Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

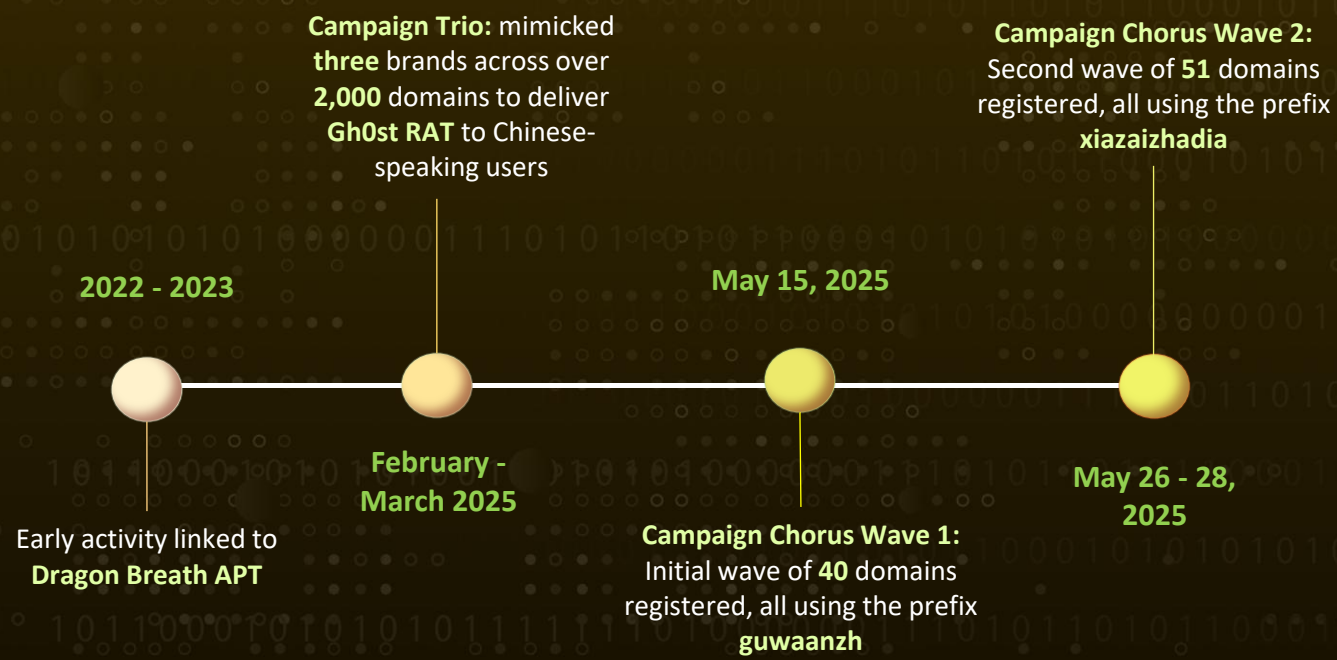
Gh0st RAT Multi-Campaign Delivery Surge Targets Chinese Speakers

Date of Publication	Admiralty Code	TA Number
November 20, 2025	A1	TA2025352

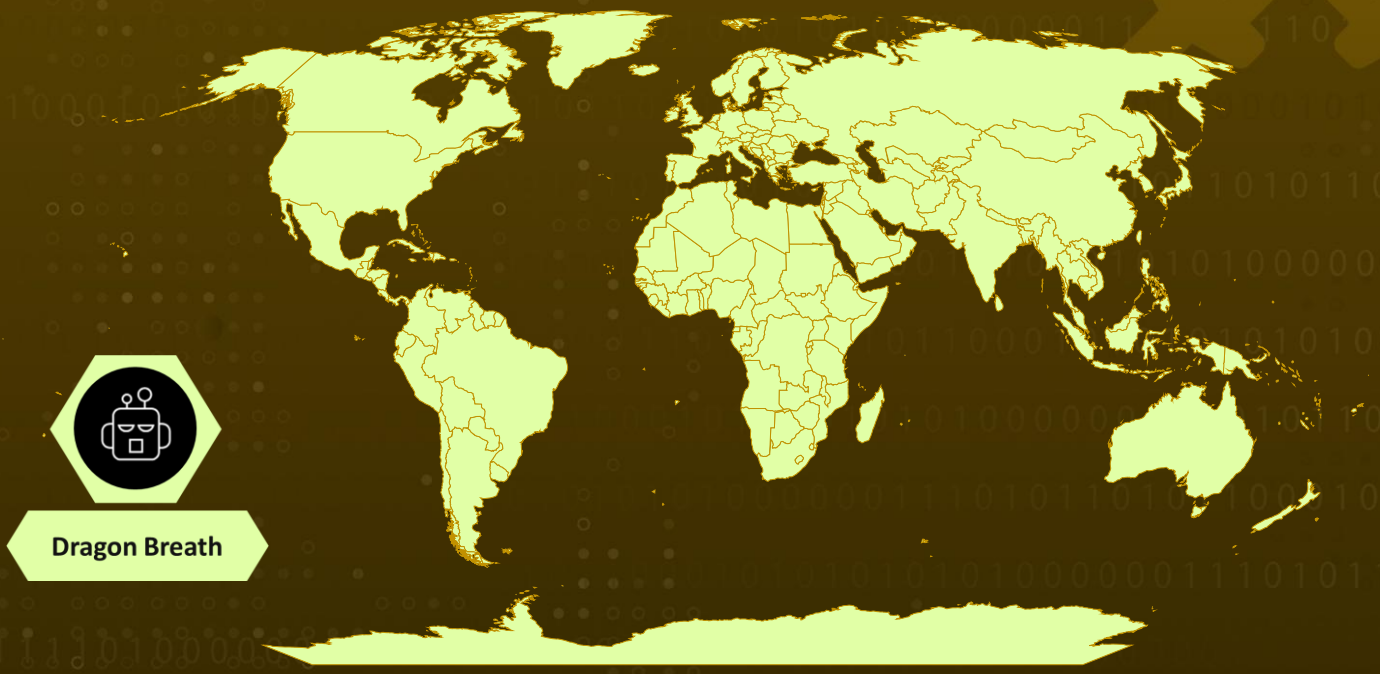
Summary

Attack Commenced: February 2025
Threat Actor: Dragon Breath (alias Golden Eye Dog, APT-Q-27)
Malware: RONINGLOADER, Gh0st RAT
Campaigns: Campaign Trio, Campaign Chorus
Targeted Regions: Worldwide (Major Chinese-Speaking Territories)
Targeted Industries: Technology, Entertainment, High-Tech
Targeted Brands: i4tools, Youdao, DeepSeek, QQ Music, Sogou browser, Google Chrome, Microsoft Teams
Attack: Dragon Breath (APT-Q-27) is driving a fast-moving, high-volume operation that blends multi-stage loaders, brand impersonation, and disposable domain infrastructure to push modified Gh0st RAT variants to Chinese-speaking users. The group relies on trojanized NSIS installers disguised as trusted software, layers extensive evasion to bypass local security tools, and sustains its reach through thousands of look-alike domains mimicking major Chinese apps.

Attack Timeline



Attack Regions



Attack Details

#1 Dragon Breath, also designated APT-Q-27, operated a campaign that employed the multi-stage loader RONINGLOADER to deploy a modified variant of Gh0st RAT. The activity targeted Chinese-speaking users. The intrusion began with a trojanized installer created with the Nullsoft Scriptable Install System (NSIS), a legitimate Windows installer framework frequently misused for malware distribution.

#2 In this case, the malicious packages were presented as trusted applications such as Google Chrome, Microsoft Teams, and other widely recognized software. The operators introduced a legitimately signed driver, enforced custom Windows Defender Application Control (WDAC) policies, and abused Protected Process Light (PPL) to interfere with Microsoft Defender.

#3 These measures produced multiple redundant guardrails intended to weaken defensive controls. When executed, the primary NSIS installer acted as a dropper containing two additional embedded NSIS installers. One installed legitimate software to preserve the appearance of authenticity, while the second executed the malicious workflow. This sequence ultimately deployed the modified Gh0st RAT.

#4 The variant contacted a remote server for tasking that enabled registry modification, event-log deletion, retrieval and execution of files from supplied URLs, clipboard manipulation, command execution through "cmd.exe," shellcode injection into "svchost.exe," and activation of payloads written to disk. It also included modules for keystroke logging, clipboard capture, and tracking of active window titles.

#5 Throughout 2025, two interlinked malware campaigns built around large-scale brand impersonation to deliver Gh0st RAT variants to Chinese-speaking users. These efforts shared infrastructure, tactics, and targeting, forming a continuous operational arc rather than isolated events.

#6 The first phase, known as Campaign Trio, ran from February to March 2025. It impersonated three major brands across more than 2,000 domains, using consistent lures and the same multi-stage delivery model. The second phase, Campaign Chorus, began in May 2025 and significantly broadened the impersonation scope to more than 40 applications.

#7 i4tools was the most frequently mimicked brand, with over 1,400 domains created to replicate this widely used Chinese-language utility for managing Apple mobile devices. More than 600 domains were dedicated to impersonating Youdao, a prominent Chinese dictionary and translation service. Five domains impersonated DeepSeek, reflecting an effort to exploit interest in contemporary AI-focused products.

#8 The scale, speed, and turnover of domain creation show a burn-and-churn strategy in which domains were treated as disposable. Operational resilience was maintained through constant replenishment and wide distribution of malicious infrastructure.

Recommendations

Forensic Log and Registry Analysis: Inspect Windows Event Logs for anomalous service creation, driver loading, and process termination, particularly entries referencing "xererre1," "ollama," or "MicrosoftSoftware2ShadowCop4yProvider." Examine registry paths such as HKEY_CURRENT_USER\offlinekey for clipboard hijacker configurations and HKEY_LOCAL_MACHINE for unauthorized WDAC policy modifications.

Increase Behavioral Endpoint Monitoring: Adopt continuous monitoring with behavioral analytics tuned to detect injection, driver tampering, and security-control termination patterns. Maintain structured kernel patching routines to close vulnerabilities exploited by multi-stage loaders.

Reinforce Recovery and Containment Architecture: Strengthen backup and disaster recovery processes to enable clean system restoration. Segment internal networks to constrain lateral movement pathways during compromise scenarios. Maintain incident response playbooks tailored to multi-stage loader infections with security-evasion capabilities.

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
TA0040 Impact	**TA0011** Command and Control	**TA0042** Resource Development	**T1059** Command and Scripting Interpreter
T1059.003 Windows Command Shell	**T1569** System Services	**T1569.002** Service Execution	**T1566** Phishing

T1543 Create or Modify System Process	**T1543.003** Windows Service	**T1548** Abuse Elevation Control Mechanism	**T1548.002** Bypass User Account Control
T1134 Access Token Manipulation	**T1562.001** Disable or Modify Tools	**T1562** Impair Defenses	**T1562.004** Disable or Modify System Firewall
T1070 Indicator Removal	**T1070.001** Clear Windows Event Logs	**T1574** Hijack Execution Flow	**T1574.001** DLL
T1055 Process Injection	**T1036.005** Match Legitimate Resource Name or Location	**T1036** Masquerading	**T1112** Modify Registry
T1553 Subvert Trust Controls	**T1553.006** Code Signing Policy Modification	**T1056** Input Capture	**T1056.001** Keylogging
T1115 Clipboard Data	**T1057** Process Discovery	**T1082** System Information Discovery	**T1033** System Owner/User Discovery
T1518 Software Discovery	**T1518.001** Security Software Discovery	**T1095** Non-Application Layer Protocol	**T1573** Encrypted Channel
T1573.001 Symmetric Cryptography	**T1583** Acquire Infrastructure	**T1204** User Execution	**T1204.002** Malicious File
T1059.005 Visual Basic	**T1059.001** PowerShell	**T1218** System Binary Proxy Execution	**T1218.007** Msiexec
T1071 Application Layer Protocol	**T1071.001** Web Protocols		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	95[.]173[.]197[.]195, 156[.]251[.]25[.]43, 156[.]251[.]25[.]112, 154[.]82[.]84[.]227, 103[.]181[.]134[.]138
Domains	yqmqhjgn[.]com, youdaxxyzy[.]top, youdaxxyzr[.]top, youdaxxddxk[.]top, youdaqqaavw[.]top, youdaovavxl[.]top, youdaovavxk[.]top, youdaoooosssj[.]top, youdaohhzi[.]top, ydbaoo52[.]cyou, ydbao11[.]cyou, xiazaizhadia9[.]cyou, xiazaizhadia8[.]cyou, xiazaizhadia51[.]cyou, xiazaizhadia50[.]cyou, xiazaizhadia46[.]cyou, xiazaizhadia44[.]cyou, xiazaizhadia42[.]cyou, xiazaizhadia41[.]cyou, xiazaizhadia40[.]cyou, xiazaizhadia39[.]cyou, xiazaizhadia37[.]cyou, xiazaizhadia36[.]cyou, xiazaizhadia35[.]cyou, xiazaizhadia34[.]cyou, xiazaizhadia33[.]cyou, xiazaizhadia31[.]cyou, xiazaizhadia30[.]cyou, xiazaizhadia29[.]cyou, xiazaizhadia27[.]cyou, xiazaizhadia24[.]cyou, xiazaizhadia22[.]cyou, xiazaizhadia21[.]cyou, xiazaizhadia20[.]cyou, xiazaizhadia2[.]cyou, xiazaizhadia19[.]cyou, xiazaizhadia18[.]cyou,

TYPE	VALUE
Domains	xiazaizhadia16[.]cyou, xiazaizhadia12[.]cyou, xiazaizhadia11[.]cyou, xiazaizhadia10[.]cyou, xiazaizhadia1[.]cyou, xiazailianjieoss[.]com, xiaofeige[.]icu, xiaobaituziha[.]com, qishuiyinyque-vip[.]top, i4toolsuuozp[.]top, i4toolsuuoxk[.]top, i4toolsllsk[.]top, i4toolsearch[.]vip, i4toolscaczu[.]top, i4toolscacvi[.]top, i4toolscacsm[.]top, i4[.]llllxiazai-web[.]vip, guwaanzh8[.]cyou, guwaanzh35[.]cyou, guwaanzh34[.]cyou, guwaanzh25[.]cyou, guwaanzh24[.]cyou, guwaanzh21[.]cyou, guwaanzh20[.]cyou, guwaanzh2[.]cyou, guwaanzh1[.]cyou, fs-im-kefu[.]7moor-fs1[.]com, djbzdhygj[.]com, deep-seek[.]rest, anydesk-www[.]cyou, 1235saddfs[.]icu
SHA256	e8c058acfa2518ddc7828304cf314b6dd49717e9a291ca32ba185c44937c422b, dbe70991750c6dd665b281c27f7be40afea8b5718b097e43cd041d698706ade4, c37d0c9c9da830e6173b71a3bcc5203fbb66241ccd7d704b3a1d809cadd551b2, bd4635d582413f84ac83adbb4b449b18bac4fc87ca000d0c7be84ad0f9caf68e, bc6fb2eab9ed8d9eb405f6186d08e85be8b1308d207970cc41cf90477aa79064, 7267a303abb5fcae2e6f5c3ecf3b50d204f760dabdfc5600bd248fcfad3fc133, 495ea08268fd9cf52643a986b7b035415660eb411d8484e2c3b54e2c4e466a58,

TYPE	VALUE
SHA256	491872a50b8db56d6a5ef1ccabe8702fb7763da4fd3b474d20ae0c98969acfe5, 299e6791e4eb85617c4fab7f27ac53fb70cd038671f011007831b558c318b369, 2232612b09b636698afcdb995b822adf21c34fb8979dd63f8d01f0d038acb454, 1c3f2530b2764754045039066d2c277dff4efabd4f15f2944e30b10e82f443c0, 18a21dbc327484b8accbd4a6d7b18608390a69033647099f807fdbfdcfff7e6d, 1395627eca4ca8229c3e7da0a48a36d130ce6b016bb6da750b3d992888b20ab8

References

https://www.elastic.co/security-labs/roningloader

https://unit42.paloaltonetworks.com/impersonation-campaigns-deliver-gh0st-rat/

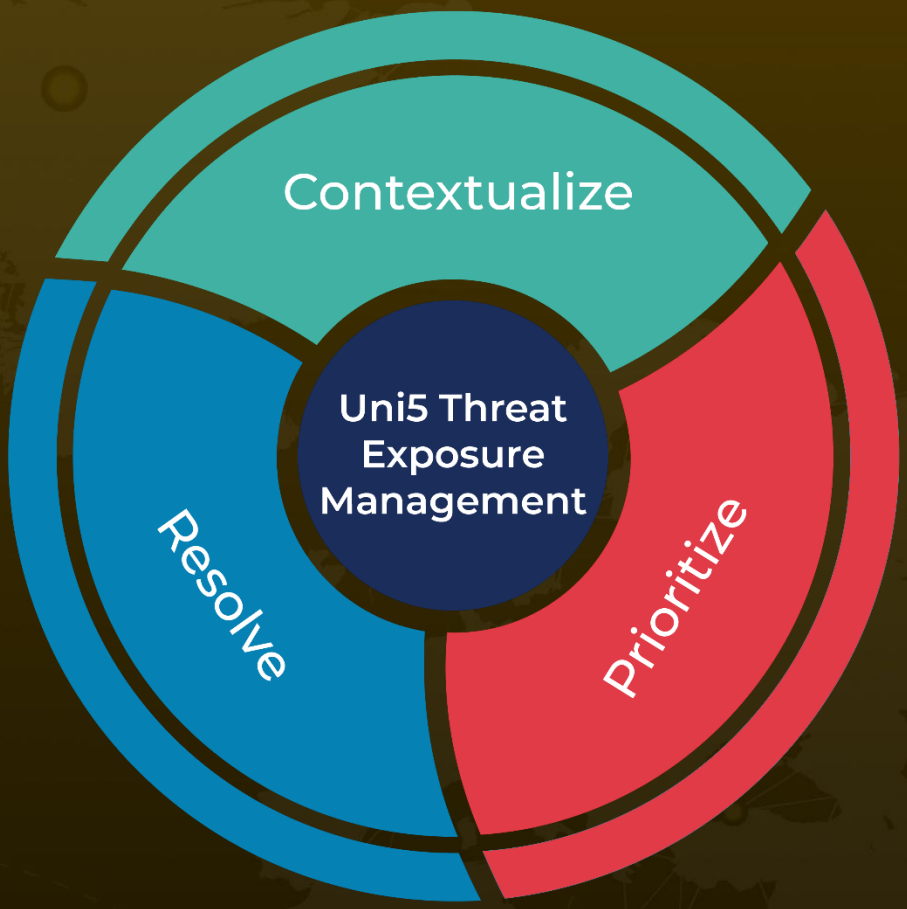
https://hivepro.com/threat-advisory/dragon-breath-apt-evolves-with-double-dll-sideloading/

https://hivepro.com/threat-advisory/hidden-in-plain-sight-the-abuse-of-nezha-and-the-ghost-rat-that-followed/

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

November 20, 2025 . 3:30 AM

More at www.hivepro.com