BIG GAME HUNTING

Peculiarities In Nation State Malware Research

Marion Marschalek

Senior Malware Researcher
Cyphort Inc.

Google
TM
Oh baby
you

THE CENTRIFUGES THAT SPIN NUCLEAR MATERIAL AT IRAN'S ENRICHMENT FACILITIES

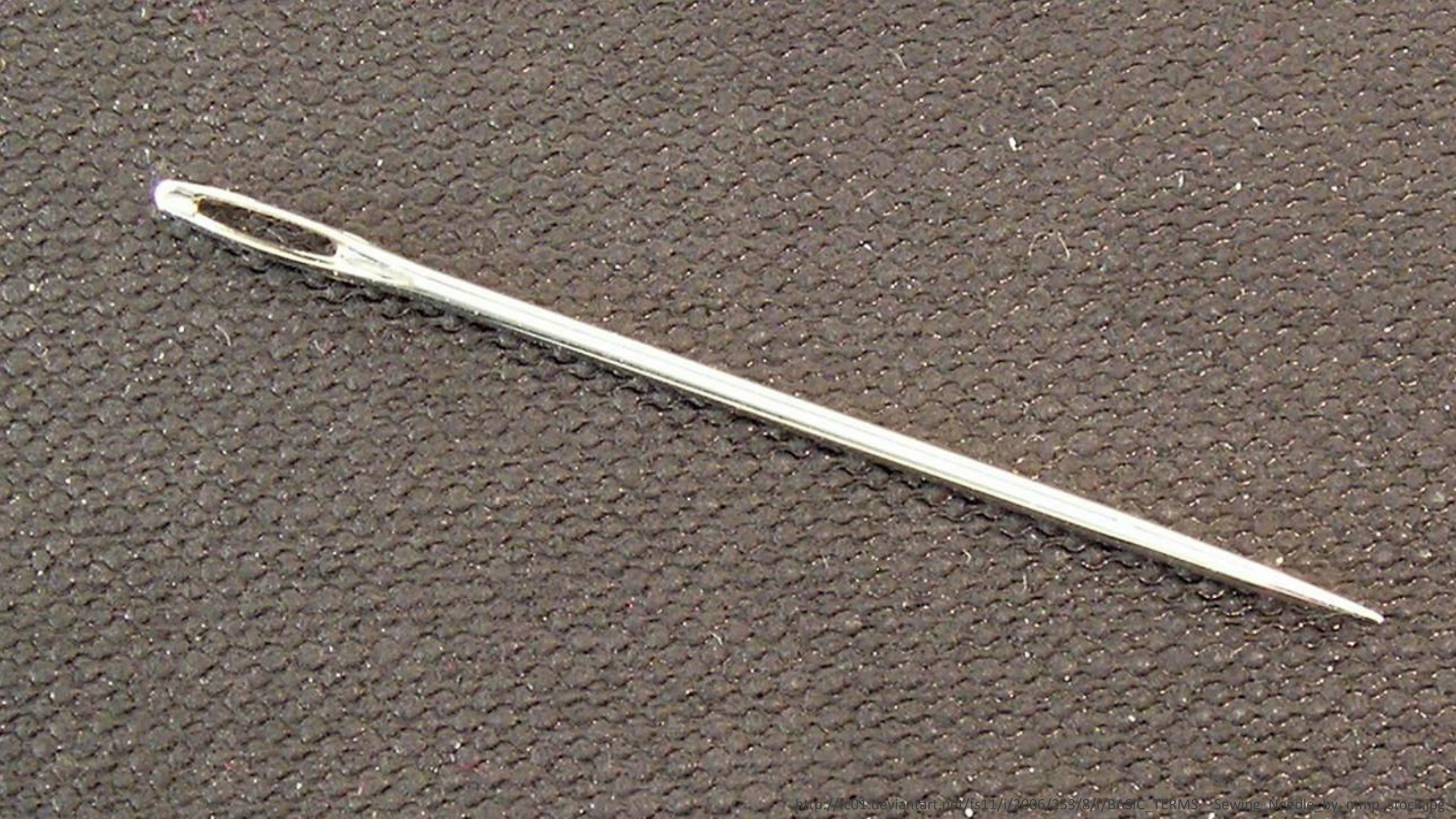

~D
AP

Offense Going Commercial

AV 2.0

… where the customer is the product
How Anti-Virus went Threat-Intel

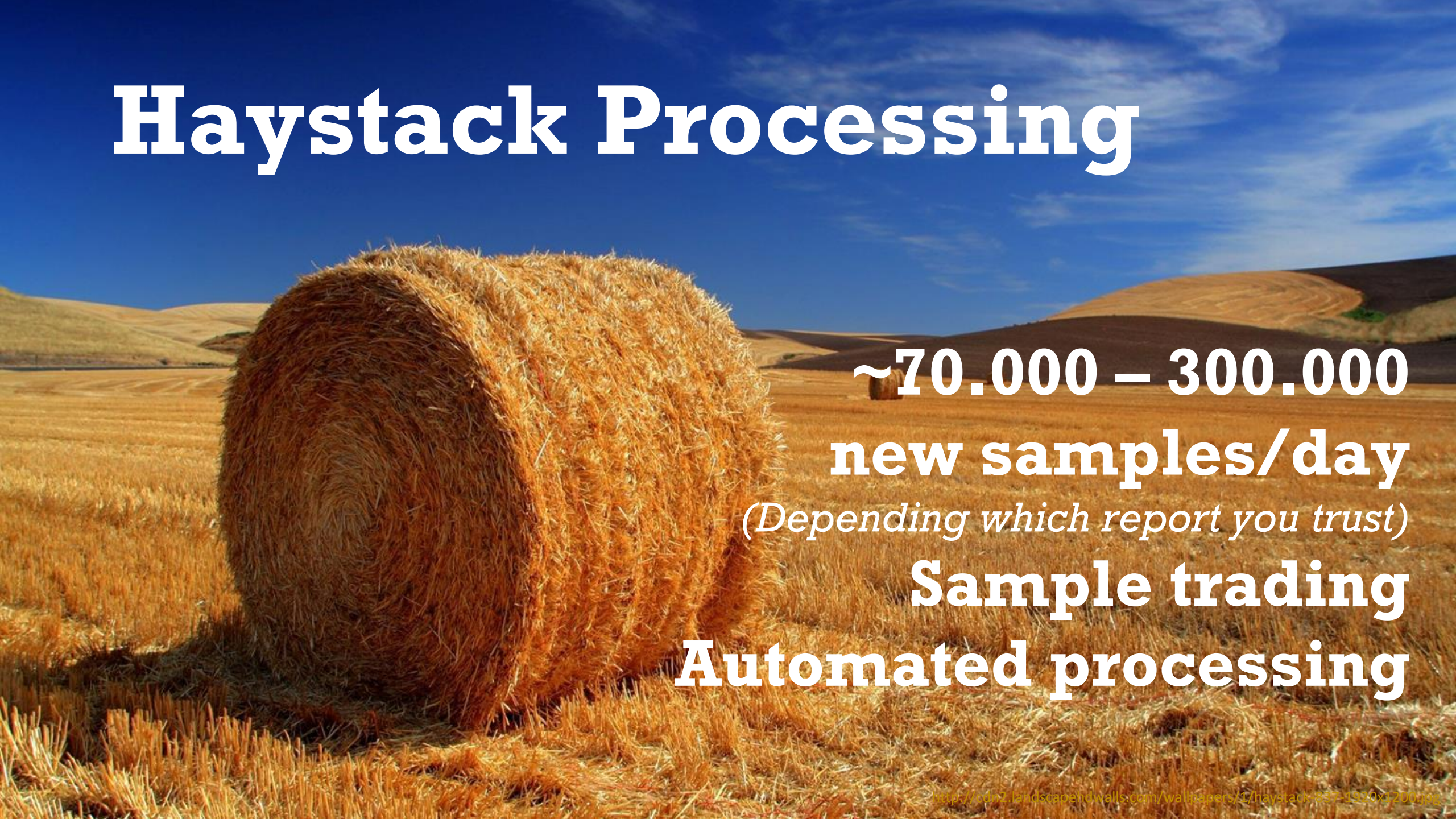
Malware.. 'watching'
Actor tracking
Publicity
APT numbering, logos & names



http://i01.deviantart.net/fs11/i/2006/233/8/f/BASIC_TERMS__Sewing_Needle_by_mmp_stock.jpg


http://cdn2.landscapehdwalls.com/wallpapers/1/haystack-837-1920x1200.jpg

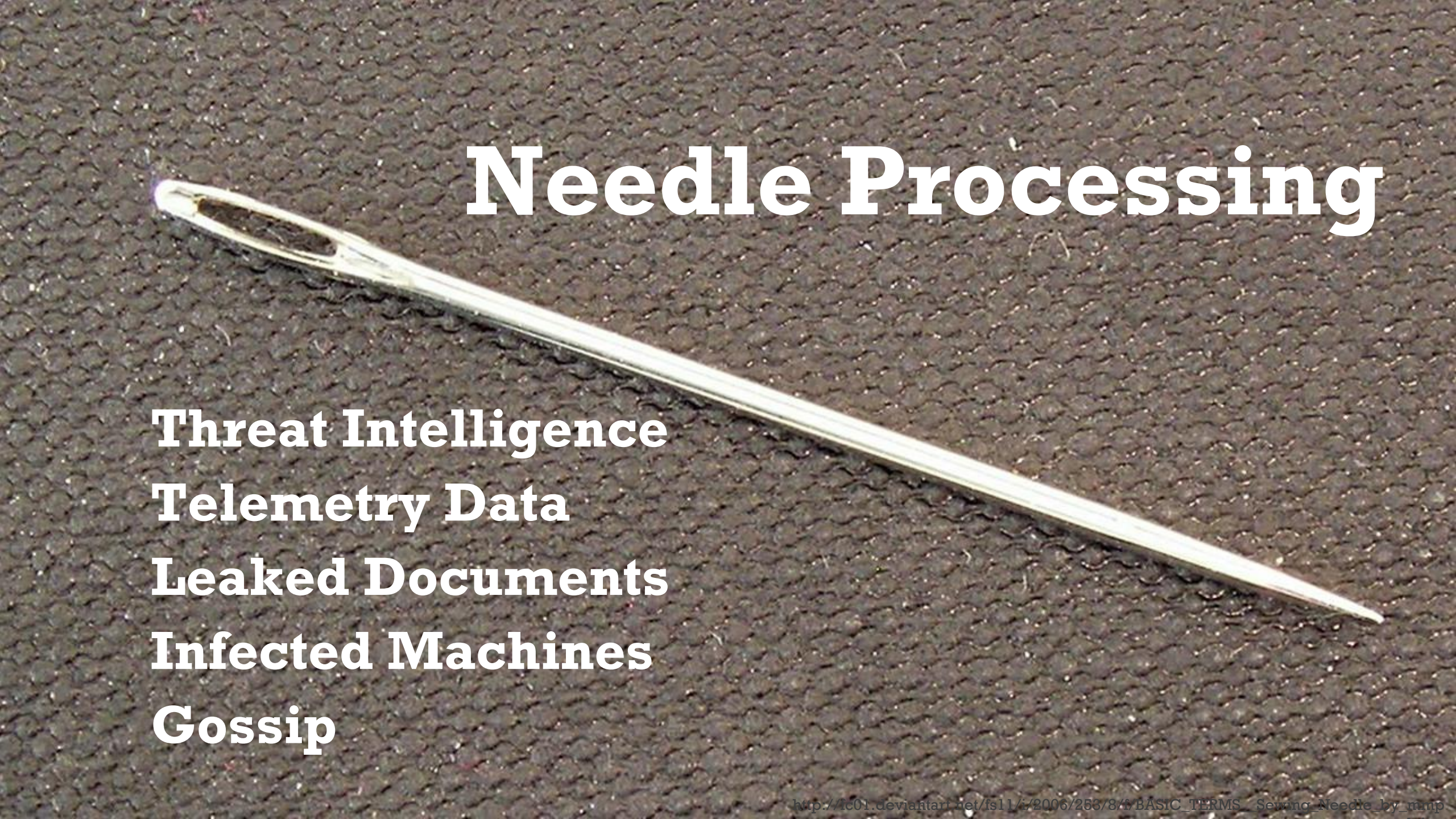
Haystack Processing



~70.000 – 300.000
new samples/day
(Depending which report you trust)
Sample trading
Automated processing

http://cdn2.landscapehdwalls.com/wallpapers/1/haystack-837-1920x1200.jpg

Needle Processing



Threat Intelligence
Telemetry Data
Leaked Documents
Infected Machines
Gossip

http://fc01.deviantart.net/fs11/i/2006/253/8/f/BASIC_TERMS__Sewing_Needle_by_mmp

ENDPOINT WARS

Endpoint agents
Threat indicators
Mitigation tactics
Silent data exchange

ENDPOINT WARS

Threat Indicators

Agent

Threat detection & mitigation

Q&A Data

- Signature hits
- Timestamps
- Hit frequencies
- Binaries

ENDPOINT WARS backstage

Signature generation & testing
Silent signatures
Binaries
Telemetry
‘Free’ security products


FRENEMIES & THE FUNGUS AMONGUS
Or: When Malware Became Intellectual Property

[REDACTED] "Where did you find this malware?"

Me: "It was sent to me by targeted activists."

[REDACTED] "That's Cheating."

Alberto Nisman


CRISTINA
BASTA
YO SOY
NISMAN
NISMAN
GRACIAS

Todo parece indicar que Nisman fue engañado. A su teléfono Motorola xt626 llegó un archivo con el título "estrictamente secreto y confidencial.pdf.jar". Acaso creyendo que se trataba de un documento importante, lo abrió sin advertir la extensión ".jar". Allí estaba el virus.

3445a61556ca52cf5950583e0be4133de7a4f6a8

Attribution IS tricky?

Network based indicators point to
Argentina and Uruguay

Also use of hosting services in the
US, Germany, and Sweden

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 |

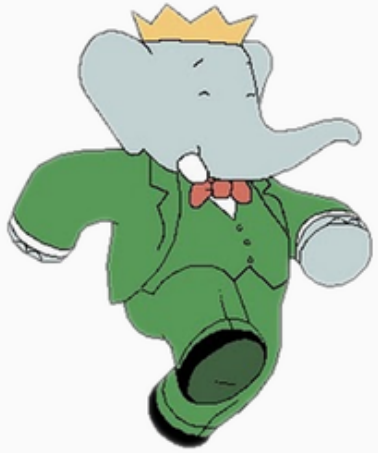
Par Jacques Follorou et Martin Untersinger

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

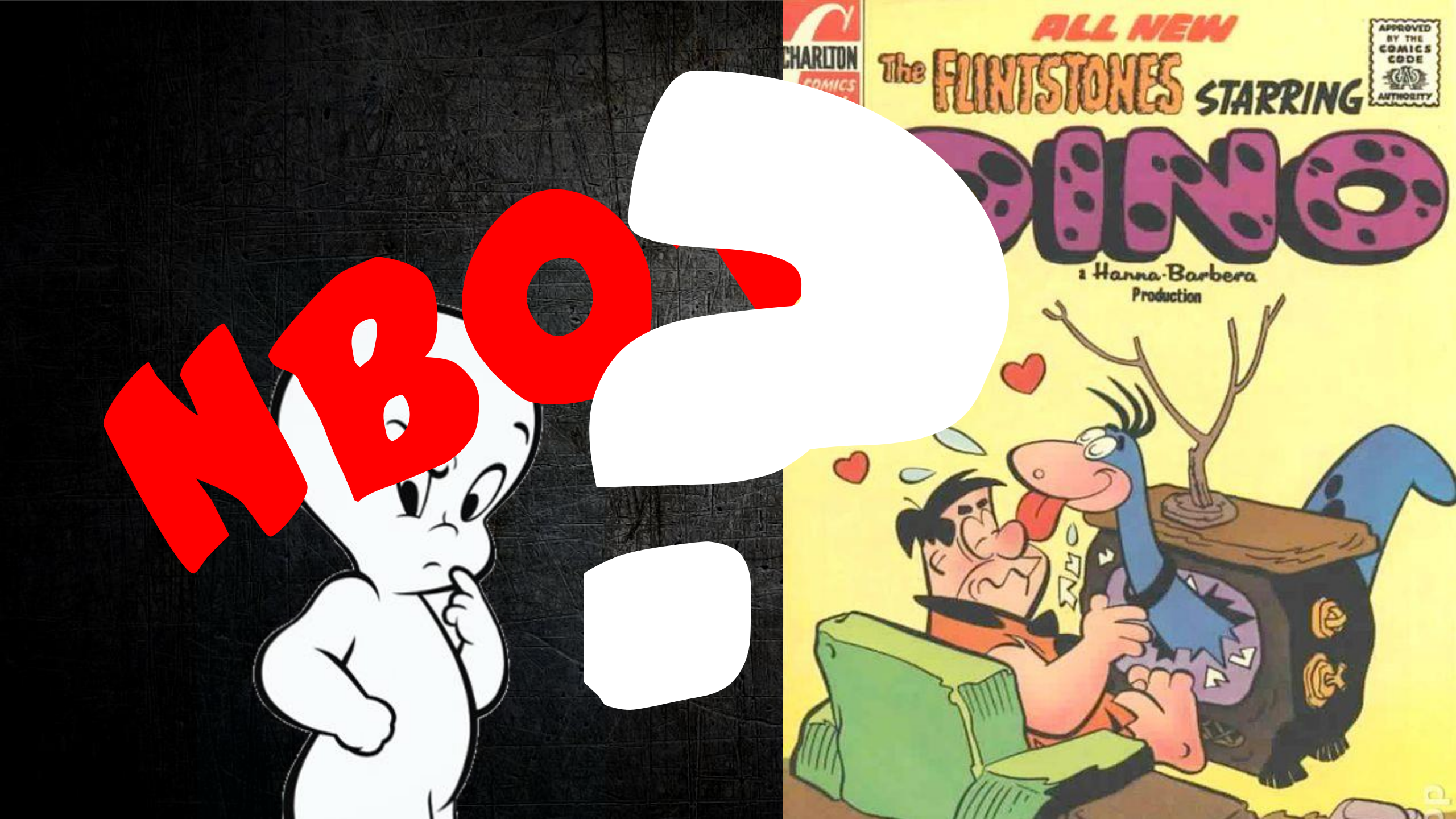


C'est une véritable traque qu'ont menée les services secrets techniques canadiens du Centre de la sécurité des télécommunications du Canada (CSEC). Elle est relatée dans le document fourni au *Monde* par Edward Snowden, dans lequel ils présentent leurs trouvailles. Avare en détails, ce document permet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


NBC?!
CHARLTON COMICS
ALL NEW
The FLINTSTONES STARRING
DINO
a Hanna-Barbera Production
APPROVED BY THE COMICS CODE AUTHORITY

MISERY BUSINESS

Who wrote the malware?

Who controlled the malware?

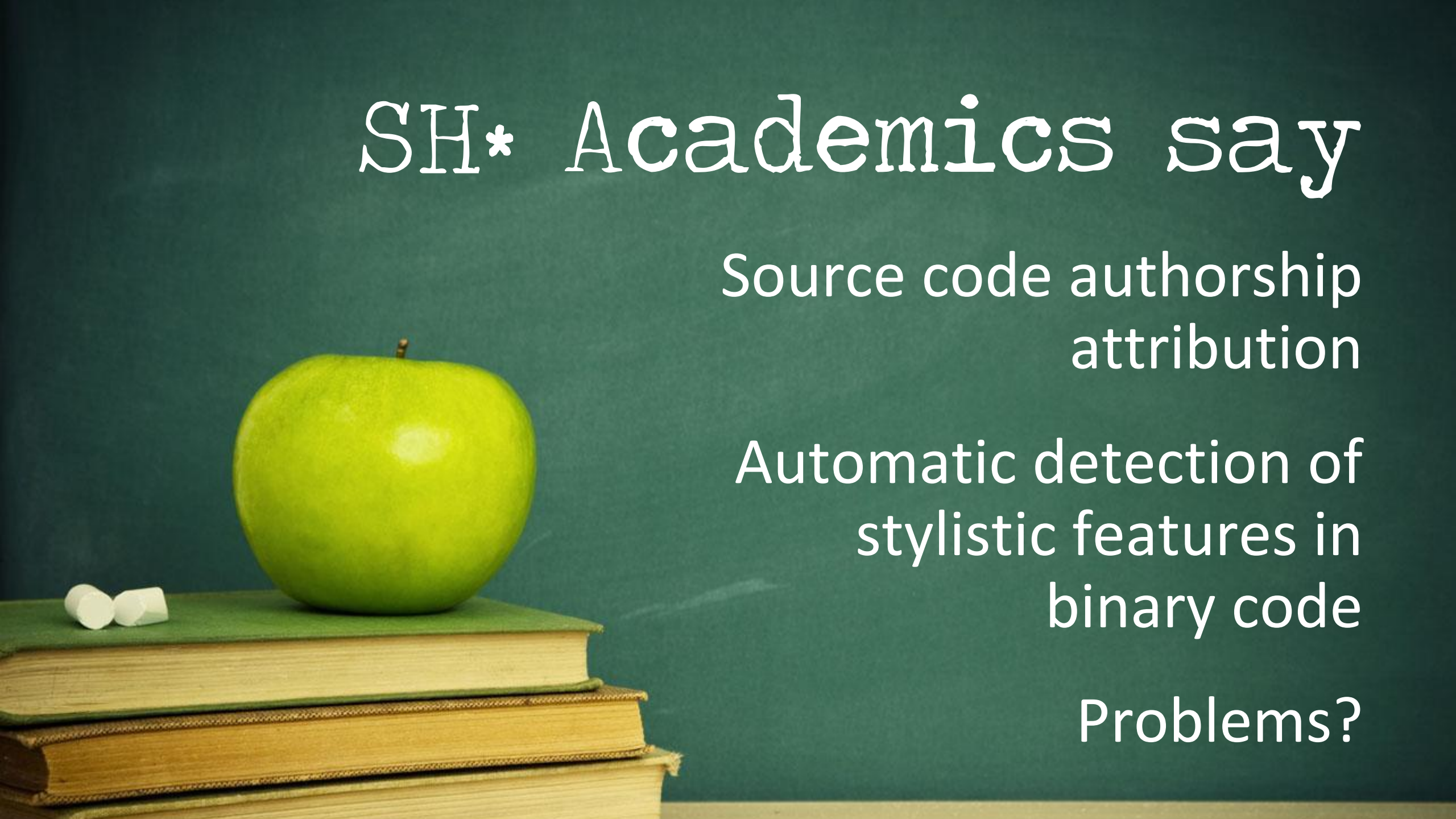
Who were the victims?

What was the aim of the operation?

MISERY BUSINESS

BINARY → CONTEXT

BINARY → BINAR A CO


SH* Academics say
Source code authorship attribution
Automatic detection of stylistic features in binary code
Problems?

Datafication of RE results

Different domains & lots of attributes

Any attribute can be faked or random

Assumption: Impossible that all vary in all cases
Goal: Even out individual human / compiler influence

STRING CONSTANTS

- Error messages
- String formatting style
- English grammar mistakes
- C&C commands
- Timestamp formatting

IMPLEMENTATION TRAITS

- Memory allocation habits
- Use of global variables
- Multi-threading model
- Software architecture and design
- Constructor design
- Dynamic API loading technique
- Exception handling
- Usage of public source code
- Programming language and compiler
- Compilation time stamps and time zones

CUSTOM FEATURES

- Obfuscation techniques
- Stealth and evasion techniques
- Use of encryption and compression algorithms
- Encryption keys
- Re-used source code
- Malware specific features
- System infiltration
- Propagation mechanisms
- Artifact naming schemes / algorithms
- Data exfiltration techniques
- System / OS version determination technique
- C&C command parsing implementation

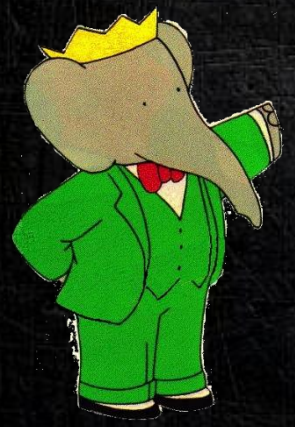
INFRASTRUCTURE

- C&C servers
- Countries / languages used for domain hosting and naming
- Beaconing style
- Communication protocol and port
- Communication intervals

	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 ed ming in context of	Lo by a try key o 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 mentation	ypted receiv , ha 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

What It's Not

No authorship attribution

Manual work

Not feasible for automation / machine learning

Interpretation in the eye of the analyst

Soft Attribution vs Hard Attribution

SECRET MALWARE IN EUROPEAN UNION ATTACK LINKED TO U.S. AND BRITISH INTELLIGENCE

BY MORGAN MARQUIS-BOIRE, CLAUDIO GUARNIERI, AND RYAN GALLAGHER @headhntr @rj_gallagher

11/24/2014

POPULAR


HEY, FEMINIST INTERNET COLLECTIVE: GOOD REPORTING DOES NOT HAVE TO BE SENSITIVE


HOW THE NSA HACKS CELLPHONE NETWORKS WORLDWIDE

THE INTERCEPT WELCOMES OUR NEW EDITOR-IN-CHIEF, BETSY REED


WHITE HOUSE GETTING COLD FEET OVER EXPOSING CIA'S TORTURE SECRETS


THE NEW PENTAGON CHIEF, ASHTON CARTER, AND THE BEAUTY OF DC BIPARTISANSHIP

USERDNSDOMAIN=BGC.NET

USERDOMAIN=BELGACOM

USERNAME=id051897a

USERPROFILE=C:\Users\id051897a

Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm

REUTERS

A cyber attack on Belgacom raised considerable attention last week. Documents leaked by Edward Snowden and seen by SPIEGEL indicate that Britain's GCHQ intelligence agency was responsible for the attack.

"Looking at the code closely, we conclude that the "QWERTY" malware is identical in functionality to the Regin 50251 plugin."

"BLIND FREDDY
COULD SEE E_QWERTY
IS A REGIN PLUGIN"

Curiouser and Curiouser!

- cried Alice

CHESHIRE CAT

SSOOOUU...

```
e2ca6cca598d47dee311f06920c1efde - 2002-11-05 02:02:19
4e0a3498438adda8c50c3e101cfa86c5 - 2007-08-13 11:02:54
3ba57784d7fd4302fe74beb648b28dc1 - 2008-08-13 15:20:23
7b0e7297d5157586f4075098be9efc8c - 2009-05-03 20:43:05
fa1e5eec39910a34ede1c4351ccecec8 - 2011-05-16 16:55:17
```

String obfuscation with XOR 9Bh

Checking for running security processes (and dummyyy.exe)

2002

Control component talking to a device driver \\.\asr2892
Sending IOCTLs 220004 & 220008

Orchestrator component executing binaries from disk
Drops ‘msrun.exe’ from .rsrc section
Redirects standard handles of spawned process, piping output back to launcher

2002

Prepared to run on _old_ Windows versions

Using APIs deprecated after Win95/98/ME

Function to check for the MZ value,
the PE value and the NE value

2002

Implementation traits and user agent string indicate Win NT 4.0 as target platform

Persists as shell extension for the icon handler

Wants to run in the context of the ‘Progman’ window

2007-2009

Implant to monitor terminal server sessions

Global hook to filter for WM_KEYFIRST, WM_SYSKEYDOWN, WM_CHAR, WM_SYSCHAR

Loads msob4k32.dll and 6 exports by ordinal

2007-2009

String obfuscation using XOR 9Bh
Evasive when network
sniffer products are running

Super stealthy network communication:
Versatile communication method
9+ C&C servers, infrequent intervals
Communication done through injected
standard browser instance

2007-2009

Fine tuned
to paddle around
Kaspersky security
products

2011


~DF
AP

"We're All Mad Here"

MORGAN

@headhntr

MARION

@pinkflawd

#FREECLAUDIO

@botherder