

Chinese Malware Delivery Domains Part V

 dti.domaintools.com/research/chinese-malware-delivery-domains-part-v

DomainTools

August 21, 2026

Introduction

In Parts I-IV of this series, we reported on a large-scale malware delivery network targeting Chinese speaking users. This cluster is frequently associated with the Silver Fox threat group and relies on thousands of typo-squatted domains. We noted previously that this infrastructure appeared to operate under an affiliate or Malware as a Service (MaaS) model. In mid June 2026, Chinese law enforcement reportedly arrested several individuals connected to Silver Fox operations. Despite this, the delivery network remained active. Multiple distinct affiliates continued registering hundreds of new malicious domains just days after the arrests. To keep these new campaigns online, the operators are blending localized .com.cn domains with abused legitimate services. We are currently tracking payloads hosted on GitHub release assets, Microsoft Store redirects, and enterprise cloud buckets across AWS, Google Cloud, and Alibaba.

The attackers behind these campaigns use software trends to maximize their infection rates. Their targeting changes based on whatever applications are currently dominating the Chinese market. Two years ago, their landing pages primarily spoofed web browsers and VPNs. Over the past year, they have capitalized heavily on the artificial intelligence boom by distributing fake installers for DeepSeek and Doubao. Regardless of the affiliate or the specific software being spoofed, the underlying infection chain identified in this campaign looks nearly identical. Victims receive a heavily modified Gh0stRAT variant hidden inside installers padded to over 100MB, which allows the malware to bypass file size limits on automated sandboxes. The execution process involves OLLVM obfuscation, a UAC bypass, and Reflective DLL Injection (sRDI) to load the malware directly into legitimate system processes. Once active, the payload communicates with its command and control servers using a custom network stack built on the hp-worker library.

Infrastructure and Lure Variations

Continuous monitoring of this cluster indicates the actor is rapidly diversifying both their distribution methods and their malware lures. While previous campaigns relied heavily on newly registered domains (NRDs), recent activity shows a systemic integration of abused legitimate services to bypass DNS reputation filtering. Analysis of the delivery URLs indicates the actor is hosting payloads across major cloud providers. Observed infrastructure used by the actor previously includes Alibaba Cloud OSS (doubaoaa.oss-cn-hongkong.aliyuncs[.com]), AWS S3 (dfgdhgg.s3.ap-east-1.amazonaws[.com]), and Google Cloud Storage (storage.googleapis[.com]). Additionally, the actor utilizes dynamic linking services like Branch.io (app[.link]), manipulates GitHub release assets, and abuses Microsoft Store search redirects (apps.microsoft[.com]).

To build trust on their landing pages, the actor frequently includes legitimate links to the Apple App Store and Google Play Store for mobile users, while serving the malicious payloads strictly to users downloading the Windows or macOS desktop executables.

Expansion of Spoofed Targets

While the actor continues to target users seeking foreign access and trading platforms (ProtonVPN, NordVPN, MetaTrader 5, AlCoin), they are increasingly spoofing domestic Chinese software.

Notable additions to the spoofing infrastructure include:

- **Artificial Intelligence:** Capitalizing on current trends, the actor has registered domains spoofing DeepSeek (ai-deepseekapp[.com][.cn]) and Doubao AI.
- **Enterprise and Productivity:** Lures include DingTalk (Alibaba's enterprise communication platform), Baidu Netdisk, and Quark Browser.
- **Security Software:** The actor is distributing payloads masquerading as Huorong Security (down.app-huorong[.cn]), a widely used Chinese antivirus and endpoint protection platform.

Post-Arrest and the Affiliate Model

In mid-June 2026, reports indicated that Chinese law enforcement executed arrests targeting operators associated with the Silver Fox malware campaigns. However, pivot analysis of the domain infrastructure reveals that these campaigns continue to be active.

Between June 17 and June 27, 2026, over 400 new malicious domains were registered and provisioned with active hosting. This sustained operational tempo validates a hypothesis generated in Part IV of this series: the malware delivery "super-cluster" operates as a decentralized Malware-as-a-Service (MaaS) platform. Rather than a single monolithic threat actor, the infrastructure is utilized by multiple distinct affiliates or operators who bring their own lures and targeting preferences while utilizing a shared baseline of Gh0stRAT-style payloads and obfuscation tooling.

Infrastructure pivot analysis isolates at least three highly distinct operational profiles active in the post-arrest window:

Cluster 1:

The most prolific active cluster is operated by an entity utilizing the email 7cf560423@baituo[.]io and the registrant name "徐涛" (Xu Tao). This operator registered 322 domains in the 10 days following the reported arrests.

- **TTPs:** This operator utilizes a highly rigid, automated infrastructure deployment model. They provision exactly one dedicated Alibaba Cloud HK IP address per spoofed brand campaign. For example, all recent Surfshark lures resolve to 8[.]210[.]120[.]164, Kraken Exchange lures to 47[.]239[.]173[.]17, and Baidu Wangpan lures to 8[.]210[.]196[.]194.
- **Targeting:** This operator focuses heavily on mass-market VPNs, cloud storage, and trending AI tools (DeepSeek, Tencent Yuanbao, Doubao).

Cluster 2:

A second distinct operator utilizes the email 3799492994@qq[.]com and the registrant name "崔勇强" (Cui Yongqiang). This actor registered 113 domains in the post-arrest window.

- **TTPs:** Like Cluster 1, this operator provisions dedicated Alibaba Cloud HK IPs (ASN 401696), but groups their infrastructure by specific deployment dates rather than strictly by brand.
- **Targeting:** This actor exhibits a highly targeted focus on financial and enterprise platforms. Lures exclusively target users of MetaTrader 4, MetaTrader 5, TradingView, AiCoin, and specialized enterprise customer service applications like WangshangLiao (旺商聊) and KefuBao (客服宝).

Cluster 3:

A third, smaller cluster operates independently from the Alibaba Cloud infrastructure, utilizing a Hong Kong hosting provider named LucidaCloud and the email daliandahouzi@gmail[.]com ("da houzi").

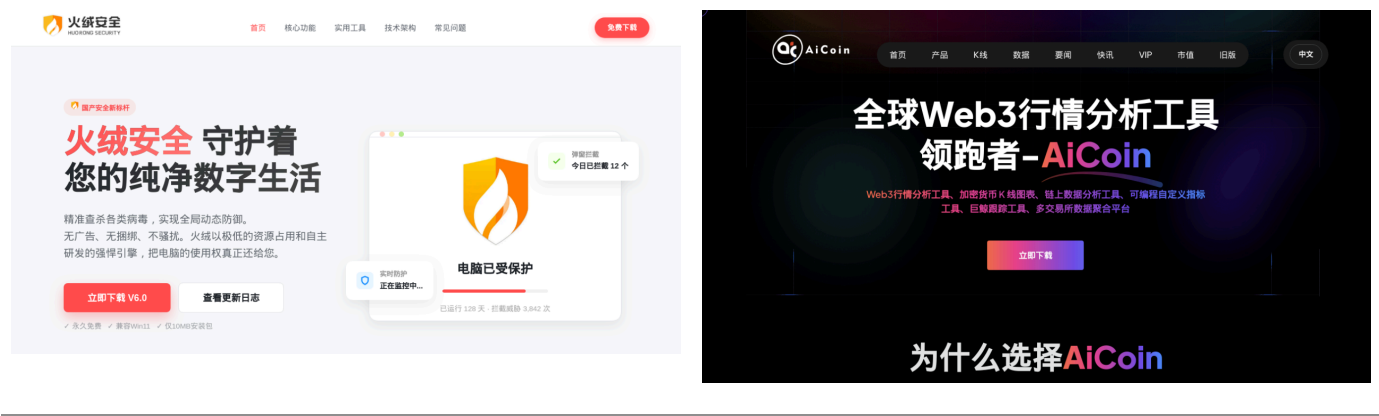
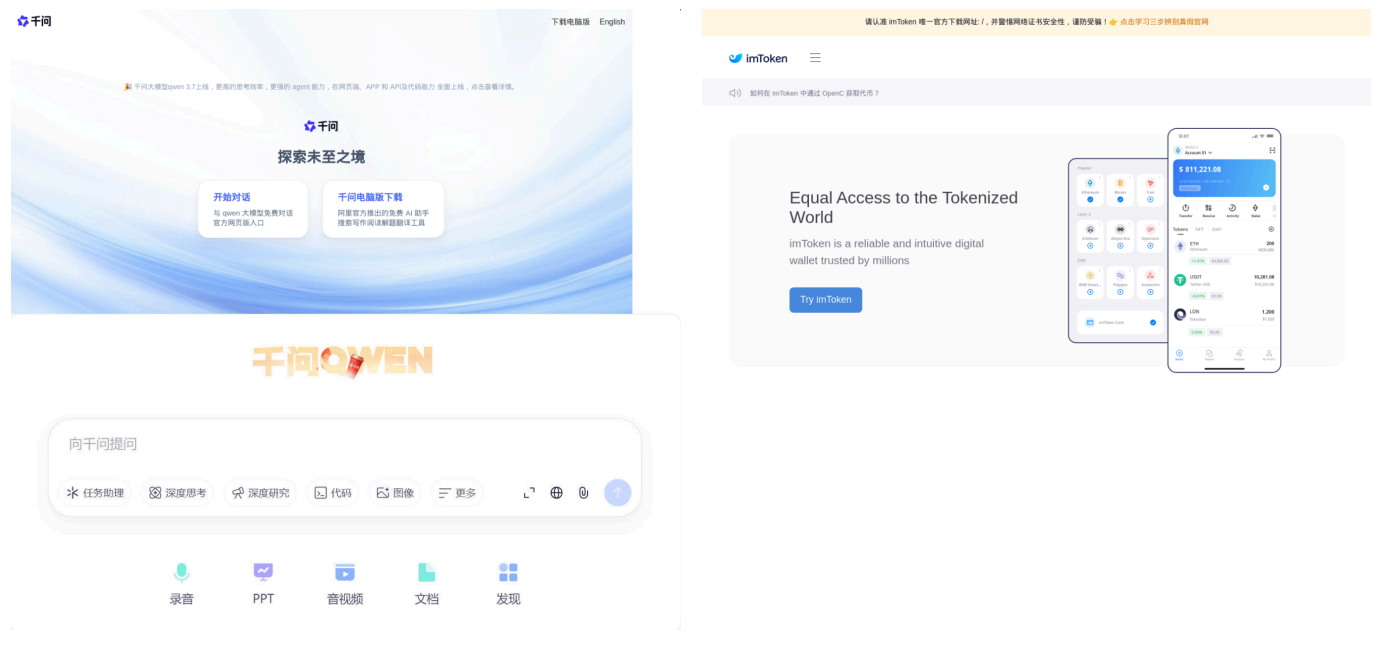
- **Targeting:** This operator specifically targets futures trading platforms, utilizing unique lures such as "奇货神器" (Rare Goods Magic Weapon - a futures trading decision platform).

Traffic Redirection and Analytics Tracking

Consistent with findings in Part II, the operators continue to leverage tracking pixels and redirect hubs to manage campaign traffic. Analysis identified the continued use of Google Analytics 4 (GA4) tags (e.g., G-3GR90RW2M5) embedded across crypto-wallet phishing sites (imToken, AiCoin) to monitor victim interaction.

Additionally, the operators utilize centralized redirect hubs. Domains such as osnenfae[.]xyz (impersonating the OpenClaw AI agent) do not host payloads directly. Instead, these domains function as traffic directors, routing victims to central hubs like opencnwl.com[.]cn where the actual payload delivery mechanisms are hosted. This compartmentalization of infrastructure complicates takedown efforts, as defenders must identify and block both the outer redirector ring and the inner payload hosting hubs.

Sample Sites Spoofing Malicious Software:



AnyDesk 远程访问

AnyWhere. AnyTime. Re-Imagine.

随时随地，高效远程办公

免费下载

BestVPN

功能 AI平台 套餐 使用条款

立即下载

全新升级 AI 模型库已更新

高速稳定的VPN服务
与全能AI助手

一站式平台，集成高速稳定的VPN服务与AI工具，电脑手机全平台通用，流畅丝滑体验，打破网络限制，释放AI无限潜能。

立即下载 了解更多

AI助手 已连接 GPT 5.4

运行正常

香港专线 HK-Q1

新加坡 SG-Premium

安全防护

当前速度 200+ Mbps

在线时长 99.9%

加密等级 AES-256

48ms

120ms

AI加速保护

安全加速 极速连接 全球覆盖

ICIBA

首页 AI工具箱 词典下载 其他

登录 注册

v2026.06 全新发布

金山词霸 AI 精准释义快速达

全网搜索·内容整合·实时展示
支持中英日韩法德等77种语言互译，AI 对话秒级响应，多端数据云端同步，让学习更高效。

免费下载 Windows 版

最新版本 v2026.6.10 · 大小 115 MB · 适用于 Win10/11

AI对话

自然流畅，秒级响应
十一位行业专家在线

已完成深度学习

AI翻译

沟通无界，秒语天成

检测为中文 - 英语

网页翻译

双选对译，沉浸式翻译操作

原文译文对照
右侧显示译文

AI帮写

深度润色，润色续写一润色

润色 续写 改写 重写

快橙 VPN

最佳好友券10%奖励 9.9 起 联系客服 立即下载

永久安全连接的
快橙 VPN！

立即注册，享受免费试用。体验极速稳定，畅享全球网络自由！

iOS 版下载 Windows 下载 Mac 版下载 安卓版下载

超过 100 万名满意用户每天信任我们

看看他们怎么说——加入我们，感受不一样的体验！

Hello Translator

Home Features Download Insights

中文 Contact us

Real-time AI translation software

Turn multilingual communication into real-time collaboration

Hello Translator is built for export sales, global support, cross-border commerce, remote meetings and document workflows. It supports real-time translation across 100+ languages on Windows, Mac, iOS and Android, covering webpage selection, document translation, voice subtitles and terminology consistency.

Download for Windows Explore features

30+ office scenarios · Up to 99% document layout retention · Common phrase response from 0.5s

更懂上下文的 AI 翻译工具

100+ Languages

0.5s Phrase response

99% Layout retention

4 Platform entries

v2rayN

下载及使用教程

首页 官网下载地址

v2rayN下载、快速入门教程

v2rayN 是 Windows、Linux 和 macOS 等系统代理软件 v2 客户端，功能强大，支持 VMess、VLESS、Trojan、Socks、Shadowsocks、Hysteria2、Tuic 等多种代理协议。

输入关键词，按回车搜索。

导航目录

- v2rayN 首页
- v2rayN 主界面预览
- v2rayN 官网下载
- v2rayN 安装教程
- v2rayN 安装目录文件
- v2rayN 图标状态说明
- 节点
 - 免费节点
 - 收费节点
 - 搭建节点
 - 添加服务器
 - 配置 V2Ray 节点
 - 配置 Shadowsocks 节点
 - 配置 Socks 节点
 - 配置 HTTP 节点
 - 配置 Trojan 节点
 - 配置 Hysteria2 节点
 - 配置 Tuic 节点
 - 配置 WireGuard 节点
- 订阅设置教程
- 选择节点
- 系统代理
- 路由模式

v2rayN 主界面预览

新版本开始新增跨平台支持 Linux 等系统，通过本文可快速掌握使用 v2rayN 配置代理协议进行国际网络加速访问。

v2rayN 主界面预览



首页

客户版下载

核心优势

套餐价格

限时优惠

安全中心

EN

立即解锁

值得信赖的
高速安全 VPN

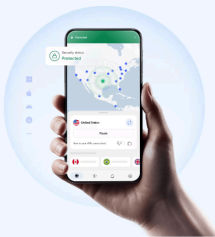
基于自研 NordLynx™ 协议，为全球用户提供军用级加密、经独立审计的零日志保护与极致流畅的网络体验。——一个账号，同时守护 10 台设备。

🟢 瑞典无日志审查认证

🟢 全球 60+ 国家服务覆盖

🕒 7x24 小时中文支持

立即开始保护



⚠️ 请遵守您在国家地区的法律法规。NordVPN 仅用于合法的网络安全隐私保护与安全访问用途。

NordVPN

保护隐私就是您的核心权益。NordVPN 以经审计过的零日志政策、全球最高安全等级全球服务器网络，为您提供真正可信的网络安全防护。



产品

客户版下载

核心优势

服务列表

NordLayer 企业版

支持

帮助中心

安装教程

联系客服

退款政策

公司

关于我们

算力网络

加入我们

媒体报道

法律与安全

隐私政策

服务协议

Cookie 设置

漏洞奖金计划

© 2020 NordVPN. All Rights Reserved.

55% 优惠

买 1 送 1 限时

VPN 续费



豆包



豆包

11

豆包 (Doubao) 是字节跳动推出的AI智能助手，提供AI对话、文案创作、翻译、情报支持等多种功能服务。基于强大的语言模型，为用户提供高效、智能的对话体验。

豆包网页版入口

豆包AI电脑版下载



AI智能对话与边缘边缘

基于千亿大模型1.6，支持持续对话深度可达250K超长上下文记忆。独创“边缘-中心”模式，将推理逻辑与实时数据深度融合，多轮动态检索全网信息，有效减少幻觉，日常决策场景信息准确率达92%以上。



文案创作与长文本生成

豆包支持10万级持续生成文本生成与图文联动创作，涵盖新闻文案、短视频脚本、学术论文、诗赋等。V5.0版本新增AI播客功能，可一键生成或插入播客节目；支持诗话、日记、文艺等多种指定风格创作。



多语言翻译与表达优化

提供高质量多语言互译服务，深度理解语境与文化习惯，输出符合本地表达习惯的翻译结果。支持商务、学术、技术等专业领域术语识别，以及实时语音翻译与全文润色优化。



知识问答与深度研究

覆盖科学、历史、文化、技术等领域，支持专业研究咨询。拒绝碎片化浅层知识问答，提供结构化方式呈现深度内容。



情感支持与语音陪伴

提供情感倾听、心理疏导与正能量鼓励，支持自然流畅的语音互动交流。作为AI伙伴，能够识别用户情绪状态，提供温暖的交流体验，帮助减轻压力与焦虑，适合恋爱陪伴与日常陪伴场景。



全平台覆盖与极速响应

豆包支持网页端、iOS/Android移动端、Windows/Mac桌面端及AI浏览器等多种交互场景。桌面端基于Chrome内核深度定制，支持跨设备同步、翻译与总结，响应速度快，服务稳定可靠，随时随地享受智能服务。



智能文档处理与AI伴读

支持PDF、Word、Excel、PPT等多种格式文件上传解析，自动提取要点，生成摘要与可视化导图。AI伴读功能可深度解析论文与财报，支持表格理解、数据可视化及多格式导出，大幅提升办公与学习效率。



多模态内容生成与编辑

集成文生图、图生图、文生视频（自然语言描述图）及生成式2D视频生成能力，支持文本到高质量2D短视频的一站式生成。新增拟声词与音乐创作，可定制化内容特性可实现内容风格与呈现形式。



代码编程与项目开发

支持多种编程语言代码生成、解释、调试优化，可一键接入GitHub仓库获取项目上下文。新增AI HTML实时预览、Python直接运行及完整项目开发生成能力；支持跨平台UI设计框架自动生成前端代码，并与Figma编辑器工具深度集成。



豆包

打开豆包一定有你

「豆包电脑版」
桌面版入口，工作学习场景的首选



Copyright © doubao

[illegible]



[首页](#)[应用介绍](#)[使用教程](#)[下载中心](#)[常见问题](#)[隐私协议](#)[机场推荐](#)

V2RayN

适用于Windows、Linux和macOS的跨平台代理客户端，支持 V2Ray、Xray、sing-box、VMess、VLESS、Trojan、Socks、Shadowsocks、Hysteria2、Tuic等多种协议，安全高效，易于配置。

[Windows 下载](#)[macOS 下载](#)[Linux 下载](#)

210M+

全球用户

99.9%

连接稳定性

50+

支持协议

24/7

技术支持

5

全平台支持

10000+

全球网络代理

闲鱼沟通提醒

为了保护您的闲鱼账号，请勿在聊天中发送 GPT、ChatGPT、OpenAI 等相关平台违禁词，否则您的闲鱼账号可能被封禁，相关消息闲鱼客服不予回复。

可以添加下方微信咨询，扫码自动通过。



扫码添加微信客服，自动通过
咨询问题、下单发货出问题均可联系

Close

Sales 1215 149.00 CNY Claude Claude Claude Pro官方直充月卡【充值账单可查 可开发票】 Auto fulfillment 官方直充 30天质保 账单可查 不质保封号 Sales 150 155.00 CNY	Sales 63 790.00 CNY Gemini Gemini Gemini Pro 年卡独享成品号 Manual delivery 专属账号 独立使用 稳定可靠 Sales 138 55.00 CNY	Sales 22 1390.00 CNY AI 会员 Apple 美国Apple ID 带密保可改密 Manual delivery 独享账号 带密保可改密 App Store专用 Sales 26 29.00 CNY	Sales 171 99.00 CNY Claude Max 5X Claude Claude Max 5X官方直充月卡【直充自己的账号 人工交付】 Manual delivery 官方直充 30天质保 账单可查 不质保封号 Sales 15 550.00 CNY
Claude Max 20X Claude Claude Claude Max 20X官方直充月卡【直充自己的账号 人工交付】	AI 会员 其它 订单补差价专用 AI	AI 会员 其它 开票专用 AI	



Malware Analysis: Modified Gh0stRAT Delivery

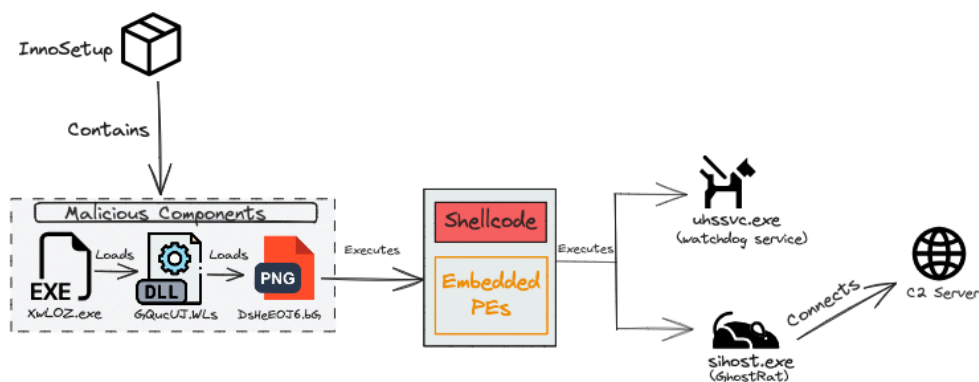


Figure 1: Gh0stRAT Malware Execution Chain

The majority of samples analyzed from this recent cluster point to an obfuscated variant of Gh0stRAT. The infection chain utilizes a multi-stage dropper process involving bloated installers, steganography, and compiler-based obfuscation. For the samples reviewed in this campaign, the technical execution chain, obfuscation methods, and final payload structure are nearly identical regardless of the lures.

Inno Setup Bundles

Validating observations from Part IV, the initial payloads are Inno Setup executables artificially padded to sizes ranging from 117MB to over 147MB. The padding is an anti-analysis technique designed to exceed the file size limits of public sandboxes, and security gateways, which are typically around 100-200 MB and subsequently deter automated analysis.

Extracting the Inno Setup files reveals legitimate, digitally signed application binaries bundled with malicious components. In several of the applications observed, the file bundles contain dozens of legitimate applications that serve no purpose other than to increase the file size and the overall application's legitimacy. The setup script utilizes the hidewizard nowait directive, which presents the user with a standard installation GUI while the malicious loader executes silently in the background.

Following the installation routine, execution passes to a 64-bit loader (e.g., XwLOZ.exe). Code analysis of the loader indicates it is heavily obfuscated utilizing OLLVM (Obfuscator-LLVM) and VMProtect/Themida-style protections to complicate control flow analysis. The loader's primary function is to map a companion DLL (e.g., GQucUJ.WLs) into memory and execute its various exports.

```

000180131F65
000180131F68
000180131F68
000180131F68      blmcIUGLM      public blmcIUGLM
000180131F68      proc near          ; DATA XREF: .rdata:off_1804B20D8+o
000180131F68
000180131F68      var_108          = qword ptr -108h
000180131F68      var_78          = qword ptr -78h
000180131F68      var_48          = qword ptr -48h
000180131F68
000180131F68      ; FUNCTION CHUNK AT .text:00000001801324B9 SIZE 00000005 BYTES
000180131F68      ; FUNCTION CHUNK AT .text:00000001801324C3 SIZE 00000636 BYTES
000180131F68      ; FUNCTION CHUNK AT .text:00000001801324FF SIZE 00000022 BYTES
000180131F68
000180131F68      xor             r11d, 0A9h
000180131F72      cmp             dword ptr cs:xmmword_180472DD0, 329EC5E3h
000180131F7C      mov             r8d, cs:dword_18047CAF5
000180131F83      test            r8d, 40h
000180131F8A      mov             cx, word ptr cs:xmmword_18049404E
000180131F91      db              66h, 66h, 66h, 66h, 66h, 66h
000180131F91      nop             word ptr [rax+rax+00000000h]
000180131FA0      movsx           r11d, byte ptr cs:qword_1804711B2
000180131FA8      mov             rdx, (offset dword_18044EF81+1)
000180131FB2      mov             r10, 396Ch
000180131FB9      xor             rcx, r10
000180131FBC      mov             r11, 1FE0h
000180131FC3      xor             r8, r11
000180131FC6      ror             rcx, 2
000180131FCA      movdqu          xmm7, xmmword ptr [rdx]
000180131FCE      pxor            xmm7, xmm7
000180131FD2      mov             r11, offset unk_180460D2F
000180131FDC      and             r10, 0F2B5h
000180131FE3      test            r8, r9
000180131FE6      and             r9, 0DF1Fh
000180131FED      cmp             dword ptr [r11], 0FB44h
000180131FF4      setnle          dl
000180131FF7      lea             r9, unk_180477FAA
000180131FFE      and             rax, 32D5h
000180132004      shl             rcx, 1

```

Figure 2: Code Obfuscation Throughout the Execution Chain

XwLOZ.exe						
Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
0004A092	N/A	00049A98	00049A9C	00049AA0	00049AA4	00049AA8
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
GQucUJ.WLs	97	0004B510	00000000	00000000	0004BA92	0003A000

OFTs	FTs (IAT)	Hint	Name
00049B48	00038638	00049F0C	00049F0E
Qword	Qword	Word	szAnsi
000000000004BCFC	000000000004BCFC	05C4	vXQPnlasrbdvzAe
000000000004C0BC	000000000004C0BC	064A	JwdyEZSBvYvvh
000000000004C0B0	000000000004C0B0	0375	imlVyThj
000000000004C0A0	000000000004C0A0	057F	pzqZJtZNOtwg
000000000004C08E	000000000004C08E	02D4	pctnJhHYnElpUG
000000000004C074	000000000004C074	0546	JPRDDxalpVYPMbCYpxqLWT
000000000004C05A	000000000004C05A	01C4	AmvrAlnYUslejNthOOaJJZ
000000000004B90C	000000000004B90C	0467	WHgFOaizJGwfZXd
000000000004B91E	000000000004B91E	01A0	oVTqaaOanNtgKhqO
000000000004B932	000000000004B932	064B	QPdnNBdRB
000000000004B93E	000000000004B93E	00DA	htzQuZZIldU
000000000004B94C	000000000004B94C	027D	WZocDHuhBhPe
000000000004B95C	000000000004B95C	0244	mRnoopADXqfQKOHtvKZ
000000000004B972	000000000004B972	0094	KHgJRMKe/CN
000000000004B980	000000000004B980	01B2	wNUSJzbtthuWffG

Figure 3: Obfuscated Export Names

Once mapped, the DLL searches the local file system for a specific data file dropped during the initial installation phase (e.g., DsHeEOJ6.bG). All DLLs analyzed share the same obfuscation compiler as the EXE loader component.

Payload Decryption

The DsHeEOJ6.bG file is structured to masquerade as an 800x600 PNG image, utilizing the standard %PNG (47 4e 50 89) magic bytes in its header. The DLL allocates a ~10MB memory segment with Read-Write (RW) permissions, removes the PNG headers, and decrypts the underlying payload. Following decryption, it uses VirtualProtect to modify the memory permissions to Read-Write-Execute (RWE) and redirects execution to the decrypted shellcode.

The decrypted shellcode is based on an sRDI (Reflective DLL Injection) implementation and uses the RtlDecompressBuffer API to unpack an embedded PE file into a new memory region.

```

000000001B1C loc_1B1C: ; CODE XREF: sub_47B+1690↑j
000000001B1C lea rax, [rbp+1F0h]
000000001B23 add rax, 0A7h
000000001B29 mov [rbp-8], rax
000000001B2D mov byte ptr [rbp+208h], 75h ; 'u'
000000001B34 mov byte ptr [rbp+255h], 70h ; '}'
000000001B38 mov byte ptr [rbp+288h], 5Ah ; 'Z'
000000001B42 mov byte ptr [rbp+2A2h], 73h ; 's'
000000001B49 mov byte ptr [rbp+1FDh], 78h ; 'x'
000000001B50 mov byte ptr [rbp+258h], 6Ah ; 'j'
000000001B57 mov byte ptr [rbp+2A0h], 72h ; 'r'
000000001B5E mov byte ptr [rbp+28Fh], 69h ; 'i'
000000001B65 mov byte ptr [rbp+270h], 60h ; 'm'
000000001B6C mov byte ptr [rbp+20Eh], 68h ; 'h'
000000001B73 mov byte ptr [rbp+264h], 6Ch ; 'l'
000000001B7A mov byte ptr [rbp+206h], 63h ; 'c'
000000001B81 mov byte ptr [rbp+2AAh], 0
000000001B88 mov byte ptr [rbp+1F3h], 61h ; 'a'
000000001B8F mov byte ptr [rbp+24Eh], 48h ; 'K'
000000001B96 mov byte ptr [rbp+289h], 6Ah ; 'j'
000000001B9D mov byte ptr [rbp+21Dh], 5Eh ; '^'
000000001BA4 mov byte ptr [rbp+22Eh], 37h ; '7'
000000001BAB mov byte ptr [rbp+242h], 71h ; 'q'
000000001BB2 mov byte ptr [rbp+1F1h], 24h ; '$'
000000001BB9 mov byte ptr [rbp+24Ch], 70h ; 'p'
000000001BC0 mov byte ptr [rbp+27Dh], 58h ; '['
000000001BC7 mov byte ptr [rbp+2ABh], 28h ; '+'
000000001BCE mov byte ptr [rbp+20Ch], 44h ; 'D'
000000001BD5 mov byte ptr [rbp+1FBh], 28h ; '+'
000000001BDC mov byte ptr [rbp+224h], 61h ; 'a'
000000001BE3 mov byte ptr [rbp+267h], 2Dh ; '-'
000000001BEA mov byte ptr [rbp+280h], 48h ; 'K'
000000001BF1 mov byte ptr [rbp+29Fh], 70h ; 'p'
000000001BF8 mov byte ptr [rbp+21Eh], 73h ; 's'
000000001BFF mov byte ptr [rbp+238h], 5Fh ; '_'
000000001C06 mov byte ptr [rbp+22Dh], 46h ; 'F'
000000001C0D mov byte ptr [rbp+283h], 65h ; 'e'
000000001C14 mov byte ptr [rbp+28Eh], 37h ; '7'
000000001C1B mov byte ptr [rbp+210h], 32h ; '2'

```

Figure 4: sRDI Style Shellcode

The shellcode injects the final unpacked DLL payload as a headless PE into a separate, legitimate system process. In observed instances, the malware targets sihost.exe (Shell Infrastructure Host). By executing exclusively within the context of a trusted system process, the malware blends its subsequent network and file operations with normal operating system behavior. Additionally a lightweight watchdog DLL is injected into a separate system process such as uhssvc.exe (Microsoft Update Health Tools). It is worth noting that the DLL payload uses the same obfuscation compiler as the loader EXE and DLL, but the watchdog DLL does not.

To ensure continuous execution of the injected Gh0stRAT payload, the malware establishes a local watchdog mechanism. It drops a batch file into the C:\Windows\ directory utilizing a randomized 8-character filename (e.g., C:\Windows<random_8_chars>.bat). The contents of this script are obfuscated, but de-obfuscation reveals a continuous monitoring loop utilizing system utilities:

```

@echo off
:9CernBcv
tasklist /fi "PID eq 1476" | findstr /i "1476" > nul
if errorlevel 1 (
    sc start "ITLHxDt1PhM0sB"
    exit
)
timeout /t 10
goto 9CernBcv

```

Figure 5: Deobfuscated Batch Script

If the tasklist command returns an error, indicating the injected uhssvc.exe process has been terminated, the batch script issues an sc start command to restart the obfuscated malicious service, effectively functioning as a persistent watchdog for the main Gh0stRAT process.

To facilitate execution within protected system boundaries and establish service-based persistence, the payload first performs a User Account Control (UAC) bypass. It achieves this by abusing the ICMLuaUtil elevated COM interface (CLSID {3E5FC7F9-9A51-4367-9063-A120244FBEC7}). This allows the malware to silently elevate its privileges without prompting the user.

Figure 6: UAC Bypass using ICMLuaUtil COM Interface

Prior to initiating network communications, the injected payload reads its configuration from a hardcoded path: C:\ProgramData\C46EEF09DFB549819FACDBF1C9081293\config.ini.

[illegible]

Figure 7: Decrypted Configuration File

Analysis of the unpacked payload confirms the core capabilities of Gh0stRAT. Extracted API calls show standard GDI and GDI+ functions (GdiCreateBitmapFromHBITMAP, BitBlt, StretchBlt) for screen capture, as well as SetWindowsHookExW and GetAsyncKeyState for keylogging. The payload utilizes WMI queries (ROOT\CIMV2) for system enumeration.

The payload also contains strings indicating targeted data collection and evasion. It queries specific paths for WeChat, Telegram, and regional browsers (e.g., %s\360se6\User Data\Default, NoLogWechat, NoLogTG). Additionally, the code checks for the presence of 360Hvm64.sys, a component of Qihoo 360 security software, indicating specific anti-analysis measures for Chinese operating systems.

Code analysis reveals class structures such as CTcpPackClientT, IPackClient, and CTcpClient, indicating the use of hp-worker (High-Performance Socket), an IOCP-based C++ networking library. This aligns with past observed behavior of other Gh0stRAT variants, which also utilize updated C++ network libraries to manage asynchronous data streams.

```
00000000 b1 01 00 00 48 8d 64 24 b1 01 00 00 08 05 00 00 ....H.d$ .....
00000010 12 ef 47 df 16 36 e4 cc 5b e5 34 ac ae 66 82 51 ..G..6.. [.4..f.Q
00000020 81 9e f2 45 a6 39 8e 06 68 b2 a9 ce 35 de 94 0d ...E.9.. h...5...
00000030 f8 14 a1 a5 03 db 66 fc 57 59 e9 9a e6 c2 9e 7e .....f. WY.....~
00000040 07 47 9c 30 6b 31 b9 40 d1 34 c8 99 77 02 b6 82 .G.0k1.@ .4..w...
00000050 e0 18 06 f8 fe 9e 75 dc c9 67 a6 95 08 ea 31 b5 .....u. .g....1.
00000060 6d 6d 91 a4 d7 e3 ac 03 58 08 00 e8 92 cd 19 d5 mm..... X.....
00000070 81 90 d2 16 f5 79 47 f7 9c 53 bb d3 02 c3 7f d1 .....yG. .S.....
00000080 2d 12 da 12 b9 3b 27 b6 71 d6 2f c6 26 30 f7 0e ~....;' q./.&0..
00000090 ae 61 84 da b0 43 4f 8c 9f df 4f 56 d3 5a 34 b1 .a...CO. ..OV.Z4.
000000A0 4f 2d 34 66 c3 d1 e0 91 4d ff 2e c1 b1 3c c9 c5 0-4f.... M....<..
000000B0 d0 17 01 10 42 1d 72 c2 75 a7 50 d6 8d e6 e0 f4 ....B.r. u.P.....
000000C0 b7 e9 40 21 23 d4 64 c2 e7 d4 95 90 0f 02 5a 44 ..@!#.d. ....ZD
000000D0 b8 20 5d e9 13 3f f1 94 46 f2 58 62 72 00 a6 28 . ]..?. F.Xbr..(
000000E0 ff c2 4c 84 5d 6c 6e 3b 9e de 44 3a d6 bc 8b 08 ..L.]ln; .D:....
000000F0 3a 44 2b c8 1f 79 bc b6 7d b0 fb 2e 1d 61 cc 5a :D+..y.. }....A.Z
00000100 89 2d 87 83 f2 72 19 57 78 98 10 2a e6 a9 4a 8a ..-...r.W x...*.J.
00000110 54 79 ad 10 12 4c da d0 5b fd ae b0 e5 af 15 5f Ty...L.. [.....
00000120 bf 25 b1 38 c6 37 74 25 52 dd 01 6e 1f a5 0c 46 .%.8.7t% R..n...F
00000130 df 07 60 c5 16 8c a5 50 88 e3 e2 e0 5b 62 d4 be ..`....P ....[b..
00000140 2d bc 01 7d 83 18 b7 fa 2c 6b 2c 93 a9 df f1 74 -. ).... ,k,...t
00000150 54 71 cb 36 d9 0c 03 2f 5e 3c cd d7 cb d2 d4 96 Tq.6.../ ^<.....
00000160 81 18 0e 55 bb 4c 91 4c 75 65 f4 ae 94 e2 ab 52 ...U.L.L ue....R
00000170 c1 9c 6b 8d d4 d2 9f 00 f5 98 5a 82 9f fa 50 46 ..k..... .Z...PF
00000180 f4 24 16 46 a7 f3 9f a0 38 29 ca bc e1 3f 22 ee .$.F.... 8)...?".
00000190 fa 50 c3 66 74 5c 7b c9 b7 1d 1b c1 21 47 70 0e .P.ft\{. ....!6p.
000001A0 ba 36 72 c5 de 1c cc c6 b8 30 53 28 bf ea 44 f5 .6r..... .0S(..D.
000001B0 b8 53 78 d1 cc ..Sx...
```

Figure 8: Network Data Stream for Gh0stRAT

Alternative Gh0stRAT Variant:

While the OLLVM/Inno Setup chain is the most prevalent in this cluster, analysis of AiCoin lures (e.g., Alcosin_x64.exe) revealed a distinct, secondary infection chain.

Like the primary variant, the initial installer is padded (~163MB); however, it utilizes an Advanced Installer package rather than Inno Setup. Execution relies on a DLL sideloading against a legitimate dropped executable (e.g., BrowserProtect.exe). The malicious DLL (DataState.dll) is 20MB in size and, notably, is signed with a valid Authenticode certificate issued to a Chinese company ("Shanxi 90s Catering Management Co., Ltd."). The use of a valid, stolen, or otherwise fraudulently obtained certificate allows the payload to bypass initial Mark-of-the-Web (MoTW) and endpoint trust checks.

This alternative chain lacks the compiler-level obfuscation seen in the primary variant. An injected DLL decrypts the final embedded payload, which matches publicly available Gh0stRAT code.

Indicators of Compromise (IoCs)

Inno Setup Installer Cluster

The majority of these samples share a common pattern: 32-bit Inno Setup installers built with a Delphi (XE2–XE6) compiler and Turbo Linker. Each drops 3 embedded files and beacons to 2 C2 addresses (a domain + an IP:port pair).

Obfuscated Gh0stRAT Variant

Installer Name	Installer SHA256	EXE Loader Name	
cnkuai_miao_x64_6lt81.exe	51385d63916a23480e38c1db5ec47608f31db3b3c7f1ebb0c5b207565b18a00f	rzjP0k.exe	dc98290d49
cnv2_raynx64_winsisuxe.exe	0796130f37db020dc1f3619391c7c750fa4527b84ef2eb7a76c69c467ad80897	bL5l.exe	b4fd12c8ae
flyfastccpn_x64.exe	57f25d75f47ccdcb0a2be98d0fb4d081d9f7893880bf0050d6462c3f652bb2cb	XrgV.exe	f1c28e53cf
kuaichenfast_x64winsis.exe	8b7d9ec5929f77617dd03cded74de742c98ea0788ebb5b3e2725c741bbb2581b	9FAZEI.exe	f1c28e53cf
letsSetup.exe	eac7b98e6fbb50b9cf72910897433d500b0e2350561d2463db5014f559146f8d	a1Ow.exe	937f6a7e86
Meta_trader_4.exe	9e2a3a468bdf99c3428bd31c29aba4c99e028ca6bdfe2e9f9657a27ff2c5f522	Kal5eivaAh.exe	595ad8fcec
Metatrader5.exe	af257229403128b1a13dc6f45a674382b5faeca693a973c25b3a2d82e44b8260	NlixJzDM.exe	7b7c25e65
sys_HR_allapp_x64.exe_EANej.exe	16f1591190994c0d38e184e57d0d9fca5f004e3eeb80934244c5472861c66692	sOeFm.exe	d424ab3b2

Installer Name	Installer SHA256	EXE Loader Name	
xia0_huojianv2x64.exe	1cca336c70e0cbf64bc0805cfc707c956a132ec2e43e24d34ff7126467d7fd2f	ulaq8Q.exe	2f26cb96f3
Aicoins_setup.exe	d3db6d0f7062b00d4abbbcb0471d3c11172389d0154ab977442404487d3746d74	NlixJzDM.exe	7b7c25e65
pron_tonx64_8Ya4.exe	a01b2afd5fda05bf5ee2b80fbb460e064c7fab8bb96653545d0415eb8ad6d57e	yD4C7.exe	224913581
doubao-AI.exe	e4aec3d3f546aa6c969337202a0899807109924e92587dc4eb597066d0d2ea26	XwLOZ.exe (confirmed role)	18abba991

Gh0stRAT Variant v2

File Name	Type	Role	SHA256	C2
Alcosin_x64.exe	EXE	Main installer (spoofed "aicoins" branding)	704ba3eb10f04f053f150e7eca60bb90931a7a0af80f571359424ad0929a4dbd	abc[.]yu32k1[.]com
6840000.dll	DLL	Gh0stRAT payload injected into the legitimate BrowserProtect process	0d44f92753f56ecb313c0271757f1212281d30f0a341a1e55329ce86f8573776	(uses parent's C2 channel)
DataState.dll	DLL	Gh0stRAT loader	cbe0e7173f3c5265ffe79951f6e456df020fd0add02bb37cd622827e5824ae2	(uses parent's C2 channel)

Payload Delivery Domains and Lure Domains are available in the DTI IoC Library on [GitHub](#).