The kings in your castle

All the lame threats that own you but will never make you famous

CIRCL
Computer Incident Response Center Luxembourg

G DATA ADVANCED ANALYTICS

http://hqwallbase.pw/images/medium/a-Ghost-in-the-Shell-wallpaper-1920x1200-39233.jpg


TROOPERS
MAKE THE WORLD A SAFER PLACE

RAPHAËL VINOT

Coding and Latex

@rafi0t

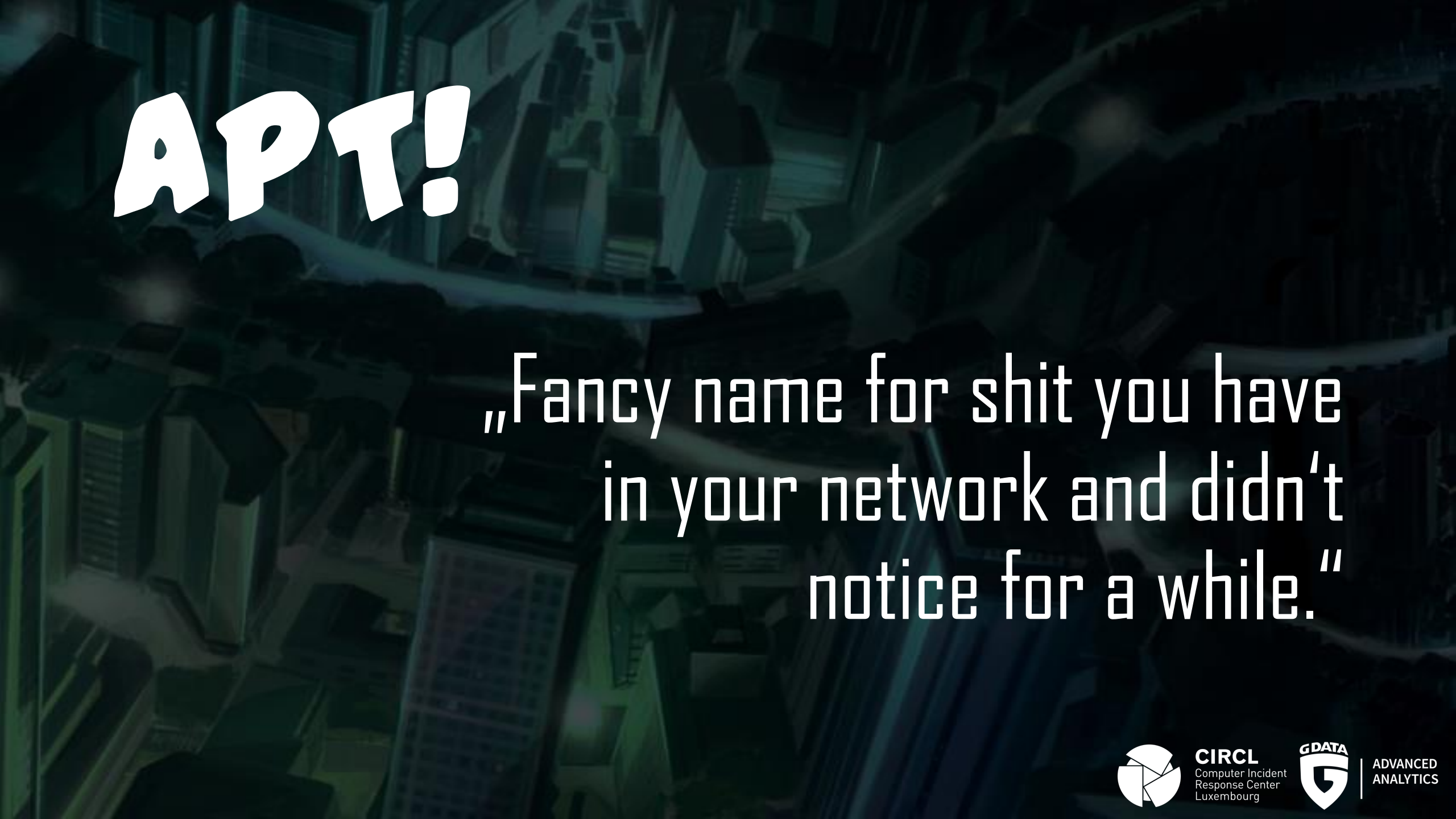
CIRCL
Computer Incident
Response Center
Luxembourg

MARION MARSCHALEK

Threat dissector & professional PPT slide artist

@pinkflawd

G DATA | ADVANCED ANALYTICS


APT!
„Fancy name for shit you have
in your network and didn‘t
notice for a while.“
CIRCL
Computer Incident
Response Center
Luxembourg
G DATA
ADVANCED
ANALYTICS

How APT happens

Reconnaissance – gather information

Incursion – break in

Discovery – look around

Capture – collect goods

Exfiltration – get goods out

CIRCL
Computer Incident
Response Center
Luxembourg

G DATA
ADVANCED
ANALYTICS

HIT BY AN (AP)T??

Don‘t feel too special.

Chances are, you‘re not the only victim.

CIRCL
Computer Incident
Response Center
Luxembourg

ADVANCED
ANALYTICS

List Events
Add Event
Import From MISP Export

List Attributes
Search Attributes

View Proposals
Events with proposals

Export
Automation

Events

« previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 next »

All : CIRCL | My Org | Filter

Published	Org	Id	Tags	#Attr.	#Corr.	Date	Threat Level	Analysis	Info	Distribution	Actions
✔		3367		75	1	2016-03-16	Low	Initial	Malspam (2016-03-16)	All	
✔		3365		398	1	2016-03-16	Low	Initial	Potential SpamBots (2016-03-16)	All	
✔		3364		42		2016-03-15	Low	Completed	Dridex botnet 222 (20160315)	All	
✔		3360		78	13	2016-03-15	Low	Initial	Malspam (2016-03-15) - TeslaCrypt	All	
✔		3359		7		2016-03-15	Low	Initial			
✔		3358		249	5	2016-03-15	Low				
✔		3356		417	1	2016-03-14	Low	Completed	Potential SpamBots (2016-03-14)		
✔		3355		182	13	2016-03-14	Low	Initial	Malspam (2016-03-14) - Locky, TeslaCrypt	All	

MISP

Tools, Techniques, Procedures, and Actors

TTPAS ;)

Correlations by IP, Domains, URLs ...

Correlations by filename, hashes

Compilation timestamps

Timings of the attacks

Whois

Grouping by imphashes

Source of the report

CIRCL
Computer Incident
Response Center
Luxembourg

ADVANCED
ANALYTICS

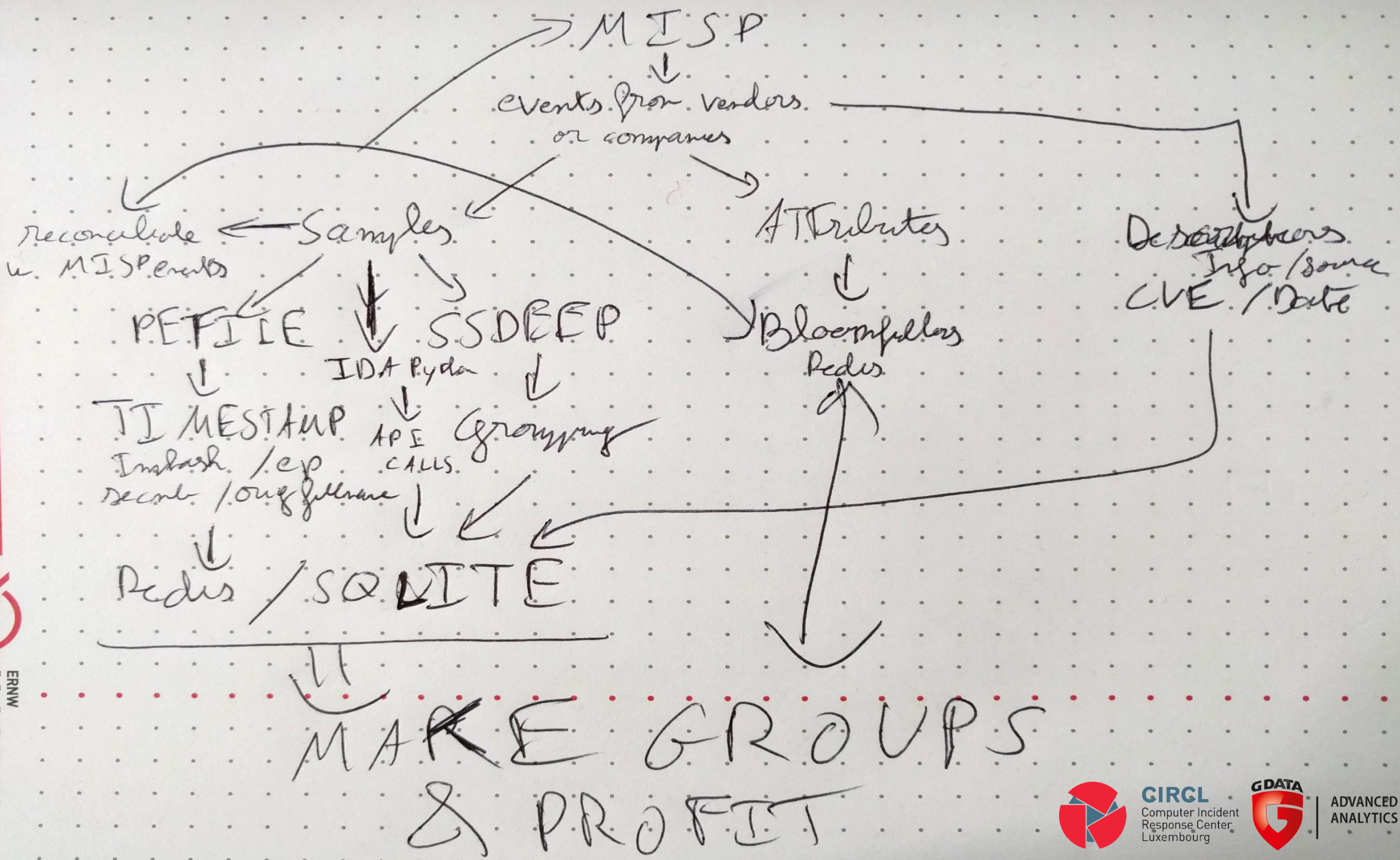
Tools

SUPER L33T TTPAS

- MISP interface
  - manual check of correlations
- PyMISP & Viper
  - to fetch all the attributes of the events we wanted to investigate
- Redis backend & fast lookup
  - to get all the events of each hashes (50k queries/s)
- MISP backend connector (python)
  - Specific queries not available through the interface
- ssdeep clustering
  - group the samples
- Dedicated code to sort the samples
  - compilation timestamps
  - filenames...
- Standalone SQLite and massive parser
  - Packer "detection", RapidMiner for visualization

CIRCL
Computer Incident
Response Center
Luxembourg

GDATA
ADVANCED
ANALYTICS



ERNW INSIGHT
expanding your knowledge.

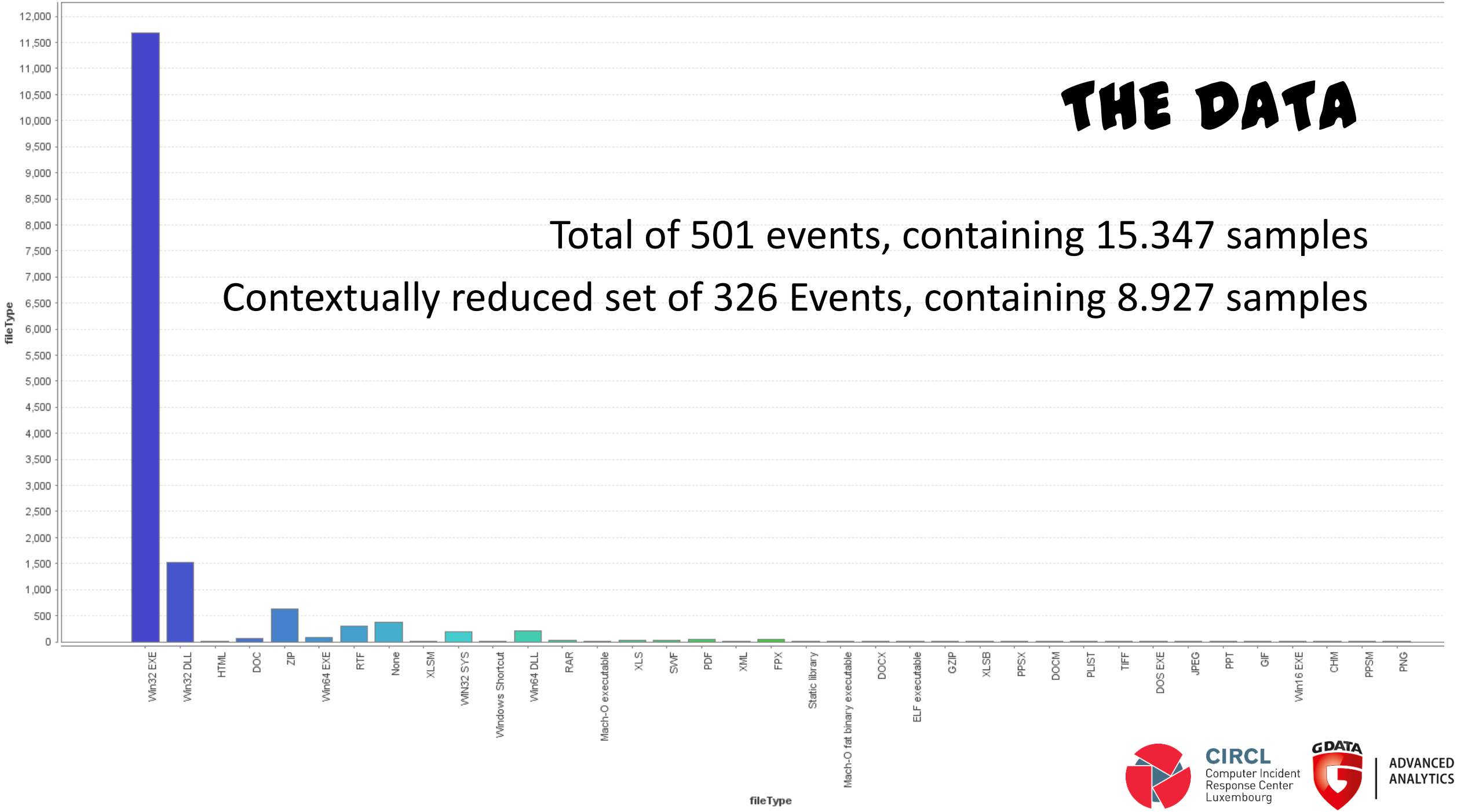
CIRCL
Computer Incident Response Center Luxembourg

GDATA ADVANCED ANALYTICS

THE DATA

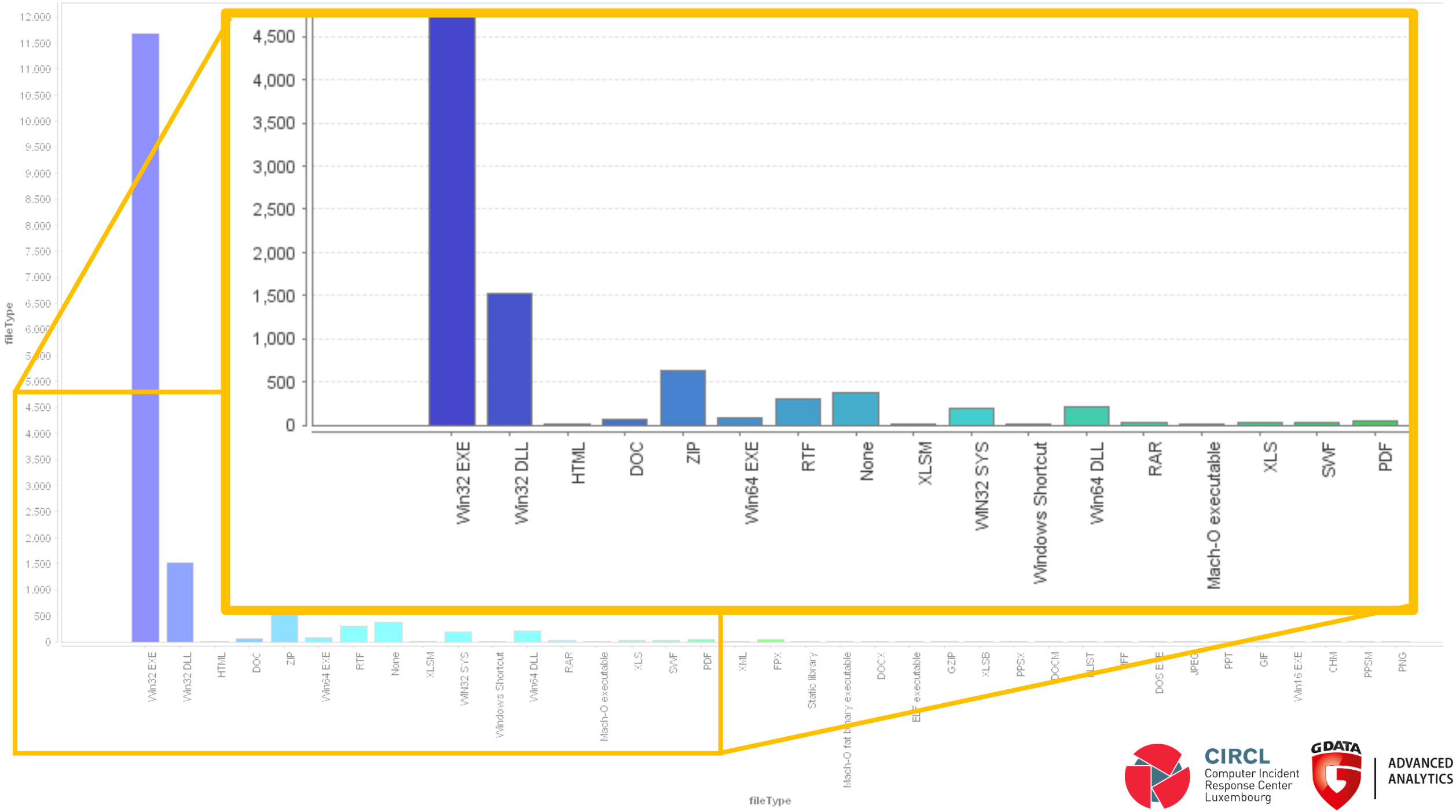
Total of 501 events, containing 15.347 samples

Contextually reduced set of 326 Events, containing 8.927 samples



CIRCL
Computer Incident
Response Center
Luxembourg

GDATA
ADVANCED
ANALYTICS



CIRCL
Computer Incident
Response Center
Luxembourg

G DATA
ADVANCED
ANALYTICS

DATASETS WRAP-UP

Events ID from MISP

Hashes (samples available on VT)

Network indicators

Vulnerability identifiers

PE Attributes

Binary intestines

Pick one, two, many, ..

CIRCL
Computer Incident
Response Center
Luxembourg

ADVANCED
ANALYTICS

CIRCL
Computer Incident
Response Center
Luxembourg

GDATA
ADVANCED
ANALYTICS

http://weneedfun.com/wp-content/uploads/2016/01/Flower-Power-1.gif

SSDEEP.. COLLISIONS?!

2 samples of PittyTiger, defering by nothing, but 5MB of padding:

152109806af8d2bbf9e945b81fbdf49d7168dcff1b4d454ec65a42c87ebd60ac
384:BM/DLTwMs0FjFOcvCyyYjfkaDllWUburdtR9:BM/D4Msi8cvCr4bGh

9addacd67c9574bf7b5233c9bd96b3b79905363da04eacfc6bac923c2aaf2df4
384:BM/DLTwMs0FjFOcvCyyYjfkaDllWUburdtR9:BM/D4Msi8cvCr4bGh

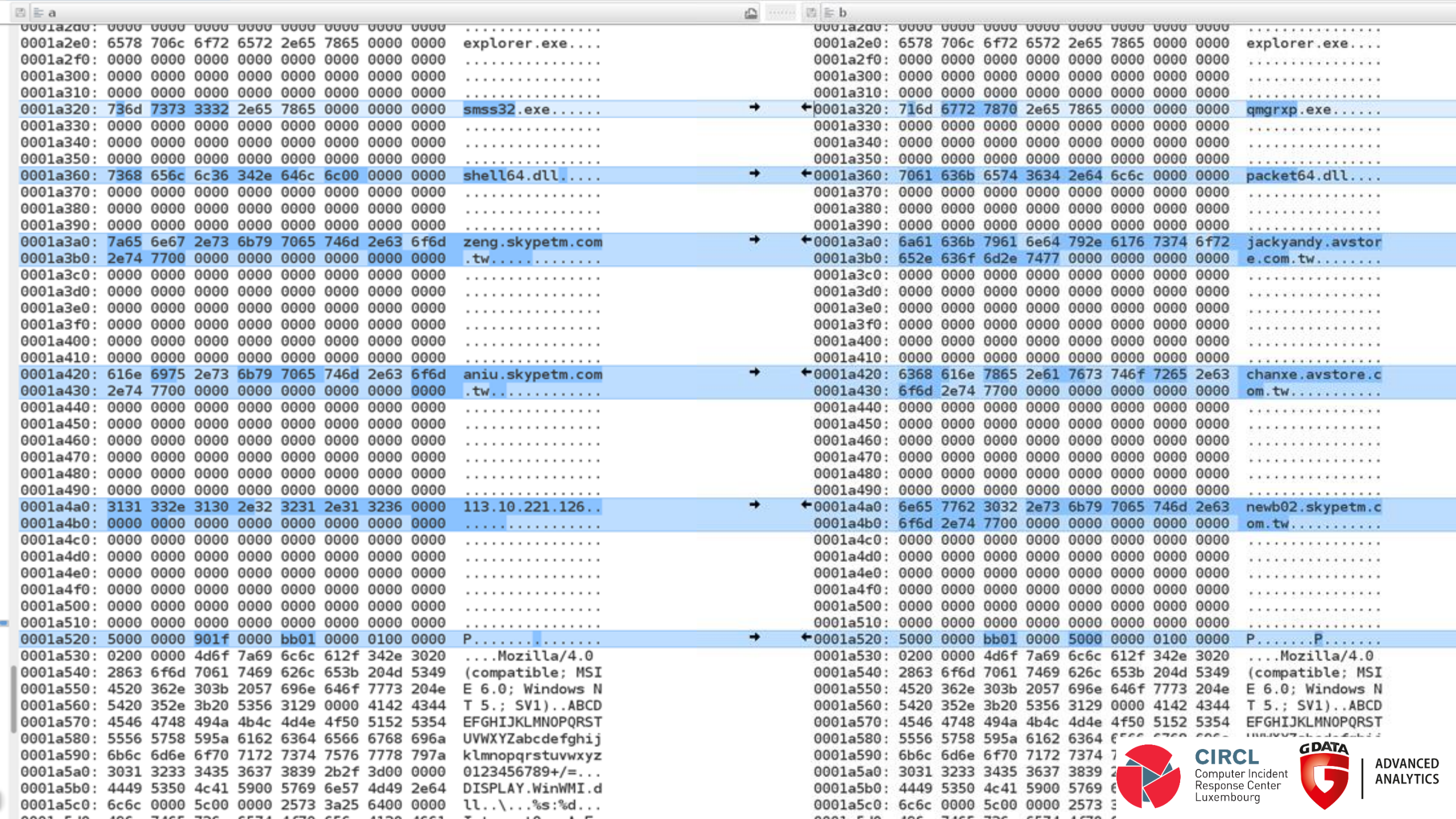
EnergeticBear / Havex:

B0faba6156c7b0cd59b94eeded37d8c1041d4b8dfa6aacd6520a6d28c3f02a5e
6144:NtWLXS1+0YUv+JfXUZkc7n1IWGWE0IhH6O5RUdAQ:NyXS1+BUWJf+j7n1LshH+

D89a80a3fbb0a4a40157c6752bd978bc113b0c413e3f73eb922d4e424edeb8a7
6144:NtWLXS1+0YUv+JfXUZkc7n1IWGWE0IhH6O5RUdAQ:NyXS1+BUWJf+j7n1LshH+

45abd87da6a584ab2a66a06b40d3c84650f2a33f5f55c5c2630263bc17ec4139
6144:NtWLXS1+0YUv+JfXUZkc7n1IWGWE0IhH6O5RUdAQ6:NyXS1+BUWJf+j7n1LshH+e

439e5617d57360f76f24daed3fe0b59f20fc9dade3008fd482260ba58b739a23
6144:NtWLXS1+0YUv+JfXUZkc7n1IWGWE0IhH6O5RUdAQ:NyXS1+BUWJf+j7n1LshH+


a
b
0001a2e0: 6578 706c 6f72 6572 2e65 7865 0000 0000 explorer.exe....
0001a320: 736d 7373 3332 2e65 7865 0000 0000 0000 smss32.exe.....
0001a360: 7368 656c 6c36 342e 646c 6c00 0000 0000 shell64.dll....
0001a3a0: 7a65 6e67 2e73 6b79 7065 746d 2e63 6f6d zeng.skypetm.com
0001a3b0: 2e74 7700 0000 0000 0000 0000 0000 0000 .tw.....
0001a420: 616e 6975 2e73 6b79 7065 746d 2e63 6f6d aniu.skypetm.com
0001a430: 2e74 7700 0000 0000 0000 0000 0000 0000 .tw.....
0001a4a0: 3131 332e 3130 2e32 3231 2e31 3236 0000 113.10.221.126..
0001a4b0: 0000 0000 0000 0000 0000 0000 0000 0000 ....
0001a520: 5000 0000 901f 0000 bb01 0000 0100 0000 P.....
0001a530: 0200 0000 4d6f 7a69 6c6c 612f 342e 3020 ....Mozilla/4.0
0001a540: 2863 6f6d 7061 7469 626c 653b 204d 5349 (compatible; MSI
0001a550: 4520 362e 303b 2057 696e 646f 7773 204e E 6.0; Windows N
0001a560: 5420 352e 3b20 5356 3129 0000 4142 4344 T 5.; SV1)..ABCD
0001a570: 4546 4748 494a 4b4c 4d4e 4f50 5152 5354 EFGHIJKLMNOPQRST
0001a580: 5556 5758 595a 6162 6364 6566 6768 696a UVWXYZabcdefghij
0001a590: 6b6c 6d6e 6f70 7172 7374 7576 7778 797a klmnopqrstuvwxyz
0001a5a0: 3031 3233 3435 3637 3839 2b2f 3d00 0000 0123456789+/=...
0001a5b0: 4449 5350 4c41 5900 5769 6e57 4d49 2e64 DISPLAY.WinWMI.d
0001a5c0: 6c6c 0000 5c00 0000 2573 3a25 6400 0000 ll..\...%s:%d...
0001a320: 716d 6772 7870 2e65 7865 0000 0000 0000 qmgrxp.exe.....
0001a360: 7061 636b 6574 3634 2e64 6c6c 0000 0000 packet64.dll....
0001a3a0: 6a61 636b 7961 6e64 792e 6176 7374 6f72 jackyandy.avstor
0001a3b0: 652e 636f 6d2e 7477 0000 0000 0000 0000 e.com.tw.....
0001a420: 6368 616e 7865 2e61 7673 746f 7265 2e63 chanxe.avstore.c
0001a430: 6f6d 2e74 7700 0000 0000 0000 0000 0000 om.tw.....
0001a4a0: 6e65 7762 3032 2e73 6b79 7065 746d 2e63 newb02.skypetm.c
0001a4b0: 6f6d 2e74 7700 0000 0000 0000 0000 0000 om.tw.....
0001a520: 5000 0000 bb01 0000 5000 0000 0100 0000 P.....P.....
0001a530: 0200 0000 4d6f 7a69 6c6c 612f 342e 3020 ....Mozilla/4.0
0001a540: 2863 6f6d 7061 7469 626c 653b 204d 5349 (compatible; MSI
0001a550: 4520 362e 303b 2057 696e 646f 7773 204e E 6.0; Windows N
0001a560: 5420 352e 3b20 5356 3129 0000 4142 4344 T 5.; SV1)..ABCD
0001a570: 4546 4748 494a 4b4c 4d4e 4f50 5152 5354 EFGHIJKLMNOPQRST
0001a580: 5556 5758 595a 6162 6364
0001a590: 6b6c 6d6e 6f70 7172 7374
0001a5a0: 3031 3233 3435 3637 3839
0001a5b0: 4449 5350 4c41 5900 5769
0001a5c0: 6c6c 0000 5c00 0000 2573
CIRCL
Computer Incident
Response Center
Luxembourg
ADVANCED
ANALYTICS

The curious case of 1992-06-19 22:22:17

708992537 – 2A425E19h – 10101001000010010111100011001b – 52204570310

UPX? Delphi?!

GOTCHA!!

originalFilename TOP-20

Ever got owned by IEXPLORE.EXE?

	originalFilename	co
1	WLMerger.exe	71
2	IEXPLORE.EXE	44
3	msiexec.exe	34
4	netscp.exe	33
5	MsJavaVM.dll	31
6	Opera.exe	30
7	Uniscribe	30
8	PCMasterSetup.exe	29
9	charmap	27
10	WinWord.exe	24
11	SMAgent.exe	23
12	rundll32.exe	22
13	AMDIDE.SYS	21
14	FlashUtil.exe	21
15	PCMaster.exe	21
16	NTLMSVC.DLL	20
17	Ultra3.sys	20
18	AcroSpeedLaunch.exe	19
19	MSRSAAP.EXE	
20	host.exe	

CIRCL
Computer Incident
Response Center
Luxembourg

GDATA
ADVANCED
ANALYTICS

A Looong-Running Cyber Espionage Operation

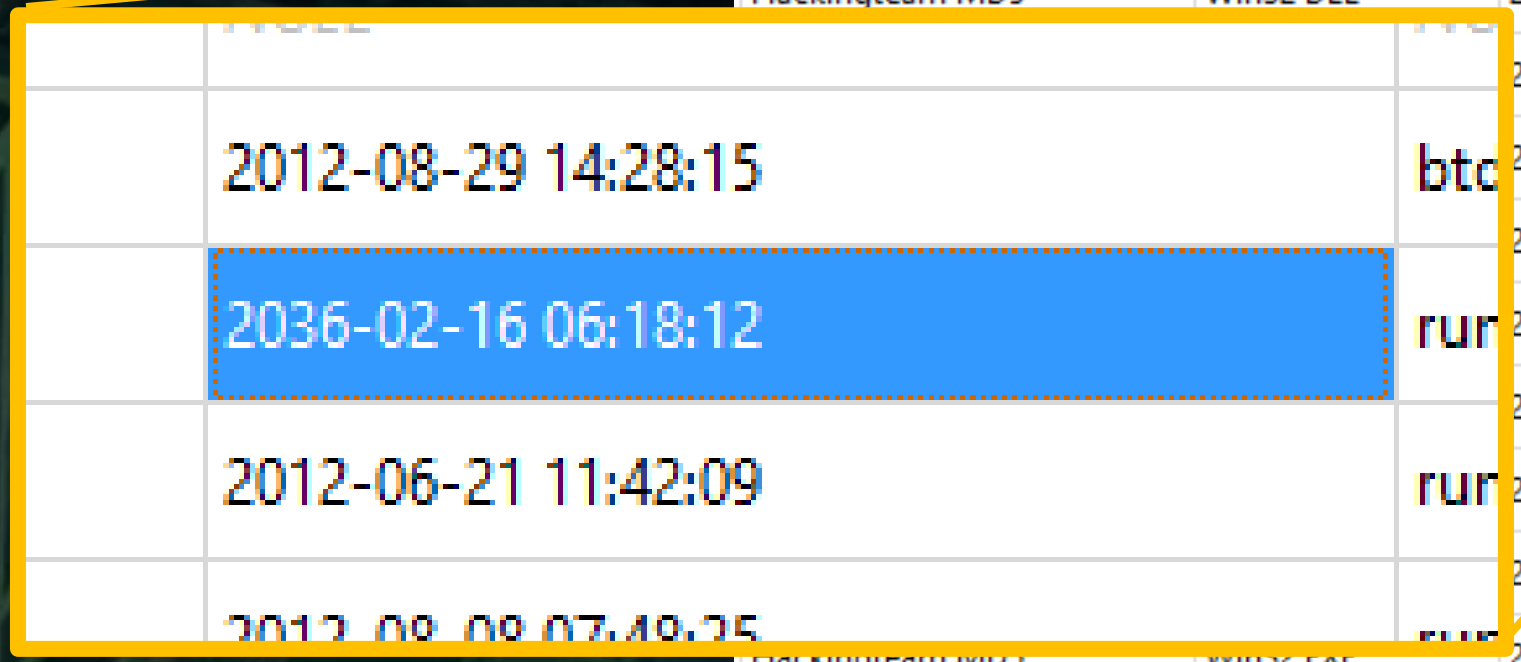
OSINT APT 30 and the Mechanics o a Long-Running Cyber Espionage Operation y FireEye	Win32 EXE	2013-05-31 02:04:39	Launcher.EXE
OSINT APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation by FireEye	Win32 EXE	2013-01-04 03:37:21	Opera.exe
OSINT APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation by FireEye	Win32 EXE	2013-04-16 02:43:43	Launcher.EXE
OSINT APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation by FireEye	Win32 EXE	1996-06-09 04:05:22	MSDEV.EXE
OSINT APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation by FireEye	Win32 EXE	2012-10-18 06:57:23	LiveUpdate.EXE
OSINT APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation by FireEye	Win32 EXE	2011-10-26 07:29:04	ForZRLnkWordDlg.EXE
OSINT APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation by FireEye	Win32 EXE	2007-08-10 01:46:04	
OSINT APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation by FireEye	Win32 EXE	2008-08-25 14:18:37	IEXPLORE.EXE
OSINT APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation by FireEye	Win32 EXE	2010-03-22 01:06:15	IEXPLORE.EXE
OSINT APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation by FireEye	Win32 EXE	2013-01-05 00:23:55	WinWord.exe
OSINT APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation by FireEye	Win32 EXE	2006-09-21 03:25:25	
OSINT APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation by FireEye	Win32 EXE	2009-03-04 12:32:37	msmsgr.exe
OSINT APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation by FireEye	Win32 EXE	2009-12-23 03:39:25	
OSINT APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation by FireEye	Win32 EXE	2013-01-04 03:36:13	

CIRCL
Computer Incident Response Center Luxembourg

GDATA ADVANCED ANALYTICS

ALSO, FAKIN' IT AIN'T EASY...

Hackingteam MD5	RAR	NULL	NULL
Hackingteam MD5	Win32 DLL	2012-08-29 14:28:15	btdll
Hackingteam MD5	Win32 DLL	2036-02-16 06:18:12	rundll
Hackingteam MD5	Win32 DLL	2012-06-21 11:42:09	rundll
		2012-08-08 07:48:25	rundll
		2011-05-11 09:14:10	
		2010-11-08 13:12:07	
		2012-08-02 12:20:05	
		2012-11-29 14:19:57	
		2011-08-30 07:12:51	blank
		2012-12-12 12:36:23	
		2012-11-05 12:18:27	
Hackingteam MD5	Win32 EXE	2012-02-26 10:00:43	



CIRCL Computer Incident Response Center Luxembourg

GDATA ADVANCED ANALYTICS

Cyber Espionage Operators Sandworm Team Leverage CVE-2014-4114 Zero-Day - Sandworm (RU)	None	2012-04-06 07:30:10	CHMView.exe
Cyber Espionage Operators Sandworm Team Leverage CVE-2014-4114 Zero-Day - Sandworm (RU)	None	NULL	NULL
Cyber Espionage Operators Sandworm Team Leverage CVE-2014-4114 Zero-Day - Sandworm (RU)	PPSX	NULL	NULL
Cyber Espionage Operators Sandworm Team Leverage CVE-2014-4114 Zero-Day - Sandworm (RU)	Win32 EXE	1970-01-01 00:00:00	host.exe
Cyber Espionage Operators Sandworm Team Leverage CVE-2014-4114 Zero-Day - Sandworm (RU)	Win32 EXE	1970-01-01 00:00:00	msiexec.exe
Cyber Espionage Operators Sandworm Team Leverage CVE-2014-4114 Zero-Day - Sandworm (RU)	Win32 EXE	1970-01-01 00:00:00	msiexec.exe
Cyber Espionage Operators Sandworm Team Leverage CVE-2014-4114 Zero-Day - Sandworm (RU)	Win32 EXE	1970-01-01 00:00:00	msiexec.exe
Cyber Espionage Operators Sandworm Team Leverage CVE-2014-4114 Zero-Day - Sandworm (RU)	Win32 EXE	1970-01-01 00:00:00	msiexec.exe
Cyber Espionage Operators Sandworm Team Leverage CVE-2014-4114 Zero-Day - Sandworm (RU)	ZIP	NULL	NULL

… and carelessness leaks information.

BACK TO SERIOUS.

http://twentytwowords.com/wp-content/uploads/Serious-Dog-Portraits-01-685x456.jpg

CIRCL
Computer Incident
Response Center
Luxembourg

G DATA
ADVANCED
ANALYTICS

OMFG!! THEY USED E.X.P.L.O.I.T.S.!!!!

According to MISP data:

Of 326 identified events,
54 knowingly include exploits
(according to MS detections 68)

CIRCL
Computer Incident
Response Center
Luxembourg

GDATA
ADVANCED
ANALYTICS

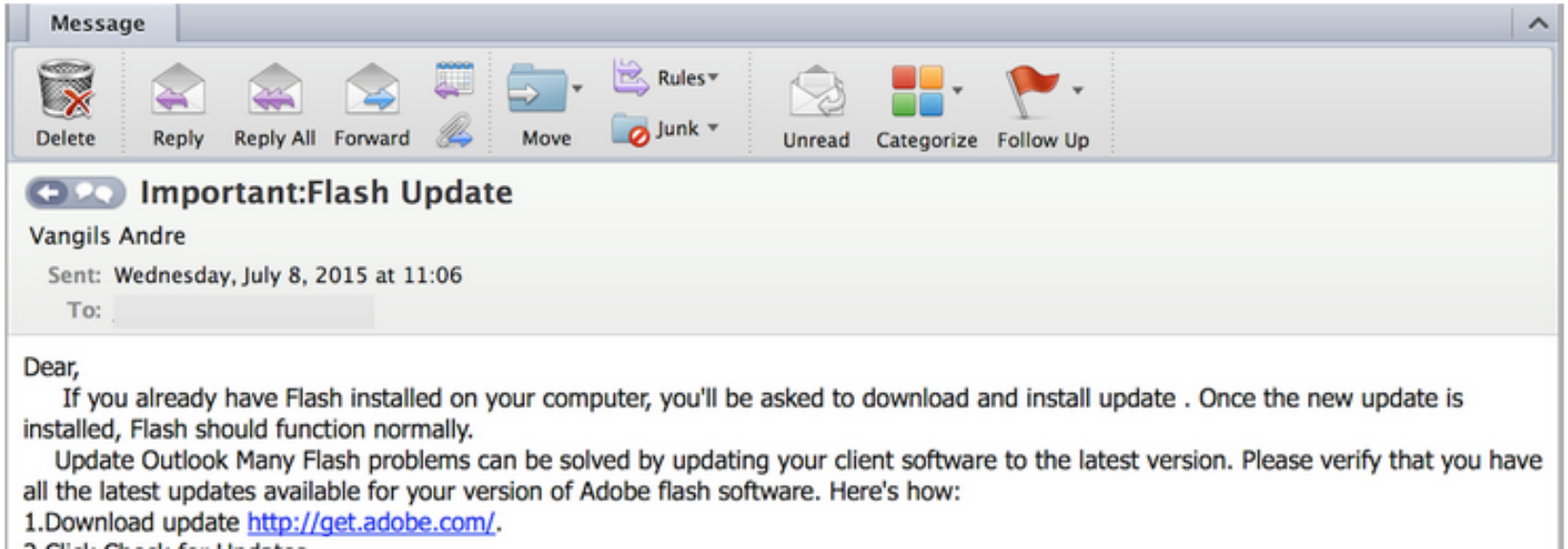
APT Group Wekby Leveraging Adobe Flash Exploit (CVE-2015-5119)

Posted on July 8, 2015 by Steven Adair

As if the recent breach and subsequent public data dump involving the Italian company Hacking Team wasn't bad enough, it all gets just a little bit worse. Emerging from the bowels of Hacking Team data dump was a Flash 0-day exploit (CVE-2015-5119) that was just patched today by Adobe as covered in APSB15-16. The exploit has since been added into the Angler Exploit Kit and integrated into Metasploit. However, not to be out done, APT attackers have also started leveraging the exploit in targeted spear phishing attacks as well. Before we start dishing the details, there is going to be one main takeaway from this blog post: If you haven't already, update/patch your Adobe Flash now.

Spear Phishing

This morning, a well known APT threat group, often referred to as **Wekby,** kicked off a rather ironic spear phishing campaign. The attackers launched spoofed e-mail messages purporting to be from **Adobe**. The e-mail messages references an Adobe Flash update and encourage the recipients to click a link to download and install the update. Take a look at an example of the spear phish e-mail message below.



HACKING TEAM EXPLOITS GONE WILD

CIRCL Computer Incident Response Center Luxembourg

G DATA ADVANCED ANALYTICS

CVE-2015-5119 rockin da charts

Group Wekby	reported 07/2015
Spearphish campaign targeting US government	reported 07/2015
BlueTermite APT	reported 08/2015
BlackEnergy	reported 01/2016

CIRCL
Computer Incident Response Center Luxembourg
G DATA ADVANCED ANALYTICS

CVE-2012-0158	23	CVE-2011-3544	1	CVE-2014-0322	1
CVE-2014-1761	6	CVE-2011-4369	1	CVE-2014-0502	1
CVE-2015-5119	5	CVE-2012-1723	1	CVE-2014-4113	1
CVE-2013-3906	3	CVE-2012-1856	1	CVE-2014-6332	1
CVE-2014-4114	3	CVE-2012-4792	1	CVE-2014-6352	1
CVE-2013-0634	2	CVE-2012-5054	1	CVE-2015-1701	1
CVE-2013-2423	2	CVE-2012-6422	1	CVE-2015-1770	1
CVE-2015-5122	2	CVE-2013-0640	1	CVE-2015-2502	1
CVE-2010-0738	1	CVE-2013-1347	1	CVE-2015-2590	1
CVE-2010-3333	1	CVE-2013-2465	1	CVE-2015-3113	1
CVE-2011-0611	1	CVE-2013-2551	1		

32 Vulnerabilities

popped up in 54 ouf of 326 events

CIRCL
Computer Incident
Response Center
Luxembourg

GDATA
ADVANCED
ANALYTICS

SOPHISTICATION

Or, what the RE gotta tell you

Difficulties by:

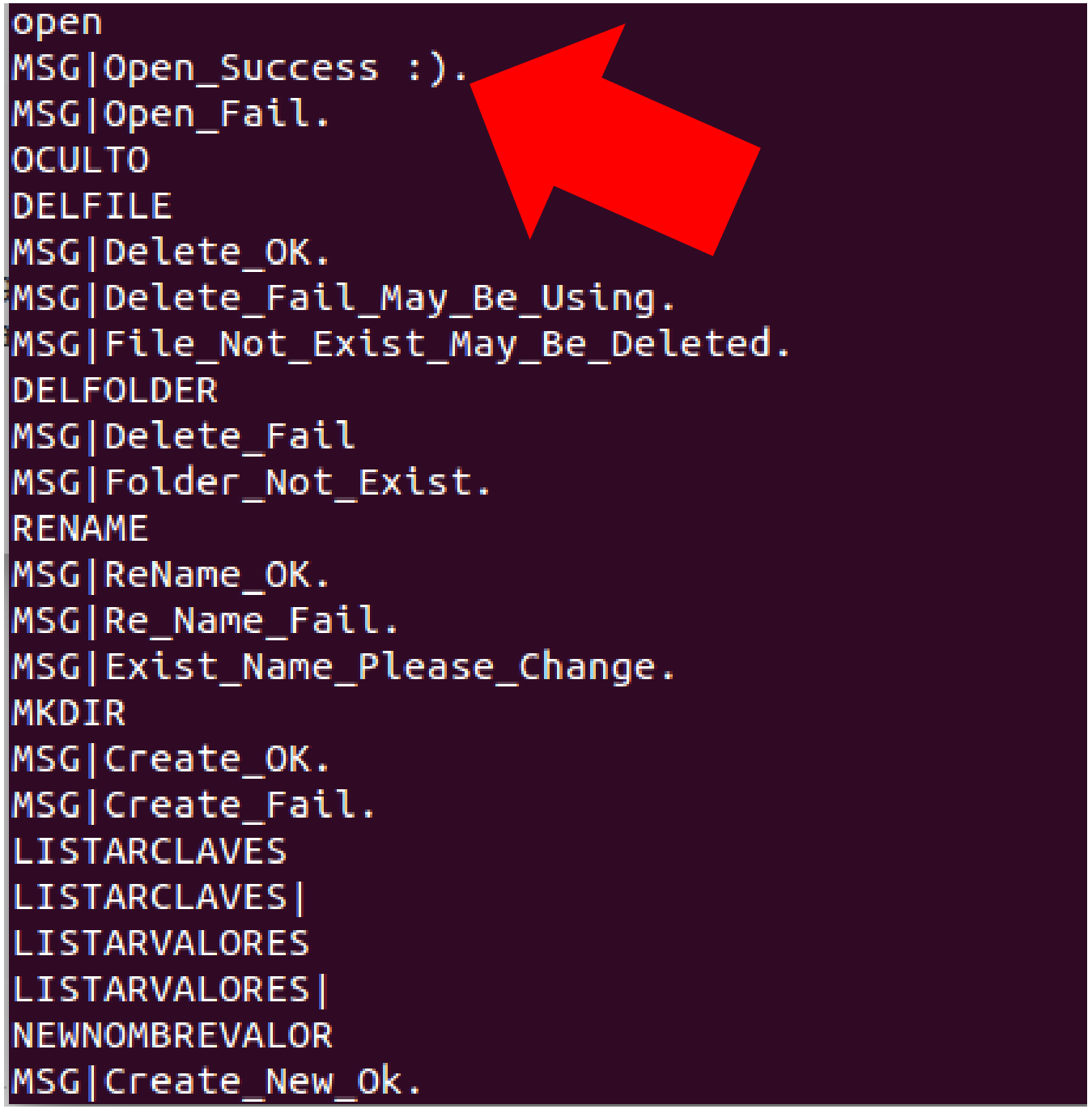
obfuscation, packers, plug-ins & missing components, exotic platforms/code, virtual machines, VB6, serious software engineering (e.g. C++ like they mean it)

Not measures of sophistication:

how long the RAT was on the network, number of data records stolen, number of different malware samples, the fact that someone wrote a RAT just for one target

Signs of advanced adversary:

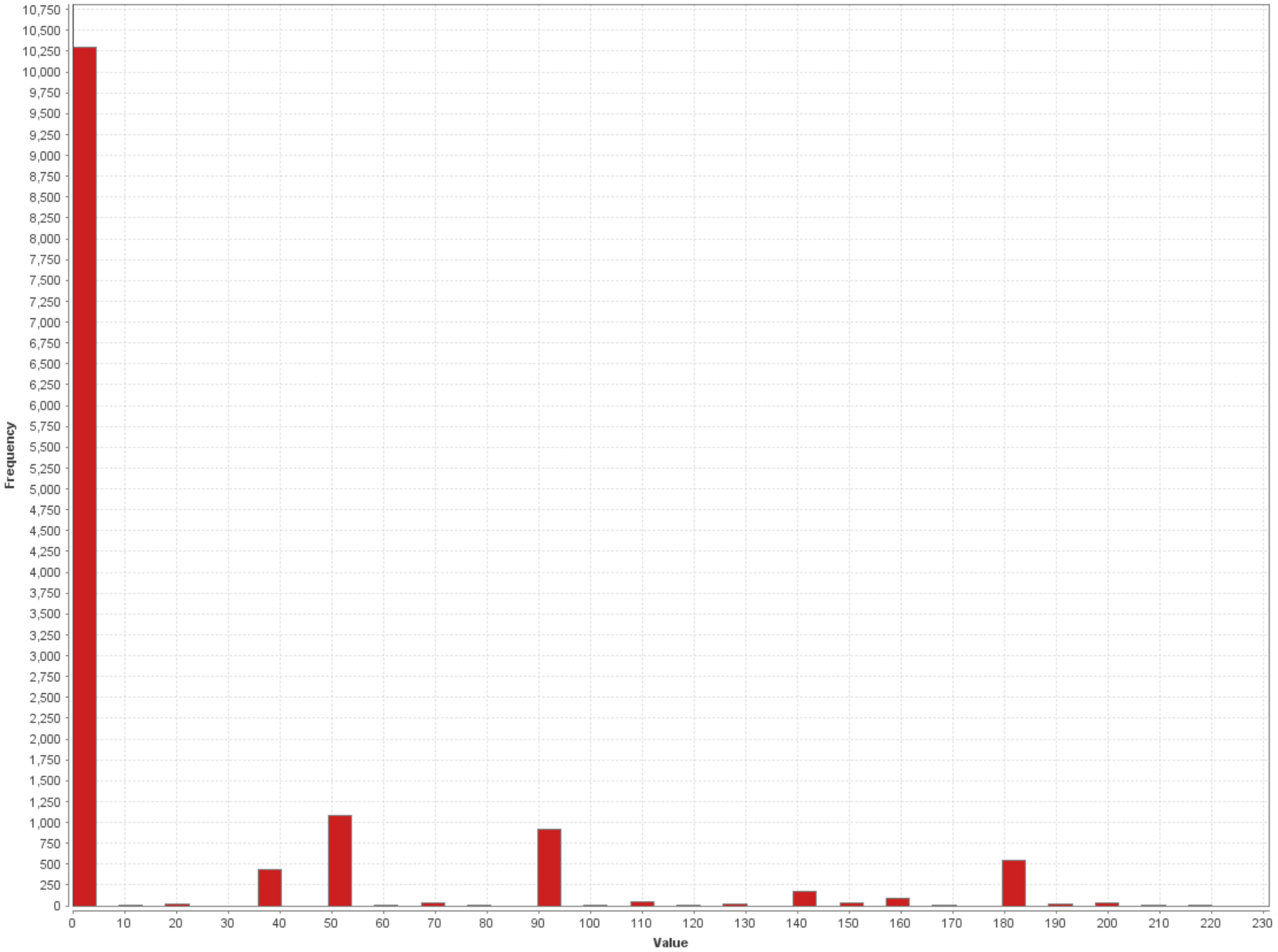
complexity of malware, or, how much money went into development in ratio with how many machines were infected



As long as your attacker is still smiley-ing, things are all ok, right? Right?!

CIRCL Computer Incident Response Center Luxembourg

G DATA ADVANCED ANALYTICS



Packers and Crypters

CIRCL
Computer Incident
Response Center
Luxembourg

GDATA | ADVANCED ANALYTICS

HUH..?

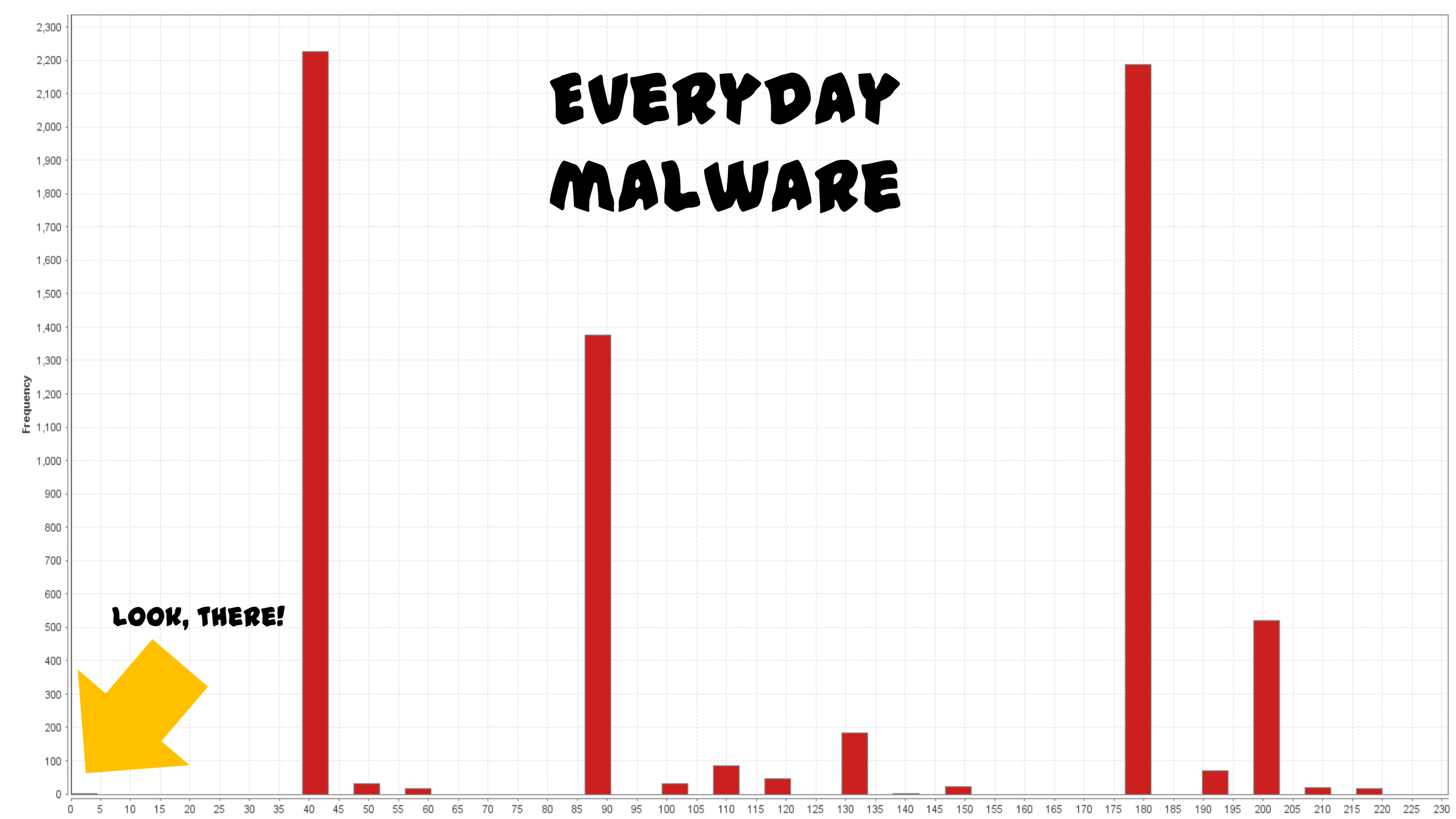
Packer Detection Like PEiD Was Broken™

Evaluation based on:

- EP section name abnormal
- EP section entropy too high/low
- Section 0 entropy too high/low
- API calls / KB ratio
- Section count too low
- Imphash missing

CIRCL
Computer Incident
Response Center
Luxembourg

ADVANCED
ANALYTICS


EVERYDAY MALWARE
LOOK, THERE!
Frequency
2,300
2,200
2,100
2,000
1,900
1,800
1,700
1,600
1,500
1,400
1,300
1,200
1,100
1,000
900
800
700
600
500
400
300
200
100
0
0 5 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 85 90 95 100 105 110 115 120 125 130 135 140 145 150 155 160 165 170 175 180 185 190 195 200 205 210 215 220 225 230

Sophistication

Or, why your attackers aren‘t too smart

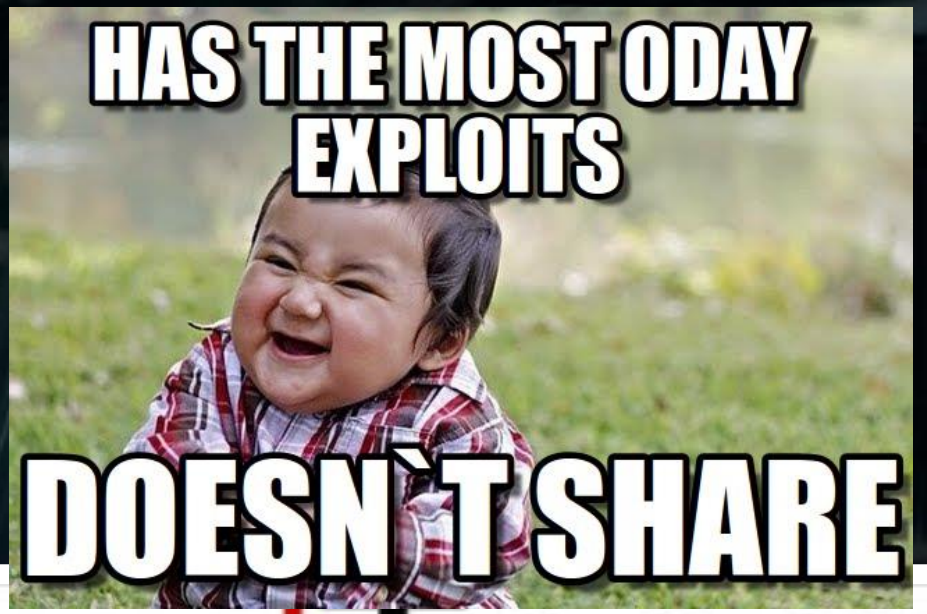
and.. why they don‘t even need to

The cosy comfort of using commodity RATs

Writing malware is not easy^Wcheap :(

Lets buy it! :)

A business legit companies jumped on as well



]Hacked Team[

PACKRAT

Seven years of a South-American threat actor, living on recycled RATs

Targeting journalists, parliamentarians, public figures; among others, Alberto Nisman

Ecuador, Venezuela, Argentina, Brazil

Malware of preference:

- CyberGate
- XTremeRAT
- AlienSpy

http://b[illegible]rensztein.com/wp-content/uploads/2015/02/0000390908-750x400.jpg

https://upload.wikimedia.org/wikipedia/commons/a/a8/Desert_Packrat_%28Neotoma_lepida%29_[illegible]_peanut.jpg

Computer Incident Response Center Luxembourg

G DATA | ADVANCED ANALYTICS

Microsoft Defender, because great naming

Re-naming, because Microsoft

DarkComet (Fynloski)

BlackShades (Bladabindi)

Adwind

PlugX

PoisonIvy (Poison)

XTremeRAT (Xtrat)

DIY APTs...?

CIRCL
Computer Incident
Response Center
Luxembourg

GDATA
ADVANCED
ANALYTICS

PLUGX

The king of lazy APTing

	ID	EventTag	SampleCount
1	837	OSINT I Know You Want Me - Unplugging PlugX fro...	59
2	623	OSINT - Operation SMN (Novetta)	19
3	2494	OSINT Bookworm Trojan: A Model of Modular Archit...	17
4	1918	PlugX Additional Updated Indicators	9
5	1201	OSINT Attacks on East Asia using Google Code for Co...	6
6	507	OSINT Operation Poisoned Hurricane blog post by Fir...	6
7	1740	OSINT Revealing the Cyber-Kraken (Threat Group 339...	5
8	2365	PlugX - additional samples via PhysicalDrive0 + CIRC...	4
9	1660	FBI Flash - A-000063-MW	3
10	1739	OSINT Technical Analysis Tracks the Sakula Malware ...	2
11	1649	Second Adobe Flash Zero-Day CVE-2015-5122 from H...	1
12	1658	OSINT Black Vine: Formidable cyberespionage group ...	1
13	2116	OSINT Threat Research Team Goes ??eyond the Exploi...	1
14	2253	OSINT - Chinese Actors Use ??102??Malware in Attack...	1
15	943	Operation GreedyWonk - Flash Zero-Day Exploit	1

CIRCL Computer Incident Response Center Luxembourg

G DATA ADVANCED ANALYTICS

Adwind	385 Samples	8 Events
DarkComet (aka. Fynloski)	29 Samples	5 Events
PoisonIvy (aka. Poison)	78 Samples	14 Events
XtremeRAT (aka. Xtrat)	21 Samples	5 Events
njRAT (aka. Bladabindi)	46 Samples	6 Events
HandpickedRATs	71 Samples	26 Events
Sample base (pre-sorted)	8927 Samples	326 Events

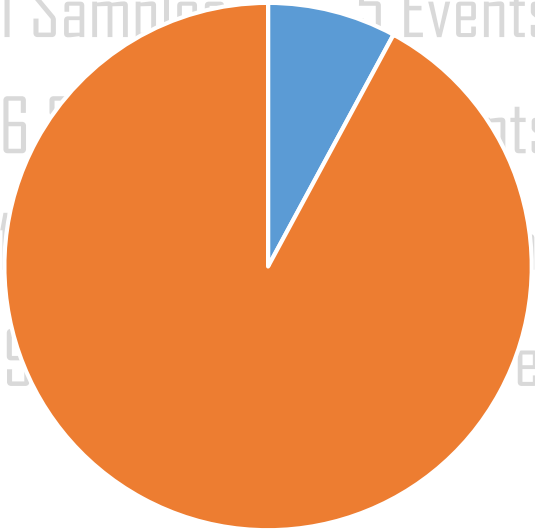
THE REST OF THE PACK

CIRCL Computer Incident Response Center Luxembourg

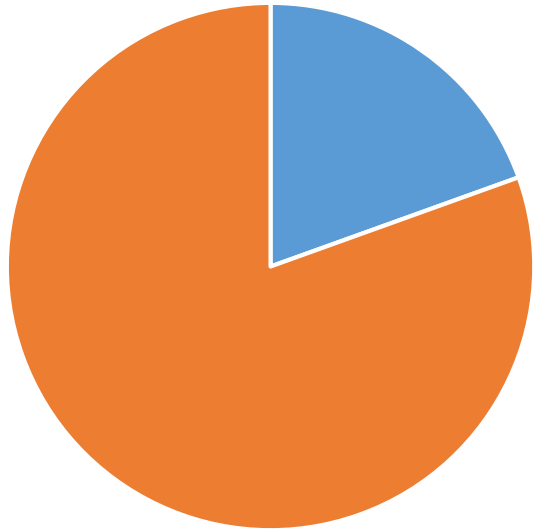
GDATA ADVANCED ANALYTICS

DATA GOES WELL WITH PIE!

Samples



Events



THE REST OF THE PACK

CIRCL Computer Incident Response Center Luxembourg

G DATA ADVANCED ANALYTICS

CORRELATIONS

Sakula/BlackVine related to ScanBox, DeepPanda and „The French Connection“

„Attacks on Civil Society Organizations“ and „APT targeting Journalists/Activists in Tibet“

ScarletMimic and TerminatorRAT report

PoisonedHandover, Poisoned Hurricane, „Attacks East Asia“ and Operation SMN

Spearphishing campaign from 2012 links to APT1

PittyTiger links to malicious RTF spearphishing event from 2014

The Dukes and Hammertoss

„Targeting of Civil Society Organizations“ and Mutter and NETTRAVELER report

„PlugX in Russa“ and „Korplug military targeted attacks in Afghanistan/Tajikistan“

RedOctober and Inception Framework

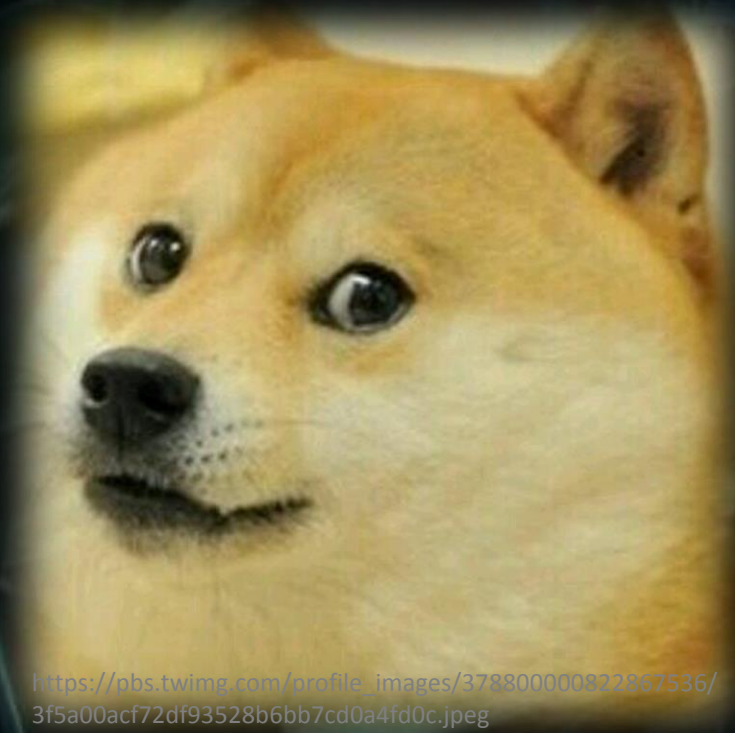
And many many many many more .....

CIRCL
Computer Incident
Response Center
Luxembourg

G DATA | ADVANCED ANALYTICS

Actor Tracking

- Operation BlockBuster (Sony)
  - Linked to Operation Troy
    - reported 2012
    - „Cyberespionage in South Korea“
  - Linked to „Duuzer back door Trojan targets South Korea to take over computers“
    - reported 10/2015
    - note, South Korea..



https://pbs.twimg.com/profile_images/378800000822867536/3f5a00acf72df93528b6bb7cd0a4fd0c.jpeg

- TurboCampaign
  - is actually Shell_Crew, reported 2014
  - just now, they feature a 64-bit Derusbi for Linux gadget

CIRCL Computer Incident Response Center Luxembourg

G DATA ADVANCED ANALYTICS

Frenemies & the Fungus Amongus

Or: When Malware Became Intellectual Property

CIRCL
Computer Incident Response Center Luxembourg

G DATA ADVANCED ANALYTICS

NAMING IS HARD

Havex

EnergeticBear

DragonFly

CrouchingYeti

NAMING IS HARD

White Elephant

Targeted Malware Attacks against NGO Linked to Attacks on Burmese Government Websites

Seven Pointed Dagger

CIRCL Computer Incident Response Center Luxembourg

GDATA ADVANCED ANALYTICS

NAMING IS HARD

Sakula

BlackVine

CIRCL Computer Incident Response Center Luxembourg

GDATA ADVANCED ANALYTICS

FUTURE RESEARCH

Implementing the manual correlating into MISP

Use MISP as a verified dataset to classify unknown samples

Provide bloomfilters of the MISP attributes

Do more classifications on more attributes

Get your own MISP account and investigate! (jump at Raphael after the talk...)

THANK YOU!!

raphael.vinot@circl.lu
@rafi0t
marion.marschalek@gdata-adan.de
@pinkflawd

RAPHAËL

MARION

CIRCL
Computer Incident
Response Center
Luxembourg

GDATA
ADVANCED
ANALYTICS

http://img14.deviantart.net/75a7/i/2011/229/9/6/ghost_in_the_shell_wallpaper_by_mobiuszeroone-d46y1xt.jpg

References

https://www.virusbulletin.com/virusbulletin/2015/11/optimizing-ssdeep-use-scale

https://github.com/circl/ssdc

http://blog.shadowserver.org/2015/08/10/the-italian-connection-an-analysis-of-exploit-supply-chains-and-digital-quartermasters/

https://citizenlab.org/2015/12/packrat-report/

http://www.crowdstrike.com/blog/french-connection-french-aerospace-focused-cve-2014-0322-attack-shares-similarities-2012/index.html

http://www.crowdstrike.com/blog/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors/

http://www.arbornetworks.com/blog/asert/uncovering-the-seven-pointed-dagger/

http://www.arbornetworks.com/blog/asert/defending-the-white-elephant/

https://citizenlab.org/2015/10/targeted-attacks-ngo-burma/

http://www.symantec.com/connect/blogs/black-vine-formidable-cyberespionage-group-targeted-aerospace-healthcare-2012

https://www.secureworks.com/research/sakula-malware-family

CIRCL
Computer Incident
Response Center
Luxembourg

GDATA | ADVANCED ANALYTICS

http://img14.deviantart.net/75a7/i/2011/229/9/6/ghost_in_the_shell_wallpaper_by_mobiuszeroone-d46y1xt.jpg