

APT-C-24（响尾蛇）组织使用application文件钓鱼攻击活动分析

 mp.weixin.qq.com/s/PALBLusD4umh_52gy2wVAg

高级威胁研究院

1.攻击流程分析

该组织通过钓鱼邮件分发PDF诱饵文档，当用户点击打开该文件后诱导用户下载application文件，application文件为ClickOnce应用程序部署配置文件，其主要功能则是远程安装白加黑组件。

在后续的样本关联中捕获到一起通过宏代码下载后续恶意组件的攻击活动，其核心载荷为Rust语言编写，该Rust载荷具备较强的反分析能力，整体功能与本次分析核心载荷保持一致。



此图片来自微信公众平台
未经允许不可引用

2.恶意载荷分析

捕获的恶意样本如下所示：

MD5	ac0623ac3349356060f8f37838ec332b
-----	----------------------------------

文件名称	--
------	----

文件类型	PDF
------	-----

响尾蛇APT组织向受害用户投递带有恶意链接的PDF文档，该文件会引导受害者点击Download file，用户点击后会通过“https[:]//webmail-pnra.gov-pk.workers[.]dev/ftp.pnra.org.application”链接下载后续载荷。而后续载荷则为application文件。

此图片来自微信公众平台
未经允许不可引用

MD5	86c3d19dcfb5775a4895832fad052d17
文件名称	ftp.pnra.org.application
文件类型	application

application文件的安装模式为在线安装，文件的URL为：
https[:]//webmail-pnra.gov-pk.workers[.]dev/ftp.pnra.org.application
配置文件的URL为：
https[:]//webmail-pnra.gov-pk.workers[.]dev/ftp.pnra.org.exe.manifest



此图片来自微信公众平台
未经允许不可引用

下载后的ftp.pnra.org.exe.manifest文件内容如下：

应用清单：

[https://webmail-pnra.gov-pk.workers\[.\]dev/ftp.pnra.org.exe.manifest](https://webmail-pnra.gov-pk.workers[.]dev/ftp.pnra.org.exe.manifest)

后续恶意组件：

[https://webmail-pnra.gov-pk.workers\[.\]dev/OneDrive.exe](https://webmail-pnra.gov-pk.workers[.]dev/OneDrive.exe)

[https://webmail-pnra.gov-pk.workers\[.\]dev/mscorsvc.dll](https://webmail-pnra.gov-pk.workers[.]dev/mscorsvc.dll)

[https://webmail-pnra.gov-pk.workers\[.\]dev/system32.dll](https://webmail-pnra.gov-pk.workers[.]dev/system32.dll)



此图片来自微信公众平台
未经允许不可引用

3.攻击组件分析

MD5	76195b41d2e0c8008c23e77363a7455a
-----	----------------------------------

文件名称	mscorsvc.dll
------	--------------

文件类型	Dll
------	-----

当OneDrive.exe进程被运行并传入“/RuntimeWide”参数后，则会执行LockDependentFiles函数，该函数主要用于加载恶意的mscorsvc.dll文件。



此图片来自微信公众平台
未经允许不可引用

会执行该dll的名为“CorInitSvcLogger”函数，开始会动态获取函数的地址，以便后续程序调用。



此图片来自微信公众平台
未经允许不可引用

接着检查OneDrive.exe进程是否在特定的目录下：

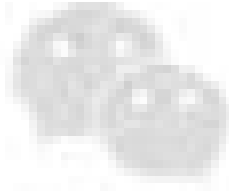
C:\PROGRAMDATA

C:\PROGRAM FILES

C:\PROGRAM FILES (X86)\APPDATA\

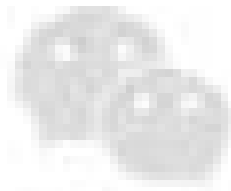
C:\WINDOWS

然后将该进程写入注册表，进行持久化操作。

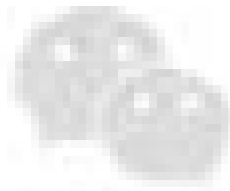


此图片来自微信公众平台
未经允许不可引用

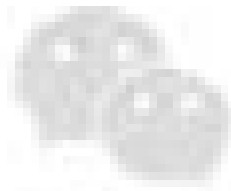
打开当前目录下的system32.dll文件，并将其读取至内存，该文件为核心载荷的加密数据。接着对其进行解密操作，调用SystemFunction032函数进行RC4解密，解密密钥为：“boikztaigkuneapfvpesuabfmpxgwnad”。解密后是一段shellcode代码为此次攻击的核心载荷。



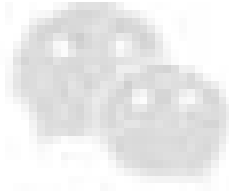
此图片来自微信公众平台
未经允许不可引用



此图片来自微信公众平台
未经允许不可引用



此图片来自微信公众平台
未经允许不可引用



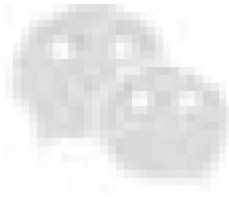
此图片来自微信公众平台
未经允许不可引用

核心载荷执行后首先会动态获取函数地址，该操作可有效地增加静态分析的分析难度，接着执行主要功能，该木马主要功能则是获取用户信息上传后，等待服务器指令，实现了远程远程控制的功能。



此图片来自微信公众平台
未经允许不可引用

样本中的加密字符通过异或算法进行解密，字符串解密后C2地址为 `www.gov-pk.workers[.]dev`。



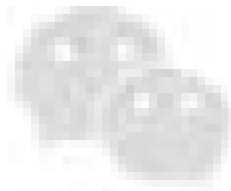
此图片来自微信公众平台
未经允许不可引用

接着获取受害用户的敏感信息作为上线包，主要获取计算机名、用户名、进程ID、时间、版本等，与device_id、computer_name、user_name等字段拼接成一个JSON格式的字符串，并写入到指定的内存缓冲区中。

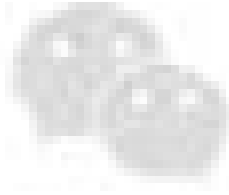


此图片来自微信公众平台
未经允许不可引用

连接服务器将收集的信息格式化为json格式后上传，上线包的url路径为/beta/deviceManagement/managedDevices。

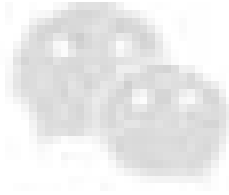


此图片来自微信公众平台
未经允许不可引用



此图片来自微信公众平台
未经允许不可引用

接着等待服务器发送远控指令执行，指令为json格式。



此图片来自微信公众平台
未经允许不可引用

指令	功能
status:reregister	上线包发送
config	配置更新
pwd	当前工作路径获取
cd	进入xx文件夹
ls dir	显示目录

download	下载文件
upload	上传文件
rm	删除文件
mkdir	创建目录
cp	复制文件
mv	移动文件
screenshot	屏幕截图
perun	运行指定进程
socks_connect	SOCKS 网络隧道连接
socks_data	向隧道写入数据并回传
socks_close	关闭隧道
shell	执行shell命令

三、关联分析

关联到另一起通过application类型文件的攻击样本，整体攻击流程与本次分析样本一致，依旧是部署白加黑组件执行。

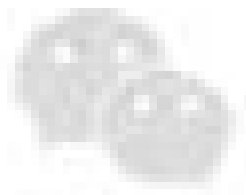
MD5 b5faa2453292b12f95580d2a4deaf37c

文件名称 AdobeReader.application

文件类型	application
MD5	9a95078a7a5f1045c61fe95ab308ec3f
文件名称	cryptbase.dll
文件类型	Dll

部署清单URL：

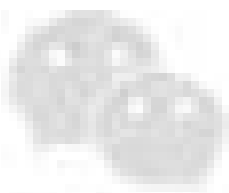
<https://itsupport.apps-sco-gov-pk.workers.dev/download/AdobeReader.application>



此图片来自微信公众平台
未经允许不可引用

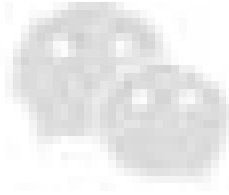
白加黑组件下载：

<https://itsupport.apps-sco-gov-pk.workers.dev/download/Svcc.exe>



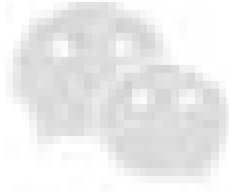
此图片来自微信公众平台
未经允许不可引用

核心载荷使用rust语言编写增加逆向难度，与本次分析的样本逻辑一致，开始依旧检测样本是否在指定的文件夹下，否则退出进程，接着开始将样本进行持久化操作。



此图片来自微信公众平台
未经允许不可引用

C2的解密方式依旧使用异或解密，C2：<https://support.cc-cvbs-sco.workers.dev>。



此图片来自微信公众平台
未经允许不可引用

接着获取用户敏感信息并发送至服务器，然后开始等待远控指令下发，远控指令与本次分析的基本一致，但此样本新增了键盘监控功能。



此图片来自微信公众平台
未经允许不可引用

关联到通过恶意宏代码释放核心载荷的攻击活动，如下：

MD5	bc43ee3b9873539932b9eb23f21e9e1b
-----	----------------------------------

文件名称	spreadsheet.xls (copy)
------	------------------------

文件类型	xls
------	-----

MD5	f310ee836f88cc43d3939f8a88b20495
-----	----------------------------------

文件名称	sppc.dll
------	----------

文件类型 dll

该xls文档文件带有恶意的宏代码，功能主要是下载白加黑组件并执行，下载链接如下：

URL	FileName
https://ftp.desco-gov-bd.workers.dev/favicon.ico	C:\ProgramData\sppc.dll
https://fancy-voice-b182.goldibrowhoami.workers.dev/audiodg.pdf	C:\ProgramData\audiodg.exe



此图片来自微信公众平台
未经允许不可引用

audiodg.exe文件运行后加载其sppc.dll，木马依旧为rust语言编写，C2：<https://api.desco-gov-bd.workers.dev:443>，解密方式依旧为异或解密。整体功能与本次分析木马一致。

四、归属研判

- 1.近期，响尾蛇（SideWinder）组织频繁滥用 workers.dev、pages.dev、netlify.app、b4a.run 等免费托管平台，用于快速部署钓鱼门户及凭证窃取页面，以降低基础设施成本并提升隐蔽性。本次披露的相关 IOC 在托管平台选择上与其既往活动高度一致。
- 2.其中，gov-pk 类域名命名符合该组织一贯采用的 IOC 构造特征，明显意在仿冒巴基斯坦政府相关机构，进一步强化了对响尾蛇组织的溯源判断。

总结

此次针对 APT-C-24（响尾蛇）组织的样本投递活动分析表明，该组织正在持续演进其初始投递手法，并不断尝试引入新的技术以提升攻击成功率与隐蔽性。本次攻击中，攻击者利用 ClickOnce 的 application 文件作为载体进行样本投递，体现出其对 Windows 应用部署机制的深入理解与滥用能力。在进一步的关联分析中发现，该组织并未局限于单一投递链路，还通过恶意宏代码下载后续恶意组件，基于 Rust 语言编写的后门木马。这表明该组织具备持续研发与快速迭代攻击技术的能力。在此提醒广大用户，提高网络安全意识，降低被网络攻击的风险。

附录 IOC

MD5

ac0623ac3349356060f8f37838ec332b
76195b41d2e0c8008c23e77363a7455a
9a95078a7a5f1045c61fe95ab308ec3f
bc43ee3b9873539932b9eb23f21e9e1b
f310ee836f88cc43d3939f8a88b20495
f80e3806ae3a0dbca9456c3ef422e1d6
a95041469ff85c7a45394e46e566b074
b53aba6a17a156a865c62d84d7e0e367
b5faa2453292b12f95580d2a4deaf37c

C2

www.gov-pk.workers[.]dev
api.ahsaanullaahkhan.workers[.]dev
https[:]//webmail-pnra.gov-pk.workers[.]dev/ftp.pnra.org.application
https[:]//webmail-pnra.gov-pk.workers[.]dev/ftp.pnra.org.exe.manifest
https[:]//webmail-pnra.gov-pk.workers[.]dev/OneDrive.exe
https[:]//webmail-pnra.gov-pk.workers[.]dev/mscorsvc.dll
https[:]//webmail-pnra.gov-pk.workers[.]dev/system32.dll
https[:]//itsupport.apps-sco-gov-pk.workers[.]dev/download/AdobeReader.application
https[:]//itsupport.apps-sco-gov-pk.workers[.]dev/download/Svcc.exe
https[:]//itsupport.apps-sco-gov-pk.workers[.]dev/download/cryptbase.dll
https[:]//support.cc-cvbs-sco.workers[.]dev

[https://ftp.desco-gov-bd.workers\[.\]dev/favicon.ico](https://ftp.desco-gov-bd.workers[.]dev/favicon.ico)

[https://fancy-voice-b182.goldibrowhoami.workers\[.\]dev/audiodg.pdf](https://fancy-voice-b182.goldibrowhoami.workers[.]dev/audiodg.pdf)

[https://api.desco-gov-bd.workers\[.\]dev](https://api.desco-gov-bd.workers[.]dev)

[https://test.netof66867.workers\[.\]dev/audiodg.pdf](https://test.netof66867.workers[.]dev/audiodg.pdf)

[https://test.netof66867.workers\[.\]dev/sppc.pdf](https://test.netof66867.workers[.]dev/sppc.pdf)