Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

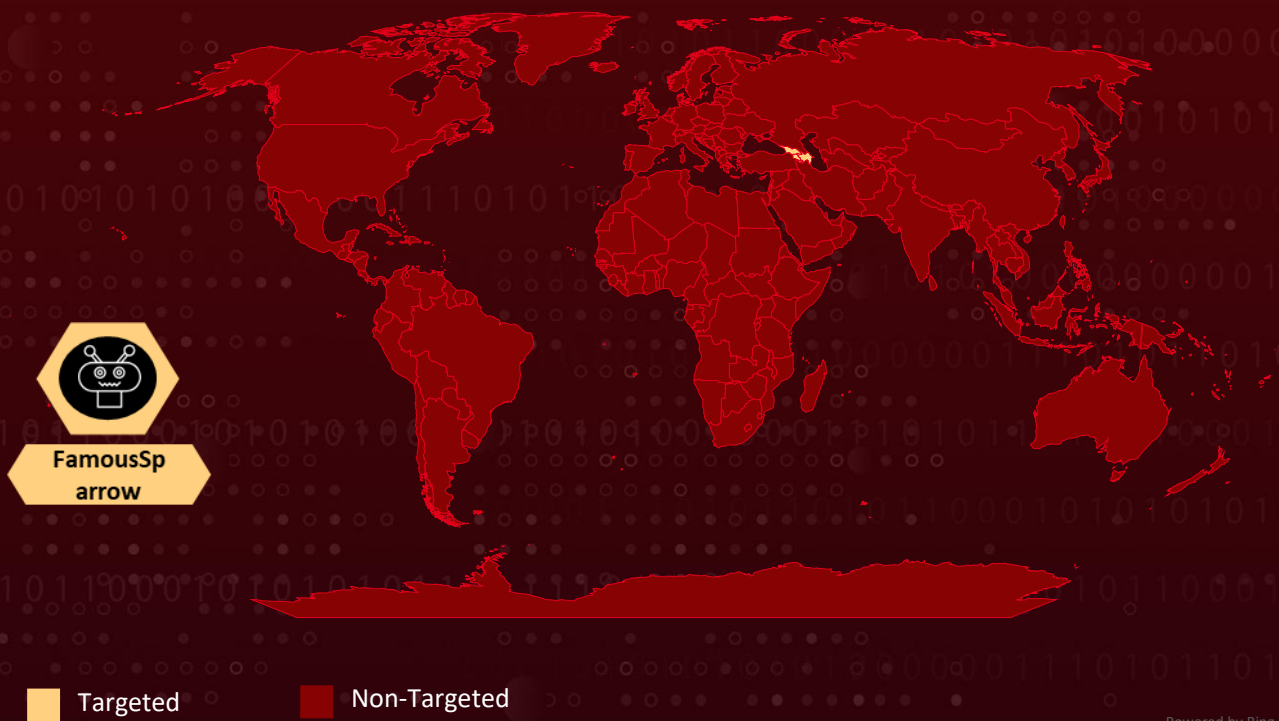
FamousSparrow's Persistent Hold on Azerbaijani Oil & Gas

Date of Publication	Admiralty Code	TA Number
May 15, 2026	A1	TA2026133

Summary

First Seen: December 25, 2025
Targeted Regions: Armenia, Azerbaijan, Georgia
Targeted Platform: Windows
Targeted Product: Microsoft Exchange Server
Targeted Industries: Oil and Gas, Energy
Threat Actor: FamousSparrow (aka UNC2286, GhostEmperor, RedMike, Operator Panda, Earth Estries, Salt Typhoon)
Malware: Deed RAT (aka Snappybee), Terndoor, Mofu loader
Attack: A multi-wave intrusion conducted by the China-linked FamousSparrow APT against an Azerbaijani oil and gas company between late December 2025 and late February 2026. The operators repeatedly re-exploited the same unpatched Microsoft Exchange Server via the ProxyNotShell chain (CVE-2022-41040 + CVE-2022-41082) to drop ASPX web shells, then deployed Deed RAT and Terndoor backdoors across three distinct waves. The intrusion is notable for an evolved DLL sideloading technique that splits malicious logic across two DLL exports to gate execution behind the host application's natural control flow, defeating sandbox triage. The operation extends FamousSparrow's known targeting map into the South Caucasus energy sector, a region of growing strategic importance to European gas supply.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2022-41040	ProxyNotShell (Microsoft Exchange Server Elevation of Privilege Vulnerability)	Microsoft Exchange Server	✓	✓	✓
CVE-2022-41082	ProxyNotShell (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✓	✓	✓

Attack Details

#1

The cyberthreat group China's **'FamousSparrow'** APT targets an Azerbaijani oil and gas firm with repeated attacks. The intrusion began on December 25, 2025, when the Microsoft Exchange IIS worker process attempted to write a malicious web shell into a publicly accessible directory on the victim's Exchange server. The command line carried the MSExchangePowerShellAppPool argument, indicating exploitation of the ProxyNotShell chain (CVE-2022-41040 paired with CVE-2022-41082). Across December 25, 26, and 29, the attackers staged multiple ASPX web shells, then deployed the Deed RAT three-component chain in the legitimate LogMeIn Hamachi binary, the malicious loader lmiguardiandll.dll, and the encrypted payload container .hamachi.lng.

#2

The components were relocated to C:\Program Files (x86)\LogMeIn Hamachi to mimic a legitimate installation, and a Windows service named "LogMeIn Hamachi" was registered to auto-launch LMIGuardianSvc.exe at startup. The sideloading mechanism is an evolution of the standard technique: malicious logic is split across two DLL exports (Init and ComMain) embedded within the host application's normal control flow. Init temporarily relaxes memory protections to patch the StartServiceCtrlDispatcherW Windows API for call redirection, then exits. When the legitimate service flow later invokes ComMain and reaches the patched API, execution is diverted into the loader, which restores the original bytes and decrypts the .hamachi.lng payload using AES-128-CBC.

#3

The decrypted shellcode resolves Windows APIs via ELF hash comparison, decrypts the orchestrator using RC4, and decompresses it with RtlDecompressBuffer (LZNT1) before transferring execution to the Deed RAT main module, identified by the updated magic value 0xFF66ABCD (previously 0xDEED4554). The orchestrator loads plugins (Startup, Config, Plugin, Network, NetSocket, NetProxy, Install, Inject) decrypted with a custom PRNG XOR routine and decompressed with Deflate a switch from Snappy in older variants. First-wave C2 was over HTTPS, with process injection targeting SearchIndexer.exe, taskeng.exe, iexplore.exe, and taskhost.exe.

#4

With persistence established, the attackers pivoted to a second host via RDP using a domain administrator account, indicating prior credential compromise. They launched a PowerShell console and manually staged LMIGuardianSvc.exe and its companion files within minutes to create a redundant foothold, then used Impacket-style atexec and smbexec utilities over SMB to reach a third machine. About a month later, the operators returned through the same Exchange entry point and attempted to deploy the Terndoor backdoor and used it to sideload a malicious winmm.dll from C:\ProgramData\USOShared. The loader was identified as Mofu Loader (previously attributed to GroundPeony) based on its NOP+CALL prologue and subtract-XOR-add decryption routine, which produces an LZNT1-compressed PE with stripped MZ/PE headers. Terndoor attempted to register a kernel driver service, but security tooling blocked the installation; recovered strings showed encrypted on-stack storage decoded via single-byte XOR and an RC4 implementation with a hardcoded key whose fingerprint matched UAT-9244 samples.

#5

The final wave in late February 2026 saw Deed RAT redeployed through the same execution chain with a refreshed configuration: C2 rotated to sentinelonepro[.]com:443 masquerading as SentinelOne, all components relocated to C:\Recovery, the service renamed to "HamachiNet", the mutex updated to HJKMNbxzcv9876asdfghj, the RSA public key rotated, and process injection retargeted at wininit.exe and dwm.exe alongside SearchIndexer.exe and taskhost.exe. Configuration data was stored under HKCU\SOFTWARE\Microsoft\LogMeIn Hamachi, with a HamachiNet entry added to HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Across all three waves, the attackers preserved access through multiple remediation cycles by swapping backdoors while reusing the same Exchange entry point — indicating sustained espionage with operational discipline rather than opportunistic compromise.

Recommendations

Patch Microsoft Exchange Servers: Apply Microsoft security updates for CVE-2022-41040 and CVE-2022-41082 immediately on all on-premises Exchange 2013, 2016, and 2019 deployments. ProxyNotShell has been patched since November 2022, and unpatched servers remain a primary entry point for FamousSparrow operations.

Monitor IIS Worker Process for Web Shell Drops: Alert on w3wp.exe writing .aspx files to publicly accessible Exchange directories, particularly under the MSExchangePowerShellAppPool context. Legitimate Exchange maintenance rarely writes web-accessible scripts through the IIS worker process.

Detect API Hooking on Critical Windows Functions: Monitor for modifications to the first bytes of frequently abused Windows APIs including StartServiceCtrlDispatcherW, NtCreateFile, CreateProcessW, and LdrLoadDll. Unsigned binaries applying API hooks should trigger immediate investigation.

Restrict Unauthorized Kernel Driver Installation: Alert on service creation events where Type=1 (kernel driver) and ImagePath points to non-standard locations such as C:\ProgramData or C:\Temp. Legitimate kernel drivers are installed through signed INF files into C:\Windows\System32\drivers.

Log Impacket-Style SMB Lateral Movement: Capture and review use of atexec, smbexec, and PsExec across the environment. These tools are rarely used in legitimate workflows outside of IT administration and are a strong indicator of hands-on-keyboard activity.

Apply Memory Scanning for Custom PE Headers: Deploy in-memory YARA scanners and memory forensics to detect characteristic Deed RAT patterns, including the magic values 0xFF66ABCD, 0xDEED4554, and 0x46B78C45, LZNT1-compressed payloads following RC4 decryption, and ELF hash-based API resolution.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Persistence	T1505: Server Software Component	T1505.003: Web Shell
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
Execution	T1569: System Services	T1569.002: Service Execution
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
Defense Evasion	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1140: Deobfuscate/Decode Files or Information	
	T1562: Impair Defenses	
	T1027: Obfuscated Files or Information	
	T1055: Process Injection	
	T1014: Rootkit	
	T1036: Masquerading	T1036.005: Match Legitimate Resource Name or Location
Credential Access	T1078: Valid Accounts	T1078.002: Domain Accounts
Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares

Tactic	Technique	Sub-technique
Discovery	T1016: System Network Configuration Discovery	
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	0554f3b69d39d175dd110d765c11347a, 762f787534a891eca8aa9b41330b4108, 505b55c2b68e32acb5ad13588e1491a5
File Path	C:\TEMP\LMIGuardianSvc.exe, C:\TEMP\lmiguardiandll.dll, C:\TEMP\.hamachi.lng, C:\Program Files (x86)\LogMeIn Hamachi\LMIGuardianSvc.exe, C:\Program Files (x86)\LogMeIn Hamachi\LMIGuardianDll.dll, C:\Program Files (x86)\LogMeIn Hamachi\.hamachi.lng, C:\ProgramData\USOShared\USOShared.exe, C:\ProgramData\USOShared\winmm.dll, C:\ProgramData\USOShared\vmflt.sys, C:\ProgramData\USOShared\cache.dat, C:\Recovery\ (Wave 3 staging directory)
File Name	key.aspx, log.aspx, errorFE_.aspx, signout_.aspx, xboxs.sys
Registry Key	HKLM\SYSTEM\CurrentControlSet\Services\vmflt\Type (value: 1), HKLM\SYSTEM\CurrentControlSet\Services\vmflt\ImagePath (value: \??\C:\ProgramData\USOShared\vmflt.sys), HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Hamachi Net, HKCU\SOFTWARE\Microsoft\LogMeIn Hamachi

TYPE	VALUE
Domain	virusblocker[.]it[.]com, sentinelonepro[.]com
URLs	hxxps[:]//virusblocker[.]it[.]com/12156011215601, hxxps[:]//virusblocker[.]it[.]com/11E6C6611E6C66
Mutex	HJBNDusadnfy3278rnhsdaf
	HJKMNbxzcv9876asdfghj
Service Name	LogMeIn Hamachi, HamachiNet, vmflt
Magic Value	0xFF66ABCD, 0xDEED4554, 0x46B78C45

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-41082

References

https://www.bitdefender.com/en-us/blog/businessinsights/famoussparrow-apt-targets-azerbaijani-oil-gas-industry

https://github.com/bitdefender/malware-ioc/blob/master/2026_05_13-famoussparrow-iocs.csv

https://hivepro.com/threat-advisory/salt-typhoon-cyber-attacks-hit-200-organizations-in-the-united-states/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

May 15, 2026 • 3:00 PM

More at www.hivepro.com