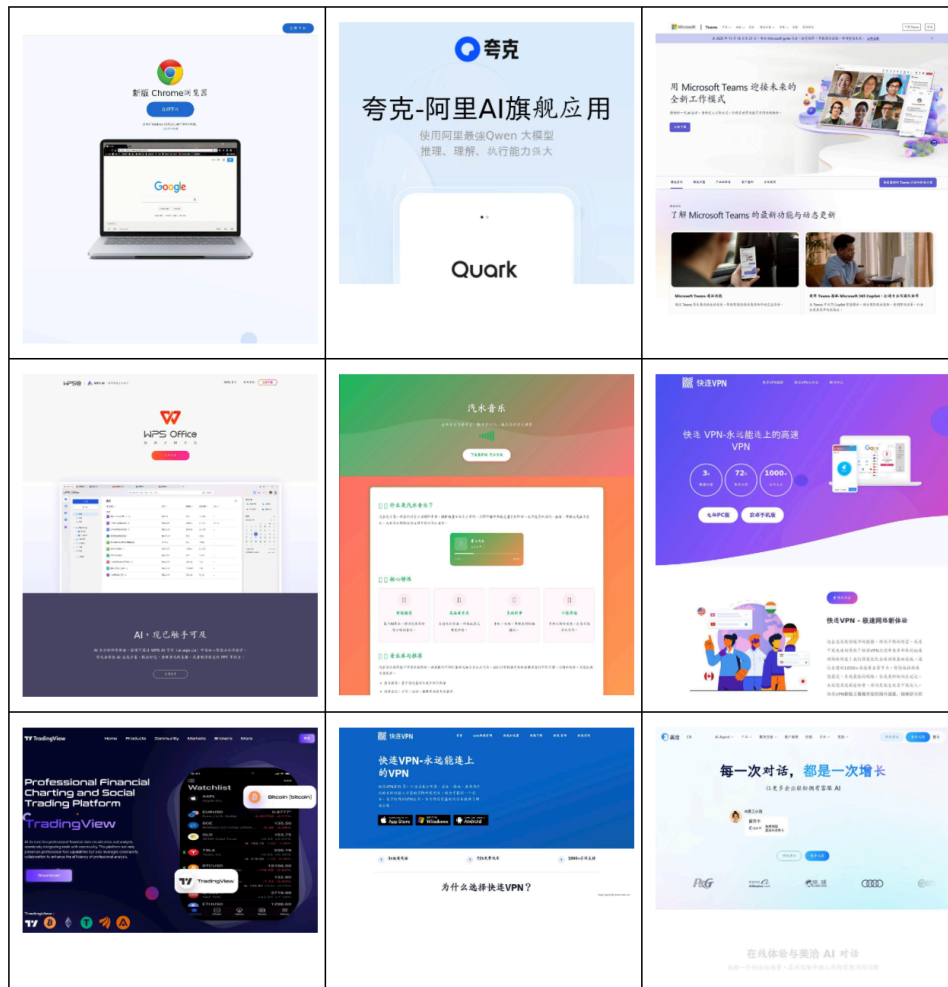


Chinese Malware Delivery Domains Part IV

dti.domaintools.com/chinese-malware-delivery-domains-part-iv

December 8, 2025



Community

Evolution of Infrastructure and AI-Powered Security Analysis

Summary

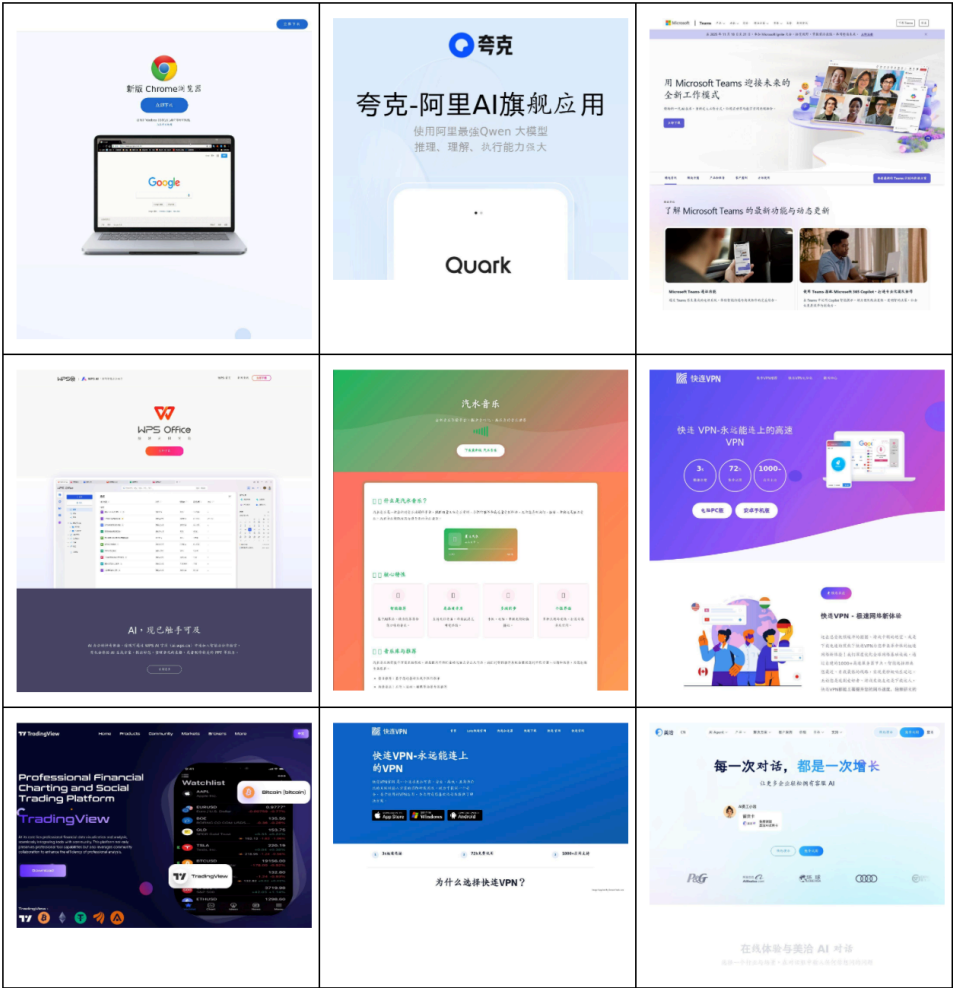
Since January 2025, DomainTools Investigations has been tracking a large cluster of malware delivery domains that's been active since June 2023. We've published three reports on the cluster in the past 11 months, and in the latest [Part III report in July 2025](#) we surmised that the cluster comprised over 2,800 domains. Since then, we've observed more than 1,900 additional malware delivery domains we suspect are tied to the same super cluster. This high volume of malware delivery domains makes for an excellent case study of AI facilitated analysis to take on the burden of website analysis, binary analysis and detection authoring.

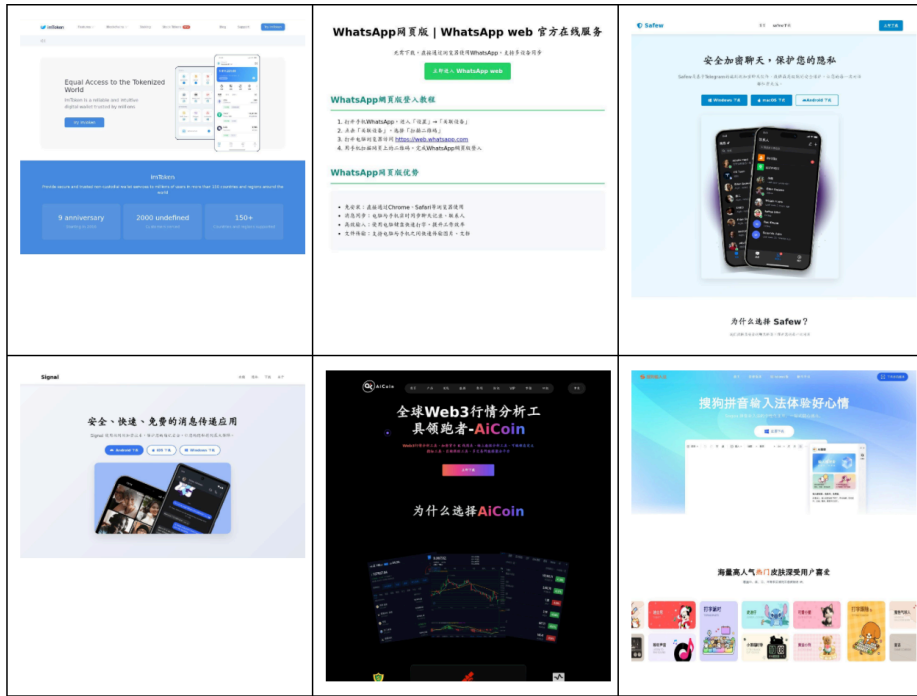
This report provides updates on the cluster following Part III and introduces a new experimental approach to defensive hunting and tracking malware delivery clusters such as the one described through the deployment of agentic AI systems that enable analysis workflows at the scale and speed necessary to match threat actor operations. Using a combination of task based AI orchestrator and sub agents, one security researcher achieved a 10x improvement in analysis throughput (assuming the websites were resistant to traditional solutions) with agents tirelessly processing over 1,900 malware delivery websites in the time traditionally required for roughly 200-400 manual investigations.

At a glance, the threat actor continues to demonstrate remarkable persistence and scale in their malware delivery operations, maintaining a wide variation in infrastructure deployment, lure sites, and malware delivery, which consistently appears to be targeting Chinese-speaking users across the globe. Our analysis from May to November 2025 reveals notable operational evolution across distinct clustering patterns and continued spoofing of common software download websites as lures to deliver trojans and credential stealers. However, the same operational security weaknesses prevail in

the form of highly leveraged SOA emails, tracking IDs for SEO manipulation, unique registrant names, and relatively unique infrastructure combinations. These factors allow for distinct campaigns to be linked together, forming the super cluster of approximately 5,000 malware delivery domains that has been active since 2023.

Sample of the malware delivery websites spoofing common application download pages:



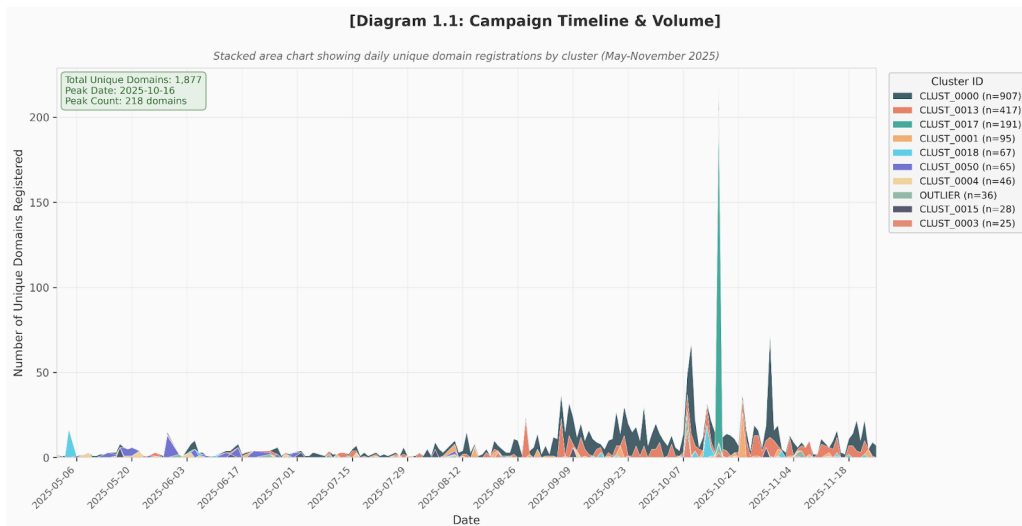


Part 1: Campaign Evolution Analysis

1.1 Infrastructure Evolution

At a high level, the actor's infrastructure has undergone an overall fragmented evolution with a few exceptions since our [July 2025 report \(Part III\)](#), which documented 2,800 domains created from January to May 2025. Current analysis indicates that approximately 1,900 additional domains have been created in the period from May 2025 to November 2025.

Initially, domain hosting infrastructure was highly consolidated prior to May 2025, but this gradually gave way to diversification in August. By November, the infrastructure fractured further into smaller, more fragmented clusters with a focus on localization and operational security improvements as well as leveraging domestic Chinese registrars and randomized domain naming patterns.



The infrastructure evolution appears to demonstrate distinct transitions with a particular surge in overall variability from August to November:

Consolidated (May-July 2025)

- Primary infrastructure: Alibaba Cloud Hong Kong
- Registrar: WebNIC (98% concentration)
- Focus: Chrome, Chinese VPN, and WPS Office spoofs

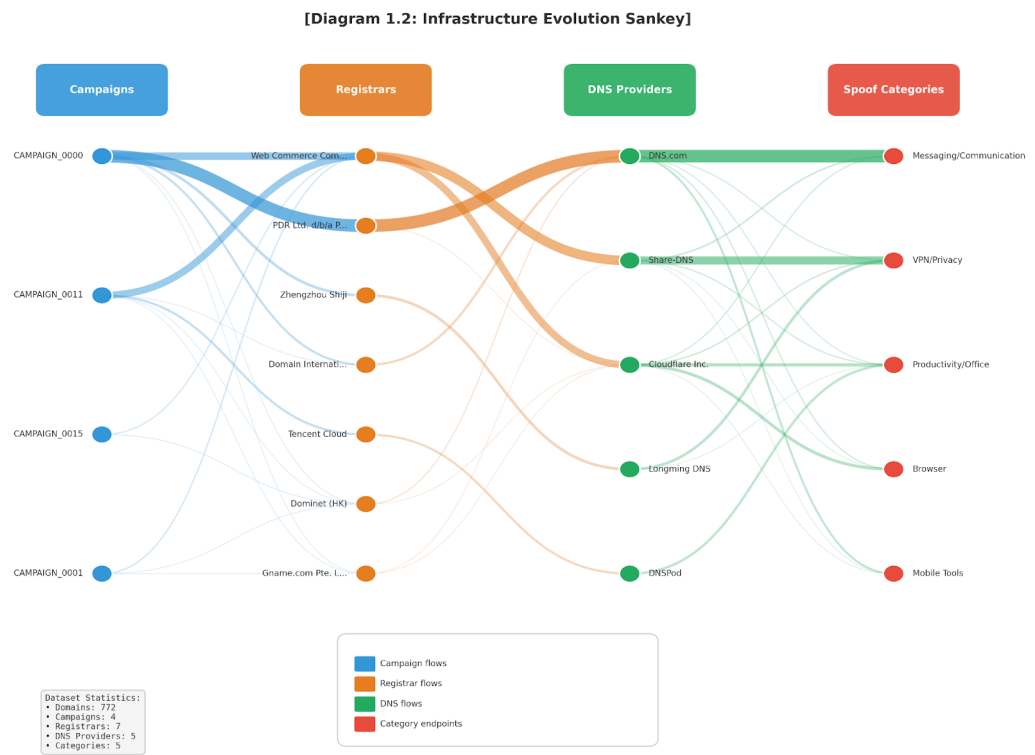
Diversified (August-September 2025)

- New targeting: Signal and Telegram messengers
- Domain clustering tightens (higher specificity scores)

Localization (October-November 2025)

- Majority use of Chinese domestic registrars
- 四川域趣网络科技有限公司 becomes primary registrar
- Random domain naming patterns emerge
- Possible OPSEC improvement attempts

[Diagram 1.2: Infrastructure Evolution Sankey] Flow diagram showing: Campaigns → Registrars → ISPs → Countries



1.2 Campaign Comparison Matrix

Campaign	Domains	Clusters	Primary DNS	Top Registrar	Active Period	Key Targets
CAMPAIGN_0000	908	1	DNS.com	PDR Ltd. (PublicDomainReg)	May-Nov 2025	Messaging, VPN, Mobile, Browser
CAMPAIGN_0011	417	1	Cloudflare	Web Commerce Comm.	May-Nov 2025	Office, Browser, Input, Messaging
CAMPAIGN_0005	196	5	Other	Sichuan Yuqu Tech	Oct-Nov 2025	Financial, Security
CAMPAIGN_0001	95	1	Cloudflare	Bangning Digital	May-Nov 2025	VPN, Messaging, Mobile
CAMPAIGN_0038	77	10	Other	Web Commerce Comm.	May-Aug 2025	VPN, Office, Messaging, Input
CAMPAIGN_0015	67	1	Share-DNS	Web Commerce Comm.	May-Nov 2025	VPN, Messaging, Financial, Browser
CAMPAIGN_0004	46	1	Cloudflare	Gname.com Pte. Ltd.	May-Nov 2025	Crypto
CAMPAIGN_0013	28	1	Cloudflare	NameSilo, LLC	May-Oct 2025	Uncategorized
CAMPAIGN_0003	25	1	Cloudflare	Dynadot Inc.	Aug-Nov 2025	Financial
CAMPAIGN_0021	19	1	Share-DNS	Gname.com Pte. Ltd.	May-Oct 2025	Remote Access
CAMPAIGN_0002	9	1	Share-DNS	Gname.com Pte. Ltd.	May-Nov 2025	Uncategorized
CAMPAIGN_0039	9	1	Cloudflare	NameSilo, LLC	Jul 2025	Browser
CAMPAIGN_0028	8	1	Cloudflare	Spaceship	Jun-Sep 2025	Browser
CAMPAIGN_0006	7	1	DNS.com	Dominet (HK) Limited	May-Nov 2025	Remote Access

1.3 Operational Adaptations

Comparing domain registration trends from January through June 2025 with June through November 2025, several adaptations emerged:

Infrastructure Resilience

VPN Services (363 domains, 22.4%)

- LetsVPN/Kuailian (快连): 129 domains
 - Pattern: kuailian*.[.]com[.]cn, kuailian-xx.[.]com[.]cn
 - Examples: kuailianwq.[.]com[.]cn, kuailianod.[.]com[.]cn, kuailian-rd.[.]com[.]cn
- Kuailian variants: 43 domains
 - Pattern: xx-kuailian[.]top, kuailian*-kuailian[.]top
 - Examples: vd-kuailian[.]top, kuailian3-kuailian[.]top

Productivity Software (229 domains, 14.2%)

- Google (search/services): 148 domains
 - Pattern: cn-*google.[.]com[.]cn, zh-*google.[.]cn, web-*google.[.]cn
 - Examples: cn-app-google.[.]com[.]cn, zh-cn-google.[.]cn, web-gg-google.[.]com[.]cn
- Youdao (translation/dict): 19 domains
 - Examples: youdao-youd.[.]com[.]cn, web-youdao.[.]com[.]cn
- WPS Office: 18 domains
 - Pattern: wps-office-*.[.]com[.]cn, wps-*.[.]com[.]cn
 - Examples: wps-office-cnzh.[.]com[.]cn, wps-jinshan.[.]com[.]cn

Web Browsers (109 domains, 6.7%)

Chrome: 53 domains

- Pattern: guge-*.[.]com[.]cn, chrome-*.[.]com[.]cn
- Examples: guge-cn.[.]com[.]cn, guge-chrome-app.[.]com[.]cn, chrome-cnzh.[.]com[.]cn

Cryptocurrency Tools (54 domains, 3.3%)

ImToken: 38 domains

- Multi-TLD strategy: .com, .org, .top, .xyz, .shop, .click
- Examples: imtz1[.]xyz, mtoken[.]shop, imtoken-im[.]click

Financial/Trading Platforms (51 domains, 3.2%)

- AlCoin: 27 domains (extensive infrastructure)
 - Multi-TLD strategy: .com, .org, .biz, .vip
 - Examples: aiiceoin.[.]com, xz-aicoin.[.]com, aicoin-zh[.]org
- AlCoin Download variants: 11 domains
 - Examples: us-aicoin.[.]com, aicoin-xz.[.]com, home-aicoin.[.]com

Input Methods & Translation (43 domains, 2.7%)

Sogou Input: 15 domains

- Pattern: *-sougoushurufa[.], *-sogou[.], sogou-*[.]
- Examples: cnzh-sougoushurufa.[.]com[.]cn, app-sougoushurufa.[.]com[.]cn, shurufa-sogou[.]top, shurufa-sogou[.]top, sogou-pc[.]cn

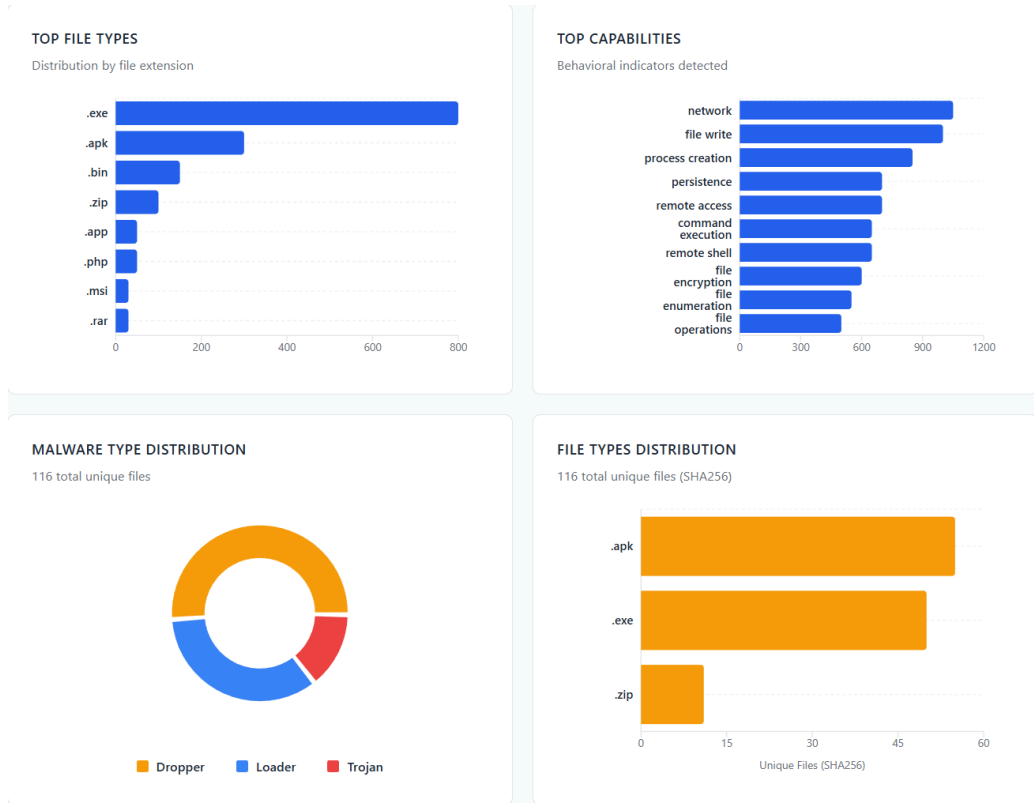
2.3 Binary Analysis Results

From workflow analysis data, we recovered and analyzed 47 unique binary samples across campaigns:

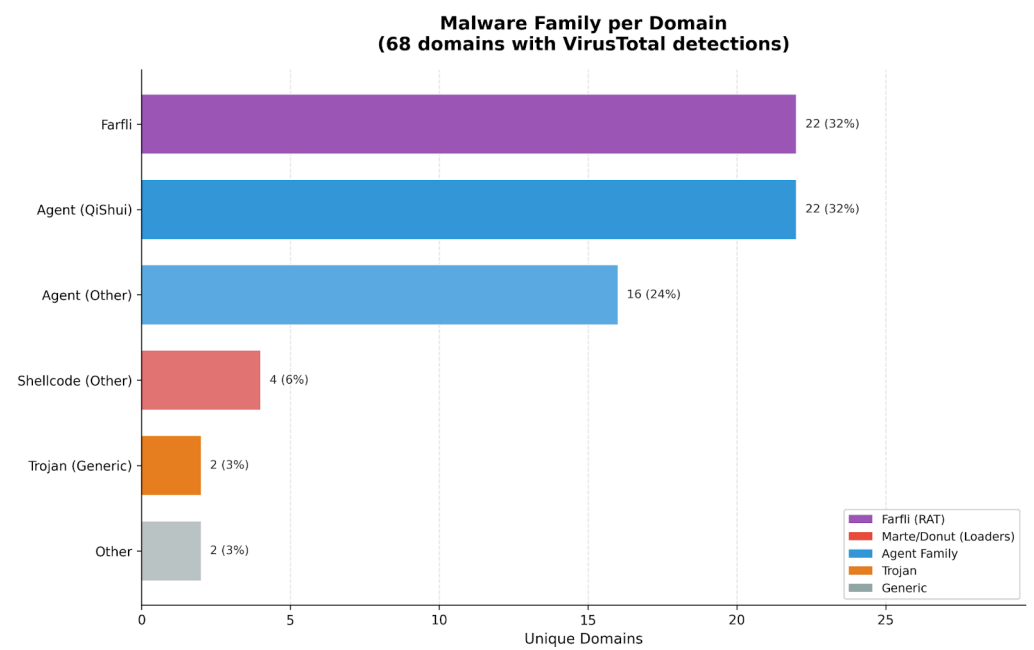
[Diagram 2.2: Binary Analysis Overview]

Malware Families Identified

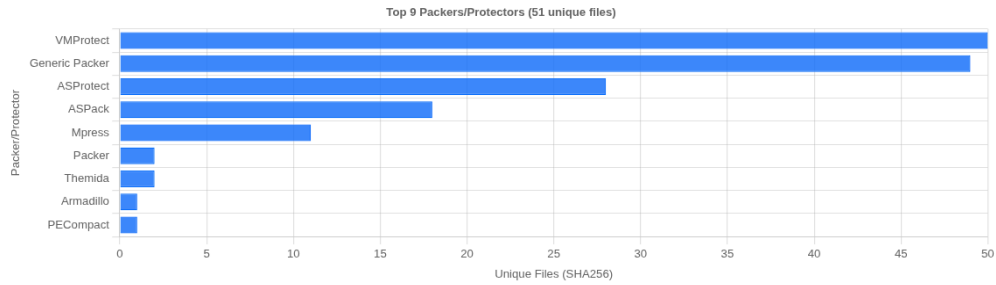
Of the 1,900 domains processed, there were approximately 116 unique executables or archive files retrieved. In many cases, the same files were being delivered across multiple sites.



Several samples identified were detected in VirusTotal; however there was a relatively consistent pattern of having large file downloads (100-250mb) from clusters. This likely prohibits most users from uploading to services like VirusTotal to scan the files without using the API.



Other prominent patterns were protected files with VMPprotect or UPX and other packers of suspected droppers.

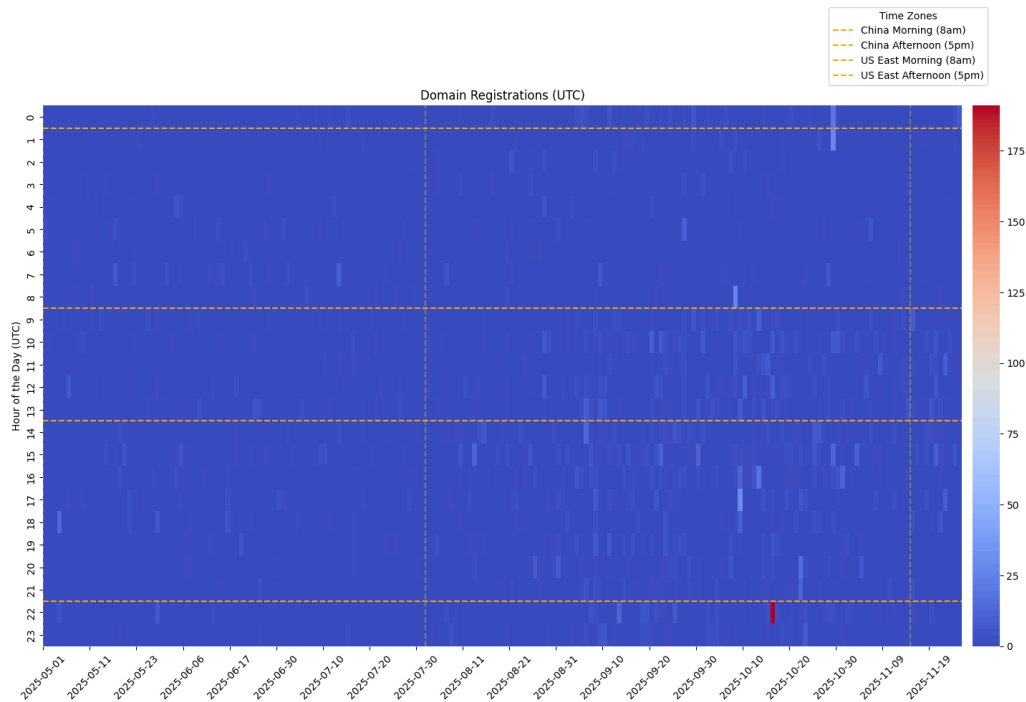


The experimental improvements to the website analysis and malware retrieval approach for research purposes provided additional insights into the malware delivery cluster: namely, that there is a relatively wide variation in the types of malware being delivered from relatively consistent web templates and relatively close clustering of domain management operations compared to previous findings in January and May 2025. This suggests that this long lived cluster dating back to 2023 has been or is evolving into a service platform where end users might bring their own malware in attempts to lure targets of opportunity.

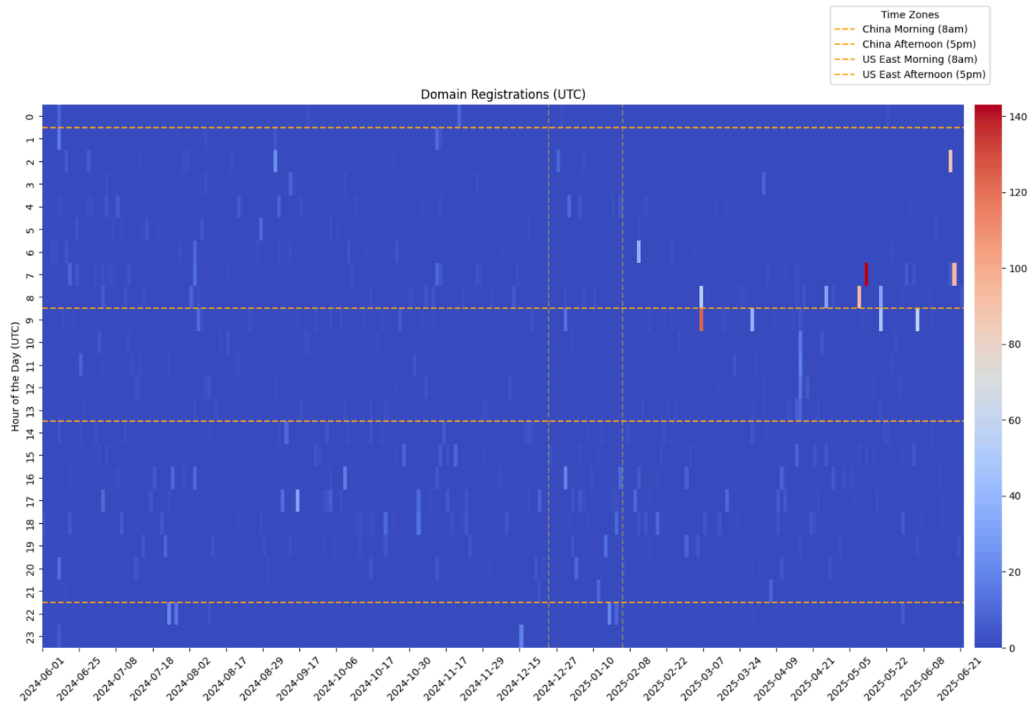
2.4 Geographic and Temporal Patterns

Prior investigations found that domain registration patterns largely aligned with East Asia business hours (8am-5pm UTC+8) in terms of overall volume, continued activity through US holidays but cessation before Chinese New Year, and approximately 40% weekend reductions. The recent data from May to November 2025 does not appear to corroborate similar findings.

[Diagram 2.3: Registration Timing Heatmap 2025-05 to 2025-11] Hour/day heatmap showing timezone working patterns



[Diagram 2.4: Registration Timing Heatmap 2024-06 to 2025-06] Hour/day heatmap showing timezone working patterns



Working Hours Analysis

Peak Activity

Primary Peak: UTC 22:00 (276 domains, 13.9%)

- Beijing: 06:00 (pre-business) | US East: 17:00 (end of day) | Moscow: 01:00 (night)
- Note: 191 of 276 domains (69%) came from a single Oct 16 bulk registration event
- This peak is anomalous for any standard timezone's business hours

Secondary Peak: UTC 15:00 (179 domains, 9.0%)

Beijing: 23:00 (late night) | US East: 10:00 (morning) | Moscow: 18:00 (evening)

Weekend Activity

- Weekday/Weekend ratio: 3.26:1 (30% above expected 2.5:1 uniform ratio)
- Thursday anomalies: 26.1% of activity (expected ~14%)

Holidays:

Holiday Type	Activity Level
Chinese early holidays (May)	Reduced (15-44% of normal)
US holidays	Reduced (20-30% of normal)
Chinese Mid-Autumn (Oct)	Increased (235% of normal)

Infrastructure Geography

Indicator	Value	Implication
.cn/.com.cn TLDs	78.90%	China-focused infrastructure
Chinese-language registrars	38.70%	Operators comfortable in Chinese
Asia-Pacific registrars	~80%+	Regional procurement preference
DNS providers	100% China-based	Infrastructure anchored in China

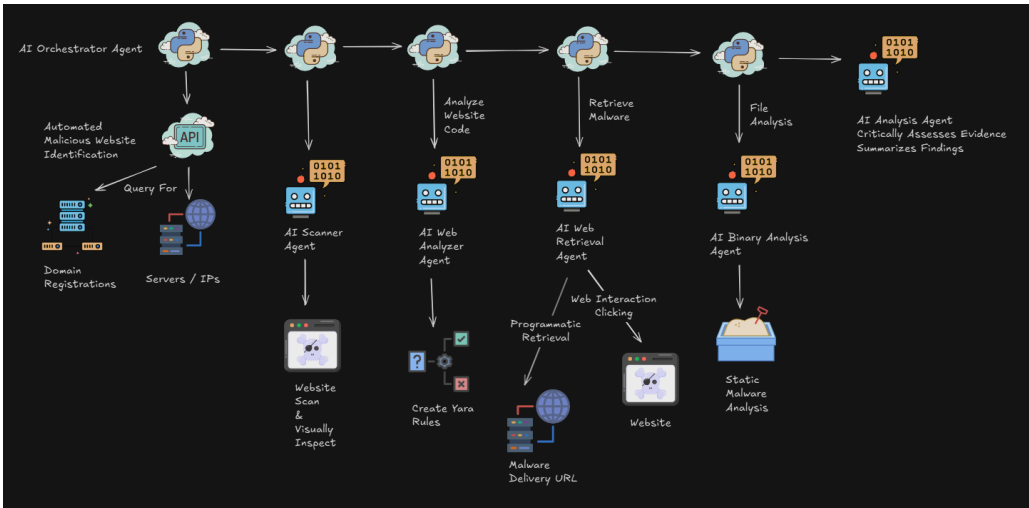
It's important to note that domain registrations can be done via API and in this case may well be, meaning they could be registered at any arbitrary time. Similarly, the TLD and regional hosting providings are typically globally accessible. Though previous analysis of this cluster found that a strong pattern of domain registrations and first observed DNS traffic were common during East Asia working hours, that is no longer evident from the data. What can be still inferred is that the focus remains consistently on primarily targeting Chinese language users. This inference was amplified by the cluster's record spike in malware delivery website configurations during the Chinese Mid-Autumn festival, suggesting the intentions of this cluster are or have been primarily targeting Chinese users.

Part 3: Agentic AI for Analysis

3.1 Architecture Overview

The game-changing capability in our analysis comes from the deployment of specialized AI agents that operate in coordinated workflows. Unlike traditional automated tools that follow rigid scripts, the agentic system demonstrates adaptive intelligence in analyzing threats.

[Diagram 3.1: Agent Orchestration Flow]



Two-Layer Agent System

Layer 1: Orchestration

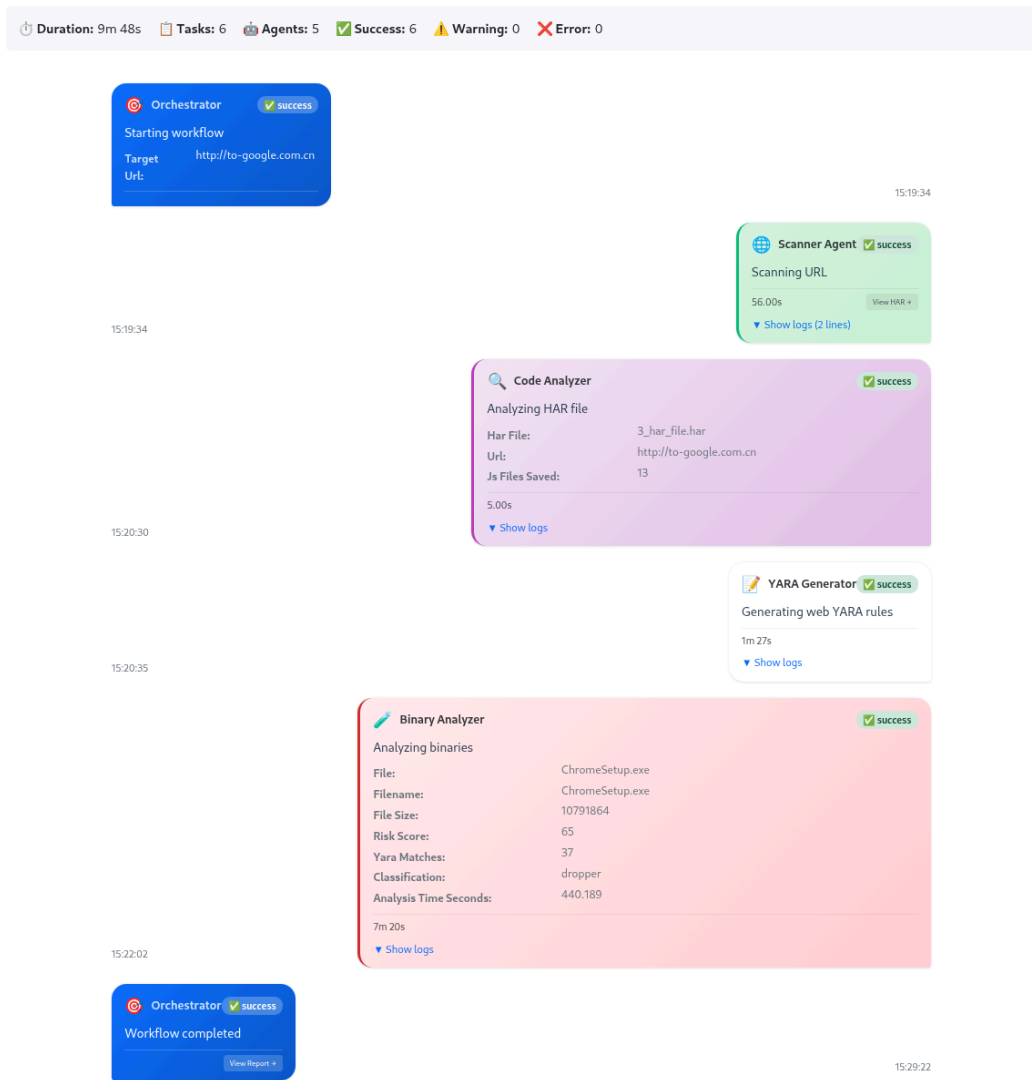
- Receives analysis requests
- Coordinates specialized agents
- Synthesizes findings into threat intelligence

Layer 2: Specialized Analysis Agents

- **ScannerAgent**: Browser automation and traffic capture
- **CodeAnalyzerAgent**: JavaScript semantic analysis
- **BinaryAnalyzerAgent**: Multi-tool malware analysis
- **YARAGeneratorAgent**: Automated rule creation

3.2 AI-Powered Analysis Workflow

The power of agentic AI is best illustrated through an actual analysis sequence. Here's how the agents collaboratively investigated a suspicious domain:



Sampling of the website code analyzer subagent looks for malicious characteristics, identifies malware delivery behaviors, and determines if Yara rules could be generated for any identified malicious code on the site. If so, they get tasked to and created by another subagent and are immediately put to use going into future analysis so the system can learn as it goes.

Screenshot of the malware delivery website spoofing as a Google Chrome download site for Chinese language users:



Agent analysis summary of the website code, visual inspection, and network traffic analysis:

JavaScript Files Analyzed
Analyzed 12 JavaScript file(s) from 20 network resources

Download Mechanism Assessment

Mechanism Type	multi_file_dynamic_construction
Description	Download mechanism uses multiple JavaScript files with dynamic loading and global variables
Verified Patterns	6 pattern(s) confirmed
Overall Confidence	HIGH
Evidence Validated	Yes

Interactive Elements Detected

[1] Download URL is constructed across multiple files using global variables: gaDeviids, globalAnimations, __cfBeacon

Files: main.min.js, autotrack.js, analytics.js, vcd15cbe7772f49c399c6a5babf22c124171689176015

Action Required: trace_and_test

Confidence: HIGH

Verified observations show dynamic loading and global variable usage across 4 files

Analysis Recommendations

- Use JavaScript tracer to reconstruct URLs from multi-file mechanisms
- Based on 6 verified patterns across 4 file(s)
- Monitor all download events during interactive testing
- Verify downloaded file hashes match expected samples

In a second example, the experimental AI service analyzed a gambling site that attempts to profile users and has anti-bot mechanisms to attempt to prevent scanners and web scrapers, and lacks a clear programmatic delivery mechanism. The screenshot below is of a download site for a purported online gambling mobile app. It serves an APK file that is packed and suspected of sideloading stealer malware.

房间号: **225070**
主营项目
168极速赛车 澳洲10 飞艇 时时彩
(进入房间需要**审核通过** 切记把昵称交给客服审核)

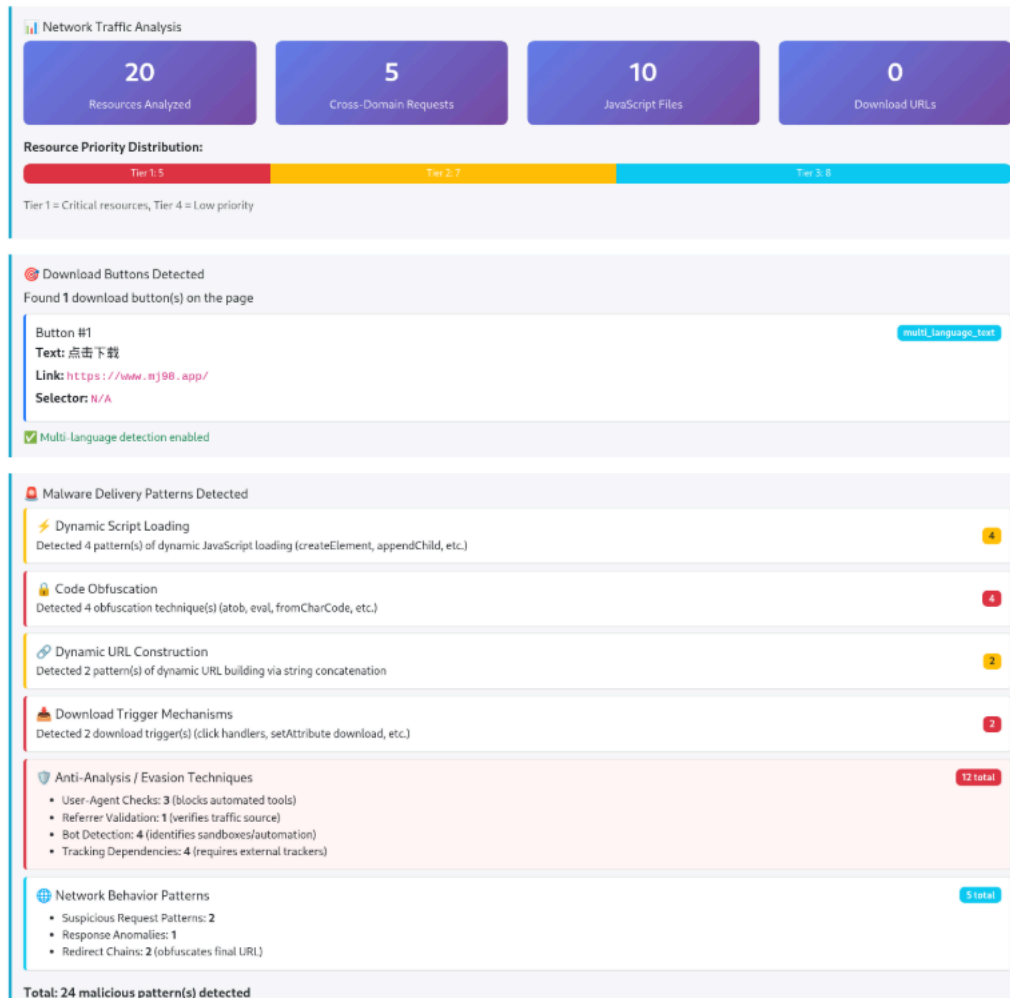
消息 【名爵房间号：225070】豪门娱乐祝您财源滚滚！以下是

微信避免封号
不会回复您任何问题!
有问题请联系左侧在线客服
或进入上方游戏平台
联系平台的在线客服

点此联系
在线客服

26326ms	名爵网页入口	打开地址
...	名爵微信扫码入口	打开地址
2853ms	名爵苹果APP	点击下载
1395ms	名爵安卓APP	点击下载

Agentic code analysis of the site:



3.3 Scaling Defense with AI

The use of AI agents changes the economics of defense. In investigating malicious websites for example, the primary pain points for a human analyst can be determining the website characteristics to identify and retrieve malware and knowledge management to discern if similar site configurations have been observed before. The timing for a human analyst doesn't scale to many websites or the many investigation avenues sometimes needed such as combining code and interactive analysis actions. Agents can run those same tools and action those same or similar interactions.

[Diagram 3.2: AI vs Manual Analysis Comparison]

Metric	Manual Analysis	AI-Powered
Domains per Day	20 – 50	2,000 – 4,000
Deep Analysis Time	10 – 90 minutes	1-10 minutes
YARA Rule Generation	5 – 30 minutes	30 seconds
Pattern Recognition	Limited to analyst knowledge	Comprehensive across corpus
Consistency	Variable	Deterministic
Scale Ceiling	~350 domains/week	~14,000 domains/week

Processing Transparency

It's important to note our actual performance metrics. During this experimentation phase we gave minimal system resources and allowed for 3 agent workers to process 1 domain each through the workflow at a time. These were their approximate completion time averages broken down by the core tasks within the analysis workflow. In one bulk processing run with 3 workers, 2,000 malware delivery domains were processed in approximately 10 hours.

- **Average Processing Time:** 1-10 minutes per domain

- **Variance Factors:**
 - Simple static sites: ~1 minute
 - Heavy JavaScript: ~3 minutes
 - Binary download and analysis: ~5 minutes
- **Parallel Processing:** Up to 3 concurrent analyses
- **Daily Throughput:** 400 – 4,000 domains

Conclusion

The threat actor continues to demonstrate capabilities in maintaining large-scale malware distribution infrastructure targeting Chinese-speaking users. Through our analysis of approximately 1,900 domains from May to November 2025, we observed an evolution in their operational tradecraft, including infrastructure diversification, enhanced evasion techniques, and additional spoofed entities such as popular Chinese AI and entertainment apps.

This investigation experimented with AI-powered analysis. The deployment of specialized AI agents enabled full coverage in analysis throughput while maintaining relatively high precision; however, agentic detection authoring remained a persistent weak point that continues to require further refinement. This capability changed the defender's equation, enabling complex and dynamic analysis workflows to scale to the volume of a large malware delivery campaign.

Special recognition goes to the AI agents that processed thousands of domains tirelessly and consistently. However, we must acknowledge limitations in our analysis. Processing times of 1-10 minutes per domain, while revolutionary compared to manual analysis, still require substantial computational resources for internet-scale defense. Attribution confidence, while high for core clusters, relied on spoof themes and infrastructure patterns rather than incorporating website and binary characteristics into clustering parameters as well. Future work seeks to incorporate an increase in the learn-as-we-go approach to identify additional sites with common malware delivery and detection evasion characteristics as well as further efforts in binary analysis integration.

As we look forward, the cybersecurity landscape has found itself balancing on the scales of an AI-pervasive era where criminals and defenders alike might empower their roles.

The malware delivery campaign highlighted in this report provides insights into the scale of modern threats and an opportunity to show that with appropriate application of AI, defenders can keep pace.

Appendices

Appendix A: IOC List

A complete list of all domains, file URIs, and hashes can be found on our [GitHub](#).

Disclaimer: This report contains analysis of malicious infrastructure for defensive purposes. All malware samples and malicious domains should be handled with appropriate security controls. The processing times and performance metrics stated are estimates based on our specific infrastructure and may vary in different environments.

Registrant Emails

1204504046[@]qq.com
18589929790[@]163.com
2035712403[@]qq.com
21033193[@]qq.com
2235053526[@]qq.com
2274677885[@]qq.com
2633067209[@]qq.com
286847215[@]qq.com
2957999579[@]qq.com
3283028829[@]qq.com
3653564961[@]qq.com
3799492994[@]qq.com
3839020959[@]qq.com
3926066154[@]qq.com
3951087743[@]qq.com
408367846[@]qq.com
515563424[@]qq.com
531679449[@]qq.com
614199941[@]qq.com
616489685[@]qq.com
624310867[@]qq.com
631599288[@]qq.com
646996136[@]qq.com
744812326[@]qq.com
9324928[@]qq.com
a685569961[@]outlook.com
aa16858895555[@]outlook.com
aisuite[@]hotmail.com
bnpk443[@]163.com
calaw19890912[@]gmail.com
chengwangyi1971[@]hotmail.com
cllhut005[@]gmail.com
ericq1027[@]gmail.com
eyuqicocafi68[@]gmail.com
fifermarti968[@]gmail.com
gfan8581[@]gmail.com
hs1726936602[@]163.com
huuhad791[@]gmail.com
jinqianj5722[@]163.com
kathyehek[@]gmail.com
liujing3721[@]outlook.com
logged567[@]gmail.com
nameibuhaore[@]outlook.com
nnaomalan042[@]gmail.com
pandashen0505[@]gmail.com
pluto_1111[@]hotmail.com
pokiohgff[@]gmail.com
raficponomarov5[@]gmail.com
sophiahernandezv[@]hotmail.com
wc18973[@]outlook.com
westabuse[@]gmail.com
winrmbcc[@]gmail.com
yaarluc55342[@]outlook.com
yaqyfwhv476149[@]outlook.com
yilufa168899[@]163.com
yiyi95788[@]gmail.com
yoyoy01[@]proton.me
zmpnz951938[@]outlook.com

Trackers

GoogleAnalytic4 codes

G-37ZJLQFQXW
G-3GR90RW2M5
G-936N0684JB
G-C31Z08KKX3
G-DDT7Z270WS
G-EK25PQRY5L
G-EVL1PWCP0M
G-GVGY3o1ft
G-MZNK5Z1NKP
G-PAWLWnpAps
G-QK5S7CE4J7
G-S0CCFL96VK
G-YYPYEVWJ1F
G-ZJuHGBTqxJ gtm_codes

GTM-5P954SP
GTM-5XB9N2J
GTM-KW3XKWM
GTM-MG73JRC
GTM-MNBPZXP
GTM-PBZC932
GTM-PR42FSR
GTM-T3SK6H7
GTM-W5DBT74
GTM-WSTQ4SK

GTM-WX6RDCT fb_codes

2140700472996352
3440778589358687
661275193346491
671933482235831
712357421178146 baidu_codes
1605bee5a12fc31c0b5bb9232d281e8f
2c583a8a0d28d3ddbec451e77062bdf6
352bf0fb165ca7ab634d3cea879c7a72
39f7c9431fdd7a3d6e06a177938de82a
4a4f0b2ee2183a70f09a260e209f9862
576cf858288eef7dc02ba30394d47747
61b4c1f7dc904a88452ac6e61b0d00e9
70ecc7c3a318165ed69d14518756aa48
749a9b99a1c14a45712efed8c3b8fedd
95878ed03acd631a38b80bc9056a0299
97881b7a6885b25d63db19094af0f5ca
db42cea977dda461f6890e8ba9c296e4
ec5f0730b33e6a7d5f6a246f8afed764
f4b3788b2247dd149fb7fdffe8aece79
fd3d9d32c2357b48b20735652ba569cd yandex_codes
98466329 matomo_codes
[https://tongji\[.\]mc52\[.\]com/](https://tongji[.]mc52[.]com/)

SHA256 File Hashes

472d238bd8da7436d93e78a94c918e10961663be784e9985684179aaa7894e2b8ddb67e0b243814c4e2062182043e11e07c7d1b9a1f60ad58fd129e74e12

Download URLs

http[:]//guge-cn[.]com[.]cn/ChromeSetup[.]exe
http[:]//wuquan[.]org[.]cn/static/file/WuQuaanrs[.]zip
http[:]//xunlei-pc[.]com[.]cn/XunLeiWebSetup12[.]4[.]7[.]3858xl11[.]exe
http[:]//cnzh-sougoushurufa[.]com[.]cn/sogou_pinyin_guanwang_15[.]8[.]exe
http[:]//qishuiyinyue[.]com[.]cn/static/file/SodaMusic-v2[.]7[.]0-official-win32_x64[.]exe
http[:]//qishuiyinyuedouyi[.]com[.]cn/static/file/SodaMusic-v2[.]7[.]0-official-win32_x64[.]exe
http[:]//qishuiyinyue-app[.]com[.]cn/SodaMusic-v2[.]7[.]0-official-win32_x64[.]exe
http[:]//chrome-m[.]com[.]cn/ChromeSetup[.]exe
http[:]//chrome-cm[.]com[.]cn/ChromeSetup[.]exe
http[:]//chrome-me[.]com[.]cn/ChromeSetup[.]exe
http[:]//qishui-yinle[.]com[.]cn/SodaMusic-v2[.]7[.]0-official-win32_x64[.]exe
http[:]//guge-chrom[.]com[.]cn/ChromeSetup[.]exe
....

Domains

7ov-kuailian[.]com[.]cn
8989faka[.]cn
aa-kuailian[.]com[.]cn
aaa666[.]cn
ackuailian[.]com[.]cn
acs-imtoken[.]com
ae-telegram[.]com[.]cn
aeg-kuailian[.]com[.]cn
aes-kuailian[.]com[.]cn
aicnion[.]com
aicoiene[.]com
aicoi-cn[.]biz
aicoi-down-pc[.]biz
aicoi-down-pc[.]com
aicoi-down-pc[.]org
aicoi-down-pc[.]vip
aicoi-down-soft[.]com
aicoi-down-soft[.]org
aicoi-download[.]com
aicoi-download[.]us[.]com
aicoi-home[.]com
aicoi-home[.]org
aicoi-home[.]us[.]com
aicoi-pc-download[.]biz
....

Related Content
