Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Operation DRAGONCLONE Strikes the Telecom Sector

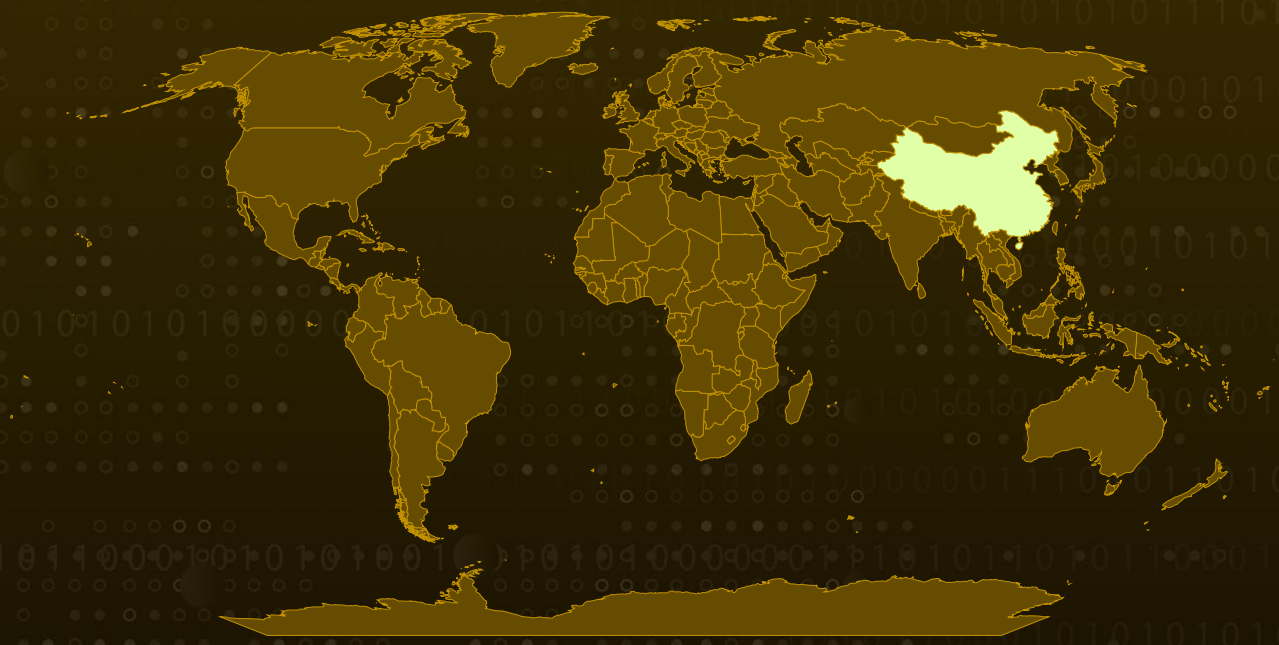
Date of Publication	Admiralty Code	TA Number
June 11, 2025	A1	TA2025181

Summary

Attack Commenced: Early 2025
Campaign: Operation DRAGONCLONE
Malware: VELETRIX and VShell
Targeted Region: China
Targeted Industry: Telecommunications

Attack: In a striking display of precision and deception, Operation DRAGONCLONE has emerged as a sophisticated cyber-espionage campaign targeting the heart of the Chinese telecom industry. Leveraging trusted software, deceptive spear-phishing, and advanced implants, the operation demonstrates how legitimate tools can be weaponized to silently breach defenses, establish covert footholds, and maintain persistent control, all while evading conventional detection measures.

Attack Regions



Attack Details

#1 Operation DRAGONCLONE is a sophisticated cyber-espionage campaign targeting the Chinese telecommunications industry. This operation revolves around a malware ecosystem primarily leveraging two key components: VELETRIX, a custom implant, and VShell, a well-known adversary simulation tool repurposed for malicious activity.

#2 The attack chain is initiated through spear-phishing emails sent to carefully selected victims within the targeted organizations. These emails carry a malicious ZIP archive as an attachment. Upon extraction, the archive contains a mixture of EXE and DLL files, many of which are legitimately Microsoft-signed binaries, while others bear valid code-signing certificates to evade security controls and reduce suspicion.

#3 A critical technique employed in this campaign is DLL sideloading, which allows the threat actor to execute malicious payloads using trusted applications covertly. In this case, a legitimate copy of Wondershare Recoverit, a data recovery tool, serves as the host for sideloading the VELETRIX implant.

#4 Once executed, VELETRIX operates as a loader or staging malware, establishing initial access to the compromised system. To evade detection and hinder analysis, it employs simple anti-analysis techniques, notably a combination of the Sleep and Beep Windows APIs to delay and disrupt automated analysis tools.

#5 After securing its foothold, VELETRIX proceeds to deploy a more advanced implant, the VShell OST Implant. This secondary payload establishes a persistent command-and-control (C2) communication channel with an external server, granting attackers ongoing remote access to the infected systems. Through this C2 infrastructure, the adversaries can interact with compromised devices, exfiltrate sensitive data, and carry out espionage operations undetected, ultimately achieving their intelligence-gathering and data theft objectives.

Recommendations

Strengthen Email Security Posture: Deploy advanced email security gateways capable of detecting spear-phishing attempts with malicious ZIP attachments. Implement AI-powered phishing detection tools to analyze email metadata, attachments, and sender anomalies.

Supply Chain and Software Integrity Management: Implement a Software Bill of Materials (SBOM) Policy to maintain an accurate, continuously updated inventory of third-party software dependencies within the environment. Verify Code-Signing Certificate Reputation before trusting digitally signed files, using external threat intel feeds and internal validation.

Apply Principle of Least Privilege (PoLP) Across Endpoints: Ensure users and processes operate with the minimum necessary privileges. Limit administrative access and enforce multi-factor authentication (MFA) for privileged operations.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0005 Defense Evasion	**TA0007** Discovery	**TA0011** Command and Control	**TA0010** Exfiltration
T1595 Active Scanning	**T1595.002** Vulnerability Scanning	**T1588** Obtain Capabilities	**T1588.002** Tool
T1140 Deobfuscate/Decode Files or Information	**T1566** Phishing	**T1566.001** Spearphishing Attachment	**T1204** User Execution
T1204.002 Malicious File	**T1083** File and Directory Discovery	**T1574** Hijack Execution Flow	**T1574.001** DLL Search Order Hijacking
T1027.007 Dynamic API Resolution	**T1027.013** Encrypted/Encoded File	**T1055** Process Injection	**T1497** Virtualization/Sandbox Evasion
T1497.003 Time Based Evasion	**T1046** Network Service Discovery	**T1587** Develop Capabilities	**T1587.002** Code Signing Certificates
T1218 System Binary Proxy Execution	**T1036** Masquerading	**T1001** Data Obfuscation	**T1041** Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
Filename	附件.zip, attachment.zip, drstat.dll, drstat.exe, tcp_windows_amd64.dll, mscoree.dll, tcp_windows_amd64.exe
SHA256	40450b4212481492d2213d109a0cd0f42de8e813de42d53360da7efac7249df4, ac6e0ee1328cfb1b6ca0541e4dfe7ba6398ea79a300c4019253bd908ab6a3dc0, 645f9f81eb83e52bbbd0726e5bf418f8235dd81ba01b6a945f8d6a31bf406992, ba4f9b324809876f906f3cb9b90f8af2f97487167beead549a8cddfd9a7c2fdc, bb6ab67ddbb74e7afb82bb063744a91f3fecf5fd0f453a179c0776727f6870c7, 2206cc6bd9d15cf898f175ab845b3deb4b8627102b74e1accefe7a3ff0017112, a0f4ee6ea58a8896d2914176d2bfbdb9e16b700f52d2df1f77fe6ce663c1426a
IPv4	62[.]234[.]24[.]38, 47[.]115[.]51[.]44, 47[.]123[.]7[.]206

References

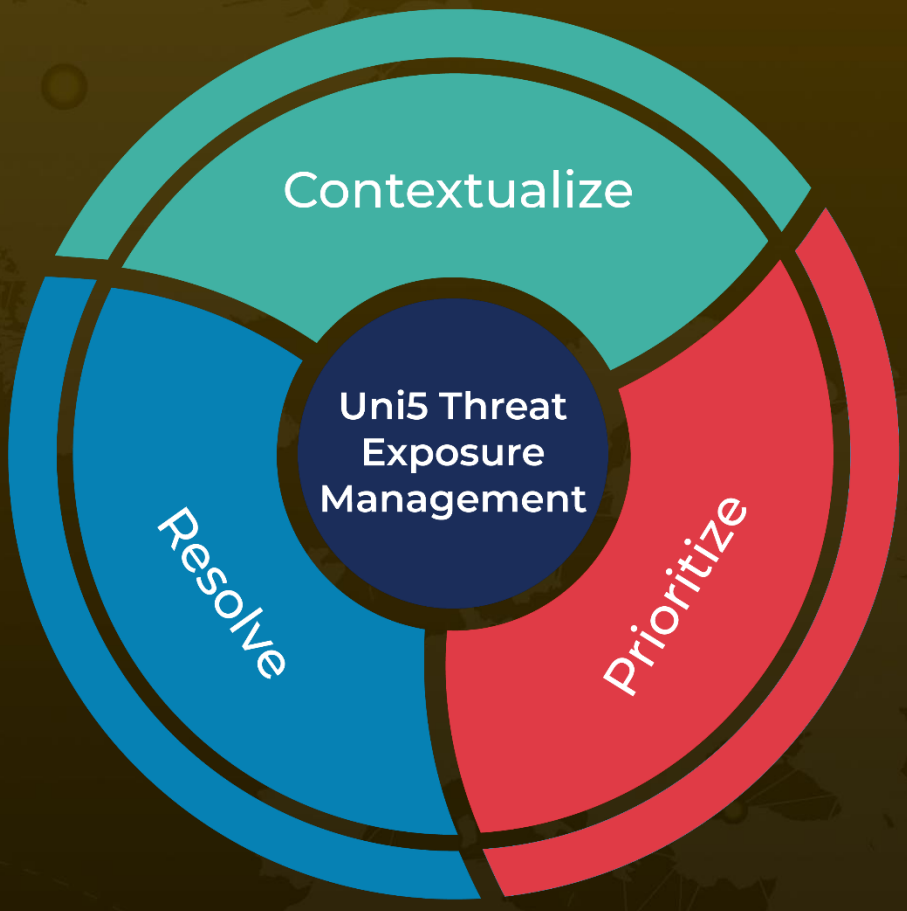
https://www.seqrite.com/blog/operation-dragonclone-chinese-telecom-veletrix-vshell-malware/

https://www.cisa.gov/sbom

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 11, 2025 • 2:00 AM

More at www.hivepro.com