奇安信威胁情报中心

背景

SideCopy组织至少自 2019 年以来一直在活动，主要针对南亚国家的国防军和武装部队人员、陆军人员进行窃密活动。该组织通过模仿响尾蛇APT的攻击手法来传递自己的恶意软件，并以此达到迷惑安全人员的目的。

2021年11月15日，奇安信威胁情报中心红雨滴团队首次发现SideCopy组织使用由Python 打包的双平台攻击武器[1]，活动中使用的初始攻击样本是一个包含Linux桌面启动文件的压缩包，该文件在执行之后会下载并播放莫迪总统访美视频以迷惑受害者，同时下载一个用于下载RAT的脚本并执行。

经分析，我们可以确认该RAT是一款支持Windows和Linux双平台的远控工具。通过C&C关联发现，该团伙武器库中还包含Mac OS平台的Bella RAT。之后我们加强了对该组织的持续关注及追踪。

2021年12月20日，我们再次捕获SideCopy APT组织以印度国防参谋长坠机相关事件为诱饵进行的攻击[2]。诱饵文档利用远程模板注入，远程加载并执行含有恶意DDE域代码的文档文件，通过恶意域代码下载vbs脚本到本机执行下发后续恶意代码。

概述

近日，红雨滴团队研究人员在日常威胁狩猎中再次捕获到一例针对Linux平台的攻击样本。与上次不同的是，此次捕获样本由Go语言编写而不是Python，该样本功能较为单一，仅实现了对目标受害者主机目录的扫描和窃取。遗憾的是，由于C2失效，我们没有获取到完整的攻击链，以及更深入的研究分析。

样本信息

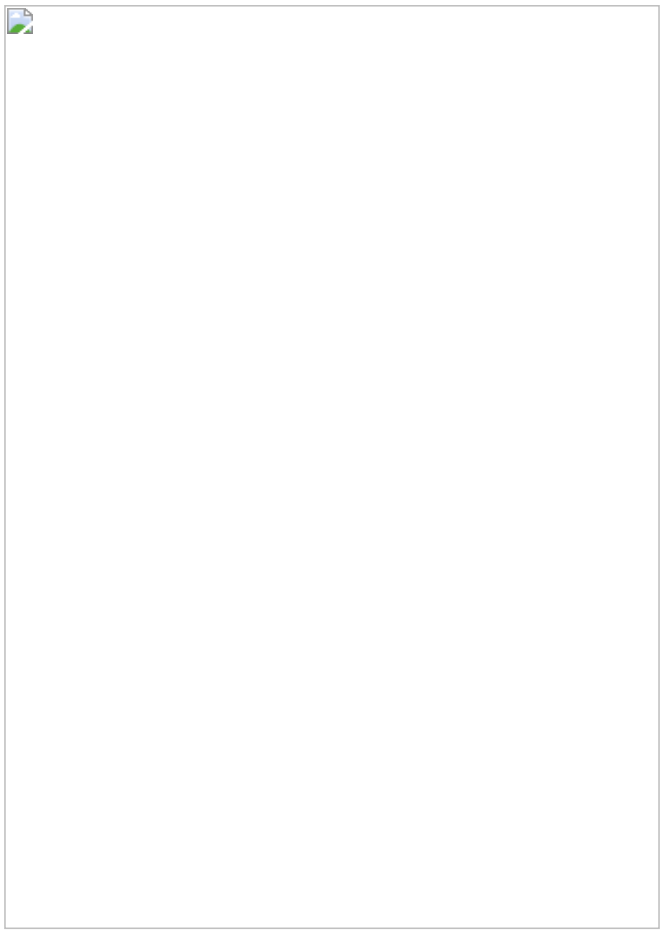
本次捕获到的样本均为Linux 64位系统的ELF文件。本文将此次捕获到的样本分为两类，两类样本在基本结构、功能上大抵相似，不同之处在于其中一类样本获取了本机IP地址并进行了持久化操作。具体信息如下：

-	-	-
文件名	**MD5**	**类型**
host	5fd6fc76b3ec2f5c97a44bf7bd3de972	1
climax	34d9dff0aa80f6ea7eea6f491d493fa3	1
update	64149e187f678f3131746d2975b8a8dc	1
version	fea8b786f469e723e8fdb7ed630ba850	2

详细分析

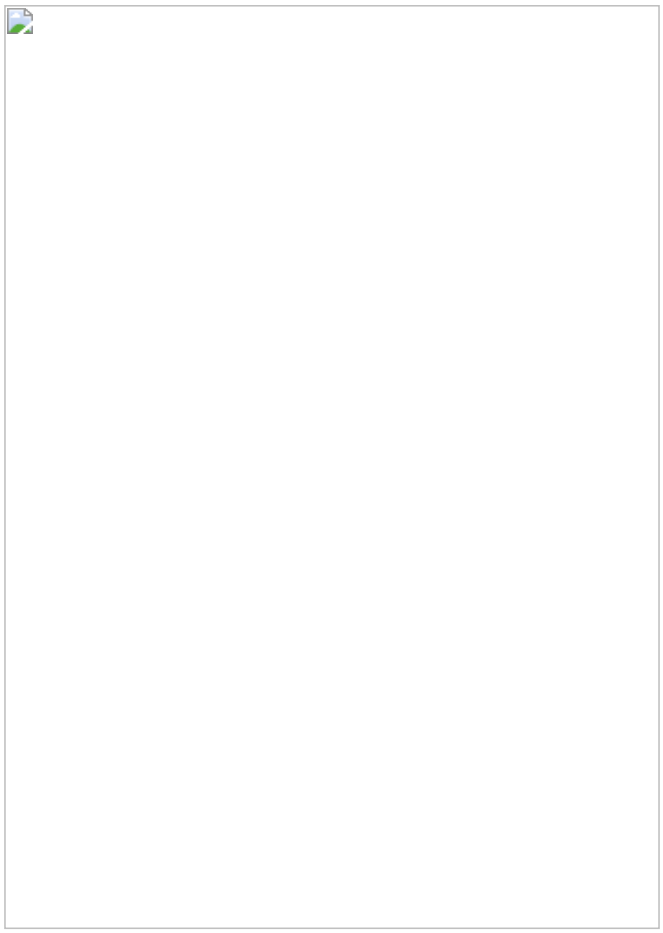
首先以第一类样本，即没有持久化的样本34d9dff0aa80f6ea7eea6f491d493fa3为例进行分析。

样本运行后将获取当前用户信息，以及主目录，并判断是否存在“/tmp/lists.txt”文件。

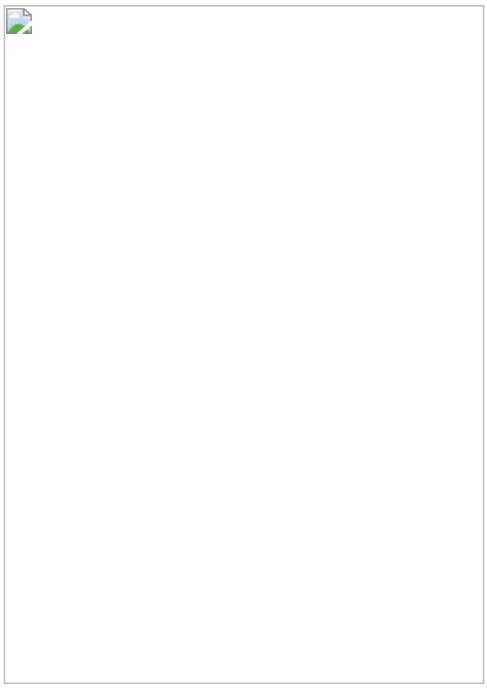


若“/tmp/lists.txt”文件不存在，则样本将会先遍历主目录信息，然后在/tmp目录下创建lists.txt，并将结果存放在里面，上传C2为207.180.243[.]186:8062。

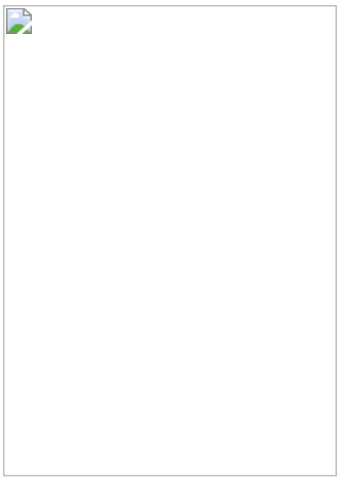
若“/tmp/lists.txt”存在则跳过主目录遍历，直接进入下一步操作。



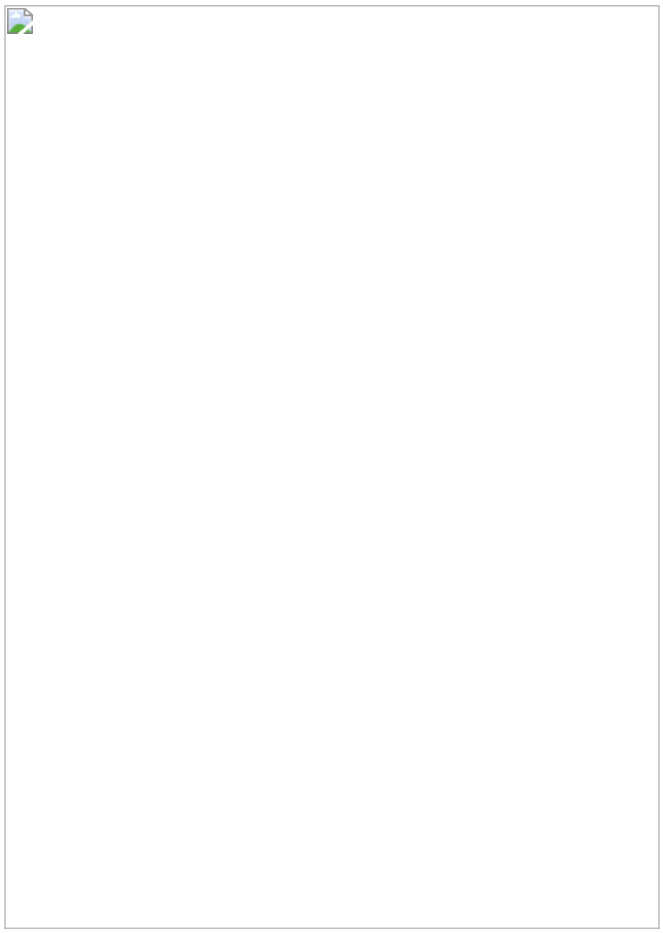
遍历的结果如下：

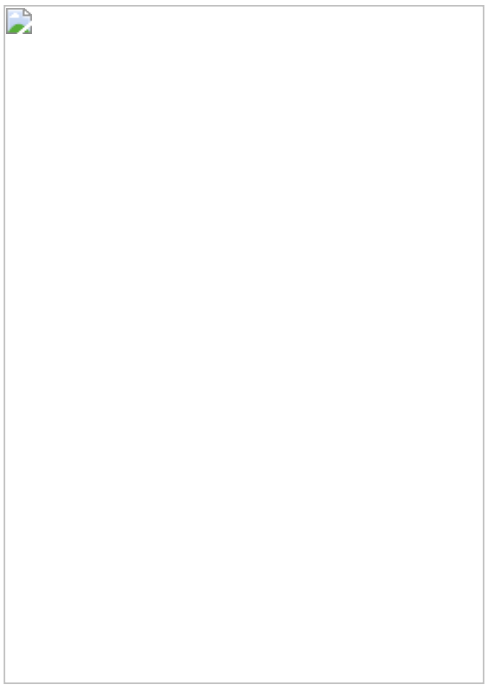


用于上传C2的部分：



之后，继续扫描/home/目录下带特定扩展名的文件，并创建/tmp/temp.txt，用于存放上传文件的记录，之后将扫描结果逐一上传C2，上传完成后便结束程序。





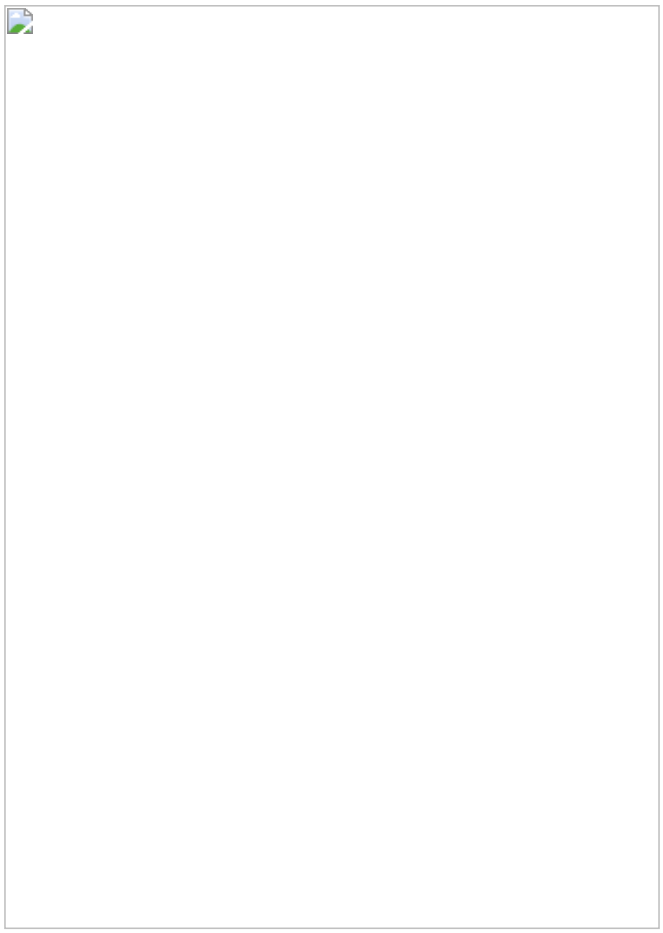
样本所扫描的扩展名包括.css、.csv、.doc、.egm、.gif、.htm、.jpg、.mjs、.odt、.oef、.pdf、.png、.ppt、.sdd、.sec、.svg、.txt、.xls、.xml等。

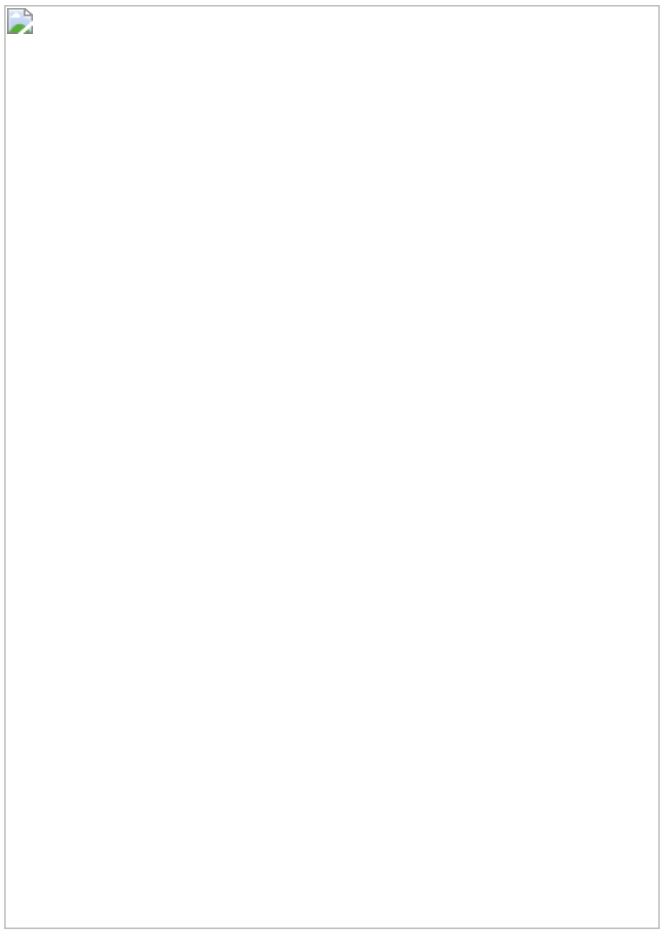
两类样本的不同之处

第二类样本与第一类样本的不同之处在于：

1. 样本运行后首先向api.ipify.org 发送GET请求获取受感染系统的IP地址，之后再进行获取用户信息的操作；

1. 在获取到用户信息之后，样本会通过“/.config/autostart/”目录实现开机自启，获得持久化。

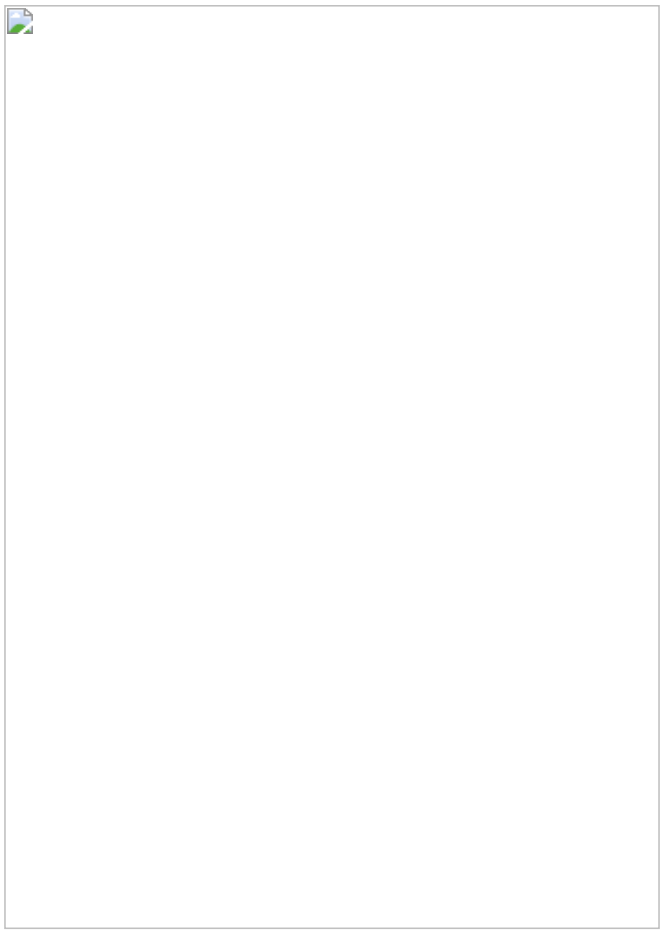




之后的流程便与第一类样本完全相同。最终连接到的C2为164.68.108[.]153:8062。

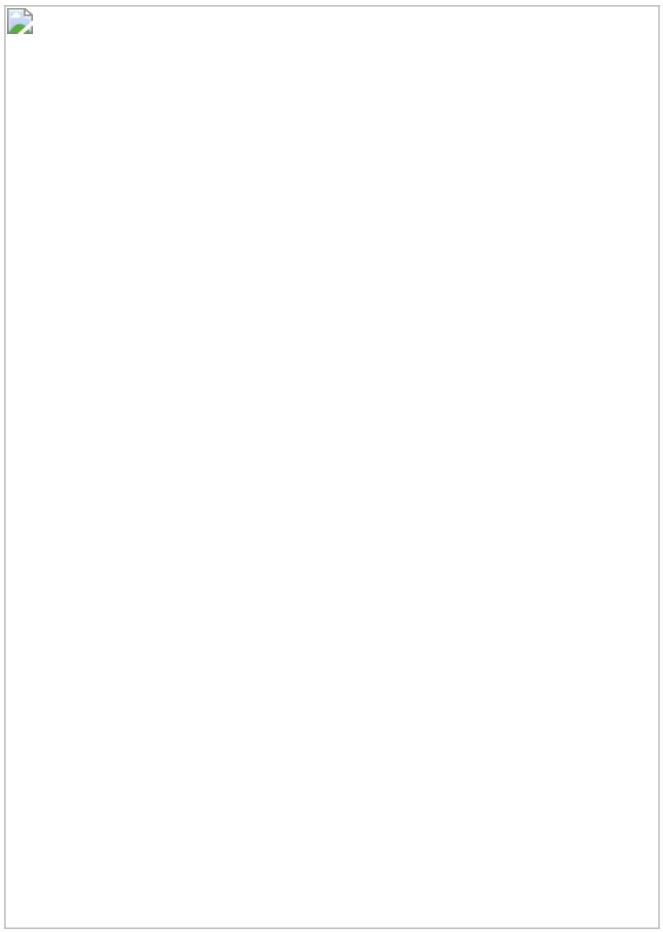
关联分析

我们在分析过程中发现，第一类样本使用的C2：207.180.243[.]186，与《印度国防参谋长坠机：SideCopy APT组织趁火打劫》[2]一文中恶意PowerShell脚本请求的C2相同，下图为文中样本执行流程：

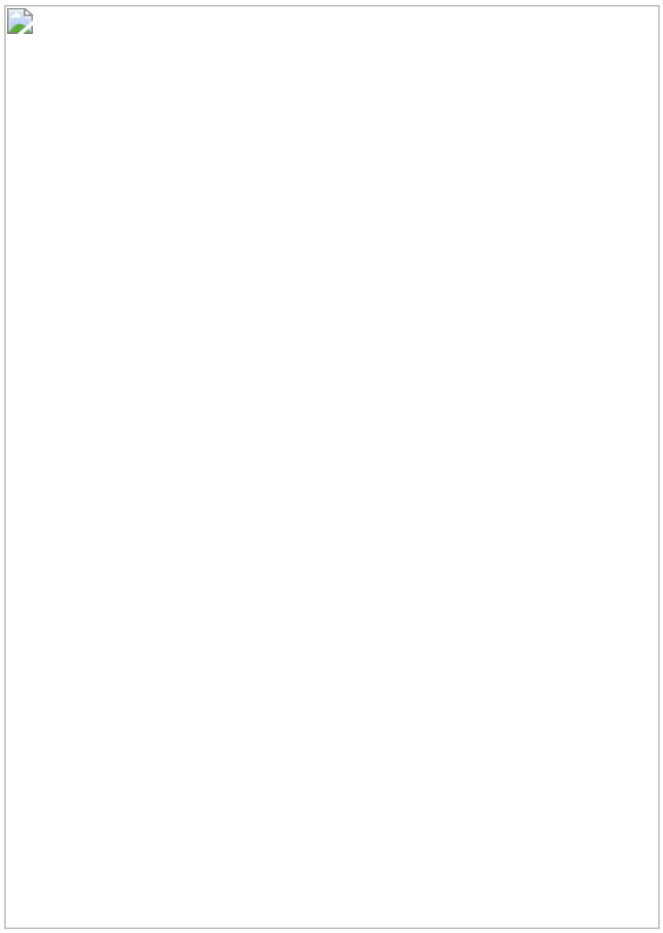


根据攻击流程来看，SideCopy组织利用207.180.243[.]186下发后续攻击组件。而本次捕获的样本功能简单，很像某条攻击链中使用的某一组件。虽然《印度国防参谋长坠机：SideCopy APT组织趁火打劫》一文中披露的是针对Windows平台的攻击，但我们猜测该组织可能在同一时期开始策划针对Linux平台的攻击。

其次通过奇安信威胁情报文件深度分析平台可知本文中样本的下载链接为“hxxp://assessment.mojochamps[.]com/uploads/v/filename”。



该下载链接与此前我们披露的SideCopy攻击活动中的诱饵文档下载链接“hxxp://assessment.mojochamps[.]com/images/Jointness.docx”、“hxxp://assessment.mojochamps[.]com/uploads/v/3.php”所属域名均相同。



结合之前的两篇分析报告，我们发现SideCopy组织在2021年11月就入侵了合法网站“hxxp://assessment.mojochamps[.]com”，并将其用于挂载诱饵文档及相关恶意后续载荷。不难看出，SideCopy组织通过这一网站同时进行了Windows、Linux两个平台的攻击活动。

此外，通过我们本次捕获到的Linux样本再次印证了该攻击团伙将攻击能力覆盖包括Linux、Windows等多个平台的意图，且为此在不断发展新的攻击武器。

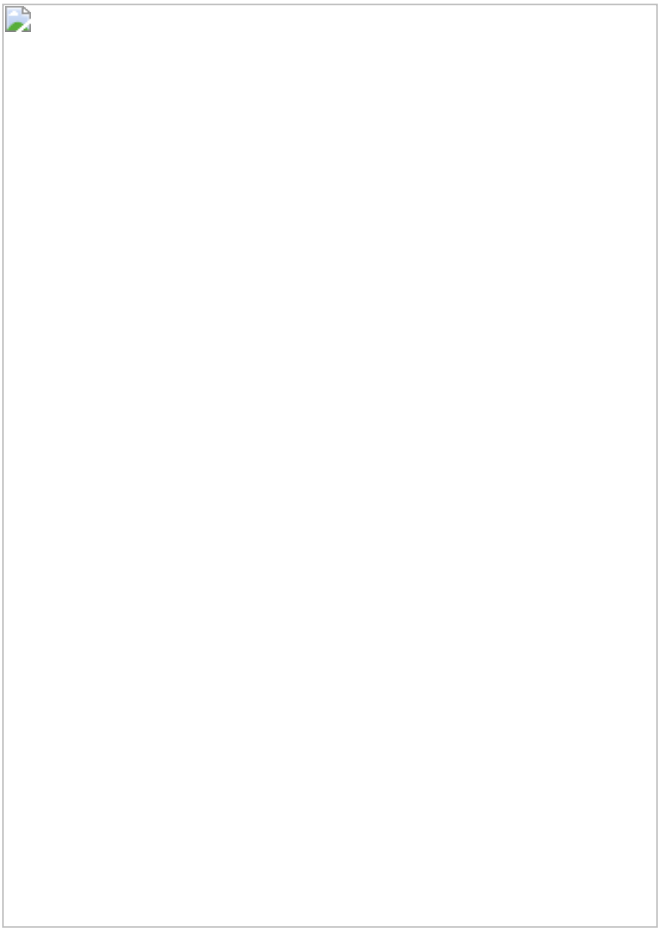
总结

SideCopy作为近年才被披露的APT组织，在2021下半年进入高度活跃的状态。近期，我们发现SideCopy组织不再满足于使用网络上开源的代码及工具，而是试图发展其攻击能力，更新其武器库。奇安信威胁情报中心会对其进行长期的溯源和跟进，及时发现安全威胁并快速响应处置。

此次捕获的样本主要针对南亚地区开展攻击活动，国内用户不受其影响。奇安信红雨滴团队提醒广大用户，切勿打开社交媒体分享的来历不明的链接，不点击执行未知来源的邮件附件，不运行标题夸张的未知文件，不安装非正规途径来源的APP。做到及时备份重要文件，更新安装补丁。

若需运行，安装来历不明的应用，可先通过奇安信威胁情报文件深度分析平台（https://sandbox.ti.qianxin.com/sandbox/page）进行判别。目前已支持包括Windows、安卓平台在内的多种格式文件深度分析。

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信NGSOC、奇安信态势感知等，都已经支持对此类攻击的精确检测。



IOCs

MD5

5fd6fc76b3ec2f5c97a44bf7bd3de972

34d9dff0aa80f6ea7eea6f491d493fa3

64149e187f678f3131746d2975b8a8dc

fea8b786f469e723e8fdb7ed630ba850

C2

164.68.108[.]153:8062

207.180.243[.]186:8062

URL

http://207.180.243[.]186:8062/one

http://164.68.108[.]153:8062/one

参考链接

1. https://ti.qianxin.com/blog/articles/Sidecopy-dual-platform-weapon/
2. https://ti.qianxin.com/blog/articles/SideCopy-APT-Group-Takes-Advantage-of-the-Fire/