Cyber Threat Advisory

JUNE 2023

Contents

Monthly Highlights - June

1. **Growing CaaS Economy Fuels Novel Attacks**

   Cybercrime-as-a-service (CaaS) is growing and is now becoming a robust ecosystem of online services that facilitate cybercrimes, including business email compromise (BEC) and human-operated ransomware. There has been a growing number of CaaS sellers offering compromised credentials, and many CaaS services and products come equipped with enhanced features that are designed to evade detection. Microsoft had blocked 2.75 million site registrations in 2022, preventing threat actors from using the listed sites to conduct attacks across the globe.

2. **Microsoft Digital Defense Report: Key Cybercrime Trends**

   Microsoft had observed that the threat actors use current events, such as the Ukrainian conflict and COVID-19, to create these hyper-realistic, targeted phishing attacks. These attacks leverage news stories to entice consumers to click on malicious links or provide sensitive information that would then enable attackers to gain access to internal networks of the impacted user. Cybercriminals use these cyber-attack vectors to gain information that is then sold and leveraged in more targeted attacks, such as ransomware, data exfiltration and extortion, and BEC.

3. **Severe RCE Bugs Open Thousands of Industrial IoT Devices to Cyberattack**

   As per Gavrilov's report - An industrial cellular router allows multiple devices to connect to the Internet from a cellular network, and these routers are commonly used in industrial settings, such as manufacturing plants or oil rigs, where traditional wired Internet connections may not be available or reliable. So, the industrial cellular routers and gateways have become one of the most prevalent components in the IIoT landscape. They offer extensive connectivity

features and can be seamlessly integrated into existing environments and solutions with minimal modifications.

4. **US Sanctions Four North Korean Entities for Global**

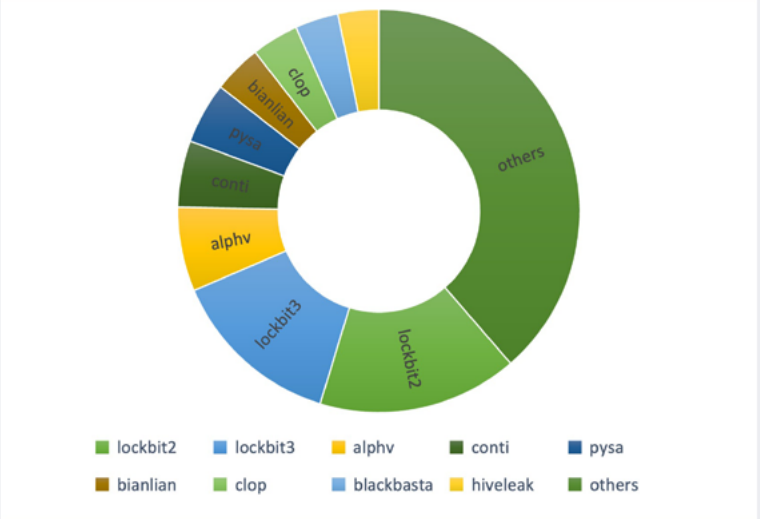
   The US Department of Treasury has imposed sanctions on four entities and one individual involved in illicit revenue generation and malicious online activities to generate revenue for the Democratic People's Republic of Korea (North Korea). RGB is North Korea's primary intelligence bureau and the main entity responsible for the country's malicious cybersecurity activities. The RGB was designated on January 2, 2015, as a controlled entity of the government of North Korea, according to a press release by the US Department of Treasury.

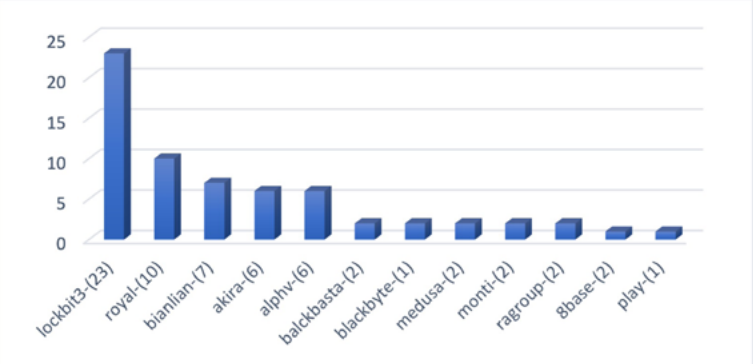
5. **Secureframe Finds 37% of Organizations Reuse Passwords for Cloud Service Providers**

   Secureframe, the leading provider of compliance automation software, has released a new research which revealed the most common security failures in organizations worldwide. These new findings were released in conjunction with the announcement of Secureframe Trust, which helps organizations build customer confidence by enabling them to demonstrate their security, compliance, and privacy posture. According to their study, three common security failures are prevalent in cloud-first organizations:

   - The access key rotation used for cloud service providers had the highest failure rate at 41%.
   - 40% of the IAM accounts and 21% of root accounts did not have two-factor or multi-factor authentication set up for cloud service providers.
   - 37% of the organizations had been reusing old passwords for cloud service provider logins.

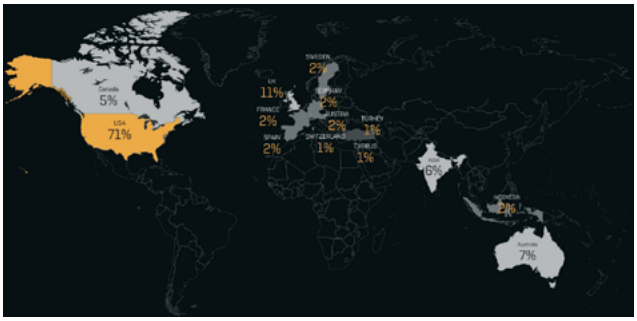
Ransomware Engagement Tracker





BianLian

- BianLian is a cybercriminal group involved in ransomware development, deployment, and data extortion.
- Since June 2022, the FBI has observed BianLian targeting organizations in multiple critical infrastructure sectors in the United States.
- The Australian Cyber Security Centre (ACSC) has observed BianLian primarily targeting private enterprises in Australia, including one critical infrastructure organization.
- Initially, BianLian employed a double-extortion model, where they exfiltrated various types of files for leverage and encrypted victims' systems.
- In 2023, the FBI observed a shift in BianLian's tactics, primarily focusing on exfiltration-based extortion while leaving victims' systems intact.
- The ACSC noted that BianLian has exclusively shifted to exfiltration-based extortion.
- BianLian actors threaten victims with potential financial, business, and legal consequences if payment is not made.



BianLian's victims since July 2022 *(Redacted)*

Detection:

Initial Access:

- BianLian group gains initial access to networks by leveraging compromised Remote Desktop Protocol (RDP) credentials. They obtain these credentials through various means, such as acquiring them from initial access brokers or conducting phishing attacks.
- The group utilizes the compromised RDP credentials to gain unauthorized access to the victim's network infrastructure.

Command and Control:

- BianLian group deploys a custom backdoor specific to each victim. The backdoor is written in the Go programming language and serves as a persistent presence in the compromised system.
- In addition to the backdoor, the actors install remote management and access software like TeamViewer, Atera Agent, SplashTop, or AnyDesk.

Defense Evasion:

- To evade detection, BianLian group employs various techniques. They use PowerShell and Windows Command Shell to disable antivirus tools, particularly Windows Defender and Anti-Malware Scan Interface (AMSI). This is achieved by modifying the Windows Registry settings.
- The actors also target specific security services like Sophos SAVEnabled, SEDEenabled, and SAVService. They disable the tamper protection for these services, allowing them to uninstall them from the compromised system.

Discovery:

- BianLian group employs a combination of compiled tools and native Windows utilities to gather information about the victim's environment.
- They utilize network scanning tools such as Advanced Port Scanner and SoftPerfect Network Scanner to identify open ports, retrieve program versions running on those ports, and discover shared folders.
- The actors also use SharpShares to enumerate accessible network shares in a domain and PingCastle to gather information about the Active Directory (AD) hierarchy and trust relationships.
- Native Windows tools and Windows Command Shell are utilized to query logged-in users, retrieve information about groups and accounts in the domain, obtain a list of domain controllers and domain trusts, and identify accessible devices on the network.

Credential Access:

- BianLian group leverages valid accounts for lateral movement within the compromised network and to perform further malicious activities.
- To obtain these credentials, the actors use Windows Command Shell to search for unsecured credentials stored on the local machine.
- Additionally, they target the Local Security Authority Subsystem Service (LSASS) memory to harvest credentials. They download a tool called RDP Recognizer to the victim system, which allows them to brute force RDP passwords or check for RDP vulnerabilities. They may also attempt to access the Active Directory domain database (NTDS.dit) to retrieve credential information.

Persistence and Lateral Movement:

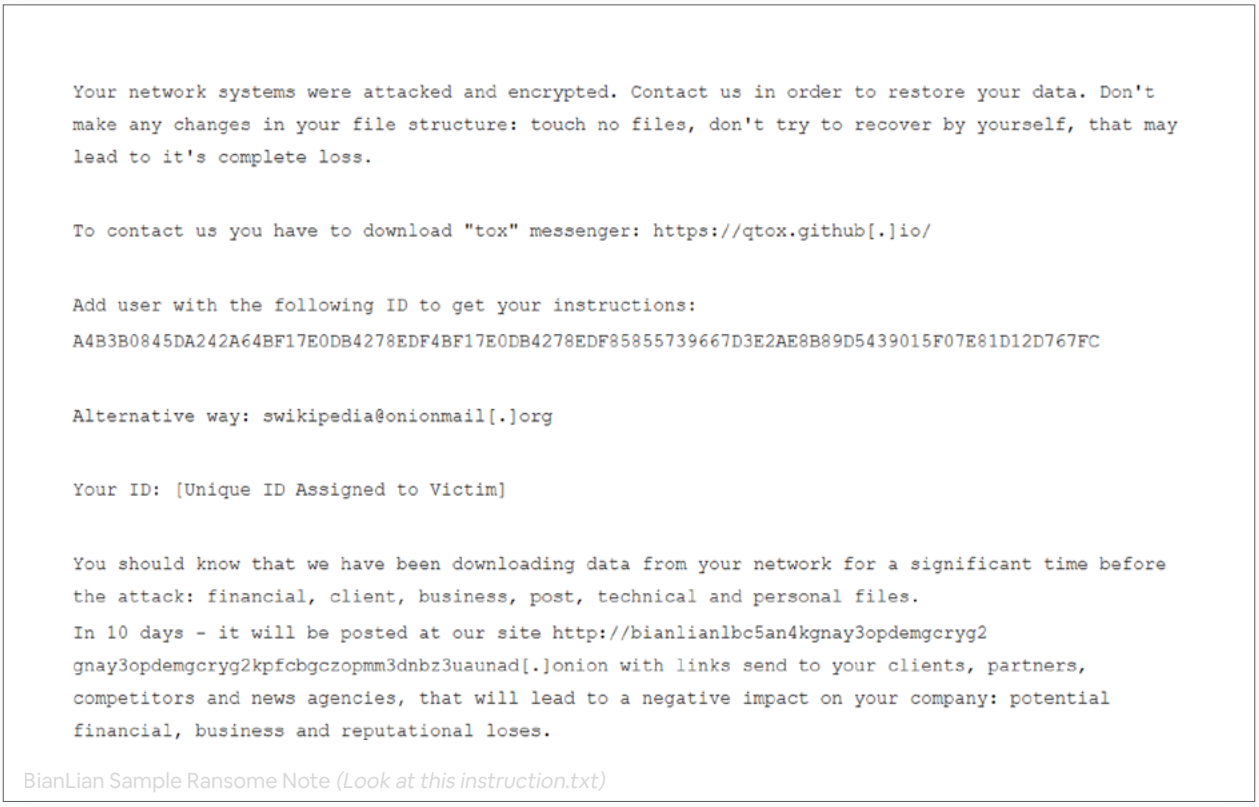
- For lateral movement within the compromised network, BianLian group utilizes tools like PsExec and RDP, using valid accounts that they have acquired.
- Before using RDP, the actors modify the compromised system by adding user accounts to the local Remote Desktop Users group, changing the added account's password, and modifying Windows firewall rules to allow incoming RDP traffic.

Collection:

- BianLian group employs malware, such as “system.exe,” to perform data collection activities on the compromised systems.
- The malware enumerates the system’s registry and files, allowing the actors to gather valuable information.
- Additionally, the actors copy clipboard data from users, potentially extracting sensitive information.

Exfiltration and Impact:

- BianLian group searches for sensitive files within the compromised systems using PowerShell scripts. These scripts assist in identifying valuable data for exfiltration.
- They use various methods for exfiltration, including File Transfer Protocol (FTP) and tools like Rclone, which enables them to sync files to cloud storage.
- BianLian group actors install exfiltration tools like Rclone in generic and typically unchecked folders such as programdata\vmware and music folders to avoid detection.
- Additionally, the group has been observed using the Mega file-sharing service for exfiltrating victim data, ensuring the stolen information is securely transferred.



```
Your network systems were attacked and encrypted. Contact us in order to restore your data. Don't
make any changes in your file structure: touch no files, don't try to recover by yourself, that may
lead to it's complete loss.

To contact us you have to download "tox" messenger: https://qtox.github[.]io/

Add user with the following ID to get your instructions:
A4B3B0845DA242A64BF17E0DB4278EDF4BF17E0DB4278EDF85855739667D3E2AE8B89D5439015F07E81D12D767FC

Alternative way: swikipedia@onionmail[.]org

Your ID: [Unique ID Assigned to Victim]

You should know that we have been downloading data from your network for a significant time before
the attack: financial, client, business, post, technical and personal files.
In 10 days - it will be posted at our site http://bianlianlbc5an4kgnay3opdemgcryg2
gnay3opdemgcryg2kpfcbgczopmm3dnbz3uaunad[.]onion with links send to your clients, partners,
competitors and news agencies, that will lead to a negative impact on your company: potential
financial, business and reputational loses.
```

BianLian Sample Ransome Note *(Look at this instruction.txt)*

- After exfiltration, BianLian group modifies all encrypted files with the “.bianlian” extension. They leave a ransom note named “Look at this instruction.txt” in each affected directory.
- The ransom note warns the victims about the encryption and exfiltration of financial, client, business, technical, and personal files. It threatens financial, business, and legal consequences if the ransom is not paid.
- If the victim refuses to pay the ransom, BianLian group threatens to publish the exfiltrated data on a leak site hosted on the Tor network.
- The group provides a Tox ID (A4B3B0845DA242A64BF17E0DB4278EDF85855739667D3E2AE8B89D5439015F07E81D12D767FC) for victim organizations to establish contact. They also offer alternative contact email addresses such as swikipedia@onionmail.org or xxx@mail2tor.com.
- The group receives ransom payments in unique cryptocurrency wallets assigned to each victim company.

Prevention:

1. Strengthen Remote Desktop Protocol (RDP) security:
   - Implement strong and complex passwords for all RDP accounts.
   - Enable multi-factor authentication (MFA) for RDP access.
   - Limit the number of RDP connections and implement account lockout policies.
2. Enhance Email Security:
   - Educate employees about phishing techniques and how to identify suspicious emails.
   - Implement email filtering and scanning solutions to detect and block malicious emails.
   - Enable email authentication mechanisms such as SPF, DKIM, and DMARC to prevent email spoofing.
3. Implement robust Endpoint Protection by enabling real-time scanning and automatic updates, regular updates and utilize behavior-based detection and intrusion prevention systems to identify and block malicious activities.
4. Enforce strong password policies.
5. Regularly patch and update systems and maintain a patch management process to promptly install security updates and patches.
6. Implement network segmentation to separate critical infrastructure and sensitive systems from regular network segments.
7. Use firewalls and access controls to restrict lateral movement within the network.
8. Enable tamper protection features in security solutions to prevent unauthorized modifications.
9. Implement security monitoring and analysis tools to detect and alert on suspicious activities or system changes.
10. Regularly back up critical data and ensure backups are stored offline or in a separate, secured network and test the restoration process to verify the integrity and availability of backup data.
11. Develop and regularly update an incident response plan to ensure a swift and coordinated response to security incidents.
12. Define roles and responsibilities, establish communication channels, and conduct periodic drills to validate the effectiveness of the plan.

Remediation:

1. Identify and Remove Compromised RDP Credentials:
   - Disable any compromised RDP accounts and change passwords for all RDP accounts.
   - Implement strong password policies and enable multi-factor authentication (MFA) for RDP access.
   - Monitor RDP logs for suspicious activities and investigate any unauthorized access attempts.
2. Detect and Remove Backdoors and Remote Management Tools:
   - Conduct a comprehensive security scan using reputable antivirus/anti-malware software to detect and remove any custom backdoors specific to the BianLian group.
   - Uninstall any unauthorized remote management tools such as TeamViewer, Atera Agent, SplashTop, or AnyDesk from affected systems.
3. Restore Antivirus Tools and Enable Tamper Protection:
   - Update antivirus/anti-malware software to the latest version and enable real-time scanning.
   - Restore any modifications made to the Windows Registry to re-enable tamper protection for security tools.
   - Ensure that Windows Defender and Anti-Malware Scan Interface (AMSI) are functioning correctly.
4. Conduct a Comprehensive System Scan and Cleanup:
   - Perform a full system scan using reputable security software to detect and remove any malware or malicious files associated with the BianLian group.
   - Remove any suspicious registry entries, files, or processes identified during the scan.
   - Regularly monitor the system for any signs of re-infection or unusual activities.
5. Review and Secure Network Configuration:
   - Review firewall rules and ensure that only necessary ports and services are exposed.
   - Implement network segmentation to isolate critical infrastructure and limit lateral movement.
   - Disable unnecessary protocols and services, such as SMB, if not required for business operations.
6. Reset Credentials and Enhance Password Security:
   - Reset passwords for all user accounts, especially privileged accounts and domain administrators.
   - Enforce strong password policies that require complex, unique passwords and regular password changes.
   - Consider implementing a password management solution to ensure password complexity and securely store credentials.
7. Conduct Security Awareness Training:
   - Provide cybersecurity awareness training to all employees to educate them about phishing techniques, social engineering, and safe browsing practices.
   - Encourage employees to report any suspicious emails, links, or activities to the IT or security team promptly.
8. Monitor and Respond to Anomalies:
   - Implement security monitoring tools and systems to detect and alert on any suspicious activities or indicators of compromise.
   - Establish an incident response process to investigate and respond to security incidents promptly.
   - Regularly review logs, network traffic, and system behavior to identify any signs of unauthorized access or data exfiltration.
9. Implement Regular Data Backups:
   - Regularly back up critical data and ensure backups are securely stored offline or in a separate network segment.
   - Test the restoration process periodically to verify the integrity and availability of backup data.
10. Engage with Law Enforcement and Cybersecurity Experts:
    - Report the incident to relevant law enforcement agencies, such as the FBI or local cybersecurity authorities.
    - Consider engaging with cybersecurity professionals or incident response teams to assist in the remediation process and forensic investigation.

Reference Link: #StopRansomware: BianLian Ransomware Group

Snake: FSB's Most Advanced Malware

- The Snake implant is a highly sophisticated cyber espionage tool developed and used by Russia's Federal Security Service (FSB) Center 16.
- It is designed for long-term intelligence collection on sensitive targets and operates through a covert peer-to-peer (P2P) network.
- Snake infrastructure has been identified in over 50 countries across North America, South America, Europe, Africa, Asia, and Australia, including the United States and Russia itself.
- While Snake uses infrastructure across various industries, its targeting is purposeful and tactical, focusing on government networks, research facilities, journalists, and other high-priority targets.
- Snake demonstrates exceptional sophistication in its stealth capabilities, adaptability, and software engineering design, making it one of the most advanced cyber espionage tools in the FSB's arsenal.
- The FSB has continuously updated and refined Snake to evade detection, employing encryption, fragmentation, and modifications to hamper identification and collection efforts.

Detection:

- The installer for Snake, known as "jpsetup.exe," is packed using a customized obfuscation technique that hides the unpacking code within a legitimate code base. It extracts an executable called "Stage 2" and an AES encrypted blob from its resources.
- The installer requires two command line arguments for execution. The first argument is a hashed string that serves as the AES key for decrypting the extracted resources. The second argument, after being modified, becomes the AES initialization vector (IV). Once decrypted, the extracted resources become the host artifacts of Snake.
- Snake's host components on Windows use obfuscation techniques to hide their presence. The malware employs a concealed storage mechanism, facilitated by a kernel module, to hide its components from the operating system. The kernel module also mediates requests between Snake's user mode components and the concealed storage, which is encrypted with a unique per-implant key. This unique keying makes it challenging to detect Snake's host components using simple signatures.
- To maintain persistence on a system, Snake registers a service named "WerFaultSvc" that executes Snake's components during boot. The components are decrypted and loaded into memory by executing a hidden instance of "WerFault.exe" from a legitimate Windows directory.
- Snake's encrypted registry key data, stored in the Windows registry, contains the AES key, IV, and path to Snake's kernel driver and kernel driver loader. The installer drops the kernel driver and a custom DLL into an encrypted file named "comadmin.dat" in the system32\Com directory. The encrypted registry blob holds the necessary information to decrypt this file.
- The Queue File is an important host-based artifact of Snake that resides in the %windows%\Registration directory. It contains various pieces of information required by Snake, such as key material,

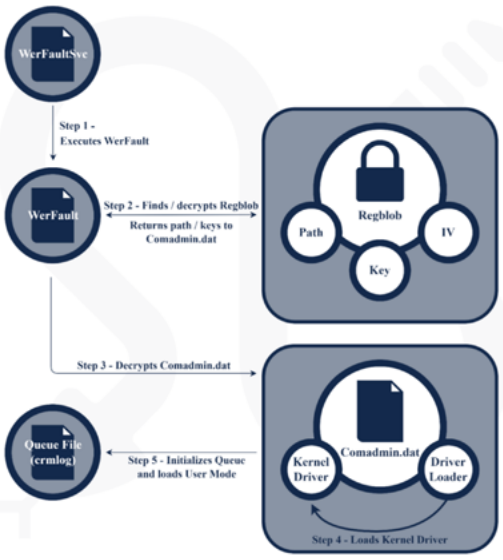


Fig 1 Snake Boot Cycle

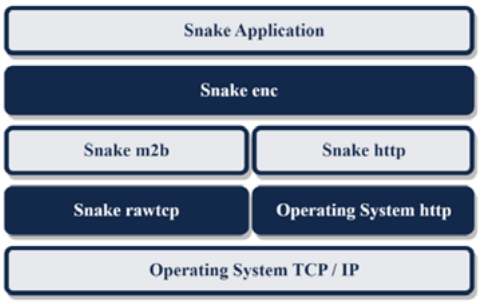


Fig 2 Snake Protocol Stack

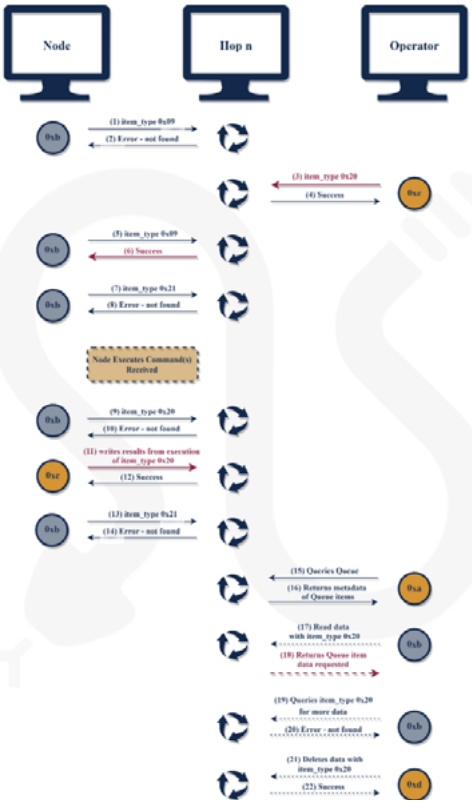


Fig 3 Passive Operations

communication channels, modes of operation, and the principal user mode component. The Queue File is encrypted using CAST-128, as are the individual Queue Items within it.

- Snake's network communications are encrypted and sent using custom methodologies over common network protocols such as HTTP, SMTP, and DNS. It uses a custom transport encryption layer and an application layer encryption mechanism to ensure secure communication between the controller and the command's destination. Snake's network traffic blends with legitimate traffic, making it difficult to detect without detailed knowledge of its custom protocols.
- Snake's kernel module enables stealthy network communications by allowing implanted machines to act as servers for other Snake nodes without opening new ports. The kernel module distinguishes Snake traffic from legitimate client traffic, reducing the effectiveness of simple IP address or domain blocking.
- Snake employs a specific authentication mechanism, called "ustart," to differentiate between Snake traffic and legitimate traffic. The kernel module intercepts the first client-to-server packet in every TCP session and authenticates it using a mathematical operation involving a random nonce and the ustart value. This technique allows Snake to function as server software without opening additional ports, making detection through network traffic monitoring more challenging.
- Snake also uses DNS queries for outbound communications. It encodes information in seemingly standard DNS queries by manipulating byte arrays and embedding data in the character string prior to the first '.' character.
- Snake operates using two main methods: Active and Passive. Active operations involve issuing commands from an operator or script to a target machine, while Passive operations allow the implant to communicate independently. During Passive operations, the implant beacons to communication channels stored within its 0x2 Container(s). It uses Queue Read commands to retrieve Queue Items intended for the beaconing implant, and it can exfiltrate data using Queue Write commands.
- To ensure resilience and persistence, Snake implants employ several mechanisms. They can create scheduled tasks or register as a Windows service to achieve persistence across system reboots. Additionally, the implants use various techniques to evade detection, such as masquerading as legitimate processes or modifying system files.
- Snake implants also have the capability to gather system information and perform reconnaissance. They can collect details about the infected system, including hardware and software configurations, network information, and user activity. This reconnaissance data is often used to identify potential targets or aid in future operations.
- Snake implants support a wide range of capabilities, including the ability to execute remote commands, upload and download files, modify the Windows Registry, capture screenshots, log keystrokes, and perform network reconnaissance. These capabilities provide the operators with extensive control and the ability to conduct targeted actions based on their objectives.
- Snake implants employ sophisticated anti-analysis and evasion techniques to avoid detection by security solutions. They may utilize encryption, obfuscation, and packing methods to conceal their code and behavior. The implants are designed to be highly modular, allowing operators to easily update or modify their functionality to adapt to evolving security measures.
- Snake implants communicate with command-and-control (C2) servers to receive instructions and transmit exfiltrated data. The C2 infrastructure is often designed to be resilient and flexible, with multiple layers of indirection to obfuscate the true location of the operators. This makes it difficult for defenders to attribute the attacks or disrupt the C2 infrastructure.
- The operators behind Snake are likely to be highly skilled and well-resourced adversaries, potentially state-sponsored threat actors. Their motives may vary, ranging from espionage and intelligence gathering to sabotage or disruption of targeted entities. The targeted victims are often high-value entities such as government organizations, defense contractors, or critical infrastructure sectors.

Prevention:

- **Keep software up to date:** Regularly apply patches and updates to operating systems, applications, and security software to address known vulnerabilities that could be exploited by Snake or similar malware.
- **Implement strong access controls:** Enforce the principle of least privilege by granting users only the necessary permissions to perform their tasks. This limits the potential impact of an infected user account.
- **Educate users about phishing and social engineering:** Train employees to recognize and avoid suspicious emails, attachments, and links. Encourage them to report any suspicious activity or potential security incidents promptly.
- **Deploy robust endpoint protection:** Use reputable antivirus/anti-malware solutions with real-time scanning and behavioral analysis capabilities. Ensure that the software is regularly updated and configured to scan all incoming files and email attachments.
- **Enable firewalls and intrusion detection/prevention systems:** Implement network security measures such as firewalls and intrusion detection/prevention systems to monitor and block malicious traffic. Regularly update and fine-tune these systems to stay ahead of emerging threats.
- **Apply application whitelisting:** Consider implementing application whitelisting to allow only approved and trusted applications to run on systems. This can help prevent the execution of unauthorized or malicious programs, including Snake implants.
- **Conduct regular vulnerability assessments and penetration testing:** Perform periodic assessments of your infrastructure to identify vulnerabilities and address them promptly. Conduct penetration testing to simulate real-world attacks and discover potential weaknesses that could be exploited by Snake or other malware.

Remediation:

- **Isolate infected systems:** If Snake or its implants are detected on a system, disconnect it from the network immediately to prevent further spread and damage. Isolate the affected system to minimize the impact on other devices and critical infrastructure.
- **Remove the malware:** Use up-to-date antivirus/anti-malware software to scan and remove the Snake malware and associated components from infected systems. Follow the recommended procedures provided by the security software vendor.
- **Restore from clean backups:** If available, restore affected systems from clean and verified backups taken before the infection occurred. This ensures that the malware and any modifications it made are completely removed.
- **Monitor and analyze network traffic:** Continuously monitor network traffic for any signs of re-infection or malicious activity associated with Snake. Analyze network logs and endpoints to identify any indicators of compromise (IOCs) and take appropriate action.
- **Strengthen security measures:** Review and enhance security controls based on the lessons learned from the incident. This may include updating security policies, implementing stronger access controls, and improving network segmentation to limit lateral movement.
- **Conduct post-incident analysis:** Investigate the source and cause of the infection to understand how Snake entered the network. Identify any vulnerabilities or gaps in security that enabled the attack and take steps to address them to prevent future incidents.
- **Enhance employee training and awareness:** Reinforce security awareness training for employees, emphasizing the importance of safe online practices, recognizing social engineering techniques, and reporting suspicious activities promptly.
- **Engage with incident response professionals:** If the scope or complexity of the Snake infection exceeds your organization's internal capabilities, consider engaging with external incident response experts to assist in containment, analysis, and remediation.

Lancefly: Group Uses Custom Backdoor to Target Orgs in Government, Aviation, Other Sectors

- New APT hacking group dubbed Lancefly uses a custom "Merdoor" backdoor malware to target government, aviation, and telecommunication organizations in South and Southeast Asia.
- Lancefly's malware called Merdoor is a powerful backdoor that appears to have existed since 2018. Researchers observed it being used in some activity in 2020 and 2021, as well as this more recent campaign, which continued in the first quarter of 2023.
- Backdoor is used very selectively, appearing on just a handful of networks and a small number of machines over the years, with its use appearing to be highly targeted. The attackers in this campaign also have access to an updated version of the ZXShell rootkit.
- Lancefly malware is focusing on cyber-espionage, aiming to collect intelligence from its victims' networks over extensive periods.

Detection:

- Researchers have found evidence that the threat group uses phishing emails, SSH credentials, brute forcing, and public-facing server vulnerabilities exploitation for unauthorized access.
- Once the attackers establish a presence on the target's system, they inject the Merdoor backdoor via DLL side-loading into either 'perfhost.exe' or 'svchost.exe,' both legitimate Windows processes that help the malware evade detection.
- Merdoor helps Lancefly maintain their access and foothold on the victim's system, installing itself as a service that persists between reboots. It establishes communications with the C2 server using one of the several supported communication protocols (HTTP, HTTPS, DNS, UDP, and TCP) and waits for instructions.
- Attackers use non-malware techniques for credential theft on victim machines:
  - PowerShell was used to launch rundll32.exe to dump the memory of a process using the MiniDump function of comsvcs.dll. This technique is often used to dump LSASS memory.
  - Reg.exe was used to dump the SAM and SYSTEM registry hives.
  - A legitimate tool by Avast was installed by the attackers and used to dump LSASS memory.

Legitimate Binary	Version	Date Assigned	Loader (Merdoor Loader)	Encrypted Payload (Merdoor Backdoor)
SiteAdv.exe (McAfee SiteAdvisor)	1.6.0.23	08/10/2006	SiteAdv.dll	SiteAdv.pak
ssr32.exe (Sophos SafeStore Restore)	1.3.0.1	11/17/2017	safestore32.dll	safestore.pak
chrome_frame_helper.exe (Google Chrome Frame)	27.0.1453.110	05/19/2013	chrome_frame_helper.dll	chrome_frame_helper.pak
wsc_proxy.eve (Avast wsc_ proxy)	1.0.0.3	10/28/2019	wsc.dll	proxycfg.pak
coInst.exe (Norton Identity Safe)	2014.7.3.12	06/26/2014	msvcr100.dll	coinstcfg.dat

Notable attack chain tools and TTPs

- **Impacket's Atexec:** A dual-use tool that can be used by malicious actors to create and run an immediate scheduled task on a remote target via SMB to execute commands on a target system. It is used by Lancefly for lateral movement across victim networks, also possibly for shellcode execution and evasion. It has been used to delete command line output files.
- **Suspicious SMB activity:** Suspicious SMB activity is seen on numerous victim machines. This is likely related to the use of Impacket by the threat actors.
- **WinRAR:** An archive manager that can be used to archive or zip files – for example, prior to exfiltration. It is not clear how the attackers exfiltrate the data from victim machines, but it is most likely via Merdoor.
- **LSSAS Dumper:** Allows the attackers to swiftly steal credentials they can then use to gain further access across victim networks.
- **NBTScan:** Open-source command-line NetBIOS scanner. This can be used to gather information on a network.

About ZXShell Rootkit

- The rootkit's loader, "FormDll.dll," exports functions that can be used to drop payloads that match the host's system architecture, read and execute shellcode from a file, kill processes, and more.
- The rootkit also uses an installation and updating utility that shares common code with the Merdoor loader, indicating that Lancefly uses a shared codebase for their tools.
- ZXShell's installation functionality supports service creation, hijacking, and launching, registry modification, and compressing a copy of its own executable for evasion and resilience.
- The loader for the rootkit is a 32-bit DLL with the export directory name "FormDll.dll" (SHA256: 1f09d177c99d429ae440393ac9835183d6fd1f1af596089cc01b68021e2e29a7).
- It has the following exports:
  - "CallDriver"
  - "DoRVA"
  - "KillAvpProcess"
  - "LoadSys"
  - "ProtectDllFile"

Indicators Of Compromise (IOCs):

Merdoor Backdoor

SHA256	Filename	Description
13df2d19f6d2719beeff3b882df1d3c9131a292cf097b27a0ffca5f45e139581	a.exe	Merdoor Dropper
8f64c25ba85f8b77cfba3701bebde119f610afef6d9a5965a3ed51a4a4b9dead	chrome_frame_helper.exe	Merdoor Dropper
8e98eed2ec14621feda75e07379650c05ce509113ea8d949b7367ce00fc7cd38	siteadv.exe	Merdoor Dropper
89e503c2db245a3db713661d491807aab3d7621c6aff00766bc6add892411ddc	siteadv.exe	Merdoor Dropper
c840e3cae2d280ff0b36eec2bf86ad35051906e484904136f0e478aa423d7744	siteadv.exe	Merdoor Dropper
5f16633dbf4e6ccf0b1d844b8ddfd56258dd6a2d1e4fb4641e2aa508d12a5075	chrome_frame_helper.dll	Merdoor Loader
ff4c2a91a97859de316b434c8d0cd5a31acb82be8c62b2df6e78c47f85e57740	chrome_frame_helper.dll	Merdoor Loader
14edb3de511a6dc896181d3a1bc87d1b5c443e6aea9eeae70dbca042a426fcf3	chrome_frame_helper.dll	Merdoor Loader
db5deded638829654fc1595327400ed2379c4a43e171870cfc0b5f015fad3a03	chrome_frame_helper.dll	Merdoor Loader
e244d1ef975fcebb529f0590acf4e7a0a91e7958722a9f2f5c5c05a23dda1d2c	chrome_frame_helper.dll	Merdoor Loader
f76e001a7ccf30af0706c9639ad3522fd8344ffbdf324307d8e82c5d52d350f2	chrome_frame_helper.dll	Merdoor Loader
dc182a0f39c5bb1c3a7ae259f06f338bb3d51a03e5b42903854cdc51d06fced6	smadhook64c.dll	Merdoor Loader
fa5f32457d0ac4ec0a7e69464b57144c257a55e6367ff9410cf7d77ac5b20949	SiteAdv.dll, chrome_frame_helper.dll	Merdoor Loader
fe7a6954e18feddeeb6fcdaaa8ac9248c8185703c2505d7f249b03d8d8897104	siteadv.dll	Merdoor Loader
341d8274cc1c53191458c8bbc746f428856295f86a61ab96c56cd97ee8736200	siteadv.dll	Merdoor Loader
f3478ccd0e417f0dc3ba1d7d448be8725193a1e69f884a36a8c97006bf0aa0f4	siteadv.dll	Merdoor Loader
750b541a5f43b0332ac32ec04329156157bf920f6a992113a140baab15fa4bd3	mojo_core.dll	Merdoor Loader
9f00cee1360a2035133e5b4568e890642eb556edd7c2e2f5600cf6e0bdcd5774	libmupdf.dll	Merdoor Loader
a9051dc5e6c06a8904bd8c82cdd6e6bd300994544af2eed72fe82df5f3336fc0	chrome_frame_helper.dll	Merdoor Loader
d62596889938442c34f9132c9587d1f35329925e011465c48c94aa4657c056c7	smadhook64c.dll	Merdoor Loader
f0003e08c34f4f419c3304a2f87f10c514c2ade2c90a830b12fdf31d81b0af57	SiteAdv.pak	Merdoor encoded payload
139c39e0dc8f8f4eb9b25b20669b4f30ffcbe2197e3a9f69d0043107d06a2cb4	SiteAdv.pak	Merdoor encoded payload
11bb47cb7e51f5b7c42ce26cbff25c2728fa1163420f308a8b2045103978caf5	SiteAdv.pak	Merdoor encoded payload
0abc1d12ef612490e37eedb1dd1833450b383349f13ddd3380b45f7aaabc8a75	SiteAdv.pak	Merdoor encoded payload
eb3b4e82ddfdb118d700a853587c9589c93879f62f576e104a62bdaa5a338d7b	SiteAdv.exe	Legit McAfee executable
1ab4f52ff4e4f3aa992a77d0d36d52e796999d6fc1a109b9ae092a5d7492b7dd	chrome_frame_helper.exe	Legit Google executable
fae713e25b667f1c42ebbea239f7b1e13ba5dc99b225251a82e65608b3710be7	SmadavProtect64.exe	Legit SmadAV executable

ZXShell Rootkit

SHA256	Filename	Description
1f09d177c99d429ae440393ac9835183d6fd1f1af596089cc01b68021e2e29a7	formdll.dll	Kernel driver loader
180970fce4a226de05df6d22339dd4ae03dfd5e451dcf2d464b663e86c824b8e	form.exe	Kernel driver loadpoint
a6020794bd6749e0765966cd65ca6d5511581f47cc2b38e41cb1e7fddaa0b221	update.exe	Kernel driver installation and update utility
592e237925243cf65d30a0c95c91733db593da64c96281b70917a038da9156ae	update.exe	Kernel driver installation and update utility
929b771eabef5aa9e3fba8b6249a8796146a3a4febfd4e992d99327e533f9798	formdll.dll	Kernel driver loader
009d8d1594e9c8bc40a95590287f373776a62dad213963662da8c859a10ef3b4	tdiproip.sys	Kernel driver x64
ef08f376128b7afcd7912f67e2a90513626e2081fe9f93146983eb913c50c3a8	tdiproip.sys	Kernel driver x32
ee486e93f091a7ef98ee7e19562838565f3358caeff8f7d99c29a7e8c0286b28	iehlpsrv.dll	Kernel driver x64 old
32d837a4a32618cc9fc1386f0f74ecf526b16b6d9ab6c5f90fb5158012fe2f8c	USBHPMS.sys	Kernel driver x32 old
d5df686bb202279ab56295252650b2c7c24f350d1a87a8a699f6034a8c0dd849	-	ZXShell

Others

SHA256	Filename	Description
a1f9b76ddfdafc47d4a63a04313c577c0c2ffc6202083422b52a00803fd8193d	ssmuidll.dll	Possible PlugX DLL loader
3ce38a2fc896b75c2f605c135297c4e0cddc9d93fc5b53fe0b92360781b5b94e	tosbtkbd.dll	Possible ShadowPad loader
210934a2cc59e1f5af39aa5a18aae1d8c5da95d1a8f34c9cfc3ab42ecd37ac92	klcsstd2.dll	Possible ShadowPad loader
530c7d705d426ed61c6be85a3b2b49fd7b839e27f3af60eb16c5616827a2a436	comhlpsvc.dll	Client to interact with driver
5018fe25b7eac7dd7bc30c7747820e3c1649b537f11dbaa9ce6b788b361133bf	comhlpsvc.dll	Client to interact with driver
efa9e9e5da6fba14cb60cba5dbd3f180cb8f2bd153ca78bbacd03c270aefd894	searchsrvc.exe	Client to interact with driver
a5a4dacddfc07ec9051fb7914a19f65c58aad44bbd3740d7b2b995262bd0c09e	comhlpsvc32.dll	Client to interact with driver
10b96290a17511ee7a772fcc254077f62a8045753129d73f0804f3da577d2793	a.exe	LDAP enumerator tool
0dcfcdf92e85191de192b4478aba039cb1e1041b1ae7764555307e257aa566a7	intel.exe	Mimikatz
415f9dc11fe242b7a548be09a51a42a4b5c0f9bc5c32aeffe7a98940b9c7fc04	tfc_windows_amd64.exe	GO Socks5 client
947f7355aa6068ae38df876b2847d99a6ca458d67652e3f1486b6233db336088	deliver.exe	Hacktool - CMD.exe injector
8d77fe4370c864167c1a712d0cc8fe124b10bd9d157ea59db58b42dea5007b63	tool.exe	Hacktool - webshell encoder
d8cc2dc0a96126d71ed1fce73017d5b7c91465ccd4cdcff71712381af788c16d	browser.exe	Infostealer
e94a5bd23da1c6b4b8aec43314d4e5346178abe0584a43fa4a204f4a3f7464b9	python27.dll	Recon DLL
5655a2981fa4821fe09c997c84839c16d582d65243c782f45e14c96a977c594e	frpc.exe	FRPC
19ec3f16a42ae58ab6feddc66d7eeecf91d7c61a0ac9cdc231da479088486169	ssf.exe	SSF
41d174514ed71267aaff578340ff83ef00dbb07cb644d2b1302a18aa1ca5d2d0	intel_drive.exe	LSASS dumping tool
67ebc03e4fbf1854a403ea1a3c6d9b19fd9dc2ae24c7048aafbbff76f1bea675	wsc.dll	BlackLoader
f92cac1121271c2e55b34d4e493cb64cdb0d4626ee30dc77016eb7021bf63414	wsc.dll	BlackLoader
859e76b6cda203e84a7b234c5cba169a7a02bf028a5b75e2ca8f1a35c4884065	smbver.exe	SMB enumeration Tool
fcdec9d9b195b8ed827fb46f1530502816fe6a04b1f5e740fda2b126df2d9fd5	smb2os.exe	SMB enumeration Tool

Others *(Continued)*

SHA256	Filename	Description
9584df964369c1141f9fc234c64253d8baeb9d7e3739b157db5f3607292787f2	ntmsvc.dll	PrcLoader
711a347708e6d94da01e4ee3b6cdb9bcc96ebd8d95f35a14e1b67def2271b2e9	ntmsvc.dll	PrcLoader
f040a173b954cdeadede3203a2021093b0458ed23727f849fc4c2676c67e25db	ntmsvc.dll	PrcLoader
90edb2c7c3ba86fecc90e80ac339a42bd89fbaa3f07d96d68835725b2e9de3ba	ntmsvc.dll	PrcLoader
b0d25b06e59b4cca93e40992fa0c0f36576364fcf1aca99160fd2a1faa5677a2	lsassunhooker.exe	LsassUnhooker
4c55f48b37f3e4b83b6757109b6ee0a661876b41428345239007882993127397	ladon.exe	Ladon
3e1c8d982b1257471ab1660b40112adf54f762c570091496b8623b0082840e9f	nbt.exe	NBTScan
9830f6abec64b276c9f327cf7c6817ad474b66ea61e4adcb8f914b324da46627	pot.exe	PortScan
79ae300ac4f1bc7636fe44ce2faa7e5556493f7013fc5c0a3863f28df86a2060	rubes.e	Rubeus

Prevention:

- Prevent with legitimate process which is used to install malicious malware.
- Use anti-cyrillic word techniques for domain detection.
- Do not click on the malicious link.
- Do not click on the spam & suspicious phishing emails.
- Do not use malicious/free VPN to access the web applications or network.
- Implement packet filtration & IDS/IPD mechanism through the firewall.
- Conduct security training and development for IT staff
- Implement network segmentation
- Do not install untrusted dll file.
- Patch all DLL files in production

Remediation:

- Conduct regular vulnerability assessments.
- Perform penetration testing to identify and remediate vulnerabilities.
- Develop and implement an incident response plan.
- Start incident procedures for investigation, and recovery
- Update the security policies.
- Apply security procedures for best practices and regulatory requirements.
- Foster a security-first culture.
- Update your machine & servers on monthly basis.
- Use paid VPN to access the web applications or network.
- Use trusted anti-malware programs.
- Deploy endpoint protection solutions.

Volt Typhoon and Other Chinese Groups Accused of Hacking the US and Others

- A hacker collective called Volt Typhoon has existed at least since 2017. The organization, which is thought to be state sponsored by China, is well-known for concentrating on information collecting and espionage. Numerous high-profile attacks, like the 2019 breach of the SolarWinds Orion software supply chain, have been connected to Volt Typhoon.
- Volt Typhoon so far appears to be focused on stealing information from "organizations" that hold data that relates to the military or government in the United States.
- China often rejects accusations of hacking, and it did so once more in the Volt Typhoon incident. However, evidence of Beijing's cyberspying operations has been accumulating for more than twenty years.
- Over the past ten years, the surveillance has come into sharper focus as Western researchers have linked breaches to specific People's Liberation Army units, and American law enforcement has accused several Chinese personnel of stealing American secrets.

Detection:

- Living off the land is one of the actor's main tactics, methods, and procedures (TTPs), and they use the built-in network administration tools to accomplish their goals. This TTP enables the actor to avoid endpoint detection and response (EDR) products that would alert on the introduction of third-party applications to the host and reduces the amount of activity that is captured in default logging configurations. It also enables the actor to blend in with regular Windows system and network activities. This actor employs several built-in utilities, including PowerShell, wmic, ntdsutil, and netsh.
- Numerous of the behavioural signs can also be actual system administration orders that manifest themselves in normal activities. It's important to use caution when drawing conclusions without conducting more research or looking for other signs of a compromised system.
- The actor has used Earthworm and a custom Fast Reverse Proxy (FRP) client with hardcoded C2 callbacks to ports 8080, 8443, 8043, 8000, and 10443 with various filenames including, cisco_up.exe, cl64.exe, vm3dservice.exe, watchdogd.exe, Win.exe, WmiPreSV.exe, and WmiPrvSE.exe.
- To do password cracking, the actor may attempt to remove the SYSTEM registry hive and the ntds.dit file from Windows domain controllers (DCs) from the network. The primary Active Directory (AD) database file, ntds.dit, is by default located at %SystemRoot%NTDSntds.dit. All domain users' usernames, password hashes, group memberships, and other information are stored in this file; the SYSTEM registry hive has the boot key that is used to encrypt data in the ntds.dit file. Another source for the SYSTEM registry hive is the Shadow Copy.
  - cmd /c vssadmin create shadow /for=C: > C:\Windows\Temp\<filename>.tmp
  - cmd /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Windows\NTDS\ntds.dit C:\Windows\Temp > C:\Windows\Temp\<filename>.tmp

Prevention:

- Block unknown scripts to run.
- Patch all DLL files in production.
- Do not click on the malicious link.
- Use anti-proxy techniques to avoid malicious IP sources.
- Disallow the RDP feature for unknown connection.
- Do not install unwanted application from untrusted source.
- Do not use malicious/free VPN to access the web applications or network.
- Implement packet filtration & IDS/IPD mechanism through the firewall.
- Enable SSL with SMTP protocol for safe transmission.
- Enable limitations on administrative access or rights.

Prevention:

- Monitor event logs for ntdsutil.exe and similar process creations.
- Administrators should limit port proxy usage within environments.
- Download only trusted software's from known sites.
- Use post method for sending & retrieving of data through communication channel.
- Update your machine & servers on monthly basis.
- Enable packet filtration through firewall.
- Configure DLP in environment in a proper way.
- Update the operating system (OS) and all programs installed programs.
- Use paid VPN to access the web applications or network.
- Use trusted anti-malware programs.
- Enable two factor authentication for transferring data packets.

TOP THREAT ACTORS

Threat Actor	IOC Reference
Volt Typhoon	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
Lancefly	https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor
BianLian	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a
Snake	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a

TOP EXPLOITED VULNERABILITIES

Threat	Description	Reference Link
ZeroDay Microsoft Windows Boot Manager BlackLotus UEFI bootkit vulnerability in Outlook CVE-2023-24932	Vulnerability can be exploited by installing a boot policy susceptible to the exploit. This would enable the attacker to gain unauthorized access to the device's boot process and execute malicious code.	Another Outlook Zero Day Vulnerability with May 2023 Patch Tuesday
ZeroDay Apple's WebKit browser platform vulnerability in Apple Devices CVE-2023-32409 CVE-2023-28204 CVE-2023-32373	CVE-2023-32409 is a vulnerability in which a remote attacker is "able to break out of Web Content sandbox. CVE-2023-28204 entails processing Web content that may disclose sensitive information. CVE-2023-32373 warns that processing "maliciously crafted Web content may lead to arbitrary code execution."	Apple Patches 3 Zero-Days Possibly Already Exploited
Trend Micro Mobile Security for Enterprises widget WFUser Authentication Bypass Vulnerability CVE-2023-32523	Vulnerability allows remote attackers to bypass authentication on affected installations of Trend Micro Mobile Security for Enterprises. The issue results from improper implementation of the authentication mechanism. The issue results from improper implementation of the authentication mechanism.	SECURITY BULLETIN: May 2023 Security Bulletin for Trend Micro Mobile Security (Enterprise)
Delta Electronics InfraSuite Device Master Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2023-1133	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Delta Electronics InfraSuite Device Master. The specific flaw exists within the installed instance of Apache ActiveMQ, which utilizes an outdated version of the JDK.	ZDI-23-683 | Zero Day Initiative
Linux Kernel ksmbd Tree Connection Race Condition Remote Code Execution Vulnerability CVE-2023-32254	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Linux Kernel. Authentication is not required to exploit this vulnerability, but only systems with ksmbd enabled are vulnerable.	CVE-2023-32254: Linux Kernel ksmbd race condition (vuldb.com)
Schneider Electric APC Easy UPS Online update-Password Authentication Bypass Vulnerability CVE-2022-42970	Vulnerability allows remote attackers to bypass authentication on affected installations of Schneider Electric APC Easy UPS Online. The specific flaw exists within the updatePassword function.	ZDI-23-636 | Zero Day Initiative
KeySight N8844A Data Analytics Web Service Unmarshal Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2023-1967	Vulnerability allows remote attackers to execute arbitrary code on affected installations of KeySight N8844A Data Analytics Web Service. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data.	CVE 2023 1967 | INCIBE-CERT | INCIBE
Microsoft Windows Active Directory Certificate Services Improper Authorization Privilege Escalation Vulnerability CVE-2022-34691	Vulnerability allows network-adjacent attackers to escalate privileges on affected installations of Microsoft Windows Active Directory Certificate Services. An attacker can leverage this vulnerability to escalate privileges and disclose stored credentials, leading to further compromise.	ZDI-23-722 | Zero Day Initiative

TOP EXPLOITED VULNERABILITIES

Threat	Description	Reference Link
D-Link D-View Use of Hard-coded Cryptographic Key Authentication Bypass Vulnerability CVE-2023-32169	Vulnerability allows remote attackers to bypass authentication on affected installations of D-Link D-View. The specific flaw exists within the TokenUtils class. The issue results from a hard-coded cryptographic key.	Critical Vulnerabilities in D-Link Products (csa.gov.sg)
(Zero-Day) Wacom Drivers for Windows Link Following Local Privilege Escalation Vulnerability CVE-2023-32163	Vulnerability allows local attackers to escalate privileges on affected installations of Wacom Drivers for Windows. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	CVE-2023-32163: Wacom Driver Local Privilege Escalation (vuldb.com)
Moxa MXsecurity Series Hardcoded JWT Key Authentication Bypass Vulnerability CVE-2023-33236	Vulnerability allows remote attackers to bypass authentication on affected installations of Moxa MXsecurity Series appliances. The issue results from a hardcoded JWT secret within the application configuration	Credential Vulnerabilities (moxa.com)

Security Bulletin

1. Royal Ransomware Expands to Target Linux, VMware ESXi

- The Royal ransomware group — which is made up of former members of the Conti gang — has ramped up operations since bursting on the scene last summer, mounting attacks against critical infrastructure and healthcare targets in particular. Most recently, it has expanded its arsenal to target Linux and VMware ESXi environments.
- That's according to Palo Alto Networks' Unit 42 division, who noted in an analysis released May 9 that the group has recently launched a variant of its encryptor malware built in the form of executable and linkable format (ELF) binary.
- "[It] is quite similar to the Windows variant, and the sample does not contain any obfuscation," the researchers explained in the posting. "All strings, including the RSA public key and ransom note, are stored as plaintext."
- Conti, which was responsible for the Ryuk ransomware, famously disbanded last May when the gang's developers began shutting down admin panels, servers, proxy hosts, chatrooms, and a negotiations service site — likely in response to law enforcement and media attention. At the time, researchers noted that it would be likely that members would regroup under new guises — and that's exactly what appears to have occurred.

2. Malware Disguised as ChatGPT Apps are Being Used to Lure Victims

- Facebook's parent company, Meta has marked a warning for public that the hackers are now taking advantage of people's interest in the new AI tools like – ChatGPT to trick the users into secretly installing the malware that pretends to provide the AI functionality.
- In the last 2 months, Meta had discovered about 10 new malware families using AI themes to compromise multiple business which are internet supported—including social media business accounts and locked over 1,000 unique Chat GPT- themed malicious URLs from being shared at their platform.
- Meta had detected malware strains like Ducktail and NodeStealer that were available in ChatGPT browser plugins and in multiple productive tools that are attributing to Vietnam-based hackers.
- Ducktail steals the browser cookies, and it also hijacks Facebook sessions to retrieve victim's account's information such as location data and two-factor authentication codes.
- Meta during the starting of January, discovered that the Nodestealer malware strain had been targeting the Windows-based browsers with the intention of stealing the cookies and saves the login details such as – usernames and passwords to compromise credentials of Facebook, Gmail and Microsoft Outlook of victims. "NodeStealer" is basically the customised Javascript and bundles the Node,js environment.

- As the response to this malware strains are specifically targeting Facebook business accounts, the company had also launched the new security features for the accounts. Meta had also introduced a new support tool that guides the users step-by-step to identify and remove the malware. Meta will also be launching Facebook at-work accounts through which a business account can be operated without requiring a personal account. This is likely to be launched later this year.

3. Meta Hit With $1.3B Record-Breaking Fine for GDPR Violations

- Meta, owner of Facebook and Instagram, had been fined $1.3 billion (€1.2 billion) for violating the European Union's General Data Protection Regulation (GDPR) by the Irish Data Protection Commission, for the transfer of EU users' personal data to US servers. This instance is the biggest penalty that's been dealt out after the European Union's strict data privacy policies went into effect in 2016; this fine had surpassed even the Amazon's previously record-breaking $808 million (€746 million) tab in 2021 due to data protection violations.

4. Credential Harvesting Tool Legion Targets Additional Cloud Services

- A commercial malware tool named as Legion is deployed by hackers on the compromised web servers that have been updated to extract credentials for additional cloud services to authenticate over SSH. The main goal of this Python –based script tool is to harvest the credentials stored in the configuration files for the Email providers, cloud service providers, server management systems, databases and payment systems. These compromised resources enable the attackers to launch email and SMS spam campaigns.
- The end goal of the attackers for using Legion is to launch the mass spam campaigns via sending emails and SMS by using hijacked Simple Mail Transfer Protocol (SMTP) credentials of the users. Some services also provide the email to SMS functionality via SMTP and the Legion contains a script for sending out the SMS in this way to most US mobile carriers.
- Attackers deploy Legion by exploiting the vulnerabilities in PHP, Apache or content management solutions which allow hackers to deploy webshells or remotely execute code on the vulnerable servers. Legion then leverages common misconfigurations in web server permissions, PHP applications or PHP frameworks such as Laravel to access configuration files and files containing environment variables that the attackers know are stored in specific locations.

5. Lemon Group Uses Millions of Pre-Infected Android Phones to Enable Cybercrime Enterprise

- Without the consent of the mobile users, the operators of the Lemon Group have pre-infected the user's devices before they even bought them, and now they are quietly using the infected phones as the tool for stealing and selling SMS messages and one-time passwords (OTPs), serving up unwanted ads, setting up online messaging and social media accounts, and other purposes.
- Lemon Group has claimed it and has a base of nearly 9 million Guerrilla-infected Android devices that its customers can abuse in different ways. But Trend Micro believes the actual number may be even higher then these.
- Trend Micro researchers had first began identifying the operation when doing forensic analysis on the ROM image of an Android device infected with malware dubbed "Guerrilla." Their investigation showed the group has infected devices belonging to Android users in 180 countries. More than 55% of the victims are from Asia, some 17% are in North America and nearly 10% in Africa.

REFERENCE LINKS

- https://www.bleepingcomputer.com/news/security/fake-ransomware-gang-targets-us-orgs-with-empty-data-leak-threats/?&web_view=true
- https://www.darkreading.com/remote-workforce/zaraza-bot-targets-google-chrome-extract-login-credentials
- https://www.darkreading.com/remote-workforce/google-emergency-chrome-update-zero-day-bug
- https://www.csoonline.com/article/3693712/app-cyberattacks-jump-137-with-healthcare-manufacturing-hit-hard-akamai-says.html#tk.rss_news
- https://cyware.com/news/new-scam-alerts-users-about-youtube-altering-policy-d158f61b
- https://www.darkreading.com/attacks-breaches/major-us-cfpb-data-breach-employee
- https://www.darkreading.com/attacks-breaches/3cx-supply-chain-attack-originated-from-breach-at-another-software-company
- https://www.darkreading.com/mobile/global-spyware-attacks-spotted-new-old-iphones-global-attacks
- https://www.darkreading.com/remote-workforce/researchers-discover-first-ever-major-ransomware-targeting-macos
- https://www.darkreading.com/attacks-breaches/russian-fancy-bear-apt-exploited-unpatched-cisco-routers-to-hack-us-eu-government-agencies
- https://www.bleepingcomputer.com/news/security/ex-conti-members-and-fin7-devs-team-up-to-push-new-domino-malware/
- https://www.cyfirma.com/outofband/the-rise-of-fusioncore-an-emerging-cybercrime-group-from-europe/
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor
- https://www.bleepingcomputer.com/news/security/stealthy-merdoor-malware-uncovered-after-five-years-of-attacks/
- Lemon Group Uses Millions of Pre-Infected Android Phones to Enable Cybercrime Enterprise (darkreading.com)
- Credential harvesting tool Legion targets additional cloud services | CSO Online
- Meta Hit With $1.3B Record-Breaking Fine for GDPR Violations (darkreading.com)
- Malware disguised as ChatGPT apps are being used to lure victims, Meta says | CSO Online
- Royal Ransomware Expands to Target Linux, VMware ESXi (darkreading.com)
- Microsoft Digital Defense Report: Key Cybercrime Trends (darkreading.com)
- WordPress Plug-in Used in 1M+ Websites Patched to Close Critical Bug (darkreading.com)
- Severe RCE Bugs Open Thousands of Industrial IoT Devices to Cyberattack (darkreading.com)
- US sanctions four North Korean entities for global cyberattacks | CSO Online
- Secureframe Finds 37% of Organizations Reuse Passwords for Cloud Service Providers (darkreading.com)
- People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection | CISA

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**.

55 North Water Street
Norwalk, CT 06854

203.866.8886

sdgc.com