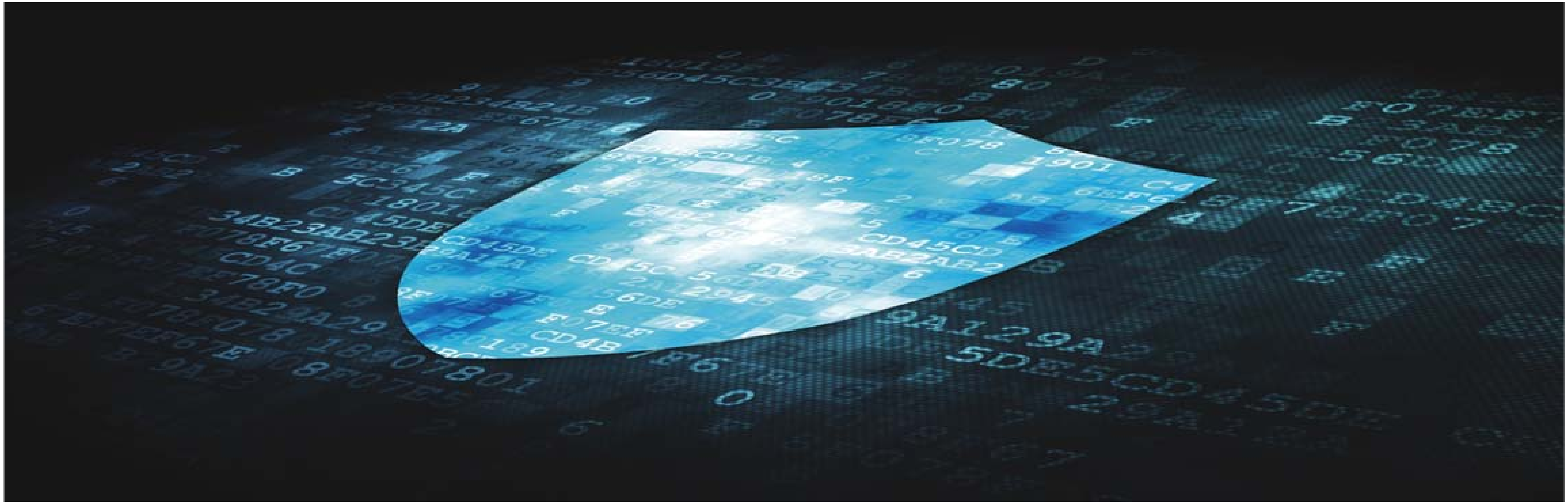
malpedia

Daniel Plohmann
daniel.plohmann@fkie.fraunhofer.de

@push_pnx
@malpedia



$whoami
Daniel Plohmann

- Security Researcher @ Fraunhofer (Europe‘s largest organisation for applied research)
- PhD Candidate @ University of Bonn

- Research Scope:
  - Malware Analysis / Reverse Engineering / Automation

- Things I do and like:

RE tooling
(IDAscope, …)

70m+ DGA domains
➔ free data&feeds!

This talk! :)

The

Malware Knowledge Archipelago

The Malware Knowledge Archipelago

A typical situation

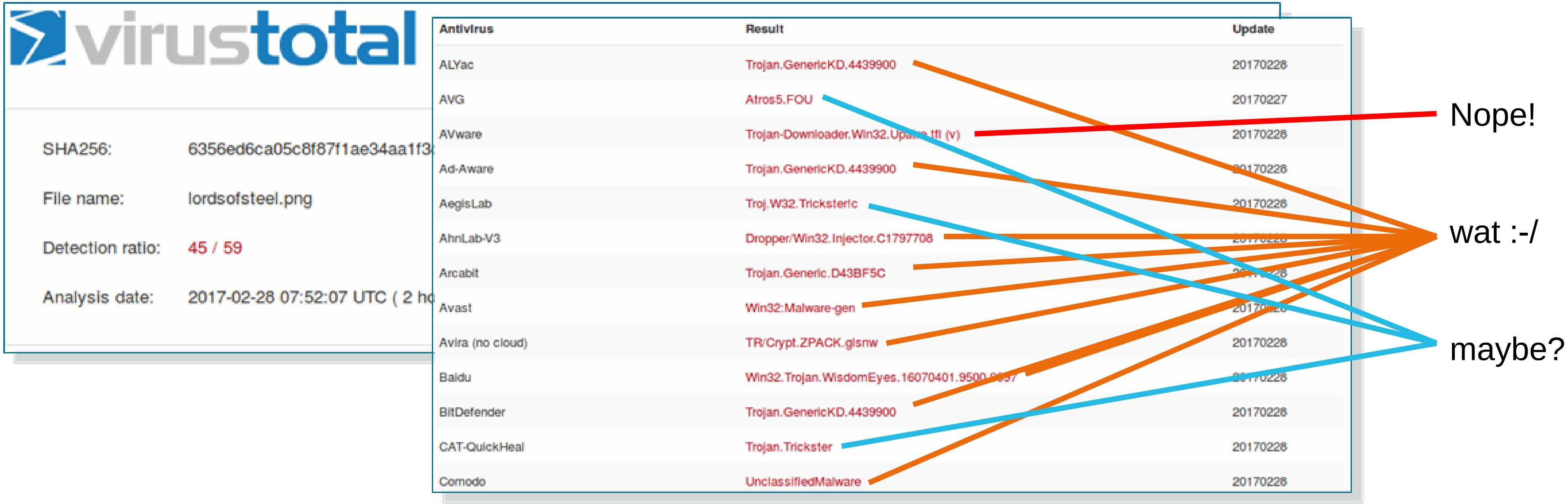
The Malware Knowledge Archipelago

A typical situation

- Your [spam protection, HTTP proxy, HIPS, …] intercepts a potential malware sample.
  - You want to know what it is.

The Malware Knowledge Archipelago
A typical situation

- Your [spam protection, HTTP proxy, HIPS, …] intercepts a potential malware sample.
  - You upload it to VirusTotal:



SHA256: 6356ed6ca05c8f87f1ae34aa1f3

File name: lordsofsteel.png

Detection ratio: 45 / 59

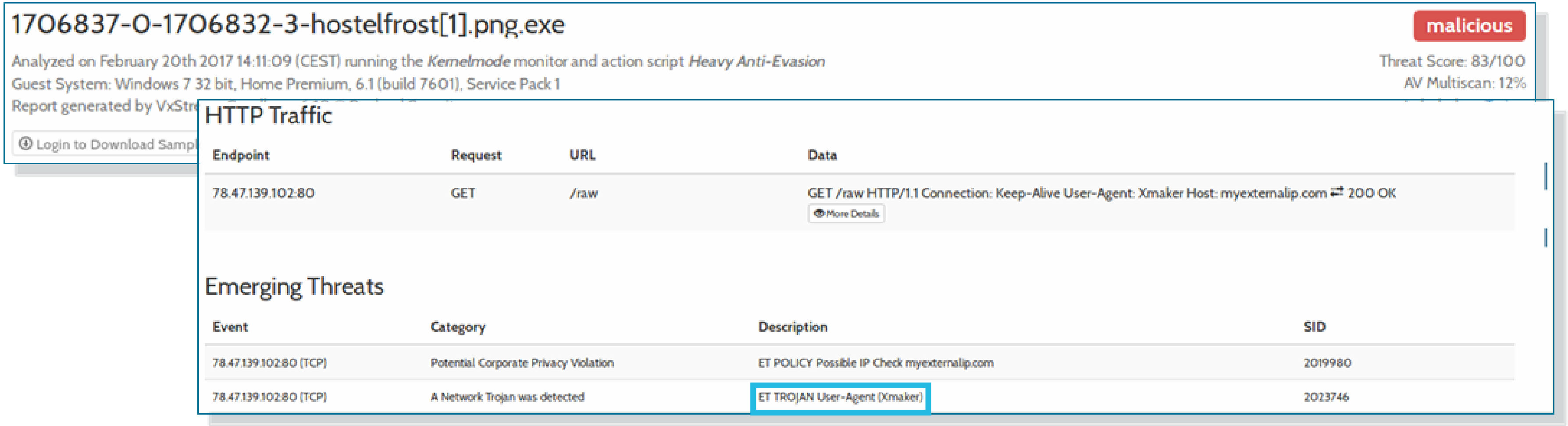
Analysis date: 2017-02-28 07:52:07 UTC (2 ho

Antivirus	Result	Update
ALYac	Trojan.GenericKD.4439900	20170228
AVG	Atros5.FOU	20170227
AVware	Trojan-Downloader.Win32.Upatre.tfl (v)	20170228
Ad-Aware	Trojan.GenericKD.4439900	20170228
AegisLab	Troj.W32.Tricksteric	20170228
AhnLab-V3	Dropper/Win32.Injector.C1797708	20170228
Arcabit	Trojan.Generic.D43BF5C	20170228
Avast	Win32:Malware-gen	20170228
Avira (no cloud)	TR/Crypt.ZPACK.glsnw	20170228
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9997	20170228
BitDefender	Trojan.GenericKD.4439900	20170228
CAT-QuickHeal	Trojan.Trickster	20170228
Comodo	UnclassifiedMalware	20170228

[1] https://www.virustotal.com/en/file/6356ed6ca05c8f87f1ae34aa1f3c4a119c5b6e811b00cb996ba688cc6695f683/analysis/

The Malware Knowledge Archipelago
A typical situation

- Your [spam protection, HTTP proxy, HIPS, …] intercepts a potential malware sample.
  - You upload it to VirusTotal:-/
  - You upload it to a sandbox (like hybrid-analysis.com):-/



1706837-0-1706832-3-hostelfrost[1].png.exe

Analyzed on February 20th 2017 14:11:09 (CEST) running the *Kernelmode* monitor and action script *Heavy Anti-Evasion*
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1
Report generated by VxStre

Threat Score: 83/100
AV Multiscan: 12%

HTTP Traffic

Endpoint	Request	URL	Data
78.47.139.102:80	GET	/raw	GET /raw HTTP/1.1 Connection: Keep-Alive User-Agent: Xmaker Host: myexternalip.com ⇄ 200 OK

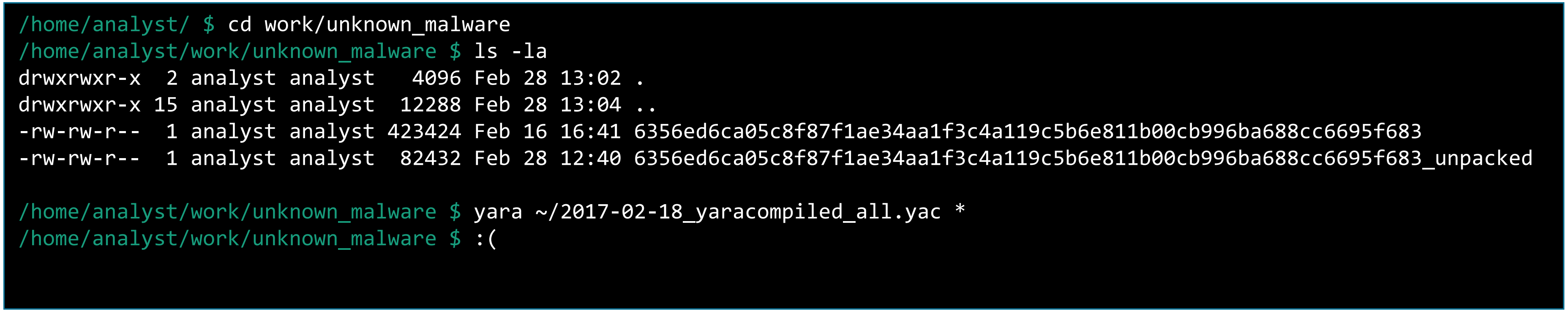
Emerging Threats

Event	Category	Description	SID
78.47.139.102:80 (TCP)	Potential Corporate Privacy Violation	ET POLICY Possible IP Check myexternalip.com	2019980
78.47.139.102:80 (TCP)	A Network Trojan was detected	ET TROJAN User-Agent (Xmaker)	2023746

[1] https://www.hybrid-analysis.com/sample/6356ed6ca05c8f87f1ae34aa1f3c4a119c5b6e811b00cb996ba688cc6695f683?environmentId=100

The Malware Knowledge Archipelago
A typical situation

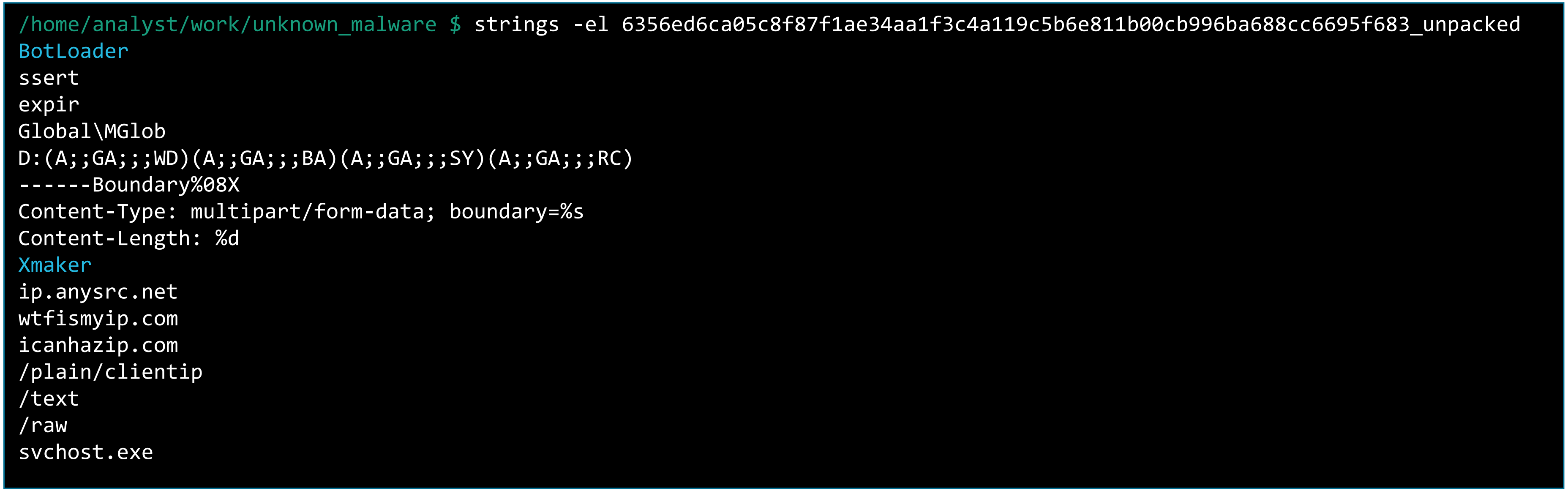
- Your [spam protection, HTTP proxy, HIPS, …] intercepts a potential malware sample.
  - So you ask your friend$^{\text{TM}}$ to unpack it and throw your wool hank of yara signatures on it:



```
/home/analyst/ $ cd work/unknown_malware
/home/analyst/work/unknown_malware $ ls -la
drwxrwxr-x  2 analyst analyst   4096 Feb 28 13:02 .
drwxrwxr-x 15 analyst analyst  12288 Feb 28 13:04 ..
-rw-rw-r--  1 analyst analyst 423424 Feb 16 16:41 6356ed6ca05c8f87f1ae34aa1f3c4a119c5b6e811b00cb996ba688cc6695f683
-rw-rw-r--  1 analyst analyst  82432 Feb 28 12:40 6356ed6ca05c8f87f1ae34aa1f3c4a119c5b6e811b00cb996ba688cc6695f683_unpacked

/home/analyst/work/unknown_malware $ yara ~/2017-02-18_yaracompiled_all.yac *
/home/analyst/work/unknown_malware $ :(
```

The Malware Knowledge Archipelago
A typical situation

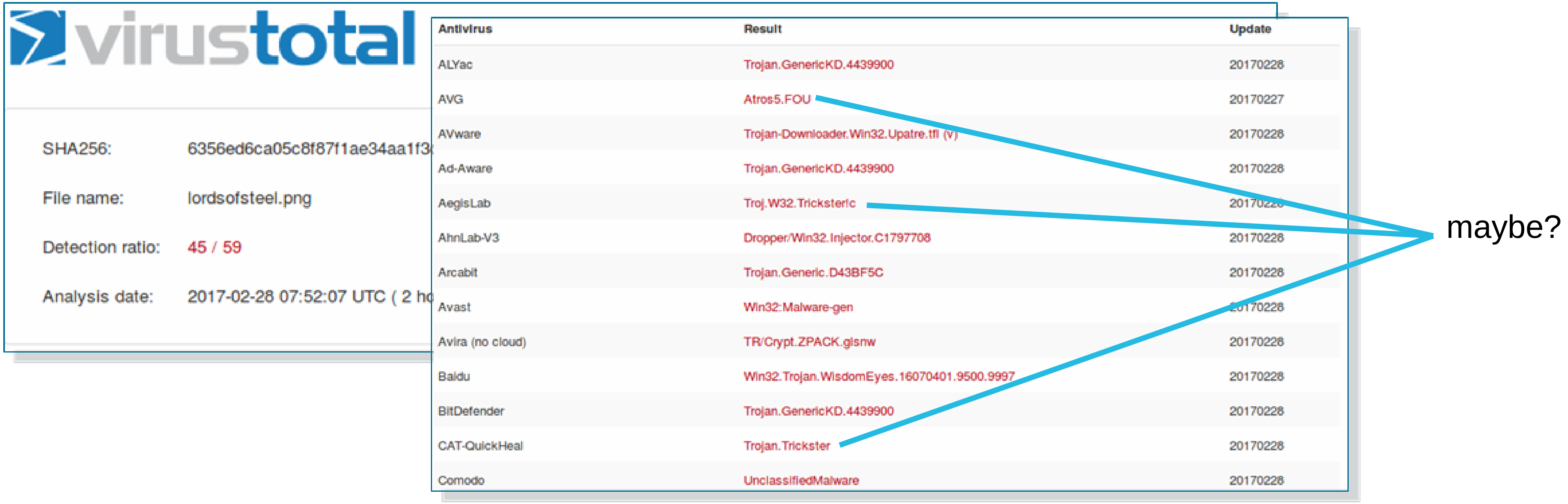
- Your [spam protection, HTTP proxy, HIPS, …] intercepts a potential malware sample.
  - Strings / Hex Editor?



```
/home/analyst/work/unknown_malware $ strings -el 6356ed6ca05c8f87f1ae34aa1f3c4a119c5b6e811b00cb996ba688cc6695f683_unpacked
BotLoader
ssert
expir
Global\MGlob
D:(A;;GA;;;WD)(A;;GA;;;BA)(A;;GA;;;SY)(A;;GA;;;RC)
------Boundary%08X
Content-Type: multipart/form-data; boundary=%s
Content-Length: %d
Xmaker
ip.anysrc.net
wtfismyip.com
icanhazip.com
/plain/clientip
/text
/raw
svchost.exe
```

The Malware Knowledge Archipelago
A typical situation

- Your [spam protection, HTTP proxy, HIPS, …] intercepts a potential malware sample.
  - You remember VirusTotal gave you some hints:



SHA256: 6356ed6ca05c8f87f1ae34aa1f3

File name: lordsofsteel.png

Detection ratio: 45 / 59

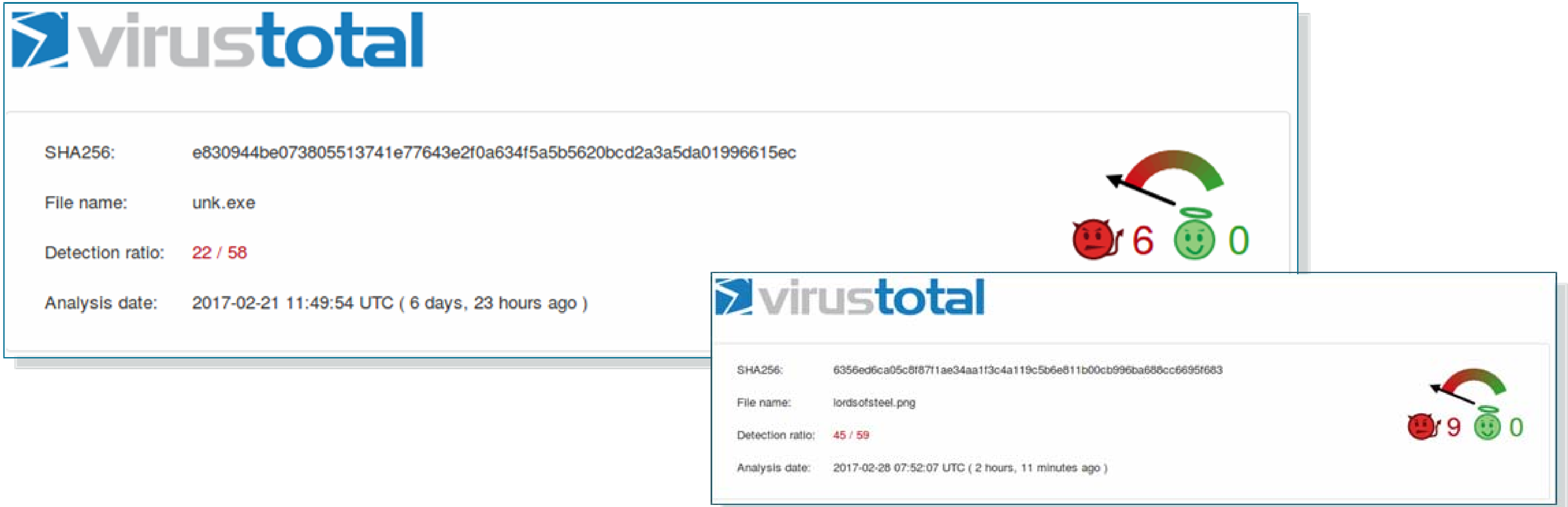
Analysis date: 2017-02-28 07:52:07 UTC (2 ho

Antivirus	Result	Update
ALYac	Trojan.GenericKD.4439900	20170228
AVG	Atros5.FOU	20170227
AVware	Trojan-Downloader.Win32.Upatre.tfl (v)	20170228
Ad-Aware	Trojan.GenericKD.4439900	20170228
AegisLab	Troj.W32.Trickster!c	20170228
AhnLab-V3	Dropper/Win32.Injector.C1797708	20170228
Arcabit	Trojan.Generic.D43BF5C	20170228
Avast	Win32:Malware-gen	20170228
Avira (no cloud)	TR/Crypt.ZPACK.gisnw	20170228
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9997	20170228
BitDefender	Trojan.GenericKD.4439900	20170228
CAT-QuickHeal	Trojan.Trickster	20170228
Comodo	UnclassifiedMalware	20170228

maybe?

The Malware Knowledge Archipelago
A typical situation

- Your [spam protection, HTTP proxy, HIPS, …] intercepts a potential malware sample.
  - Eventually, you re-upload the now unpacked sample to VirusTotal:



SHA256: e830944be073805513741e77643e2f0a634f5a5b5620bcd2a3a5da01996615ec

File name: unk.exe

Detection ratio: 22 / 58

Analysis date: 2017-02-21 11:49:54 UTC (6 days, 23 hours ago)

SHA256: 6356ed6ca05c8f87f1ae34aa1f3c4a119c5b6e811b00cb996ba688cc6695f683

File name: lordsofsteel.png

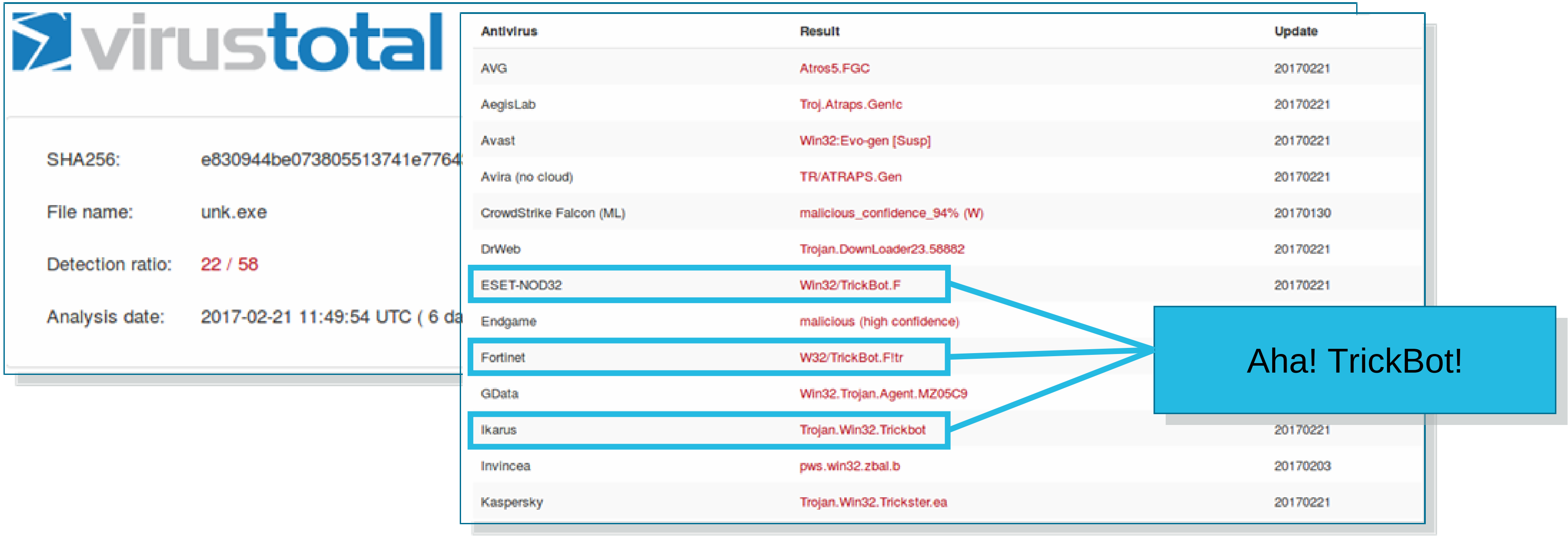
Detection ratio: 45 / 59

Analysis date: 2017-02-28 07:52:07 UTC (2 hours, 11 minutes ago)

[1] https://www.virustotal.com/en/file/6356ed6ca05c8f87f1ae34aa1f3c4a119c5b6e811b00cb996ba688cc6695f683/analysis/

The Malware Knowledge Archipelago
A typical situation

- Your [spam protection, HTTP proxy, HIPS, …] intercepts a potential malware sample.
  - Eventually, you re-upload the now unpacked sample to VirusTotal:



SHA256: e830944be073805513741e7764

File name: unk.exe

Detection ratio: 22 / 58

Analysis date: 2017-02-21 11:49:54 UTC (6 da

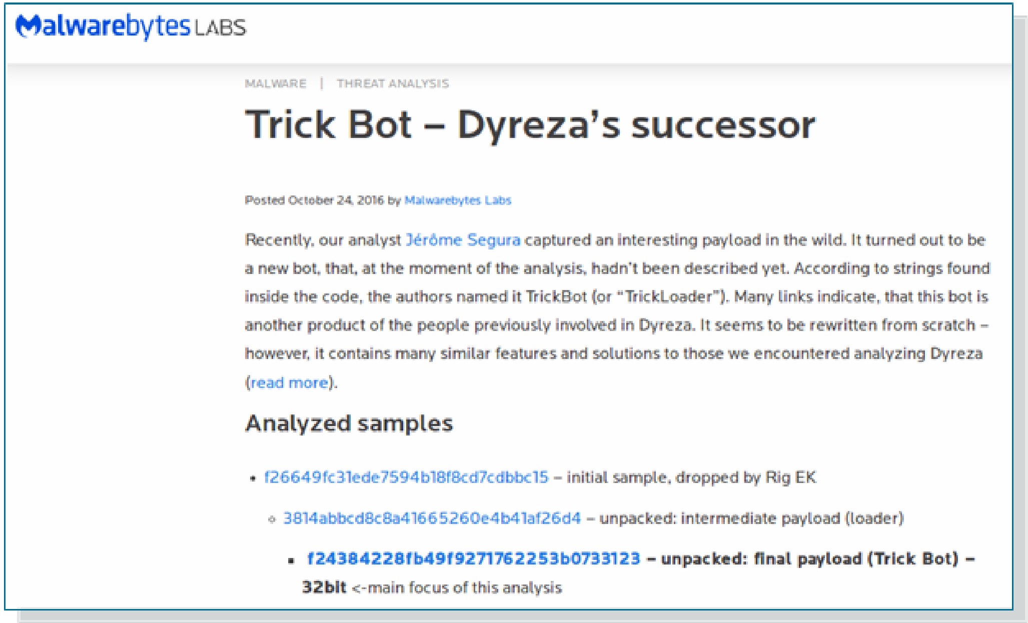
Antivirus	Result	Update
AVG	Atros5.FGC	20170221
AegisLab	Troj.Atraps.Gen!c	20170221
Avast	Win32:Evo-gen [Susp]	20170221
Avira (no cloud)	TR/ATRAPS.Gen	20170221
CrowdStrike Falcon (ML)	malicious_confidence_94% (W)	20170130
DrWeb	Trojan.DownLoader23.58882	20170221
ESET-NOD32	Win32/TrickBot.F	20170221
Endgame	malicious (high confidence)	
Fortinet	W32/TrickBot.Fltr	
GData	Win32.Trojan.Agent.MZ05C9	
Ikarus	Trojan.Win32.Trickbot	20170221
Invincea	pws.win32.zbal.b	20170203
Kaspersky	Trojan.Win32.Trickster.ea	20170221

Aha! TrickBot!

[1] https://www.virustotal.com/en/file/6356ed6ca05c8f87f1ae34aa1f3c4a119c5b6e811b00cb996ba688cc6695f683/analysis/

The Malware Knowledge Archipelago
A typical situation

- Your [spam protection, HTTP proxy, HIPS, …] intercepts a potential malware sample.
  - You google it and happyness ensues:



MALWARE | THREAT ANALYSIS

Trick Bot – Dyreza's successor

Posted October 24, 2016 by Malwarebytes Labs

Recently, our analyst Jérôme Segura captured an interesting payload in the wild. It turned out to be a new bot, that, at the moment of the analysis, hadn't been described yet. According to strings found inside the code, the authors named it TrickBot (or "TrickLoader"). Many links indicate, that this bot is another product of the people previously involved in Dyreza. It seems to be rewritten from scratch – however, it contains many similar features and solutions to those we encountered analyzing Dyreza (read more).

Analyzed samples

- f26649fc31ede7594b18f8cd7cdbbc15 – initial sample, dropped by Rig EK
  - 3814abbcd8c8a41665260e4b41af26d4 – unpacked: intermediate payload (loader)
    - **f24384228fb49f9271762253b0733123 – unpacked: final payload (Trick Bot) – 32bit** <-main focus of this analysis

[1] https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/

The Malware Knowledge Archipelago

How I feel about the malware research community

- Malware „knowledge“ is heavily based on personal experience but also fragmented in the community
- Information frequency is potentially too high to comfortably keep up

- The outlined identification journey might have been shortened by e.g.
  - Being familiar with its various names: Trickster == TrickLoader == TrickBot
  - Knowing u„BotLoader“ is a stable string and also unique string for this malware family
  - Knowing u“Xmaker“ replaced u„BotLoader“ as user agent in the most recent version

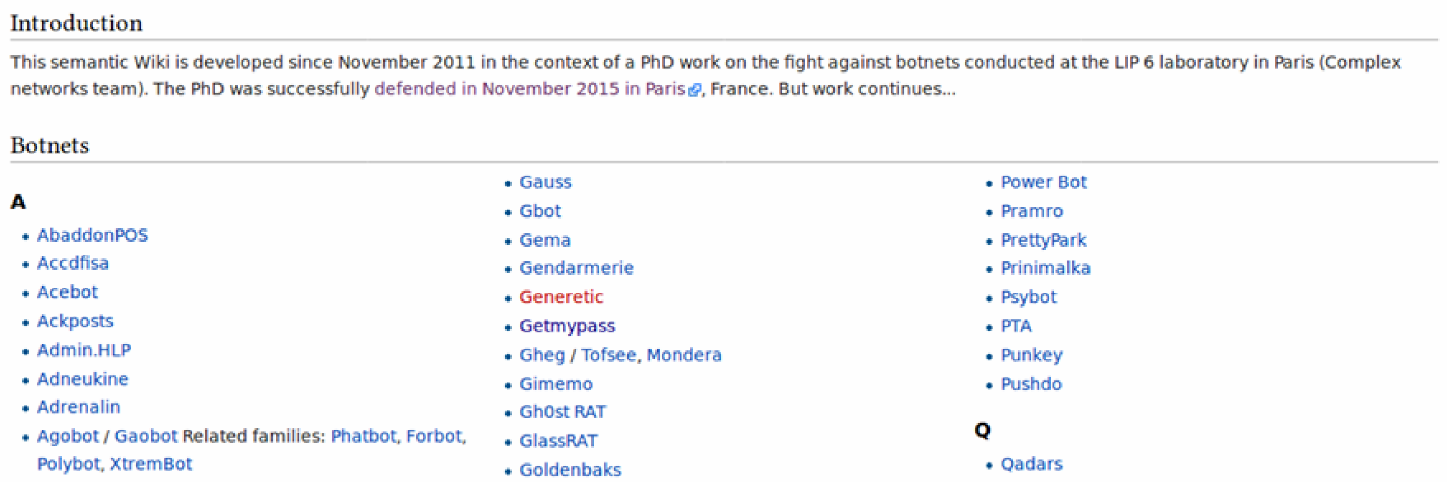
[1] https://grethascholtz.wordpress.com/2011/12/19/life-in-the-finnish-archipelago/

Other

Efforts to Systematize

The Malware Knowledge Archipelago
Other projects

- Wiki-like:
  - https://www.botnets.fr/
    by Éric Freyssinet
  - started 2011, 1,557 content pages



Introduction

This semantic Wiki is developed since November 2011 in the context of a PhD work on the fight against botnets conducted at the LIP 6 laboratory in Paris (Complex networks team). The PhD was successfully defended in November 2015 in Paris, France. But work continues...

Botnets

A

- AbaddonPOS
- Accdfisa
- Acebot
- Ackposts
- Admin.HLP
- Adneukine
- Adrenalin
- Agobot / Gaobot Related families: Phatbot, Forbot, Polybot, XtremBot

- Gauss
- Gbot
- Gema
- Gendarmerie
- Generetic
- Getmypass
- Gheg / Tofsee, Mondera
- Gimemo
- Gh0st RAT
- GlassRAT
- Goldenbaks

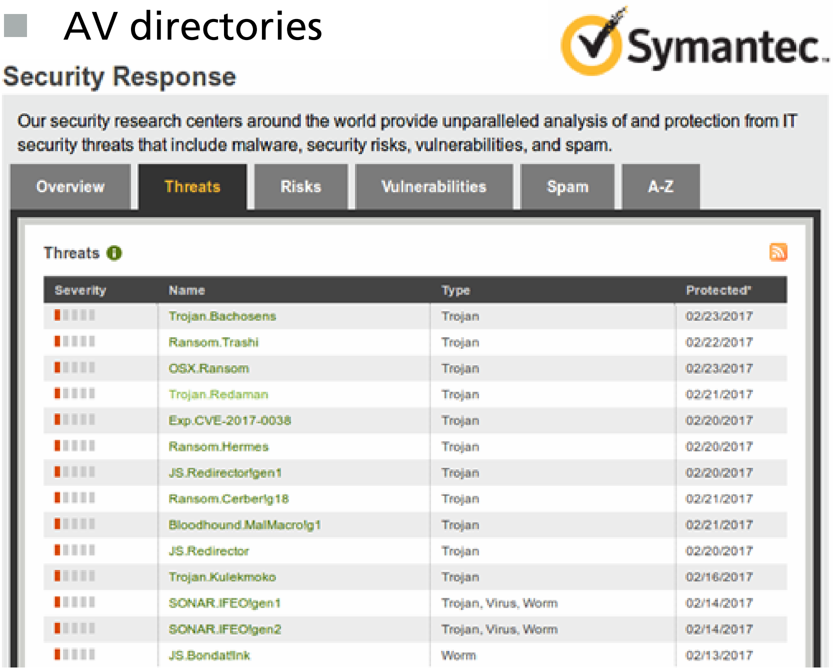
- Power Bot
- Pramro
- PrettyPark
- Prinimalka
- Psybot
- PTA
- Punkey
- Pushdo

Q

- Qadars

The Malware Knowledge Archipelago
Other projects

- Wiki-like:
  - AV directories



Security Response

Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam.

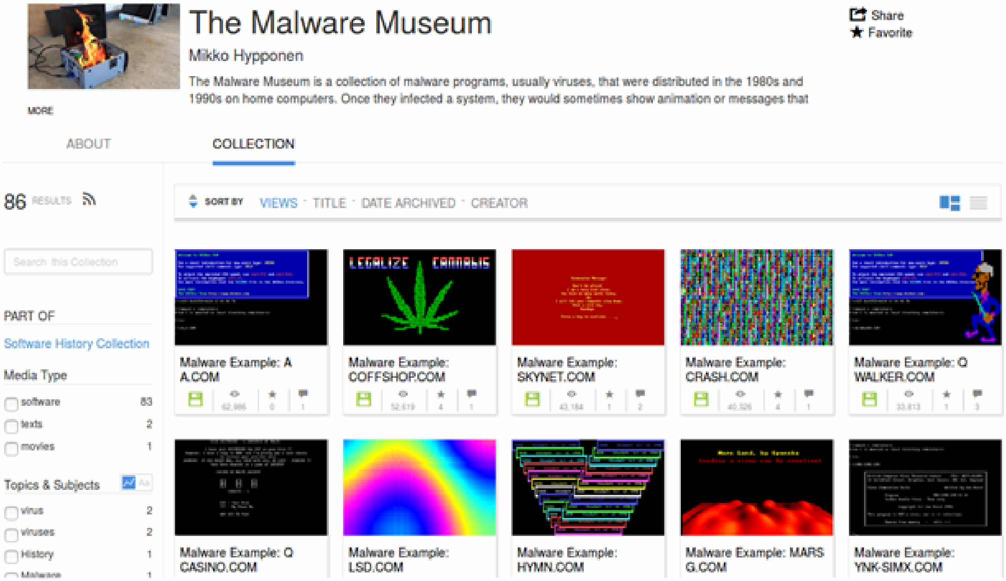
Threats

Severity	Name	Type	Protected*
▮▯▯▯▯	Trojan.Bachosens	Trojan	02/23/2017
▮▯▯▯▯	Ransom.Trashi	Trojan	02/22/2017
▮▯▯▯▯	OSX.Ransom	Trojan	02/23/2017
▮▯▯▯▯	Trojan.Redaman	Trojan	02/21/2017
▮▯▯▯▯	Exp.CVE-2017-0038	Trojan	02/20/2017
▮▯▯▯▯	Ransom.Hermes	Trojan	02/20/2017
▮▯▯▯▯	JS.Redirectorlgen1	Trojan	02/20/2017
▮▯▯▯▯	Ransom.Cerber!g18	Trojan	02/21/2017
▮▯▯▯▯	Bloodhound.MalMacro!g1	Trojan	02/21/2017
▮▯▯▯▯	JS.Redirector	Trojan	02/20/2017
▮▯▯▯▯	Trojan.Kulekmoko	Trojan	02/16/2017
▮▯▯▯▯	SONAR.IFEOlgen1	Trojan, Virus, Worm	02/14/2017
▮▯▯▯▯	SONAR.IFEOlgen2	Trojan, Virus, Worm	02/14/2017
▮▯▯▯▯	JS.Bondatlink	Worm	02/13/2017

[1] https://www.symantec.com/security_response/landing/threats.jsp

The Malware Knowledge Archipelago
Other projects

- Wiki-like:
  - https://archive.org/details/malwaremuseum



The Malware Museum

Mikko Hypponen

The Malware Museum is a collection of malware programs, usually viruses, that were distributed in the 1980s and 1990s on home computers. Once they infected a system, they would sometimes show animation or messages that

MORE

Share
Favorite

ABOUT COLLECTION

86 RESULTS

SORT BY VIEWS · TITLE · DATE ARCHIVED · CREATOR

Search this Collection

PART OF
Software History Collection

Media Type

□ software	83
□ texts	2
□ movies	1

Topics & Subjects

□ virus	2
□ viruses	2
□ History	1
□ Malware	1

Malware Example: A A.COM — 62,986 · 0 · 1

Malware Example: COFFSHOP.COM — 52,619 · 4 · 1

Malware Example: SKYNET.COM — 43,184 · 1 · 2

Malware Example: CRASH.COM — 40,326 · 4 · 1

Malware Example: Q WALKER.COM — 33,813 · 1 · 3

Malware Example: Q CASINO.COM

Malware Example: LSD.COM

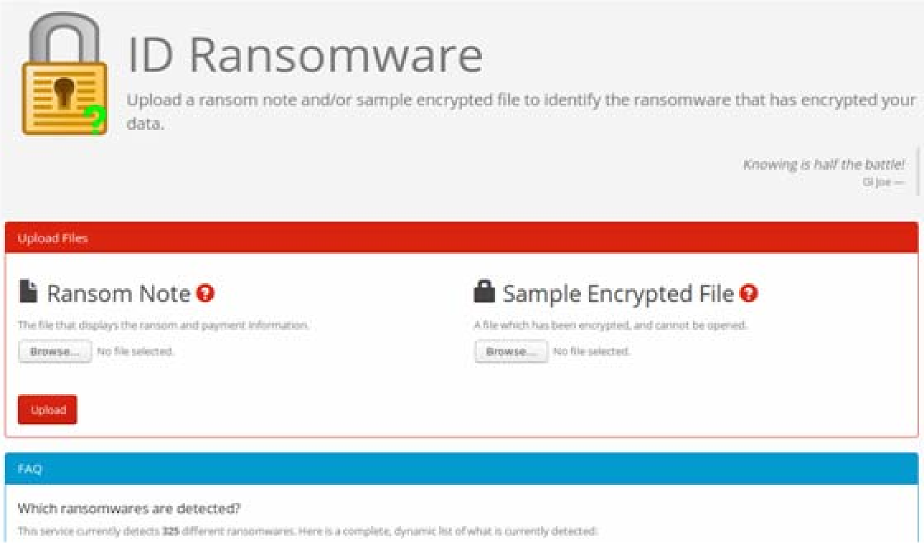
Malware Example: HYMN.COM

Malware Example: MARS G.COM

Malware Example: YNK-SIMX.COM

The Malware Knowledge Archipelago
Other projects

- „Hidden collection“:
  - https://id-ransomware.malwarehunterteam.com/index.php
  - By MalwareHunterTeam



ID Ransomware

Upload a ransom note and/or sample encrypted file to identify the ransomware that has encrypted your data.

Knowing is half the battle!
GI Joe —

Upload Files

Ransom Note

The file that displays the ransom and payment information.

Sample Encrypted File

A file which has been encrypted, and cannot be opened.

FAQ

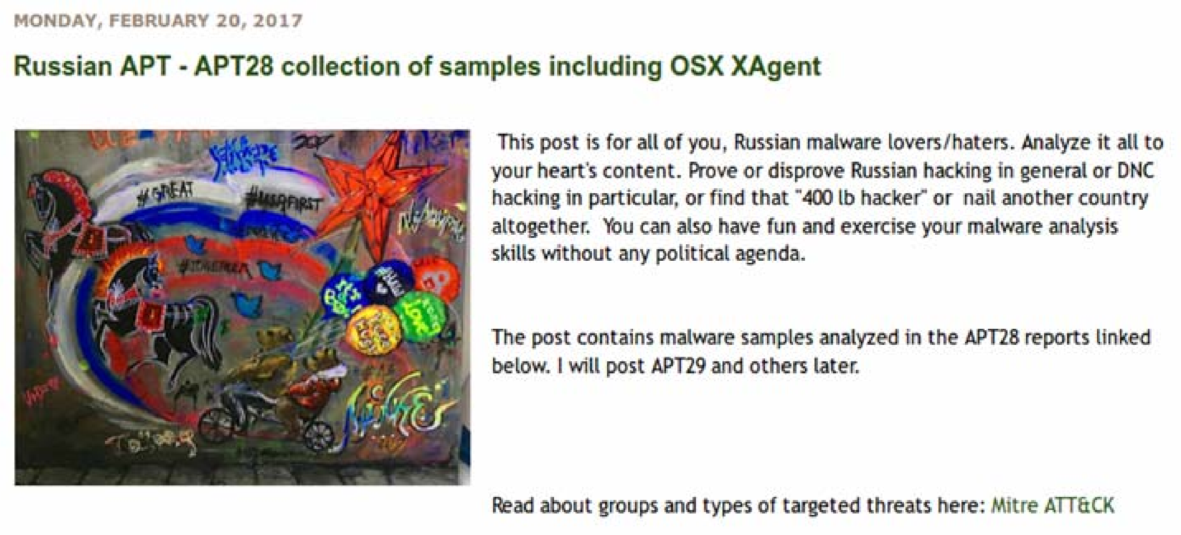
Which ransomwares are detected?

This service currently detects **325** different ransomwares. Here is a complete, dynamic list of what is currently detected:

The Malware Knowledge Archipelago
Other projects

- Code Archives:
  - http://contagiodump.blogspot.com
    by Mila Parkour

contagio
malware dump



MONDAY, FEBRUARY 20, 2017

Russian APT - APT28 collection of samples including OSX XAgent

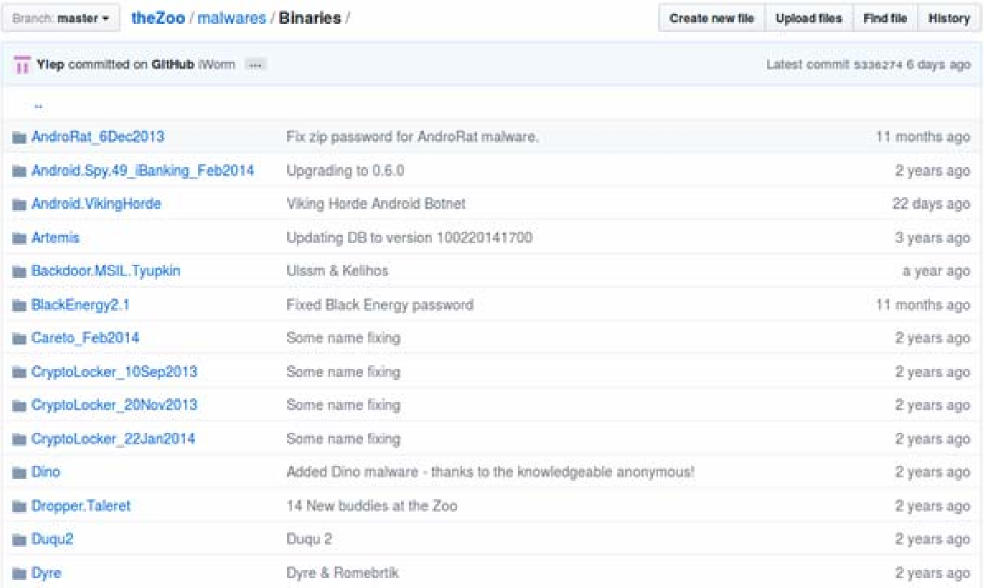
This post is for all of you, Russian malware lovers/haters. Analyze it all to your heart's content. Prove or disprove Russian hacking in general or DNC hacking in particular, or find that "400 lb hacker" or nail another country altogether. You can also have fun and exercise your malware analysis skills without any political agenda.

The post contains malware samples analyzed in the APT28 reports linked below. I will post APT29 and others later.

Read about groups and types of targeted threats here: Mitre ATT&CK

The Malware Knowledge Archipelago
Other projects

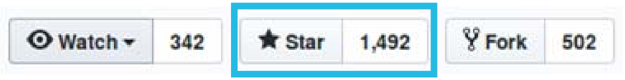
- Code Archives:
  - https://github.com/ytisf/theZoo



theZoo / malwares / Binaries /

Ylep committed on GitHub iWorm … Latest commit 5336274 6 days ago

..		
AndroRat_6Dec2013	Fix zip password for AndroRat malware.	11 months ago
Android.Spy.49_iBanking_Feb2014	Upgrading to 0.6.0	2 years ago
Android.VikingHorde	Viking Horde Android Botnet	22 days ago
Artemis	Updating DB to version 100220141700	3 years ago
Backdoor.MSIL.Tyupkin	Ulssm & Kelihos	a year ago
BlackEnergy2.1	Fixed Black Energy password	11 months ago
Careto_Feb2014	Some name fixing	2 years ago
CryptoLocker_10Sep2013	Some name fixing	2 years ago
CryptoLocker_20Nov2013	Some name fixing	2 years ago
CryptoLocker_22Jan2014	Some name fixing	2 years ago
Dino	Added Dino malware - thanks to the knowledgeable anonymous!	2 years ago
Dropper.Taleret	14 New buddies at the Zoo	2 years ago
Duqu2	Duqu 2	2 years ago
Dyre	Dyre & Romebrtik	2 years ago



The Malware Knowledge Archipelago
Other projects

- And a dozen more:
  - OpenMalware: http://www.offensivecomputing.net/
  - AVCaesar: https://avcaesar.malware.lu/product_description
  - Das Malwerk: http://dasmalwerk.eu/
  - Kernelmode: https://kernelmode.info
  - MalShare: http://malshare.com/
  - Virusign: http://www.virusign.com/
  - VirusShare: http://virusshare.com/
  - Abuse.ch trackers: https://ransomwaretracker.abuse.ch/
  - […]

Indexing?
Verified / unpacked samples?
☹

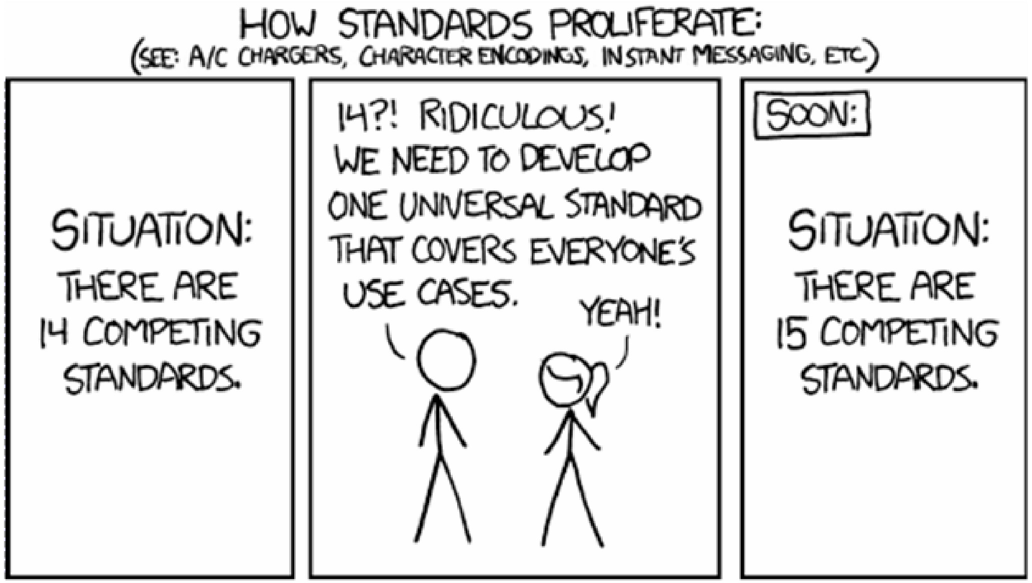
As listed by: http://www.megabeets.net/fantastic-malware-and-where-to-find-them/

The Malware Knowledge Archipelago
An idea is born

- In March 2016, I started reorganizing my little island
  - Re-Inventorization of case / sample collection
  - Motivated by DGArchive I wanted to centralize and share

The Malware Knowledge Archipelago

Why another one?!


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

[1] https://xkcd.com/927/

The Malware Knowledge Archipelago
That‘s why.

- My observations:
  - Millions of samples available, but consolidated ground truth is missing
  - There is no „convenient“ malware corpus freely available
  - Especially not tailored for static analysis
  - I need something like this for my PhD thesis anyway :)

Introducing

Malpedia

Malpedia
The central concept

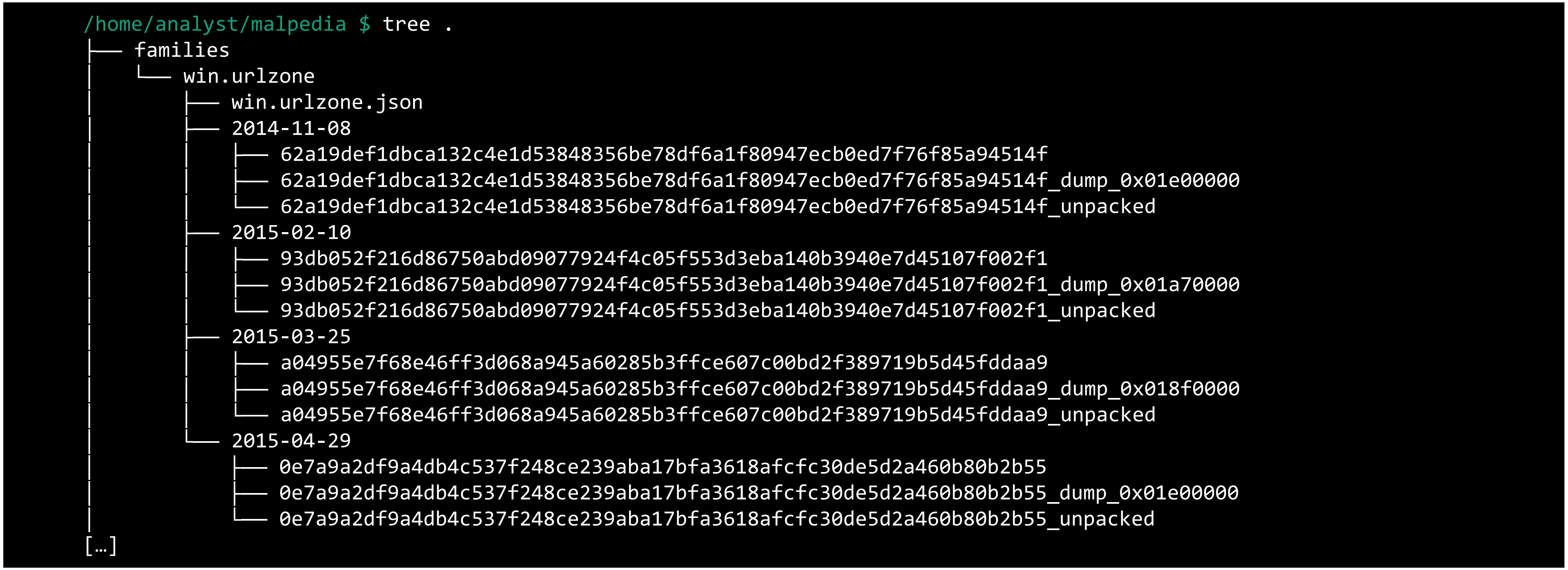
- Goal: **A curated, high-quality malware corpus**
- Approach up until now:
  - Coverage: as many families as possible
    - Follow OSINT sources (e.g. twitter) and crawl threat intel / anti-malware blogs backwards in time
    - Prefer quality over quantity
    - Prioritize prevalent malware families
  - Focus on static analysis: dumped / unpacked representative samples
    - Manual processing / verification
    - The same two reference VM snapshots used for everything (Win XP SP3, Win 7 SP1 x64)
  - Context: Meta information
    - Aliases, programming language, (personal notes)
    - References of analysis reports etc.
    - Structural Aspects
  - Future proof: SHA256! :)

Say **NO** to packers! :)

Suddenly we talk
dozens instead of millions
of samples for a family

Malpedia
First Steps

- I started by reorganizing my malware inventory into a git repository in a disciplined way:



```
/home/analyst/malpedia $ tree .
├── families
│   └── win.urlzone
│       ├── win.urlzone.json
│       ├── 2014-11-08
│       │   ├── 62a19def1dbca132c4e1d53848356be78df6a1f80947ecb0ed7f76f85a94514f
│       │   ├── 62a19def1dbca132c4e1d53848356be78df6a1f80947ecb0ed7f76f85a94514f_dump_0x01e00000
│       │   └── 62a19def1dbca132c4e1d53848356be78df6a1f80947ecb0ed7f76f85a94514f_unpacked
│       ├── 2015-02-10
│       │   ├── 93db052f216d86750abd09077924f4c05f553d3eba140b3940e7d45107f002f1
│       │   ├── 93db052f216d86750abd09077924f4c05f553d3eba140b3940e7d45107f002f1_dump_0x01a70000
│       │   └── 93db052f216d86750abd09077924f4c05f553d3eba140b3940e7d45107f002f1_unpacked
│       ├── 2015-03-25
│       │   ├── a04955e7f68e46ff3d068a945a60285b3ffce607c00bd2f389719b5d45fddaa9
│       │   ├── a04955e7f68e46ff3d068a945a60285b3ffce607c00bd2f389719b5d45fddaa9_dump_0x018f0000
│       │   └── a04955e7f68e46ff3d068a945a60285b3ffce607c00bd2f389719b5d45fddaa9_unpacked
│       └── 2015-04-29
│           ├── 0e7a9a2df9a4db4c537f248ce239aba17bfa3618afcfc30de5d2a460b80b2b55
│           ├── 0e7a9a2df9a4db4c537f248ce239aba17bfa3618afcfc30de5d2a460b80b2b55_dump_0x01e00000
│           └── 0e7a9a2df9a4db4c537f248ce239aba17bfa3618afcfc30de5d2a460b80b2b55_unpacked
│
[…]
```

Malpedia
The Vision

- Goals:
  - Web UI + REST API: Make this thing usable
  - Embrace contribution: like DGArchive, malpedia will remain semi-open, free and non-profit
  - Enable Analysis: A playground for (static) analysis approaches with actually „convenient“ data

- Impossible to compete with private AV / TI malware archives
  - Offer at least a decent, open alternative as community effort

Status Quo

Malpedia: Status Quo

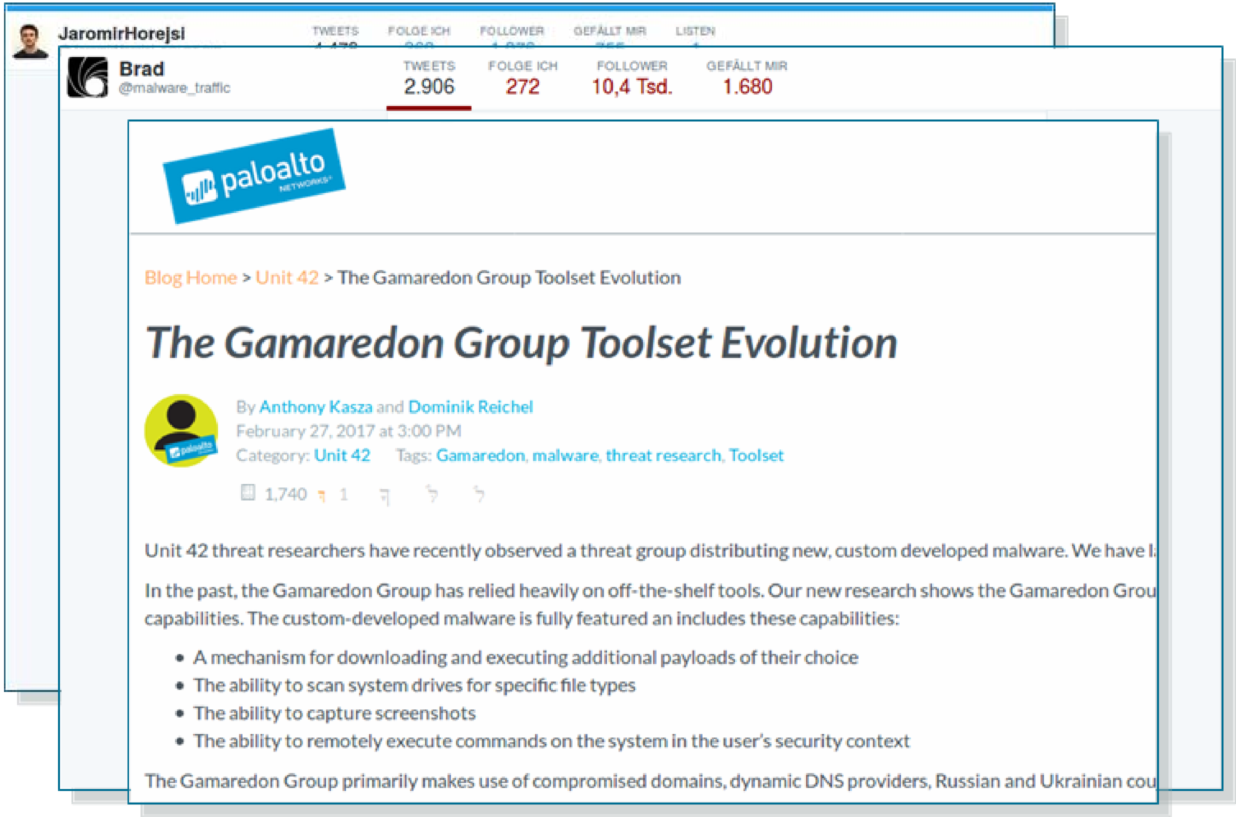
Progress

- Data acquisition procedure and progress
- Web UI
- A glimpse at the data (analysis)

How it is done so far

Status Quo: Data Acquisition & Progress

Malpedia: Status Quo
Data acquistion



JaromirHorejsi

TWEETS | FOLGE ICH | FOLLOWER | GEFÄLLT MIR | LISTEN

Brad
@malware_traffic

TWEETS	FOLGE ICH	FOLLOWER	GEFÄLLT MIR
2.906	272	10,4 Tsd.	1.680

Blog Home > Unit 42 > The Gamaredon Group Toolset Evolution

The Gamaredon Group Toolset Evolution

By Anthony Kasza and Dominik Reichel
February 27, 2017 at 3:00 PM
Category: Unit 42 Tags: Gamaredon, malware, threat research, Toolset

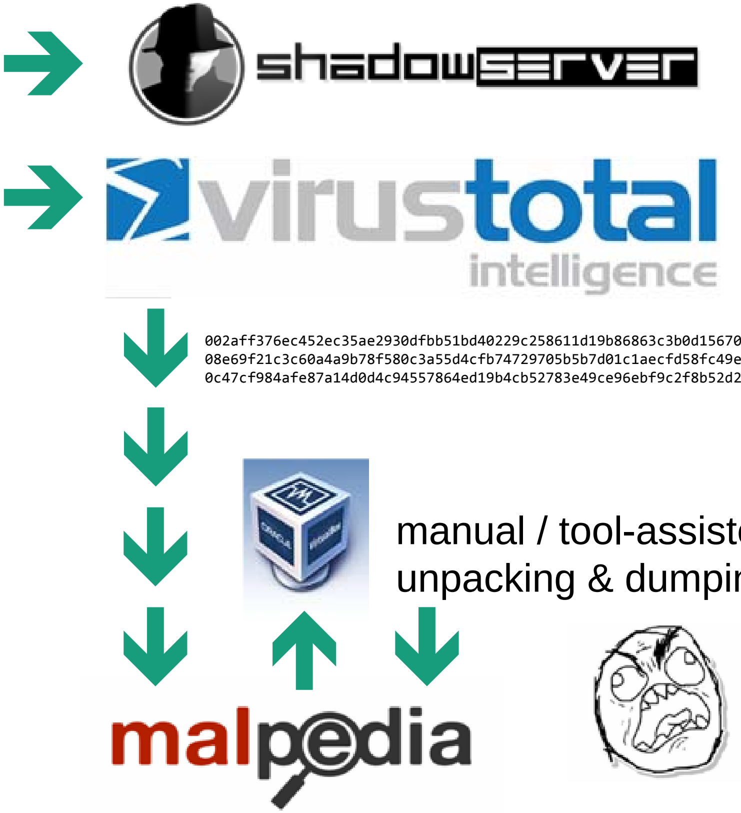
1,740 1

Unit 42 threat researchers have recently observed a threat group distributing new, custom developed malware. We have l

In the past, the Gamaredon Group has relied heavily on off-the-shelf tools. Our new research shows the Gamaredon Grou capabilities. The custom-developed malware is fully featured an includes these capabilities:

- A mechanism for downloading and executing additional payloads of their choice
- The ability to scan system drives for specific file types
- The ability to capture screenshots
- The ability to remotely execute commands on the system in the user's security context

The Gamaredon Group primarily makes use of compromised domains, dynamic DNS providers, Russian and Ukrainian cou



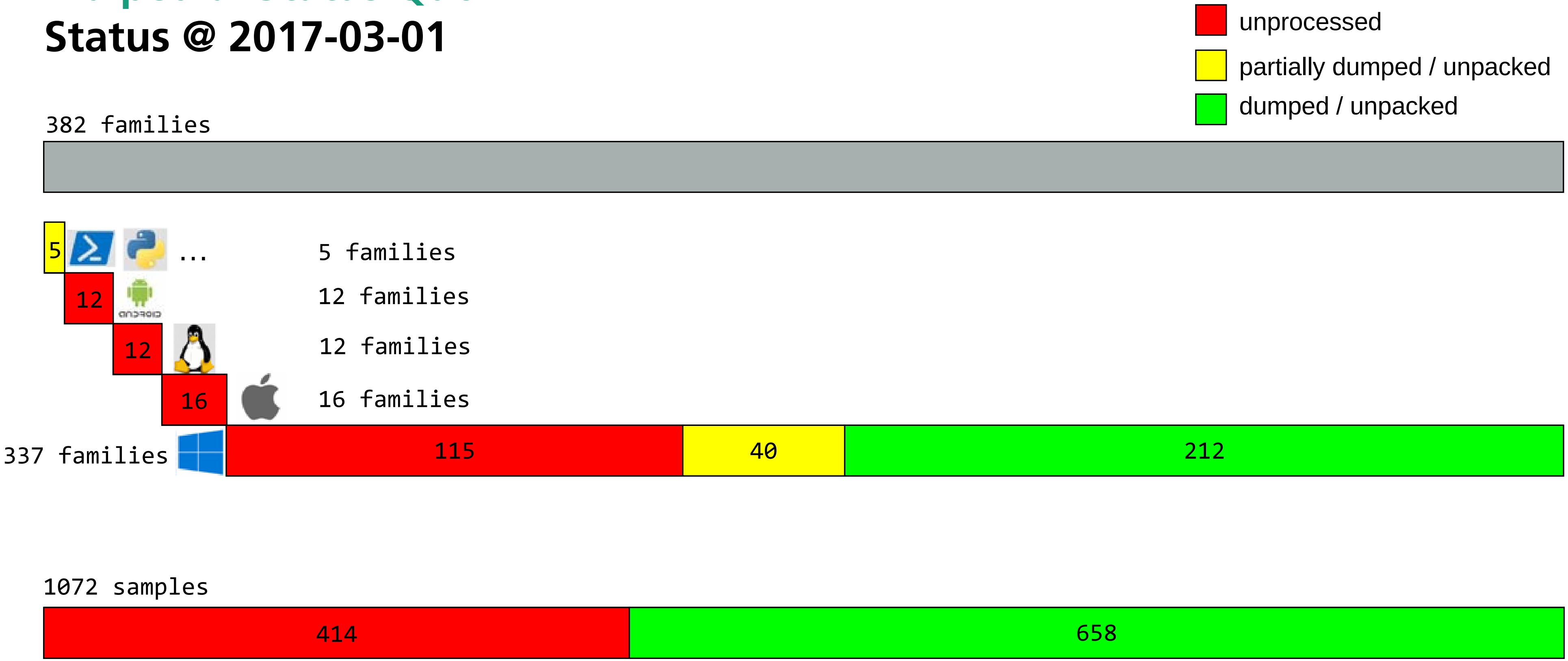
```
002aff376ec452ec35ae2930dfbb51bd40229c258611d19b86863c3b0d156705
08e69f21c3c60a4a9b78f580c3a55d4cfb74729705b5b7d01c1aecfd58fc49e6
0c47cf984afe87a14d0d4c94557864ed19b4cb52783e49ce96ebf9c2f8b52d27
```

manual / tool-assisted unpacking & dumping

[1] https://twitter.com/JaromirHorejsi
[2] https://twitter.com/malware_traffic
[3] http://researchcenter.paloaltonetworks.com

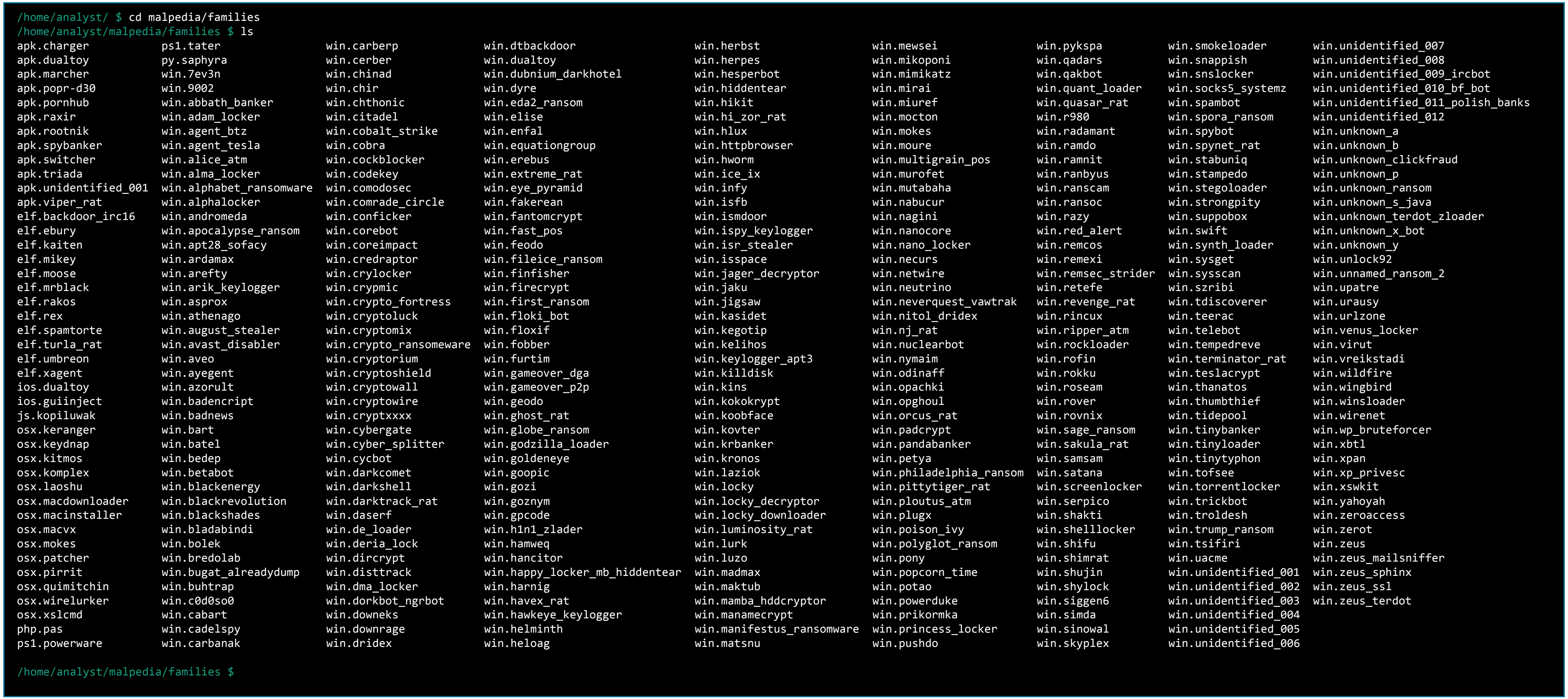
Malpedia: Status Quo

Status @ 2017-03-01



- @30min per sample: ~329 hours or about 2 full months of non-stop unpacking work days.

Malpedia: Status Quo



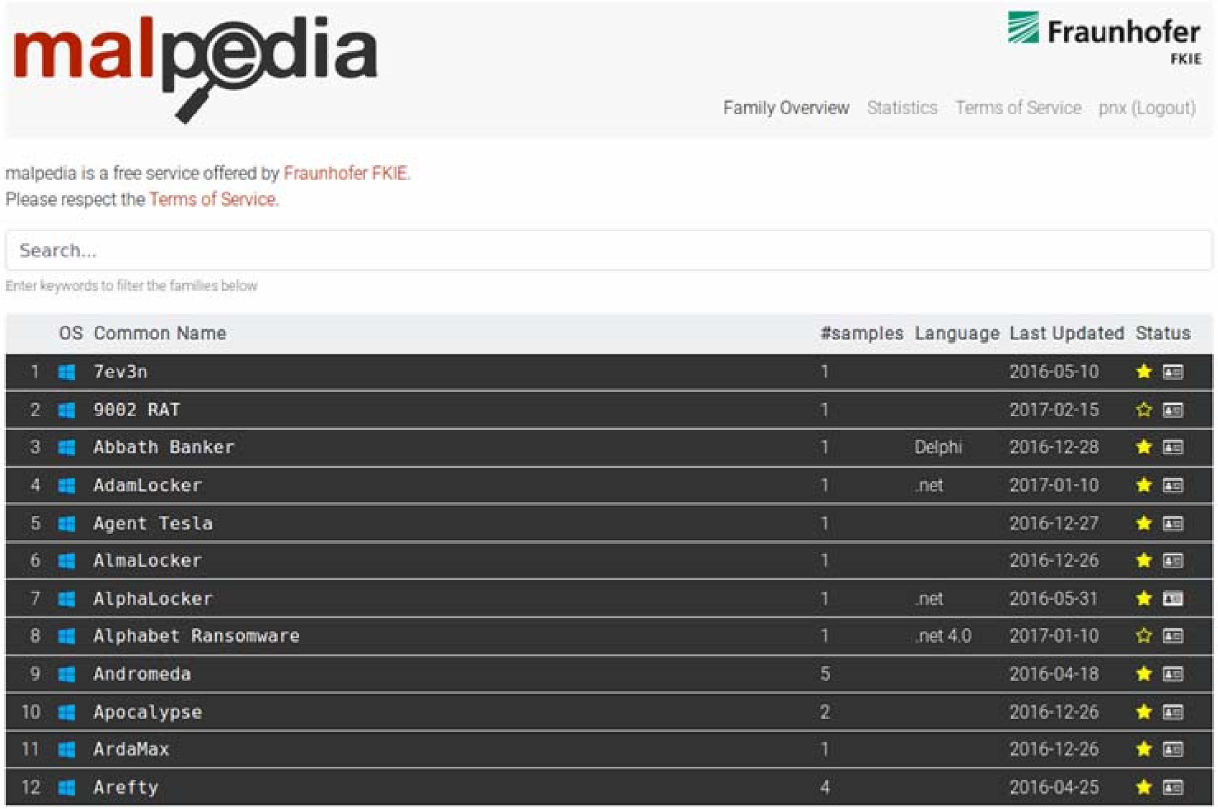
```
/home/analyst/ $ cd malpedia/families
/home/analyst/malpedia/families $ ls
apk.charger           ps1.tater                win.carberp             win.dtbackdoor                  win.herbst                 win.mewsei               win.pykspa          win.smokeloader       win.unidentified_007
apk.dualtoy           py.saphyra               win.cerber              win.dualtoy                     win.herpes                 win.mikoponi             win.qadars          win.snappish          win.unidentified_008
apk.marcher           win.7ev3n                win.chinad              win.dubnium_darkhotel           win.hesperbot              win.mimikatz             win.qakbot          win.snslocker         win.unidentified_009_ircbot
apk.popr-d30          win.9002                 win.chir                win.dyre                        win.hiddentear             win.mirai                win.quant_loader    win.socks5_systemz    win.unidentified_010_bf_bot
apk.pornhub           win.abbath_banker        win.chthonic            win.eda2_ransom                 win.hikit                  win.miuref               win.quasar_rat      win.spambot           win.unidentified_011_polish_banks
apk.raxir             win.adam_locker          win.citadel             win.elise                       win.hi_zor_rat             win.mocton               win.r980            win.spora_ransom      win.unidentified_012
apk.rootnik           win.agent_btz            win.cobalt_strike       win.enfal                       win.hlux                   win.mokes                win.radamant        win.spybot            win.unknown_a
apk.spybanker         win.agent_tesla          win.cobra               win.equationgroup               win.httpbrowser            win.moure                win.ramdo           win.spynet_rat        win.unknown_b
apk.switcher          win.alice_atm            win.cockblocker         win.erebus                      win.hworm                  win.multigrain_pos       win.ramnit          win.stabuniq          win.unknown_clickfraud
apk.triada            win.alma_locker          win.codekey             win.extreme_rat                 win.ice_ix                 win.murofet              win.ranbyus         win.stampedo          win.unknown_p
apk.unidentified_001  win.alphabet_ransomware  win.comodosec           win.eye_pyramid                 win.infy                   win.mutabaha             win.ranscam         win.stegoloader       win.unknown_ransom
apk.viper_rat         win.alphalocker          win.comrade_circle      win.fakerean                    win.isfb                   win.nabucur              win.ransoc          win.strongpity        win.unknown_s_java
elf.backdoor_irc16    win.andromeda            win.conficker           win.fantomcrypt                 win.ismdoor                win.nagini               win.razy            win.suppobox          win.unknown_terdot_zloader
elf.ebury             win.apocalypse_ransom    win.corebot             win.fast_pos                    win.ispy_keylogger         win.nanocore             win.red_alert       win.swift             win.unknown_x_bot
elf.kaiten            win.apt28_sofacy         win.coreimpact          win.feodo                       win.isr_stealer            win.nano_locker          win.remcos          win.synth_loader      win.unknown_y
elf.mikey             win.ardamax              win.credraptor          win.fileice_ransom              win.isspace                win.necurs               win.remexi          win.sysget            win.unlock92
elf.moose             win.arefty               win.crylocker           win.finfisher                   win.jager_decryptor        win.netwire              win.remsec_strider  win.sysscan           win.unnamed_ransom_2
elf.mrblack           win.arik_keylogger       win.crypmic             win.firecrypt                   win.jaku                   win.neutrino             win.retefe          win.szribi            win.upatre
elf.rakos             win.asprox               win.crypto_fortress     win.first_ransom                win.jigsaw                 win.neverquest_vawtrak   win.revenge_rat     win.tdiscoverer       win.urausy
elf.rex               win.athenago             win.cryptoluck          win.floki_bot                   win.kasidet                win.nitol_dridex         win.rincux          win.teerac            win.urlzone
elf.spamtorte         win.august_stealer       win.cryptomix           win.floxif                      win.kegotip                win.nj_rat               win.ripper_atm      win.telebot           win.venus_locker
elf.turla_rat         win.avast_disabler       win.crypto_ransomeware  win.fobber                      win.kelihos                win.nuclearbot           win.rockloader      win.tempedreve        win.virut
elf.umbreon           win.aveo                 win.cryptorium          win.furtim                      win.keylogger_apt3         win.nymaim               win.rofin           win.terminator_rat    win.vreikstadi
elf.xagent            win.ayegent              win.cryptoshield        win.gameover_dga                win.killdisk               win.odinaff              win.rokku           win.teslacrypt        win.wildfire
ios.dualtoy           win.azorult              win.cryptowall          win.gameover_p2p                win.kins                   win.opachki              win.roseam          win.thanatos          win.wingbird
ios.guiinject         win.badencript           win.cryptowire          win.geodo                       win.kokokrypt              win.opghoul              win.rover           win.thumbthief        win.winsloader
js.kopiluwak          win.badnews              win.cryptxxxx           win.ghost_rat                   win.koobface               win.orcus_rat            win.rovnix          win.tidepool          win.wirenet
osx.keranger          win.bart                 win.cybergate           win.globe_ransom                win.kovter                 win.padcrypt             win.sage_ransom     win.tinybanker        win.wp_bruteforcer
osx.keydnap           win.batel                win.cyber_splitter      win.godzilla_loader             win.krbanker               win.pandabanker          win.sakula_rat      win.tinyloader        win.xbtl
osx.kitmos            win.bedep                win.cycbot              win.goldeneye                   win.kronos                 win.petya                win.samsam          win.tinytyphon        win.xpan
osx.komplex           win.betabot              win.darkcomet           win.goopic                      win.laziok                 win.philadelphia_ransom  win.satana          win.tofsee            win.xp_privesc
osx.laoshu            win.blackenergy          win.darkshell           win.gozi                        win.locky                  win.pittytiger_rat       win.screenlocker    win.torrentlocker     win.xswkit
osx.macdownloader     win.blackrevolution      win.darktrack_rat       win.goznym                      win.locky_decryptor        win.ploutus_atm          win.serpico         win.trickbot          win.yahoyah
osx.macinstaller      win.blackshades          win.daserf              win.gpcode                      win.locky_downloader       win.plugx                win.shakti          win.troldesh          win.zeroaccess
osx.macvx             win.bladabindi           win.de_loader           win.h1n1_zlader                 win.luminosity_rat         win.poison_ivy           win.shelllocker     win.trump_ransom      win.zerot
osx.mokes             win.bolek                win.deria_lock          win.hamweq                      win.lurk                   win.polyglot_ransom      win.shifu           win.tsifiri           win.zeus
osx.patcher           win.bredolab             win.dircrypt            win.hancitor                    win.luzo                   win.pony                 win.shimrat         win.uacme             win.zeus_mailsniffer
osx.pirrit            win.bugat_alreadydump    win.disttrack           win.happy_locker_mb_hiddentear  win.madmax                 win.popcorn_time         win.shujin          win.unidentified_001  win.zeus_sphinx
osx.quimitchin        win.buhtrap              win.dma_locker          win.harnig                      win.maktub                 win.potao                win.shylock         win.unidentified_002  win.zeus_ssl
osx.wirelurker        win.c0d0so0              win.dorkbot_ngrbot      win.havex_rat                   win.mamba_hddcryptor       win.powerduke            win.siggen6         win.unidentified_003  win.zeus_terdot
osx.xslcmd            win.cabart               win.downeks             win.hawkeye_keylogger           win.manamecrypt            win.prikormka            win.simda           win.unidentified_004
php.pas               win.cadelspy             win.downrage            win.helminth                    win.manifestus_ransomware  win.princess_locker      win.sinowal         win.unidentified_005
ps1.powerware         win.carbanak             win.dridex              win.heloag                      win.matsnu                 win.pushdo               win.skyplex         win.unidentified_006

/home/analyst/malpedia/families $
```

What’s already done

Status Quo: Web UI

Malpedia: Status Quo

Web UI



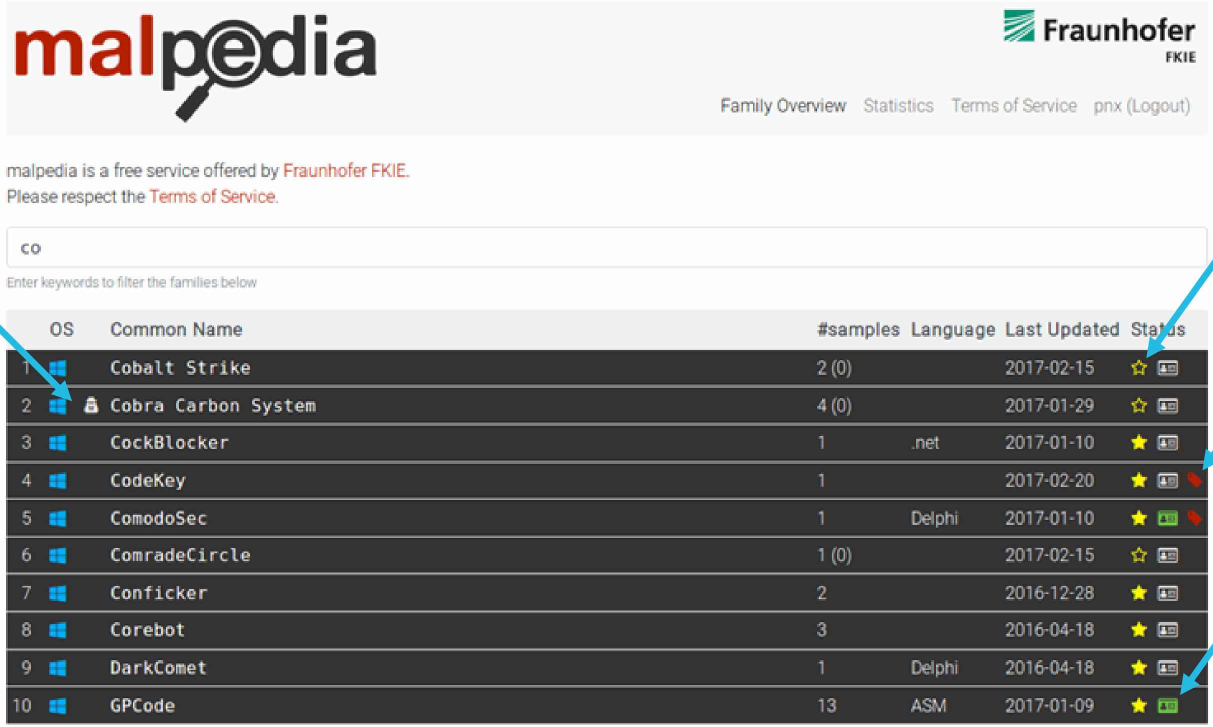
malpedia is a free service offered by Fraunhofer FKIE.
Please respect the Terms of Service.

Search...

Enter keywords to filter the families below

	OS	Common Name	#samples	Language	Last Updated	Status
1	⊞	7ev3n	1		2016-05-10	★ ▤
2	⊞	9002 RAT	1		2017-02-15	☆ ▤
3	⊞	Abbath Banker	1	Delphi	2016-12-28	★ ▤
4	⊞	AdamLocker	1	.net	2017-01-10	★ ▤
5	⊞	Agent Tesla	1		2016-12-27	★ ▤
6	⊞	AlmaLocker	1		2016-12-26	★ ▤
7	⊞	AlphaLocker	1	.net	2016-05-31	★ ▤
8	⊞	Alphabet Ransomware	1	.net 4.0	2017-01-10	☆ ▤
9	⊞	Andromeda	5		2016-04-18	★ ▤
10	⊞	Apocalypse	2		2016-12-26	★ ▤
11	⊞	ArdaMax	1		2016-12-26	★ ▤
12	⊞	Arefty	4		2016-04-25	★ ▤

Malpedia: Status Quo
Web UI



malpedia is a free service offered by Fraunhofer FKIE.
Please respect the Terms of Service.

co

Enter keywords to filter the families below

	OS		Common Name	#samples	Language	Last Updated	Status
1	⊞		Cobalt Strike	2 (0)		2017-02-15	☆ ▤
2	⊞	🔒	Cobra Carbon System	4 (0)		2017-01-29	☆ ▤
3	⊞		CockBlocker	1	.net	2017-01-10	★ ▤
4	⊞		CodeKey	1		2017-02-20	★ ▤ 🏷
5	⊞		ComodoSec	1	Delphi	2017-01-10	★ 🟩 🏷
6	⊞		ComradeCircle	1 (0)		2017-02-15	☆ ▤
7	⊞		Conficker	2		2016-12-28	★ ▤
8	⊞		Corebot	3		2016-04-18	★ ▤
9	⊞		DarkComet	1	Delphi	2016-04-18	★ ▤
10	⊞		GPCode	13	ASM	2017-01-09	★ 🟩

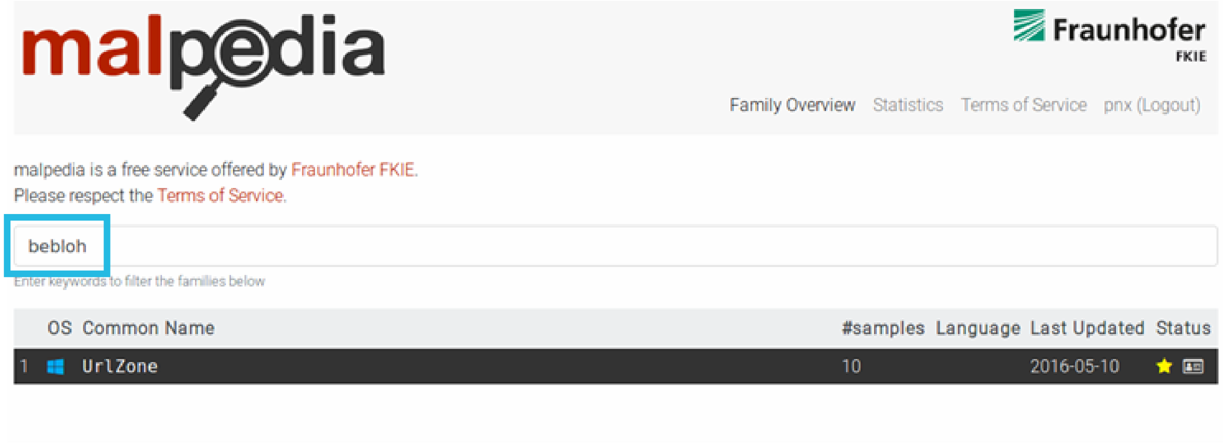
Tied to a known actor

Unpacked/Dumped Status

YARA rule available

Complete context info available

Malpedia: Status Quo
Web UI



malpedia

Fraunhofer FKIE

Family Overview   Statistics   Terms of Service   pnx (Logout)

malpedia is a free service offered by Fraunhofer FKIE.
Please respect the Terms of Service.

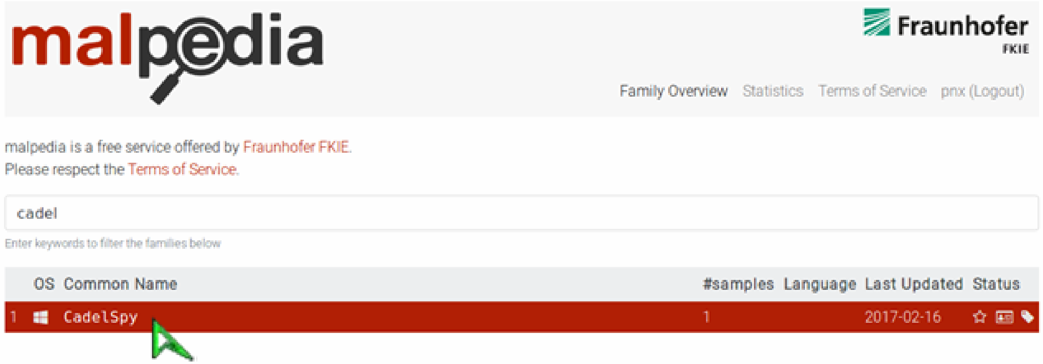
bebloh

Enter keywords to filter the families below

	OS	Common Name	#samples	Language	Last Updated	Status
1	⊞	UrlZone	10		2016-05-10	★ ▭

Malpedia: Status Quo

Web UI



malpedia is a free service offered by Fraunhofer FKIE.
Please respect the Terms of Service.

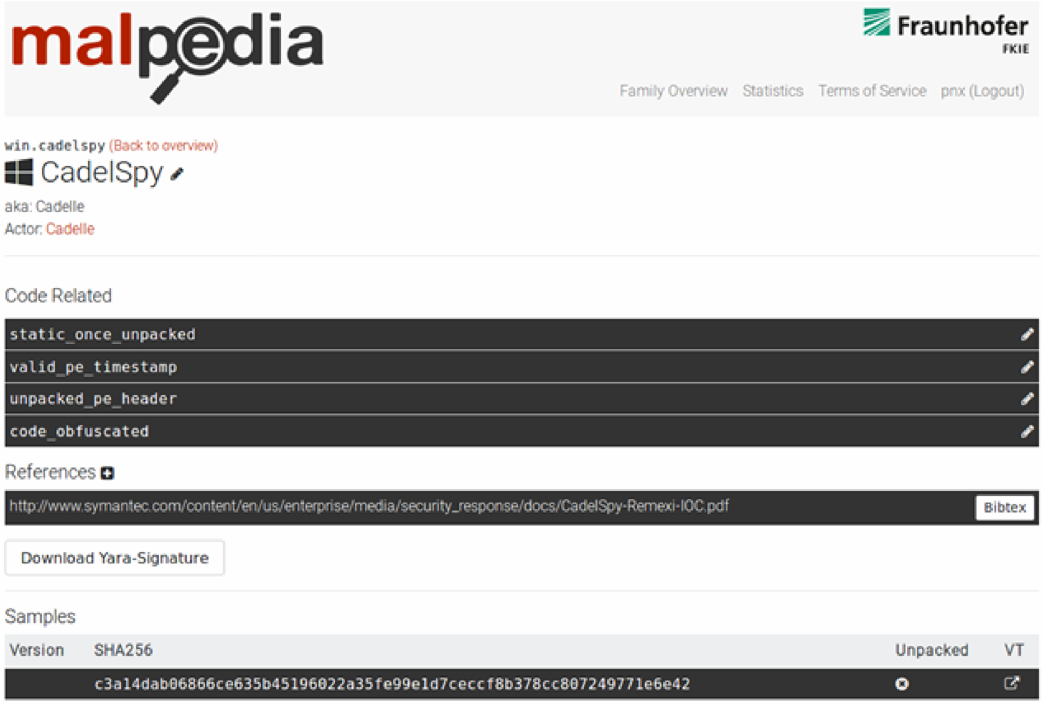
cadel

Enter keywords to filter the families below

	OS	Common Name	#samples	Language	Last Updated	Status
1	⊞	CadelSpy	1		2017-02-16	☆

[1] http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/CadelSpy-Remexi-IOC.pdf

Malpedia: Status Quo
Web UI



malpedia

Fraunhofer FKIE

Family Overview Statistics Terms of Service pnx (Logout)

win.cadelspy (Back to overview)

CadelSpy

aka: Cadelle

Actor: Cadelle

Code Related

static_once_unpacked

valid_pe_timestamp

unpacked_pe_header

code_obfuscated

References

http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/CadelSpy-Remexi-IOC.pdf Bibtex

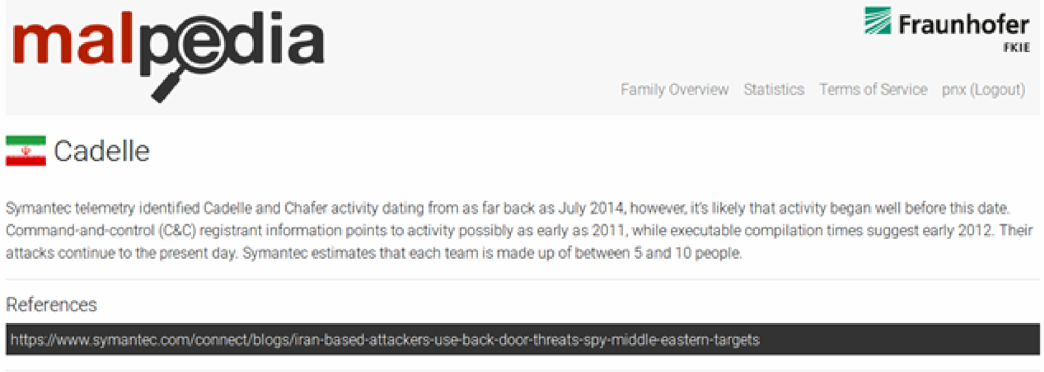
Download Yara-Signature

Samples

Version	SHA256	Unpacked	VT
	c3a14dab06866ce635b45196022a35fe99e1d7ceccf8b378cc807249771e6e42	●	↗

[1] http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/CadelSpy-Remexi-IOC.pdf

Malpedia: Status Quo
Web UI



Cadelle

Symantec telemetry identified Cadelle and Chafer activity dating from as far back as July 2014, however, it's likely that activity began well before this date. Command-and-control (C&C) registrant information points to activity possibly as early as 2011, while executable compilation times suggest early 2012. Their attacks continue to the present day. Symantec estimates that each team is made up of between 5 and 10 people.

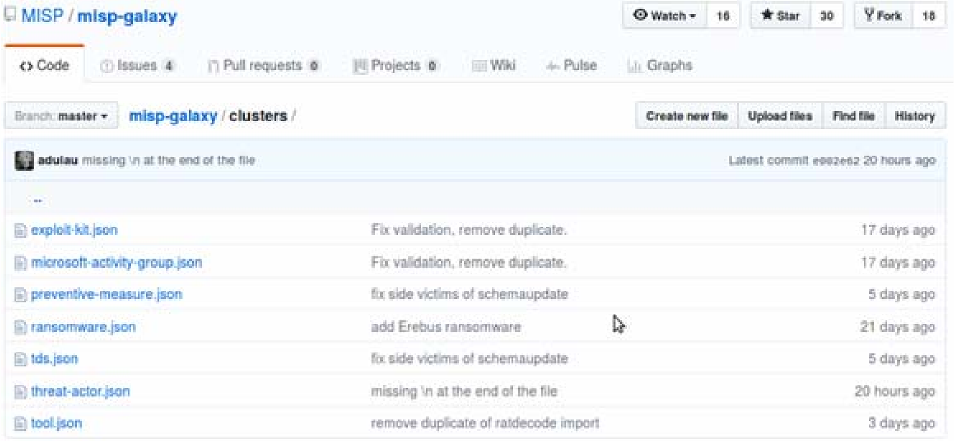
References

https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets

Credits: MISP Project

circl.lu
Computer Incident
Response Center
LUXEMBOURG

MISP
Threat Sharing



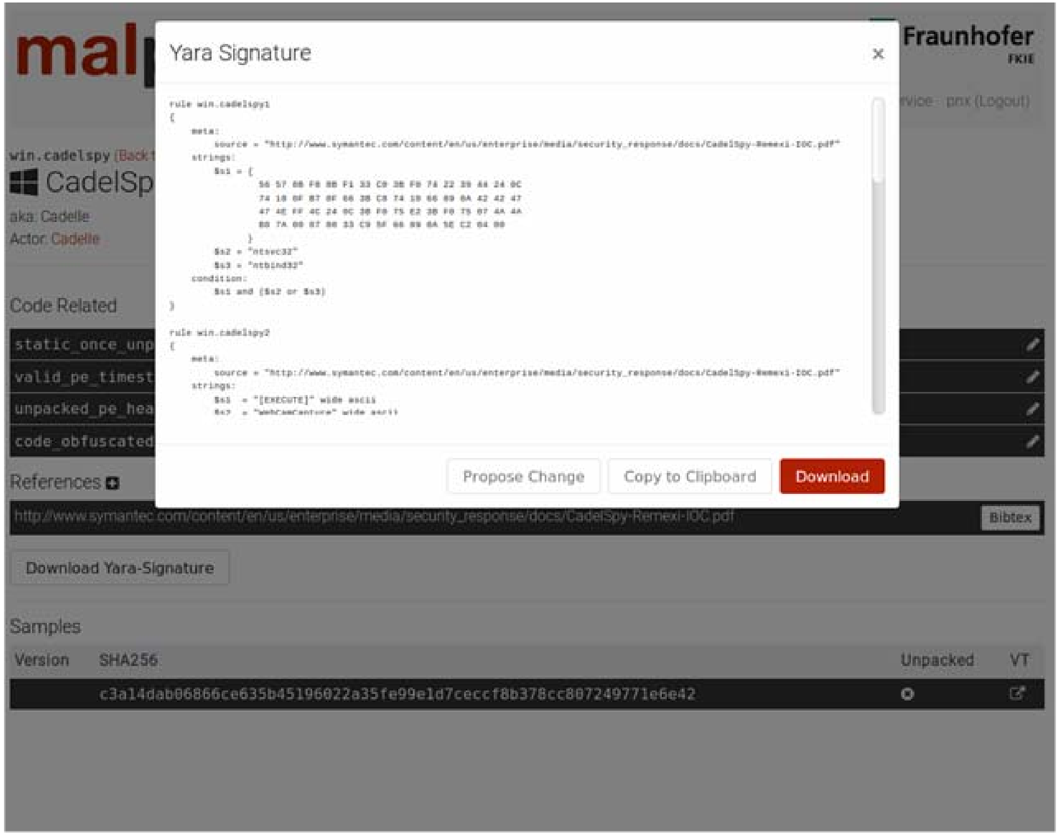
misp-galaxy / clusters /

adulau missing \n at the end of the file — Latest commit e8e2e62 20 hours ago

..		
exploit-kit.json	Fix validation, remove duplicate.	17 days ago
microsoft-activity-group.json	Fix validation, remove duplicate.	17 days ago
preventive-measure.json	fix side victims of schemaupdate	5 days ago
ransomware.json	add Erebus ransomware	21 days ago
tds.json	fix side victims of schemaupdate	5 days ago
threat-actor.json	missing \n at the end of the file	20 hours ago
tool.json	remove duplicate of ratdecode import	3 days ago

[1] https://github.com/MISP/misp-galaxy
[2] https://www.circl.lu/

Malpedia: Status Quo
Web UI



```
rule win.cadelspy1
{
    meta:
        source = "http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/CadelSpy-Remexi-IOC.pdf"
    strings:
        $s1 = {
                56 57 8B F8 8B F1 33 C9 3B F9 74 22 39 44 24 0C
                74 18 0F B7 0F 66 3B C8 74 10 66 89 0A 42 42 47
                47 4E FF 4C 24 0C 3B F9 75 E2 3B F9 75 07 4A 4A
                B8 7A 00 07 80 33 C9 5F 66 89 0A 5E C2 04 00
              }
        $s2 = "ntsvc32"
        $s3 = "ntbind32"
    condition:
        $s1 and ($s2 or $s3)
}

rule win.cadelspy2
{
    meta:
        source = "http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/CadelSpy-Remexi-IOC.pdf"
    strings:
        $s1  = "[EXECUTE]" wide ascii
        $s2  = "WebCamCapture" wide ascii
```

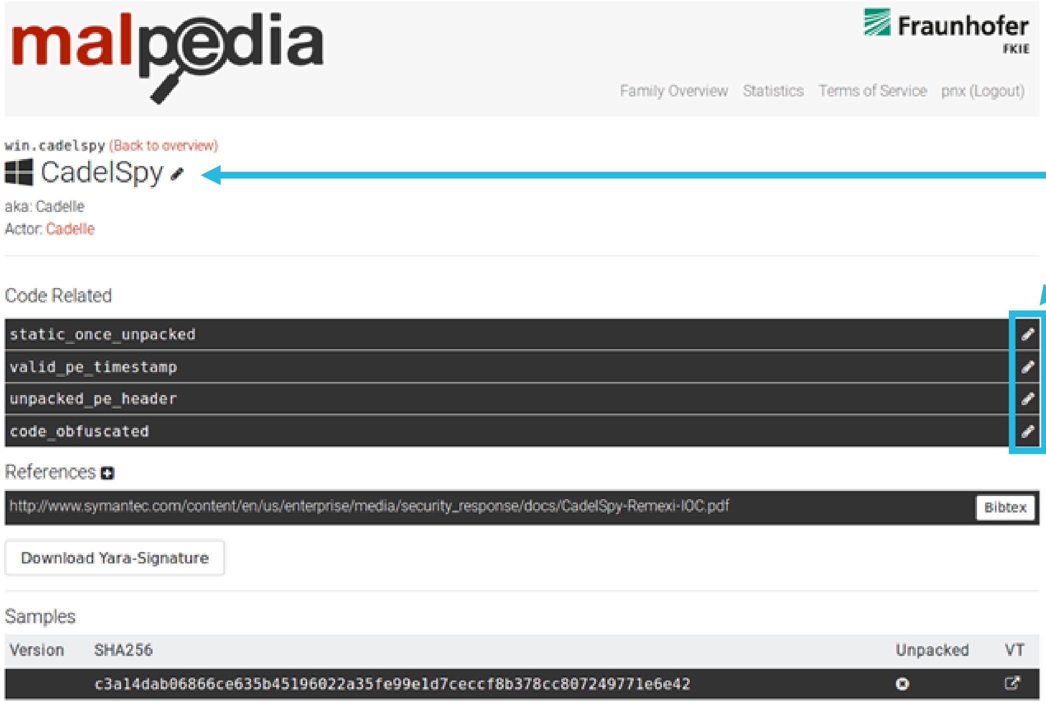
http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/CadelSpy-Remexi-IOC.pdf

Version	SHA256	Unpacked	VT
	c3a14dab06866ce635b45196022a35fe99e1d7ceccf8b378cc807249771e6e42	○	↗

[1] http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/CadelSpy-Remexi-IOC.pdf

Malpedia: Status Quo

Web UI



win.cadelspy (Back to overview)

CadelSpy

aka: Cadelle

Actor: Cadelle

Code Related

static_once_unpacked

valid_pe_timestamp

unpacked_pe_header

code_obfuscated

References

http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/CadelSpy-Remexi-IOC.pdf Bibtex

Download Yara-Signature

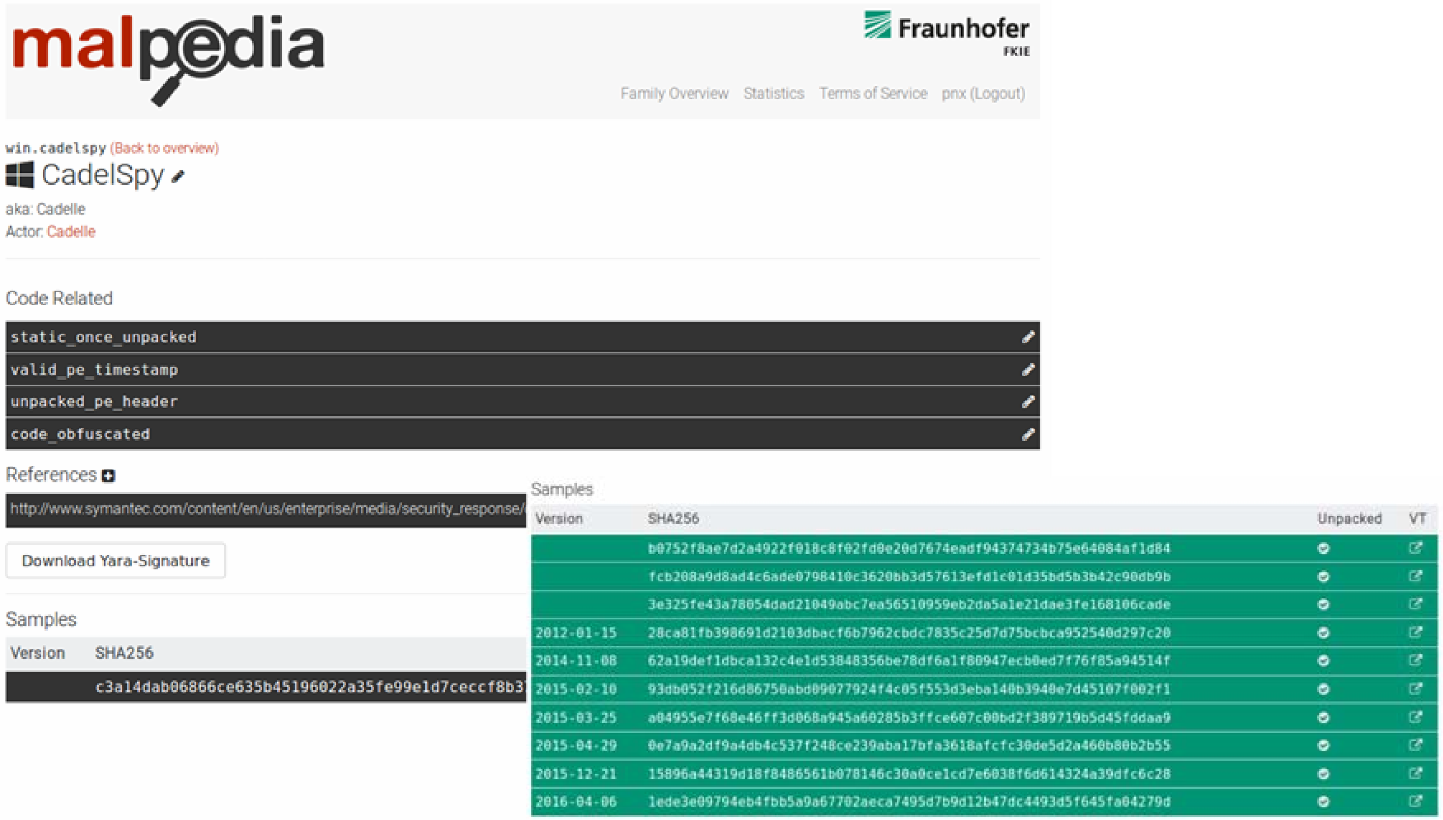
Samples

Version	SHA256	Unpacked	VT
	c3a14dab06866ce635b45196022a35fe99e1d7ceccf8b378cc807249771e6e42	●	

Allow users to propose changes

[1] http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/CadelSpy-Remexi-IOC.pdf

Malpedia: Status Quo
Web UI



win.cadelspy (Back to overview)

CadelSpy

aka: Cadelle

Actor: Cadelle

Code Related

```
static_once_unpacked
valid_pe_timestamp
unpacked_pe_header
code_obfuscated
```

References

http://www.symantec.com/content/en/us/enterprise/media/security_response/

Samples

Version	SHA256
	c3a14dab06866ce635b45196022a35fe99e1d7ceccf8b3

Samples

Version	SHA256	Unpacked	VT
	b0752f8ae7d2a4922f018c8f02fd0e20d7674eadf94374734b75e64084af1d84	✓	↗
	fcb208a9d8ad4c6ade0798410c3620bb3d57613efd1c01d35bd5b3b42c90db9b	✓	↗
	3e325fe43a78054dad21049abc7ea56510959eb2da5a1e21dae3fe168106cade	✓	↗
2012-01-15	28ca81fb398691d2103dbacf6b7962cbdc7835c25d7d75bcbca952540d297c20	✓	↗
2014-11-08	62a19def1dbca132c4e1d53848356be78df6a1f80947ecb0ed7f76f85a94514f	✓	↗
2015-02-10	93db052f216d86750abd09077924f4c05f553d3eba140b3940e7d45107f002f1	✓	↗
2015-03-25	a04955e7f68e46ff3d068a945a60285b3ffce607c00bd2f389719b5d45fddaa9	✓	↗
2015-04-29	0e7a9a2df9a4db4c537f248ce239aba17bfa3618afcfc30de5d2a460b80b2b55	✓	↗
2015-12-21	15896a44319d18f8486561b078146c30a0ce1cd7e6038f6d614324a39dfc6c28	✓	↗
2016-04-06	1ede3e09794eb4fbb5a9a67702aeca7495d7b9d12b47dc4493d5f645fa04279d	✓	↗

[1] http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/CadelSpy-Remexi-IOC.pdf

Malpedia: Status Quo
Web UI

- Eternal thanks to my student assistant **Steffen Enders** who is implementing this UI!
  - He will soon write a Bachelor‘s Thesis on compiler fingerprinting supervised by me :)

What’s already possible

Status Quo: A glimpse at the Data

Malpedia: Status Quo
A glimpse at the Data

- Or some examples why I consider malpedia already useful
  - YaraRules.com vs. Malpedia
  - Static Analysis vs. Malpedia

- Data set freeze: 2017-03-01

What’s already possible

Status Quo: YaraRules vs Malpedia

Malpedia: Status Quo
YaraRules.com vs. Malpedia

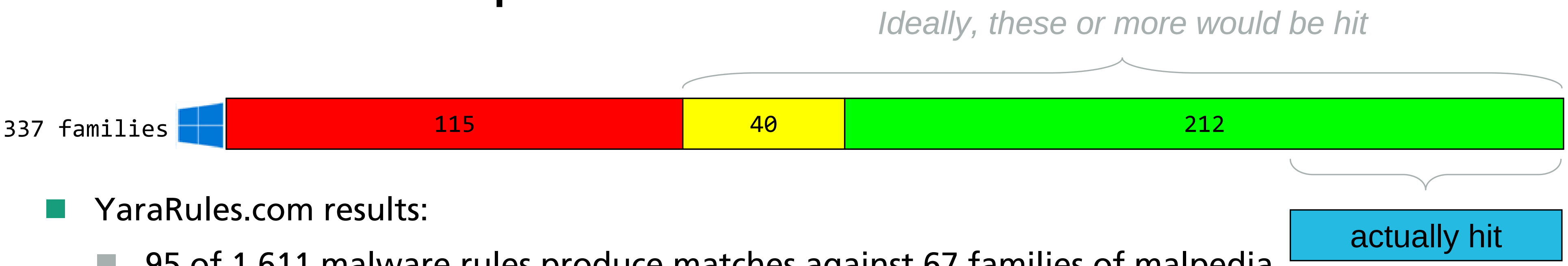
- YaraRules.com
  - Probably the most comprehensive public body of YARA rules

```
/home/analyst/repos/yara-rules $ grep ^rule * -R | wc -l
12065
/home/analyst/repos/yara-rules $ cd malware
/home/analyst/repos/yara-rules/malware $ grep ^rule * -R | wc -l
1611
/home/analyst/repos/yara-rules/malware $ ls -l | wc -l
268
^^^ =267 files -> families
```

- The ideal YARA rules:
  - One rule matches one family only. (no false positives)
  - One rule matches all samples of this same family. (no false negatives)

Malpedia: Status Quo

YaraRules.com vs. Malpedia



- YaraRules.com results:
  - 95 of 1,611 malware rules produce matches against 67 families of malpedia
    - For some families, multiple rules exist and hit (5x BlackShades RAT, 5x Codoso, 3x Turla, …)
  - 5 rules (6%) produce False Positives against 3 or more families
    - Conditions are chosen so wide that they allow one or more FP strings as a group to already fulfil the rule
      - Example: „data_inject“ (generic for many webinjects, matches a bunch of bankers)
      - Example: „mario“ AND „RFB 003.033“ AND „FIXME“ (matches basically every Zeus offspring)
  - 19 families (28%) were hit incompletely
    - On average they match only 29.58% of the samples present for the respective family.

Malpedia: Status Quo
YaraRules.com vs. Malpedia

- IMHO: Writing YARA rules is challenging because of imperfect information
  - Often limited samples available as ground truth for the target family
  - There are limited resources to check if the rules are prone to FPs
  - Basically no material on how to write great YARA rules

- Expectation:
  - It will become way more convenient to write solid YARA rules with Malpedia

What’s already possible

Status Quo: Static Analysis vs Malpedia

Malpedia: Status Quo
Static Analysis vs. Malpedia

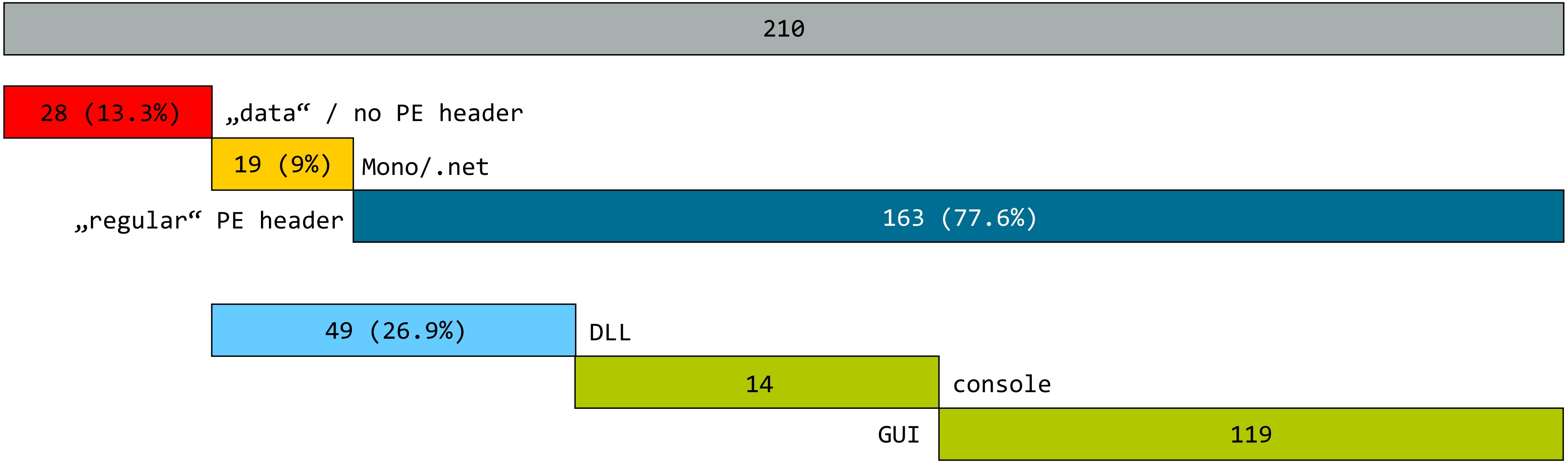
- Some cursory examples of static analysis
  - „File“ characteristics of dumped malware
  - PDB path presence
  - Programming language frequencies
  - Function Count
  - Example: Investigation of an Anti-Analysis Pattern

- Please consider this only a tiny outlook for future work and possibilities

Malpedia: Status Quo
file vs. Malpedia

- One sample per 210 families chosen as representative (x86, windows only)

```
/home/analyst/malpedia/acsc_subset $ file *
```



210

28 (13.3%) „data“ / no PE header

19 (9%) Mono/.net

„regular“ PE header 163 (77.6%)

49 (26.9%) DLL

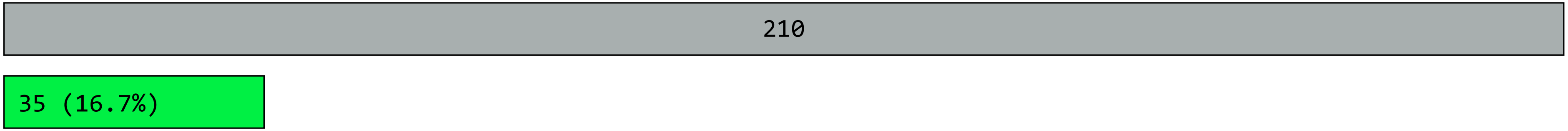
14 console

GUI 119

Malpedia: Status Quo
grep vs. Malpedia

- One sample per 210 families chosen as representative (x86, windows only)

```
/home/analyst/malpedia/acsc_subset $  grep -aoP "[ -~]+\\.pdb" *
```



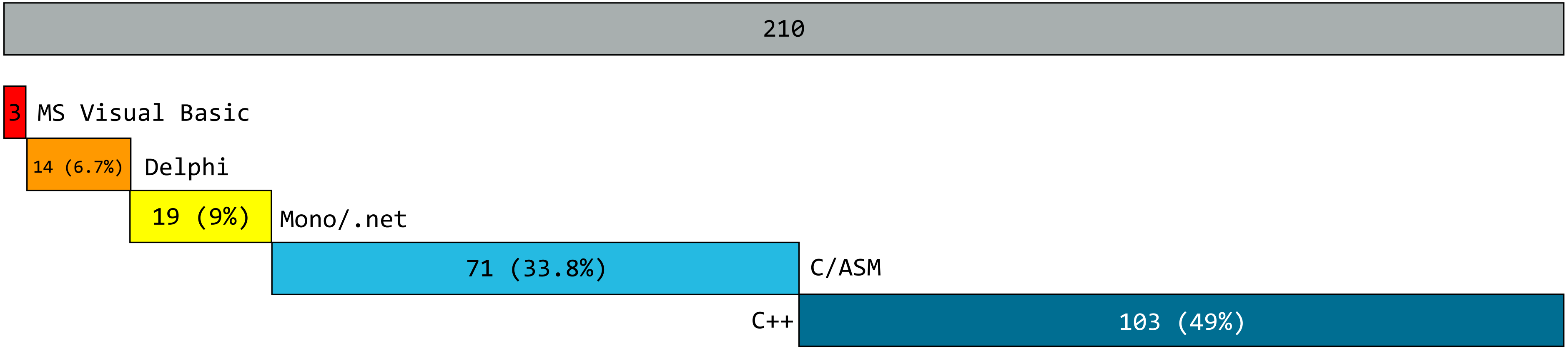
examples

```
adam_locker       C:\Users\Surox\Documents\Visual Studio 2015\Projects\EncryptRansomByhumanpuff69\EncryptRansombyhumanpuff69\obj\x86\Release\adm_64.pdb
Aveo              C:\Users\SoundOF\Desktop\aveo\Release\aveo.pdb
Cockblocker       C:\Users\classyjakey\Documents\Visual Studio 2015\Projects\Cockblocker\Cockblocker\obj\Release\Cockblocker.pdb
Corebot           C:\work\itco\core\bin\x86\Release\core.pdb
Darkshell         F:\NTDDK\DEMO\NetBot\i386\ReSSDT.pdb
Herbst            C:\Users\Win7\Documents\Visual Studio 2012\Projects\Alt\Kryptolocker\Kryptolocker\obj\Debug\Kryptolocker.pdb
Herpes            C:\Documents and Settings\Frk7\Desktop\Nohrpmeplease\h3rpes\Herpes4\Release\Herpes.pdb
Hikit             h:\JmVodServer\hikit\bin32\RServer.pdb
isr_stealer       f:\Projects\VS2005\WebBrowserPassView\Release\WebBrowserPassView.pdb
Samsam            f:\SAM\clients\Sam6\SAM\obj\Release\samsam.pdb
Skyplex           C:\Users\s\Desktop\Home\Code\Skyplex v1.0\Release\Skyplex.pdb
Snslocker         C:\Users\Saad\Desktop\SNSLocker\SNSLocker\SNSLocker\SNSLocker\obj\Debug\SNSLocker.pdb
Thanatos          H:\Alpha\Bot\Release\Core.pdb
Tidepool          c:\BS2005\BS2005\release\IE.pdb
unidentified_008  z:\src\_cpp\bwin3\Release\bwin3.pdb
```

Malpedia: Status Quo

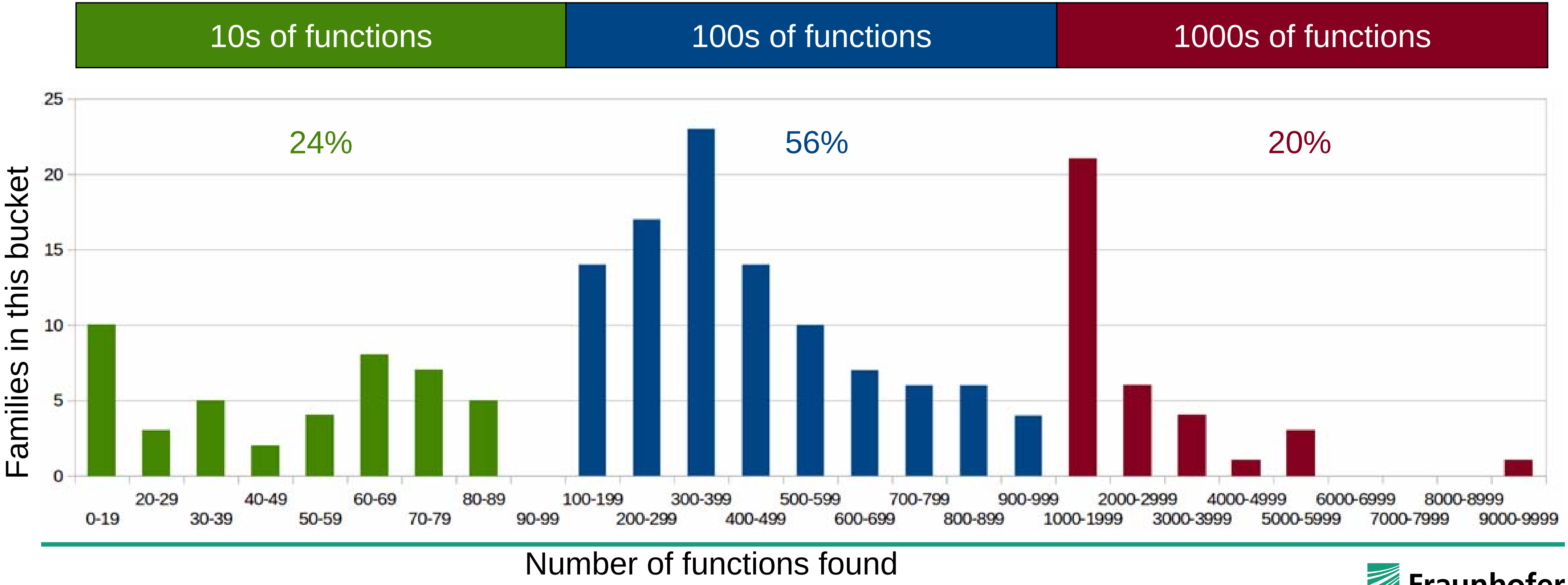
Disassembler vs. Malpedia: Programming Languages

- One sample per 210 families chosen as representative (x86, windows only)
  - Programming language frequencies (rough heuristical determination)



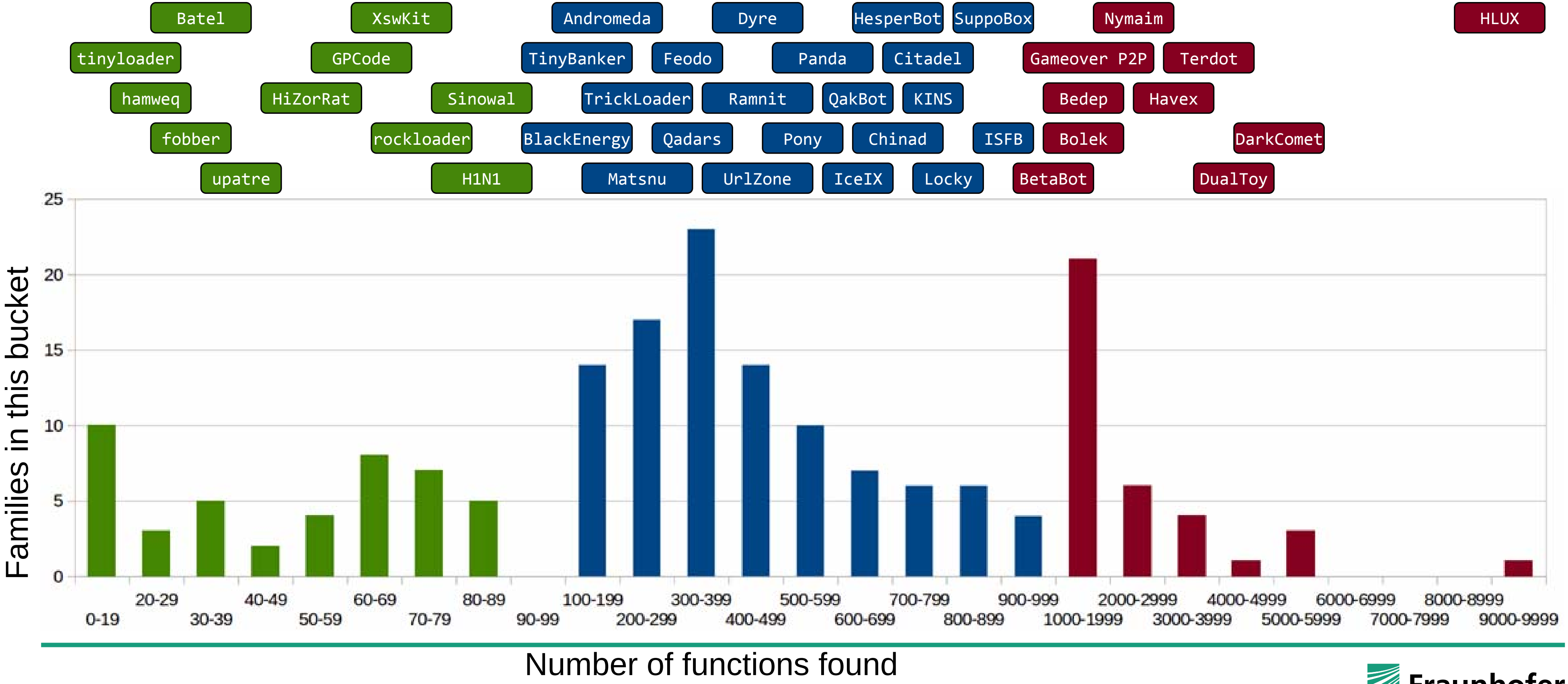
Malpedia: Status Quo

Disassembler vs. Malpedia: Number of Functions



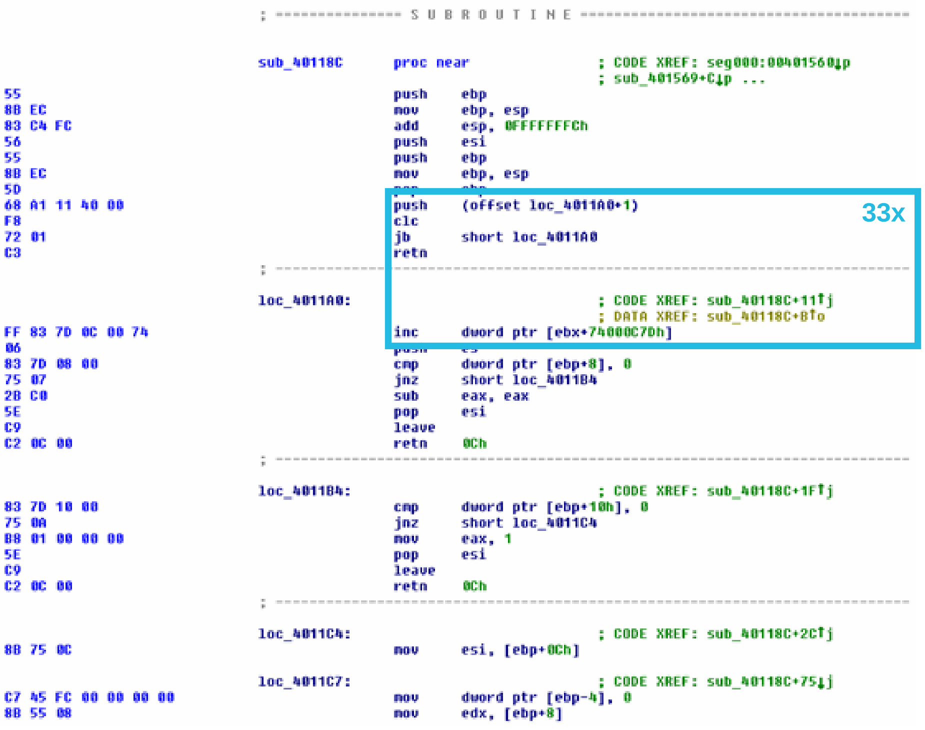
Malpedia: Status Quo

Disassembler vs. Malpedia: Number of Functions



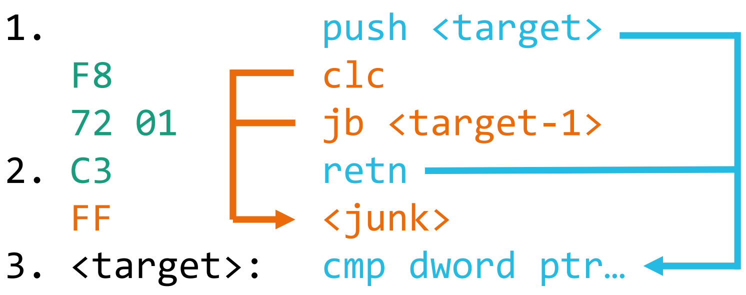
Malpedia: Status Quo

Disassembler vs. Malpedia: Presence of Anti-Analysis Patterns



```
                         ; =============== S U B R O U T I N E =======================================

                         sub_40118C      proc near               ; CODE XREF: seg000:00401560↓p
                                                                 ; sub_401569+C↓p ...
55                                       push    ebp
8B EC                                    mov     ebp, esp
83 C4 FC                                 add     esp, 0FFFFFFFCh
56                                       push    esi
55                                       push    ebp
8B EC                                    mov     ebp, esp
5D                                       pop     ebp
68 A1 11 40 00                           push    (offset loc_4011A0+1)
F8                                       clc
72 01                                    jb      short loc_4011A0
C3                                       retn
                         ; ---------------------------------------------------------------------------

                         loc_4011A0:                             ; CODE XREF: sub_40118C+11↑j
                                                                 ; DATA XREF: sub_40118C+B↑o
FF 83 7D 0C 00 74                        inc     dword ptr [ebx+74000C7Dh]
06                                       push    es
83 7D 08 00                              cmp     dword ptr [ebp+8], 0
75 07                                    jnz     short loc_4011B4
2B C0                                    sub     eax, eax
5E                                       pop     esi
C9                                       leave
C2 0C 00                                 retn    0Ch
                         ; ---------------------------------------------------------------------------

                         loc_4011B4:                             ; CODE XREF: sub_40118C+1F↑j
83 7D 10 00                              cmp     dword ptr [ebp+10h], 0
75 0A                                    jnz     short loc_4011C4
B8 01 00 00 00                           mov     eax, 1
5E                                       pop     esi
C9                                       leave
C2 0C 00                                 retn    0Ch
                         ; ---------------------------------------------------------------------------

                         loc_4011C4:                             ; CODE XREF: sub_40118C+2C↑j
8B 75 0C                                 mov     esi, [ebp+0Ch]

                         loc_4011C7:                             ; CODE XREF: sub_40118C+75↓j
C7 45 FC 00 00 00 00                     mov     dword ptr [ebp-4], 0
8B 55 08                                 mov     edx, [ebp+8]
```

some Pony strain
bfe2a403158191c413379c9ef67f9c0bf0e442f7a47dde33d8100905123be6f2



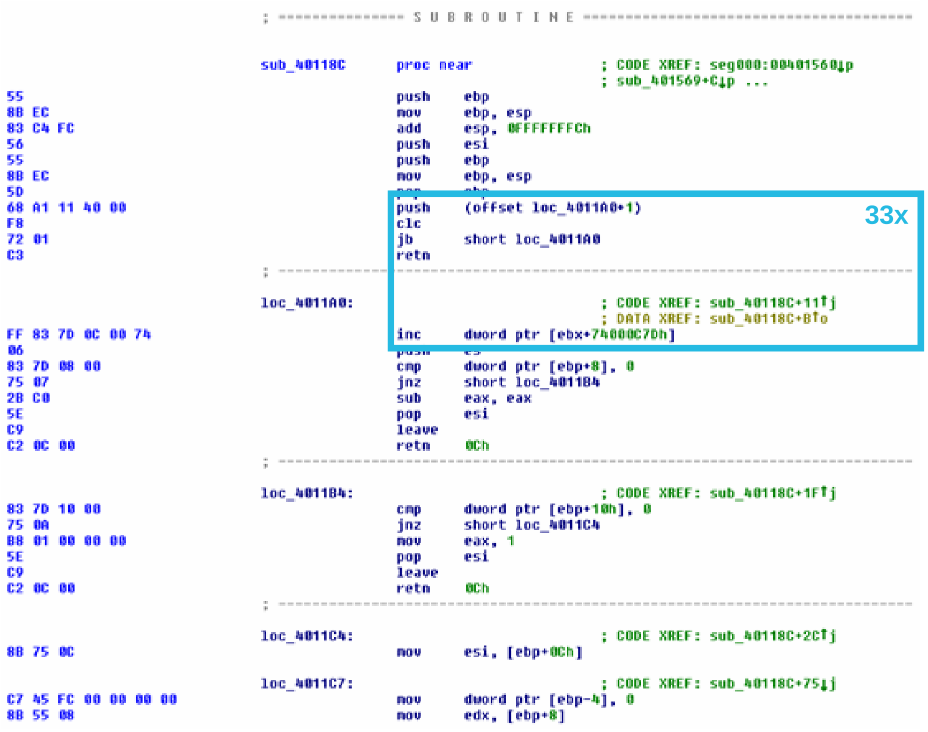
```
1.               push <target>
   F8            clc
   72 01         jb <target-1>
2. C3            retn
   FF            <junk>
3. <target>:     cmp dword ptr…
```

Does this „technique“ appear in any other families?

„F8 72 01 C3“ ?

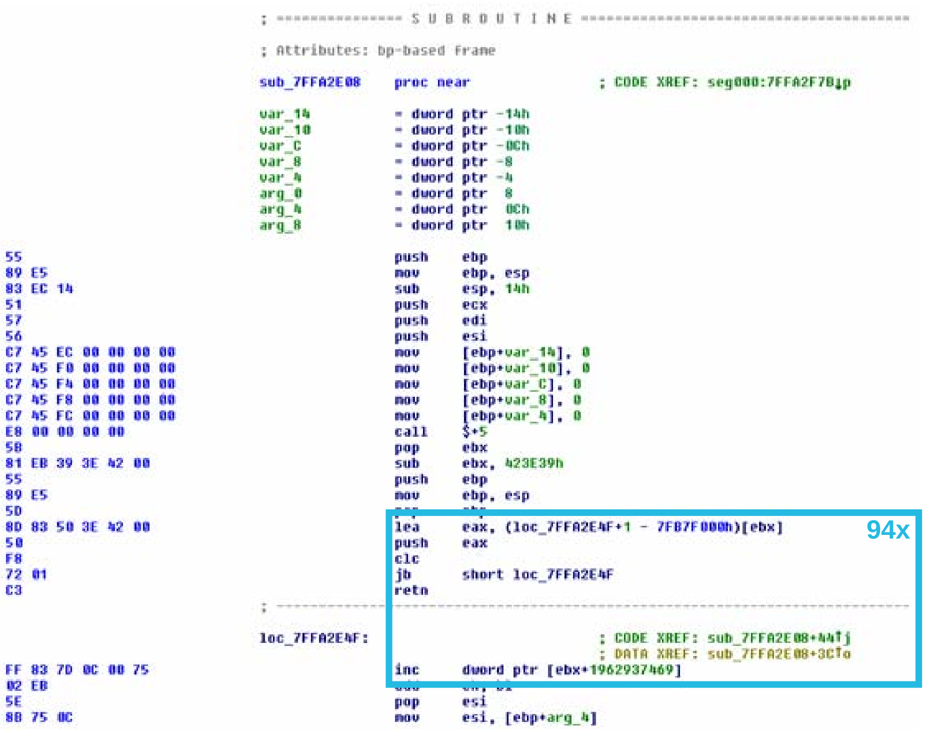
Malpedia: Status Quo

Disassembler vs. Malpedia: Presence of Anti-Analysis Patterns



```
                  ; =============== S U B R O U T I N E =======================================

                  sub_40118C      proc near               ; CODE XREF: seg000:00401560↓p
                                                          ; sub_401569+C↓p ...
55                                push    ebp
8B EC                             mov     ebp, esp
83 C4 FC                          add     esp, 0FFFFFFFCh
56                                push    esi
55                                push    ebp
8B EC                             mov     ebp, esp
5D
68 A1 11 40 00                    push    (offset loc_4011A0+1)
F8                                clc
72 01                             jb      short loc_4011A0
C3                                retn
                  ; ---------------------------------------------------------------------------

                  loc_4011A0:                             ; CODE XREF: sub_40118C+11↑j
                                                          ; DATA XREF: sub_40118C+B↑o
FF 83 7D 0C 00 74                 inc     dword ptr [ebx+74000C7Dh]
06
83 7D 08 00                       cmp     dword ptr [ebp+8], 0
75 07                             jnz     short loc_4011B4
2B C0                             sub     eax, eax
5E                                pop     esi
C9                                leave
C2 0C 00                          retn    0Ch
                  ; ---------------------------------------------------------------------------

                  loc_4011B4:                             ; CODE XREF: sub_40118C+1F↑j
83 7D 10 00                       cmp     dword ptr [ebp+10h], 0
75 0A                             jnz     short loc_4011C4
B8 01 00 00 00                    mov     eax, 1
5E                                pop     esi
C9                                leave
C2 0C 00                          retn    0Ch
                  ; ---------------------------------------------------------------------------

                  loc_4011C4:                             ; CODE XREF: sub_40118C+2C↑j
8B 75 0C                          mov     esi, [ebp+0Ch]

                  loc_4011C7:                             ; CODE XREF: sub_40118C+75↓j
C7 45 FC 00 00 00 00              mov     dword ptr [ebp-4], 0
8B 55 08                          mov     edx, [ebp+8]
```

Pony
bfe2a403158191c413379c9ef67f9c0bf0e442f7a47dde33d8100905123be6f2



```
                  ; =============== S U B R O U T I N E =======================================

                  ; Attributes: bp-based frame

                  sub_7FFA2E08    proc near               ; CODE XREF: seg000:7FFA2F7B↓p

                  var_14          = dword ptr -14h
                  var_10          = dword ptr -10h
                  var_C           = dword ptr -0Ch
                  var_8           = dword ptr -8
                  var_4           = dword ptr -4
                  arg_0           = dword ptr  8
                  arg_4           = dword ptr  0Ch
                  arg_8           = dword ptr  10h

55                                push    ebp
89 E5                             mov     ebp, esp
83 EC 14                          sub     esp, 14h
51                                push    ecx
57                                push    edi
56                                push    esi
C7 45 EC 00 00 00 00              mov     [ebp+var_14], 0
C7 45 F0 00 00 00 00              mov     [ebp+var_10], 0
C7 45 F4 00 00 00 00              mov     [ebp+var_C], 0
C7 45 F8 00 00 00 00              mov     [ebp+var_8], 0
C7 45 FC 00 00 00 00              mov     [ebp+var_4], 0
E8 00 00 00 00                    call    $+5
5B                                pop     ebx
81 EB 39 3E 42 00                 sub     ebx, 423E39h
55                                push    ebp
89 E5                             mov     ebp, esp
5D
8D 83 50 3E 42 00                 lea     eax, (loc_7FFA2E4F+1 - 7FB7F000h)[ebx]
50                                push    eax
F8                                clc
72 01                             jb      short loc_7FFA2E4F
C3                                retn
                  ; ---------------------------------------------------------------------------

                  loc_7FFA2E4F:                           ; CODE XREF: sub_7FFA2E08+44↑j
                                                          ; DATA XREF: sub_7FFA2E08+3C↑o
FF 83 7D 0C 00 75                 inc     dword ptr [ebx+1962937469]
02 EB
5E                                pop     esi
8B 75 0C                          mov     esi, [ebp+arg_4]
```

Matsnu
d60254a66bdeb81329db9c0c905cc2d49a13c3d3cf2c23e9857b0991823819f4

Things to come

Roadmap

Roadmap

Ingredients for Future Goodness

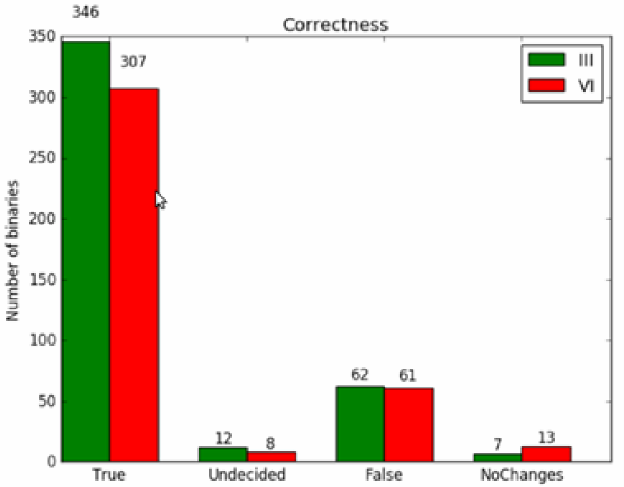
- Enable users to upload samples for analysis

- Results from Master‘s thesis I recently supervised:
  - RoAMer – Thorsten Jenke
  - Gabby – Pavlo Hordiienko

- Malware config (C&C, crypto keys, …) extraction?

Roadmap
RoAMer: Robust Automated Malware Unpacker

- Master‘s thesis by **Thorsten Jenke**:
  - *„Implement what Daniel has learned unpacking 600+ samples by hand into a methodology + tool that achieves similar results, but way faster and with a lot less pain.“*



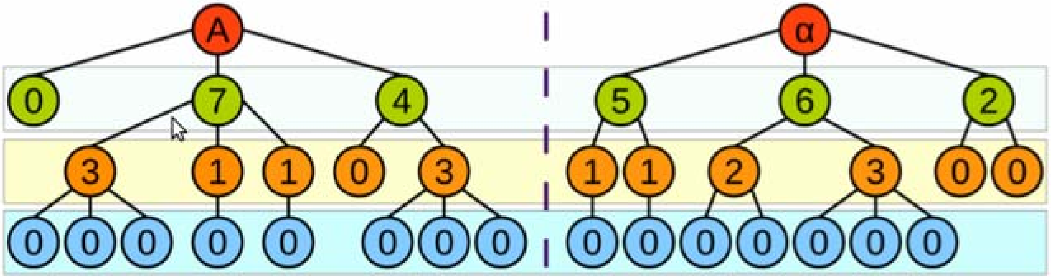
85% success, <3 min processing per sample
speedup: 10x

[1] „Robust Malware Unpacking“. Jenke, T. Master‘s Thesis, 2016.

Roadmap

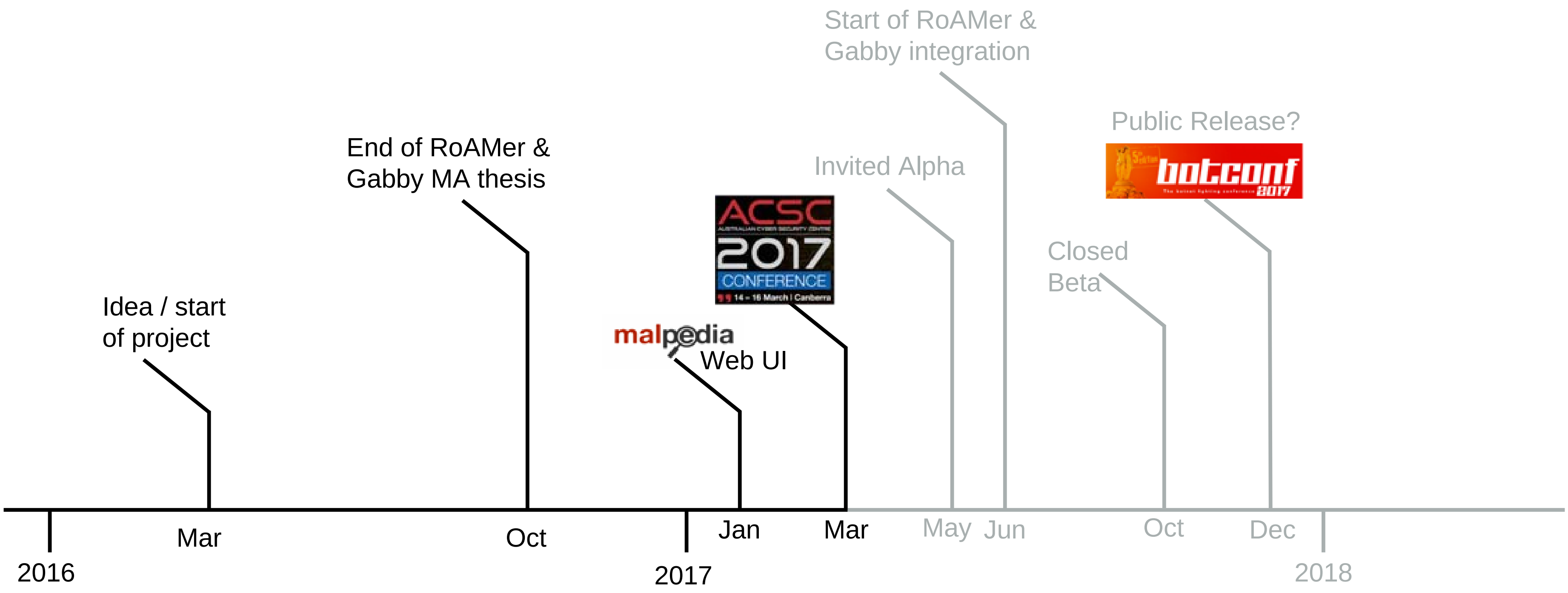
Gabby: A Malware Classification System Based On Structural Static Analysis

- Master‘s thesis by **Pavlo Hordiienko**:
  - *„Develop scalable algorithms to fingerprint unknown binary code and match it against a reference database.“*



[1] „ A Malware Classification System Based On Structural Static Analysis“. Hordiienko, P. Master‘s Thesis, 2016.

Roadmap
Timeline



Idea / start of project

End of RoAMer & Gabby MA thesis

Web UI

Start of RoAMer & Gabby integration

Invited Alpha

Closed Beta

Public Release?

Conclusion

Conclusion
Malpedia

- „Building bridges across the Malware Knowledge Archipelago“

- **A curated, high-quality malware corpus**
  - Coverage: as many families as possible
  - Focus on static analysis: dumped / unpacked representative samples
  - Context: Meta information

- Let me if you want to be notified about start of closed beta.
  - daniel.plohmann@fkie.fraunhofer.de
  - @push_pnx // @malpedia

- Request For Comments!

[1] https://grethascholtz.wordpress.com/2011/12/19/life-in-the-finnish-archipelago/

Thank You for Your Attention!

Daniel Plohmann
daniel.plohmann@fkie.fraunhofer.de

@push_pnx
@malpedia