SECURITY ADVISORY

CYBER STASH

February, 2025

# FatalRAT: Targeting Chinese-Speaking Regions

## Context

FatalRAT is a sophisticated Remote Access Trojan (RAT) used for cyber espionage, data exfiltration, and persistent access to compromised systems. This multi-stage infection exploits legitimate software, using advanced evasion techniques to ensure long-term access. The malware's use of DLL sideloading and custom payloads demonstrates the advanced capabilities of the responsible actor. The actor behind FatalRAT appears to be a nation-state or advanced cybercriminal group, initially targeting Chinese-speaking environments for cyber surveillance or data theft. However, its flexibility makes it easily adaptable to English-speaking targets and industries worldwide.

FatalRAT has significant re-purposing potential for intellectual property theft, corporate espionage, and disruption in sectors like government, finance, and technology. Its ability to evade detection and exploit vulnerabilities means it could easily target other industries globally. This makes it a growing threat, as it can be adjusted to target regions and sectors outside of its current focus.

Given its evolving nature, FatalRAT poses a major risk not just to Chinese-speaking targets, but to global organizations. Its capabilities underline the critical need for robust cybersecurity and proactive threat defenses to protect against such highly adaptable threats.

## Mitigation

Defending against FatalRAT requires proactive measures, including:

**Email and Zip File Security:** Implement advanced email filtering to block malicious attachments and suspicious zip files.

**Block Traffic to High-Risk Infrastructures:** Leverage advanced analytics to identify high-risk traffic patterns and restrict access to critical infrastructures, reducing the attack surface.

**Adversary Behavior Detection:** Deploy behavioural analysis tools to detect anomalous activity that indicates advanced threat behavior, such as lateral movement or privilege escalation.

**Proactive Post-Breach Threat Hunting:** Use forensic analysis and threat hunting techniques to identify and neutralize any undetected threats, minimizing long-term impact.

# Technical Details

**Initial Delivery**

FatalRAT is often delivered through phishing emails or malicious Zip files shared via unsecured channels like Telegram. These files are disguised as legitimate software updates or system tools. Once opened, they drop loader components that fetch the RAT payload. In some cases, compromised legitimate software (e.g., PureCodec) is used, with altered configuration files directing the system to download the malicious payload.

**Stage 1: Initial Loader (Before.dll)**

The first-stage loader, Before.dll, serves to configure the malware environment and gather information about the infected system. It utilizes a custom note structure hosted on Youdao (note.youdao.com) to retrieve dynamically encrypted configuration information. The configuration contains several URLs for further malware download, which are tested sequentially until a working link is found. Upon successful retrieval, the Before.dll module writes the vanconfig.ini configuration file and stores a victim ID in history.txt. Before.dll also creates a fake invoice document to distract the user, simulating normal application behavior to avoid detection.

**Stage 2: Second-Stage Loader (Fangao.dll)**

Fangao.dll further configures the infected machine and begins the critical task of downloading the FatalRAT payload. The loader first checks several system configurations to ensure the malware is not operating in a virtual machine or sandbox environment (via system checks like time zone, language, etc.). Once the system is deemed suitable, Fangao.dll uses the configuration file created by Before.dll to download the FatalRAT payload, dll.dll, decrypting it in memory using a seven-byte XOR key. After successful decryption, Fangao.dll launches FatalRAT, ensuring it operates without detection by the user through the presentation of a misleading error message.

**Stage 3: Exploitation of PureCodec (0user.exe)**

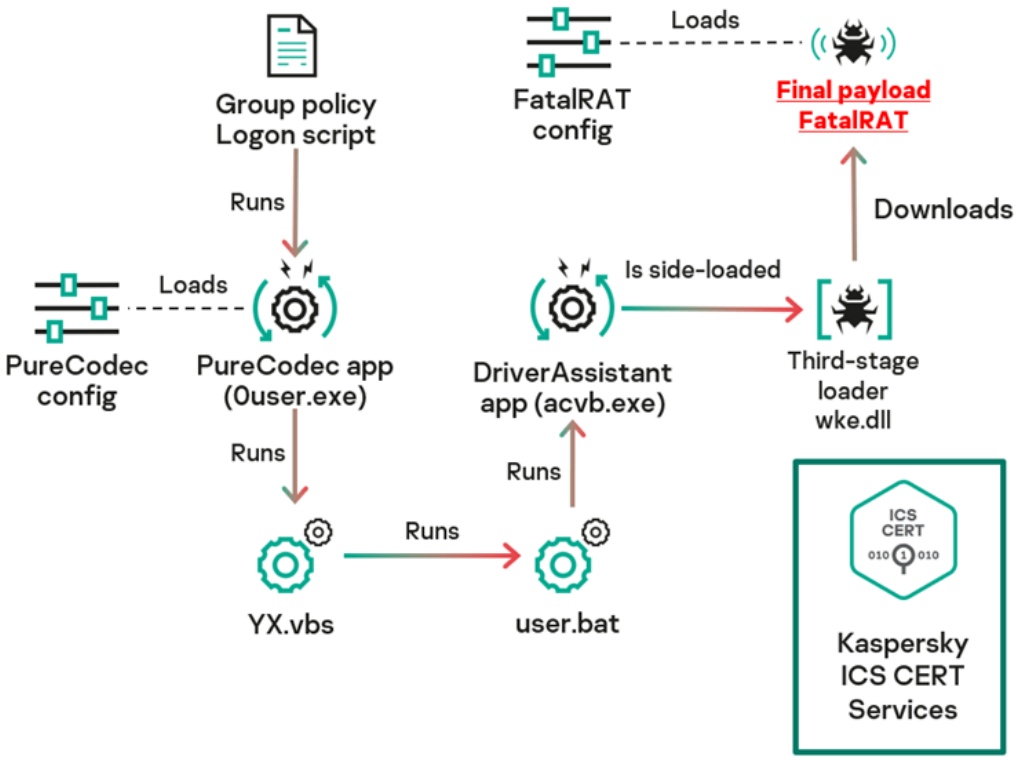
The PureCodec application, disguised as 0user.exe, plays a pivotal role in executing the malware's next phase. Originally a legitimate media player (PurePlayer.exe), the attacker modifies the update.ini file to launch a malicious VBScript (YX.vbs) rather than a legitimate program update. YX.vbs executes a user.bat script, which manipulates system directories and file attributes, creating hidden and read-only files in C:\usero and setting up malicious DLLs and executables for further exploitation. The script performs DLL sideloading on acvb.exe, the legitimate DriverAssistant tool, to execute the malicious wke.dll.

**Stage 4: Final Payload (FatalRAT)**

The final payload, FatalRAT, is delivered and executed through wke.dll, which is loaded into memory via DLL sideloading in acvb.exe. Upon execution, FatalRAT conducts a series of checks to identify if it is operating in a virtual machine or sandbox environment. If the system passes these checks, FatalRAT performs various malicious activities, including keylogging, data exfiltration, and modifying system settings to ensure persistence. Notably, FatalRAT sets a registry key to prevent the computer from being locked by disabling the LockWorkstation function and sends the collected data to a command and control (C&C) server.

# Infection Chain Diagram

This campaign demonstrates a high level of sophistication, employing a multi-stage, purposeful attack that strategically uses a combination of phishing, trusted relationships, DLL side-loading, and evasion techniques. The actors meticulously craft their malware to evade detection, persist on compromised systems, and stealthily communicate with command-and-control servers, showcasing a well-organized and deliberate approach to maintain long-term access.




**Source:** Kaspersky ICS CERT Services

CyberStash notes that it would be unusual for an attacker to put so much effort into a multi-stage, highly detailed campaign and limit their target scope to only Chinese-speaking individuals. While the current scope may be restricted, it is expected that other threat actors will adapt and modify this campaign to target additional regions and languages, leveraging its sophisticated tactics and methods for broader exploitation.

CyberStash advises that, given the ease with which attackers can modify file hashes and names, relying solely on these indicators of compromise (IOCs) for detection is insufficient. Instead, it is more effective to follow the previously provided recommendations, focusing on behavioural analysis based on the attack's tactics and techniques, proactive threat hunting, and attack-surface reduction. This approach is critical as it enables organizations to identify and respond to the evolving nature of the campaign, even when IOCs are modified.

# Tactics, Techniques and Procedures

The following TTPs have been observed in relation to FatalRAT campaign:

**Initial Access**

- Phishing (T1566): Utilizing email attachments with ZIP archives to deliver malicious loaders.
- Trusted Relationship (T1199): Exploiting legitimate cloud services (e.g., myqcloud and Youdao Cloud Notes) to host and deliver malicious payloads, bypassing security filters.

**Persistence**

- DLL Side-Loading (T1574.002): Loading malicious DLLs through legitimate executables to maintain persistence and evade detection.
- Privilege Escalation
- Exploitation for Privilege Escalation (T1075): Exploiting legitimate software (e.g., DriverAssistant) to gain elevated privileges and load malicious DLLs.

**Defense Evasion**

- Virtualization/Sandbox Evasion (T1497): Performing multiple checks to detect virtual environments and halting execution if such environments are detected.
- File and Directory Permissions Modification (T1070.006): Modifying file and directory attributes (hidden, read-only, system) to evade detection and prevent removal.
- Masquerading (T1036): Using filenames and paths that resemble legitimate system files (e.g., acvb.exe) to disguise malicious payloads.

**Discovery**

- System Information Discovery (T1082): Gathering system details (OS version, running processes, security software) to adjust behavior and avoid detection.

**Collection**

- Keylogging (T1056.001): Intercepting keystrokes with a keylogger to collect sensitive information for exfiltration.

**Command and Control**

- Command and Control over HTTP (T1071.001): Communicating with C2 servers using HTTP protocols to blend with normal traffic.

# Cyber Threat Intelligence

Despite the lack of definitive attribution, several significant indicators point to a Chinese-speaking threat actor behind FatalRAT. These include the use of Chinese language in the malware's infrastructure and metadata, as well as the exploitation of Chinese cloud services (e.g., myqcloud and Youdao) to host malicious payloads. Furthermore, the use of DLL side-loading via Chinese-language software, DriverAssistant, suggests the involvement of Chinese -speaking actors. The exploitation of legitimate regional services and the application of obfuscation techniques commonly associated with Chinese cyber operations further support this hypothesis.

## Why Now?

The increasing sophistication of this multi-stage campaign, its purposeful targeting of Chinese-speaking regions, and the use of Chinese-language infrastructure suggest that the attacker is focused on specific objectives within those regions. The tailored approach and the evolving attack vectors make it a highly targeted and adaptable campaign. The geopolitical context—especially the ongoing tensions and security concerns in China—also adds a layer of complexity to these attacks, with non-state actors potentially leveraging the gap in resources for political or financial gain. As the infrastructure evolves, it is expected that threat actors will repurpose this campaign to target regions beyond China.

While direct attribution remains elusive, the overlap in infrastructure, including domains and IP addresses previously linked to Ghost RAT, suggests that FatalRAT may be an evolution of, or closely related to, previous campaigns involving Ghost RAT. The use of non-standard ports and unique command-and-control infrastructure also aligns with tactics commonly employed by Chinese APT groups.

**Prediction:** Based on the increasing sophistication, geographic targeting, and shared infrastructure, CyberStash predicts that FatalRAT is most likely the work of a non-state, financially motivated actor, rather than a state-sponsored group. However, the attack's operational tactics, use of regional cloud services, and association with Chinese language and infrastructure still suggest it could be the work of a Chinese-speaking cybercriminal group or a non-state actor operating in the region. Given the adaptable nature of the campaign, it is expected that other threat actors will repurpose this attack to target regions beyond China, potentially broadening its scope.

## Why Non-State Actors:

- **Targeting Chinese-Speaking Regions:** The use of Chinese language artifacts and cloud services suggests familiarity with the region, but non-state actors, especially cybercriminal groups, are more likely to exploit these targets for convenience or profitability rather than for any political motive.

- **Non-state Actor Motivation:** The malware's persistence, data exfiltration, and stealth tactics align with the typical goals of financially motivated actors who are more focused on high-value data and operational efficiency than geopolitical objectives.

- **Malware Adaptability:** FatalRAT shows signs of being adaptable and reusable, characteristics typical of non-state actors who are primarily motivated by financial gain, rather than political or strategic agendas.

# References

## IOCs:

https://ics-cert.kaspersky.com/publications/reports/2025/02/24/fatalrat-attacks-in-apac-backdoor-delivered-via-an-overly-long-infection-chain-to-chinese-speaking-targets/

## Public Intelligence:

- https://thehackernews.com/2025/02/fatalrat-phishing-attacks-target-apac.html
- https://malpedia.caad.fkie.fraunhofer.de/details/win.fatal_rat
- https://cyberpress.org/chinese-hackers-launch-sophisticated-fatalrat-attack/?amp=1
- https://ics-cert.kaspersky.com/publications/reports/2025/02/24/fatalrat-attacks-in-apac-backdoor-delivered-via-an-overly-long-infection-chain-to-chinese-speaking-targets/