APT组织Confucius针对巴基斯坦IBO反恐行动的网络攻击事件分析

blog.nsfocus.net/aptconfuciuspakistanibo/

伏影实验室

一、概述

受多方因素影响，巴基斯坦长期遭受严重的地方恐怖主义威胁，该国一直以来也将反恐作为重要的国家安全战略。2022年下半年，巴基斯坦安全部队在俾路支省、开伯尔区、北瓦济里斯坦区等地展开了多次基于情报的行动（intelligence-based operation, IBO）,突袭并击毙了多名恐怖分子。

巴基斯坦方面近期在反恐方面的高调表现引发了印度方面的关注。11月30日，绿盟科技伏影实验室捕获了一起针对巴基斯坦木尔坦地区武装力量的网络攻击事件，攻击者以木尔坦的罗德兰区IBO行动报告为诱饵，尝试投递一种变种木马程序以控制受害者设备。绿盟科技伏影实验室经过分析，确认该事件的主导者为印度方面的APT组织Confucius。

二、组织关联

Confucius是一个由印度资助的APT组织，从2013年开始执行网络攻击活动，主要目标为巴基斯坦、中国等印度邻国，对军事、政府与能源等领域的目标具有浓厚兴趣。

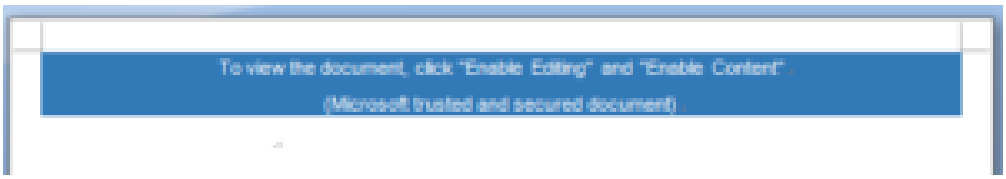
Confucius组织会同时使用Windows端木马程序与Andriod端木马程序对目标进行间谍攻击以窃取情报，使用的攻击工具包括SubBird、CharSpy和Hornbill等，具有较强的开发能力和渗透能力。

本次攻击事件中，Confucius攻击者沿用了其常见的诱饵构建模式，并且使用了该组织已知攻击工具MessPrint的新版本变种程序。

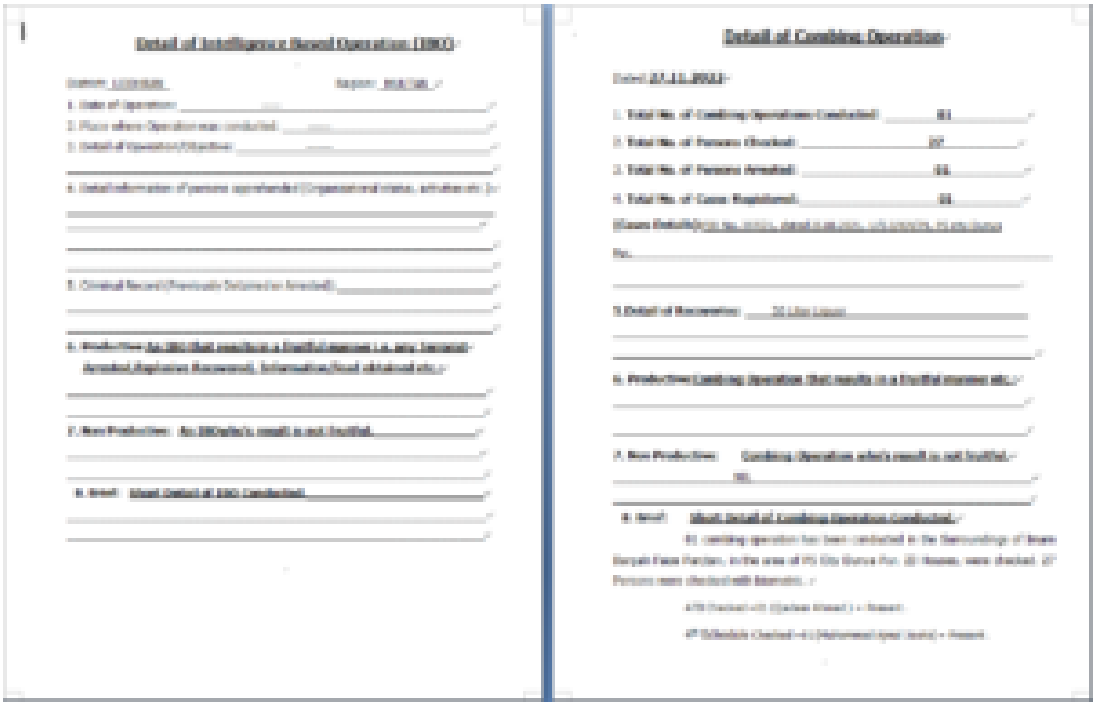
三、攻击流程

本次网络攻击事件中，Confucius攻击者构建了名为“IBO_Lodhran.doc”（罗德兰地区基于情报的行动）的钓鱼文档以及名为“US_Dept_of_State_Fund_Allocations_for_Pakistan.doc”（美国国务院对巴基斯坦的资金分配）的钓鱼文档，分别针对巴基斯坦的安全部队与外交类政府部门。

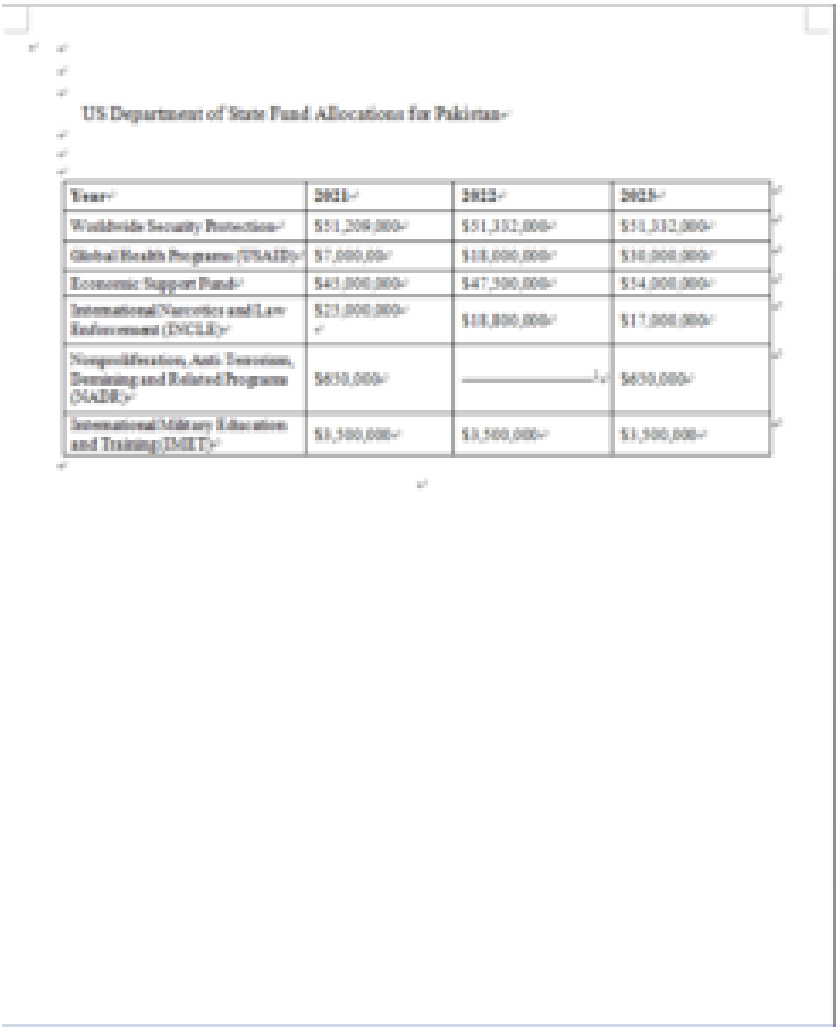
这些钓鱼文档携带了具有一定真实度的情报内容，并通过提示信息诱使受害者启动文档的编辑功能，进而执行一种植入变种木马的攻击流程。



钓鱼文档的提示信息



IBO_Lodhran.doc钓鱼文档内容

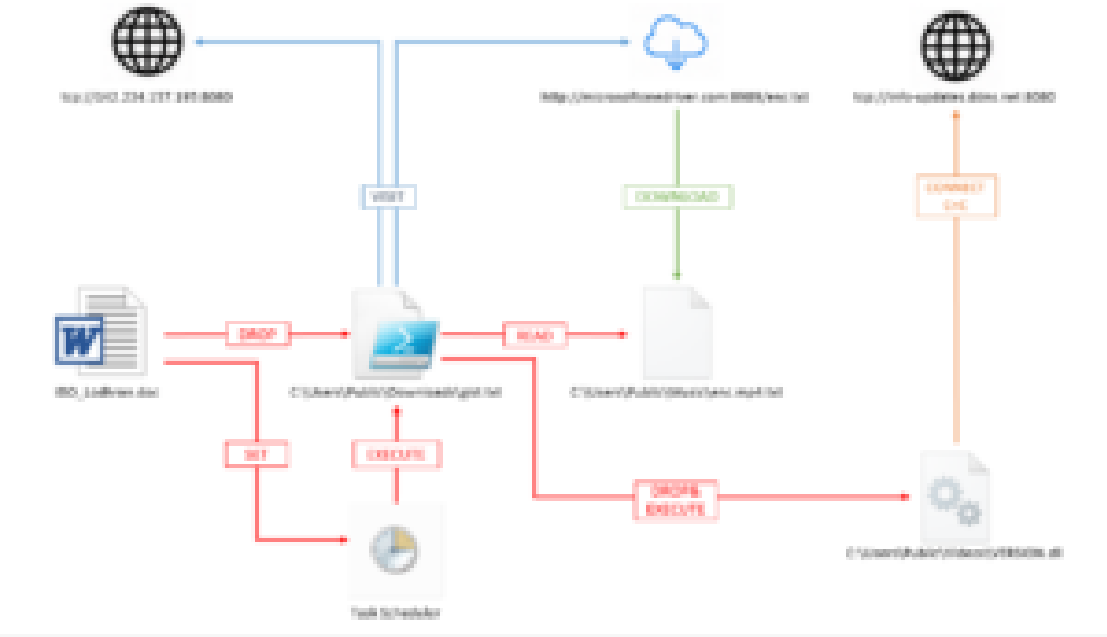


US Department of State Fund Allocations for Pakistan

Year	2021	2015	2025
Worldwide Security Protection	$51,209,000	$51,332,000	$51,332,000
Global Health Programs (USAID)	$7,000,00	$10,000,000	$10,000,000
Economic Support Fund	$43,000,000	$47,500,000	$54,000,000
International Narcotics and Law Enforcement (INCLE)	$23,000,000	$18,800,000	$17,000,000
Nonproliferation, Anti-Terrorism, Demining and Related Programs (NADR)	$650,000	———————	$650,000
International Military Education and Training (IMET)	$3,500,000	$3,500,000	$3,500,000

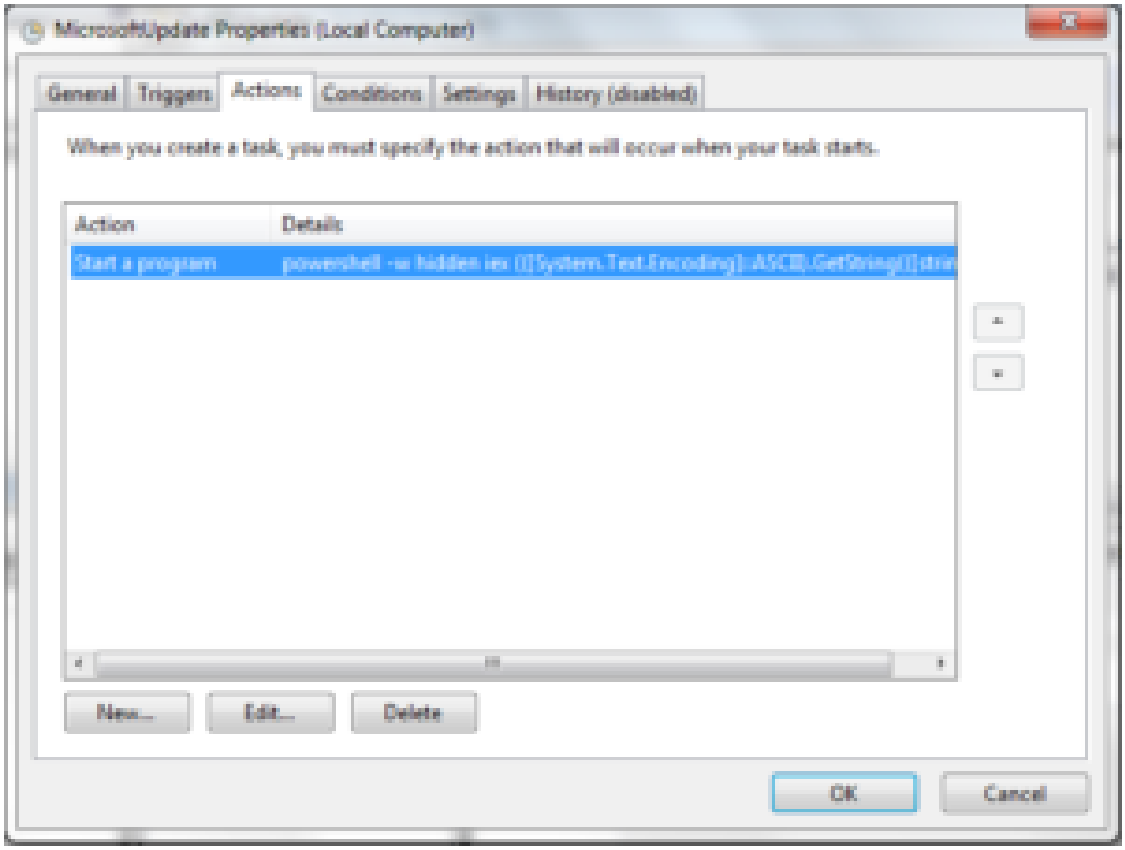
图 3.3 US_Dept_of_State_Fund_Allocations_for_Pakistan.doc钓鱼文档内容

本次事件中的典型攻击流程如下图所示。



本次事件的典型攻击流程

当上述钓鱼文档中的宏被执行后，文档向指定目录释放一个名为gist.txt的加密文件，并设定一个每30分钟运行一次的计划任务定期运行该文件。



钓鱼文档设置的计划任务

被运行的gist.txt实际上是一种powershell木马，首先向固定位置tcp://142.234.157[.]195:8080发起链接以测试连通性，并上传本机的用户名、计算机名、mac地址、系统信息等内容作为注册信息；随后从固定位置http://microsoftonedriver[.]com:8989/enc.txt下载一段加密数据，解密为VERSION.dll并借助rundll32组件加载执行。

该VERSION.dll文件为Confucius攻击者在本次事件中使用的主要木马程序，其连接CnC为tcp://info-updates.ddns[.]net:8080。

四、木马分析

本次事件中出现的主要木马程序VERSION.dll，是Confucius一种已知攻击组件的变种程序。为方便后续跟踪，伏影实验室将该攻击组件暂命名为MessPrint。

与既往版本相比，本次Confucius使用的新版MessPrint木马程序在功能和对抗方面的变化很大，其主版本号也从2.X.X升级至3.1.0。

功能

本次出现的MessPrint变种木马，其主要功能分为运行日志记录、受害者主机信息上传与命令执行三部分。

木马运行后，首先在C:\ProgramData目录下创建一个名为log.txt的日志文件，后续木马在运行至每个阶段时，都会将提示信息记录至该日志文件中。我们没有在既往版本木马程序中发现该记录功能，因此推测该版本的木马是测试版本，被Confucius攻击者直接使用在网络攻击活动当中。

随后，木马程序收集受害者主机的各项信息，并将这些信息汇总为一段加密数据发送至CnC处。该木马收集的信息见下表。

木马收集的信息列表

MessPrint变种木马收集的主机信息	内容示例
主机名\用户名	WIN-SBSB6AEF44L\superlove
适配器mac地址	00:0C:29:D0:13:FA
操作系统主版本	Windows 7
操作系统位数	version x64
当前进程PID与路径的列表	PID NO:300——C:\Windows\System32\smss.exe PID NO:396——C:\Windows\System32\csrss.exe

已安装软件列表	AddressBook Connection Manager

上述信息直接使用固定符号#$#*作为分隔符，末尾使用固定符号iqaz作为结束标志。

上述信息将使用以下加密方式加密后再发送给CnC：

1. 逐字节异或0x1D；
2. Base64转码；

该变种木马程序与CnC的后续通信皆遵循以上加密方式。

发送主机信息后，该变种木马程序与CnC使用”check_status”、”verified”、”hi”、”order”等关键词进行多轮确认后，最终进入指令执行模式。在指令执行部分，该MessPrint木马可以响应CnC下发的以下指令和参数，进行文件下载、程序运行、CMD指令执行等命令。

木马CnC指令列表

CnC指令	指令参数1	指令参数2	功能
DWN	文件保存位置		下载CnC处发送的文件至指定位置
ALT	程序位置	程序运行参数	运行CnC指定的程序
APP	CMD命令		运行CnC指定的CMD命令
black	休眠时间		休眠指定的时间

通过分析发现，该版本的MessPrint木马程序在功能部分作出了很多改动，一方面通过加密的方式保护CnC通信过程，另一方面大幅削减了既往版本木马中的文件窃取与反弹shell等功能。

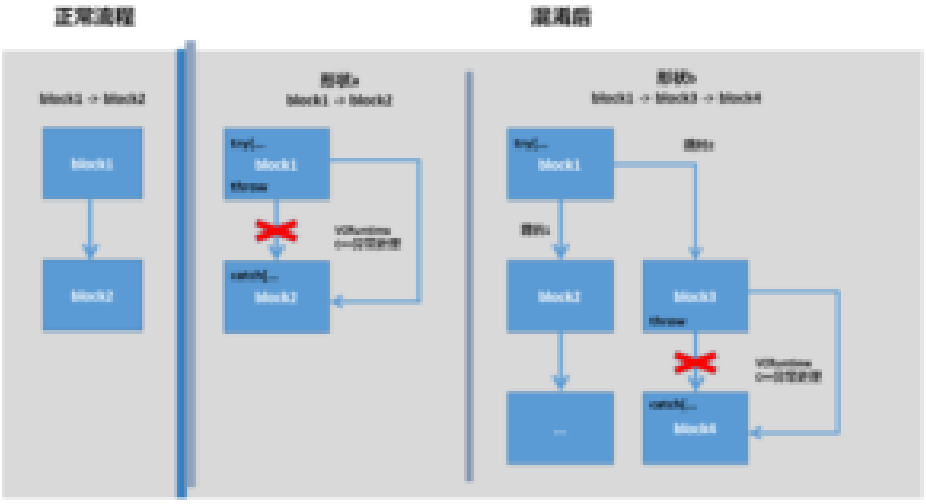
上述改变说明，该木马程序的定位从全功能间谍软件转变为Stub类后门木马，通过组件拆分将后续的间谍木马功能分离成独立的组件。这种变化在近几年的APT攻击组件发展过程中十分常见，APT攻击者可以通过这种细化来降低整体框架的暴露风险。

对抗

在本次出现的MessPrint木马程序中，Confucius开发者加入了大量反分析技术，增加了木马程序的分析难度。

该MessPrint木马主要使用了一种基于异常的控制流混淆技术，这种混淆将普通的线性流程改为try-throw-catch结构，使得原来线性相接的两段代码被分割到不再相邻的try与catch块中。这样，在特定位置throw出c++对象，使得执行流程需通过VS的C++异常处理来跳至原本在线性结构下可以直接执行的代码。

下图展示了这种基于异常的控制流混淆的基本逻辑：



MessPrint木马使用的混淆思路

这种混淆方式可针对一些反编译工具的静态分析，因为多数伪代码无法正常还原上述异常处理流程。

此外，Confucius开发者还在该MessPrint木马中滥用了一些常见的代码混淆技术，如栈膨胀、花指令和无意义代码，进一步阻碍静态分析。考虑到该版本MessPrint木马中出现的大量开发中的痕迹，我们推测Confucius开发者是在不得已启用开发版本程序的情况下，希望使用混淆的方式减少暴露后造成的损失。

五、小结

作为国家武装力量在和平时期的直接展示，巴基斯坦近期举行的一系列IBO反恐行动使印度方面非常敏感，本次捕获的APT攻击事件也说明印度方面开始将网络攻击力量投入到相关的侦察活动当中。

通过对本次Confucius攻击事件的分析，我们一方面发现Confucius开发者依然保持比较活跃的攻击组件开发节奏，另一方面也证实了APT组织开发者正在普遍进行攻击组件的拆分和框架化工作。由于近年来防守方在APT捕获、分析和披露流程的逐渐完善，APT攻击者不得不使用框架化的思路重新构建攻击工具，通过逐级投递的方式控制各级组件的使用，以减少完全暴露的风险。

六、IoC

钓鱼文档：

c75b8c150054b5ba27cf08c46e13354e

23537d81e9cd285b41185a0e4c3d37c1

加密powershell木马文件：
ab34c3eb8635fc13e4a586cba3c7469d

powershell木马CnC:

142.234.157[.]195:8080

下载地址：
http[:]//microsoftonedriver[.]com:8989/enc.txt

MessPrint变种木马程序：
65d9b142924d4e74cb729166f41b16fa

MessPrint木马CnC:
info-updates.ddns[.]net:8080

关于伏影实验室

研究目标包括Botnet、APT高级威胁，DDoS对抗，WEB对抗，流行服务系统脆弱利用威胁、身份认证威胁，数字资产威胁，黑色产业威胁及新兴威胁。通过掌控现网威胁来识别风险，缓解威胁伤害，为威胁对抗提供决策支撑。