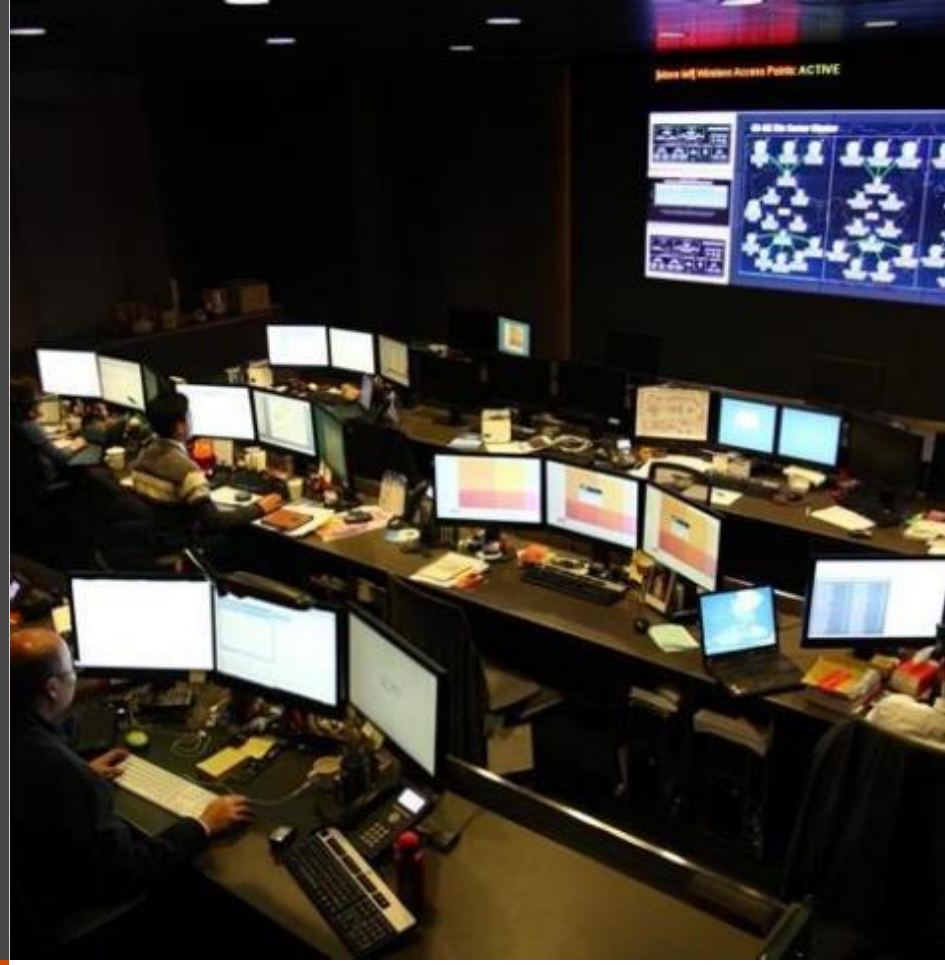
Cyber Threat Intelligence Weekly Report

TLP: AMBER



21 December 2024 – 27 December 2024

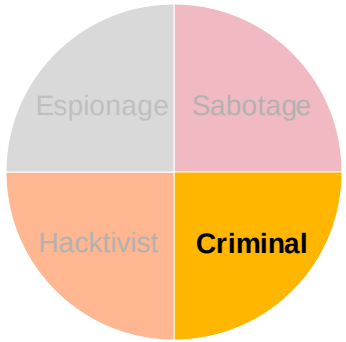
pwc

Table of Contents

Emerging Ransomware Family NotLockBit Takes Inspiration from the Infamous LockBit

Global

No specific industry targeting



Destructive	**Data Exfiltration**
Malware	Attack on Cloud Services
DDoS	Operational Technology Compromise
Web Defacement	Malicious Insider
Business Email Compromise	Supply Chain
Cryptojacking	**Ransomware**

MITRE ATT&CK TTPs

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
		Phishing	Command and Scripting Interpreter	Boot or Logon Autostart Execution: Login Items	Create or Modify System Process: Windows Service	Indicator Removal: Timestomp							
		Exploit Public-Facing Application			Exploitation for Privilege Escalation								
					Abuse Elevation Control Mechanism: Sudo and Sudo Caching								

Details (Analysis in Appendices)

Researchers have discovered the evolving attack processes of the emerging NotLockBit ransomware family. Mimicking the notorious LockBit gang, the new ransomware group displays similar branding, tactics and behavior, with the distinguishing ability of fully functional cross platform targeting of macOS an Windows systems. It is able to leverage this capability through Go programming language.

The NotLockBit ransomware campaign demonstrates a highly sophisticated execution chain which abuses AES-based encryption, strategic file targeting, and AWS S2 for successful system information collection, data encryption, and data exfiltration. The malware includes a self deletion mechanism as well as a psychological manipulation strategy which changes the desktop wallpaper screen for ransomware visibility. It is expected for the threat to continue evolving and mimicking well-known ransomware families while minimising forensic trace through self-deletion.

Recommendations

Prevention

- Enforce a layered defense strategy incorporating secure network security protocols (including but not limited to firewall, proxy filtering, intrusion detection systems (IDS), intrusion prevention systems (IPS), secure VPNs and security gateways).
- Employ network segmentation to limit the spread of malware during incidents of endpoint compromisation.

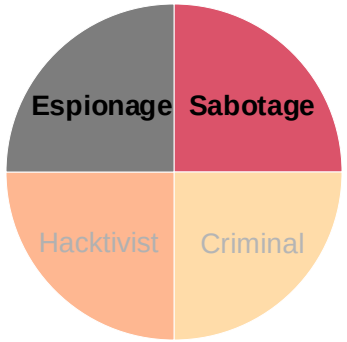
Detection

- Implement an Endpoint Detection and Response solution to continuously monitor endpoints, detect anomalies and quickly respond to threats via isolation and remediation.
- Monitor network traffic for unusual patterns that may indicate data exfiltration or command control server communication.

Evolving Threats: Lazarus Group's Latest Malware Campaign

Global

Defense, Aerospace, Cryptocurrency



Destructive	Data Exfiltration
Malware	Attack on Cloud Services
DDoS	Operational Technology Compromise
Web Defacement	Malicious Insider
Business Email Compromise	Supply Chain
Cryptojacking	Ransomware

MITRE ATT&CK TTPs

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
		Exploit Public-Facing Application	User Execution: Malicious File	Hijack Execution Flow: DLL Side-Loading		Process Injection					Data Encoding		
											Encrypted Channel		
											Web Service		

Details (Analysis in Appendices)

Over the past few years in a campaign known as the DeathNote campaign or “Operation DreamJob” the Lazarus group has been spreading its malicious software by posting fake job listings to target employees in industries such as defense, aerospace, cryptocurrency, and other sectors worldwide.

Researchers have recently discovered a new campaign conducted by the Lazarus group that shows a significant update in their infection chain, leveraging both previous used malware and new updated malware to tailor their attacks. The new attack observed involves the delivery of archive files containing malicious content by the Lazarus group to at least two individuals linked with the same nuclear-related organisation within the span of a month. Upon investigation, researchers unravelled a sophisticated infection chain comprising various malware forms, including a downloader, loader, and backdoor. We highlight Lazarus’ latest campaign given their historic targeting of victims in Hong Kong and wider APAC.

Recommendations

Prevention

- Conduct regular security awareness training to recognize suspicious job offers or skill assessment requests.
- Implement advanced email filtering to detect and block malicious attachments, especially ISO and ZIP files.

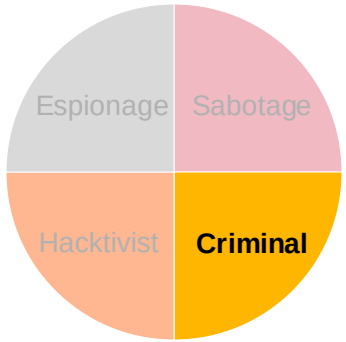
Detection

- Use behavioral analysis tools to detect anomalies in user behavior, such as unusual file downloads or execution of unknown software.
- Implement rules and alerts specific to the TTPs used by Lazarus, such as those related to VNC and DLL side-loading.
- Utilize advanced detection tools like EDR (Endpoint Detection and Response) and SIEM (Security Information and Event Management) systems to identify and respond to threats in real-time.

The “You She” Group Distributes Malicious Installers Through Phishing Websites

China

Unspecified



Destructive	**Data Exfiltration**
Malware	Attack on Cloud Services
DDoS	Operational Technology Compromise
Web Defacement	Malicious Insider
Business Email Compromise	Supply Chain
Cryptojacking	Ransomware

MITRE ATT&CK TTPs

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
		Phishing		Scheduled Task/Job		Msiexec				Clipboard Data	Non-Application Layer Protocol		
						Encrypted/Encoded File				Data from Local System			
						Match Legitimate Name or Location							
						Disable or Modify Tools							

Details (Analysis in Appendices)

The “You She” black industry Group (a.k.a. “Yin Hu”, “UTG-Q-1000”, etc.) has launched a large number of attacks against Chinese users since 2022. The group mainly spreads malware through instant messaging software, SEO, phishing emails, and watering hole websites, so as to steal data or commit fraud. The group has many malicious file variants, and frequently changes its anti-virus evasion techniques. Recently, the security team has observed its latest attack to distribute malicious MSI files through phishing websites that contain counterfeit software.

In this attack, the “You She” group used the phishing websites that impersonate the download sites of remote control software such as ToDesk and Sunlogin to spread malicious programs. In addition, the group used fake Gmail and other email login pages to send phishing emails for attacks. The malicious program distributed by the group downloads and executes components used to steal cryptocurrency wallet addresses and keys.

Recommendations

Prevention

- Raise security awareness among employees to download software from official channels.
- Verify the legitimacy of the URL and the current website when accessing a login page.

Detection

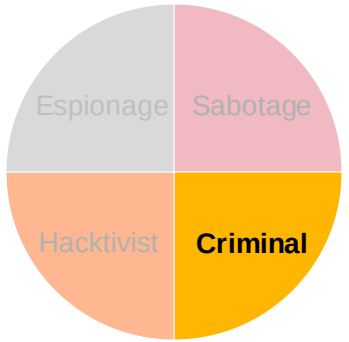
- Users should retrieve the historical log records and set alerts for the indicators of compromise (IOC) listed in the appendix to this article.
- Check whether there is a folder named “MM” in the path “C:\Users\Public\Document\”, and if yes, further check for suspicious exe and dll files.

Appendices / Technical Analysis

Emerging Ransomware Family NotLockBit Takes Inspiration from the Infamous LockBit – Technical Analysis

Global

No specific industry targeting



Destructive	**Data Exfiltration**
Malware	Attack on Cloud Services
DDoS	Operational Technology Compromise
Web Defacement	Malicious Insider
Business Email Compromise	Supply Chain
Cryptojacking	**Ransomware**

Technical Analysis

Researchers have identified the evolving execution chain of the new NotLockBit ransomware family. This new ransomware mimics the infamous and persistent LockBit ransomware, indicating that new threat actors are looking towards historically successful and established ransomware to mimic their behaviors, tactics, and branding NotLockBit, however, is distinct from the LockBit ransomware by its ability to execute on both macOS and Windows. The new malware is written in Go programming language which facilitates cross-platform compatibility, robust performance and fast development cycles.

During the initial reconnaissance phase, in the case of macOS, NotLockBit gathers critical system information which allows the malware to adapt its behavior based on the target system specifics. The ransomware begins by using the `go-sysinfo module` to gather detailed system information regarding the host's hardware, software, and network configuration. In the next step, the malware uses a public key encoded in Privacy enhanced Mail (PEM) format. NotLockBit then generates a random value that is encrypted using RSA details (exponent and modules) from the PEM file. These components are used by the RSA encryption to securely encrypt the random value so its decryption is only enabled by a corresponding private key. NotLockBit was then observed retrieving the collected information and storing it in a file named `encrypted-master-key.txt` on the user desktop. In other observed samples, the text file with the stored data was named `Readme.txt`. These text files included details about the encrypted key, machine architecture, timestamp, IP information, machine version information, and Machine UUID. The ransomware then utilizes `StaticCredentailsProvider` from the AWS Software Development Kit for Go v2 library to configure static credentials.

In the data exfiltration step, NotLockBit transfers files to a storage repository configured as an Amazon S3 bucket or other remote storage server in the threat actor's control. This step grants threat actors continuous access to the victim's sensitive information, allowing for potential double extortion tactics. NotLockBit completes data encryption by scanning the file system and skipping directories such as `/proc/, /sys/, /dev/, /usr/,` and `/run/` rather opting to target file systems with certain extensions, and focusing on personal and professional data as well as virtual machine files. The malware references a predefined list of extensions including .csv, .doc, .png, .jpg, .txt, .vdmk, .vmsd, and .vbox which refer to common formats such as documents, image files, and other data types that are commonly used in personal and professional contexts. AES is then used to encrypt file contents, and RSA may be used to secure this process. The ransomware then deletes the original file ensuring recovery is not possible without the decryption key.

Post exploitation, NotLockBit uses the `osascript` command to replace the desktop wallpaper with a custom LockBit ransom banner. On MacOs, AppleScript code is used from the command line with the script `"tell application "System Evens" to tell every desktop to set picture to "%s"."` This psychological manipulation strategy increases the ransomware visibility to its victim. Post wallpaper change, self deletion is triggered leading to the deletion of the shadow copy.

Conclusion

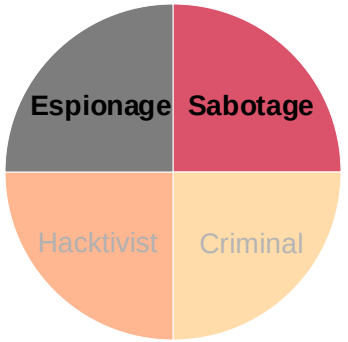
NotLockBit represents a evolving ransomware family that mimics the successful and infamous LockBit group which has been known to target victims in Hong Kong. It remains imperative to be wary of this malware's adaptability and implement proactive prevention and detection solutions. Furthermore, through our continuous tracking of the ransomware landscape, we continue to observe new, smaller ransomware groups arising, leveraging 'tried and tested' approaches to ransomware attacks, as well as new capabilities to expand their targeting for ransomware encryption.

Reference: blog.qualys.com/vulnerabilities-threat-research/2024/12/18/notlockbit-a-deep-dive-into-the-new-ransomware-threat#detections-threat-hunting

Evolving Threats: Lazarus Group's Latest Malware Campaign – Technical Analysis

Global

Defense, Aerospace, Cryptocurrency



Destructive	Data Exfiltration
Malware	Attack on Cloud Services
DDoS	Operational Technology Compromise
Web Defacement	Malicious Insider
Business Email Compromise	Supply Chain
Cryptojacking	Ransomware

Technical Analysis

As part of their DeathNote campaign, Lazarus had conducted their supply chain attacks in two methods. The first method is conducted by sending a malicious document or a trojanized PDF viewed that showcasing a job description that is tailored to that particular individual's job experience. The second method that Lazarus has historically adopted is distributing trojanized remote access tools such as VNC or PuTTY to prompt targets to connect to a designated server for skill evaluations.

In the most recent incident, Lazarus utilised the second approach, however except the initial vector, the remaining techniques and tactics used in their infection chain has all been updated. In this case the targets all received at least three archive files that were designed to mimic skills assessments for IT positions at renowned aerospace and defense companies. To avoid detection, Lazarus sent harmful compressed ISO files to its targets as ZIP archives are frequently flagged by security services. While ZIP archives were prevalent in past instances, it is suspected that the initial file was also in ISO format. The method of downloading these files by the victims remains unclear, however it is suspected that the ISO file was obtained through a Chromium-based browser. Within the first VNC-related archive, a corrupted VNC was discovered, while the second held both a genuine UltraVNC Viewer and a malevolent DLL file.

The initial ISO image includes a ZIP file containing `AmazonVNC.exe` and `readme.txt`. AmazonVNC.exe is a modified version of TightVNC, an open-source software. When launched, `AmazonVNC.exe` displays a window prompting the user for an IP address and password stored in the readme.txt file. Victims were likely instructed to use this IP through messaging platforms like LinkedIn or Telegram, where Lazarus often poses as recruiters. Upon entering the IP, an XOR key is generated to decrypt the VNC executable's internal resources, revealing a downloader called Ranid Downloader, executed by `AmazonVNC.exe` for further malicious activities. In a separate file named `[Company name]_Skill_Assessment_new.zip`, a legitimate `vncviewer.exe` from UltraVNC is embedded. This ZIP file also contains `vnclang.dll`, a malicious file loaded through side-loading.

One of the malware instances found is CookieTime, however the delivery method remains uncertain. Following the LPEClient installation, CookieTime operates as the SQLExplorer service. Initially, it directly receives and executes commands from the C2 server, later transitioning to downloading payloads. CookieTime downloads various malware strains, including LPEClient, Charamel Loader, ServiceChanger, and an updated CookiePlus version. Charamel Loader decrypts and loads internal resources with a key using the ChaCha20 algorithm.

ServiceChanger halts a legitimate service, ssh-agent, to introduce malicious files, like `libcrypto.dll`, via DLL side-loading when the service restarts. Contrary to Kimsuky's approach of registering a new service, Lazarus exploits existing services for DLL side-loading. CookiePlus, a new plugin-based malware discovered on Host C, is initiated by ServiceChanger and Charamel Loader. While both loading methods differ slightly, the behavior remains consistent. Initially disguised as ComparePlus, a Notepad++ plugin, recent samples masquerade as DirectX-Wrappers, hinting at a shift in Lazarus's tactics. CookiePlus acts as a downloader, transmitting limited data to the C2 server for authentication. The payload undergoes encryption and decryption processes, with the potential for continuous payload downloads until the C2 server ceases communication. Various shellcodes, converted DLLs, are executed and sent to the C2 server.

Conclusion

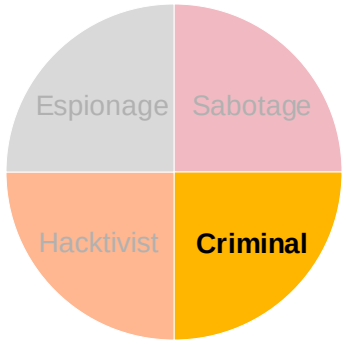
Lazarus represents the continuing sophistication of advanced persistent threat (APT) actors, particularly those originating from North Korea. Historically the group predominately used only a few types of malware like Mata and Gopuram Loader. However they've recently introduced the use of new modular malware like CookiePlus. As CookiePlus behaves just like a downloader, it is difficult to investigate whether CookiePlus downloaded just a small plugin or the next meaningful payload.

Reference: https://securelist.com/lazarus-new-malware/115059/

The “You She” Group Distributes Malicious Installers Through Phishing Websites – Technical Analysis

China

Unspecified



Destructive	**Data Exfiltration**
Malware	Attack on Cloud Services
DDoS	Operational Technology Compromise
Web Defacement	Malicious Insider
Business Email Compromise	Supply Chain
Cryptojacking	Ransomware

Technical Analysis

In this attack, the “You She” group distributed a malicious MSI disguised as remote control software. Once executed, the MSI releases the normal ToDesk downloader and a malicious program named “aaaInstall9.exe” (i.e. aaa安装9.exe) into the installation path chosen by the user, and executes the malicious program. Also, the malicious MSI creates a shortcut on the desktop that links to the normal ToDesk downloader in order to confuse users. Upon execution, “aaaInstall9.exe” downloads a shellcode file from the hardcoded URL and saves it as the file “C:\ProgramData\3”. The malicious program then reads the file, requests a segment of memory space according to the file size, and writes the contents of the file into the requested space for execution. This shellcode, once executed, decrypts its own code by XOR decryption. After decryption, the shellcode continues to request a segment of memory space, writes the PE file embedded in it to that segment, specifies the memory protection attribute as PAGE_EXECUTE_READWRITE, and then executes the PE file. This PE file is actually a DLL file, formerly known as “1.dll”.

Once executed in the memory, “1.dll” checks whether the file “C:\Users\Public\Documents\MM\svchos1.exe” exists. If the file does not exist, it checks whether the current process has administrator privileges, and if not, it re-executes the current process with administrator privileges. After confirming that the current process has administrator privileges, “1.dll” executes the cmd command to create the MM folder in the path “C:\Users\Public\Documents”, and copies “aaaInstall9.exe” to the folder and renames it “svchos1.exe”. Subsequently, “1.dll” creates two threads to download “4.txt” and “7.txt” from the specified URLs to “C:\Users\Public\Documents\MM”, and loads and executes the two shellcodes. After the aforementioned operations are completed, “1.dll” executes its Shellex function.

When the shellcode “4.txt” is called, it also uses the XOR algorithm for self-decryption, and then writes the embedded PE file into memory for execution. The original name of this PE file is “RpcTsch.dll”, and the pdb path is “C:\Users\ZZ\Desktop\RpcTsch\Release\RpcTsch.pdb”. “RpcTsch.dll” creates a scheduled task named “MM” via RPC, which is used to execute “C:\Users\Public\Documents\MM\svchos1.exe” when any user logs in. The other shellcode “7.txt” also writes the embedded PE file into memory for execution after decryption. The original name of the PE file is “Dll1.dll”, and the pdb path is “C:\Users\ZZ\Desktop\Screenshot\Release\Dll1.pdb”. The function of “Dll1.dll” is to continuously monitor the clipboard, stealing the clipboard content that meets the conditions every 0.5 seconds, so as to take a screenshot. The monitoring conditions for this function are as follows: When the clipboard content starts with T and is less than 45 characters in length, the DLL file saves the content to “C:\ProgramData\Microsoft Drive\stop.ini”. Then, the DLL file creates a folder named after the current date and time in the same folder, and captures 20 screenshots in a row and saves them to this folder. When the clipboard content meets one of the following conditions: (1) The string length is 64 characters; (2) The string length is greater than 65 characters and the 66th character is T; (3) The string starts with Key and is longer than 68 characters; (4) The string starts with 0x and is longer than 40 characters, the file saves the clipboard content to “C:\ProgramData\Microsoft Drive\Desktop.ini”, and captures 20 screenshots in a row and save them to a folder named after the current date and time. “1.dll” executes the Shellex function by first parsing the configuration information hardcoded in it, which is then used to select whether or not to execute the specified function. The current date and time are then obtained, and the date and time are written into the “C:\ProgramData\Microsoft Drive\Mark.sys” file, and also written into “MarkTime” in the registry “HKCU\TGByte\Setup”. Eventually, the malicious program traverses the window and checks for the presence of the specified string in the window caption bar, thus checking whether the relevant security product or tool is currently running on the system. When it is found that the aforementioned security product or tool is running on the current system, the malicious file shuts down the network socket and continuously monitors it every 1 second. When it is confirmed that there is no relevant security product or tool running on the system, the malicious file collects various system information that is used to build the online package to send to the C2 server. As a result, the attacker can use the malicious file to perform malicious behaviours such as remote control and keyboard monitoring.

Conclusion

In this incident, the “You She” group still uses phishing websites that contain counterfeit software, which warns users that they need to raise their security awareness, and download software from official websites. In addition, enterprises can provide employees with a unified download portal for some commonly used software. In this attack, the attacker also used a spoofed email login page, which is also common in many phishing attacks. Enterprises are also advised to raise awareness of network security among employees. In particular, when employees encounter a login page, they should confirm that the site is compliant and secure before logging in.

Reference: https://mp.weixin.qq.com/s/TCZVQEut9CvSiJ4VPwKJYg

Appendices

Emerging Ransomware Family NotLockBit Takes Inspiration from the Infamous LockBit

blog.qualys.com/vulnerabilities-threat-research/2024/12/18/notlockbit-a-deep-dive-into-the-new-ransomware-threat#conclusion

Evolving Threats: Lazarus Group's Latest Malware Campaign

securelist.com/lazarus-new-malware/115059/

The “You She” Group Distributes Malicious Installers Through Phishing Websites

mp.weixin.qq.com/s/TCZVQEut9CvSiJ4VPwKJYg

Indicators of Compromise: Emerging Ransomware Family NotLockBit Takes Inspiration from the Infamous LockBit (1 of 1)

Indicator	Type
14fe0071e76b23673569115042a961136ef057848ad44cf35d9f2ca86bd90d31	SHA-256
2e62c9850f331799f1e4893698295d0b069ab04529a6db1bfc4f193fe6aded2c	SHA-256
a28af0684456c26da769a2e0d29c5a726e86388901370ddf15bd3b355597d564	SHA-256
aca17ec46730f5677d0d0a995b65504e97dce65da699fac1765db1933c97c7ec	SHA-256
e02b3309c0b6a774a4d940369633e395b4c374dc3e6aaa64410cc33b0dcd67ac	SHA-256

Indicators of Compromise: Evolving Threats: Lazarus Group's Latest Malware Campaign (1 of 1)

Indicator	Type
c6323a40d1aa5b7fe95951609fb2b524	MD5
cf8c0999c148d764667b1a269c28bdcb	MD5
80ab98c10c23b7281a2bf1489fc98c0d	MD5
4c4abe85a1c68ba8385d2cb928ac5646	MD5
00a2952a279f9c84ae71367d5b8990c1	MD5
5eac943e23429a77d9766078e760fc0b	MD5

Indicators of Compromise: The “You She” Group Distributes Malicious Installers Through Phishing Websites (1 of 1)

Indicator	Type
6A6A3529EEBD138E16D6D146E231B0EC	MD5
F24B9A556E5387C7BA4C76ED1A93C289	MD5
hxxps[:]//fs-im-kefu.7moor-fs1[.]com/ly/4d2c3f00-7d4c-11e5-af15-41bf63ae4ea0/1732365864209/3.txt	URL
hxxps[:]//fs-im-kefu.7moor-fs1[.]com/ly/4d2c3f00-7d4c-11e5-af15-41bf63ae4ea0/1728896464326/4.txt	URL
hxxps[:]//fs-im-kefu.7moor-fs1[.]com/ly/4d2c3f00-7d4c-11e5-af15-41bf63ae4ea0/1730714903137/7.txt	URL

Weekly OSINT Snapshot

PwC intelligence analysts uncovered the following articles during routing open source intelligence (OSINT) collection. While the information included was deemed of potential interest, these threats have not directly affected geography or sectors relevant to clients.

Source Title	Source
Cloud Atlas seen using a new tool in its attacks	securelist.com/cloud-atlas-attacks-with-new-backdoor-vbcloud/115103
BellaCPP: Discovering a new BellaCiao variant written in C++	securelist.com/bellacpp-cpp-version-of-bellaciao/115087
“DeceptionAds” — Fake Captcha Driving Infostealer Infections and a Glimpse to the Dark Side of Internet Advertising	labs.guard.io/deceptionads-fake-captcha-driving-infostealer-infections-and-a-glimpse-to-the-dark-side-of-0c516f4dc0b6
Winos4.0 “Online Module” Staging Component Used in CleverSoar Campaign	esentire.com/blog/winos4-0-online-module-staging-component-used-in-cleversoar-campaign
Christmas "Gift" Delivered Through SSH	isc.sans.edu/diary/rss/31538
Now You See Me, Now You Don’t: Using LLMs to Obfuscate Malicious JavaScript	unit42.paloaltonetworks.com/using-llms-obfuscate-malicious-javascript

Critical Vulnerability Alert (CVA) Weekly Summary

Our Approach

PwC evaluates critical vulnerabilities against a set of criteria to develop a risk-based approach to prioritise vulnerability management and alerting.

Capability

- **Initial Access** – Can the vulnerability be exploited by unauthenticated attackers?
- **Impact of Exploitation** – What does successful exploitation enable the attacker to achieve?
- **Proof of Concept (PoC)** – Does a PoC/exploit exist which may be weaponised by attackers?
- **Attack Complexity** – How easy is it for attackers to exploit the vulnerability?
- **Privileges Required** – Does the attacker require any privileges to exploit the vulnerability?
- **User Interaction** – Does exploitation require user execution?
- **Attack Vector** – What level of access is required to exploit the vulnerability?

Intent

- **Exploitation in the Wild** – Is the vulnerability being actively exploited by attackers?
- **Discussion on the Dark Web** – Are attackers discussing the vulnerability on hacking forums?
- **Discussion on Social Media** – Is the vulnerability garnering attention via social media?
- **Open Source Intelligence** – Is the vulnerability being reported by security researchers?
- **EPSS Score** – What is the weighted score indicating likelihood of exploitation?

Opportunity

- **Age of Vulnerability** – How recently was the vulnerability released?
- **CvSS v3 Impact Score** – What is the weighted score indicating the severity of the vulnerability?
- **Patch or Mitigation Available** – Is a patch or workaround available to mitigate the vulnerability?
- **Exposed Assets** – Via passive scanning, do we observe any exposed instances?

CVE Summary

The following table summarises the details of the Common Vulnerabilities and Exposures (CVEs) evaluated within the last week.

Date of Evaluation	23/12/2024	23/12/2024	23/12/2024	24/12/2024	27/12/2024
Vulnerability CVE ID	CVE-2024-56145	CVE-2023-34990	CVE-2024-12727	CVE-2024-53961	CVE-2024-12356
Name of Vulnerability	PoC Released for PHP Configuration System Craft CMS Unauthenticated Remote Code Execution	Fortinet FortiWLM Remote Unauthenticated C2 Vulnerability	Sophos Firewall Pre-Auth SQL Injection Vulnerability Allows RCE	PoC Released for Adobe ColdFusion Critical Vulnerability Allows Arbitrary File System Read	Actively Exploited BeyondTrust Multiple Products Command Injection Vulnerability
Product	Craft CMS	FortiWLM	Sophos Firewall	Adobe ColdFusion	BeyondTrust Remote Support (RS) & Privileged Remote Access (PRA)
Impacted Versions	>= 5.0.0-RC1, < 5.5.2 >= 4.0.0-RC1, < 4.13.2 >= 3.0.0, < 3.9.14	FortiWLM 8.5.0 through 8.5.4	versions older than 21.0 MR1 (21.0.1)	ColdFusion 2023: Update 11 and earlier versions ColdFusion 2021: Update 17 and earlier versions	Privileged Remote Access (PRA) 24.3.1 and earlier Remote Support (RS) 24.3.1 and earlier
Vendor Advisory	github.com	https://fortiguard.fortinet.com/psirt/FG-IR-23-144	sophos.com	helpx.adobe.com	beyondtrust.com
Third Party Advisory	assetnote.io	socradar.io	securityonline.info	securityonline.info	arcticwolf.com

*Note: This table summarises CVEs evaluated within the period of Friday 20 December and Thursday 26 December 2024.
Note: Please note this information is as of the date of evaluation (Row 1).

Criteria

The following table summarises the criteria used to evaluate the criticality of the CVE and their respective outcomes.

Date of Evaluation	23/12/2024	23/12/2024	23/12/2024	24/12/2024	27/12/2024
Vulnerability CVE ID	CVE-2024-56145	CVE-2023-34990	CVE-2024-12727	CVE-2024-53961	CVE-2024-12356
Age of Vulnerability	Last Week (7 Days)	Last Week (7 Days)	Last Week (7 Days)	Last 3 Days	Last Week (7 Days)
CvSS v3 Impact Score	Critical - 9.0 to 10.0	Critical - 9.0 to 10.0	Critical - 9.0 to 10.0	High - 7.0 to 8.9	Critical - 9.0 to 10.0
Initial Access	Yes - Unauthenticated	Yes - Unauthenticated	Yes - Unauthenticated	Yes - Unauthenticated	Yes - Unauthenticated
Impact of Exploitation	Remote Code Execution	Remote Code Execution	Command Injection	Information Disclosure	Command Injection
Attack Complexity	Low	Low	Low	High	Low
Privileges Required	None	None	None	None	None
User Interaction	No	No	No	No	No
Attack Vector	Network	Network	Network	Network	Network
Proof-of-Concept	Yes	No	No	Yes	Yes
Exploited in the Wild	No Exploitation in the Wild	No Exploitation in the Wild	No Exploitation in the Wild	No Exploitation in the Wild	Yes, Global/Opportunistic Targeting
Threat Discussion - Dark Web	No	No	No	No	No
Threat Discussion - Social Media	No	No	No	No	Yes
Threat Discussion - OSINT	No	No	No	No	No
Patch or Mitigation Available	Yes	Yes	Yes	Yes	Yes
Potentially Vulnerable Victims in Hong Kong, Macau, China, Malaysia?	No	No	No	No	No
EPSS Score at time of evaluation	0.04%	0.04%	0.04%	No	1.30%
Outcome	No further escalation required	No further escalation required	Email Communications	Draft Critical Vulnerability Alert	Draft Critical Vulnerability Alert
Manual Override?	No	No	No	No	No

*Note: This table summarises CVEs evaluated within the period of Friday 20 December and Thursday 26 December 2024.
Note: Please note this information is as of the date of evaluation (Row 1).

Further Information

This report has been prepared for PwC Dark Lab Cyber-as-a-Service clients. Please email *darklab.cti@hk.pwc.com* for more detailed analysis and information on the threats discussed in this report.

Traffic Light Protocol

This report is classified as TLP:AMBER. Recipients may only share TLP:AMBER information with members of their own organization who need to know the information to protect themselves or prevent further harm.