# APT-C-60（伪猎者）的近期活动分析与技术演进

**APT-C-60**

**伪猎者**

APT-C-60（伪猎者）是一伙以持续监控受影响用户、窃取相关信息为目的朝鲜半岛APT组织。我们于2018年发现该组织的活动，溯源分析最早的攻击活动可疑追溯到2014年。受影响用户大部分为涉韩的政府、经贸、文化有关的企事业单位，以及劳务咨询公司。

## 一、概述

本文将重点分析该组织在我们于2025年6月发布《APT-C-60（伪猎者）攻击演进：基于GitHub的动态载荷分发与指令中继》报告后，所展现出的快速响应与战术升级。

报告发布后，“伪猎者”组织几乎立刻调整了其攻击策略，展现出高度的警觉性和对抗能力。其迭代升级主要体现在以下三个方面：

1. 战术升级：“阅后即焚”式的载荷分发。利用GitHub平台特性，实现恶意载荷的短暂、动态托管，并在受害者下载后立即抹除痕迹，极大提升了隐蔽性和追溯难度。
2. 技术强化：核心组件的对抗性升级。通过轮换加密密钥、升级混淆算法，特别是引入数据与函数指针化技术，显著增强了恶意软件的免杀和反分析能力。
3. 设施整合：攻击链的平台统一化。将原先托管于Bitbucket的最终后门载荷迁移至GitHub，实现了攻击基础设施的集中管理与策略协同。

下文将对这些变化进行详细剖析。

## 二、核心变化详述

### 1. 隐蔽性的显著增强：从动态更新到“阅后即焚”

为应对曝光，“伪猎者”组织首先对其攻击基础设施进行了敏捷调整。

动态更新与“马甲”账号：该组织迅速停用或隐藏了已被曝光的GitHub仓库，并注册了新的账号作为新的攻击载荷分发点(如下图，2025625 创建)，保持其攻击基础设施的灵活性和隐蔽性。

“阅后即焚”式的载荷分发：攻击者采用了“短暂入库，拉取即毁”的策略。恶意代码仅在受害者系统触发下载指令时，才被临时上传至GitHub仓库。一旦下载完成，攻击者会立即通过git push –force等强制手段抹除提交历史。这种做法好比将情报写在沙滩上，潮水（下载完成）一来，痕迹便消失得无影无踪，极大地增加了安全研究人员事后追溯和取证的难度。(如下图)

**2. 组件迭代：对抗技术的持续深化**

其攻击载荷的核心功能模块（如Observer Install和Backdoor Install）虽然保留了基本架构，但通过以下方式进行了强化，以对抗检测。

密钥轮换与代码混淆：类似于定期更换文件、内部API字符串的Xor密码，该组织对恶意代码中的加密/解密密钥进行了更换，并对代码逻辑进行混淆处理。这使得基于旧样本特征的检测规则失效，提升了载荷进入受害机器的成功率。

**三、载荷迭代细节**

**1. Observer Install组件**

此组件在此次迭代中变动很小，主要进行了载荷下载后解码密钥的轮换。这种“换汤不换药”的策略是该组织惯用的伎俩。

**1）新旧版本组件对比**

新版本组件：sgznqhtgnghvmzxponum

原版本组件：u8b34ys8j5yogq7r32bm

**2. Backdoor Install组件**

该组件是植入后门的关键，其核心流程保持不变，但引入了数据与函数指针化的混淆技术，提升载荷进入受害机器的成功率。

- 技术解读： 在程序运行前或运行时，它不再直接调用功能代码或使用明文数据，而是将这些代码和数据的内存地址（即“指针”）预先存入一个全局的“地址簿”（全局对象）中。当需要执行某个功能时，程序会去翻阅这个“地址簿”，通过地址间接调用。
- 带来的挑战： 这种做法极大地提升了静态分析的难度。对于分析人员来说，直接阅读代码（静态分析）就像是看一本满是代号和暗语的书，必须在程序实际运行时（动态分析）才能理清其真实的指令和数据流。这一思路与该组织此前对Backdoor组件V3.X版本的迭代方式一脉相承。

**1）配置信息初始化新旧对比**

新Backdoor Install组件首次出现“全局对象预置”，原版本组件则无此步骤。

Backdoor Install对比 Backdoor(V3.X)，其对象体积更小、结构更简单。

新Backdoor Install组件初始化流程

老版本Backdoor Install组件初始化流程

**2）持久化新旧对比**

新版本组件部分关键行为函数依赖外部传入的全局对象指针“p_RCX”，老版本组件直接传递操作参数即可。

老版本Backdoor Install组件

**3. Backdoor Loader组件**

该组件常被忽略，因为其作用十分简单，仅作为加载最终后门程序的“启动器”，该组件的字符串解密算法也发生了细微但关键的变化。其解密逻辑从原先的(xor 2) – 1或(xor 3) – 1 调整为新的 (xor 2) – 4。下图进行对比，由于API比对处于逆操作状态，逻辑请反着看。

**1）新旧版本组件对比**

新版本组件。

旧版本组件

**4. Backdoor载荷托管平台迁移**

作为基础设施整合的一部分，该组织已将最终攻击阶段的后门（Backdoor）程序，从原先的Bitbucket平台迁移到了GitHub进行托管，以适应其整体策略的调整。

**四、归属研判**

我们将此次活动归因于APT-C-60（伪猎者）组织，主要基于以下两方面：

**1. 技术手法的同源性**

- 加密风格一致： 新样本中的字符串加密算法与历史样本的风格高度吻合。
- 核心逻辑一致： 各组件的核心功能与代码架构继承自该组织的历史版本。
- 代码特征一致： 在未经过深度混淆处理的代码部分，其特征与历史样本依然能够关联。

**2. 基础设施的关联性**

- 账号体系关联：新旧恶意仓库关联源头均隶属于同一攻击者的GitHub账户体系之下，存在管理上的关联。

## 总结

APT-C-60（伪猎者）组织近期的活动表现出一种成熟且敏捷的攻击姿态，其特点可概括为：
高强度的隐蔽策略：通过“阅后即焚”式的仓库管理和不断更换“马甲”账号，极力规避追踪与溯源。
持续升级的对抗能力：将代码混淆技术与Git操作特性相结合，为恶意软件分析设置了层层障碍。
这些迹象明确表明，“伪猎者”组织正密切关注着安全社区的分析与披露，并具备快速迭代其攻击工具、技术和流程（TTPs）的能力。可以预见，随着攻击行动的持续，该组织的攻击载荷、功能模块以及投递方式仍将不断演变，保持其威胁的持久性与有效性。

## 附录 IOC

boygem436/botgen

23.81.42.154

185.181.230.110

92fc5b1fe70f10f518597fc85a70c451(Backdoor)

76edf07d868817689728150311c6a490(Backdoor Install)

## 团队介绍

**TEAM INTRODUCTION**
**360高级威胁研究院**
**360高级威胁研究院是360政企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。**

本篇文章来源于微信公众号: 360威胁情报中心