


NETWITNESS 
FIRSTWATCH

INTSUM REPORT

1 Aug -13 Sep 2024



BIWEEKLY INTELLIGENCE SUMMARIES (INTSUM) WILL REPORT ON THE MOST NOTEWORTHY RANSOMWARE ATTACKS, WIDELY EXPLOITED VULNERABILITIES AND THE LATEST IN DATA PRIVACY AND SECURITY POLICY NEWS TO PROVIDE A VALUABLE SNAPSHOT AND BRIEF SYNOPSIS OF THE CURRENT THREAT LANDSCAPE



GreenCharlie Launches Advanced Phishing and Malware Campaign Against US Political Bodies

In August 2024, open sources revealed that officials and affiliates of US political campaigns were targeted by the Mint Sandstorm and APT42 operations. This discussion focuses on the activities of an Iran-related group called GreenCharlie, which has connections with Mint Sandstorm, Charming Kitten, and TA453. Recorded Future has been monitoring the activities and malicious infrastructure of GreenCharlie since 2020 and has identified a significant and rapidly evolving cluster of infrastructure supporting GreenCharlie's cyber-espionage efforts. Recent findings have linked this network directly to the targeting of US political campaigns. Malware associated with GreenCharlie includes POWERSTAR (also known as CharmPower and GorjolEcho) and NokNok, which are used in targeted spearphishing operations.

On August 14, 2024, Google-Mandiant's (TAG) report introduced malware sample hashes known as GORBLE, which operates on GreenCharlie's infrastructure for command-and-control (C2) purposes. Analysis of GORBLE, POWERSTAR, and TAMECAT (also tied to APT42 by Google-Mandiant) reveals that they are variants of the same malware family. Additionally, infrastructure that overlaps between APT42 and what they track as GreenBravo.

Over July and August 2024, analysis pinpointed various Iran-based IP addresses interacting with GreenCharlie's





GreenCharlie Launches Advanced Phishing and Malware Campaign Against US Political Bodies (cont.)

infrastructure, likely for phishing activities, possibly including testing and training phases. They are highly likely to use ProtonVPN and/or ProtonMail for these operations.

GreenCharlie has registered its infrastructure using multiple dynamic DNS (DDNS) providers, including Dynu, DNSEXIT, and Vitalwerks. In line with established patterns, the group has also exploited the Namecheap provider to register many other domains, forming part of the infrastructure cluster analysts have been monitoring since June 2024.

NetWitness Takeaways:

- Organizations must be careful about phishing campaigns and deploy proper email security mechanisms to detect and prevent such threats.
- The network should be monitored for incoming and outgoing traffic to malicious domain names and IP addresses to avoid damaging or transferring sensitive data.

IOCs:

Domains:

- Activeeditor[.]info
- Personalwebview[.]info
- Longlivefreedom[.]ddns.net
- Hugmefirstddd[.]ddns.net
- Icenotebook[.]ddns.net

IPs:

- 193[.]111.236.130 94[.]74.175.209 172[.]86.77.85
- 185[.]143.233.120 185[.]241.61.86





Iranian Hackers Target WhatsApp Accounts of Biden and Trump Staffers, Escalate Phishing Campaigns Against Israel and U.S.

Multiple researchers have highlighted the aggressive measures taken by APT42 to compromise campaigns related to both the Democratic and Republican parties, along with targeting Israeli military, government, and diplomatic organizations. Around a dozen people linked to both Trump and Joe Biden, including current and former government officials and individuals associated with the two political campaigns, were targeted by APT42 in May and June.

This equal opportunity cyberspying strategy, according to John Hultquist of Mandiant, a cybersecurity firm owned by Google, is not surprising given that APT42 also targeted both campaigns in 2020, reflecting the Iranian government's significant interest in both candidates, Trump and now Vice President Kamala Harris.

One campaign, reminiscent of the 2016 Russian hack-and-leak operations, had its sensitive files breached and leaked, though it remains unconfirmed if APT42 was responsible. Microsoft and Google have both reported incidents involving APT42, including the targeting of a high-ranking official on a presidential campaign and the successful access to a political consultant's personal Gmail account

In addition to presidential campaigns, Google noted that APT42 has also targeted Israeli organizations through phishing websites that impersonate Israeli and Israel-related





Iranian Hackers Target WhatsApp Accounts of Biden and Trump Staffers, Escalate Phishing Campaigns Against Israel and U.S. (cont.)

groups. The FBI is currently investigating the apparent hacking of the Trump campaign, with a senior law enforcement official indicating a potential cyberattack originating from Iran aiming to access accounts of top Democrats. The investigation's extent or whether it includes other campaigns or political figures hasn't been specified, but there's no indication that these efforts have been successful.

A campaign official for Vice President Kamala Harris reported no known breaches to their systems. Trump's adviser, Roger J. Stone, mentioned that both his Hotmail and Gmail accounts were compromised, with Iran suspected to be the perpetrator, according to Microsoft and the FBI. While investigations are ongoing, Vice President Kamala Harris's team has not reported any breaches to its systems.

Additionally, Trump's longtime adviser, Roger J. Stone, has been informed by Microsoft and the FBI about suspected compromises of his email accounts.

In conclusion, it's crucial to acknowledge the diligent efforts of cybersecurity experts and law enforcement in addressing and investigating these cyber threats. It's imperative for all individuals and organizations, particularly those involved in high-stakes political activities, to remain vigilant and take proactive measures to safeguard their digital assets from potential malicious activities



Iranian Hackers Target WhatsApp Accounts of Biden and Trump Staffers, Escalate Phishing Campaigns Against Israel and U.S. (cont.)

NetWitness Takeaways:

- APT42 uses watering hole tactics as a part of their attack methodology. Watering hole is an attack where the attacker targets a website commonly visited by a specific group. By compromising the site, the attacker aims to infect the devices of individuals or organizations from that group when they visit the infected site.
- To protect against watering hole attacks, organizations should ensure their systems and software are regularly updated, employ security tools like antivirus and anti-malware solutions, and exercise caution when accessing websites. Additionally, web administrators should focus on enhancing website security to reduce the risk of potential breaches.
- APT42 employs credential harvesting tactics. To protect against such tactics, organizations should implement strong authentication methods, use complex and unique passwords, and enable multi-factor authentication (MFA).
- Continuous system monitoring and implementing endpoint detection and response solutions (EDR) are the best ways to counter attackers' persistence mechanisms.

MITRE ATT&CK Techniques:

T1566.001: Phishing - Spear Phishing Attachment

T1566.002: Phishing - Spear Phishing Link

T1608.003: Stage Capabilities - Upload Malware

T1589.003: Gather Victim Identity Information - Employee Names

T1204.002: User Execution - Malicious File





Chinese Volt Typhoon Targets Global IT Sectors Through Versa Director Exploit

A vulnerability in Versa Networks' Versa Director software, affecting versions before 22.1.4, has exposed 163 devices across the US, Philippines, Shanghai, and India. Despite the availability of patches, these devices remain vulnerable to exploitation. In response, Versa Networks has advised customers to isolate these devices from the internet and place them in a protected network environment, highlighting the vulnerability's 'high-severity' rating due to its potential for facilitating large-scale cyber attacks.

This specific vulnerability, CVE-2024-39717, allows attackers to utilize a web shell named “VersaMem” for intercepting credentials, thus gaining unauthorized access to networks. Black Lotus Labs, under Lumen Technologies, has attributed several ongoing attacks to Volt Typhoon, a Chinese cyber espionage group, expressing moderate confidence in this assessment. Although Versa Networks has confirmed only one instance of exploitation by an Advanced Persistent Threat (APT) actor, Black Lotus Labs has identified additional instances of exploitation at four US and one non-U.S. companies within the ISP, MSP, and IT sectors since June 12.

The Versa Director systems, mainly used by ISPs and MSPs, are now advised to upgrade to version 22.1.4 or newer to address this vulnerability. Versa has partly blamed customer negligence for these breaches, citing failing to adhere to recommended system hardening and firewall guidelines.



Chinese Volt Typhoon Targets Global IT Sectors Through Versa Director Exploit (cont.)

U.S. government agencies including the NSA, FBI, and CISA have previously issued warnings about Volt Typhoon, indicating their sophisticated use of SOHO network devices for espionage activities.

The operation patterns identified by Black Lotus Labs, including Java-based backdoors and exploits of zero-day vulnerabilities, closely match those traditionally associated with Chinese state-sponsored cyber operations.

NetWitness Takeaways:

- Monitoring web traffic, command line activity and file changes is essential to detect Volt Typhoon.
- Following application rules are provided by NetWitness to help monitor and alert such activity.
 - Runs WMI command-line tool
 - Command line writes script files
 - Runs PowerShell downloading content
 - Runs PowerShell decoding base64 string
 - Runs PowerShell with hidden window



Chinese Volt Typhoon Targets Global IT Sectors Through Versa Director Exploit (cont.)

MITRE ATT&CK Techniques:

T1059: Command and Scripting Interpreter

T1047: Windows Management Instrumentation (WMI)

T1543: Create or Modify System Process

T1543: Create or Modify System Process

T1021: Remote Services

T1563: Remote Service Session Hijacking

T1105: Ingress Tool Transfer





RansomExx Exploits Jenkins Vulnerability in Targeted Attack Against Indian Banks

Researchers at CloudSEK blamed a recent ransomware attack impacting the digital payment systems of over 300 small Indian banks on successfully exploiting CVE-2024-23897, an arbitrary file read vulnerability in Jenkins, against a misconfigured publicly accessible Jenkins server. The attack, claimed by the RansomExx ransomware gang, targeted the technology service provider C-Edge Technologies, which supports several cooperative and regional rural banks in the country.

In a post on their leak site, RansomExx operators announced the retrieval of 142 GB worth of data. To curb the ransomware's spread, the National Payments Corporation of India (NPCI) isolated the affected banks from their payment system, locking customers out of access to ATM withdrawals and the Unified Payments Interface (UPI) for a day. CVE-2024-23897, [first](#) disclosed in January 2024, allows for unauthorized access to sensitive data through Jenkins'

Command Line Interface (CLI). Due to improper input validation in the Jenkins CLI command processing system, an attacker can use SSH, Websocket, or HTTP requests via the CLI endpoint to read the first several lines of any file on a Jenkins system. In addition to sensitive data leakage, when exploited, this vulnerability can lead to remote code execution or, in this case, ransomware deployment.

RansomExx, active since 2018 under its previous name, Defray777 (rebranded to RansomExx in 2020), is an advanced



RansomExx Exploits Jenkins Vulnerability in Targeted Attack Against Indian Banks (cont.)

ransomware group known for its substantial ransom demands and highly targeted human-operated attacks against high-profile organizations. Some of their previous victims included the Italian automaker Ferrari, Peru's Ministry of Defense, and the Taiwanese electronics company LITEON.

RansomExx updated to its more sophisticated v2.0 ransomware to combat increasingly effective defensive mitigations. The newer improved version added upgraded functionality, including:

- Use of the more robust AES-256 encryption algorithms
- A Linux variant giving it cross-platform functionality
- Increased evasion techniques, including the use of legitimate system tools

Along with its enhanced capabilities, RansomExx v2.0 adopted the double extortion model. In this tactic, attackers threaten to release sensitive, exfiltrated data if victims do not meet ransom demands.

NetWitness Takeaways:

- The command parser feature responsible for CVE-2024-23897 is fixed in all Jenkins releases since Jenkins 2.442, LTS 2.426.3, and LTS 2.440.1. It is highly recommended to patch any vulnerable Jenkins servers immediately.
- For those unable to patch, disabling access to the CLI provides a short-term workaround to prevent exploitation of CVE-2024-23897.





RansomExx Exploits Jenkins Vulnerability in Targeted Attack Against Indian Banks (cont.)

NetWitness Takeaways (cont.):

- NetWitness users can use the Jenkins log collector (jenkins) to collect Jenkins server logs. Jenkins offers in depth logging capabilities which can assist defenders during triage.
- For NDR/Packet customers, the HTTP Lua Parser has been updated with the following detection:
 - Jenkins Arbitrary File Read Attempt
- The following Endpoint Application Rules, currently available on NetWitness Live, detect TTPs associated with RansomExx activity:
 - Logs Disabled with Wevtutil.exe
 - Cipher.exe Overwrite Deleted Data on C Drive

MITRE ATT&CK Techniques:

T1005: Data from Local System

T1041: Exfiltration Over C2 Channel

T1059.001: Command and Scripting Interpreter - PowerShell

T1068: Exploitation for Privilege Escalation

T1074.001: Data Staged - Local Data Staging

T1078: Valid Accounts

T1089: Disabling Security Tools

T1190: Exploit Public-Facing Application

T1486: Data Encrypted for Impact

T1489: Service Stop

T1490: Inhibit System Recovery

T1562.001: Disabling Security Tools

T1567.002: Exfiltration Over Web Service

T1569.002: System Services - Service Execution





New Voldemort Malware Disguises as Google Apps to Elude Security Systems

In August 2024, a sophisticated cyberattack campaign targeted over 70 organizations globally, dispatching more than 20,000 malicious emails designed to impersonate national tax authorities from the US, the UK, France, Germany, Italy, India, and Japan. The onslaught began on August 5, with activity spiking to around 6,000 messages on August 17.

This campaign was meticulously tailored, with messages crafted in the respective languages of the impersonated tax agencies. It was aimed at individuals based on their country of residence rather than where their employer is located. Analysis by Proofpoint revealed that the threat actors utilized compromised domains to lend credibility to their emails, further indicating a high level of sophistication in their approach.

The attackers indiscriminately targeted a wide range of industries, with insurance companies making up nearly a quarter of the targeted organizations, alongside significant numbers in aerospace, transportation, and academia. The campaign utilized a combination of emerging cybercriminal techniques and methods typically associated with espionage, suggesting a dual-purpose aim that complicates the understanding of the attackers' capabilities and intentions.





New Voldemort Malware Disguises as Google Apps to Elude Security Systems (cont.)

Notably, the campaign exploited TryCloudflare Tunnels to obscure its attacks, which aligns with trends seen in cybercriminal activities but suggests potential espionage motives. This blend of advanced and basic tactics, along with the campaign's broad scope and targeted nature, underscores its unusual and potentially dual-threat nature as both a cybercriminal and espionage activity.

While the immediate objective appeared to focus on information gathering, the comprehensive blend of techniques and the expansive nature of the campaign signals a complex threat landscape where actors may pursue espionage objectives under the guise of cybercrime, making it a significant security concern for organizations worldwide.

NetWitness Takeaways:

- Any non-browser processes making network connections to cloud services should be investigated.
- Organizations may consider restricting access to external file sharing services to only known, safelisted servers
- Block network connections to TryCloudflare if it is not required for business purposes.
- Check for unexpected or excessive HTTPS connections to sheets[.]googleapis.com.





New Voldemort Malware Disguises as Google Apps to Elude Security Systems (cont.)

NetWitness Takeaways (cont.):

YARA:

```
rule Voldemort_PPFT_August_2024 {
  meta:
    sharing = "TLP:WHITE"
    source = "Proofpoint"
    author = "@Bry_Campbell"
    description = "Basic string values derived from published samples"
    category = "MALWARE"
    malware = "Voldemort"
    reference = "https://www.proofpoint.com/us/blog/threat-insight/malware-
must-not-be-named-suspected-espionage-campaign-delivers-voldemort"
    date = "2024-08-30"
    SHA256 =
"fa383eac2bf9ad3ef889e6118a28aa57a8a8e6b5224ecdf78dcffc5225ee4e1f"
  strings:
    $a1 = "Voldemort_gdrive_c.dll" ascii fullword
    $a2 = "SparkEntryPoint" ascii fullword
    $a3 = "abHost.exe" ascii fullword
    $a4 = "Content-Type: application/json" ascii fullword
    $a5 = "addSheet" ascii fullword
    $a6 = "access_token" ascii fullword
  condition:
    (
      uint16(0) == 0x5A4D and // Check for the "MZ" header indicating a PE file
      uint16(uint32(0x3C) + 4) == 0x8664 and // Check for the "PE" header and x64
architecture (0x8664)
      filesize < 300KB
    )
    and 4 of ($a*)
}
```





MoonPeak: North Korean Hackers Deploy Evolving XenoRAT Variant in Sophisticated Cyber Campaign

A North Korean-linked cyber threat actor, likely connected to the notorious Kimsuky group, is actively developing and deploying a new variant of the XenoRAT malware named MoonPeak. This information-stealing trojan is being distributed using a sophisticated infrastructure of command-and-control (C2) servers, staging systems, and test machines. Researchers at Cisco Talos, who identified MoonPeak, noted that the malware constantly develops, with attackers making incremental changes to improve its functionality and evade detection. MoonPeak retains the core capabilities of XenoRAT, such as keylogging and bypassing User Access Control (UAC), while introducing modifications like a Hidden Virtual Network Computing feature for covert remote access.

Cisco Talos has observed the activity of a threat actor it tracks as UAT-5394, whose tactics, techniques, and procedures (TTPs) show considerable overlap with the Kimsuky group, leading researchers to suggest that UAT-5394 may either be a subgroup of Kimsuky or a separate entity utilizing similar infrastructure. Modifications to MoonPeak include changing the XenoRAT client namespace from "xeno rat client" to "cmdline," ensuring that unauthorized implants or unmodified XenoRAT variants cannot connect to MoonPeak's custom servers. The attackers have also adopted more advanced obfuscation techniques, such as employing asynchronous state machines, significantly increasing the complexity of the malware and making it more challenging to analyze and reverse-engineer.





MoonPeak: North Korean Hackers Deploy Evolving XenoRAT Variant in Sophisticated Cyber Campaign (cont.)

In addition to changes in the malware itself, UAT-5394 has shifted its operational infrastructure, moving away from public cloud services and setting up private servers for hosting C2. Some servers linked to MoonPeak have connections to other malware, such as Quasar RAT, indicating a sophisticated operation. Researchers suggest that UAT-5394 is deliberately evolving MoonPeak in small increments to avoid detection while ensuring that specific trojan variants are compatible only with dedicated C2 servers, complicating defensive efforts.

NetWitness Takeaways:

- Block and query for malicious command and control (C2) Communications. This includes C2 servers and IPs tied to malware activity, including MoonPeak's evolving C2 infrastructure.
- Threat Hunting for Indicators of Compromise (IOCs): Actively hunt for MoonPeak-related IOCs such as changes to "cmdline" client namespaces or traffic patterns resembling XenoRAT activity. Keep threat intelligence feeds updated.
- MoonPeak was found to use RDP to access C2 infrastructure. It is recommended to review over RDP traffic and logs associated to the protocol.





FIRSTWATCH

MoonPeak: North Korean Hackers Deploy Evolving XenoRAT Variant in Sophisticated Cyber Campaign (cont.)

NetWitness Takeaways (cont.)

IOCs:

Domains:

- pumaria[.]store
- yoiroyse[.]store
- nmailhostserver[.]store
- nsonlines[.]store

IPs:

167[.]88.173.173 95[.]164.86.148 80[.]71.157.55 84[.]247.179.77
45[.]87.153.79 45[.]95.11.52 104[.]194.152.251
27[.]255.81.118 212[.]224.107.244 27[.]255.80.162
159[.]100.29.122 210[.]92.18.169 91[.]194.161.109

Ports:

9966 9936 8936 9999 8989

MITRE ATT&CK Techniques:

T1071: Application Layer Protocol

T1056: Input Capture (Keylogging)

T1105: Ingress Tool Transfer

T1027: Obfuscated Files or Information

T1036: Masquerading

T1129: Shared Modules





State-Sponsored Attacks and Commercial Surveillance Exploits

The recent analysis of the cyber threat landscape identifies a significant and troubling trend: the escalated targeting of mobile devices by state-sponsored attackers and commercial surveillance vendors through zero-day vulnerabilities. This report zeroes in on vulnerabilities within Android systems (CVE-2023-20963) and WebKit (CVE-2022-42856), which have been exploited to compromise device security and gain unauthorized access to sensitive data. Such breaches allow attackers to execute arbitrary code and secure complete control over devices, primarily targeting individuals like journalists, human rights advocates, and political dissidents.

These cyber operations, often a collaboration between state-backed groups and vendor-supplied surveillance tools, highlight the complexities of current cyber security challenges, notably ineffective patch management and adherence to secure protocols. Despite the availability of patches, delays in application have allowed attackers to continue exploiting them, underscoring the critical need for improved response mechanisms and the role each of us plays in this process.

Google's Threat Analysis Group (TAG) has documented the exploitation of these vulnerabilities in sophisticated campaigns, emphasizing the severe implications of





State-Sponsored Attacks and Commercial Surveillance Exploits (cont.)

unauthorized sensitive data access and expanding spying capabilities through commercial surveillance products. This evolving threat scenario underscores the need for immediate action to bolster patching processes, enhance vigilance, and foster stronger collaboration across governments, the private sector, and international entities to fortify privacy and security safeguards.

In summary, the persistence of attacks exploiting zero-day vulnerabilities on mobile platforms evidences a pressing challenge in cybersecurity: the need to expedite and enhance patching practices, cultivate awareness among high-risk groups, such as government officials, corporate executives, and individuals in sensitive industries, and facilitate international cooperation to protect individual rights and privacy against unauthorized access and surveillance.

NetWitness Takeaways:

- **Patch Management:** Organizations and individuals must ensure prompt patching of known vulnerabilities, especially on mobile devices, to mitigate the risk posed by these exploit chains. Monitoring the patch status of CVE-2023-20963 and CVE-2022-42856 is critical for effective defense.
- Analysts should look for indicators such as unexpected mobile traffic patterns, connections to known malicious infrastructure, and signs of privilege escalation on iOS and Android devices.





State-Sponsored Attacks and Commercial Surveillance Exploits (cont.)

NetWitness Takeaways (cont.):

IOCs:

Domains:

- ceo-adviser[.]com
- track-adv[.]com

Hashes:

- 8bd9a73da704b4d7314164bff71ca76c15742dcc343304def49b1e4543478d1a (VALIDVICTOR)
- d19dcbb7ab91f908d70739968b14b26d7f6301069332609c78aafc0053b6a7e1 (COOKIESNATCH)
- 21682218bde550b2f06ee2bb4f6a39cff29672ebe27acbb3cee5db79bf6d7297
- df21c2615bc66c369690cf35aa5a681aed1692a5255d872427a2970e2894b2e3 (ANDROSNATCH)

