Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

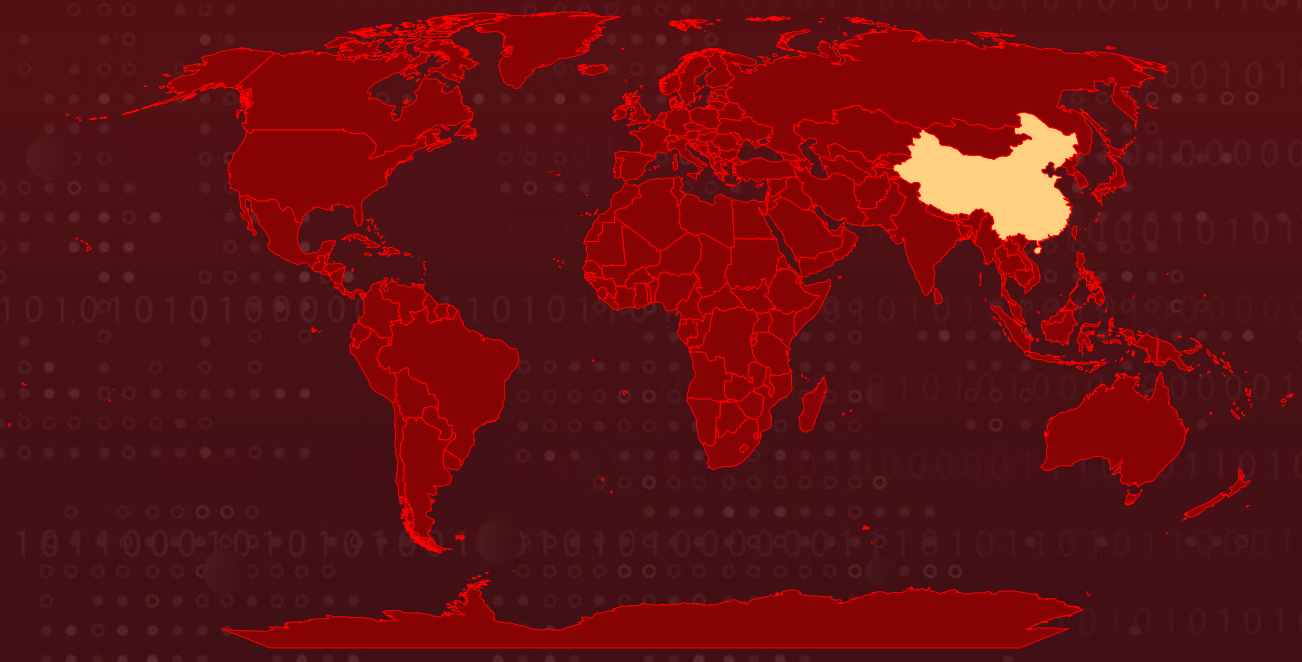
Operation Silk Lure Scam: When Job Hunts Leads to Malware

Date of Publication	Admiralty Code	TA Number
October 17, 2025	A1	TA2025320

Summary

Attack Discovered: 2025
Targeted Country: China
Targeted Industries: FinTech, Cryptocurrency Exchange, and Trading Platform Sectors
Campaign: Operation Silk Lure
Affected Platform: Windows
Malware: ValleyRAT
Attack: An ongoing campaign dubbed Operation Silk Lure has emerged, using fake Chinese-language resumes to target professionals in the fintech and cryptocurrency sectors. Masquerading as legitimate job opportunities, the attackers deliver malicious .LNK files that trigger stealthy malware infections. Once inside, the threat executes reconnaissance, steals sensitive data, and deploys the ValleyRAT backdoor to maintain persistence and evade antivirus tools. The decoy résumé of a blockchain engineer, written in fluent Simplified Chinese with convincing local details, makes the lure particularly believable for Chinese-speaking victims. This campaign blends social engineering and technical sophistication, turning the simple act of opening a job application into a full-blown cyber-espionage threat.

Attack Regions



Attack Details

#1 An ongoing campaign has been observed weaponized to target Chinese-speaking professionals seeking roles in fintech, cryptocurrency exchanges, and trading platforms. Attackers use carefully tailored spear-phishing lures, believable Chinese-language resumes, and emails that conceal malicious LNK files inside what appear to be legitimate documents. When opened, those shortcuts kick off an initial compromise chain that quietly drops and executes additional payloads on the victim's machine.

#2 Once deployed, the malware conducts broad reconnaissance: it captures screenshots, harvests document metadata, and exfiltrates the collected material to remote servers. Those actions expose victims to a range of harms from credential theft and identity compromise to long-term espionage, because sensitive technical details and personal information may be siphoned off without the user's knowledge.

#3 The decoy material is highly localized and tailored. The malicious PDF masquerades as the résumé of "Li Hanbing," a senior backend/blockchain full-stack engineer, written in Simplified Chinese and referencing a bachelor's degree from South China Agricultural University plus roles in Guangdong. It lists relevant technologies and production experience with trading exchanges and DeFi protocols, details intended to build credibility and increase the likelihood that Chinese targets will open the file.

#4 At the heart of the intrusion is a staged loader and secondary payloads. A dropped binary, keytool.exe, acts as a self-extracting loader that locates an embedded, marker-tagged blob, uses RC4 with a fixed key to decrypt it, and then executes the concealed shellcode. That second-stage component contains **ValleyRAT**, which implements persistence via a scheduled "Security" task, file-dropping behavior, runtime decryption of its payload, and housekeeping routines to prepare execution while concealing traces.

#5 The campaign also includes aggressive anti-defense and surveillance features. The malware probes the environment for virtualization and enumerates installed AV products via COM/WMI queries, attempts to disrupt defenses, and sets up keylogging, log rotation, and system-survey routines to fingerprint victims. The attackers host C2 and decoy content on a cluster tied to SONDERCLOUDLIMITED, using a family of .work domains that mimic job portals, a pattern consistent with what defenders are calling Operation Silk Lure and one that yields clear hunting indicators.

Recommendations

Be Cautious With Unexpected Job-related Documents: If you receive a résumé, portfolio, or offer letter from an unknown sender, especially one containing unusual file types like .lnk, .zip, or .rar, avoid opening it. Legitimate recruiters or candidates typically send standard formats like .pdf or .docx.

Disable Windows Shortcut (LNK) File Execution When Possible: Malicious .lnk files are often disguised as harmless documents. Restrict execution of these shortcuts through Group Policy or endpoint protection settings to reduce infection risks.

Strengthen Email Security Controls: Enable attachment scanning and sandboxing in mail gateways to detect and block malicious links or file attachments. Configure rules to flag or quarantine emails from unknown domains or with mismatched sender addresses.

Enforce Least-privilege Access And Isolation: Restrict user permissions, limit script execution, and use application control to prevent untrusted binaries like keytool.exe from running on endpoints.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	T1566 Phishing	T1566.001 Spearphishing Attachment

T1059 Command and Scripting Interpreter	**T1059.001** PowerShell	**T1059.005** Visual Basic	**T1053** Scheduled Task/Job
T1053.005 Scheduled Task	**T1204** User Execution	**T1204.002** Malicious File	**T1547** Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	**T1055** Process Injection	**T1055.001** Dynamic-link Library Injection	**T1055.002** Portable Executable Injection
T1140 Deobfuscate/Decode Files or Information	**T1574** Hijack Execution Flow	**T1574.001** DLL	**T1070** Indicator Removal
T1070.004 File Deletion	**T1070.009** Clear Persistence	**T1036** Masquerading	**T1036.008** Masquerade File Type
T1112 Modify Registry	**T1027** Obfuscated Files or Information	**T1027.009** Embedded Payloads	**T1027.010** Command Obfuscation
T1027.013 Encrypted/Encoded File	**T1497** Virtualization/Sandbox Evasion	**T1497.001** System Checks	**T1497.002** User Activity Based Checks
T1555 Credentials from Password Stores	**T1555.003** Credentials from Web Browsers	**T1056** Input Capture	**T1056.001** Keylogging
T1056.002 GUI Input Capture	**T1556.004** Network Device Authentication	**T1083** File and Directory Discovery	**T1115** Clipboard Data
T1005 Data from Local System	**T1039** Data from Network Shared Drive	**T1113** Screen Capture	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1041** Exfiltration Over C2 Channel	**T1047** Windows Management Instrumentation	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	6ea9555f1874d13246726579263161e8, f5b9ad341ccfe06352b8818b90b2413e, 83b341a1caab40ad1e7adb9fb4a8b911, 3ca440a3f4800090ee691e037a9ce501, e94e7b953e67cc7f080b83d3a1cdcb1f
IPv4	206[.]119[.]175[.]65, 206[.]119[.]175[.]178
SHA256	190d493255c71f3cebb968c197aeef67c62d597b488c4a0b8cd77751e5999b94, ae857addc8eb51dbfa7d0a76b19dae7a6f275f7bf1042d1c982aca4f80ce635e, 158f2617bd2780ce4f1285f8b520a1407f5383e04eed259d014724b0cc4d76eb, 3f7819debdca5df5a6cd50147b51bceba12c5e0f8a6961b1612777080496dde1, 367c0bbc72b885e313f6731e98c7e4fa2d95c3cadb76e642a8492f8b12b3d9de

References

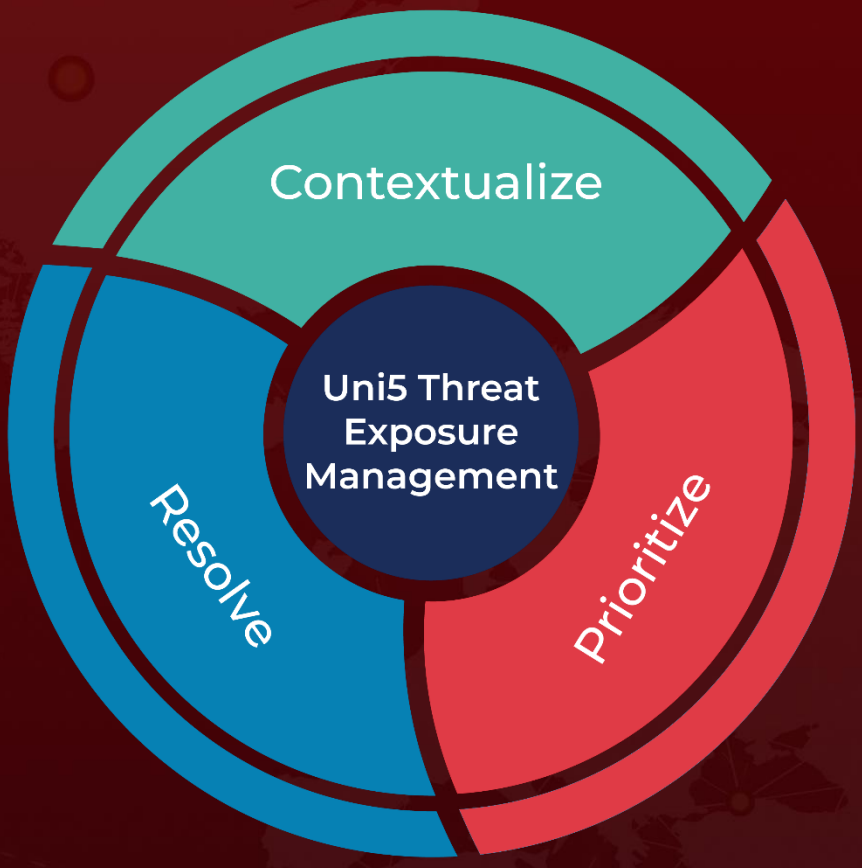
https://www.seqrite.com/blog/operation-silk-lure-scheduled-tasks-weaponized-for-dll-side-loading-drops-valleyrat/

https://hivepro.com/threat-advisory/valleyrat-strikes-organizations-with-stealthy-dll-hijacking-attack/

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

October 17, 2025 • 10:00 AM

More at www.hivepro.com