

Operation Phnom Penh : 银狐Ghost分发商针对特定目标投递MODBEACON特马

 secrss.com/articles/91908

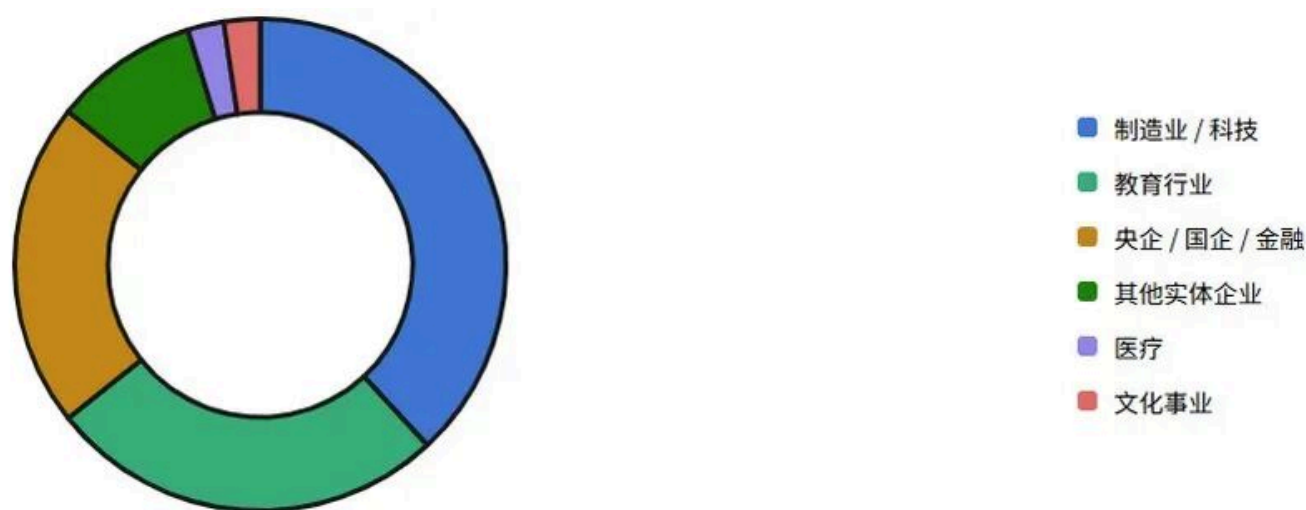
病毒木马 奇安信威胁情报中心 2026-07-06

2026 年 6 月中旬，奇安信威胁情报中心红雨滴团队的私有情报 AI 生产流程检测到一伙 ghost 分发商在特定目标下发一款由 Rust 编写、高度模块化的特种木马；基于其特殊字符串特征，我们将该木马命名为 MODBEACON。

背景

"银狐/UTG-Q-1000"长期被视作低水平、高活跃度、以 SEO 为渠道投递仿冒软件的黑产的代名词，但其背后实为多个分发商构成的、类似境外 Malware-as-a-Service (MaaS) 的组织架构。这些分发商借助 ghost 变种、winos (ValleyRat) 等木马家族，在亚洲地区借仿冒软件安装包的 SEO 投放开展活动。2025 年我们反制了其中一个分发商[1]，其远控目的仅限于在 IM 群聊中投递诈骗链接，并不涉及窃密与政治动机。

2026 年 6 月中旬，奇安信威胁情报中心红雨滴团队的私有情报 AI 生产流程检测到一伙 ghost 分发商在特定目标下发一款由 Rust 编写、高度模块化的特种木马；基于其特殊字符串特征，我们将该木马命名为 MODBEACON。其受害目标呈现高度定制化，涉及科技、教育、国企等领域：



MODBEACON 请求的 C2 域名托管于 Amazon CDN 与 Cloudflare CDN。该木马是一款专业且私有的 C2 框架：加载器与 beacon 分离、配置可注入、beacon 采用插件化架构 (native-v3 插件，带 entry/init/fini RVA)、gRPC 隧道流式通信，整体工程化程度较高。其核心亮点在于复用开源抗审查代理框架 (Xray/V2Ray) 的传输层作为 C2 信道

(xray.transport.internet.grpc.encoding.GRPCService/Tun) ——该协议本用于将

VMess/VLESS/Trojan 等代理协议的数据流伪装为一次普通的 gRPC 双向流式调用，使流量在网络层呈现为标准的 HTTP/2 + gRPC 请求，从而规避基于流量特征的封锁与审查。

在后续对这伙ghost分发商的溯源中，我们进一步发现其还针对柬埔寨的博彩行业展开"黑吃黑"活动，投递的诱饵命名风格与当年我们披露金眼狗[2]、金指狗[3]时颇为相似。结合其按特定行业筛选目标、并分权限下发MODBEACON特马的行为特征，该分发商的动机已难以单纯以经济目的加以解释，背后可能存在外包性质的政治意图，这引起了我们对该分发商的浓厚兴趣

天擎“六合”高级威胁防御引擎已经可以对MODBEACON stage shellcode进行拦截：



银狐ghost分发商溯源

涉及投递MODBEACON特马的ghost C2如下：

www.nd9c887r.com

www.damaix9k.com

vaeth.cn

182.16.88.242

kkuu8899.org

基于我们现场排查的下载记录定位到上层的仿冒域名和下载链接：

SEO活动仿冒域名

cn-mumu.com.cn

下载链接

https://asd268668.oss-ap-southeast-1.aliyuncs.com/MeiqiWintsetup_x64.zip



基于元数据扩线发现这批仿冒域名最早于2025年9月份开始活跃,涉及的仿冒域名如下：

- 1 sogou-xp.com↓
- 2 sogou-pv.top↓
- 3 sogou-xp.top↓
- 4 sosou-win.top↓
- 5 lightninguxvpn.com.cn↓
- 6 xy-kuaimiao.com.cn↓
- 7 win-letstalk.com.cn↓
- 8 cn-mumu.com.cn↓
- 9 win-yifanyi.com.cn↓
- 10 winmumu.com.cn↓
- 11 i4as-cn.com.cn↓
- 12 lightningxanx.com.cn↓
- 13 cnmumu.cn↓
- 14 kuaimiao-kv.com.cn↓
- 15 kuaimiao-vs.com.cn↓
- 16 lightninshanlian.com.cn↓

基于VT数据也能观察到该分发商的日常活动主要是仿冒国内流行软件，大量政企中招。

2026-04-18	15 / 71	Win32 EXE	Szc_Wps_Office_v2.0_x64_win.exe
2026-05-07	23 / 68	Win32 EXE	Szc_OpenClaw_v1.0_x64_win.zip.exe
2026-05-17	31 / 72	Win32 EXE	ToDesk_3.6.8.8_x64_win.exe
2026-04-18	32 / 70	Win32 EXE	infected/Szc_Wps_Office_x64_win.exe
2026-03-30	12 / 70	Win32 EXE	sogou_pinyin_x64_v10_win.exe
2026-05-28	46 / 72	Win32 EXE	Doubao_online_installer_2.0_win.exe
2026-05-02	22 / 67	Win32 EXE	TencentMeeting_v2.0_x64_win.exe
2026-05-23	41 / 68	ZIP	QQHong_7a870310f6797dee446e9fa8ef38f85e
2026-04-04	35 / 70	Win32 EXE	0EE09A1EDE91D0C8AC5BF7BA3E94919F3738B8FBD37C0F6B594243059A64E98B.exe
2026-04-12	5 / 66	ZIP	10dc4de89f0786ad98600b60e390bc629f4cc0b0f50bb59a10fa0da106a1e5f0
2026-04-26	26 / 70	Win32 EXE	sogoupinyin_x64_v1.1_win.exe
2026-04-12	9 / 70	Win32 EXE	sogoupinyin_x64_v2.0_win.exe
2026-04-04	21 / 71	Win32 EXE	C:\Windows\navhw9fj0.exe
2026-04-08	13 / 64	Win32 EXE	sogoupinyin_x64_v2.0_win.exe

基于MODBEACON的域名我们关联到了另一批ghost诱饵，文件名多以柬埔寨打击诈骗园区、治安事件为噱头，极具时效性与猎奇性：Poipet（波贝，边境诈骗重镇）、Sihanoukville（西哈努克港）、Phnom Penh（金边）还有对应的高棉语版本。

1.https://api.skystackservice.com

偏移：0x79708

代码引用：0x32160

2.https://api.fast-cloud-node.com

偏移：0x79727

代码引用：0x32182、0x5ab99，另有 0x0dc5a 附近间接引用命中

Agent Token / Hash

b68e2067cc88985339154ef7b9674fa1fe958039ce15a8820195217495cded7994d660f181fe1
367337ac8d6b372473c596be3f40ee989007bad57c2736be017

长度：128 hex chars

位置：紧跟两个 HTTPS endpoint 之后，起始约 0x79746

互斥体/环境变量

Global\\CBP.QZKVM.Exe.Mutex，偏移 0x7159c

CBPUserSvc，偏移 0x71578

APP_RUNTIME，偏移 0x71582

APP_EXE_PATH，偏移 0x7158c

MODBEACON_AGENT_TOKEN_PATCH_V1，偏移 0x7fc98

协议/服务名

/xray.transport.internet.grpc.encoding.GRPCService/Tun

xray.transport.internet.grpc.encoding.GRPCService

Tun

x-agent-token

application/grpc

grpc-status

grpc-message

grpc-timeout

控制流概览

初始化与单实例

在 0x149a、0x17ce、0x170a 附近可见对 CBPUserSvc、APP_RUNTIME、Global\\CBP.QZKVM.Exe.Mutex 的 RIP 相对引用。导入区包含 CreateMutexW、GetEnvironmentVariableW、SetEnvironmentVariableW、GetModuleFileNameW 等 API。推测初始化流程包括：

1. 读取运行环境变量和程序路径。
2. 创建 Global\\CBP.QZKVM.Exe.Mutex 防止多实例。
3. 通过 Windows API 初始化运行时、线程和网络组件。

C2 配置选择与 token patch

0x32120 附近函数集中引用默认 C2 和 token patch 字符串：

0x32160 使用 RIP 相对地址加载 https://api.skystackservice.com 附近配置。

0x32182 加载 https://api.fast-cloud-node.com 附近配置。

0x321b8 引用 MODBEACON_AGENT_TOKEN_PATCH_V1，后续有 0x200 字节循环检查逻辑，疑似读取/覆盖内置 agent token。

该函数栈帧较大，符合 Rust 配置构造、字符串对象和错误处理路径的形态。结合字符串 parse grpc endpoint、connect grpc endpoint、invalid agent token metadata，可判断其负责解析 endpoint、构建 token metadata，并选择可用 C2。

gRPC/TLS 通信流程

字符串池在 0x794c8 起给出主流程状态文本：

parse grpc endpoint

connect grpc endpoint

build native TLS connector

queue hello

```
invalid agent token metadata  
  
x-agent-token  
  
open grpc tun stream  
  
read hello ack  
  
read server frame  
  
grpc response stream ended  
  
heartbeat timeout  
  
grpc response stream ended before hello ack
```

这说明通信流程为：

1. 解析内置 HTTPS C2。
2. 建立 native TLS connector。
3. 使用 gRPC Tun 服务打开双向隧道。
4. 在 metadata 中携带 x-agent-token。
5. 发送 hello，等待 HelloAck。
6. 维持 heartbeat。
7. 接收 server frame 并分发命令。
8. 上传状态刷新和命令执行结果。

导入区同时出现 WSASStartup、WSASocketW、connect、send、recv、shutdown、CertGetCertificateChain、CertVerifyCertificateChainPolicy、InitializeSecurityContextW、EncryptMessage、DecryptMessage，支持上述网络/TLS 判断。

主机指纹采集

0x465c5 附近引用 SOFTWARE\\Microsoft\\Cryptography\\MachineGuid，字符串池还包含：

COMPUTERNAME

HOSTNAME

USERNAME

USERLOGNAME

SystemRoot

windir

SystemDrive

platform

system-disk

host-user

windows-system-volume:

推测该阶段采集主机唯一标识、用户名、主机名、系统目录和磁盘信息，用于注册 agent、生成上线状态或环境标签。

命令与插件分发

protobuf/gRPC 语义字符串位于 0x7b600+：

Command

command_id

HelloAck

Heartbeat

ConfigSync

LoadPlugin

UnloadPlugin

StatusRefresh

PluginSessionFrame

artifact_bytes

artifact_format

sha256

target

source_flag

0x44003 附近多处引用 PluginSessionFrame，0x4475f 附近多处引用 LoadPlugin 相关枚举/字段，说明服务端 frame 被解析后进入不同命令处理分支。

native-v3 内存插件加载

字符串池 0x79900-0x7a758 包含完整 native-v3 loader 错误路径：

load plugin artifact

load native-v3 plugin module

plugin loaded in memory

plugin reloaded in memory

plugin unloaded

native-v3 plugin on_load failed

native-v3 plugin on_session is missing

artifact target architecture does not match this agent

segment protection failed

relocation overflow

entry rva is not executable

segment cannot be writable and executable

这表明样本支持从 C2 下发 native-v3 格式插件，在内存中分配镜像、校验架构、映射 segment、应用 relocation、设置内存保护并调用插件入口/会话回调。该能力可用于后续按需扩展窃密、横向移动、代理转发或其他载荷。

总结

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信NGSOC、奇安信态势感知等，都已经支持对

此类攻击的精确检测。



IOC

MODBEACON-MD5:

13aff4f82171d42e7f0a72dc96346c45
f6c69d8026d2114e5322f06f69471a6c
9913b09fddbe47d4459c1ae0aa8c4953
e32797efc17c8a9a663f6f0e64fcfa08

MODBEACON C2:

skystackservice.com
fast-cloud-node.com
ghost C2:
www.nd9c887r.com
www.damaix9k.com

vaeth.cn

182.16.88.242:22

kkuu8899.org

参考链接

[1] https://mp.weixin.qq.com/s/BUDSvqc_DhBNad71kl2VuA

[2] [https://ti.qianxin.com/blog/articles/operation-dragon-breath-\(apt-q-27\)-dimensionality-reduction-blow-to-the-gambling-industry/](https://ti.qianxin.com/blog/articles/operation-dragon-breath-(apt-q-27)-dimensionality-reduction-blow-to-the-gambling-industry/)

[3] <https://www.secrss.com/articles/27069>

声明：本文来自奇安信威胁情报中心，版权归作者所有。文章内容仅代表作者独立观点，不代表安全内参立场，转载目的在于传递更多信息。如有侵权，请联系 anquanneican@163.com。

病毒木马

相关资讯

- **[UTG-Q-1000团伙近期仿冒Zinst等软件分发银狐木马新变种](#)**

[病毒木马](#) [奇安信威胁情报中心](#) 21小时前

[近期奇安信威胁情报中心通过云沙箱捕获到多个UTG-Q-1000黑产团伙的新银狐木马变种，这批新变种从2026年6月初起开始投递使用，根据奇安信威胁情报中心的检测，该系列变种近...](#)

- **[国家计算机病毒应急处理中心：关于仿冒教育培训类APP的手机木马病毒的预警报告](#)**

[教育科研](#) [国家计算机病毒应急处理中心](#) 2026-07-10

[该恶意APP为金融盗窃类手机木马病毒的新变种，具有拦截用户短信、窃取通讯录、窃取手机密码、开启摄像头、录屏、录音等侵犯公民个人信息的恶意功能，并进一步通过短信和社...](#)

- **[工信部：关于防范Remcos恶意软件新变种的风险提示](#)**

[病毒木马](#) [网络安全威胁和漏洞信息共享平台](#) 2026-06-30

[一种Remcos新型变种正在活跃传播，其利用DonutLoader内存加载技术进行投放。](#)