Cyber Threat Advisory

MAY 2024

Contents

Monthly Highlights - May

1. **AT&T Confirms Data for 73 Million Customers Leaked on Hacker Forum** – AT&T has confirmed being affected by a data breach involving 73 million current and former customers, reversing its initial denial that the leaked data came from their systems.

   Despite AT&T's previous denials over the past two weeks, the company now acknowledges that a significant amount of customer data was leaked, impacting 73 million individuals. The leaked data includes information from approximately 7.6 million current AT&T account holders and about 65.4 million former account holders.

   AT&T stated that the leaked dataset appears to be from 2019 or earlier. The company also revealed that security passcodes for 7.6 million customers were compromised.

   The breach was first publicized in 2021 by a threat actor known as Shiny Hunters, who claimed to have stolen data from 73 million AT&T customers. In 2024, another threat actor leaked the same dataset on a hacking forum, confirming it was the data stolen by Shiny Hunters. Bleeping Computer verified the data and found it contained sensitive information such as names, addresses, phone numbers, social security numbers, and birth dates.

   Following the leak, Bleeping Computer interviewed over 50 AT&T and DirectTV customers who confirmed that the leaked data included information specific to their AT&T accounts. These customers reported using disposable email

addresses from Gmail and Yahoo, which were only used for their DirectTV or AT&T accounts, indicating that the leaked data likely originated from DirectTV or AT&T.

Troy Hunt, creator of Have I Been Pwned, also confirmed the authenticity of the leaked data. DirectTV, which has spun off from AT&T, directed inquiries to AT&T, as they no longer have access to AT&T systems to verify the data.

AT&T has stated that it will only provide further information about the breach through its official statements and a new page dedicated to securing AT&T accounts. The company has reset the passcodes for the affected 7.6 million customers and emphasized the importance of these passcodes for securing their accounts. Customers use these passcodes for customer support, managing accounts at retail stores, and accessing online accounts.

2. **Apple Fans Deluged with Phony Password Reset Requests** – Apple device owners, take heed: a targeted campaign using multi-factor authentication (MFA) bombing is underway, aiming to wear down users into unwanted password resets.

   Initially highlighted by AI entrepreneur Parth Patel on Twitter and later confirmed by security blogger Brian Krebs, the campaign appears directed at specific individuals who receive an overwhelming number of password reset requests. Patel noted that since the alerts are sent at the system level, he had to clear each one individually before he could access his iPhone, Apple Watch, or MacBook. Patel had to dismiss over 100 notifications, a volume echoed by several of his friends and other victims identified by Krebs.

   This attack resembles other MFA fatigue attacks seen over the years, designed to tire users into inadvertently permitting a password change or doing so to halt the flood of requests. Microsoft adjusted how its MFA codes operate due to such abuses, but Apple has not made similar changes yet. Nevertheless, the attackers in this case displayed sophistication beyond mere spamming. Approximately 15 minutes after clearing the notifications, Patel received a call from someone posing as an Apple support representative using a spoofed caller ID. The caller claimed Patel's account was under attack and asked for verification of his information, including a one-time reset code. Suspicious, Patel requested verification of some personal details, and the caller was mostly able to provide accurate information, including Patel's date of birth, email, phone number, and current and past addresses.

   Patel, who regularly monitors his online presence, recognized that the data likely came from PeopleDataLabs, a B2B information firm, as he recalled being confused with an elementary school teacher named Anthony S. from the Midwest in their database. This realization confirmed to Patel that the call was a scam.

   The scammer's direct call suggests they were able to exploit Apple's iForgot page—which only requires an email address, a solved CAPTCHA, and the account's phone number—to submit a password reset request. The high volume of requests raises concerns about a potential rate-limiting flaw in Apple's iForgot system, which may allow for repeated bombardment of users with reset requests. Apple did not address these questions directly but directed users to a support page on recognizing scams and phishing attempts targeting Apple users.

3. **73% Brace for Cybersecurity Impact on Business in the Next Year or Two** – According to Cisco, only 3% of organizations worldwide have achieved the 'mature' level of readiness required to withstand modern cybersecurity threats. Despite facing a range of attacks such as phishing, ransomware, supply chain, and social engineering, companies struggle to defend against them. This challenge is compounded by their complex security setups, dominated by multiple-point solutions.

   Despite these challenges, 80% of companies remain moderately to very confident in their ability to defend against cyberattacks with their current infrastructure. This discrepancy between confidence and readiness suggests a potential overestimation of their ability to handle cyber threats.

   Jeetu Patel, EVP and GM of Security and Collaboration at Cisco, emphasized the danger of overconfidence, stating that organizations need to prioritize integrated platforms and leverage AI to operate at scale and shift the advantage to defenders.

   The survey found that 73% of respondents expect a cybersecurity incident to disrupt their business in the next 12 to 24 months. Being unprepared can lead to substantial costs, with 54% reporting a cybersecurity incident in the last year, costing at least $300,000 for 52% of those affected.

   The traditional approach of using multiple cybersecurity point solutions has not been effective, with 80% of respondents noting that it slowed down their team's ability to detect, respond, and recover from incidents. Despite this, 67% of organizations have deployed ten or more-point solutions, and 25% have 30 or more.

   Additionally, 85% of companies reported that their employees access company platforms from unmanaged devices, with 43% spending 20% of their time logged in from such devices. Furthermore, 29% stated that their employees switch between at least six networks in a week.

Critical talent shortages are further hindering progress, with 87% of companies citing this as an issue. Nearly half (46%) reported having more than ten unfilled cybersecurity roles in their organization at the time of the survey.

To address these challenges, organizations are planning significant upgrades to their IT infrastructure, with 52% planning to do so in the next 12 to 24 months, up from 33% last year. Plans include upgrading existing solutions (66%), deploying new solutions (57%), and investing in AI-driven technologies (55%). Additionally, 97% of companies plan to increase their cybersecurity budget in the next year, with 86% expecting an increase of 10% or more.

To overcome these challenges, companies need to accelerate investments in security, adopt innovative security measures and a security platform approach, strengthen network resilience, make meaningful use of generative AI, and increase recruitment to address the cybersecurity skills gap.

4. **22,500 Palo Alto Firewalls "Possibly Vulnerable" to Ongoing Attacks** – Around 22,500 Palo Alto GlobalProtect firewall devices have been found to be exposed and likely vulnerable to the critical CVE-2024-3400 flaw, which is a command injection vulnerability that has been actively exploited in attacks since at least March 26, 2024.

   CVE-2024-3400 affects specific versions of Palo Alto Networks' PAN-OS in the GlobalProtect feature, allowing unauthenticated attackers to execute commands with root privileges by triggering command injection through arbitrary file creation. Palo Alto Networks disclosed the flaw on April 12 and advised system administrators to immediately apply provided mitigations until a patch was available. Patches were released between April 14 and 18, 2024, depending on the PAN-OS version, limiting the exposure to post-disclosure risks to two to six days. It was later discovered that Palo Alto's mitigation of disabling telemetry was insufficient, and the only effective solution was to apply the security patches.

   Researchers at Volexity, who first identified the exploitation, revealed that state-backed threat actors known as 'UTA0218' used the flaw to infect systems with a custom backdoor named 'Upstyle.'

   Recently, researchers shared technical details and a proof-of-concept exploit for CVE-2024-3400, demonstrating how unauthenticated attackers could easily execute commands as root on unpatched endpoints. The availability of the exploit has led to numerous threat actors conducting their own attacks, leaving system administrators with no room for delaying patching.

   Greynoise's scanners confirmed an increase in exploitation, with a larger number of unique IP addresses attempting to exploit the CVE-2024-3400 flaw. Despite the urgency, the ShadowServer Foundation threat monitoring service reported approximately 22,500 instances that are still "possibly vulnerable" as of April 18, 2024.

   Most of the exposed devices are located in the United States (9,620), followed by Japan (960), India (890), Germany (790), the UK (780), Canada (620), Australia (580), and France (500).

   Earlier, Shadow Server reported over 156,000 PAN-OS firewall instances exposed on the internet without specifying how many might be vulnerable. Last week, threat researcher Yutaka Sejiyama conducted scans and observed 82,000 vulnerable firewalls, potentially accounting for 73% of all exposed PAN-OS systems being patched within a week.

   For those who have not acted, it is advised to follow the recommendations in the Palo Alto security advisory, which has been updated several times with new information and instructions on detecting suspicious activity.

5. **Hackers Exploit Fortinet Flaw, Deploy ScreenConnect, Metasploit in New Campaign** – A recent cybersecurity investigation has unveiled a fresh campaign exploiting a newly disclosed security vulnerability in Fortinet FortiClient EMS devices to deploy ScreenConnect and Metasploit Powerfun payloads.

   The campaign revolves around exploiting CVE-2023-48788 (CVSS score: 9.3), a critical SQL injection flaw that could enable the unauthorized execution of code or commands by an unauthenticated attacker through meticulously crafted requests.

   Cybersecurity company Forescout has dubbed the campaign Connect:fun due to the utilization of ScreenConnect and Powerfun for post-exploitation activities.

   The breach targeted an unnamed media company whose vulnerable FortiClient EMS device was exposed to the internet, occurring shortly after the publication of a proof-of-concept (PoC) exploit for the flaw on March 21, 2024.

   In the subsequent days, the unidentified threat actor unsuccessfully attempted to download ScreenConnect and later resorted to installing the remote desktop software using the msiexec utility. However, by March 25, the PoC exploit was employed to execute PowerShell code, downloading Metasploit's Powerfun script and establishing a reverse connection to another IP address.

   Additionally, SQL statements were identified, aimed at downloading ScreenConnect from a remote domain ("ursketz[.]com") using

certutil, subsequently installed via msiexec before connecting to a command-and-control (C2) server.

There are indications that the threat actor behind the campaign has been active since at least 2022, showing a preference for targeting Fortinet appliances and employing Vietnamese and German languages in their infrastructure.

Security researcher Sai Molige noted that the observed activity exhibited a manual component, evident from the failed attempts to download and install tools, along with the considerable time intervals between attempts. This suggests a targeted campaign rather than automated exploitation by cybercriminal botnets.

Forescout highlighted tactical and infrastructure similarities between this attack and other incidents documented by Palo Alto Networks Unit 42 and Blumira in March 2024, involving the exploitation of CVE-2023-48788 to download ScreenConnect and Atera.

Organizations are advised to apply patches provided by Fortinet, monitor for suspicious traffic, and employ a web application firewall (WAF) to thwart potentially malicious requests.

6. **Cisco Warns of Global Surge in Brute-Force Attacks Targeting VPN and SSH Services** – Cisco has issued a warning regarding a global increase in brute-force attacks targeting various devices, including Virtual Private Network (VPN) services, web application authentication interfaces, and SSH services, starting from at least March 18, 2024.

   According to Cisco Talos, these attacks are originating from TOR exit nodes and a variety of other anonymizing tunnels and proxies. If successful, these attacks could lead to unauthorized network access, account lockouts, or denial-of-service conditions.

   The attacks are described as broad and opportunistic, with the following devices being targeted:

   - Cisco Secure Firewall VPN
   - Checkpoint VPN
   - Fortinet VPN
   - SonicWall VPN
   - RD Web Services
   - Mikrotik
   - Draytek
   - Ubiquiti

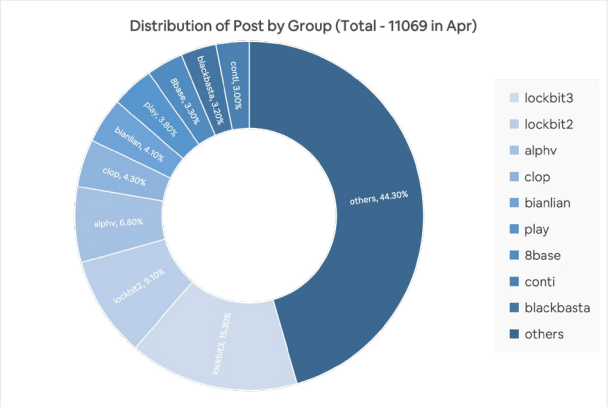
   Cisco Talos noted that the brute-force attempts involve both generic and valid usernames for specific organizations, indiscriminately targeting a wide range of sectors across different regions.

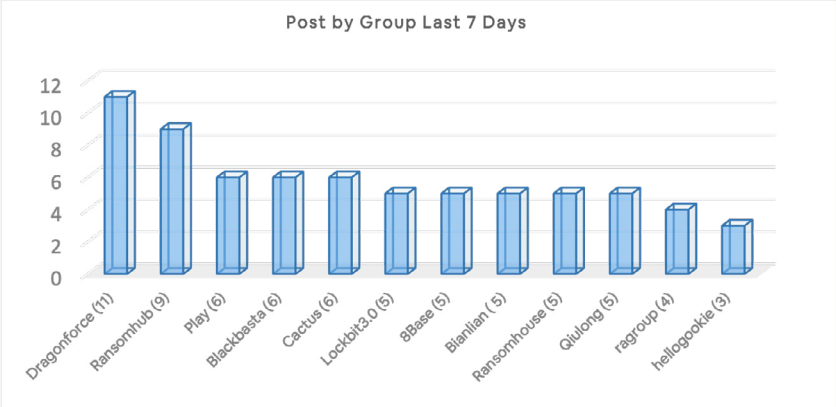
   The source IP addresses for the attacks are frequently associated with proxy services, including TOR, VPN Gate, IPIDEA Proxy, BigMama Proxy, Space Proxies, Nexus Proxy, and Proxy Rack, among others.

   This development coincides with Cisco's earlier warning about password spray attacks targeting remote access VPN services as part of reconnaissance efforts. Additionally, Fortinet FortiGuard Labs reported that threat actors are exploiting a now-patched security flaw affecting TP-Link Archer AX21 routers (CVE-2023-1389, CVSS score: 8.8) to distribute DDoS botnet malware families such as AGoent, Condi, Gafgyt, Mirai, Miori, and MooBot.

   Security researchers Cara Lin and Vincent Li emphasized the importance of vigilance against DDoS botnets and prompt application of patches to protect network environments from infection and to prevent them from being exploited by malicious actors.

Ransomware Tracker





Threat Group FIN7 Targets the U.S. Automotive Industry

The Anunak backdoor was introduced into systems by the financially motivated threat actor FIN7, who used spear-phishing emails to target IT department staff at a major American automaker.

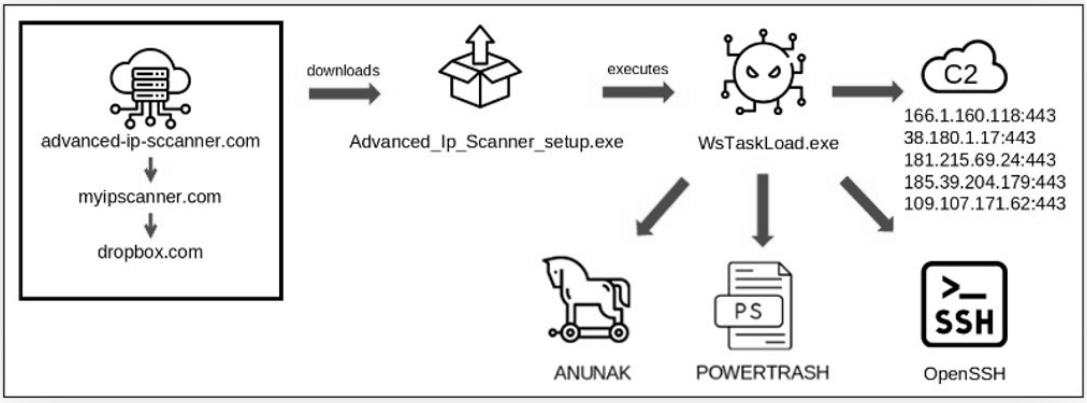
The attack occurred late last year, and living-off-the-land binaries, scripts, and libraries (LoLBas) were used, according to BlackBerry researchers. Targets with elevated levels of access were the primary focus of the threat actor, who enticed them with links to a malicious URL that mimicked the official Advanced IP Scanner tool.

The use of distinct PowerShell scripts that utilized the adversary's signature 'PowerTrash' obfuscated shellcode invoker—first observed in a 2022 campaign—led BlackBerry to confidently attribute the attacks to FIN7.

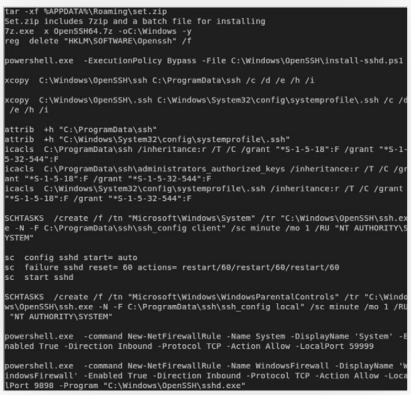
In addition to installing the ransomware payloads for Black Basta and Clop on corporate networks, FIN7 was observed targeting Microsoft Exchange servers and exposed Veeam backup servers.

Detection:

- The spear-phishing emails that FIN7 used to launch their attack were directed toward highly privileged workers in the IT department of a major American automaker.
- Email links would direct recipients to "advanced-ip-scanner[.]com," which is a misspelling of the actual scanner project located at "advanced-ip-scanner.com."
- The phony website, the researchers found, redirected to "myipscanner[.]com" (which is currently unavailable). The next screen that the visitor would see would be a Dropbox page that offered a malicious executable (called "WsTaskLoad.exe") that was posing as the official Advanced IP Scanner installer.
- After the file is run, it starts a multi-step process that includes shellcode execution, WAV files, and DLLs. This process loads and decrypts a file called "dmxl.bin," which holds the Anunak backdoor payload.



- FIN7 uses several malware tools, including Diceloader, Griffon, PowerPlant, Loadout, and Anunak/Carbanak.
- In addition to installing OpenSSH for persistent access, WsTaskLoad.exe also creates a scheduled task. BlackBerry claims that while FIN7 has used OpenSSH for lateral movement in the past, they did not see this in the campaign they examined.



IoCs (Indicators of Compromise):

Hashes (md5, sha-256)	87aa5f3f514af2b9ef28db9f092f3249
ITW File Name	ff4c287c60ede1990442115bddd68201d25a735458f76786a938a0aa881d14ef
Compilation Stamp	Advanced_Ip_Scanner_setup.exe
File Type/	2022-04-14 16:10:23 UTC
Signature	Win32 EXE
File Size	18155592
Compiler Name/Version	Embarcadero Delphi (10.3 Rio) [Professional]
Installer Name	Inno Setup Module (6.1.0) [unicode]
Hashes (md5, sha-256)	bb23dde1e3ecef7d93a39e77e32ef96c d63060e61c98074c58926a6239185e8128fd0fbc2a45ccf60f3c831bb18ffc93
ITW File Name	WsTaskLoad.exe
Compilation Stamp	2018-10-10 03:56:59 UTC
File Type/Signature	Win32 EXE
File Size	2234880
Compiler Name/Version	Embarcadero Delphi (2009)

Domain/IP	String	Type
Domain	advanced-ip-sccanner[.]com	Delivery
Domain	myipscanner[.]com	Delivery
Domain	theipscanner[.]com	Delivery
Domain	ipscanneronline[.]com	Delivery
Domain	ipscannershop[.]com	Delivery
Domain	myscannappo[.]com	Delivery
Domain	myscannappo[.]info	Delivery
Domain	myscannappo[.]online	Delivery
IP	181[.]215.69[.]24	C2
IP	166[.]1.160[.]118	C2
IP	185[.]39.204[.]179	C2
IP	109[.]107.171[.]62	C2
IP	38[.]180.1[.]17	C2
IP	109[.]107.170[.]47	SSH Proxy
IP	162[.]248.224[.]79	SSH Proxy
IP	166[.]1.190[.]171	SSH Proxy
IP	166[.]1.190[.]186	SSH Proxy
IP	172[.]82.87[.]69	SSH Proxy
IP	185[.]161.210[.]18	SSH Proxy
IP	185[.]72[.]8.6	SSH Proxy
IP	185[.]72.8[.]70	SSH Proxy
IP	193[.]233.206[.]146	SSH Proxy

Domain/IP	String	Type
IP	207[.]174.31[.]205	SSH Proxy
IP	207[.]174.31[.]206	SSH Proxy
IP	209[.]209.113[.]91	SSH Proxy
IP	217[.]196.101[.]116	SSH Proxy
IP	38[.]180.14[.]240	SSH Proxy
IP	38[.]180.40[.]23	SSH Proxy
IP	46[.]246.98[.]196	SSH Proxy
IP	5[.]181.159[.]11	SSH Proxy
IP	62[.]233.57[.]98	SSH Proxy
IP	104[.]166.127[.]197	SSH Proxy - Moderate Confidence Relation
IP	104[.]166.127[.]200	SSH Proxy - Moderate Confidence Relation
IP	155[.]254.192[.]66	SSH Proxy - Moderate Confidence Relation
IP	166[.]1.190[.]48	SSH Proxy - Moderate Confidence Relation
IP	185[.]72.8[.]147	SSH Proxy - Moderate Confidence Relation
IP	193[.]233.22[.]136	SSH Proxy - Moderate Confidence Relation
IP	193[.]233.22[.]28	SSH Proxy - Moderate Confidence Relation
IP	193[.]233.22[.]36	SSH Proxy - Moderate Confidence Relation
IP	193[.]233.22[.]43	SSH Proxy - Moderate Confidence Relation
IP	193[.]233.23[.]177	SSH Proxy - Moderate Confidence Relation
IP	207[.]174.31[.]253	SSH Proxy - Moderate Confidence Relation
IP	23[.]133.88[.]52	SSH Proxy - Moderate Confidence Relation
IP	38[.]180.1[.]103	SSH Proxy - Moderate Confidence Relation
IP	38[.]180.20[.]94	SSH Proxy - Moderate Confidence Relation
IP	5[.]61.39[.]157	SSH Proxy - Moderate Confidence Relation
IP	5[.]8.63[.]105	SSH Proxy - Moderate Confidence Relation
IP	5[.]8.63[.]108	SSH Proxy - Moderate Confidence Relation
IP	5[.]8.63[.]139	SSH Proxy - Moderate Confidence Relation
IP	5[.]8.63[.]245	SSH Proxy - Moderate Confidence Relation
IP	62[.]233.57[.]195	SSH Proxy - Moderate Confidence Relation
IP	91[.]149.254[.]85	SSH Proxy - Moderate Confidence Relation

Prevention:

- Implement multi-factor authentication (MFA) on all user accounts
- Provide proper training so employees can steer away from malicious lures
- Use strong & unique passwords
- Must change password within 45 days
- Keep all software updated
- Monitor the network for suspicious behavior
- Add advanced email filtering technique

Remediation:

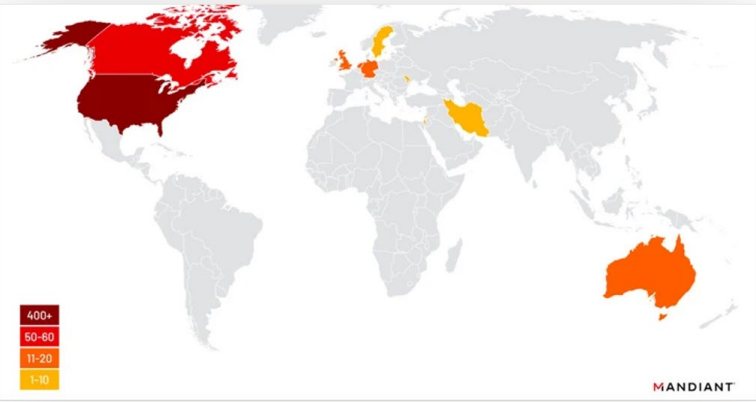
- Enable data protection and encryption procedure
- Apply email filtering and data authentication technique
- Keep active incident response team
- Implement monitoring tool to detect suspicious behavior
- Apply endpoint security policies
- Apply security updates every month and patch their systems
- Enable multi-factor authentication for every account

China-Linked Group Breaches Networks via Connectwise, F5 Software Flaws

- In an “aggressive” campaign, a China-linked threat cluster took advantage of security holes in the F5 BIG-IP and Connectwise ScreenConnect software to deliver custom malware that could open more backdoors on compromised Linux hosts.
- Mandiant, which is owned by Google, is monitoring the activity under the uncategorized moniker UNC5174, also known as Uteus or Uetus. It describes the activity as coming from a former member of Chinese hacktivist groups, but it also appears that it is acting as a contractor for China’s Ministry of State Security (MSS), primarily carrying out access operations.
- The threat actor is thought to have used the ScreenConnect bug to plan extensive attacks against research and education institutions in Southeast Asia and the United States, as well as businesses, nonprofits, and non-governmental organizations (NGOs) in Hong Kong, between October and November 2023 and again in February 2024.

Detection:

- Exploiting known security vulnerabilities in Atlassian Confluence (CVE-2023-22518), ConnectWise ScreenConnect (CVE-2024-1709), F5 BIG-IP (CVE-2023-46747), Linux Kernel (CVE-2022-0185), and Zyxel (CVE-2022-3052) makes it easier to gain initial access to target environments.
- After gaining a foothold, UNC5174 conducts thorough reconnaissance and scans internet-facing systems for security flaws. Additionally, it creates administrative user accounts with elevated privileges to carry out malicious operations, such as releasing the C-based ELF downloader SNOWLIGHT.
- The goal of SNOWLIGHT is to communicate with SUPERSHELL, an open-source command-and-control (C2) framework that enables attackers to create a reverse SSH tunnel and start interactive shell sessions to run arbitrary code and download the next-stage payload, an obfuscated Golang backdoor called GOREVERSE, from a remote URL.
- The threat actor also uses other programs such as afrog, DirBuster, Metasploit, Sliver, sqlmap, and GOHEAVY, a Golang-based tunneling tool that is likely used to allow lateral movement within compromised networks.



- The threat actors have been observed applying mitigations for CVE-2023-46747 in an uncommon occurrence noticed by the threat intelligence firm. This is probably an attempt to stop other unrelated adversaries from weaponizing the same loophole to gain access.
- UNC5174 (also known as Uteus) has worked with “Genesis Day” / “Xiaoqiying” and “Teng Snake,” and was formerly a part of the Chinese hacktivist collectives “Dawn Calvary,” according to Mandiant. It seems that this person left these groups in the middle of 2023 and has since concentrated on carrying out access operations in order to facilitate access to compromised environments.
- The threat actor’s purported claims in dark web forums provide evidence that they are the MSS’s ally and could be an initial access agent. This is supported by the fact that another access broker known as UNC302 concurrently targeted a few U.S. defense and U.K. government entities.
- The results highlight the ongoing efforts by Chinese nation-state groups to compromise edge appliances by quickly obtaining newly discovered vulnerabilities and zero-days for their arsenal, allowing them to carry out large-scale cyber espionage operations.
- Following the CVE-2023-46747 exploitation, Mandiant researchers reported that in late 2023, UNC5174 was seen attempting to sell access to appliances used by U.S. defense contractors, U.K. government agencies, and institutions in Asia.
- UNC5174 and UNC302 are similar, indicating that they function in an MSS initial access broker environment. These resemblances point to potential exploits and operational priorities that these threat actors have in common, but more research is needed to establish attribution with certainty.

Indicators of Compromise (IOCs):

Network IOCs

IP Address	ASN	NetBlock	Location
118.140.151[.]242	9304	HGC Global Communications Limited	(HK)
61.239.68[.]73	9269	Hong Kong Broadband Network Ltd.	(HK)
172.245.68[.]110	36352	Colocrossing	(U.S.)

URLs

URL	Description
http://172.245.68[.]110:8888	9304

Host IOCs

MD5 Hash	Filename	Type	Code family
c867881c56698f938b4e8edafe-76a09b	LG	ELF	SNOWLIGHT
df4603548b10211f0aa-77d0e9a172438	N/A	ELF	SNOWLIGHT
0951109dd1be0d84a33d52c-135ba9c97	N/A	ELF	SNOWLIGHT
9c3bf506dd19c08c0ed3af-9c1708a770	memfd:a	ELF	N/A
0ba435460fb7622344eec-28063274b8a	undefined	ELF	SNOWLIGHT
a78bf3d16349e-ba86719539ee8ef562d	N/A	ELF	SNOWLIGHT

Host Based Indicators (Commands)

```
cmd_data=run util bash -c "echo dG1zaCAtcSAtYyAnY2QgLztzaG93IHJ1bm5pbmctY29uZmlnIHJlY3Vyc2l2ZSc= | base64 -d | sh"  "tmsh -q -c 'cd /;show running-config recursive'"
```

Prevention:

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 levels
7. Disable all user accounts and access to organizational resources of 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

Remediation:

1. Restrict access to the F5 TMUI from the internet
2. Immediately apply the F5 mitigation script published in [K000137353] to any vulnerable F5 appliances
3. Investigate vulnerable F5 appliances for evidence of compromise
4. Review appliance configurations for unauthorized modifications
5. Review file system and operating system (OS) artifacts for evidence of privileged account creation and remove any unauthorized accounts
6. Consider revoking and re-issuing sensitive cryptographic material such as certificates and private keys

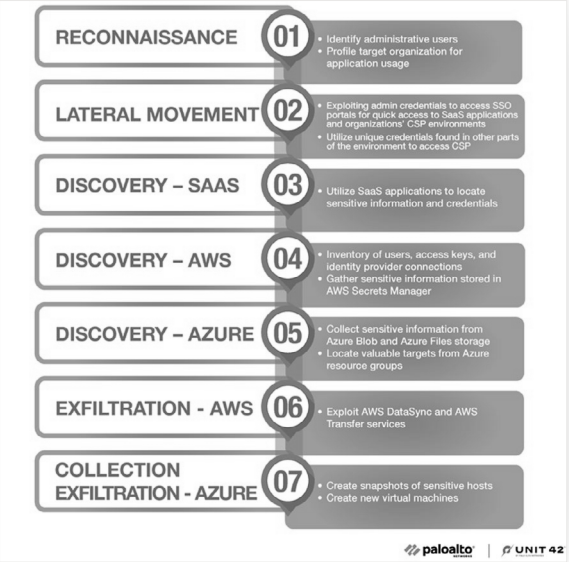
Muddled Libra Shifts Focus to SaaS and Cloud for Extortion and Data Theft Attacks

- Muddled Libra is a threat actor that has been seen aggressively targeting cloud service provider (CSP) environments and software-as-a-service (SaaS) applications to steal confidential information.
- Businesses frequently use CSP services and store a range of data in SaaS applications, according to a report released last week by Palo Alto Networks Unit 42.
- Threat actors have started attempting to use this data to help advance their attacks and to extort payment for their labor.
- Muddled Libra is a well-known cybercrime organization that has used advanced social engineering techniques to obtain initial access to target networks. It is also known by the names Scatter Swine, Scattered Spider, Starfraud, and UNC3944.

Detection:

- The U.S. government stated in an advisory late last year that Scattered Spider threat actors have historically avoided detection on target networks by navigating victim networks using allowlisted applications and living off the land techniques—and by regularly changing their TTPs. Additionally, the attackers have a track record of making money off victim networks through a variety of means, such as ransomware-enabled extortion and data theft.
- There is overlap between the intrusion cluster and The Com, a larger cybercriminal gang involved in swatting attacks, real-world violence, cryptocurrency theft, and subscriber identity module (SIM) swapping.
- The designation “Muddled Libra” originates from the “confusing muddled landscape” linked to the 0ktapus phishing kit, which has been exploited by other threat actors to carry out credential harvesting attacks, as Unit 42 previously told The Hacker News. The use of reconnaissance techniques to identify administrative users that attackers target when assuming the identity of helpdesk staff and making phone calls to obtain their passwords is a crucial component of the threat actor’s tactical evolution. As part of the recon phase, Muddled Libra also conducts in-depth research to learn more about the cloud service providers and applications that the target organizations use.

- Security researcher Margaret Zimmermann explained that the Okta cross-tenant impersonation attacks that took place in late July to early August 2023, where Muddled Libra evaded IAM restrictions, show how the group uses Okta to access SaaS applications and an organization's multiple CSP environments.
- By using the admin credentials to access single sign-on (SSO) portals and quickly access cloud infrastructure and SaaS applications, the information acquired at this point can be leveraged to carry out lateral movement.
- In the case that SSO is not integrated into a target's CSP, Muddled Libra conducts extensive discovery operations to find the CSP credentials, which are likely kept in unsecured locations, to achieve their goals. SaaS application data is also utilized to extract details about the compromised system and collect as many credentials as possible to expand the breach's scope through lateral movement and privilege escalation.
- Afterwards, attackers can create new vectors for lateral movement inside an environment. Organizations' distinct CSP environments house a wide range of data, which makes these centralized areas a prime target for Muddled Libra.



- The discovery actions specifically target Microsoft Azure and Amazon Web Services (AWS) to extract pertinent data, targeting services like AWS IAM, Amazon Simple Storage Service (S3), AWS Secrets Manager, Azure storage account access keys, Azure Blob Storage, and Azure Files.
- The process of data exfiltration involves the misuse of authorized CSP features and services. This includes services and products such as Amazon DataSync, Amazon Transfer, and the technique known as snapshot, which allows data to be moved out of an Azure environment by staging the stolen data in a virtual machine.

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 of 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:

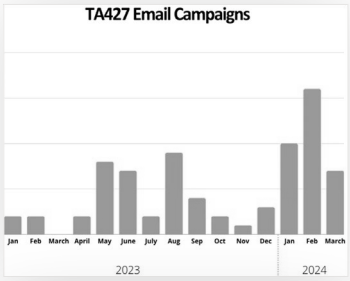
1. Implement network segmentation to isolate federation servers
2. Revoke unnecessary public access to the cloud environment
3. Ensure logging is turned on for application, access, and security logs
4. Store logs in a central system
5. Document a list of threats and cyber actor TTPs relevant to your 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

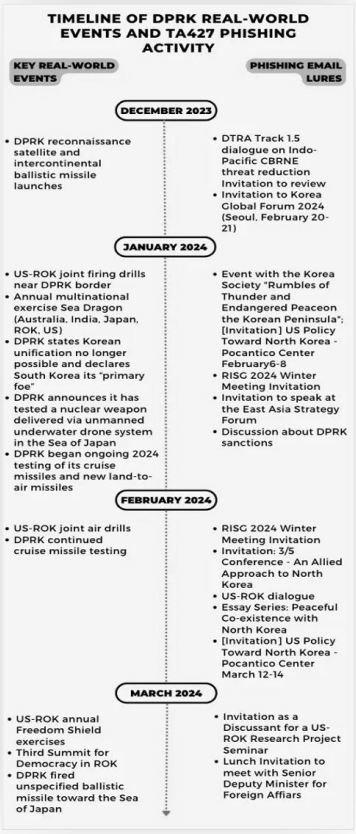
From Social Engineering to DMARC Abuse: TA427's Art of Information Gathering

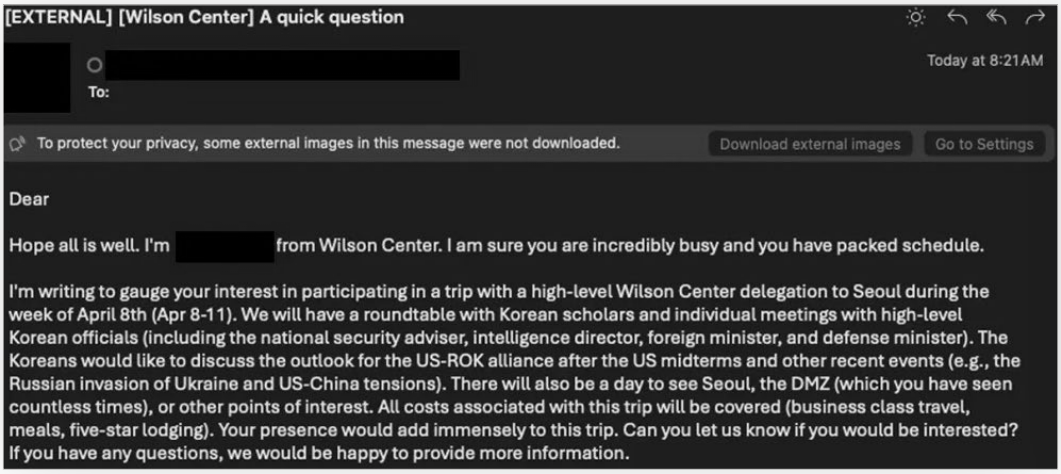
- Cybercriminals target DMARC because it acts as a defense against phishing and email spoofing attempts. They get around email authentication protocols by breaking into Domain-based Message Authentication Reporting and Conformance (DMARC). This allows them to impersonate legitimate senders and trick recipients. They can create more plausible and beneficial phishing campaigns in this way, which can result in data theft or profit.
- ProofPoint's cybersecurity researchers have found that North Korean hackers are actively abusing the DMARC to validate their illegal emails.

Detection:

- Proofpoint monitors the North Korean state-aligned group TA427 (also known as Emerald Sleet, APT43, THALLIUM, Kimsuky), which works for the Reconnaissance General Bureau and conducts phishing campaigns against experts on U.S. and South Korean foreign policy.
- Through innocent conversation-starting emails, TA427 has been directly seeking the opinions of foreign policy experts on nuclear disarmament, U.S.-ROK policies, and sanctions since 2023.
- Researchers saw a consistent stream of this activity, occasionally growing.
- Although TA427 continuously uses email infrastructure rotation and social engineering, it started abusing lax DMARC policies in December 2023 for persona spoofing and started using web beacons for target profiling in February 2024.
- An expert in social engineering, TA427 is a threat actor that most likely helps North Korea gather strategic intelligence on South Korean and American foreign policy endeavors.
- TA427 establishes rapport with targets over time by using aliases and casual conversations to engage them. This allows them to share their opinions and provide analysis, particularly regarding foreign policy negotiation tactics.
- Instead of sending malware or harvesting credentials directly, TA427 asks targets to share their opinions via emails, papers, or articles by using tailored, timely lure content and posing as well-known DPRK researchers.
- The intelligence requirements of TA427 may be satisfied by this direct input method, and the correspondence insights enhance future targeting and connection-building for further engagement. The aim seems to be increasing North Korean intelligence to guide negotiation tactics.
- Invitations to events on North Korean affairs, as well as inviting viewpoints on deterrence tactics, nuclear programs, and potential conflicts, are some of their enticements. Tactics entail transferring conversations between a target's email addresses, including personal and corporate.
- Think tanks, NGOs, media, academic institutions, and governmental bodies use DMARC abuse, typosquatting, and free email spoofing as ways to justify their actions, which is how TA427 hides itself.






[EXTERNAL] [Wilson Center] A quick question

Today at 8:21 AM

To:

To protect your privacy, some external images in this message were not downloaded. Download external images Go to Settings

Dear

Hope all is well. I'm [redacted] from Wilson Center. I am sure you are incredibly busy and you have packed schedule.

I'm writing to gauge your interest in participating in a trip with a high-level Wilson Center delegation to Seoul during the week of April 8th (Apr 8-11). We will have a roundtable with Korean scholars and individual meetings with high-level Korean officials (including the national security adviser, intelligence director, foreign minister, and defense minister). The Koreans would like to discuss the outlook for the US-ROK alliance after the US midterms and other recent events (e.g., the Russian invasion of Ukraine and US-China tensions). There will also be a day to see Seoul, the DMZ (which you have seen countless times), or other points of interest. All costs associated with this trip will be covered (business class travel, meals, five-star lodging). Your presence would add immensely to this trip. Can you let us know if you would be interested? If you have any questions, we would be happy to provide more information.

- Beginning in early February 2024, a different strategy involved using web beacons to conduct reconnaissance over the victim's active email account and the recipient's surroundings.
- TA427 is one of the actors that Proofpoint tracks the most frequently. Instead of maximizing profits, TA427 strategically targets experts by modifying its tactics, infrastructure components, or even avatars to steal information or obtain first access for intelligence purposes.

Indicators of compromise (IOCs)

Indicator	Type
Track 1.5 dialogue on CBRNE threat reduction in the Indo-Pacific Invitation: August DPRK meeting Draft Taiwan Issue emergence of Indigenous Nuclear Weapons Debate Request for Meeting (Korean Embassy) Invitation: 20/9 Conference - An Allied Approach to North Korea Invitation: 30/9 Conference - An Allied Approach to North Korea Request for Comments Invitation: 25/10 Conference - An Allied Approach to North Korea Invitation to CTR Workshop November 9 Track 1.5 dialogue on CBRNE threat reduction in the Indo-Pacific Invitation: August DPRK meeting Draft Taiwan Issue emergence of Indigenous Nuclear Weapons Debate Request for Meeting (Korean Embassy) Invitation: 20/9 Conference - An Allied Approach to North Korea Invitation: 30/9 Conference - An Allied Approach to North Korea Request for Comments Invitation: 25/10 Conference - An Allied Approach to North Korea Invitation to CTR Workshop November 9 DTRA Track 1.5 dialogue on Indo-Pacific CBRNE threat reduction Invitation to review Invitation to Korea Global Forum 2024 (Seoul, February 20-21) Event with the Korea Society "Rumbles of Thunder and Endangered Peaceon the Korean Peninsula" [Invitation] US Policy Toward North Korea - Pocantico Center February6-8 RISG 2024 Winter Meeting Invitation Invitation to speak at the East Asia Strategy Forum Discussion about DPRK sanctions Invitation: 3/5 Conference - An Allied Approach to North Korea US-ROK dialogue Seeking Comments Essay Series: Peaceful Co-existence with North Korea [Invitation] US Policy Toward North Korea - Pocantico Center March 12-14 Invitation as a Discussant for a US-ROK Research Project Seminar Lunch Invitation to meet with Senior Deputy Minister for Foreign Affiars	2023 & 2024 Email Subjects
stimson[.]shop stimsonn[.]org nknevvs[.]org wilsoncenters[.]org wilsoncentre[.]org	2023 & 2024 Spoofed Domains

Prevention

- Block unknown links from running.
- Don't use the same password for different accounts.
- For critical accounts, use two-factor authentication
- Do not click on the malicious link.
- 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 mechanism through the firewall.
- Enable SSL with SMTP protocol for safe transmission.
- Enable limitations on administrative access or rights.

Remediation

- Use network monitoring and Endpoint Detection and Response (EDR) tools to detect abnormal activities.
- Keep your anti-malware and anti-virus software up to date.
- Keep software and firmware regularly updated.
- 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
Sandworm	https://www.virustotal.com/gui/collection/0bd93a520cae1fd917441e6e54ff263c88069ac5a7f8b9e55ef99cd961b6a1c7/iocs
Fin7	https://blogs.blackberry.com/en/2024/04/fin7-targets-the-united-states-automotive-industry
TA427	https://www.proofpoint.com/us/blog/threat-insight/social-engineering-dmarc-abuse-ta427s-art-information-gathering?&web_view=true
Muddled Libra	https://unit42.paloaltonetworks.com/muddled-libra-evolution-to-cloud/
UNC5174	https://therecord.media/chinese-government-hacker-exploiting-bugs-to-target-defense-government-sectors?&web_view=true

TOP EXPLOITED VULNERABILITIES

Vulnerability Name	Description	References
Apple macOS Metal Framework PVR File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability CVE-2024-23264	Vulnerability allows remote attackers to disclose sensitive information on affected installations of Apple macOS. Interaction with the Metal Framework library is required to exploit this vulnerability, but attack vectors may vary depending on the implementation.	https://support.apple.com/en-us/HT214084
Progress Software Telerik Report Server ObjectReader Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2024-1800	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Progress Software Telerik Report Server. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data.	https://docs.telerik.com/report-server/knowledge-base/deserialization-vulnerability-cve-2024-1800
Microsoft uAMQP for Python azure-iot-sdks-ci Uncontrolled Search Path Element Remote Code Execution Vulnerability	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Microsoft uAMQP for Python. When installed from the official Microsoft GitHub repository, the installation attempts to load a non-existent cloud resource that is vulnerable to takeover.	https://msrc.microsoft.com/update-guide/en-us/acknowledgement/online
Microsoft Windows MHT File Mark-Of-The-Web Bypass Remote Code Execution Vulnerability CVE-2024-29991	Vulnerability allows remote attackers to bypass the Mark-Of-The-Web security feature to execute arbitrary code on affected installations of Microsoft Windows. The specific flaw exists within the handling of .MHT files.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29991

TOP EXPLOITED VULNERABILITIES

Vulnerability Name	Description	References
Wazuh Active Response Module Improper Input Validation Remote Code Execution Vulnerability CVE-2023-50260	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Wazuh. The issue results from the lack of proper validation of JSON messages.	https://github.com/wazuh/wazuh/security/advisories/GHSA-mjq2-xf8g-68vw
Wazuh Analysis Engine Event Decoder Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-32038	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Wazuh. The flaw exists win Analysis Engine service, which listens on default TCP port 1514. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer.	https://github.com/wazuh/wazuh/security/advisories/GHSA-fcpw-v3pg-c327
Ivanti Avalanche WLAvalancheService Directory Traversal Remote Code Execution Vulnerability CVE-2024-27976	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Ivanti Avalanche. The specific flaw exists within the WLAvalancheService, which listens on TCP port 1777 by default.	https://forums.ivanti.com/s/article/Avalanche-6-4-3-Security-Hardening-and-CVEs-addressed?language=en_US
Ivanti Avalanche WLInfoRailService Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-24996	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Ivanti Avalanche. The specific flaw exists within the WLInfoRailService, which listens on TCP port 7225 by default.	https://forums.ivanti.com/s/article/Avalanche-6-4-3-Security-Hardening-and-CVEs-addressed?language=en_US
GStreamer AV1 Video Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-50186	Vulnerability allows remote attackers to execute arbitrary code on affected installations of GStreamer. Interaction with this library is required to exploit this vulnerability but attack vectors may vary depending on the implementation.	https://gstreamer.freedesktop.org/security/sa-2023-0011.html
Arista NG Firewall ReportEntry SQL Injection Remote Code Execution Vulnerability CVE-2024-27889	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Arista NG Firewall. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries.	https://www.arista.com/en/support/advisories-notices/security-advisory/19038-security-advisory-0093
Microsoft Windows Installer Service Link Following Local Privilege Escalation Vulnerability CVE-2024-26158	Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. By creating a symbolic link, an attacker can abuse the service to write arbitrary registry values.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26158
Microsoft Windows Internet Shortcut SmartScreen Bypass Vulnerability CVE-2024-29988	Vulnerability allows remote attackers to bypass the SmartScreen security feature to execute arbitrary code on affected installations of Microsoft Windows. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988
Flexera Software FlexNet Publisher Uncontrolled Search Path Element Local Privilege Escalation Vulnerability CVE-2024-2658	Vulnerability allows local attackers to escalate privileges on affected installations of Flexera Software FlexNet Publisher. The specific flaw exists within the configuration of OpenSSL.	https://community.flexera.com/t5/FlexNet-Publisher-Knowledge-Base/CVE-2024-2658-FlexNet-Publisher-potential-local-privilege/ta-p/313003
Siemens Simcenter Femap MODEL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2024-27907	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Siemens Simcenter Femap. The specific flaw exists within the processing of MODEL files within the CatiaV4_2022_2 executable.	https://cert-portal.siemens.com/productcert/html/ssa-000072.html
Wireshark NetScreen File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-6175	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Wireshark. The specific flaw exists within the parsing of packet capture files in the NetScreen format.	https://www.wireshark.org/security/wnpa-sec-2023-29.html
Schneider Electric EcoStruxure Power Design - Ecodial BinSerializer Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2024-2229	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Schneider Electric EcoStruxure Power Design - Ecodial. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data.	https://www.cisa.gov/news-events/ics-advisories/icsa-24-072-01
Softing edgeConnector Siemens Cleartext Transmission of Credentials Authentication Bypass Vulnerability CVE-2024-0860	Vulnerability allows network-adjacent attackers to bypass authentication on affected installations of Softing edgeConnector Siemens. The specific flaw exists within the web console, which listens on TCP port 8099 by default. HTTP traffic to this port contains unprotected credentials.	https://www.cisa.gov/news-events/ics-advisories/icsa-24-074-13
Softing edgeConnector Siemens Directory Traversal Remote Code Execution Vulnerability CVE-2023-38126	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Softing edgeConnector Siemens. In the case of a network-adjacent attacker, the existing authentication mechanism can be bypassed.	https://www.cisa.gov/news-events/ics-advisories/icsa-24-074-13

TOP EXPLOITED VULNERABILITIES

Vulnerability Name	Description	References
SolarWinds Access Rights Manager OpenFileStreamLocal Directory Traversal Remote Code Execution Vulnerability CVE-2024-23479	Vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Access Rights Manager. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations.	https://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2023-2-3_release_notes.htm
Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability CVE-2024-30371	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader. The issue results from the lack of validating the existence of an object prior to performing operations on the object.	https://www.foxit.com/support/security-bulletins.html
Linux Kernel nft_exthdr_ipv6_eval Stack-based Buffer Overflow Information Disclosure Vulnerability CVE-2023-52628	Vulnerability allows local attackers to disclose sensitive information on affected installations of the Linux Kernel. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer.	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?h=v6.1.67&id=d9ebfc0f21377690837ebbd119e679243e0099cc
Autodesk DWG TrueView DWG File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2024-23138	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Autodesk DWG TrueView. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0006
RARLAB WinRAR Mark-Of-The-Web Bypass Vulnerability CVE-2024-30370	Vulnerability allows remote attackers to bypass the Mark-Of-The-Web protection mechanism on affected installations of RARLAB WinRAR. A crafted archive entry can cause the creation of an arbitrary file without the Mark-Of-The-Web.	https://www.rarlab.com/rarnew.htm#27.%20Busgs%20fixed
(Pwn2Own) Google Chrome V8 Enum Cache Out-Of-Bounds Read Remote Code Execution Vulnerability CVE-2024-3159	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Google Chrome. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure.	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?h=v6.1.67&id=d9ebfc0f21377690837ebbd119e679243e0099cc
Microsoft Azure ODSP nikisos Uncontrolled Search Path Element Remote Code Execution Vulnerability	Vulnerability allows remote attackers to execute arbitrary code on affected installations of ODSP for Microsoft Azure. When installed from the official Microsoft GitHub repository, the installation attempts to load a non-existent cloud resource that is vulnerable to takeover.	https://msrc.microsoft.com/en-us/security-guidance/researcher-acknowledgments-online-services

Security Bulletin

Cisco Password-Spraying Attacks Target VPN Services & High-Severity Vulnerability in IMC CLI

Cisco has issued a warning regarding recent password-spraying attacks directed at Remote Access VPN (RAVPN) services configured on Cisco Secure Firewall devices. These attacks have also targeted third-party VPN concentrators, as noted in a recent report by the company. Password spraying involves attempting to log in using a list of usernames with a single password, such as “Secure@123,” across multiple accounts to evade detection mechanisms that might lock out accounts during typical brute force attacks.

Indicators of Compromise (IoC) for these attacks include difficulty establishing VPN connections with Cisco Secure Client (AnyConnect) and an unusual volume of authentication requests. To defend against these attacks, Cisco recommends several measures, including enabling logging to a remote syslog server for better incident correlation; securing default remote access VPN profiles; leveraging TCP shunning to block malicious IPs manually; configuring Control-plane ACL on the ASA/FTD to filter unauthorized public IPs; and implementing certificate-based authentication for RAVPN to enhance security.

In addition to the warning about password-spraying attacks, Cisco has disclosed a high-severity vulnerability, CVE-2024-20295, affecting the Command Line Interface (CLI) of the Cisco Integrated Management Controller (IMC). This vulnerability could enable an authenticated, local attacker to gain root access to a victim’s operating system. While a proof-of-concept (PoC) exploit exists, there’s no evidence of malicious use at present.

Affected products include the 5000 Series Enterprise Network Computer Systems, Catalyst 8300 Series Edge uCPE, UCS C-Series rack servers, and UCS E-Series servers. Cisco has released software updates to address the vulnerability and recommends users upgrade to the fixed versions.

It's worth noting that Cisco products have been targeted by threat actors in the past, highlighting the importance of promptly applying security updates to mitigate the risk of exploitation.

ShadowRay: Exploiting Unpatched Vulnerabilities in the Ray Framework for Data Theft and Resource Hijacking

A hacking campaign named "ShadowRay" has emerged, targeting an unpatched vulnerability in Ray, a widely-used open-source AI framework, to exploit computing resources and extract sensitive data from numerous companies. These attacks, as reported by application security firm Oligo, have been ongoing since at least September 5, 2023, affecting sectors such as education, cryptocurrency, and biopharma.

Ray, developed by Anyscale, facilitates the scaling of AI and Python applications across machine clusters for distributed computational tasks. With over 30,500 stars on GitHub, it is employed by prominent organizations like Amazon, Spotify, and OpenAI for various purposes, including training ChatGPT.

Anyscale disclosed five vulnerabilities in Ray in November 2023, fixing four but leaving a critical remote code execution flaw, CVE-2023-48022, unresolved due to its long-standing lack of authentication. Despite being disputed as a vulnerability by Anyscale, this flaw has been actively exploited in inadequately secured environments, leading to unauthorized access and data breaches.

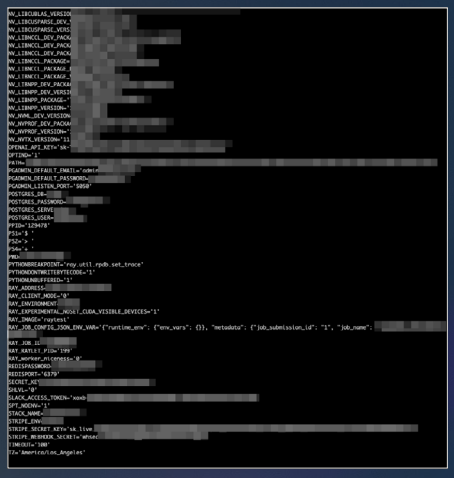
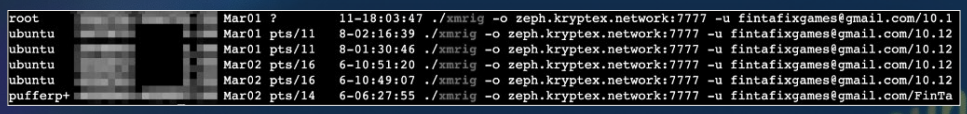


Figure 1. Exposed secrets Source: Oligo

Investigation revealed compromised Ray servers exposing sensitive information, including AI models and production database credentials. Attackers exploited these vulnerabilities for cryptocurrency mining and executing arbitrary code, posing significant risks to affected organizations.



Multiple XMRig miners running on a compromised server Source: Oligo

To defend against ShadowRay attacks, it is advised to secure Ray deployments within controlled environments, enforce firewall rules, add authorization to the Ray Dashboard port, and implement continuous anomaly monitoring. Other recommendations include avoiding default settings and utilizing security-enhancing tools for better cluster protection.

Malicious PyPi Packages Exploit Typosquatting to Target Machine Learning Libraries: A Detailed Analysis

Early on March 28, 2024, the Mend.io research team uncovered over 100 malicious packages aimed at popular machine learning (ML) libraries within the PyPi registry. Notable targets include Pytorch, Matplotlib, and Selenium. Employing a typosquatting technique, the attackers created deceptive package names such as "Matplotltib", "selennim", and "PyToich" to lure unsuspecting developers into downloading malicious versions.

These malicious packages utilize the Fernet mechanism for decryption, revealing a script that initiates further attack stages per its instructions. The investigation revealed that the malware aims to steal personal information, including passwords and tokens, while also attempting to collect cryptocurrencies. Additionally, it persists in trying to install itself in the system's startup path.

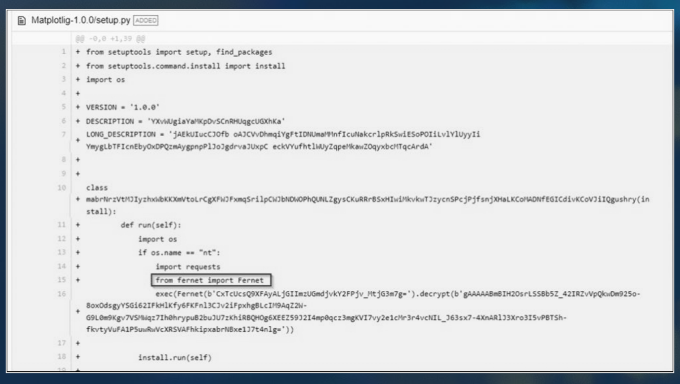


Figure 1. Setup.py file with encrypted Fernet payload

The execution flow of these packages begins with the setup.py file, which triggers the initial stage of execution, housing an encrypted Fernet payload. Upon decryption, subsequent stages unfold, culminating in the execution of a deobfuscated script revealing various malicious capabilities:

- Environment setup and data extraction: Creation of storage directories, extraction of extension and wallet data, including ZIP archives uploaded to a remote server.
- Discord token theft: Unauthorized access attempts to Discord accounts by retrieving authentication tokens.
- File search and upload: Scanning for sensitive files and uploading findings to a server.
- Persistence and remote control: Attempted download of a Python script for persistence and evasion techniques to hide execution.
- Injection into wallet applications: Targeting popular cryptocurrency wallet applications and injecting malicious components to compromise their security and user assets. The injection process involves identifying wallet applications, downloading and replacing legitimate application files with malicious ones, ensuring execution, and repeating attempts for robustness.

This attack underscores the necessity of thoroughly verifying all components introduced into code, especially in the context of ML development where sophisticated attacks targeting developers are on the rise.

MITRE Adds New North Korean Exploited Techniques: TCC Manipulation and Phantom DLL Hijacking

MITRE will be expanding its ATT&CK database this month with two sub-techniques that have been extensively exploited by North Korean threat actors. The first involves the manipulation of Transparency, Consent, and Control (TCC) on macOS, while the other exploits "phantom" dynamic link library (DLL) references in Windows.

TCC Manipulation

TCC manipulation has become a favored tactic among North Korean advanced persistent threats (APTs) targeting macOS systems. Despite macOS's security measures like System Integrity Protection (SIP) and Full Disk Access (FDA), attackers have found ways to circumvent these controls, often by exploiting scenarios where developers or users disable security features for troubleshooting or flexibility. This manipulation grants attackers unauthorized access to the TCC database, allowing them to grant themselves permissions without user notification. Various malware tools, including Lazarus Group malware and CloudMensis by APT37, have been designed to exploit these TCC vulnerabilities.

To counter TCC manipulation, experts advise keeping SIP enabled and being aware of app permissions. Exercising the principle of least privilege is crucial, removing unnecessary permissions for apps whenever possible.

Phantom DLL Hijacking

On the Windows front, North Korean threat actors have exploited "phantom" DLL references, leveraging the operating system's tendency to reference non-existent DLL files. This flaw provides hackers with an opportunity to create and deploy malicious DLLs with the same names, which are then loaded by the operating system without detection. The Lazarus Group and APT41 have utilized this tactic, targeting DLL references like "wlbsctrl.dll" and "wbemcomn.dll" to execute malicious activities.

To mitigate the risks associated with phantom DLL hijacking, companies are advised to employ monitoring solutions, proactive application controls, and automatic blocking of remote DLL loading, especially on Windows Server environments.

CoralRaider: Vietnamese Financially Motivated Hackers Target Businesses in Asia

Vietnamese financially motivated hackers, known as CoralRaider, have been targeting businesses across Asia in a campaign aimed at harvesting corporate credentials and financial data for resale on online criminal markets. Cisco Talos researchers have identified this cluster of hacking activity primarily attacking India, China, South Korea, Bangladesh, Pakistan, Indonesia, and domestic targets using exfiltration malware.

Talos attributes the origins of CoralRaider to Vietnam, citing evidence such as the use of Vietnamese language in their Telegram command-and-control channel and Vietnamese words hardcoded into payload binaries. The group's IP address traces back to Hanoi. They employ RotBot, a customized remote access tool based on the Quasar RAT, to download an information stealer designed to target business social media accounts containing valuable data, including payment cards.

The attackers focus on stealing victims' credentials, financial data, and social media accounts, with a particular emphasis on business and advertisement accounts. The CoralRaider attack initiates when users open a malicious Windows shortcut file, which

triggers the infection chain. While it's unclear how the threat actor delivers the files to victims, the activated LNK file downloads an HTML application file, initiating a series of PowerShell scripts in memory, ultimately leading to the execution of RotBot.

The XClient info stealer, loaded by RotBot, collects a wide range of data from various web browsers and communication platforms, including cookies, credentials, financial information, and details from social media accounts such as Facebook, Instagram, TikTok, and YouTube. Additionally, it gathers information about payment methods and permissions associated with Facebook business and advertising accounts.

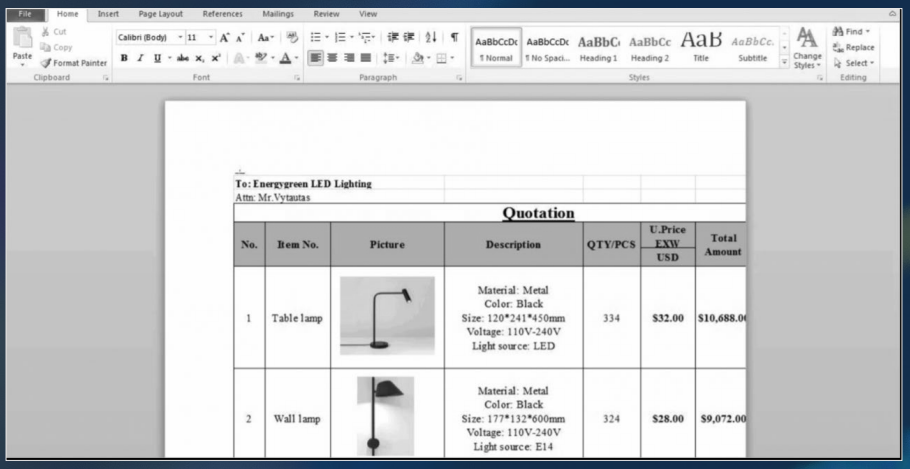
This campaign underscores the importance of robust cybersecurity measures for businesses in Asia, as financially motivated threat actors continue to evolve their tactics to target valuable corporate assets.

TA558's SteganoAmor Campaign: Concealing Malware in Images via Steganography

The notorious TA558 hacking group has initiated a new campaign dubbed "SteganoAmor," employing steganography to conceal malicious code within seemingly innocuous images to deliver various malware tools onto targeted systems. Steganography, a technique for hiding data inside files to evade detection, is the backbone of this campaign.

TA558, known for targeting hospitality and tourism organizations globally since 2018, with a focus on Latin America, has intensified its operations with SteganoAmor. Positive Technologies uncovered this campaign, identifying over 320 attacks affecting various sectors and countries.

The modus operandi of SteganoAmor involves malicious emails containing benign-looking document attachments (e.g., Excel and Word files), exploiting the CVE-2017-11882 vulnerability in Microsoft Office Equation Editor. These emails are dispatched from compromised SMTP servers to increase legitimacy.



To: Energygreen LED Lighting
Attn: Mr.Vytautas

Quotation

No.	Item No.	Picture	Description	QTY/PCS	U.Price EXW USD	Total Amount
1	Table lamp		Material: Metal Color: Black Size: 120*241*450mm Voltage: 110V-240V Light source: LED	334	$32.00	$10,688.0
2	Wall lamp		Material: Metal Color: Black Size: 177*132*600mm Voltage: 110V-240V Light source: E14	324	$28.00	$9,072.00

Figure 1. Sample of document used in the campaign Source: Positive Technologies

Victims with outdated Microsoft Office versions become targets of the exploit, which fetches a Visual Basic Script (VBS) from a legitimate service upon opening the document. This script retrieves an image file (JPG) containing a base64-encoded payload. Subsequently, PowerShell code within the script downloads the final payload hidden inside a text file, encoded in reverse base64.

Figure 2. Malicious code inside the text file Source: Positive Technologies

Security researchers have observed several malware families being deployed through this attack chain:

- AgentTesla: Spyware acting as a keylogger and credential stealer.
- FormBook: Infostealer collecting credentials and monitoring user activity.
- Remcos: Remote administration tool enabling attacker control over compromised systems.
- LokiBot: Info-stealer targeting various sensitive data.
- Guloader: Downloader for distributing secondary payloads.
- Snake Keylogger: Data-stealing malware capturing keystrokes and sensitive information.
- XWorm: Remote Access Trojan (RAT) facilitating remote control over infected computers.

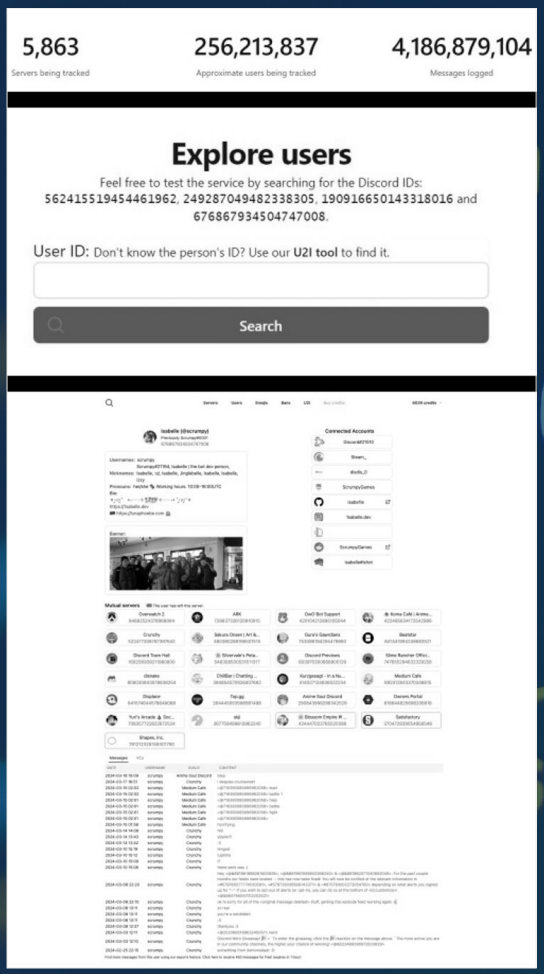
The use of legitimate cloud services like Google Drive to host malicious payloads, coupled with compromised FTP servers for command and control (C2) infrastructure, enhances the campaign's evasiveness.

While the campaign's reach extends worldwide, the majority of attacks have been concentrated in Latin American countries. However, defending against SteganoAmor is relatively straightforward—update Microsoft Office to render these attacks ineffective.

Privacy Breach: Discord Users' Private Messages Sold on Clear Web

A major privacy breach has occurred involving private data, including messages of millions of Discord users being sold on a clear web website named Spy.pet. The website, functioning as an internet-scraping company, has been collecting data from Discord since November 2023.

Figure 1. A screenshot from the website shows what it offers (Credit: Hackread.com)



Hackread.com reports that Spy.pet has already sold four billion public Discord messages extracted from 14,201 servers, which host a staggering 627,914,396 users. The ownership of the website remains unclear, but the nature of the leaked data – scraped messages – points to potential security vulnerabilities in Discord's interaction with bots or third-party applications.

Scraping, the method used by Spy.pet, involves automated tools extracting information from platforms like Discord by exploiting weaknesses in bot or unofficial app access. This exposes private chats, server chats, and direct messages, potentially revealing personal information, financial details, and company secrets. Previous instances of scraped databases from various platforms underline the severity of this issue.

Spy.pet operates as a chat-harvesting platform, offering user data through profiles containing aliases, pronouns, connected accounts, Discord servers, and public messages. Access to profiles and conversation archives requires purchasing credits, with cryptocurrency being the only accepted payment method. Despite being DDoS'ed in February 2024, the platform sustained minimal damage, according to its owner.

To protect oneself, it's advisable to review Discord privacy settings, restrict access to authorized applications, change passwords, enable two-factor authentication, and avoid sharing sensitive information in Discord chats. Suspected compromises should be reported to Discord promptly.

Discord is actively investigating Spy.pet and is committed to safeguarding user privacy, pledging appropriate action against violations of its Terms of Service and Community Guidelines.

United Kingdom MPs Targeted in Suspected Spear-Phishing Attack, Prompting Police Investigation

A police investigation has been initiated following reports of a "spear-phishing" attack targeting Members of Parliament (MPs), raising concerns about potential threats to parliamentary security. The inquiry was launched after an MP filed a complaint regarding unsolicited messages received last month, believed to be part of an attempt to compromise parliamentary systems.

Multiple individuals working in Westminster, including MPs, political journalists, broadcasters, and party staff, reported receiving unsolicited WhatsApp messages from suspicious mobile numbers over the past six months. The messages, attributed to a user named “Abigail” or “Abi,” were sent to a diverse range of targets, including members of both the Conservative and Labour parties.

The phishing operation, suspected to have been ongoing for at least 14 months, has drawn attention from senior political figures, who have suggested the involvement of a foreign state in what is being described as a “honeytrap” type attack. While parliamentary authorities have been actively involved in addressing the issue, police intervention underscores the seriousness of the incident.

Parliamentary spokespersons emphasized the institution’s commitment to security, stating that tailored advice and security measures have been provided to MPs and staff. However, the origin of the messages remains under investigation, with speculation ranging from hostile nation-states to opportunistic individuals.

Experts have highlighted the evolving nature of espionage tactics, emphasizing the importance of vigilance and resilience in the face of such threats. The incident has reignited discussions about the need for robust cybersecurity measures, particularly in the context of upcoming elections and the influx of new MPs and staffers into parliament.

Efforts to safeguard national security and democratic processes have been underscored, with calls for adequate resourcing of initiatives like the Defending Democracy Taskforce to address the evolving landscape of security risks. As concerns persist about the vulnerability of communication platforms like WhatsApp, ensuring comprehensive protection against potential threats remains a priority.

REFERENCE LINKS

- https://www.darkreading.com/vulnerabilities-threats/dprk-exploits-mitre-sub-techniques-phantom-dll-hijacking-tcc-abuse?&web_view=true
- https://www.mend.io/blog/over-100-malicious-packages-target-popular-ml-pypi-libraries/?&web_view=true
- https://www.bleepingcomputer.com/news/security/hackers-exploit-ray-framework-flaw-to-breach-servers-hijack-resources/?&web_view=true
- https://www.techtarget.com/searchsecurity/news/366581456/Cisco-discloses-high-severity-vulnerability-PoC-available
- https://www.govinfosecurity.com/vietnamese-threat-actor-targeting-financial-data-across-asia-a-24796?&web_view=true
- https://www.bleepingcomputer.com/news/security/new-steganoamor-attacks-use-steganography-to-target-320-orgs-globally/?&web_view=true
- https://www.hackread.com/website-selling-private-messages-of-discord-users/?web_view=true
- https://www.theguardian.com/uk-news/2024/apr/04/police-launch-inquiry-after-mps-targeted-in-apparent-spear-phishing-attack?&web_view=true
- https://www.proofpoint.com/us/blog/threat-insight/social-engineering-dmarc-abuse-ta427s-art-information-gathering?&web_view=true
- https://gbhackers.com/north-korean-hackers-dmarc-abuse/
- https://thehackernews.com/2024/04/muddled-libra-shifts-focus-to-saas-and.html
- https://unit42.paloaltonetworks.com/muddled-libra-evolution-to-cloud/
- https://www.bleepingcomputer.com/news/security/fin7-targets-american-automakers-it-staff-in-phishing-attacks/
- https://thehackernews.com/2024/04/fin7-cybercrime-group-targeting-us-auto.html
- https://blogs.blackberry.com/en/2024/04/fin7-targets-the-united-states-automotive-industry
- https://www.bleepingcomputer.com/news/security/atandt-confirms-data-for-73-million-customers-leaked-on-hacker-forum/?&web_view=true
- https://www.theregister.com/2024/03/27/apple_passcode_attack/?&web_view=true
- https://www.helpnetsecurity.com/2024/04/02/cybersecurity-risks-readiness-level/?web_view=true
- https://www.bleepingcomputer.com/news/security/22-500-palo-alto-firewalls-possibly-vulnerable-to-ongoing-attacks/
- https://thehackernews.com/2024/04/hackers-exploit-fortinet-flaw-deploy.html?&web_view=true
- https://thehackernews.com/2024/04/cisco-warns-of-global-surge-in-brute.html?&web_view=true

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