猎影追踪：APT37利用朝鲜政治话题针对韩国的攻击活动分析

By 猎影实验室

Archived: 2026-04-05 18:37:27 UTC

近日，安恒信息猎影实验室在日常威胁狩猎中发现APT37组织多次利用朝鲜相关政治话题诱饵，向目标用户下发ROKRAT木马窃取信息。

猎影

针对韩国的APT组织

APT37组织又名Group123、InkySquid、Operation Daybreak、Operation Erebus、Reaper Group、Red Eyes、ScarCruft、Venus 121。

该组织至少从2012年开始活跃，主要针对韩国的公共和私营部门。2017年，APT37将其目标扩展到朝鲜半岛之外，包括日本、越南和中东，并扩展到更广泛的垂直行业，包括化学、电子、制造、航空航天、汽车和医疗保健实体。

2023年，APT37组织开始针对国内用户进行网络钓鱼，涉及Windows和Android平台。

样本信息

我们捕获的两条较为攻击样本如下：

样本一：(安全专栏)安全机构不应对反国家势力束手无策.zip

文件名	(안보칼럼) 반국가세력에안보기관이무기력해서는안된다.zip (安全专栏)安全机构不应对反国家势力束手无策.zip
文件hash	5127bf820b33e4491a93165cfdd25be4
文件格式	zip
文件大小	221.43MB

样本一中释放的诱饵为韩国国家安全与统一研究所高级研究员、檀国大学行政法研究生院兼职教授、21世纪战略研究所所长发布的专栏文章，文章讨论了朝鲜敌意的加剧以及对外部渗透和间谍活动的担忧。

样本二：对朝鲜的贡献(1).zip

文件名	북한지기고문 (1).zip 对朝鲜的贡献(1).zip

文件hash	29f494e0a66158a808b39299267c5c53
文件格式	zip
文件大小	53.62 MB

样本2具有多个诱饵，为朝鲜研究所研究员以及社会人士发表的各类朝鲜政治话题的文章，推测该样本用于攻击朝鲜政治主题相关研究人员。

思考总结

随着近期朝鲜领导人提出“北南关系再也不是同族关系、同质关系，而且完全固定为敌对的两个国家关系、战争中的两个交战国关系”，朝韩关系骤然紧张。

APT37组织多年来持续性的对韩国发起攻击，持续恶化的两国关系不仅为该组织提供了更多的攻击动机，韩国民众对于朝韩关系关注度的上升也有利于该组织使用鱼叉式钓鱼邮件等方式进行攻击。

从本次捕获的攻击样本来看，该组织的核心攻击木马较一年前无太大变化，仅通过改变诱饵文件以及木马加载方式来提高攻击成功率。

这种简单快捷的攻击方式虽然可快速发起攻击，但也存在易被安全产品检测的问题，因此该组织在不断提高压缩包的大小以逃避检测。随着两国关系的持续紧张，相信未来该组织会进行更多类似的攻击活动。

防范建议

目前安全数据部已具备相关威胁检测能力，对应产品已完成IoC情报的集成。针对该事件中的最新IoC情报，以下产品的版本可自动完成更新，若无法自动更新则请联系技术人员手动更新：

1. AiLPHA分析平台V5.0.0及以上版本

2. AiNTA设备V1.2.2及以上版本

3. AXDR平台V2.0.3及以上版本

4. APT设备V2.0.67及以上版本

5. EDR产品V2.0.17及以上版本

安恒云沙箱已集成了海量威胁情报及样本特征。

用户可通过云沙箱：https://sandbox.dbappsecurity.com.cn/对可疑文件进行威胁研判并下载分析报告。或用沙箱打开不明来源的未知文件，在虚拟环境中进行内容预览，免于主机失陷、受到木马或病毒文件攻击。

下载方式

猎影追踪

《APT37利用朝鲜政治话题针对韩国的攻击活动分析报告》为安恒研究院猎影实验室独家发布，**如对此研究感兴趣或欲了解报告更多详细，请前往下载。**

方式一：扫描下方二维码即可下载

方式二：点击下方链接或文末“阅读原文”即可下载

https://app-martech.dbappsecurity.com.cn/resources/ResourcePc/ResourcePcInfo?pf_uid=17709_1776&id=321&source=1&pf_type=3&channel_id=8987&channel_name=%E5%AE%89%E6%81%92%E7%A0%94%E7%A9%B6%E9%

方式三：联系安恒信息当地商务人员获取

关于猎影追踪系列报告

猎影追踪系列报告旨在提供有价值的网络安全信息和洞察，包含对网络安全领域最新的威胁趋势、漏洞发现、攻击手法以及防御策略等内容。该报告还基于猎影实验室的研究成果和实战经验，针对不同的安全问题提出可依循、可执行的建议，帮助企业提升自身的安全防护能力，更好地应对不断变化的网络安全挑战。
