Suspected China-Based Espionage Operation Against Military Targets in Southeast Asia

By Lior Rochberger, Yoav Zemah

Published: 2026-03-12 · Archived: 2026-04-05 17:48:29 UTC

Executive Summary

We identified a cluster of malicious activity targeting Southeast Asian military organizations, suspected with moderate confidence to be operating out of China. We designate this cluster as CL-STA-1087, with STA representing our assessment that the activity is conducted by state-sponsored actors. We traced this activity back to at least 2020.

The activity demonstrated strategic operational patience and a focus on highly targeted intelligence collection, rather than bulk data theft. The attackers behind this cluster actively searched for and collected highly specific files concerning military capabilities, organizational structures and collaborative efforts with Western armed forces.

The objective-oriented tool set used in the malicious activity includes several newly discovered assets: the AppleChris and MemFun backdoors, and a custom Getpass credential harvester.

This persistent espionage campaign against regional military entities is characterized by the deployment of custom-developed tools and highly stable operational infrastructure. We share our analysis of the attackers' methods and tools to help defenders detect and protect against these advanced attacks.

Palo Alto Networks customers are better protected from the threats discussed above through the following products and services:

- Advanced URL Filtering and Advanced DNS Security
- Advanced WildFire
- Cortex XDR and XSIAM
- Cortex Cloud
- Cortex Cloud Identity Security

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Playing the Long Game

The investigation began after Cortex XDR agents, newly deployed across the environment, detected suspicious PowerShell activity indicating an existing compromise. The detection revealed an ongoing attack targeting

multiple endpoints within the network. Attackers established persistence on an unmanaged endpoint that they used to execute malicious PowerShell scripts remotely across selected systems. The script content is shown in Figure 1.

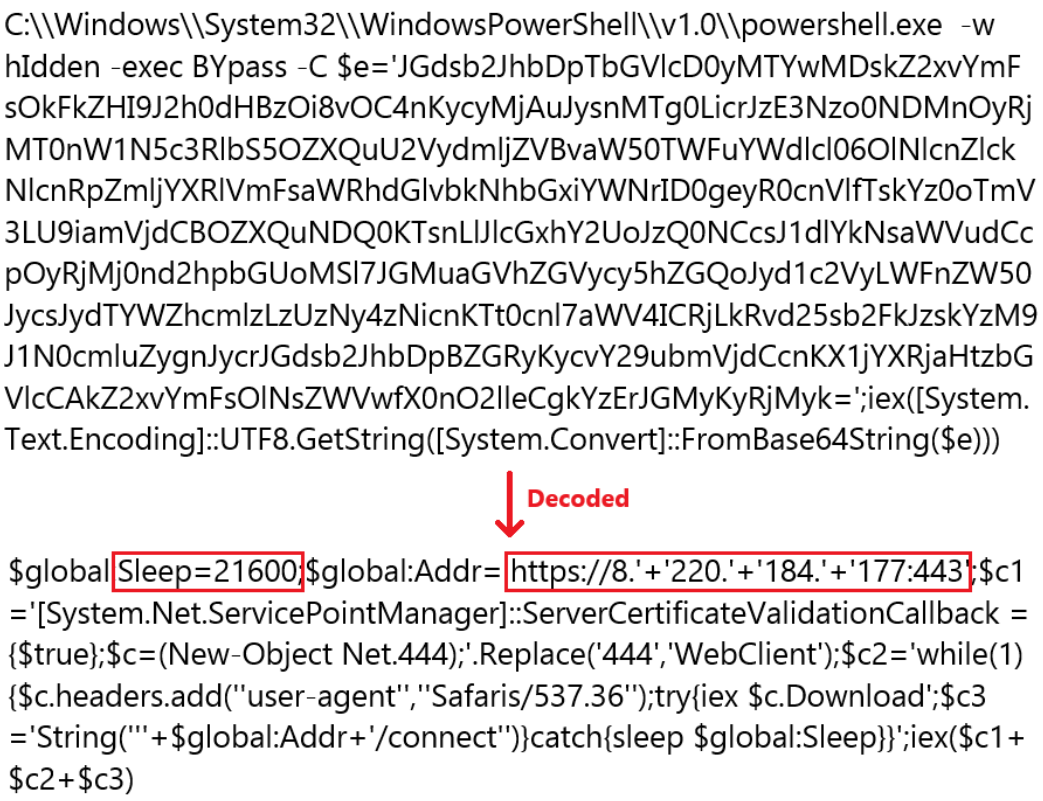

Figure 1. The decoded PowerShell script that was passed as a command-line argument.

The PowerShell scripts were designed to sleep for six hours (21,600 seconds) and then create reverse shells to one of four command and control (C2) servers:

- 154.39.142[.]177
- 154.39.137[.]203
- 8.212.169[.]27
- 109.248.24[.]177

Our analysis of the timeline and script deployment patterns indicated that this was part of an established intrusion already in progress. The initial infection vector remains undetermined. Following the identification of the persistence mechanism, the environment appeared to be dormant for several months, with no observable malicious activity. We assess that the attackers deliberately maintained their foothold in the environment, waiting for an opportune moment to resume their operations.

Returning to the Network

When the attackers renewed active operations from the unmanaged endpoint, multiple security alerts were triggered, as Figure 2 shows.

ALERT NAME	DESCRIPTION
Remote service start from an uncommon source	A remote host initiated the service update.exe. The command line used: c:\windows\update.exe. This host has initiated remote services on 0 dif
Uncommon remote service start via sc.exe	The 'service control' command was executed on to start a service on a remote host. sc \\ start swprv. 0 other such command inv
Uncommon remote service start via sc.exe	The 'service control' command was executed on to start a service on a remote host. sc \\ start winsv. 0 other such command inv
Uncommon remote service start via sc.exe	The 'service control' command was executed on to start a service on a remote host. sc \\ start winsv. 0 other such command inv
Remote service start from an uncommon source	A remote host initiated the service update.exe. The command line used: c:\windows\update.exe. This host has initiated remote services on 0 dif
SYNC - Remote Activity - 152206032	Suspicious service created from remote machine
SYNC - Remote Activity - 152206032	Suspicious service created from remote machine
Remote command execution via wmic.exe	cmd.exe executed remote commands via WMI. Command line: wmic /node: /user: /password: proces

Figure 2. Alerts triggered by CL-STA-1087 activity, as seen in Cortex XDR.

The alerts indicated the deployment of several malicious tools and suspicious activity across the compromised environment including outbound C2 communications, lateral movement and persistence.

Spreading Across the Network

The renewed campaign began with attackers delivering an initial backdoor payload from the unmanaged endpoint to a server in the environment. We named this backdoor AppleChris, after the 0XFEXYCDAPPLE05CHRIS mutex that forms part of the malware infection chain. From this initial foothold, the attackers orchestrated a systematic spread across the network. They used a combination of Windows Management Instrumentation (WMI) and native Windows .NET commands to deploy malware to additional endpoints, as Figure 3 shows.

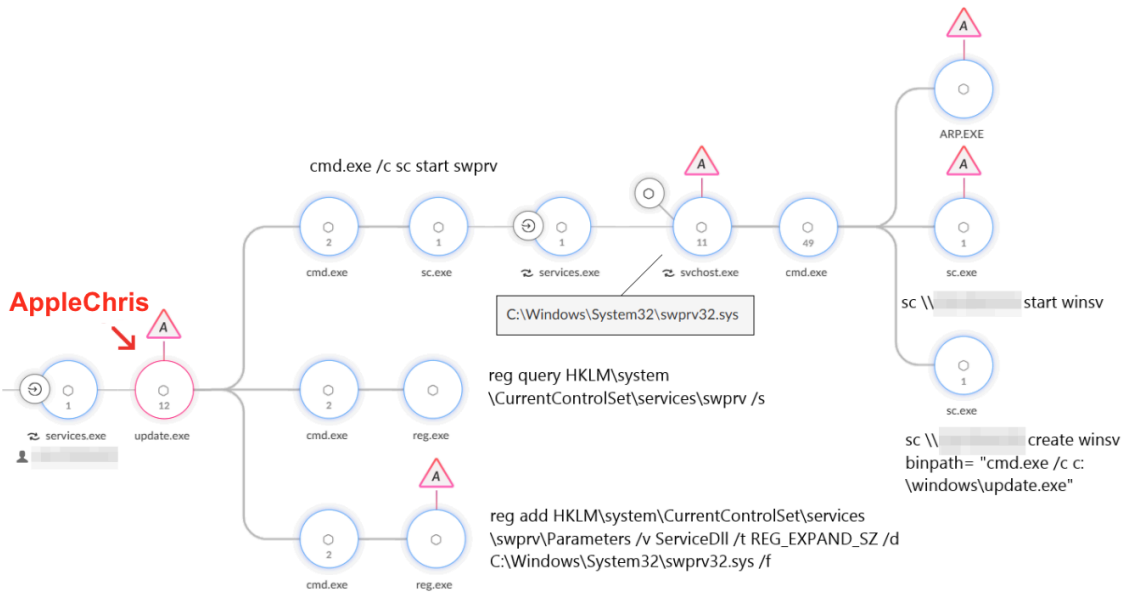

Figure 3. AppleChris causality chain.

The attackers targeted critical network infrastructure components:

- Domain controllers
- Web servers
- IT workstations
- Executive-level assets

To establish persistence, the attackers created a new service to facilitate payload execution. They also carried out DLL hijacking by storing a malicious DLL in the system32 folder and registering it to be loaded by an existing shadow copy service.

While the core of the AppleChris malware remained consistent throughout the campaign, the attackers deployed different variants across target endpoints. This approach was likely taken to maintain persistence across diverse system configurations and to evade detection by varying their operational signatures. The list of variants observed and analyzed is available in the New and Undocumented Tools section.

Strategic Intelligence Collection

After moving laterally through the network and establishing persistence, the attackers began to collect data. We observed highly selective searches for sensitive files related to:

- Official meeting records
- Joint military activities
- Detailed assessments of operational capabilities

The attackers showed particular interest in files related to military organizational structures and strategy, including command, control, communications, computers and intelligence (C4I) systems.

New and Undocumented Tools

During our investigation, we identified two different backdoors deployed by the attackers: AppleChris and MemFun. The backdoors differ in functionality and capabilities but share a common pattern: Both use custom HTTP verbs and the dead drop resolver (DDR) technique to access a shared Pastebin account. Figure 4 shows that both backdoors use the same Pastebin repository to resolve their respective C2 addresses.

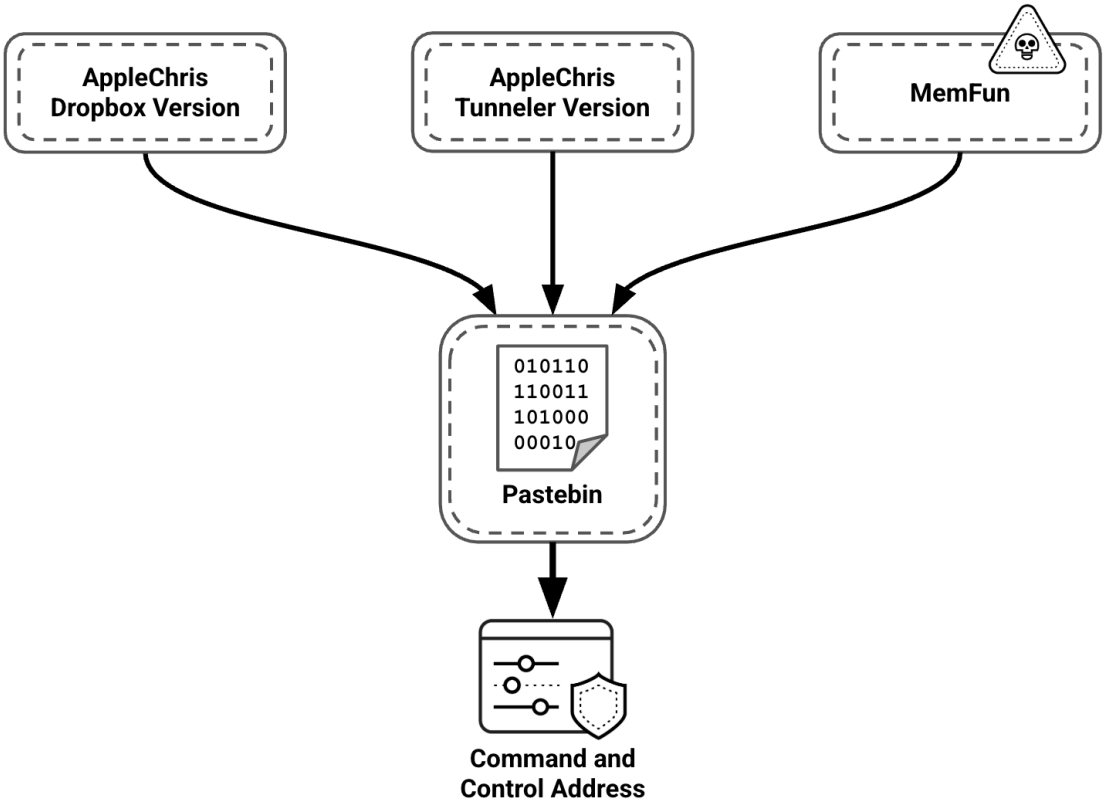

Figure 4. The different types of malware that use the same DDR technique.

AppleChris Backdoor

Our analysis revealed multiple variants of the AppleChris backdoor. We recovered different types of Portable Executable (PE) files and categorized them into two primary variants, based on their functionality and compilation timestamp. The variants share similar core backdoor functionality but differ in their DDR implementation strategies:

- **Dropbox variant**
  - The initial iteration represents the earlier development phase, with the filename swrpv.sys
  - The Dropbox variant implements a dual DDR approach:
    - Using an attacker-controlled Dropbox account as the primary DDR source
    - Falling back to a Pastebin-based DDR as a secondary option
- **Tunneler variant**
  - The more recent variant with expanded capabilities, using the following names:
    - swrpv.sys
    - update.exe
    - Googleupdate.exe
  - The Tunneler variant represents a streamlined evolution that consolidates to a single Pastebin-based DDR, while introducing advanced network proxy capabilities

At the time of our investigation, both variants were still in use. A detailed comparison table of notable features of both variants is available in Appendix A.

The following analysis focuses on the more recent Tunneler variant and demonstrates the full spectrum of AppleChris capabilities.

Initial Execution and Evasion

AppleChris enables flexible deployment through multiple PE variants. While some variants operate as standalone executables, others are deployed as DLLs, using various persistence techniques.

In several observed instances, the attackers performed DLL hijacking by placing the malicious swprv32.sys AppleChris DLL in the system32 directory. Subsequently, they established persistence by registering the malicious DLL as a component of the Volume Shadow Copy Service. This allowed the malware to leverage elevated privileges while masquerading as a legitimate Windows process to evade detection.

To bypass automated security systems, some of the malware variants employ sandbox evasion tactics at runtime. These variants trigger delayed execution through sleep timers of 30 seconds (EXE) and 120 seconds (DLL), effectively outlasting the typical monitoring windows of automated sandboxes. Single-instance execution is enforced via the 0XFEXYCDAPPLE05CHRIS mutex, which causes the process to terminate if another instance is detected.

C2 Resolution Using DDR

AppleChris employs a DDR technique to dynamically resolve its C2 server IP address. This approach effectively evades static block lists and hard-coded indicators-of-compromise (IoC) detection. It also provides operational flexibility, allowing threat actors to modify C2 infrastructure without redeploying malware.

The backdoor accesses a specific Pastebin URL to retrieve the encrypted C2 IP address. The retrieved content undergoes a two-stage decryption process:

- The raw text is Base64-decoded
- The decoded text is decrypted using an embedded RSA-1024 private key

This cryptographic approach ensures that even if the Pastebin account is discovered, the actual C2 server information remains protected, as the corresponding private key is embedded within the malware. The alert for Pastebin access is shown in Figure 5.

ALERT SOURCE	ACTION	ALERT NAME	DESCRIPTION
XDR Analytics BIOC	Detected	Non-browser access to a pastebin-like site	*The non-browser process svchost.exe accessed pastebin.com. This domain can be used as a command and control or to exfiltrate data*

Figure 5. Alert triggered by suspicious Pastebin access, as seen in Cortex XDR.

AppleChris Main Functionality

Following successful C2 resolution, AppleChris enters its primary beaconing loop. To facilitate session management and command execution, the malware generates a 10-byte random sequence as a unique session identifier, which is concatenated with the computer name and hex-encoded MAC address. This registration data is

RSA-encrypted and transmitted to the C2 server within the payload of an HTTP GET request, demonstrating a dual-key architecture that securely shares the session key for subsequent communication.

The server's response contains the command payload, which is then decrypted using AES. The 10-byte session ID, padded with 14 zeros, serves as the key. A hard-coded initialization vector embedded in the binary is also used:

- [SessionID (10 bytes)] + [0xFF (14 bytes)]

The malware implements a comprehensive command dispatcher that interprets single-byte command identifiers to execute a wide range of backdoor functionality, including:

- Drive enumeration
- Directory listing
- File upload, download and deletion
- Process enumeration
- Remote shell execution
- Silent process creation

In addition, the Tunneler variant supports a command to activate the proxy tunneling module.

Each command response utilizes custom HTTP requests as communication parameters (PUT, POT, DPF, UPF, CPF, LPF) to facilitate command tracking and response handling. An example is shown in Figure 6 below. The full list is provided in Appendix B.

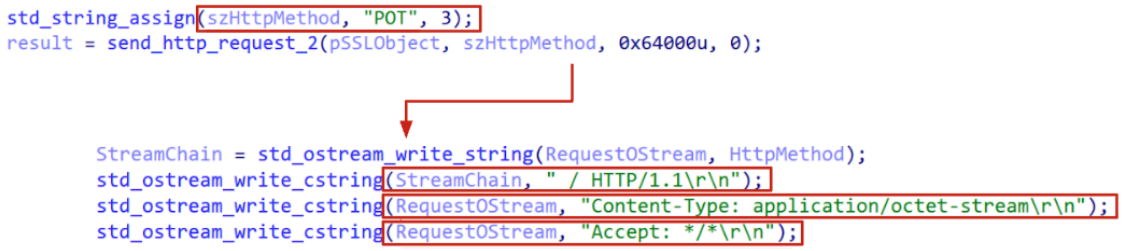

Figure 6. An example of the custom HTTP verb used by the malware, as seen in IDA Pro decompiler.

MemFun Backdoor

MemFun is multi-stage malware that consists of three components:

- Initial loader named GoogleUpdate.exe
- In-memory downloader
- Final payload – a DLL retrieved from the C2 server containing the MemFun export

After the initial dropper execution, the entire attack chain operates in memory, employing evasion techniques and reflective loading. The loader's primary purpose is to establish communication with the C2 server and download an additional DLL that contains an exported MemFun function. This function is then executed to initiate the main backdoor. Since the final payload is retrieved from the C2 server, attackers can deploy different modules based on their objectives, making MemFun a modular malware platform rather than a static backdoor.

The MemFun execution chain is illustrated in Figure 7.

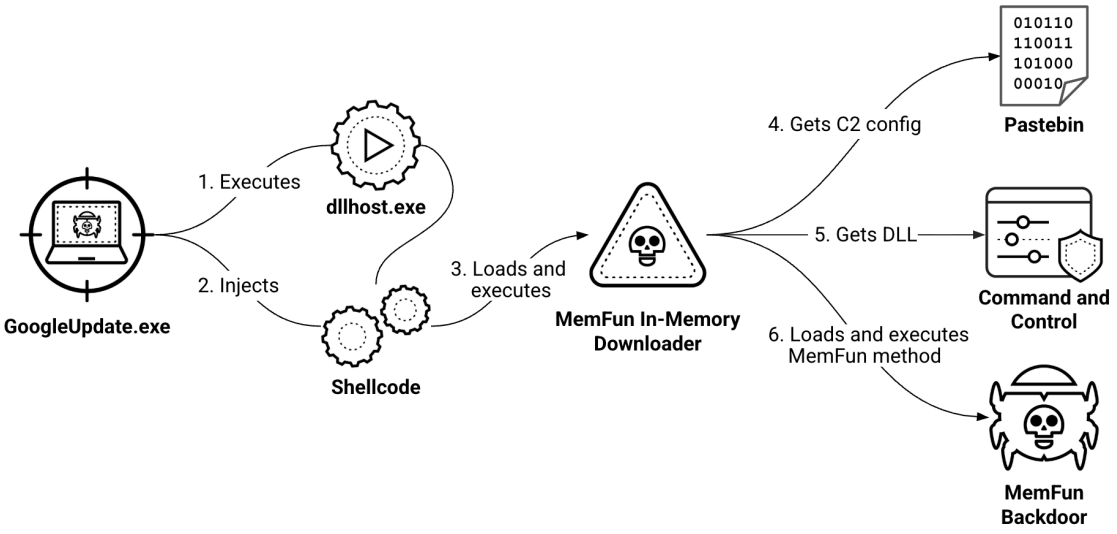

Figure 7. MemFun execution chain.

Initial Execution and Anti-Forensic Evasion

The execution chain begins with the MemFun dropper, which immediately runs anti-forensic checks to avoid detection. Upon execution, the dropper performs timestomping. It retrieves the creation timestamp of the Windows System directory and sets its own file creation timestamp to match it, making the malware appear to be the same age as legitimate system files.

Rather than writing additional files to disk, the dropper employs process hollowing to inject its payload into memory. It launches dllhost.exe in a suspended state and decrypts an embedded shellcode payload using the XOR key 0x25. The decrypted shellcode is then injected into the suspended process, which is resumed to execute the malicious code. This technique ensures that the malicious code runs under the guise of a legitimate Windows process, while leaving no additional artifacts on disk.

Shellcode Bootstrap and Reflective Loading

The injected shellcode functions as a loader that locates itself in memory and scans to find the embedded MemFun Loader DLL.

The shellcode performs reflective DLL loading. Before transferring execution to the MemFun Loader, the shellcode implements another anti-forensics measure: zeroing the first 4 KB of allocated memory, to erase DOS and PE headers. This makes the loaded module invisible to memory analysis tools that rely on header signatures.

C2 Discovery and Final Payload Retrieval

The MemFun in-memory downloader initializes with multiple evasion techniques, including the creation of a mutex named GOOGLE and anti-debug measures to evade analysis. The downloader performs token impersonation to steal and impersonate logged-on user credentials, allowing it to inherit user proxy settings and bypass network restrictions that might block system-level processes.

Communication with the C2 server uses HTTP requests with a custom pattern Q instead of the standard GET/POST commands, targeting the /DL1 resource to download the final payload. The requests also include distinctive headers such as Get: 0 and User-Agent: MyIE.

The downloader implements session-specific encryption by generating a unique 24-byte Blowfish key for each execution. This dynamically generated key is sent to the C2 server via the HTTP Cookie header, allowing the server to encrypt the backdoor payload specifically for that execution session. Upon receiving the encrypted MemFun backdoor from the /DL1 resource, the loader decrypts the payload using its unique session key. It then performs reflective loading to execute the backdoor in memory by calling the exported MemFun function.

Getpass, a Custom Modified Mimikatz Variant

In addition to the two backdoors, our analysis revealed a custom credential-harvesting tool. We have designated this tool Getpass, reflecting the internal getpass name utilized by the attackers. Getpass is a custom version of Mimikatz, packaged as a standalone DLL that attempts to masquerade as a legitimate Palo Alto Networks tool under the Cyvera directory, as Figure 8 shows.

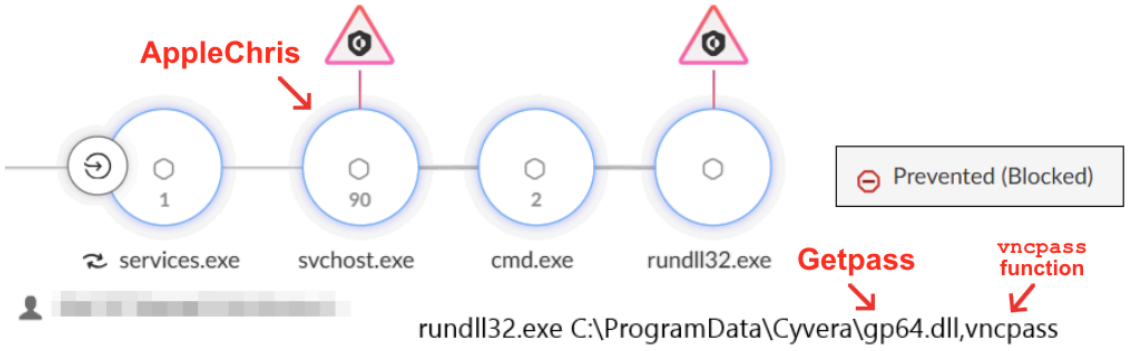

Figure 8. Getpass execution through AppleChris.

Upon execution, the malware's vncpass function escalates privileges by acquiring SeDebugPrivilege. It then systematically targets 10 specific Windows authentication packages, including MSV, WDigest, Kerberos and CloudAP. The malware attempts to extract plaintext passwords, NTLM hashes and authentication data directly from the lsass.exe process memory. Unlike standard Mimikatz, which provides an interactive console, this variant automatically runs its credential-harvesting routine and logs the stolen data to a file named WinSAT.db, which masquerades as a legitimate Windows system database.

The Attackers' Infrastructure: Persistent, Segmented and Scalable

The infrastructure behind CL-STA-1087 reveals insights into the entire operation's scope and longevity. File timestamps, Pastebin creation dates and malware compilation times all trace back to 2020, indicating a long-running campaign. The timestamps for the Pastebin account creation and the pastes are shown in Figure 9.

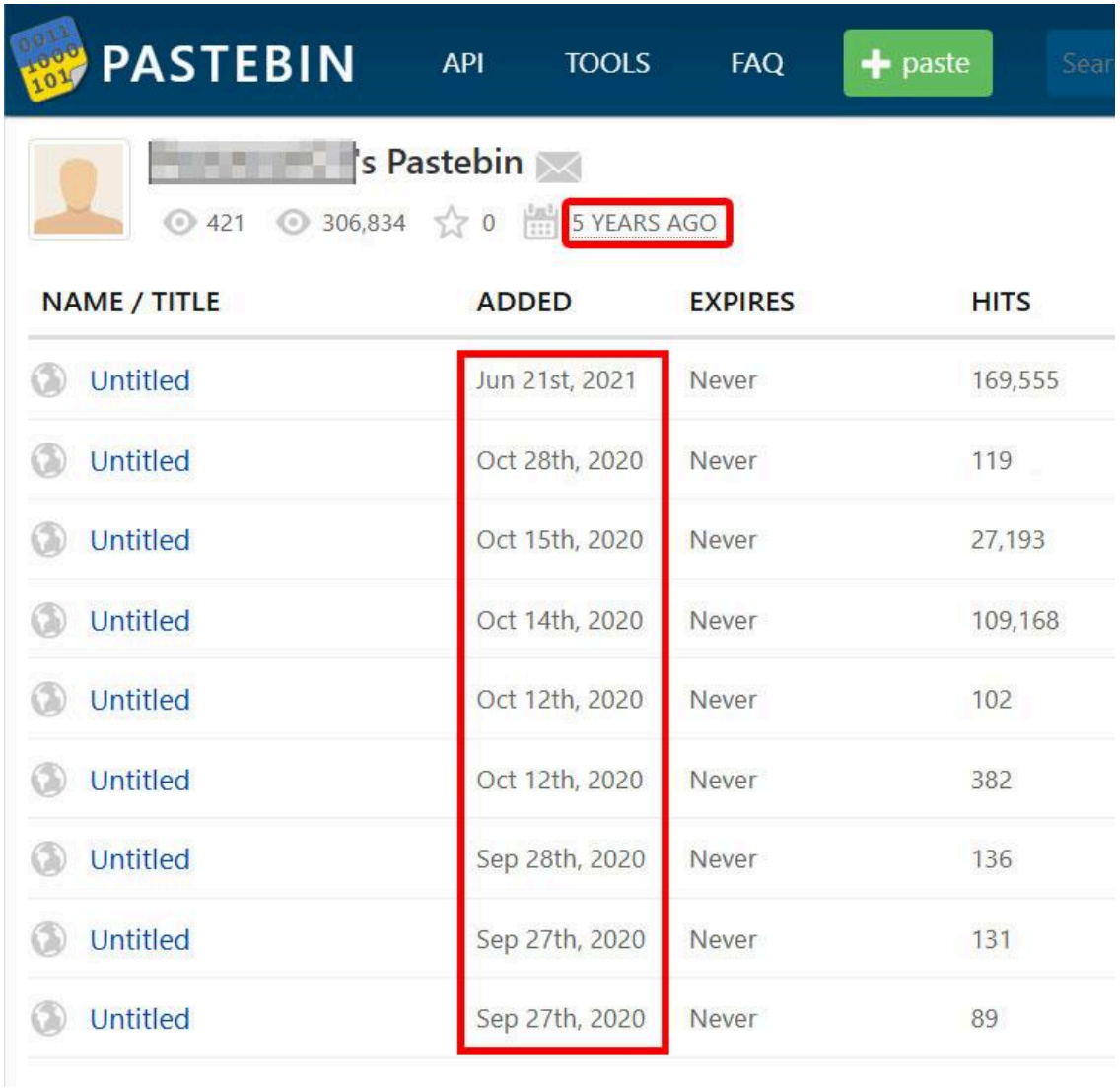

Figure 9. The Pastebin account pastes.

The presence of multiple C2 IP addresses in the Pastebin pages indicates operational compartmentalization, allowing the actor to rotate infrastructure based on the target's profile.

Our analysis suggests that the attackers maintained communication with multiple compromised networks over an extended period, leveraging Pastebin and Dropbox for C2 distribution. Notably, while the AppleChris Dropbox samples we encountered appeared to be older than the Tunneler samples, they were still functional and in active use at the time of our investigation. Evidence suggests the threat actor behind the activity cluster continues to update their Dropbox account with updated infrastructure files.

Connection to the Chinese Nexus

We identified multiple indications that this activity was conducted by a threat actor affiliated with the Chinese nexus.

Activity Time Frame

Our analysis of command execution timestamps and interactive session logs revealed the attackers' operational schedule. By examining hands-on-keyboard activity originating from both backdoors and the unmanaged endpoint over multiple weeks, we identified distinct temporal patterns in their operations.

The data revealed that malicious activities consistently occurred during business hours, specifically aligning with a UTC+8 time zone schedule. As Figure 10 illustrates, the periods of activity align with typical office hours across several Asian regions, including China.

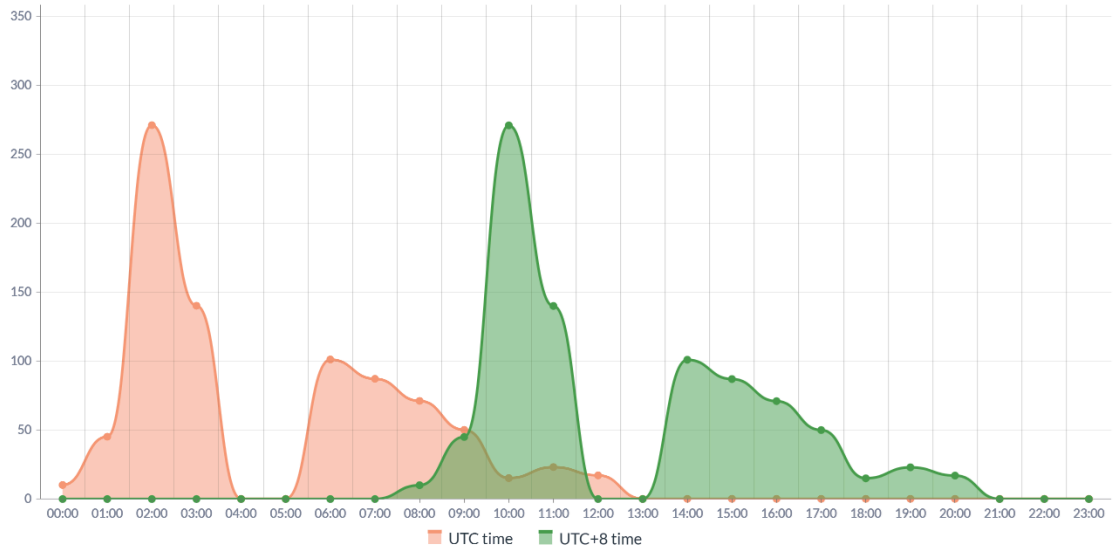

Figure 10. Activity time chart in UTC and UTC+8 times.

Victimology and Motivation

The threat actor targets military organizations in Southeast Asia. We observed specific searches for military-related information.

Infrastructure and Linguistics

The attackers used China-based cloud network infrastructure for their C2 servers. We also observed that the login page of one of the C2 servers was written in Simplified Chinese.

Conclusion

The activity cluster CL-STA-1087 is a suspected espionage campaign operating out of China and targeting military organizations across Southeast Asia. The threat actor behind the cluster demonstrated operational patience and security awareness. They maintained dormant access for months while focusing on precision intelligence collection and implementing robust operational security measures to ensure campaign longevity.

The backdoors used in this campaign operate on shared infrastructure and employ evasion methods such as Dead Drop Resolver. These techniques demonstrate the attackers' long-term commitment to their objectives and meticulous attention to operational security practices that are designed to maintain persistent access.

We encourage security practitioners to leverage the indicators and analysis provided in this article to enhance detection capabilities, and to strengthen defensive postures against advanced persistent threats targeting critical military infrastructure and strategic assets.

Palo Alto Networks Protection and Mitigation

For Palo Alto Networks customers, our products and services provide the following coverage associated with this activity cluster:

- Advanced WildFire cloud-delivered malware analysis service accurately identifies the AppleChris and MemFun samples mentioned in this article as malicious.
- Advanced URL Filtering and Advanced DNS Security identify known network IoCs associated with this activity as malicious.
- Cortex XDR and XSIAM help to prevent the threats described above, by employing the Malware Prevention Engine. This approach combines several layers of protection, including Advanced WildFire, Behavioral Threat Protection and the Local Analysis module, designed to prevent both known and unknown malware from causing harm to endpoints.
- The use of a legitimate cloud service to host C2 infrastructure indicates the potential for the actor behind CL-STA-1087 to use cloud-native operations. Cortex Cloud customers are better protected through the proper placement of Cortex Cloud XDR endpoint agent and serverless agents within a cloud environment. Designed to protect a cloud's posture and runtime operations against these threats, Cortex Cloud helps detect and prevent the malicious operations or configuration alterations or exploitations discussed within this article.
- Cortex Cloud Identity Security encompasses Cloud Infrastructure Entitlement Management (CIEM), Identity Security Posture Management (ISPM), Data Access Governance (DAG) as well as Identity Threat Detection and Response (ITDR) and provides clients with the necessary capabilities to improve their identity-related security requirements. Should the operations move into cloud environments, Cortex Cloud can help detect misconfigurations and unwanted access to sensitive data. It also conducts real-time analysis of usage and access patterns. This provides visibility into cloud identities and their permissions.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America: Toll Free: +1 (866) 486-4842 (866.4.UNIT42)
- UK: +44.20.3743.3660
- Europe and Middle East: +31.20.299.3130
- Asia: +65.6983.8730
- Japan: +81.50.1790.0200
- Australia: +61.2.4062.7950
- India: 000 800 050 45107
- South Korea: +82.080.467.8774

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to

their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

SHA256 hashes of the AppleChris tunnel variant:

- 9e44a460196cc92fa6c6c8a12d74fb73a55955045733719e3966a7b8ced6c500
- 5a6ba08efcef32f5f38df544c319d1983adc35f3db64f77fa5b51b44d0e5052c
- 0e255b4b04f5064ff97da214050da81a823b3d99bce60cdd9ee90d913cc4a952

SHA256 hashes of the AppleChris Dropbox variant:

- 413daa580db74a38397d09979090b291f916f0bb26a68e7e0b03b4390c1b472f
- 2ee667c0ddd4aa341adf8d85b54fbb2fce8cc14aa88967a5cb99babb08a10fae

SHA256 hash of MemFun:

- ad25b40315dad0bda5916854e1925c1514f8f8b94e4ee09a43375cc1e77422ad

SHA256 hash of Getpass:

- ee4d4b7340b3fa70387050cd139b43ecc65d0cfd9e3c7dcb94562f5c9c91f58f

IPv4 addresses of the C2 servers:

- 8.212.169[.]27
- 8.220.135[.]151
- 8.220.177[.]252
- 8.220.184[.]177
- 116.63.177[.]49
- 118.194.238[.]51
- 154.39.142[.]177
- 154.39.137[.]203

Additional Resources

- Hijack Execution Flow: DLL – MITRE ATT&CK
- Indicator Removal: Timestomp – MITRE ATT&CK
- Mimikatz – MITRE ATT&CK
- Process Injection: Process Hollowing – MITRE ATT&CK
- Reflective Code Loading – MITRE ATT&CK
- Web Service: Dead Drop Resolver – MITRE ATT&CK
- It's All in the Name: How Unit 42 Defines and Tracks Threat Adversaries – Unit 42, Palo Alto Networks
- Blowfish Cipher – Wikipedia

Appendix A: Comparison of AppleChris Backdoor Variants

Table 1 shows the differences between the two AppleChris variants: Dropbox and Tunnel.

Feature	Dropbox Variant	Tunnel Variant
Unique Commands	Three unique commands: # – **Sleep Control**: Updates the beacon sleep interval dynamically. (– **Kill Process**: Terminates processes. + – **Recent Files Exfil**: Steals files from the Recent Files folder.	One unique command: ? – **Proxy Tunnel**: Creates a reverse TCP tunnel for network pivoting.
Dead Drop Resolver (DDR)	Uses Dropbox as the primary DDR, with Pastebin as a fallback and an additional Dropbox access token as a final fallback.	Relies solely on Pastebin.
Anti-Debugging	Contains an anti-debugging mechanism.	Relies on a long sleep (30-120s).
Network Spam (Decoy)	Spawns a background thread to generate fake traffic to support.microsoft[.]com every 30 seconds.	Does not generate decoy traffic.
Privilege and Proxy Handling	Steals the active user's access token to impersonate the user. Captures the user's specific proxy configuration.	Runs in the existing context without active token or proxy manipulation.
Mutex	Does not create a mutex.	Creates the hard-coded 0XFEXYCDAPPLE05CHRIS mutex.

Table 1. Comparison table between AppleChris variants.

Appendix B: AppleChris Commands

Table 2 lists the AppleChris commands shared by the Dropbox and Tunnel variants.

Symbol	Name	Description	Custom HTTP Verb
[	**Get Drive Info**	Surveys the target's storage environment to identify all connected drives (local, removable or optical) and calculates their available	PUT

		disk space.	
$	**List Directory**	Enumerates the contents of a specified directory, providing the attacker with a full list of files and subfolders, along with their last-modified timestamps.	POT
%	**Download File**	Retrieves a payload or file from the C2 server and writes it directly to the target's disk.	DPF
^	**Upload File**	Exfiltrates a specific file from the target's machine to the attacker. Includes logic to resume interrupted transfers if the connection is lost.	UPF
@	**Execute Shell**	Executes arbitrary shell commands via cmd.exe and actively streams the console output (stdout/stderr) back to the C2 server.	CPF
!	**List Processes**	Provides a simple list of process names and PIDs for all currently running processes.	LPF
*****	**Create Process**	Silently launches an executable or command-line instruction in a hidden window, preventing the user from seeing any visual interface. This command executes blindly without confirming success to the attacker.	None
-	**Delete File**	Permanently removes a targeted file from the file system. This command executes blindly without confirming success to the attacker.	None

Table 2. AppleChris supported commands.
