

Digital Doppelgangers: Anatomy of Evolving Impersonation Campaigns Distributing Gh0st RAT

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

Keerthiraj Nagaraj, Vishwa Thothathri, Nabeel Mohamed, Reethika Ramesh

November 14, 2025

Executive Summary

We have identified two interconnected malware campaigns active throughout 2025, using large-scale brand impersonation to deliver Gh0st remote access Trojan (RAT) variants to Chinese-speaking users. From the first campaign to the second, the adversary advanced from simple droppers to complex, multi-stage infection chains that misuse legitimate, signed software to bypass modern defenses.

This report provides a detailed breakdown of the campaigns' anatomy, offering new intelligence on the attackers' operational playbook. We analyze an initial campaign from February–March 2025 that mimicked three brands across over 2,000 domains and a more sophisticated campaign starting in May 2025 that impersonated over 40 applications. The impersonated software primarily includes widely used enterprise tools, secure messaging apps, gaming platforms and popular AI software.

By analyzing the evolution of the attack methods, infrastructure and targeting, we establish a clear operational playbook. Understanding the adversary's adaptive tactics, techniques and procedures (TTPs), such as using cloud infrastructure for payload delivery and DLL side-loading for evasion, provides crucial insights for enhancing security postures.

Our analysis is based on data from Palo Alto Networks products, including Advanced URL Filtering and Advanced WildFire, which provided visibility into the malware's behavior and infection chains. This internal data was supplemented by passive DNS (pDNS) analysis and open-source intelligence. We provide organizations with indicators of compromise (IoCs) to mitigate against this threat.

Palo Alto Networks customers are better protected from this activity through the following products and services:

- [Advanced WildFire](#)
- [Advanced URL Filtering](#) and [Advanced DNS Security](#)
- [Advanced Threat Prevention](#)
- [Cortex XDR](#) and [XSIAM](#)
- Cortex Cloud [DSPM](#)

If you think you might have been compromised or have an urgent matter, contact the [Unit 42 Incident Response team](#).

The Rise of Impersonation at Scale: A Persistent Threat to Chinese-Speaking Users

In recent years, malware campaigns specifically tailored to target Chinese-speaking users globally have emerged as a notable trend in the threat landscape. These operations demonstrate a complex understanding of the target demographic's digital ecosystem and online behaviors.

The lures used are often not generic. Instead, attackers carefully select them to appeal to this specific audience. Attackers frequently impersonate the following types of applications:

- Software that is widely popular within the community (e.g., Youdao dictionary or Sogou browser)
- Tools used to circumvent state-imposed internet restrictions (e.g., VPNs and encrypted messaging applications)

How would potential victims find these malicious sites impersonating legitimate software? Attackers have a variety of options. They could generate traffic to these sites through malicious online ads or search engine poisoning. Attackers can also post on social media and other online forums to promote these sites. Email is another vector for leading potential victims to these sites.

The choice to target people seeking tools to bypass censorship is particularly strategic. This suggests an adversary who is interested in people already attempting to operate outside of easily monitored channels, making them prime targets for surveillance or espionage.

The final payload in these campaigns is often a RAT that grants the attacker comprehensive control over a compromised system. The Gh0st RAT and its many variants are a prominent choice, particularly for Chinese-nexus cybercrime and espionage actors who have used these tools for over a decade.

Anatomy of the First Campaign: Campaign Trio

We refer to this initial activity as Campaign Trio due to its impersonation of three distinct software brands. Active from February–March 2025, this phase established a baseline operational model of the adversary. This campaign involved a massive number of domains, used an aggressive approach to infrastructure deployment and a clear, focused targeting strategy.

The malware distribution strategy of this campaign relied on a vast network of malicious websites that convincingly mimicked legitimate software download portals to lure victims.

Mass Domain Registration

Between February and March 2025, attackers registered over 2,000 domains, with significant surges in activity in early February and early March. Attackers appear to have automated their domain registration, typically combining the impersonated brand name with a random-looking alphanumeric suffix and using TLDs like .top or .vip.

The entire network of over 2,000 domains was hosted on just three IP addresses:

- 154.82.84[.]227
- 156.251.25[.]43
- 156.251.25[.]112

This high-volume domain approach is designed to persist in the face of reputation-based blocking systems. It also ensures that even if some domains are taken down, many other domains remain available.

Figure 1 shows a sample attack infrastructure of Campaign Trio including the following info:

- Three clusters of brand impersonating domains
- Their association with web server IP addresses
- An additional server hosting the malware for downloading

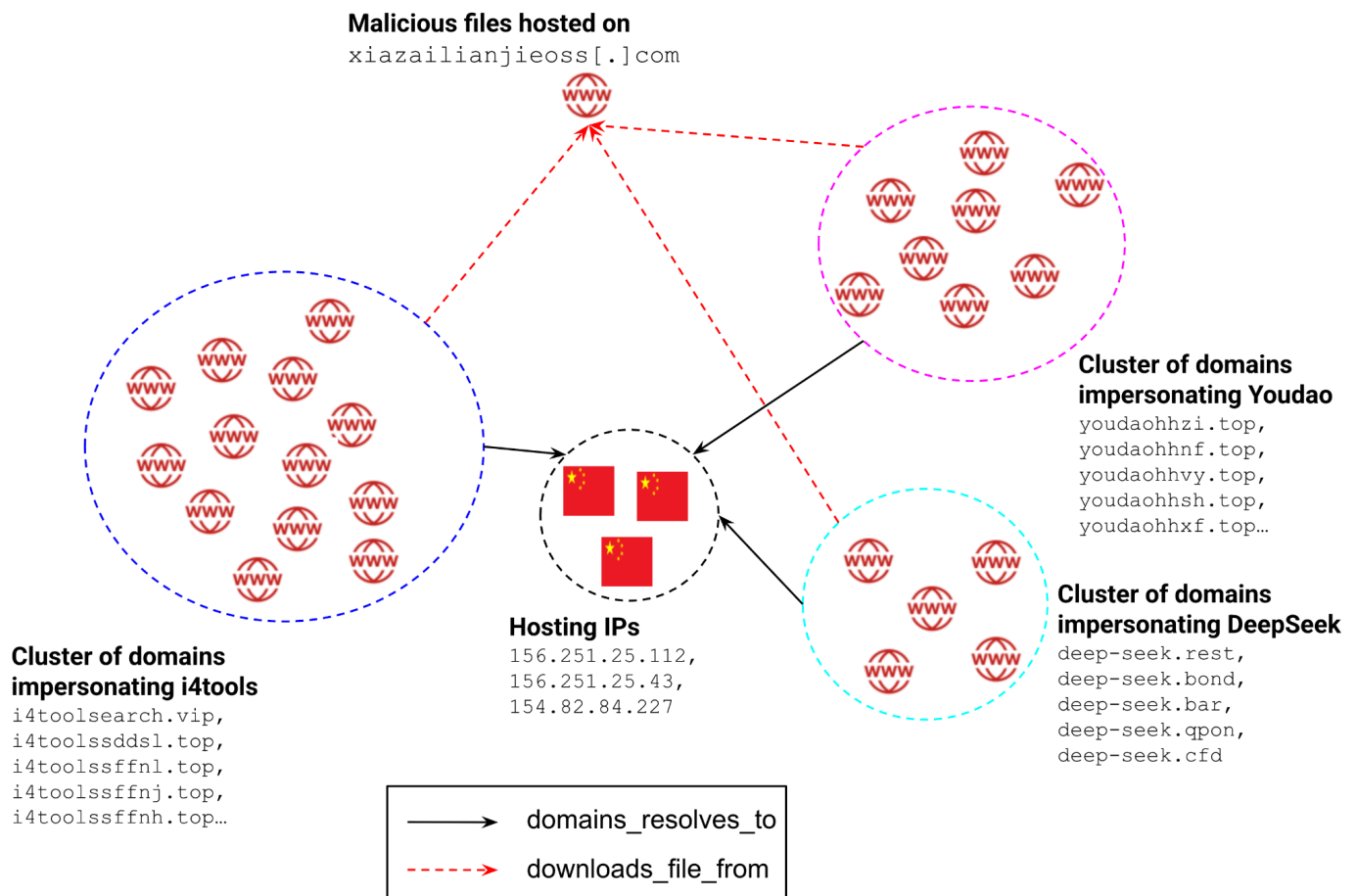


Figure 1. The Campaign Trio's attack infrastructure.

This centralized model, with over 2,000 domains resolving to just three IP addresses, suggests that attackers viewed components of the infrastructure as disposable. This also implies an aggressive approach to infrastructure deployment that allows the attackers to rapidly establish new websites.

Targeted Impersonation

The choice of impersonated brands for this campaign reveals a deliberate targeting strategy:

- **i4tools:** With over 1,400 domains, this was the most impersonated brand. This is Chinese-language, multi-function software for managing and transferring files to and from Apple-based mobile devices.
- **Youdao:** Attackers created over 600 domains to impersonate this popular Chinese dictionary and translation application, strongly indicating a focus on Chinese-speaking users.
- **DeepSeek:** We identified only five domains. The impersonation of this AI company demonstrates the attackers' interest in capitalizing on current technology trends.

The landing pages hosted on these domains closely mimicked the legitimate sites to deceive victims into downloading the trojanized software installers shown in Figures 2, 3 and 4.



```
view-source:https://deep-seek.rest

1 <!DOCTYPE html>
2 <html lang="zh" class="__className_d65c78">
3
4 <head>
5   <meta charset="utf-8">
6   <script charset="UTF-8" id="LA_COLLECT" src="//sdk.51.la/js-sdk-pro.min.js?id=KkdZjq8QfK9A7Jgd&ck=KkdZjq8QfK9A7Jgd"></script>
7   <script src='static/js/jquery.min.js'></script>
8   <script>
9     let Ahref = "https://xiazailianjieoss.com/baidu/deepseek_release_X64.zip" ;//大嘴下载文件路径
10    $(document).ready(function(){
11      $('a').each(function(){
12        $(this).attr("href",Ahref);
13      });
14    });
15  </script>
```

Figure 2. Example of a malicious landing page impersonating DeepSeek and the malicious payload URL in the page content.



Figure 3. Example of a malicious landing page impersonating Youdao and the malicious payload URL in the page content.



Figure 4. Example of a malicious landing page impersonating i4tools and the malicious payload URL in the page content.

Execution and Payload Delivery: A Centralized Model

Webpages from over 2,000 domains served their malicious payloads from a single source: `hxxps[:]//xiazaillianjieoss[.]com`.

This domain hosted ZIP archives containing the trojanized installers. The downloaded archives contained either a malicious Microsoft Installer (MSI) file or a standalone executable. The MSI installers used a custom action to execute a secondary, smaller executable, separating the malicious logic from the main installer to bypass static analysis.

Final Payload: The Gh0st RAT

MSI-based malware delivery can include a substantial variety of actions also typically executed by benign MSI files. This allows malicious actions to hide within the many legitimate operations generated by an attacker's MSI file.

Figure 5 illustrates this concept in action. It shows a malicious MSI sample from Campaign Trio running the embedded malware within the MSI package. Using Microsoft's [Orca](#) tool, we can search the malicious MSI file's custom actions for anything suspicious. Running the malicious executable is one of 43 custom actions, not including all the normal actions and processes generated by an MSI file.

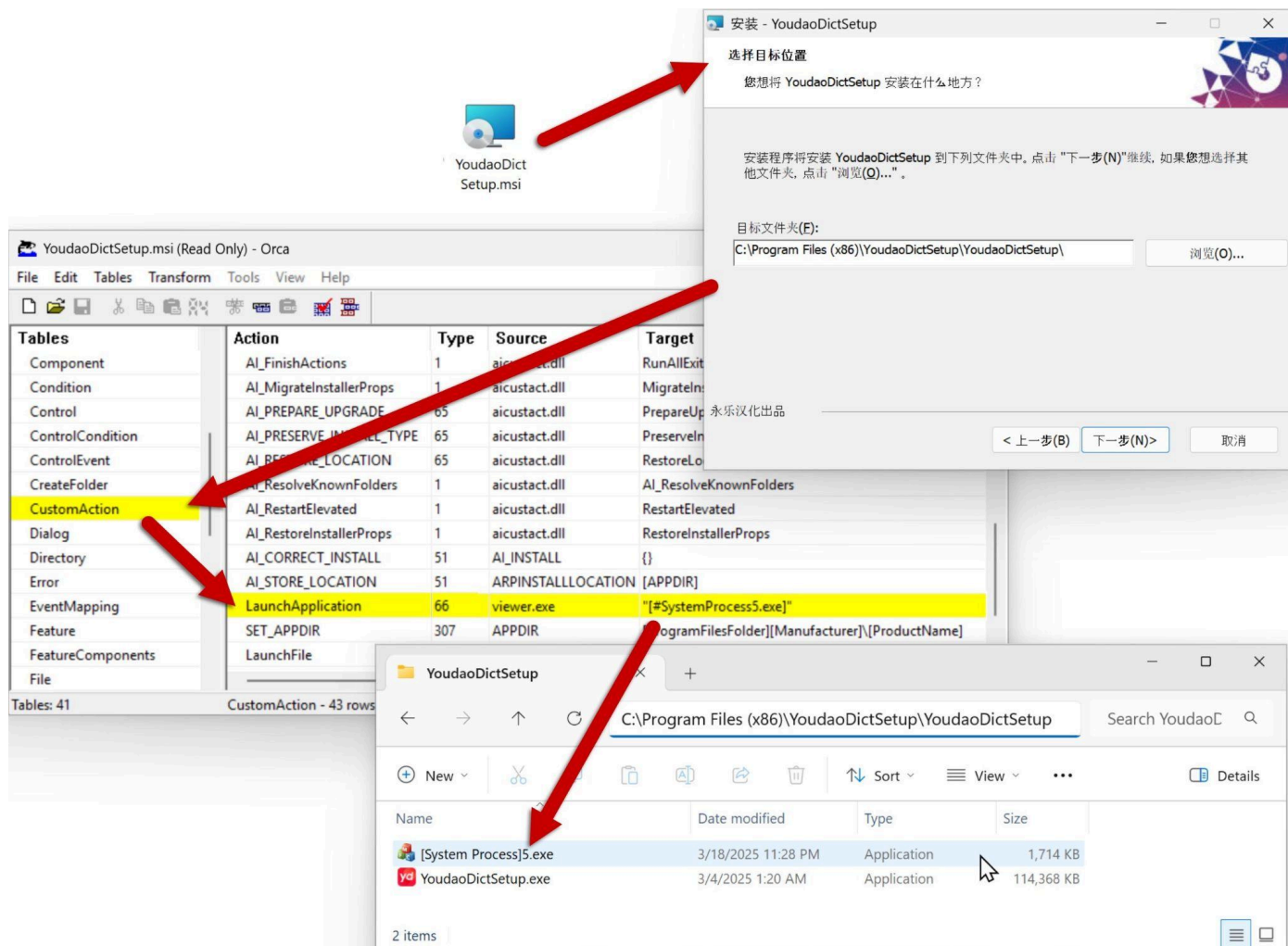


Figure 5. Examining a malicious MSI file from Campaign Trio.

The MSI file in Figure 5 employs a seemingly legitimate graphical user interface (GUI) for its installation procedure. The Orca tool reveals the MSI file's custom action table, where we've highlighted the malicious action run in the background during the installation. In this instance, the custom action LaunchApplication executes the second-stage malware, a 1.7 MB executable named [System Process]5.exe.

Primary functions of [System Process]5.exe are to:

- Download an obfuscated binary from a staging server
- Decode the binary and
- Run it

The obfuscated binary was hosted on URLs from fs-im-kefu.7moor-fs1[.]com, a malware distribution point [linked to previous Gh0st RAT activity](#).

The deobfuscated binary is the final payload. We identified this final payload as Gh0st RAT, which provides attackers with the following capabilities:

- Logging keystrokes
- Capturing screenshots
- Remote shell access
- Downloading additional malware

These Gh0st RAT samples create scheduled tasks for persistence and use powershell.exe to add exclusions in Windows Defender, so they can run undetected. Once active, these Gh0st RAT samples establish command and control (C2) communication via encrypted TCP traffic over port 8080 to servers with domains like xiaobaituziha[.]com, which resolved to 103.181.134[.]138.

Anatomy of the Second Campaign: Campaign Chorus

We refer to the second campaign as Campaign Chorus because attackers expanded their lures to impersonate over 40 different software applications. Launched in May 2025, this campaign built upon the foundation of the first and showed a significant expansion in targeting. Its TTPs evolved to enhance evasion and bypass security controls.

Expanded Targeting, Refined TTPs

While maintaining a focus on Chinese-speaking users, attackers broadened their lure selection to maximize their potential targets. The attackers organized Campaign Chorus in a more structured manner.

Broader Scope and Wave-Based Attacks

In Campaign Chorus, attackers impersonated widely used enterprise messaging software, Chinese versions of secure messaging apps and popular gaming platforms. They also continued targeting software popular with Chinese speakers, such as QQ Music and Sogou browser. This indicates a strategy to reach a wider demographic of Chinese speakers.

Figure 6 shows examples of impersonated applications from this campaign.

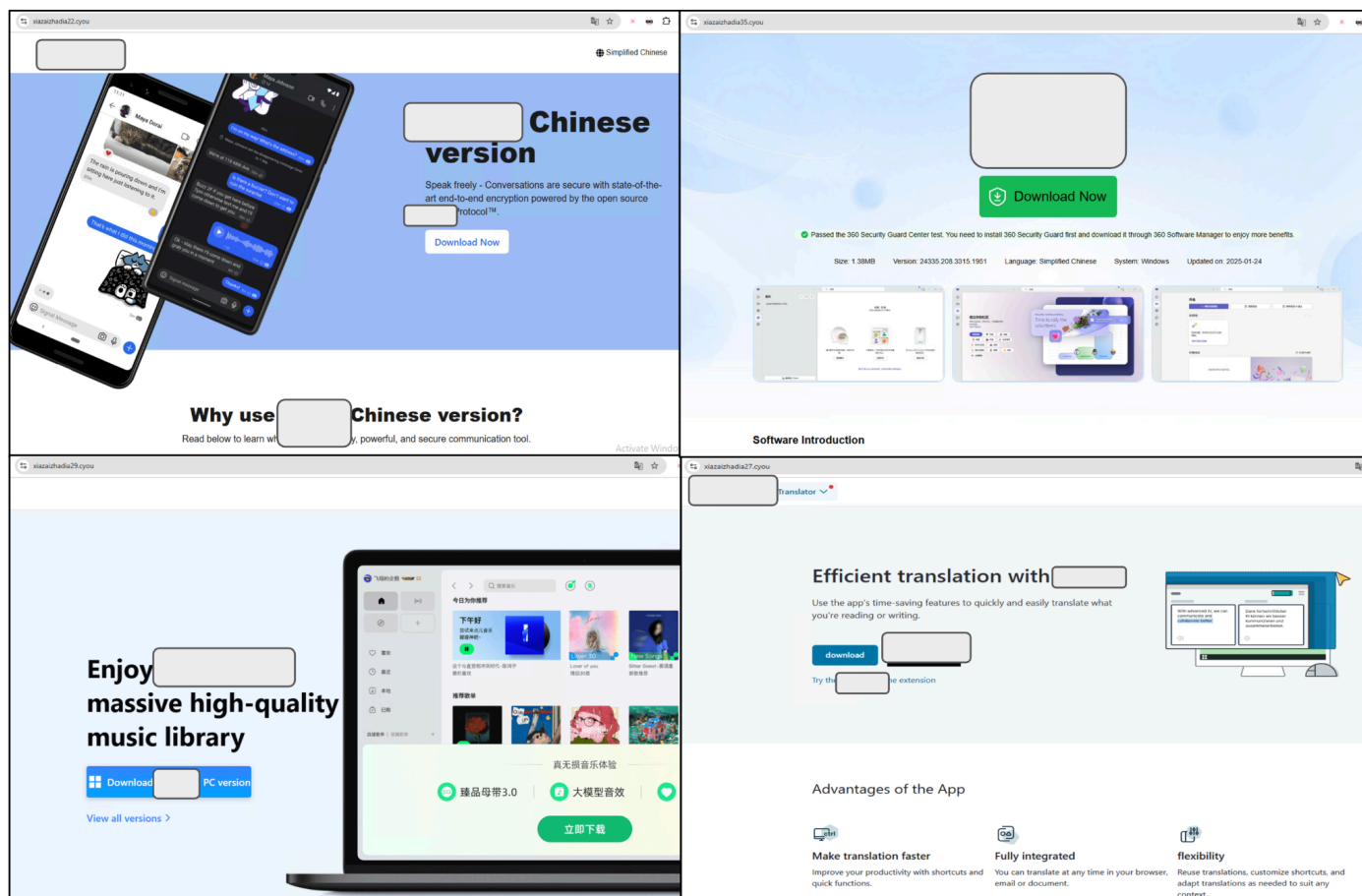


Figure 6. Software impersonation examples from The Chorus phase.

This campaign was initially executed in two distinct waves, distinguished by domain naming conventions and registration dates:

- Wave 1 (registered May 15, 2025): This wave consisted of 40 domains, all beginning with the prefix guwaanzh
- Wave 2 (registered May 26–28, 2025): This wave included 51 domains, all starting with the prefix xiazaizhadia

The use of structured, wave-based attacks with different domain prefixes and corresponding redirection servers (djbzdhygj[.]com for Wave 1 and yqmghjgn[.]com for Wave 2) suggests a more organized and possibly experimental approach. The attackers could have been testing the effectiveness of different lures or attempting to compartmentalize their infrastructure to make it more resilient to takedowns.

Figure 7 shows an infrastructure map diagram illustrating the two distinct attack waves, their respective redirection servers and how the domains were hosted on a single IP address.

Campaign Infrastructure Map

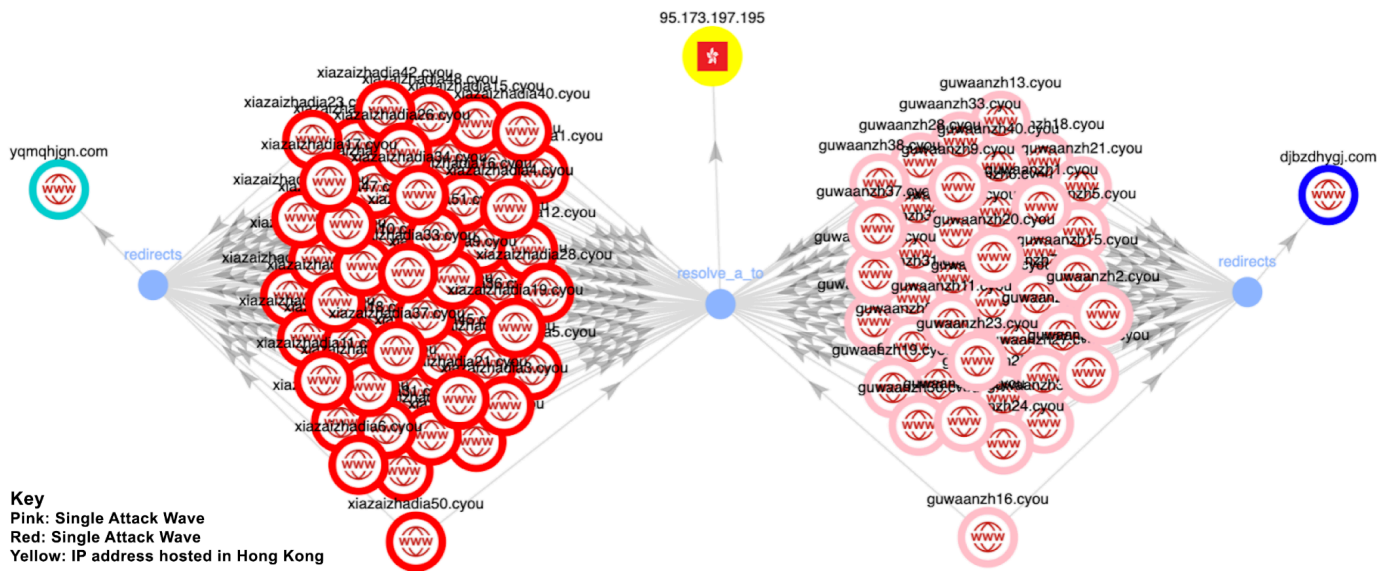


Figure 7. Attack infrastructure map for Campaign Chorus.

A More Evasive Infection Chain

Figure 8 shows the most significant advancement during this campaign: adopting a more intricate and elusive infection chain. This multi-stage evolution from the previous campaign increases the complexity of malware embedded in the MSI file. This indicates an increased effort to evade detection.

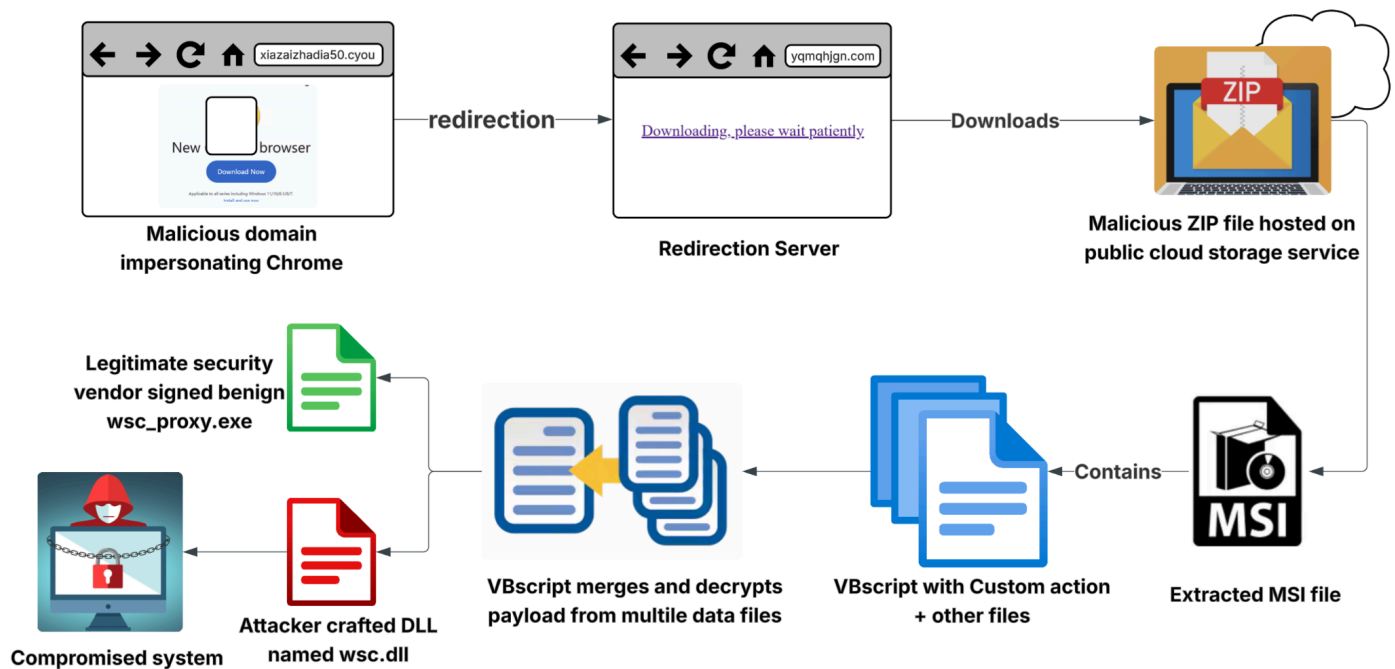


Figure 8. The multi-stage infection chain of Campaign Chorus.

The previous campaign's infection chain was more easily detectable by endpoint detection and response (EDR) solutions. This new chain is explicitly designed to circumvent these protections.

Redirection via Cloud-Hosted Payloads

In a tactical shift from previous activity, the actor behind Campaign Chorus moved away from a single, self-hosted payload server. Instead, the malicious landing pages used intermediary redirection domains to fetch the malicious ZIP archives from public cloud service buckets.

For this tactic, attackers misused cloud services, leveraging trusted reputations to make malicious download traffic appear benign. Consequently, the malicious downloads might bypass network filters that would otherwise block traffic from an unknown or newly registered domain. This also increases the actor's operational resilience, as disrupting a cloud service bucket is a more involved process for defenders than simply blocklisting a malicious IP address.

The VBScript Dropper

As noted earlier in Figure 8, the core of this new infection chain is an embedded VBScript file run as a custom action by the MSI installer. The VBScript file acts as a file assembler and decryptor for the next-stage malware.

This next-stage payload is stored within the MSI file, but not as a single encoded binary. Instead, it is split across multiple data files contained within the MSI's embedded .cab archive.

The VBScript file reads these separate components, merges them into a single binary and uses a stored password to decrypt the combined data. This process creates the next-stage malware. This technique is designed to evade static analysis tools that might otherwise detect a single binary containing malicious content within the MSI.

Execution via DLL Side-Loading

The final and most complex step in the infection chain is using DLL side-loading to execute the payload. The VBScript file decodes data binaries within the MSI and saves the resulting two files to disk:

- The first file is a copy of a legitimate signed executable (wsc_proxy.exe)
- The second file is a malicious, attacker-crafted DLL named wsc.dll

When wsc_proxy.exe is executed, the Windows loader searches for its required dependency, wsc.dll. Because the malicious version is in the same directory, it is loaded into the process memory before the legitimate version in the system directory would be found.

This is a classic example of DLL side-loading. It is an [evasion technique](#) that allows the attacker's code to run under the guise of a trusted, signed process. The misuse of a legitimate executable is meant to bypass application allow-listing and process-based monitoring. The parent process

initiating the malicious activity is itself benign and digitally signed by a reputable vendor. This makes it significantly harder for security tools to flag the activity as malicious.

Campaign Profile: A Unified Operational Playbook

When analyzed together, the evidence from Campaign Trio and Campaign Chorus reveals a consistent operational playbook, allowing us to build a distinct behavioral profile. The technical differences are best understood not as the work of two unrelated campaigns, but as the logical evolution of a single group adapting its methods.

The campaigns have several key characteristics that form a strategic signature:

- **Mass-scale programmatic infrastructure:** Both campaigns rely on the programmatic generation of domains for brand impersonation using a consistent naming convention.
- **Specific demographic focus:** Both campaigns focus heavily on software popular with Chinese-speaking users, even when deploying infrastructure in regions like the U.S. and Singapore. This indicates an actor with a deep and specific understanding of this demographic, rather than an opportunistic actor casting a wide, generic net.
- **“Burn-and-churn” operational tempo:** Both campaigns use a centralized and disposable infrastructure model. The strategy of hosting thousands of domains on a handful of IP addresses demonstrates a rapid deployment approach where the attackers consider the infrastructure expendable. The actor prioritizes the speed and scale of deployment over stealth and long-term resilience. They are confident in their ability to quickly pivot to new domains and servers.
- **Two-tiered infrastructure:** The actor exhibits a clear separation between its disposable, high-volume access infrastructure (the thousands of impersonation domains) and its more critical operational infrastructure (the payload and C2 servers). While the access layer is designed to be burned, the operational layer shows evolution (from self-hosted to cloud-hosted) aimed at increasing longevity and resilience. This architectural choice allows the actor to absorb the loss of their frontend domains without losing its core payload delivery and C2 capabilities.

TTP Profile

Table 1 shows the adversary's methods mapped to the MITRE ATT&CK framework, providing a standardized view of its operational tactics.

Tactic	Technique ID	Technique Name	Use in These Campaigns
Resource Development	T1583	Acquire Infrastructure	The actor acquired over 2,000 domains and multiple IP addresses to host malicious websites and C2 servers

Initial Access	T1566	Phishing	Malicious websites impersonating legitimate software were used to lure users into downloading trojanized installers
Execution	T1204.002	User Execution: Malicious File	The infection chain relies on the user executing a downloaded MSI or EXE file
Execution	T1059.001	Command and Scripting Interpreter: PowerShell	PowerShell was used post-infection to add Windows Defender exclusions for the malware payload
Execution	T1059.005	Command and Scripting Interpreter: Visual Basic	VBScript was embedded as a custom action in MSI installers to act as a multi-stage dropper
Execution	T1218.007	System Binary Proxy Execution: Msixexec	Malicious MSI installers were used as the primary delivery vehicle for the initial droppers
Defense Evasion	T1574.001	Hijack Execution Flow: DLL Side-Loading	A legitimate, signed AVAST executable (wsc_proxy.exe) was used to load a malicious DLL (wsc.dll) to execute the final payload
Defense Evasion	T1562.001	Impair Defenses: Disable or Modify Tools	The malware adds exclusions to Windows Defender to prevent detection of its components
Command and Control (C2)	T1071.001	Application Layer Protocol: Web Protocols	C2 traffic was observed using standard TCP and HTTP protocols
Command and Control (C2)	T1573.001	Encrypted Channel: Symmetric Cryptography	C2 communication over TCP port 8080 was encrypted to evade network inspection

Table 1. TTP profile summary (MITRE ATT&CK mapping).

Observed Campaign Activity and Infrastructure Expansion

The results of our investigation reinforce that these campaigns are not isolated, short-term events. Attackers are actively maintaining and expanding their infrastructure, indicating a persistent, long-term operation.

We investigated the WHOIS creation dates of domains associated with both these campaigns and found that they have consistently registered domains from February–August 2025.

Our analysis showed a significant surge in activity between February and May 2025. During these four months, attackers created over 2,500 domains, accounting for 87.4% of all malicious domains identified in connection with these campaigns.

Figure 9 shows the distribution of domains belonging to these campaigns created per week according to their WHOIS creation dates. In February and March of 2025, we observed over 1,500 domains belonging to the first campaign being registered.

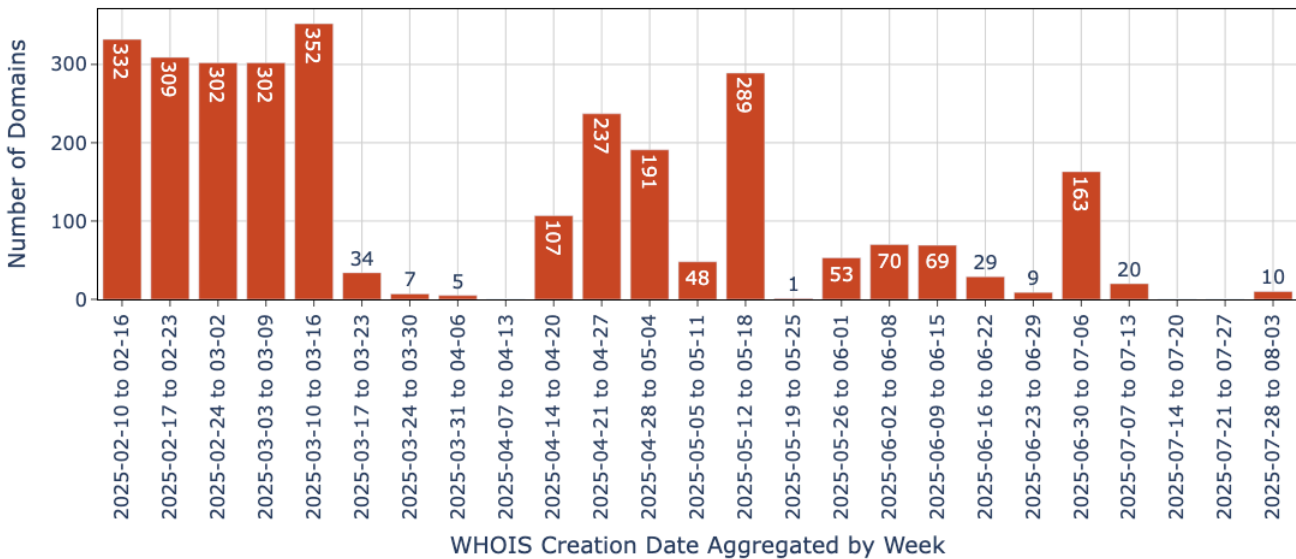


Figure 9. Number of domains from the two campaigns registered over time, highlighting periodic bursts.

We also noticed an interesting pattern where attackers registered between 100-200 domains every week for a month.

- This pattern started with 100 domains registered on April 15, 2025.
- This was followed by 237 more in the week of April 21–27, the majority of which were registered on April 22.
- This was followed by another 191 domains between April 28–May 4. Of these, 104 were registered on April 29.
- This was followed by a week of low activity (around May 5, 2025) and ended with almost 261 domains registered between May 13–15, 2025.

This regularity suggests an automated or highly structured process for routine infrastructure replenishment, likely to replace domains that have been blocked during operations.

From the pDNS data, we find that these new domains are pointed to the same core IP addresses used in both campaigns, with activity observed as recently as July 2025. Domains associated with the first campaign's infrastructure continue to resolve to 156.251.25[.]112. For example, we observed domains such as youdaxxyzr[.]top and i4toolscacsm[.]top actively resolving to this IP address. This demonstrates that the actor did not simply abandon its initial core IP address infrastructure but continued to leverage the IP address for ongoing attacks.

Similarly, the infrastructure for the second campaign remains active. The IP address 95.173.197[.]195 continues to serve new malicious domains as of early October 2025. Continuously registering and refreshing domains is a clear tactic to evade blocklists. It helps ensure the longevity of the campaigns, pointing to a well-resourced and determined adversary.

Figure 10 depicts a graph of the first campaign. It shows domains involved in both campaigns. Both campaigns use the same elements, like nameservers and hosting IP addresses. This graph depicts 683 domains that share the same set of nameservers and resolve to the same hosting IP address 156.251.25[.]112. This IP address is geolocated to Hong Kong.

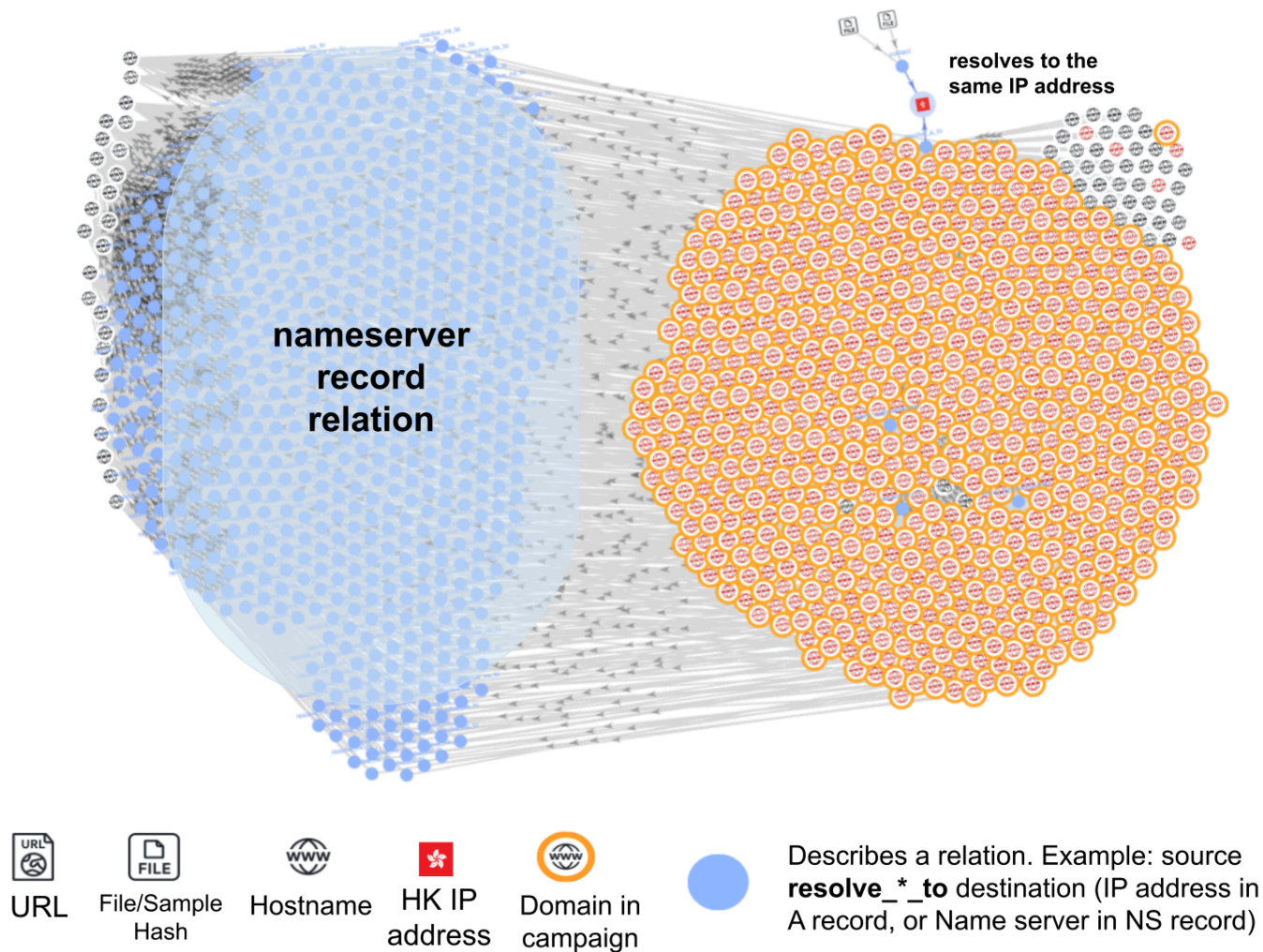


Figure 10. Large-scale activity graph showing infrastructure overlap between the two campaigns.

Furthermore, we analyzed pDNS query volumes for domains associated with the first campaign to quantify its sustained activity over time. We found that while daily query volumes fluctuated, there was a gradual upward trend in queries toward domains associated with this campaign between March 2025 and July 2025.

Figure 11 shows a large peak in the number of queries toward these domains on July 12, 2025. We investigated domains contributing to this peak, and over 68% of these queries were generated for domains registered between March 6 and March 13, 2025, representing an exact four-month

gap. This increase in query volume could be due to changes in the attackers' content or their connections to other entities.

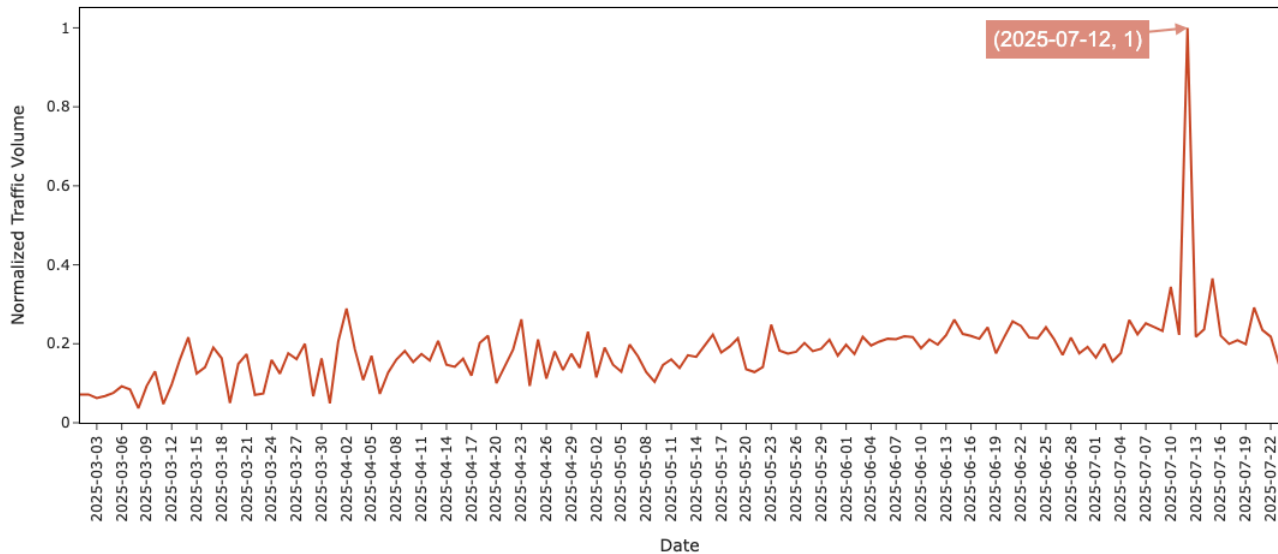


Figure 11. Normalized pDNS traffic volume of this activity from March through July 2025.

The parallel operation of both old and new infrastructure through sustained activity suggests an operation that is not merely evolving but consists of multiple infrastructures and distinct tool sets simultaneously. This could indicate A/B testing of TTPs, targeting different victim sets with different levels of complexity, or simply a cost-effective strategy of continuing to leverage older assets as long as they remain effective.

Conclusion

The campaigns detailed in this article represent a persistent, large-scale and evolving threat. Operating at scale combined with a continuous adaptation of TTPs presents a significant challenge for defenders.

There is a clear evolution in these two campaigns. Campaign Trio, the first campaign, uses direct droppers. Campaign Chorus, the second campaign, leverages a more complex multi-stage infection chain and uses DLL sideloading.

The following traits are notable:

- Consistent focus on a Chinese-speaking demographic
- Programmatically generating thousands of domains
- Strategically using both self-hosted and major cloud provider infrastructure

This signals a broader trend where threat actors will increasingly leverage legitimate cloud services and signed software, shifting the defensive focus from blocking known-bad indicators to detecting sophisticated behavioral anomalies.

Palo Alto Networks customers are better protected from the threats discussed above through the following products:

- The [Advanced WildFire](#) machine-learning models and analysis techniques have been reviewed and updated in light of the indicators shared in this research.
- [Advanced URL Filtering](#) and [Advanced DNS Security](#) identify known domains and URLs associated with this activity as malicious.
- [Advanced Threat Prevention](#) has an inbuilt machine learning-based detection that can detect exploits in real time.
- [Cortex XDR](#) and [XSIAM](#) are designed to prevent the execution of known malicious malware, and also prevent the execution of unknown malware using Behavioral Threat Protection and machine learning based on the Local Analysis module.
- Cortex Cloud [DSPM](#) can help organizations detect if their cloud infrastructure has been used to host malicious binaries like those described in this article by routinely scanning cloud storage containers and properly classifying the data within.
 - This functionality can assist organizations from unwittingly being used to host malicious binaries placed by threat actors.
 - While the nature of the article does not point to the compromise of victim cloud environments to host these binaries, Cortex Cloud DSPM can detect malicious data and prevent it from harming the organization itself or, in this case, external organizations.

If you think you may have been compromised or have an urgent matter, get in touch with the [Unit 42 Incident Response team](#) or call:

- North America: Toll Free: +1 (866) 486-4842 (866.4.UNIT42)
- UK: +44.20.3743.3660
- Europe and Middle East: +31.20.299.3130
- Asia: +65.6983.8730
- Japan: +81.50.1790.0200
- Australia: +61.2.4062.7950
- India: 00080005045107

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the [Cyber Threat Alliance](#).

Indicators of Compromise (IoCs)

A comprehensive list of IoCs associated with these campaigns can be found in the tables below.

Campaign Trio IoCs

Indicator Type	Indicator Value
Hosting IP address	156.251.25[.]112
Hosting IP address	156.251.25[.]43
Hosting IP address	154.82.84[.]227
Payload Domain	xiazailianjieoss[.]com
C2 Domain	fs-im-kefu.7moor-fs1[.]com
C2 Domain	xiaobaituziha[.]com
C2 IP address	103.181.134[.]138
SHA256 hash and name or description of the file	c37d0c9c9da830e6173b71a3bcc5203fbb66241ccd7d704b3a1d809cadd551b2 (deepseek_release_X64.exe)
SHA256 hash and name or description of the file	495ea08268fd9cf52643a986b7b035415660eb411d8484e2c3b54e2c4e466a58 (i4Tools8_v8.33_Setup_x64.msi)
SHA256 hash and name or description of the file	7267a303abb5fcae2e6f5c3ecf3b50d204f760dabdfc5600bd248fcfad3fc133 (YoudaoDictSetup.msi)
SHA256 hash and name or description of the file	299e6791e4eb85617c4fab7f27ac53fb70cd038671f011007831b558c318b369 (svchos1.exe / Gh0st RAT)

SHA256 hash and name or description of the file	1395627eca4ca8229c3e7da0a48a36d130ce6b016bb6da750b3d992888b20ab8 (svchos1.exe / Gh0st RAT)
SHA256 hash and name or description of the file	2232612b09b636698afcdb995b822adf21c34fb8979dd63f8d01f0d038acb454 (com.qihoo.appstore_300101314.apk)

Campaign Chorus IoCs

Type	Indicator
Hosting IP address	95.173.197[.]195
Redirection domain	yqmqhjgn[.]com
Redirection domain	djbzdhygj[.]com
C2 domain	xiaofeige[.]icu
C2 domain	1235saddfs[.]icu
SHA256	18a21dbc327484b8accbd4a6d7b18608390a69033647099f807fdbfcdfff7e6d (aa84e841b4.zip)
SHA256	dbe70991750c6dd665b281c27f7be40afea8b5718b097e43cd041d698706ade4 (f5c84e20eca5434a8f7661d26565.zip)
SHA256	e8c058acfa2518ddc7828304cf314b6dd49717e9a291ca32ba185c44937c422b (f83acd4249e44e.zip)
SHA256	491872a50b8db56d6a5ef1ccabe8702fb7763da4fd3b474d20ae0c98969acfe5 (win64wsotusapdeuw.msi)
SHA256	bc6fb2eab9ed8d9eb405f6186d08e85be8b1308d207970cc41cf90477aa79064 (WindowsX64sipwgdwudtrsu.msi)
SHA256	bd4635d582413f84ac83adbb4b449b18bac4fc87ca000d0c7be84ad0f9caf68e (wsc_proxy.exe)
SHA256	1c3f2530b2764754045039066d2c277dff4efabd4f15f2944e30b10e82f443c0 (wsc.dll)

Impersonated Brand Examples and Corresponding Domains From Campaigns Trio and Chorus

Malicious Domain	Brand/Product Info
deep-seek[.]rest	Chinese AI company
i4toolsearch[.]vip	Software to manage and transfer files in macOS devices
youdaohhzi[.]top	Popular Chinese dictionary and translation software
xiazaizhadia9[.]cyou	An import-export and e-commerce trading company based in China
xiazaizhadia8[.]cyou	Translation tool
xiazaizhadia51[.]cyou	A popular Chinese office suite
xiazaizhadia50[.]cyou	Web browser
xiazaizhadia46[.]cyou	An anti-detection browser
xiazaizhadia44[.]cyou	Multilingual translation service
xiazaizhadia42[.]cyou	VPN service
xiazaizhadia41[.]cyou	Chinese web browser
xiazaizhadia40[.]cyou	VPN service
xiazaizhadia39[.]cyou	Digital distribution platform for PC video games
xiazaizhadia37[.]cyou	Chinese Pinyin input method editor
xiazaizhadia36[.]cyou	A privacy-focused instant messaging application
xiazaizhadia35[.]cyou	Business communication and collaboration platform
xiazaizhadia34[.]cyou	A video game distribution platform
xiazaizhadia33[.]cyou	Server management web panel
xiazaizhadia30[.]cyou	Typing training software
xiazaizhadia29[.]cyou	Music streaming service
xiazaizhadia27[.]cyou	Translation service
xiazaizhadia24[.]cyou	Image viewing application
xiazaizhadia22[.]cyou	Messaging service

xiazaizhadia21[.]cyou	Photo editing and beautification software
xiazaizhadia20[.]cyou	A Chinese subscription video-on-demand streaming service
xiazaizhadia2[.]cyou	A Chinese music streaming service
xiazaizhadia19[.]cyou	A Chinese video live streaming platform
xiazaizhadia18[.]cyou	A major web browser in China
xiazaizhadia16[.]cyou	Software designed to automatically find and update hardware drivers on a Windows PC
xiazaizhadia12[.]cyou	A Chinese music streaming service
xiazaizhadia10[.]cyou	Remote desktop control software popular in China
xiazaizhadia1[.]cyou	An anti-detection browser
guwaanzh8[.]cyou	A privacy-focused, end-to-end encrypted messaging application that uses distributed technology
guwaanzh35[.]cyou	Server management web panel used widely in China
guwaanzh34[.]cyou	A video game distribution platform in China
guwaanzh25[.]cyou	A lightweight Chinese internet security suite
guwaanzh24[.]cyou	Instant messaging application
guwaanzh21[.]cyou	Screen capture and video recording software
guwaanzh20[.]cyou	Social media and payment application
guwaanzh2[.]cyou	A major Chinese music streaming and download service

Observed Domain Activity (Based on pDNS Data)

Domain	First Seen (UTC)	Last Seen (UTC)
ydbao052[.]cyou	2025-06-16 13:11:39	2025-08-20 00:10:29
i4toolscacvi[.]top	2025-04-16 01:18:16	2025-08-19 23:04:08
youdaqqaaavw[.]top	2025-04-29 19:19:45	2025-08-19 20:39:49
i4toolsuozp[.]top	2025-04-22 09:04:45	2025-08-17 05:26:12
i4toolsllsk[.]top	2025-03-09 10:20:15	2025-08-15 23:00:12
youdaovavxl[.]top	2025-04-16 01:28:55	2025-08-14 03:20:36

youdaxxddxk[.]top	2025-04-26 13:42:59	2025-07-23 04:53:57
youdaovavxk[.]top	2025-04-16 01:28:55	2025-07-22 23:02:23
ydbao11[.]cyou	2025-06-10 05:08:35	2025-07-08 10:56:29
youdaoosssj[.]top	2025-06-10 09:16:41	2025-06-11 11:22:28
qishuiyinyque-vip[.]top	2025-05-18 04:06:29	2025-06-11 11:08:24
i4toolsuoxk[.]top	2025-04-23 03:20:02	2025-06-11 09:22:28
i4toolscacsm[.]top	2025-04-15 18:06:37	2025-06-11 06:47:22
youdaxxyzr[.]top	2025-04-25 03:35:13	2025-06-11 03:17:04
i4toolscaczu[.]top	2025-04-16 01:18:17	2025-06-10 21:16:29
youdaxxyzy[.]top	2025-04-24 10:09:16	2025-06-10 13:28:26
xiazaizhadia31[.]cyou	2025-05-26 18:14:44	2025-06-10 03:46:14
guwaanzh1[.]cyou	2025-05-15 12:09:46	2025-06-09 22:06:13
xiazaizhadia11[.]cyou	2025-05-26 15:27:15	2025-06-09 14:56:12
anydesk-www[.]cyou	2025-05-03 03:12:06	2025-06-09 08:29:06
i4.llllxiazai-web.vip	2025-05-07 09:03:49	2025-05-19 01:33:38

Acknowledgments

The authors would like to thank Shehroze Farooqi, Bradley Duncan and Alex Starov for their valuable insights and feedback to improve the research work mentioned in this article.

Additional Resources

- [Trojanized Installer Distribution Campaign](#) – Unit 42, Palo Alto Networks
- [Legitimate Software Impersonation Campaign](#) – Unit 42, Palo Alto Networks
- [Ghost RAT \(Malware Family\)](#) - Malpedia
- [Gh0st RAT: malware active for 15 years is still used by threat operators](#) – Side Channel Blog
- [7m-sdk.7moor-fs1.com URL Report](#) – IBM X-Force Exchange
- [Behind the Great Wall Void Arachne Targets Chinese-Speaking Users](#) – TrendMicro
- [Malware Campaigns Targets Chinese Speaking Users With Fake Installers](#) – DigiAlert
- [Musical Chairs: A Multi-Year Campaign Involving a New Variant of Gh0st Malware](#) – Unit 42, Palo Alto Networks