Cyber Threat Advisory

MARCH 2024

Contents

Monthly Highlights - March

1. **Americans Lost Record $10 Billion to Fraud in 2023, FTC Warns** – The U.S. Federal Trade Commission (FTC) reported that Americans lost over $10 billion to scammers in 2023, a 14% increase from the previous year. Imposter frauds were the most reported category, followed by online shopping frauds and schemes involving prizes, sweepstakes, and lotteries.

   Investment frauds topped the list in terms of monetary loss, totaling more than $4.6 billion, a 21% increase from 2022. Imposter frauds ranked second, with losses totaling nearly $2.7 billion. The FTC received over 2.6 million fraud reports, similar to 2022. The agency added 5.4 million consumer reports to its secure online database, including 1.1 million reports of identity theft through IdentityTheft.gov.

   However, the FTC noted that these figures represent only a fraction of the total harm caused by scammers, as many frauds go unreported. To report fraud, individuals can visit ReportFraud.ftc.gov or file identity theft reports at IdentityTheft.gov. The FTC's Sentinel database, which contains these reports, is accessible to approximately 2,800 law enforcement professionals, aiding in fraud detection and prevention efforts.

2. **How AI is Revolutionizing Identity Fraud** – Nearly half of businesses report an increase in synthetic identity fraud, alongside rising instances of biometric spoofing and counterfeit ID attempts, according to AuthenticID. Both consumers and businesses face new challenges in the digital landscape, from

navigating the implications of digital identity to grappling with tools like generative AI. The proliferation of AI has ushered in a new era of identity fraud, potentially leading to a significant global shift in the near future.

In 2023, the surge in AI technology blurred the lines of authenticity, making it difficult to distinguish human-authored content from AI-generated text. These empowered fraudsters now leverage AI to create seamless fake IDs, complete with convincing headshots (computer-generated or stolen) and undetectable document compositions. This sophisticated, scalable, and hard-to-detect identity-based fraud empowers malicious actors. 68% of individuals admit that the threat of identity fraud and scams influences their purchasing behavior, account opening, and business interactions.

Key statistics paint a worrying picture:

- 50% of businesses report a rise in synthetic fraud.
- Biometric spoof fraud attempts tripled from 2022 to 2023.
- Counterfeit ID fraud attempts are increasing, particularly in telecom and wireless industries.
- Over 30% of businesses reported data and security breaches in 2023.
- Synthetic fraud affects more than just finance; it extends to e-commerce, gaming, and other sectors.

Blair Cohen, President of AuthenticID, highlights that 2023 saw record levels of identity-related breaches and business attacks. These attacks, fueled by sophisticated technology, lead to significant economic losses and erosion of customer trust. Businesses must move beyond mere vigilance and actively stay ahead of these evolving threats.

Consumers also face increased identity-focused attacks, with most individuals reporting being targeted at least six times per year via various channels.

"Protecting identity is not just good business, it's crucial for individual security," states Chris Borkenhagen, Chief Digital Officer/ Information Security Officer at AuthenticID. Malicious actors constantly adapt their strategies to exploit new opportunities, maximizing their gains. Businesses need to be aware of these trends and be agile in adapting their identity-proofing strategies to minimize damage.

With AI-powered fraud on the rise, some think tanks predict that the first arrest of an individual using AI for impersonation will occur in 2024. Governments worldwide grapple with legislating this rapidly evolving technology. Identity fraud fuels other illegal activities like human trafficking, making it a lucrative business for crime syndicates globally. Organized hacking groups made headlines in 2023, employing techniques like SQL injections and malware to exploit vulnerabilities in high-profile attacks.

3. **QR Code 'Quishing' Attacks on Execs Surge, Evading Email Security** – Cybercriminals are increasingly using QR codes to launch phishing attacks, with executives facing a staggering 42 times more attempts compared to regular employees in Q4 2023. This alarming trend underscores the need for businesses to beef up digital security measures, especially for their leadership teams.

Sneaky Phishing Tactics:

- Quishing emails: These emails, carrying malicious QR codes, often bypass spam filters, infiltrating inboxes of Microsoft 365 and DocuSign users, as reported by Abnormal Security.
- Hidden links: Attackers cleverly embed phishing links within the QR code images, fooling victims into thinking they're safe.
- Physical placement: Malicious QR codes can even be placed in real-world environments like stickers, completely bypassing digital safeguards.

Why Target Executives?

- Higher access: Executives and privileged users often have access to sensitive information and financial resources, making them lucrative targets.
- Social engineering: Impersonating these individuals leverages established trust within the organization, increasing the attack's success rate.

The QR code, once seen as a convenient tool, has become a potential security risk. Here's what you can do:

- Educate employees: Train everyone, especially leaders, to be wary of suspicious QR codes, even in seemingly legitimate contexts.
- Implement security measures: Use multi-factor authentication and security tools that can detect and block malicious QR codes.
- Verify before scanning: Always double-check the destination URL before scanning any QR code, and never scan codes from unknown sources.

Remember: Vigilance is key in today's cybersecurity landscape. By staying informed and taking proactive measures, organizations can protect themselves from falling victim to these evolving phishing tactics.

4. **Ransomware Payments Reached Record $1.1 Billion in 2023** – Ransomware payments shattered records in 2023, exceeding $1.1 billion for the first time. This marks a significant turn from the decline observed in 2022, highlighting a resurgent and highly profitable threat landscape for cybercriminals.

   2022 Anomaly Explained: While 2021 remained the previous record holder, 2022's decline seemed unusual. The Chainalysis report sheds light on this, attributing it to geopolitical factors (like the Ukraine war) and law enforcement actions (e.g., dismantling of the Hive operation).

   2023 Surge: Targeting Big and Bold: The record-breaking year in 2023 is linked to several factors. These include:

   - Major Attacks: Escalating attacks against critical infrastructure and institutions boosted the overall ransom haul.
   - Clop's MOVEit Campaign: This campaign affected countless organizations worldwide, significantly contributing to the surge.
   - Shifting Strategies: Ransomware groups adapted to declining payments by focusing on "big game hunting," targeting large enterprises willing to pay bigger ransoms.

   Top Ransomware Players: The report identifies prolific groups like ALPHV/Blackcat, Clop, and LockBit, each employing different tactics to achieve high payouts. While LockBit relies on steady attacks and moderate sums, Clop and Dark Angels favor fewer attacks but with larger ransoms. ALPHV/Blackcat finds success through a high volume of moderate-sized payouts.

   The Cat-and-Mouse Game: While Coveware reports a decrease in victims paying ransoms, Chainalysis warns that this alone may not be enough. As long as attacks increase and large organizations pay hefty ransoms, ransomware operations stay profitable.

   Looking Ahead: Law enforcement is actively taking down rogue exchanges and mixers used for laundering ransom payments. Hopefully, the trend of victims refusing to pay will continue, eventually making ransomware less financially viable.

5. **Mother Of All Breaches – A Historic Data Leak Reveals 26 Billion Records** – Data breaches come in various sizes, but the latest discovery dwarfs them all. Dubbed the Mother of all Breaches (MOAB), this massive collection comprises records from thousands of meticulously gathered leaks, breaches, and privately sold databases.

   Bob Dyachenko, a cybersecurity researcher, and owner of SecurityDiscovery.com, along with the Cybernews team, uncovered billions of exposed records on an open instance whose owner is unlikely to ever be identified. The researchers suspect that the owner has a vested interest in storing vast amounts of data, suggesting potential malicious intent, involvement in data brokering, or association with a data-intensive service.

   The sheer scale of this dataset poses an enormous threat, as threat actors could exploit the aggregated data for a wide array of attacks, including identity theft, sophisticated phishing schemes, targeted cyberattacks, and unauthorized access to personal and sensitive accounts, the researchers warned.

   Rather than containing only newly stolen data, the supermassive MOAB is likely the largest compilation of multiple breaches (COMB) to date. Although the team identified over 26 billion records, duplicates are highly probable. However, the leaked data goes beyond credentials, encompassing a vast amount of sensitive information that is highly valuable to malicious actors.

   A cursory examination of the data reveals an astounding number of records amassed from previous breaches. The largest portion, 1.4 billion records, originates from Tencent QQ, a Chinese instant messaging app. Additionally, there are purportedly hundreds of millions of records from various other platforms such as Weibo (504M), MySpace (360M), Twitter (281M), Deezer (258M), Linkedin (251M), AdultFriendFinder (220M), Adobe (153M), Canva (143M), VK (101M), Daily Motion (86M), Dropbox (69M), Telegram (41M), among many others.

   The leak also includes records from various government organizations in the US, Brazil, Germany, the Philippines, Turkey, and elsewhere. The potential consumer impact of this supermassive breach could be unprecedented, as many people reuse usernames and passwords, leaving them vulnerable to credential-stuffing attacks.

   The researchers cautioned that if users utilize the same passwords across different accounts, attackers could leverage this to pivot toward more sensitive accounts. Individuals whose data is part of the supermassive MOAB could also be at risk of spear-phishing attacks or inundation with spam emails, the researchers added.

6. **Tech Giant HP Enterprise Hacked by Russian Hackers Linked to DNC Breach** – Hackers believed to have ties to the Kremlin are suspected of penetrating Hewlett Packard Enterprise's (HPE) cloud email system to steal mailbox data. The company revealed in a regulatory filing with the U.S. Securities and Exchange Commission (SEC) that the breach occurred in May 2023 and affected a small percentage of HPE mailboxes, including those belonging to individuals in cybersecurity, go-to-market, business segments, and other functions.

   The attack has been attributed to APT29, a Russian state-sponsored group also known as BlueBravo, Cloaked Ursa, Cozy Bear, Midnight Blizzard (formerly Nobelium), and The Dukes. This disclosure comes shortly after Microsoft accused the same group

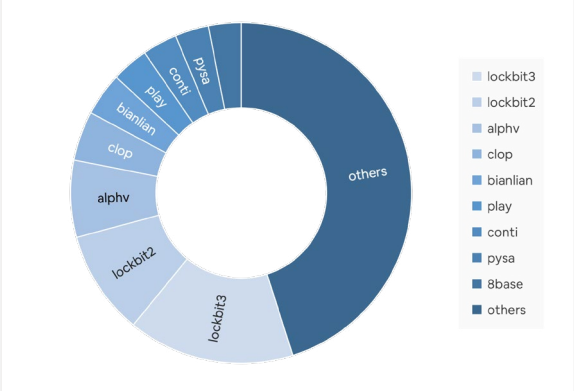
of breaching its systems in late November 2023 to access emails and attachments from senior executives and individuals in cybersecurity and legal departments.

HPE was informed of the breach on December 12, 2023, indicating that the threat actors remained undetected within its network for over six months. The company suspects a connection to a previous security incident, also attributed to APT29, involving unauthorized access and data exfiltration from a limited number of SharePoint files as early as May 2023, which was discovered in June 2023.

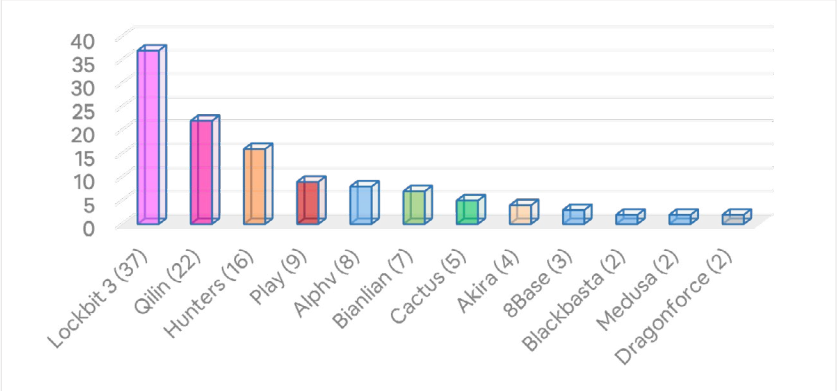
Despite the breach, HPE stated that the incident has not materially affected its operations thus far. The company did not disclose the extent of the attack or specify the exact email data that was compromised.

Ransomware Tracker

Distribution of Post by Group (Total - 10189 in Feb)



Post by Group Last 7 Days



Unveiling the Threat: The Rise of Akira Ransomware

Executive Summary:

- Akira ransomware, a sophisticated threat, has emerged as a significant concern in the cybersecurity landscape.
- Akira ransomware has gained prominence as an advanced cyber threat in the cybersecurity landscape due to its sophisticated tactics and data exfiltration capabilities.
- This ransomware operation, launched in March 2023, has targeted organizations across various industries worldwide, encrypting files and demanding hefty ransoms.
- The Akira group's modus operandi involves breaching corporate networks, encrypting files with a wide range of extensions, and threatening to expose stolen data if ransoms are not paid.
- Akira employs advanced techniques to evade detection and disable security monitoring tools, posing challenges for organizations attempting to defend against these attacks.
- Implementing robust detection, prevention, and remediation strategies is essential to mitigate the impact of Akira ransomware incidents.

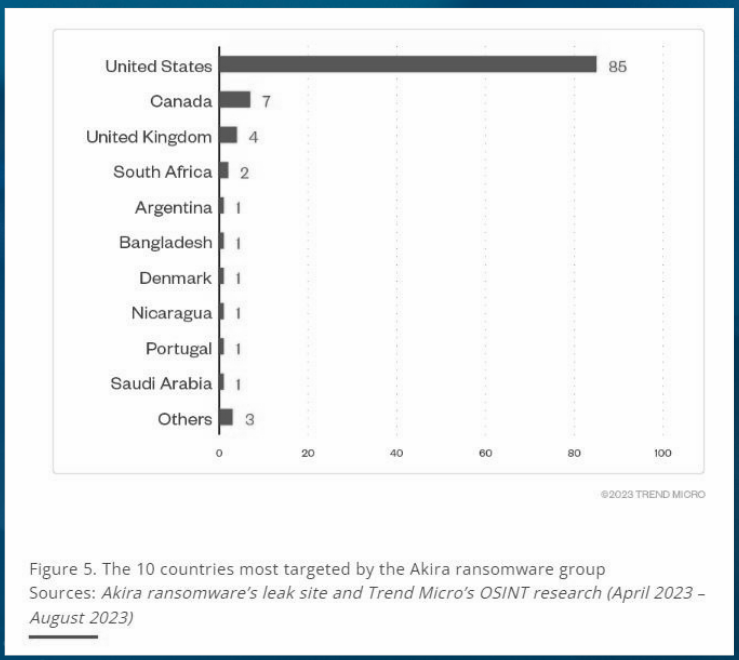


Figure 5. The 10 countries most targeted by the Akira ransomware group
Sources: *Akira ransomware's leak site and Trend Micro's OSINT research (April 2023 – August 2023)*

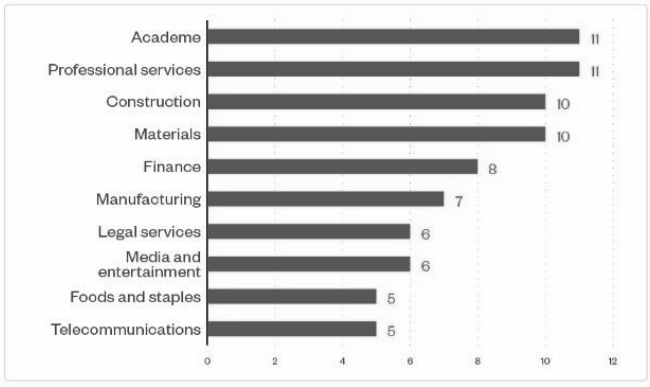


Figure 7. The 10 industries most targeted by Akira ransomware threat actors
Sources: *Akira ransomware's leak site and Trend Micro's OSINT research (April 2023 – August 2023)*

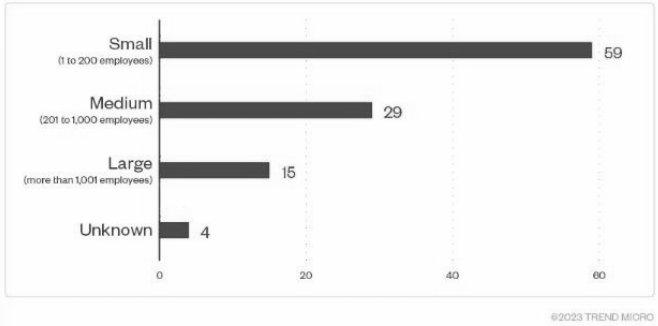


Figure 6. The distribution by organization size of Akira ransomware's victim organizations
Sources: *Akira ransomware's leak site and Trend Micro's OSINT research (April 2023 – August 2023)*

Technical Details:

- Akira ransomware utilizes a potent encryptor capable of deleting Windows Shadow Volume Copies and encrypting files with a wide array of extensions.
- It selectively encrypts files with specific extensions, avoiding critical system files to maintain system functionality and ensure successful encryption.

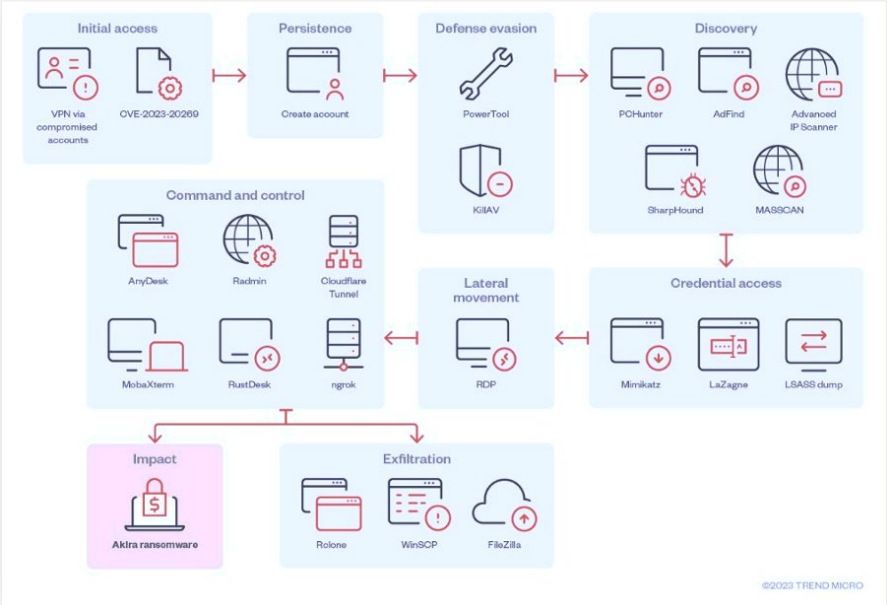
Initial Access	Persistence	Execution	Defense Evasion	Credential Access	Discovery	Command and Control	Lateral Movement	Exfiltration	Impact
T1078 - Valid Accounts	T1136.002 - Create Account: Domain Account	T1059 - Command and Scripting Interpreters	T1562.001 - Impair Defenses: Disable or Modify Tools	T1003.001 - OS Credential Dumping: LSASS Memory	T1082 - System Information Discovery	T1219 - Remote Access Software	T1570 - Lateral Tool Transfer	T1567.002 - Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1490 - Inhibit System Recovery
Uses compromised VPN credentials.	Once initial access is established, Akira operators will create a domain account on the compromised system	Accepts parameters for its routines such as "-n 10" (for encryption percent) or "-s {filename}" (for shared folder encryption)	It has been observed to use PowerTool or a KillAV tool that abuses Zemana AntiMalware driver to terminate AV-related processes	Uses Mimikatz, LaZagne, or a command line to dump LSASS from memory	Uses PCHunter and SharpHound to gather system information	May use either AnyDesk, Radmin, Cloudflare Tunnel, MobaXterm, RustDesk, or Ngrok to gain remote access on targeted systems	Uses RDP to move laterally within the victim's network	Uses RClone to exfiltrate stolen information over web service	Deletes shadow copies to inhibit recovery
T1190 - Exploit Public-Facing Application	-	-	-	-	T1069.002 - Permission Groups Discovery: Domain Groups	-	-	T1048.003 - Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	T1486 - Data Encrypted for Impact
Targets vulnerable Cisco devices via CVE-2023-20269	-	-	-	-	Uses AdFind, net Windows command, and nltest to gather domain information	-	-	Uses FileZilla or WinSCP to exfiltrate stolen information via FTP	Akira ransomware is used to encrypt files
-	-	-	-	-	T1018 - Remote System Discovery	-	-	-	-
-	-	-	-	-	Uses Advanced IP Scanner and MASSCAN to discover remote systems	-	-	-	-

- The ransomware utilizes the Windows Restart Manager API to close processes or shut down Windows services that may impede the encryption process, and it prioritizes data exfiltration over ransomware deployment.
- The ransomware employs tools like WinRAR, WinSCP, rclone, and MEGA for exfiltrating sensitive data to attacker-controlled infrastructure.
- Akira actors utilize runas to run commands in the context of a different user, making tracking their activity challenging for defenders.
- Additionally, the threat actors attempt to evade detection by removing the tools they use for file collection after completing their activity.
- Each victim is provided with a unique negotiation password for communication with the threat actors via a Tor-based negotiation site, facilitating ransom payment discussions.
- Data exfiltration is a key component of Akira ransomware operations, with threat actors stealing sensitive information for extortion purposes.

Initial Access	Defense Evasion	Discovery	Credential Access	Command and Control	Lateral Movement	Exfiltration
VPN via compromised accounts	PowerTool	AdFind	Mimikatz	AnyDesk	RDP	WinSCP
CVE-2023-20269	KillAV (Terminator from GitHub)	PCHunter	LaZagne	Radmin	-	Rclone
-	-	Advanced IP Scanner	LSASS dump	Cloudflare Tunnel	-	FileZilla
-	-	SharpHound	-	MobaXterm	-	-
-	-	MASSCAN	-	RustDesk	-	-
-	-	-	-	ngrok	-	-

Detection:

- Detecting Akira ransomware requires robust endpoint protection solutions capable of identifying and mitigating suspicious behavior.
- Organizations should deploy multi-factor authentication to safeguard VPN access and maintain vigilant patch management practices to address vulnerabilities promptly.
- Implementing network traffic monitoring solutions can help identify anomalous activity indicative of Akira ransomware infections.
- Anomaly detection algorithms and behavioral analysis tools can enhance the organization's ability to detect and respond to Akira ransomware incidents proactively.



Indicators of Compromise

SHA-256 hash or URL	Detection name	Description
337d21f964091417f22f35aee35e31d94fc3f35179c-36c0304eef6e4ae983292	Ransom.Win64.AKIRA.SMTH	Akira ransomware
3c92bfc71004340ebc00146ced294bc94f-49f6a5e212016ac05e7d10fcb3312c	Ransom.Win64.AKIRA.THDBFBC	Akira ransomware
637e28b38086ff9efd1606805ff57aaf6cdec4537378f-019d6070a5efdc9c983	Ransom.Win64.AKIRA.SMTH	Akira ransomware
67afa125bf8812cd943abed2ed56ed6e07853600ad-609b40bdf9ad4141e612b4	Ransom.Win64.AKIRA.THEOIBC	Akira ransomware
678ec8734367c7547794a604cc65e74a0f42320d85a6d-ce20c214e3b4536bb33	Ransom.Win64.AKIRA.THEOIBC	Akira ransomware
7b295a10d54c870d59fab3a83a8b983282f6250a0be9d-f581334eb93d53f3488	Ransom.Win64.AKIRA.THDBFBC	Akira ransomware
8631ac37f605daacf47095955837ec5abbd5e98c540ffd-58bb9bf873b1685a50	Ransom.Win64.AKIRA.THEAABC	Akira ransomware
1d3b5c650533d13c81e325972a912e3ff8776e36e18bca-966dae50735f8ab296	Ransom.Linux.AKIRA.THFBCBC	Akira Linux ransomware
094d1476331d6f693f1d546b53f1c1a42863e6cde014e2ed655f-3cbe63e5ecde	HackTool.Win32.ToolPow.SM	PowerTool binary
35415d97038e091744e9cab3b88c78c1a7ca87f78d-2b4a363f72f2c28d65932b	Trojan.Win64.KILLAV.YXDFGZ	Terminator from GitHub
6192beb56de670de902193a33380e5eb0f3b4b2e3e848e7ee-a8950075f00f2e5	PUA.Win64.PCHUNTER.L	PCHunter binary
d1aa0ceb01cca76a88f9ee0c5817d24e7a15ad40768430373ae-3009a619e2691	PUA.Win64.PCHunter.YACIU	PCHunter binary
f157090fd3ccd4220298c06ce8734361b724d80459592b10a-c632acc624f455e	HackTool.Win32.ADFind.B	AdFind binary
akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z-636bad[.]onion	N/A	Akira ransomware leak site
akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7e-fvr2id[.]onion	N/A	Akira TOR negotiation portal

Prevention:

- Preventing Akira ransomware attacks necessitates a multifaceted approach encompassing proactive measures and user awareness initiatives.
- Organizations should prioritize the implementation of multi-factor authentication to safeguard VPN access and diligently apply security patches to mitigate known vulnerabilities.
- Robust endpoint protection solutions, coupled with user training programs, can enhance the organization's resilience against ransomware threats.
- Implementing least privilege access controls and regularly auditing user permissions can limit the impact of ransomware attacks by restricting unauthorized access to critical systems and data.

Remediation:

- In the event of a ransomware attack, organizations should promptly isolate infected systems from the network to prevent further spread of the ransomware.
- Maintaining comprehensive backup and recovery procedures is crucial for restoring encrypted files and minimizing downtime.
- Having a well-documented incident response plan in place ensures a coordinated and effective response to ransomware incidents, facilitating timely communication with stakeholders and law enforcement agencies.
- Organizations should conduct post-incident analysis to identify weaknesses in their security posture and implement measures to prevent future ransomware incidents.

Decoding Water Hydra: A Deep Dive Into a Sophisticated APT Group and Their Exploits

Executive Summary

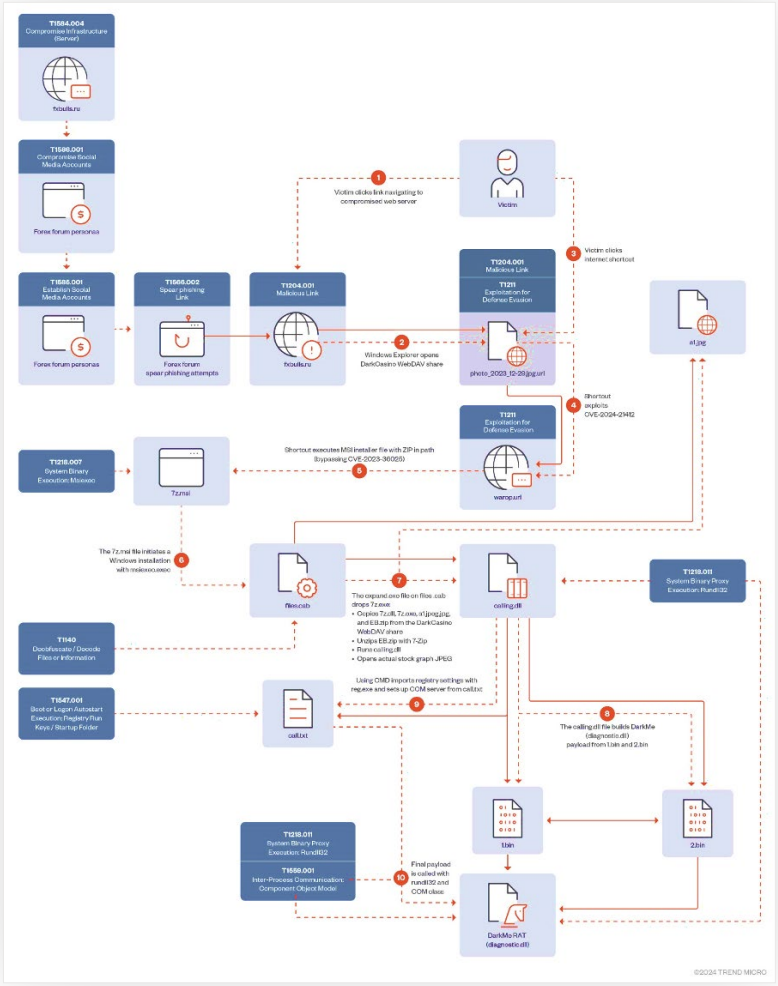
- A zero-day vulnerability tracked as CVE-2024-21412 (ZDI-CAN-23100) was discovered by the Trend Micro Zero Day Initiative (ZDI).
- The vulnerability was exploited by the advanced persistent threat (APT) group Water Hydra (aka DarkCasino) to bypass security measures and target financial market traders.
- Water Hydra is known for its sophisticated attacks on the financial industry, including banks, cryptocurrency platforms, forex, and stock trading platforms.
- The attack involved a complex chain of exploitation, leveraging internet shortcuts and WebDAV components.
- The APT group's tactics include spear phishing campaigns on forex trading forums, using JPEG and PDF files as lures, and abuse of the search protocol to customize Windows Explorer windows.

Technical Details:

- Water Hydra utilized CVE-2024-21412 to bypass Microsoft Defender SmartScreen, allowing the deployment of DarkMe malware.
- The attack chain involved the use of internet shortcuts (.URL) and WebDAV components to deliver the payload.
- Over time, Water Hydra's campaign evolved with updated infection chains and deployment techniques.
- DarkMe malware, delivered through the attack chain, is a sophisticated remote access tool (RAT) capable of gathering system information, executing commands, and communicating with a command-and-control (C&C) server.
- The malware employs various obfuscation techniques to avoid detection and enhance its capabilities, including encoding important strings and utilizing hidden windows for communication.

Detection:

- Detection of Water Hydra attacks requires monitoring of spear phishing attempts on financial trading forums and stock trading channels.
- Suspicious URLs pointing to internet shortcuts and WebDAV shares should be analyzed for signs of malicious activity.
- Unusual file behavior, such as internet shortcuts linking to other shortcuts, should raise red flags for potential exploitation attempts.
- Monitoring network traffic for connections to known C&C servers associated with Water Hydra can help detect ongoing attacks.



Detailed IOC Link:

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-smartscreen-zero-day/ioc-list-water-hydra-cve-2024-21412.txt

Prevention:

- Implementing strong email security measures to prevent spear phishing attacks is crucial in preventing initial access by threat actors.
- Regularly updating and patching software vulnerabilities, especially those exploited in zero-day

attacks like CVE-2024-21412, can mitigate the risk of exploitation.

- Restricting access to WebDAV components and internet shortcut files can prevent attackers from leveraging these components in their attack chain.
- Employing endpoint protection solutions capable of detecting and blocking known malware variants associated with Water Hydra can further enhance defense mechanisms.

Remediation:

- In the event of a Water Hydra attack, immediate isolation of affected systems and networks is essential to prevent further spread of the malware.
- Incident response teams should conduct thorough forensic analysis to identify the extent of the compromise and remove any traces of the malware from infected systems.
- Close monitoring of network traffic and endpoint activities can help ensure that the threat actor has been fully eradicated from the environment.
- Implementing security best practices and conducting regular security assessments can help strengthen defenses against future attacks by Water Hydra and similar APT groups.

Chinese Hackers Hid in US Infrastructure Network for 5 Years

According to a joint advisory from CISA, the NSA, the FBI, and partner Five Eyes agencies, the Chinese cyber espionage group Volt Typhoon infiltrated a critical infrastructure network in the United States and remained undetectable for at least five years before becoming known.

Living off the land (LOTL) tactics are widely employed by Volt Typhoon hackers in their assaults on critical infrastructure organizations.

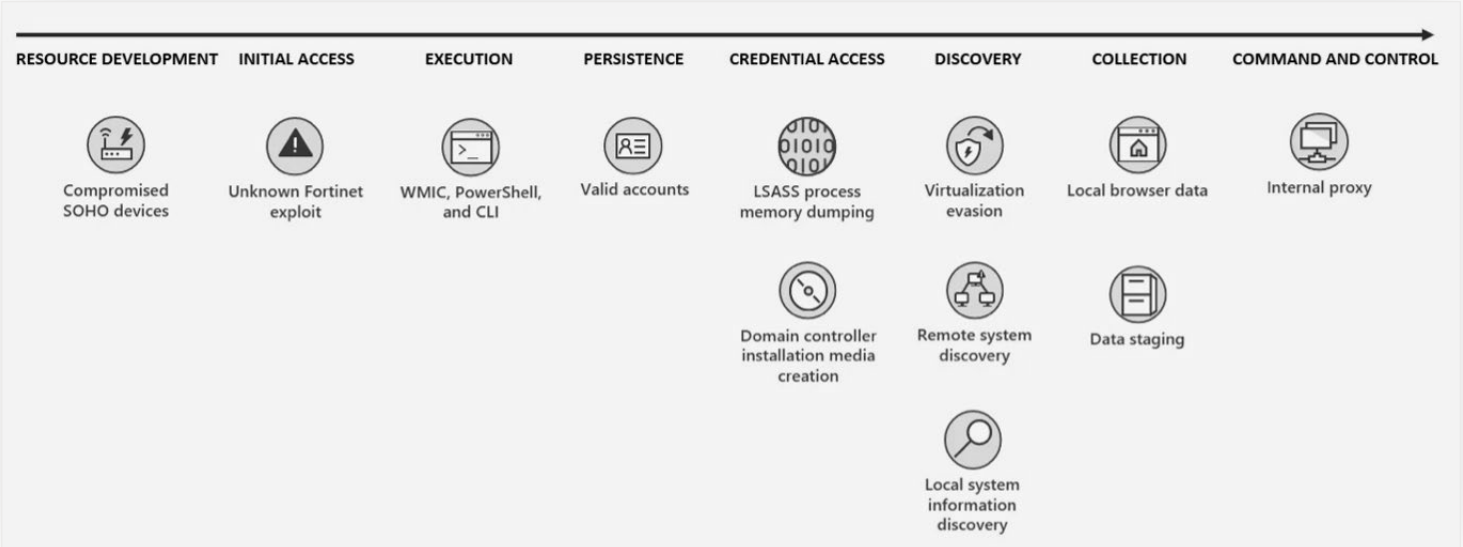
To evade detection and continue to exist over time on compromised systems, they also use strong operational security and stolen accounts.

Volt Typhoon actors have been observed by U.S. authoring agencies to have retained access and footholds in certain victim IT environments for a minimum of five years.

Detection:

Volt Typhoon actors invest a lot of resources in pre-exploitation reconnaissance to gain a thorough understanding of the target organization and its surroundings; they customize their tactics, techniques, and procedures (TTPs) to fit the victim's environment; and they keep going back to maintain persistence and gain a deeper understanding of the target environment even after the initial compromise.

The Chinese threat group primarily targets the energy, transportation, water/wastewater, and communications sectors, but it has also successfully penetrated the networks of several critical infrastructure organizations across the United States.

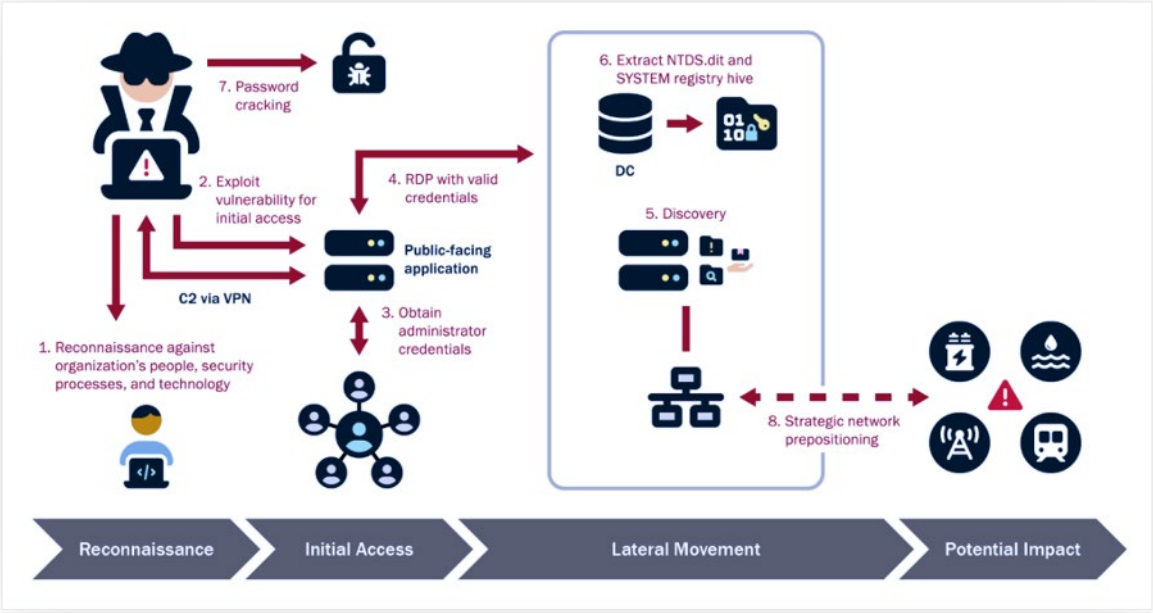


Authorities concluded with high confidence that the group aims to position itself within networks that give them access to Operational Technology (OT) assets with the goal of disrupting critical infrastructure, as their behavior and target selection defies traditional cyber espionage or intelligence gathering operations.

Authorities in the United States are especially concerned that Volt Typhoon may use its access to vital networks for disruptive purposes in the event of a military conflict or other geopolitical unrest. In the event of a significant crisis or conflict with the United States, Volt Typhoon actors may aim to position themselves on IT networks using living off the land (LOTL) techniques to launch disruptive or destructive cyber activity against U.S. critical infrastructure.

Volt Typhoon actors adapt their TTPs to the victim environment, but the actors generally follow the same pattern of behavior across identified intrusions, according to the U.S. authoring agencies.

1. Volt Typhoon investigates the network architecture and operational protocols of the target organization through comprehensive pre-compromise reconnaissance.
2. In general, Volt Typhoon uses known or zero-day vulnerabilities in networks that are accessible to the public to get initial access to the IT network.
3. Targeting vulnerabilities for privilege escalation in the operating system or network services, Volt Typhoon seeks to obtain administrator credentials within the network.
4. Volt Typhoon moves laterally to the domain controller (DC) and other devices by using legitimate administrator credentials.
5. Volt Typhoon uses LOTL binaries for stealth while conducting discovery within the victim's network.
6. Volt Typhoon extracts the Active Directory database (NTDS.dit) from the DC to accomplish full domain compromise.
7. Volt Typhoon most likely decodes these hashes using offline password cracking methods.
8. Elevated credentials are utilized by Volt Typhoon for deliberate network intrusion and further exploration, with a common goal of obtaining the ability to access OT resources.



Volt Typhoon actors show little activity in the compromised environment (apart from the previously mentioned discovery) after they have successfully gained access to legitimate accounts, indicating that their goal is persistence rather than quick exploitation.

Event ID (Log)	Event Detail	Description
216 (Windows ESENT Application Log)	A database location change was detected from 'C:\Windows\NTDS\ntds.dit' to '\\?\GLOBALROOT\Device\{redacted}VolumeShadowCopy1\Windows\NTDS\ntds.dit'	There has been a change in the location of the NTDS.dit database. This may indicate that the database is being ready for extraction in the first stage of NTDS credential dumping.
325 (Windows ESENT Application Log)	The database engine created a new database (2, C:\Windows\Temp\tmp\Active Directory\ntds.dit).	Signifies the formation of a fresh NTDS.file in a directory that is not typical. Frequently a clue that data is being staged for exfiltration. Keep an eye out for odd database activities in temporary folders.
637 (Windows ESENT Application Log)	C:\Windows\Temp\tmp\Active Directory\ntds.jfm-++- (0) New flush map file "C:\Windows\Temp\tmp\Active Directory\ntds.jfm" will be created to enable persisted lost flush detection.	For NTDS.dit, a new flush map file is being generated. This might indicate that NTDS credential dumping operations are still going on and that uncommitted changes to the NTDS.dit file are being recorded.
326 (Windows ESENT Application Log)	C:\$SNAP_{redacted}_VOLUMEC$\Windows\NTDS\ntds.dit-++-0-++- [1] The database engine attached a database. Began mounting of C:\Windows\NTDS\ntds.dit file created from volume shadow copy process	Symbolizes the mounting of a volume shadow copy of an NTDS.dit file. This crucial stage of NTDS credential dumping shows that a domain controller's data is actively being manipulated.
327 (Windows ESENT Application Log)	C:\Windows\Temp\tmp\Active Directory\ntds.dit-++-1-++- [1] The database engine detached a database (2, C:\Windows\Temp\tmp\Active Directory\ntds.dit). Completion of mounting of ntds.dit file to C:\Windows\Temp\tmp\Active Director	The removal of a database, especially one located in a temporary directory, may signify the end of the credential dumping procedure, possibly in conjunction with exfiltration preparations.
21 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Session logon succeeded: User: {redacted}\{redacted} Session ID: {redacted} Source Network Address: {redacted}	Authentication to a Remote Desktop Services session completed successfully.
22 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Shell start notification received: User: {redacted}\{redacted} Session ID: {redacted} Source Network Address: {redacted}	An effective new Remote Desktop session has been launched. This could indicate unauthorized remote access or lateral movement, particularly if the user or session appears out of the blue.
23 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Session logoff succeeded: User: {redacted}\{redacted} Session ID: {redacted}	Logout of the Remote Desktop session was successful.
24 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Session has been disconnected: User: {redacted}\{redacted} Session ID: {redacted} Source Network Address: {redacted}	A user may disconnect a remote desktop session or there may be problems with network connectivity.
25 (Windows Terminal Services Local Session Manager Operational Log)	Remote Desktop Services: Session reconnection succeeded: User: {redacted}\{redacted} Session ID: {redacted} Source Network Address: {redacted}	Reconnected to a Remote Desktop Services session successfully. This could indicate unauthorized remote access or lateral movement, particularly if the user or session appears out of the blue.
1017 (Windows System Log)	users\{redacted}\downloads\History.zip Durable: 1 Resilient or Persistent: 0 Guidance: The server closed a handle that was previously reserved for a client after 60 seconds.	A client's handle was closed by the server. While uncommon patterns or locations (such as History.zip in a user's downloads) may indicate data collection from a local system, they are common in network operations.
1102 (Windows Security Log)	All	As logs are typically not cleared and this is a known Volt Typhoon tactic to cover their tracks, all Event ID 1102 entries should be investigated.

Remediation:

1. Apply patches for internet-facing systems within a risk-informed span of time.
2. Do not store credentials on edge appliances/devices.
3. Configure Group Policy settings to prevent web browsers from saving passwords.
4. Enforce strict policies via Group Policy and User Rights Assignments.
5. Consider using a privileged access management (PAM) solution.
6. Implement an Active Directory tiering model to segregate administrative.
7. Disable all user accounts and access to organizational resources for employees on the day of their departure.
8. Limit the use of RDP and other remote desktop services.
9. Ensure that sensitive accounts use their administrator credentials only on hardened, secure computers.

Prevention:

1. Implement network segmentation to isolate federation servers.
2. Revoke unnecessary public access to the cloud environment.
3. Ensure logging is turned on for application, access, and security logs.
4. Store logs in a central system.
5. Document a list of threats and cyber actor TTPs relevant to your organization.
6. Implement periodic training for all employees and contractors that covers basic security concepts.
7. Change default passwords.
8. Enforce strict access policies for accessing OT networks.
9. Lock or limit set points in control processes to reduce the consequences of unauthorized controller access.
10. Closely monitor all connections into OT networks for misuse, anomalous activity, or OT protocols.

Russian Hackers Hit Mail Servers in Europe for Political and Military Intel

Threat actors with ties to Russia and Belarus have been connected to a recent cyber espionage campaign that targeted more than 80 organizations, most likely by taking advantage of cross-site scripting (XSS) vulnerabilities in Roundcube webmail servers.

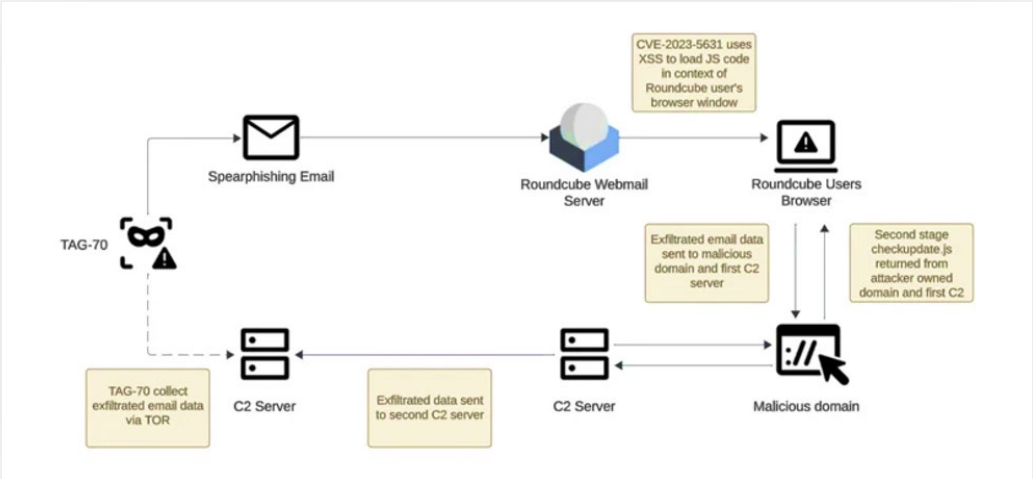
According to Recorded Future, which linked the intrusion set to a threat actor known as Winter Vivern—also known as TA473 and UAC0114—these entities are mainly situated in Georgia, Poland, and Ukraine.

The hacking group is being monitored by the cybersecurity company under the codename Threat Activity Group 70 (TAG-70).

ESET first reported in October 2023 that Winter Vivern was exploiting security holes in Roundcube email servers, joining the ranks of other Russia-affiliated threat actor groups that are known to target email software, including APT28, APT29, and Sandworm.

Detection:

Active since December 2020, the intruder has also been connected to the exploit of an email software vulnerability in Zimbra Collaboration that was fixed last year, which allowed it to infiltrate agencies in Moldova and Tunisia in July 2023.



The campaign that Recorded Future uncovered ran from the beginning of October 2023 until the middle of the month, aimed at gathering intelligence on military and political activity throughout Europe.

The attacks coincide with additional TAG-70 activity against government mail servers in Uzbekistan, which was previously discovered in March 2023.

According to the company, TAG70 has proven to be highly skilled in its attack techniques. The threat actors circumvented the defenses of governmental and military institutions by using social engineering tactics and taking advantage of cross-site scripting vulnerabilities in Roundcube webmail servers to obtain unauthorized access to targeted mail servers.

The attack chains use JavaScript payloads that are intended to exfiltrate user credentials to a command-and-control (C2) server by taking advantage of Roundcube vulnerabilities.

Additionally, Recorded Future discovered proof that TAG-70 targeted the Georgian Embassy in Sweden as well as the Iranian embassies in the Netherlands and Russia.

Prevention:

- Block unknown JS scripts from running.
- Patch all .exe files on production.
- Do not click on malicious links.
- Use anti-proxy techniques to avoid malicious IP sources.
- Disallow the RDP feature for unknown connections.
- Do not install unwanted applications from untrusted sources.
- Do not use malicious/free VPNs to access web applications or networks.
- Implement packet filtration & IDS/IPD mechanisms through the firewall.
- Enable SSL with SMTP protocol for safe transmission.
- Enable limitations on administrative access or rights.

Remediation:

- Deploy anti-JS scripts in the production environment.
- Use network monitoring and Endpoint Detection and Response (EDR) tools to detect abnormal activities.
- Implement network segmentation to control traffic and prevent ransomware spread.
- Enhance email security by disabling risky links and encrypting backup data.
- Secure and limit Remote Desktop Protocol (RDP) usage with best practices and MFA.
- Maintain offline backups and adhere to a robust data recovery plan.
- Follow NIST standards for strong, less frequently changed passwords.
- Monitor remote access tools and implement phishing-resistant multifactor authentication (MFA).
- Keep systems and software regularly updated, focusing on patching vulnerabilities.

TOP THREAT ACTORS

Threat Actor	IOC Reference
Akira Ransomware	https://documents.trendmicro.com/assets/txt/ransomware-spotlight-akira-iocssrFFEFh.txt
Water Hydra	https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-smartscreen-zero-day/ioc-list-water-hydra-cve-2024-21412.txt
Volt Typhoon	https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
TAG-70	https://go.recordedfuture.com/hubfs/reports/cta-2024-0217.pdf

TOP EXPLOITED VULNERABILITIES

Vulnerability Name	Description	References
Linux Kernel ksmbd Mech Token Out-Of-Bounds Read Information Disclosure Vulnerability	Vulnerability allows local attackers to escalate privileges on affected installations of Trend Micro Deep Security. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	https://success.trendmicro.com/dcx/s/solution/000296387?language=en_US
Sante PACS Server Token Endpoint SQL Injection Remote Code Execution Vulnerability	Vulnerability allows remote attackers to disclose sensitive information on affected installations of Linux Kernel. Only systems with ksmbd enabled are vulnerable. The specific flaw exists within the handling of SMB2 Mech Tokens.	https://security-tracker.debian.org/tracker/CVE-2024-26594

TOP EXPLOITED VULNERABILITIES

Vulnerability Name	Description	References
Schneider Electric EcoStruxure IT Gateway Hard-Coded Credentials Local Privilege Escalation Vulnerability	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DCS-8300LHV2 IP cameras. The specific flaw exists within the handling of the Authorization header by the RTSP server, which listens on TCP port 554.	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10370
Trimble SketchUp SKP File Parsing Use-After-Free Remote Code Execution Vulnerability	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Trimble SketchUp. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	https://help.sketchup.com/en/release-notes/sketchup-desktop-202302
Inductive Automation Ignition getJavaExecutable Directory Traversal Remote Code Execution Vulnerability CVE-2023-50233	Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. An attacker obtains the ability to execute low-privileged code on the target system to exploit this vulnerability. Only systems with long Win32 path support enabled are affected.	https://security.inductiveautomation.com/?tcuUid=fc4c4515-046d-4365-b688-693337449c5b
ESET Smart Security Premium ekrn Link Following Local Privilege Escalation Vulnerability CVE-2024-0353	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations.	https://support.eset.com/en/ca8612-eset-customer-advisory-link-following-local-privilege-escalation-vulnerability-in-eset-products-for-windows-fixed
Siemens Simcenter Femap MODEL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-24924	Vulnerability allows local attackers to escalate privileges on affected installations of ESET Smart Security Premium. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	https://cert-portal.siemens.com/productcert/html/ssa-000072.html
Siemens Tecnomatix Plant Simulation WRL File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-23798	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Siemens Tecnomatix Plant Simulation. The specific flaw exists within the parsing of WRL files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer.	https://cert-portal.siemens.com/productcert/html/ssa-017796.html
SolarWinds Orion Platform AppendUpdate SQL Injection Remote Code Execution Vulnerability CVE-2023-50395	Vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Orion Platform. The specific flaw exists within the AppendUpdate method. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries.	https://documentation.solarwinds.com/en/success_center/orionplatform/content/release_notes/solarwinds_platform_2024-1_release_notes.htm
Adobe Audition AVI File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-20739	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Audition. The specific flaw exists within the parsing of AVI files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer.	https://www.tenable.com/plugins/nessus/190458
Adobe Acrobat Pro DC Annotation Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-20728	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Acrobat Pro DC. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	https://www.tenable.com/cve/CVE-2024-20728
Microsoft Windows Internet Shortcut SmartScreen Bypass Vulnerability CVE-2024-21412	Vulnerability allows remote attackers to bypass the SmartScreen security feature to execute arbitrary code on affected installations of Microsoft Windows. The specific flaw exists within the handling of Internet Shortcut (.URL) files.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412
Microsoft Office Word PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-21379	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Microsoft Office Word. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21379
Autodesk AutoCAD STP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Autodesk AutoCAD. The specific flaw exists within the parsing of STP files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0002
X.Org Server DeviceFocusEvent Improper Validation of Array Index Local Privilege Escalation Vulnerability CVE-2023-6816	Vulnerability allows local attackers to escalate privileges on affected installations of X.Org Server. The specific flaw exists within the handling of SetInputFocus requests. The issue results from the lack of proper validation of user-supplied data, which can result in a memory access past the end of an allocated array.	https://access.redhat.com/security/cve/CVE-2023-6816
Centreon updateDirectory SQL Injection Remote Code Execution Vulnerability CVE-2024-0637	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Centreon. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries.	https://access.redhat.com/errata/RHBA-2024:0637
Allegra Hard-coded Credentials Authentication Bypass Vulnerability CVE-2023-22360	Vulnerability allows remote attackers to bypass authentication on affected installations of Allegra. The specific flaw exists within the configuration of a database. The issue results from the use of a hardcoded password.	https://www.trackplus.com/en/service/release-notes-reader/7-5-1-release-notes-2.html

TOP EXPLOITED VULNERABILITIES

Vulnerability Name	Description	References
Oracle Product Lifecycle Management ExportServlet Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2024-20953	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Oracle Product Lifecycle Management. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data.	https://www.oracle.com/security-alerts/cpujan2024verbose.html
Canon imageCLASS MF753Cdw Fax Job Heap-Based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-0244	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Canon imageCLASS MF753Cdw printers. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer.	https://www.canon-europe.com/support/product-security-latest-news/
(Pwn2Own) Lexmark CX331adwe Missing Authentication Remote Code Execution Vulnerability CVE-2023-50737	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Lexmark CX331adwe printers. The issue results from the lack of authentication prior to allowing access to functionality.	https://www.lexmark.com/en_us/solutions/security/lexmark-security-advisories.html
PDF-XChange Editor PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-27327	Vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer.	https://www.pdf-xchange.com/support/security-bulletins.html

Security Bulletin

Local Governments in Colorado, Pennsylvania and Missouri

This week, several local governments have been grappling with ransomware breaches and other intrusions that have disrupted county hospitals, libraries, and other local services.

With a population of about 650,000, Bucks County, Pennsylvania, announced on Wednesday that it is still dealing with a cybersecurity incident that has taken down the computer-aided dispatch (CAD) system of the Emergency Communications Department. The local police, fire, and emergency services departments use it.

According to the New Hope Free Press, the county 911 system, which was unavailable on Sunday, handled emergency calls for roughly 130 departments throughout the county. While using pen and paper to receive and route 911 calls, the technology assists first responders and dispatchers with incident reporting. Officers reported that they were unable to utilize the terminals and applications that are housed inside of vehicles, even though the 911 phone line and first responder radio systems continue to function.

“Our dispatchers will get you the help you need if you call us for an emergency response,” stated Audrey Kenny, director of emergency services for Bucks County. “I want the public and our first responder partners to know that our 911 system is up and running. To support our ongoing investigation, the County has enlisted the help of top-tier incident response specialists and partnered with both state and federal agencies.”

According to those who spoke with New Hope Free Press, the problem was probably a “ransomware-type attack,” since the CAD system contains vast amounts of private data about thousands of individuals and occurrences.

The news site reported that the Pennsylvania National Guard had been called in, but it did not provide an estimated time of arrival for the resolution of the problem. Requests for information regarding whether it was a ransomware assault and whether other county systems were impacted were unanswered by county officials. All the scheduled court dates were rescheduled for Friday.

This week, Washington County, a different Pennsylvanian town, also disclosed a cybersecurity incident. According to the county court system, there are “network outages occurring at this time.”

The Court is being impacted by these interruptions. The court system stated in a statement that during these disruptions, online access to court services and court records may be impacted. The Cybersecurity and Infrastructure Security Agency (CISA) reportedly ordered government officials on Wednesday morning to take down their servers, according to local news outlets.

County Commissioner Nick Sherman told WPXI, “We received confirmation about three in the morning that there was a phishing

expedition taking place on our servers in Washington County. Usually, our IT department is the source of reports like these, but they contacted me to let me know that Homeland Security was the source. Our servers were shut down at that point and remained shut down after that."

There were several additional occurrences this week that municipal governments stated were caused by ransomware. The FBI and other law enforcement agencies were contacted by the Kansas City Area Transportation Authority (KCATA) after they discovered ransomware on Tuesday.

The organization clarified on Wednesday that "the primary customer impact is that calls cannot be received by any KCATA landline or regional RideKC call centers. KCATA will have its systems back up and running as soon as possible. We are working around the clock with our outside cyber professionals."

Operating several bus systems, the public transportation organization handled over 10.5 million rides in 2022, or over 40,000 every day. Equal representation from Kansas and Missouri officials oversees the organization. The organization announced on Wednesday that all its services are still available and gave phone numbers to anybody who needed them.

Another intrusion on Colorado's Douglas County Libraries was likewise caused by ransomware. Recorded Future News was informed by a library representative that they suffered "temporary catalog and service outages" because of a ransomware attack that was first detected on January 14. They took their network offline, impacting several of their services, after finding suspicious behavior.

A spokeswoman added, "We also immediately launched an investigation into the issue with the support of external cybersecurity specialists, and this investigation is still ongoing today. All of our branches are open to customers even though we are working to restore our systems. To the best of our abilities, we will continue to provide the community with first-rate library services throughout these disruptions."

The negotiations are being managed by their cyber insurance firm, according to library officials, who declined to comment to CBS Colorado about whether they intended to pay the ransom.

According to CBS Colorado, the perpetrators of the event were the Play ransomware gang, a worldwide group that has also attacked the Swiss government, Dallas County, Stanley Steemer, a local transit system in Virginia, and a sizable Spanish bank. In December, the FBI and other US agencies announced that since June 2022, the organization was responsible for over 300 successful events.

Microsoft Warns of Widening APT29 Espionage Attacks Targeting Global Orgs

Microsoft said on Thursday that it has started notifying other businesses about the Russian state-sponsored threat actors that were behind a cyberattack on its networks in late November 2023.

The revelation that Hewlett Packard Enterprise (HPE) had been the target of an attack by a hacker group known as APT29—also referred to as BlueBravo, Cloaked Ursa, Cozy Bear, Midnight Blizzard (previously Nobelium), and The Dukes—occured one day prior to this development.

The Microsoft Threat Intelligence team stated in a recent advisory that "this threat actor is known to primarily target governments, diplomatic entities, non-governmental organizations (NGOs), and IT service providers, primarily in the U.S. and Europe."

By keeping footholds for extended periods of time without drawing notice, these espionage missions aim to obtain sensitive information of strategic relevance to Russia.

The most recent revelation suggests that the campaign's scope may have exceeded initial estimates. But the tech behemoth withheld the identities of the other organizations that were targeted.

Using authentic but hacked accounts, APT29 operates covertly by gaining and extending access to a target environment. Additionally, it has been observed to recognize and misuse OAuth applications for post-compromise operations including email collection as well as to travel laterally across cloud infrastructures.

"They utilize diverse initial access methods ranging from stolen credentials to supply chain attacks, exploitation of on-premises environments to laterally move to the cloud, and exploitation of service providers' trust chain to gain access to downstream customers," stated Microsoft.

Using compromised user identities to create, edit, and grant OAuth applications high permissions that they can then abuse to conceal harmful activities is another noteworthy method. The company noted that this allows threat actors to continue having access to applications even if they are unable to access the originally hacked account.

In the end, these malicious OAuth apps are used to target Microsoft business email accounts and authenticate to Microsoft Exchange Online to steal relevant data.

The November 2023 incident that targeted Microsoft saw the threat actor successfully breach a legacy, non-production test tenant account that lacked multi-factor authentication (MFA) by using a password spray assault.

“In this observed Midnight Blizzard activity, the actor tailored their password spray attacks to a limited number of accounts, using a low number of attempts to evade detection and avoid account blocks based on the volume of failures,” added the statement.

Afterward, the hackers used their original access to locate and breach a legacy test OAuth application that provided them with elevated access to the Microsoft corporate network. They then used this compromised application as a weapon to develop more malicious OAuth apps and get the Office 365 Exchange Online full_access_as_app role, which allowed them to access mailboxes.

To hide their origins, these assaults are conducted from a distributed residential proxy architecture. This gives the threat actor access to a large network of IP addresses that are also used by authorized users, which they may use to communicate with both Exchange Online and the compromised tenant.

Organizations must take precautions against rogue OAuth apps and password spraying because Midnight Blizzard’s use of residential proxies to obfuscate connections renders traditional indicators of compromise (IoC)-based detection infeasible due to the high rate of IP address changeover, according to Redmond.

Black Basta Gang Claims the Hack of the UK Water Utility Southern Water

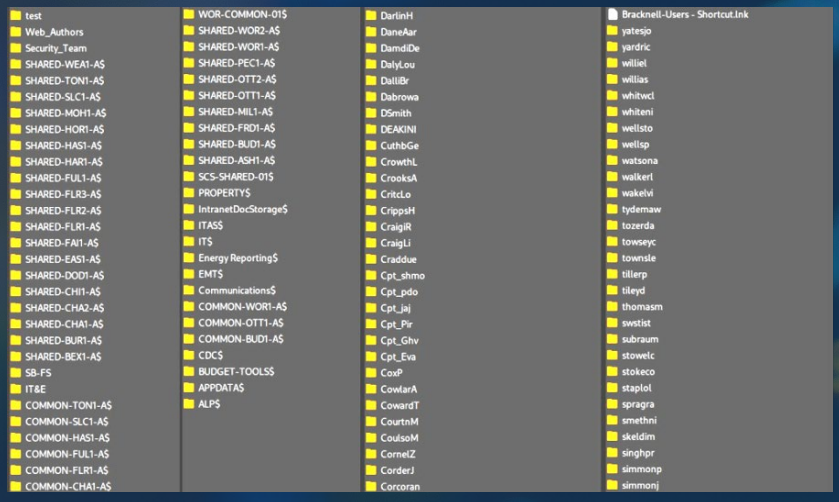
About half of this region receives public water supply from Southern Water, a private utility business that oversees gathering and treating wastewater in Kent, West Sussex, East Sussex, Hampshire, and the Isle of Wight.

The company, which employs over 6,000 people and has an annual revenue of over £1 billion, is a prominent participant in the UK water market. It is dedicated to offering its clients top-notch wastewater and water services.

On its Tor data leak website, the Black Basta ransomware organization listed Southern Water as one of its victims. The group also threatened to release the stolen data on February 29, 2024.

The gang alleges that they have taken 750 gigabytes of sensitive data, including business and personal information from individuals.

The group released a few screenshots showing passports, ID cards, and employee personal information as evidence of the attack.



What ransom the organization has requested from the victim is unknown currently.

Like previous ransomware groups, the Black Basta organization has been operating since April 2022 and employs a double-extortion assault technique.

Early in January, the independent security research and consulting group SRLabs found a flaw in the encryption used by the Black Basta ransomware and used it to generate a free decryptor.

Elliptic and Corvus Insurance conducted a combined study that showed the group had received at least $107 million in Bitcoin ransom payments since the beginning of 2022. ABB, Capita, Dish Network, and Rheinmetall are among the over 329 victims that the ransomware gang has infected, according to the experts.

After examining blockchain transactions, the researchers were able to establish a direct connection between Black Basta and the Conti Group.

The Conti gang stopped operating in 2022, the same year that the Black Basta organization entered the threat environment.

The Russian cryptocurrency exchange Garantex served as the group's primary means of money laundering.

After examining the ransomware's encryption technique, SRLabs found a specific flaw in the version that the gang was using in April 2023. The ransomware performs XOR operations on 64-byte-long segments of the file using encryption based on a ChaCha keystream.

The researchers discovered that, as seen in the ranges, the file size controls the location of the encrypted blocks.py. The first 5000 bytes are encrypted by the ransomware, depending on the size of the file.

The size of the file dictates where the encrypted blocks are located. The ransomware encrypts the first 5,000 bytes, depending on the size of the file.

According to our findings, files may be recovered if the 64 encrypted bytes' plaintext is known. The size of a file determines whether it may be recovered entirely or partially. Files with less than 5000 bytes in size cannot be restored. Complete recovery is achievable for files ranging in size from 5000 bytes to 1GB. The first 5000 bytes of files larger than 1GB will be lost; however, the remaining bytes can be restored.

The recovery depends on deciphering the file's 64 encrypted bytes' plaintext. To put it another way, simply knowing 64 bytes is insufficient since the known plaintext bytes must be in a file location that is encrypted according to the malware's algorithm for figuring out which portions of the file to encrypt. It is possible to determine 64 bytes of plaintext in the correct location for some file types, particularly virtual machine disk images.

The experts noted that the first 5,000 bytes of a file cannot be recovered because the vulnerability has no effect on the encryption operation during this time. This indicates that files smaller than 5000 bytes are not recoverable.

Tools created by SRLabs let users examine encrypted data and assess whether they can be decrypted.

Files containing encrypted zero bytes might be recoverable with the decryptauto tool.

"Manual review is required to fully recover a file, depending on how many times and to what extent the malware encrypted the file," the researchers add.

The issue has been resolved by Black Bast, which is unfortunate. Only files encrypted prior to December 2023 can be recovered with the decryptor.

"Black Basta victims from November 2022 to this month may be able to have their files back for free thanks to the decryptor. But according to researchers, the Black Basta developers repaired the encryption routine problem around a week ago, barring the use of this decryption approach in more recent attacks.

Trello API Abused to Link Email Addresses to 15 Million Accounts

Private email addresses can be linked to Trello accounts using an accessible Trello API, allowing millions of data profiles with both public and private information to be created.

Businesses frequently use Trello, an online project management platform owned by Atlassian, to arrange information and tasks into boards, cards, and lists.

The Trello data leak was made public last week when an individual going by the username "emo" tried to sell 15,115,516 Trello members' data on a well-known hacking site.

It includes full names, emails, usernames, and other account information. 15,115,516 unique lines," the hacker forum post states.

"Selling one copy to whoever wants it, message on me on-site or on telegram if you're interested."

The email addresses connected to these profiles are private, even if practically all of the information in them is available to the public.

When Researchers reached out to Trello over the data leak last week, they informed us that the information was obtained through public data scraping rather than by illegal access to Trello's servers.

The owner of Trello, Atlassian, told Researchers last week that "all evidence points to a threat actor testing a pre-existing list of email addresses against publicly available Trello user profiles."

"Despite performing a thorough examination, we have not discovered any proof of illegal access to user profiles or Trello.

But there seems to be more to the story about the threat actor's method of verifying the email addresses.

Abusing an Exposed API

Researchers learnt through an informal chat that email addresses were linked to public Trello profiles with an openly accessible API.

Trello provides developers with a REST API so they may include the service into their apps. Developers can use a Trello ID or username to inquire for public profile information using one of the API calls.

But emo found out that you can also use an email address to query this API endpoint and, if there's an account linked with it, get the public profile information.

Emo added that anyone may query the API without needing to log into a Trello account or use an API authentication key because it was publicly available.

After compiling a list of 500 million email addresses, the threat actor pushed the data into the API to find out if any of the addresses were linked to a Trello account.

Although Researchers were informed that Trello's API has a rate limit per IP address, the threat actor claimed to have bought proxy servers to switch up connections so they could continuously query the API.

Since then, the API has been strengthened to require authentication, although anyone who registers for a free account can still access it.

In response to Researchers' inquiry about Trello's plans to further secure the API against abuse, Trello released the following statement: "Trello users now have the ability to send email invitations to members or guests for their public boards, thanks to the Trello REST API. We have changed the API, nevertheless, such that unauthenticated users and services are no longer able to email another user to seek their public information due to the abuse of the system that was discovered during this study. This API still allows authenticated users to request publicly accessible data from another user's profile. This modification maintains the functionality of the "invite to a public board by email" feature for our users while also prohibiting API abuse. We'll keep an eye on how the API is being used and take any required action."

Email addresses linked to Trello accounts were intended for account holders alone to know, while scraping publicly available data is typically not a problem because the information was already available.

Thus, the severity of the breach is increased when private information, such an email address, is connected to the public profile.

Furthermore, by pretending to be Trello, this information might be utilized in targeted phishing attacks that steal passwords and other sensitive data.

Threat actors took use of a Twitter API weakness in 2021 to release a similar leak in which users could input phone numbers and email addresses to verify if they were linked to a Twitter ID.

The threat actors combined the public data with associated private email addresses and phone numbers of Twitter users by using another API to scrape the public Twitter data for the ID.

When Twitter resolved this issue in January 2022, it was already too late—more than 200 million Twitter profiles' worth of data had

been compromised by several threat actors.

Massive Cloud Database Leak Exposes 380 Million Records

Cybersecurity researcher Jeremiah Fowler discovered something very concerning: apparently a Zenlayer cloud database breach was left vulnerable and incorrectly configured. The fact that it held an astounding 380 million records of sensitive data is even more startling.

384,658,212 records – 57.46 GB of Database

More investigation on the server turned to a startling discovery. Not only did commonplace details get released, but the information also included internal company operations and, perhaps more worrisome, client information. A staggering 384,658,212 documents, weighing 57.46 GB in total, were made public.

The fact that this data mine wasn't secured by even a simple password is really concerning. It was clearly visible and available to everyone, even those with bad intentions. It was essentially a "come and take it, no questions asked" situation, which left the door open for any threat actors to take advantage of.

Trove of Records Leaked

Numerous servers, error, and monitoring logs that detailed both internal operations and consumer activity were discovered within this database. These logs are essential for tracking server performance, resolving problems, and maintaining system security, but they also pose a risk.

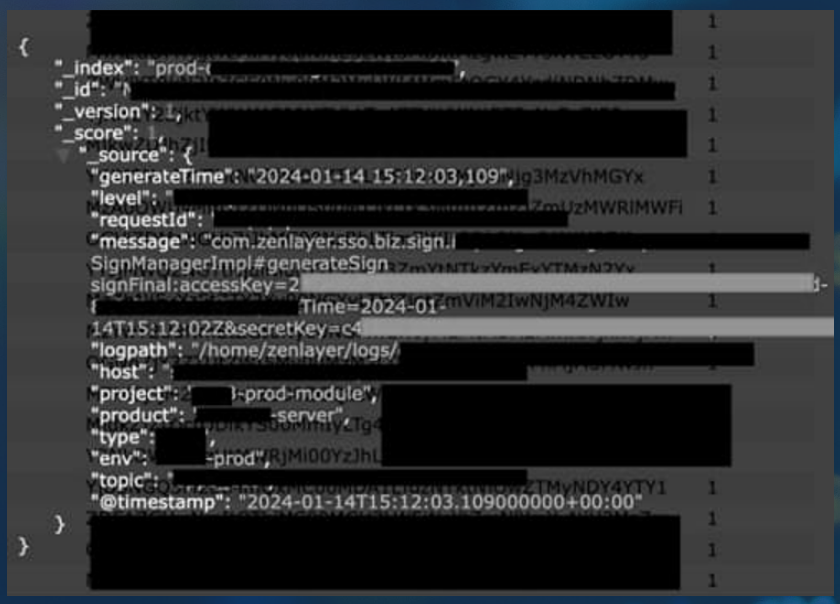
To put it briefly, Zenlayer is a global network services provider that works with major brands in the gaming, telecom, media, entertainment, cloud computing, and blockchain industries. It also offers SD-WAN, CDN, and cloud services. With offices in Shanghai and Los Angeles, the company operates more than 290 data centers on six continents. It was placed third on the list of America's Fastest Growing Telecom Companies by Financial Times in 2021.

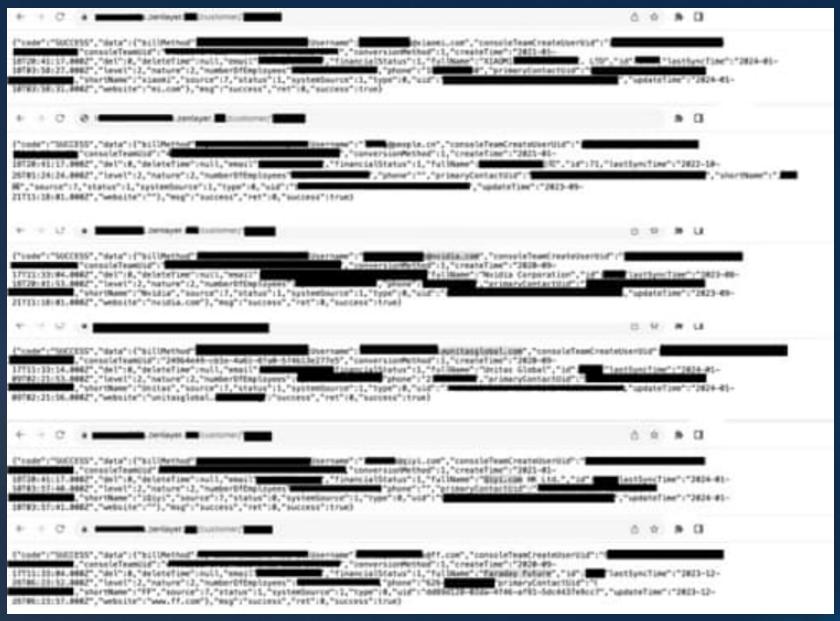
If these logs are made public, private information may be revealed. If misused or accessed by unauthorized parties, what was intended to be a precaution against possible risks and an instrument for improving operational efficiency might soon become a problem.

Logging records for several programs, dashboards, suppliers, notifications, and security were also stored on the server. Targeted phishing attacks or fraudulent actions could be carried out using the exposed customer data, which includes the names and emails of authorized users. Attackers might, for instance, pretend to be Zenlayer salespeople and request bank account information or payment details.

Furthermore, the database leak revealed internal email addresses in addition to sensitive data like user roles. Cybercriminals may find this data to be quite useful in executing social engineering and frauds.

Malicious actors might use these emails to launch phishing attacks directed at workers, which could reveal sensitive information, install malware, and compromise login credentials.





Russian Data

According to Fowler's blog post on Website Planet, some of the records included information from a Russian telecom carrier company that was partially owned by a state-controlled entity that was sanctioned. The company was suspected of being involved in BGP (Border Gateway Protocol) hijacking, which is the process by which attackers can intercept, examine, or alter network traffic.

Fowler made it clear that he wasn't asserting that the BGP hijacking included a Zenlayer client.

Additionally, Fowler found logs with VPN records and many IP addresses, such as PXE IPMI, IP LAN, and controller host IP, and controller IP. These IPs might make the internal network architecture of the company visible, which might help hackers map the network, find targets, or organize more cyberattacks.

However, the day following Fowler's notification of Zenlayer, public access was blocked. The database's management, duration of exposure, and potential third-party access are all unknown. Zenlayer may have been the only one with access to it.

Fortunately, the administrators were able to secure the exposed database in less than a day because of Fowler's timely and responsible disclosure. Even with this prompt response, the researcher's efforts were not acknowledged or acknowledged by the corporation. Consequently, it is still unclear if Zenlayer managed the database directly or if it was managed by a different entity.

"We have fixed the problem, are in contact with the researcher who first found the data leak and are aware of the data breach. Further details will be provided after the investigation is finished."

REFERENCE LINKS

- https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira
- https://www.bleepingcomputer.com/news/security/meet-akira-a-new-ransomware-operation-targeting-the-enterprise/
- https://news.sophos.com/en-us/2023/12/21/akira-again-the-ransomware-that-keeps-on-taking/
- https://therecord.media/local-governments-across-us-dealing-with-ransomware?&web_view=true
- https://thehackernews.com/2024/01/microsoft-warns-of-widening-apt29.html?&web_view=true
- https://securityaffairs.com/157951/cyber-crime/black-basta-gang-claims-the-hack-of-the-uk-water-utility-southern-water.html?web_view=true
- https://www.bleepingcomputer.com/news/security/trello-api-abused-to-link-email-addresses-to-15-million-accounts/?&web_view=true
- https://www.hackread.com/massive-cloud-database-leak-exposes-380-records/?web_view=true
- https://www.trendmicro.com/en_us/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html
- https://www.bleepingcomputer.com/news/security/americans-lost-record-10-billion-to-fraud-in-2023-ftc-warns/?&web_view=true
- https://www.helpnetsecurity.com/2024/02/09/identity-fraud-growth/?web_view=true
- https://www.darkreading.com/endpoint-security/qr-code-quishing-attacks-execs-email-security?&web_view=true
- https://www.bleepingcomputer.com/news/security/ransomware-payments-reached-record-11-billion-in-2023/
- https://securityaffairs.com/157933/breaking-news/largest-data-leak-ever.html?web_view=true
- https://thehackernews.com/2024/01/tech-giant-hp-enterprise-hacked-by.html?&web_view=true
- https://www.hackread.com/russian-hackers-mail-servers-europe-intel/
- https://thehackernews.com/2024/02/russian-linked-hackers-breach-80.html
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
- https://www.bleepingcomputer.com/news/security/chinese-hackers-hid-in-us-infrastructure-network-for-5-years/#google_vignette

About SDG

SDG is a global cybersecurity, identity governance, GRC, risk consulting and advisory firm. SDG's SaaS platform TruOps in combination with its services deliver a comprehensive range of identity, cybersecurity, risk, compliance, and cloud security solutions that enable organizations to identify and mitigate cyber risk, protect cyber assets, and manage their business securely.

To learn how SDG can help ensure the security and compliance of your technology and data infrastructure visit **www.sdgc.com** and **www.truops.com**.

SDG

75 North Water Street
Norwalk, CT 06854

203.866.8886

sdgc.com