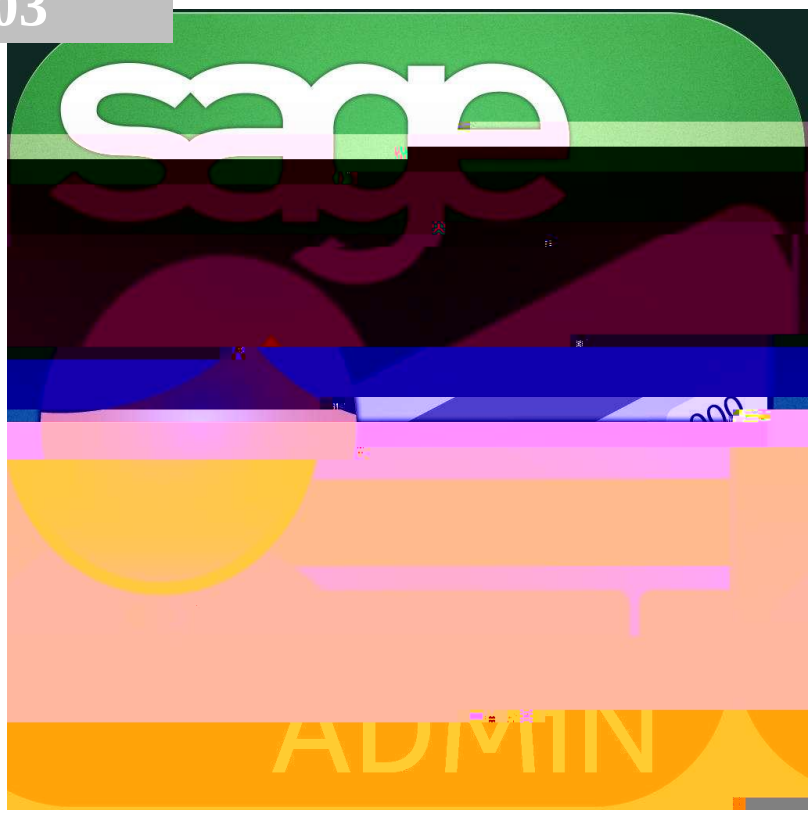


Sage 2.0

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

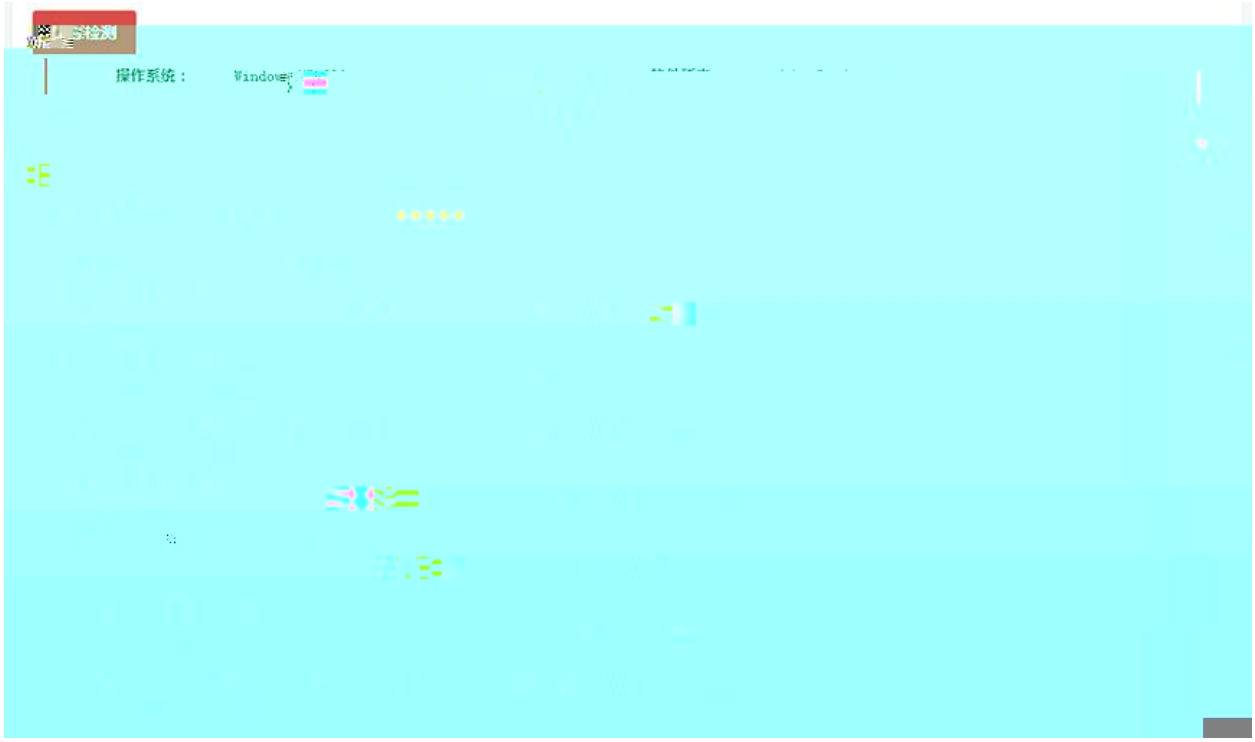
zip Word

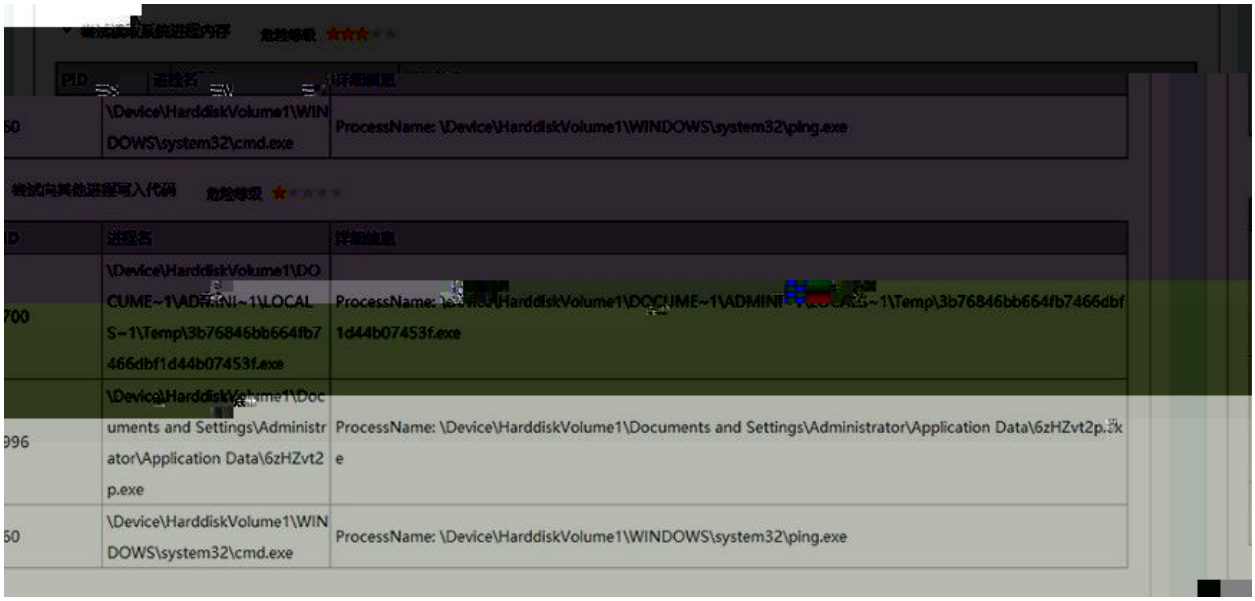
. Sage

2.1

2.2 -

Ṕ

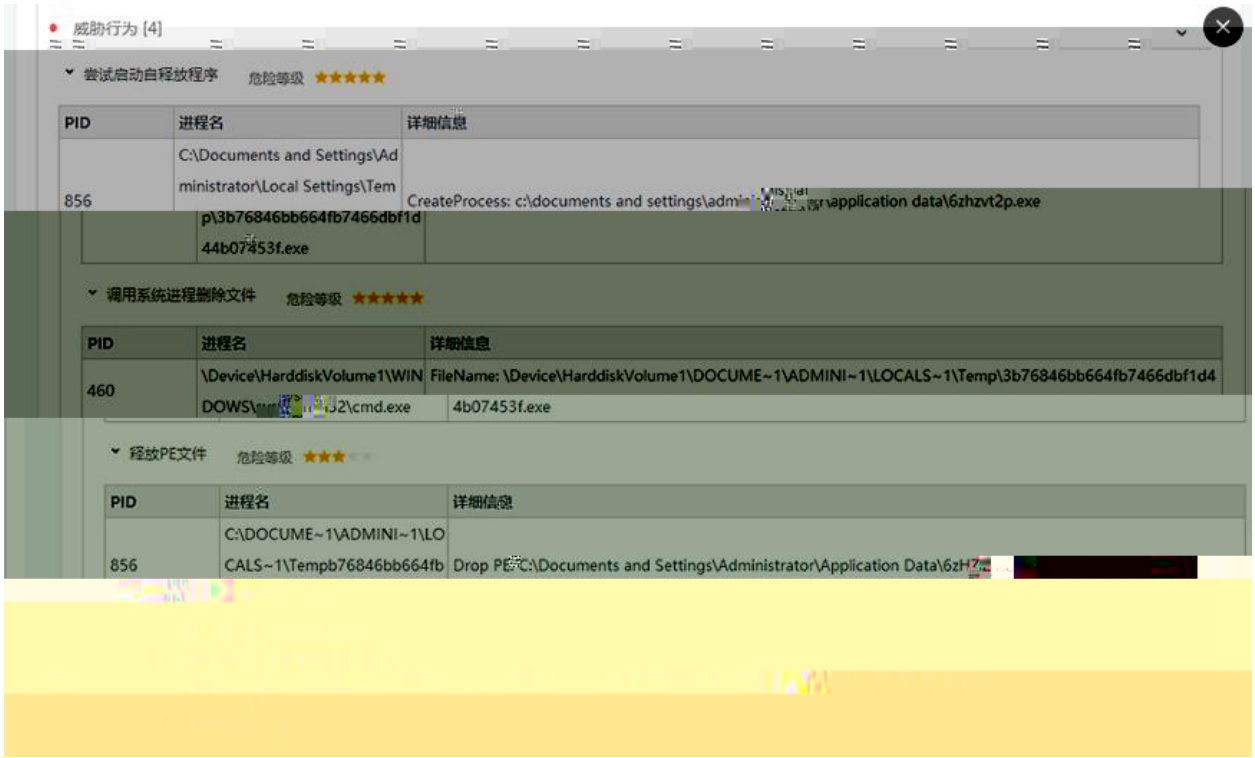


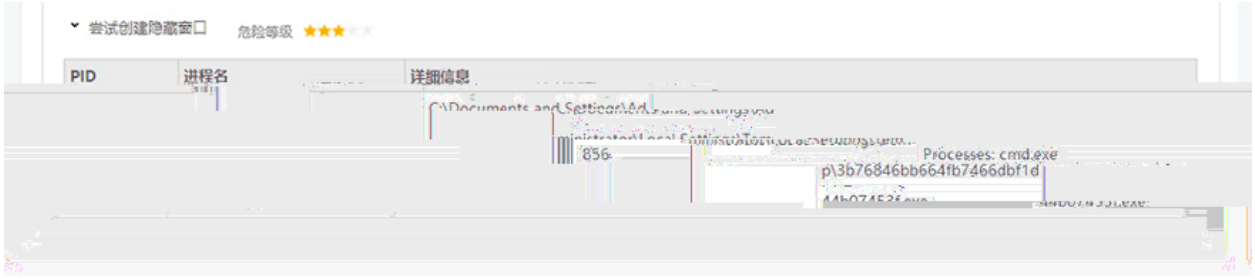


PID	进程名	详细信息
60	\Device\HarddiskVolume1\WINDOWS\system32\cmd.exe	ProcessName: \Device\HarddiskVolume1\WINDOWS\system32\ping.exe

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


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
检测到可疑UDP请求
反调试 [1]
尝试检测调试器
危险等级


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\3b76846bb664fb7466dbf1d\44b07453f.exe
CreateProcess: c:\documents and settings\admi 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\ 2\cmd.exe
FileName: \Device\HarddiskVolume1\DOCUME~1\ADMINI~1\LOCALS~1\Temp\3b76846bb664fb7466dbf1d4\4b07453f.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\Tempb76846bb664fb
Drop PE:C:\Documents and Settings\Administrator\Application Data\6zH

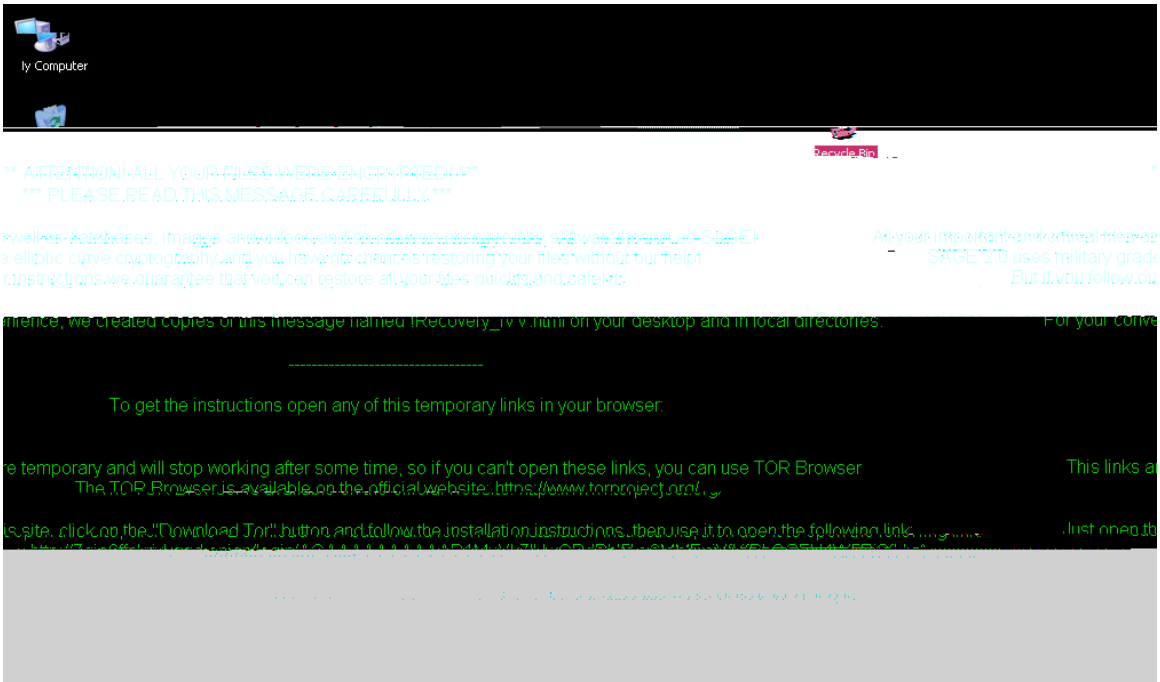


. Sage

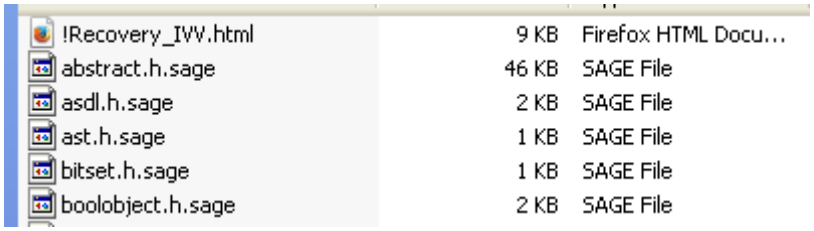
3.1

345KB

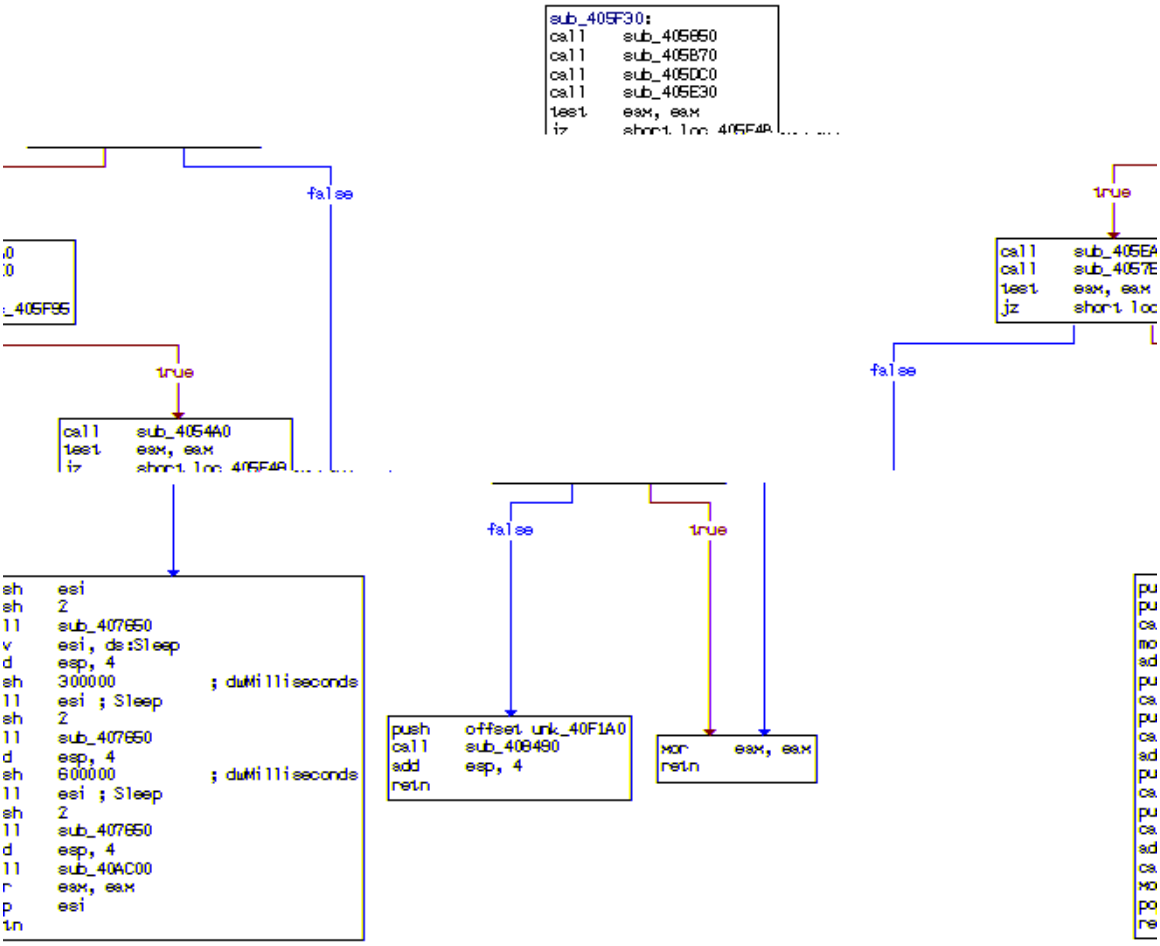
3.2





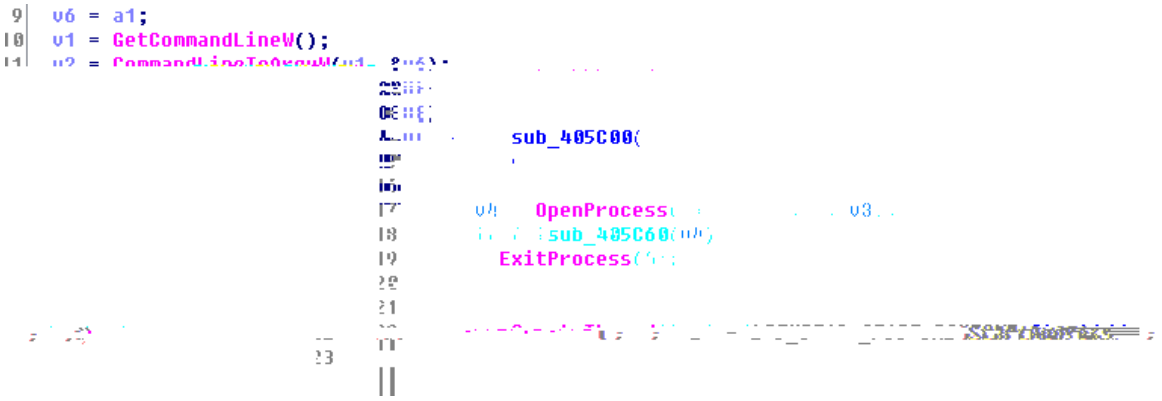

!Recovery_IVV.html 9 KB Firefox HTML Docu...
abstract.h.sage 46 KB SAGE File
asdl.h.sage 2 KB SAGE File
ast.h.sage 1 KB SAGE File
bitset.h.sage 1 KB SAGE File
boolobject.h.sage 2 KB SAGE File

3.3

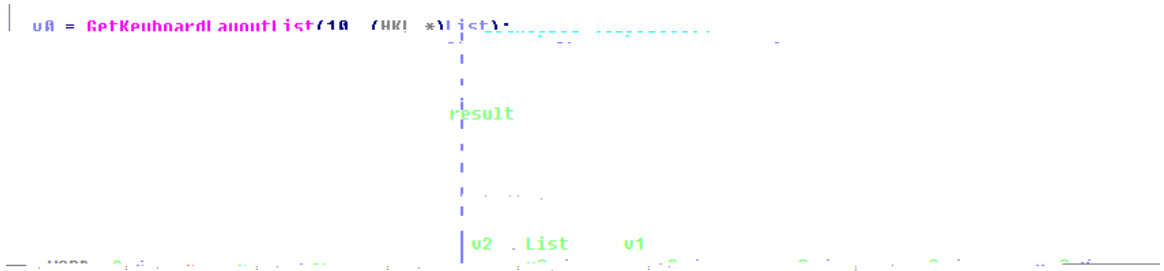



```
39  v12 = -1665792991;
40  LoadLibraryA("wlanapi.dll");
41  LoadLibraryA("ntdll.dll");
42  LoadLibraryA("mpr.dll");
43  LoadLibraryA("iphlpapi.dll");
44  sub_405640(&v13, 9, &v9, 4);
45  WSAStartup(2u, &WSAData);
46  CoInitialize(0);
47  [redacted]
48  [redacted]
49  [redacted]
50  sub_4092E0([redacted]);
51  [redacted]
52  [redacted]
53  [redacted]
54  [redacted]
55  [redacted]
56  if ( [redacted] != (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);
```






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









.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]
    result = DeleteFileW(u8);
  }
  [redacted]
}
```

. APT

4.1 APT

APT

APT