contractor. Notably, the use of a wiper exceeds the typical capabilities associated with hacktivist groups, underscoring Karma as a serious and formidable threat.

While the use of wipers in hacktivist activities is uncommon, Karma exhibits some similarities with another threat actor known as Moses Staff, an Iran-backed group. This connection further emphasizes the significance of Karma's capabilities and the potential geopolitical implications of their actions.

Anonymous Sudan

The group known as Anonymous Sudan has been actively engaged since 2023, and questions surrounding its origins and motives persist. Despite self-identifying as Sudanese hacktivists, compelling evidence suggests their connection to Russian interests.

A comprehensive report by Netscout[7] provides detailed insights into the group's origin and activities, shedding light on its preferred targets. The sectors favored by the group include Airlines, Education, Financial Services, Governmental departments and ministries, Hospitals, and Petroleum distributors.

Notably, Anonymous Sudan has recently declared its utilization of the SkyNet botnet, and is actively promoting access to its DDoS-as-a-service platform on Telegram. This underscores a clear financial motivation behind the group's actions. The group has claimed responsibility for recent attacks on prominent entities such as Netflix, Spotify, OpenAI, and the United Arab Emirates.

[4] Security Joes. 2023. Mission "Data Destruction": A Large-scale Data-Wiping Campaign Targeting Israel.

[5] Security Joes. 2023. BiBi-Linux: A New Wiper Dropped By Pro-Hamas Hacktivist Group.

[6] ESET Research. 2023. Twitter post.

[7] Conrad, C. and Nawrocki, M. 2023. Anonymous Sudan Campaign Analysis.

Mirai spreading

Akamai has uncovered[8] the exploitation of two zero-day vulnerabilities, reportedly orchestrated to establish a Mirai botnet capable of launching DDoS attacks. In their report, Akamai refrains from naming specific vendors or providing detailed information, citing the ongoing proper disclosure process. However, it reveals that routers and network video recording equipment are implicated, typical targets for botnets.

Mirai, a well-established and widely used botnet variant since 2016, has spawned multiple variants and spin-offs. Typically, access to Mirai botnets is traded for the express purpose of conducting DDoS attacks. The creation and availability of such botnets are increasingly becoming a problematic focus for hacktivist groups, which leverage them as platforms for executing disruptive attacks. This situation poses a growing threat and raises concerns about the potential ramifications of such activities in the cybersecurity landscape.

Water supplies targeted

CISA is responding[9] to incidents involving the compromise of Unitronics Programmable Logic Controllers (PLCs) which are commonly used in the water and wastewater industry. One such incident involved the compromise[10] of The Municipal Water Authority of Aliquippa in Pennsylvania, USA and Unitronics PLCs are likely the cause behind incidents across the US.

The attacks are being claimed by the Iran-backed group CyberAv3ngers. The group is spreading anti-Israel sentiment and acting in the interests of Iran and Hamas, displaying an ideologically motivated message on compromised equipment.

These compromises are reportedly due to the use of default credentials on PLC systems - a massive oversight - as well as a reminder that security is multi-layered and replacing default credentials with hardened ones is vital in all environments, but especially within critical national infrastructure on which millions of people rely. It also serves as a reminder that geopolitically motivated attackers and hacktivist groups can and do target organizations and individuals operating outside of the immediate geographical and industrial sphere.

" Geopolitically motivated attackers and hacktivist groups can and do target organizations and individuals operating outside of the immediate geographical and industrial sphere. "

Indian Cyber Army

The Indian hacktivist group Indian Cyber Army have begun a campaign directed at Qatari organizations and entities; these attacks are in response to the Qatar courts sentencing 8 Indian Navy officers to death following their trial in relation to alleged espionage.

The Indian Cyber Army are a capable group who engage in DDoS, website defacements and breach exposed and vulnerable networks and systems, including CCTV. The group actively promote their activity on X and Telegram and are also actively targeting Pakistan and China. Any geopolitical event in opposition to the interests of India is likely to place the opposing nation within scope of Indian Cyber Army attacks.

[8] Howard, T. 2023. InfectedSlurs Botnet Spreads Mirai via Zero-Days.

[9] U.S. Cybersecurity & Infrastructure Security Agency. 2023. Exploitation of Unitronics PLCs used in Water and Wastewater Systems.

[10] Stanish, E. 2023. Municipal Water Authority of Aliquippa hacked by Iranian-backed cyber group. CBS News.

Hacktivist Landscape

Paolo Points Out

This collection of articles highlights the growing use of cyber operations as tools for geopolitical influence and retaliation.

It is often challenging to attribute and identify whether these groups are motivated by economic, political, or geopolitical goals. However, hacktivist groups now tend to effectively incorporate the tactics, tools, and techniques used by cyber criminals in their playbook.

The state of the infostealer marketplace

October 2023 Threat Report, p.4

Infostealers (a contraction of “information stealers”) have become a common issue in the cybersecurity landscape, and now account for a large proportion of all infections that victims experience.

Upon infection with an infostealer, the malware commonly identifies, gathers, collates and exfiltrates the following information:

- Credentials (saved in browser, but also for specific applications)
- Cookies and tokens, which can be used to login to accounts by passing MFA
- Saved form data, such as credit card numbers
- Personal identifiable information,
- Cryptocurrency recovery “seed phrases”, which can be used to empty wallets
- Hardware and software information
- Screenshots
- Specific files from common directories (desktop, downloads, etc)

The following are popular infostealers currently readily available for hire/purchase on the deep and dark web. This is not an exhaustive list, but representative of the landscape:

Name	Approx. Cost
Vidar	$300 per month
RisePro	$300 per month
Lumma	$250 per month
Rhadamanthys	$250 per month
Steal C	$200 per month
Raccoon	$200 per month
Redline	$150 per month
Exela	$20 per month

This table is sorted by approximate cost per month, and there is a clear outlier in the form of newcomer Exela stealer. This new infostealer is currently being sold as a MaaS offering for the low-cost of $20, or alternatively $120 for lifetime access. This is by far the cheapest a professionalized infostealer has been offered, and greatly lowers the barrier to cybercrime entry to almost everyone.

WithSecure™ Insight

The widespread adoption and proliferation of infostealer variants is an example of the continued professionalization of cyber-crime[1]. Infostealers are quickly becoming a primary source for breached legitimate credentials, which are then weaponized and abused to commit other cyber-attacks such as the deployment of ransomware or to commit data theft. It has become a highly profitable and widespread business.

At the time of writing, the most prolific infostealer variant is arguably Redline, with stealer logs being sold in massive volumes and also freely distributed on certain Telegram channels. This is in part due to its marketing, availability, and functionality, but also its cost ($150 per month) makes it fairly accessible. The newcomer Exela is being advertised at the very low cost of $20 per month, and this is likely to make it a very popular option in the marketplace (if it’s not a scam).

As services such as infostealers become more available and popular, it will undoubtably continue to drive the price lower as groups compete for dominance. At current, a wannabe cyber-criminal can easily and with little knowledge spend their pocket money and begin their credential stealing campaign; this is a worrying issue.

[1] WithSecure. N.d. The Professionalization of Cyber Crime.

What can you do?

- Infostealers are commonly spread through the following vectors:

- **Malvertising –** The abuse of legitimate advertising platforms (Google, Facebook, etc) to direct victims to malicious websites.

- **SEO poisoning –** Similar to malvertising but relies on the manipulation of search engine algorithms to push malicious websites to the top page of search results, driving interaction.

- **Phishing/Spam –** Malware distributed via email remains a common technique and is still a major issue, especially if combined with social engineering pretexts.

- **Other –** Infostealers are commonly associated with "cracked" (pirated) software and video games, and clickbait style YouTube videos on topics such as crypto, video games or software. These vectors are aimed at consumers and the majority of "free logs" seem to originate in this type of compromise.

Organizations can help combat infostealers by raising awareness on and delivering training on these initial access vectors, as well as using security products. WithSecure's security solutions contain detections for the behaviors exhibited by infostealer malware and these are regularly tuned and updated.

Paolo Points Out

What we're seeing here is that information is power. I believe that infostealers are the equivalent of a market service run by normal businesses, in as far as threat actors can reach out and gain information about their customers.

The only difference here is that the customer or prospective customer is rather unwilling to participate! It is the same process as getting to know your target customer and then learning how to approach them, what makes them tick, and what to propose to them. Depending on the sophistication of the threat actor, this kind of profiling can lead to very sophisticated attacks.

An interesting takeaway for us is that many of the mechanics of cyber crime mirror the ways that other businesses are run.

Who will fill the QakBot void?

September 2023 Threat Report, p.3

On the 29th of August 2023 the FBI, in co-operation with law enforcement agencies across the world, announced[1] that it had disrupted and shut down the infrastructure of QakBot (QBot). QakBot is a malware and botnet used by cyber-criminals as a launchpad for other attacks, particularly ransomware, since 2008. Its scale and dominance in the cyber underground means that its demise leaves a void which must be filled and a need that must be met.

Intelligence from PRODAFT[2] and Deutsche Telekom's CERT[3] indicates some of the threat actors behind QakBot attacks/ distribution have switched to the malware DARKGATE. This includes TA577, a group known to act as an Initial Access Broker (IAB) for ransomware affiliates.

" DARKGATE is also being distributed via less common methods, such as through Microsoft Teams and LinkedIn messages. "

WithSecure™ is currently undertaking research into DARKGATE, and while we have observed what is almost certainly different campaigns to PRODAFT, their intelligence is valid and important in tracking the wider DARKGATE network.

The demise of QakBot unfortunately coincides with the return[4] of Bumblebee, following a two month hiatus. Bumblebee is another loader strongly related to ransomware infections, including the Conti spin-off group Akira.

[1] U.S. Federal Bureau of Investigation. 2023. FBI, Partners Dismantle Qakbot Infrastructure in Multinational Cyber Takedown. FBI News Stories.

[2] PRODAFT. 2023. Twitter post.

[3] Deutsche Telekom CERT. 2023. Twitter post.

[4] Intel471. 2023. Bumblebee Loader Resurfaces in New Campaign.

WithSecure™ Insight

Thanks to the shutdown of QakBot, threat actors that relied upon the malware and distributed it via phishing have had to turn to an alternative, with DARKGATE being chosen by some.

DARKGATE, is an infostealer, RAT and loader malware, and much like QakBot can be used as a springboard for further attacks. Likewise, DARKGATE is distributed in similar ways, including phishing and mal vertising. There are reports[5] however, that DARKGATE is also being distributed via less common methods, such as through Microsoft Teams and LinkedIn messages.

DARKGATE was first advertised on hacker forum XSS in June 2023 by user “Rastafareye”, being sold at a price of $100,000 per year and apparently limited to 10 buyers. This wider adoption of DARKGATE by former QakBot users suggests the malware may have been sold or adapted well beyond this initial advertisement and is likely to become a widespread issue. While our own research does not focus on a connection between DARKGATE and QakBot, it is being used almost interchangeably with multiple other malware families, including DUCKTAIL, DUCKPORT, and Redline Stealer. We have noted that the number of samples relating to DARKGATE has increased dramatically since its introduction, and this growth is ongoing.

[5] Arntz, P. 2023. Microsoft Teams used to deliver DarkGate Loader malware. Malwarebytes LABS.

What can you do?

The initial findings of PRODAFT highlight the distribution of DARKGATE globally, with a concentration of victims in North American, Russia, India, and Germany, matching the normal distribution of most malware types.

DARKGATE is primarily distributed via phishing and malvertising; our research indicates this is often via fake job advertisements targeting the digital marketing sector.

Phishing and malvertising can often be identified and therefore prevented by users who receive appropriate training. WithSecure™ has strong detections for DARKGATE, and the behavior exhibited by the malware.

Paolo Points Out

As with every type of business, cyber crime has its own ‘shadow’ supply chain. This is made up of a variety of suppliers that come and go within the space.

QakBot is an example of an implant or infrastructure that could be rented or acquired. It had competitors that are now trying to capitalize on its disappearance, highlighting, once again, that cyber criminals rely on a supply chain that is no less real than the one we see in traditional business.

Ivanti EPMM

August 2023 Threat Report, p.3

Last month's we reported on the exploitation of a vulnerability (CVE-2023-35078) in Ivanti Endpoint Manager Mobile (EPMM, formerly known as MobileIron), which led to the breaches within the Norwegian government. Since then, further vulnerabilities have been identified

These include:

- CVE-2023-35081, which has a CVSS score of 7.2 allows arbitrary unauthenticated file writes. This can be combined with CVE-2023-25078 to upload and execute files and deploy web shells.

- CVE-2023-35082, which is essentially the same vulnerability as CVE-2023-25078, but it applies to a different API endpoint. Initially, Ivanti believed that the vulnerability only existed on MobileIron versions 11.2 and below. Ivanti have since stated that this vulnerability in fact applies to all versions of EPMM, whether they have been patched for CVE-2023-25078 or not.

- CVE-2023-32560, which relates to two buffer overflow vulnerabilities in Ivanti's Avalanche product.

- CVE-2023-38035, which is another API authentication bypass vulnerability, this time in Ivanti Sentry (formerly known as MobileIron Sentry). This vulnerability is believed to be actively exploited, and according to Ivanti can be abused to "change configurations, run system commands, or write files onto the system".

WithSecure™ Insight

These new vulnerabilities come after a spate of zero-day attacks utilizing MobileIron services to target governmental departments of Norway last month. The assailants remain unknown but are almost certainly advanced and capable threat actor(s), which we reported in July's Threat Highlight Report[1].

The most recent vulnerability, CVE-2023-38035 is reported to be under active exploitation by both Ivanti and CISA, and there is a realistic possibility it is being abused by the same sophisticated threat actor who carried out last month's attacks, either at that time, or subsequently.

Proof of exploit (PoE) code for this most recent vulnerability has been published online, lowering the barrier for subsequent exploitation by less-skilled threat actors, and making patching even more important.

What can you do?

Ivanti has released patches for all the vulnerabilities referenced in this article, and you should follow their guidance as appropriate.

Regarding the newest actively exploited vulnerability in Ivanti Sentry (CVE-2023-38035), exposure is limited to Ivanti Sentry versions 9.18 and prior, and Ivanti have released a patch which should be installed urgently, due to the ongoing risk of exploitation. The vulnerability does not impact other Ivanti products, such as Ivanti EPMM or Ivanti Neurons for MDM. Ivanti has noted that while the CVSS score is high, exploitability significantly drops for customers not "exposing 8443 to the internet".

[1] WithSecure. 2023. Threat Highlight Report – July 2023. Available at: https://www.withsecure.com/content/dam/withsecure/en/resources/July2023_THR_Public.pdf

Paolo Points Out

This again reminds us of the challenges we face within supply chain security. It shows us that even if you run a really tight ship in terms of cyber security, it is difficult to achieve perfect security posture for yourself when you need to deal with the security posture of your vendors – particularly if there are many of them. A lack of visibility can therefore lead to situations like the one described in this article.

Managing this complexity then becomes even more challenging when you consider that suppliers and vendors have their own suppliers and vendors. This is where we see the chain aspect in full flow, and it can be challenging to conduct thorough due diligence on every vendor.

Further, flaws in software cannot be completely excluded, no matter how thorough you are, so it's essential to choose commercial partners that have a good track record of effectively addressing security issues. Ivanti is an excellent case in point, as they did very well to mitigate the challenges for their customers.

Microsoft ignores TeamsPhisher

July 2023 Threat Report, p.6

The default configuration of Microsoft Teams deployments allows external users to message internal users. But when they do, messages from external users are marked as external, and they will not be able to send files. This mitigates the risk of malware ingressing into a network via Teams, a vector that some may struggle to monitor, particularly without incurring additional cost.

Researchers have discovered that these security controls are implemented in the client, not the server. As such, by editing the HTTP POST request to swap the internal recipient ID and the external sender ID, the message is not flagged as internal, and sent files are received by the recipient as if they were from a trusted internal sender.

The TeamsPhisher[1] tool is a python script which not only automates the process of exploiting this vulnerability to send a message, but accepts a list of users to target, a message text, and a payload file.

Unfortunately, Microsoft have dismissed the issue and apparently do not have any plans to address the vulnerability.

“ Unfortunately, Microsoft have dismissed the issue and apparently do not have any plans to address the vulnerability. ”

[1] Reid, A. 2023. Send phishing messages and attachments to Microsoft Teams users. Published on Github under the username Oktoberfest7.

WithSecure™ Insight

Microsoft Teams is an almost ubiquitous enterprise collaboration platform, and many users in a large enterprise will trust that a message received via Teams which is not marked as internal, in contradiction to how they would normally treat contact from an unknown source.

The researchers behind TeamsPhisher have demonstrated that this issue can be used to phish a victim very easily and simply during a live red-team engagement. As they point out, phishing protections for email do not apply to Microsoft teams, so reputation, domain age, etc., are not considered. An attacker can simply register a similar domain and use it straight away in an attack.

The TeamsPhisher tool will enable attackers with very basic technical skills, who may not otherwise have been able to exploit this vulnerability, to use it in phishing campaigns against organizations which use Microsoft Teams. As such, it is likely that the targeting of this vulnerability will increase.

Microsoft's dismissal of this vulnerability is frustrating and perhaps highlights the issue of where a single organization is responsible for intended functionality and security, and there-fore has to prioritize one over the other.

What can you do?

The default configuration of Microsoft Teams means that external contacts can message members of the organization, making them vulnerable to the use of TeamsPhisher. It is possible to block this behavior by changing to the configuration of Microsoft Teams to block messages from external domains.

This is potentially problematic, as organizations may need to communicate with external parties and, as such, the better option is to add those domains to an "allow" list, while blocking all others. This would need to be maintained as and when new connections are made with other third parties.

Paolo Points Out

What this case describes is, essentially, attackers trying to take advantage of an architectural choice to deliver social engineering attacks. So, what is so interesting about that? On the surface, nothing.

But that's not entirely true. In this case, attackers didn't need to rely on sophisticated vulnerabilities. Instead, threat actors took advantage of an architectural design that didn't fully reflect the threat model that developed as a consequence of the shift in business communication from email to chat.

Clop exploits MOVEit

June 2023 Threat Report, p.3-4

Those readers with an 'ear to the ground' of the cyber landscape will be long aware of this. That said, due to its significance, and as the event has continued throughout all of June, we would like to give a comprehensive overview of the events surrounding MoveIT.

Since the end of May, Russian cyber-criminal gang Clop (Cl0p) has been exploiting vulnerabilities in the managed file transfer (MFT) service MOVEit, which is produced by Progress[1].

Vulnerable versions include:

- MOVEit Transfer 2023.0.0
- MOVEit Transfer 2022.1.x
- MOVEit Transfer 2022.0.x
- MOVEit Transfer 2021.1.x
- MOVEit Transfer 2021.0.x
- MOVEit Transfer 2020.1.x
- MOVEit Transfer 2020.0.x

The SQL injection vulnerability is tracked as CVE-2023-34362[2] and is being exploited by Clop to install a web shell called "LemurLoot". The end goal of the compromise is the theft of data, which is then used to extort impacted organizations, with the threat of the data being leaked on Clop's dark web leak site.

RegardingLemurLoot, CISA says[3]:

"LemurLoot was used as a method of persistence, information gathering and data stealing in CVE-2023-34362. The web shell imports multiple libraries including `MOVEit.DMZ.ClassLib`, `MOVEit.DMZ.Application.Files`, and `MOVEit.DMZ.Application.Users` to interact with MOVEit managed file transfer software. The web shell was initially observed with the name `human2.aspx` in an effort to masquerade as the legitimate human.aspx file present as part of MOVEit Transfer software".

This attack is widespread, with at least 3,000 vulnerable instances of MOVEit being initially detected, all of which could have been compromised by Clop. So far, Clop has posted about 80 organizations on its leak site during June, but this number is expected to grow. Clop initially made a statement saying: "if you are a government, city or police service, we erased all your data." However, this has proven to be untrue, since leaks from governmental organizations and cities are listed. Victims come from numerous sectors and are from several different nations.

The issue has snowballed due to the complexity of modern supply chains, with hundreds if not thousands of organizations becoming involved as their data was held by other – impacted – third parties. The scale of data involved is massive, and likely includes personal identifiable information (PII) which could be abused to commit fraud and identity theft.

A large number of large organizations have appeared on Clop's breach site - and continue to appear. Vast quantities of data continues to be posted to the site for download.

[1] Progress. MOVEit – Managed File Transfer Software.

[2] CVE. SQL injection vulnerability tracking of CVE-2023-34362.

[3] U.S. Federal Bureau of Investigation. 2023. #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability.

[4] Kerbs, B. 2021. Ukrainian Police Nab Six Tied to CLOP Ransomware.

WithSecure™ Insight

Clop is a well-equipped financially motivated cyber-crime group, part of a wider Russian language organized crime group often tracked as TA505. The group has developed malware (FlawedAmy, FlawedGrace, TrueBot, Dewmode, LemurLoot), compromised a myriad of organizations, developed and deployed ransomware, and engaged in data theft.

There is no evidence to suggest that Clop is motivated by anything other than money, and it has targeted multiple sectors and nations. There is no evidence to link Clop to the Russian government, suggesting the group is not state-backed, and previous arrests[4] suggest members come from former member nations of the USSR, including Ukraine.

The compromise of MOVEit aligns with other attacks by Clop, such as the attacks on GoAnywhere MFT, and Accellion File Transfer Appliance (FTA). It is clear that Clop is actively developing zero-day exploits for prevalent enterprise software, with the intention of striking large numbers of organizations within a rapid timeframe. The attractiveness of targeting file transfer services is that data can be stolen and then used for extortion, a tactic used by Clop since its origins as a ransomware group.

What can you do?

Progress, makers of MOVEit, has provided continual updates throughout the exploitation of MOVEit and have released patches to fix the zero-day SQL vulnerability, and has identified two other vulnerabilities (CVE-2023-35036[5], CVE-2023-35708[6]) which could have been exploited if not identified and patched.

This incident has also highlighted the complexity of the modern digital supply chain, with organizations being affected due to their relationship with third parties running MOVEit. Trust relationships within the supply chain are complex, and incidents like this highlight how important risk management is; can your partner ensure the safety of your data?

Unfortunately, the nature of zero-day vulnerabilities and the speed at which Clop struck makes it a very difficult thing to defend against. EDR/MDR solutions can detect anomalous behavior such as the dropping of files, etc, but early intervention is paramount.

[5] U.S. National Vulnerability Database. 2023. CVE-2023-35036 Detail.

[6] CVE. SQL injection vulnerability tracking of CVE-2023- 35708.

Paolo Points Out

This article is a stark reminder of the speed at which criminals react to vulnerabilities and how they are always ready to take advantage of weak spots in software and services. This inevitably makes the topic of supply chain security a very difficult one, where it becomes essentially impossible to completely eliminate the risk of issues originating from third-party vendors.

It is true that we are put at risk by our supply chain, but we are part of the supply chain for someone else. Therefore, it is essential that organizations take care of their own cyber security hygiene as well. Threat actors might choose our organization as a target, not for what we do but for who our customers are.

The silver lining in this story was MoveIt's approach to the situation, which was proportionate and focused on reducing the risk for its users.

Zip, a file extension or a domain

May 2023 Threat Report, p.3-4

This month Google have launched 8 new top-level domains, which include:

- .dad
- .esq
- mov
- .phd
- .foo
- .nexus
- .prof
- .zip

The security community has instantly identified the risk of domains which could easily be mistaken for file extensions such as zip archives or video files.

This has been excellently demonstrated by security researcher mr.d0x[1] who has created a proof-of-concept that demonstrates how a file archive software like WinRAR can be emulated in the browser, to create a highly convincing malicious website.

This technique would be highly compelling for the typical end-user, and would undoubtably lead to interaction at a greater level than a standard phishing email or malicious site.

There is already evidence of threat actors seeking to exploit the new TLDs with many suspicious domains being registered[2], suggesting that infrastructure aligned with common phishing themes is being built.

Some malign examples include:

- microsoft[.]zip
- microsoft-windows-update[.]zip
- chromeupdatex64[.]zip
- browser-update[.]zip
- attachment[.]zip

This issue is further aggravated by some websites/services such as YouTube automatically converting prior mentions of zip files into new hyperlinks. An example of this issue is an innocuous mention of a file called 42[.]zip on a four year old comment, which is now a clickable link that directs to a malicious domain.

This issue isn't limited to the .zip domain, and you can certainly imagine similar tactics and techniques being used to exploit the new .mov domain with video file style themes and lures.

WithSecure™ Insight

Phishing domains are often hard to detect, with threat actors going to a lot of effort to disguise them, often making them indistinguishable from a legitimate domain. The addition of new TLDs that can be easily confused with file extensions is only going to add to this problem; exploitation is already evident, with over 45k suspicious .zip domains and 2k .mov domains being identified on VirusTotal since their introduction (about 1,000 have detections on VirusTotal).

These links are often so convincing that even experienced and security-conscious users can be tricked, and training will not be enough to stop every potential incident. The onus is therefore on defenders to come up with mitigations to prevent these attacks from being successful. Very soon after public registration of .zip domains became possible, WithSecure™ telemetry detected instances of outbound requests to .zip domains where it was almost certain that filenames were being misinterpreted as domain names. This presents an issue for network monitoring teams as it decreases the fidelity of rules based on domain name matching, and analysts risk alert fatigue when investigating high risk TLDs where a lot of false positives are expected.

[1] Mr.d0x.com. 2023. File Archiver In The Browser.

[2] Sanket Yeram (@SankyYeram). 2023. Twitter post.

What can you do?

There are not many legitimate reasons for an organization to use these domains. Most companies and providers make use of the common gTLD's (General Top Level Domains) such as .com, .org, and nation specific (ccTLDs) examples such as .co.uk and .fi.

We therefore suggest that defenders consider the business need for allowing communication to domains in the zone of these new top level domains, especially .zip and .mov, and provide awareness training to end users about the dangers of file extension imitation within domains.

Paolo Points Out

The article essentially describes how to take advantage of technological change to carry out social engineering attacks. By abusing the newly introduced top-level domains, threat actors can, for example, trick people into visiting malicious websites.

This case shows once more that technological changes are strongly linked to the cyber security world. It's inevitable – and expected – that threat actors look at these changes with prying eyes, to see how they can take advantage of them.

The exploitation of 3CX

March 2023 Threat Report, p.3

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[1], CrowdStrike[2], and SentinelOne[3] 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[4], which caused widespread problems and a rethink of how organizations deal with third party software.

[1] Iddon, G. et al. 2023. Update 2: 3CX users under DLL-sideloading attack: What you need to know. Sophos News.

[2] CrowdStrike. 2023. CrowdStrike Falcon Platform Detects and Prevents Active Intrusion Campaign Targeting 3CXDesktopApp Customers. CrowdStrike Blog.

[3] Guerrero-Saade, J. A. 2023. SmoothOperator | Ongoing Campaign Trojanizes 3CXDesktopApp in Supply Chain Attack. SentielOne Blog.

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.

[4] Wikipedia. 2024 (last edited). 2020 United States federal government data breach.

Paolo Points Out

In this case, 3CX was used as a stepping stone to get to its customers – in much the same way as Solarwinds in 2021.

It proves that you might be the most security savvy company in the world, with the CISO of your dreams. Yet, when you introduce a supply chain into the equation, your estate is at increased risk of becoming compromised. Attackers will always choose the easiest path into your organization, provided it enables them to achieve their objectives.

Of course, these risks can be mitigated – for example, by doing your due diligence when selecting vendors and choosing to work with good partners.

Russia and Iran using social engineering

February 2023 Threat Report, p.5

The UK National Cyber Security Centre (NCSC) have reported[1] on two separate, but similar, spear phishing campaigns being conducted by the Russian threat actor Callisto (SEABORGI-UM) and Iranian TA453 (Charming Kitten).

The report states that both groups are targeting the following sectors/persons:

- Education
- Defense
- Government
- Non-governmental organizations
- Think-tanks
- Politicians
- Journalists
- Activists

[1] UK National Cyber Security Centre. 2023. SEABORGIUM and TA453 continue their respective spear-phishing campaigns against targets of interest. NCSC UK News.

WithSecure™ Insight

These campaigns are noteworthy, as both Callisto and TA453, are apparently using very similar TTPs, despite being entirely unconnected, and are both using social engineering to increase the likelihood of target interaction.

Social engineering is becoming far more commonplace, likely due to threat actors realizing that mass spam phishing is failing to gain the same victim interaction that it once did, thanks to better security practices and user education. In these incidents, social engineering involves:

- Reconnaissance to identify suitable targets within organizations, often conducted using social media
- Contacting targets and attempting to build rapport, often by discussing topics that would seem legitimate to the target
- Delivery of malicious links designed to capture credentials, by:
  - Typical phishing links
  - Embedded malicious links within benign documents
  - Malicious links imitating Zoom meeting links
  - Malicious links delivered via the chat capability within a video meeting

What can you do?

The NCSC are recommending the following mitigations, which we fully agree with:

- Use strong passwords
- Use multi-factor authentication (MFA), and if possible those which cannot be bypassed through MFA fatigue, sim-swapping or social engineering.
- Exercise vigilance, and be wary of unsolicited contact from any person, especially if they are asking to exchange correspondence via your personal email address.

Paolo sums up

In a nutshell, this is traditional phishing by state actors. However, just because it is nothing new, doesn't make it any less dangerous; we shouldn't lower our defences against these attacks. As a matter of fact, we are expecting more and more sophisticated attacks of this kind due to the advances in generative AI.

SEO poisoning at an all-time high

January 2023 Threat Report, p.4

Search Engine Optimization (SEO) poisoning, which is a malware delivery technique that involves getting malicious websites ranked or advertised in Google search results is reportedly[1] at an all-time high. The plethora of malware strains using Google search results as a delivery mechanism includes:

- Gootkit
- Gootloader
- IcedID[2]
- BATLOADER[3]
- PrivateLoader
- NullMixer
- RedLine infostealer
- Rhadamanthys stealer[4]
- VIDAR stealer[5]
- Yellow Cockatoo's RAT[6]
- VagusRAT

The technique involves the inclusion of specific SEO keywords that result in threat actors' malicious websites being pushed towards the top of Google search results, or alternatively, threat actors actually paying Google to get themselves to the 'Ad' top section of results, something which has been witnessed[7] on numerous occasions.

Public frustration in Google's response time and success of such campaigns may suggest a continuation of actors utilising this technique, at least in the short term.

[1] Deutsche Telekom CERT. 2023. Twitter post.

[2] Kenefick, I. 2022. IcedID Botnet Distributors Abuse Google PPC to Distribute Malware. Trend Micro Business.

[3] Kiat, N. et al. 2022. Zoom For You — SEO Poisoning to Distribute BATLOADER and Atera Agent. Mandiant.

[4] Malware-Traffic-Analysis.net. 2023. Fake Notepad++ Google Ad.

[5] Wojcieszek, K. et al. 2022. Threat Actors use Google Ads to Deploy VIDAR Stealer. Kroll.

[6] Red Canary. 2023. Yellow Cockatoo. Red Canary 2023 Threat Detection Report.

[7] Malwarebytes Threat Intelligence Team. 2022. Google ads lead to major malvertising campaign. Malwarebytes LABS.

WithSecure™ Insight

The abuse of Google search results to direct victims to malicious websites and deliver malware is something that has been occurring for a long time, that we have reported on numerous times within our Threat Highlight Report. Unfortunately, it appears that this technique has grown to be the preferred delivery mechanism for many actors, and this is likely because:

- It's non-technical, and therefore easy to set up.
- It's cheaper to set up than a spam delivery network.
- It's very common for people to search for websites/software and click the first result rather than input the full address in their browser.

" SEO poisoning is reportedly at an all-time high. "

- By imitating high-profile brands/typosquatting threat actors are able to drive victim interaction.
- Google appears to be slower to respond to takedown requests than automated spam filtering, allowing malicious search results to appear for a longer time.
- Good use of email filtering/rules and education around phishing have hampered the effectiveness of spam campaigns.

The best way to combat this technique is appropriate user education and training surrounding the use of search engines, and the use of appropriate security products that can detect malicious in-browser activity.

SEO poisoning at an all-time high

Paolo Points Out

This emphasizes the point that threat actors are using the same approaches as normal businesses to run their organization. The current situation means that any technology – no matter how seemingly harmless or far-removed from cyber crime – can be repurposed for bad. For example, using SEO techniques to push malware towards victims, as described in this article.

Paolo Sums Up

This is a fascinating set of articles, which again shows that WithSecure Intelligence is right at the forefront of cyber security. I am very proud of the team and the work they put in to highlight these issues. I would also like to mention that our team would not be able to function at such a high level without the work of the other brilliant teams within the organization.

If I had to condense my thoughts regarding cyber security research over the last 12 months, the following four issues are the most interesting considerations:

- Ransomware. It's not going anywhere and, if anything, is getting stronger.
- The professionalization of cyber crime. Cyber crime remains a professional activity and we can expect a further increase in the professionalism of cyber crime groups. More than ever, we cannot lower our guard.
- Supply chain security. It's a big issue that impacts everyone, and it is not easy to manage.
- The human factor. Humans are a major weakness in cyber security. This is not a trivial issue to overcome and we need more education, more awareness, more processes, and more policies within organizations and in our society.

Paolo Palumbo
Vice President, WithSecure Intelligence

The illusion of security

A hacker's playbook on public complacency, systematic vulnerability and the lack of understanding exposure

We tracked down a hacker and convinced them to give us their perspective on how easy it can be to break into company systems these days. The only stipulation? They had to remain anonymous...

Yet another news article about millions of passwords being leaked online. Seems this will be a good day, at least for us hackers.

The online media can't help itself and is in their usual frenzy, doing the work for me. You see, the more these news articles ooze themselves into news feeds with big scary numbers, the more it becomes background noise and people get security fatigue.

When everything is considered "breaking news", media companies get to keep writing their headlines and get their clicks and advertisement revenue. But to me and my associates, it means free victim conditioning. Your average person has enough to worry about as it is and something they have no control or understanding about quickly gets squared away in the "not me" part of the brain and is forgotten. Exactly where we want them.

And especially when headlines are written with their usual dose of fatalism – so if you can't change anything about it and everyone is a victim, why bother worrying, right?

We're always watching

People have no idea that their lives and the patterns they live by are being watched by attackers. Like busy carps going about their day while the cranes watch them, almost invisible but always stoic. Ready to act when acting is appropriate, and ready to disappear when detected.

Attackers have time to watch trends, to look at what has value in society. This means we can work out how that value is perceived, how people make up their value structure and, above all, how they react to certain impulses that move them away from a sea of uncertainty and noise towards a small convenient island of certainty. One that has been carefully prepared by the attacker, complete with fake sand and a cardboard cut-out of a palm tree. As long as you give me what I need.

The people that do understand will make sure to save their own skin. So, they change their own passwords to something that is equally lacking in strength and imagination. Ready to become next year's hacker treasure trove when the next credential dump appears.

But here's the kicker. It's not about the few individuals that are in the know, it's about the whole. It's about the trust relationships already established between all the parties. You, your customers, your IT vendors, your suppliers. Everything that makes your organization work. In the same way that a network of any kind increases in value with an increasing number of nodes. Any kind of breach or collection of passwords that leaks gives a unique insight into a company and its employees, but more importantly, their suppliers and suppliers' suppliers, and so on.

It allows any attacker the luxury to choose the path of least resistance. If the big company you want to hit with your ransomware or I.P. theft has only two contractors where one of them has passwords like ChangeMe!5 or ChangeMe!6, where their company e-mail addresses were used for personal reasons, as an attacker you know what to do. The new passwords will match the password policy and all is well, right?

You still use passwords!

This is where compliance kills. All of this wouldn't matter if businesses weren't so reliant on passwords anymore. But currently, despite more elaborate ways of bringing down risk, this is where we are. But convenience – and the storms of complaints that came before it – always wins if an organization isn't able to develop a security culture organically.

And even then, Fortune 500 companies usually have a rule that as part of their on-boarding the first five login attempts can be performed with just a password. Only thing to do now is skim LinkedIn and other social media to see which person is starting where in their new position and let the games begin. I will get lucky. I just need one. Just one. And once logged in as the new hire you put in an e-mail forwarding rule to an external e-mail address that will forward all e-mails to my throw-away e-mail account once a day at rush hour. Now, we are able to not just access the services you will be given access to, we also get to see every conference call ID and record every meeting. The perfect source for at least a dozen future phishing campaigns or making sure no one will bat an eye when I send them a file to open.

Companies and the departments that run them can only be responsible for so much. They have no clue that the developer of their supplier might have software exposed that is 15 years old with no patches installed. "We have nothing of value", they said. At least not according to them.

Or how about sensitive source code sitting on a public source code repository website filled with bugs for anyone to see and try and exploit? Companies have enough problems as it is trying to convince themselves that they can win the software update and patch race. But attackers scan the entire Internet every day looking for what is out there, so they can use it later when that new 0day vulnerability drops.

It's no longer a matter of days, it's a matter of minutes – and my bots don't need sleep. A fresh batch of target systems every day. Combine that with the fact that companies have gone to the cloud with their data and don't really know where their data is or how it can get exposed and you've got yourself a target-rich environment and enough incentives for people to start building underground careers out of it.

I just need one way in. But don't you worry. Besides, you said you weren't a target, right?

End

Notes

Notes

Notes

Notes

Notes

Notes

Notes

Notes

Notes

About WithSecure™

WithSecure™, formerly F-Secure Business, is Europe's cyber security partner of choice. Trusted by IT service providers, MSSPs, and businesses worldwide, we deliver outcome-based cyber security solutions that protect mid-market companies. Committed to the European Way of data protection, WithSecure™ prioritizes privacy, data sovereignty, and regulatory compliance.

Boasting more than 35 years of industry experience, WithSecure™ has designed its portfolio to navigate the paradigm shift from reactive to proactive cyber security. In alignment with its commitment to collaborative growth, WithSecure™ offers partners flexible commercial models, ensuring mutual success across the dynamic cyber security landscape.

Central to WithSecure's™ cutting-edge offerings is Elements Cloud, which seamlessly integrates AI-powered technologies, human expertise, and co-security services. Further, it empowers mid-market customers with modular capabilities spanning endpoint and cloud protection, threat detection and response, and exposure management.

WithSecure™ Corporation was founded in 1988, and is listed on the NASDAQ OMX Helsinki Ltd.