

# YoroTrooper组织针对独联体及周边区域的攻击活动分析

---

 [mp.weixin.qq.com/s](https://mp.weixin.qq.com/s)

高级威胁研究院

## YoroTrooper

YoroTrooper，又名SilentLynx、Tomiris、Cavalry Werewolf，是一个被评估为疑似具有哈萨克斯坦国家背景支持的高级持续威胁（APT）组织。该组织长期针对中亚、欧洲及中东地区的政府机构、能源企业与关键基础设施，实施高密度的网络渗透与深度战略间谍活动。

其攻击活动活跃轨迹至少可追溯至2021年，核心使命旨在通过网络手段服务于特定的地缘政治利益，涵盖了从高价值情报采集、政府内部通信监控到关键基础设施机密数据持续外传的全频谱间谍作战。

该组织表现出极高的活跃度与技术韧性。即便近年来面临全球安全行业的追踪与曝光，YoroTrooper非但未曾缩减其行动规模，反而展现出更敏捷的技术进化与武器库扩充能力。从早期依赖单一手段，到近期观测到的“通用工具与自研载荷并重”的复合型渗透框架——该组织正以更加灵活、隐蔽的战术策略，持续加剧着跨国政企机构面临的安全挑战。

### 01

#### 攻击活动分析

##### 1.攻击流程分析



此图片来自微信公众平台  
未经允许不可引用

该恶意样本的初始投递渠道为即时通讯软件 Telegram。

受害者在接收到名为 Temp\_rar.rar 的恶意压缩包并尝试打开时，触发了后续攻击组件的执行。

## 2. 恶意载荷分析

---

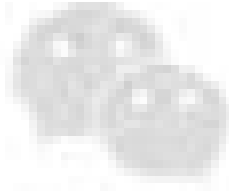
### 2.1 ReverseShell

---

#### 2.1.1 Laplas

---

Laplas为基于 TLS 加密的交互式反向 Shell 模块。为对抗静态特征检测与启发式查杀采用字符串混淆技术，在运行时利用硬编码密钥通过 XOR 算法动态解密出目标进程字符串 "cmd.exe"。Laplas调用内置OpenSSL库连接远端C2(updates-check-microsoft.ddns.net:443)，通过禁用证书校验建立 TLS 加密隧道。利用 Windows 匿名管道机制劫持cmd.exe其标准输入、输出及错误流，将I/O 数据直接重定向至加密 Socket 中，以此构建高度隐蔽的远程交互控制链路。

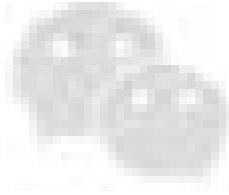


此图片来自微信公众平台  
未经允许不可引用

### 2.1.2 hosts-ReverseShell

---

与Laplas不同，hosts-ReverseShell为TCP直连版反向 Shell。为规避安全厂商的自动化分析与沙箱检测，程序内部集成了多重反分析与逃逸机制：在数据侧，采用栈字符串混淆（Stack String Obfuscation）技术动态拼接 C2 地址以隐藏网络特征；在执行侧，通过探测底层 CPU 微架构层面的执行精度差异，精准识别并逃避模拟器或沙箱分析环境。



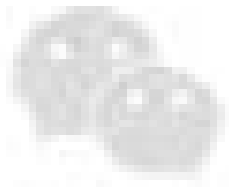
此图片来自微信公众平台  
未经允许不可引用

### 2.1.3 C#SSLrevshell

---

在对该组织基础设施的溯源追踪中，我们关联捕获到一款基于 C# (.NET) 开发的反向 Shell 变种。该样本核心逻辑与 Laplas 高度一致，其关键技术特征如下：

在通信与驻留层面，载荷启动后调用系统API隐藏控制台窗口以实现静默运行；随后主动连接硬编码C2（45.130.146.197:443），并通过显式覆写证书验证回调函数，强制信任自签名证书，借此构建隐蔽的 TLS 加密隧道。



此图片来自微信公众平台  
未经允许不可引用

在执行与守护层面，载荷在后台静默拉起 `cmd.exe`，利用多线程异步机制将系统命令行的标准输入、输出及错误流与TLS隧道进行双向重定向。同时，主函数内置异常捕获逻辑，在遭遇网络阻断或底层进程异常退出时，将以 5 秒为间隔持续发起重连尝试，保障远控通道的高可用性。



此图片来自微信公众平台  
未经允许不可引用

该.NET 变种的投入使用，表明 YoroTrooper 组织正积极通过跨语言开发重构其核心武器库，旨在分散静态特征维度，进一步增强规避安全检测的对抗能力。

## 2.2 持久化

---

### 2.2.1 Netsvc

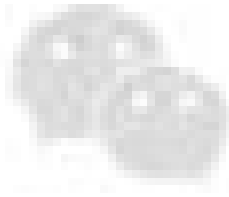
---

在持久化阶段，Netsvc将自身注册为系统服务，Netsvc通过配置欺骗性的服务描述"The Network Discovery Service(Network Service Discovery Protocol)" 以实施名称伪装。通过将其启动类型显式设置为 SERVICE\_AUTO\_START（开机自启动），该恶意载荷确保在每次系统重启时，都能以 SYSTEM 最高权限在后台自动加载。这是一种典型且广泛使用的系统持久化机制。



此图片来自微信公众平台  
未经允许不可引用

目标子进程成功启动后，Netsvc的守护线程会调用 `WaitForSingleObject` 挂起当前执行流，对该进程的生命周期实施阻塞式监控。该函数的超时阈值被硬编码为 `0x112A880` 毫秒（折合 18,000 秒，即 5 小时）。基于此机制，若核心载荷持续稳定运行，守护线程将以 5 小时为周期进行轮询唤醒；一旦目标进程在超时窗口内主动退出或被外部异常终止，该阻塞状态将被即时打破，从而快速触发外层的载荷复活逻辑。

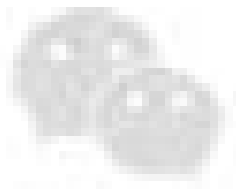


此图片来自微信公众平台  
未经允许不可引用

### 2.2.2 同源变种分析

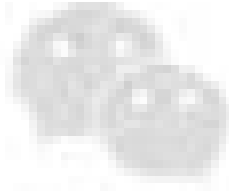
---

在本次攻击活动中，我们还捕获到了功能机制完全一致的同源变种服务外壳（SSDPSRV）及其关联载荷（srvdriv.exe）。



此图片来自微信公众平台  
未经允许不可引用

该变种在免杀对抗上同样展现了典型的名称混淆手法：合法的 Windows SSDP 发现服务名称通常为 SSDPSRV，而该恶意服务将名称故意错拼为 SSDSPSRV（增加冗余字符 'S'），同时其显示名称与描述完全照抄系统自带的合法服务，以此掩人耳目。



此图片来自微信公众平台  
未经允许不可引用

该变种服务同样复用了上述的“5小时轮询守护机制”来静默拉起并监控核心载荷 `srvdriv.exe`。  
`srvdriv.exe` 启动后，会主动通过 TCP Socket 连接至内置 C2 (212.193.2.162:8443)。



此图片来自微信公众平台  
未经允许不可引用

并完全复用了 Laplas 建立 TLS 加密隧道与匿名管道劫持 `cmd.exe` I/O 流的技战术，最终实现同等的高隐蔽性交互式反向 Shell 控制



此图片来自微信公众平台  
未经允许不可引用

## 02

### 归属研判

综合对本次攻击事件的受害者画像、战术技术与过程（TTPs）、恶意软件代码特征及网络基础设施的深度溯源与多维交叉比对，本次攻击活动高度置信归属于 APT 组织 YoroTrooper。

本次攻击活动的中招用户包含顿涅茨克人民共和国、乌兹别克斯坦政府相关部门人员。YoroTrooper 组织长期以地缘政治为导向，主要针对独联体（CIS）国家及周边特定冲突区域的政府机构、外交实体与关键基础设施实施网络间谍活动。本次攻击的受害者身份、所在区域及潜在的情报窃取诉求，与YoroTrooper组织的长期战略目标与历史攻击画像完全一致。

本次攻击的初始投递渠道为即时通讯软件 Telegram，通过社会工程学手段诱导受害者执行恶意压缩包。利用流行社交/通讯软件进行定向钓鱼，并附带伪装的高危附件，是YoroTrooper组织极其惯用且高度依赖的初始突破策略。

攻击者未完全依赖开源武器库，而是使用了高度定制化的 C/C++ 反向 Shell 组件。其利用 Windows 匿名管道劫持 cmd.exe 配合 TLS 隧道实现隐蔽通信的手法，是该组织工具集的重要标志。

载荷中硬编码的 C2 地址使用了动态域名服务，并试图伪装成合法的微软更新流量。这种滥用免费 DDNS 服务并结合“域名白化”的伪装策略，极大降低了基础设施的采购溯源风险，是 YoroTrooper 长期采用的基础设施构建模式。

基于上述多维度的特征重合，我们有极高的置信度认为，本次针对顿涅茨克人民共和国、乌兹别克斯坦政府人员的定向攻击行动，系由 YoroTrooper 组织发起的一场以情报窃取为核心目的的攻击活动。

## 附录 IOC

MD5：

eb9fef447c5e883c0af807992f450b60  
3f9ee4b62da9a197b9380f6594aeef12  
c05c4deddf9f4e4ec43cc510af903b9f  
63ae17d887528e335080dcd73d4c5af3  
f67337f2dcb3136fb687f901c66b34f7  
5864668137c23d7248bbb137a5e43d07  
55655d252dcc2d5e1168d30fff2b5e48  
eeab58e64ed72098f778cda42537883c  
d3e3d99b077a4193b1d93b604b096456  
8fc604898e84fc7bf349e8359cd4a125  
3cf8b84d4a5dde2cf789ebd8d3006029  
5dc74828289a95682f3cfbb8ac47a624  
e8e1555d1f8b3b56e30f2baaaffc491f  
f9446fc64a6c06a94979b5ee311f7673  
365a6d29a9b45c155c6e7d2704f1192d

5148c3ed171faf38bb33cab45307c245

02489f4e0fede5dcb8966e840e0adbbf

c2cc85e71cd58a78d2c1f336771533a9

0ae77c4ba8f8e8100c8889de3e64f48b

19319ac8398ce44bddf8cb56e90de9e0

e8e1555d1f8b3b56e30f2baaaffc491f

C2 :

45.130.146.197:80/443

212.193.2.162:8443

microsoft-updates-windows.servehttp.com

updates-check-microsoft.ddns.net