

APT-C-35（肚脑虫）近期针对巴基斯坦新型木马攻击活动分析 | CTF导航

ctfiot.com/284246.html

APT-C-35

肚脑虫

APT-C-35（肚脑虫）组织（又称Donot）是一个来自南亚地区的境外APT攻击组织。该组织主要针对巴基斯坦及周边国家的政府机构开展网络攻击活动,以窃取敏感信息为主要目标，攻击活动最早可追溯到2016年，近年来其活动频率明显增加，使用的攻击组件也不断更新迭代。

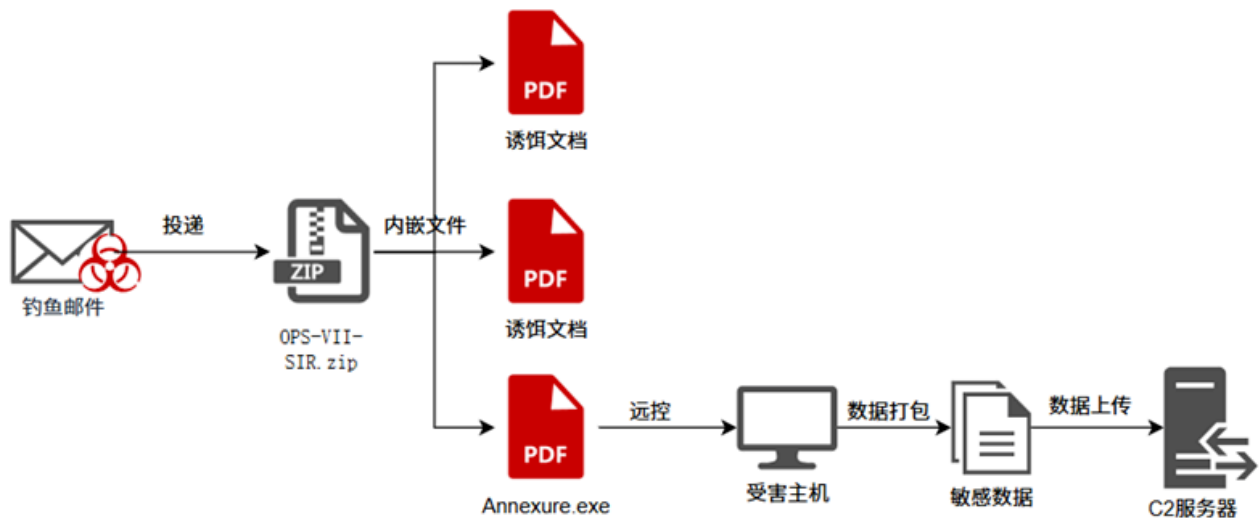
一、概述

近期360安全大脑监测到肚脑虫组织针对巴基斯坦的攻击活动，此次活动中使用新型的远控木马—ShadowAgent，该木马对进程图标进行伪装，诱使用户点击，使用WebSocket+HTTP与服务器进行通信。本文将对攻击活动相关组件进行分析。

一、攻击活动分析

1. 攻击流程分析

本次攻击活动中，该组织使用含有木马的压缩包作为攻击载体。文件解压后，压缩包内包含两个诱饵文档，以及一个将恶意木马程序伪装成PDF文档图标的可执行文件。当用户误执行该木马后，其首先会从自身的资源段中读取经过加密的配置信息，随后通过创建计划任务的方式在系统中建立持久化驻留。最终，该木马会窃取用户设备上的敏感数据并外传至攻击者控制的服务器。



2. 恶意载荷分析

在本次攻击活动中，捕获的恶意样本基础信息如下：

MD5 1c335be51fc637b50d41533f3bef2251

文件名称 OPS-VII-SIR.zip

文件大小 1.04 MB (1088584 bytes)

文件类型 zip

压缩包内嵌文件如下：

基于对该诱饵文档的详细内容分析，推测此次攻击活动目标为巴基斯坦。

样本运行后首先从可执行文件中加载名为“TYPELIB”的资源段。该资源段大小为0x1A1字节，整体内容以加密形式存储，用于隐藏核心运行参数与通信配置。

解密后的配置如下：

```
{
  "network": {
    "domain": "www.mydropboxbackup.com",
    "port": 443,
    "https": true,
    "prefix": "analytics"
  },
  "identity": {
    "project": "CTD KP",
    "contact": "kpctd@gov.pk",
    "process_lock": "hardcoded_lock",
    "cf_uid": "SA",
    "agent_name": "ShadowAgent"
  },
  "persistence": {
    "filename": "CHANGE_THIS.exe",
    "mute_x_prefix": "asus_4df7009c18a879e7",
    "task_name": "",
    "startup_method": 1,
    "location": 1,
    "enable_app_path": true
  }
}
```

样本通过schtasks创建名为“NVIDIA_taskHost”的伪装计划任务，每天上午9:00自动执行恶意文件Annexure.exe，用于在系统中维持持久化。

接着将获取到的用户信息进行拼接，其中包括设备标识、主机名、用户名、安全产品等。

样本将收集到的用户信息JSON结构打包，以post请求的方式发送至远程服务器（www.mydropboxbackup[.]com:443）。

接着会对比服务器响应的数据，是否为如下值。

构造WebSocket URL，用于与远控服务器建立连接。

木马上线后，主控端WebSocket发送指令从而对受害者机器实现远程控制，指令格式同样为json格式。

指令	功能
input	用于向开启的cmd或powershell进行指令输入
F1A5C3	读取cmd或powershell中指令执行结果
B8C1D2	创建cmd
E4F5A6	创建powershell
FL_SH1	结束cmd或powershell
C9E3D4	组合指令，主要功能从指定url下载数据。
E7F8A9	支持指定zip文件下载，并支持密码参数。
H1k4R8	
C0V3RT	
F2B3C4	磁盘遍历
D5E6F7	文件上传
A8B9C0	文件下载

D1E2F3 文件删除

A4B5C6 文件移动（重命名）

D7E8F9 文件夹相关操作

三、关联分析

与此同时，我们还关联到肚脑虫组织的另一款下载器木马，与本次分析的样本存在相同的数字签名信息，基础信息如下。

MD5 20c9ac59c444625a7ee364b410da8f11

文件名称 suv3xx.exe

文件大小 602.60 KB (617064 bytes)

文件类型 exe

样本在运行初期会创建名为“twl”的互斥体（Mutex），通过此机制实现单实例控制。

样本中的敏感字符串均未以明文形式存储，而是采用Base64编码+AES对称加密的组合方式进行保护。

Key:AB BD 3A 7B 8C B2 B4 C6 AB C7 D9 09 E4 E5 C2 C1 ,

Iv:BB B3 44 58 95 B3 C7 E1 75 C6 E7 D6 D9 D5 BD DB。

接着通过COM组件创建名为“.NET Framework NGEN v4.0.30319 64Update”的计划任务，实现样本持久化操作。

接着开始对受害主机进行窃密行为，获取主机的CPU信息、Windows版本、用户名、计算机名、安装软件列表等信息。通过AES+Base64进行数据加密，再与“mopd=”字符串进行拼接。

创建C:\ProgramData\pintokgkl.lnk文件，将加密的用户基础信息写入到文件中。

解密的配置信息如下图。

连接[https://brityservice\[.\]info:443//ZxStpliGBsfduMawer/lkhgBrPUyXbgllErASstylzsh](https://brityservice[.]info:443//ZxStpliGBsfduMawer/lkhgBrPUyXbgllErASstylzsh)，接着将加密的用户敏感数据作为上线包发送至服务器。

检查接收的数据是否包含“MFG”以及“？”字符串，接收数据需符合相应格式才会下载后续组件。

再次连接服务器，url路径为ZxStpliGBsfduMawer/lkhgBrPUyXbgllErAStylzsh/N1/SA，接着发送加密数据，解密后格式如下：用户名-计算机名-b0671###[#DI1104KillJunk32.dll](#)。然后创建C:\Users[username]\AppData\Local\EdgeUpdate\Wi0m.dll文件并写入数据。

样本会在系统中创建新的计划任务，以实现持久化驻留。该任务的执行内容为调用rundll32.exe加载并执行指定的恶意 DLL 文件，从而在系统重启自动重新激活样本。

最后执行“cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q “%s””，将下载器样本删除。

遗憾的是，目前已无法下载到后续的攻击载荷。

四、归属研判

1. 根据诱饵文档推测此次的攻击活动目标为巴基斯坦，符合攻击者目标。
2. 关联的下载器样本与历史APT-C-35（肚脑虫）组织的攻击武器代码存在较高相似度。

在下载器样本中，针对目标用户的敏感信息存储格式以及数据加密部分和以往APT-C-35（肚脑虫）组织的攻击武器保持高度一致，将窃取的数据进行AES+Base64加密并与某字符串进行拼接，最后作为上线包上传至服务器。上线包格式都是以“字符串=”为前缀。

其对C2返回数据处理逻辑也均是，判断首字节是否为“？”字符串，并判断返回数据中是否携带特定三字节字符。

该下载器样本与该组织历史攻击武器的逻辑一致，从远程服务器下载dll文件并保存到本地，创建计划任务进行持久化操作，而任务的执行内容都为调用rundll32.exe加载并执行指定的恶意DLL文件。

3.针对brityservice.info进行测绘，我们发现，该域名的jarm指纹信息为“28d28d28d00028d00042d42d00000051af7d8070a18e002eaaedf620fa118c”以及证书是Let's Encrypt、域名是.info域名，以上都符合我们所掌握的该组织基础设施测绘特征。

4.下载器木马与本次的分析的样本具有相同的证书，证书路径、序列号等信息均保持一致，属于强关联证据，表明签名文件由同一实体控制。

综上所述，我们将此次攻击活动归属APT-C-35（肚脑虫）组织。

总结

APT-C-35（肚脑虫）组织从2016年被披露后，从未停止相关攻击活动，并且有越来越活跃的趋势。本次针对巴基斯坦的攻击活动中，其使用的ShadowAgent木马将文件图标进行伪装并诱使用户点击，从而开展一系列的恶意行为，可见，该组织在持续优化攻击技术的同时，也在不断丰富其攻击武器库，以应对日益完善的网络安全防护措施。

在此提醒广大用户，请务必保持警惕加强网络安全意识，切勿点击陌生链接或运行来源不明的文件。以此降低被网络攻击的风险。

附录 IOC

MD5

1c335be51fc637b50d41533f3bef2251

f78fd7e4d92743ef6026de98291e8dee

20c9ac59c444625a7ee364b410da8f11

Domain

brityservice[.]info

www.mydropboxbackup[.]com

URL

wss://www.mydropboxbackup[.]com:443/analytics/stream?device_token=b4c08eab17da3c59

https://brityservice[.]info:443//ZxStpliGBsfdutMawer/lkhgBrPUyXbgIIErAStyilzsh

https://brityservice[.]info:443//ZxStpliGBsfdutMawer/lkhgBrPUyXbgIIErAStyilzsh/N1/SA

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