Governments As Malware Authors: The Next Generation

Mikko Hypponen
CRO
F-Secure

@mikko
Different governmental uses for malware

- Law Enforcement
- Espionage
- Surveillance
- Sabotage
- Warfare
Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

SUN KAILIANG

Aliases: Sun Kai Liang, Jack Sun
Masking "file.scr"

- Screen saver
  - file.scr
  - 917 KB

- PDF
  - fdp.4102-hcraM-tropeR-yriruceS-senilepiP-saG-eniarkU.scr

- PDF
CosmicDuke remnants

- c:\botgenstudio\generations\8f1777b0\bin\Bot.pdb
- d:\production\nitro\sva\generations\809113dd\bin\Bot.pdb
- d:\sva\nitro\botgenstudio\interface\generations\80ddfcc1\bin\Bot.pdb
- D:\PRODUCTION\NITRO\KSK\Generations\70BCDEA1\bin\Bot.pdb
- C:\Projects\NEMESIS\nemesis-gemina\nemesis\bin\carriers\ezlzma_x86_exe.pdb
MALWARE ANALYSIS

Cosmu with a twist of MiniDuke

TLP: WHITE

In this document we report on our analysis of CosmuDuke - the first malware seen to include code from both the notorious MiniDuke APT group and another longstanding threat, the information-stealing Cosmu family. When active on an infected machine, CosmuDuke will search for and launch login details from a range of programs and forward the data to remote servers, some of which were active at the time of writing.

F-SECURE LABS
SECURITY RESPONSE
Whitepaper
<table>
<thead>
<tr>
<th>12</th>
<th>MTMxMjMxMg==</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>havex</td>
</tr>
<tr>
<td>10800000</td>
<td>12</td>
</tr>
<tr>
<td>Explorer.EXE</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>47</td>
</tr>
<tr>
<td>46</td>
<td><a href="http://www.pc-service-fm.de/modules/mod_search/src.php">www.pc-service-fm.de/modules/mod_search/src.php</a></td>
</tr>
<tr>
<td>48</td>
<td>artem.sataev.com/blog/wp-includes/pomo/src.php</td>
</tr>
<tr>
<td>354</td>
<td>swissitaly.com/includes/phpmailer/class.pop3.php</td>
</tr>
</tbody>
</table>
Programm was started at %02i:%02i:%02i %02i:%02i:%02i.%04i:

***********************
Start finging of LAN hosts...
Finding was fault. Unexpектив error
Was found %i hosts in LAN:
Hosts wasn't found.

Start finging of OPC Servers...
Was found %i OPC Servers.

CLSID: %s
UserType: %s
VerIndProgID: %s
OPC version support: %s

OPC Servers not found. Programm finished
Industrial Routers, Industrial Wireless Router, VPN Routers

Industrial Remote Access Router

A key strategy for many machine OEMs involves building solid, long-term relationships with their customers by providing dependable, superior after-sales support. They have come to realize the value that remote machine support provides to their customers, as well as to themselves.

eWON COSY 141
Industrial VPN Router

eWON 2005CD/4005CD
Industrial LAN Router
F-Secure has published a new description:

- Worm:W32/Agent.BTZ - Low (1)
  http://www.f-secure.com/v-descs/worm_w32_agent_btz.shtml
  2008-06-26, 17:30:41
<table>
<thead>
<tr>
<th>Address</th>
<th>Type</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000000A</td>
<td>C</td>
<td>Log end.\n</td>
<td></td>
</tr>
<tr>
<td>0000010</td>
<td>C</td>
<td>%02d:%02d:%02d</td>
<td></td>
</tr>
<tr>
<td>000001F</td>
<td>C</td>
<td>Error in sprintf copy bytes \n</td>
<td></td>
</tr>
<tr>
<td>000001F</td>
<td>C</td>
<td>Log: Error(%d) get file size.\n</td>
<td></td>
</tr>
<tr>
<td>000002F</td>
<td>C</td>
<td>Log: Size of log(%dB) is too big, stop write.\n</td>
<td></td>
</tr>
<tr>
<td>000002A</td>
<td>C</td>
<td>Size of log(%dB) is too big, stop write.\n</td>
<td></td>
</tr>
<tr>
<td>000018</td>
<td>C</td>
<td>%s\system32\winview.ocx</td>
<td></td>
</tr>
<tr>
<td>00001B</td>
<td>C</td>
<td>%02d.%02d.%04d Log begin:\n</td>
<td></td>
</tr>
<tr>
<td>000009</td>
<td>C</td>
<td>%system%</td>
<td></td>
</tr>
<tr>
<td>00000A</td>
<td>C</td>
<td>%windows%</td>
<td></td>
</tr>
<tr>
<td>00000C</td>
<td>C</td>
<td>%s\system32</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address</th>
<th>Type</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000A</td>
<td>C</td>
<td>Log end.\n</td>
<td></td>
</tr>
<tr>
<td>000016</td>
<td>C</td>
<td>%s\system32\vtmon.bin</td>
<td></td>
</tr>
<tr>
<td>00001A</td>
<td>C</td>
<td>Exception CEncLog::Open.\n</td>
<td></td>
</tr>
<tr>
<td>00001B</td>
<td>C</td>
<td>%02d.%02d.%04d Log begin:\n</td>
<td></td>
</tr>
<tr>
<td>000032</td>
<td>C</td>
<td>Buffer is too big(%dB), LogSize(%dB), Limit(%dB)\n</td>
<td></td>
</tr>
<tr>
<td>000010</td>
<td>C</td>
<td>%02d:%02d:%02d</td>
<td></td>
</tr>
<tr>
<td>000015</td>
<td>C</td>
<td>%02d:%02d:%02d %04x</td>
<td></td>
</tr>
<tr>
<td>000021</td>
<td>C</td>
<td>Error in sprintf, max %d bytes\n</td>
<td></td>
</tr>
<tr>
<td>000011</td>
<td>C</td>
<td>assistant_helper</td>
<td></td>
</tr>
<tr>
<td>00000A</td>
<td>C</td>
<td>assistant</td>
<td></td>
</tr>
<tr>
<td>00001F</td>
<td>C</td>
<td>Log: Error(%d) get file size.\n</td>
<td></td>
</tr>
<tr>
<td>00002F</td>
<td>C</td>
<td>Log: Size of log(%dB) is too big, stop write.\n</td>
<td></td>
</tr>
<tr>
<td>00002A</td>
<td>C</td>
<td>Size of log(%dB) is too big, stop write.\n</td>
<td></td>
</tr>
</tbody>
</table>
Developer Signatures

$Id: event.c 14097 2010-11-01 14:46:27Z gilg $

$Id: mime64.c 12892 2010-06-24 14:31:59Z vlad $

$Id: named_mutex.c 15594 2011-03-18 08:04:09Z gilg $

$Id: nt.c 20719 2012-12-05 12:31:20Z gilg $

$Id: ntsystem.c 19662 2012-07-09 13:17:17Z gilg $

$Id: snake_config.c 5204 2007-01-04 10:28:19Z vlad $
جنگ سایبری

نگاه به مهمترین حملات سایبری در جهان

بیان می‌شود که این سایبری‌ها به نوعی از نبرد اطلاعاتی می‌گردند که ترتیب جنگ از آن برابر با سیاست و شبکه‌های رایانه‌ای استفاده می‌کنند. این اطلاعات نشان می‌دهند که گستره آن می‌تواند شکست نیز از جنگ را از دست بدهد.

گروه‌های حمله

- White hat hackers
- Black hat hackers
- Gray hat hackers
- Pink hat hackers

STUXNET

نام حمله: STUXNET
تاریخ: 2009
هدف: هدفی ساخته شده برای فرمت‌های ویژه violation
آسیب دیدگان: حمله داده‌های بخش اتوماتیک

RAVENSBURGER

نام حمله: RAVENSBURGER
تاریخ: 2008
هدف: هدفی ساخته شده برای فرمت‌های ویژه violation
آسیب دیدگان: حمله داده‌های بخش اتوماتیک

AURORA

نام حمله: AURORA
تاریخ: 2009
هدف: هدفی ساخته شده برای فرمت‌های ویژه violation
آسیب دیدگان: حمله داده‌های بخش اتوماتیک

BYZANTINE CANDOR

نام حمله: BYZANTINE CANDOR
تاریخ: 2009
هدف: هدفی ساخته شده برای فرمت‌های ویژه violation
آسیب دیدگان: حمله داده‌های بخش اتوماتیک

GHOSTNET

نام حمله: GHOSTNET
تاریخ: 2009
هدف: هدفی ساخته شده برای فرمت‌های ویژه violation
آسیب دیدگان: حمله داده‌های بخش اتوماتیک

SHADOW IN THE CLOUD

نام حمله: SHADOW IN THE CLOUD
تاریخ: 2009
هدف: هدفی ساخته شده برای فرمت‌های ویژه violation
آسیب دیدگان: حمله داده‌های بخش اتوماتیک

WIkiLeAKS TAKE DOWN

نام حمله: WIkiLeAKS TAKE DOWN
تاریخ: 2009
هدف: هدفی ساخته شده برای فرمت‌های ویژه violation
آسیب دیدگان: حمله داده‌های بخش اتوماتیک

مراجع:
- NewScientist
- www.infographics.ir
To Kill a Centrifuge

A Technical Analysis of What Stuxnet’s Creators Tried to Achieve

Ralph Langner

November 2013
The control units in the pictures above display process pressure and setpoints. The picture below shows the same product (MKS PR-4000) as advertised on the Internet for sale (fergutec.com).

The pressure controllers must be compromised in order to disable the Cascade Protection System’s stage exhaust valves. This suggests a link between the Cascade Protection System’s main controller, the Siemens S7-417, to the pressure controllers. Since the PR-4000 doesn’t come with a built-in PROFIBUS interface, communication is most likely established via a PROFIBUS-to-serial gateway, as shown in the diagram below; a configuration that is used in similar applications. From the attack code it can be inferred that a total of 21 pressure controllers were used per cascade, with the lower 15 controlling stage exhaust valves.
Nuclear Energy a Symbol of Pride for Nation
"There was also some music playing randomly on several of the workstations during the middle of the night with the volume maxed out. I believe it was the American band AC/DC *Thunderstruck*. It was all very strange and happened very quickly. The attackers also managed to gain root access to the machine they entered from and removed all the logs."
Gauss encryption

```assembly
mov    ecx, (LENGTHOF tToCrypt)-1
mov    edx, OFFSET tToCrypt
mov    ebx, OFFSET tEncrypt
L1:
    mov    eax, [edx]
    XOR    eax, ACDC
    not    eax
    mov    [ebx], eax
    inc    edx
    inc    EBX

LOOP L1

mov    edx, OFFSET tOutEncr
call   WriteString
mov    edx, OFFSET tEncrypt
call   WriteString
call   Crlf
ret
```
Crypto breakthrough shows Flame was designed by world-class scientists

The spy malware achieved an attack unlike any cryptographers have seen before.

by Dan Goodin - June 7 2012, 2:20pm EDT
Mikko Hypponen
@mikko

I've now been accused of helping al-Qaeda, because our antivirus blocks malware created by the US Government.

8:22 PM - 1 Jun 2012
N. Korea doubles cyber war personnel

JULY 6, 2014

SEOUL, July 6 — North Korea has doubled the number of its elite cyber warriors over the past two years and established overseas bases for hacking attacks, a report said today.

The North’s cyber war unit now has 5,900 personnel, compared with 3,000 two years ago, the South’s Yonhap news agency said.

“The communist country operates a hacking unit under its General Bureau of Reconnaissance, which is home to some 1,200 professional hackers,” a military source was quoted as saying.
FinFly

Usage Example 2: Intelligence Agency

The customer deployed FinFly ISP within the main Internet Service Provider of their country. It was combined with FinFly Web to remotely infect Targets that visited government offensive websites by covertly injecting the FinFly Web code into the targeted websites.
<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported Version</th>
<th>Latest Version on the Market</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>2.x.x, 3.x.x, 4.0.x, 4.1.x, 4.2.x, 4.4.x</td>
<td>4.4.x</td>
</tr>
<tr>
<td>Blackberry</td>
<td>5.x, 6.x, 7.x</td>
<td>10.1</td>
</tr>
<tr>
<td>iOS</td>
<td>Untethered Jailbreak required: 4.3.x, 5.x, 6.x, 7.0.x</td>
<td>7.1</td>
</tr>
<tr>
<td>Symbian</td>
<td>Symbian ^3, Anna, Belle, S60 v5.x v3.x</td>
<td>Symbian ^3 Anna, Belle</td>
</tr>
<tr>
<td>Windows Mobile</td>
<td>6.1, 6.5</td>
<td>6.5</td>
</tr>
<tr>
<td>Windows Phone</td>
<td>Not Supported Yet</td>
<td>8</td>
</tr>
</tbody>
</table>
UAE, Bahrain, Saudi Arabia, Syria...

- Finfisher (Gamma)
- RCS (Hacking Team)
- DarkComet
- BlackShades
- Xtreme RAT
- Spynet
From: Melissa Chan <melissa.aljazeera@gmail.com>
Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights Bahrain reports of torture on Mr. Nabeel Rajab after his recent arrest.

Please check the attached detailed report along with torture images.

1 attachment: Rajab.rar 1.4 MB
Hacker Units inside UKUSA intelligence agencies

- Show me all the exploitable machines in country X
THE EYES

• **FIVE EYES**: USA, UK, Canada, Australia, New Zealand

• **NINE EYES**: Five Eyes + Denmark, Norway, The Netherlands and France

• **FOURTEEN EYES**: Nine Eyes + Sweden, Germany, Belgium, Italy and Spain
FREE Peter Sunde
Geneva Convention

“Legitimate military targets are limited to those objects which by their nature make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage”
Thank You

Please fill your feedback form if you have nice things to say. Otherwise, never mind.