

CNCERT：关于RCtea僵尸网络大范围传播的风险提示



secrss.com/articles/87776

[病毒木马](#) [国家互联网应急中心CNCERT](#) 2026-02-10

该家族目前正处于快速传播与能力构建阶段，具备极强的对抗与反检测反追踪意识，已具备成熟的DDoS攻击能力，且主要针对物联网（IoT）设备。

感谢北京神州绿盟科技有限公司在本报告的样本分析工作中做出的重要贡献。

一、概述

近期，CNCERT监测到一个新型僵尸网络正在互联网上大范围传播，该僵尸网络自2025年12月下旬起开始活跃。该家族在通信协议、数据存储及反追踪机制上均展现出高度的复杂性和规避性，其核心特征为广泛使用基于RC4、ChaCha20及TEA算法变种的深度定制加密方案。据此，我们将其命名为RCtea僵尸网络。

分析表明，该家族目前正处于快速传播与能力构建阶段，具备极强的对抗与反检测反追踪意识，已具备成熟的DDoS攻击能力，且主要针对物联网（IoT）设备。现将其主要情况分析披露如下。

二、僵尸网络分析

（一）主要传播方式与目标

RCtea家族目前的传播活动具有明确的针对性。在目标设备方面，已发现的传播样本均针对ARM和MIPS架构的系统进行编译，这清晰地表明其当前主要攻击目标是路由器、摄像头等各类物联网设备，尚未发现面向传统Linux服务器或主机的样本。

在传播手段上，该家族主要依赖Telnet暴力破解进行对外扩散。木马在成功入侵一台设备后，会主动对外发起扫描，并尝试使用内置的常见弱口令列表进行破解，从而感染更多的在线设备，实现僵尸网络规模的快速扩张。

（二）核心检测与对抗手段

攻击者为规避安全检测与追踪，采用了多层精心设计的技术手段。

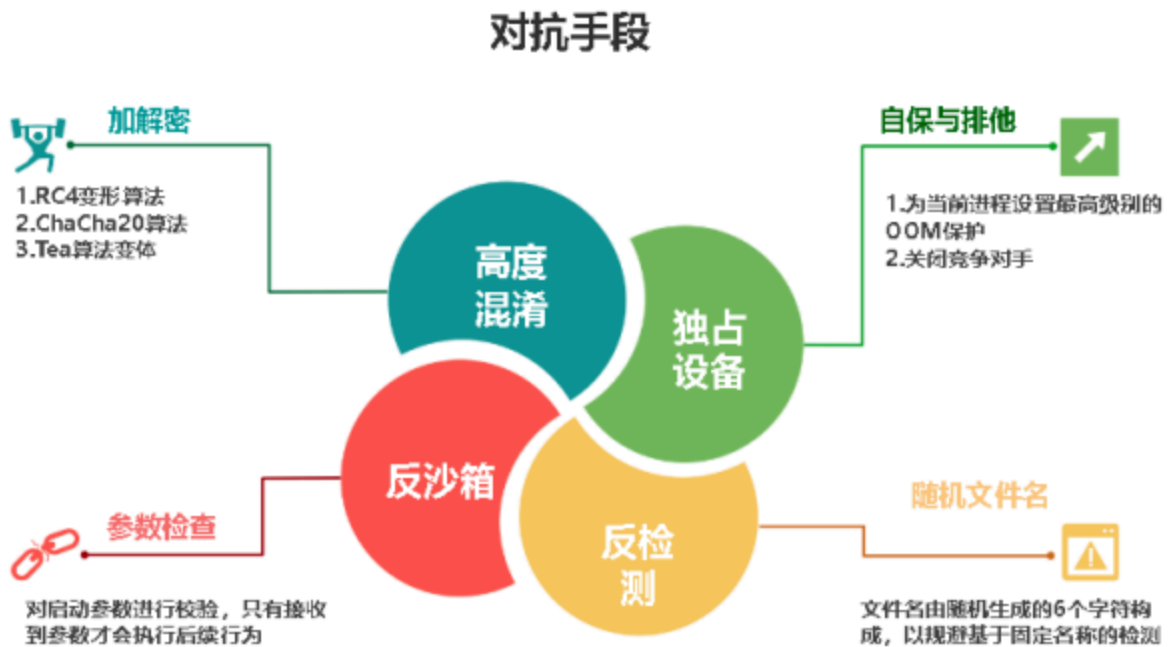


图 1 RCtea对抗手段

首先，木马具备独特的参数启动机制，只有在运行时接收到攻击者预设的特定参数（如当前版本的“telnet.curl”）才会激活核心恶意功能，否则将主动退出。此设计能有效绕过依赖自动执行进行行为分析的沙箱环境。

其次，在数据保护层面，木马对所有核心配置及通信内容共计使用了三种经过高度变形和混淆的加密算法变种（RC4、ChaCha20、TEA），具备较高的对抗性，提升分析难度。

为了保证自身能够稳定运行，木马还会为当前进程设置最高级别的OOM（Out-Of-Memory）保护，确保恶意进程在系统内存不足时拥有最高生存优先级，在系统内存耗尽时不会被内核强制终止。

木马在下载至受害者设备时，其文件名由随机生成的6个字符构成，以规避基于固定名称的检测。执行后，木马会在控制台输出“here we are”作为调试标记，该行为可为动态分析提供可见线索。

（三）命令控制与网络特征

该家族的命令与控制网络设计体现了较强的抗打击意识。木马并非使用固定的IP或域名，而是内置了多组地址及端口。在通信时，木马会随机选取其中一组进行连接。这种多冗余、随机选择的架构显著提升了僵尸网络控制通道的稳定性和存活能力。

而在网络通信时，所有上线认证及指令数据均使用自定义的TEA变种算法（密钥“FrshPckBnnnSplit”）和ChaCha20算法配合加密，并将上线过程拆分为十余个数据包分轮发送，极大地增加了流量分析与解密还原的难度。

（四）主要功能与潜在意图

根据对样本的逆向分析，RCtea木马已具备发起多种DDoS攻击的能力，支持包括SYN FLOOD、ACK FLOOD、UDP FLOOD及TCP FLOOD（含多种变体）在内的攻击方式。结合其当前活跃的传播态势与尚未观测到大规模攻击的现象综合研判，该僵尸网络很可能正处于规模扩张或功能升级的准备期。攻击者目前的首要目标可能是尽可能多地控制设备，构建庞大的僵尸网络资源，为后续可能发起的大规模、竞争性攻击或其他非法活动做准备。

（五）关联性分析

尽管RCtea从代码结构上看是一个全新构建的家族，未大范围沿用已知僵尸网络的模块结构，但其在多个关键技术选型与实现偏好上，与已知的AISURU僵尸网络存在显著相似性。这些共同点包括：均倾向于使用并配置多组冗余地址；均采用对基础加密算法（如RC4、TEA、ChaCha20）进行深度自定义变形处理来保护关键信息；均将上线认证流程拆分为多轮完成。这些共性强烈暗示，两者背后的运营方可能存在关联、继承或共享同一技术来源。

三、僵尸网络感染规模

通过监测分析发现，2026年1月20日至25日期间，RCtea僵尸网络在我国境内已确认的活跃“肉鸡”规模达9827台，境内日上线肉鸡数量最高达4870台，肉鸡C2日访问量最高达27.8万次。上线肉鸡IP数量分布情况如下：

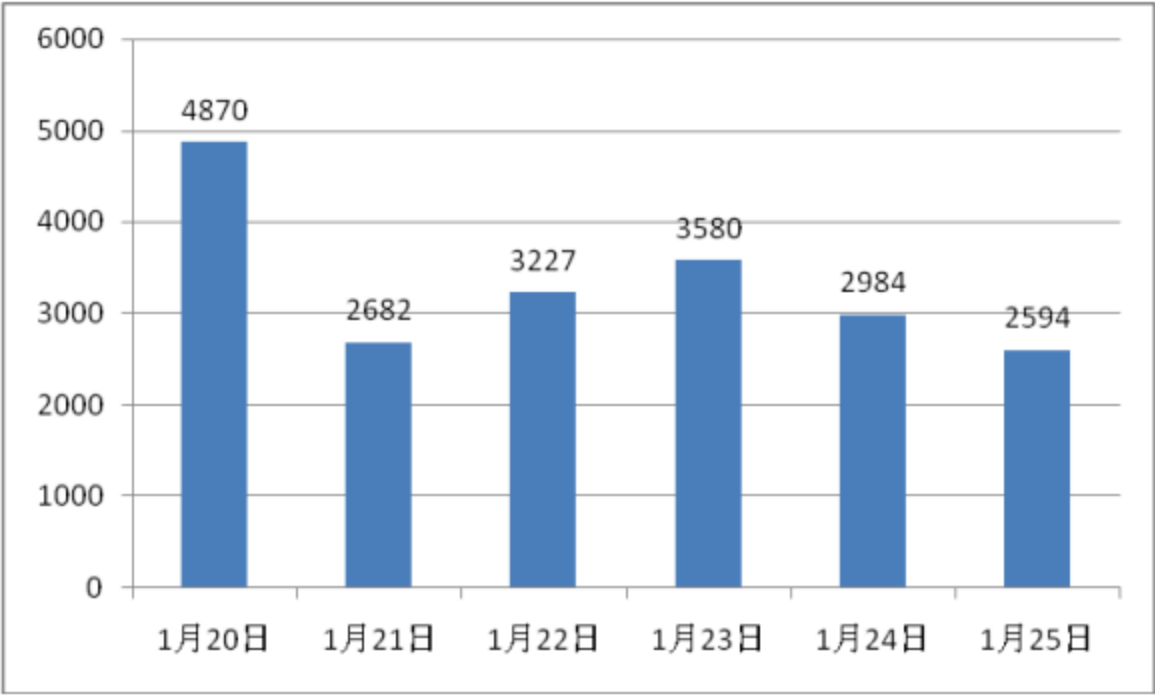


图 2 境内日上线肉鸡数量分布情况

四、防范建议

请广大网民强化风险意识，加强安全防范，避免不必要的经济损失，主要建议包括：

- （1）梳理已有资产列表，及时修复相关系统漏洞，包括历史漏洞和最新曝光的漏洞。

(2) 加强口令强度，避免使用弱口令，密码设置要符合安全要求，并定期更换。建议使用16位或更长的密码，包括大小写字母、数字和符号在内的组合，同时避免多个服务器使用相同口令。

(3) 当发现主机感染僵尸木马程序后，立即核实主机受控情况和入侵途径，并对受害主机进行清理。

五、相关IOC

样本HASH：

b1c2458d22bbb0b7580470d9481654fae096a2bc0e8aab742ba9ac584568094d

f4d312c31b3f1170621721ea7dda0ceb50977bda8f04527cf060f85dda15c513

45168bc663329c3b1d883b83a59fe84f08b6e01895c37144ddfa9156bea3eae

下载链接：

<http://91.92.242.42/wget.sh>

<http://91.92.242.42/curl.sh>

<http://91.92.242.42/arm>

<http://91.92.242.42/arm5>

<http://91.92.242.42/arm7>

<http://91.92.242.42/mips>

<http://91.92.242.42/mpsl>

<http://91.92.242.42/arc>

<http://91.92.242.42/aarch64>

<http://5.255.127.15/wget.sh>

<http://5.255.127.15/curl.sh>

<http://5.255.127.15/arm>

<http://5.255.127.15/arm5>

<http://5.255.127.15/arm7>

<http://5.255.127.15/mips>

<http://5.255.127.15/mpsl>

<http://5.255.127.15/arc>

<http://5.255.127.15/aarch64>

<http://103.146.23.241/wget.sh>

<http://103.146.23.241/curl.sh>

<http://103.146.23.241/arm>

<http://103.146.23.241/arm5>

<http://103.146.23.241/arm7>

<http://103.146.23.241/mips>

<http://103.146.23.241/mpsl>

<http://103.146.23.241/arc>

<http://103.146.23.241/aarch64>

<http://103.149.29.38/wget.sh>

<http://103.149.29.38/curl.sh>

<http://103.149.29.38/arm>

<http://103.149.29.38/arm5>

<http://103.149.29.38/arm7>

<http://103.149.29.38/mips>

<http://103.149.29.38/mpsl>

<http://103.149.29.38/arc>

<http://103.149.29.38/aarch64>

控制域名：

www.gokart.su

www.boatdealers.su

kieranellison.cecilioc2.xyz

nineelevan.gokart.su

www.plane.cat

mail.gokart.su

声明：本文来自国家互联网应急中心CNCERT，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](#) [物联网](#) [监管](#)

相关资讯

- [**暗网市场出现新OT攻击框架，可针对性破坏电力系统**](#)

[电力能源](#) [看雪学苑](#) 2026-02-02

[一套据称可精准操控电力分布、甚至能对设备进行“压力测试”的工业系统攻击框架，正在暗网秘密兜售。](#)

- [**iPhone隐私指示灯成摆设？Predator间谍软件通过Hook完美隐身**](#)

[病毒木马](#) [玄月调查小组](#) 2026-02-01

[这一技术细节的曝光再次证明：没有任何操作系统是绝对安全的。](#)

- [**下载量超150万！两款AI编程VS Code扩展被曝窃取用户源代码**](#)

[病毒木马](#) [看雪学苑](#) 2026-01-27

[这两款官方市场热门的VS Code扩展，竟是代码窃取工具。](#)