NOTHING SAYS 'SECURITY' LIKE A DOZEN FIREWALLS AND A BIOMETRIC SCANNER

OVERKILL SECURITY

MONTHLY DIGEST. 2024 / 04

Welcome to the next edition of our Monthly Digest, your one-stop resource for staying informed on the most recent developments, insights, and best practices in the ever-evolving field of security. In this issue, we have curated a diverse collection of articles, news, and research findings tailored to both professionals and casual enthusiasts. Our digest aims to make our content both engaging and accessible. Happy reading!

Find more:

BOOSTY.TO

SPONSR.RU

TELEGRAM

Free Issue - Casual

The perfect starting point for those new to the world of cybersecurity without financial commitment.

Paid Issue – Regular

Tailored for regular readers who have a keen interest in security and wish to stay abreast of the latest trends and updates.

Paid Issue – Pro

Designed for IT pro, cybersecurity experts, and enthusiasts who seek deeper insights and more comprehensive resources.

Read more: Boosty | Sponsr | TG

I. NEWS SECTION

Read more: Boosty | Sponsr | TG

SharpADWS is a tool for Red Team ops

SharpADWS is a tool designed for Red Team operations that focuses on reconnaissance and exploitation of Active Directory (AD) environments through the Active Directory Web Services (ADWS) protocol. Unlike traditional methods of interacting with Active Directory, which often use the Lightweight Directory Access Protocol (LDAP), tool leverages ADWS to perform its operations without directly communicating with the LDAP server. Instead, LDAP queries are wrapped in SOAP messages and sent to the ADWS server, which then unpacks and forwards them to the LDAP server. This can result in LDAP queries appearing to originate from the local address 127.0.0.1 in logs, which might be overlooked by security systems. SharpADWS can also be used to modify Active Directory data, such as granting DCSync privileges to an account for domain persistence or enabling the "Do not require kerberos preauth" option for an account to perform an AS-REP Roasting attack.

Firebase misconfiguration

Firebase is a platform that requires developers to secure individual tables and rows. However, it appears that developers either lacked the necessary security training or did not allocate sufficient time in the development lifecycle to apply the correct security controls. The misconfigurations of Firebase instances that led to the exposure of 19 million plaintext passwords and sensitive user data

Causes of the Firebase Misconfigurations

📌 **Lack of Security Rules:** Some Firebase instances had no security rules enabled, which should act as a first line of defense against unauthorized access.

📌 **Incorrect Setup:** In other cases, security rules were set up incorrectly. This improper configuration allowed for the public exposure of data that should have been private.

Affected Industries

📌 **Retail and Hospitality:** Fast food chains and other retail businesses were among those affected, with instances such as Chattr's Firebase implementation exposing user data.

📌 **Healthcare:** Healthcare applications were found to have exposed personal family photos and token IDs.

📌 **E-commerce:** E-commerce platforms leaked data from cryptocurrency exchange platforms.

📌 **Education:** A learning management system for teachers and students exposed records of 27 million users.

📌 **Technology and App Development:** The very nature of Firebase as a development platform means that a wide array of mobile and web applications across various sectors were impacted.

Integration of Evilginx 3.3 with GoPhish

Updates to Evilginx and its integration with GoPhish represent significant advancements in phishing campaign technology, offering users more sophisticated tools for creating and managing phishing attempts with enhanced customization and tracking capabilities.

📌 **Integration with GoPhish:** Evilginx now officially integrates with GoPhish by Jordan Wright. This collaboration allows users to create phishing campaigns that send emails with valid Evilginx lure URLs, leveraging GoPhish's user interface to monitor the campaign's effectiveness, including email opens, lure URL clicks, and successful session captures.

📌 **API Enhancements:** The update has introduced additional API endpoints in GoPhish, enabling changes to the results status for every sent email. This improvement facilitates more dynamic and responsive campaign management.

📌 **Lure URL Generation:** In the new workflow, when creating a campaign in GoPhish, users no longer select a "Landing Page." Instead, they generate a lure URL in Evilginx and input it into the "Evilginx Lure URL" text box. This process streamlines the creation of phishing campaigns.

📌 **Custom Parameters and Personalization:** GoPhish automatically generates encrypted custom parameters with personalized content for each link embedded in the generated email messages. These parameters include the recipient's first name, last name, and email. This feature allows for the customization of phishing pages through js_inject scripts, enhancing the effectiveness of phishing attempts.

📌 **Expanded TLD Support:** Evilginx has expanded its support for new Top-Level Domains (TLDs) to improve the efficiency of URL detection in proxied packets. This update aims to better differentiate between phishing and original domains by recognizing URLs ending with a broader range of known TLDs. The updated list includes a variety of TLDs, such as .aero, .arpa, .biz, .cloud, .gov, .info, .net, .org, and many others, including all known 2-character TLDs.

** Evilginx and GoPhish are tools used in cybersecurity, particularly in the context of phishing simulations and man-in-the-middle (MitM) attack frameworks. They serve different purposes but can be used together to enhance phishing campaigns and security testing.

📌 **Evilginx** is a man-in-the-middle attack framework that can bypass two-factor authentication (2FA) mechanisms.

It works by tricking a user into visiting a proxy site that looks like the legitimate site they intend to visit. As the user logs in and completes the 2FA challenge, Evilginx captures the user's login information and the authentication token. This method allows the attacker to replay the token and access the targeted service as the user, effectively bypassing 2FA protections.

📌 **GoPhish** is an open-source phishing toolkit designed for businesses and security professionals to conduct security awareness training and phishing simulation exercises.It allows users to create and track the effectiveness of phishing campaigns, including email opens, link clicks, and data submission on phishing pages.

Read more: Boosty | Sponsr | TG

Data Leakage and Breaches stories

There are several mentioned involve serious breaches of trust and security within the U.S. military, highlighting the challenges of safeguarding sensitive information and technology.

📌 U.S. Navy contractor who, in 2007, inserted malicious code into the software of a submarine's threat detection system. This act was a deliberate sabotage that could have compromised the safety and operational capabilities of the submarine. Malicious code in such critical systems could potentially disable threat detection, leading to undetected navigation hazards or enemy actions.

📌 Robert Birchum, a retired U.S. Air Force intelligence officer, who was sentenced to three years in federal prison for unlawfully possessing and retaining classified documents. Birchum, who retired in 2018 as a lieutenant colonel, had a 29-year career during which he served in various intelligence positions, including roles that required him to work with classified intelligence information for the Joint Special Operations Command, the Special Operations Command, and the Office of the Director of National Intelligence.

📌 Harold Martin, a former National Security Agency contractor, was arrested in August 2016 for stealing and retaining highly classified top-secret documents covering 20 years. Martin kept these documents in his home and vehicle. The stolen documents contained sensitive information about NSA planning, intelligence collection, U.S. Cyber Command capabilities, and gaps in U.S. cyber capabilities.

📌 Jerry Chun Shing Lee, a former CIA officer, was arrested in January 2018 on charges of unlawful retention of national defense information. Lee possessed notebooks that contained handwritten notes of classified information, including the true names and phone numbers of assets and covert CIA operational notes.

📌 Jack Teixeira, a member of the Massachusetts Air National Guard, pleaded guilty to leaking highly classified military documents on a social media platform. Teixeira faced a sentence of 11 to 16 years in prison for his actions.

EDR comparison

The ‘EDR Telemetry” github project aims to track and compare the telemetry features implemented in various EDR systems for Windows. The document serves as a telemetry comparison table, detailing the capabilities of different EDR products in capturing specific types of telemetry data that are relevant to cybersecurity.

📌 CrowdStrike and Microsoft Defender for Endpoint (MDE) appear to have a comprehensive implementation of features across multiple categories. Both products have a high number of features marked as fully implemented (✅) across various telemetry feature categories. This indicates a broad coverage in terms of telemetry data collection capabilities, which is crucial for effective endpoint detection and response.

📌 On the other end of the spectrum, WatchGuard and Harfanglab have a noticeable number of features marked as not implemented (❌) or partially implemented (⚠️). This suggests that these products may have gaps in their telemetry data collection capabilities compared to other EDR products listed in the document

Fake Facebook Meta Pixel tracker script

Cybersecurity researchers have recently uncovered a sophisticated credit card skimming operation that cleverly masquerades as a harmless Facebook tracker, specifically a fake Meta Pixel tracker script.

The Mechanism of the Attack

The attackers exploit the trust placed in widely recognized scripts, such as Google Analytics or JQuery, by naming their malicious scripts in a manner that mimics these legitimate services. The fake Meta Pixel tracker script, upon closer inspection, reveals JavaScript code that substitutes references to the legitimate domain "connect.facebook[.]net" with "b-connected[.]com," a legitimate e-commerce website that has been compromised to host the skimmer code. This substitution is a key part of the skimmer's operation, as it allows the malicious code to execute under the guise of a legitimate service

The Skimming Process

Once the malicious script is loaded on a compromised website, it monitors for specific actions, such as a visitor reaching a checkout page. At this point, it serves a fraudulent overlay designed to capture the credit card details entered by the victim. The stolen information is then exfiltrated to another compromised site, "www.donjuguetes[.]es," showcasing the multi-layered nature of this attack

What2Log

The What2Log is a blog dedicated to discussing various aspects of log management and analysis. The blog features updates on the What2Log tool, insights into specific logging features, and discussions on challenges related to log management. Key topics covered in the blog include:

📌 **What2Log Updates:** The blog provides detailed updates on new versions of the What2Log tool, such as the Aspen and Alder updates. These posts discuss the changes and enhancements introduced in these versions.

📌 **EventRecordID:** One of the blog posts highlights the EventRecordID, a hidden XML tag in Windows Event Logs that enriches log information.

📌 **Event ID 4672:** This post discusses the significance of Event ID 4672 in Windows, which logs special privileges assigned to new logons.

📌 **Log Management Challenges:** Several posts in the blog series titled "The Struggle is Real" address various challenges in log management, including log volume management, log analysis, event correlation, and log aggregation. These posts discuss the complexities and necessary considerations in effectively managing and analyzing logs.

Overall, the blog serves as a resource for individuals interested in the technical aspects of log management, offering both educational content and updates on the What2Log tool on Github

Read more: Boosty | Sponsr | TG

AttackGen

The GitHub repository for AttackGen provides a cybersecurity incident response testing tool that integrates large language models with the MITRE ATT&CK framework to generate tailored incident response scenarios

📌 **Scenario Generation:** AttackGen can generate unique incident response scenarios based on selected threat actor groups

📌 **Customization:** Users can specify their organization's size and industry for scenarios tailored to their specific context

📌 **MITRE ATT&CK Integration:** The tool displays a detailed list of techniques used by the chosen threat actor group according to the MITRE ATT&CK framework

📌 **Custom Scenarios:** There is an option to create custom scenarios based on a selection of ATT&CK techniques

📌 **Docker Container:** The tool is available as a Docker container image for easy deployment

📌 **Running the Tool:** Instructions are provided for running AttackGen and navigating to the provided URL in a web browser

📌 **Scenario Selection:** Users can select their company's industry, size, and the desired threat actor group to generate scenarios

SharpTerminator

SharpTerminator is part of a class of attack known as Bring Your Own Vulnerable Driver (BYOVD). This strategy involves leveraging legitimate but vulnerable drivers to bypass security measures, terminate antivirus and EDR processes, and execute malicious activities without detection. The Terminator tool represents a significant threat due to its ability to disable security solutions, thereby facilitating a range of malicious activities. These activities can range from deploying additional malware to extensive system compromise and operational disruption. The tool leverages the BYOVD technique, exploiting vulnerabilities in legitimate drivers to bypass security measures.

The use of the Terminator tool and its variants in real-world attacks has been documented, including a notable attack on a healthcare organization on December 15, 2023. In this attack, the perpetrators attempted to execute a PowerShell command to download a text file from a C2 server, which was designed to install the XMRig cryptominer on the targeted system.

Common techniques used by attackers to abuse the Terminator tool:

📌 **Exploiting Legitimate but Vulnerable Drivers**

Attackers implant a legitimate driver, which is vulnerable, into a targeted system and then exploit the vulnerable driver to perform malicious actions. This is the core principle of BYOVD attacks, where the Terminator tool leverages vulnerabilities in drivers such as zam64.sys (Zemana Anti-Logger) or zamguard64.sys (Zemana Anti-Malware) to gain kernel privileges and execute attacker-provided code in kernel context

📌 **Kernel-Level Privilege Escalation**

Successful exploitation allows attackers to achieve kernel-level privilege escalation, granting them the highest level of access and control over system resources. This escalated privilege is leveraged by disabling endpoint security software or evading their detection, thereby enabling attackers to engage in malicious activities without any obstruction

📌 **Disabling Security Solutions**

Once endpoint security defenses are compromised, attackers are free to disable antivirus and Endpoint Detection and Response (EDR) processes, deploy additional malware, or perform other malicious activities without detection. The Terminator tool specifically targets and terminates processes associated with security solutions, effectively blinding them to ongoing attacks

📌 **Use of IOCTL Codes**

The Terminator tool and its variants abuse IOCTL (Input/Output Control) codes to request functionalities from the vulnerable driver, such as attempting to terminate targeted processes. This involves sending specific IOCTL codes along with parameters like the process ID of a running process to manipulate the driver's behavior to the attacker's advantage

📌 **Administrative Privileges and UAC Bypass**

To abuse the driver effectively, a threat actor would need administrative privileges and a User Account Control (UAC) bypass, or they would need to convince a user to accept a UAC prompt. This requirement highlights the importance of privilege escalation tactics and social engineering in the successful deployment of the Terminator tool

📌 **Evading Detection**

Attackers have evolved their techniques to evade detection by security solutions. For example, the Terminator tool attempts to emulate legitimate protocol/file headers to bypass security measures, although this has been met with varying degrees of success. The use of legitimate protocols and services as command-and-control (C&C) servers or communication channels is another tactic to cover their tracks

📌 **Leveraging Public Platforms and Protocols**

Attackers also use legitimate platforms and protocols, such as instant messengers (IMs) and free email services, to communicate with compromised systems and maintain control over their targets. This technique helps to blend malicious traffic with legitimate network activity, making detection more challenging

Read more: Boosty | Sponsr | TG

BITE DISASSEMBLER FOR RUST

BiTE is designed as a platform-agnostic executable analysis tool. Its primary purpose is to provide an environment for inspecting the content of binaries and their debug information. The tool aims to support various architectures, making it versatile for different executable formats.

- **Assembly Listing Viewing:** Allows users to view a binary's disassembly alongside its associated source code.
- **GUI Porting:** Plans to port the graphical user interface to wgpu + winit.
- **Interactive Elements:** Includes a header with buttons and options, assembly listing exploration, and an interactive terminal.
- **Assembly Instruction Byte Patching:** Enables users to modify the binary directly.
- **Hex Binary Viewer:** Provides a hexadecimal view of the binary for detailed inspection.
- **Debugging Front-Ends:** Supports front-end interfaces for debugging purposes.
- **Architecture Support:** Includes support for multiple architectures such as X86-64, AArch64/Armv7, Riscv64gc/Riscv32gc, and MIPS-V.
- **Demangling Support:** Offers demangling for various targets including MSVC, Itanium, and Rust.
- **Decoding Data Structures:** Capable of decoding data structures based on each section of the binary.
- **Assembly Listing Lifting:** Transforms assembly listings into a higher-level representation.
- **Resolving Addresses:** Helps in resolving addresses within the binary.
- **Interpreting Non-Code Data:** Allows for the interpretation of data within the binary that is not executable code.
- **Creating Labels for Relative Jumps:** Facilitates the creation of labels for relative jump instructions within the disassembly

M-TRENDS 2024

The Google Mandiant report, as detailed in the M-Trends 2024, highlights a significant reduction in the time it takes for organizations to detect cyber intrusions, marking a notable improvement in cybersecurity defenses globally. It provides a mixed but cautiously optimistic view of the current state of cybersecurity.

Reduction in Median Dwell Time

The global median dwell time, which measures the average duration attackers remain undetected within a network, has decreased to its lowest point in over a decade. In 2023, this figure was recorded at 10 days, down from 16 days in 2022, and significantly lower than the 78 days observed six years ago

Increase in Ransomware Detection

The report attributes part of the reduction in dwell time to an increase in ransomware incidents, which are typically easier to detect due to their disruptive nature. Ransomware-related intrusions accounted for 23% of the total in 2023, up from 18% in 2022. These incidents are generally identified more quickly, with ransomware being detected in about six days when the notification comes from an internal source, and in five days from external notifications

Improvement in Internal Detection Capabilities

There has been a notable improvement in the ability of organizations to detect compromises internally. In 2023, 46% of intrusions were detected internally, up from 37% in 2022. This suggests that investments in cybersecurity tools and training are yielding positive results.

Geographic and Sectoral Variations

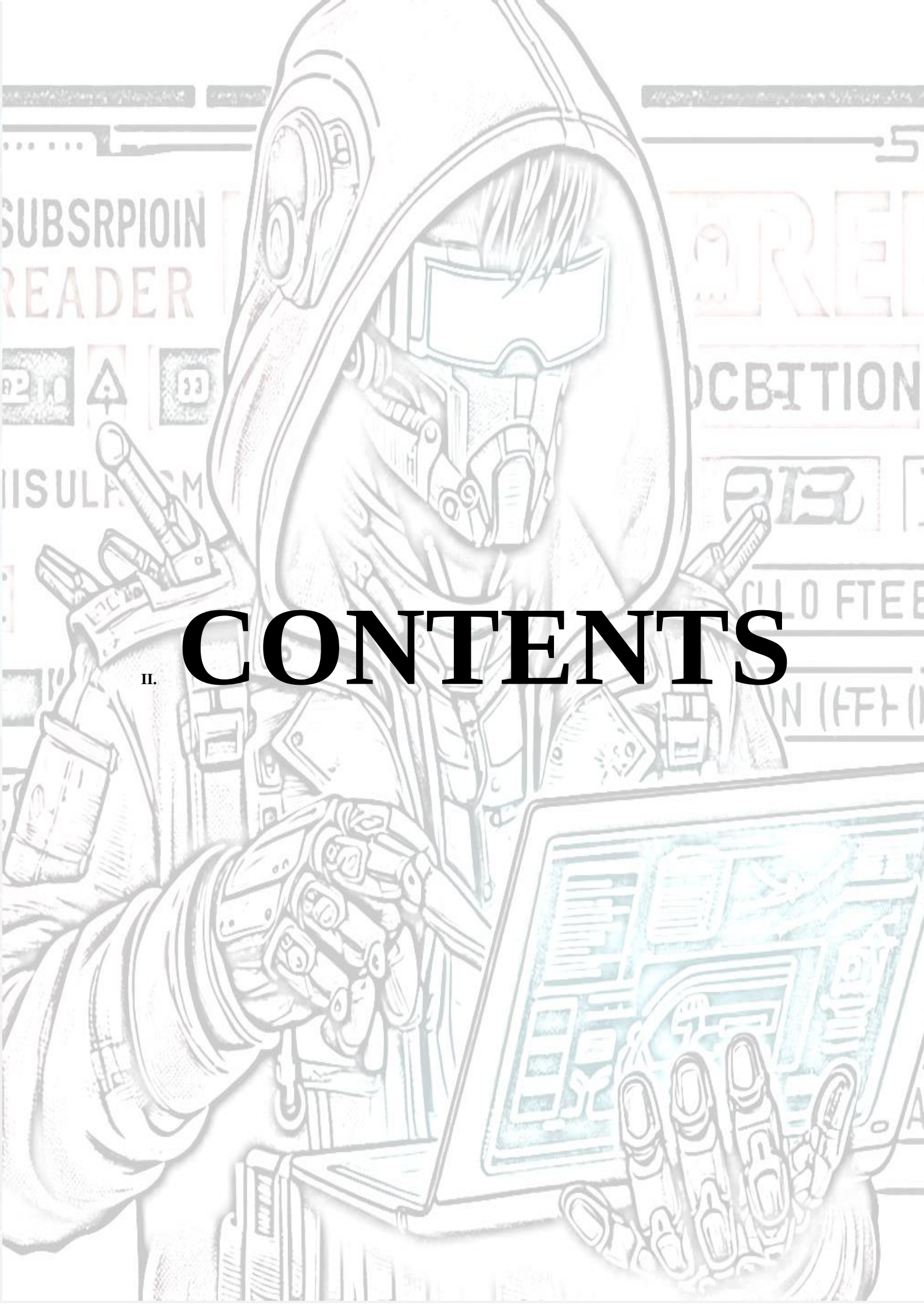
- While the global trend shows improvement, not all regions experienced the same level of progress. For instance, organizations in the Asia-Pacific region saw a dramatic decrease in median dwell time to nine days, whereas in Europe, the Middle East, and Africa, the median dwell time slightly increased
- Financial services, business and professional services, high technology, retail and hospitality, and health sectors were identified as the most targeted by cyber attackers, primarily due to the sensitive nature of the data they handle

Evolving Threat Tactics

- The report also highlights a shift in attacker tactics, with an increased focus on evasion techniques. Cyber attackers are increasingly targeting edge devices and exploiting zero-day vulnerabilities to maintain their presence undetected within networks for extended periods
- Espionage activities, particularly by groups allegedly linked to China, have intensified, with these groups focusing on acquiring zero-day exploits and targeting platforms with minimal security measures

Challenges and Recommendations

- Despite the improvements, the report underscores the ongoing challenges in cybersecurity. Attackers are adapting quickly, utilizing sophisticated methods such as "living off the land" tactics and zero-day exploits
- Mandiant emphasizes the importance of robust security strategies that include effective threat hunting programs and comprehensive investigations and remediations following breaches



CONTENTS

Read more: Boosty | Sponsr | TG

CVE Fortra's GoAnywhere MFT

CVE-2024-0204 is like a key under the mat that has not been authenticated and wants to create its own administrator user. This vulnerability can be exploited remotely and is a classic example of CWE-425: "Forced access when a web application is simply too polite to provide proper authorization." Once they've tiptoed through the secret passage, they can create an admin user with read, write, command execution, access sensitive data, deploy malware, or just take complete control because, why not? It's free-for-all!

Vulnerable versions 6.x starting from 6.0.1 and version 7.x up to 7.4.1, in which they decided to hang a lock on the door. If you're feeling DIY, the advisory suggests a workaround: delete the endpoint /InitialAccountSetup.xhtml and restart the service. For those fancy container-deployed instances, just replace the file with an empty one and give it a good ol' reboot.

StarBlizzard Phishing attacks

"Star Blizzard" should not be confused with a celestial weather phenomenon or a limited-edition threat from the Dairy Queen. This saga takes place in a digital space where the only snowflakes are the unique identifiers of each hacked system.

The audacity of Blizzard, which conducts targeted social engineering attacks on Microsoft Teams using ready-made infrastructure against everyone who uses it. The group has been doing this since November 2023, remaining unnoticed until January 12, 2024. And not just sneaking around, but camping, making a bonfire in your digital backyard while you serenely watched your favorite TV series.

In the world of cybersecurity, where the stakes are high and the attackers are always looking for the next weak link, it's a wonder that any industry can keep a straight face. So, let's all have a nervous chuckle and then maybe, just maybe, update those passwords.

ARK PINK APT

The action of the next cyber saga takes place in the mystical lands of the Asia-Pacific region, where the main characters began their digital activities in the middle of 2021 and qualitatively strengthened it in 2022. Corporate espionage, document theft, audio recordings, and data leaks from messaging platforms were all a matter of one day for Dark Pink. Their geographical focus may have started in the Asia-Pacific region, but their ambitions knew no bounds, targeting a European government ministry in a bold move to expand their portfolio. Their victim profile was as diverse as a UN meeting, targeting military organizations, government agencies, and even a religious organization. Because discrimination is not a fashionable agenda.

In the world of cybercrime, they serve as a reminder that sometimes the most serious threats come in the most unassuming packages with a pink bow.

Meet KillNet: the cyber star of the drama club "DDoS"

KillNet has risen to the top of the cyber activity leaderboard, eclipsing over a hundred other groups in grandiose proxy cyber wars. Their favorite weapon? A very sophisticated distributed Denial of Service (DDoS) attack that hits a sore spot: vital infrastructure, government services, airport websites and, why not, media companies in NATO countries. Europe is their favorite playground, where more than 180 attacks have been reported, while North America is in the corner with less than 10. However, they are not picky: the financial industry, transportation, government agencies and business services. Healthcare in the USA? Taken aim at. Gov websites from Romania to the United States? The following.

To prove themselves as professionals in their field, they expanded their activities, moving from using ready-made tools to creating their own... with a subscription to let you share your achievements.

Read more: Boosty | Sponsr | TG

UK Phishing

Phishing attacks are on the rise in the UK, and it seems our cybercriminal friends have been busy updating their deception toolkit. They're no longer just sending out those fancy "I'm the deposed prince" emails. No, they switched to high technology, plunging into the exciting world of QR phishing (or "quishing", because apparently everything is better with "q") and even connecting AI to write these such convincing fraudulent emails.

QR codes are the new golden ticket for scammers on social media, preying on the unsuspecting masses looking for concert tickets or the next big sale. Meanwhile, AI is making it easier than ever to fake someone's identity, because who needs real fingerprints or faces anymore if you got a link from "Her Majesty's Secret Service" promising you a tax refund in Poundcoin.

DCRAT (Dark Crystal Rat)

DCRat, the Swiss Army knife of the cyber underworld, a true testament to the entrepreneurial spirit thriving in the dark corners of the internet. Since its grand debut in 2018, DCRat has been the go-to gadget for every aspiring villain with a penchant for digital mischief. For the low, low price of $7, you too can own a two-month subscription to this marvel of modern malware to dip your toes into the exhilarating world of cybercrime. And for those who are truly committed to the cause, a lifetime license is available for the princely sum of $40. DCRat lures its victims with the digital equivalent of "free candy" signs. Adult content-themed baits? Check. Fake OnlyFans promises? Double-check. It's like the malware is saying, "Hey, I know you were just here for some risqué entertainment, but how about a side of identity theft?"

COMMON VULNERABILITY SCORING SYSTEM (CVSS) V4

The cybersecurity world has been graced with the latest and greatest iteration of the Common Vulnerability Scoring System, CVSS v4.0. This new version promises to revolutionize the way we assess the severity and impact of software vulnerabilities, because clearly, v3.1 was just a warm-up act.

And for those who felt left out, CVSS v4.0 now supports multiple scores for the same vulnerability. Because why have one score when you can have several?

So, there you have it, folks. CVSS v4.0 is here to save the day, with its enhanced clarity, simplicity, and a focus on resiliency. Because, as we all know, the only thing more fun than assessing vulnerabilities is doing it with a new, more complex system.

Ransomware Q3

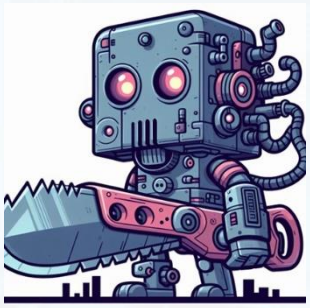
The average enterprise ransom payment soared to over $100,000, with demands averaging a cool $5.3 million. But here's the kicker: 80% of organizations have a "Do-Not-Pay" policy, and yet, 41% ended up paying the ransom last year. And for those thinking insurance might save the day, think again. A whopping 77% of organizations found out the hard way that ransomware is the party crasher not covered by their security insurance. It's like showing up to a hurricane with an umbrella.

With Ransomware as a Service (RaaS) making it easier for any wannabe cybercriminal to join the fun, we can only expect more chaos, more victims, and more snarky retellings like this one. So, here's to 2023, a year that will be remembered not for technological breakthroughs or cyber defense victories, but for the sheer audacity and success of ransomware groups. May 2024 be a bit less... successful for them.

Read more: Boosty | Sponsr | TG

Ransomware Q4

In the thrilling conclusion to 2023, ransomware groups had a banner year, really outdoing themselves in the "make everyone's life miserable" department. LockBit 3.0 took gold in the hacking olympics, followed by the plucky upstarts Clop and ALPHV/BlackCat. Apparently, 48% of organizations were feeling left out and decided to get in on the cyber attack action. Business services won the "most likely to get digitally mugged" award, with education and retail nipping at their heels. Hackers expanded their repertoire beyond boring old encryption to the much more exciting world of extortion. The US, UK and Canada took top honors in the "countries most likely to pay up" category. Bitcoins were the currency of choice for discerning hackers, because who doesn't love untraceable money?



Infamous Chisel Malware

Crafted by the digital artisans known as Sandworm, The Chisel is not just malware; it's a masterpiece of intrusion. This collection of digital tools doesn't just sneak into Android devices; it sets up shop, kicks back with a martini, and gets to work exfiltrating all sorts of juicy information. System device info, commercial application data, and oh, let's not forget the pièce de résistance, military-specific applications. Because why go after boring, everyday data when you can dive into the secrets of the military?

The Chisel doesn't just exfiltrate data; it curates it. Like a connoisseur of fine wines, it selects only the most exquisite information to send back to its creators. System device information? Check. Commercial application data? Check. Military secrets that could potentially alter the course of international relations? Double-check. It's not just stealing; it's an art form.

Cyber Toufan Al-Aqsa hacking group

In the world of cyber warfare, where the stakes are as high as the egos, the Cyber Toufan Al-Aqsa burst onto the scene in 2023 with all the subtlety of a bull in a china shop. They've been busy bees, buzzing from one Israeli company to another, leaving a trail of digital chaos in their wake. And who's behind this masquerade of mischief? Well, the jury's still out, but fingers are wagging towards Iran, because if you're going to accuse someone of cyber shenanigans, it might as well be your geopolitical frenemy, right?

The analysis delves into various aspects of the group's operations, including its background and emergence, modus operandi, notable attacks and breaches, alleged state sponsorship, and the implications of its activities for cybersecurity professionals and other specialists across different industries. It also aims to highlight its significant impact on cybersecurity practices and the broader geopolitical landscape.

Mallox

The Mallox is the digital Robin Hoods of our time, except they steal from everyone and give to themselves. Since mid-2021, they've been playing hide and seek with unsecured MS SQL servers, encrypting data, and then graciously offering to give it back for a modest Bitcoin donation. Mallox decided to go shopping for new malware toys, adding the Remcos RAT, BatCloak, and a sprinkle of Metasploit to their collection.

The analysis delves into various aspects of the group's operations, including its distinctive practice of appending targeted organizations' names to encrypted files, the evolution of its encryption algorithms, and its tactics for establishing persistence and evading defenses.

AlphV

What a dramatic cyber soap opera we've witnessed with the Alpha ransomware group, also known by their edgy alias, BlackCat. It's like a game of digital whack-a-mole, with the FBI and friends swinging the mallet of justice and the ransomware rascals popping up with a cheeky "unseized" banner as if they're playing a high-stakes game of capture the flag.

The FBI's initial victory lap was cut short when AlphV's site reemerged, now mysteriously devoid of any incriminating victim lists.

Will the FBI finally pin the cyber tail on the Black Cat, or will these digital desperados slip away once more? Stay tuned for the next episode of "Feds vs. Felons: The Cyber Chronicles."

III. VULNERABILITY IN FORTRA'S GOANYWHERE MFT (MANAGED FILE TRANSFER)

A. Introduction

CVE-2024-0204 is an authentication bypass vulnerability in Fortra's GoAnywhere MFT (Managed File Transfer) product. This vulnerability allows an unauthenticated attacker to create an administrative user for the application. The vulnerability is remotely exploitable and is listed as CWE-425: Forced Browsing, a weakness that occurs when a web application does not adequately enforce authorization on scripts or files.

The vulnerability affects Fortra GoAnywhere MFT versions 6.x from 6.0.1 and versions 7.x before 7.4.1. It was fixed in version 7.4.1, which was released on December 7, 2023. In terms of threat landscape, in 2023, file transfer applications were a top target by threat actors, highlighting the importance of securing such applications.

The vulnerability was originally discovered by researchers malcolm0x and Islam Elrfai. Fortra made customers aware of the issue through an internal security advisory post and made a patch available on December 4, 2023. Also, a proof-of-concept (PoC) exploit code for this vulnerability has been made public.

The advisory suggests that the vulnerability can be mitigated by deleting the endpoint /InitialAccountSetup.xhtml and restarting the service. For container-deployed instances, the file can be replaced with an empty file and then the service can be restarted.

B. GoAnywhere Managed File Transfer (MFT)

GoAnywhere Managed File Transfer (MFT) is a secure software solution that streamlines the exchange of data between systems, employees, customers, and trading partners. It is designed to centralize, simplify, and automate data movements, improving security and meeting compliance requirements.

GoAnywhere MFT can be deployed in various environments including on-premises, in the cloud on platforms like Microsoft Azure and AWS, or within hybrid environments. It is compatible with multiple operating systems such as Windows, Linux, AIX, and IBM i.

The software provides an intuitive browser-based interface with drag-and-drop controls, allowing users to easily customize their dashboard. It also offers a comprehensive set of workflow features that help eliminate the need for single-function tools, manual processes, or unsecure file transfer methods like FTP servers.

GoAnywhere MFT supports a wide range of protocols for secure file transfer, including SFTP (FTP over SSH), FTPS (FTP over SSL/TLS), SCP (Secure Copy over SSH), HTTP/s, AS2, AS3, AS4, and others. It also provides over 60 different tasks that can be chained together in workflows, with no programming or scripting required.

In addition to its core file transfer capabilities, GoAnywhere MFT also includes features for password security, two-factor authentication, and integration with various other systems and applications.

C. Industries covered by GoAnywhere Managed File Transfer (MFT)

GoAnywhere Managed File Transfer (MFT) is commonly used across a variety of industries due to its ability to securely automate the exchange of data. The top industries that use GoAnywhere MFT include:

- Information Technology and Services
- Computer Software
- Financial Services
- Hospital & Healthcare
- Manufacturing
- Consulting

In the IT and services industry, GoAnywhere MFT is used to integrate with web and cloud applications, ensuring data security and providing secured and automated file transfers using a centralized enterprise-level approach. It can also be used to standardize file transfer processes, reducing the need to involve development teams when transferring files:

- **Integrating with Web and Cloud Applications**: It helps in securely integrating file transfers with web and cloud-based applications.
- **Centralizing File Transfer Processes**: GoAnywhere MFT provides a centralized platform to manage all file transfers, reducing the need for development teams to be involved in the transfer process.
- **Automating File Transfers**: It automates repetitive and complex file transfer tasks, saving time and reducing errors.
- **Enhancing Security**: The solution offers enterprise-level security features, helping IT services firms to protect sensitive data during transfers.

In the computer software industry, GoAnywhere MFT can be used to automate and secure file transfers, reducing the need for custom scripts and manual processes. It can also be used to create, edit, and monitor file transfer jobs, and to perform various workflows and data translations.

- **Automating Software Distribution**: Securely automating the distribution of software updates and patches to clients.
- **Collaboration**: Enabling secure collaboration between developers, especially when working with source code and other sensitive data.
- **Regulatory Compliance**: Assisting software companies in meeting compliance requirements for software development and data handling.

In the financial services industry, GoAnywhere MFT is used to protect sensitive customer data and meet compliance requirements. It helps control the exchange of sensitive cardholder data and track file movements for easy auditing. For example, Sentinel Benefits & Financial Group uses GoAnywhere MFT to create and edit file transfer jobs, monitor security, perform various workflows, and complete hundreds of transactions in seconds.

- **Secure Transactions**: Automating and securing financial transactions, ensuring sensitive data is protected.
- **Compliance**: Meeting strict compliance requirements such as PCI DSS for the protection of cardholder data.
- **Efficient Data Handling**: Streamlining the process of creating, editing, and monitoring file transfer jobs, as demonstrated by Sentinel Benefits & Financial Group.

In the healthcare industry, GoAnywhere MFT can be used to securely transfer patient data and other sensitive information, helping healthcare organizations meet compliance requirements such as HIPAA. It can also be used to automate file transfers, reducing the need for manual processes and improving efficiency.

- **Patient Data Protection**: Securely transferring patient health information (PHI) while complying with HIPAA regulations.
- **Secure Patient Data Exchange**: Securely exchanging patient data between healthcare providers, insurers, and other stakeholders.
- **Interoperability**: Facilitating the exchange of healthcare data between different systems and organizations.
- **Compliance with Healthcare Regulations**: Ensuring that data transfers comply with healthcare regulations such as HIPAA.
- **Automating Healthcare Data Transfers**: Automating the transfer of electronic health records (EHRs), lab results, and other critical healthcare data.
- **Automating Healthcare Workflows**: Automating the transfer of lab results, billing information, and other healthcare-related data.

In the manufacturing industry, GoAnywhere MFT can be used to automate and secure the transfer of design files, production data, and other sensitive information. It can also be used to integrate with other systems and applications, improving efficiency and reducing the need for manual processes.

- **Secure Design File Transfers**: Protecting the transfer of sensitive design and production files.
- **Supply Chain Integration**: Integrating with supply chain partners for efficient data exchange.
- **Automating Manufacturing Processes**: Automating the transfer of manufacturing data, such as inventory levels, order data, and shipment tracking.

In the consulting industry, GoAnywhere MFT can be used to securely transfer sensitive client data and other information. It can also be used to automate file transfers, reducing the need for manual processes and improving efficiency.

- **Client Data Security**: Ensuring the secure transfer of sensitive client data during consulting engagements.
- **Project Collaboration**: Facilitating secure collaboration on projects that involve data sharing between consultants and clients.
- **Efficiency and Automation**: Automating the exchange of data and reports with clients, improving efficiency and reducing manual effort.

D. Root cause of CVE

The root cause of CVE-2024-0204 is identified as CWE-425: Forced Browsing. This weakness occurs when a web application does not adequately enforce authorization on scripts or files, allowing attackers to bypass authentication mechanisms and gain unauthorized access. Specifically, the vulnerability in Fortra's GoAnywhere MFT allows an unauthenticated attacker to create an admin user through the administration portal.

The exploit takes advantage of a path traversal issue, which is a type of security vulnerability that allows attackers to access files and directories that are stored outside the web root folder. Attackers can manipulate variables that reference files with dot-dot-slash (../) sequences and similar methods to access arbitrary files and directories stored on the file system. In the case of CVE-2024-0204, the path traversal issue allows access to the vulnerable /InitialAccountSetup.xhtml endpoint of the GoAnywhere MFT administration portal.

Once the attacker has access to this endpoint, they can create an administrative user with all the associated admin read and write permissions, and command execution capabilities. This effectively bypasses the normal authentication requirements, as the attacker does not need to provide any valid credentials to gain administrative access to the system.

This vulnerability is particularly risky for customers who have an admin portal exposed to the internet, as it makes the system easily accessible to potential attackers.

E. CVE Impact and affected systems

The impact of CVE-2024-0204 on GoAnywhere MFT users is significant due to the critical nature of the vulnerability. Here are the key impacts:

- **Creation of Unauthorized Admin Users**: The vulnerability allows an unauthenticated attacker to create an administrative user, which could lead to unauthorized access to the system
- **Potential for Data Breach**: With administrative access, attackers could potentially access sensitive data, which could result in a data breach
- **Malware Deployment**: Attackers with admin privileges could deploy malware, including ransomware, which could disrupt operations and lead to financial losses
- **Complete System Takeover**: The creation of admin-level users could allow attackers to take complete control of the affected system
- **Risk of Extortion**: Given the ease of exploitation, there is a risk of extortion, with attackers potentially threatening to publish sensitive data unless they receive payment
- **Operational Disruption**: Unauthorized access and potential subsequent attacks could disrupt the normal operations of the affected organizations
- **Compliance and Legal Issues**: Organizations affected by a breach resulting from this vulnerability could face compliance issues and legal consequences

GoAnywhere MFT has a CVSS score of 9.8 (severity of the vulnerability). It's also worth noting that a proof-of-concept exploit for this vulnerability has been made public, which could potentially make it easier for attackers to exploit this vulnerability.

The difference between a CVSS score of 9.8 and 10.0 primarily lies in the "Scope" metric within the CVSS scoring system. A CVSS score of 10.0 indicates that the vulnerability has the most severe impact and exploitability metrics, and its impact extends beyond the vulnerable component itself, affecting other components as well. In contrast, a CVSS score of 9.8 also represents a vulnerability with the most severe exploitability and impact metrics, but its impact does not extend beyond the vulnerable component.

In simpler terms, a CVSS score of 10.0 suggests a vulnerability that can cause more widespread damage across the system, potentially compromising additional systems beyond the initial point of exploitation. A score of 9.8, while still critical, indicates a vulnerability that is confined to the affected component and does not have the ability to impact other parts of the system.

F. Attack flow and scenario

The attack complexity level of CVE-2024-0204 is low. This means that the conditions required to exploit the vulnerability are not difficult to achieve, and the attack can be carried out consistently without any special conditions. The low complexity level, combined with the critical severity of the vulnerability, makes it a significant security concern.

1)Attack flow

The attack flow for CVE-2024-0204, an authentication bypass vulnerability in Fortra's GoAnywhere MFT, is as follows:

- **Initial Access**: The attacker, who is unauthenticated, accesses the GoAnywhere MFT administration portal. This is possible due to the path traversal issue that the vulnerability presents
- **Exploitation**: The attacker exploits the path traversal issue to gain access to the /InitialAccountSetup.xhtml endpoint
- **Creation of Admin User**: Once the attacker has access to the /InitialAccountSetup.xhtml endpoint, they can create an administrative user. This user has all the associated admin read and write permissions, and command execution capabilities
- **Potential Further Exploitation**: With administrative access, the attacker could potentially access sensitive data, deploy malware, or take complete control of the system

2)Attack scenario

Potential attack scenarios for CVE-2024-0204 could include:

- **Ransomware Attacks**: Given the history of file transfer products being used as gateways for ransomware attacks, there is a concern that CVE-2024-0204 could be exploited in a similar manner. Attackers could use the admin access gained through this vulnerability to deploy ransomware, encrypting files and demanding a ransom for their decryption
- **Data Exfiltration**: Attackers could use the admin access to exfiltrate sensitive data. This could include personal data, financial information, or proprietary business data. The stolen data could be sold on the dark web, used for identity theft, or used to gain a competitive advantage
- **System Takeover**: With admin access, attackers could potentially take complete control of the system. This could be used to disrupt operations, deploy additional malware, or use the system as a launchpad for further attacks
- **Extortion**: Attackers could threaten to publish sensitive data unless they receive payment. This could be particularly damaging for organizations that handle sensitive customer data or proprietary information
- **Sabotage**: In a more destructive scenario, attackers could use the admin access to delete or alter data, disrupt operations, or otherwise sabotage the organization. This could result in significant business impacts, including downtime and financial losses

G. Consequences

The potential consequences of an attack exploiting CVE-2024-0204 on GoAnywhere MFT users include:

- **Unauthorized Administrative Access**: Attackers can create an admin user via the administration portal without proper authorization, leading to unauthorized access to the system
- **Data Breach**: With admin access, attackers could potentially access, exfiltrate, or manipulate sensitive data, leading to a data breach
- **System Compromise**: Attackers could leverage the admin access to further compromise the system, potentially affecting the integrity, availability, and confidentiality of the system and data
- **Operational Disruption**: The unauthorized access could be used to disrupt operations, which could have significant business impacts, including downtime and financial losses
- **Extortion and Ransomware**: There is a risk of extortion, with attackers threatening to publish sensitive data unless they receive payment. The vulnerability could also be used as a gateway for ransomware attacks, as seen with previous vulnerabilities in file transfer products
- **Reputation Damage**: A successful attack could damage the reputation of the affected organization, leading to loss of customer trust and potential legal consequences
- **Compliance Violations**: Organizations could face regulatory fines and sanctions if the breach results in non-compliance with data protection laws and industry regulations

H. CVE PoC

The GitHub link https://github.com/horizon3ai/CVE-2024-0204/ leads to a Python script, which is a PoC-exploit for the vulnerability. This script, developed by Horizon3.ai, demonstrates how the authentication bypass vulnerability in GoAnywhere MFT can be exploited.

The script works by sending a POST request to the /InitialAccountSetup.xhtml endpoint of the GoAnywhere MFT application. The request includes parameters to create a new administrative user, effectively bypassing the authentication mechanism.

1)Scripts parameters

These parameters include information necessary to create a new user account, such as:

- **Username**: The desired username for the new administrative account.
- **Password**: The password for the new account, which must meet the complexity requirements of GoAnywhere MFT.
- **Email Address**: The email address associated with the new administrative account.
- **Full Name**: The full name of the individual associated with the new account.
- **Permissions**: The level of access or roles assigned to the new user, in this case, administrative privileges.

These parameters are sent in the body of the HTTP POST request as part of the request payload. The server processes these parameters and creates a new user account with the specified details.

After running the PoC-script for CVE-2024-0204, the expected response would be an indication that the script successfully created a new administrative user in the GoAnywhere MFT application. The specific details of the response would depend on the application's behavior upon user creation, but generally, you might expect:

- **HTTP Success Response**: A status code indicating success (e.g., HTTP 200 OK) from the web server, signifying that the POST request was successfully processed.
- **Confirmation Message**: A message or JSON response from the application confirming that the new administrative user has been created.
- **Error Messages**: Error messages that would indicate the request was unsuccessful.
- **Administrative Access**: The ability to log in with the newly created administrative user credentials, confirming that the user has been created with the expected permissions.

I. Other vulnerabilities related to CVE

Other vulnerabilities that have been discovered in GoAnywhere MFT include:

- CVE-2021-46830
- CVE-2023-0669

CVE-2021-46830 is a path traversal issue that could potentially allow an external user who self-registers to access unintended areas of the application. It affects versions of GoAnywhere MFT prior to 6.8.3.

CVE-2023-0669 is a pre-authentication command injection that could be exploited by an arbitrary user. It was specifically a concern for customers with an admin portal accessible through the internet. Vulnerability involves deserializing untrusted data without proper validation, impacting confidentiality and integrity.

1)Attack flow [CVE-2021-46830] and scenario

Based on the nature of CVE-2021-46830 the attack flow for such a vulnerability involves the following steps:

- **Discovery**: The attacker discovers that the web application is vulnerable to path traversal due to inadequate input validation.
- **Exploitation**: The attacker crafts a request that includes directory traversal sequences (e.g., ../) to navigate from the web root to directories that should be inaccessible.

- **Access**: The crafted request allows the attacker to access or execute files that are outside of the intended web-accessible directories.
- **Impact**: Depending on the files or directories accessed, the attacker could potentially read sensitive information, execute unauthorized commands, or leverage the access to further compromise the system.

For CVE-2021-46830 specifically, the vulnerability allowed an external user who self-registers to access unintended areas of the GoAnywhere MFT application, which could potentially lead to unauthorized information disclosure or further attacks.

A potential attack scenario could look like this:

- **Initial Access**: An attacker identifies a GoAnywhere MFT application that is accessible over the network and allows self-registration of users.
- **Exploitation**: The attacker self-registers and then manipulates file paths in the application to access directories and files outside of the intended scope.
- **Information Disclosure**: The attacker reads files that they should not have access to, potentially gaining access to sensitive information.
- **Further Attacks**: Depending on the nature of the accessed data and the functionality of the application, the attacker could potentially use the information gained to carry out further attacks.

2)Attack flow [CVE-2023-0669] and scenario

Based on the nature of CVE-2021-46830 the attack flow for such a vulnerability involve the following steps:

- **Reconnaissance**: The attacker identifies a vulnerable target system that is accessible and has the specific vulnerability, in this case, CVE-2023-0669.
- **Crafting the Attack**: The attacker creates a malicious input or payload designed to exploit the vulnerability.
- **Delivery**: The attacker sends the crafted payload to the target system. This could be through network requests, malicious files, or other means depending on the nature of the vulnerability.
- **Exploitation**: The payload triggers the vulnerability, allowing the attacker to execute arbitrary code or commands, bypass security mechanisms, or otherwise compromise the system.
- **Post-Exploitation**: After successful exploitation, the attacker may perform actions such as establishing persistent access, escalating privileges, stealing data, or spreading to other systems.

A potential attack scenario for a vulnerability like CVE-2023-0669, which requires human interaction, could involve:

- **Social Engineering**: An attacker might use social engineering techniques to trick a user into performing certain actions that would trigger the vulnerability. This could involve sending a malicious document or link to the user.
- **Malicious Document**: The attacker could craft a document that exploits the vulnerability when opened or interacted with by the user. This document could be disguised as a legitimate file to increase the chances of the user opening it.
- **Remote Code Execution**: If the vulnerability allows for remote code execution, the attacker could potentially execute arbitrary code on the victim's system once the malicious document is processed.
- **Privilege Escalation**: The attacker could use the vulnerability to gain higher privileges on the system, potentially leading to a full system compromise.
- **Data Theft or Manipulation**: With the ability to execute code, the attacker could steal sensitive data, manipulate data, or install additional malicious software on the system.
- **Persistence**: The attacker could establish a persistent presence on the affected system, allowing for continued access and further exploitation.

3)Attack flow and scenario differences

In terms of impact, CVE-2024-0204 allows an attacker to bypass authentication and create an admin user, while CVE-2021-46830 allows an attacker to traverse directories and access or execute files outside of the intended web-accessible directories.

In terms of impact, CVE-2024-0204 involves a path traversal issue in a web application that allows an attacker to bypass authentication and create an admin user, while CVE-2023-0669 involves a vulnerability that can be triggered by processing a specially crafted document.

In terms of scenario, CVE-2024-0204 involves an attacker gaining full administrative access to the system, while CVE-2021-46830 involves an attacker gaining unauthorized access to certain areas of the application.

In terms of scenario, the key difference between the two is that CVE-2024-0204 allows for direct administrative access without the need for user interaction, while CVE-2023-0669 requires a user to interact with a malicious document to trigger the vulnerability. CVE-2024-0204 is a web application vulnerability, whereas CVE-2023-0669 involves document handling, likely in a desktop or server context.

4)Impact [CVE-2021-46830]

The impact of CVE-2021-46830 is that it allows an external user who self-registers to access unintended areas of the GoAnywhere MFT application. This could potentially lead to unauthorized information disclosure or further attacks.

The severity of the impact would depend on the specific data and functionality exposed by the unintended access. For example, if the accessed areas contain sensitive data, the attacker could potentially steal this data. If the accessed areas allow the

execution of certain commands or functions, the attacker could potentially use this to further compromise the system.

5)Impact [CVE-2023-0669]

The impact of CVE-2023-0669 could include:

- **Unauthorized Access**: The attacker could potentially gain unauthorized access to the system or data, depending on the nature of the vulnerability and the system's configuration.
- **Data Theft**: If the vulnerability allows access to data, the attacker could potentially steal sensitive information.
- **System Compromise**: In some cases, the attacker could potentially use the vulnerability to execute arbitrary code or commands, which could lead to a full system compromise.
- **Denial of Service**: If the vulnerability causes the system to crash or become unresponsive, it could potentially lead to a denial of service.

6)Impact diffenences

CVE-2024-0204 has a more severe impact as it allows an attacker to gain full administrative access to the system, while CVE-2021-46830 could potentially lead to unauthorized information disclosure or further attacks.

CVE-2024-0204 has a more severe impact as it allows an attacker to gain full administrative access to the system, while the impact of CVE-2023-0669 would depend on the nature of the vulnerability and the system's configuration.

7)Consequences [CVE-2021-46830]

The potential consequences of an attack exploiting this vulnerability could include:

- **Unauthorized Access**: An attacker could potentially gain unauthorized access to directories and files outside of the intended scope. This could lead to unauthorized access to sensitive information or system resources.
- **Information Disclosure**: The attacker could potentially read files that they should not have access to, leading to the disclosure of sensitive information.
- **System Compromise**: Depending on the nature of the accessed data and the functionality of the application, the attacker could potentially use the information gained to carry out further attacks, potentially leading to a full system compromise.
- **Data Manipulation**: If the attacker gains write access to certain files or directories, they could potentially manipulate data, which could have various impacts depending on the nature of the data and the system's functionality.

8)Consequences [CVE-2023-0669]

The potential consequences of CVE-2023-0669 could include:

- **Unauthorized Access**: The attacker could gain unauthorized access to the system, potentially leading to further exploitation.
- **Data Theft**: The attacker could steal sensitive data from the compromised system, which could include personal, financial, or proprietary information.
- **System Compromise**: The attacker could execute arbitrary code, which could lead to a full system compromise, allowing them to modify, delete, or encrypt files.
- **Malware Deployment**: The attacker could use the vulnerability to deploy malware, including ransomware or a backdoor, to maintain persistent access to the system.
- **Denial of Service**: The attacker could disrupt services by crashing the system or consuming resources, leading to a denial of service.
- **Privilege Escalation**: If the vulnerability allows, the attacker could escalate their privileges on the system, gaining higher levels of control.

9)Consequences diffenences

CVE-2024-0204 could lead to a full system compromise due to unauthorized administrative access, while CVE-2021-46830 could lead to unauthorized access to certain areas of the application and potential information disclosure.

Both vulnerabilities could lead to a full system compromise, but they do so in different ways. CVE-2024-0204 involves unauthorized administrative access to a web application, while CVE-2023-0669 involves remote code execution, potentially through a path traversal flaw.

IV. STAR BLIZZARD PHISHING ATTACKS

A. Introduction

Star Blizzard, also known as the Callisto Group, SEABORGIUM, BlueCharlie, TA446, COLDRIVER, and TAG-53 is known for targeting governmental organizations, defense industry, academia, think tanks, NGOs, politicians, and others in the U.S., UK, other NATO countries, and countries neighboring Russia.

Star Blizzard's spear-phishing campaigns typically involve sending spoofed emails that appear to be from legitimate individuals or organizations. These emails are designed to trick victims into providing their email account credentials, which the group then uses to gain unauthorized, persistent access to the victims' email accounts. Once they gain access, Star Blizzard is known to set up mail forwarding rules, granting them ongoing visibility of a victim's correspondence and contact lists, and using this information for follow-on targeting and phishing activities.

B. Common targets of spear-phishing attacks

Spear-phishing campaigns typically target specific individuals or organizations with the goal of stealing sensitive information such as login credentials or infecting systems with malware. The targets are often carefully researched to increase the likelihood of a successful attack. Here are some common targets:

- **High-ranking officials within organizations**: These individuals often have access to sensitive information, making them attractive targets for spear-phishing campaigns
- **Individuals involved in confidential operations**: People who handle sensitive data or operations within a company are often targeted due to the valuable information they can provide
- **Specific employees within a company**: Spear-phishing campaigns may target specific employees within a company, especially those who have access to valuable data or systems
- **Specific organizations**: Organizations themselves can be targets of spear-phishing campaigns, especially those in sectors like government, defense, academia, and non-governmental organizations (NGOs)
- **Social media users**: Spear-phishers often use social media and other publicly available sources to gather information about potential targets

Recent years have seen a variety of spear phishing attacks, some of which include:

- **Fake Websites**: Attackers create counterfeit websites that mimic legitimate ones to deceive individuals into entering their personal information
- **CEO Fraud**: This involves impersonating a high-level executive and sending emails to employees, often in the finance department, to authorize wire transfers to fraudulent accounts
- **Malware**: Emails with malicious attachments or links that install malware on the victim's device when opened
- **Smishing and Vishing**: These are forms of spear phishing via SMS (smishing) or voice calls (vishing), where attackers pose as legitimate entities to extract personal details or financial information

Spear phishing campaigns use various tactics to increase their success rate:

- **Target Selection**: Attackers choose individuals or organizations with potential access to valuable data or financial gain
- **Reconnaissance**: Extensive research is conducted on the target to gather personal information, job roles, and interests
- **Personalization**: Emails are crafted using the target's specific information to appear credible and relevant
- **Urgency and Pressure**: Messages often convey a sense of urgency or pressure to prompt immediate action from the target
- **Shared Interests**: Attackers may exploit known interests of the target to create a convincing pretext for the email
- **Authority**: Impersonating someone in a position of authority or a known contact to elicit trust and compliance

C. Targets of Star Blizzard Campaigns

Star Blizzard has targeted a variety of sectors and individuals since 2019, including:

- **Academia**: Educational institutions and individuals associated with research or possessing valuable intellectual property

- **Defense**: Entities within the defense sector, including contractors and suppliers to the military and defense industry
- **Governmental Organizations**: Various government agencies and departments that have access to sensitive national security information
- **Non-Governmental Organizations (NGOs)**: These organizations may be targeted for their involvement in sensitive political, social, or humanitarian activities
- **Think Tanks**: Organizations that perform research and advocacy on topics such as social policy, political strategy, economy, military, technology, and culture
- **High-Profile Individuals**: Politicians and other individuals who may have access to confidential information or influence over important decisions

Specific Targets of Star Blizzard's Spear-Phishing Campaigns:

- **Personal Email Addresses**: They have predominantly sent spear-phishing emails to targets' personal email addresses, which may have less stringent security controls than corporate or business email addresses
- **Corporate or Business Email Addresses**: They have also used targets' corporate or business email addresses, indicating a comprehensive approach to targeting both personal and professional aspects of their victims' lives
- **Mailing List Data and Contacts**: By gaining access to a victim's email account, they have accessed mailing list data and a victim's contacts list, which they then use for follow-on targeting and further phishing activities
- **Compromised Email Accounts**: These are used for additional phishing activity, indicating a cycle of compromise and exploitation that can self-perpetuate and expand the scope of their campaigns

1)Common Themes or Subjects in Star Blizzard's Spear-Phishing Emails

Star Blizzard's spear-phishing emails often revolve around topics of interest to the target, which they identify through extensive research using open-source resources, including social media and professional networking platforms. They may impersonate known contacts of their targets or respected experts in the field, and create email accounts and fake social media or networking profiles to engage their targets.

2)Common Attachments or Links Included in Star Blizzard's Spear-Phishing Emails

Star Blizzard's spear-phishing emails often contain malicious links or attachments. These are designed to trick the victim into providing their email account credentials, which the group then uses to gain unauthorized, persistent access to the victims' email accounts. They also create malicious domains that resemble legitimate organizations.

3)Common Indicators of Compromise (IOCs) Associated with Star Blizzard's Spear-Phishing Campaigns

Common IOCs associated with Star Blizzard's spear-phishing campaigns include:

- Unauthorized access to personal and corporate email accounts
- Setting up of mail-forwarding rules, which gives them ongoing visibility of a victim's correspondence and contact lists
- Access to mailing list data and a victim's contacts list, which they then use for follow-on targeting
- Use of compromised email accounts for further phishing activity
- Use of the open-source framework Evilginx in their spear-phishing campaigns, which allows them to harvest credentials and session cookies to bypass the use of two-factor authentication

4)Common File Types Included in Star Blizzard's Spear-Phishing Emails

Star Blizzard often includes malicious attachments in their spear-phishing emails and use file types such as PDFs, Word documents (.doc, .docx), Excel spreadsheets (.xls, .xlsx), or other types of files that can contain embedded scripts or macros

5)Common Domains or URLs Used in Star Blizzard's Spear-Phishing Campaigns

Star Blizzard has been known to use URLs that mimic legitimate file-sharing services. Some of the URLs look like this:

- https://drive.google.com/file/d/XXXXXXXXXXXXX/view?usp=sharing
- https://onedrive.live.com/?authkey=%XXXXXXXXXXXXXXXXXXXXXXXX%XXXX&cid=8XXXXXXXXX9B7
- https://www.dropbox.com/s/XXXXXXXXXXXXX/Star_Blizzard_Report.pdf?dl=0

These URLs may look legitimate, but they are actually designed to trick victims into entering their credentials or downloading malicious files

D. Techniques of Star Blizzard Campaigns

1)Specific Techniques Used by Star Blizzard in Their Spear-Phishing Campaigns

Star Blizzard uses a variety of techniques in their spear-phishing campaigns:

- **Targeted Emails**: They predominantly send spear-phishing emails to targets' personal email addresses, although they have also used targets' corporate or business email addresses
- **Impersonation**: They create email accounts impersonating known contacts of their targets. They also create fake social media or networking profiles that impersonate respected experts
- **Malicious Domains**: They create malicious domains resembling legitimate organizations

- **Evilginx**: Star Blizzard actors use the open-source framework Evilginx in their spear-phishing campaigns, which allows them to harvest credentials and session cookies to bypass the use of two-factor authentication
- **Mail Forwarding**: After compromising the target's credentials, Star Blizzard sets up mail forwarding rules to establish ongoing visibility of a victim's correspondence and contact lists

2)Common Social Engineering Techniques Used by Star Blizzard

Star Blizzard's social engineering techniques include:

- **Research and Preparation**: They conduct extensive research using social media and professional networking platforms to identify topics of interest to engage their target
- **Impersonation**: They create email accounts and fake social media or networking profiles impersonating known contacts or respected experts
- **Building Rapport**: By leveraging the information gathered, they build a rapport with the target to make their spear-phishing attempts more convincing
- **Email Delivery**: The emails are crafted to appear legitimate and relevant to the target's interests or responsibilities, often containing malicious links or attachments
- **PDF Lures**: The PDF file sent by Star Blizzard is typically unreadable, with a prominent button purporting to enable reading the content. Pressing the button causes the default browser to open a link embedded in the PDF, leading to a credential-stealing

E. New Tactics, Techniques, and Procedures (TTPs) and Evasion Techniques of Star Blizzard

Star Blizzard has notably enhanced its ability to evade detection since 2022, focusing on improving its detection evasion capabilities. It was identified five new Star Blizzard evasive techniques:

- **Use of Email Marketing Platforms:** Star Blizzard has begun to utilize email marketing services like Mailerlite and HubSpot for directing phishing campaigns
- **Password-Protected PDF Lure Documents:** To aid in sneaking past email filters, Star Blizzard has started using password-protected PDF lure documents
- **Use of Compromised Victim Email Accounts:** They often use compromised victim email accounts to conduct spear-phishing activity against contacts of the original victim
- **Malicious Links in Email Attachments:** They use malicious links embedded in email attachments to direct victims to their credential-stealing sites
- **Use of Compromised Credentials:** Star Blizzard has been observed using compromised credentials, captured from fake log-in pages, to log in to valid victim user accounts

1)Server-side scripts

Star Blizzard has started using server-side scripts to prevent automated scanning of their actor-controlled servers. This tactic is an interesting approach that enhances their evasion capabilities.

Server-side scripts are scripts that run on the server, as opposed to client-side scripts that run in the user's browser. By using server-side scripts, Star Blizzard can control what information is sent to the client and what is kept on the server, making it harder for automated scanning tools to detect malicious activity.

The use of server-side scripts is part of a shift in tactics by Star Blizzard, demonstrating their adaptability and sophistication in evasion techniques. This tactic, along with others such as the use of email marketing platforms, password-protected PDF lure documents, and the use of compromised victim email accounts, has allowed Star Blizzard to continue its spear-phishing campaigns with increased stealth.

Here are some examples of functions that these server-side scripts might perform:

- **Collect and Send User Data**: In April 2023, Star Blizzard was observed moving away from using hCaptcha servers as the sole initial redirection. Instead, they started executing JavaScript code titled 'Collect and Send User Data' before redirecting the user
- **Refining the JavaScript Code**: In May 2023, the threat actor refined the JavaScript code, resulting in an updated version titled 'Docs', which is still in use today
- **Assessing the User's Environment**: The server-side JavaScript code is used to assess the user's environment. This information can be used to tailor the attack to the specific user, increasing the chances of success

The functions pluginsEmpty(), isAutomationTool(), and sendToBackend(data) are examples of the methods used in these scripts.

- **pluginsEmpty**(): This function checks if the plugins property of the navigator object is empty. Automated scanning tools often do not emulate plugins, so this function can help Star Blizzard identify and ignore such tools.
- **isAutomationTool**(): This function checks for signs that the client is an automated tool rather than a human user. This could involve checking for specific user agent strings, the presence of certain JavaScript properties, or the speed of interactions.
- **sendToBackend**(data): This function sends collected data back to the server. The data could include the results of the previous checks or other information about the client's environment. This information can be used to tailor the attack to the specific user, increasing the chances of success.

2)Email marketing platform services

Star Blizzard has begun to utilize email marketing services like Mailerlite and HubSpot for directing its phishing campaigns. These platforms allow the threat actor to create an

email campaign, which provides them with a dedicated subdomain on the service that is then used to create URLs. These URLs act as the entry point to a redirection chain ending at actor-controlled servers.

The use of these services offers several advantages to the threat actor. Firstly, emails sent through these platforms may be less likely to be flagged as spam or malicious by email filters, as they come from reputable services. Secondly, these platforms often provide tracking capabilities, allowing the threat actor to monitor the success of their campaigns.

Most Star Blizzard HubSpot email campaigns have targeted multiple academic institutions, think tanks, and other research organizations using a common theme, aimed at obtaining their credentials for a US grants management portal.

3)DNS provider

Star Blizzard has been using a Domain Name Service (DNS) provider to resolve actor-controlled domain infrastructure. This tactic allows the threat actor to manage and control the domains used in their attacks.

The use of a DNS provider offers several advantages to the threat actor. Firstly, it allows them to set up new domains quickly and easily for their attacks. Secondly, it can make it harder for defenders to block or take down the domains, as they are managed by a third-party service.

4)Randomizing DGA for actor registered domains

Star Blizzard has been using Domain Generation Algorithms (DGAs) to randomize the domain names for their infrastructure. DGAs are algorithms that generate a large number of domain names, which can be used as rendezvous points for command-and-control (C&C) servers or for other malicious purposes.

The use of DGAs makes it difficult for security teams and automated systems to predict and block malicious domains because the domains change frequently and can appear random. This technique is a form of domain fluxing, which helps the threat actor evade detection by blocklists, signature filters, reputation systems, and other security controls.

By using a DGA, Star Blizzard can systematically switch between domains during their attacks, making it harder for defenders to track and remove these domains. This tactic is part of their sophisticated approach to maintaining their malicious operations and avoiding disruption by cybersecurity measures.

5)Password-protected PDF lures or links to cloud-based file-sharing platforms

Star Blizzard has been using password-protected PDF lure documents or links to cloud-based file-sharing platforms as part of their spear-phishing campaigns. These tactics serve multiple purposes:

- **Password-Protected PDF Lure Documents**: By using password-protected PDFs, Star Blizzard can bypass some automated email scanning systems that cannot analyze the content of encrypted documents. The passwords for these documents are typically provided in the same phishing email or in a follow-up email.
- **Links to Cloud-Based File-Sharing Platforms**: These links lead to cloud-based platforms where the protected PDFs are stored. The use of legitimate file-sharing services can lend an air of credibility to the phishing attempt and may also evade detection by security systems that trust content hosted on these platforms.

The PDFs often contain a call to action, such as a button or link, which when clicked, redirects the user to a malicious site designed to steal credentials or other sensitive information. This technique is effective because it exploits the user's trust in familiar file-sharing services and the expectation of receiving legitimate documents.

F. attacks impact

Microsoft did fall victim to a cyberattack by threat actor known as Blizzard, also referred to as Nobelium, APT29, or Cozy Bear. The attack was detected on January 12, 2024, and began in late November 2023.

The threat actor used a password spray attack to compromise a legacy non-production test tenant account and gain a foothold. They then used the account's permissions to access a very small percentage of Microsoft corporate email accounts, including members of the senior leadership team and employees in cybersecurity, legal, and other functions.

The attackers exfiltrated some emails and attached documents, and the investigation indicates they were initially targeting email accounts for information related to Blizzard itself. The attack was not the result of a vulnerability in Microsoft products or services, and there is no evidence that the threat actor had any access to customer environments, production systems, source code, or AI systems.

1)Actions Taken by Microsoft in Response to the Blizzard Cyberattack and Secure Future Initiative

In response to the Blizzard cyberattack, Microsoft took immediate action to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access. They have begun notifying employees whose email accounts were compromised during the attack.

Microsoft assured staff and the world that the attack was not due to any specific vulnerability in Microsoft products or services, and there is no evidence that the threat actor had any access to customer environments, production systems, source code, or AI systems.

Microsoft announced that they will apply their current security standards to Microsoft-owned legacy systems, even when these changes might cause disruption to existing business processes. They also plan to make significant changes to their internal security practices.

Microsoft's response underscores its commitment to addressing the threat posed by nation-state actors like Blizzard and its commitment to responsible transparency as recently affirmed in their Secure Future Initiative (SFI).

The Secure Future Initiative (SFI) is a program introduced by Microsoft in November 2023. The SFI rests on three key pillars:

- The development of AI-based cyber defenses.
- Advancements in fundamental software engineering.

- A strategic shift in the balance between security and business risk, acknowledging that the traditional calculus is no longer sufficient

G. Defense (Microsoft Advisory)

1)Defense and protection guidance

In response to the ' Blizzard' cyberattack, Microsoft has provided guidance for defense and protection against such nation-state attacks. This guidance includes:

- **Multi-Factor Authentication (MFA)**: Microsoft emphasized the importance of enabling MFA, as the test tenant account compromised in the attack did not have MFA enabled.
- **Monitoring OAuth Applications**: Threat actors like Blizzard often use OAuth applications to help hide their activities. Microsoft recommends monitoring for suspicious OAuth applications and revoking any that are not recognized or needed.
- **Awareness of Social Engineering Attacks**: Microsoft Threat Intelligence has identified highly targeted social engineering attacks using credential theft phishing lures sent as Microsoft Teams chats by Blizzard. Awareness and training can help users recognize and avoid these attacks.
- **Network Traffic Analysis**: Blizzard used residential proxy networks to launch their attacks, routing traffic through a vast number of IP addresses also used by legitimate users. Monitoring and analyzing network traffic for suspicious patterns can help detect such activities.
- **Regular Patching and Updating**: Keeping systems and software up-to-date is crucial in defending against attacks that exploit known vulnerabilities.

Defend Against Malicious OAuth Applications

- **Audit Privilege Levels**: Use the Microsoft Graph Data Connect authorization portal to audit the privilege level of all identities, both users and service principals, in your tenant. Scrutinize privileges, especially if they belong to unknown identities, are attached to identities no longer in use, or are excessive.
- **Review ApplicationImpersonation Privileges**: Audit identities with ApplicationImpersonation privileges in Exchange Online, as these allow a service principal to impersonate a user. Use the PowerShell command Get-ManagementRoleAssignment -Role ApplicationImpersonation -GetEffectiveUsers to review these permissions.
- **Identify Malicious OAuth Apps**: Use anomaly detection policies to detect malicious OAuth apps that make sensitive Exchange Online administrative activities. Investigate and remediate any risky OAuth apps through App governance.
- **Conditional Access App Control**: Implement conditional access app control for users connecting from unmanaged devices to monitor and control how they access cloud apps.
- **Review Permissions**: Review any applications that hold EWS.AccessAsUser.All and EWS.full_access_as_app permissions. Remove them if they are no longer required.
- **Role-Based Access Control**: Implement granular and scalable role-based access control for applications in Exchange Online to ensure they are only granted access to the specific mailboxes required.

Protect Against Password Spray Attacks

- **Eliminate Insecure Passwords**: Encourage the use of strong, unique passwords and eliminate common or weak passwords that are easily guessable.
- **Educate Users**: Train users to review sign-in activity and report suspicious attempts as "This wasn't me".
- **Reset Compromised Passwords**: Reset passwords for any accounts targeted during a password spray attack, and investigate further if those accounts had system-level permissions.
- **Use Microsoft Entra ID Protection**: Detect, investigate, and remediate identity-based attacks with solutions like Microsoft Entra ID Protection.
- **Microsoft Purview Audit**: Investigate compromised accounts using Microsoft Purview Audit (Premium).
- **Enforce Password Protection**: Use Microsoft Entra Password Protection for Microsoft Active Directory Domain Services on-premises.
- **Risk Detections for User Sign-Ins**: Utilize risk detections to trigger multifactor authentication or password changes.
- **Password Spray Investigation Playbook**: Investigate any potential password spray activity using the password spray investigation playbook.

2)Detection and hunting guidance

In the wake of the Blizzard cyberattack, Microsoft has provided detailed guidance for detection and hunting of such threats. Hunting for Indicators of Compromise

- **Log Data Analysis**: Microsoft has provided detailed guidance on what to look for in log data to hunt and detect malicious activity associated with Blizzard
- **Posture Management** Tools: These tools can help organizations inventory all non-human identities and highlight unused OAuth applications, especially those with over-permissive access to impersonate every user when authenticating to Office 365 Exchange.

Microsoft's detection and hunting guidance for the Blizzard cyberattack involves reviewing Exchange Web Services (EWS) activity and using Microsoft Entra ID Protection, which has several relevant detections that help organizations identify these techniques or additional activity that may indicate anomalous activity. The use of residential proxy network infrastructure by threat actors is generally more likely to generate Microsoft Entra

ID Protection alerts due to inconsistencies in patterns of user behavior compared to legitimate activity.

Microsoft Entra ID Protection alerts that can help indicate threat activity associated with this attack include:

- **Unfamiliar sign-in properties**: This alert flags sign-ins from networks, devices, and locations that are unfamiliar to the user.
- **Password spray**: This risk detection is triggered when a password spray attack has been successfully performed.
- **Threat intelligence**: This alert indicates user activity that is unusual for the user or consistent with known attack patterns.
- **Suspicious sign-ins (workload identities)**: This alert indicates sign-in properties or patterns that are unusual for the related service principal.

3)XDR and SIEM alerts and protection

Microsoft Defender for Cloud Apps and Microsoft Defender XDR also provide alerts that can help indicate associated threat activity. These alerts include indications of a significant increase in calls to the Exchange Web Services API, suspicious metadata associated with mail-related activity, and the creation of an OAuth application that accessed mailbox items.

Microsoft Defender XDR and Microsoft Sentinel customers can also use specific hunting queries and analytic rules to find related activity in their networks. These include queries to find sign-ins by a labeled password spray IP and rules to identify password spray attempts, the granting of full_access_as_app permission to an OAuth application, and the addition of services principal/user with elevated permissions

Once an actor decides to use OAuth applications in their attack, a variety of follow-on activities can be identified in alerts to help organizations identify and investigate suspicious activity.

The following Microsoft Defender for Cloud Apps alerts can help indicate associated threat activity:

- App with application-only permissions accessing numerous emails – A multi-tenant cloud app with application-only permissions showed a significant increase in calls to the Exchange Web Services API specific to email enumeration and collection. The app might be involved in accessing and retrieving sensitive email data.
- Increase in app API calls to EWS after a credential update – This detection generates alerts for non-Microsoft OAuth apps where the app shows a significant increase in calls to Exchange Web Services API within a few days after its certificates/secrets are updated or new credentials are added.
- Increase in app API calls to EWS – This detection generates alerts for non-Microsoft OAuth apps that exhibit a significant increase in calls to the Exchange Web Services API. This app might be involved in data exfiltration or other attempts to access and retrieve data.
- App metadata associated with suspicious mail-related activity – This detection generates alerts for non-Microsoft OAuth apps with metadata, such as name, URL, or publisher, that had previously been observed in apps with suspicious mail-related activity. This app might be part of an attack campaign and might be involved in exfiltration of sensitive information.
- Suspicious user created an OAuth app that accessed mailbox items – A user that previously signed on to a medium- or high-risk session created an OAuth application that was used to access a mailbox using sync operation or multiple email messages using bind operation. An attacker might have compromised a user account to gain access to organizational resources for further attacks.

The following XDR alert can indicate associated activity:

- Suspicious user created an OAuth app that accessed mailbox items – A user who previously signed in to a medium- or high-risk session created an OAuth application that was used to access a mailbox using sync operation or multiple email messages using bind operation. An attacker might have compromised a user account to gain access to organizational resources for further attacks

Extended Detection and Response (XDR) and Security Information and Event Management (SIEM) systems can provide alerts and protection against malicious activities such as those carried out by the Blizzard threat group.

Microsoft Defender for Cloud Apps can generate alerts for various suspicious activities, including:

- An app with application-only permissions accessing numerous emails.
- An increase in app API calls to Exchange Web Services (EWS) , especially after a credential update.
- App metadata associated with suspicious mail-related activity.
- A suspicious user creating an OAuth app that accessed mailbox items.
- XDR can also generate an alert when a suspicious user creates an OAuth app that accesses mailbox items.

According to MS guidance these alerts can help organizations identify and investigate suspicious activities related to OAuth applications, which are often used in attacks like those carried out by Blizzard.

- To detect password spray attacks, security teams can use various hunting queries that analyze log data for signs of such attacks. Here are some examples of hunting queries and techniques that can be used:
- **Failed Authentication Attempts Across Multiple Accounts:** Look for sudden spikes in the number of failed login attempts or locked accounts, which can indicate a password spray attack
- **Sign-in Attempts from Suspicious Locations:** Monitor sign-in attempts from locations that are unusual

for the user, as attackers may use IP addresses from different geographic regions

- **Unusual Sign-in Times:** Password spray attacks often occur at odd hours when fewer users are likely to be active, so monitoring for authentication attempts during these times can be useful
- **Low and Slow Attack Indicators:** Detect password spray attacks that attempt to stay under the radar by not triggering account lockouts or bad password thresholds
- **Advanced Hunting Queries:** Use a query-based threat hunting tool like Microsoft Defender's Advanced Hunting to inspect events in your network and gather more information related to password spray alerts
- **Alert Classification:** Check whether the user received other alerts before the password spray activity, such as impossible travel alerts, activity from infrequent countries/regions, or suspicious email deletion activity

Here are some hunting queries provided by Microsoft:

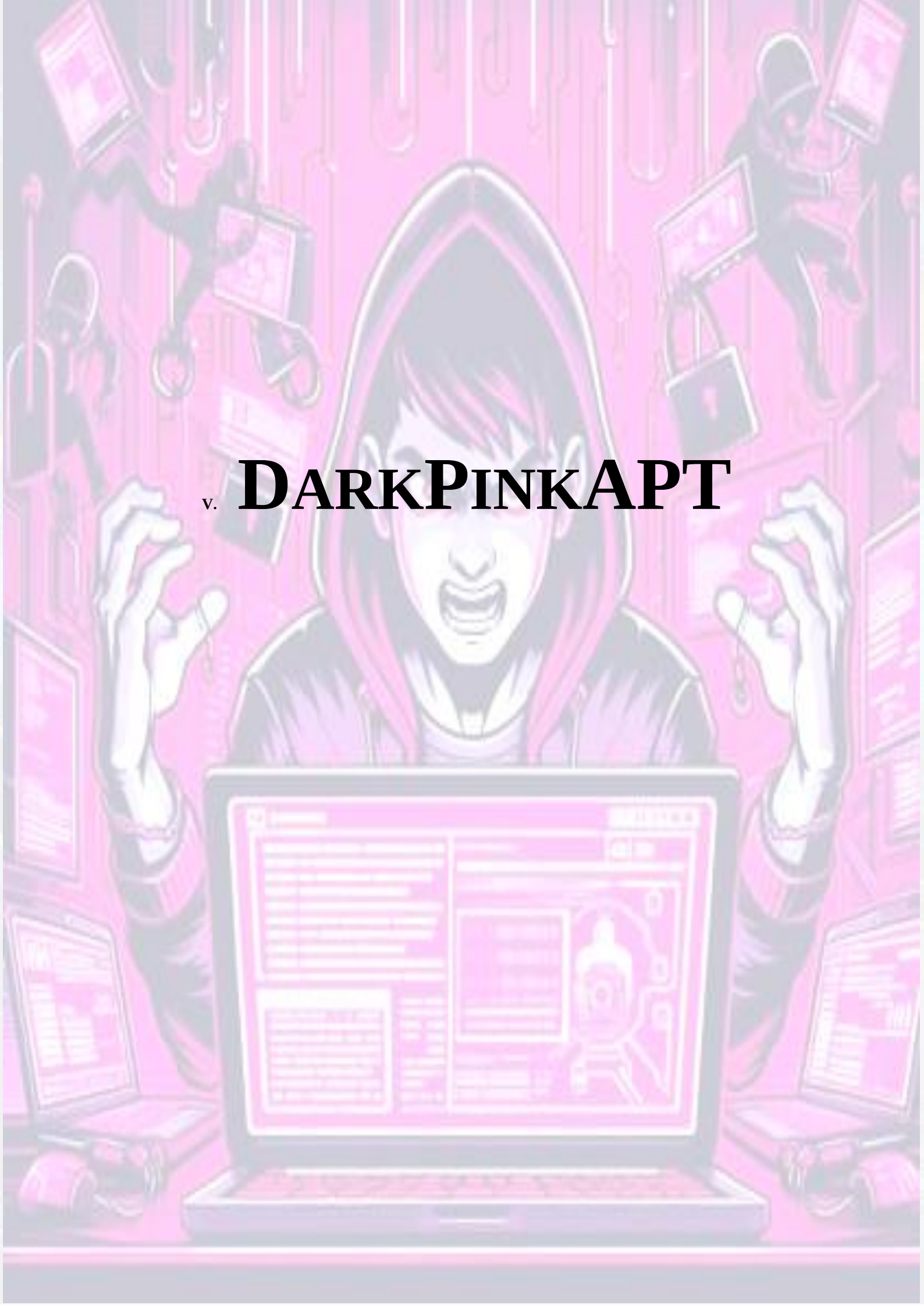
```
// Find sign-ins by a labeled password spray IP
IdentityLogonEvents
| where Timestamp between (startTime .. endTime)
| where isnotempty(IPTags) and not(IPTags has_any('Azure','Internal Network IP','branch office'))
| where IPTags has_any ("Brute force attacker", "Password spray attacker", "malicious", "Possible Hackers")

// Find MailItemsAccessed or SaaS actions performed by a labeled password spray IP
CloudAppEvents
| where Timestamp between (startTime .. endTime)
| where isnotempty(IPTags) and not(IPTags has_any('Azure','Internal Network IP','branch office'))
| where IPTags has_any ("Brute force attacker", "Password spray attacker", "malicious", "Possible Hackers")
```

Network traffic analysis can be a powerful tool in detecting password spray attacks:

- **Intrusion Detection Systems (IDS):** IDS tools monitor network traffic and flag suspicious login activities. They analyze login attempts, account lockouts, and authentication failures to identify potential password spraying attacks
- **Security Monitoring**: Continuous monitoring of user login activities and abnormal patterns can help identify potential attacks. Monitoring tools can track login attempts from unusual locations, or at unusual times, which could indicate a password spraying attack
- **User Behavior Analysis:** Analyzing user behavior can help detect suspicious activities. Deviations from normal behavior, such as login attempts outside of regular working hours or simultaneous login attempts from multiple locations, can be red flags for password spraying attacks
- **Configure Security Password Settings:** If your organization utilizes a Security Logging Platform, ensure that it's configured to identify or detect failed login attempts across all systems. This will help you detect those tell-tale signs of password spraying attacks in the future
- **Monitoring and Logging:** These are some of the best proactive ways to detect password-spraying attacks. They help to detect failed login attempts and inform the IT Administrator accordingly. For example, if there are 5 unsuccessful login attempts, the password policy locks out the user account, and the network monitoring solution triggers an alarm to the IT Administrator
- **SIEM (Security Information and Event Management):** In case there is unusual behavior in your organization, your SIEM will pick it up. SIEM solutions aggregate and analyze event data in real time from network devices, servers, domain controllers and more, providing security intelligence for real-time analysis of security alerts generated by applications and network hardware

Organizations can use OAuth application permissions to detect potential security vulnerabilities in several ways:

- **Investigate, Remediate Risky OAuth Apps:** Organizations can use tools like Microsoft Defender for Cloud Apps to investigate and remediate risky OAuth apps. This involves scrutinizing apps that have not been updated recently, apps that have irrelevant permissions, and apps that appear suspicious based on their name, publisher, or URL. OAuth app audit can be exported for further analysis of the users who authorized an app
- **Create Policies to Control OAuth Apps:** Organizations can set permission policies to get automated notifications when an OAuth app meets certain criteria. For example, alerts can be set up for apps that require a high permission level. OAuth app policies enable organizations to investigate which permissions each app requested and which users authorized those permissions
- **Identify Vulnerabilities in OAuth Implementation:** Vulnerabilities can arise in the client application's implementation of OAuth as well as in the configuration of the OAuth service itself. Identifying and exploiting these vulnerabilities can help organizations protect their own applications against similar attacks
- **Monitor for Malicious OAuth Applications:** Threat actors can misuse OAuth applications to automate financially driven attacks. Monitoring for such misuse can help organizations detect and respond to potential security vulnerabilities. For example, Microsoft provides queries that can be used to identify high outbound email senders and suspicious email events
- **Understand the Impact of Malicious OAuth Application Consent:** If a user grants access to a malicious third-party application, the application can access the user's data and perform actions on their behalf. Understanding the impact of such actions can help organizations develop strategies to detect and mitigate potential security vulnerabilities



v. DARKPINKAPT

A. Introduction

Advanced persistent threat (APT) attacks spreading throughout the Asia-Pacific (APAC) region, attributed to a group known as Dark Pink, also referred to as the Saaiwc Group began as early as mid-2021, but escalated significantly in the latter part of 2022. Many of these attacks were directed at APAC countries, but the threat actors also expanded their scope to target a European governmental ministry.

In October 2022, Dark Pink initiated an unsuccessful attack against a European state development agency operating in Vietnam. The group employs a variety of tools and custom-built malicious software designed for data theft and espionage. A significant part of Dark Pink's success can be attributed to the spear-phishing emails used to gain initial access. These emails contain a shortened URL linking to a free-to-use file sharing site, where the victim is presented with the option to download an ISO image that contains all the files needed for the threat actors to infect the victim's network.

Dark Pink APT attacks are characterized by their sophistication and versatility. The group uses spear-phishing emails as the initial access vector, luring victims into downloading a malicious ISO image. The group employs a suite of customized malware tools to execute their attacks. They also use advanced techniques to evade detection.

The consequences of a successful Dark Pink APT attack can be devastating for the affected organization and potentially for national security, given the high-profile nature of their targets. The group's advanced persistence mechanisms allow them to maintain access to a victim's network for a long period of time, enabling them to continue to exfiltrate data and potentially cause further damage.

Timeline of Dark Pink APT Group's Operations

- **Mid-2021**: The Dark Pink APT group's activities are first observed.
- **2022**: Their operations escalate, particularly in the latter part of the year.
- **October 2022**: An unsuccessful attack is launched against a European state development agency operating in Vietnam.
- **January-April 2023**: New modules are uploaded to a GitHub account associated with the group, suggesting ongoing development of their toolset

B. Primary Objectives of Dark Pink APT Group

This part discusses the main goals of the Dark Pink APT, which include corporate espionage, document theft, and data exfiltration. It also mentions the group's links to a GitHub account where they store PowerShell scripts, ZIP archives, and custom malware. The primary objectives of the Dark Pink APT group include:

- **Corporate Espionage**: One of the main goals of the Dark Pink APT group is to conduct corporate espionage, which involves stealing sensitive information from corporations for competitive advantage or other malicious intent
- **Document Theft**: The group is actively engaged in the theft of documents, which likely contain confidential and proprietary information, from their targets
- **Audio Surveillance**: Dark Pink has the capability to capture audio through the microphones of compromised devices, which can be used for eavesdropping on private conversations and meetings
- **Data Exfiltration from Messaging Platforms**: The group also focuses on exfiltrating data from various messaging platforms, indicating an interest in personal communications and potentially sensitive information shared through these channels
- **Geographical Focus**: While the majority of Dark Pink's attacks have been directed at countries in the Asia-Pacific region, they have also targeted a European governmental ministry, showing an expansion in their geographical scope
- **Victim Profile**: Confirmed victims include military organizations in the Philippines and Malaysia, government agencies in Cambodia, Indonesia, and Bosnia and Herzegovina, as well as a religious organization, demonstrating the group's interest in high-value and diverse targets
- **Spear-Phishing for Initial Access**: A significant factor in the success of Dark Pink's operations is the use of spear-phishing emails that contain a shortened URL. This URL leads victims to a file-sharing site where they are tricked into downloading an ISO image containing malicious files necessary for network infection
- **Evolution of Exfiltration Techniques**: Dark Pink has evolved its data exfiltration techniques, moving from using email and public cloud services like Dropbox to employing the HTTP protocol and a Webhook service in more recent attacks

C. Tools Used by Dark Pink APT Group

This section introduces the tools widely used by Dark Pink APT Group to attack, gain access and exfiltrate data from devices across the world.

1) Tools Used by Dark Pink APT Group

The Dark Pink APT group utilizes a suite of customized malware tools in their attacks, primarily relying on spear-phishing emails to gain access to their targets' networks. Notably, they use TelePowerBot and KamiKakaBot, which are designed to exfiltrate sensitive data from compromised hosts. They have been linked to a new version of the KamiKakaBot malware, which is delivered via phishing emails containing a malicious ISO file. This file contains a WinWord.exe file, which is used to stage a dynamic link library (DLL) sideloading attack. The group has also been found to use legitimate MsBuild.exe to run the KamiKakaBot malware on victims' devices. The malware's obfuscation technique has improved to better evade anti-malware measures, and it uses an open-source .NET obfuscation engine to hide itself. The group also uses a special messenger exfiltration utility named ZMsg, which is downloaded from GitHub and used to steal communications from Viber, Telegram, and Zalo.

In addition to these, Dark Pink has been found to use DLL side-loading and event-triggered execution methods to run its payloads. They also employ a variety of techniques and services for data exfiltration, including email, public cloud services like Dropbox.

2)Modifications Made to the Tools Used by Dark Pink APT Group

The group has links to a GitHub account where they store PowerShell scripts, ZIP archives, and custom malware designed for future deployment on targeted devices. They have also been observed exploiting the WinRAR 0-Day vulnerability (CVE-2023-38831) in their attacks to execute malicious unauthorized code. They have been exploiting this vulnerability by embedding malicious executables within commonly used file types, such as PDFs and JPGs, within ZIP archives. This tactic allows attackers to install malware on a user's device without arousing suspicion, as the victim believes they are interacting with a harmless file. The exploitation file constructed by Dark Pink includes a PDF bait file and a folder with the same name. Inside the folder, there are two files: one is an exe program with the same name as the PDF bait file, and the other is a library file named ‘twinapi.dll’. The group also uses techniques such as USB infection and DLL exploitation.

3)New Tactics Employed by Dark Pink APT Group

New tactics employed by the Dark Pink APT group include the use of different Living Off the Land Binaries (LOLBins) techniques and leveraging the functionalities of an MS Excel add-in to ensure persistence. They have also been found to exfiltrate stolen data over HTTP using services like webhook.site, which allows them to set up temporary endpoints to capture and view incoming HTTP requests. Payloads are also being distributed through the TextBin.net service, and the group has been observed exfiltrating stolen data over HTTP using a service. These new tactics indicate the group's ongoing efforts to enhance their capabilities, evade detection, and maintain control over compromised networks.

D. Data Extraction Techniques

The data extraction techniques include:

- **Variety of Exfiltration Techniques**: Dark Pink has employed a range of techniques and services to exfiltrate data from their targets. This demonstrates the group's adaptability and sophistication in ensuring successful data theft
- **Public Services**: Publicly available cloud services such as Dropbox have been used by Dark Pink for data exfiltration
- **Use of Email and Cloud Services**: In previous attacks, the group sent stolen information via email or utilized public cloud services like Dropbox for data exfiltration. This indicates that they leveraged commonly used communication and storage platforms to move data out of compromised networks
- **Shift to HTTP Protocol and Webhook Service**: More recently, Dark Pink has shifted to using the HTTP protocol and a Webhook service to exfiltrate stolen data. This change in tactics could be an attempt to evade detection by security systems that are more focused on traditional exfiltration methods
- **Evolution of Tactics**: The evolution from using email and cloud services to HTTP and Webhook services suggests that Dark Pink is continuously refining its exfiltration methods to stay ahead of cybersecurity defenses

As mentioned above The Dark Pink APT group uses Telegram and a service called Webhook for data exfiltration.

Telegram: Dark Pink uses Telegram for both command-and-control and data exfiltration. The group has been observed to use a Telegram bot for executing commands and managing data theft. The stolen data is often sent to a Telegram chat in a zip archive. This method provides a secure and encrypted channel for data exfiltration, making it harder for security systems to detect and block the data transfer

Webhook: Dark Pink has also been observed to use a service called Webhook.site for data exfiltration. Webhook.site is a service that allows users to create temporary endpoints to capture and view incoming HTTP requests. Dark Pink uses this service to exfiltrate stolen data over HTTP. This method allows the group to send data to a specific URL, which can then be accessed and retrieved by the threat actors. This technique can be used to evade detection by security systems that are more focused on traditional exfiltration methods

The group uses a private GitHub repository to host additional modules downloaded by its malware. They have also developed new data exfiltration tools to dodge detection. One of the group's techniques involves the use of the KamiKakaBot malware, which is primarily designed to steal data stored in web browsers such as Chrome, Edge, and Firefox, including saved credentials, browsing history, and cookies. Dark Pink has also been found to exfiltrate stolen data over HTTP using a service.

Furthermore, they employ a specialized toolkit that includes a custom information stealer coded in .NET, known as Cucky. This tool is proficient in extracting passwords, browsing history, login credentials, and cookies from a range of web browsers targeted by the group. The stolen data is stored locally in the %TEMP%\backuplog directory, without transmitting it over the network

E. Dark Pink Origins and Affiliates

Many Dark Pink's attacks were directed at countries in the Asia-Pacific region, although the group expanded its scope to target a European governmental ministry. This indicates a broadening of their operational scope.

1)Industries Targeted by Dark Pink APT Group

The Dark Pink APT group has targeted a wide range of industries, including government, military, non-profit

organizations, educational institutions, and development agencies across the Asia-Pacific region and Europe. Specific industries mentioned in the context of their attacks include retail, healthcare, gaming, technology, software, pharmaceuticals, aerospace, defense, automotive, and media.

2)New Industries Targeted by Dark Pink APT Group

The Dark Pink APT group has expanded its target industries and geographical reach. While the group was previously thought to focus mainly on Southeast Asian countries, new victims have been identified in Belgium, Thailand, and Brunei. The group has been linked to five new attacks aimed at various entities in these countries, including educational institutions, government agencies, military bodies, and non-profit organizations. This indicates the group's continued focus on high-value targets and its expansion into new industries and regions.

In addition to these, the group has also targeted entities in the retail, healthcare, gaming, technology, software, pharmaceuticals, aerospace, defense, automotive, and media industries. The group's targets include diplomatic, military, and various industries in countries such as Cambodia, Indonesia, Malaysia, the Philippines, Vietnam, Bosnia and Herzegovina, and others

F. Initial Access and Trojan Execution and Persistence

This section explains how Dark Pink gains initial access to their targets, primarily through spear-phishing emails containing a shortened URL that leads to a free-to-use file sharing site.

The initial methods include:

- **Spear-Phishing Emails**: A significant part of Dark Pink's success can be attributed to the spear-phishing emails used to gain initial access. These emails contain a shortened URL linking to a free-to-use file sharing site
- **ISO Image**: The victims are presented with the option to download an ISO image from the file sharing site. This image contains all the files needed for the threat actors to infect the victim's network
- **Trojan Execution and Persistence**: Once the ISO image is downloaded and opened, it triggers the execution of a Trojan on the victim's device. This Trojan is designed to maintain persistence on the infected system, allowing the threat actors to maintain access over an extended period

Spear-phishing is a type of phishing attack that targets specific individuals or groups within an organization. It is a potent variant of phishing, a malicious tactic which uses emails, social media, instant messaging, and other platforms to get users to divulge personal information or perform actions that cause data loss or financial loss. Spear-phishing attacks are highly personalized and often involve prior research about the target. The attackers disguise themselves as a trustworthy friend or entity to acquire sensitive information, typically through email or other online messaging. The goal of spear-phishing is to steal sensitive information such as login credentials or infect the victim's device with malware. Spear-phishing is a targeted form of phishing where cybercriminals send highly convincing emails to specific individuals within an organization. These emails often contain malicious attachments or links that, when clicked, can deliver Trojans to the victim's system. For instance, the Ursnif Trojan uses a company's stored emails to send what appear to be legitimate emails. These emails contain a Word document attachment with a malicious macro that downloads the malware. Once the payload is executed, the victim's computer becomes a delivery vehicle to spread within an organization

ISO images are files that contain a complete copy of a CD, DVD, or other types of media. They are often used to distribute software or data. Cybercriminals have started using ISO files for their initial compromise because they can help evade security checks designed to look for zipped files. Malicious ISO files have been used to deliver various types of malware, including the IcedID, LokiBot, and NanoCore trojans. The ISO file is typically delivered as part of a malspam campaign, and when the user clicks on the ISO file, it creates a new virtual hard drive disk. ISO images can also be used to deliver malware. Cybercriminals have been observed using ISO image files in malicious spam campaigns to deliver Trojans like LokiBot and NanoCore. The ISO file is delivered as a ZIP archive via a malicious spam mail campaign. When the user clicks on the ISO file, it creates a new virtual hard drive disk. The ISO file contains a malicious LNK file and a hidden directory containing a payload. When the victim clicks on the LNK file, it triggers the execution of the payload. This technique has grown in use as threat actors look to evade Mark-of-the-Web controls. ISO files are often overlooked by antivirus software, making it more likely that attackers can deliver their payload undetected.

Trojan execution refers to the process of a Trojan horse program being run on a computer system. Trojans are malicious programs that disguise themselves as legitimate software. They can be used to gain unauthorized access to a computer system and perform various malicious activities. For example, the IcedID malware contained within an ISO image is executed when the user clicks on a LNK file within the virtual hard drive created by the ISO file. Trojans use various persistence techniques to ensure they continue to run on a system, even after it has been rebooted or after the security software has been run. Some common methods include modifying the registry, creating scheduled tasks, installing itself as a service, or using rootkits to hide its presence. Other techniques include abusing legitimate operating system processes, such as adding an entry to the run keys in the Windows Registry or the Startup folder, which ensures that any referenced programs will be executed when a user logs in. Some less common but more sophisticated methods include abusing Image File Execution Options for debugging and hijacking the shortcut icons Target attribute.

Persistence refers to the techniques used by attackers to maintain access to a compromised system even after the system has been rebooted or the initial infection vector has been removed. Attackers use various methods to achieve persistence, including adding entries to the run keys in the Windows Registry or the Startup folder, so that their malicious programs are executed every time the system is started or a user logs in. Persistence allows attackers to maintain access to a network as they search for the data they want, and it can also be used to spread other malware. Some Trojans, like the Ursnif Trojan, use fileless persistence techniques, which involve storing an encoded command inside a registry key and launching it using

the Windows Management Instrumentation Command-line (WMIC).

1)Examples of Trojans Delivered Through Spear-Phishing Attacks

Trojans can be delivered through spear-phishing attacks, which are highly targeted and often involve sophisticated social engineering techniques:

- **OutSteel and SaintBot**: These Trojans were used in attacks targeting an energy organization in Ukraine as part of a larger campaign
- **Ursnif**: This banking Trojan uses a company's stored emails to send what appear to be legitimate emails with a Word document attachment containing a malicious macro that downloads the malware
- **TrickBot**: An advanced Trojan that has been spread primarily by spear-phishing campaigns using tailored emails with malicious attachments or links
- **IcedID**: Delivered within an ISO image as part of a malspam campaign, this Trojan has been used to evade Mark-of-the-Web controls.

2)Common Signs of Trojan Infection Using ISO Images

When a computer has been infected with a Trojan that uses ISO images to deliver malware, there may be several signs indicating the infection:

- **Unexpected Advertisements**: Advertisements may appear in places they shouldn't be, which can be a symptom of adware, a type of Trojan
- **Changed Homepage**: The web browser's homepage might change without permission, indicating that a browser hijacker, another type of Trojan, may be present
- **Suspicious Processes**: Processes related to the Trojan, such as "Your File Is Ready To Download.iso," may run in the background without the user's knowledge
- **Redirected Links**: Website links may redirect to sites different from what was expected, which can be a sign of a Trojan manipulating web traffic
- **Corrupted Files**: Opening a file and finding it corrupted could be a red flag that ransomware or another form of malware has infected the system
- **Strange Popups**: Some forms of malware can disguise themselves as legitimate programs, and unexpected popups may be a sign of such deceptive tactics
- **New or Modified Files**: Some types of malware may make copies of files or introduce new files into the system, often with generic-sounding names to avoid detection

G. Indicators of Compromise (IOCs)

The Indicators of Compromise (IOCs) related to the Dark Pink APT group, as listed in the CyberInt research, include:

IP Addresses:

- 185.141.63[.]128
- 185.141.63[.]129
- 185.141.63[.]130
- 185.141.63[.]131

Domains:

- hxxp://185.141.63[.]128/office/update/
- hxxp://185.141.63[.]129/office/update/
- hxxp://185.141.63[.]130/office/update/
- hxxp://185.141.63[.]131/office/update/
- hxxp://185.141.63[.]128/office365/update/
- hxxp://185.141.63[.]129/office365/update/
- hxxp://185.141.63[.]130/office365/update/
- hxxp://185.141.63[.]131/office365/update/

File Hashes:

- 5f4dcc3b5aa765d61d8327deb882cf99
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6

VI. MEET KILLNET: THE CYBER STAR OF THE DRAMA CLUB "DDOS"

A. Introduction

KillNet is a cyber mercenary group that has emerged as a frontrunner among over a hundred similar groups stemming from proxy cyberwars. KillNet's primary strategies revolve around conducting low-level Distributed Denial of Service (DDoS) attacks against vital infrastructure, government services, airport websites, and media enterprises in NATO nations.

KillNet is also known for its robust and confrontational misinformation efforts targeted at its 90,000 Telegram followers. These campaigns involve openly taunting the victims of their DDoS attacks and issuing threats that suggest the attacks could result in loss of human life, contradicting their proclaimed anti-war stance.

KillNet directed its focus towards the Parliament's website, resulting in the site becoming temporarily unavailable. In response to an investigation initiated against KillNet due to its assault on the European Parliament, the group targeted Belgium's Cybersecurity Center.

The self-proclaimed hacktivist group Anonymous Sudan appears to have increased KillNet's capabilities and the group has become the collective's most prolific affiliate in 2023, conducting a majority of claimed DDoS attacks. KillNet has also claimed to have 280 members in the US, attributing an attack on Boeing to their US "colleagues".

KillNet's victimology is extensive and includes a variety of sectors and countries:

- **Geographical Focus**: The majority of KillNet's victims are in Europe, with over 180 documented attacks. North America has experienced fewer than 10 attacks
- **Targeted Industries**: Common targets include the financial industry, transportation, governmental institutions, and business services
- **Healthcare Sector**: KillNet has targeted the U.S. healthcare industry, causing concerns due to the potential impact on critical health services
- **Government Services**: Attacks on government websites have been reported in several countries, including Romania, Moldova, Latvia, and the United States
- **Transportation**: U.S. airports and other transportation systems have been targeted by DDoS attacks
- **Media Enterprises**: Media companies within NATO countries have also been affected

Over time, KillNet developed a semi-formal organizational structure with a significant presence on Telegram and began to expand its operations. The group started to build a global team of operators from the darknet, offering services such as misinformation, impact on network infrastructure, reputation killing, data exfiltration, and data leaks, along with DDoS attacks. They also developed their own tools and botnets after initially using open-source tools.

B. Primary Strategies of KillNet & tactics, techniques, and procedures (TTPs)

KillNet's primary strategies revolve around DDoS attacks and brute-force dictionary attacks.

1) DDoS Attacks

KillNet primarily employs low-level DDoS attacks and has been known to use brute-force dictionary attacks. The group does not typically use sophisticated tools or strategies, and while their DDoS attacks can cause service outages, they usually do not result in major damage. KillNet conducts DDoS attacks on the OSI model's layer 4 (SYN flood attacks) and layer 7 (high volume POST/GET requests). These attacks aim to cause resource exhaustion by flooding a target service with malicious connection requests.

2) Brute-Force Dictionary Attacks

KillNet also employs brute-force dictionary attacks against various services. These attacks use predefined wordlists to hunt for exposed services that seek to exploit default or weak credentials. The group primarily targets services like FTP (port 21), HTTP (port 80), HTTPS (port 443), and SSH (port 22), with a particular focus on the root account. They also target Minecraft and TeamSpeak servers.

3) Targets of KillNet's DDoS Attacks

KillNet's DDoS attacks have primarily targeted critical infrastructure, government services, and media companies within NATO countries, including the U.S., Canada, Australia, Italy, and others. The group has also targeted organizations in the healthcare and public health sectors. Other targeted industries include the financial industry, transportation, and business services.

KillNet has also targeted or intends to target military entities, marine terminals and logistics facilities, other forms of transportation, and online trading systems. The group has been particularly active in targeting U.S. organizations, including state government websites and major airport domains.

In addition to these, KillNet has targeted international institutions such as NATO and countries including Germany, Denmark, Sweden, France, Poland, Slovakia, Ukraine, Israel, the United Arab Emirates (UAE), and other NATO ally and partner countries such as Japan.

It's important to note that while KillNet's DDoS attacks can cause service outages lasting several hours or even days, they usually do not cause major damage. However, they can disrupt essential services and pose a significant threat to organizations, especially those in critical sectors like healthcare.

4) Techniques, and procedures (TTPs)

KillNet's primary attack vector is DDoS, which involves flooding a target service with malicious connection requests, causing resource exhaustion. The group has also been known to engage in data exfiltration from targeted networks, including high-ranking officials' email inboxes and bank data.

In terms of tools, KillNet has used a variety of methods, including DDoS scripts and stressors, recruiting botnets, and utilizing spoofed attack sources. One In October 2023, KillNet began selling a new DDoS tool, which analysts fear will encourage more attacks. This tool is reportedly efficient and sophisticated, with precision-targeting capabilities and a user-friendly interface.

They utilize several known DDoS scripts, including "Aura-DDoS," "Blood," "DDoS Ripper," "Golden Eye," "Hasoki," and "MHDDoS". They also use a tool called "CC-Attack," a publicly available attack script that automates the use of open proxy servers and incorporates randomization techniques to evade signature-based detection. In addition, KillNet has been observed using slow POST DDoS attacks and other techniques such as ICMP flood, IP fragmentation, TCP SYN flood, TCP RST flood, TCP SYN/ACK, NTP flood, DNS amplification, and LDAP connectionless (CLAP) attacks.

5)Recruitements

KillNet's activities have not been limited to cyberattacks. The group has also engaged in recruitment, fundraising, and promoting their message through various channels, including social media to expand its support base, targeting individuals with diverse skill sets—including coders, network engineers, penetration testers, system administrators, and social engineers. Despite claims of the group's leader, KillMilk, stepping away from the group in mid-2022, he continues to be a central coordinator for the KillNet Collective.

In 2023, the group announced the launch of its Dark School, a cybercrime school that aims to train the next cohort and swell the ranks of the collective. KillNet recruits new members by actively seeking suitable candidates from supporters of their cause, leveraging various social media channels like Telegram and VK. They have a detailed form that potential recruits must fill out before they are considered for membership. KillNet operates with a military-like structure, with a clear top-down hierarchy and multiple smaller squads, which they call their "Legion," that act upon instructions given out in their Telegram channels.

C. Targets, Impact and consequences of KillNet attacks

The impact of KillNet's attacks can range from temporary service outages to potential financial losses and damage to reputation. Governmental responses have included classifying KillNet as a terrorist organization and issuing alerts through cybersecurity agencies.

1)Healthcare industry

KillNet has targeted the United States health and public health (HPH) sector since December 2022. Their signature DDoS attacks on critical infrastructure sectors typically cause service outages lasting several hours or even days. These attacks have severe consequences for patient care as they can interrupt patient care, lead to patient data loss, and disrupt communication between healthcare providers. In January 2023, KillNet and its affiliates conducted numerous coordinated DDoS attacks on healthcare organizations in the US, which resulted in service outages and significant disruption to routine and critical day-to-day operations. In some cases, the group has also exfiltrated data from a number of hospitals.

In the healthcare sector, Killnet's attacks have caused service outages lasting several hours or even days. These attacks have primarily targeted healthcare systems with at least one hospital and lone hospitals with Level I trauma centers. The group has also targeted pharmaceutical and life sciences industries.

The role of law enforcement in addressing Killnet's attacks includes investigating the incidents, coordinating with international law enforcement groups, and taking actions to disrupt the group's activities. For instance, the FBI, in coordination with international law enforcement groups and Europol, has previously infiltrated the infrastructure of other cyber threat groups.

The Cybersecurity and Infrastructure Security Agency (CISA) also plays a crucial role in helping organizations respond to such attacks. CISA provides resources and guidance to help organizations protect against cyber threats, and it works with affected organizations to mitigate the impacts of attacks.

2)Energy and financial industry

In the energy sector, the attacks could disrupt industrial control systems that support US energy infrastructure. While the impact on the energy sector's ability to provide localized services has been minimal so far, the threat remains. If successful, these attacks could potentially disrupt energy supply, leading to power outages and affecting critical infrastructure.

In the financial sector, DDoS attacks have become a growing concern. These attacks can cause intermittent downtime, forcing security staff to repel the attacks and potentially disrupting financial transactions. Killnet has even threatened imminent attacks on the SWIFT banking system and other financial institutions. While the actual impact of these threats is uncertain, they could potentially disrupt global financial transactions if successful.

It's important to note that while Killnet uses DDoS as its main tool, this method is typically used more to draw attention than to do major damage. However, the group has been increasing its capabilities and has shown a willingness to target critical infrastructure. Therefore, while the actual damage

caused by Killnet's attacks has been minimal so far, the potential for more significant disruption exists.

3)Aviation industry

These attacks have primarily targeted public-facing websites of airports, causing them to slow down or become completely inaccessible. The group has targeted more than 30 European airports and several major U.S. airports, including Hartsfield-Jackson Atlanta International Airport, Los Angeles International Airport, Chicago O'Hare International Airport, Orlando International Airport, Denver International Airport, Phoenix Sky Harbor International Airport, and others.

The impact of these attacks on the aviation industry has been primarily disruptive rather than destructive. The DDoS attacks have caused interruptions to airport websites, affecting customer interactions with airlines. However, the attacks have not impacted critical airport operations or disrupted flights. The European Air Traffic Control Agency Eurocontrol, for instance, confirmed that a DDoS attack by KillNet affected its website but did not disrupt flights or pose any threat to air traffic.

Despite the limited impact of these attacks, experts warn of the potential for more severe attacks in the future. The group has shown a willingness to target critical infrastructure and has called on other groups to launch similar attacks against U.S. civilian infrastructure, including marine terminals, logistics facilities, weather monitoring centers, and healthcare systems. Therefore, while the actual damage caused by KillNet's attacks on the aviation industry has been minimal so far, the potential for more significant disruption exists.

The airlines that have been affected by KillNet's attacks are not publicly known. However, the attacks have targeted the websites of several major U.S. airports, which could indirectly affect airlines operating at those airports by disrupting customer interactions with airlines. The airports that have been targeted include Hartsfield-Jackson Atlanta International Airport (ATL), Los Angeles International Airport (LAX), Chicago O'Hare International Airport (ORD), Orlando International Airport (MCO), Denver International Airport (DIA), and Phoenix Sky Harbor International Airport (PHX). While the DDoS attack have caused interruptions to airport websites, they have not impacted critical airport operations or disrupted flights.

The damage caused by KillNet's attacks on the aviation industry, including airlines, has been primarily disruptive rather than destructive. The group's Distributed Denial of Service (DDoS) attacks have targeted the websites of several major U.S. airports, causing them to slow down or become completely inaccessible. However, these attacks have not impacted critical airport operations or disrupted flights.

The impact on airlines operating at these airports would primarily be in the form of disrupted customer interactions. For instance, passengers may have experienced difficulties accessing flight information, booking or changing flights, or checking in online while the airport websites were down. However, the actual extent of this disruption is unknown.

4)Other industries

Besides the healthcare and energy sectors, KillNet has targeted a variety of other sectors and industries. These include:

- Government Services: KillNet has attacked government websites in several countries, including at least three states in the U.S. last year
- Transportation: U.S. airport websites have been victims of KillNet's DDoS attacks
- Media and News Outlets: Media companies have also been affected by KillNet's operations
- Dark Web Markets: KillNet has engaged in attacks against dark web markets
- Financial Sector: The group has threatened the financial sector, including the SWIFT banking system and other financial institutions
- Critical Infrastructure: KillNet has targeted critical airport websites, government services, and media companies within NATO countries, including the U.S., Canada, Australia, Italy, and Poland, as well as Ukrainian supporters in practically all Eastern European, Nordic, and Baltic countries

VII. PHISHING IN UK

A. Introduction

Phishing attacks in the UK are indeed on the rise, with cybercriminals using increasingly sophisticated methods to deceive individuals and organizations into revealing sensitive information. The National Cyber Security Centre (NCSC) and other organizations like Action Fraud are actively working to combat these threats, providing resources for individuals to report suspicious activities and offering guidance on how to avoid falling victim to these scams. The 2023 Data Breach Investigations Report revealed that 74% of breaches involved the human element, which includes social engineering attacks, errors, or misuse.

Emerging scams include QR phishing, also called 'quishing', where criminals hide malicious links in QR codes. These scams often start on social media, with criminals responding to fans who posted, looking for tickets or listing fake tickets themselves.

Artificial Intelligence (AI) is also being used by cybercriminals to enhance their phishing attacks. Generative AI can be used to create well-written, personalized phishing emails, making them more convincing and effective. In addition, AI has made deepfaking, a method used to impersonate biometric authentication methods like fingerprints, facial recognition, and voice recognition, much less costly.

B. Tackling phishing in the UK

Tackling phishing in the UK involves a multi-faceted approach that includes government initiatives, collaboration with tech companies, law enforcement actions, and education and awareness programs.

The UK government has taken several steps to combat phishing and other forms of cybercrime. The National Cyber Security Centre (NCSC), a UK government organization, has the power to investigate and take down scam email addresses and websites. The government has also signed a "world-first" charter with some of the biggest technology companies, which commits these companies to blocking and removing fraudulent content from their platforms. In addition, the government has launched a new Fraud Strategy, which includes a new National Fraud Squad led by the National Crime Agency and the City of London Police.

Law enforcement agencies are also playing a crucial role in combating phishing. The National Crime Agency (NCA) is committed to improving the UK's resilience to cyber-attacks and improving the law enforcement response to the cyber-crime threat. The Metropolitan Police Cyber Crime Unit has led multi-agency and international law enforcement operations to take down facilities used by fraudsters.

Education and awareness are key to preventing phishing attacks. Various organizations offer Phishing Awareness Training Courses that educate individuals and employees about the threat posed by phishing and how to recognize and prevent such attacks. The NCSC provides guidance on how to defend against phishing attacks and how to spot and report scam emails, texts, websites, and calls.

Collaboration with international partners is also crucial in tackling phishing, especially given that many cyber threats originate from overseas. The UK's NCSC has joined forces with the National Security Agency (NSA) in the US and other international partners to release updates about ongoing threats and provide guidelines to protect against them.

C. Why phishing in the UK matters

Phishing in the UK matters because it is a significant and growing threat to individuals, businesses, and the nation's critical infrastructure. Phishing attacks, which often involve tricking people into revealing sensitive information or installing malware, have become increasingly sophisticated and prevalent. The National Cyber Security Centre (NCSC) has warned of targeted spear-phishing campaigns against UK organizations and individuals, highlighting the enduring and significant threat to the UK's critical infrastructure.

The financial impact of phishing is substantial, with businesses reporting staggering losses. For instance, in 2021, phishing attacks resulted in a loss totaling $44.2 million globally, and the average cost for an organization to recover from a data breach in the UK surpasses £3.4 million. Moreover, the UK is the biggest target for phishing attacks in Europe, with 96% of organizations in the UK being targeted by phishing.

Phishing also has a considerable impact on the public. Around nine in ten online adults in the UK have encountered content they suspected to be a scam or fraud. The psychological effects on individuals can include anxiety, stress, and other emotional disturbances, which can lead to decreased productivity and absenteeism.

1)Recent phishing attacks in UK

Phishing attacks continue to be a significant cybersecurity threat in the UK, with various recent examples demonstrating the diverse tactics used by cybercriminals.

- **Vishing Attacks from Ukraine and Czech Republic**: In November 2023, an international operation disrupted a phishing campaign that defrauded victims of tens of millions of euros. The criminals carried out vishing

(voice phishing) attacks from call centres in Ukraine, posing as bank employees to pressure victims into transferring money

- **Hotel Employee Phishing Campaign**: In the same month, phishing campaigns targeted hotel employees. The attackers sent emails to hotel employees, tricking them into clicking a malicious link that downloaded infostealer malware. Once infected, the attackers exfiltrated customer data
- **Fake USPS Emails**: In May 2023, the USPS and the Postal Inspection Service reported the circulation of fake emails/email scams claiming to be from USPS officials. These emails prompted recipients to confirm their personal delivery information by clicking a button that, when opened, could activate a virus and steal information
- **UK Transport Business Phishing Attack**: In the first quarter of 2021, a UK transport business was hit by a cyber-attack where an email with a document containing a link to a fake portal was sent to the employees of the organization. The fake portal required the recipient to log in using Office 365/G-Suite authentication credentials. When recipients logged in, their credentials and passphrases were harvested and then used to access the victims' mailboxes
- **QR Phishing**: In 2024, a new form of phishing called 'quishing' emerged, where criminals hide malicious links in QR codes. They try to get people to hand over their personal information or download malware. This type of phishing can appear as emails claiming a package hasn't been delivered or that there's a problem
- **Phishing Attack on Law Firm**: A law firm employee failed to recognize a phishing attack. They received an email, clicked a link to download a document, then inadvertently entered login credentials into what they believed was a legitimate website. This resulted in a data breach

2)Recent phishing attacks targeting UK business

Phishing attacks continue to be a significant threat to businesses in the UK, with several notable incidents occurring in recent years.

- **British Library Cyber Attack (January 2024)**: The British Library suffered a cyber attack that rendered its IT systems inoperable. The Rhysida ransomware gang claimed responsibility for the attack and leaked internal human resources data, including scans of employee passports and employment contracts, on the dark web
- **WhatsApp Job Offer Scam (November 2023)**: Thousands of job seekers were targeted by scammers on WhatsApp, who used fake job offers to lure victims into their scheme
- **Phishing Attacks on Small Businesses (2023)**: Research revealed that scams and phishing made up 82% of online threats for small businesses in the UK in 2023. In the first half of 2023 alone, email-based phishing attacks surged 464% in comparison to 2022
- **Phishing Attacks on UK Organizations (2022-2023)**: 83% of UK businesses and charities that suffered a cyber attack identified phishing as the attack type

3)Recent phishing attacks targeting UK individuals

Phishing attacks continue to be a significant cybersecurity threat in the UK, with various recent incidents highlighting the evolving tactics of cybercriminals.

- **Phishing attack on Booking.com**: In November 2023, a phishing attack targeted Booking.com. The criminals carried out vishing (voice phishing) attacks from call centres in Ukraine, posing as bank employees to pressure victims into transferring money
- **Phishing attacks on UK parliamentarians**: In December 2023, there were spear-phishing attacks targeting UK parliamentarians from multiple political parties
- **Phishing attacks impersonating government emails**: In 2022, the National Cyber Security Centre (NCSC) reported on government impersonation scams, where phishing attacks were carried out by impersonating government emails

4)Phishing Scams Targeting Employees

Phishing scams targeting employees, also known as Business Email Compromise (BEC) scams, often target specific roles within a company, such as executives or HR professionals, who have access to sensitive information. These scams typically involve sending emails that appear to be from a senior executive or CEO, requesting a wire transfer or payroll information. Some common employee-targeted phishing scams include:

- **Whaling attacks**: These are targeted attempts to steal sensitive information from a company by impersonating top executives like CEOs or CFOs
- **W-2 phishing scam**: In this scam, the attacker impersonates an executive or organization leader and sends a message to a payroll or HR employee asking for W-2 information
- **New employee phishing**: New employees are often targeted because they are eager to impress and may overlook subtle signs of a phishing attack

5)Phishing Scams Targeting Consumers

Phishing scams targeting consumers often impersonate well-known companies or organizations, such as banks or government agencies, to gain the trust of the targeted individuals. These scams typically involve sending emails or text messages that appear to be from these entities, asking consumers to provide personal identifying information. The scammers then use this information to commit fraud, such as opening new accounts in the consumer's name or invading their existing accounts. Some common consumer-targeted phishing scams include:

- **The check-cashing scam**: Scammers target people selling items online. They overpay with a check and ask for the excess to be wired back, only for the original check to bounce

- **The sales scam**: Online shoppers looking for a bargain are targeted on auction sites with high-end electronics. Even if the consumer doesn't win the item, they still have to pay
- **The job scam**: An apparent employer conducts a phone interview and tells a job seeker they have received a job. The job seeker is then asked to fill out an online credit form, which is used to steal their identity

D. Strategies to get ahead of phishing

Phishing is a significant cybersecurity threat, and early detection is crucial to prevent victims from falling prey to these attacks.

- **Detect Phishing Early and Often**: Early detection of phishing attacks is vital as 50% of victims fall prey to a phishing attack within 24 hours. Leveraging technology and automation can help identify phishing pages earlier. Deep learning models combined with browser automation can be used to build an automated solution for early detection
- **Use DMARC**: Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a global standard for email authentication that helps verify the origin of emails and block out fake emails. It allows senders to verify that the email really comes from whom it claims to come from, helping curb spam and phishing attacks
- **Monitor Domain Registrations**: Monitoring domain registrations can help detect fraudulent websites set up to steal login credentials, divert web traffic, or sell counterfeit products. Services like PhishLabs and Red Points offer domain monitoring services that can automate the process of finding and removing fake accounts, apps, websites, and domains
- **Automate Phishing Detection**: Machine learning can help detect phishing attacks by learning patterns and creating models that can automatically distinguish between legitimate and malicious websites or other forms of communication. There are also various anti-phishing tools and services available that can help businesses protect against phishing attacks
- **Collaborate Across Teams**: Collaboration across teams is essential in combating phishing. Regular staff awareness training can ensure that employees know how to spot a phishing email, even as fraudsters' techniques become increasingly more advanced

1)Detect Phishing Early and Often

Early detection of phishing is critical because the first 24 hours are when victims are most susceptible. To detect phishing early and often, organizations can employ various technologies:

- **Automated Scanning**: Use automated scanning tools to regularly search for phishing websites and emails. These tools can scan and analyze web pages, emails, and other digital content for phishing indicators.
- **Machine Learning**: Implement machine learning algorithms that can learn from patterns of known phishing attacks and predict new ones. These algorithms can process large volumes of data to identify potential threats more quickly than humans.
- **User Reporting**: Encourage users to report suspected phishing attempts. Quick reporting can lead to faster takedown of phishing sites and prevent further damage.

2)Use DMARC

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is an email-validation system designed to protect domain names from being used in phishing scams, email spoofing, and other cybercrimes:

- **Email Authentication**: DMARC works by ensuring that legitimate email is properly authenticated against established DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework) standards.
- **Reporting**: DMARC also provides a way for email receivers to report back to senders about messages that pass and/or fail DMARC evaluation.
- **Policy Enforcement**: Senders can set policies for how receivers should handle mail that doesn't pass authentication checks, potentially preventing delivery of fraudulent emails.

3)Monitor Domain Registrations

Monitoring domain registrations can help identify potential phishing sites before they become active:

- **Domain Watch Services**: Use services that monitor domain name registrations for names that are similar to your brand or trademarks.
- **Automated Alerts**: Set up automated alerts to notify your security team when a potentially fraudulent domain is registered.
- **Take-down Services**: Engage with take-down services that can help remove phishing sites once they are identified.

4)Automate Phishing Detection

Automation in phishing detection involves using software to identify and respond to phishing threats:

- **Phishing Databases**: Utilize databases of known phishing sites to block access to them.
- **Real-time Analysis**: Implement systems that perform real-time analysis of web pages and emails to detect phishing content.
- **Integration**: Integrate phishing detection into security infrastructure like firewalls, email gateways, and endpoint protection for a comprehensive defense.

5)Collaborate Across Teams

Collaboration is key to a successful anti-phishing strategy:

- **Cross-departmental Training**: Conduct regular training sessions across all departments to educate employees about the latest phishing tactics and how to recognize them.

- **Shared Intelligence**: Share intelligence about new phishing threats between security teams, IT departments, and other relevant stakeholders.
- **Incident Response Planning**: Develop and practice an incident response plan that involves multiple teams to ensure a coordinated response to phishing attacks.

E. Phishing detection and response software

Phishing detection and response software is a set of cybersecurity tools that allow organizations to identify and remediate phishing threats. Here are some tools that can be used to automate phishing detection:

- **Agari Phishing Response**: This service is a phishing incident response system designed to accelerate phishing triage, forensics, remediation, and breach containment
- **IRONSCALES**: This self-learning email security platform is designed to proactively fight phishing. It combines human interaction and AI-oriented identification to prevent phishing attempts, including Business Email Compromise (BEC)
- **Avanan**: This anti-phishing software for cloud-hosted email ties into your email provider using APIs to train their AI using historical email. The service analyzes not just message contents, formatting, and header information, but evaluates existing relationships between senders and receivers to establish a level of trust
- **Barracuda Sentinel**: This tool leverages mail provider APIs to protect against phishing. It uses artificial intelligence to learn the unique communications patterns of your organization to identify and block real-time spear phishing and cyber fraud attacks
- **Proofpoint Targeted Attack Protection (TAP)**: This tool helps organizations efficiently detect, mitigate, and block advanced targeted attacks that arrive via email
- **RSA FraudAction**: This tool specializes in detecting and preventing phishing attempts, Trojans, and rogue websites
- **PhishER**: This lightweight Security Orchestration, Automation, and Response (SOAR) platform helps orchestrate threat response and manage the high volume of phishing threats
- **Zphisher**: This is a phishing tool for beginners and novices, which includes some automated phishing tests
- **Evilginx2**: This phishing tool describes itself as a man-in-the-middle attack framework used for phishing login credentials along with session cookies, allowing bypass of 2-factor authentication
- **DTonomy AIR Enterprise**: This AI-based tool includes batch mode analysis of phishing emails, task and case management automation, and hundreds of playbooks

1)Key Features in Phishing Detection and Response Software

When selecting phishing detection and response software, consider the following key features:

- **Domain Identification**: The ability to identify and verify the authenticity of the domain from which an email originates, helping to prevent domain spoofing
- **Header Analysis**: Analyzing email headers for inconsistencies or signs of tampering that may indicate a phishing attempt
- **Link Analysis**: Examining links within emails or web content to determine if they lead to known phishing sites or malicious content
- **Attempted Impersonation Features**: Detecting attempts to impersonate legitimate entities or individuals, which is a common tactic in spear-phishing attacks
- **AI Analytics**: Using artificial intelligence to proactively identify suspicious behavior patterns and predict new phishing threats
- **Cross-referencing with Threat Libraries**: Comparing against databases of known threats, which are often manually updated by security experts, to identify phishing attempts
- **End-user Reporting**: Enabling users to report suspected phishing attempts, which can lead to faster takedown of phishing sites and prevent further damage

2)How Phishing Simulation and Testing Tools Work

Phishing simulation and testing tools are designed to give users real-world experience in combating phishing attacks:

- **Realistic Simulations**: Distribute a range of realistic phishing scenarios that mimic the latest attack methods, including vishing (voice phishing), to train users
- **Regularly Updated Templates**: Use templates that are frequently updated to reflect the latest phishing tactics, ensuring that training remains relevant
- **Automated Testing Frequency**: Automate the frequency of phishing simulation tests to ensure consistent training rather than sporadic, one-off sessions
- **Active Environment Testing**: By seeing a phishing email in an active environment, users must apply their knowledge to prevent becoming a victim, reinforcing their training
- **Admin Insights**: From an admin perspective, deploying simulations and training provides insight into the effectiveness of the training and the organization's security posture

3)Implementing phishing detection and response software

Implementing phishing detection and response software effectively requires a combination of technical solutions, user education, and organizational policies:

- **Regular Employee Training in Cybersecurity Awareness**: Continuous training ensures that employees can recognize and respond to phishing

attempts. Engaging training platforms can keep employees updated on the latest phishing tactics

- **Implement Email Security Best Practices**: Utilize protocols like DMARC (Domain-based Message Authentication, Reporting, and Conformance) to authenticate emails and prevent spoofing. This protocol builds on SPF and DKIM standards to verify the origin of emails and block fake ones
- **Leverage AI and Automation**: AI-powered software can scan incoming messages for signs of phishing with high accuracy. Machine learning algorithms can also predict new phishing threats by learning from patterns of known attacks
- **Monitor Phishing Results**: Use phishing simulation tools to monitor employee responses to simulated attacks. This can help identify vulnerabilities and measure the effectiveness of training programs
- **Filter DNS Traffic**: DNS filtering solutions can prevent users from accessing malicious websites by blocking requests to blacklisted domains. Some filters can proactively evaluate websites for harmful code and add them to the blacklist
- **Use Technical Solutions**: Implement strong passwords, employ DNS filtering, set up antivirus solutions, enable safe web browsing policies, and use secure email services to prevent phishing compromises
- **Implement Incident Response and Reporting Measures**: Have a plan in place for responding to identified phishing activity. This includes remediation steps and reporting mechanisms to address and mitigate the impact of successful attacks
- **Secure Email Gateway Capabilities**: Deploy email filters that screen based on headers and malicious content, categorize email, and inspect URLs against reputation feeds
- **Harden User Endpoints**: Ensure that user endpoints are secure by implementing endpoint protections and educating users on safe browsing and email practices

4)Implementation mistakes

When implementing phishing detection and response software, there are several common mistakes to avoid:

- **Not updating software regularly**: Regular updates are crucial to ensure that the software can effectively detect and respond to the latest phishing threats
- **Over-reliance on IT departments**: While IT departments play a crucial role in managing and maintaining phishing detection software, it's important for all employees to understand how to identify and respond to phishing attempts
- **Relying on antivirus software alone**: While antivirus software can help detect and prevent some phishing attempts, it's not sufficient on its own. Endpoint detection and response (EDR) and extended detection and response (XDR) solutions can provide more comprehensive protection
- **Not conducting thoughtful phishing simulations**: Phishing simulations can be a useful tool for training employees to recognize and respond to phishing attempts. However, it's important to conduct these simulations thoughtfully and to communicate clearly with all relevant stakeholders
- **Not taking a defense-in-depth strategy**: Relying solely on an anti-phishing program can be risky, as it only takes one mistake for an attacker to succeed. A defense-in-depth strategy, which includes multiple layers of security, can provide more robust protection

When selecting phishing detection and response software, consider the following key factors:

- **Integration with other tools**: The software should be able to integrate with other security tools for a comprehensive security approach
- **Machine learning capabilities**: Many modern tools use machine learning to analyze endpoint and network activities and detect potential threats
- **Threat prioritization**: The software should be able to prioritize threat alerts to help your team focus on the most serious threats first
- **Agent vs. agentless monitoring**: Both agent-based and agentless monitoring have their pros and cons, and you may need a combination of both for optimal security
- **Monitoring and analysis capabilities**: The software should be able to monitor endpoint behaviors and detect, prioritize, track, and alert on indicators of compromise (IOCs) and indicators of attack (IOAs)

  Detection vs. prevention: Some solutions focus more on detecting phishing attempts, while others focus more on preventing them
- **Automated real-time threat detection**: This feature can help your security team quickly identify and respond to threats

F. Holiday Phishing risks

- **Increased Online Activity**: During the holidays, people are more active online, shopping for gifts, booking travel, and donating to charities. This increased activity provides more opportunities for scammers to trick people into revealing sensitive information
- **Distraction**: The holiday season is a busy time, and people are often distracted and may not be as vigilant as they usually are. Scammers take advantage of this by sending phishing emails that appear to be from reputable sources, such as banks or popular retailers
- **Emotional Manipulation**: Scammers often use emotional manipulation during the holiday season. They may impersonate charities or family members to trick people into sending money or revealing personal information
- **Seasonal Themes**: Scammers use holiday-themed emails, messages, and websites to trick victims. They

may send fake order and tracking emails, charity emails, and messages related to holiday events or schedules

- **Opportunistic Behavior**: Scammers take advantage of the fact that many companies offer bonuses or seasonal jobs during the holidays. They create phishing campaigns that target employees with fake bonus offerings or job seekers with fraudulent job ads
- **Social Engineering**: Scammers use social engineering tactics to create a sense of urgency or fear, such as claiming that a package delivery was missed or that a recipient's account has been hacked. This can prompt hasty actions like clicking on malicious links
- **Fake Online Stores or "Lookalike Stores"**: Scammers create fraudulent websites that mimic legitimate online retailers to trick consumers into entering their personal and financial information
- **Missed Delivery/Non-Delivery Notification**: Victims receive notifications claiming a delivery was missed or a package was not delivered, prompting them to click on a link that could lead to a phishing site or install malware
- **Gift Card Scams**: Scammers send spoofed emails or texts asking victims to purchase multiple gift cards for personal or business reasons, often pretending to be someone the victim knows
- **Fake Charities**: Criminals set up bogus charities and solicit donations from individuals who believe they are contributing to a legitimate cause
- **Social Media Scams**: Scammers use social media platforms to offer holiday promotions, vouchers, or gift cards that require completing surveys designed to steal personal information
- **Fraudulent Seasonal Jobs**: Fake job ads are posted online offering good money for very little work, targeting individuals seeking to make extra money during the holidays
- **Phishing Emails**: These are particularly prevalent during the holiday season and can take the form of bogus delivery confirmation requests or other communications seeking personal information
- **Package Theft**: Scammers may pose as delivery services and send fraudulent notifications about package theft or delivery issues to trick recipients into providing personal details
- **Vacation Scams**: Offers for fake holiday vacations or travel deals that aim to steal money or personal information from unsuspecting victims
- **Brushing Scams**: Unsolicited items are sent to individuals, which may seem harmless but could be a sign that the scammer has access to the recipient's personal information

VIII. DCRAT (DARK CRYSTAL RAT)

A. Introduction

DCRat, also known as Dark Crystal Rat, is a commercial backdoor that is predominantly sold on underground forums. It has been around since 2018 and operates as a modular remote access trojan (RAT) offered as a Malware-as-a-Service (MaaS). The malware is designed to provide threat actors unauthorized access to systems by circumventing security measures.

In terms of pricing, DCRat is sold for approximately $7 for a two-month subscription. Its one-month license goes for a mere $5, while a lifetime use license costs $40. Despite its low cost, DCRat is a versatile and dangerous cybersecurity threat.

In 2022, DCRat's developer announced on their GitHub page that the it would be discontinued, along with a link to its successor and a claim the new source code would remain private and not sold.

B. DCRat Features

DCRat is a modular remote access trojan (RAT) with a range of features that make it a versatile tool.

The DCRat product itself consists of three components: a stealer/client executable, a single PHP page serving as the C2 endpoint/interface, and an administrator tool. It uses a modular framework that deploys separate executables for each module, most of which are compiled .net binaries programmed in C#.

DCRat is capable of a range of nefarious uses, including surveillance, reconnaissance, information theft, Distributed Denial of Service (DDoS) attacks, and dynamic code execution in a variety of different languages. It can also steal credentials used to login to social media accounts, specifically Telegram and Discord. DCRat has been detected targeting Windows systems, with a specific focus on bypassing security safeguards.

As of 2023, DCRat has been updated with several new capabilities and features:

- **CryptoStealer** Module: This module allows attackers to access users' cryptocurrency wallets
- **Dynamic Code Execution**: DCRat can execute code in multiple programming languages
- **Crypto-Mining**: Instances of DCRat deploying crypto-mining software on victim endpoints have been documented
- **Delivery Methods**: DCRat has been disseminated through enticing adult content-themed baits, infected files, and network propagation
- **Evasion Techniques**: DCRat has been observed to evade sandbox environments that use fake internet to spoof internet connection for malware analysis
- **Persistence**: DCRat has been found to exploit a zero-day vulnerability in the Microsoft support diagnostic tool (MSDT), CVE-2022-30190 (Follina), to maintain persistence on the infected machine

As of 2023, DCRat has the following key features (**full list**):

- Information Theft
- Surveillance and Control
- Disruptive Attack Capabilities
- Modularity and Customization
- System Interaction
- Administration and Control
- Deployment and Distribution
- Stealth and Evasion

1)Information Theft

- **Information Theft**: DCRat can steal sensitive data from victimized systems, including capturing screenshots, harvesting clipboard data
- **Keylogging**: It can log keystrokes to capture sensitive information like passwords
- **Stealing Browser Data**: DCRat can extract session cookies, auto-fill credentials, personal information, and credit card details from browsers
- **Clipboard Data Harvesting**: It can copy and steal the contents of the user's clipboard
- **Credential Theft**: The malware can steal credentials from popular FTP applications and social media accounts, particularly targeting Telegram and Discord

2)Surveillance and Control

- **Screenshots**: It can take screenshots to monitor user activity
- **System Information Collection**: DCRat collects system information such as CPU and GPU stats, hostname, usernames, language preferences, and installed applications

3)Disruptive Attack Capabilities

- **DDoS Attacks**: DCRat can launch Distributed Denial of Service (DDoS) attacks against selected targets

- **Dynamic Code Execution**: It offers the ability to execute code dynamically in multiple programming languages

4)Modularity and Customization

- **Modular Architecture**: DCRat uses a modular framework, deploying separate executables for each module, most of which are compiled .NET binaries programmed in C#
- **Plugin Framework**: It has a plugin development framework that allows for the creation of new modules, enhancing its capabilities

5)System Interaction

- **Persistence**: DCRat can persist on compromised hosts using techniques such as creating scheduled tasks, Registry Run Keys, and Winlogon Autostart Registry Keys
- **Crypto-Mining**: There have been instances where DCRat deployed crypto-mining software on victim endpoints

6)Administration and Control

- **C2 Administration**: The malware includes a command-and-control (C2) administration interface that allows attackers to upload modules, execute commands remotely, and exfiltrate data
- **Stealer/Client Executable**: It consists of a .NET executable designed to exploit Windows systems

7)Deployment and Distribution

- **Malware-as-a-Service (MaaS)**: DCRat operates as a MaaS, allowing it to be purchased and used by various threat actors
- **Low-Cost Licenses**: It is sold for approximately $7 for a two-month subscription, with other pricing options available for longer-term use

8)Stealth and Evasion

- **Concealment**: DCRat employs techniques to stay undetectable, such as hiding its presence and disguising its network traffic
- **Anti-Detection Features**: Plugins are available that can resist running in a virtual machine, disable Windows Defender, and disable webcam lights on certain models
- **Persistence Mechanisms**: It can use techniques like creating scheduled tasks, Registry Run Keys (incl. Winlogon Autostart) to maintain its hold on the system

C. DCRat Deployment

DCRat operates as a Malware-as-a-Service (MaaS). DCRat is deployed via first-stage attacks employing a wide array of tactics, including malspam, phishing, spear-phishing, and pirated (or “cracked”) commercial software such as rogue updaters and anti-virus products.

Once installed, the DCRat C2 administration allows attackers to upload modules to the infected host, execute commands remotely, and exfiltrate data. DCRat uses a modular framework that deploys separate executables for each module, most of which are compiled .net binaries programmed in C#. The malware is capable of stealing information from browsers, such as session cookies, auto-fill credentials, personal information, and credit card details. It can also monitor the infected host by logging and exfiltrating keystrokes and screenshots.

DCRat establishes a connection between the victim's device and the attacker's device through a command-and-control (C2) server. Once the malware is installed on the victim's device, it connects back to the C2 server controlled by the attacker. This server can send commands to the compromised device, allowing the attacker to access and modify data, steal sensitive information, and ensure persistence by reconnecting to the C2 server even after reboots or attempts to remove the malware.

The most common lures used to distribute DCRat include:

- **Adult Content-Themed Lures and Fake OnlyFans**: DCRat has been distributed using explicit lures related to OnlyFans pages and other adult content. Victims are tricked into downloading malicious files, often ZIP archives, which contain the malware
- **Phishing and Malspam**: DCRat is also spread through phishing emails and malspam campaigns, where victims receive emails with malicious attachments or links that, when opened, install the malware
- **Network Propagation**: The malware can spread through network propagation, exploiting vulnerabilities or using other methods to move laterally within a network and infect multiple devices

D. DCRat Evade techniques

DCRat employ several techniques to evade detection:

- **Process Infiltration**: DCRat rarely produces malicious activity in its current process. Instead, it prefers to create large process trees and infiltrate a harmless process at some point
- **Persistence Algorithm**: DCRat can execute a persistence algorithm to retain control over the system. For instance, it can copy itself to a random running process and to the root directory. It can also create shortcuts to these copies in the user's Startup folder and add registry values that point to these shortcuts
- **Delay Execution**: DCRat can delay execution for a period of time after the infection, which can help it evade immediate detection
- **Obfuscation**: DCRat's payload has been protected with Enigma Protector to prevent analysis
- **Use of SSL/TLS Certificates**: DCRat, like many other malware families, uses self-signed SSL/TLS certificates, which can help it blend in with normal encrypted traffic and evade detection

E. DCRat Effectiveness

DCRat is known for its cost-effectiveness, versatility, and continuous updates, which make it a significant cybersecurity threat. DCRat allows threat actors to take control over an infected machine and steal sensitive information such as clipboard contents and personal credentials from apps. DCRat is developed and maintained by a single user who actively markets

their product on several underground forums as well as a Telegram channel. This is unlike most other RATs, which are typically the work of sophisticated and well-resourced cyber-criminal groups.

DCRat differs from other RATs in several ways. It can also function as a loader, dropping other types of malware on the infected computer. DCRat uses three distinct techniques for persistence on the compromised host: creating a scheduled task, creating a Registry Run Key, and creating a Winlogon Autostart Registry Key. It also uses the W32tm "stripchart" command as a delay tactic for its execution and beaconing, which is not commonly used by other RATs.

In terms of effectiveness, DCRat is surprisingly effective despite its low cost. The malware is under active development, with new capabilities being added regularly. It is also capable of evading detection by security software, making it a potent cybersecurity threat.

The most common features of other remote access trojans include the ability to establish complete to partial control over infected computers, the capability to spawn a child process, and the use of the Task Scheduler to ensure persistence within the compromised system. They can also exfiltrate sensitive information, establishing connections with command and control (C2) servers. Some RATs, like njRAT, operate on the .NET framework and enable hackers to remotely control a victim's PC, giving them access to the webcam, keystrokes, and passwords stored in web browsers and desktop apps.

F. DCRat Detection

1) Common IoC's features

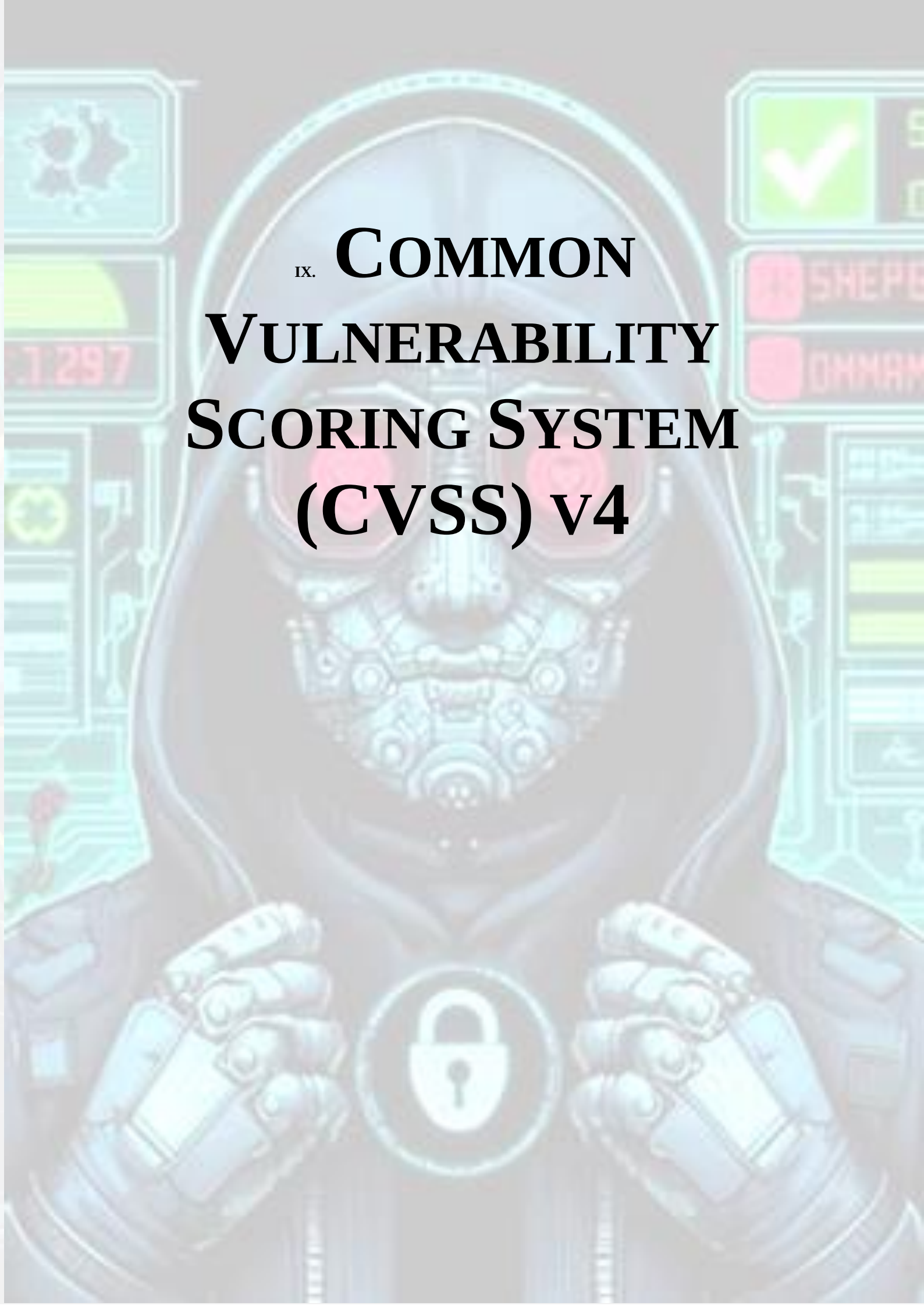
The most common indicators of compromise (IOCs) for DCRat attacks relate to the following features:

- Monitoring the infected host by logging and exfiltrating keystrokes and screenshots
- Stealing information from browsers, such as session cookies, auto-fill credentials, personal information, and credit card details, including popular FTP applications
- The ability to record the victim's keystrokes, which can be used to steal passwords and other sensitive information
- The ability to collect information about the system (CPU and GPU stats, etc.)

2) Network IoC's features

The most common indicators of compromise (IOCs) for DCRat attacks relate to the following networks features:

- **Network Traffic**: DCRat communicates with its Command & Control (C2) server to exfiltrate data and receive commands. This communication can be detected as unusual network traffic
- **Data Collection**: DCRat collects sensitive information from compromised hosts, such as server type, username, and GPU info, which can be detected by monitoring for unusual data access or movement
- **Persistence Mechanisms**: DCRat uses several techniques for persistence, including creating a scheduled task, creating a Registry Run Key, and creating a Winlogon Autostart Registry Key. These entries can be detected by monitoring for changes in the system's scheduled tasks, registry, and startup processes
- **DDoS Attacks**: DCRat can orchestrate Distributed Denial of Service (DDoS) attacks against targeted websites. This can be detected by monitoring for unusual network traffic patterns or an increase in requests to a specific website
- **Dynamic Code Execution**: DCRat has the ability to execute code in multiple programming languages. This can be detected by monitoring for unusual code execution or process behavior
- **Information Theft**: DCRat can facilitate the theft of sensitive data from victim devices, including capturing screenshots and harvesting credentials. This can be detected by monitoring for unusual data access
- **Crypto-Mining**: Instances of DCRat deploying crypto-mining software on victim endpoints have been documented. This can be detected by monitoring for unusual CPU usage or network traffic



IX. COMMON VULNERABILITY SCORING SYSTEM (CVSS) V4

A. Introduction

The Common Vulnerability Scoring System (CVSS) version 4.0 is the latest iteration of the industry-standard scoring system for assessing and quantifying the severity and impact of software vulnerabilities.

CVSS v4.0 introduces several significant changes and improvements over the previous version (v3.1) to provide a more granular, accurate, and comprehensive assessment of vulnerabilities.

This analysis will delve into various facets of CVSS v4.0, including its enhanced metrics, the introduction of new categories, and the implications these changes have for cybersecurity professionals and organizations. By dissecting the CVSS v4.0 specification, we will offer a qualitative summary that encapsulates the core improvements and modifications from its predecessor, CVSS v3.1, thereby equipping readers with a nuanced understanding of its impact on vulnerability management processes. Through a meticulous examination of the CVSS v4.0 framework alongside insights from cybersecurity experts, this analysis endeavors to provide a clear, actionable guide for effectively leveraging CVSS v4.0 in enhancing organizational security postures.

B. Key changes

Key Updates in CVSS v4.0 as for now:

- **New Base Metrics and Values**: CVSS v4.0 introduces new base metrics that capture additional aspects of risk, such as the potential consequences of a successful attack, including explicit assessment of impact to Vulnerable System (VC, VI, VA) and Subsequent Systems (SC, SI, SA)
- **Simplified Threat Metrics**: The Temporal Score has been renamed to Threat Metric Group and now includes only one metric, which is Exploit Maturity
- **New Supplemental Metric Group**: This group is introduced for Enhanced Extrinsic Attributes, providing additional insight into the characteristics of a vulnerability
- **Changes to Vector String**: The Vector String has been updated to begin with CVSS:4.0 rather than CVSS:3.1. Although no other changes have been made to the Vector String, CVSS v4.0 contains changes to the definition of some of the metric values and to the formulas
- **Improved Guidance**: CVSS v4.0 provides improved guidance to CVSS analysts to produce consistent scores. It also provides guidance on scoring vulnerabilities in software libraries and supports multiple CVSS scores for the same vulnerability that affects different platforms or operating systems
- **Enhanced Clarity and Simplicity**: CVSS v4.0 aims to provide a more streamlined scoring process, reducing subjectivity through clearer metric guidance and definitions
- **Focus on Resiliency**: The latest iteration of CVSS introduces a renewed focus on resiliency, particularly in the early stages of an exploit, addressing the increasing concerns around the security of operational technology (OT), industrial control systems (ICS), and the Internet of Things (IoT)
- **Renaming of Key Metrics**: The Temporal metrics in CVSS 3.1 have been renamed to Threat Metrics in CVSS 4.0
- **User Interaction**: CVSS 4.0 has made the User Interaction metric more granular. While CVSS 3.1 had the values None (N) or Required (R) for this metric, CVSS 4.0 has expanded the options to Active, Passive, and None
- **New Base Metrics and Values**: CVSS 4.0 introduces new base metrics and values, providing a more granular and accurate assessment of vulnerabilities
- **Assessing Effects on Vulnerable and Subsequent Systems**: CVSS 4.0 provides clearer insight into the impact of vulnerabilities on both the vulnerable system and subsequent systems
- **Simplifying Threat Metrics**: The Threat metrics in CVSS 4.0 have been simplified to focus only on Exploit Maturity
- **New Supplemental Metric Group**: CVSS 4.0 introduces a new Supplemental Metric Group for Enhanced Extrinsic Attributes
- **Attack Requirements**: CVSS 4.0 introduces a new base metric, "Attack Requirements", which gets the value "Present" if there is a pre-attack requirement
- **Scope Changes**: The "Scope" feature from CVSS v3.1 was retired and replaced with the concepts of "Vulnerable System" and "Subsequent System"
- **Support for Multiple Scores**: CVSS 4.0 is designed to support multiple CVSS scores for the same vulnerability that affects different platforms, operating systems, etc

- **Guidance for Other Sectors**: CVSS 4.0 provides guidance to extend the CVSS framework for other industry sectors such as privacy, automotive, etc

C. Benefits of using cvss v4.0 over previous versions

CVSS v4.0 improves vulnerability assessments by introducing several enhancements that provide a more nuanced and accurate representation of the risks associated with software vulnerabilities:

- **More Granular Base Metrics** – CVSS v4.0 includes new base metrics and values that capture additional aspects of risk, such as the potential consequences of a successful attack. This includes explicit assessment of impact to Vulnerable System (VC, VI, VA) and Subsequent Systems (SC, SI, SA), which allows for a more detailed understanding of the vulnerability's impact
- **Integration of Threat Intelligence** – The Threat Metrics group in CVSS v4.0 adjusts the severity of a vulnerability based on real-time factors, such as the availability of proof-of-concept code or active exploitation. This integration of threat intelligence ensures that the scoring reflects the current threat landscape and the likelihood of an attack
- **Environmental Metrics** – CVSS v4.0's Environmental Metrics further refine the severity score to a specific computing environment. They consider factors such as the presence of mitigations and the criticality of the affected system within the user's environment, allowing for a more tailored risk assessment
- **Simplified Threat Metrics** – The Threat Metrics group, previously known as Temporal Metrics, has been simplified to focus on the most critical aspect of real-time vulnerability assessment—Exploit Maturity. This simplification helps users better understand the risk of vulnerabilities
- **Enhanced Clarity and Simplicity** – CVSS v4.0 aims to reduce ambiguities and inconsistencies in vulnerability assessments that were common in previous versions. The new version provides clearer metric guidance and definitions, which should lead to more consistent scoring
- **Support for Multiple Scores** – The new framework is designed to support multiple CVSS scores for the same vulnerability when it affects different platforms or operating systems, providing a more comprehensive assessment
- **Focus on Resiliency** – CVSS v4.0 introduces a renewed focus on resiliency, particularly in the early stages of an exploit, which is increasingly important for the security of operational technology (OT), industrial control systems (ICS), and the Internet of Things (IoT)
- **Vendor-Supplied Severity and Impact Scoring** – The framework now integrates vendor-supplied severity and impact scoring, accommodating a wider range of perspectives and aligning the scoring process more closely with real-world scenarios
- **Enhanced Fidelity in Vulnerability Assessment** – The objective behind CVSS v4.0 is to offer enhanced fidelity in vulnerability assessment for the industry and the public, incorporating various refinements to improve the accuracy of vulnerability scoring

D. Finer-grained metrics in cvss v4.0 & Scoring process

CVSS v4.0 introduces several finer-grained metrics to provide a more nuanced understanding of the technical characteristics of vulnerabilities. One of the key changes is a more granular breakdown of the Base Metrics, which includes new values for User Interaction, categorized as either Passive or Active. The User Interaction (UI) metric in CVSS v4.0 provides more granularity to the amount of interaction required. Additionally, CVSS v4.0 introduces a new Attack Requirement metric, which provides more granularity in capturing the prerequisite conditions enabling an attack.

CVSS v4.0 simplifies the scoring process in several ways. The Threat Metrics, previously known as Temporal Metrics, have been simplified and renamed to emphasize real-time vulnerability assessment. Remediation Level (RL) and Report Confidence (RC) have been retired, and Exploit "Code" Maturity has been renamed to Exploit Maturity (E). The Temporal Metrics have been simplified to help consumers better understand the risk of vulnerabilities. The scoring system in CVSS v4.0 is simpler and more flexible compared to previous versions, aiming to provide a universal framework for scoring different vulnerabilities.

E. List of Metrics

The Common Vulnerability Scoring System (CVSS) version 4.0 consists of four metric groups: Base, Threat, Environmental, and Supplemental.

The Base metric group represents the intrinsic characteristics of a vulnerability that are constant over time and across user environments. The Base Score is calculated using a specific formula that examines factors such as the vulnerability's impact on integrity, confidentiality, availability, exploitability, and scope.

The Threat metric group, previously known as the Temporal Metrics Group, provides additional context to the Base metrics. However, the Threat metrics do not significantly impact the final CVSS score.

The Environmental metric group represents the characteristics of a vulnerability that are unique to a user's environment. These metrics allow organizations to customize the CVSS scores based on their specific environment. However, the Environmental metrics are specified by users and do not directly impact the publicly visible CVSS scores, which are based solely on the Base Score.

The Supplemental metric group is a new addition in CVSS v4.0. It includes metrics that provide additional context, such as Automatable, Value Density, Recovery, Provider Urgency, and Vulnerability Response Effort. However, the Supplemental metrics are optional and do not have any impact on the final calculated CVSS score.

1) Base Metrics

The Base Metrics represent the intrinsic qualities of a vulnerability. They include:

- Attack Vector (AV)
- Attack Complexity (AC)
- Privileges Required (PR)
- User Interaction (UI)
- Scope (S)
- Impact Metrics: Vulnerable System Confidentiality (VC), Integrity (VI), Availability (VA), and Subsequent System(s) Confidentiality (SC), Integrity (SI), Availability (SA)

a) Purpose

The Base metric group represents the intrinsic qualities of a vulnerability that are constant over time. It is composed of two sets of metrics: the Exploitability metrics and the Impact metrics. The Exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited, while the Impact metrics reflect the direct consequences of a successful exploit. The Base metrics help determine the initial severity score for a vulnerability. In CVSS v3.1, the base metric group consisted of four main metrics: Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR), and User Interaction (UI). CVSS 4.0 introduced a metric called the Attack Requirements (AT) to increase the granularity of the scoring system

b) Impact on Score

The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Threat and Environmental metrics. The Base score only reflects the technical severity of a vulnerability when considered in isolation. It's important to note that the Base score is only the starting point for building a full picture of the risk associated with a vulnerability.

c) Usage

The Base metric group is used to assess the fundamental qualities of a vulnerability that maintain their constancy over time. It is used to evaluate the severity of vulnerabilities and their impact on organizations without considering temporal or environmental factors

d) Calculation

The Base Metrics are divided into Exploitability Metrics and Impact Metrics. When these Base Metrics are assigned values by an analyst, they result in a score ranging from 0.0 to 10.0.

The CVSS v4.0 calculator, which is a reference implementation of the CVSS standard, can be used for generating scores based on the values of these metrics. The calculator applies the formula specified in the CVSS version 4.0 standard to produce the Base Score

e) Prioritizing vulnerabilities

Base metrics represent the intrinsic qualities of a vulnerability that are constant over time and across user environments. They include exploitability metrics (such as Attack Vector, Attack Complexity, Attack Requirement, Privileges Required, and User Interaction) and vulnerable system impact metrics (such as Confidentiality, Integrity, and Availability) and subsequent system impact metrics. The Base metrics produce a score ranging from 0 to 10, which reflects the technical severity of a vulnerability when considered in isolation. This score is essential when analyzing a vulnerability and helps in prioritizing vulnerabilities based on their inherent characteristics

2) Threat Metrics

The Threat Metrics, previously known as Temporal Metrics, adjust the severity of a vulnerability based on real-time factors. They include:

- Exploit Maturity (E)
- Remediation Level (RL)
- Report Confidence (RC)

a) Purpose

The purpose of the Threat metric group is to adjust the severity of a vulnerability based on factors such as the availability of proof-of-concept code or active exploitation. This group captures vulnerability characteristics related to a threat, which may change over time.

For example, it can capture information such as whether the vulnerability has been exploited or if there is any proof-of-concept exploit available. The values found in this metric group may change over time, reflecting the evolving threat landscape.

b) Impact on Score

The Threat metric group impacts the final CVSS score by adjusting the severity of a vulnerability based on the threat landscape. The absence of explicit Threat metric selections will still result in a score, but the inclusion of the “T” in the nomenclature is appropriate if any Threat metrics are used to adjust the score

c) Usage

The Threat metric group is used to refine the severity score of a vulnerability based on applicable threat intelligence. It is used in combination with the Base metric group, which represents the intrinsic qualities of a vulnerability that are constant over time, and the Environmental metric group, which represents the characteristics of a vulnerability that are unique to a specific computing environment.

d) Calculation

The Threat Metrics in the Common Vulnerability Scoring System (CVSS) version 4.0 adjust the severity of a vulnerability based on factors such as the availability of proof-of-concept code or active exploitation. These metrics reflect the characteristics of a vulnerability related to threat that may change over time.

In CVSS v4.0, the Threat Metrics replaced the Temporal Metrics from previous versions, resulting in clearer and simplified metrics. The Remediation Level (RL) and Report Confidence (RC) metrics, which were part of the Temporal Metrics in previous versions, have been removed in CVSS v4.0.

The values assigned to the Threat Metrics are used in the calculation of the final score, along with the Base and Environmental Metrics. If explicit Threat Metric values are not provided, default values that assume the highest severity are used.

The CVSS v4.0 calculator, which is a reference implementation of the CVSS standard, can be used for

generating scores based on the values of these metrics. The calculator applies the formula specified in the CVSS version 4.0 standard to produce the final score, which includes the Threat Metrics.

e) Prioritizing vulnerabilities

Threat metrics, previously known as Temporal Metrics, adjust the severity of a vulnerability based on factors such as the availability of proof-of-concept code or active exploitation. These metrics reflect the characteristics of a vulnerability that change over time, such as whether the vulnerability has been exploited or if any proof-of-concept exploit exists. The values in this metric group may change over time, and they help in real-time vulnerability assessment. By considering the likelihood of exploitation and the potential impact of a successful attack, CVSS v4.0 aims to offer a more holistic and accurate assessment of vulnerabilities.

3)Environmental Metrics

The Environmental Metrics allow organizations to customize the CVSS scores based on their specific environment. They include:

- Modified Base metrics
- Collateral Damage Potential (CDP)
- Security Requirement metrics: Confidentiality Requirement of the vulnerable system (CR), Integrity Requirement of the vulnerable system (IR), and Availability Requirement of the vulnerable system (AR)

a) Purpose

The Environmental Metric Group in CVSS v4.0 represents the characteristics of a vulnerability that are unique to a user's environment. It allows organizations to adjust the Base Score of a vulnerability to reflect its impact within their specific context. This group accounts for the presence of security controls that may mitigate some or all consequences of a vulnerability and the relative importance of a vulnerable system within a technology infrastructure.

b) Impact on Score

The Environmental Metrics enable analysts to customize the CVSS score with inputs regarding IT asset importance and the presence of mitigations, which can increase or decrease the severity of a vulnerability. These metrics are modifiers to the base metric group and are designed to account for aspects of an enterprise that might influence the severity of a vulnerability. . The Environmental Metric Group impacts the final CVSS score by allowing adjustments based on the specific environment where the vulnerability exists.

c) Usage

The Environmental Metric Group is used to tailor the CVSS score to an organization's unique environment, considering factors such as the importance of the affected IT asset and the effectiveness of existing security controls. These metrics are the modified equivalent of the Base Metrics and are specified by users to provide a more accurate assessment of the risk posed by a vulnerability in their specific operational context.

d) Calculation

The Environmental Metrics in the Common Vulnerability Scoring System (CVSS) version 4.0 are designed to adjust the Base Score of a vulnerability to reflect the impact within a specific organizational context. These metrics account for the protection goals of the affected system and the presence of security controls that mitigate vulnerability.

The Environmental Metrics are calculated by first determining the Modified Base Metrics, which are the Base Metrics adjusted for the presence of mitigations or compensating controls. The Security Requirements are used to indicate the importance of the affected IT asset to the organization, which can amplify or reduce the severity based on the asset's criticality. The Collateral Damage Potential metric reflects the potential for non-direct damage to the environment or entities beyond the IT asset.

The final Environmental Score is derived by combining the Modified Base Metrics with the Security Requirements and Collateral Damage Potential, using a formula specified in the CVSS v4.0 Specification Document. This score provides a more tailored assessment of the vulnerability's severity within the specific environment of the organization

e) Prioritizing vulnerabilities

Environmental metrics further refine the resulting severity score to a specific computing environment. They consider factors such as the presence of mitigations in that environment and the criticality of the systems. These metrics are specified by users and can lead to a disconnect between the score and the actual risk in the real world due to their subjective nature. However, they are crucial in providing a more precise assessment of vulnerabilities in a specific environment, thus enhancing vulnerability prioritization and risk management.

4)Supplemental Metrics

The Supplemental Metrics provide additional context and describe aspects of a vulnerability that are outside the core CVSS standard. They include:

- Automatable (A)
- Value Density (VD)
- Recovery (R)
- Provider Urgency (PU)
- Vulnerability Response Effort (VRE)

a) Purpose

The purpose of the Supplemental Metric Group is to provide users with contextual information that allows for a more nuanced understanding of vulnerabilities. These metrics offer valuable insights into extrinsic aspects of vulnerabilities, allowing consumers to delve deeper into specific contextual considerations. They are designed to provide a more complete understanding of vulnerabilities by describing and measuring additional extrinsic attributes

b) Impact on Score

Unlike core CVSS metrics, Supplemental metrics do not contribute to the calculation of CVSS scores. They do not have any impact on the final calculated CVSS score. Instead, they serve as supplementary information for a more nuanced vulnerability assessment. Organizations may then assign importance and/or effective impact of each metric, or set/combination of metrics, giving them more, less, or absolutely no effect on the final risk analysis

c) Usage

The usage of each metric within the Supplemental metric group is determined by the scoring consumer. This contextual information may be employed differently in each consumer's environment. The information consumer can then use the values of these Supplemental Metrics to take additional actions if they so choose, applying locally significant importance to the metrics and values

d) Calculation

The Supplemental Metrics in the Common Vulnerability Scoring System (CVSS) version 4.0 are a new addition designed to provide additional context and describe extrinsic attributes of a vulnerability. These metrics are optional and do not contribute to the calculation of the final CVSS score. Instead, they serve as supplementary information for a more nuanced vulnerability assessment.

The usage and response plan of each metric within the Supplemental metric group is determined by the scoring consumer. This contextual information may be employed differently in each consumer's environment. Organizations may then assign importance and/or effective impact of each metric, or set/combination of metrics, giving them more, less, or absolutely no effect on the final risk analysis.

e) Prioritizing vulnerabilities

Supplemental metrics are a new addition in CVSS v4.0. They measure extrinsic attributes of a vulnerability and provide contextual information. These metrics do not affect the vulnerability score but can be used to inform the companies that purchase the products. They include concepts such as "Automatable," "Recovery," and "Mitigation Effort," which provide additional context for vulnerability and remediation teams

5)Differences

The Supplemental Metric Group is used to provide additional context and does not affect the CVSS score, whereas the Base, Threat, and Environmental Metric Groups contribute directly to the scoring process and are essential for calculating the severity of a vulnerability. The Supplemental Metric Group in CVSS v4.0 is distinct from the Base, Threat, and Environmental Metric Groups in several ways:

Supplemental Metric Group:

- **Purpose**: Provides additional context and describes extrinsic attributes of a vulnerability that are outside the core CVSS standard
- **Impact on Score**: The metrics in this group do not impact the final calculated CVSS score. They are optional and are used to convey additional information that may influence an organization's risk analysis and response plan
- **Usage**: The usage and response plan of each metric within the Supplemental Metric Group is determined by the scoring consumer, and this contextual information may be employed differently in each consumer's environment

Base, Threat, and Environmental Metric Groups:

- **Purpose**: These groups contain metrics that directly contribute to the calculation of the CVSS score, reflecting the intrinsic qualities of a vulnerability (Base), the real-time threat landscape (Threat), and the specific impact within an organizational context (Environmental)
- **Impact on Score**: The metrics in these groups directly affect the final CVSS score, with each group providing a different perspective on the severity and impact of the vulnerability
- **Usage**: The Base Metrics are provided by the organization maintaining the vulnerable system or a third party, while the Threat and Environmental Metrics are intended for end consumers to enrich the Base metrics with additional context

F. Operational technology exposure metrics in cvss v4.0

In CVSS v4.0, new metrics have been introduced to address the exposure and impact of vulnerabilities in Operational Technology (OT). These metrics are particularly relevant due to the increasing concerns around the security of OT, industrial control systems (ICS), and the Internet of Things (IoT). The updates aim to provide a more accurate assessment of the risks associated with vulnerabilities in these environments

1)Safety Metrics

Safety metrics have been added to both the Supplemental and Environmental metric groups in CVSS v4.0. These metrics assess the potential safety impact of exploiting a vulnerability, which is especially important in sectors like healthcare or industrial control systems where safety is a critical concern

2)OT-Specific Considerations

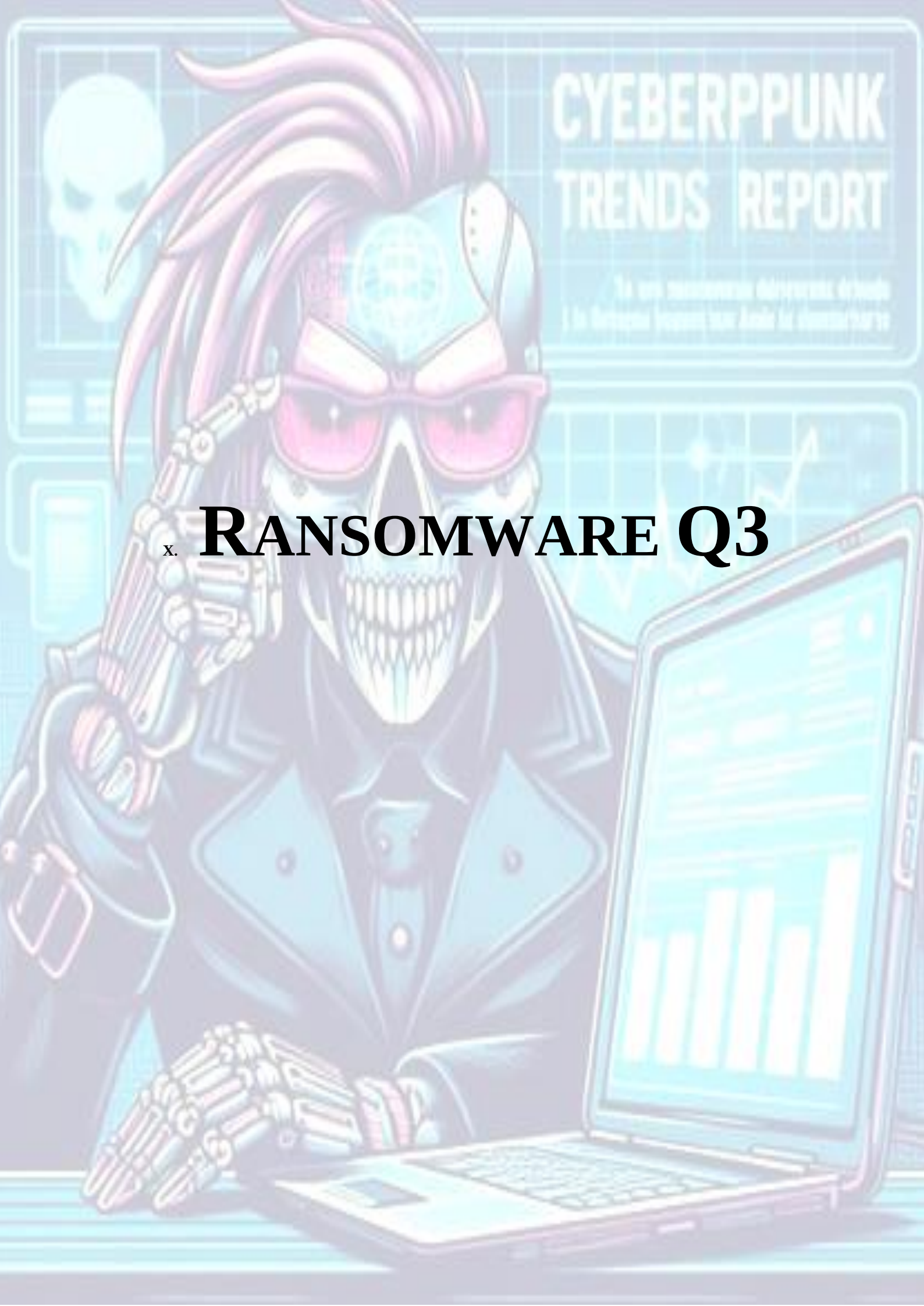
The new metrics for Operational Technology exposure include considerations for whether the "consequences of the vulnerability meet the definition of IEC 61508," which is a standard for the functional safety of electrical/electronic/programmable electronic safety-related systems . This inclusion reflects the growing concern about OT cyber risk and the need for a scoring system that can adequately capture the unique risks associated with OT environments

3)Impact on Vulnerable and Subsequent Systems

CVSS v4.0 also emphasizes evaluating the impact of vulnerability exploitation on both the vulnerable system and subsequent systems. This is particularly relevant for OT environments where a vulnerability in one component could potentially have cascading effects on other interconnected systems

4)Use of Supplemental and Environmental Metrics

While the Supplemental metrics do not directly impact the final CVSS score, they provide valuable contextual information that can be used by organizations to inform their risk analysis and response plans. The Environmental metrics allow for customization of the CVSS scores based on the specific environment, which can include OT settings



x. RANSOMWARE Q3

A. Introduction

According to different reports the year 2023 is considered the most successful year for ransomware groups in history, with a total of 4,368 victims, marking a rise of over 55.5% since the previous year. Q2 and Q3 alone claimed more victims than the entirety of 2022, with 2,903 victims. In Q2 2023, there was a significant increase of 67% in ransomware cases compared to the previous quarter, with ransomware groups compromising 1,386 victims worldwide.

Below, we will analyze in detail the public materials on ransomware for the third quarter of 2023, delving into various aspects of the current situation, changing trends in attacks, industries and the geography of the phenomenon. The materials make it possible not only to assess the quantitative factors of incidents, but also to provide a qualitative synthesis of these tactics used by attackers and the consequences for cybersecurity strategies in the future. The purpose of the analysis is to provide readers with useful information and a deeper understanding of the phenomenon of ransomware in its current form and its trajectory in the field of cybersecurity

B. 2023 Ransomware Overview

- **Ransomware Attacks Increase**: The number of known attacks, where the victim did not pay a ransom, was 457 in November alone; the total number of attacks recorded was 1,900, and the undisclosed attacks were a massive 1,815 in the first six months of the year. The number of ransomware-related posts was 4,082, with an average of 371.1 posts per month.
- **Ransomware Attacks on Healthcare Sector**: with a 278% increase in ransomware attacks on the health sector over the past four years. The large breaches reported in 2023 affected over 88 million individuals, a 60% increase from the previous year.
- **Ransomware Gangs**: Several ransomware gangs were shut down in 2023, including Hive, RansomedVC, and ALPHV. However, new and evolving players such as Hunters International, Dragon Force, and WereWolves emerged.
- **Ransomware Payment**: The average enterprise ransom payment exceeded $100,000, with a $5.3 million average demand. However, 80% of organizations have a "Do-Not-Pay" policy on ransomware, and only 41% of organizations attacked last year paid the ransom.
- **Ransomware Insurance**: 77% of organizations found out that ransomware is specifically excluded from their security insurance. Insurance companies are catching on, with 74% seeing their premiums increase, 43% seeing increased deductibles, and 10% seeing their coverage benefits reduced.
- **Ransomware Targets**: manufacturing sector emerged as a prime target for 48 distinct ransomware groups In US.
- **High-Profile Attacks**: High-profile attacks were carried out on Toyota, Boeing, and more using a Citrix Bleed vulnerability (CVE-2023-4966).
- **Ransomware as a Service (RaaS)**: The proliferation of RaaS was a notable trend in 2023, simplifying the execution of ransomware attacks for cybercriminals.
- **Prominent Ransomware Groups**: Groups such as CL0P played a major role in the spike of ransomware activity in 2023, with CL0P exploiting the file transfer software and impacting over 130 victims.
- **Ransomware Success**: The year 2023 is noted as the most successful year for ransomware groups historically, with a total of 4,368 victims, which is a 55.5% increase from the previous year. The second and third quarters of 2023 alone surpassed the total number of victims in 2022, with 2,903 victims.
- **Q2 2023 Ransomware Surge**: There was a 67% increase in ransomware cases in Q2 2023 compared to the previous quarter, with 1,386 victims globally. Leading ransomware groups during this period were LockBit3.0, ALPHV, and Cl0p.
- **MOVEit Campaign**: The MOVEit campaign was singled out as the most successful of the year, underscoring the significance of supply chain attacks and the need for robust version control and attack surface understanding. The United States was the primary target, with approximately 64% of the cases.
- **Record-Breaking Q3 2023**: Q3 2023 was the most successful quarter ever for ransomware, with the industry heavily impacted by the exploitation of critical vulnerabilities. The rise of new ransomware groups and families contributed to this growth.

C. Highlight on MOVEit Campaign

- **Exploitation**: CVE-2023-34362 affected both on-premises and cloud-based versions of MOVEit related to SQL injection, a common entry point into applications that enables data manipulation or database access.

- **The Perpetrators**: The Clop group was responsible for the attacks and they were also linked to the GoAnywhere and PaperCut incidents earlier in the same year.
- **The Impact**: The campaign had a significant impact, affecting over 1,062 organizations and approximately 65,435,641 individuals by the end of August 2023. The victims spanned a range of industries and included both private entities and public sector organizations.
- **The Response**: Progress Software responded promptly to the discovery of the vulnerability, issuing a patch and advising customers to apply it immediately. However, the victim count continued to grow months later, suggesting that many organizations were breached in the first few days and weeks of the campaign.
- **The Aftermath**: The MOVEit campaign highlighted the importance of proactive cybersecurity and vulnerability management as well as potential damage that can be caused by supply chain cyber-attacks, as many organizations were compromised not because they used MOVEit directly, but because they employed third-party contractors or subcontractors who did.

D. Geographical Impact

- **Global Spread of Ransomware**: Cybercriminals expanded their geographical reach in 2023, taking proven malware tools to new countries and regions.
- **Countries Most Affected**: The United States was the most affected country, with the highest number of breached accounts. Other countries significantly impacted by ransomware attacks included the UK and Canada, Mozambique, Angola, and Ghana.
- **Ransomware by Industry**: Ransomware attacks affected some verticals more than others. The top targets by industry included education, construction and property, central and federal government, media, entertainment and leisure, and local and state gov.
- **Ransomware Trends**: New ransomware groups like Rhysida, BianLian, IceFire, Sparta, Bl00dy emerged, underscoring the evolving nature of the industry.

E. *Q3 2023: A Record Quarter*

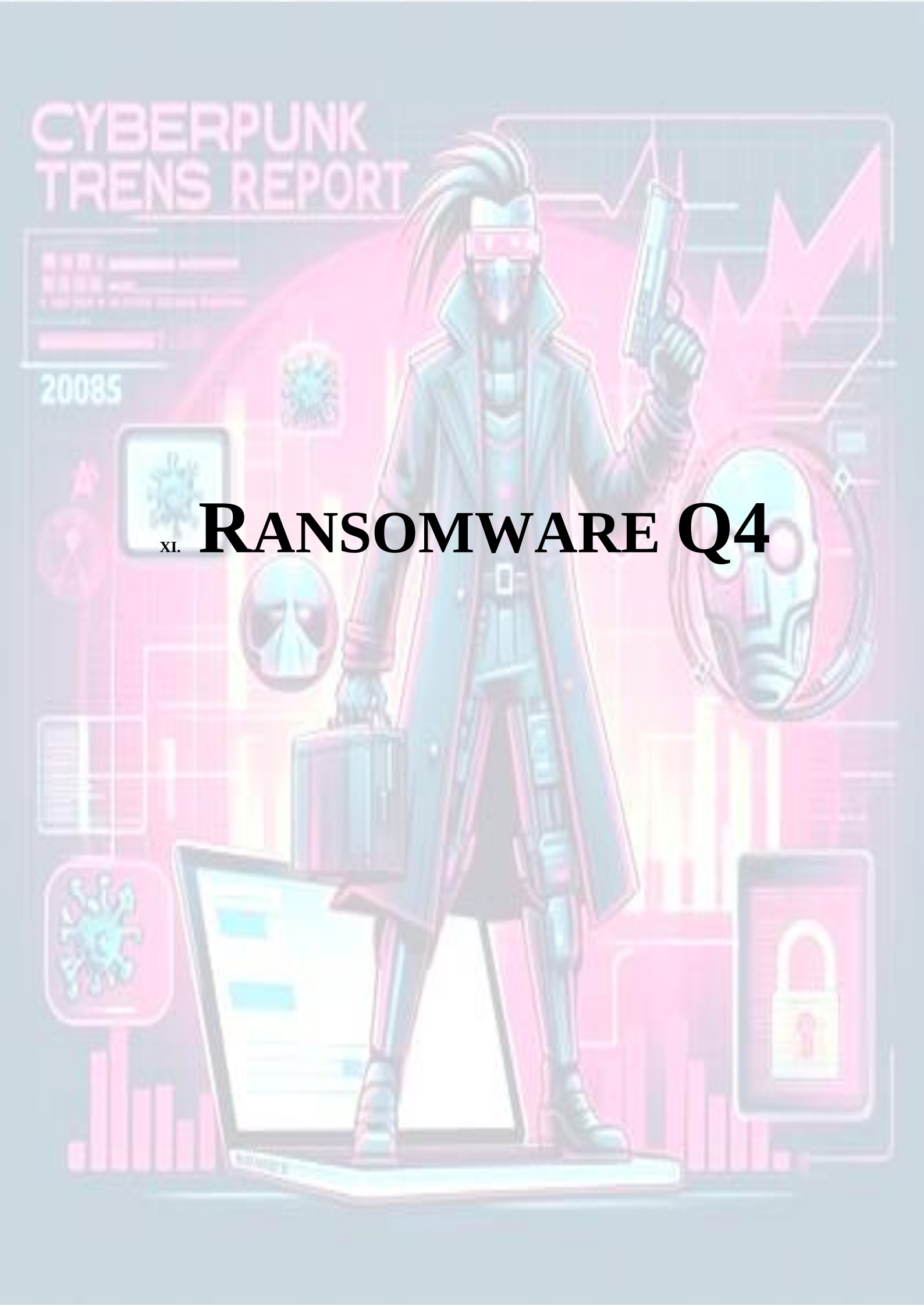
- **Record-Breaking Ransomware Activity**: The third quarter of 2023 witnessed a significant surge in ransomware activity, with global ransomware attack frequency up by 11% over Q2 and 95% year-over-year.
- **Ransomware Victims**: The number of ransomware victims in 2023 has already surpassed what was observed for 2021 and 2022.
- **Emerging Ransomware Groups**: New ransomware groups such as MalasLocker, 8base, and Nokoyawa gained attention in Q3 2023. In their first quarter of operations, these groups collectively claimed a total of 305 victims.
- **Ransomware by Industry**: Ransomware attacks affected some sectors more than others. The sectors hardest hit by the record-breaking spike in ransomware attack frequency included law practices, government agencies, manufacturing, oil and gas, transportation, logistics, and storage sectors.
- **Future Trends**: Based on the activity at the end of Q3 and early Q4, it is expected that the numbers will surpass anything witnessed in previous years

F. Outlook for 2024

- **Continued Growth of Ransomware**: the ransomware industry will reach new heights in 2024, continuing to deliver a high number of victims as promising newcomers establish their presence
- **Supply Chain Attacks**: Ransomware groups are expected to take advantage of and compromise supply chain infrastructures while still sticking to traditional methods such as exploiting old leaked credentials and using social engineering techniques
- **Ransomware Trends**: ransomware industry is expected to evolve with new groups and tactics emerging.
- **Law Enforcement and Industry Efforts**: Efforts to combat ransomware will continue, with a focus on shutting down major cyber groups and preventing attacks
- **Ransomware Insurance**: As ransomware attacks increase, the role of insurance in cybersecurity will become more critical, with organizations needing to navigate the complexities of coverage for ransomware incidents
- **Technological Developments**: The cybersecurity landscape will continue to evolve, with a shift towards more comprehensive defense strategies that include prevention, detection, remediation, and forensics
- **Global Impact**: The geographical impact of ransomware is expected to remain significant, with cybercriminals continuing to target a wide range of countries and industries
- **Ransomware Variants**: The emergence of new ransomware strains and the continued activity of existing ones will likely persist, posing ongoing challenges for cybersecurity defenses

G. Conclusion

- **Ransomware in 2023**: 2023 was a record-breaking year for the ransomware industry, with a significant increase in the number of attacks. The most targeted sector was the business services sector, followed by the retail and manufacturing sectors
- **Ransomware Industry Growth**: Despite the efforts of law enforcement, the ransomware industry continued to grow rapidly. New groups emerged, and existing groups like LockBit3.0, ALPHV, and Cl0p caused severe damage to organizations worldwide
- **Law Enforcement Efforts**: Law enforcement authorities worldwide have been working to stop the growth of the ransomware industry. They had some success in shutting down several major cybercrime groups, such as HIVE
- **Outlook for 2024**: the ransomware industry will continue to grow in 2024, with new and existing groups posing significant threats to organizations worldwide



XI. RANSOMWARE Q4

Abstract – The analysis of the ransomware trends for the 4th quarter of 2023 aims to understand the multifaceted threat landscape associated with ransomware.

Delving into the specifics, we intend to reveal the nuances of ransomware operations, including the identification of the dominant groups of ransomware, their target sectors and the geographical distribution of attacks.

Furthermore, the analysis will highlight significant trends, such as the surge in ransomware incidents, the evolution of extortion tactics, and the implications of these developments on cybersecurity strategies.

This knowledge will be useful for both technical and strategic security professionals, offering information that can guide the development of reliable protection mechanisms, inform risk management decisions and, ultimately, increase the resilience of organizations to the ever-present threat of ransomware.

The significance of this analysis extends beyond mere academic interest; it equips security practitioners with actionable intelligence, enabling them to anticipate and counteract the sophisticated strategies employed by ransomware operators.

A. Introduction

In Q4 2023, the most common types of ransomware attacks were primarily carried out by three groups: LockBit 3.0, Clop Ransomware, and ALPHV/BlackCat ransomware.

LockBit 3.0 remained the most active ransomware group, claiming an average of around 23 victims per week. Other prominent groups included Clop Ransomware and ALPHV/BlackCat ransomware. Notable incidents included LockBit's attack on Royal Mail and the shutdown of Hive Ransomware.

The Quarterly Threat Report by Air IT highlighted that ransomware attacks, phishing, and insider threats continued to pose significant risks, with a surge in data volume and global connectivity widening vulnerabilities. The report from ISACA's State of Cyber Security for 2023 indicated that 48% of organizations experienced a rise in cyber attacks in Q4 2023.

TechTarget's report on ransomware trends heading into 2024 suggested that supply chain attacks and the exploitation of cloud and VPN infrastructure would continue to be key trends. The report also mentioned that since 2020, more than 130 different ransomware strains have been detected, with the GandCrab family being the most prevalent.

The environmental services industry faced an unprecedented surge in DDoS attacks, with a 61,839% increase in attack traffic year-over-year, as reported by Cloudflare. This surge was associated with the COP 28 event and highlighted the growing intersection between environmental issues and cyber threats.

Trend Micro's report on ransomware in the first half of 2023 showed that LockBit, BlackCat, and Clop were the top RaaS groups, with a significant increase in the number of victim organizations compared to the last half of 2022.

Check Point Research described 2023 as the year of mega ransomware attacks, with a shift in tactics from encryption to leveraging stolen data for extortion. The education/research sector was the most impacted by ransomware attacks in 2023.

B. Affected industries

- In Q4 2023, the industries most affected by ransomware attacks were the business services sector, education/research sector, and the retail/wholesale sector.
- The business services sector was the most targeted sector. The United States, being the most targeted country, likely contributed to the high number of attacks on this sector.
- The education/research sector was also heavily impacted by ransomware attacks, accounting for 22% of all attacks in 2023, according to Check Point Research.
- The retail/wholesale sector experienced a significant 22% spike in attacks weekly compared to 2022, as reported by Check Point Research.

Other industries that were notably affected include the IT, healthcare, and manufacturing sectors, which were the most targeted sectors in terms of ransomware file detections in the first half of 2023, according to Trend Micro. The report from TechTarget also listed several industries as top targets, including construction and property, central and federal government, media, entertainment and leisure, local and state government, energy and utilities infrastructure, distribution and transport, financial services, and business, professional and legal services.

C. Takeaways from Ransomware Q4

- **Record Number of Victims**: The year 2023 marked the most successful year for ransomware groups in history, with a total of 4,368 victims, which is a 55.5% increase from the previous year. The fourth quarter alone saw 1,386 victims

- **Dominant Ransomware Groups**: LockBit 3.0 remained the most active ransomware group, claiming an average of around 23 victims per week. Clop Ransomware and ALPHV/BlackCat ransomware were also prominent, with 104 and 81 victims respectively
- **High-Profile Incidents**: Notable incidents included LockBit's attack on Royal Mail and the shutdown of Hive Ransomware
- **Industry Impact**: The business services sector, education/research sector, and the retail/wholesale sector were among the most affected by ransomware
- **Geographical Focus**: The United States was the most targeted country, followed by the UK and Canada
- **Trends in Attack Techniques**: There was a shift in tactics from encryption to leveraging stolen data for extortion, with attackers focusing more on data theft and extortion campaigns that did not necessarily involve data encryption
- **Ransomware Strains**: Since 2020, more than 130 different ransomware strains have been detected, with the GandCrab family being the most prevalent
- **Increased Response from Governments and Vendors**: There has been an increased response from government and technology vendors to help stem the tide of ransomware attacks
- **Ransomware as a Service (RaaS)**: RaaS remains a key driver for the ongoing frequency of attacks, with groups like LockBit operating under this model
- **Extortion Tactics**: Double and triple extortion attacks have become more prevalent and potentially more impactful and costly for affected companies
- **Supply Chain Attacks**: Supply chain attacks have become an established part of the ransomware threat landscape, extending the impact of attacks beyond single victims

D. Ransomware Payments

In Q4 2023, the most common payment methods used in ransomware attacks continued to be cryptocurrencies, with Bitcoin being the most prevalent. Bitcoin accounted for approximately 98% of ransomware payments due to its perceived anonymity and ease of use. However, there were early indications that more privacy-focused digital currencies, such as Monero, were growing in popularity as the payment method of choice for cybercriminals. This shift was due to the increasing ease of detecting the flow and sources of Bitcoin.

Despite the prevalence of ransom payments, the proportion of victims who paid ransoms was decreasing. Only 37% of ransomware victims paid a ransom in Q4 2023, a record low. This decrease was attributed to improved security measures and backup continuity investments, which allowed more organizations to recover from attacks without paying ransoms.

The average ransom payment in Q4 2023 was significantly high, with the average payment being $408,643, a 58% increase from Q3 2022, and the median payment being $185,972, a 342% increase from Q3 2022. This increase in payment amounts was seen as a tactic by cybercriminals to compensate for the declining number of victims willing to pay ransoms.

E. Ransomware Entry Points

- **Phishing Attacks**: Phishing attacks were the primary delivery method for ransomware, with 62% of successful ransomware attacks using phishing as their entry point in the victim's system. Phishing attacks rose by 173% in Q3 2023. Attackers used increasingly sophisticated social engineering techniques to trick employees into providing sensitive information
- **Exploitation of Vulnerabilities**: Vulnerabilities in software and systems were another common entry point. For instance, the ransomware group CL0P exploited GoAnywhere file transfer software. Two new ransomware strains, CACTUS and 3AM, emerged in Q4 2023, with CACTUS exploiting known vulnerabilities in VPN appliances
- **Credential Theft and Brute Force Attacks**: Credential theft was used in 44% of successful ransomware attacks, and brute force credentials, such as password guessing, were used in 17% of attacks
- **Supply Chain Attacks**: Attackers targeted third-party vendors to gain access to an organization’s network
- **Insider Threats**: Insider threats continued to pose significant risks to organizations
- **Social Engineering Attacks**: these attacks, including Business Email Compromise (BEC), were also common

F. Ransomware Encryption methods

The encryption methods used in these attacks have evolved over time, with attackers adopting a mix of symmetric and asymmetric encryption techniques to increase the effectiveness of their attacks. In this approach, the ransomware generates two sets of keys, and a chain of encryption is used to increase the attack effectiveness.

In addition to these encryption methods, there has been a notable shift in the execution strategies of ransomware attacks. Increasingly, cybercriminals are focusing more on data theft, followed by extortion campaigns that do not necessarily involve data encryption.

G. Ransomware Delivery methods

In Q4 2023, the most common delivery methods used in ransomware attacks were supply chain attacks, double extortion techniques, and Ransomware-as-a-Service (RaaS) operations.

Supply chain attacks became a solid technique for mature and experienced ransomware groups. In these attacks, instead of directly attacking a single victim, the attackers target third-party vendors to gain access to an organization's network.

Double extortion was another prevalent method. In this technique, attackers not only encrypt the victim's data but also threaten to leak stolen data if the ransom is not paid.

Ransomware-as-a-Service (RaaS) operations also played a significant role. In RaaS, developers create ransomware software and sell access to this tool to criminals who then spread it among potential targets. The access is subscription-based, which is why it is called RaaS.

Phishing with malicious attachments and exploiting vulnerabilities, such as zero-day vulnerabilities, were also used as initial access methods to the target system

H. Vulnerabilities exploited by ransomware

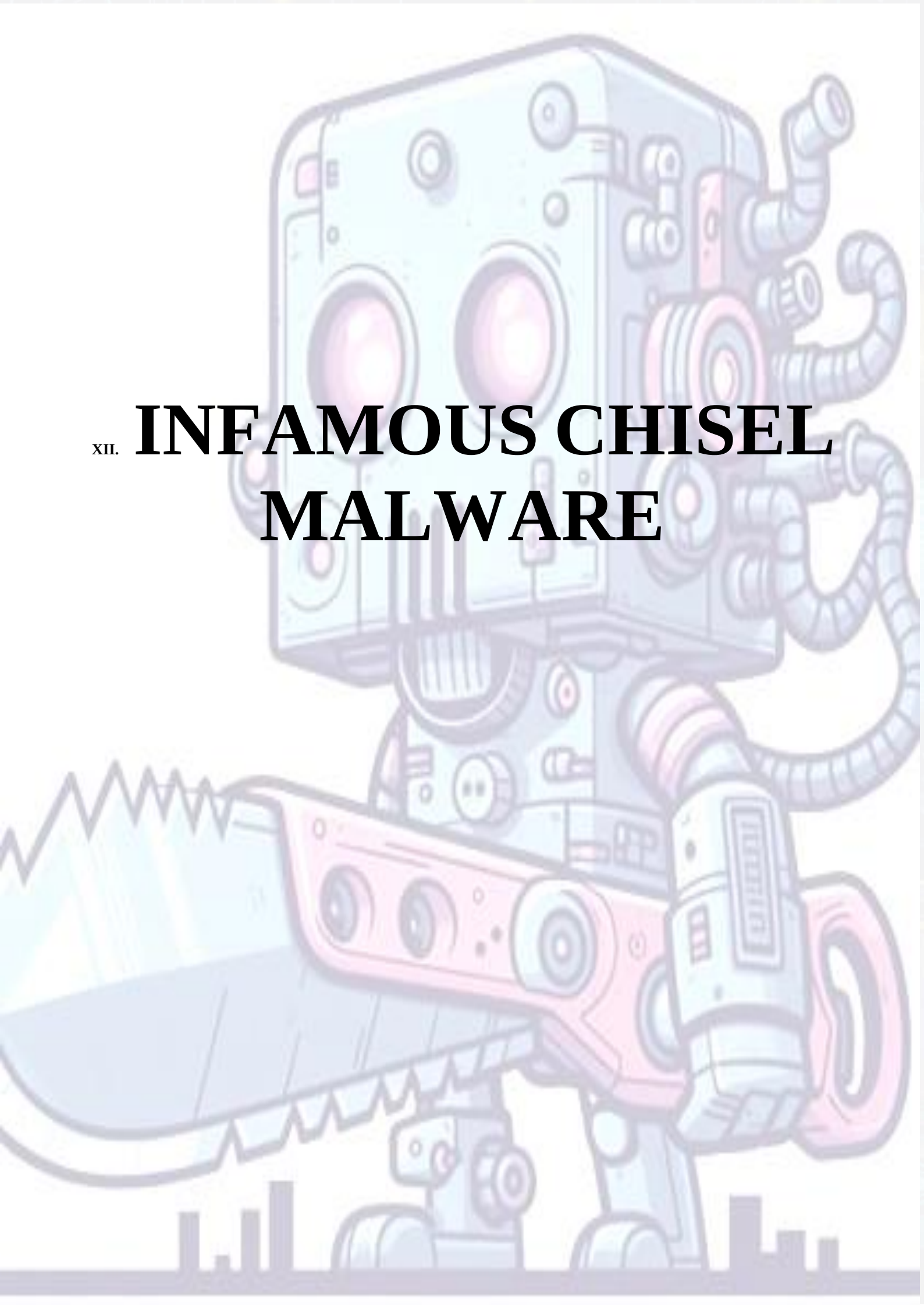
In Q4 2023, ransomware attackers continued to exploit a range of vulnerabilities to compromise organizations. One of the most notable vulnerabilities exploited was a two-year-old vulnerability for which a patch had been available for around the same time. This highlights the importance of timely patch management and version control within organizations.

Additionally, attackers used a flaw in MagicLine4NX software, affecting versions before 1.0.026, to initiate their attacks. The MOVEit vulnerability was also significant, accounting for a notable percentage of victims in previous quarters, and it is likely that such vulnerabilities continued to be a target for ransomware groups.

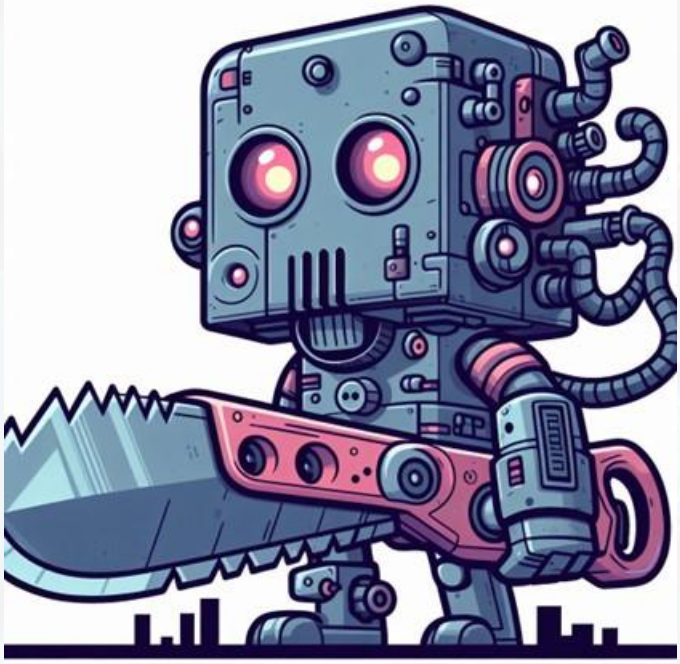
The year 2023 also saw a surge in the use of zero-day exploits in ransomware attacks, which are vulnerabilities that are unknown to the software vendor or have no patch available at the time of the attack. This trend of exploiting zero-day vulnerabilities underscores the adaptability of cyber threat actors and the need for organizations to enhance their defenses against such evolving threats.

I. Effective ways to prevent ransomware attacks

- **Robust Data Backup**: Regularly backing up data is a crucial step in mitigating the impact of a ransomware attack. A secure, robust data backup solution can ensure that even if data is encrypted by ransomware, the organization can restore its systems without having to pay the ransom
- **Cyber Awareness Training**: Training employees to recognize and avoid potential ransomware threats, such as phishing emails and malicious attachments, can significantly reduce the risk of successful attacks
- **Patch Management**: Regularly updating and patching software can eliminate known vulnerabilities that ransomware might exploit
- **Advanced Threat Prevention**: Automated threat detection and prevention systems can identify and resolve most ransomware attacks before they cause significant damage
- **Endpoint Security**: Robust endpoint security solutions, including antivirus and anti-malware software, can detect and block ransomware threats
- **Network Segmentation**: Dividing the network into separate segments can prevent ransomware from spreading across the entire system
- **Zero Trust Security Model**: Implementing a zero-trust model, where access to resources is granted only after a user has successfully verified their identity, can reduce the attack surface against ransomware
- **Multi-factor Authentication (MFA)**: Implementing MFA can add an additional layer of security, making it more difficult for attackers to gain access to systems
- **Least Privilege Access**: Ensuring that users have the minimum levels of access necessary to perform their tasks can limit the potential damage of a ransomware attack
- **Application Whitelisting**: Allowing only approved applications to run on a system can prevent ransomware from executing



XII. INFAMOUS CHISEL MALWARE



Abstract – This document presents an analysis of the "Infamous Chisel" malware, a sophisticated cyber threat attributed to the Sandworm group. The analysis delves into various aspects of the malware, including its capabilities, components, and the implications of its deployment against specific targets, notably Android devices.

By dissecting the malware's components and tactics, the document sheds light on the sophisticated nature of cyber threats and their potential to compromise sensitive information and disrupt operations. The findings underscore the critical need for vigilance and proactive defense measures in the face of such advanced threats.

For cybersecurity professionals and other specialists across various sectors, this analysis serves as a valuable resource for understanding the mechanics and implications of advanced malware threats like Infamous Chisel. The document's insights can inform the development of more effective defense strategies and technologies, enhancing the security posture of organizations and protecting against the ever-evolving landscape of cyber threats.

A. Introduction

The Chisel malware targets Android devices, enabling remote access and exfiltrating information from these devices. Sandworm has used this malware in a campaign targeting Android devices used by the military sector. The malware is a collection of components that enable persistent access to an infected Android device over the Tor network and periodically collates and exfiltrates victim information from compromised devices. The information exfiltrated includes system device information, commercial application information, and applications specific to the military sector.

B. Components of infamous chisel

Infamous Chisel is a collection of components associated with Sandworm, designed to enable remote access and exfiltrate information from Android phones.

The components of Infamous Chisel include:

- **netd**: This component is used to perform automated device information collection and exfiltration. It also searches multiple directories for files matching a predefined set of extensions which are then exfiltrated.
- **killer**: This component kills the malicious netd process.
- **blob**: This component is executed by netd and is responsible for configuring and executing the Tor utility td.
- **td**: This utility is Tor with no obvious modifications.
- **tcpdump**: This utility is tcpdump with no obvious modifications.
- **ndbr_armv7l and ndbr_i686**: These utilities are multi-call containing: dropbear, dropbearkey, ssh, scp, nmap, dbclient, watchdog, rmflag, mkflag.
- **db**: This utility is multi-call containing: dropbear, dropbearkey, ssh, scp, nmap, dbclient, watchdog, rmflag, mkflag.

C. Network and other features

Infamous Chisel is designed to persist on the system by replacing the legitimate netd system binary at the path /system/bin/netd. When the malicious netd is executed, it will check if init is the parent process which executed it. This parent process is responsible for creating the processes listed in the script init.rc. The malicious replacement netd when executed in this way will fork and execute the legitimate process backed up at the path /system/bin/netd_ passing through the command line parameters. This retains the normal functionality of netd, while allowing the malicious netd to execute as root.

The netd component of Infamous Chisel provides the bulk of the custom functionality which the actor deploys. The main purpose of netd is to collate and exfiltrate information from the compromised device at set intervals. It uses a combination of shell scripts and commands to collect device information. It also searches multiple directories to which files matching a predefined set of extensions are exfiltrated.

Infamous Chisel has several other capabilities:

- **Network Monitoring and Traffic Collection**: Infamous Chisel can monitor network activity and collect network traffic data. This allows it to gather information about the network environment and potentially capture sensitive data transmitted over the network
- **SSH Access**: Infamous Chisel can establish SSH connections, which can be used for remote command execution and data transfer
- **Network Scanning**: The malware can scan the local network, collating information about active hosts, open ports, and banners. This can help identify other potential targets within the network

- **SCP File Transfer**: Infamous Chisel can use the Secure Copy Protocol (SCP) for file transfers. This can be used to exfiltrate data from the infected device or to transfer malicious files onto the device
- **Information Exfiltration**: Infamous Chisel performs periodic scanning of files and network information for exfiltration. System and application configuration files are exfiltrated from an infected device
- **Device Information Collection**: Infamous Chisel collects various system device information, commercial application information, and applications specific to the military sector
- **Automated Exfiltration**: Infamous Chisel automatically exfiltrates files at regular intervals
- **Service Stop**: Infamous Chisel can stop the legitimate netd service

D. Exploited Vulnerabilities

The Infamous Chisel campaign exploits a variety of vulnerabilities and techniques to enable unauthorized access and control over targeted Android devices. the Infamous Chisel campaign exploits a combination of system vulnerabilities, insecure configurations, and network protocols to achieve its objectives. These include gaining persistence and elevated privileges, evading detection, accessing credentials, collecting sensitive information, establishing covert command and control channels, and potentially moving laterally within the network.

The primary vulnerabilities and techniques exploited by Infamous Chisel include (without specific CVE):

- **Persistence and Privilege Escalation**: Infamous Chisel achieves persistence on the infected device by replacing the legitimate netd system binary. This replacement allows the malicious netd to execute as root, thereby gaining elevated privileges.
- **Defense Evasion**: The malware employs several defense evasion techniques. For instance, it checks that it is executed by init and at the path for the legitimate netd, ensuring its malicious activities are less likely to be detected. Additionally, the blob component decompresses executables from bzip archives, which could be a method to evade detection by unpacking its payload only after it has bypassed initial security checks.
- **Credential Access**: Infamous Chisel uses the tcpdump utility to sniff network interfaces and monitor network traffic, potentially capturing credentials transmitted over the network. It also scrapes multiple files containing credentials and key information, exploiting the storage and handling of sensitive information on the device to gain unauthorized access to accounts and services.
- **Discovery and Collection**: The malware performs extensive discovery and collection activities, such as enumerating data directories to discover files of interest, collecting GPS information, listing installed packages, and gathering various system information. This indicates that Infamous Chisel exploits the lack of secure storage and inadequate permissions settings on the device to access and collect sensitive information.
- **Command and Control (C2) and Exfiltration**: Infamous Chisel configures and executes Tor with a hidden service, which forwards to a modified Dropbear binary providing an SSH connection. This setup allows the malware to establish a covert communication channel with the infected device, exploiting network protocols and services to maintain control over the device and exfiltrate collected data.
- **Network Scanning and Lateral Movement**: The malware contains functionality to scan the local network, collating information about active hosts, open ports, and banners. This capability suggests that Infamous Chisel exploits the network environment of the infected device to identify other potential targets within the network for lateral movement or further exploitation

E. Infiltration

The Infamous Chisel campaign exfiltrates information from infected Android devices through a series of automated and manual processes. The malware, associated with the Sandworm threat actor, performs periodic scanning of files and network information for exfiltration. It searches for files matching a predefined set of extensions and exfiltrates system and application configuration files from the infected device.

The exfiltration process is detailed as follows:

- **File Hashing and Avoiding Duplication**: When a file is selected for exfiltration, it is hashed using MD5 and cross-referenced with a list of previously sent file hashes held in a file at one of three locations supporting different Android versions. This ensures that the same file isn't sent multiple times.
- **File exfiltration from data directories**: The malware searches specified directories for files with certain extensions and exfiltrates them.
- **Exfiltration of configuration and configuration backup files**: The malware searches for .json or .json.bak files in specified directories and exfiltrates them.
- **File Exfiltration**: The malware exfiltrates files using a HTTP POST request. The server response is expected to be HTTP, and the exfiltration is considered complete when the server sends 'Success' anywhere in its response.
- **Information Gathering and Exfiltration**: Infamous Chisel collects various hardware configuration information about the device and writes this information to files in the /data/local directory, which are then exfiltrated. This includes the Android ID, networking information, a list of installed applications, and various device hardware information.
- **Local Area Network Scanning**: The malware includes a built-in network scanner that performs IP

scanning of the local network to discover other devices. The results of this scan are exfiltrated immediately, providing the attackers with information that could facilitate lateral movement within the network.

- **Exfiltration Frequency**: The malware is designed to automatically exfiltrate files at regular intervals, with specific intervals set for different types of data collection. For example, file and device information compilation takes place every 23 hours and 53 minutes, while sensitive military information is siphoned every 10 minutes.
- **Use of Tor and SSH for Secure Exfiltration**: Infamous Chisel uses Tor and SSH for command and control communications, providing an encrypted channel that can be difficult to detect and intercept. This setup allows the malware to maintain a covert communication channel with the infected device, making detection and mitigation more challenging

When a file is selected for exfiltration, it is MD5-hashed and cross-referenced with a list of previously sent file hashes held in a file at one of three locations supporting different Android versions. The first existing directory path will be used: /sdcard/Android/data/.google.index, /storage/emulated/0/Android/data/.google.index, or /storage/emulated/1/Android/data/.google.index.

The file exfiltration is considered complete when the server sends "Success" anywhere in its response. This exfiltration uses a Hypertext Transfer Protocol (HTTP) POST, and this server response is also expected to be HTTP, but this is not explicitly checked for. The 16 raw bytes of the MD5 are appended to the end of the .google.index file, ensuring that the same file isn't sent multiple times. As the .google.index file contains raw bytes, without prior knowledge, it would appear to contain random data. The initial allocation size is 256 Kb filled with NULLs providing space for up to a maximum of 16,384 file hashes. All hash entries will be checked for every file prior to exfiltration. When the end of the .google.index file is reached, the position is reset to the start, overwriting the previous hashes. This means if the number of files to exfiltrate from the device exceeds 16,384, files will be sent multiple times

The netd component of Infamous Chisel enters a main loop upon execution, where various timers trigger the execution of different tasks, including file and device information exfiltration. This process occurs every 86,000 seconds (approximately 23 hours, 53 minutes, and 20 seconds), during which the malware searches specified directories for files matching a list of extensions and collects various hardware configuration information about the device. The collected information is written to files in the /data/local directory and then exfiltrated.

F. Impact & Geo scope

The impact of Infamous Chisel on Android devices is significant. It leads to loss of sensitive information, privacy breaches, and potential misuse of the device for further malicious activities.

The Infamous Chisel campaign primarily targeted Android devices used by the military sector. The malware, associated with the Sandworm activity, was designed to enable remote access and exfiltrate information from these devices. The campaign was identified and reported by multiple organizations including the UK National Cyber Security Centre (NCSC), the US National Security Agency (NSA), US Cybersecurity and Infrastructure Security Agency (CISA), US Federal Bureau of Investigation (FBI), New Zealand's National Cyber Security Centre (NCSC-NZ), the Canadian Centre for Cyber Security, and Australian Signals Directorate (ASD).

G. Infecting ways

Based on the capabilities and methods of operation described in the document, we can infer some potential infection vectors that such a sophisticated malware campaign use:

- **Phishing Attacks**: Attackers may use phishing techniques to trick users into installing malicious applications or clicking on links that lead to the download of the malware.
- **Exploiting Vulnerabilities**: The malware may exploit known vulnerabilities in the Android operating system or in installed applications to gain unauthorized access and install itself.
- **Social Engineering**: Social engineering tactics could be used to convince users to grant permissions or disable security features that would otherwise prevent the malware from executing or gaining persistence.
- **Third-Party App Stores**: Infamous Chisel could be distributed through third-party app stores or websites offering infected applications that appear legitimate.
- **Malvertising**: Malicious advertisements could redirect users to websites that automatically download and install the malware on their devices.
- **Spear Phishing**: Targeted spear-phishing campaigns could be used to infect devices of specific individuals or organizations with the malware.
- **Supply Chain Attack**: Compromising software supply chains to inject malicious code into legitimate applications could be another method, although this is a more sophisticated and less common approach.

H. Proactive and Reactive measures

The approach to defending against such sophisticated malware campaigns typically involves a combination of proactive and reactive cybersecurity practices. It is important for organizations to adopt a layered security approach that includes both preventive and detective controls to protect against sophisticated malware campaigns. Additionally, staying informed about the latest cyber threats and collaborating with cybersecurity agencies and industry partners can enhance an organization's ability to defend against such threats

Proactive measures include:

- **Cybersecurity Awareness and Training**: Educating employees about the risks of malware and the

importance of following security best practices, such as not clicking on suspicious links or downloading unverified attachments.

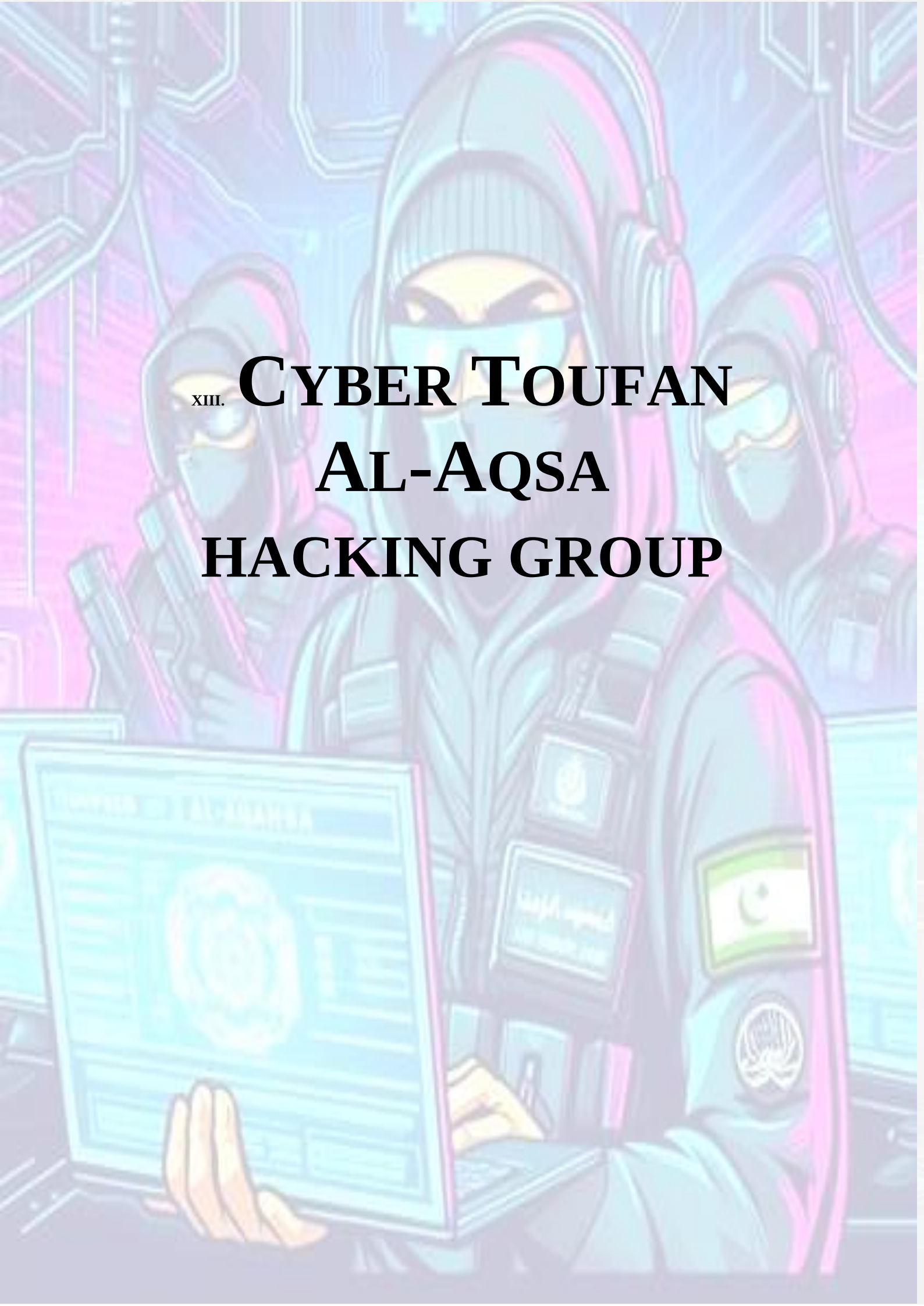
- **Regular Software Updates**: Ensuring that all software, including operating systems and applications, are kept up-to-date with the latest security patches to mitigate known vulnerabilities.
- **Robust Anti-Virus and Anti-Malware Solutions**: Deploying comprehensive anti-virus and anti-malware solutions that can detect and prevent the execution of malicious code on organizational devices.
- **Network Security**: Implementing network security measures such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to monitor and control incoming and outgoing network traffic based on an applied rule set.
- **Access Controls**: Enforcing strict access controls and using the principle of least privilege to ensure that users have only the access necessary to perform their job functions.
- **Incident Response Planning**: Developing and maintaining an incident response plan to quickly and effectively respond to potential security incidents.

Reactive measures include:

- **Threat Intelligence Sharing**: Participating in threat intelligence sharing with other organizations and cybersecurity agencies to stay informed about the latest threats and mitigation strategies.
- **Monitoring and Detection**: Continuously monitoring systems for signs of compromise and having detection mechanisms in place to alert on suspicious activities.
- **Forensic Analysis**: Conducting forensic analysis in the event of a security breach to understand the scope of the compromise, eradicate the threat, and recover affected systems.
- **Regular Security Audits**: Performing regular security audits and vulnerability assessments to identify and address security gaps in the organization's infrastructure.
- **Backup and Recovery**: Maintaining regular backups of critical data and having a disaster recovery plan to restore operations in the event of a malware attack.

Android Device measures:

- **Keep Software Updated**: Regularly update the Android operating system and all installed applications to ensure that known vulnerabilities are patched. Malware often exploits security flaws in outdated software.
- **Install Security Software**: Use reputable antivirus and anti-malware solutions designed for Android devices. These can help detect and remove malicious software.
- **Avoid Unknown Sources**: Disable the installation of apps from unknown sources in the device settings. Only download apps from trusted sources like the Google Play Store.
- **Be Cautious with Links and Attachments**: Do not click on links or download attachments from unknown or suspicious sources. Phishing is a common method used to distribute malware.
- **Use a VPN**: When connecting to public Wi-Fi networks, use a Virtual Private Network (VPN) to encrypt your internet connection and protect against network sniffing.
- **Enable Two-Factor Authentication (2FA)**: Use 2FA for online accounts to add an extra layer of security, making it harder for attackers to gain access even if they manage to steal credentials.
- **Monitor Network Traffic**: For organizations, monitoring network traffic for unusual activity can help detect the presence of malware like Infamous Chisel. Implement network segmentation to limit the spread of malware.
- **Educate Users**: Raise awareness among users about the risks of malware and the importance of following best security practices.
- **Backup Important Data**: Regularly backup important data stored on the device. In case of a malware infection, having backups can prevent data loss.
- **Use Device Encryption**: Enable device encryption to protect the data on your device. This makes it more difficult for attackers to access your information if the device is compromised.
- **Restrict App Permissions**: Review and restrict the permissions granted to applications. Limiting permissions can reduce the amount of data an app can access, thereby limiting what can be exfiltrated by malware.



XIII. CYBER TOUFAN AL-AQSA HACKING GROUP

Abstract – This document presents an analysis of the Cyber Toufan Al-Aqsa hacking group, a newly emerged cyber threat that has rapidly gained notoriety for its sophisticated cyberattacks primarily targeting Israeli organizations.

The analysis delves into various aspects of the group's operations, including its background and emergence, modus operandi, notable attacks and breaches, alleged state sponsorship, and the implications of its activities for cybersecurity professionals and other specialists across different industries. It also aims to highlight its significant impact on cybersecurity practices and the broader geopolitical landscape.

The analysis serves as a valuable resource for cybersecurity professionals, IT specialists, and industry leaders, offering insights into the challenges and opportunities presented by the evolving cyber threat landscape.

A. Introduction

The Cyber Toufan Al-Aqsa is a hacking group that emerged in late 2023, claiming responsibility for a series of cyberattacks against Israeli companies and organizations.

The group has been involved in various types of cyberattacks, including website defacement, unauthorized access to institutions, businesses, and private residences, compromise of security cameras, and data breaches. One of the attacks was against Signature-IT, an Israeli company that specializes in hosting international websites for businesses, and it was stolen approximately 16 gigabytes of data files.

The group has also targeted other significant entities such as Radware, a cybersecurity firm, the Israel Innovation Authority, and Ikea in Israel. The group's activities have not been limited to data breaches; they have also used the corporate email domains of their victims to spread hacktivist messages.

The identity of the attackers behind the Cyber Toufan Al-Aqsa remains unconfirmed. However, some suggest a potential link to Iran due to the style and capabilities demonstrated in the attacks, which are common to Iranian-backed cyber groups.

As of late December 2023, the group declared a "ceasefire," stopping the release of data leaks. However, the group is still causing damage to its victims and those connected to them.

B. Impact of attacks

The group has demonstrated high capabilities and a direct style common to Iranian-backed cyber operations. They have targeted a range of high-profile Israeli entities, causing significant data breaches. Notable attacks include the one on Signature-IT, where data files totaling approximately 16 gigabytes were stolen. This attack led to the daily disclosure of new victims.

The operation compromised more than 150 targets spread across government, manufacturing, e-commerce, cybersecurity, and other sectors. The group claimed to have destroyed over 1,000 servers and breached 150 Israeli targets. The attacks have not crippled the Israeli economy, but they have caused a lot of damage, and some companies are still paying the price.

The group also engaged in psychological warfare against Israel by justifying their cyberattacks as retaliation for what they perceive as Israeli cruelty and crimes. They declared a ceasefire in November 2023, but expressed their intent to resume operations after the ceasefire, with a focus on targeting major Israeli corporations.

C. Impact of attacks on israeli infrastructure

The potential impact of attacks on Israeli infrastructure is multifaceted and significant. The ongoing conflict between Israel and various entities, including Hamas and Iran-affiliated groups, has led to an increase in cyberattacks targeting Israeli infrastructure, businesses, and government entities.

These attacks have targeted a wide range of sectors, including government, e-commerce, water, energy, shipping, distribution, and telecommunications. The attacks have involved various methods, such as Distributed Denial of Service (DDoS) attacks, defacement attacks, data breaches, and the exploitation of default credentials in critical systems.

The cyberattacks have also had a significant impact on the Israeli cybersecurity sector. The conflict has absorbed manpower and focus from the cybersecurity sector, affecting the operation of companies and potentially leading to a temporary setback in cybersecurity innovation.

However, despite the increase in cyberattacks, Israel seems confident in its ability to deal with these threats. The country has a robust cybersecurity infrastructure and a rich startup ecosystem that has produced many globally recognized cybersecurity companies

D. Takeaways of attack Tactics

The Cyber Toufan Al-Aqsa group has employed a variety of tactics to carry out their cyberattacks. Here are some key methodologies they have used:

- **Website Defacement**: this involves altering the appearance of a website, often to display a political message or to demonstrate that the site has been compromised
- **Unauthorized Access**: involves unauthorized access to various institutions, businesses, and private residences. This could involve exploiting vulnerabilities in software, using phishing techniques to steal login credentials, or other methods of bypassing security measures
- **Compromise of Security Cameras**: this involves compromising security cameras, potentially allowing to monitor the activities of their targets
- **Data Breaches**: the group has been adept at extracting large volumes of data from their targets, which they then release publicly. This not only harms the targeted organizations but also potentially impacts individuals whose personal information may be included in the breached data
- **Use of Social Media Platforms**: the group has been observed to be active on social media platforms like Twitter and Telegram, where they disseminate information about their activities and potentially coordinate attacks
- **Wiper Malware**: The group has used wiper malware in their attacks, which is designed to delete data or disrupt systems
- **Psychological Warfare**: In addition to their technical tactics, Cyber Toufan has also engaged in psychological warfare. They have released publications justifying their cyberattacks on Israel, citing retaliation for what they perceive as Israeli cruelty and crimes
- **Follow-on Attacks**: After initial breaches, the group has been known to conduct follow-on attacks, potentially exploiting the compromised systems to further infiltrate the target's network or to attack other linked systems

E. Targets and Consequences

The targets of Cyber Toufan's attacks have been quite diverse, including:

- **Government Entities**: The group has compromised targets spread across the Israeli government sector
- **Manufacturing**: Manufacturing firms have been among the affected sectors
- **E-commerce**: Online commerce platforms and businesses have been targeted, which could include customer data and business transaction information
- **Cybersecurity Firms**: Notably, the group has attacked cybersecurity companies, such as Radware, which indicates a focus on entities that are integral to Israel's cyber defense

1)Government Entities

The consequences of attacks on government entities:

- **Data Breaches**: The group has successfully breached several government entities, leading to substantial data leaks. This not only compromises the security and privacy of the affected organizations but also potentially impacts individuals whose personal information may be included in the breached data
- **Disruption of Services**: The attacks have led to the disruption of services, affecting the normal functioning of the targeted government entities
- **Damage to Reputation**: The public nature of these attacks and the subsequent data leaks can damage the reputation of the targeted entities, eroding public trust and confidence
- **Potential for Follow-on Attacks**: The initial breaches can potentially be used to conduct follow-on attacks, exploiting the compromised systems to further infiltrate the target's network or to attack other linked systems
- **Psychological Impact**: The attacks serve as a form of digital psychological warfare, creating a climate of fear and uncertainty
- **Economic Impact**: The attacks can have economic consequences, including the costs associated with incident response, system recovery, and potential regulatory fines or lawsuits related to the data breaches
- **National Security Concerns**: Given the sensitive nature of government entities, attacks can potentially pose national security concerns, depending on the nature of the breached data and the affected systems

2)Manufacturing

The consequences of attacks on the manufacturing sector:

- **Operational Disruption**: Cyberattacks, particularly ransomware, can halt production lines, leading to significant operational disruptions. This can force manufacturers to take their physical systems offline, sometimes for extended periods, to mitigate the attack and restore normal operations
- **Financial Losses**: The financial impact of cyberattacks on manufacturers is substantial. The average cost of a data breach in the manufacturing sector was reported to be $4.47 million in 2022, an increase from the previous year. These costs include investigating, remediating, and responding to cyberattacks, as well as potential losses from halted production and sales
- **Data Breaches and Intellectual Property Theft**: Cyberattacks can lead to the theft of sensitive data, including intellectual property, trade secrets, and customer information. This not only has immediate financial implications but can also result in long-term competitive disadvantages
- **Supply Chain Vulnerabilities**: The interconnected nature of the manufacturing supply chain means that an attack on one manufacturer can have ripple effects, impacting suppliers, partners, and customers. Supply chain attacks can compromise the integrity of products and services, leading to broader security concerns
- **Reputational Damage**: Public disclosure of a attack can erode trust in a manufacturer, affecting customer relationships and potentially leading to loss of business.

The damage to a company's reputation can be one of the most challenging consequences to recover from

- **Compliance and Legal Risks**: Manufacturers may face regulatory fines and legal action if cyberattacks result in the loss of protected or sensitive data. This is especially true for manufacturers in highly regulated industries or those handling personal data
- **Physical Damage and Safety Risks**: In cases where operational technology (OT) systems are targeted, cyberattacks can cause physical damage to equipment and pose safety risks to employees. Manipulating industrial processes can lead to equipment failure, environmental harm, and even endanger human lives
- **Psychological Warfare**: Beyond the tangible impacts, cyberattacks can also serve as a form of psychological warfare, creating a climate of fear and uncertainty among employees, management, and stakeholders

3)E-commerce

The consequences of attacks on the e-commerce sector:

- **Operational Disruption**: Cyberattacks can severely disrupt the operations of e-commerce businesses, affecting their ability to process transactions and serve customers. This disruption can lead to downtime, which directly impacts sales and service delivery
- **Financial Losses**: The financial impact of cyberattacks on e-commerce businesses can be substantial. This includes direct costs related to investigating, remediating, and responding to the attacks, as well as indirect costs such as lost sales during downtime. The average cost of a data breach in 2022 reached $4.35 million, highlighting the significant financial burden these incidents can impose
- **Data Breaches and Loss of Sensitive Information**: E-commerce platforms often store large amounts of personal and financial data. Cyberattacks can lead to data breaches, exposing sensitive customer information such as credit card details, addresses, and personal identification information. This not only violates customer privacy but also exposes the business to regulatory penalties and lawsuits
- **Damage to Reputation and Customer Trust**: The public disclosure of a cyberattack can significantly damage an e-commerce business's reputation, leading to a loss of customer trust. Rebuilding this trust can be a long and challenging process, and some businesses may never fully recover
- **Regulatory and Compliance Risks**: E-commerce businesses are subject to various regulations and compliance standards related to data protection and privacy. Cyberattacks that result in data breaches can lead to non-compliance, attracting significant fines and penalties
- **Increased Cybersecurity Costs**: Following a cyberattack, e-commerce businesses often need to invest heavily in improving their cybersecurity posture. This includes adopting new technologies, hiring additional security personnel, and implementing more stringent security measures. These increased costs can impact the business's bottom line and may be passed on to consumers in the form of higher prices
- **Supply Chain Vulnerabilities**: E-commerce businesses are part of a larger digital and physical supply chain. Attacks on one e-comm platform can have ripple effects, impacting suppliers, partners, and customers. This interconnectedness can amplify the consequences of an attack, affecting a broader ecosystem

4)Cybersecurity Firms

The consequences of attacks on cybersecurity firms:

- **Operational Disruption**: Cybersecurity firms, like any other business, can face operational disruptions as a result of cyberattacks. This can affect their ability to serve clients and carry out daily operations, potentially leading to a temporary reduction in the security services they provide
- **Financial Losses**: The financial impact on cybersecurity firms can be substantial, encompassing the costs of investigating, remediating, and responding to the attacks. Additionally, there may be financial losses due to operational downtime and potential compensation claims from affected clients
- **Data Breaches and Intellectual Property Theft**: Cybersecurity firms often hold sensitive data, including proprietary security tools and techniques, as well as client information. A breach can lead to the loss of intellectual property and sensitive client data, undermining the firm's competitive position and client trust
- **Damage to Reputation**: Perhaps more so than in other industries, a cyberattack on a cybersecurity firm can significantly damage its reputation. Clients expect these firms to be the most secure, and a breach can lead to a loss of trust, making it difficult to retain and attract clients
- **Regulatory and Compliance Risks**: Cybersecurity firms are subject to stringent regulatory requirements. A cyberattack resulting in data breaches can lead to non-compliance issues, attracting fines, and legal action
- **Increased Cybersecurity Costs**: Following an attack, a cybersecurity firm will likely need to invest heavily in bolstering its defenses. This could include adopting new technologies, hiring additional personnel, and implementing more stringent security measures, all of which can be costly
- **Supply Chain Vulnerabilities**: Cybersecurity firms are part of a larger digital ecosystem. An attack on one firm can have ripple effects, potentially compromising the security of clients and partners
- **Psychological Impact and Loss of Morale**: Cyberattacks can create a climate of fear and uncertainty among employees and management. For a cybersecurity firm, being the victim of an attack can also lead to a loss of morale, as it directly challenges the core mission of the organization

XIV. MALLOX

Abstract – This document provides a analysis of the Target Company ransomware group, also known as Smallpox, which has been rapidly evolving since its first identification in June 2021.

The analysis delves into various aspects of the group's operations, including its distinctive practice of appending targeted organizations' names to encrypted files, the evolution of its encryption algorithms, and its tactics for establishing persistence and evading defenses.

The insights gained from this analysis are crucial for informing defense strategies and enhancing preparedness against such evolving cyber threats.

A. Malware and Evasion Tactics

The TargetCompany ransomware group, aka Mallox, is known for its targeted ransomware attacks, primarily focusing on unsecured internet-facing Microsoft SQL servers. The ransomware encrypts victims' data and demands a ransom, typically in cryptocurrency, for the decryption key

The group has added tools like the Remcos RAT, BatCloak, and Metasploit to their arsenal, showcasing advanced obfuscation methods to avoid detection. They use fully undetectable (FUD) obfuscator packers to scramble their ransomware, making it harder for security software to detect and block the malware. They collect sensitive data using tools like MIMIKATZ, and executing attacks with Trojan.BAT.TARGETCOMP*. They also employ defense evasion methods such as GMER, advanced Process Termination, and YDArk

B. Mitigation and Decryption

Mallox ransomware appends a unique encrypted file extension to the names of the targeted organization's files. It has been observed to avoid encrypting certain folders and file types to keep the infected system operational. The ransomware drops a note in every directory on the victim's drive, providing instructions for payment

Avast has released free decryptors for TargetCompany ransomware, which can decrypt files under certain circumstances. It is important to note that paying the ransom does not guarantee that the attackers will provide the decryption key, and it may encourage further criminal activity

C. Ransomware-as-a-Service (RaaS)

Mallox operates under a RaaS model, leveraging underground forums to advertise its services. The group maintains a TOR-based leak site where it posts announcements about recently compromised data

1)Mallox Spreading

TargetCompany ransomware, also known as Mallox ransomware, spreads through various methods. The ransomware primarily targets companies rather than individual users.

One of the initial access techniques used by TargetCompany is phishing, where it uses malicious Microsoft OneNote files to gain access to the victim's system. Another method is through brute-force attacks on Microsoft SQL (MS SQL) Servers. The ransomware group is known for exploiting inadequately secured MS-SQL servers, using dictionary attacks as an entry point to infiltrate victims' networks.

Once inside the system, the ransomware employs a PowerShell command to fetch the ransomware payload from a remote server. The payload attempts to halt and eliminate SQL-related services, erase volume shadow copies, clear system event logs, and end security-related processes. After these steps, it initiates the encryption process and subsequently leaves a ransom note in each directory.

The ransomware also collects system information and transfers it to the command-and-control (C2) server. The stolen data is then held hostage, with threats of publication on leak sites to coax victims into paying the ransom.

The ransomware encrypts the victim's files using the ChaCha20 encryption algorithm and generates the encryption key using ECDH, an example of elliptic curve cryptography, and AES-128. The encrypted files are appended with extensions that are the affected company's name.

2)Symptoms of a TargetCompany Ransomware Attack

The symptoms of a TargetCompany ransomware attack can vary depending on the specific variant of the ransomware and the tactics. However, some common symptoms include:

- **Inability to access files**: The most immediate and noticeable symptom of a ransomware attack is the inability to open or access files stored on your computer. The files are encrypted by the ransomware, and their extensions are changed to the affected company's name, such as ".artiis", ".brg", ".mallox", ".architek", ".tohnichi", ".herrco", and others
- **Increased CPU and disk activity**: Increased disk or main processor activity may indicate that ransomware is working in the background

- **Ransom note**: After the encryption process, the ransomware leaves a ransom note titled "How to decrypt files.txt" or “RECOVERY FILES.txt” in each directory. This note typically contains instructions for how to pay the ransom in order to receive the decryption key
- **Network anomalies**: The ransomware uses network scanning to collect network connection information, which can lead to unusual network activity
- **Termination of specific processes and services**: The ransomware attempts to halt and eliminate SQL-related services, erase volume shadow copies, clear system event logs, and end security-related processes

3)Methodology

- **Initial Access**: The group often gains initial access to victim systems through phishing campaigns that involve malicious OneNote files. They also exploit weak SQL servers for initial stage deployment
- **Execution**: The ransomware payload is executed using various methods. For instance, the group injects the ransomware executable into AppLaunch.exe. They also use command lines and PowerShell to download the ransomware payload from a remote server
- **Persistence**: The group aims for persistence via diverse methods, including altering URLs or paths until the execution of the Remcos RAT (Remote Access Trojan) succeeds
- **Defense Evasion**: The group uses Fully Undetectable (FUD) obfuscator packers to evade detection by security solutions. They also delete registry keys and shadow copies to damage recovery services
- **Privilege Escalation**: The ransomware assigns the SeTakeOwnershipPrivilege and SeDebugPrivilege for its process to ease its own malicious work
- **Discovery**: group uses network scanning for discovery
- **Collection**: The group uses tools like MIMIKATZ for data collection
- **Command and Control (C&C)**: The group establishes a connection to a C&C server with a “/ap.php” endpoint
- **Encryption**: The ransomware gets the mask of all logical drives in the system using the GetLogicalDrives() Win32 API. Each drive is checked for the drive type by GetDriveType(). If that drive is valid (fixed, removable, or network), the encryption of the drive proceeds
- **Impact**: After encryption, the ransomware leaves a ransom note. The group uses the double extortion method, threatening to leak stolen data if the ransom is not paid

4)Entry points & Delivery methods

Ransomware attacks can infiltrate a system through various entry points:

- **Compromised Credentials**: Attackers often gain access to a network by using stolen or compromised credentials. This can occur when employees fall victim to phishing attacks or when credentials are purchased on the dark web
- **Unmanaged Devices or Bring Your Own Device (BYOD)**: Unmanaged devices or personal devices used for work purposes can be an entry point for ransomware if they are not properly secured
- **Internet-facing Applications with Vulnerabilities**: Vulnerabilities in applications that are exposed to the internet can be exploited by attackers to gain access to a network. This includes applications like SSL VPNs, Microsoft Exchange Servers, and Telerik UI-based web interfaces
- **Phishing**: Phishing attacks often target end users, tricking them into revealing sensitive information or downloading malicious software. Employees play a vital role in defending against this threat, making it imperative for organizations to invest in educating their workforce on recognizing and avoiding phishing attempts
- **Infected Software Packages or Patches**: Compromised patches or software packages can become entry points for ransomware criminals. This tactic capitalizes on the fact that users often quickly download and install updates to keep their systems secure, inadvertently allowing ransomware to infiltrate
- **Brute Force Attacks on External Gateways**: Cybercriminals are increasingly using techniques like brute force attacks to gain access to systems. This involves systematically attempting all possible combinations of passwords until the correct one is found
- **Remote Desktop Protocol (RDP) and Credential Abuse**: Attackers often exploit vulnerabilities in remote services like RDP or VPN servers. They may resort to phishing activities to get hold of the credentials or employ the credential dumps available on dark web forums
- **Email**: Email is a common entry point for ransomware attacks. Attackers often attach malicious files to emails. When unsuspecting victims open these documents, macros will execute, running the ransomware payload

The Mallox uses various entry points to infiltrate systems:

- **Remcos Backdoor**: The group uses the Remcos backdoor as an initial access point. Remcos is a Remote Access Trojan (RAT) that allows attackers to control the infected system remotely
- **Unsecured Microsoft SQL Servers**: The group targets unsecured Microsoft SQL Servers, using them as entry points into victims' ICT infrastructures
- **BatLoader**: The group leverages BatLoader to execute ransomware payloads. BatLoader is a malicious

software that downloads and installs additional malware onto the infected system

- **Network Scan**: The group uses network scanning as a discovery method to identify potential targets within the network
- **Trojan.BAT.TARGETCOMP**: This is a malicious program used by the group for execution. It is designed to compromise the security of the infected system
- **GMER**: The group uses GMER, a rootkit detector and remover, for defense evasion. This allows the group to hide their activities and maintain persistence on the infected system

a) Entry points in industries

Manufacturing

- **Industrial Control Systems (ICS) and Industrial Internet of Things (IIoT) Devices**: Vulnerabilities in these systems are exploited to disrupt manufacturing operations
- **Supply Chain Attacks**: Compromising the supply chain, including third-party vendors, can provide an entry point for ransomware

Retail

- **Point of Sale (POS) Systems**: Malware can infect these systems to steal credit/debit card information
- **Microsoft SQL Servers**: Targeting unsecured MS-SQL servers used in retail operations

Telecommunications

- **Remote Code Execution (RCE) Vulnerabilities**: Exploiting vulnerabilities like CVE-2019-1069 and CVE-2020-0618 to execute arbitrary code
- Microsoft SQL Servers: Leveraging the xp_cmdshell feature in Microsoft SQL for remote execution

Business Services

- **Outdated and Unpatched Systems**: Relying on outdated systems makes it easier for criminals to gain access
- **Functional IT Dependency**: The inability to operate without IT incentivizes quick ransom payments

Healthcare

- **Phishing and Social Engineering**: Using deceptive emails to trick healthcare staff into installing ransomware
- **Compromised Credentials**: Utilizing stolen credentials to access healthcare networks

Finance

- **Server Access Attacks and Misconfigurations**: Exploiting server vulnerabilities and configuration errors
- **Phishing and Credential Theft**: Targeting high-value accounts like those of CEOs and CFOs

Government

- **Phishing and Social Engineering**: Using deceptive emails to trick government employees
- **Ransomware-as-a-Service (RaaS)**: Utilizing RaaS models to target government entities

Education

- **Phishing and Social Engineering**: Using deceptive emails to trick educational staff and students
- **Compromised Credentials**: Utilizing stolen credentials to access educational networks

Information Technology

- **Software Vulnerability Exploits**: Exploiting known vulnerabilities in IT infrastructure
- **Account Takeover**: Gaining access to IT systems through compromised accounts

Transportation

- **Phishing and Social Engineering**: Targeting employees with phishing emails to gain access to the network
- **Compromised Credentials**: Utilizing stolen credentials to access transportation networks

Utilities

- **Industrial Control Systems (ICS)**: Targeting vulnerabilities in ICS that are crucial for utility operations
- **Phishing and Social Engineering**: Using deceptive emails to trick utility staff into installing ransomware

D. Geographic Focus and Industry Targets

Mallox, has targeted a range of company sizes, with a significant focus on small to medium-sized businesses. 37% of companies hit by ransomware had fewer than 100 employees, and 82% of ransomware attacks in 2021 were against companies with fewer than 1,000 employees. While the proportion of large organizations was higher in H1 2022, the proportion of small and midsize organizations was higher in H1 2023, indicating a trend toward more small and midsize business targets. However, ransomware groups, including TargetCompany, are targeting large enterprises at a rate of nearly 25%. The median target company size of a ransomware attack was 275 employees, up 10% from the previous quarter

The group has primarily targeted enterprises in the Asia-Pacific region, followed by Europe and the Middle East (United States, India, Saudi Arabia, Canada, Germany, Australia, Brazil, Bulgaria, China, Vietnam). They have launched attacks on organizations in various sectors, including retail, wholesale, and legal services (Manufacturing, Retail, Telecommunications, Automobile, Business Services, Healthcare, Finance,

Government, Education, Information Technology, Transportation, Utilities).

1)Manufacturing

In the manufacturing industry, ransomware attacks often exploit vulnerabilities in Industrial Control Systems (ICS) and Industrial Internet of Things (IIoT) devices. These systems are integral to manufacturing operations, and their compromise can lead to significant disruption.

These attacks extend beyond immediate financial losses, leading to significant breach response costs, possible exposure to third parties, diminution of market share, and damage to corporate reputation. In some cases, attackers may also demand a ransom in exchange for allowing the business to regain access to its computer systems. Moreover, ransomware attacks can lead to the loss of sensitive and personal information, which can have long-term implications for the affected companies and their customers

Operational Disruption

Ransomware attacks disrupt manufacturing operations significantly, often leading to substantial losses in production and disjointed operations. When ransomware disrupts production, operations can be halted for days or weeks, resulting in staggering financial losses. In some cases, ransomware attacks have led to production lines being brought to a standstill, meaning that customer orders cannot be fulfilled.

Financial Impact

The financial impact of ransomware attacks on the manufacturing sector is enormous. Between 2018 and 2023, 478 manufacturing companies suffered a ransomware attack, leading to a loss of approximately $46.2 billion in downtime alone. The cost of downtime is significant, with day-to-day operations impacted and production lines sometimes brought to a standstill.

Reputational Damage

Ransomware attacks can also cause significant reputational damage. The fallout from a ransomware attack can be long-lasting and can sometimes lead to a business never recovering from the reputational fallout.

Data Breach and Privacy Concerns

Data breaches are a common consequence of ransomware attacks. In 32% of attacks, attackers stole the data in addition to encrypting it. More than 7.5 million individual records were breached as a result of these attacks.

Legal and Regulatory Consequences

Legal and regulatory consequences can arise from ransomware attacks, particularly when they result in data breaches. Companies may face penalties for failing to adequately protect customer data, and they may also face lawsuits from customers or business partners affected by the breach.

Long-Term Effects

The long-term effects of ransomware attacks can include unplanned workforce reductions and even closure of the business altogether. In some cases, ransomware attacks have led to companies asking to be put in receivership, threatening jobs.

Increased Frequency of Attacks

In 2023, the manufacturing sector was the hardest hit, signaling significant vulnerabilities in this sector. The number of attacks against manufacturing plants also jumped about 107% compared with the previous year

2)Retail

In the retail industry, one of the common entry points for ransomware attacks is through Point of Sale (POS) systems. Attackers often use malware to infect these systems and steal credit/debit card information. Additionally, ransomware groups have been observed targeting and attacking Microsoft SQL (MS-SQL) servers, which are often used in retail operations

Ransomware attacks can cripple a retail business, leading to direct financial losses, operational halts, long-term reputational damage, and legal consequences. The retail sector's reliance on digital systems and the handling of sensitive customer data make it a lucrative target for cybercriminals.

Operational Disruption

- **Sales Loss**: A ransomware attack can lead to thousands of lost sales opportunities, especially during peak seasons like Black Friday or Christmas
- **Business Continuity**: ransomware attacks can disrupt critical business operations, preventing or limiting access to systems and prevent goods selling
- **Downtime**: Even a few hours of web shop downtime can have a huge financial impact, and customers may turn to other platforms to get their products

Financial Impact

- **Revenue Loss**: Retail organizations report significant loss of revenue following ransomware attacks
- **Ransom Payments**: Retailers may feel compelled to pay ransoms, especially during high sales periods, and the proportion of retail organizations paying higher ransoms has increased
- **Recovery Costs**: Victim retailers that pay ransoms end up with median recovery costs four times higher than those that don't

Reputational Damage

- **Customer Trust**: Ransomware attacks can shatter customer trust if personal information is compromised
- **Brand Damage**: The perception of an "unsafe" business can be more damaging than the immediate financial loss, affecting the retailer's reputation
- **Public Perception**: Successful attacks may be seen as an indication of weak security practices, leading customers to conduct business elsewhere

Data Breach

- **Sensitive Information**: Retailers process credit card data and personal information, which is at risk of being exposed as a result of a ransomware attack
- **Data Leakages**: Ransomware attacks pose significant risks of data leakages, which can lead to loss of consumer confidence

Employee Impact

- **Layoffs**: Nearly half of Retailers experienced employee layoffs after falling victim to ransomware
- **Suspension of Business**: A third of Retailers had to temporarily suspend or halt their business operations

Supply Chain and Third-Party Risks

- **Supply Chain Attacks**: Attackers can infect many organizations by targeting vendors, leading to supply chain disruptions
- **Third-Party Dependencies**: Retailers rely on extended supply chains and third-party dependencies, which can introduce cybersecurity risks

Legal and Regulatory Consequences

Retailers may face legal consequences if customer data is compromised, including fines and penalties for non-compliance with data protection regulations.

3)Telecommunications

In the telecommunications industry, ransomware attacks often exploit remote code execution (RCE) vulnerabilities, such as CVE-2019-1069 and CVE-2020-0618, which allow attackers to execute arbitrary code. The attackers may also leverage remote execution via the xp_cmdshell feature in Microsoft SQL

Ransomware attacks can cripple a telecom business, leading to direct financial losses, operational halts, long-term reputational damage, and legal consequences.

Operational Disruption

- **Service Interruption**: Ransomware attacks can disrupt telecommunications services, affecting both individual and business communications
- **Network Infiltration**: The interconnected nature of telecom networks increases the risk of infiltration, potentially providing access to information across various connected systems

Financial Impact

- **Revenue Loss**: A ransomware attack can severely affect the operating capability of an organization, leading to a decline in revenue or a complete halt of operations while recovering
- **Ransom Payments and Recovery Costs**: Companies may face significant costs related to ransom payments, recovery efforts, legal fees, and other related expenses

Reputational Damage

- **Customer Trust**: A successful attack can damage the reputation of a telecom company, leading customers to conduct business elsewhere due to perceived weak security practices
- **Brand Damage**: The perception of an "unsafe" business can be more damaging than the immediate financial loss

Data Breach and Privacy Concerns

- **Sensitive Data Exposure**: Telecom companies house extensive customer data, and ransomware attacks can lead to breaches of sensitive data
- **Double Extortion**: Attackers may threaten to release the organization's sensitive data if the ransom is not paid, leading to double-extortion attacks

Legal and Regulatory Consequences

Companies may face legal consequences if customer data is compromised, including fines and penalties for non-compliance with data protection regulations

Supply Chain and Third-Party Risks

- **Supply Chain Attacks**: Attackers can infect many organizations by targeting vendors, leading to supply chain disruptions
- **Third-Party Dependencies**: Telecom companies rely on extended supply chains and third-party dependencies, which can introduce cybersecurity risks

Intellectual Property Theft

The valuable intellectual property of telecom companies is at risk of being stolen or compromised, potentially harming competitive advantages and innovative efforts

Long-Term Espionage

Some attacks on telecom providers are conducted by highly sophisticated threat groups aiming for long-term espionage

4)Automobile & Transportation

Ransomware attacks can cripple an business, leading to direct financial losses, operational halts, long-term reputational damage, and legal consequences. These sectors' reliance on digital systems and the handling of sensitive customer data make it a lucrative target for cybercriminals. It is essential for automotive companies to implement robust cybersecurity measures, maintain regular backups, and have an incident response plan to mitigate the risks associated with ransomware attacks

Operational Disruption

- **Production Halts**: Ransomware attacks can lead to the shutdown of manufacturing plants, causing delays in production and delivery
- **Supply Chain Vulnerability**: The supply chain is complex and interconnected, making it vulnerable to attacks that can have cascading effects

Financial Impact

- **Ransom Payments**: The automotive industry has seen some of the highest ransom payments, with industrial companies spending $6.9 million in 2019, which was 62% of all ransomware payoffs
- **Revenue Loss**: Attacks can severely affect the operating capability of organizations, leading to a decline in revenue or a complete halt of operations while recovering

Reputational Damage

- **Customer Trust**: Successful attacks can damage the reputation of automotive companies, leading customers to conduct business elsewhere due to perceived weak security practices
- **Brand Damage**: The perception of an "unsafe" business can be more damaging than the immediate financial loss

Data Breach and Privacy Concerns

- **Sensitive Data Exposure**: Automotive companies house extensive customer data, and ransomware attacks can lead to breaches of sensitive data
- **Double Extortion**: Attackers may threaten to release the organization's sensitive data if the ransom is not paid, leading to double-extortion attacks

Legal and Regulatory Consequences

Companies may face legal consequences if customer data is compromised, including fines and penalties for non-compliance with data protection regulations

Intellectual Property Theft

The valuable intellectual property of companies is at risk of being stolen or compromised, potentially harming competitive advantages and innovative efforts

Long-Term Espionage

Some attacks on automotive providers are conducted by highly sophisticated threat groups aiming for long-term espionage

5)Business Services

Ransomware attacks can cripple a business in the services industry, leading to direct financial losses, operational halts, long-term reputational damage, and legal consequences.

Operational Disruption

- **Downtime**: Ransomware attacks can bring operations to a halt, causing significant downtime and disrupting business activities
- **Loss of Business**: If critical files are encrypted, businesses may be unable to operate, leading to lost opportunities and revenue

Financial Impact

- **Ransom Payments**: Businesses may feel compelled to pay the ransom to quickly regain access to their data, especially if backups are not available or are also compromised
- **Recovery Costs**: Beyond the ransom payment, businesses face substantial costs in remediation efforts, including IT services, legal fees, and potential regulatory fines
- **Revenue Loss**: The inability to operate during and after an attack can lead to a significant decline in revenue

Reputational Damage

- **Customer Trust**: A ransomware attack can severely damage a company's reputation, leading customers to lose trust and potentially take their business elsewhere
- **Brand Damage**: The perception of inadequate security measures can tarnish a brand's image, affecting long-term business prospects

Data Breach and Privacy Concerns

- **Sensitive Data Exposure**: Business services firms often handle sensitive client data. A ransomware attack can lead to data breaches, exposing confidential information
- **Double Extortion**: Attackers may not only encrypt data but also threaten to release it publicly if the ransom is not paid, compounding the impact

Legal and Regulatory Consequences

If customer data is compromised, businesses may face legal consequences and fines for non-compliance with data protection regulations

Supply Chain and Third-Party Risks

Ransomware attacks can extend beyond the directly affected business, impacting clients, partners, and suppliers

Intellectual Property Theft

For firms that rely on proprietary methods or data, ransomware attacks pose a risk of intellectual property theft

Long-Term Espionage

Some attacks may be part of long-term espionage efforts, aiming to gather strategic information over time

6)Healthcare

Ransomware attacks can cripple healthcare organizations, leading to direct financial losses, operational halts, long-term reputational damage, and legal consequences.

Operational Disruption

- **Service Interruption**: Ransomware attacks can disrupt healthcare operations by encrypting or rendering medical records and systems inaccessible, leading to delays in patient care and potentially causing patient deaths
- **Increased Patient Mortality**: Research indicates that ransomware attacks increase in-hospital mortality for patients admitted during an attack, with a significant rise in the risk of dying

Financial Impact

- **Revenue Loss and Remediation Costs**: Healthcare organizations may face financial losses tied to revenue

loss, ransom payments, remediation costs, as well as brand damage and legal fees. The average cost of a healthcare ransomware attack was $4.82 million in 2021

- **Downtime-Related Losses**: Ransomware attacks on healthcare have resulted in downtime-related losses of more than $77 billion for the U.S. economy

Reputational Damage

Successful ransomware attacks can severely damage the reputation of healthcare providers, leading to a loss of patient trust and potentially driving patients to seek care elsewhere

Data Breach and Privacy Concerns

- **Sensitive Data Exposure**: Healthcare organizations house extensive patient data. Ransomware attacks can lead to breaches of sensitive data, including personal health information (PHI), exposing millions of patients to privacy risks
- **Double Extortion**: Attackers may threaten to release sensitive data if the ransom is not paid, compounding the impact of the attack

Legal and Regulatory Consequences

If patient data is compromised, healthcare organizations may face legal consequences and fines for non-compliance with data protection regulations

Supply Chain and Third-Party Risks

Ransomware attacks can extend beyond the directly affected healthcare provider, impacting clients, partners, and suppliers

Intellectual Property Theft

Ransomware attacks pose a risk of intellectual property theft, potentially harming competitive advantages and innovative efforts

Long-Term Espionage

Some attacks on healthcare providers are conducted by highly sophisticated threat groups aiming for long-term espionage

7)Finance

Ransomware attacks can cripple financial institutions, leading to direct financial losses, operational halts, long-term reputational damage, and legal consequences.

Operational Disruption

- **Service Interruption**: Ransomware attacks can disrupt financial operations by encrypting or rendering financial records and systems inaccessible, leading to delays in financial transactions and potentially causing significant operational disruptions
- **Network Infiltration**: The interconnected nature of financial networks increases the risk of infiltration, potentially providing access to information across various connected systems

Financial Impact

- **Revenue Loss and Remediation Costs**: Financial organizations may face financial losses tied to revenue loss, ransom payments, remediation costs, as well as brand damage and legal fees. The average cost of a financial ransomware attack was $5.9 million per cyber incident in 2023
- **Downtime-Related Losses**: Ransomware attacks on financial services have resulted in substantial financial losses, including the costs associated with the severity of the attack and the extent of the data exposure

Reputational Damage

- **Loss of Trust**: Successful ransomware attacks can severely damage the reputation of financial institutions, leading customers to lose trust and potentially take their business elsewhere
- **Brand Damage**: The perception of inadequate security measures can tarnish a brand's image, affecting long-term business prospects

Data Breach and Privacy Concerns

- **Sensitive Data Exposure**: Financial institutions house extensive customer data. Ransomware attacks can lead to breaches of sensitive data, exposing millions of customers to privacy risks
- **Double Extortion**: Attackers may threaten to release sensitive data if the ransom is not paid, compounding the impact of the attack

Legal and Regulatory Consequences

If customer data is compromised, financial institutions may face legal consequences and fines for non-compliance with data protection regulations

Supply Chain and Third-Party Risks

Ransomware attacks can extend beyond the directly affected financial institution, impacting clients, partners, and suppliers

Intellectual Property Theft

Ransomware attacks pose a risk of intellectual property theft, potentially harming competitive advantages and innovative efforts

Long-Term Espionage

Some attacks on financial institutions are conducted by highly sophisticated threat groups aiming for long-term espionage

8)Government

Ransomware attacks on government entities can cripple vital operations, lead to significant financial losses, damage public trust, and have long-lasting effects on the community.

Operational Disruption

- **Service Interruption**: Ransomware can shut down digital assets such as payment platforms or citizen portals, grinding municipal operations to a halt
- **Emergency Services**: Attacks that shut down 911 or 311 dispatch systems could put lives at risk

- **System Downtime**: Government employees may be left without their systems, resorting to manual processes

Financial Impact

- **Costs**: Between 2018 and December 2023, ransomware attacks on US government organizations cost an estimated $860.3 million
- **Ransom Payments**: Governments may be forced to pay ransoms or face the costly decision to rebuild systems

Reputational Damage

- **Public Trust**: A ransomware attack can damage the reputation of government entities, potentially resulting in the loss of public confidence
- **Perception of Security**: Successful attacks may be seen as an indication of weak security practices, leading the public to question the government's ability to protect sensitive information

Data Breach and Privacy Concerns

- **Sensitive Information**: Governments risk losing control of classified, confidential, and personal information, such as social security numbers or credit card information
- **Data Loss**: Ransomware can render data and systems unusable, leading to potential data loss if backups are not available or are compromised

Legal and Regulatory Consequences

Governments may face legal consequences and fines for non-compliance with data protection regulations if citizen data is compromised

Long-Term Effects

- **Learning and Monetary Loss**: Ransomware attacks on schools, for example, can cause learning loss as well as monetary loss
- **Psychosocial Impact**: There may be significant short- and long-term social and psychological effects on individuals affected by the attacks

Increased Frequency of Attacks

There has been a significant increase in ransomware attacks on government organizations, with a 313% rise in endpoint security services incidents reported

9)Education

Ransomware attacks can cripple educational institutions, leading to direct financial losses, operational halts, long-term reputational damage, and legal consequences. The education sector's reliance on digital systems and the handling of sensitive student and staff data make it a lucrative target for cybercriminals.

Operational Disruption

- **Service Interruption**: Ransomware can shut down digital assets such as payment platforms or citizen portals, grinding municipal operations to a halt
- **Emergency Services**: Attacks that shut down 911 or 311 dispatch systems could put lives at risk
- **System Downtime**: Government employees may be left without their systems, resorting to manual processes

Financial Impact

- **Costs**: Between 2018 and December 2023, ransomware attacks on US government organizations cost an estimated $860.3M; The average cost of an educational ransomware attack was $2.73M per cyber incident.
- **Ransom Payments**: Governments may be forced to pay ransoms or face the costly decision to rebuild systems

Reputational Damage

- **Public Trust**: A ransomware attack can damage the reputation of government entities, potentially resulting in the loss of public confidence
- **Perception of Security**: Successful attacks may be seen as an indication of weak security practices, leading the public to question the government's ability to protect sensitive information

Data Breach and Privacy Concerns

- **Sensitive Information**: Governments risk losing control of classified, confidential, and personal information, such as social security numbers or credit card information
- **Data Loss**: Ransomware can render data and systems unusable, leading to potential data loss if backups are not available or are compromised

Legal and Regulatory Consequences

Governments may face legal consequences and fines for non-compliance with data protection regulations if citizen data is compromised

Long-Term Effects

- **Learning and Monetary Loss**: Ransomware attacks on schools, can cause learning loss as well as monetary loss
- **Psychosocial Impact**: There may be significant short- and long-term social and psychological effects on individuals affected by the attacks

Increased Frequency of Attacks

There has been a significant increase in ransomware attacks on government organizations, with a 313% rise in endpoint security services incidents reported

10) Information Technology

Ransomware attacks can cripple IT businesses, leading to direct financial losses, operational halts, long-term reputational damage, and legal consequences.

Operational Disruption

- **Service Interruption**: Ransomware can disrupt IT operations by encrypting or rendering systems and data inaccessible, leading to delays in services and potentially causing significant operational disruptions

- **Network Infiltration**: The interconnected nature of IT networks increases the risk of infiltration, potentially providing access to information across various connected systems

Financial Impact

- **Revenue Loss**: Organizations may experience a decline in revenue or a complete halt of operations while recovering from a ransomware attack, even if they have functional backups
- **Ransom Payments and Recovery Costs**: Companies may face significant costs related to ransom payments, system recovery, legal fees, and other related expenses

Reputational Damage

- **Customer Trust**: A successful attack can damage the reputation of IT companies, leading customers to conduct business elsewhere due to perceived weak security practices
- **Brand Damage**: The perception of an "unsafe" business can be more damaging than the immediate financial loss, affecting the company's reputation

Data Breach and Privacy Concerns

- **Sensitive Data Exposure**: IT companies house extensive customer and operational data. Ransomware attacks can lead to breaches of sensitive data, exposing customers to privacy risks
- **Double Extortion**: Attackers may threaten to release sensitive data if the ransom is not paid, leading to double-extortion attacks

Legal and Regulatory Consequences

If customer data is compromised, IT companies may face legal consequences and fines for non-compliance with data protection regulations

Supply Chain and Third-Party Risks

Ransomware attacks can extend beyond the directly affected IT company, impacting clients, partners, and suppliers

Intellectual Property Theft

Ransomware attacks pose a risk of intellectual property theft, potentially harming competitive advantages and innovative efforts

Long-Term Espionage

Some attacks on IT companies are conducted by highly sophisticated threat groups aiming for long-term espionage

11) Utilities

Ransomware attacks can cripple utilities businesses, leading to direct financial losses, operational halts, long-term reputational damage, and legal consequences.

Operational Disruption

- **Service Interruption**: Ransomware attacks can disrupt utilities operations by encrypting or rendering systems and data inaccessible, leading to delays in services and potentially causing significant operational disruptions
- **Network Infiltration**: The interconnected nature of utilities networks increases the risk of infiltration, potentially providing access to information across various connected systems

Financial Impact

- **Revenue Loss**: Organizations may experience a decline in revenue or a complete halt of operations while recovering from a ransomware attack, even if they have functional backups
- **Ransom Payments and Recovery Costs**: Companies may face significant costs related to ransom payments, system recovery, legal fees, and other related expenses

Reputational Damage

- **Customer Trust**: A successful attack can damage the reputation of utilities companies, leading customers to conduct business elsewhere due to perceived weak security practices
- **Brand Damage**: The perception of an "unsafe" business can be more damaging than the immediate financial loss, affecting the company's reputation

Data Breach and Privacy Concerns

- **Sensitive Data Exposure**: Utilities companies house extensive customer and operational data. Ransomware attacks can lead to breaches of sensitive data, exposing customers to privacy risks
- **Double Extortion**: Attackers may threaten to release sensitive data if the ransom is not paid, leading to double-extortion attacks

Legal and Regulatory Consequences

If customer data is compromised, utilities companies may face legal consequences and fines for non-compliance with data protection regulations

Supply Chain and Third-Party Risks

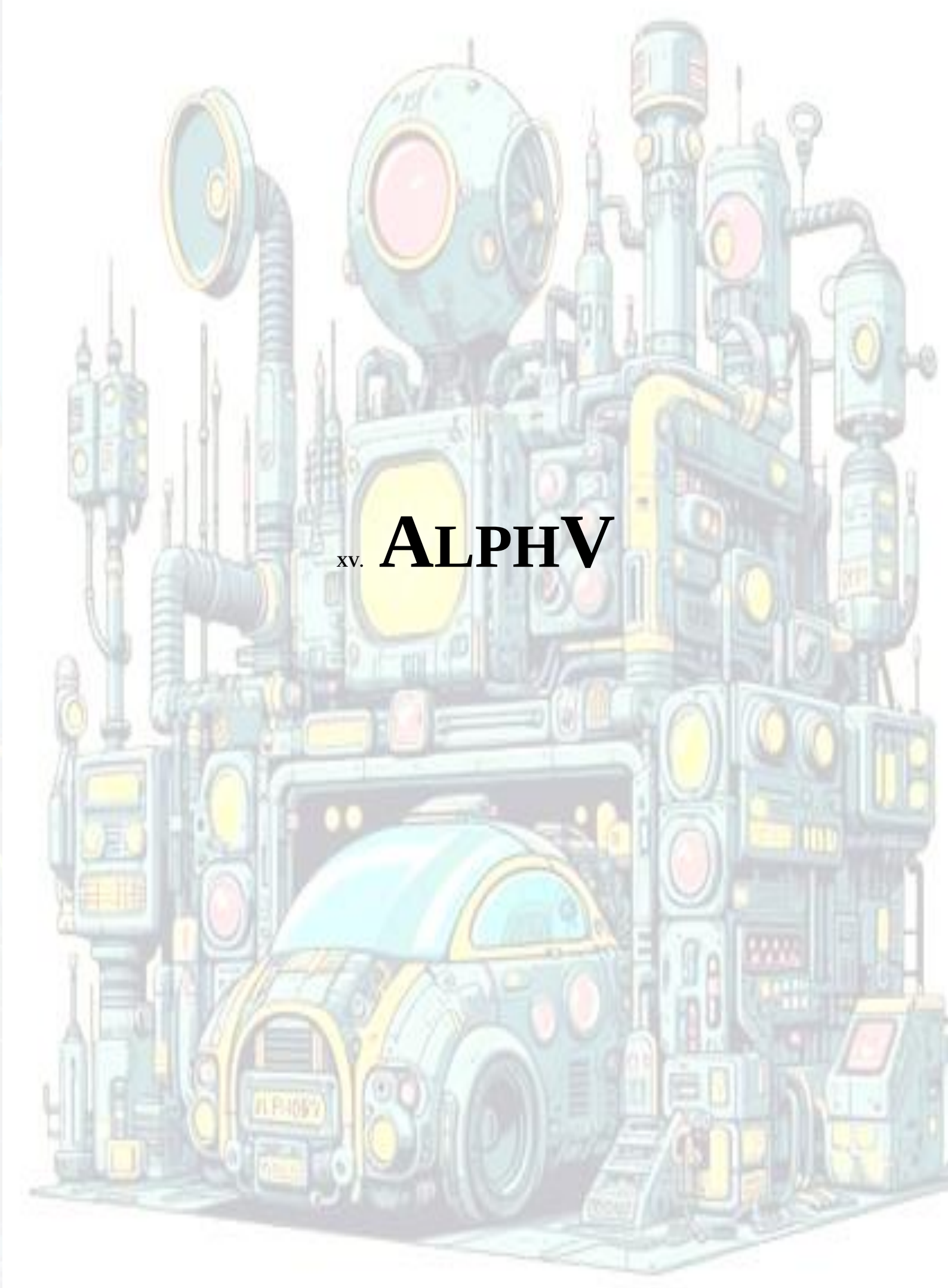
Ransomware attacks can extend beyond the directly affected utilities company, impacting clients, partners, and suppliers

Intellectual Property Theft

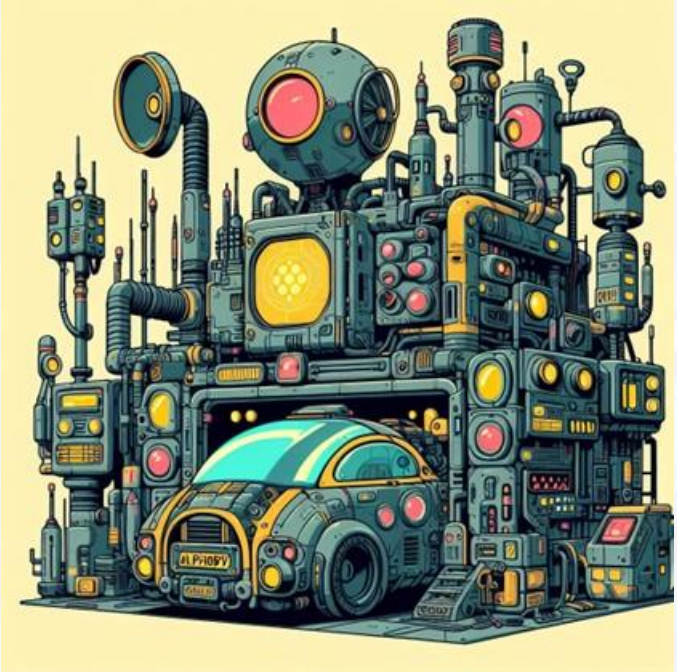
Ransomware attacks pose a risk of intellectual property theft, potentially harming competitive advantages and innovative efforts

Long-Term Espionage

Some attacks on utilities companies are conducted by highly sophisticated threat groups aiming for long-term espionage



xv. AlphV



Abstract – This document presents a analysis of the Alpha ransomware site, associated with the ransomware group also known as BlackCat. The analysis covers the ransomware technical details, including its encryption mechanisms, initial access vectors, lateral movement techniques, and data exfiltration methods.

The insights gained from this analysis are important for cybersecurity practitioners, IT professionals, and policymakers. Understanding the intricacies of AlphV/BlackCat ransomware enables the development of more effective defense mechanisms, enhances incident response strategies.

A. Introduction

The AlphV ransomware site, associated with the ransomware group also known as BlackCat, experienced a series of disruptions and takedowns by the FBI, followed by attempts by the group to regain control. On December 19, 2023, the FBI, in a coordinated effort with international law enforcement, seized the group's website and shared a seizure notice on the leak site. This action was part of a disruption campaign against the BlackCat ransomware group, which has targeted the computer networks of over 1,000 victims worldwide, including those supporting U.S. critical infrastructure.

The FBI also developed a decryption tool that was provided to hundreds of ransomware victims globally, enabling businesses, schools, healthcare, and emergency services to recover and come back online. However, AlphV officials quickly responded by regaining temporary control of their site and posting a new notice stating, "This website has been unseized." They downplayed the significance of the FBI's action and announced that 'VIP' affiliates would receive a private program on separate isolated data centers.

Despite the initial success of the FBI's seizure, the AlphV site came back online, stripped of all references to victims previously published as part of their extortion strategy. The group also claimed that the FBI only had decryption keys for about 400 companies, leaving more than 3,000 victims with encrypted data. In retaliation, AlphV lifted its self-imposed ban on attacking critical infrastructure sectors, including healthcare and nuclear facilities.

The back-and-forth between the FBI and AlphV led to multiple instances of the website being seized and then "unseized," showcasing a tug-of-war over control of the site. Despite these events, the FBI and its partners continue to investigate and pursue the individuals behind BlackCat, with the goal of bringing them to justice.

B. AlphV ransomware

The ALPHV ransomware operates by running with an access token consisting of a 32-byte value. It comes with an encrypted configuration that contains a list of services/processes to a list of whitelisted directories/files/file extensions, and a list of stolen credentials from the victim environment. The ransomware scans the volumes on the local machine, mounts all unmounted volumes, and starts encrypting files. It also deletes all Volume Shadow Copies, making it harder for victims to recover their data.

Ransomware has evolved to include more complex arguments, making it harder to detect. Its configuration data is not JSON formatted, but raw structures, and it contains junk code and thousands of encrypted strings which hinder static analysis.

ALPHV ransomware has been observed to exploit vulnerabilities in exposed services or weak credentials for initial access. It also uses tools like ExMatter to steal sensitive data before deploying ransomware.

C. AlphV Tactics

The ALPHV ransomware employs several distribution tactics to compromise systems:

- **Phishing Emails**: These deceptive messages are crafted to lure victims into opening malicious content, often disguised as legitimate communications
- **Malvertising**: This involves the use of malicious advertisements to distribute malware. The ALPHV ransomware group has been known to manipulate Google Ads to lead unsuspecting users to malicious sites
- **Infected Software Installers**: The group often uses infected software installers to deliver the ransomware. This includes cloned webpages of legitimate organizations, which are used to distribute malware via infected links or files
- **Exploitation of Software Vulnerabilities**: The group exploits vulnerabilities in Windows operating systems, exchange servers, and Secure Mobile Access products to gain access to victims' networks
- **Triple Extortion Method**: This emerging threat involves stealing data from local machines and cloud servers, executing ransomware, and then introducing

additional pressure on the victim via DDoS attacks or data leaks

D. AlphV Entry Points

The ALPHV ransomware has been identified as one of the most prolific ransomware-as-a-service variants in the world, affecting various sectors including Manufacturing, Technology, Retail & Wholesale, Finance, Healthcare and Public Health, Government and Energy, and Professional Services.

The initial entry points of ALPHV ransomware into victim networks are primarily through compromised user credentials and exploiting software vulnerabilities. For instance, ALPHV affiliates have been observed targeting publicly exposed Veritas Backup Exec installations, which were vulnerable to specific CVEs, for initial access to victim environments.

In the healthcare sector, ransomware attacks often exploit multiple possible entry points, including phishing emails, software vulnerabilities, Remote Desktop Protocol attacks, and drive-by downloads from malicious websites. The ALPHV ransomware has been a significant threat to the Healthcare and Public Health (HPH) sector.

In the financial sector, ALPHV ransomware attacks have underscored the need for enhanced incident detection capabilities and robust, timely reporting in the face of evolving cyber threats.

In the technology sector, the ALPHV ransomware gang has been known to compromise digital lending technology vendors, as seen in the attack on MeridianLink.

In the government sector, the disruptions caused by the ransomware variant have affected U.S. critical infrastructure, including government facilities.

In the energy sector, the ALPHV ransomware has been observed to target networks that support U.S. critical infrastructure.

In the professional services sector, the ALPHV ransomware has been known to target legal, IT, industrial, and financial services.

In addition to these methods, ALPHV ransomware also leverages Windows administrative tools and Microsoft Sysinternals tools during compromise. It's also worth noting that some ALPHV affiliates exfiltrate data and extort victims without ever deploying ransomware.

E. Encryption and Payments methods

ALPHV ransomware employs sophisticated encryption methods to lock victims' data. The ransomware uses a combination of symmetric and asymmetric encryption, although specific details about these algorithms are not publicly disclosed. More specifically, ALPHV ransomware uses either AES or ChaCha20 encryption, depending on its configuration. The ransomware generates a random AES key for each file, which is then encrypted using an RSA public key stored in the BlackCat configuration. The file is then encrypted using AES.

As for payment methods, ALPHV ransomware affiliates typically request ransom payments in cryptocurrencies, specifically Bitcoin and Monero. These cryptocurrencies are favored due to their decentralized nature and the anonymity they provide to the recipients. The ransom amounts demanded by ALPHV are often exorbitant, ranging from five to six digits in USD. However, it's worth noting that the threat actors have been known to negotiate and accept payments below the initial ransom demand

F. AlphV Targets

The ALPHV ransomware has been found to target organizations of various sizes. According to data from ransom leak sites, the most victims come from companies with 51-200 employees, accounting for 20.57% of the total. This is followed by companies with less than 50 employees, which make up 16.91% of the victims:

- Companies with 501-1,000 employees: 7.12%
- Companies with 1,000-5,000 employees: 9.92%
- Companies with 5,000-10,000 employees: 2.38%
- Companies with 10,000+ employees: 4.46%

However, it's important to note that there is a category labeled "unknown," accounting for 27.87% of the total, indicating that the company size of some victims is not know.

In the fourth quarter of 2022, BlackCat's successful attacks primarily targeted small businesses, making up 38.9% of the total, followed by midsize companies at 28.6%.

ALPHV ransomware targets a wide range of organizations across multiple sectors:

- **Healthcare Organizations**: ALPHV has been linked to attacks on healthcare organizations, including the leaking of sensitive images of breast cancer patients. Norton Healthcare was also a victim of an ALPHV attack
- **Financial Institutions**: Fidelity National Financial was targeted by ALPHV. The ransomware group also claimed a breach in the systems of accounting software vendor Tipalti, with plans to extort the vendor's clients
- **Oil Companies**: Two German oil companies were targeted by the BlackCat ransomware group
- **Hospitality and Entertainment**: High-profile attacks have been linked to ALPHV, including those on MGM Resorts and Caesars Entertainment
- **Manufacturing and Warehousing**: ALPHV has targeted a manufacturer and a warehouse provider
- **Government Facilities and Emergency Services**: The DOJ connected the ALPHV ransomware variant to attacks against U.S. critical infrastructure, including government facilities and emergency services
- **Schools**: Schools have also been targeted by ALPHV
- **Defense Industrial Base Companies**: These companies have been targeted by ALPHV as part of its attacks on U.S. critical infrastructure

1)Healthcare Organizations industry

This ransomware variant has been involved in numerous incidents, affecting healthcare organizations by encrypting sensitive data, including patient information, and demanding ransom for decryption keys. The attacks have not only led to financial losses but also posed serious risks to patient care and safety. The aggressive enforcement actions by law enforcement agencies, including the development of decryption tools, have provided some relief to victims.

Notable Attacks and Impacts

- **McLaren HealthCare Ransomware Attack**: A significant ransomware attack on McLaren HealthCare, a large Michigan healthcare provider, highlighted the vulnerability of healthcare systems to cyber threats.
- **Targeting of Hospitals and Healthcare Networks**: The ALPHV/BlackCat ransomware group has attacked numerous hospitals, exposing sensitive patient data and placing patient care and lives at risk. These attacks have been part of a broader pattern of targeting networks that support U.S. critical infrastructure
- **Impact on Patient Care and Data Security**: The ransomware attacks on healthcare organizations have had devastating effects, including the disruption of healthcare services, exposure of sensitive health information, and financial losses.

Law Enforcement Response

- **DOJ Disruption Campaign**: The Department of Justice (DOJ), in collaboration with the FBI and international partners, launched a disruption campaign against the ALPHV/BlackCat ransomware group. This campaign aimed to mitigate the threat posed by the ransomware to critical infrastructure, including the healthcare sector
- **FBI Decryption Tool**: As part of the disruption efforts, the FBI developed a decryption tool that was provided to victims of the ALPHV ransomware, including healthcare organizations. This tool helped save victims from ransom demands totaling approximately $68 million, enabling affected businesses and healthcare facilities to recover and resume operations

2)Financial Institutions industry

The ALPHV has posed a significant threat to the financial institutions industry, leveraging sophisticated tactics to target banks, insurance companies, and other financial service providers. This ransomware variant is known for its stealthy operations, aiming to encrypt files, steal sensitive data, and demand ransom, often employing double-extortion tactics.

Notable Attacks and Impacts

- **Fidelity National Financial Attack**: One of the most high-profile incidents involved Fidelity National Financial, a Fortune 500 provider of title insurance. The ALPHV/Black Cat group claimed responsibility for this cyberattack, which led to disruptions in title insurance, escrow, and other related services.
- **Increased Ransomware Threats**: The financial industry has seen a surge in ransomware attacks, with a notable increase in both the frequency and sophistication of these incidents. Financial organizations are attractive targets due to the vast amounts of sensitive customer and partner data they hold, making them ideal for double-extortion attacks. The Clop, LockBit, and ALPHV/BlackCat ransomware groups have been particularly active in targeting this sector
- **Impact on Financial Operations**: Attacks on financial institutions can have severe consequences, including the disruption of critical financial services and trading activities. For instance, a suspected ransomware attack against the U.S. trading arm of the Industrial and Commercial Bank of China disrupted trading in the U.S. Treasury market, underscoring the potential for ransomware to impact financial stability

Law Enforcement Response and Industry Recommendations

- **Infrastructure Takedown** Efforts: Law enforcement agencies, including the FBI, have taken action against the infrastructure of the ALPHV ransomware group. These efforts aim to disrupt the group's operations and mitigate the threat they pose to critical sectors, including financial institutions
- **Cybersecurity Measures**: Financial institutions are advised to enhance their cybersecurity defenses to protect against ransomware threats. This includes investing in skilled personnel, advanced tools, and fostering a culture of proactive defense. Regular training, continuous monitoring, and collaboration within the cybersecurity community are essential strategies to combat sophisticated ransomware groups like ALPHV/BlackCat.

3)Oil Companies industry

The group operates under a ransomware-as-a-service (RaaS) model and has targeted organizations worldwide, including many in the United States

Notable Attacks and Impacts

ALPHV ransomware, also known as BlackCat, has targeted the oil industry with significant attacks. Notably, the group exposed 400 GB of data claimed to be stolen from Encino Energy, Ohio's primary oil producer. Despite this, Encino Energy reported no impact on their operations from the attack. In Europe, ALPHV was implicated in an attack on German oil companies Mabanaft and Oiltanking, which disrupted their loading and unloading systems and forced energy giant Shell to reroute supplies. These attacks demonstrate ALPHV's capability to target and disrupt critical energy infrastructure.

Law Enforcement Response

Law enforcement agencies, including the FBI, have taken action against the infrastructure of the ALPHV ransomware group. The FBI and international law enforcement agencies infiltrated and shut down the group's infrastructure, which had targeted more than 1,000 victims over 18 months. While no arrests were announced as part of the takedown, the operation represents a significant effort to disrupt the activities of

ransomware groups targeting critical sectors like the oil industry.

4)Hospitality and Entertainment industry

Alphv has targeted the hospitality and entertainment industry with several high-profile attacks. The group's operations are characterized by the theft of sensitive data, including customer personal and financial information, followed by demands for ransom. The sophisticated tactics employed by the group include the use of social engineering and malvertising.

Notable Attacks and Impacts

- **LBA Hospitality Attack**: ALPHV targeted LBA Hospitality, which manages hotels under major chains like Marriott and Hilton. The group claimed to have compromised around 200GB of "highly confidential" internal company data, including client and employee personal details, financial reports, credit card information, and more
- **MGM Resorts International Attack**: ALPHV was responsible for a cyberattack on MGM Resorts, causing significant operational disruptions. The attack disabled online reservation systems, digital room keys, slot machines, and websites. The group used social engineering tactics to gain access to MGM's systems and deployed ransomware to more than 100 ESXi hypervisors within MGM's network
- **Caesars Entertainment Attack**: Caesars Entertainment was another victim of ALPHV, which resulted in at least $100 million in damages and a reported ransom payment of $15 million
- **Westmont Hospitality Group Breach**: ALPHV/BlackCat ransomware gang claimed to have breached Westmont Hospitality Group, one of the world's largest privately-held hospitality businesses
- **Motel One Data Breach**: The group attacked the hotel chain Motel One and threatened to leak 6 TB of stolen data, including customer contact details, internal documents, and credit card data

Tactics and Techniques

The group has been known to abuse Google search ads to spread ransomware, using major brands as lures to direct users to malicious sites. They also employ social engineering tactics, such as spear-phishing and calling help desks to gain access to networks.

5)Manufacturing and Warehousing industry

The Alphv has been linked to a series of high-profile attacks on various sectors, including manufacturing and warehousing. The group has targeted more than 1,000 victims over the past 18 months, making it the second-most prolific ransomware-as-a-service group in the world.

Notable Attacks and Impacts

One of the most significant attacks attributed to the previously mentioned ALPHV/BlackCat group was on MGM Resorts International. The ALPHV/BlackCat ransomware group has also been observed using Google Ads to distribute malware, targeting businesses including a manufacturer and a warehouse provider. ALPHV/BlackCat affiliates often pose as company IT and/or helpdesk staff and use phone calls or SMS messages to obtain access to systems.

Another notable attack was on Clarion, a global manufacturer of audio and video equipment for cars and other vehicles. The group claimed to have leaked confidential data about their business and their partners, including the engineering information of the company's customers.

Organizations should also be aware that the group targets both Windows and Linux devices, as well as network-attached storage (NAS) devices, which are often used to store backups and sensitive data.

6)Government Facilities and Emergency Services industry

The Alpvh has significantly impacted the government facilities and emergency services industry. This ransomware variant, recognized for its sophisticated tactics and global reach, has targeted critical infrastructure, including government facilities and emergency services, causing disruptions and posing threats to national security and public safety.

Notable Attacks and Impacts

- **Disruption to Critical Infrastructure**: The ALPHV ransomware variant has been connected to attacks against U.S. critical infrastructure, encompassing government facilities and emergency services.
- **Global Scale of Operations**: ALPHV/BlackCat has emerged as the second most prolific ransomware-as-a-service variant globally. Its activities have led to significant global repercussions, with the group compromising over 1,000 entities worldwide.
- **Financial Impact and Ransom Payments**: The group has demanded over USD 500 million in ransoms and received nearly USD 300 million in payments. This financial impact highlights the lucrative nature of ransomware operations targeting critical sectors, including government facilities and emergency services

Law Enforcement Response

- **DOJ Disruption Campaign**: The Department of Justice, in collaboration with the FBI and international partners, launched a disruption campaign against the ALPHV/BlackCat ransomware group. This campaign aimed to mitigate the threat posed by the ransomware to critical infrastructure, including government facilities and emergency services
- **FBI Decryption Tool**: As part of the disruption efforts, the FBI developed a decryption tool provided to victims of the ALPHV ransomware, including those in the government facilities and emergency services industry. This tool helped save victims from ransom demands totaling approximately USD 68 million, enabling affected entities to recover and resume operations

7)Schools industry

ALPHV ransomware has targeted the education sector, including K-12 schools, universities, and other educational institutions. These attacks have disrupted educational processes and compromised sensitive student and staff data. The sector's susceptibility to cyber threats, due to often limited resources and a large number of potential adversaries, necessitates a proactive approach to cybersecurity, including regular updates,

employee training, and the implementation of strong security protocols.

Notable Attacks and Impacts

- **Increased Ransomware Attacks**: There has been a sharp increase in ransomware attacks on schools, with a 17 percent rise in such incidents. The attacks have involved the encryption of files and threats to leak stolen data if ransoms are not paid
- **High-Profile School Districts Affected**: School districts such as Dallas Public Schools and Minneapolis have been among the high-profile victims of ransomware attacks.
- **Global Reach**: The attacks on schools have not been limited to the United States; educational institutions in the United Kingdom, Australia, Germany, France, and Brazil have also encountered ransomware attacks
- **Impact on Educational Operations**: Ransomware attacks on schools can lead to significant operational disruptions, including the interruption of the application process, operations, and classes. In some cases, the attacks have been severe enough to contribute to the closure of schools

Tactics and Techniques

- **Double Extortion**: ALPHV ransomware operators often employ double extortion tactics, where they encrypt files and also threaten to leak stolen data. This approach puts additional pressure on the victims to pay the ransom
- **Exploitation of Vulnerabilities**: The leading cause of ransomware attacks in the education sector has been the exploitation of vulnerabilities in devices. Schools often lack the resources for robust cybersecurity measures, making them susceptible to such attacks

8)Defense Industrial Base Companies industry

The Alpvh has targeted a wide array of sectors, including the defense industrial base companies. This focus on critical infrastructure sectors underscores the strategic approach of the group to compromise entities that are vital to national security and economic stability.

Notable Attacks and Impacts

- **Targeting Critical Infrastructure**: The Department of Justice (DOJ) has identified the defense industrial base companies as one of the critical infrastructure sectors targeted by the ALPHV ransomware variant.
- **Financial and Operational Impact**: The global losses attributed to ALPHV, which employs multiple-extortion attack models, are substantial. The group's activities have resulted in significant financial demands and have underscored the potential for operational disruptions within the defense sector