
The
Elephant
In the Room
CYPHORT


Marion Marschalek
@pinkflawd
Cyphort Inc.
CYPHORT

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

SNOWGLOBE:

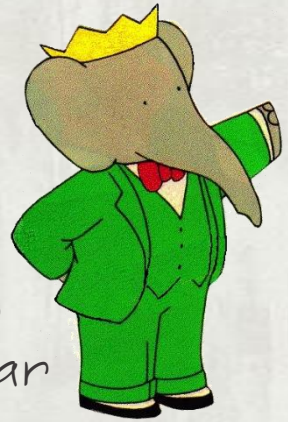
From Discovery to Attribution

[redacted]
CSEC CNT / Cyber CI
SIGDEV 2011 Cyber Thread

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

Canada

CYPHORT



Babar
Superstar

Spear phishing
with a PDF 0-day

Active in Iran

TFC

NGBD

NBOT

DDoS, plugins &
what not

Watering hole on
website of
Syrian ministery
of justice

2009

2011

2014

TIME

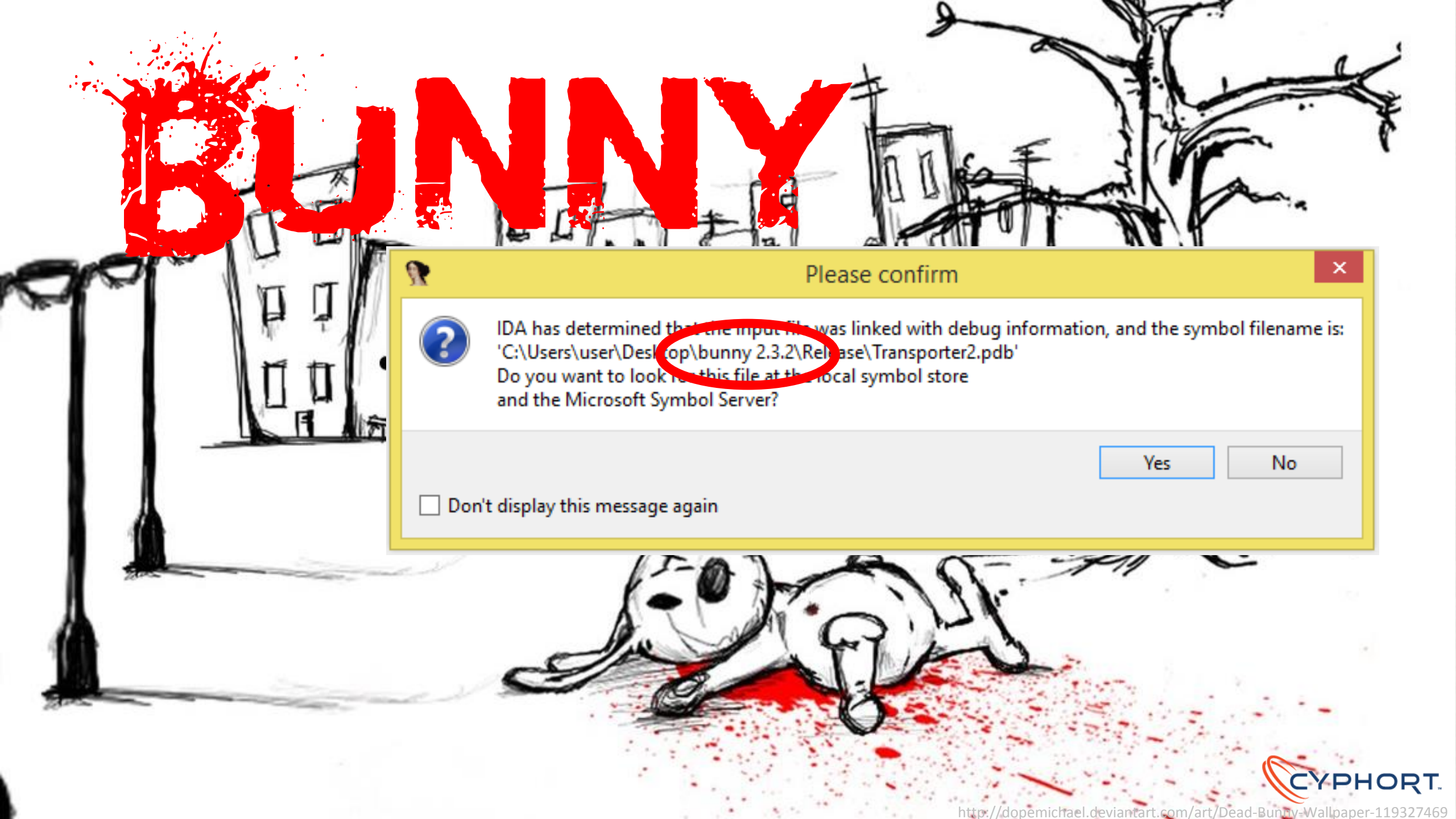
CYPHORT

TFC.. IRC BOT.. IRC GBD.. IRC WOT?

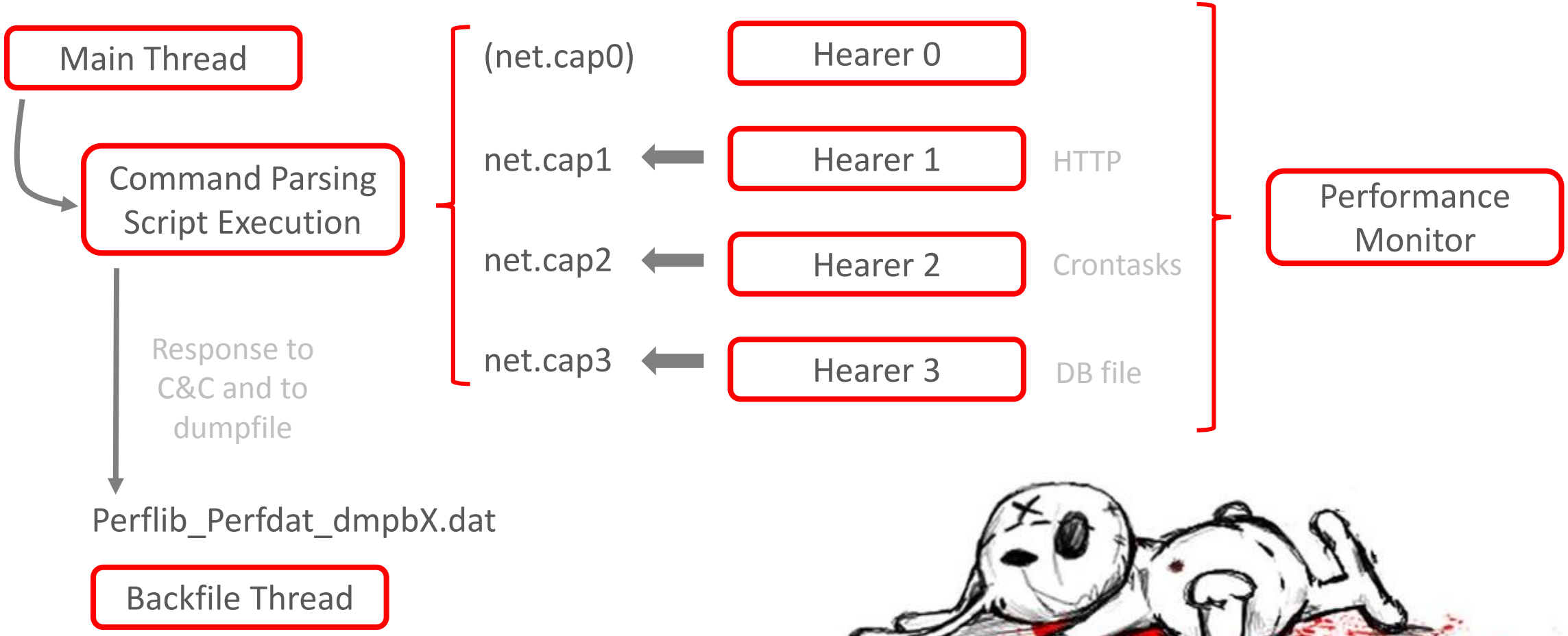
- Lots of code sharing
- Lots of shouty capitals
- DDoS bots
- Plugin platforms & Reconnaissance

```
unicode 0, <HTTPF>,0
                                ; DATA XREF: cto
                                ; ctor_ASPFLOOD+
unicode 0, <ASPFLOOD>,0
db    0
db    0
                                ; DATA XREF: cto
                                ; ctor_TCPFLOOD+
unicode 0, <TCPFLOOD>,0
db    0
db    0
                                ; DATA XREF: cto
                                ; ctor_WEBFLOOD+
unicode 0, <WEBFLOOD>,0
db    0
db    0
                                ; DATA XREF: cto
                                ; ctor_POSTFLOOD
unicode 0, <POSTFLOOD>,0
                                ; DATA XREF: cto
                                ; ctor_STATISTIC
unicode 0, <STATISTICS>,0
db    0
db    0
                                ; DATA XREF: cto
                                ; ctor_KILL+18↑o
unicode 0, <KILL>,0
db    0
```

CYPHORT



SCRIPTABLE BOT through lua script injection



Bunny Evasion

Emulator check
Containing directory name check
Payload's creation time stamp changed
Number of running processes 15+
Time API hook detection
Obfuscation of subset of APIs
Infection „strategy"
Payload only started on reboot

CYPHORT

Bunny Evasion

Searching for.. Sandboxes?

```
if ( strstr(modulefilename, "klavme") )
{
  result = 1;
}
else if ( strstr(modulefilename, "myapp") )
{
  result = 1;
}
else if ( strstr(modulefilename, "TESTAPP") )
{
  result = 1;
}
else if ( strstr(modulefilename, "afyjevmv.exe") )
{
  result = 1;
```

Bitdefender

Kaspersky

Also Kaspersky:

lstcvix.exe
tudib.exe
izmdmv.exe
ubgncn.exe
jidgdsp.exe
evabgzib.exe
qzqjafyt.exe
cnyporqb.exe
...

CYPHORT

CYPHORT

M International

Quand les Canadiens partent en chasse de « Babar »

Le Monde | 21.03.2014 à 12h26 • Mis à jour le 19.05.2014 à 14h13 |

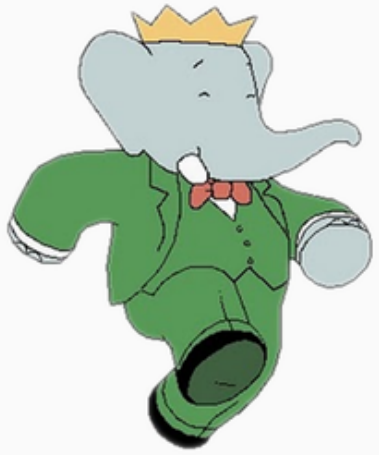
Par Jacques Follorou et Martin Untersinger

ntrass.exe

- DLL Loader uploaded to a victim as part of tasking seen in collection
- Internal Name: Babar
- Developer username: titi

Babar is a popular French children's television show

Titi is a French diminutive for Thiery, or a colloquial term for a small person



C'est une véritable traque qu'ont menée les services secrets techniques canadiens du Centre de la sécurité des télécommunications du Canada (CSEC). Elle est relatée dans le document fourni au *Monde* par Edward Snowden, dans lequel ils présentent leurs trouvailles. Avare en détails, ce document permet néanmoins de retracer l'enquête qui a permis de pointer la France du doigt.

Comme dans une partie de chasse, ce sont des empreintes qui attirent en premier lieu l'attention des services canadiens. La note interne indique en effet que le CSEC collecte quotidiennement et automatiquement un certain nombre de

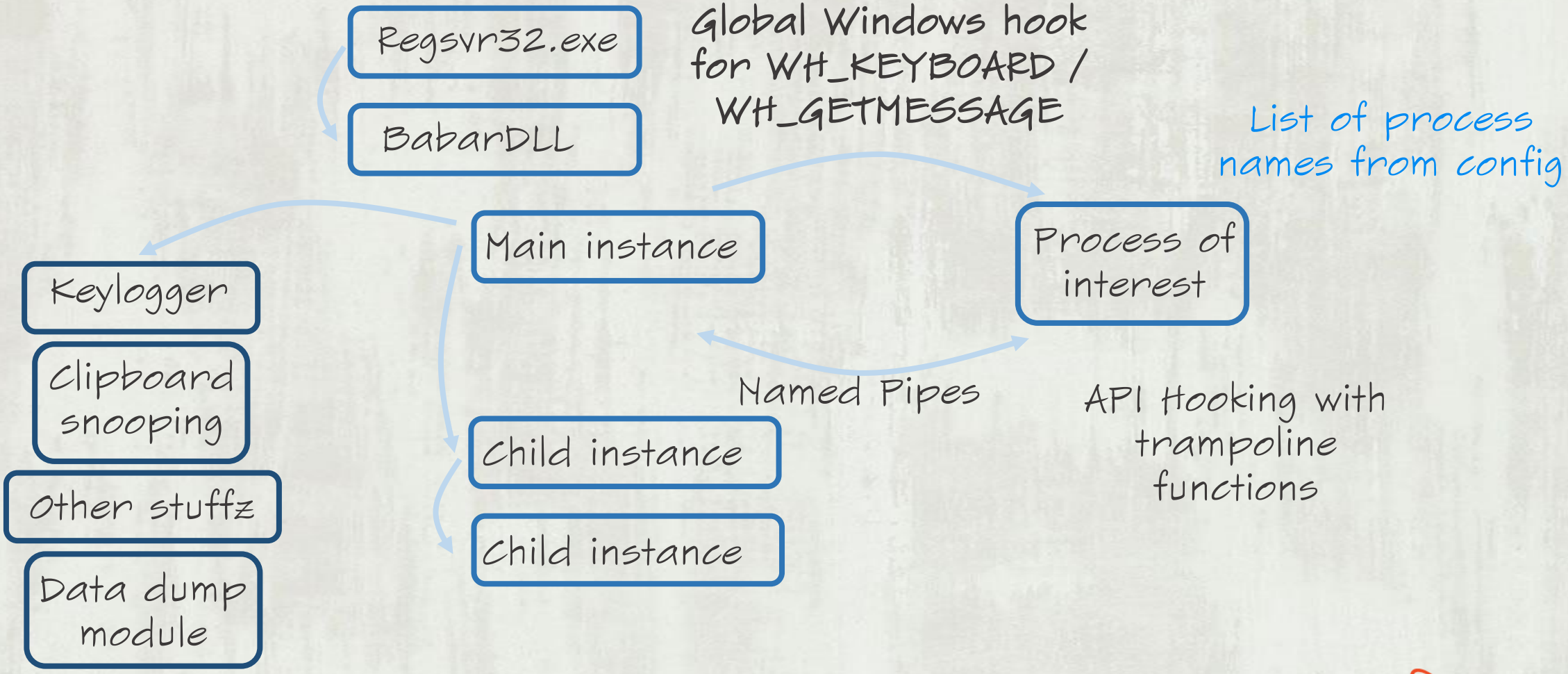
Babar

PET Persistent Elephant Threat

- Espionage par excellence
  - Keylogging, screenshots, audio captures, clipboard data, what-not.
- Via local instance or through:
  - hooking APIs in remote processes
    - after invading them via global Windows hooks

CYPHORT

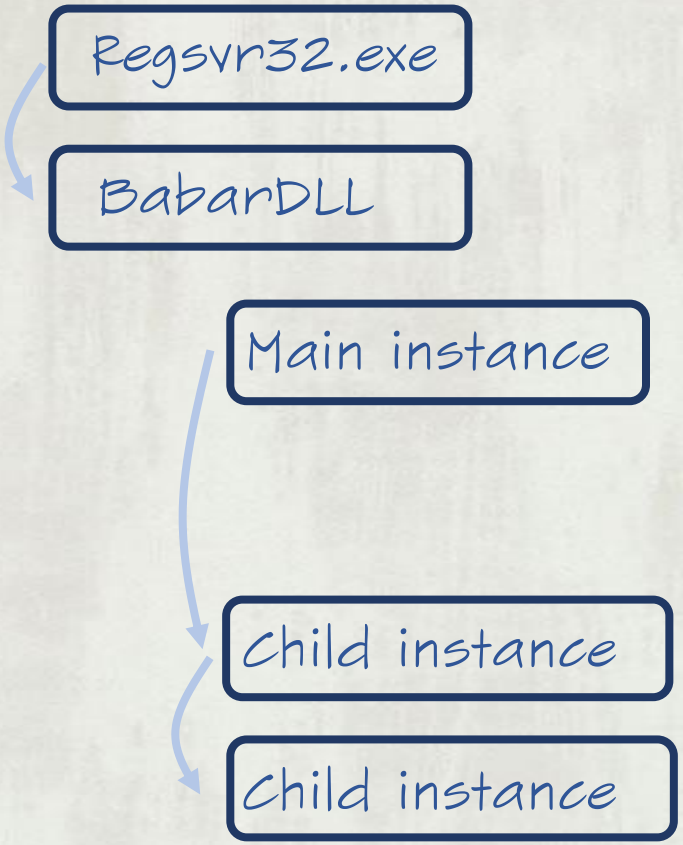
Modus Operandi Elephanti



CYPHORT

Hiding in plain sight

CYPHORT



Create section object with crucial information
- Pipe name
- number of existing instances
- export name to be called

Copy function stub to target process memory

Create remote thread
- loads Babar DLL
- calls indicated export
- Hands over data from shared object

Happily run DLL

Invisible message-only window

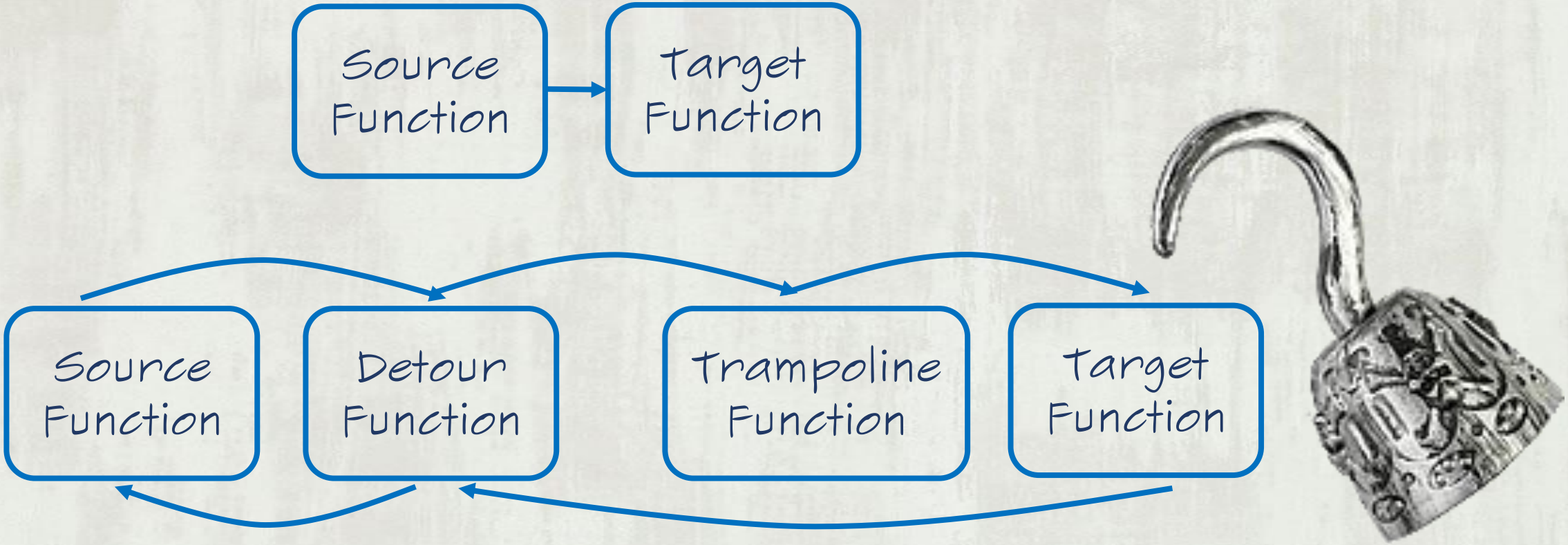
Message dispatching

- Receive WM_INPUT register raw input device with RAWINPUTDEVICE struct as follows:
  - Set RIDEV_INPUTSINK flag – receive system wide input
  - usUsagePage set to 1 – generic desktop controls
  - usUsage set to 6 – keyboard

On WM_INPUT call GetRawInputData

Map virtual key code to character & log to file

Rooootkittykittykitty



Internet communication | File creation | Audio streams

http://research.microsoft.com/en-us/projects/detours/

CYPHORT

Reconnaissance malware

AV ‚strategies‘

Spooking in Syria

Reversing Casper

CYPHORT

```
***** SECURITY INFORMATION *****
AntiVirus: N/A
Firewall: N/A

***** EXECUTION CONTEXT *****
Version: 4.4.1
...[REDACTED]...

***** SYSTEM INFORMATION *****
Architecture: x86
OS Version: 5.1
Service Pack: Service Pack 3
Default Browser: firefox.exe
User Agent: Mozilla/4.0 (compatible; MSIE 7.0; Win32)
Organization:
Owner: john
Country: United States

***** Running PROCESS *****
...[REDACTED]...

*****HKLM AutoRun x86 PROCESS *****
...[REDACTED]...

*****HKLM AutoRun x64 PROCESS *****
...[REDACTED]...

*****HKCU AutoRun x86 PROCESS *****
...[REDACTED]...

*****HKCU AutoRun x64 PROCESS *****
```

Espionage backdoor with numerous features

Popped up in Iran in 2013

Module Name Purpose

PSM	Encrypted on disk copy of Dino modules
CORE	Configuration storage
CRONTAB	Tasks scheduler
FMGR	Files upload and download manager
CMDEXEC	Commands execution manager
CMDEXECQ	Storage queue for commands to execute
ENVVAR	Storage for environment variables


```
;
; Export Address Table for Dino.exe
;
```

CYPHORT

Binary handwriting

Any attribute can be faked.

Question is, how many attributes can be faked.

Approach: Collect as many attributes as possible....

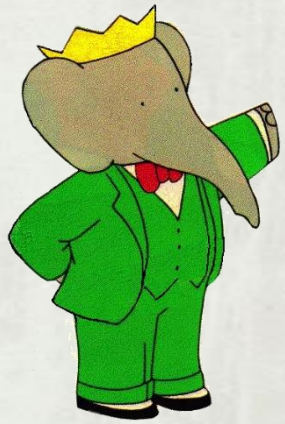
.... from different domains ....

.... and rely the adversary was not genius enough to fake all.

	A	B	C	D	E
1			NBOT/TFC	Bunny	Babar
2	String constants				
3		Error / status messages	No	Many	Many
4		String formatting style	All plain, commands/config all caps, no special charact	Partially plain, config encrypted, config all caps in XML t	All plain, config all caps, enclosed in '%' characters
5		English grammar mistakes	No	Many	Many
6		C&C commands	PING,EXEC,HTTPF,ASPFLOOD,TCPFLOOD,WEBFLOOD,POSTFI	mainfrequency,getconfig,ftpput,ftpget,sendfile,getfile,u	N/A
7		Timestamp formatting	Time APIs _time64, _mktime64; '%02d:%02d:%02d', Time	Time API GetSystemTime(), 'timestamp %04d-%02d-%02(	N/A
8	Implementation traits				
9		Memory allocation habits	direct calls to _malloc/_free, no wrappers	GetProcessHeap()/HeapAlloc()/HeapFree() in large nun	direct calls to _malloc/_free, no wrappers
10		Use of global variables	Few	Few, storing of event handles, strings, global flags use	Few, storing of event handles, strings
11		Multi-threading model	Simple, main thread with several worker threads	Simple, main thread with several worker threads	Complex, multi-threading in various instances coordinat
12		Software architecture and design	Standalone executable, classical bot structure	Standalone executable, classical bot structure, integrat	DLL, designed to run in context of arbitrary process, mai
13		Constructor design	MSVC++ default	MSVC++ default	MSVC++ default with complex object dependencies
14		Dynamic API loading technique	Present, subset of APIs only, per API, API name identifie	Present, subset of APIs only, per API, API name identifie	Present, subset of APIs only, per API, API name identifie
15		Exception handling	C++ EH and unhandled exception filter: ExitThread()	C++ EH and unhandled exception filter: ExitThread() (dy	C++ EH default
16		Usage of public source code	None (known)	Lua engine, C/Invoke bindings	Keylogger from codeproject.com, OpencoreAMR library,
17		Programming language and compiler	C++ / MSVC++ 8.0	C++ / MSVC++ 8.0	C++ / MSVC++ 8.0
18		Compilation time stamps and time zones	2010:03:11 17:55:03+01:00 2010:02:16 18:05:54+01:00 2010:05:06 15:47:37+02:00	 2011:10:25 21:28:39+02:00 2011:10:25 21:28:00+02:00	2011:08:29 15:02:29+02:00 2011:08:29 13:48:42+02:00 2011:07:06 15:50:11+02:00
19	Custom features				
20		Obfuscation techniques	Obfuscation of subset of API names that are to be load	Obfuscation of subset of API names that are to be load	Obfuscation of subset of API names that are to be loade
21		Stealth and evasion techniques	Obfuscation of subset of APIs	Emulator check,Containing directory name check,Payloa	Obfuscation of subset of APIs,Infection ‚strategy' based
22		Use of encryption and compression algorithms	API name obfuscation custom algorithm	API name obfuscation custom algorithm	API name obfuscation custom algorithm, adaption of Sl
23		(Shared) encryption keys	XOR key AB34CD77h	XOR key AB34CD77h, keys for command/data en-/decryp	128bit AES, 24 FE C5 AD 34 56 F7 F8 12 01 00 AE B6 7C DE A
24		Re-used source code in general	Timestamp generation, API name hashing and loading,	API name hashing and loading, infection strategy and A	infection strategy and AV product enumeration through
25		Malware specific features	DDoS bot for flooding of network packets	Lua scripted bot for automation of tasks	Espionage malware and userland rootkit
26		ystem infi	gned to	ning in context of	Lo y a try key	unning in context c	Loaded through registry key which invokes regsvr32.exe
27		opag anis		N/		N/A
28		Artifa g scheme gori	g v aming pref	Inte unny ayloa e netmgr.exe, r	Internal name Babar64, payload dump21cb.dll, directory
29		ation techn	sent to C&C nand	Log-/ le regula hed t	Dumpfiles regularly pushed to C&C (assumption)
30		en de ati		N/A	N/A
31		C&C con ing	ypted ecei over as	Encryp ommand rece &C, command parsi	N/A
32		Malware configuration	hardcoded / plaintext	hardcoded / encrypted	hardcoded / encrypted
33	Infrastructure				
34		C&C servers	http://callientefever.info/, http://fullapple.net/	http://le-progres.net/, http://ghatreh.com/, http://usthb	http://www.horizons-tourisme.com/, http://www.gezelin
35		Countries / languages used for domain hosting and namin	US/English	US/French, US/Iranian, US/Algerian	US/Algerian, US/Turkish
36		User agent / beaconing style	User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows	User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)	User-Agent: Mozilla/4.0 (compatible; MSI 6.0; Windows N
37		Communication protocol / port	HTTP/80	HTTP/80	HTTP/80
38		Communication intervals	On demand	Regular, interval configurable	Regular (assumption)

Stylometry in Attribution

BABAR
linked to French government



BUNNY
spearphishing with 0-days

NBOT
Denial-of-Service

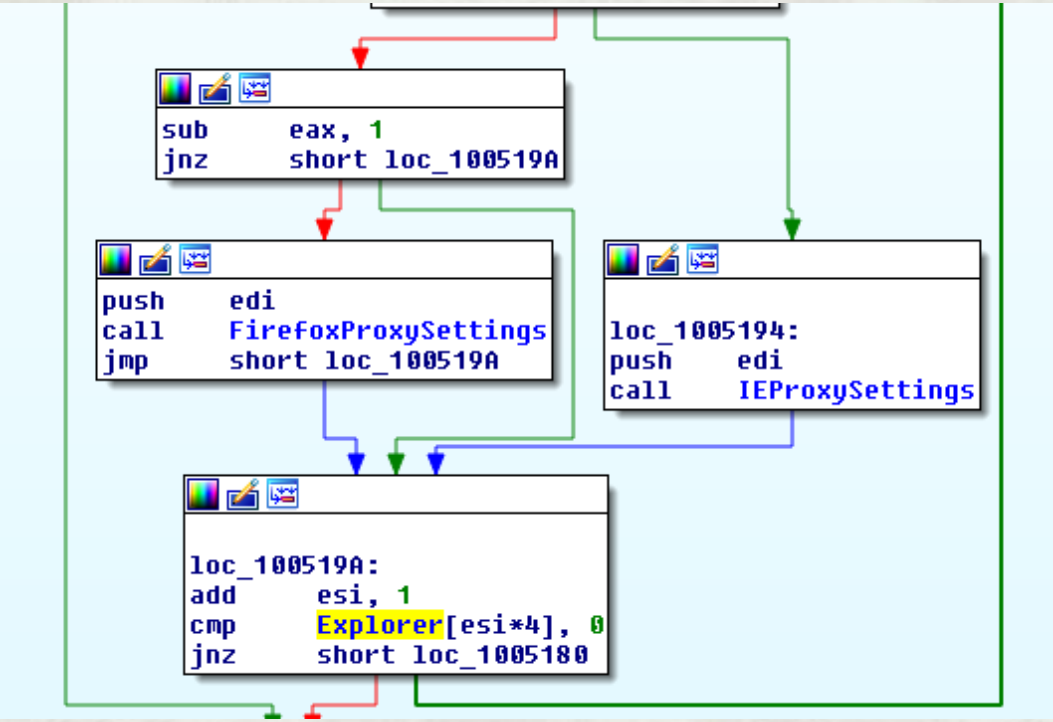
DINO
spying in Iran

CASPER
active in Syria in 2014

CYPHORT

CYPHORT™

Proxy Bypass



- Babar starts up using regsvr32.exe process for loading payload
- Process remains running, when rootkit has looong dissappeared

Stealth FTW

CYPHORT

Crash me, if you can

- NBOT dropper crashes with a STATUS_SHARING_VIOLATION 0xC0000043 on CreateFile of own binary
- A file cannot be opened because the share access flags are incompatible.

- Bunny dropper won't invoke its payload
- Does not delete dropper either
- Bypasses sandboxes, but leaves unnecessary artifacts lying around

Bug & Feature & Bug

CYPHORT

Attribution is hard.

sécurité des télécommunications du Canada avait dé
iciel espion nommé "Babar". Les autorités canadiennes y voyaient
services de renseignement français. "La France est aussi active
la chercheuse australienne Marion Marschalek (Cyphort)

CYPHORT

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

SNOWGLOBE.

- CSEC assesses, with moderate certainty, SNOWGLOBE to be a state-sponsored CNO effort, put forth by a French intelligence agency

CYPHORT

Cartoons allegedly originate from France,
main suspect is DGSE

Linked by document from CSEC

Iran as main target

Other victims in Syria, Norway, Canada

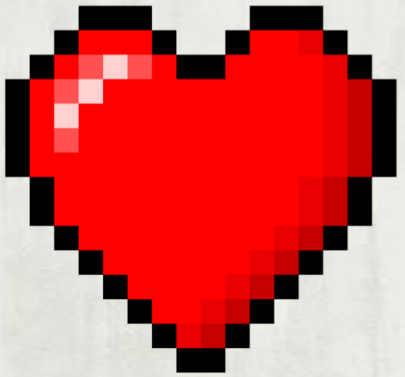
.. and Mr. Brown said [abt. Iran not meeting international demands], *"The international community has no choice today but to draw a line in the sand."* – NYT, Sep.2009

A cyberwarfare tale on nuclear matters

A blog by Matt Suiche

CYPHORT

Special Thanks



Go to

-Joan Calvet

-Paul Rascagnères

-Morgan Marquis-Boire

-Edward Snowden & CSEC Canada

Further Reading

- Babar Reversed http://www.cyphort.com/babar-suspected-nation-state-spyware-spotlight/
- Bunny Reversed http://www.cyphort.com/evilbunny-malware-instrumented-lua/
- Casper Reversed by Joan Calvet http://www.welivesecurity.com/2015/03/05/casper-malware-babar-bunny-another-espionage-cartoon/
- Linking the Cartoon Malware to CSEC slides by Paul Rascagneres https://blog.gdatasoftware.com/blog/article/babar-espionage-software-finally-found-and-put-under-the-microscope.html
- Slides „TS/NOFORN" at Hack.lu2015 http://2014.hack.lu/archive/2014/TSNOFORN.pdf
- Slides on Snowglobe from CSEC http://www.spiegel.de/media/media-35683.pdf and http://www.spiegel.de/media/media-35688.pdf
- A cyberwarfare tale on nuclear matters by Matt Suiche http://www.msuiche.net/2015/03/09/did-alleged-dgse-used-stackoverflow-like-to-write-their-malwares/
- Animal Farm https://securelist.com/blog/research/69114/animals-in-the-apt-farm/

CYPHORT

Hashes

Bunny:

- 3bbb59afdf9bda4ffdc644d9d51c53e7
- b8ac16701c3c15b103e61b5a317692bc
- c40e3ee23cf95d992b7cd0b7c01b8599
- eb2f16a59b07d3a196654c6041d0066e

Babar:

- 4525141d9e6e7b5a7f4e8c3db3f0c24c
- 9fff114f15b86896d8d4978c0ad2813d
- 8b3961f7f743daacfd67380a9085da4f
- 4582D9D2120FB9C80EF01E2135FA3515

NBOT:

- 8132ee00f64856cf10930fd72505cebe
- 2a64d331964dbdec8141f16585f392ba
- e8a333a726481a72b267ec6109939b0d
- 51cd931e9352b3b8f293bf3b9a9449d2

Casper:

- 4d7ca8d467770f657305c16474b845fe
- cc87d090a1607b4dde18730b79b78632

Dino:

- 30bd27b122c117fabf5fbfb0a6cdd7ee

Other:

- bbf4b1961ff0ce19db748616754da76e
- 330dc1a7f3930a2234e505ba11da0eea

CYPHORT

Thank you!

Marion Marschalek
@pinkflawd
marion@cyphort.com

CYPHORT™

http://karmadecay.com/