



Thank you for your attention!

Costin G. Raiu, [craiu@kaspersky.ro](mailto:craiu@kaspersky.ro)  
Vitaly Kamluk, [vitaly.kamluk@kaspersky.com](mailto: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



24<sup>th</sup> 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.

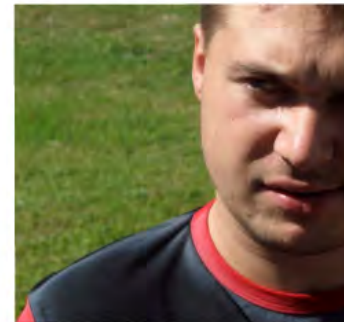
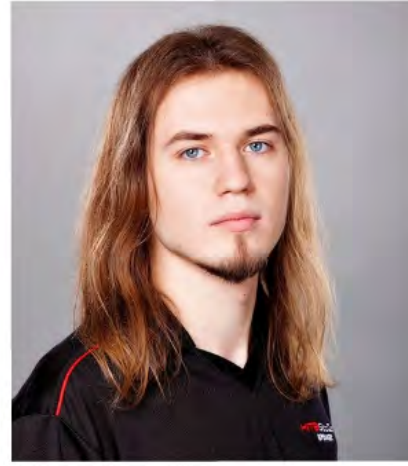


Vitaly Kamluk - Linux power user, Debian /  
Ubuntu fan, KL forensics expert.





# Kaspersky Duqu research team

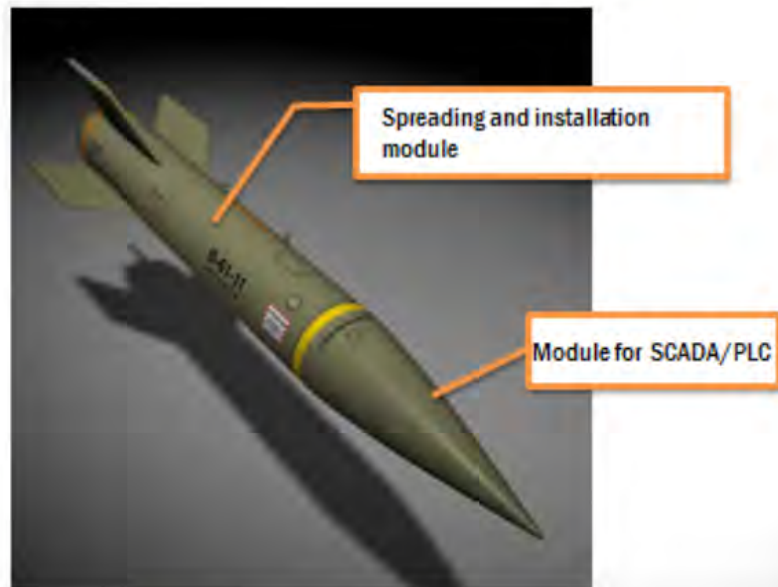


# What is Duqu?

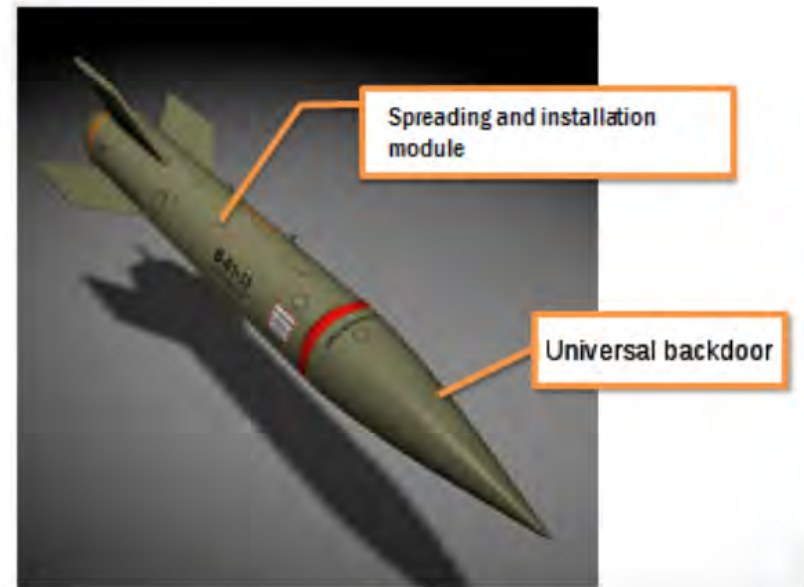
- Sophisticated attack platform.
- Discovered in August 2011 by the Hungarian research lab CrySyS.
- Brother/sister/cousin/friend of **Stuxnet**
- Active since 2008.
- **The high-end of nation state-sponsored cyber-espionage malware.**

# A Cyber Missile Concept

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

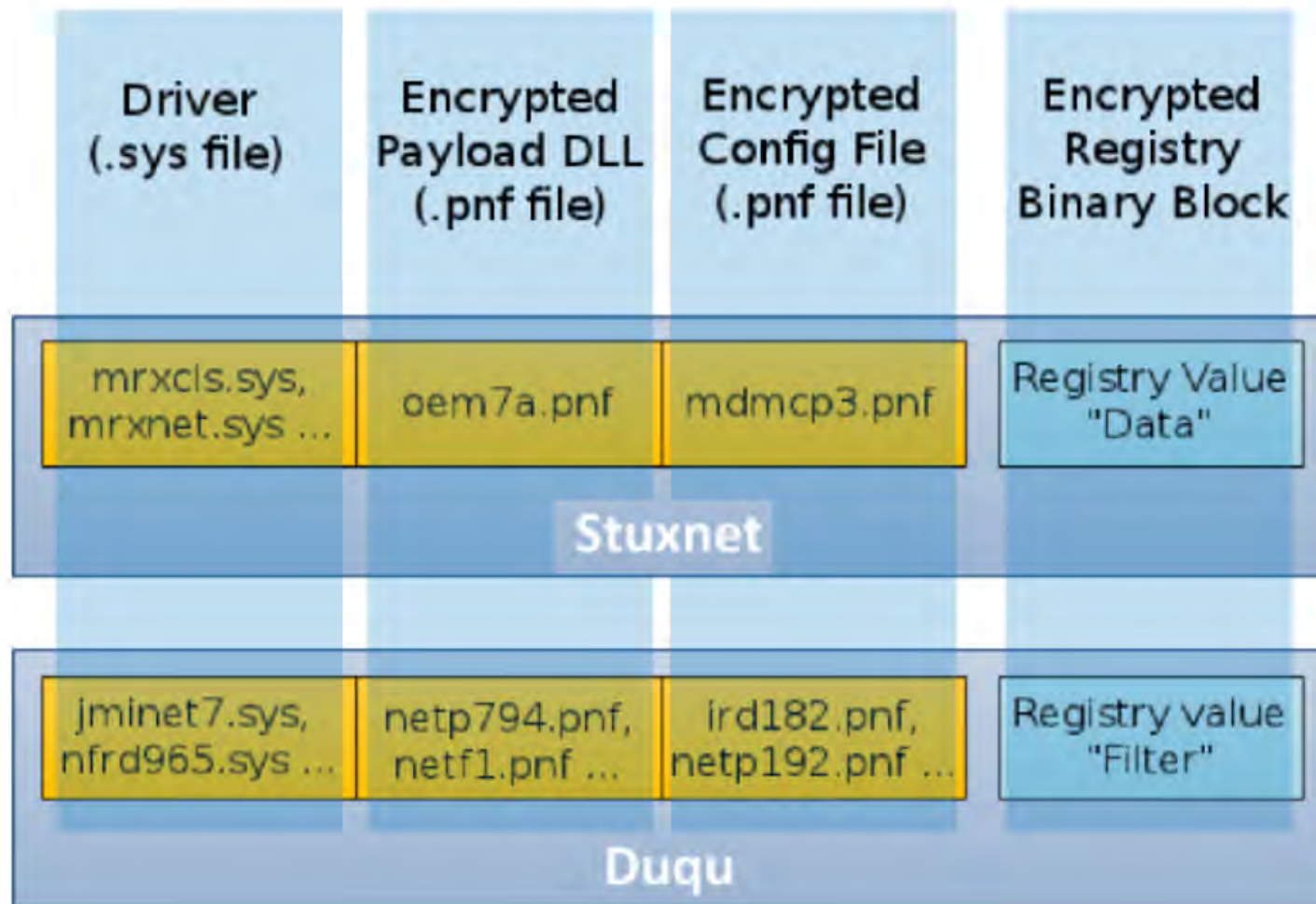


**Stuxnet**



**Duqu**

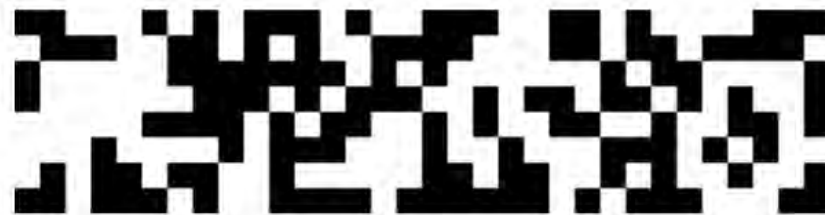
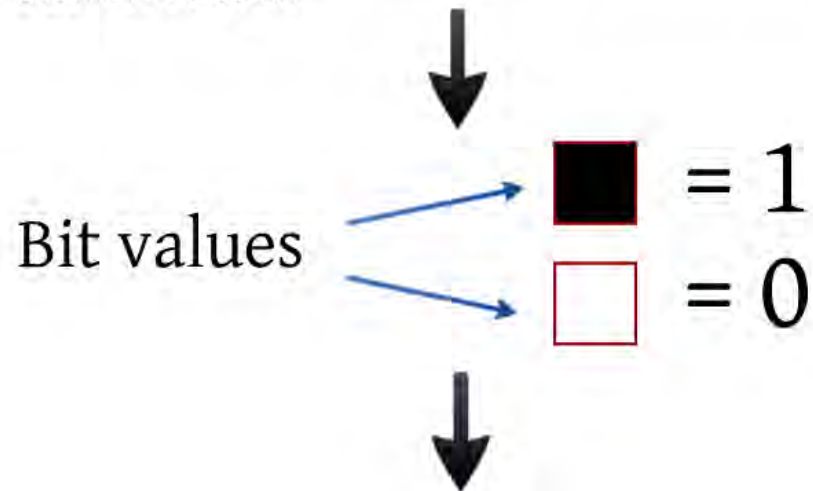
# Architectural similarity





# Game of Binary Similarity

10100011 00101110 01100111 11100001 11001110 11001010  
01100011 01111011 11000001 01011111 10000001 10000110  
10000001 11101011 10110100 10010101 11100000 00110101  
01100101 10110010 00001000 00011101 10001001 00101011  
11011010 00000100 10011011 10010010 10111011 10111100  
01011111 11000111



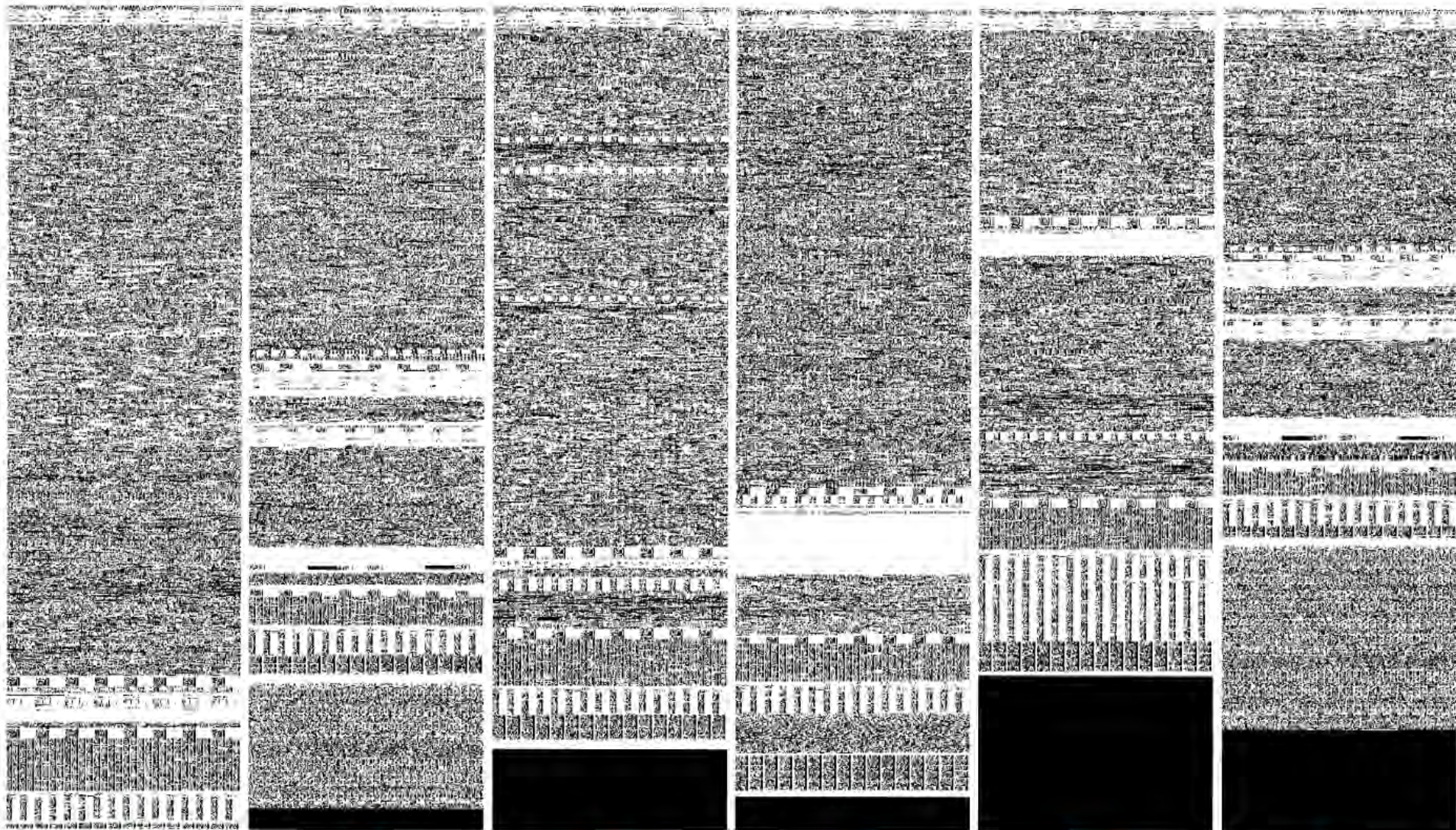


driver from MS

controller driver

firewall driver

driver



1

2

3

4

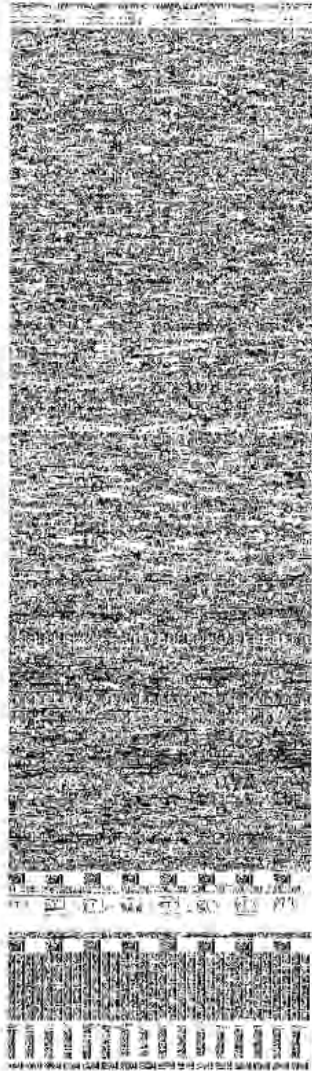
5

6

# Game of Binary Similarity



atmpvc.sys  
ATM network  
driver from MS



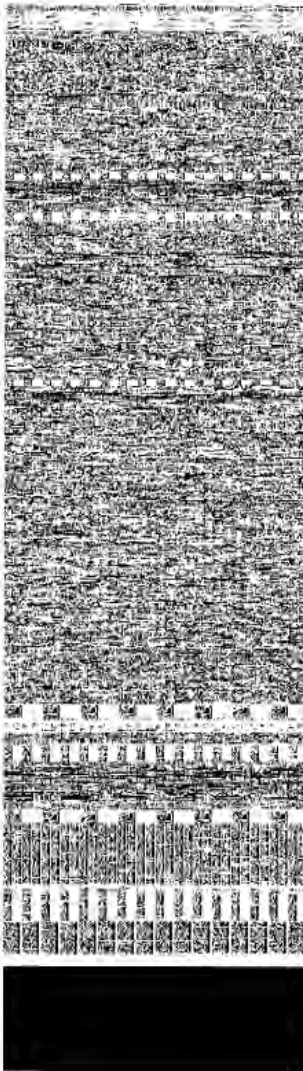
1

cmi4432.sys  
Duqu driver



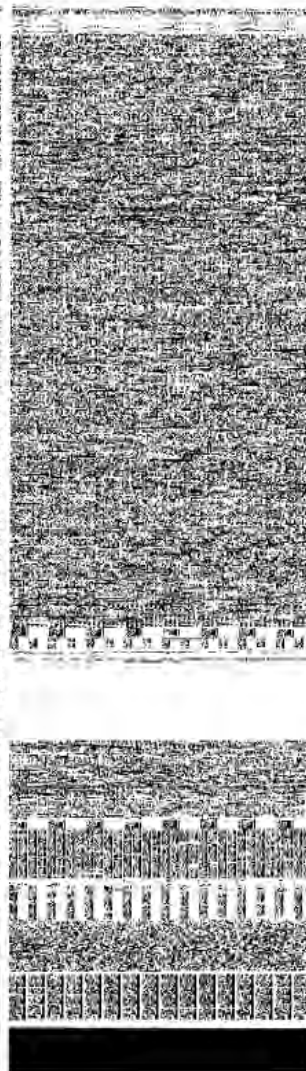
2

fdc.sys  
Floppy disk  
controller driver



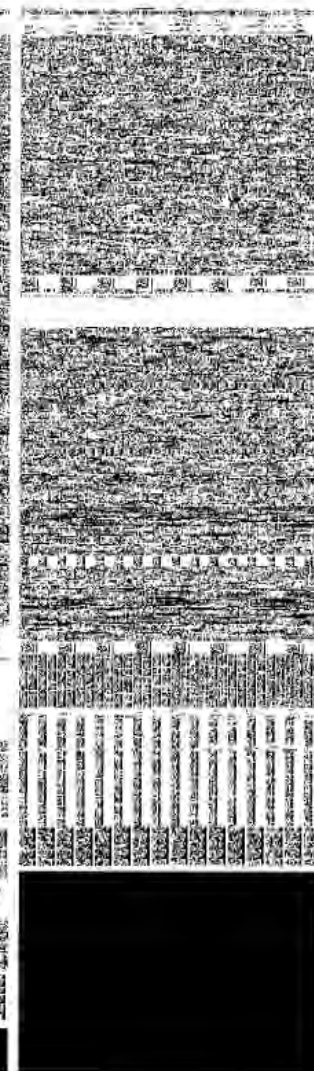
3

ip6fw.sys  
IPv6 Windows  
Firewall driver



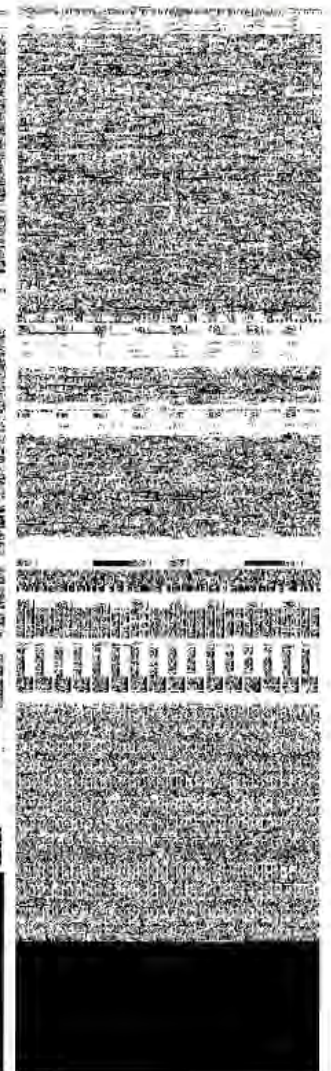
4

kbdclass.sys  
Keyboard class  
driver



5

mrxcsl.sys  
Stuxnet driver



6



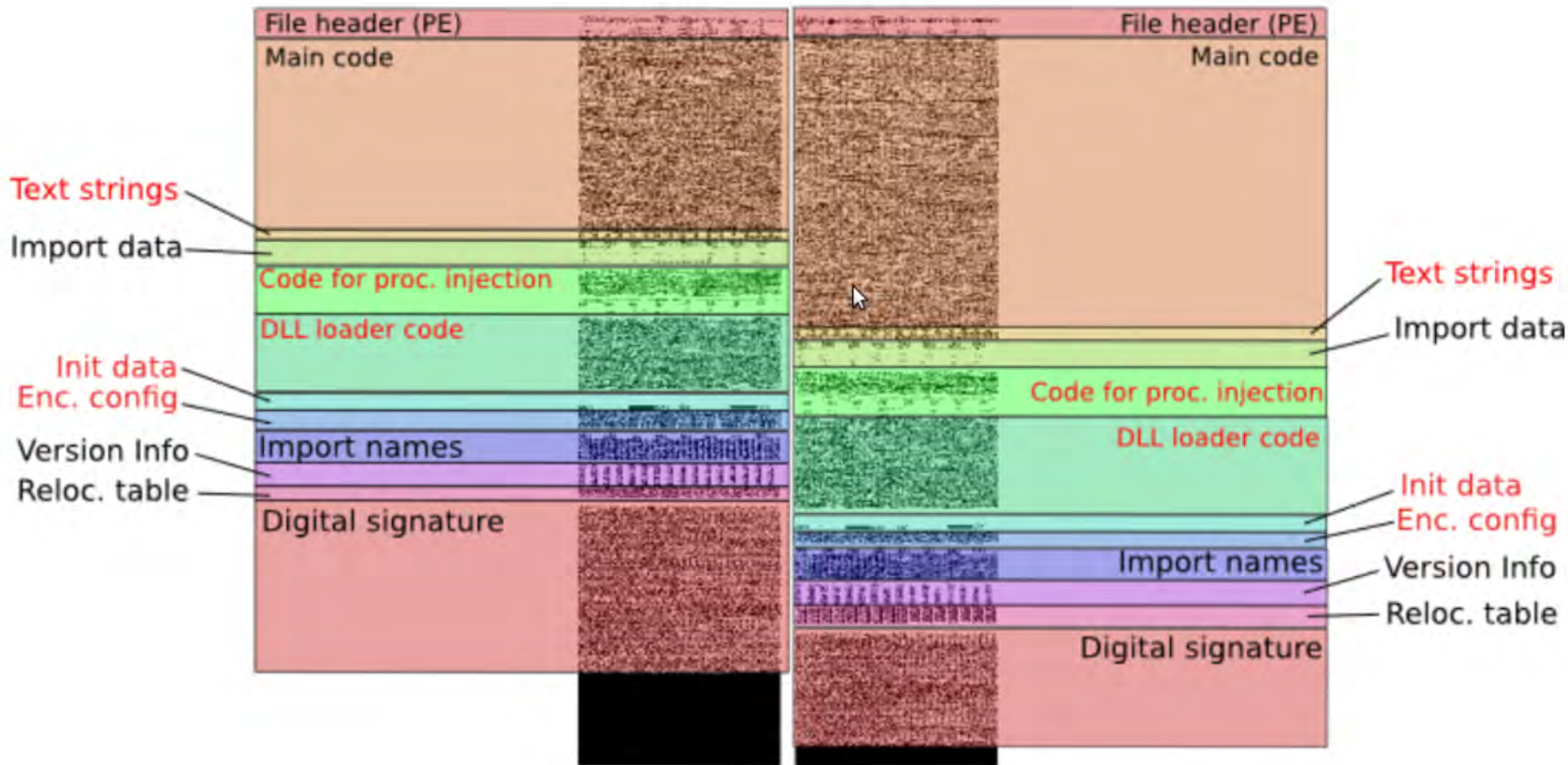
Duqu

Stux.



Stuxnet

Duqu





## Duqu embedded config

```
\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\cmi4432  
FILTER  
\Device\{3093AAZ3-1092-2929-9391}
```

---

## Stuxnet embedded config

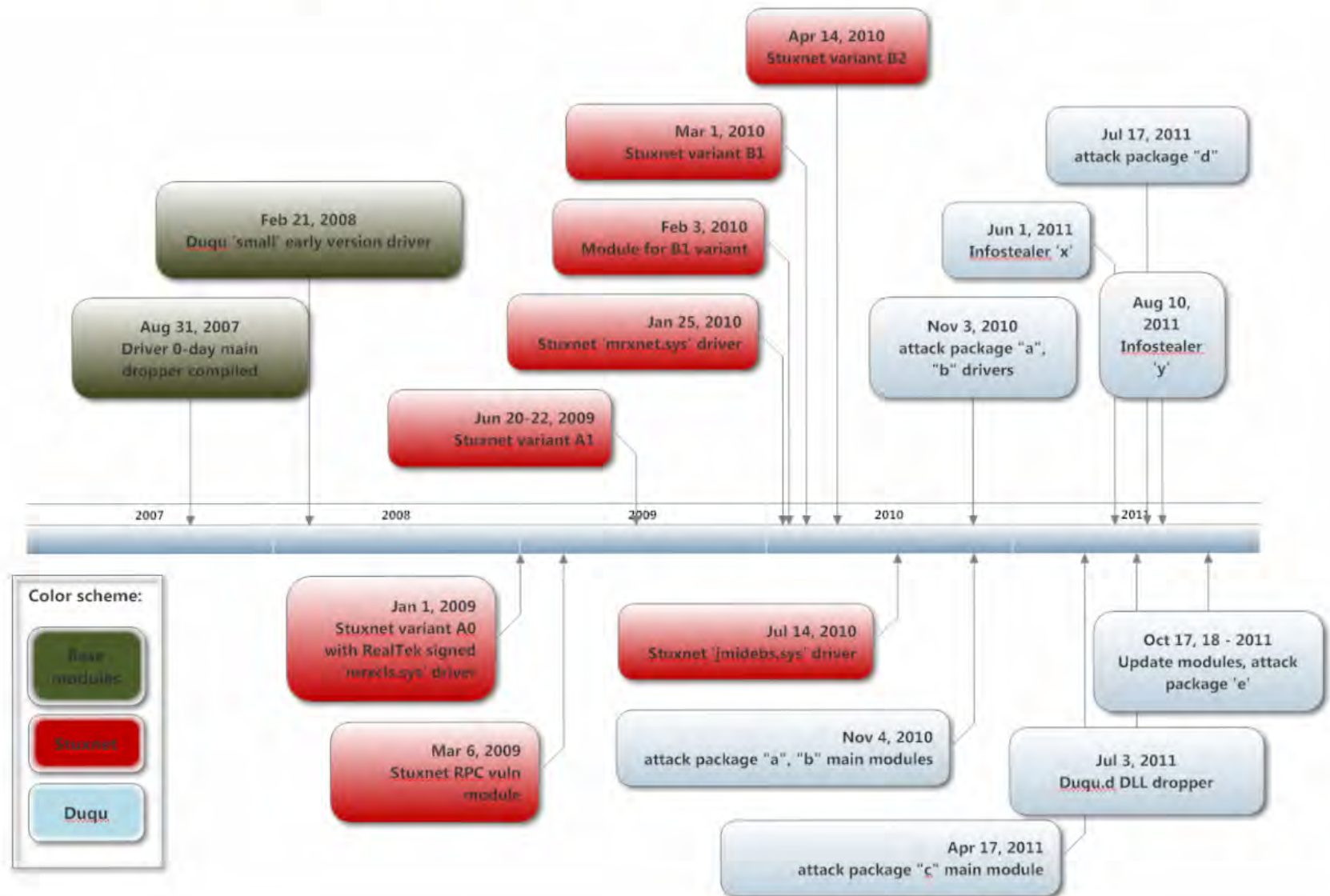
```
\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls  
Data  
\Device\MRxClsDvX
```

## Duqu driver installer PE header timestamp

Count of sections	6	Machine	intel386
Symbol table	00000000[00000000]		<b>Fri Aug 31 00:09:14 2007</b>
Size of optional header	00E0	Magic optional header	010B
Linker version	8.00	OS version	6.00
Image version	6.00	Subsystem version	5.00
Entry point	00000316	Size of code	00002F80
Size of init data	00000680	Size of uninit data	00000000
Size of image	00003900	Size of header	00000300
Base of code	00000300	Base of data	00002E80
Image base	00010000	Subsystem	Native
Section alignment	00000080	File alignment	00000080
Stack	00040000/00001000	Heap	00100000/00001000
Checksum	00013615	Number of directories	16

Development probably started around 2007.

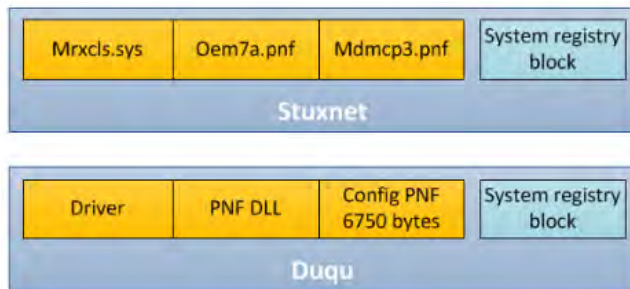
# Tilded Platform Timeline





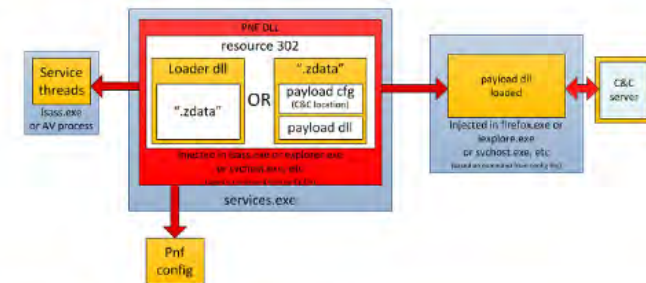
# Duqu research@Kaspersky

10-part research blogs at [www.securelist.com](http://www.securelist.com):



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?



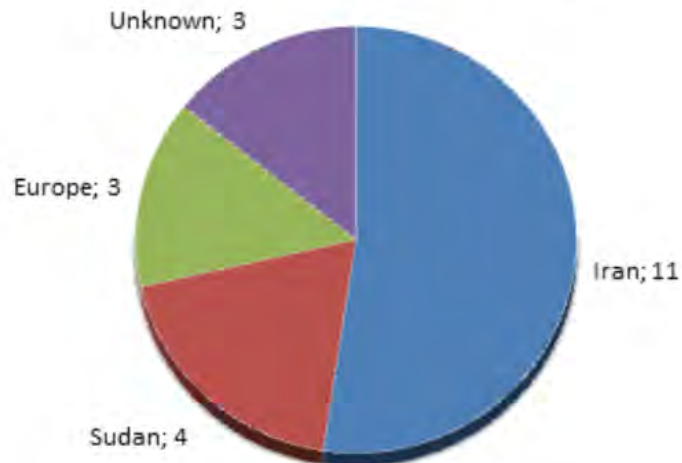
```
File: 'root'
Size: 4096          Blocks: 16          IO Block: 4096  directory
Device: 812h/2066d Inode: 7201921      Links: 9
Access: (0750/drwxr-x---)  Uid: (  0/
Context: root:object r:user_home_dir_t:s0
Access: 2011-11-03 12:12:45.000000000 +0300
Modify: 2011-10-20 18:07:28.000000000 +0300
Change: 2011-10-20 18:07:28.000000000 +0300
```



# Victims of Duqu:

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

## Many located in Iran



# **The Duqu victim scenario**



**How do you get infected  
with Duqu?**

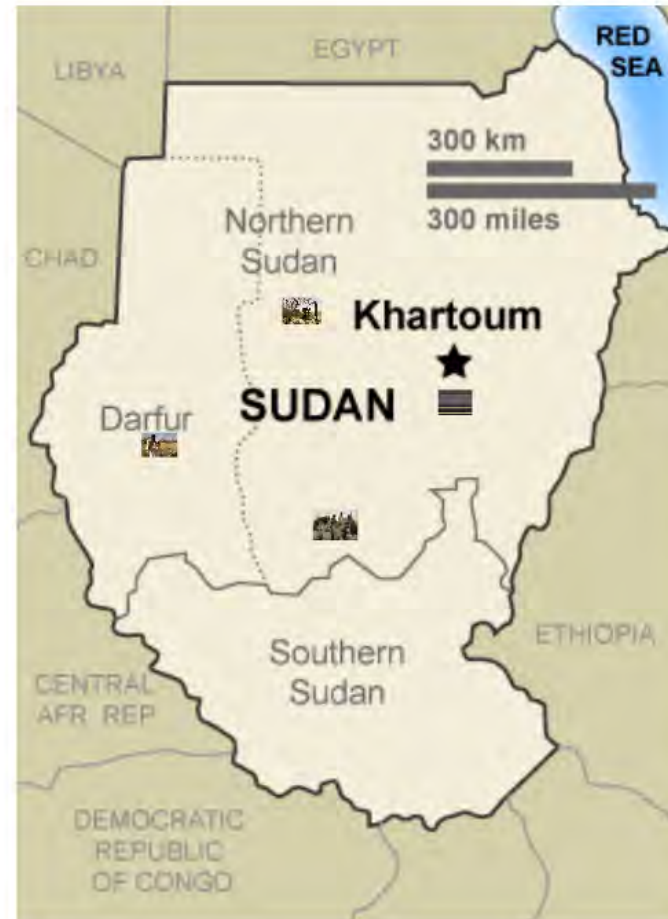


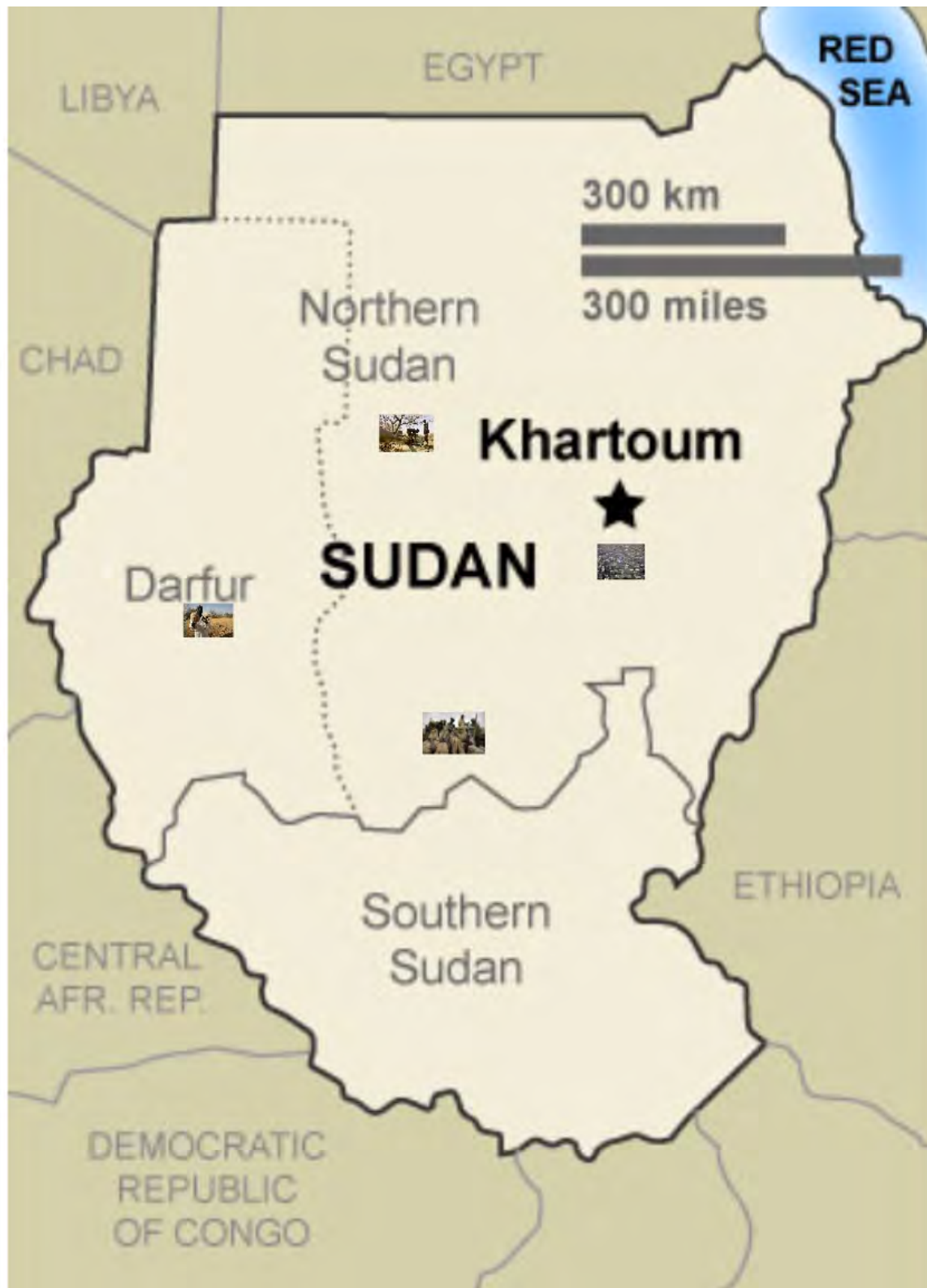
Very few real-world Duqu infections  
were fully analyzed.

The upcoming data was collected  
from a **real Duqu victim**.



# Our first detection of Duqu























# You have e-mail!

From: Jason B <bjason1[REDACTED].com>

Sent: Bc 17.04.2011 14:26

To: [REDACTED]

Cc:

Subject: [REDACTED] - Request for services

Message [REDACTED] request.doc (262 KB)

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

# You have

From: Jason B <bjason1[REDACTED].com>

To: [REDACTED]

Cc:

Subject: [REDACTED] - Request for services



Message



[REDACTED]request.doc (262 KB)

Dear Sir

I found the details of your company on yo

cooperation with your company. In the att

# CVE-2011-3402: TTF parsing vulnerability

Please send m  
1. Your co  
2. Recomm  
3. Price lis  
4. Price lis  
5. Do you



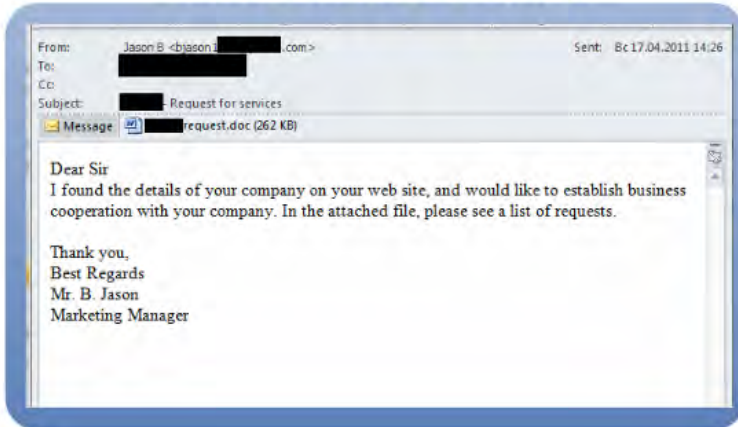
# CVE-2011-3402: TTF parsing vulnerability

Please send me the following information:

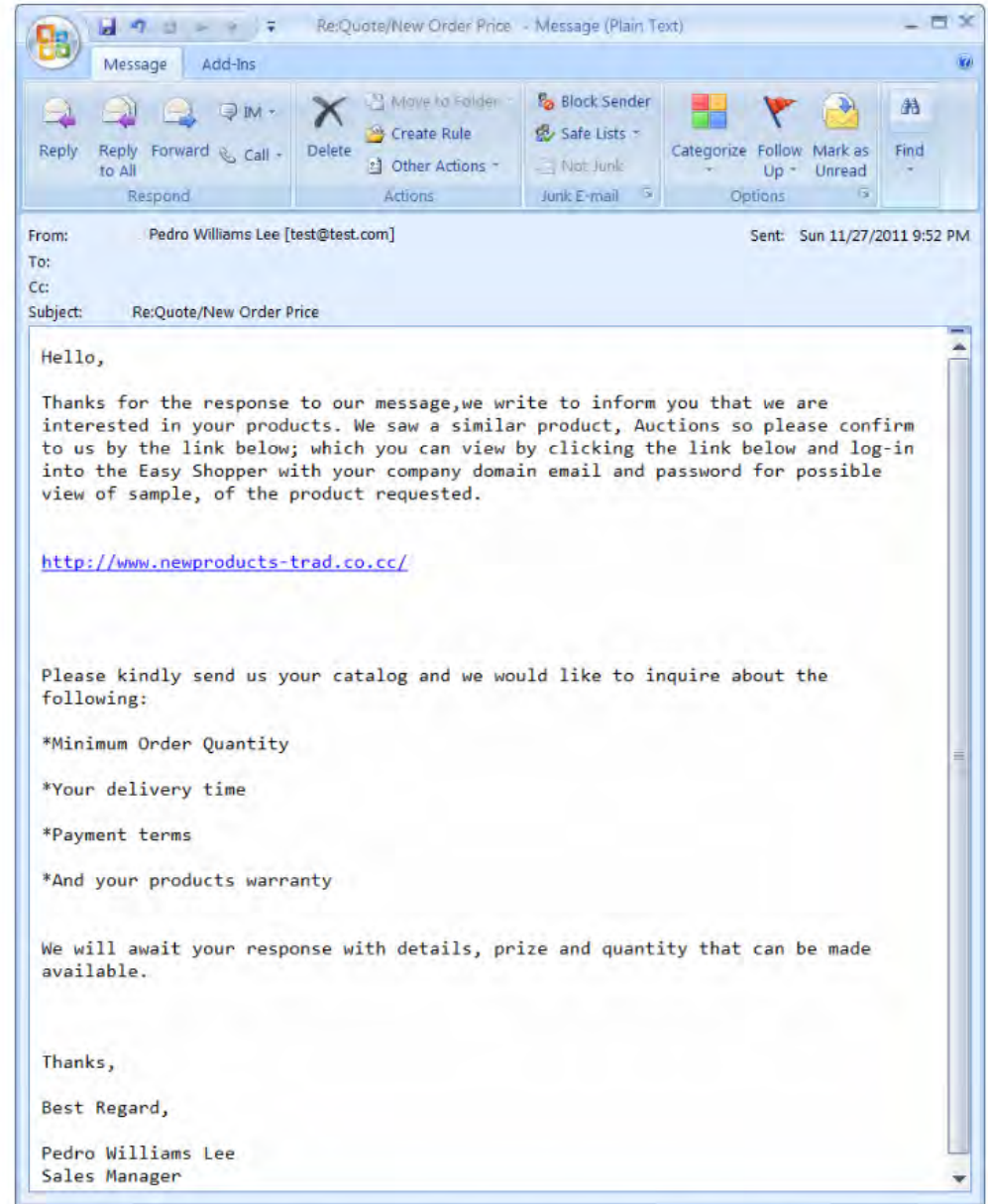
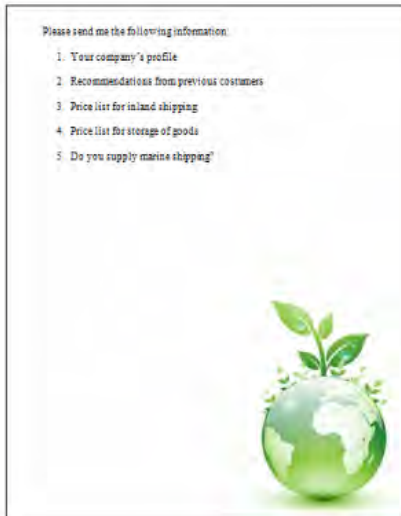
1. Your company's profile
2. Recommendations from previous costumers
3. Price list for inland shipping
4. Price list for storage of goods
5. Do you supply marine shipping?



# You have e-mail!

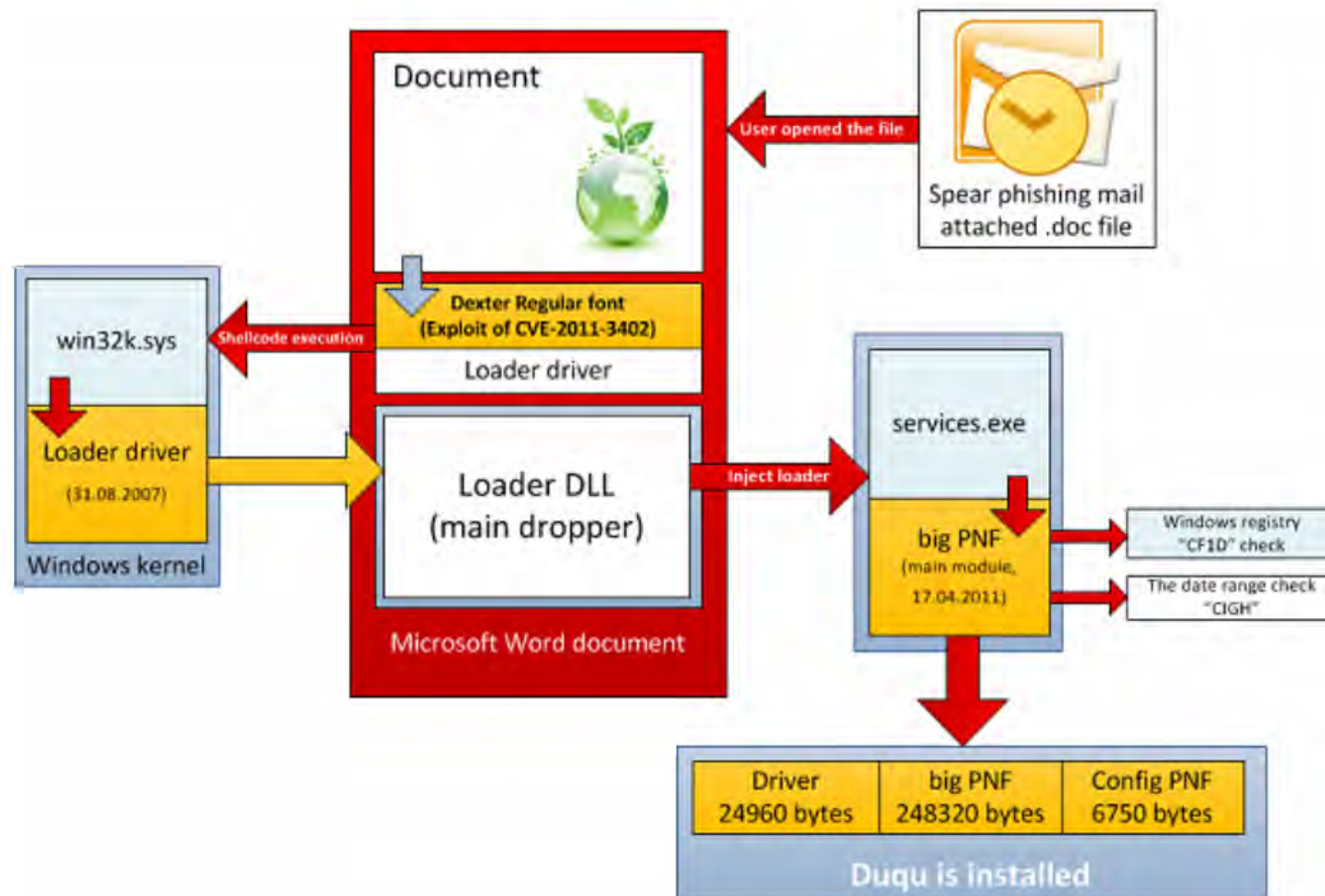


CVE-2011-3402: TTF parsing vulnerability



Based on real, world tested phishing mails.

# The Duqu full cycle





**Victim is infected!**  
**Now what?**

# Encrypted PNF

0000h:	ED 6F C8 DA 30 EE D5 01 D4 AE 8B 1F B5 A3 D2 A1 31 8D C3 2B 06 7F 6E F2 DC 31 0F 18 4E 80 0E C7	íøÉÚ0i0.0ø« .uf0;1.Ā+..nòU1..Ne.Ç
0020h:	BD C5 33 90 1F 78 15 9D 45 93 65 A1 8D 3D 43 CE CB 1C 26 45 B0 FF FC DD 93 A3 91 58 42 0D C6 A1	½Ā3..x..E"e;. =CİĒ. &E°yüY"ε'XB.E;
0040h:	B6 0E E0 B4 F8 AA 00 1E 51 0C 5A AD ED CA 8B CA 5F D3 63 12 59 DA 48 A1 75 6F 4E DD DA D5 0D 2C	Ÿ.à'ø*. .Q.Z-iĒ<Ē Ē Óc.YŪH;uoNYŪÓ.,
0060h:	3B 63 E5 B5 69 57 3C 7E 49 0E 8D 35 7C D0 0E A6 F4 1B 40 83 6E 01 C8 BF D6 9F B1 A5 C0 43 DF E5	;câuiW<-I..5]D.;Ē.Ēfn.Ēz;OY±ŸACBĀ
0080h:	AB FB A3 8E AC AC 0A E6 E6 13 40 D6 3B 1B 06 52 E9 45 78 B5 9C 38 CB B6 D7 AE 85 A7 41 EE 86 26	«ûiZ~-.ææ.Ē0;..RÉExpø8EŸ*ø...SAit&
00A0h:	3C B5 23 FA A0 2E E9 4C ED 31 8F 83 0D 0C E6 7D 5D A9 AB EE 7E F8 48 F0 77 22 02 6C C8 8B FA 90	<µ#ú .éLil.f.æ)]@«i-øHöw".lĒ<ú.
00C0h:	FE 41 7C 74 DC BF C9 C0 25 B6 9A 32 F2 01 4C 6F A9 15 E3 70 06 EE 71 4B BA A0 F6 41 3F D3 37 24	pAltÜ;ĒĀŸŸš2ð.Loo.ăp.iqK° øA?ó7Ÿ
00E0h:	D3 D8 C6 75 EA 25 9E 53 25 80 A1 18 49 85 C9 36 AC 45 7A 00 76 96 DA 0B 49 2A D8 15 9F 20 F1 D3	ÓØEuêšZšE; .I..Ē6-Ēz.v-Ū.I*ø.Y nÓ
0100h:	A5 E5 1E 87 61 FA B8 E7 C7 CD 56 67 9E E7 A2 D9 82 05 86 1E FA AB 6C 0B FB 2F AA 38 4A F4 81 72	ŸĀ. taú.ççÍVgžççŪ. .t.ú<l.Ū/*8Jð.r
0120h:	99 2D ED 5E 7F E6 18 20 A2 2A 66 1C 96 FA 15 EB DB FB A5 17 94 E6 41 B6 6D DA D6 8F CE 72 7B 7C	™-i^æ. ç*f.-ú.eŪŪŸ."æAŸMŪÓ.Ÿr{
0140h:	6F AA 03 52 B1 8E 87 E5 46 56 CC 4A 6E 13 AB 95 F5 8B 89 5A 8A A7 0F 2B D7 8A AE 79 07 DF 25 05	o*.Riž+âFVİŸn.«*ç%ZšŸ. +xšøy.š%
0160h:	5E B5 2B 6B 13 C2 26 0A 71 B7 99 65 E5 34 0E D6 63 87 A7 38 B4 47 A7 D7 D1 37 1F C0 5C 88 EB 56	^µ+k.Ā.š.q.™eâ4.Ōc+Ÿ8'GšN7.Ā\^ev
0180h:	9E 92 61 EF E4 D9 67 6A 43 87 F8 FA DF 3C 14 DD 3F BA BB 1D 11 9E BF 98 D7 52 E5 CD 19 76 7A CF	ž' aiäŪgjc+øúš<.Ÿ?°»..žž~*RáI.vzİ
01A0h:	E4 77 1F 13 B6 8C 38 21 BF 4A 63 B4 76 38 AB C5 ED 8D 47 68 4B 5C B1 1E DF 04 3F 48 98 6A 4E 3D	ăw..ŸŸB!;žc'v8Ā.Ī.GhK\±.š.žH~jN=
01C0h:	A1 89 D9 CB 8F 48 98 4E 79 F1 53 BA 9F 61 C7 CB 53 97 EB 15 22 44 AD A2 2D A9 7B 3B 7A 03 5F D0	;kŪĒ.H~NyŸš°ŸaçšEš-ē."D-ç-@(;z. Đ
01E0h:	74 FB 4A 6A CA E3 A3 4D E2 63 AC 55 83 7F 57 85 1F B4 73 4A 5E 4E A7 10 3A 37 5F DA 38 3B EE 6C	tŪjĒĀĒMâc-Uf.W... 'sJ^Nš.:7 Ū8;il
0200h:	99 1D E9 C8 63 D2 6E 60 62 BF 22 4B C2 27 BF D4 3D 7A 5D ED 02 F0 7E 1B E8 B5 7D C3 4A AE 92 63	™.ĒĒcòñ'bç"KĀ'žĒ=z]i.Ē.ĒèjĀŸø'c
0220h:	D3 40 04 7E 4F 02 67 46 E3 EB 6E E0 30 5C A4 E2 2D 3A BC 7D E0 2A 5C 97 2D ED C2 C4 3A C5 04 31	Ō@.~o.gFĀĒnà0\mâ-:¼}à*~--iĀĀ:Ā.1
0240h:	3F 0F 5F C9 26 64 59 A0 7D 68 E3 16 EF E1 8B 9F BB EA C3 3F DC 41 89 1C 40 22 7B 84 EF D4 67 99	? . Ē&dY }hĀ.iâ<Ÿ>ĒĀ?ŪĀk.@{"iŌg™
0260h:	60 23 2B 7E F8 29 BC C4 78 10 96 B8 0D E2 18 0E 7F E7 B5 34 76 3E 71 D7 8F F8 84 9C A0 FC 0D 56	`#+~ø)¼Āx.-.â...çµ4v>qx.ø„æ ū.v
0280h:	91 1B 6B 28 E0 0F 04 93 9A 18 71 1B 7D 2E 19 E3 71 13 84 1B 3F 33 06 DB D8 9E E5 E4 4E 92 CC 32	'k(â.. "š.q.). .ăq„. ?3.ŪðžĀĀñ'İ2
02A0h:	4B 74 F0 00 B5 96 77 42 8C BC EB F9 A4 F0 EC 4D 6F 20 94 57 18 FA CA 6F AE 7B 65 4B 81 91 D0 E3	Ktð.µ-wBç*æùmđiMo "W.úĒø@{eK. 'ĐĀ
02C0h:	31 DF EA BA 71 F1 EB A1 78 EC A9 E1 1E 25 46 7E D3 B5 1C 5C 42 58 68 B7 0F 8F 89 BA 58 FD 51 12	lšê°qñĒ;xiçá.%F~Ōµ.\BXh..%°XŸQ.
02E0h:	A6 AA 42 18 26 24 4B 5E 18 E3 5D E6 E8 12 97 73 17 AF E8 7D 65 F5 23 C8 41 C3 4F 88 6D 0D 85 FC	;'*B.&šK^ .ă]æĒ.-s.Ē)èð#ĒĀĀO'm...ú
0300h:	23 87 AB AC 19 A5 08 6D 11 30 4A 5F 4C 71 53 14 91 7E 03 93 DD 56 EF 2F 84 F6 1F 55 A1 E8 8E 76	#+«-.Ÿ.m.0J LqS.'~. "ŸŸVi/„ð.U;èžv
0320h:	3F 7A 02 0E 49 0E 63 20 57 71 DE 07 98 6F F0 97 6B 87 F8 6C 48 02 02 2C 02 BE 3B 3A 93 10 87 2C	?z..I.c Wqđ.~oð-k+ølH...:¼;:"+. ,
0340h:	C2 D3 F3 98 39 AC 3E BB FA CD 9F 11 F0 34 87 91 52 28 E0 2D D0 8C 4D 22 11 11 08 AA 62 1C FA A1	ĀŌó'9->»úíŸ.ð4+'R(à-ĐEM"...'b.ú;
0360h:	3A 8F 20 72 E8 16 4B 7A 41 4F E3 B7 B0 AD 5F A1 63 11 16 80 F3 53 2E 37 F0 6E 6C DE B4 98 B9 52	:. rē.KzAOĀ°- ;c..e6s.7ðñlB'™R
0380h:	2C 46 19 36 53 91 31 61 02 39 0D 63 61 9D 93 46 6F 04 3D 20 16 8F 3F 42 68 FA FD C7 50 84 4A CE	,F.6S'la.9.ca."Fo.= ..?BhúŸCP„JĪ
03A0h:	90 89 94 02 39 16 D1 58 E3 28 F1 80 DD 90 85 79 F0 D6 40 42 52 33 0A 05 17 E9 D3 FB E7 F4 10 6E	.%".9.NXĀ (ñĒŸ...yðŌ@BR3...éŌŸçð.n
03C0h:	28 08 5D 85 44 35 AB 0A BB 83 E4 81 18 0F 73 8E E3 68 F0 D9 52 01 B6 9C 35 EA 8E 35 06 67 6F 28	(. ]...D5«.»fĀ...sžĀhðŪR.Ÿæ5ēž5.go(
03E0h:	CC F0 E2 1F 93 CE F9 1B F8 F3 24 4C D4 EC 30 5A C8 63 B3 E8 18 42 F4 C6 0F 56 C4 1C 7F 55 AA A1	İĒĀ."İù.ðøŸlŌi0ZĒç°è.BŌĒ.VĀ..Ū*;
0400h:	BA 67 89 80 ED 00 EB 81 16 41 55 EF C4 74 FB 94 1F 75 61 3D 30 EE 0D C8 D2 92 40 8C 1F 77 97 BF	°g%Ēi.ē..AUIĀtŪ".ua=0i.Ēò'@E.w-ž
0420h:	F9 B0 29 22 A4 57 86 5E 59 AF D4 FA 24 03 EE C0 5E 3C 6C B0 D8 C9 5B C6 5B 38 F8 47 E2 5F AD E8	ù°)"mW+Ÿ'ŪŸš.iĀ<l°ŌĒ]Ē[8øGĀ -ē

Large .PNF file inside "C:\Windows\inf"



# Decrypted PNF

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF0123456789ABCDEF		
0000h:	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	MZ.....ÿÿ.....@.....		
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	00	00	00	.....	
0040h:	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	..°.!.í!..Lí!This program cannot		
0060h:	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	be run in DOS mode....\$.....		
0080h:	96	29	1C	7A	D2	48	72	29	D2	48	72	29	D2	48	72	29	CC	1A	F6	29	D9	48	72	29	CC	1A	E7	29	C7	48	72	29	-).zòHr)òHr)òHr)ì.ò)ÙHr)ì.ç)ÇHr)		
00A0h:	CC	1A	F1	29	D4	48	72	29	DB	30	F6	29	F3	48	72	29	DB	30	F1	29	88	48	72	29	F5	8E	09	29	C1	48	72	29	ì.ñ)òHr)Ù0ò)óHr)Ù0ñ)^Hr)òŽ.)ÁHr)		
00C0h:	D2	48	73	29	33	48	72	29	DB	30	F8	29	81	48	72	29	DB	30	E0	29	D3	48	72	29	CC	1A	E6	29	D3	48	72	29	òHs)3Hr)Ù0ø).Hr)Ù0à)óHr)ì.æ)óHr)		
00E0h:	DB	30	E3	29	D3	48	72	29	52	69	63	68	D2	48	72	29	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	Ù0ä)óHr)RichòHr).....		
0100h:	50	45	00	00	4C	01	06	00	93	4F	5B	4D	00	00	00	00	00	00	00	00	00	00	E0	00	02	2D	0B	01	09	00	00	00	PE..L...`O[M.....à.-.....°..		
0120h:	00	2A	04	00	00	00	00	69	30	01	00	00	10	00	00	00	C0	01	00	00	00	00	10	00	10	00	00	00	02	00	00	00	.*.i0.....À.....		
0140h:	05	00	00	00	00	00	00	05	00	00	00	00	00	00	00	00	10	07	00	00	10	00	00	00	00	00	00	00	02	00	00	00	.....		
0160h:	00	00	10	00	00	10	00	00	00	10	00	00	00	00	00	00	00	10	00	00	00	00	00	E0	C2	01	00	4A	00	00	00	00	.....àÀ..J...		
0180h:	24	4E	02	00	B4	00	00	00	00	D0	03	00	58	F6	02	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	\$N..'.D..Xò.....		
01A0h:	00	D0	06	00	34	23	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	.D..4#.....		
01C0h:	00	00	00	00	00	00	00	00	C8	F1	01	00	40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....Èñ..@.....	
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	00	00	00	.....text...	
0200h:	66	AE	01	00	00	10	00	00	00	B0	01	00	00	04	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	f@.....°.....`	
0220h:	2E	72	64	61	74	61	00	00	0E	9D	00	00	C0	01	00	00	9E	00	00	00	B4	01	00	00	00	00	00	00	00	00	00	00	00	.rdata.....À...ž.....	
0240h:	00	00	00	00	40	00	00	40	2E	64	61	74	61	00	00	00	A0	44	01	00	00	60	02	00	00	00	00	00	00	00	00	00	00	...@..@.data... D...`...>...R..	
0260h:	00	00	00	00	00	00	00	00	00	00	00	40	00	00	C0	2E	63	64	61	74	61	00	00	5E	1A	00	00	00	B0	03	00	00	00	.....@..À.cdاتا.^.....°..	
0280h:	00	1C	00	00	00	90	02	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	.....@..À.rsrc...	
02A0h:	58	F6	02	00	00	D0	03	00	00	F8	02	00	00	AC	02	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	Xò...D...ø...~.....@..@	
02C0h:	2E	72	65	6C	6F	63	00	00	82	39	00	00	00	D0	06	00	00	3A	00	00	00	A4	05	00	00	00	00	00	00	00	00	00	00	.reloc.,9...D...:...=.....	
02E0h:	00	00	00	00	40	00	00	42	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	...@..B.....	
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	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	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	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	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	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	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	00	00	00	00	.....
03E0h:	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	00	00	00	00	.....
0400h:	B8	4F	9D	01	10	E8	0A	7C	01	00	8B	4D	08	E8	46	71	00	00	83	4D	FC	FF	8B	4D	F4	8B	45	08	64	89	0D	00	00	00	.O...è. ...<M.èFq...fMuy<Mò<E.d%..
0420h:	00	00	00	C9	C2	04	00	B8	4F	9D	01	10	E8	E3	7B	01	00	83	4D	FC	FF	FF	75	08	E8	0E	00	00	00	8B	4D	F4	00	00	...ÉÁ...O...èã{...fMuyÿu.è....<Mó







# .rsrc section

0000h:	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 40 00 00 00 00 00 00	MZ.....yy...@.....
0020h:	00 00	.....è...
0040h:	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	..°..'í!..Lí!This program cannot
0060h:	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	be run in DOS mode...\$.....
0080h:	C7 5E 5E 5C 83 3F 30 0F 83 3F 30 0F 83 3F 30 0F A4 F9 4B 0F 86 3F 30 0F 83 3F 31 0F A8 3F 30 0F	Ç^^\f?0.f?0.f?0.mùK.†?0.f?1."?0.
00A0h:	8A 47 B3 0F 8D 3F 30 0F 9D 6D A5 0F 80 3F 30 0F A4 F9 4D 0F 82 3F 30 0F 8A 47 B9 0F 8B 3F 30 0F	ŠG³..?0..m¥.€?0.mùM.,?0.ŠG¹.<?0.
00C0h:	8A 47 A2 0F 82 3F 30 0F 8A 47 A1 0F 82 3F 30 0F 52 69 63 68 83 3F 30 0F 00 00 00 00 00 00 00 00	ŠGç.,?0.ŠG;.,?0.Richf?0.....
00E0h:	00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00 1F 68 10 4D 00 00 00 00 00 00 00 00 00 00	.....PE..L...h.M.....à..-
0100h:	0B 01 09 00 00 38 00 00 00 BC 02 00 00 00 00 00 E0 12 00 00 00 10 00 00 00 00 50 00 00 00 00 10	.....8...¼.....à.....P.....
0120h:	00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 03 00 00 04 00 00	.....0.....
0140h:	00 00 00 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 10 00 00 00	.....@.....
0160h:	40 72 00 00 D1 00 00 00 24 6F 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@r..Ñ...šo..(.....
0180h:	00 00 00 00 00 00 00 00 20 03 00 74 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....t.....
01A0h:	00 00	.....m..@.....
01C0h:	00 50 00 00 94 00	.P.."......
01E0h:	2E 74 65 78 74 00 00 00 8C 36 00 00 00 10 00 00 00 38 00 00 00 04 00 00 00 00 00 00 00 00 00	.text...€6.....8.....
0200h:	00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 00 11 23 00 00 00 50 00 00 00 24 00 00 00 3C 00 00	.... ..`rdata...#...P...\$...<..
0220h:	00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2E 64 61 74 61 00 00 00 0C 32 00 00 00 80 00 00	.....@..@.data...2...€..
0240h:	00 32 00 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0 2E 7A 64 61 74 61 00 00	.2...`.....@..À.zdata..
0260h:	CD 5C 02 00 00 C0 00 00 00 60 02 00 00 92 00 00 00 00 00 00 87 55 39 BC 00 00 00 00 40 00 00 C0	í\...À...`...'.....+U9%...@..À
0280h:	2E 72 65 6C 6F 63 00 00 50 03 00 00 20 03 00 00 04 00 00 00 F2 02 00 00 00 00 00 00 00 00 00	.reloc..P.....ò.....
02A0h:	00 00 00 00 40 00 00 42 00	...@..B.....
02C0h:	00 00	.....
02E0h:	00 00	.....
0300h:	00 00	.....
0320h:	00 00	.....
0340h:	00 00	.....
0360h:	00 00	.....
0380h:	00 00	.....
03A0h:	00 00	.....
03C0h:	00 00	.....
03E0h:	00 00	.....
0400h:	55 8B EC 83 EC 0C 8B 45 10 53 56 33 F6 57 8B 7D 08 33 C9 89 75 FC C7 45 F8 01 00 00 00 F6 C1 7F	U<i fi.<E.SV36W<} .36%uüÇEø....øÁ.
0420h:	74 04 03 C9 EB 09 0F B6 0C 3E 8D 4C 09 01 46 BB 00 01 00 00 85 CB 74 0F 8A 14 3E 8B 5D FC FF 45	t..Éé..¶.>.L..F».....Et.Š.>< úyE



# .zdata section

0000h:	0E 12 39 D1 57 81 04 00 FE 93 71 74 48 57 97 00	..9ÑW...p"qtHW-
0010h:	5F EA 03 00 24 BE 96 0D 33 01 F6 07 24 1C ED 00	_ê..\$¾-.3.ö.\$.í.
0020h:	96 00 01 3F 4D 5A 90 00 03 6B 0E 04 06 65 FF FF	-...?MZ...k...eÿÿ
0030h:	B0 B8 2F ED 40 00 01 57 E8 6F 06 0E 1F BA 0E FF	°,/í@..Wèö...°.ÿ
0040h:	00 B4 09 CD 21 B8 01 4C 7F 09 54 68 69 73 FF 20	.'.í!.,L..Thisÿ
0050h:	70 72 6F 67 72 61 6D FF 20 63 61 6E 6E 6F 74 20	programÿ cannot
0060h:	FF 62 65 20 72 75 6E 20 69 7F 05 44 4F 53 20 FF	ÿbe run i..DOS ÿ
0070h:	6D 6F 64 65 2E 0D 0D 0A B0 24 87 FF C7 5E 5E 5C	mode....°\$+ÿÇ^^\
0080h:	83 3F 30 B1 0F 07 FD A4 F9 4B 0F 86 9E 17 31 0F	f?0±..ÿáùK.†ž.1.
0090h:	A8 DF 0E 8A 47 B3 0F 8D 37 9D 6D A5 D9 0F 80 3F	"B.ŠG³..7.mÿÙ.€?
00A0h:	EC 4D 0F 82 2F F6 B9 0F 8B 0F 6C A2 1F 36 A1 0F	iM.,/ö¹.<.lç.6;.
00B0h:	7D 52 69 63 68 C1 8E 57 47 50 BE 45 07 4C 01 0F	}RichÁŽWGP¾E.L..
00C0h:	CB 1F 68 D8 10 4D 27 FF E0 00 02 2D 0B 01 BD 09	Ë.hØ.M'ÿà...-...½.
00D0h:	11 38 AC 18 5C 27 36 12 08 BB 10 60 1D 36 10 17	.8-.\'6..».`.6..
00E0h:	6F 02 05 05 61 67 63 0F C3 00 D0 69 0B 3D 3B 40	o...agc.Ã.Đi.=;@
00F0h:	01 69 3D 10 00 00 AD 0F BD 0D 40 72 ED 07 D1 0E	.i=...-...½.@rí.Ñ.
0100h:	24 BC 6F 07 28 34 99 1D C0 F0 05 74 02 D5 E7 78	\$¾o.(4 <sup>m</sup> .Àð.t.Õçx
0110h:	A0 6D A8 37 41 4E 5A 94 5F 07 2E 74 ED 65 78 74	m"7ANZ"__..tiext
0120h:	0E 8C 82 36 21 18 38 2B 6F 63 01 BF 20 05 60 2E	.€.,6!.8+oc.¿ .`.



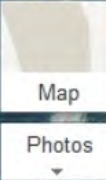
# Inside .zdata

9640h:	00 44 00 52 00 30 00 30 00 30 00 31 00 2E 00 74	.D.R.0.0.0.1...t
9650h:	00 6D 00 70 00 20 00 00 00 33 BC 0F FE 14 17 B0	.m.p. ...3¼.p..°
9660h:	33 EF 22 9F 45 FA 42 25 5A 4E 5A 9E 20 11 6C CD	3i"ŸEúB%ZNZž .lí
9670h:	13 13 0A 61 44 93 09 96 45 96 00 00 00 01 00 F4	...aD".-E-.....ô
9680h:	01 2C 01 2C 01 0A 00 22 00 01 00 02 00 1E 00 14	.....".....
9690h:	00 02 00 3C 00 00 00 01 00 01 00 00 00 00 00 2C	...<.....,
96A0h:	00 00 00 BB 01 00 00 00 00 90 1F 32 00 30 00 36	...».....2.0.6
96B0h:	00 2E 00 31 00 38 00 33 00 2E 00 31 00 31 00 31	...1.8.3...1.1.1
96C0h:	00 2E 00 39 00 37 00 00 00 00 00 00 00 00 1E	...9.7.....
96D0h:	00 14 00 02 00 3C 00 00 00 01 00 02 00 01 00 00	.....<.....
96E0h:	00 13 00 00 00 CE B7 6F 61 50 00 03 02 00 DC 05	.....Î·oaP....Û.
96F0h:	00 00 00 00 00 00 00 00 01 00 00 00 13 00 00 00	.....
9700h:	CE B7 6F 61 50 00 02 02 00 DC 05 00 00 00 00 00	Î·oaP....Û.....
9710h:	00 00 00 4D 5A 90 00 03 00 00 00 04 00 00 00 FF	...MZ.....ÿ
9720h:	FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00	ÿ..,.....@....
9730h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
9740h:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 F8	.....ø
9750h:	00 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD	.....°..´.í! ,.lí
9760h:	21 54 68 69 73 20 70 72 6F 67 72 61 6D 20 63 61	!This program ca
9770h:	6E 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44	nnot be run in D
9780h:	4F 53 20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00	OS mode....\$....

**206.183.111.97**

**Duqu's C&C server IP**





Web Werks, Data Center & Dedicated Servers Mumbai

Blue Star

Utsav Restaurant & Banquets

Imagery ©2012 DigitalGlobe, GeoEye - Edit in Google Map Maker

200 ft  
50 m

Adarsh English High School Secondary

Anant Vishram Nagvekar Mg

TATA Press

Future Generali India Life Insurance Company Limited

National Institute of Personnel Management

Paville House

Vitesse Trading Pvt. Ltd

Hindustan Mills

Deccan Manor

Shan Apartment

Electronics Corporation of India Limited

Downtown Dhaba

Yadav Patel Ln

Petrol Pump

HDFC Bank

Kamat Industrial Estate

Swatantra Veer Savarkar Marg

Engineered Materials

Domino's Pizza

Siddhivinayak Temple

walia packers movers

Kohinoor Park

Kohinoor Hall And Banquets

Kakasaheb Gadgil Marg

Sane Guruji Garden

Eknath Buwa Hatiskar Marg

Silver Dune

Yuvati Sharan

Gcafe

Pratamesh CHS

P. Balu Marg

Green Veggies

Sea Side

Bus Stop

DCB

Dena Bank





Pvt. Ltd

Paville House

Hindustan Mills

TANTRAA BRAND SOLUTIONS PVT

Web Werks, Data Center & Dedicated Servers Mumbai

Kamat Industrial Estate

National Institute of Personnel Management

Engineered Materials

Domino

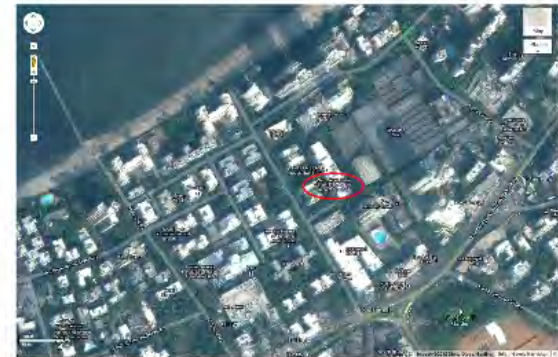


# Duqu known C&C servers

Everybody knows...

206.183.111.97 - India, Mumbai

77.241.93.160 - Belgium, Gent



Other "Unknown" C&C's:

112.213.x.x - Vietnam

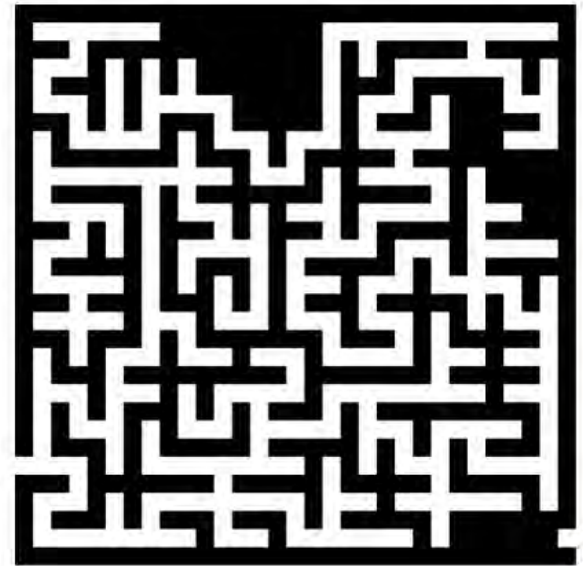
123.30.x.x - Vietnam

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

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

**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 -dlr 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...  
  
Connected to centos-vm (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

```
# GSSAPI options
```

```
GSSAPIAuthentication yes
```

```
UseDNS yes
```

Before hack

```
# GSSAPI options
```

```
GSSAPIAuthentication no
```

```
UseDNS no
```

After hack

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'.

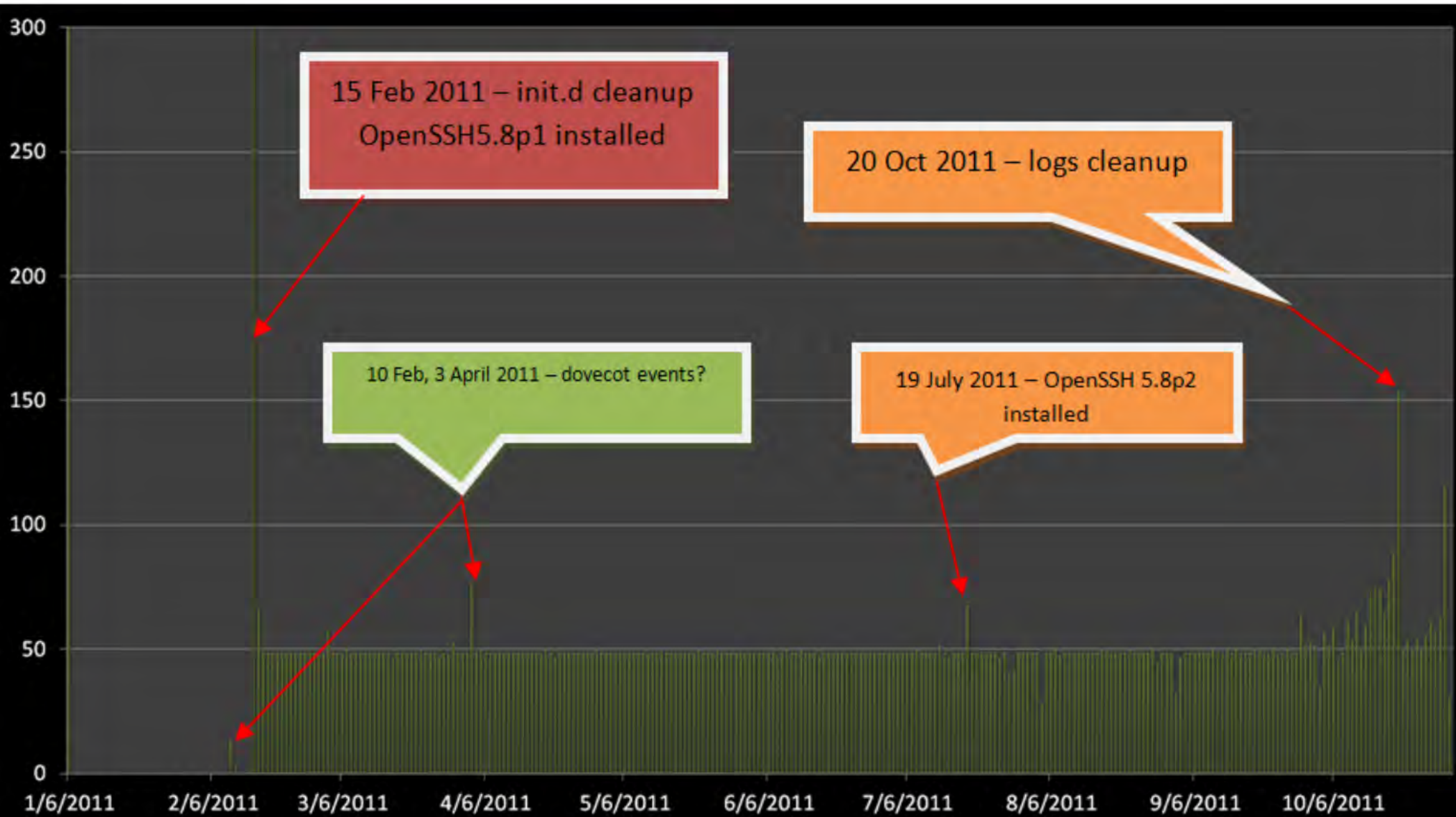
# Pitfalls of file deletion

## 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!**





# 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. [REDACTED] user=root
Nov 18 15:21:13 n8s005 sshd[29072]: Failed password for root from 202.45. [REDACTED] port 46503 ssh2
Nov 18 15:21:50 n8s005 sshd[29073]: Connection closed by 202.45. [REDACTED]
Nov 18 15:21:50 n8s005 sshd[29072]: PAM 2 more authentication failures; logname= uid=0 euid=0
tty=ssh ruser= rhost=202.45. [REDACTED] user=root
...
Nov 18 15:27:12 n8s005 sshd[29098]: Failed password for root from 202.45. [REDACTED] port 46643 ssh2
Nov 18 15:27:14 n8s005 sshd[29099]: Connection closed by 202.45. [REDACTED]
Nov 18 15:29:53 n8s005 sshd[29104]: Accepted password for root from 202.45. [REDACTED] 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. [REDACTED] user=root
Nov 18 15:21:13 n8s005 sshd[29072]: Failed password for root from 202.45. [REDACTED] port 46503 ssh2
Nov 18 15:21:50 n8s005 sshd[29073]: Connection closed by 202.45. [REDACTED]
Nov 18 15:21:50 n8s005 sshd[29072]: PAM 2 more authentication failures; logname= uid=0 euid=0
tty=ssh ruser=rhost=202.45. [REDACTED] user=root
...
Nov 18 15:27:12 n8s005 sshd[29098]: Failed password for root from 202.45. [REDACTED] port 46643 ssh2
Nov 18 15:27:14 n8s005 sshd[29099]: Connection closed by 202.45. [REDACTED]
Nov 18 15:29:53 n8s005 sshd[29104]: Accepted password for root from 202.45. [REDACTED] port 46712 ssh2
```

# How do they get hacked?

Theory nr 2:

CentOS 0-day (in OpenSSH 4.3)

07-03-2009, 09:06 PM

**jon-f**  
Disabled

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 **say they are 100% positive it is an openssh 4.3 exploit** they said updating t wrong but even a rumor of an ssh exploit will have me upgrading.

Sometimes, well most of the time, RHEL team is slow on updates and Centos is even slower because they have to wait on them a 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 under 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 grsecurity 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. S

Attached Files

**opensshd\_sniff\_bug.zip** (189.3 KB, 898 views)



**That's (too) scary!!!**

# How do they get hacked?

Theory nr 3:  
Another malware!

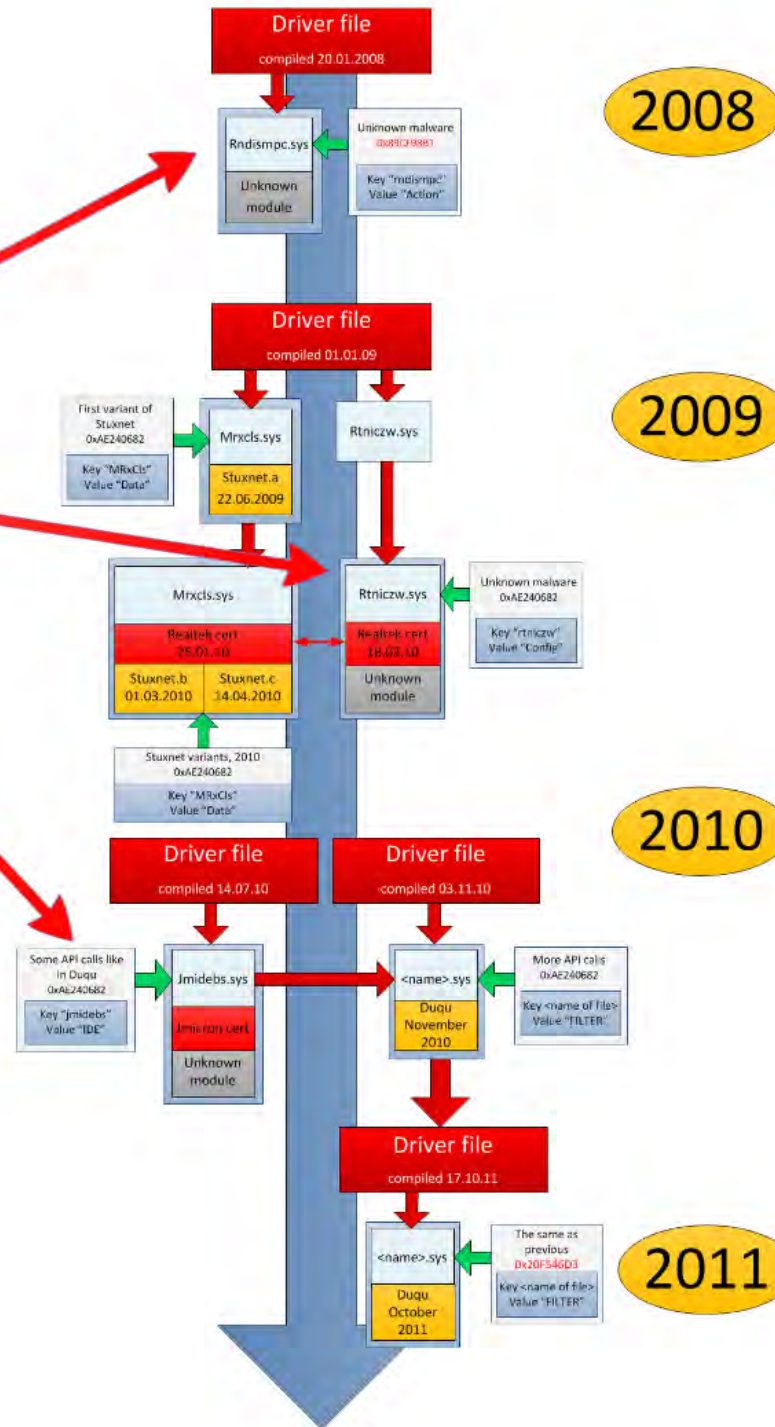
1. Password stealer malware
2. A version of Duqu
3. Purchase of credentials on black market

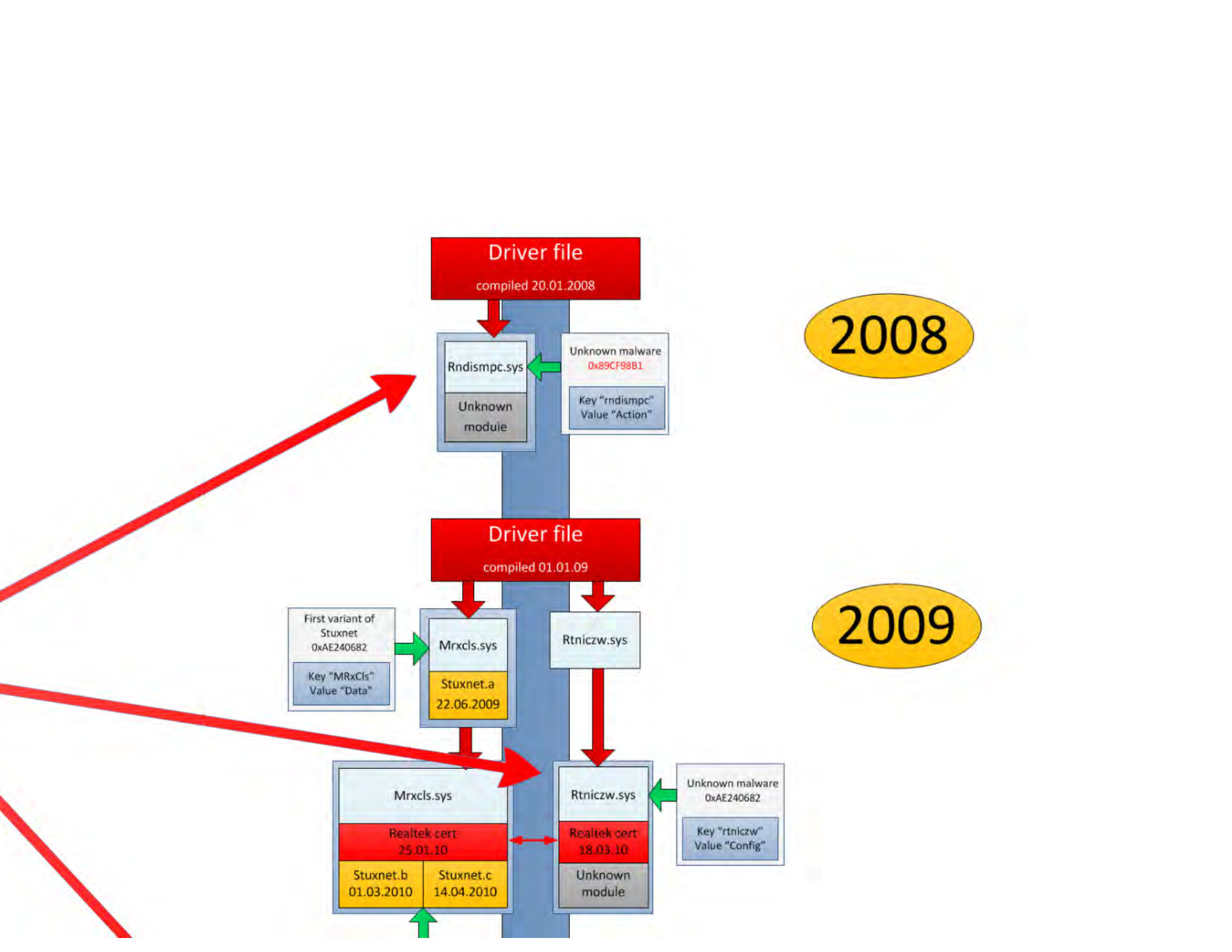


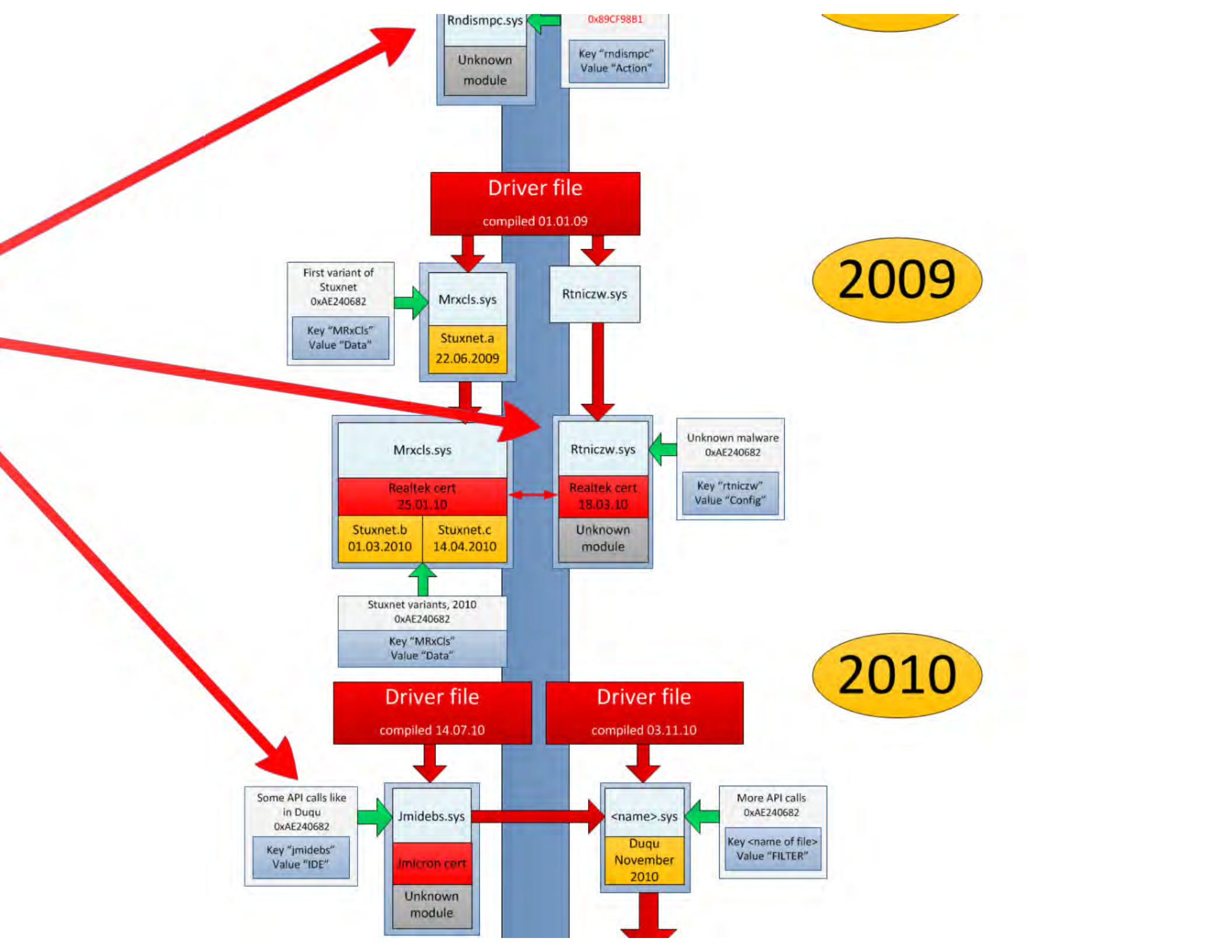
## How do they get hacked?

Theory nr 3:  
Another malware!

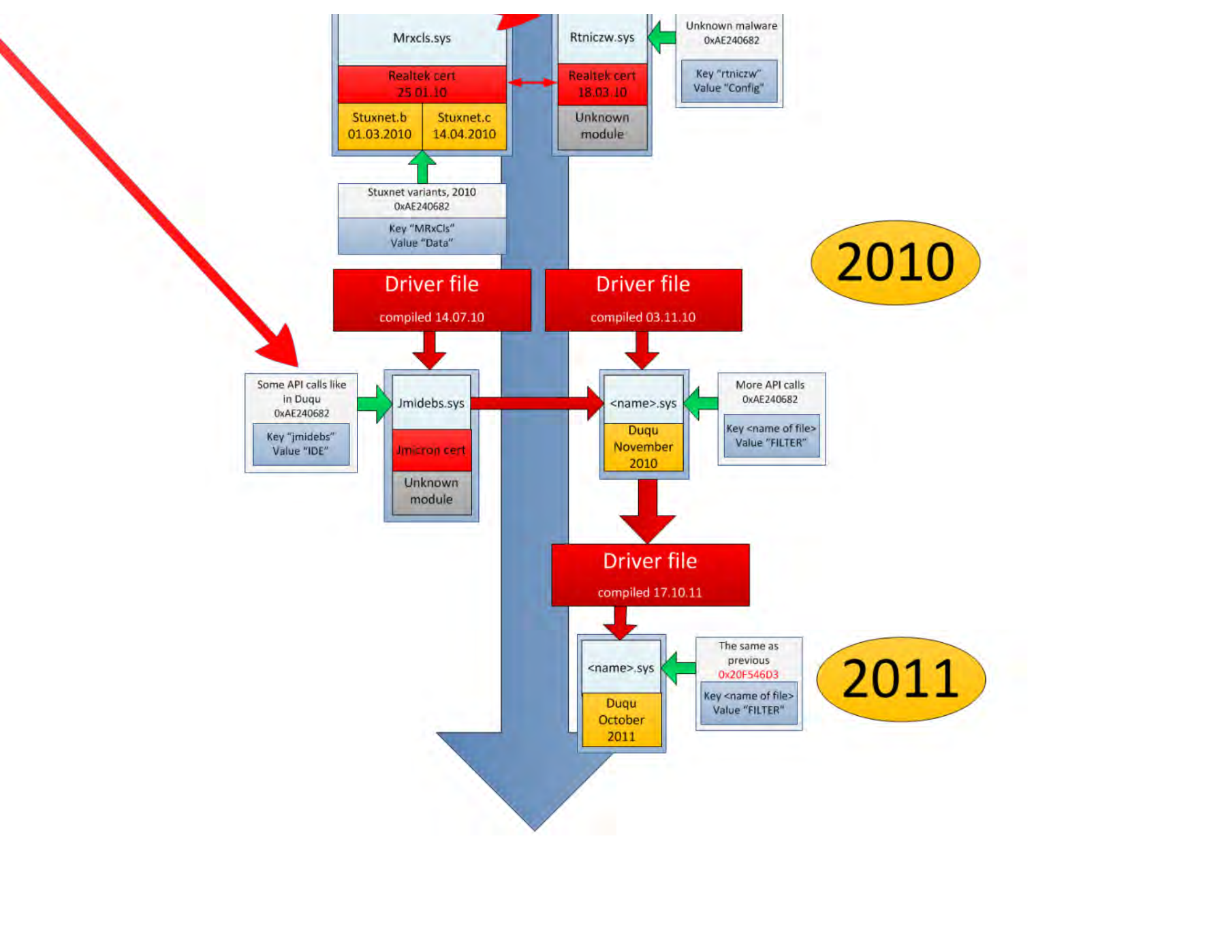
1. Password stealer malware
2. A version of Duqu
3. Purchase of credentials on black market













# Server 'B'

A special case:

Memory dump!





# Deep inside the memory dump...

```
#4 forwarded-tcpip: listening port 443 for 0.0.0.0 port 0, connect from 90.13.
port 2177 (t4 r136480 i0/0 o0/0 fd 11/11 cfd -1)
#5 forwarded-tcpip: listening port 443 for 0.0.0.0 port 0, connect from 90.13.
port 2178 (t4 r136483 i0/0 o0/0 fd 12/12 cfd -1)
#6 server-session (t4 r136578 i3/0 o3/0 fd 14/14 cfd -1)
(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
@1ysatoA
3des-cbcA
```

```
(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  
@1ysatoA  
3des-cbcA
```

# What is SharpSSH-3.0?

Let's Google it!





Search

About 117,000 results (0.25 seconds)

Everything

Images

Maps

Videos

News

Shopping

More

Show search tools

Ad - Why this ad?

[Tired of \*\*SharpSSH\*\* bugs? | eldos.com](#)[www.eldos.com/SecureBlackbox](http://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](http://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/](http://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](http://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/](http://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/](http://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...](http://danielcai.blogspot.com/.../sharpssh-recompiled-version-compatible.ht...)26 Nov 2010 – NET framework itself, I have to look for alternative solution, so I ended up with the open source library called **SharpSSH** which is pretty

## 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](#).

### Feaure 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

### ABOUT ME



Searching with my good eye closed ;-)

Enter search term

Search also comments

### MENU

[Home](#)

[Blog](#)

[SharpSSH](#)

[SharpPcap](#)

[Pictures](#)

[Music](#)

### CALENDAR

<< January 2012 >>

Mo Tu We Th Fr Sa Su



# 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#?

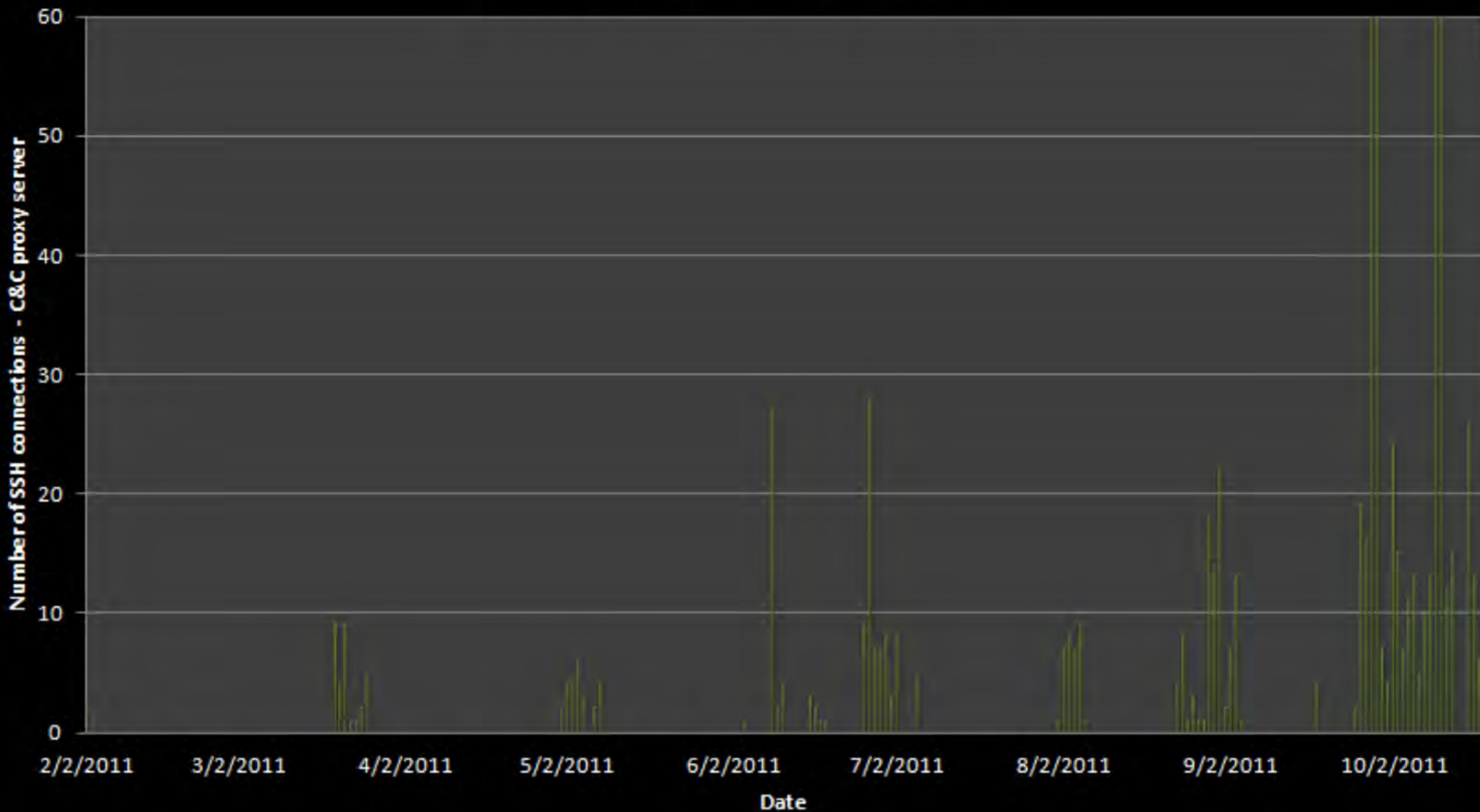
**But wait!**

**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

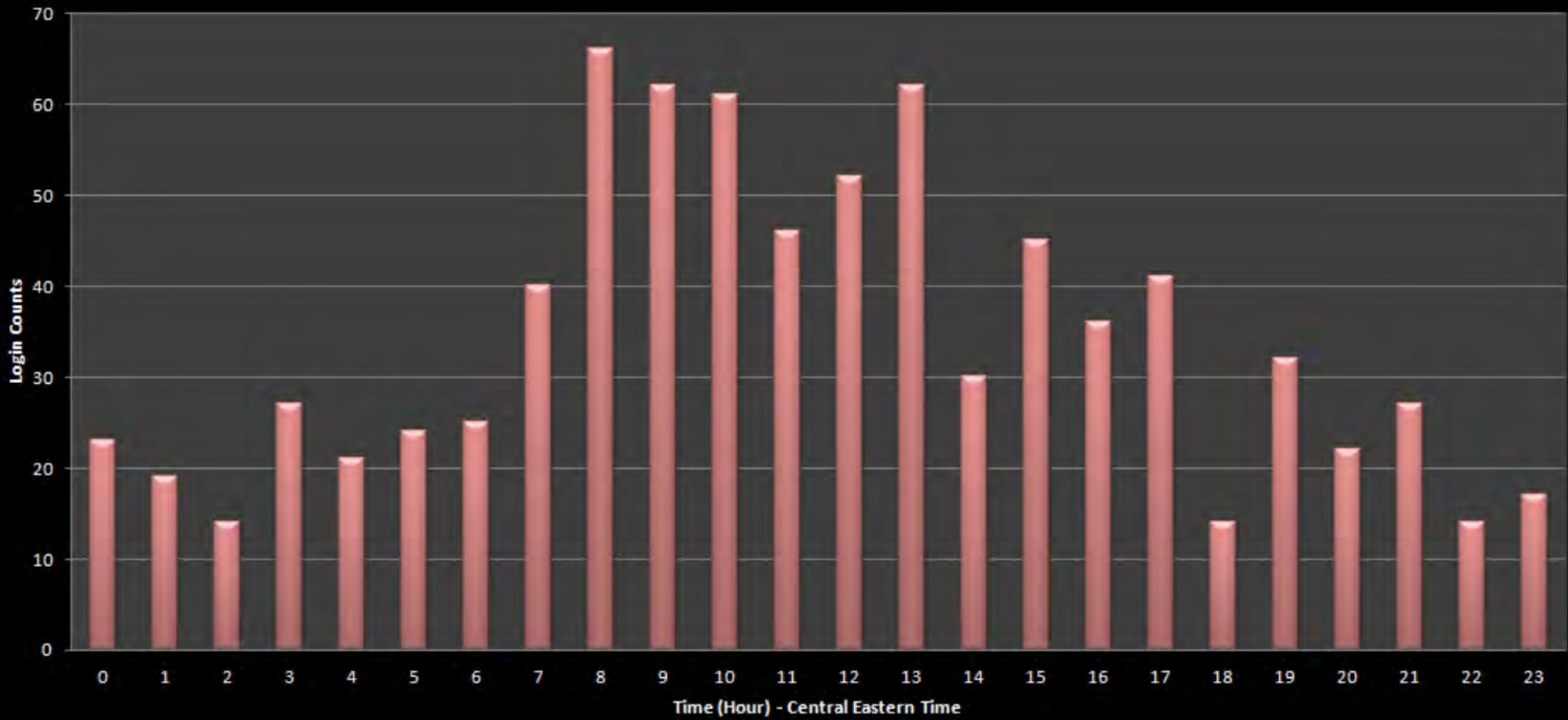


# Connections from 114.202.x.x



0  
2/2/2011 3/2/2011 4/2/2011 5/2/2011 6/2/2011 7/2/2011 8/2/2011 9/2/2011 10/2/2011  
Date

### Login times - Duqu C&C proxy server



# 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?



# 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_GREEN=36

TEXT_WHITE=37

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 ""
```

```
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 !"
if [ -d /proc/xen ]; then
echo "Xen !"
else
echo "Unknown"
read x
echo ""
echo ""
announceLine "Versions:"
echo "- GCC: "
gcc -v
echo "*****"
urgentLine "- SSH: "
ssh -V
echo "*****"
```



```
urgentLine "- iptables: "
```

```
iptables -V
```

```
echo "*****"
```

```
echo "- wget: "
```

```
wget -V
```

```
read x
```

```
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 "NAT Support: "
```

```
iptables -t nat -L -n
```

```
read x
```

```
echo ""
```

```
announceLine "coming:"
```

```
ifconfig -a
```

```
read x
```

```
echo ""
```

```
echo ""
```

```
echo "Route: "
```

```
route -n
```

```
echo ""
```

```
echo ""
```

```
announceLine "netstat: "
```

```
netstat -tunlp
```

```
read x
```

```
echo ""
```

```
echo ""
```

```
announceLine "-----Trace---Route-----"
```

```
echo ""
```

```
echo ""
```

```
tracert http://www.google.com
```

```
read x
```

```
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*****
***"
```



```
read x
```

```
echo ""
```

```
echo ""
```

```
announceLine "-----Trace---Route-----"  
_"
```

```
echo ""
```

```
echo ""
```

```
traceroute http://www.google.com
```

```
read x
```

```
echo ""
```

```
echo ""
```

```
echo ""
```

```
echo "DNS Configuration: "
```

# 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 -anp | grep 1234
iptables --help
iptables -F
iptables
iptables -L
iptables
iptables -h
iptables -L
iptables -L
iptables -u
iptables -L -u
iptables -L -uu
openssh -u
sshd -u
sshd -help
sshd --help
sshd -h
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
pico /var/log/mes
nano /var/log/messages
sshd
locate sshd
```

```
netstat -an
netstat -an
netstat -ano
netstat -anp
ps -Af | grep
telnet localhost
nc -l -p 1234
nc -l 1234
nc -l 0.0.0.0
initcon
yum install
yum install
yum search r
yum search r
yum search r
ls /etc/init
ls /etc/rc3.d
ps -afl grep
ls /etc/rc5.d
netstat -an
netstat -anp
ps -af | grep
ps -Af | grep
netstat -anp
service port
service rpc
netstat -anp
```

```
grep 1234
p
u
enssh5
nssh
nssh-server
sshd_config
co
no
sshd_config
g
estart
mes
messages
```

```
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 rcconf
yum search rcconf
yum search rc-conf
yum search rc conf
ls /etc/init.d/
ls /etc/rc3.d/
ps -afl | grep nfs
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
```

```
ssh
```

```
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**



## Another example

wget kernel.org ←

rm index.html

ftp ftp://ftp.kernel.org/pub/ ←

man ftp ←

ftp -v ftp.kernel.org/pub ←

ftp -v ftp.kernel.org

iptables -L

ftp -v ftp://ftp.kernel.org ←

ftp ftp://ftp.kernel.org ←



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
```

```
*****  
*****DONE*****
```





# Code section, Duqu payload DLL

.10001000	C++ Standard Template Library functions
.10004250	Native C++ code with STL
.1000C2C9	Payload Other Language / C framework No C++
.10023878	Native C++ code with STL
.10028F2C	Run-Time library code
.1002EAD1	Native C code for injection
.100300A4	API thunks, Exception handlers

```

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

```

Original Duqu disassembled code


# 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




igorsk  
2012 Mar 08, 15:07

1

*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".



igorsk  
2012 Mar 09, 10:20

0

*Simple Object Orientation (for C)*

It seems someone over at reddit (<http://www.reddit.com/r/ReverseEngineering/>) hit the jackpot: the code snippets look *very* similar to what this would produce:

<http://daifukkat.su/wiki/index.php/SOO>

There are a few other OO frameworks for C, but they don't match as well:  
<http://ooc-coding.sourceforge.net/>  
<http://sooc.sourceforge.net/>



igorsk

2012 Mar 09, 19:07

1

*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".

0

, 16:20

*ientation (for C)*

me over at reddit (<http://www.reddit.com/r/ReverseEngineering/>) hit the jackpot:

```

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

```

Original Duqu disassembled code



```

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

```

Original Duqu disassembled code

```

class2_ctor  proc near          ; CODE XREF: ...
arg_0        = dword ptr 4

    push    esi
    push    450h                ; dwBytes
    call    sub_401038
    mov     esi, eax
    pop     ecx
    test    esi, esi
    jz     short loc_401106
    lea    eax, [esi+28h]
    push   eax                  ; lpCriticalSection
    call   ds:InitializeCriticalSection
    mov    eax, [esp+4+arg_0]
    mov    dword ptr [esi], offset nullsub_1
    mov    dword ptr [esi+4], offset sub_401082
    mov    dword ptr [esi+8], offset sub_40108A
    mov    dword ptr [esi+0Ch], offset sub_40108A
    mov    dword ptr [esi+10h], offset sub_40108A
    mov    dword ptr [esi+14h], offset sub_40108A
    mov    dword ptr [esi+18h], offset sub_40108A
    mov    dword ptr [esi+1Ch], offset sub_40108A
    mov    dword ptr [esi+20h], offset sub_40108A
    mov    dword ptr [esi+24h], offset sub_40110E
    mov    [esi+40h], eax
    call   sub_40108A
    test   eax, eax
    jnz   short loc_40110A
    push  esi                    ; lpMem
    call  sub_40110E
    pop  ecx

loc_401106:                    ; CODE XREF: ...
    xor   eax, eax
    pop  esi
    retn

-----
loc_40110A:                    ; CODE XREF: ...
    mov  eax, esi
    pop  esi
    retn
class2_ctor  endp

```

Duqu reconstructed compiled code

```

tCLASS2* class2_ctor(void *p_compare_func)
{
    tCLASS2* result;
    if ( ( result = dqmalloc(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->dctor = &class2_dctor;
        result->p_compare_func = p_compare_func;
        if ( ! class2_allocate_block_pair( result ) ) {
            class2_dctor( result );
            return NULL;
        }
        else {
            return result;
        }
    }
    return NULL;
}

```

Duqu reconstructed C source





# Unsolved mysteries

**Duqu unsolved mysteries**

- There are many unsolved mysteries in the Duqu story

**Two unsolved Duqu mysteries**

- On one of the servers, we recovered a fragment of a SSH "known\_hosts" file

"known\_hosts"

```
ftp.ubuntu.com,192.168.1.100,192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.104,192.168.1.105,192.168.1.106,192.168.1.107,192.168.1.108,192.168.1.109,192.168.1.110,192.168.1.111,192.168.1.112,192.168.1.113,192.168.1.114,192.168.1.115,192.168.1.116,192.168.1.117,192.168.1.118,192.168.1.119,192.168.1.120,192.168.1.121,192.168.1.122,192.168.1.123,192.168.1.124,192.168.1.125,192.168.1.126,192.168.1.127,192.168.1.128,192.168.1.129,192.168.1.130,192.168.1.131,192.168.1.132,192.168.1.133,192.168.1.134,192.168.1.135,192.168.1.136,192.168.1.137,192.168.1.138,192.168.1.139,192.168.1.140,192.168.1.141,192.168.1.142,192.168.1.143,192.168.1.144,192.168.1.145,192.168.1.146,192.168.1.147,192.168.1.148,192.168.1.149,192.168.1.150,192.168.1.151,192.168.1.152,192.168.1.153,192.168.1.154,192.168.1.155,192.168.1.156,192.168.1.157,192.168.1.158,192.168.1.159,192.168.1.160,192.168.1.161,192.168.1.162,192.168.1.163,192.168.1.164,192.168.1.165,192.168.1.166,192.168.1.167,192.168.1.168,192.168.1.169,192.168.1.170,192.168.1.171,192.168.1.172,192.168.1.173,192.168.1.174,192.168.1.175,192.168.1.176,192.168.1.177,192.168.1.178,192.168.1.179,192.168.1.180,192.168.1.181,192.168.1.182,192.168.1.183,192.168.1.184,192.168.1.185,192.168.1.186,192.168.1.187,192.168.1.188,192.168.1.189,192.168.1.190,192.168.1.191,192.168.1.192,192.168.1.193,192.168.1.194,192.168.1.195,192.168.1.196,192.168.1.197,192.168.1.198,192.168.1.199,192.168.1.200,192.168.1.201,192.168.1.202,192.168.1.203,192.168.1.204,192.168.1.205,192.168.1.206,192.168.1.207,192.168.1.208,192.168.1.209,192.168.1.210,192.168.1.211,192.168.1.212,192.168.1.213,192.168.1.214,192.168.1.215,192.168.1.216,192.168.1.217,192.168.1.218,192.168.1.219,192.168.1.220,192.168.1.221,192.168.1.222,192.168.1.223,192.168.1.224,192.168.1.225,192.168.1.226,192.168.1.227,192.168.1.228,192.168.1.229,192.168.1.230,192.168.1.231,192.168.1.232,192.168.1.233,192.168.1.234,192.168.1.235,192.168.1.236,192.168.1.237,192.168.1.238,192.168.1.239,192.168.1.240,192.168.1.241,192.168.1.242,192.168.1.243,192.168.1.244,192.168.1.245,192.168.1.246,192.168.1.247,192.168.1.248,192.168.1.249,192.168.1.250,192.168.1.251,192.168.1.252,192.168.1.253,192.168.1.254,192.168.1.255
```

Indicates login attempts into these 2 servers.

How many C&C proxies in total?

[ftp.unusualstatuecollection.net](http://ftp.unusualstatuecollection.net)

[ftp.ubuntu.com](http://ftp.ubuntu.com) (91.189.92.172)



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

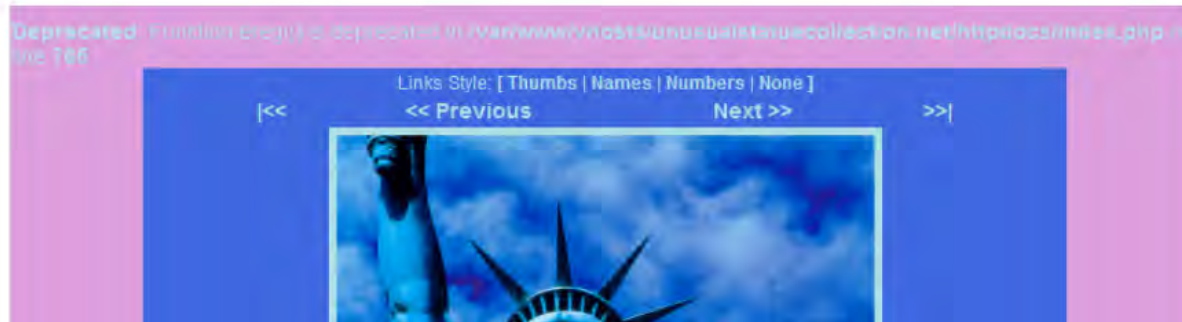
## "known\_hosts"

```
ftp.unusualstatuecollection.net,80.74.132.39 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAQEAyJTNdL9UiluvEJH+wWOLKFTJUsruw7hjR1qggS0eJ41ffyy22HILAAu0z6cJ6a0ItSmNmGQs+signfoG  
CixvoBI81Cy+fYNTsQ5QIUzu0KAPU/Nwjwa45tPm+8eLy6XwI7mPjY0tGbUK18T36/ZhWPXtAoYRhDbw  
p8Mq5nxy4Lj8CUHDbgGt+jNk9ixMKENBGZ/mF4tMn0SUxwKuwmqbPxTj7ggM0iM0FdkMEgotonXXKUww  
1DNqLYNPZ4eLs0W0f0GPnKRnImHup20B0d2Khvuo8znT4uijDenNoM/y0ghe1uUH1E1UdoaBnpLniUtF  
cUxrTqD8j1AWZ/qc8AuT9TQ==  
ftp.ubuntu.com,91.189.92.172 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAQEA0HizMCGfuF4fr8  
U5kPh2n8mGIN0EUEt8f84UHD1PK0dN0n/gakm2vm3Hm0U16KjkwFUbcUmq6b9hZ+8Yd1a16f6mwWrF0r  
o1C08t5tESqxEXQ98Ac/AkboZmLy8jA0PaQx+1Y0WJQJdijcs4hzz0Fum03Ei7iINg1uux/rWiaImPW1  
wybKLodIU2e/Cub/GGnMUse1wAcN7Li7BSkzCJq1EH+1P7FPsyKwUfKaKuQUaF8o6ybgqUA1Sq+8pU04  
/08HTrLhb1EdK/D35IkBvuL8qDBxXjZ2SrCD2sWkziDmyi/LMu+3JtH51R/DUWKbXum5iUxapBIHBxLF  
Cy1yuzw==
```

**Indicates login attempts into these 2 servers.**



# ftp.unusualstatuecollection.net



**Stuxnet's C&C servers:**

**[www.mypremierfutbol.com](http://www.mypremierfutbol.com)**

**[www.todaysfutbol.com](http://www.todaysfutbol.com)**

Links Style: [ Thumbs | Names | Numbers | None ]

|<<

<< Previous

Next >>

>>|

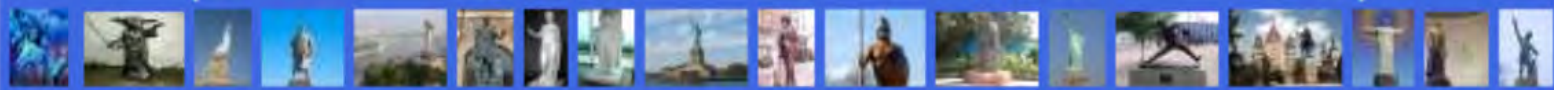


|<<

<< Previous

Next >>

>>|





**ftp.ubuntu.com (91.189.92.172)**





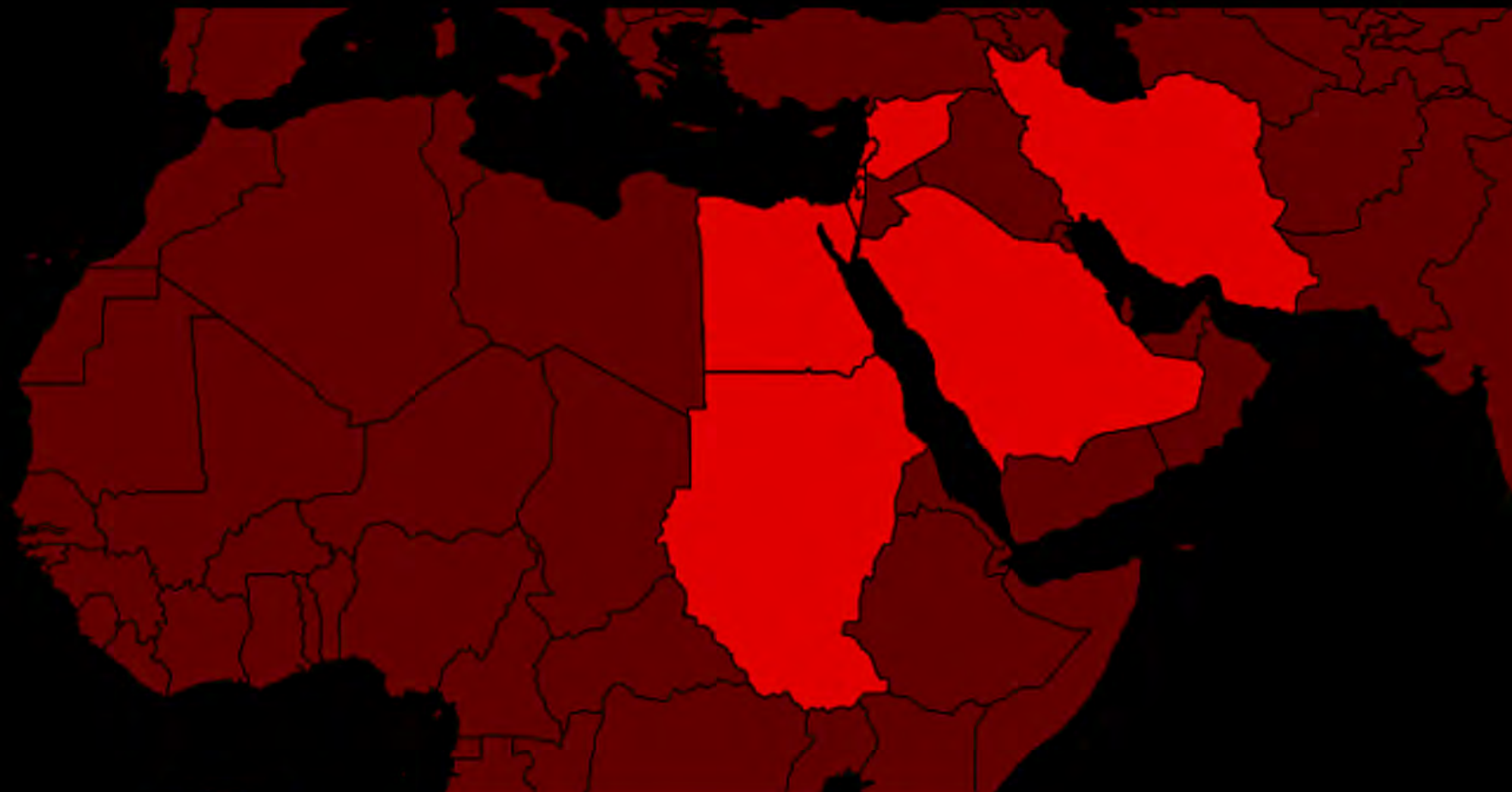
## Flame Features:

- 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



Iran  
189

Israel  
Palestine  
98

Sudan  
32

Syria  
30

Lebanon  
18

Saudi  
Arabia  
10

Egypt  
5

"Flame is so hardcore  
that the whole Stuxnet is kept  
in it's SQLite database."



- MD5 collision attack
- Forged digital certificates
- MITM against Windows Update

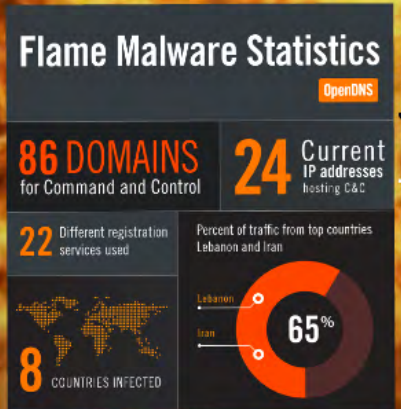
Complex cryptographic attack

Used to be a part of Stuxnet

- Same mutex name prefix: TH\_POOL\_SHD...
- String decryption algorithm
- Mangled class names: ?AVvxys\_uwip, etc.
- Similar shellcode style
- Own import procedure

# FLAME

Uses huge C&C infrastructure



\*Courtesy of OpenDNS



- MD5 collision attack
- Forged digital certificates
- MiTM against Windows Update

# Complex cryptographic attack

- 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

OpenDNS

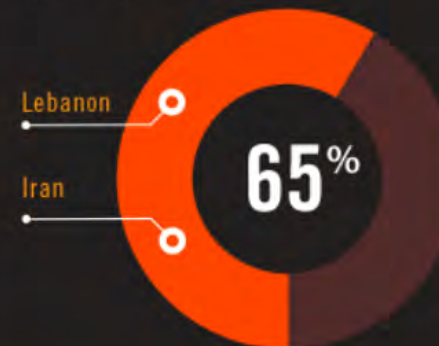
**86** DOMAINS  
for Command and Control

**24** Current  
IP addresses  
hosting C&C

**22** Different registration  
services used

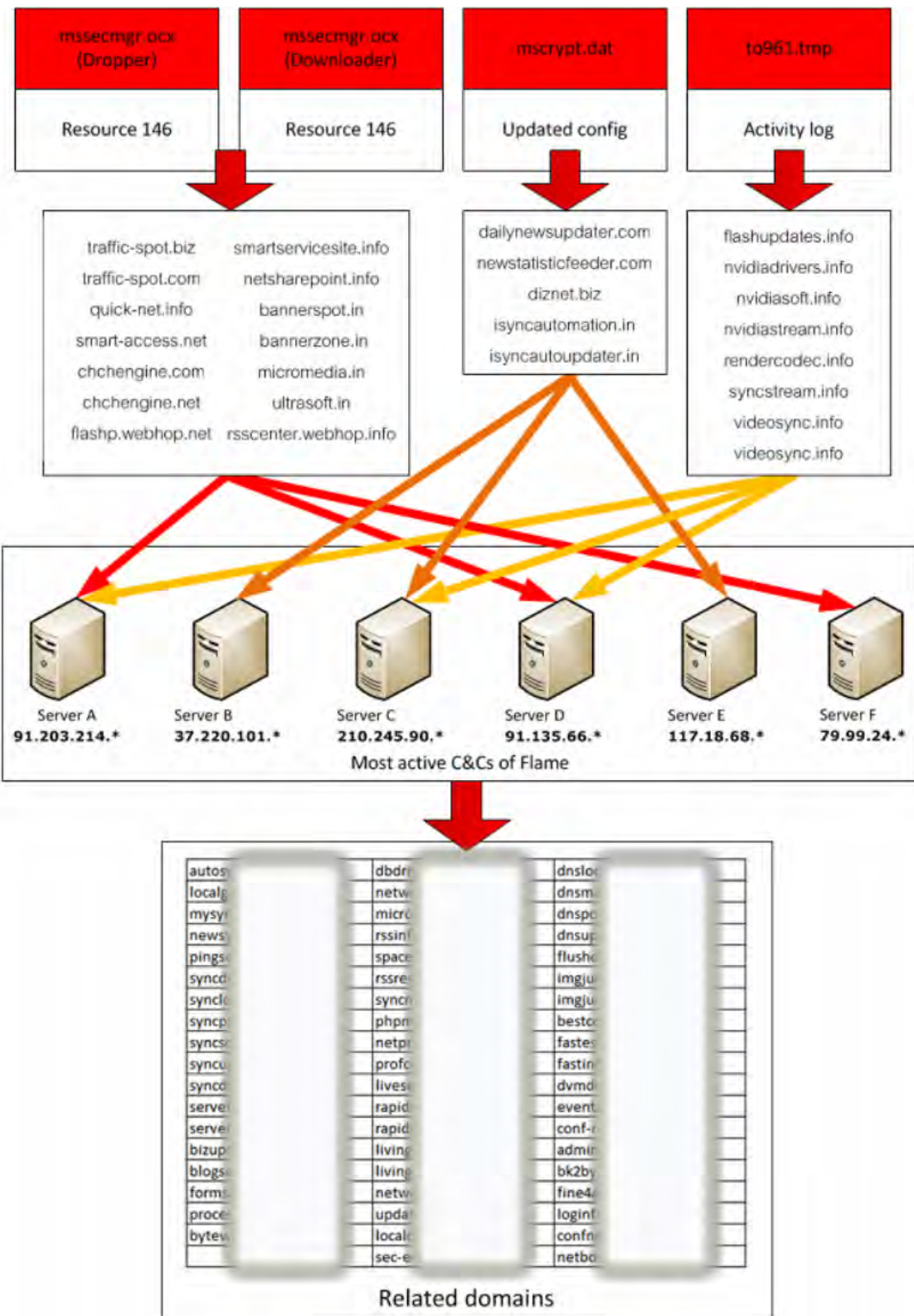
Percent of traffic from top countries  
Lebanon and Iran

**8** COUNTRIES INFECTED



\*Courtesy of OpenDNS





~ DQ

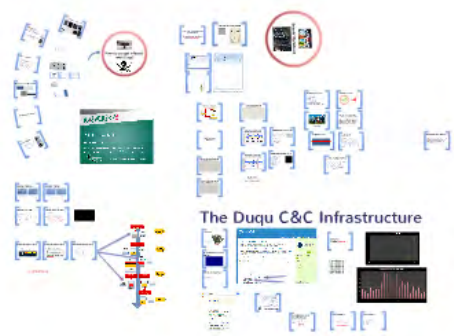
	Duqu	Flame
Server OS	CentOS Linux	Ubuntu Linux
Control scripts	Running on remote server, shielded through SSH port forwarding	Running on servers
Number of victims per server	2-3	50+
Encryption of connections to server	SSL + proprietary AES-based encryption	SSL
Compression of connections	No	Yes, Zlib and modified PPMD
Number of known C&C's domains	n/a	<b>80+</b>
Number of known C&C IPs	5	15+
Number of proxies used to hide identity	10+	Unknown
Time zone of C&C operator	GMT+2 / GMT+3	Unknown
Infrastructure programming	.NET	Unknown
Locations of servers	India, Vietnam, Belgium, UK, Netherlands, Switzerland, Korea, etc...	Germany, Netherlands, UK, Switzerland, Hong Kong, Turkey, etc...
Number of built-in C&C IPs/domain in malware	1	5, can update list
SSL certificate	self-signed	self-signed
Servers status	Most likely hacked	Most likely bought
SSH connections	no	yes



**This is not the end.**

**Contact us:**

**[theflame@kaspersky.com](mailto:theflame@kaspersky.com)**



### The Duqu C&C Infrastructure



### Some goodies

### Unsolved mysteries



### Data hierarchy mystery



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100





Thank you for your attention!

Costin G. Raiu, [craiu@kaspersky.ro](mailto:craiu@kaspersky.ro)

Vitaly Kamluk, [vitaly.kamluk@kaspersky.com](mailto:vitaly.kamluk@kaspersky.com)