

360AI安全专家独立发现新型僵尸网络-安全资讯-360官网

 news.safe.360.cn/n/13046.html



- 2026-08-25 17:37:45
- 我要分享

近年来，人工智能快速发展，正在深刻改变生产、生活和网络空间。与此同时，AI能力也逐渐被攻击者用于恶意软件开发、自动化攻击和对抗分析，网络攻击正呈现出更加智能化、自动化的新趋势。在此背景下，360 AI安全分析专家持续探索AI赋能安全实战，独立发现新型僵尸网络，为应对AI时代不断演变的网络安全风险提供了新的技术支撑。



AI追捕缉拿AI大盗

近日，360 AI安全分析专家在对银狐木马的控制服务器（C2）进行日常巡检排查过程中，自主捕获并协同处置了一个全新的僵尸网络家族。AI安全专家自主对其进行了数据挖掘，该僵尸网络自今年7月出现以来，对全球范围内至少1311台服务器发动了涵盖13种网络协议的密码喷射攻击，被感染设备覆盖全球超20个国家和地区。而如此穷凶极恶的僵尸网络此前却从未被曝光，AI安全专家研判认为，该僵尸网络仍处于早期建设阶段。根据其用于伪装的样本名称（Endpoint），我们暂且将其定名为“端点僵尸网络”。

根据溯源分析，本次巡检发现的攻击事件也是一个由AI驱动的僵尸网络发起，它会攻击银狐木马C2服务器（也正是这一特征指标让其清晰地暴露在我们的AI安全专家的视野中）。端点僵尸网络在部署过程中会伪装成curl工具或EDR客户端，其内部数据采用AES算法完全自主加密，具有极高隐蔽性。同时，其还具备多系统支持及完善的自动传播能力，功能非常全面。

对于Windows和Linux端两个初始投递样本，virustotal给出了全绿和未采集到样本的结论。



Q 8aaf0d617683c366912d6ff4af3d1df0a78a3352ec8a87bdb81495ee1e41c3d6

COMMENTS 0

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).



Q 5616052f9947a1fccb866ec6c1b9be667b1ee8efe9c8e7ab9f4f468c7c7c3277

0

/ 63

Community Score

-1

✔ No security vendors flagged this file as malicious

5616052f9947a1fccb866ec6c1b9be667b1ee8efe9c8e7ab9f4f468c7c7c3277

endpoint

elf 64bits shared-lib

步步为营，智能追凶

360反病毒团队依托先进的AI工具，结合团队内部多位顶尖安全专家多年的技术经验积累，搭建起了一套高效且专业的人工智能安全分析体系。该体系能够自主完成日常安全数据的巡查、分析、排查、溯源以及更为复杂的多级关联分析研判等工作。

而本次事件最初的起源，是一次针对流行恶意程序“银狐木马”的常规巡检流程。AI安全分析专家在对银狐C2服务器连接数据进行分析时，发现了一组不同寻常的程序，其对多个银狐C2服务器发起了“攻击”，而非接收控制指令。

134.122.204.183	14347f1482489dac...	C:\Windows\System32\ragent\apps\ragent-a\current\RuntimeAgent.exe	深层, 嵌套, 境外	路径深层嵌套, 连接境外IP, 端口5985
202.96.11.155	14347f1482489dac...	C:\Windows\System32\ragent\apps\ragent-a\current\RuntimeAgent.exe	深层, 嵌套, 境外	路径深层嵌套, 连接境外IP, 端口5985
143.92.61.119	14347f1482489dac...	C:\Windows\System32\ragent\apps\ragent-a\current\RuntimeAgent.exe	深层, 嵌套, 境外	路径深层嵌套, 连接境外IP, 端口5985

	md5	ip+端口	域名	协议	AI评分
ows\System32\ragent\apps\ragent-a\current\RuntimeAgent.exe		161.248.14.98:5985		TCP(6)	偏黑 70
ows\System32\ragent\apps\ragent-a\current\RuntimeAgent.exe		43.248.172.11:5985		TCP(6)	偏黑 70
ows\System32\ragent\apps\ragent-a\current\RuntimeAgent.exe		192.253.229.64:5985		TCP(6)	偏黑 70
ows\System32\ragent\apps\ragent-a\current\RuntimeAgent.exe		134.122.204.183:5985		TCP(6)	偏黑 70
ows\System32\ragent\apps\ragent-a\current\RuntimeAgent.exe		202.95.11.155:5985		TCP(6)	偏黑 70
ows\System32\ragent\apps\ragent-a\current\RuntimeAgent.exe		143.92.61.119:5985		TCP(6)	偏黑 70

AI安全专家在采集这组程序信息后，便对其开展了分析。AI安全专家从样本库中找出了该样本，并对其进行了逆向分析。在反编译分析过程中，AI先是注意到了样本中含有的反调试、日志获取、提升权限等较为敏感的指令，进而继续深入探索，又发现了其内置的数据加密、证书操作、网络连接等行为。

【思考内容】

[DebugAgent:debug_agent_1] 这是一个 Windows 服务程序 (StartServiceCtrlDispatcherW、RegisterServiceCtrlHandlerExW、SetServiceStatus)，导入了大量加密相关函数 (BCrypt*、CRYPT32)，网络相关函数 (IPHLAPI)，注册表操作函数。

有意思的导入包括：

- IsDebuggerPresent - 反调试检查
- BCryptDecrypt / BCryptDeriveKeyPBKDF2 - 加密解密
- RegisterEventSourceW / ReportEventW - 事件日志
- ImpersonateLoggedOnUser / DuplicateTokenEx / AdjustTokenPrivileges - 权限操作

继续查看更多导入，特别是网络相关和进程注入相关的。让我继续查看导入列表，同时查看字符串。

在经过综合对比研判后，AI安全专家认为此样本属于下载器类恶意软件，本身是一个具有“保活”“隐蔽”“接收指令”功能的下载器框架，需要进一步挖掘分析。

****样本定性****: EndpointRuntimeAgent.exe - 一个用 .NET NativeAOT 编译的 Windows 服务程序 (伪装成企业端点管理)

1. 以 SYSTEM 权限安装为 Windows 服务 "EndpointRuntimeAgent" (自描述为 "Downloads, updates, and runs endp
2. 创建 schtasks 计划任务 "EndpointRuntimeAgentWatchdog" (每分钟、SYSTEM、HIGHEST 权限) 双重持久化
3. 服务失败自动重启 (60s*3) + delayed-auto 启动
4. 周期性向硬编码的 <https://curlservice.com/manifest> 发送 GET 请求 (带 X-Agent-Host 头上报主机名、User-Age
5. 解析 manifest JSON: {agentPolicyVersion, apps: [{id, enabled, version, processName, installDir, exeI
6. 对每个 enabled 应用: 下载 packageUrl 指定的压缩包 (.download 临时文件), 校验 SHA256, 解压安装到 installD
7. 以 hidden (CreateNoWindow) 模式启动 exePath 进程, keepAlive=true 时持续监控并自动重启 (restartDelaySec
8. 状态持久化在 agent-state.json

恶意性判断:

- 本体不含传统恶意载荷 (无勒索、无窃密代码)，但它是一个**通用的远程程序投放/执行框架 (downloader + RAT loader
- curlservice.com 不是已知合法软件厂商域名——企业合法端点管理产品不会用这种域名
- 攻击者通过控制 manifest 服务器可任意下发并执行任意程序 (以 SYSTEM 权限)，支持隐藏运行、保活、自动更新
- 双重持久化 (服务 + 计划任务看门狗) + 停机自愈设计
- 该域名 curlservice.com 与 curl 官方 (curl.se / haxx.se) 无关，是抢注/伪装域名

此后AI安全专家进行了主动挖掘，自主获取了其控制端下发的控制指令，并对其加密算法进行了分析破解，获取了其完整工作内容。

【思考内容】

[DebugAgent:debug_agent_1] 重大成果! manifest 完全解密。C2 下发两个应用：

1. ****winagent-a**** (WindowsEndpointAgent 1.0.3):
 - 安装到 C:/Windows/System32/winagent/apps/winagent-a/current (系统目录!)
 - keepAlive=true, hidden=true (隐藏运行+保活)
 - 每 60 秒重启
 - 从 <https://curlservice.com/download/WindowsEndpointAgent.zip> 下载
 - SHA256: 5A48186220850A85385E3E715CE078787663C65405F0FD8F13CC3A3DB396EC69
2. ****ragent-a**** (RuntimeAgent 1.0.7):
 - 安装到 C:/Windows/System32/ragent/apps/ragent-a/current
 - 同样 hidden + keepAlive
 - 从 <https://curlservice.com/download/RuntimeAgent.zip> 下载
 - SHA256: 1660564787E5E4B73EB103EB20452527FD6E9C34B8F5D7FFA060DB92AD0D417B

现在应该尝试下载这两个载荷进行分析。这是 C2 下发的实际载荷。让我下载这两个 zip (只下载不运行)。

随后，AI使用各类技术手法继续对新发现的载荷样本展开分析研判，结合大数据日志对获取的各项指标信息展开溯源工作。最终，以一个样本作为切入点，向上追溯出了其部署工具和脚本，向下则解析出了其释放的攻击载荷，甚至还从数据中筛查出了位于旁支的一个跨平台 (Linux系统) 部署器样本，整个溯源过程层层递进、步步为营。

二、下发途径：通过 WinRM 远程管理 (Windows Remote Management) 推送安装

该文件并非通过浏览器下载、即时通讯软件投递或钓鱼邮件等常规途径进入用户计算机，而是通过 **WinRM 远程管理协议** 被远程推送并安装。完

```
svchost.exe (WinRM服务)
├─ wsmprovhost.exe (WinRM宿主进程, 命令行参数: -Embedding)
│   └─ EndpointRuntimeInstaller.exe (安装器, 位于 C:\Windows\Temp\)\
│       ├── netsh.exe int ipv4 set dynamicport tcp start=1000 num=60000 (修改动态端口范围)
│       ├── install (安装命令, 将 EndpointRuntimeAgent.exe 部署到 C:\Program Files\EndpointRuntimeAgent\)
│       └─ schtasks.exe /Create /TN EndpointRuntimeAgentWatchdog /SC MINUTE /MO 1 /RU SYSTEM /RL HIGHEST (创
```

关键证据：

1. **wsmprovhost.exe** 是 Windows Remote Management (WinRM) 的 COM 宿主进程，命令行参数 **-Embedding** 表明通过 COM 接口被远程
2. 安装器 **EndpointRuntimeInstaller.exe** (MD5: **586a03ff6c6a0a3c9b66e259f85f4519**) 被放置在 **C:\Windows\Temp** 临时目录中
3. 安装器执行 **install** 命令完成目标文件的部署
4. 安装后通过 **schtasks.exe** 创建名为 **EndpointRuntimeAgentWatchdog** 的计划任务，每1分钟以 SYSTEM 最高权限运行一次，实现持久
5. **无下载记录**：dl_protect 日志中未发现该安装器或目标文件的任何下载记录，排除了通过浏览器/下载工具下发的可能

最终，经AI安全专家全面分析，发现本次捕获到的“端点僵尸网络”是一个由AI驱动编写的跨平台凭据喷射网络。其通过三层架构模式，展开分布式的入侵操作，支持13种常见网络协议。

wsman	ssh	rdp	http	https
httpv2	telnet	sftp	ftp	socks4
socks4a	socks5	gopher		

AI安全专家分析确认，该僵尸网络还具备大量信息采集、攻击下发的能力，根据解密出的攻击数据来看，当前主要攻击目标网络为微软WinRM/GSSAPI普遍采用的Web服务管理协议（wsman）。当前共发现了1311台分布于世界各地的服务器正在遭受该僵尸网络的凭据喷射攻击，而这些服务器的运营商更是覆盖了腾讯云、阿里云、AWS、Azure、Hetzner、OVH等多家主流云服务提供商。

出于安全考虑，当前并未赋予“AI安全分析专家”真正的处置能力，最终“AI安全分析专家”将完整事件报告与处置建议提交人类安全专家审核实施。

curlservice.com 分布式凭据喷射网络 — 全家族完整分析报告

报告时间: 2026-08-20 (UTC+8)

一、执行摘要

本次分析共涉及 5 个样本，构成一个跨平台 (Windows + Linux) 三层架构分布式 WinRM/GSSAPI 凭据喷射网络。攻击者通过伪装为“Endpoint Runtime Agent”软件的安装包分发恶意程序，利用 Windows 服务 + 计划任务实现双持：服务器 (curlservice.com, 疑似抢注 curl 官方域名) 下载两个 Worker 载荷：一个负责信息采集，另一个负责对全球目标执行 WinRM guest 弱口令密码喷洒。全链路使用 AES-256-GCM + GZip 加密，但密钥硬编码于所有样本中，已完

关键发现:

- C2 当前活跃，type=2 队列中实时存有 1311 个唯一全球目标 IP 的喷射任务
- 所有目标均使用 guest 账户，配合 6 组轮换弱口令
- 目标覆盖腾讯云、阿里云、AWS、Azure、Hetzner、OVH 等全球主流云服务商
- 存在 Linux 跨平台变体，通过 GSSAPI 同样参与密码验证

二、样本家族清单

#	样本名称	MD5	SHA256	文件大小	平台	角色
1	EndpointRuntimeInstaller.exe	586a03ff6c6a0a3c9b66e259f85f4519	8aaf0d617683c366912d6ff4f3d1df0a78a3352ec8a87bdb81495ee1e41c3d6	5,830,656 B	Windows	初始投递安装器
2	EndpointRuntimeAgent.exe	b9e0ad3962249a1eea0c99e3f598ed1f	27c825045337bcde30d2af470d00da978a1ef617746e834ba8b40c982e6a08a8	6,251,520 B	Windows	部署器/守护服务
3	WindowsEndpointAgent.exe	b2e37d9a0f65f37f229ecc319d00a515	6fd0462e59c64edb7297bf0c44673a290cd02ce9657180ef5dfc01c18feae69	6,353,920 B	Windows	Worker A (type=1 信息采集)
4	RuntimeAgent.exe	cc4fc1f9e55bc1d867dccc2e821b87ca	6cd1010d1125ff916bcc7285e7638b86753e9db60ff4af38e0af25f45a460ab7	8,094,720 B	Windows	Worker B (type=2 凭据喷射)
5	endpoint (Endpoint-linux-x64)	99fb8f6cc0a7b1e496789ffa423030ef	5616052f9947a1fccb866ecc1b9be667b1ee8efe9c8e7ab9f4f468c7c7c3277	7,121,072 B	Linux	部署器(跨平台变体)

投递链证据闭环: C2 /download/EndpointRuntimeAgent.zip 解压所得 EXE 与本地主样本 (b9e0ad39...) 逐字节一致；EndpointRuntimeInstaller.exe 下载 URL 与其内部字符串互证；所有载荷 SHA256 与 manifest 声明值一致。

三 加密基础设施

AI赋能助力安全

本次对“端点僵尸网络”的发现与分析，展示了360 AI安全分析专家在国产开源大模型GLM-5.3的加持下，可以自主完成对可疑样本的溯源、分析、加密流量破解等重难点工作，最终成功获取了攻击样本完整组件及攻击配置文件。同时，又基于智能分析结论，建立了对控制指令的监测机制，彻底斩断了攻击“黑手”。



360 AI安全分析专家在日常巡检中，还曾发现过多起漏报、误报事件，已然成为人类安全专家不可或缺的可靠后盾，成为安全运营能力提升的新途径。

IOCs

MD5s

586a03ff6c6a0a3c9b66e259f85f4519

b9e0ad3962249a1eea0c99e3f598ed1f

b2e37d9a0f65f37f229ecc319d00a515

cc4fc1f9e55bc1d867dccd2e821b87ca

99fb8f6cc0a7b1e496789ffa423030ef

Domains

curlservice[.]com

URLs

hxxps://curlservice[.]com/download/install-agent.sh

hxxps://curlservice[.]com/download/Endpoint-linux-x64.zip

hxxps://curlservice[.]com/download/WindowsEndpointAgent.zip

hxxps://curlservice[.]com/download/EndpointRuntimeAgent.zip

hxxps://curlservice[.]com/download/RuntimeAgent.zip

hxxps://curlservice[.]com/manifest

hxxps://curlservice[.]com/api/jobs/claim?type=1&count=

hxxps://curlservice[.]com/api/jobs/results

hxxps://curlservice[.]com/api/status