# Multi-year Chinese APT Campaign Targets South Korean Academic, Government, and Political Entities

https://go.recordedfuture.com/hubfs/reports/cta-2023-0919.pdf

## Initial Access:

**T1566.001 - Spearphishing Attachment**

TAG74, a Chinese state-sponsored threat activity group, used spearphishing attachments as a method to gain access to victim systems. The group employed a specific technique known as "Spearphishing Attachment" (ATT&CK code T1566.001) to execute their attacks. They distributed Compiled HTML (.chm) files via spearphishing emails, which contained three primary components. First, an embedded legitimate executable vulnerable to DLL search order hijacking, such as vias.exe or LBTWiz32.exe. Second, a malicious DLL loaded via the vulnerable executable using DLL search order hijacking. And third, an HTML file that displayed a decoy document to the user and executed a script to decompile the contents of the .chm file. This script also executed the vulnerable executable, either directly or via the RUN registry key, initiating the DLL search order hijacking chain. This technique allowed TAG74 to establish initial access to victim systems and execute their customized version of the open-source VBScript backdoor ReVBShell.

## Execution

**T1059.005 - Command and Scripting Interpreter: VisualBasic**

TAG74, in their multi-year campaign targeting South Korean organizations, utilized Visual Basic as a command and scripting interpreter to execute malicious commands and automate behaviors. They employed a customized version of the open-source VBScript backdoor called ReVBShell, which was loaded through a DLL search order hijacking execution chain triggered by .chm files. The modified ReVBShell variant included additional functions for base64-encoding C2 traffic, execution guardrails to exit the malware if ESET antivirus was detected, and various commands for code execution, changing sleep intervals, self-deletion, and enumeration via WMI command-line. The VBScript backdoor was configured to sleep for a specified interval and communicated with the threat actor's command-and-control infrastructure using encoded data. The payload loaded by the backdoor included commands for sending process information, drive lists, file information, process termination, executing commands, file download and upload, file deletion, recreating sockets, and sending socket objects. These commands and behaviors were specific to the use of Visual Basic as the scripting language for the malware.

**T1204.002 - User Execution: Malicious File**

TAG74, a Chinese state-sponsored threat activity group, used a malicious file to gain execution in their cyber-espionage campaign. They employed a specific technique known as DLL search order hijacking, which involves hijacking the execution flow of a legitimate executable by loading a malicious DLL. In this case, TAG74 used Compiled HTML (.chm) files as malicious files, which were likely distributed via spearphishing. These .chm files contained three primary components: an embedded legitimate executable vulnerable to DLL search order hijacking, a malicious DLL loaded via the legitimate

executable, and an HTML file that displayed a decoy document to the user and executed a script to decompile the contents of the .chm file. This script triggered the DLL search order hijacking chain, allowing the malicious DLL to be loaded and executed. The specific technical indicators related to this technique include the use of .chm files, the presence of embedded legitimate executables vulnerable to DLL search order hijacking, and the execution of scripts to trigger the hijacking chain.

## Persistence

**T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder**

The threat actor group TAG74 used the Registry Run Keys / Startup Folder attack technique to establish persistence on the compromised system. They achieved this by adding malicious entries to the Windows Registry or placing malicious files in the Startup Folder. These entries or files are executed automatically when the system starts up or when a user logs in, ensuring that the malware is launched every time the system is rebooted or the user logs in. The specific technical indicators related to this technique include the following:

- The threat actor group TAG74 used the Registry Run Keys to add malicious entries. These entries are typically located in the "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" or "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" keys.
- They may have used commands such as "reg add" or "regedit" to add the malicious entries to the Registry.
- The malware or malicious file that was placed in the Startup Folder may have had a specific filename or location, such as "C:\Users\Username\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\malware.exe".

By leveraging the Registry Run Keys / Startup Folder attack technique, the threat actor group TAG74 ensured that their malware would be executed every time the system started up or a user logged in, allowing them to maintain persistence and continue their malicious activities on the compromised system.

## Defense Evasion

**T1574.001 - Hijack Execution Flow: DLL Search Order Hijacking**

The threat actor group known as TAG74 used DLL Search Order Hijacking as a technique to execute their own malicious payloads. They exploited the vulnerability by using .chm files, which are Compiled HTML files, likely distributed through spearphishing. These .chm files contained three primary components: an embedded legitimate executable vulnerable to DLL search order hijacking, a malicious DLL loaded via the legitimate executable, and an HTML file that displayed a decoy document to the user. The HTML file also executed a script to decompile the contents of the .chm file and execute the vulnerable executable. This execution chain triggered the DLL search order hijacking, allowing the threat actors to load their customized version of the open-source VBScript backdoor called ReVBShell. This backdoor provided them with initial access to the compromised system. The use of DLL search order hijacking allowed the threat actors to bypass security measures and execute their malicious payloads.

**T1218.001 - System Binary Proxy Execution: Compiled HTML File**
The threat actor group TAG74 used Compiled HTML (.chm) files as a method to conceal malicious code and deliver their malware. They distributed these .chm files through spearphishing emails. The .chm files contained three primary components: an embedded legitimate executable vulnerable to DLL search order hijacking, a malicious DLL loaded via the legitimate executable, and an HTML file.

The HTML file was responsible for displaying a decoy document to the user and executing a script to decompile the contents of the .chm file. It used the native Windows HTML Help executable program (hh.exe) to decompile the .chm file and execute the legitimate executable vulnerable to DLL search order hijacking. The script simulated a mouse-click on the objects within the HTML file, triggering the DLL search order hijacking chain.

The malicious DLL, once loaded, created and executed a customized version of the open-source VBScript backdoor called ReVBShell. This backdoor had additional functions for base64-encoding C2 traffic, execution guardrails to exit the malware if ESET antivirus was detected, and various commands for code execution, changing sleep intervals, self-deletion, and enumeration via WMI command-line.

The use of .chm files allowed the threat actors to hide their malicious code within seemingly legitimate documents, making it more difficult for detection by security systems.

## Discovery

**T1518.001 - Software Discovery: Security Software Discovery**
TAG74, a Chinese state-sponsored threat activity group, used various commands and techniques to obtain information about security software on targeted systems. They leveraged commands such as netsh, reg query, dir, and Tasklist to conduct Security Software Discovery. These commands allowed the threat actors to gather information about the security tools and software installed on the compromised systems. By using netsh, they could query network configurations and interfaces, potentially identifying security-related settings. The reg query command enabled them to access the Windows Registry and retrieve information about installed security software and their configurations. The dir command allowed them to list the contents of directories, potentially revealing the presence of security-related files or directories. Finally, the Tasklist command provided information about running processes, including security software processes, which could help the threat actors identify and potentially evade detection by security tools. These commands were likely used by TAG74 to assess the security posture of the compromised systems and plan their subsequent actions accordingly.

## Command and Control

**T1132.001 - Data Encoding: Standard Encoding**
The threat actor group TAG74, in their multi-year Chinese state-sponsored cyber-espionage campaign, utilized Standard Encoding to encode command and control (C2) information. This encoding technique was employed to obfuscate the communication between the malware and the C2 infrastructure, making it more difficult for security tools to detect and analyze the malicious traffic. The specific technical indicators related to the use of Standard Encoding include:

The presence of Base64-encoding and decoding functions within the customized ReVBShell backdoor variant used by TAG74.

- The use of a string decryption algorithm that is consistent with the encoding and decoding process of Standard Encoding.
- The encoding and decoding of data using the Base64 algorithm, as evidenced by the additional functions present in the customized ReVBShell variant responsible for Base64-encoding and decoding data.
- The use of the magic bytes "0A 1B 2C 3D" in the C2 communications, which is a characteristic marker associated with the encoding and decoding process of Standard Encoding.

By employing Standard Encoding, the threat actor group TAG74 aimed to conceal the true nature of their C2 communications, making it more challenging for defenders to identify and block their malicious activities.

**T1071.001 - Application Layer Protocol: Web Protocols**
The threat actor, known as TAG74, used web protocols to communicate and blend in with existing traffic. They employed the following specific technical commands, codes, and indicators related to web protocols:

- They utilized Virtual Private Server (VPS) infrastructure geolocated within South Korea and spread across multiple hosting providers.
- TAG74 heavily relied on dynamic DNS (DDNS) domains for their malware command-and-control (C2) infrastructure.
- The threat actor spoofed specific South Korean organizations by using DDNS domains that mimicked the names of these organizations.
- They used IP addresses associated with hosting providers such as AS�CHOOPA, G�Core Labs, EstNOC OY, and Korea Telecom.
- TAG74 communicated with their C2 infrastructure using web protocols, such as HTTP, to establish a connection and exchange data.
- The C2 communications included basic victim information, such as computer name, username, operating system, IP address, and campaign/target codes.
- The threat actor used standard encoding techniques to obfuscate the data being transmitted over the web protocols.

By leveraging web protocols and blending in with legitimate web traffic, TAG74 aimed to evade detection and maintain a covert presence within the targeted networks.

**T1573.001 - Encrypted Channel:Symmetric Cryptography**
The threat actor group TAG74 used Symmetric Cryptography to conceal their command and control (C2) traffic. This technique involves encrypting the communication between the malware and the C2 server using a shared secret key. The encrypted traffic appears as random data, making it difficult for network defenders to detect and analyze. The specific technical indicators related to the use of Symmetric Cryptography by TAG74 include the presence of encryption algorithms and functions within the malware code, such as AES or DES, which are commonly used for symmetric encryption. Additionally, the use of

encryption libraries or APIs, such as OpenSSL or Crypto++, may be observed in the malware's code. These indicators suggest that the threat actor group employed Symmetric Cryptography to protect the confidentiality and integrity of their C2 communications.

## Exfiltration

**T1041 - Exfiltration Over C2 Channel:**

TAG74, a Chinese state-sponsored threat activity group, utilized exfiltration over a command and control (C2) channel to steal data. The specific technical indicators related to this exfiltration method include the use of data encoding techniques, such as standard encoding, to obfuscate the stolen information. The threat actors established an encrypted channel using symmetric cryptography to ensure secure communication between the compromised systems and the C2 infrastructure. They exploited application layer protocols, specifically web protocols, to transmit the exfiltrated data. By leveraging these techniques, TAG74 successfully exfiltrated sensitive information from the targeted organizations, allowing them to gather intelligence and potentially use it for malicious purposes.