TO BE ON THE SAFE SIDE

Kusza szálak: Miért nehéz a célzott támadások kivizsgálása?

Boldizsár Bencsáth PhD
Budapest University of Technology and Economics
Department of Networked Systems and Services
Laboratory of Cryptography and System Security (**CrySyS Lab**)
www.crysys.hu

CrySyS Lab - activities

- CrySyS Lab is a small research lab at BME Budapest, Hungary
- A handful of permanent members, PhD students and many undergrad students (incl. !SpamAndHex! Hacker team at CTF competitions)
- 09/2011 discovery, naming, and first analysis of **Duqu** malware
- 05/2012 published detailed technical analysis on **Flame** (sKyWIper) malware
- 02/2013 Together with Kaspersky Labs, we published information on the **MiniDuke** malware
- 03/2013 After the joint work with NSA HUN, we published results of investigations on the **TeamSpy** campaign
- Worked on **Gauss**, **Miniduke2 (CosmicDuke, M2O**), **Turla/Snake/Uroburos -Worldcupsec/WipBot/Epic/TadjMakhal** and some other attacks

Complexity

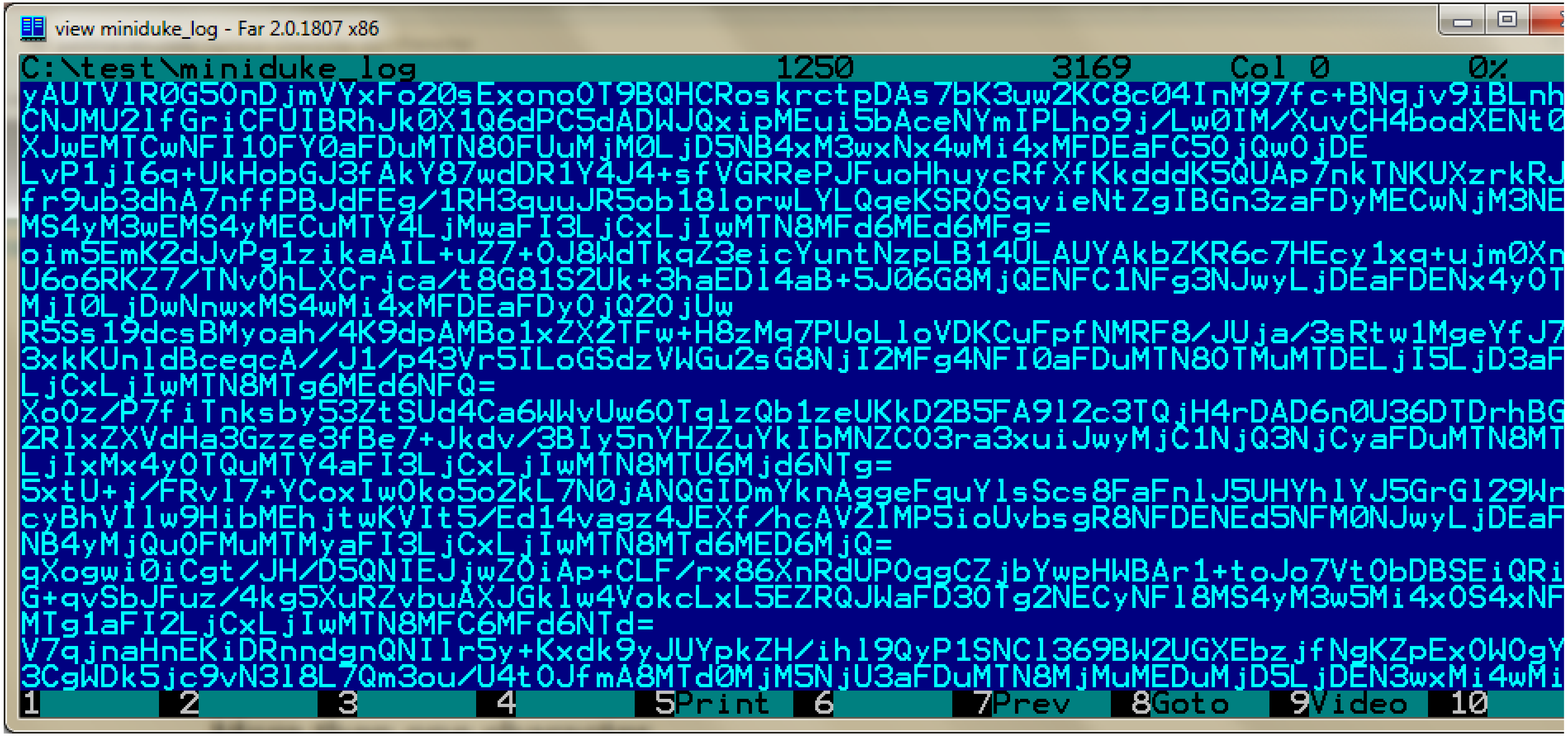
- Attacks are seemingly more and more complex
  - Maybe we are seeing more that the tip of the iceberg
  - Attackers work more and more – possible evidence that can be collected also grows
- More complexity – **more questions**
- **Harder** to store, handle, remember on all parts of the story
- More likely that investigators **miss** to identify interesting items
- Harder to **pinpoint** most **important** things
- More likely that multiple parties work on the same threat, but they only see a **partial picture**
- More **collaboration needed** to get the big picture

Complexity 2.

- When to **publish** and what?
- Almost impossible to get “ALL” information before publishing
- More complex threat – most likely others will also find it
- Avoid publishing at all?
- Needs coordination of publishing
- Most important is to help victims (e.g. notification based on data)
- and be able to detect and prevent attacks somehow (e.g. based on information gathered)

C&C data handling – example - Miniduke

- An example log of encrypted Miniduke logs



```
C:\test\miniduke_log                           1250              3169        Col 0          0%
yAUTV1R0G5OnDjmVYxFo20sExonoOT9BQHCRoskrctpDAs7bK3uw2KC8c04InM97fc+BNqjv9iBLnh
CNJMU2lfGriCFUIBRhJk0X1Q6dPC5dADWJQxipMEui5bAceNYmIPLho9j/Lw0IM/XuvCH4bodXENt0
XJwEMTCwNFI1OFY0aFDuMTN8OFUuMjM0LjD5NB4xM3wxNx4wMi4xMFDEaFC5OjQwOjDE
LvP1jI6q+UkHobGJ3fAkY87wdDR1Y4J4+sfVGRRePJFuoHhuycRfXfKkdddK5QUAp7nkTNKUXzrkRJ
fr9ub3dhA7nffPBJdFEg/1RH3guuJR5ob18lorwLYLQgeKSROSqvieNtZgIBGn3zaFDyMECwNjM3NE
MS4yM3wEMS4yMECuMTY4LjMwaFI3LjCxLjIwMTN8MFd6MEd6MFg=
oim5EmK2dJvPg1zikaAIL+uZ7+OJ8WdTkqZ3eicYuntNzpLB14OLAUYAkbZKR6c7HEcy1xq+ujm0Xn
U6o6RKZ7/TNvOhLXCrjca/t8G81S2Uk+3haEDl4aB+5J06G8MjQENFC1NFg3NJwyLjDEaFDENx4yOT
MjI0LjDwNnwxMS4wMi4xMFDEaFDyOjQ2OjUw
R5Ss19dcsBMyoah/4K9dpAMBo1xZX2TFw+H8zMq7PUoLloVDKCuFpfNMRF8/JUja/3sRtw1MgeYfJ7
3xkKUnldBceqcA//J1/p43Vr5ILoGSdzVWGu2sG8NjI2MFg4NFI0aFDuMTN8OTMuMTDELjI5LjD3aF
LjCxLjIwMTN8MTg6MEd6NFQ=
XoOz/P7fiTnksby53ZtSUd4Ca6WWvUw6OTglzQb1zeUKkD2B5FA9l2c3TQjH4rDAD6n0U36DTDrhBG
2RlxZXVdHa3Gzze3fBe7+Jkdv/3BIy5nYHZZuYkIbMNZCO3ra3xuiJwyMjC1NjQ3NjCyaFDuMTN8MT
LjIxMx4yOTQuMTY4aFI3LjCxLjIwMTN8MTU6Mjd6NTg=
5xtU+j/FRvl7+YCoxIwOko5o2kL7N0jANQGIDmYknAggeFquYlsScs8FaFnlJ5UHYhlYJ5GrGl29Wr
cyBhVIlw9HibMEhjtwKVIt5/Ed14vagz4JEXf/hcAV2IMP5ioUvbsgR8NFDENEd5NFM0NJwyLjDEaF
NB4yMjQuOFMuMTMyaFI3LjCxLjIwMTN8MTd6MED6MjQ=
gXogwi0iCgt/JH/D5QNIEJjwZOiAp+CLF/rx86XnRdUPOggCZjbYwpHWBAr1+toJo7VtObDBSEiQRi
G+qvSbJFuz/4kg5XuRZvbuAXJGklw4VokcLxL5EZRQJWaFD3OTg2NECyNFl8MS4yM3w5Mi4xOS4xNF
MTg1aFI2LjCxLjIwMTN8MFC6MFd6NTd=
V7qjnaHnEKiDRnndgnQNIlr5y+Kxdk9yJUYpkZH/ihl9QyP1SNCl369BW2UGXEbzjfNgKZpExOWOgY
3CgWDk5jc9vN3l8L7Qm3ou/U4tOJfmA8MTd0MjM5NjU3aFDuMTN8MjMuMEDuMjD5LjDEN3wxMi4wMi
1        2        3        4        5Print   6        7Prev    8Goto    9Video   10
```

Miniduke log decodes to sthg similar

```
1132034214|0.45|54.204.42.114|06.02.2014|01:26:22
115365341|0.45|114.65.14.141|06.02.2014|14:34:35
241543565|0.45|25.54.142.11|03.02.2014|15:26:45
4042361101|0.45|54.204.42.114|06.02.2014|11:32:23
2411346166|0.45|54.204.42.114|06.02.2014|06:25:32
2054243265|0.45|112.16.222.2|04.02.2014|10:21:13
1612151360|0.45|14.43.41.115|05.02.2014|12:15:32
2165026661|0.45|14.43.41.115|05.02.2014|12:26:32
```

- In many cases these IPs belong to DSL/broadband home users
- ISPs can help to identify or notify victims

Sent to an ambassador - Uroburos

```
rem dir c:\
del /Q C:\Users\REDACT~1.ED_\AppData\Local\Temp\DMR0867.dat
rem del /Q C:\Users\REDACT~1.ED_\AppData\Local\Temp\jar*.tmp
rem dir "C:\Users\REDACT~1.ED_\AppData\Local\Temp\"
rem dir "C:\Users\REDACT~1.ED_\AppData\Local\Temp\Adobe\acrobat\"
C:\windows\Temp\hpzscr10.exe a -ta20121119010101 C:\Users\REDACT~1.ED_\AppData\Local\Temp\DMR0867.dat
"C:\Users\REDACT~1.ED_\AppData\Local\Temp\*NATO*.msg"
rem C:\windows\Temp\hpzscr10.exe a -ta20121119010101 C:\Users\REDACT~1.ED_\AppData\Local\Temp\DMR0867.dat
"C:\Users\REDACT~1.ED_\AppData\Local\Temp\Polen*.msg"
rem C:\windows\Temp\hpzscr10.exe a -m5 -ta20121119010101
C:\Users\REDACT~1.ED_\AppData\Local\Temp\DMR0867.dat "C:\Users\REDACT~1.ED_\AppData\Local\Temp\Antici*.msg"
rem C:\windows\Temp\hpzscr10.exe a -m5 -ta20121119010101
C:\Users\REDACT~1.ED_\AppData\Local\Temp\DMR0867.dat
"C:\Users\REDACT~1.ED_\AppData\Local\Temp\Estland*.msg"
C:\windows\Temp\hpzscr10.exe a -m5 -ta20121119010101 C:\Users\REDACT~1.ED_\AppData\Local\Temp\DMR0867.dat
"C:\Users\REDACT~1.ED_\AppData\Local\Temp\OSZE*.msg"
rem C:\windows\Temp\hpzscr10.exe a -m5 -ta20121119010101
C:\Users\REDACT~1.ED_\AppData\Local\Temp\DMR0867.dat "C:\Users\REDACT~1.ED_\AppData\Local\Temp\Island*.msg"
rem C:\windows\Temp\hpzscr10.exe a -m5 -ta20121119010101
C:\Users\REDACT~1.ED_\AppData\Local\Temp\DMR0867.dat "C:\Users\REDACT~1.ED_\AppData\Local\Temp\EU*.msg“
…
```

“Budapest*.msg”

```
rem C:\windows\Temp\hpzscr10.exe a -m5 -ta20121119010101
C:\Users\REDACT~1.ED_\AppData\Local\Temp\DMR0867.dat
"C:\Users\REDACT~1.ED_\AppData\Local\Temp\*tZZZ5qy.msg"
rem C:\windows\Temp\hpzscr10.exe a -ta20121119010101
C:\Users\REDACT~1.ED_\AppData\Local\Temp\DMR0867.dat
"C:\Users\REDACT~1.ED_\AppData\Local\Temp\*gZZZZtgr.msg"
rem C:\windows\Temp\hpzscr10.exe a -m5 -ta20121119010101
C:\Users\REDACT~1.ED_\AppData\Local\Temp\DMR0867.dat
"C:\Users\REDACT~1.ED_\AppData\Local\Temp\Norwegen*.msg"
rem C:\windows\Temp\hpzscr10.exe a -m5 -ta20121119010101
C:\Users\REDACT~1.ED_\AppData\Local\Temp\DMR0867.dat
"C:\Users\REDACT~1.ED_\AppData\Local\Temp\Polen*.msg"
rem C:\windows\Temp\hpzscr10.exe a -ta20121119010101
C:\Users\REDACT~1.ED_\AppData\Local\Temp\DMR0867.dat
"C:\Users\REDACT~1.ED_\AppData\Local\Temp\Budapest*.msg"
```

Complexity – lot of old data

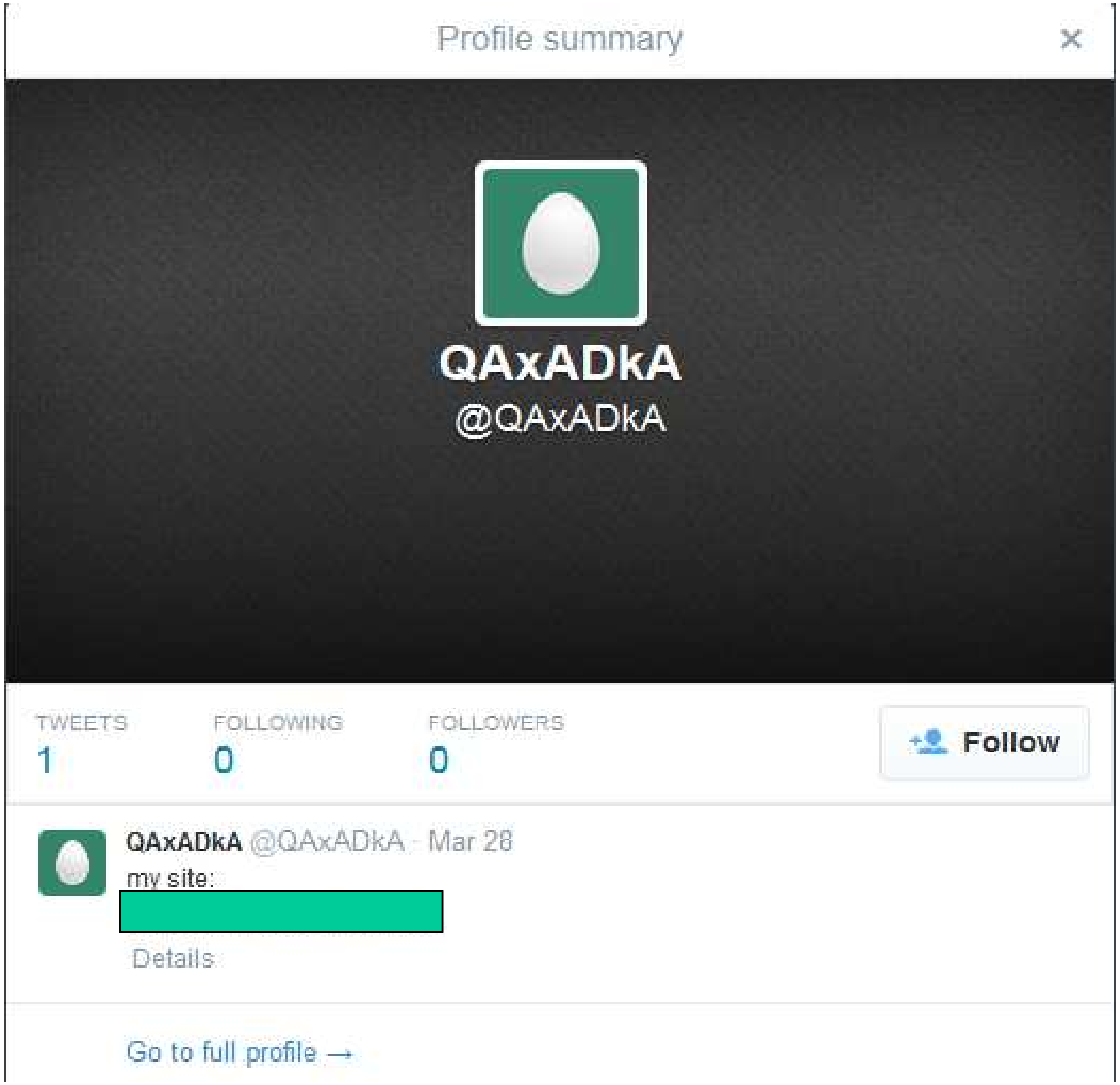
- In some campaigns, gathered information is old
  - TeamSpy: years old dynamic IP addresses
  - Uroburos: same, lot of old information
- (nearly) impossible to find out owner of a dynamic address years ago
- Heat maps can be misguiding if they are based on IP address only, e.g. no victim i.d. available
  - Victims with dynamic, changing IPs might be counted multiple times

C&C communications

- We generally don’t know full victim list
- But we know precious information to detect attacks or to find out victims in the past from logs
- IP address for communications 1.2.3.4
- DNS name (comm logs, passive DNS logs) e.g.
- URL scheme modules/db/mgr.php?F=3?m&Auth=80B8A0BA&Session=11E19A6A733FBE59&DataID=1&FamilyID=1147A8FE6D7142E...
- Data formats, executable files, registry settings, other forensics evidence

Digging ISP logs might help

Miniduke Twitter C&C redirection



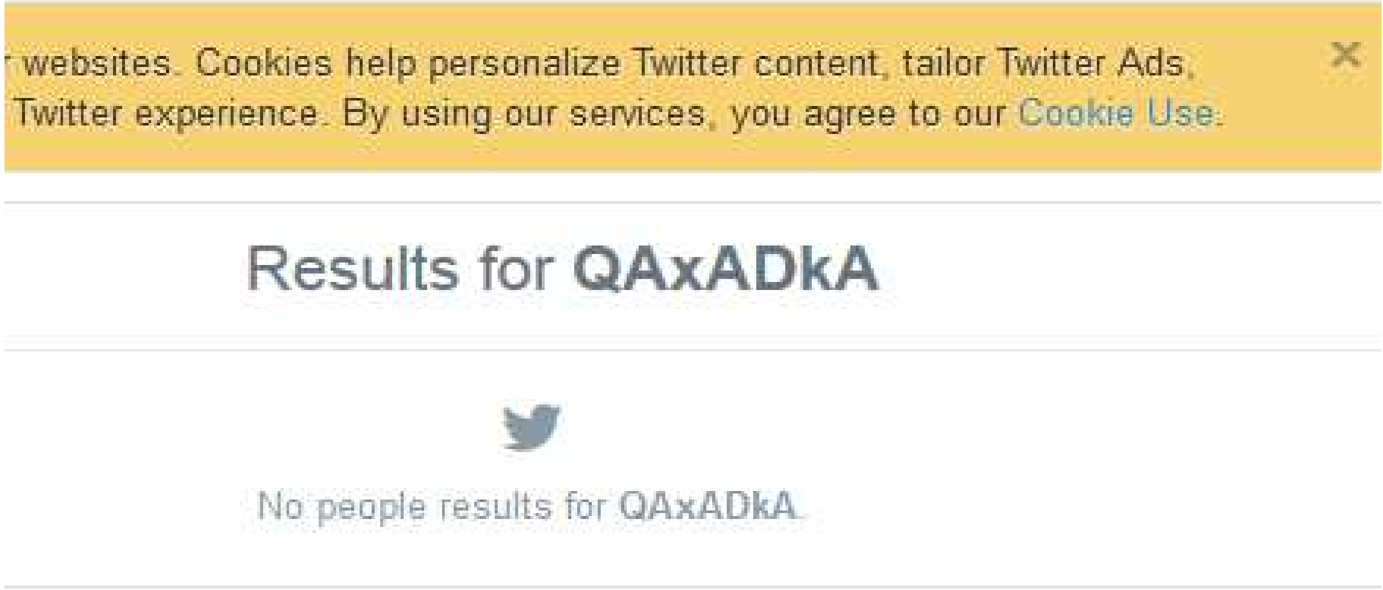
Profile summary ×

QAxADkA
@QAxADkA

TWEETS	FOLLOWING	FOLLOWERS
1	0	0

QAxADkA @QAxADkA · Mar 28
my site:
[redacted]
Details

Account was later removed, tweet missing…



r websites. Cookies help personalize Twitter content, tailor Twitter Ads, Twitter experience. By using our services, you agree to our Cookie Use.

Results for QAxADkA

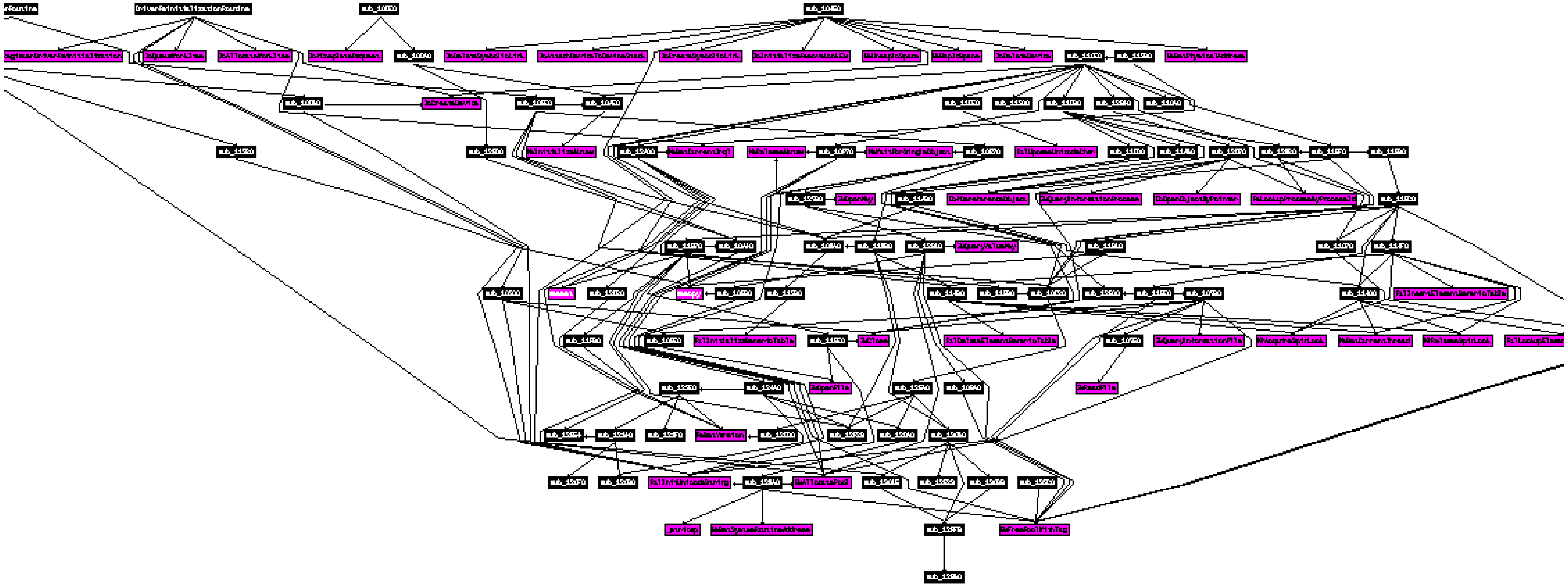
No people results for QAxADkA.

Cooperation

- Cooperation with IPSs might help to find other victims
- To identify and notify victims
- To seize C&C servers or get information on the attack
- Example on twitter: other C&Cs might be identified by cooperation with providers

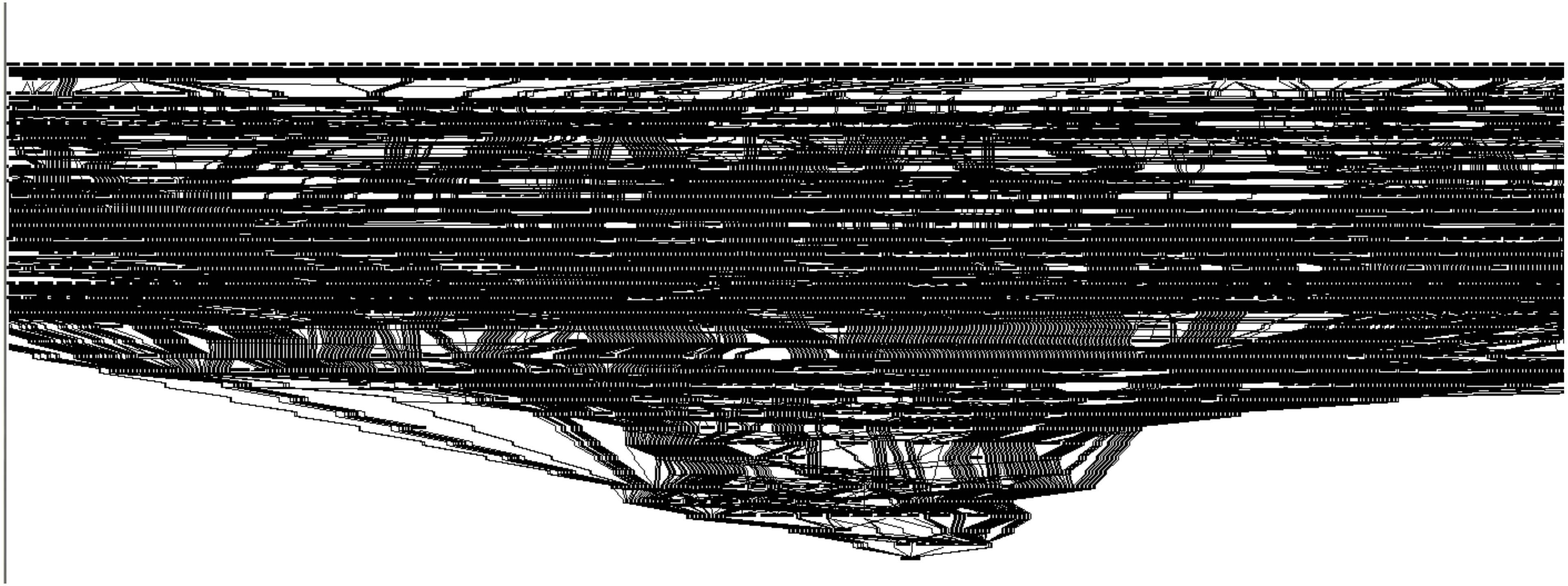
Duqu – jminet7 driver structure

- Code complexity on a picture

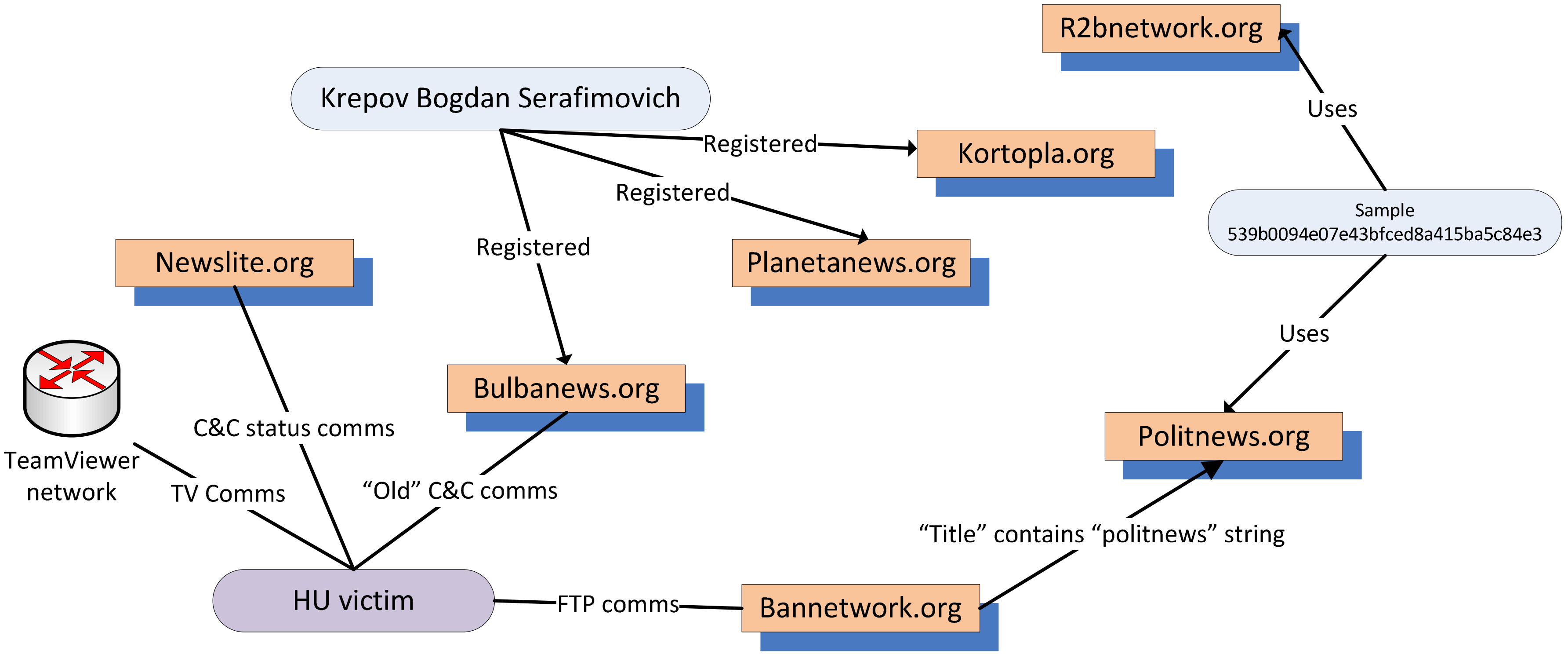


Browse32 module of Flame

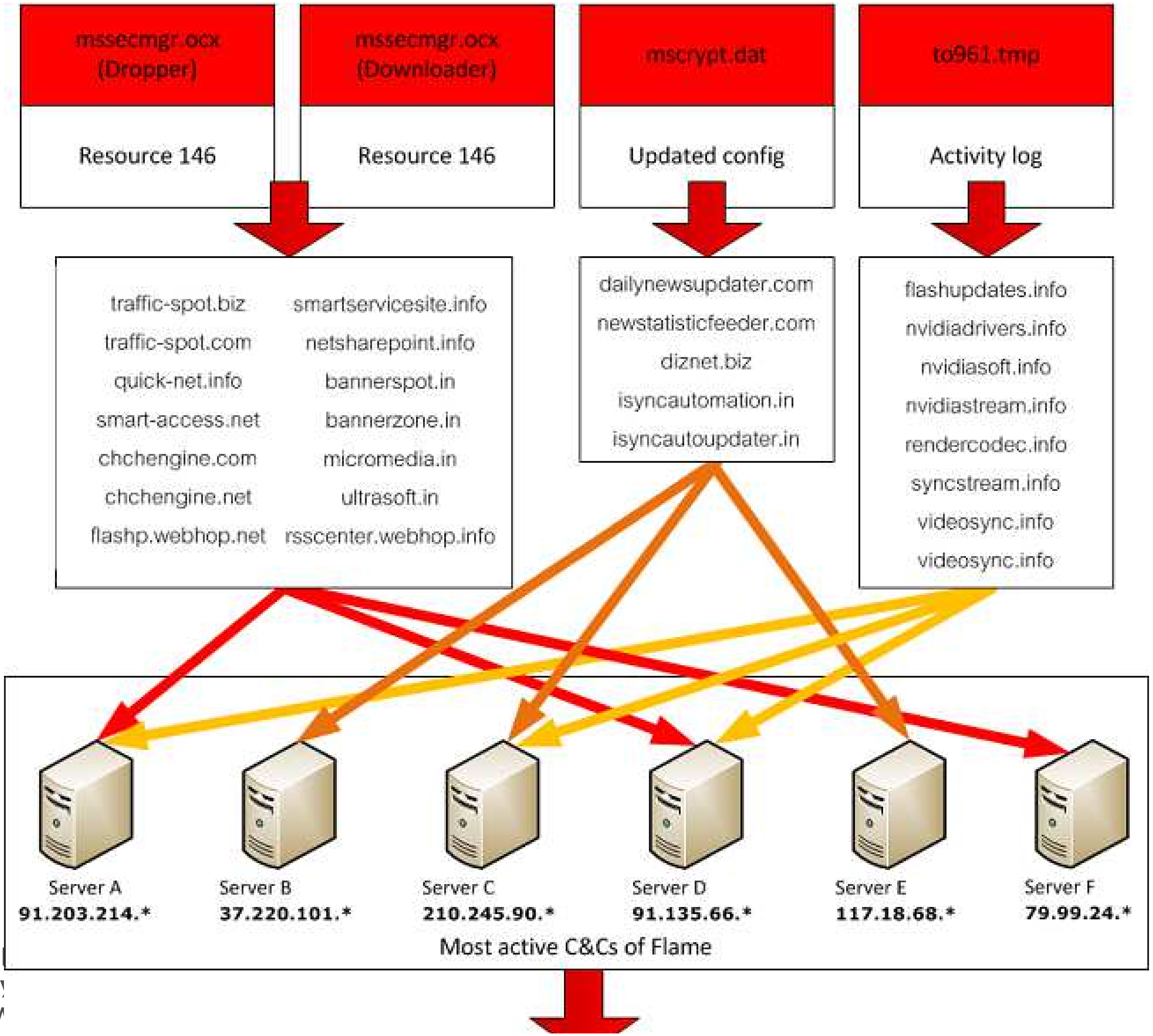
- Flame Suicide module, Browse32 is 450k large



Mapping an ATP by domains – sample info from TeamSpy



Depicting C&C comms of flame – from Kaspersky Lab

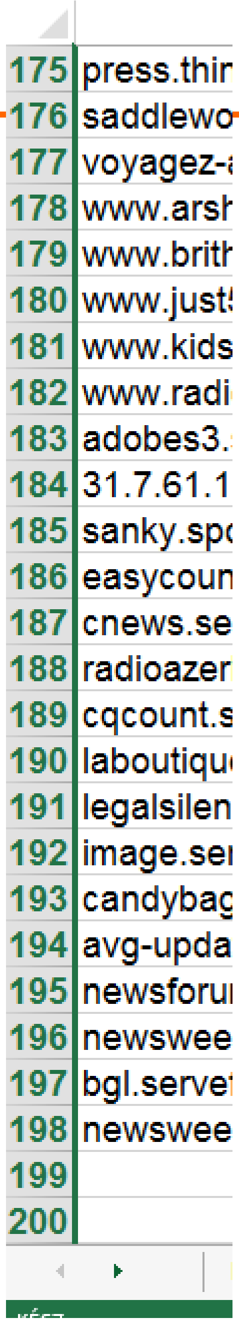


What’s your name?

- APT names/identifiers became problematic. Let’s see the latest example:
  - Turla Uroburos Snake (Agent.BTZ)
  - WorldCupSec Epic Wipbot Tadjmakhal
  - Tavdig
  - Pfinet
  - Turla Dragon / Faking Dragon
  - Sofacy?
- All related to a complex series of attacks
- How to identify/name then my lonely sample?
- How these components relate to each other?
- How many attackers, developers are behind?
- How to pick name for the next attack?

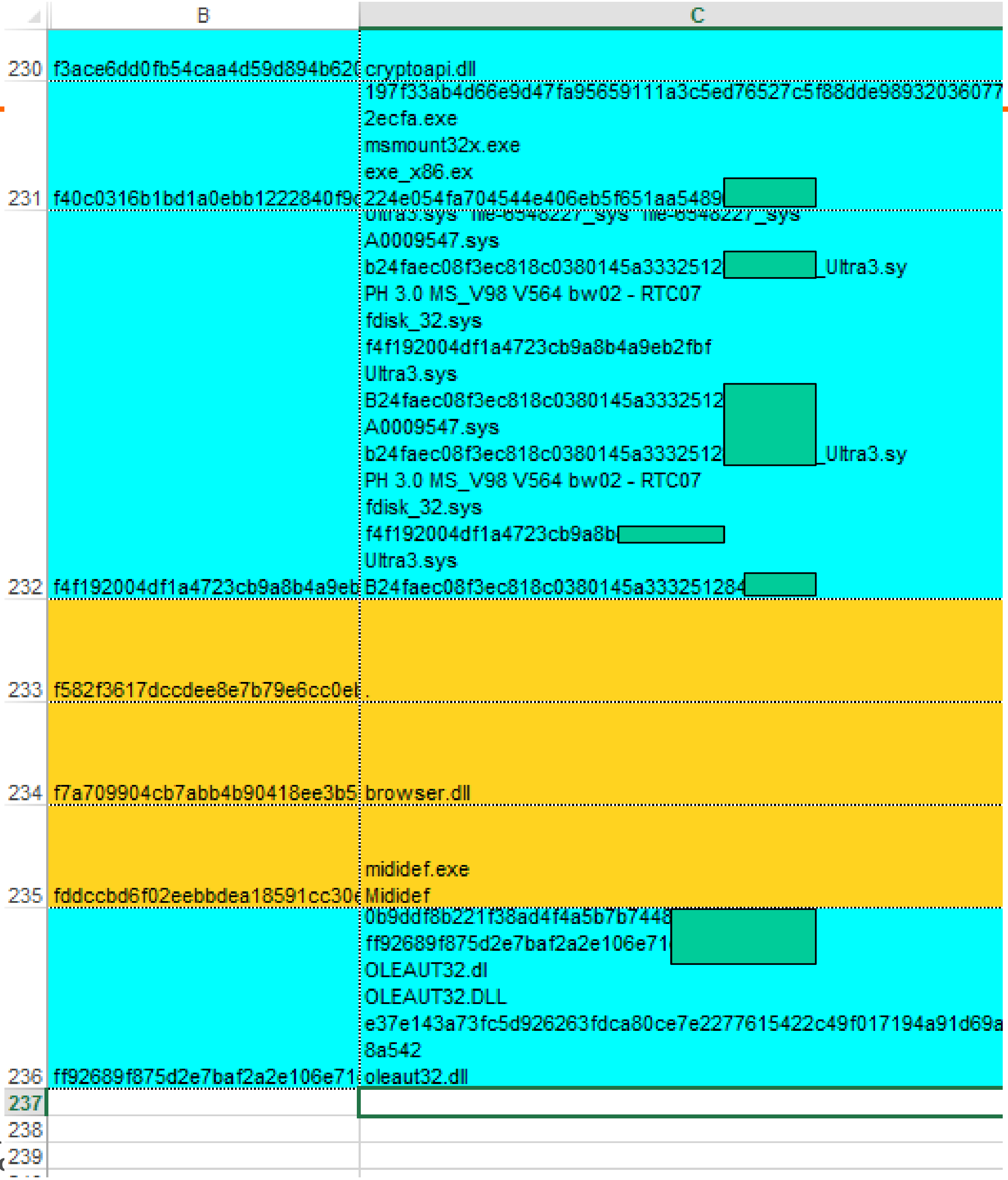
Very complex campaigns

- At least 198 domains, IP addresses relate to Uroburos/Turla/Snake
- Not counting Epic, etc.
- Also hundreds of hosts: Red October, Flame, Mask, Energetic Bear (Crouching Yeti), etc.



175	press.thir
176	saddlewo
177	voyagez-a
178	www.arsh
179	www.brith
180	www.just5
181	www.kids
182	www.radi
183	adobes3.
184	31.7.61.1
185	sanky.spo
186	easycoun
187	cnews.se
188	radioazer
189	cqcount.s
190	laboutiqu
191	legalsilen
192	image.ser
193	candybag
194	avg-upda
195	newsforu
196	newswee
197	bgl.serve
198	newswee
199	
200	

- At least 236 samples under different names just for Uruburos



	B	C
230	f3ace6dd0fb54caa4d59d894b62(	cryptoapi.dll
231	f40c0316b1bd1a0ebb1222840f9(	197f33ab4d66e9d47fa95659111a3c5ed76527c5f88dde98932036077 2ecfa.exe msmount32x.exe exe_x86.ex 224e054fa704544e406eb5f651aa5489[redacted]
232	f4f192004df1a4723cb9a8b4a9eb	Ultra3.sys file-6548227_sys file-6548227_sys A0009547.sys b24faec08f3ec818c0380145a3332512[redacted]_Ultra3.sy PH 3.0 MS_V98 V564 bw02 - RTC07 fdisk_32.sys f4f192004df1a4723cb9a8b4a9eb2fbf Ultra3.sys B24faec08f3ec818c0380145a3332512[redacted] A0009547.sys b24faec08f3ec818c0380145a3332512 _Ultra3.sy PH 3.0 MS_V98 V564 bw02 - RTC07 fdisk_32.sys f4f192004df1a4723cb9a8b[redacted] Ultra3.sys B24faec08f3ec818c0380145a333251284[redacted]
233	f582f3617dccdee8e7b79e6cc0et	.
234	f7a709904cb7abb4b90418ee3b5	browser.dll
235	fddccbd6f02eebbdea18591cc30e	midindef.exe Mididef
236	ff92689f875d2e7baf2a2e106e71	0b9ddf8b221f38ad4f4a5b7b7448[redacted] ff92689f875d2e7baf2a2e106e71 OLEAUT32.dl OLEAUT32.DLL e37e143a73fc5d926263fdca80ce7e2277615422c49f017194a91d69a 8a542 oleaut32.dll
237		
238		
239		

International law and collaboration – case study

- A “Flame” C&C server was a VS in .nl
- The computer was maintained by a .de company
- The VS was resold by a .uk company
- The .uk company was founded and ran by Hungarians
- Attackers might be e.g. from .il (not sure)
- Victims probably from .ir, Sudan, .il etc.
- So who’s law system is applicable for seizing it?

Any questions?

```
0x34E574F7 1C21 8E76 5ABA E98C 1400 F82E 3BBE CCF0 34E5 74F7
0x20667F5A A3A5 63E2 4605 6856 11A9 DCE6 E51B 50D9 2066 7F5A
```

Dr. Bencsáth Boldizsár

adjunktus

BME HIT CrySyS Lab

bencsath@crysys.hit.bme.hu