Thank you for your attention!

Costin G. Raiu, craiu@kaspersky.ro
Vitaly Kamluk, vitaly.kamluk@kaspersky.com
~DQ: A cyber-missile

Darkly Digging Deep.

Vitaly Kamluk, Chief Malware Expert, Global Research and Analysis, Kaspersky Lab
Costin G. Raiu, Director, Global Research and Analysis, Kaspersky Lab
Aleks Gostev, Chief Security Expert, Global Research and Analysis, Kaspersky Lab

24th annual First Conference, Malta, 17-22 June 2012
Who are we?

About the presenters:

Costin G. Raiu - Linux user since 1996; RedHat Linux fan, CentOS heavy user.

Vitaly Kamluk - Linux power user, Debian / Ubuntu fan, KL forensics expert.
Kaspersky Duqu research team
What is Duqu?

- Sophisticated attack platform.
- Discovered in August 2011 by the Hungarian research lab CrySyS.
- Brother/sister/cousin/friend of Stuxnet
- Active since 2008.
- The high-end of nation state-sponsored cyber-espionage malware.
A Cyber Missile Concept

- Carrier - Driver
- Ballistic Control - Config
- Warhead - Payload

Stuxnet

Duqu
Architectural similarity

- Driver (.sys file)
- Encrypted Payload DLL (.pnf file)
- Encrypted Config File (.pnf file)
- Encrypted Registry Binary Block

Stuxnet:
- Driver: mrxcis.sys, mrxnet.sys...
- Encrypted Payload DLL: oem7a.pnf
- Encrypted Config File: mdmcp3.pnf
- Encrypted Registry Binary Block: Registry Value "Data"

Duqu:
- Driver: jminet7.sys, nfrd965.sys...
- Encrypted Payload DLL: netp794.pnf, netf1.pnf...
- Encrypted Config File: ird182.pnf, netp192.pnf...
- Encrypted Registry Binary Block: Registry value "Filter"
Game of Binary Similarity

\[
\begin{align*}
10100011 & \ 00101110 \ 01100111 \ 11000001 \ 11001110 \ 11001010 \\
01100011 & \ 01111011 \ 11000001 \ 01011111 \ 10000001 \ 10000110 \\
10000001 & \ 11101011 \ 10110100 \ 10010101 \ 11100000 \ 00110101 \\
01100101 & \ 10110010 \ 00001000 \ 00011101 \ 10001001 \ 00101011 \\
11011010 & \ 00000100 \ 10011011 \ 10010010 \ 10111101 \ 10111100 \\
01011111 & \ 11000111
\end{align*}
\]

Bit values:

- ☐ = 1
- ☐ = 0

QR Code Image
Game of Binary Similarity
<table>
<thead>
<tr>
<th>atmpvc.sys</th>
<th>cmi4432.sys</th>
<th>fdc.sys</th>
<th>ip6fw.sys</th>
<th>kbdclass.sys</th>
<th>mrxcls.sys</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM network driver from MS</td>
<td>Duqu driver</td>
<td>Floppy disk controller driver</td>
<td>IPv6 Windows Firewall driver</td>
<td>Keyboard class driver</td>
<td>Stuxnet driver</td>
</tr>
</tbody>
</table>
Duqu embedded config
\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\cmi4432
FILTER
\Device\{3093AAZ3-1092-2929-9391}\n
Stuxnet embedded config
\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls
Data
\Device\MRxClsDvX
Duqu driver installer PE header timestamp

<table>
<thead>
<tr>
<th>Count of sections</th>
<th>6</th>
<th>Machine</th>
<th>intel386</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symbol table</td>
<td>00000000[00000000]</td>
<td>Magic optional header</td>
<td>010B</td>
</tr>
<tr>
<td>Size of optional header</td>
<td>00E0</td>
<td>OS version</td>
<td>6.00</td>
</tr>
<tr>
<td>Linker version</td>
<td>8.00</td>
<td>Subsystem version</td>
<td>5.00</td>
</tr>
<tr>
<td>Image version</td>
<td>6.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entry point</td>
<td>00000316</td>
<td>Size of code</td>
<td>00002F80</td>
</tr>
<tr>
<td>Size of init data</td>
<td>00000680</td>
<td>Size of init data</td>
<td>00000000</td>
</tr>
<tr>
<td>Size of image</td>
<td>00003900</td>
<td>Size of uninit data</td>
<td>00000000</td>
</tr>
<tr>
<td>Base of code</td>
<td>00000300</td>
<td>Size of header</td>
<td>000000300</td>
</tr>
<tr>
<td>Image base</td>
<td>00010000</td>
<td>Base of data</td>
<td>000002E80</td>
</tr>
<tr>
<td>Section alignment</td>
<td>00000080</td>
<td>Subsystem</td>
<td>Native</td>
</tr>
<tr>
<td>Stack</td>
<td>00040000/00001000</td>
<td>File alignment</td>
<td>000000080</td>
</tr>
<tr>
<td>Checksum</td>
<td>00013615</td>
<td>Number of directories</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Development probably started around 2007.
Duqu research@Kaspersky

10-part research blogs at www.securelist.com:
Victims of Duqu:

- Power and energy industry
- Supply chain, shipment and procurement
- Military
- PLC design
- Certificate Authorities (or Authority?)

Many located in Iran

Unknown: 3
Europe: 3
Iran: 11
Sudan: 4
The Duqu victim scenario
How do you get infected with Duqu?
Very few real-world Duqu infections were fully analyzed.

The upcoming data was collected from a real Duqu victim.
Our first detection of Duqu
Dear Sir
I found the details of your company on your web site, and would like to establish business cooperation with your company. In the attached file, please see a list of requests.

Thank you,
Best Regards
Mr. B. Jason
Marketing Manager
Dear Sir,

I found the details of your company on your cooperation with your company. In the attachment, I have attached a document "request.doc (262 KB)" for your reference.

Thank you for your time.

Best Regards,

[Name]
CVE-2011-3402: TTF parsing vulnerability
Please send me the following information:

1. Your company’s profile
2. Recommendations from previous customers
3. Price list for inland shipping
4. Price list for storage of goods
5. Do you supply marine shipping?
You have e-mail!

From: [redacted]  
To: [redacted]  
Subject: Request for services

Dear Sir,

I found the details of your company on your website and would like to establish business cooperation with your company. In the attached file, please see a list of requests.

Thank you,
Best Regards,
Mr. B. Jones
Marketing Manager

---

Based on real, world tested phishing mails.

From: Pedro Williams Lee [test@test.com]  
To: [redacted]  
Subject: Re:Quote/New Order Price

Hello,

Thanks for the response to our message; we write to inform you that we are interested in your products. We saw a similar product, Auctions so please confirm to us by the link below and log in into the Easy Shopper with your company domain email and password for possible view of sample, of the product requested.

http://www.newproducts-trad.co.cc/

Please kindly send us your catalog and we would like to inquire about the following:

* Minimum Order Quantity
* Your delivery time
* Payment terms
* And your products warranty

We will await your response with details, price and quantity that can be made available.

Thanks,
Best Regard,
Pedro Williams Lee
Sales Manager

---

CVE-2011-3402: TTF parsing vulnerability
The Duqu full cycle

- User opened the file
- Spear phishing mail attached .doc file
-win32k.sys
- Loader driver (31.08.2007)
- Loader DLL (main dropper)
- Windows kernel
- Dexter Regular font (Exploit of CVE-2011-3402)
- Document
- Microsoft Word document
- services.exe
- big PNF (main module, 17.04.2011)
- Driver 24960 bytes
- big PNF 248320 bytes
- Config PNF 6750 bytes
- Duqu is installed
- Windows registry "CF10" check
- The date range check "CIGH"
Victim is infected!
Now what?
| Large .PNF file inside "C:\Windows\inf" |
Decrypted PNF
This program cannot be run in DOS mode...
.rsrc section

```
0000h: 4D 5A 90 00 03 00 00 00 04 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0140h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0180h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0200h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0240h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0260h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0280h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0300h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0320h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0340h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0360h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0380h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0400h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0420h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```
```
.zdata section
Inside .zdata
206.183.111.97
Duqu's C&C server IP
Duqu known C&C servers

Everybody knows...

206.183.111.97 - India, Mumbai
77.241.93.160 - Belgium, Gent

Other "Unknown" C&C's:

112.213.x.x - Vietnam
123.30.x.x - Vietnam
95.x.x.x - Netherlands
Duqu "jump points" maze

114.202.x.x - South Korea
188.40.x.x - Germany
87.117.x.x - UK
82.194.x.x - Spain
89.187.x.x - Czech Republic
87.236.x.x - Czech Republic
202.45.x.x - Singapore
62.2.x.x - Switzerland
203.211.x.x - Singapore
...

Server forensics
How to get access?

1. Ask nicely
2. Beg
3. Keep asking
4. Explain the threat
5. Work with CERTs / LEA
Our success rate

+6  -4
If you are wondering...

Where is the most safe bullet-proof hosting?
Switzerland
## Analyzed servers

<table>
<thead>
<tr>
<th>Location</th>
<th>Server 'A'</th>
<th>Server 'B'</th>
<th>Server 'C'</th>
<th>Server 'D'</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Asia</td>
<td>Europe</td>
<td>Europe</td>
<td>Europe</td>
</tr>
<tr>
<td>OS</td>
<td>CentOS 5.5</td>
<td>CentOS 5.4</td>
<td>CentOS 5.6</td>
<td>CentOS 5.3</td>
</tr>
<tr>
<td>Arch</td>
<td>32 bit</td>
<td>64 bit</td>
<td>32 bit</td>
<td>64 bit</td>
</tr>
<tr>
<td>Access</td>
<td>Key+pw</td>
<td>Pw</td>
<td>Key+pw</td>
<td>Key+pw</td>
</tr>
<tr>
<td>Installed</td>
<td>Dec-09</td>
<td>Nov-09</td>
<td>Apr-11</td>
<td>Nov-09</td>
</tr>
<tr>
<td>Hacked</td>
<td>Feb-11</td>
<td>Nov-09</td>
<td>May-11</td>
<td>Feb-10</td>
</tr>
</tbody>
</table>

All Duqu infrastructure servers run some version of CentOS.
Tools used:

SleuthKit - 'fls -d' - to find deleted files
'strings' - extract all strings from images
'grep', FAR - search for stuff
010 editor (on Windows) - complex search
dezero - internal tool - get rid of empty space
netlocate - internal tool - find TCP packets

VirtualBox - emulation
Server analysis HOWTO:

1. dezero - get rid of spaces (tens of GB's)
2. strings imagefile > strings.txt
3. fls -d1r imagefile > deleted.txt
4. grep stuff (eg. 'Accepted', 'sshd[', utmp/wtmp fragments, "RSA PRIVATE", "ssh-rsa", "port 443", etc...)
Findings: #Upgrades

[root@-vm ~]# telnet centos-vm 22
Trying 192.168.200.108...
Escape character is '^['.

SSH-2.0-OpenSSH_4.3

Before hack

[root@-vm ~]# telnet 112.213.x.x 22
Trying 112.213.x.x...
Connected to 112.213.x.x (112.213.x.x).
Escape character is '^['.

SSH-2.0-OpenSSH_5.8

After hack

RedHat Linux / CentOS 5.x comes with OpenSSH 4.3

First thing the attackers do: update it to 5.8
Findings: #Tuning

- Before hack:
  - # GSSAPI options
  - GSSAPIAuthentication yes
  - UseDNS yes

- After hack:
  - # GSSAPI options
  - GSSAPIAuthentication no
  - UseDNS no

Secondly, they patch "sshd_conf"

Possible reasons: speed / compatibility
Findings: #Cleanup

Oct 20, 2011 - Major cleanup!

Attackers wiped /var/log/*, /root/.ssh and other relevant system locations.

On ALL servers. (took hours)

Securely. Using 'shred'.

Pitfalls of file deletion

Linux ext3 filesystem

1. We can still see what files were deleted
2. Deleting logs doesn't take care of slack space
3. File reallocation / truncations (passwd, wtmp, utmp)

Wiping all tracks off a hacked Linux server can be an almost impossible task for the hackers!
15 Feb 2011 – init.d cleanup
OpenSSH5.8p1 installed

20 Oct 2011 – logs cleanup

10 Feb, 3 April 2011 – dovecot events?

19 July 2011 – OpenSSH 5.8p2 installed
How do they get hacked?

Theory nr 1:
Brute-forcing the root password

Nov 18 15:21:11 n8s005 sshd[29072]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.45. __user=root
Nov 18 15:21:13 n8s005 sshd[29072]: Failed password for root from 202.45. _port 46503 ssh2
Nov 18 15:21:50 n8s005 sshd[29073]: Connection closed by 202.45.
Nov 18 15:21:50 n8s005 sshd[29072]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=202.45. __user=root
... 
Nov 18 15:27:12 n8s005 sshd[29098]: Failed password for root from 202.45. _port 46643 ssh2
Nov 18 15:27:14 n8s005 sshd[29099]: Connection closed by 202.45.
Nov 18 15:29:53 n8s005 sshd[29104]: Accepted password for root from 202.45. _port 46712 ssh2
Theory nr 1:
Brute-forcing the root password

Nov 18 15:21:11 n8s005 sshd[29072]: pam_unix(sshd:auth): authentication failure; logname= uid=0
euid=0 tty=ssh ruser= rhost=202.45. port 46503 ssh2
Nov 18 15:21:13 n8s005 sshd[29072]: Failed password for root from 202.45.
Nov 18 15:21:50 n8s005 sshd[29073]: Connection closed by 202.45.
Nov 18 15:21:50 n8s005 sshd[29072]: PAM 2 more authentication failures; logname= uid=0 euid=0
tty=ssh ruser= rhost=202.45. port 46503 ssh2
Nov 18 15:27:12 n8s005 sshd[29098]: Failed password for root from 202.45. port 46643 ssh2
Nov 18 15:27:14 n8s005 sshd[29099]: Connection closed by 202.45.
Nov 18 15:29:53 n8s005 sshd[29104]: Accepted password for root from 202.45. port 46712 ssh2
How do they get hacked?

Theory nr 2: CentOS 0-day (in OpenSSH 4.3)

well, the hackers sure aren’t gonna notify the vendor, they are some group who is against anyone advocating people secure and they think everyone should leave the internet vulnerable just for them.

Here is a pcap log of the exploit being used. It is encrypted SSH traffic though so I doubt it is of any use.

The people I heard this from are reliable sources and they say they are 100% positive it is an openssh 4.3 exploit.

Sometimes, well most of the time, RHEL team is slow on updates and CentOS is even slower because they have to wait on them and if they knew it would take some time to get it fixed. A lot of the versions on RHEL software has made me nervous in the past. I do understand that instead of just throwing a few patches together on the same version.

From what I have gathered this same hacker group has hacked centos 4 and centos 5 boxes this way. There is a possible exploit may have been fixed. I will still run the latest gsecurity to try and be somewhat safe.

Of course we can never make an unhackable server but we cant let people scare us into not trying to keep each other informed. So
That's (too) scary!!!
How do they get hacked?

Theory nr 3:
Another malware!

1. Password stealer malware
2. A version of Duqu
3. Purchase of credentials on black market
How do they get hacked?

Theory nr 3:
Another malware!
1. Password stealer malware
2. A version of Duqu
3. Purchase of credentials on black market
Driver file
compiled 01.01.09

First variant of Stuxnet 0xAE240682
Key "MrxCls" Value "Data"

Mrxcls.sys
Stuxnet.a 22.06.2009

Rtniczw.sys

Unknown module

Driver file
compiled 14.07.10

Realtek cert 25.01.10
Stuxnet.b 01.03.2010
Stuxnet.c 14.04.2010
Stuxnet variants, 2010 0xAE240682
Key "MrxCls" Value "Data"

Driver file
compiled 03.11.10

Realtek cert 18.03.10
Unknown module

Unknown malware 0xAE240682
Key "rtniczw" Value "Config"

Some API calls like in Duqu 0xAE240682
Key "jmidebs" Value "IDE"

Jmidebs.sys

Micron cert
Unknown module

<name>.sys
Duqu November 2010

More API calls 0xAE240682
Key <name of files> Value "FILTER"
The Duqu C&C Infrastructure

Deep inside the memory dump...

Tamir Gal

Tamir Gal - A Secure Shell (SSH) library for .NET

A special case... Memory dumps...

Deep inside the memory dump...

What is SharpSSH-3.0?

Let’s change it!

Connections from 144.202.94.33

Login times - Duqu C&C proxy server

But wait! Is it fully automatic?

The Duqu Automated C&C Infrastructure

Observations - 1

- They are smarter.
- 6-8 connections per C2
- No connection exists to C2
- No connections after 10min.

Observations - 2

- 3-4 connections and C2 search
- Connections made in minutes
- High data rate in the first 5 minutes
- Low data rate after 5 minutes.
Server 'B'

A special case:
Memory dump!
Deep inside the memory dump...

<table>
<thead>
<tr>
<th>#4 forwarded-tcpip: listening port 443 for 0.0.0.0 port 0, connect from 90.13.177.217 (t4 r136480 i0/0 o0/0 fd 11/11 cfd -1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>#5 forwarded-tcpip: listening port 443 for 0.0.0.0 port 0, connect from 90.13.177.217 (t4 r136483 i0/0 o0/0 fd 12/12 cfd -1)</td>
</tr>
<tr>
<td>#6 server-session (t4 r136578 i3/0 o3/0 fd 14/14 cfd -1)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>08#, port listener</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
</tr>
<tr>
<td>3des-cbc</td>
</tr>
<tr>
<td>hmac-md5</td>
</tr>
<tr>
<td>none</td>
</tr>
<tr>
<td>NEST</td>
</tr>
<tr>
<td>CEST</td>
</tr>
<tr>
<td>SSH-2.0-OpenSSH_4.3</td>
</tr>
<tr>
<td>SSH-2.0-SharpSSH-3.0.0.0-JSCH-0.1.28</td>
</tr>
<tr>
<td>3des-cbc</td>
</tr>
<tr>
<td>NEST</td>
</tr>
<tr>
<td>CEST</td>
</tr>
<tr>
<td>hmac-md5</td>
</tr>
<tr>
<td>none</td>
</tr>
<tr>
<td>@lysatoA</td>
</tr>
<tr>
<td>3des-cbcA</td>
</tr>
</tbody>
</table>
(08#
port listener
none
3des-cbc
hmac-md5
none
NEST
CEST
SSH-2.0-OpenSSH_4.3
SSH-2.0-SharpSSH-3.0.0.0-JSCH-0.1.28
3des-cbc
NEST
CEST
hmac-md5
none
@lysatoA
3des-cbcA
What is SharpSSH-3.0?

Let's Google it!
Tired of SharpSSH bugs? | eldos.com
www.eldos.com/SecureBlackbox
Check professional components for SSH and SFTP in .NET

Tamir Gal | SharpSSH - A Secure Shell (SSH) library for .NET
www.tamirgal.com/blog/page/SharpSSH.aspx
SharpSSH is a pure .NET implementation of the SSH2 client protocol suite. It provides an API for communication with SSH servers and can be integrated into ...

SharpSSH | Free Security & Utilities software downloads at ...
sourceforge.net/projects/sharpssh/
★★★★★ Rating: 82% - 47 reviews
19 Dec 2011 – SharpSSH is a pure .NET implementation of the SSH2 client protocol suite. It provides an API for communication with SSH servers and can be ...

sharpSsh - A Secure Shell (SSH) library for .NET - CodeProject®
www.codeproject.com › ... › Internet / Network › Network
★★★★★ 95 reviews
29 Oct 2005 – A C# implementation of the SSH2 protocol.; Author: Tamir Gal; Updated: 29 Oct 2005; Section: Internet / Network; Chapter: General ...

SharpSSH2
sharpssh2.codeplex.com/
21 Aug 2008 – This release of SharpSSH is based on Sharp SSH 1.1.1.13 posted to code project and target to Net 1.1 framework. This version has been ...

Enhanced SharpSSH – In .NET 3.5 & Support for SFTP Delete ...
ketulpatel.wordpress.com/2010/05/13/enhanced-sharpssh/
13 May 2010 – SharpSSH was written in older version of .NET and relies on algorithms in Org.Mentalis.Security.Cryptography for encryption and hashing ...

Daniel Cai's Blog: SharpSSH: A Recompiled Version Compatible ...
danielcai.blogspot.com/.../sharpssh-recompiled-version-compatible.ht...
SharpSSH - A Secure Shell (SSH) library for .NET

SharpSSH is a pure .NET implementation of the SSH2 client protocol suite. It provides an API for communication with SSH servers and can be integrated into any .NET application.

The library is a C# port of the JSch project from JCraft Inc. and is released under BSD style license.

SharpSSH allows you to read/write data and transfer files over SSH channels using an API similar to JSch’s API. In addition, it provides some additional wrapper classes which offer even simpler abstraction for SSH communication.

SharpSSH is hosted on sourceforge, please check out its project page.

Feature List

SharpSSH is not yet a full port of JSch. The following list summarizes the features currently supported by SharpSSH:

- SharpSSH is pure .NET, but it depends on Mentalis.org Crypto Library for encryption and integrity functions.
- SSH2 protocol support
- SSH File Transfer Protocol (SFTP)
- Secure Copy (SCP)
- Key exchange: diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1
- Cipher: 3des-cbc, aes128-cbc
- MAC: hmac-md5
- Host key type: ssh-rsa, ssh-dss
- Userauth: password, publickey (RSA, DSA)
- Port Forwarding
- Stream Forwarding
- Remote Exec
- Generating DSA and RSA key pairs
Who is Tamir Gal?

Current: Manager, Software Development at Compass-EOS, Israel

- C/C++ software design and development under GNU/Linux.
- Strong background and experience in networking and network protocols including TCP/IP, L3 Routing, MPLS, L2 Switching and Network Security.
The Duqu Automated C&C infrastructure

- Stealthy port 443, 80 forwarding over ssh
- Login: password and public key
- C&C proxies - hacked servers
- main server - UNKNOWN
- main server software - C#?
But wait!
Is it fully automatic?
Jun 27 00:01:58 server sshd[21747]: Accepted publickey for root from 114.202.x.
Jun  4 00:06:46 server sshd[10530]: Accepted publickey for root from 114.202.x.
Oct 16 09:26:54 server sshd[15444]: Accepted password for root from 114.202.x.x
Oct 16 09:29:24 server sshd[15526]: Accepted password for root from 114.202.x.x
Oct 16 10:03:19 server sshd[16746]: Accepted password for root from 114.202.x.x
Oct 16 10:26:08 server sshd[17483]: Accepted password for root from 114.202.x.x
Oct 16 10:33:14 server sshd[17767]: Accepted password for root from 114.202.x.x
Oct 16 11:07:17 server sshd[18945]: Accepted password for root from 114.202.x.x
Oct 16 11:09:47 server sshd[19027]: Accepted password for root from 114.202.x.x
Oct 16 15:24:38 server sshd[27579]: Accepted password for root from 114.202.x.x
Oct 16 16:05:23 server sshd[29035]: Accepted password for root from 114.202.x.x
Oct 16 16:26:28 server sshd[29724]: Accepted password for root from 114.202.x.x
Oct 16 17:12:27 server sshd[31351]: Accepted password for root from 114.202.x.x
Observations - 1

- They are human!
- 2-3 operators?
- Main time zone - GMT+2 / GMT+3

When do you go to work?
Observations - 2

• 2-3 victims per C&C server
• Operations take place in waves
• Many network errors, etc...
• SharpSSH is unreliable?
Some goodies
Startup hack script

- Recovered from server 'C'
- Run by the attackers immediately after hack.
#!/bin/bash

TEXT_BLACK=30
TEXT_RED=31
TEXT_GREEN=32
TEXT_YELLOW=33
TEXT_BLUE=34
TEXT_PURPLE=35
TEXT_WHITE=36
BACK_BLACK=40
BACK_RED=41
BACK_GREEN=42
BACK_YELLOW=43
BACK_BLUE=44
BACK_PURPLE=45
BACK_GREEN=46
BACK_WHITE=47

THEME_BACK=$BACK_BLACK
THEME_NORMAL=$TEXT_WHITE
THEME_ANNOUNCEMENT=$TEXT_GREEN
THEME_URGENT=$TEXT_RED

function color
echo -en "\033[1m\033[2m"

function coloredLine
function urgentLine
    coloredLine $THEME_BACK $THEME_URGENT "$1"

announceLine "Welcome!"

echo ""

echo ""

announceLine "Uptime:"

uptime

echo ""

echo ""

echo ""

last

read x

echo ""

echo ""

announceLine "ls -a: (/, /root, /home)"

echo "ls output of /:"

ls -a /

echo

echo "ls output of /root"

ls -a /root

echo

echo "ls output of /home"
echo ""
urgentLine "OS Version :"
cat /etc/issue
uname -a
echo ""
echo ""
announceLine "Virtualization method :"
if [-d /proc/vz ]; then
echo "Virtuozzo !"
fi
if [-d /proc/xen ]; then
echo "Xen !"
else
echo "Unknown"
read x
echo ""
echo ""
echo ""
announceLine "Versions:"
echo ".- GCC:"
gcc -v
echo "***********
urgentLine ".- SSH:"
ssh -V
echo "***********
iptables -V

echo "**********"

echo " - wget:"

wget -V

read x

echo ""

echo ""

echo ""'

echo "Sys info:"

echo " - CPU:"

cat /proc/cpuinfo

read x

echo " - Memory:"

cat /proc/meminfo

echo " - Harddisk info:"

df -h

read x

echo ""

echo ""

echo ""

echo "NAT Support:"

iptables -t nat -L -n

read x

echo ""
announced line incoming:

ifconfig -a
read x
echo ""
echo ""
echo ""
echo "Route:"
route -n
echo ""
echo ""
echo ""
announceLine "netstat:"
netstat -f unix
read x
echo ""
echo ""
echo ""
announceLine "---------------------------------Trace--Route---------------------------------"
echo ""
echo ""
echo ""
traceroute [http://www.google.com]
read x
echo ""
echo ""
echo ""
echo ""
echo ""
echo "DNS Configuration:"
cat /etc/resolv.conf
read x
echo ""
echo ""
echo ""
echo ""

urgentLine "iptables config:"

iptables -L -n

echo ""

echo ""

urgentLine "----------------------WGet-Speed-Test-------------------""  

echo ""

echo ""

wget http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.28.tar.gz

rm linux-2.6.28.tar.gz

echo ""

echo ""

echo

***************************************************************************DONE***************************************************************************

****
traceroute http://www.google.com
Startup hack script

'traceroute http://www.google.com' - What the fox???

[root@vm ~]# traceroute http://www.google.com

http://www.google.com: Name or service not known

Cannot handle "host" cmdline arg
`http://www.google.com' on position 1 (argc 1)

[root@vm ~]#
More Linux cmd fun

[root@vm ~]# man man
Formatting page, please wait...
netstat -an | grep 443
netstat -an | grep 443
netstat -ano | grep 443
netstat -anp | grep 443
ps -Af | grep 2291
telnet localhost 443
nc -l -p 1234
nc -l 1234
nc -l 0.0.0.0 1234
initcon
yum install rc-conf
yum install rccconf
yum search rccconf
yum search rc-conf
yum search rc conf
ls /etc/init.d/
ls /etc/rc3.d/
ls /etc/rc5.d/
netstat -an
netstat -anp
ps -af | grep 2291
ps -Af | grep 2291
netstat -anp
service portmap stop
service rpc.statd stop
netstat -anp
yum install rc-conf

Definition: rcconf: Debian Runlevel configuration tool This tool configures system services in connection with system runlevels. It turns on/off services using the scripts in /etc/init.d/. Rcconf works with both System-V style and file-rc runlevel configuration. It is a TUI frontend to the update-rc.d command.

No rc-conf on CentOS!
Do NOT try this at home!

"yum search rc conf"

[root@vm tmp]# yum search rc conf > tmp.txt
[root@vm tmp]# cat tmp.txt | wc
  8782   61572   524430
up2date
uname -a
yum --help
cat /etc/issue
yum install openssh5
yum search openssh
yum update openssh-server
pico /etc/ssh/sshd_config
yum install pico
yum install nano
nano /etc/ssh/sshd_config
man sshd_config
service sshd restart
Another example
wget kernel.org
rm index.html
man ftp
ftp -v ftp.kernel.org/pub
ftp -v ftp.kernel.org
iptables -L
ftp ftp.kernel.org
iptables -L -n

echo ""

echo ""

urgentLine "-------------------------------------WGet-Speed-Test-------------------------------------"

echo ""

echo ""

wget http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.28.tar.gz

rm linux-2.6.28.tar.gz

echo ""

echo ""

echo ""
Duqu framework mystery

Duqu pseudocode

Community suggestions:
- Variants of LISP
- Forth
- Erlang
- Google Go
- Delphi
- OO C
- Old compilers for C++ and other languages
<table>
<thead>
<tr>
<th>Offset</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.10001000</td>
<td>C++ Standard Template Library functions</td>
</tr>
<tr>
<td>.10004250</td>
<td>Native C++ code with STL</td>
</tr>
<tr>
<td>.1000C2C9</td>
<td>Payload</td>
</tr>
<tr>
<td></td>
<td>Other Language / C framework</td>
</tr>
<tr>
<td></td>
<td>No C++</td>
</tr>
<tr>
<td>.10023878</td>
<td>Native C++ code with STL</td>
</tr>
<tr>
<td>.10028F2C</td>
<td>Run-Time library code</td>
</tr>
<tr>
<td>.1002EAD1</td>
<td>Native C code for injection</td>
</tr>
<tr>
<td>.100300A4</td>
<td>API thunks, Exception handlers</td>
</tr>
</tbody>
</table>
class2_ctor proc near ; CODE XREF: ....
arg_0_p_compare_func= dword ptr 4

push esi
push 450h ; dwBytes
call new
mov esi, eax
pop ecx
test esi, esi
jz short loc_100125B3
lea eax, [esi+class_2.csec]
push eax ; lpCriticalSection
call ds:InitializeCriticalSection
mov eax, [esp+4+arg_0_p_compare_func]
mov [esi+class_2.setup_class13], offset class2_setup_class13
mov [esi+class_2.append], offset append_to_existing
mov [esi+class_2.remove], offset class2_remove ; (this, key)
mov [esi+class_2.clear], offset class2_clear
mov [esi+class_2.exists], offset class2_exists
mov [esi+class_2.count], offset class2_count
mov [esi+class_2.get_next_value], offset class2_get_next_value
mov [esi+class_2.get_prev_value], offset class2_get_prev_value
mov [esi+class_2.get_values_as_array], offset class2_get_values_in_array
mov [esi+class_2.dtor], offset class2_dtor
mov [esi+class_2.p_compare_func], eax
call class2_allocate_block_pair ; 1 = success
; 0 = fail
test eax, eax
jnz short loc_100125B7
push esi ; lpMem
call class2_dtor
pop ecx

loc_100125B3: ; CODE XREF: ....
xor eax, eax
pop esi
retn

; ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

loc_100125B7: ; CODE XREF: ....
mov eax, esi
pop esi
retn

class2_ctor endp
Duqu pseudocode

SocketObjectConstructor {
    NativeSocket = socket();
    SocketEvent = new MonitoredEvent(NativeSocket);
    SocketObjectCallback = new ObjectCallback(this, SocketEvent, OnCallbackFunc);
    connect(NativeSocket, ...);
}

OnCallbackFunc {
    switch(GetType(Event)) {
    case Connected: ...
    case ReadData: ...
    ...
    }
}
Community suggestions:

- Variants of LISP
- Forth
- Erlang
- Google Go
- Delphi
- OO C
- Old compilers for C++ and other languages
igork
2012 Mar 09, 19:07

Re: Other C/C++ compiler?
I'm 99% sure the machine code was generated by MSVC. It's something you get a feel with experience, but I can point out two things that are quite characteristic of MSVC: 1) it uses esi as the first candidate for temporary storage; 2) "pop ecx" instead of "add esp, 4".

whiteknight
16:20

C irritation (for C)
On the over at reddit (http://www.reddit.com/r/ReverseEngineering/) hit the jackpot:
Original Duqu disassembled code
Original Duqu disassembled code

Duqu reconstructed compiled code
tCLASS2* class2_ctor(void *p_compare_func)
{
    tCLASS2* result;
    if ( ( result = dgmalloc(sizeof(*result)) ) != NULL ) {
        InitializeCriticalSection(&result->csec);
        result->setup_class13 = &class2_setup_class13;
        result->append = &class2_append;
        result->remove = &class2_remove;
        result->clear = &class2_clear;
        result->exists = &class2_exists;
        result->count = &class2_count;
        result->get_next_value = &class2_get_next_value;
        result->get_prev_value = &class2_get_prev_value;
        result->get_values_as_array = &class2_get_values_as_array;
        result->dtor = &class2_dtor;
        result->p_compare_func = p_compare_func;
        if ( ! class2_allocate_block_pair(-result) ) {
            class2_dtor(result);
            return NULL;
        }
        else {
            return result;
        }
    }
    return NULL;
}
Duqu framework mystery

Duqu pseudocode

Community suggestions:
- Variants of LISP
- Forth
- Erlang
- Google Go
- Delphi
- OO C
- Old compilers for C++ and other languages
Unsolved Mysteries

Duqu unsolved mysteries
- There are many unsolved mysteries in the
  Duqu story.

Two unsolved Duqu mysteries
- Or one of the servers, we received a
  fragment of a SSH `known_hosts` file.

"known_hosts"
Indicates login attempts into these 2 servers.

ftp.unusualstatuecollection.net

ftp.ubuntu.com (91.189.92.172)

How many C&Cs proxies in total?

What is the IP address of the Duqu central C&C?
Duqu unsolved mysteries

• There are many unsolved mysteries in the Duqu story
How many C&C proxies in total?
What is the IP address of the Duqu central C&C?
Two unsolved Duqu mysteries

• On one of the servers, we recovered a fragment of a SSH "known_hosts" file
Indicates login attempts into these 2 servers.
Stuxnet's C&C servers:

www.mypremierfutbol.com
www.todaysfutbol.com
Flame Features:

- Backdoor
  - Making screenshots
  - Textual window grabbing
  - Audio recording
  - File search and transfer
  - Bluetooth scan & beacon
- Network worm
  - Printer Spool Service vuln.
  - Windows Update MiTM
- USB storage worm
  - LNK vuln.
Technical details:

- Windows DLL file (*.ocx)
- Modular application
- Partly written in Lua with C++ extensions
- Main module is 6Mb+ in size (overall 20Mb+)
- Uses public code of
  - zlib
  - libbz2
  - ppmd
  - sqlite3
  - Lua vm
"Flame is so hardcore that the whole Stuxnet is kept in its SQLite database."
Complex cryptographic attack

Uses huge C&C infrastructure

FLAME

Countered by OpenDNS

Flame Malware Statistics

86 DOMAINS
24 ip addresses
22 beaconing servers

MD5 collision attack
Forged digital certificates
MITM against Windows Update

Omnipotent Procedure
Simian artificial spine
Malware class names
String decryption algorithm
Same mix 64328
Complex cryptographic attack

- MD5 collision attack
- Forged digital certificates
- MiTM against Windows Update
• Same mutex name prefix: TH_POOL_SHD...
• String decryption algorithm
• Mangled class names: ?AVnxys_uwip, etc.
• Similar shellcode style
• Own import procedure

Used to be a part of Stuxnet
Uses huge C&C infrastructure

![Flame Malware Statistics](Image)

- **86 DOMAINS** for Command and Control
- **24 Current IP addresses** hosting C&C
- **22 Different registration services used**
- **8 COUNTRIES INFECTED**

Percent of traffic from top countries: **65%**

- Lebanon
- Iran
<table>
<thead>
<tr>
<th></th>
<th>Duqu</th>
<th>Flame</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server OS</strong></td>
<td>CentOS Linux</td>
<td>Ubuntu Linux</td>
</tr>
<tr>
<td><strong>Control scripts</strong></td>
<td>Running on remote server,</td>
<td>Running on servers</td>
</tr>
<tr>
<td></td>
<td>shielded through SSH port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>forwarding</td>
<td></td>
</tr>
<tr>
<td><strong>Number of victims per server</strong></td>
<td>2-3</td>
<td>50+</td>
</tr>
<tr>
<td><strong>Encryption of connections to</strong></td>
<td>SSL + proprietary AES-</td>
<td>SSL</td>
</tr>
<tr>
<td><strong>server</strong></td>
<td>based encryption</td>
<td></td>
</tr>
<tr>
<td><strong>Compression of connections</strong></td>
<td>No</td>
<td>Yes, Zlib and modified PPMD</td>
</tr>
<tr>
<td><strong>Number of known C&amp;C’s domains</strong></td>
<td>n/a</td>
<td>80+</td>
</tr>
<tr>
<td><strong>Number of known C&amp;C IPs</strong></td>
<td>5</td>
<td>15+</td>
</tr>
<tr>
<td><strong>Number of proxies used to hide</strong></td>
<td>10+</td>
<td>Unknown</td>
</tr>
<tr>
<td><strong>Identity</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Time zone of C&amp;C operator</strong></td>
<td>GMT+2 / GMT+3</td>
<td>Unknown</td>
</tr>
<tr>
<td><strong>Infrastructure programming</strong></td>
<td>.NET</td>
<td>Unknown</td>
</tr>
<tr>
<td><strong>Locations of servers</strong></td>
<td>India, Vietnam, Belgium, UK,</td>
<td>Germany, Netherlands, UK,</td>
</tr>
<tr>
<td></td>
<td>Netherlands, Switzerland,</td>
<td>Switzerland, Hong Kong,</td>
</tr>
<tr>
<td></td>
<td>Korea, etc...</td>
<td>Turkey, etc...</td>
</tr>
<tr>
<td><strong>Number of built-in C&amp;C IPs/domain in malware</strong></td>
<td>1</td>
<td>5, can update list</td>
</tr>
<tr>
<td><strong>SSL certificate</strong></td>
<td>self-signed</td>
<td>self-signed</td>
</tr>
<tr>
<td><strong>Servers status</strong></td>
<td>Most likely hacked</td>
<td>Most likely bought</td>
</tr>
<tr>
<td><strong>SSH connections</strong></td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>
This is not the end.

Contact us:

theflame@kaspersky.com
Thank you for your attention!

Costin G. Raiu, craiu@kaspersky.ro
Vitaly Kamluk, vitaly.kamluk@kaspersky.com