APT-C-35（肚脑虫）组织针对南亚某制造公司的攻击活动分析

By 高级威胁研究院

Archived: 2026-04-05 13:24:07 UTC

APT-C-35

肚脑虫

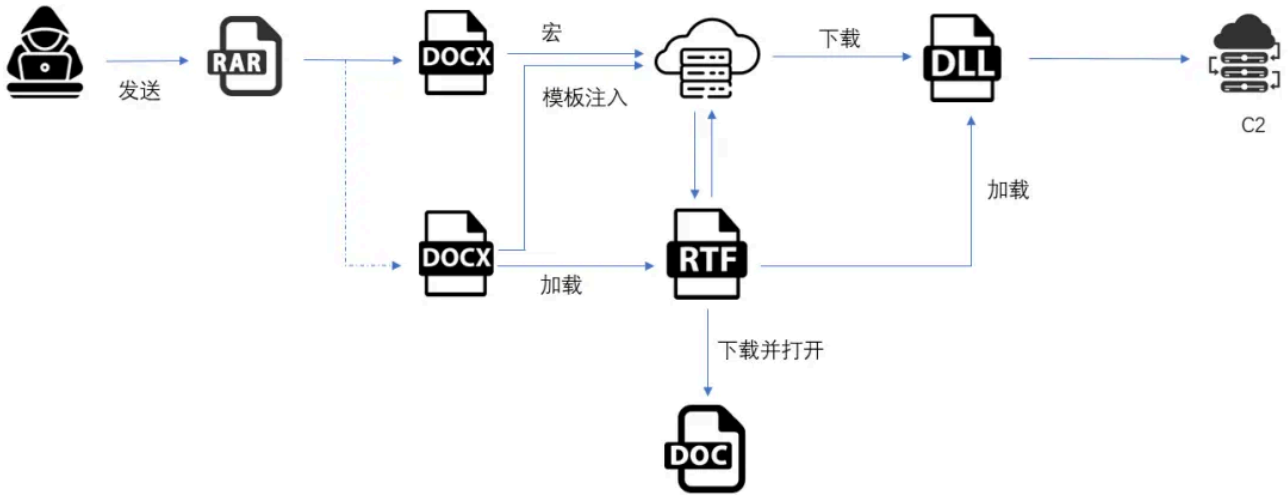
APT-C-35（肚脑虫）（又称Donot）是一个来自南亚地区的境外APT攻击组织。该组织主要针对巴基斯坦及周边国家的政府机构开展网络攻击活动,以窃取敏感信息为主要目标，攻击活动最早可追溯到2016年，近年来其活动频率明显增加，使用的攻击组件也不断更新迭代。

近期，360高级威胁研究院在日常威胁狩猎中多次发现APT-C-35组织针对巴基斯坦的攻击活动。在本轮攻击行动中，该组织采用宏文档和漏洞文档作为恶意载体，加载.NET全新攻击组件，从而实现窃密行动。鉴于这组件在以前的攻击活动中很少见，而且处于开发阶段，因此这里进行分析说明以免用户中招。

一、攻击活动分析

1.攻击流程分析

本轮攻击中，APT-C-35组织使用了两种方式来加载恶意组件，第一种方式是使用带宏的诱饵文件执行多层Shellcode，继而下载恶意DLL；第二种方式是使用模板注入加载含漏洞的RTF文档，当用户打开文档触发漏洞后就会下载诱饵文件，并释放恶意DLL。整个攻击流程如下所示：



2.恶意载荷分析

本次捕获了多个恶意样本，下面以其中一个宏样本进行分析，样本基本信息如下所示：

MD5	bd2b06d17faabc2b916ba89f56f7e200

文件大小	176 KB (180,878 字节)
文件名	SOP - Payables.doc

“SOP - Payables.doc”是一个含有恶意宏代码，伪装成Shibli Electronics Limited公司财会相关的SOP说明文档。Shibli Electronics Limited公司是巴基斯坦专门从事安全系统设计和制造的公司，其部分伪装内容如下所示。

比较有意思的是内嵌的宏代码在执行关键函数之前会校验密码，如果校验不通过则不会执行剩余的宏代码，猜测该密码可能通过上层邮件传递给受害者，以此避免沙箱等动态工具的查杀。同时期我们也捕获到没有校验密码的恶意宏文档。

校验通过后该宏代码会根据不同的系统架构通过CryptEnumOIDInfo函数执行不同的Shellcode。

Shellcode主要功能是下载后续DLL，但在此过程中会检测杀毒软件，且经过多层加密。Shellcode运行后首先会进行取非操作和异或运算进行代码自解密，然后动态获取关键API函数地址，接着从http[:]//office-updatecentral.com/eigenvalue/Odyssey/froth/imminently/intervene获取第二阶段Shellcode，并进行解密操作，如果解密之后的数据符合条件则跳转到解密之后的Shellcode。

第二阶段Shellcode主要是根据驱动程序名判断Bitdefender，卡巴斯基，360等杀毒软件是否存在。

若通过检测，则继续异或自解密，获取到存储伪装文件和恶意payload的URL。

然后从“http://office-updatecentral.com/eigenvalue/Odyssey/froth/imminently/creep”下载载荷，将其存放在“C:\\Users\\user\\AppData\\Local\\Temp\\winlst.dll”，接着修复winlst.dll的DOS头，以保证后续能正常运行。最后使用LoadLibrary函数加载该模块，并显示调用winlst.dll的IntegrateCheck函数。

3.攻击组件分析

加载的winlst.dll文件信息如下所示：

MD5	a9630f7c64dd3147284b7230e2b76aa2
文件大小	40.0 KB (40,960 字节)
文件名	winlst.dll

编译时间	2024-07-18 15:10:13

Winlst.dll是一个C#编译的程序，主要功能是上传信息和下载后续payload执行，可能还处于前期开发阶段，之前未见该组织使用这种组件。下图是该样本的部分配置信息。

样本执行后首先会判断域名regionserverbackup.info是否正常通讯,并将当前目录路径复制到“C:\ProgramData\”目录下，并随机命名。然后创建一个名字为“WMIaPNSRC{46b62409-40c1-4af9-8656-1e011c6970d1}”计划任务，执行的程序仍然为winlst.dll，但是执行的导出函数为“SSDPrvSrc”。

当通过计划任务利用rundll32.exe执行winlst.dll的SSDPrvSrc导出函数时，首先会删除临时目录下的原始的winlst.dll文件，然后创建互斥体，并再次连接配置中的服务器看是否能访问，如果不可访问，则在注册表HKCU\SOFTWARE\ServerChecker创建“NotFoundCount”和“LastCheckedDate”用于标记不可访问次数和最后一次检查时间。

接着获取主机名和用户名信息通过HTTP发送给“https[:]//regionserverbackup.info”。如果返回正常，则尝试读取返回的配置信息，诸如“downloadURL”，“fileDropEnvironment”等信息。并根据返回的配置信息，选择是否实现自删除(Self_Destructio开关)，以及是否执行下一阶段载荷并持久化(Execution开关)。

如果域名访问不通，首先获取相关的主机配置信息并上传。
最后继续并根据保存在代码的配置信息执行下一阶段操作，但是此时的Self_Destructio开关和Execution开关都处于关闭状态，故不会执行任何操作。并且代码中的配置信息下载URL为“http[:]//example.com/payload.dll”，这个URL看上去是攻击者随意填写，侧面也看出这类攻击组件应该还处于开发初期，部分功能还在完善中。

二、关联分析

根据下载链接的域名office-updatecentral[.]com，我们在同一时期也关联到Donot组织针对把巴基斯坦使用的漏洞攻击样本，样本信息如下：

MD5	e96e2ed88e2f2fb80d02e7cd99a1420d
文件大小	43.5 KB (44544字节)
文件名	STATUS OF KoM PROPOSAL & TIMELINES.doc

样本成功执行后会显示由巴基斯坦国家信息技术委员会出的一份申明模板。

本次样本为docx类型文件，使用模板注入加载远程链接“http://office-updatecentral.com/armorer/opposing/stratifies/beachheads/knolls”执行。

该链接为一个包含CVE-2017-11882漏洞的RTF文件，RTF文档被加载起来时执行Shellcode，其功能继续从“http://office-updatecentral.com/armorer/opposing/stratifies/beachheads/exacerbating”下载第二阶段shellcode。

第二阶段Shellcode执行时，会自身异或解密，接着会遍历驱动检查卡巴和360杀毒软件是否存在，再修复通过RTF释放在temp目录下ztNU9wPs.dll的PE头4字节数据，并加载其IntegrateCheck函数。

接着通过“http://office-updatecentral.com/armorer/opposing/stratifies/beachheads/canto”下载伪装文件保存到temp目录下document.doc并打开。

由于释放的DLL与恶意宏样本释放的DLL一致，不再详细叙述。

三、归属研判

通过对本次攻击活动的相关信息进行深入分析，我们认为此类攻击活动符合Donot组织以往的TTP，具体表现在：

1）样本中的宏代码与以往样本类似，存在很多次的无用循环，只是单纯赋值操作，并且shellcode的执行流程也基本一致，而且也都是通过检测驱动判断杀软；
2）RTF漏洞样本的执行流程与以往也十分类似，并且调试过程中出现了Donot之前使用的文件路径“%Roaming%\wingui.dll”；
3）无论宏样本下载的dll还是漏洞样本释放的dll,头4字节均需修复，这一点在Donot组织以往的攻击活动中多次出现。此外，攻击目标符合该组织攻击对象。因此，将其归属于APT-C-35（肚脑虫）组织。

总结

APT-C-35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。本次攻击中攻击者通过Shellcode层层解密加载载荷，并结合定时任务实现持久化。此外，本次捕获的新载荷，表明该组织在持续地进行更新恶意代码的功能和形态，并呈现出功能化模块化的特点。

因此在这里提醒用户加强安全意识，无论何种操作系统，切勿执行未知样本或点击来历不明的链接等操作。这些行为可能导致系统在没有任何防范的情况下被攻陷，从而导致机密文件和重要情报的泄漏。

附录 IOC

MD5：

e96e2ed88e2f2fb80d02e7cd99a1420d

9656246f97e1a18c5e4bf1afcd139c79

ea6f3e8c2fa7c995a607224038b7f63a

d7e9217c2bcf1e8519458cca63f2b69f

c2f88dc91c44b18b036f536f0844a709

a9630f7c64dd3147284b7230e2b76aa2

bd2b06d17faabc2b916ba89f56f7e200

URL:

http[:]//office-updatecentral.com/armorer/opposing/stratifies/beachheads/knolls

http[:]//office-updatecentral.com/eigenvalue/Odyssey/froth/imminently/empower

http[:]//office-updatecentral.com/eigenvalue/Odyssey/froth/imminently/relaxations

http[:]//office-updatecentral.com/armorer/opposing/stratifies/beachheads/exacerbating

https[:]//regionserverbackup.info/wall/restrict.php

http[:]//office-updatecentral.com/eigenvalue/Odyssey/froth/imminently/intervene

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。
