Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

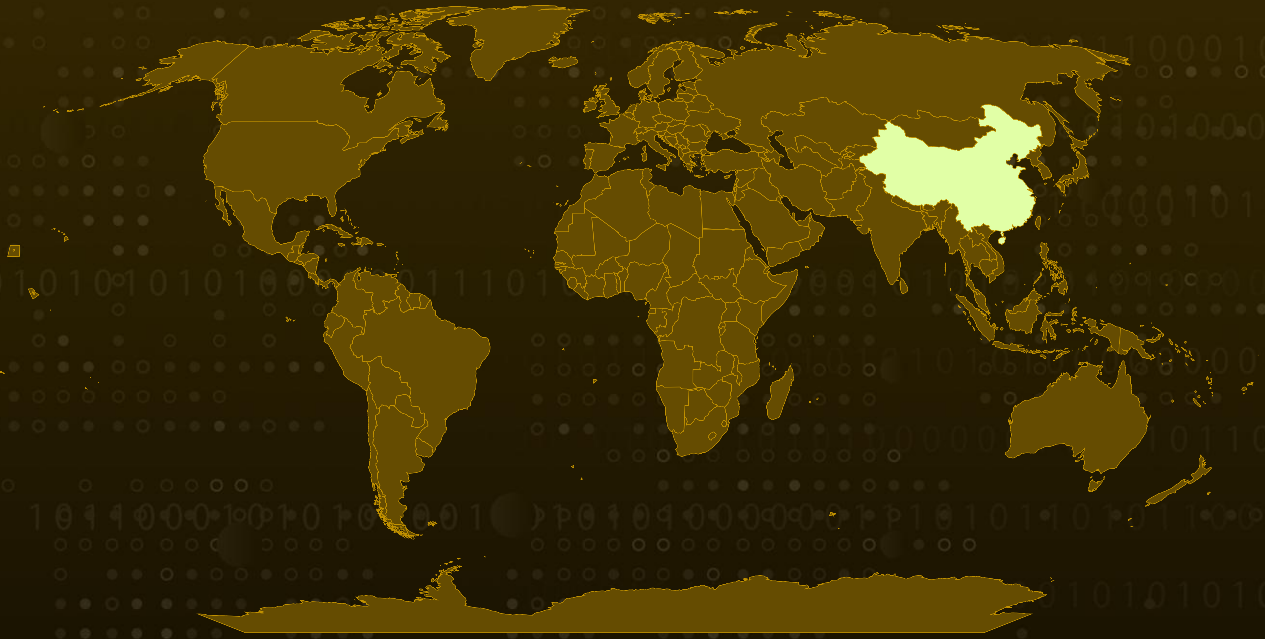
kkRAT Malware Campaign Targeting Chinese-Speaking Users

Date of Publication	Admiralty Code	TA Number
September 12, 2025	A1	TA2025280

Summary

First Seen: May 2025
Targeted Country: China
Malware: kkRAT, ValleyRAT, FatalRAT
Affected Platform: Windows
Attack: kkRAT is a newly discovered remote access trojan active since May 2025, distributed through phishing pages disguised as software installers. It employs strong anti-analysis techniques, privilege escalation, and BYOVD methods to evade detection and disable security tools. The malware achieves persistence via scheduled tasks, registry changes, and startup shortcuts. Its plugin-based design enables remote control, system discovery, proxying, and clipboard hijacking to steal cryptocurrency.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

kkRAT is a recently identified remote access trojan (RAT) first seen in a campaign targeting Chinese-speaking users since May 2025. The campaign lures victims with phishing pages that impersonate popular software installers (hosted on GitHub Pages) and delivers one of several payloads, ValleyRAT, FatalRAT, or kkRAT, via ZIP archives containing malicious executables.

#2

The initial loader applies multiple anti-analysis measures, including timing and hardware checks for sandbox/VM detection, obfuscated API resolution and string decoding, and manipulation of Windows process/registry structures to frustrate automated analysis. Once executed, the malware attempts to escalate privileges and can temporarily disable network adapters to interfere with endpoint communications.

#3

The operators employ a Bring-Your-Own-Vulnerable-Driver (BYOVD) approach to neutralize security product callbacks by exploiting a known vulnerable driver, then remove or disrupt security processes at user level. Persistence mechanisms observed include scheduled tasks, registry run-key modifications, and shortcuts placed in startup locations so the payload survives reboots and user logons.

#4

The kkRAT payload is modular and plugin-driven, it fingerprints the host (OS and hardware details, network configuration, peripheral presence, and installed security software), then communicates with command-and-control servers using a zlib-compressed, XOR-obfuscated protocol.

#5

Available plugins provide remote desktop/control, shell and process management, network enumeration and proxying (including SOCKS5), and clipboard monitoring that can substitute cryptocurrency wallet addresses with attacker-controlled values. The campaign’s design emphasizes stealth, modularity, and monetization-focused capabilities.

Recommendations

Immediate containment & network controls: Block and monitor the malicious domains, GitHub Pages accounts, and C2 endpoints listed in the report at the edge (proxy/web filter and perimeter firewall). Prioritize any IP:port combinations used for C2 and the download hosts for 2025.bin / output.log records.

Harden privilege and driver controls: Restrict who can install drivers or run elevated installers, and enforce least privilege for standard users. Where possible, block installation of unsigned or known-vulnerable drivers at policy level. These controls reduce the ability of attackers to use BYOVD techniques.

Strengthen Email Security and User Awareness: Ensure that email gateways are configured to detect and quarantine spear-phishing messages with encoded script attachments. Implement attachment filtering to block high-risk file types, and use URL sandboxing for links embedded in contract-themed lures. Conduct regular phishing simulation exercises to increase user awareness of socially engineered messages designed to impersonate business communications.

Network Segmentation and Traffic Control: Segment high-value systems from general user networks to limit lateral movement. Apply strict firewall policies to block outbound traffic to known kkRAT command-and-control domains. Inspect DNS logs and network telemetry for anomalous connections or encrypted data flows originating from suspicious processes or hosts.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control
TA0040 Impact	T1566 Phishing	T1204 User Execution	T1204.002 Malicious File

T1497 Virtualization/Sandbox Evasion	T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1140 Deobfuscate/Decode Files or Information
T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder
T1037 Boot or Logon Initialization Scripts	T1037.001 Logon Script (Windows)	T1010 Application Window Discovery	T1057 Process Discovery
T1082 System Information Discovery	T1083 File and Directory Discovery	T1056 Input Capture	T1056.001 Keylogging
T1113 Screen Capture	T1115 Clipboard Data	T1219 Remote Access Tools	T1090 Proxy
T1573 Encrypted Channel	T1041 Exfiltration Over C2 Channel	T1529 System Shutdown/Reboot	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	02cce1811ed8ac074b211717e404fbadffa91b0881627e090da97769f616c434, 140426a92c3444d8dc5096c99fa605fd46cb788393c6522c65336d93cb53c633, 181b04d6aea27f4e981e22b66a4b1ac778c5a84d48160f7f5d7c75dffd5157f8, 35385ab772ebcc9df30507fd3f2a544117fb6f446437c948e84a4fdf707f8029, 36e8f765c56b00c21edcd249c96e83eb6029bc9af885176eaca9893ebad5d9bd, 3e5efe81a43d46c937ba27027caa2a7dc0072c8964bf8df5c1c19ed5626c1fe1,

TYPE	VALUE
SHA256	003998d12e3269286df1933c1d9f8c95ab07c74fa34e31ce563b524e22bb7401, 71ca5dd59e90ec83518f9b33b2a8cdb6a0d6ad4c87293b27885fa2a8e8e07f1c, 80b7c8193f287b332b0a3b17369eb7495d737b0e0b4e82c78a69fa587a6bcf91, a0f70c9350092b31ae77fc0d66efa007ccacbbc4b9355c877c1f64b29012178c, f557a90c1873eeb7f269ae802432f72cc18d5272e13f86784fdc3c38cbaca019
URLs	hxxps[://]github[.]com/sw124456, hxxps[://]youdaoselw[.]icu, hxxps[://]kmhhla[.]top/, hxxp[://]key2025[.]oss-cn-hongkong[.]aliyuncs[.]com/2025[.]bin, hxxp[://]key2025[.]oss-cn-hongkong[.]aliyuncs[.]com/output[.]log, hxxp[://]key2025[.]oss-cn-hongkong[.]aliyuncs[.]com/trx38[.]zip
IPv4:Port	154[.]44[.]30[.]27[:]8250, 156[.]238[.]238[.]111[:]8111, 103[.]199[.]101[.]3[:]8081

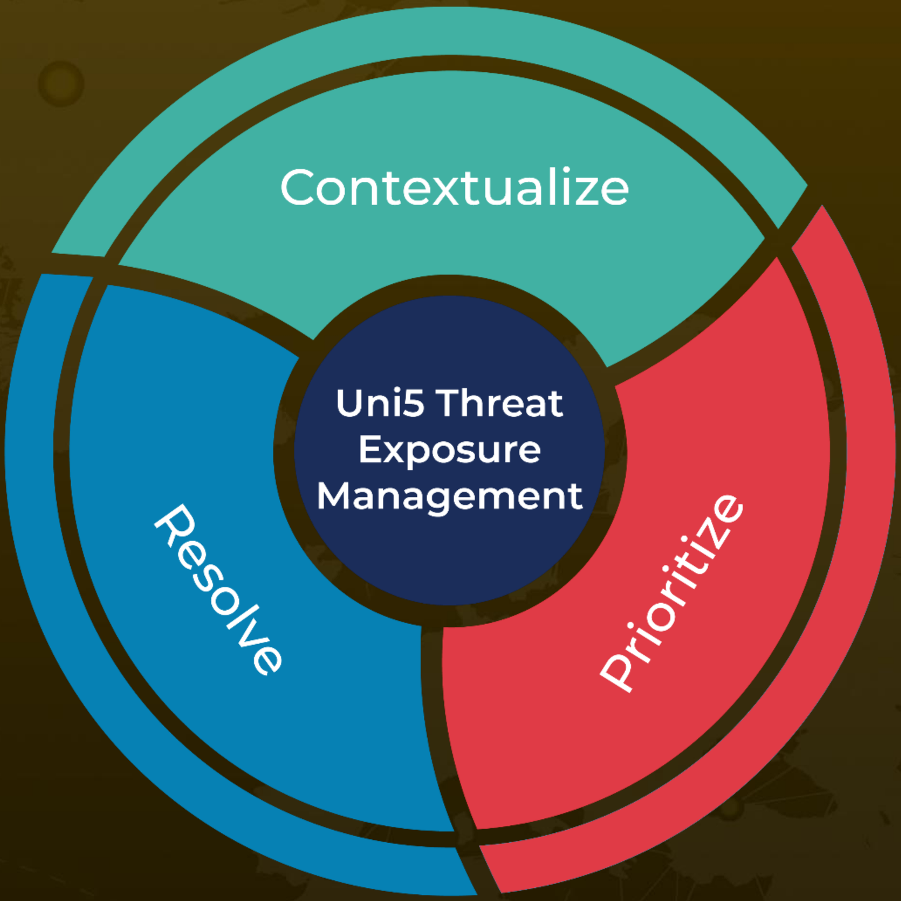
References

https://www.zscaler.com/blogs/security-research/technical-analysis-kkrat

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

September 12, 2025 • 6:30 AM

More at www.hivepro.com