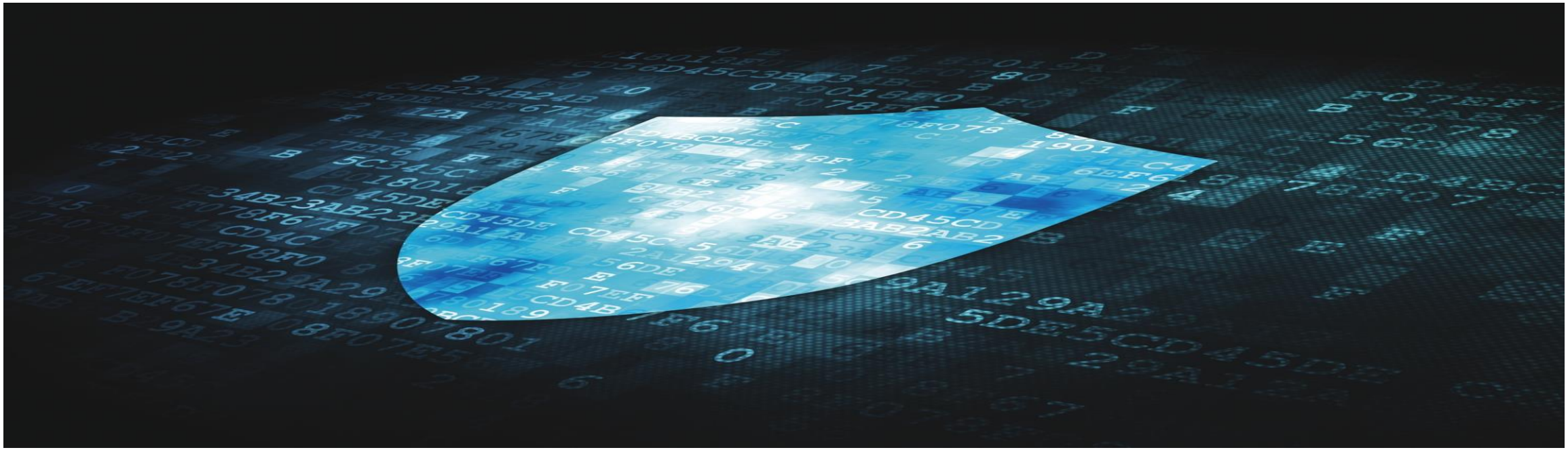
malpedia

Inventarisierung und Vergleich von Schadsoftware

Dr. Daniel Plohmann
daniel.plohmann@fkie.fraunhofer.de

2023-02-08 | 30. DFN-Konferenz, Hamburg



Fraunhofer FKIE

Einleitung
$whoami

Fraunhofer FKIE

universitätbonn

- IT-Sicherheitsforscher @ Fraunhofer FKIE & Universität Bonn
- Forschungsschwerpunkt:
  - Analyse von Schadsoftware / Reverse Engineering / Analyseautomation
- Aktivitäten:

RE tooling: IDAscope, ApiScout, SMDA, MCRIT, …

Botnet Takedowns

DGArchive malpedia

Datensätze

Fraunhofer FKIE

Einleitung
Inhalt

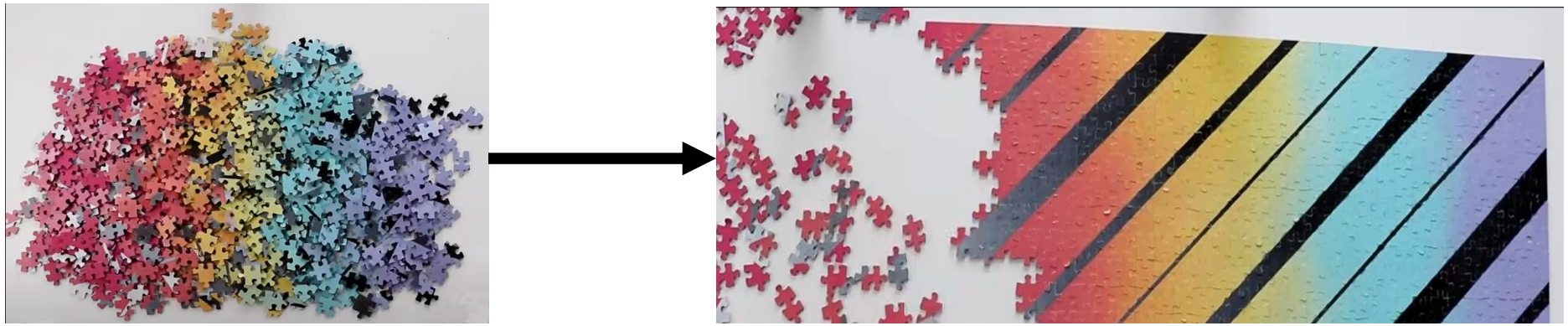
- Vorstellung Malpedia
  - Ursprung und Konzept
- Nutzungsaspekte
  - Integration
  - Statistische Auswertungen
  - Automatisierte Regelerstellung (YARA)
  - Codeähnlichkeitsanalysen

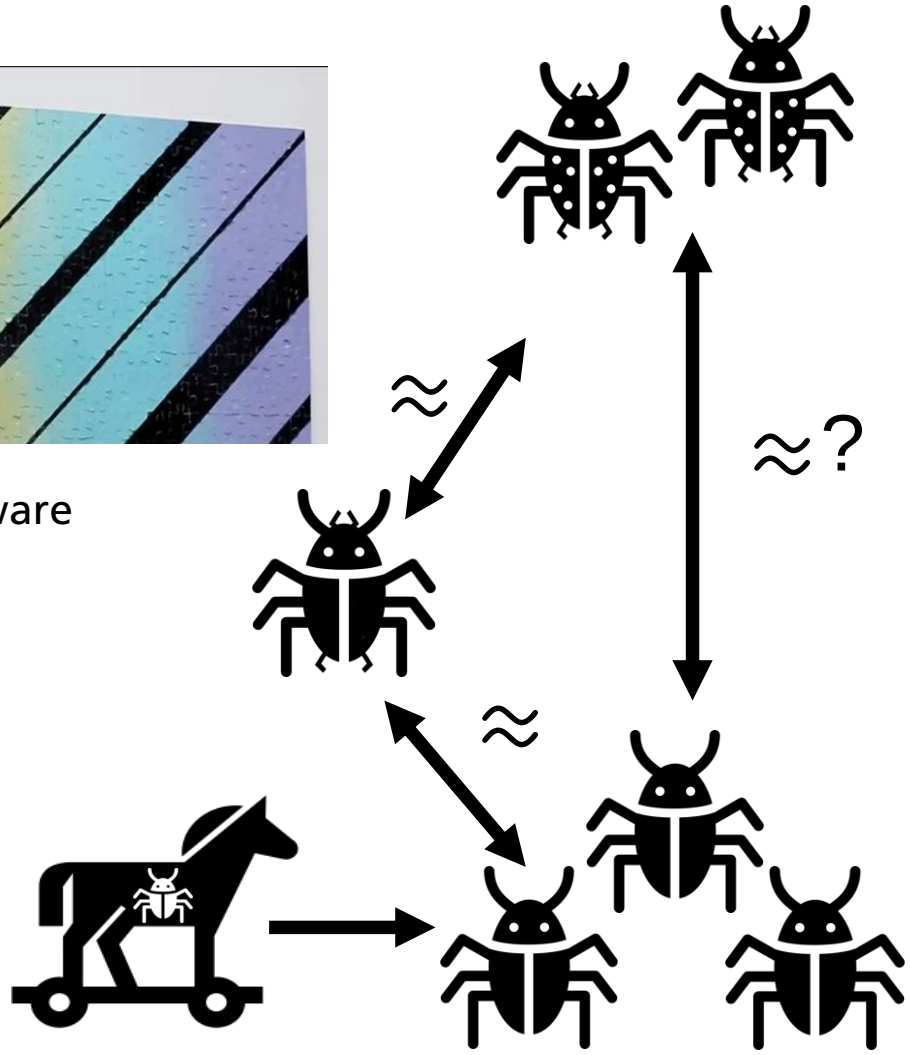
Ursprung und Konzept

Fraunhofer FKIE

Motivation

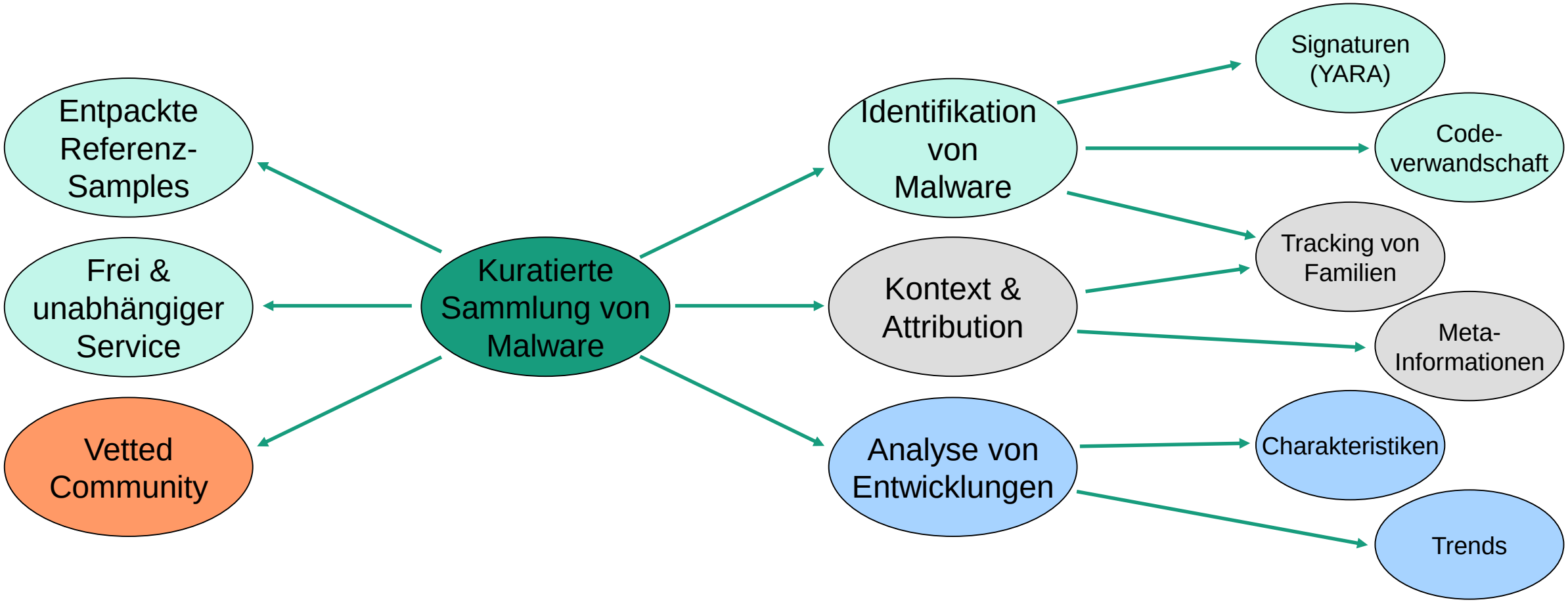
Zeitreise in die Vergangenheit: Situation 2016





- Stattliche Sammlung von „okay, aber nicht herausragend“ sortierter Malware
- Identifikation von Malware signifikantes Problem:
  - Packing
  - Evolution in Familien
  - viele Synonyme, …
- Gute Erfahrungen mit DGArchive – Übertragbar auf Schadsoftware?
  - Code-zentrischer Ansatz mit Fokus auf statischer Analyse
- Entwicklung des Projekts zusammen mit Steffen Enders

malpedia

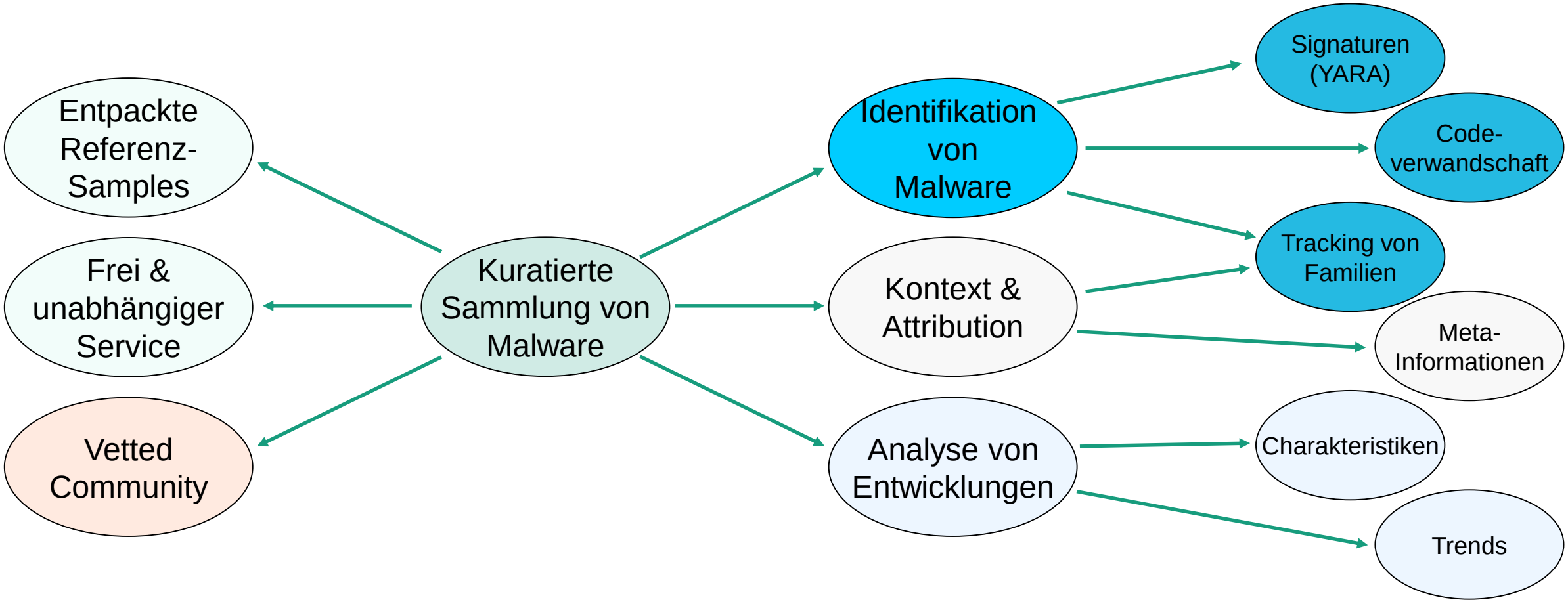


[1] https://malpedia.caad.fkie.fraunhofer.de
[2] https://malpedia.io

Fraunhofer FKIE

malpedia

Forschungs-schwerpunkte



[1] https://malpedia.caad.fkie.fraunhofer.de
[2] https://malpedia.io

Fraunhofer FKIE

malpedia

Library | Families | Actors

Click here to download all references as Bib-File.

Search...

Enter keywords to filter the library entries below or Propose new Entry

2023-01-31 · Darktrace · Roberto Martinez
Vidar Info-Stealer Malware Distributed via Malvertising on Google
Vidar

2023-01-30 · Checkpoint · Arie Olshtein
Following the Scent of TrickGate: 6-Year-Old Packer Used to Deploy the Most Wa
Agent Tesla | Azorult | Buer | Cerber | Cobalt Strike | Emotet | Formbook | HawkEye Keylogger | Loki Password St | REvil | TrickBot

2023-01-29 · Acronis · Ilan Duhin
Petya/Not Petya Ransomware Analysis
EternalPetya

2023-01-26 · ANY.RUN · ANY.RUN
CryptBot Infostealer: Malware Analysis
CryptBot

2023-01-26 · Mandiant · Govand Sinjari, Andy Morales
Welcome to Goot Camp: Tracking the Evolution of GOOTLOADER Operations
GootLoader

2023-01-26 · Palo Alto Networks Unit 42 · Mike Harbison, Jen Miller-Osborn
Chinese PlugX Malware Hidden in Your USB Devices?
PlugX

2023-01-26 · Acronis · Ilan Duhin
Unpacking Emotet Malware
Emotet

2023-01-26 · Recorded Future · Insikt Group
Title: BlueBravo Uses Ambassador Lure to Deploy GraphicalNeutrino Malware
GraphicalNeutrino

malpedia

Fraunhofer FKIE

Analytics | Inventory | Statistics | Usage | Users | pnx 14

Quicksearch...

win.graphical_neutrino (Back to overview)

GraphicalNeutrino

Actor(s): APT29

This loader abuses the benign service Notion for data exc

References

2023-01-26 · Recorded Future · Insikt Group
Title: BlueBravo Uses Ambassador Lure t
GraphicalNeutrino

There is no Yara-Signature yet.

Samples

Version	SHA256
	381a3c6c7e119f58dfde6f03a9890353a

MISP Threat Sharing

APT29 (Back to overview)

aka: Group 100, COZY BEAR, The Dukes, Minidionis, SeaDuke, YTTRIUM, IRON HEMLOCK, Grizzly Steppe, G0016, ATK7, Cloaked Ursa, TA421, Blue Kitsune, ITG11

A 2015 report by F-Secure describe APT29 as: 'The Dukes are a well-resourced, highly dedicated and organized cyberespionage group that we believe has been working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making. The Dukes show unusual confidence in their ability to continue successfully compromising their targets, as well as in their ability to operate with impunity. The Dukes primarily target Western governments and related organizations, such as government ministries and agencies, political think tanks, and governmental subcontractors. Their targets have also included the governments of members of the Commonwealth of Independent States;Asian, African, and Middle Eastern governments;organizations associated with Chechen extremism;and Russian speakers engaged in the illicit trade of controlled substances and drugs. The Dukes are known to employ a vast arsenal of malware toolsets, which we identify as MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke, and GeminiDuke. In recent years, the Dukes have engaged in apparently biannual large - scale spear - phishing campaigns against hundreds or even thousands of recipients associated with governmental institutions and affiliated organizations. These campaigns utilize a smash - and - grab approach involving a fast but noisy breakin followed by the rapid collection and exfiltration of as much data as possible.If the compromised target is discovered to be of value, the Dukes will quickly switch the toolset used and move to using stealthier tactics focused on persistent compromise and long - term intelligence gathering. This threat actor targets government ministries and agencies in the West, Central Asia, East Africa, and the Middle East; Chechen extremist groups; Russian organized crime; and think tanks. It is suspected to be behind the 2015 compromise of unclassified networks at the White House, Department of State, Pentagon, and the Joint Chiefs of Staff. The threat actor includes all of the Dukes tool sets, including MiniDuke, CosmicDuke, OnionDuke, CozyDuke, SeaDuke, CloudDuke (aka MiniDionis), and HammerDuke (aka Hammertoss). '

Associated Families

win.gdrive | win.miniduke | win.tdiscoverer | win.boombox | win.cozyduke | win.seadaddy | win.beatdrop | win.cloud_duke | win.cosmicduke | win.fatduke | win.liteduke | win.newpass | win.onionduke | win.pinchduke | win.polyglotduke | win.unidentified_098 | win.unidentified_099 | win.vapor_rage | win.graphical_neutrino

References

2023-01-26 · Recorded Future · Insikt Group
Title: BlueBravo Uses Ambassador Lure to Deploy GraphicalNeutrino Malware
GraphicalNeutrino

2022-11-30 · Qianxin Threat Intelligence Center · Red Raindrop Team
Analysis of APT29's attack activities against Italy
Unidentified 098 (APT29 Slack Downloader)

2022-09-21 · Check Point · Jiří Vinopal
Native function and Assembly Code Invocation
MiniDuke

[1] https://malpedia.caad.fkie.fraunhofer.de
[2] https://malpedia.io

malpedia

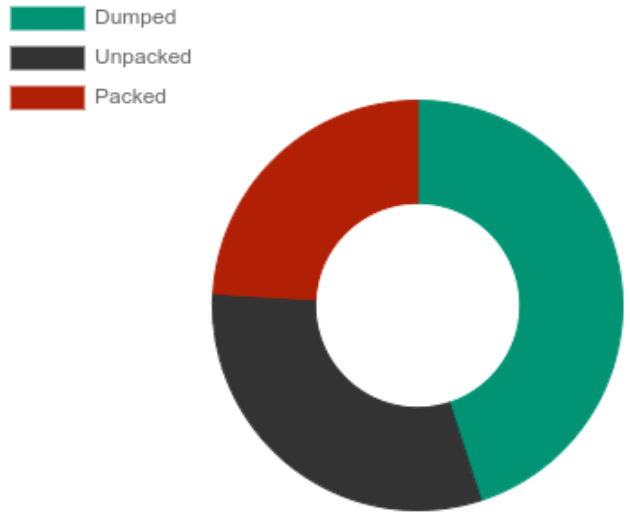
```
├──────── apk.anubis
[…]
├──────── win.urlzone
│         ├── win.urlzone.json
│         ├── 2014-11-08
│         │   ├── <sha256>
│         │   ├── <sha256>_dump_0x01e00000
│         │   └── <sha256>_unpacked
│         ├── 2015-04-29
│         │   ├── <sha256>
│         │   ├── <sha256>_dump_0x01e00000
│         │   └── <sha256>_unpacked
│         └── yara
│             └── tlp_green
│                 └── win.urlzone_g0.yar
[…]
├──────── win.zyklon
└── malpedia.bib
```

General Statistics

2707 Families

6998 Samples

Samples



- Git-Repository
  - Versionskontrolle, Abschottung, Synchronisation
  - Malware Samples:
    packed + unpacked und/oder memory dumped
  - Direkte Einbettung von YARA-Regeln und Metadaten

[1] https://malpedia.caad.fkie.fraunhofer.de
[2] https://malpedia.io

Fraunhofer FKIE

malpedia

	07. Dezember 2017	02. Februar 2023
Accounts	~120 (Launch)	2100+
Contributions	~300	16.805
Malware Families	614	2.707
Malware Samples	1.630	6.998
Referenzen	906	13.188
YARA-Regeln	113 / 116 / 20	1.737 / 245 / 152

→ ~ 70% Community-Anteil!

Herzlicher Dank an alle Beitragenden!

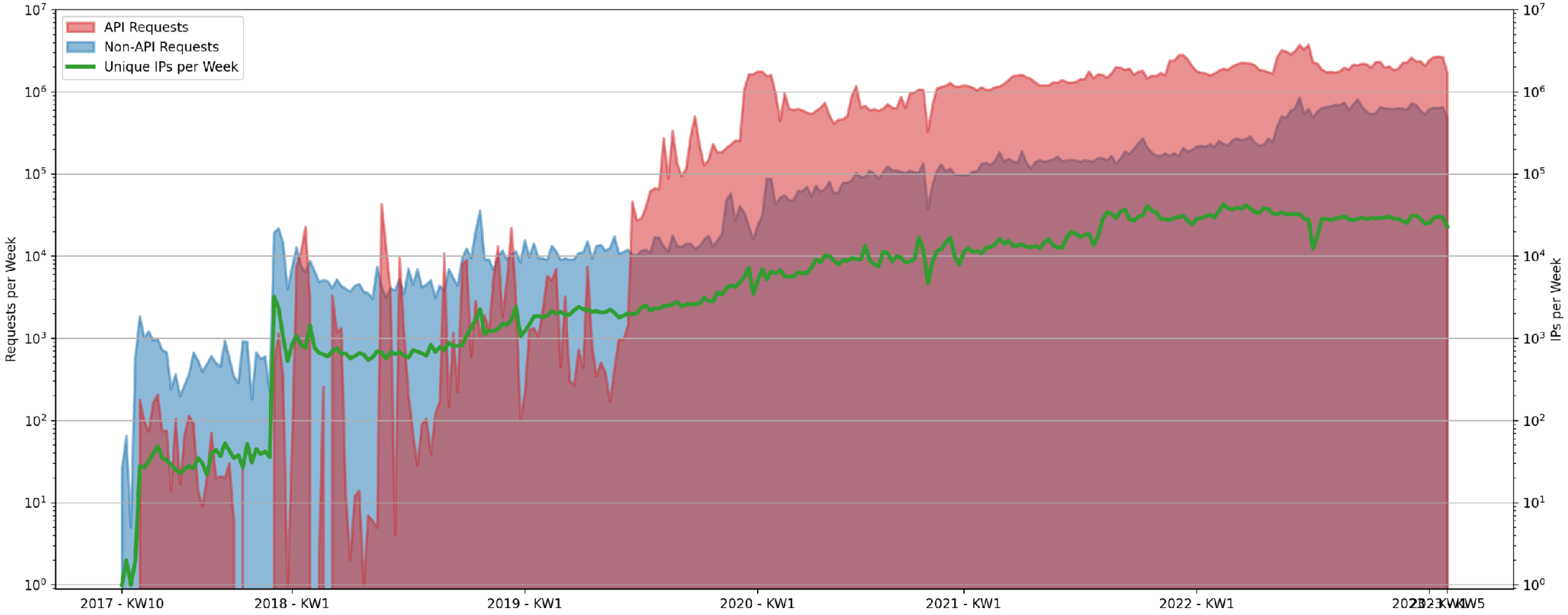
→ INTERNET ARCHIVE WayBackMachine

[1] https://malpedia.caad.fkie.fraunhofer.de
[2] https://malpedia.io

Fraunhofer FKIE

Aggregierte Nutzungsstatistiken

- Täglicher Durchschnitt, letzte 30 Tage:
  - 6.200 IPs
  - 475.000 Requests (380.000 API, also ~80%)
- Requests insgesamt seit Launch: 296.000.000



hofer
FKIE

Nutzungsaspekte

Nutzungsaspekte
Integration mit anderen Tools und Frameworks

- Kontextualisierung
  - Referenzen für Familien, Akteure, …
- Malware-Identifikation
  - YARA
  - Suche / Vergleich
  - Label Provider (Clustering)
- QA / Regression Testing
  - Analyse-Tools, Extraktoren, etc

[1] https://github.com/MISP/misp-galaxy/blob/main/clusters/malpedia.json

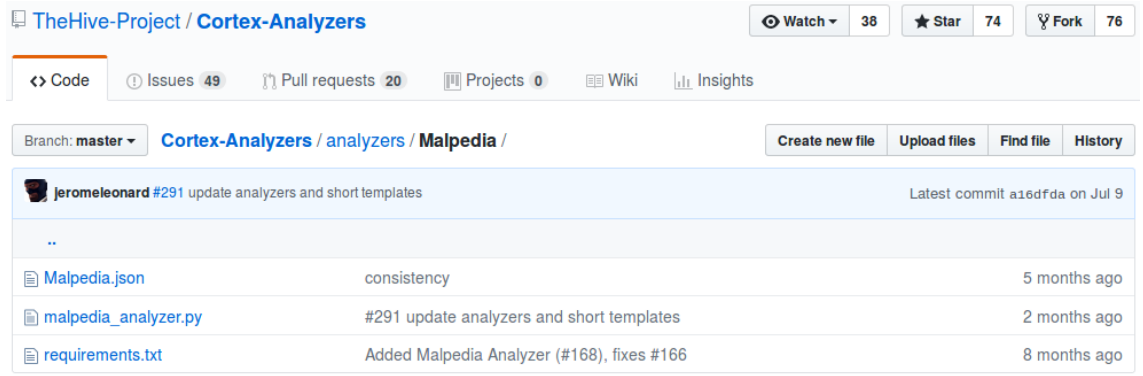
Nutzungsaspekte
Integration mit anderen Tools und Frameworks

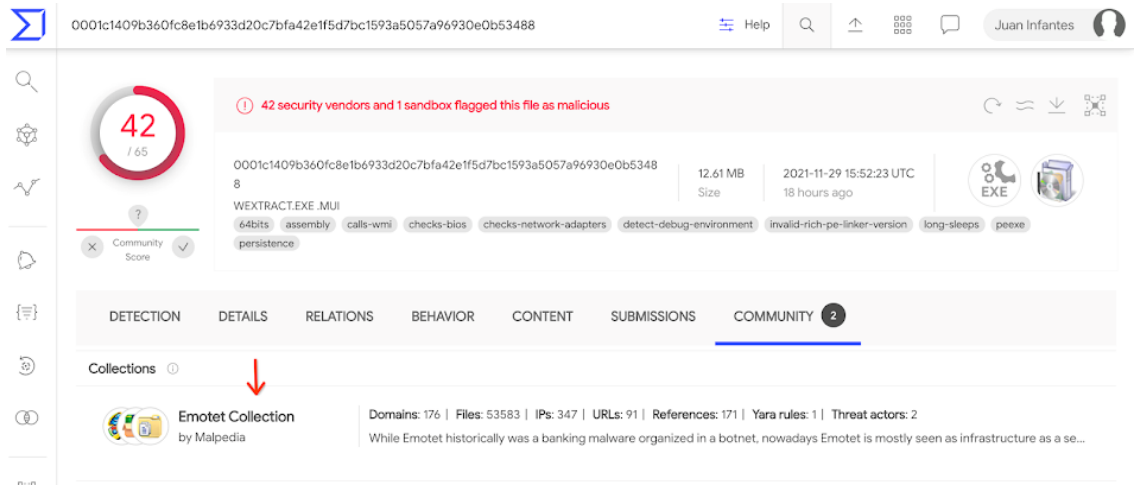
- Beispiele:
  - MISP
  - OpenCTI
  - IntelOwl

  Enrichment

  - MalwareBazaar, YARAify
  - TheHive Cortex
  - Unpac.me
  - CAPE Sandbox
  - VirusTotal
  - …

  YARA / Scanning





[1] https://github.com/TheHive-Project/Cortex-Analyzers
[2] https://blog.virustotal.com/2021/11/introducing-virustotal-collections.html

Nutzungsaspekte
Generierung von YARA-Regeln

- Idee:
  - Generierung passender YARA-Regeln für so viele Malware-Familien wie möglich
  - Automatisierung der Auswahlmethode für code-basierte YARA strings (byte sequences)
  - Qualitätskontrolle (vs. VT Goodware)

- Methode:
  - Disassemblierung -> Shingling -> Aggregation und Selektion via Datenbank

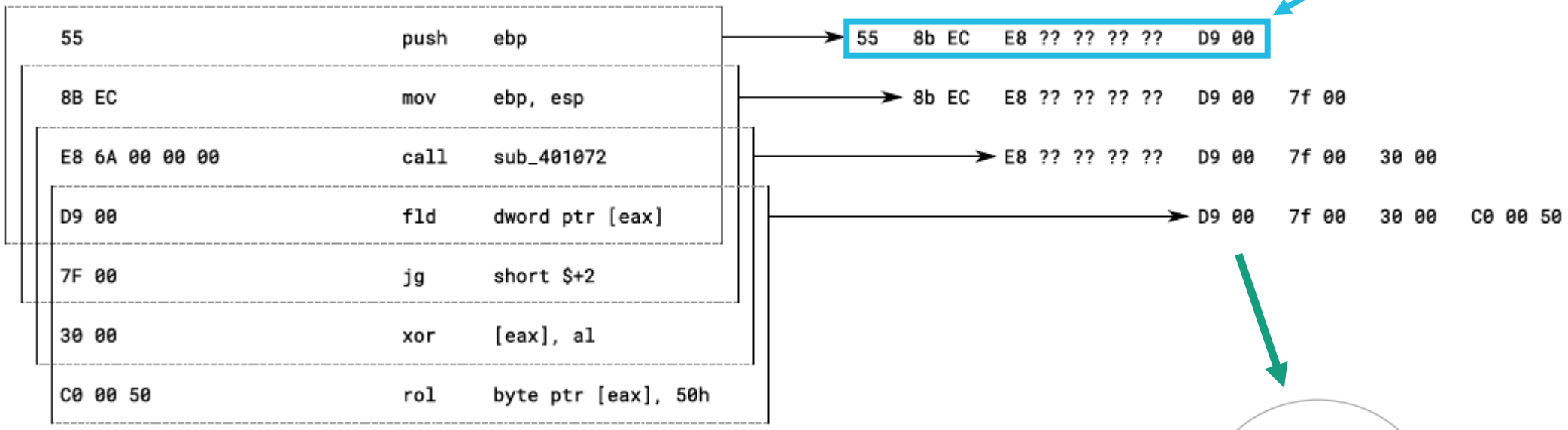
- Framework: YARA-Signator [1]
  - Ergebnis Bachelor Thesis von Felix Bilstein

[1] https://github.com/fxb-cocacoding/yara-signator

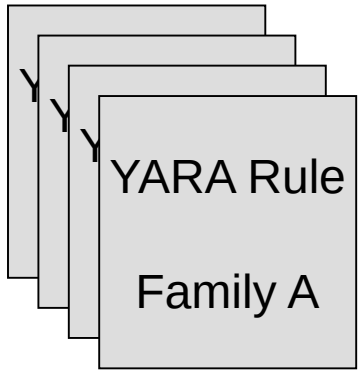
Nutzungsaspekte
Generierung von YARA-Regeln

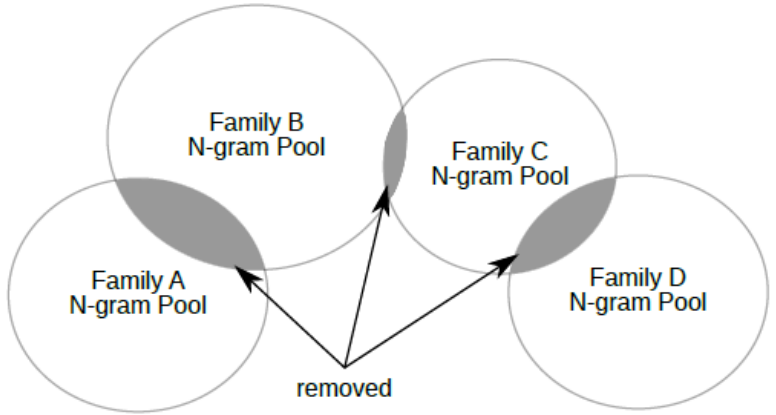
Berechnung über ~1.2 Milliarden solcher N-gramme

- Methode (Instruktions-N-gramme der Länge 4-7)




```
$sequence_1 = { ffd6 85c0 7512
                e8???????? eb03 }
  // n = 5, score = 4000
  //   ffd6         | call   esi
  //   85c0         | test   eax, eax
  //   7512         | jne    0x14
  //   e8????????   | call   ??
  //   eb03         | jmp    5
```





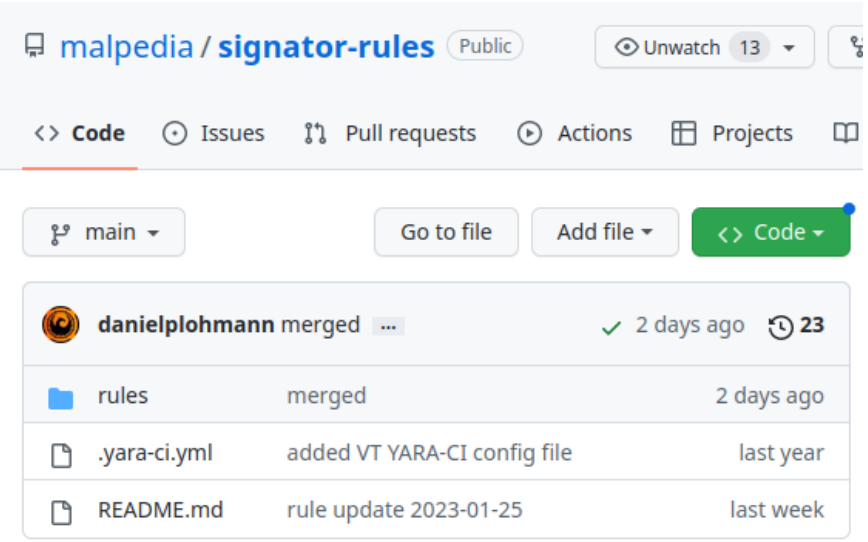
[1] F. Bilstein, D. Plohmann, “YARA-Signator: Automated Generation of Code-based YARA Rules”, In: The Journal on Cybercrime & Digital Investigations, v.5, 2019.

Fraunhofer FKIE

Nutzungsaspekte
Generierung von YARA-Regeln

- Malpedia's YARA-Signator rules
  - Monatlich neu generiert
  - Frei verfügbar (CC BY-SA 4.0) via Malpedia und Github [1]

```
Aktuelles Release:          2023-01-24
Samples:                       12.710
Detektierbar:                   5.244
Familien:                       2.696
----
Familien abgedeckt:             1.233
Saubere Regeln:                 1.132
----
False Positives:                   43
False Negatives:                  225
----
Precision:                      0,992
Recall:                         0,957
F1:                             0,974
```

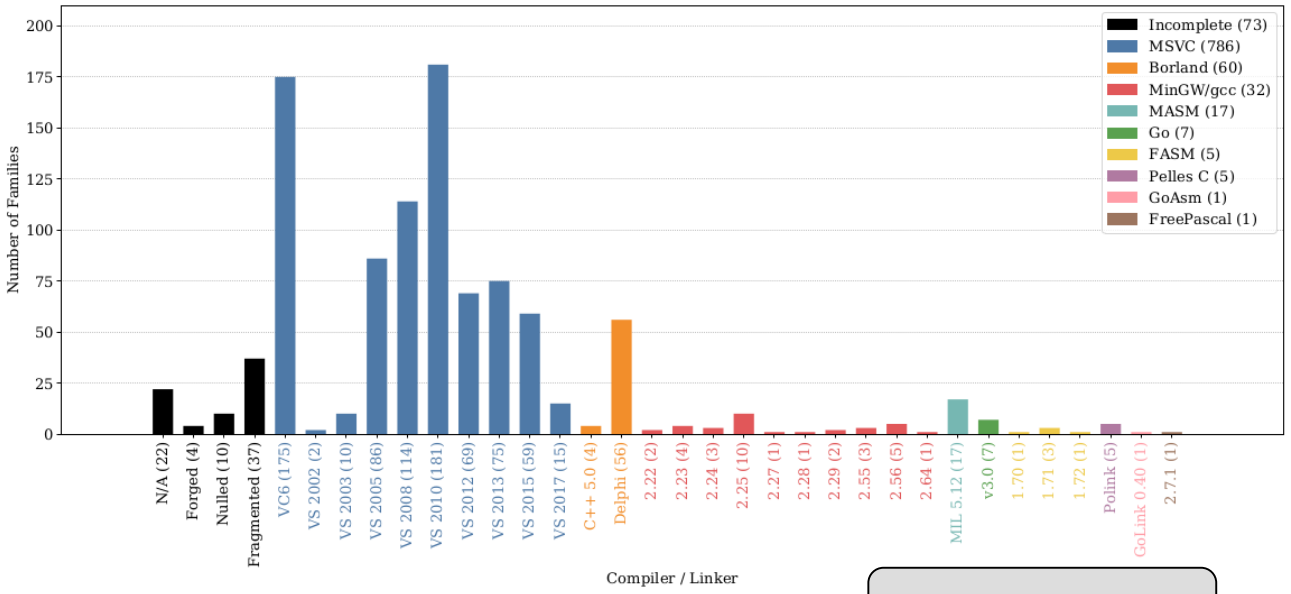


[1] https://github.com/malpedia/signator-rules/

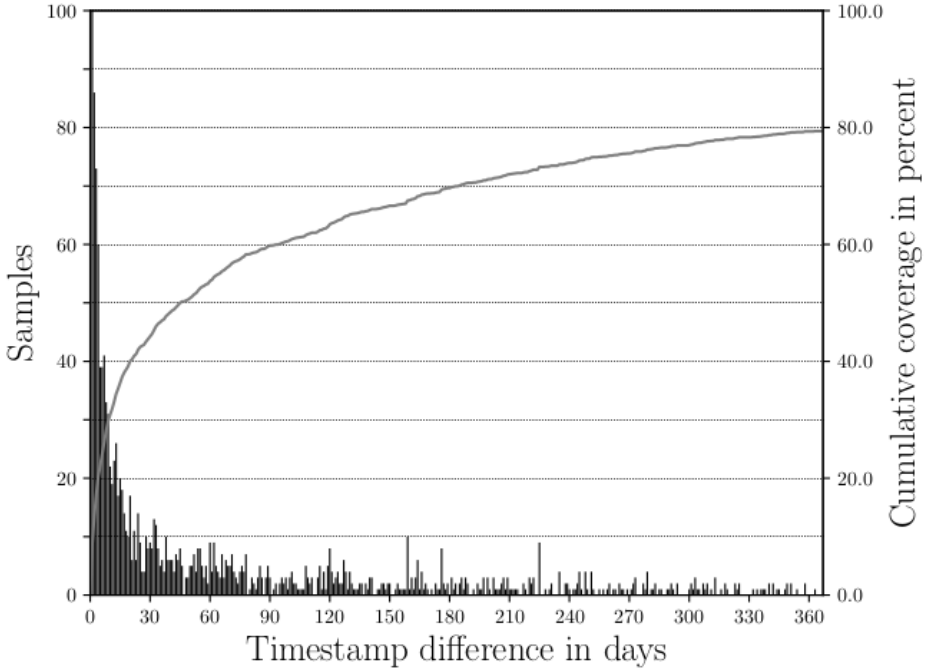
Fraunhofer FKIE

Nutzungsaspekte
Statistische Auswertungen

- PE Header
- Windows API
- (Code)



2023 – Go: 91!



	APIs	DLLs
Minimum	0	0
25%	79	5.27
50%	114	7.66
75%	169	10
Maximum	717	26
Mean	139.51	8.06
STD	106.36	3.99
Count	4,994	80

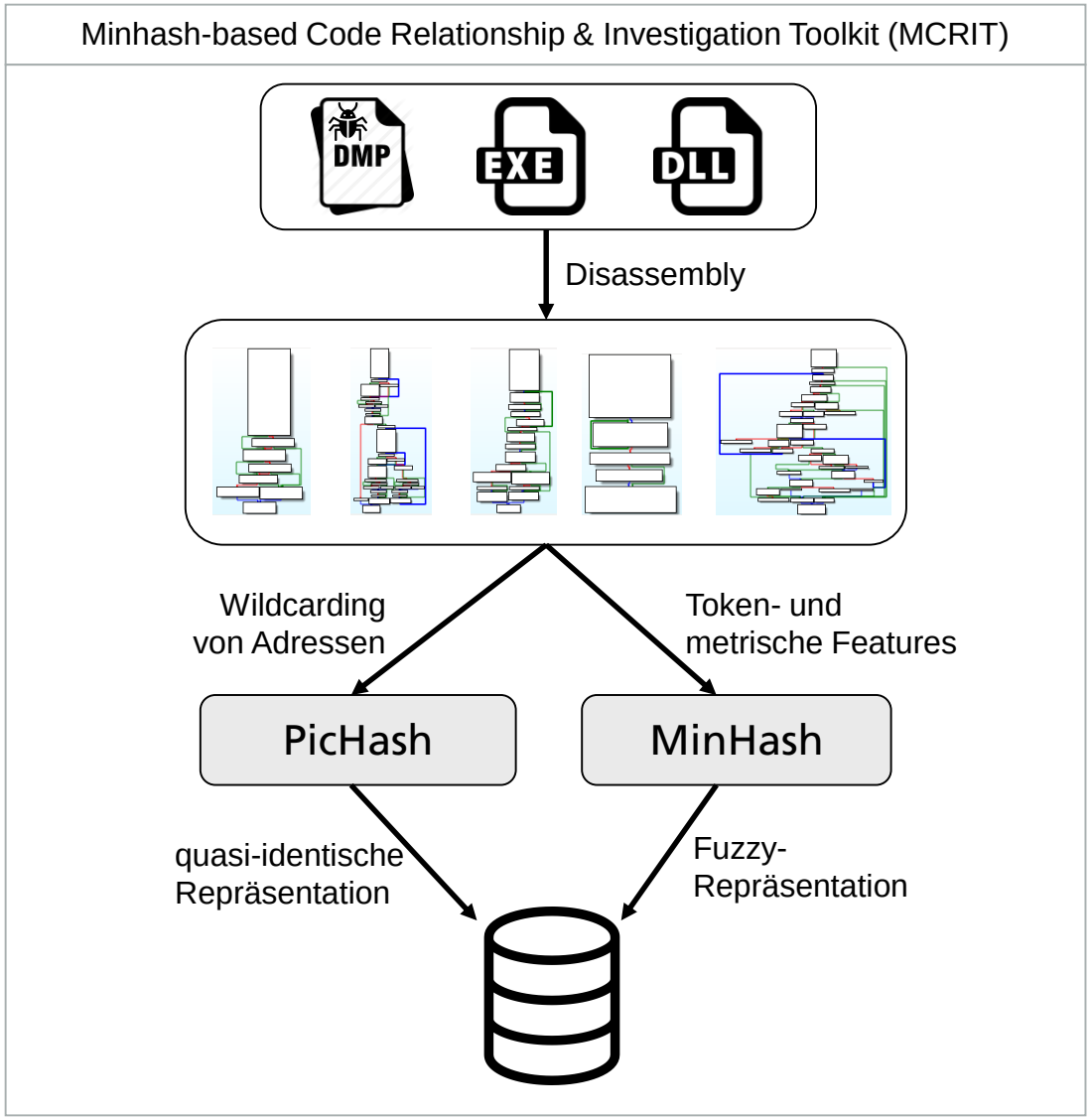
Table 5.5.: API and DLL Occurrence Frequencies per Family.

[1] D. Plohmann, „Classification, Characterization, and Contextualization of Windows Malware using Static Behavior and Similarity Analysis“, PhD Thesis, University of Bonn, 2022.

Fraunhofer FKIE

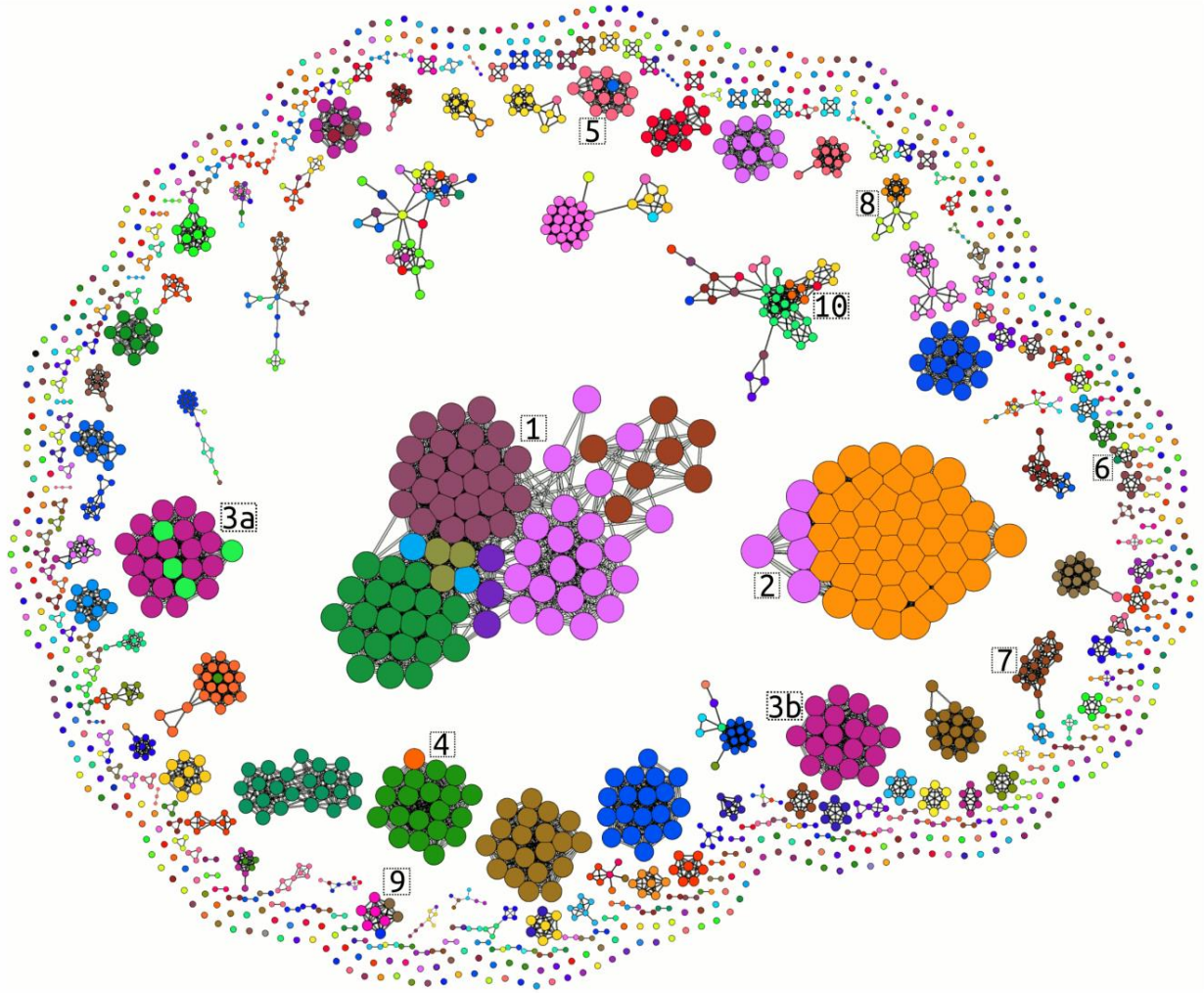
Nutzungsaspekte
Codeähnlichkeitsanalysen

- Ausgangslage 2019
  - Survey von Haq et al. [1]:
    50+ Arbeiten zu Codeähnlichkeit seit 2010
  - Kaum Arbeiten mit größeren Malware-Corpora
  - Nur 1 Arbeit zu FOSS-Nutzung in Malware (Alrabaee et al. [2])
- Anforderungen
  - Robuste Ähnlichkeitsbewertung
  - Skalierbarkeit bis Millionen von Funktionen
- MCRIT
  - Kombination von quasi-identischer und Fuzzy-Repräsentation von Code
  - Effizientes 1:n Matching von Samples via LSH
  - Release im April 2023 (Botconf)



[1] I. U. Haq and J. Caballero, "A survey of binary code similarity", In: Arxiv.org Computers & Security, 2019.
[2] S. Alrabaee, P. Shirani, L. Wang, and M. Debbabi, "FOSSIL: A Resilient and Efficient System for Identifying FOSS Functions in Malware Binaries", In: ACM Trans. Priv. Secur., vol. 21, 2018.

Nutzungsaspekte
Codeähnlichkeitsanalysen: Clustering



- Clustering Malpedia (link: 10%+ Ähnlichkeit)
  - Filterung von Bibliothekscode
  - Gewichtung via Häufigskeitsanalyse
- Ausgewählte Cluster:
  1) Zeus-like families
  2) Vmzeus / pandabanker
  3) Dridex (and Friedex), 32bit vs 64bit
  4) Locky + Locky Decryptor
  5) GPCode + CryptoFortress
  6) Sage Ransom, Crylocker, Ransoc
  7) ISFB + Snifula
  8) Pony + IcedID (module)
  9) Murofet + GameoverP2P + GameoverDGA
  10) Mismatches due to OpenSSL, VCTools (XTunnel, ZeusOpenSSL, RokRAT, …)

Nutzungsaspekte
Codeähnlichkeitsanalysen: Identifikation

LockBit ransomware goes 'Green,' uses new Conti-based encryptor

By Lawrence Abrams — February 1, 2023 — 05:48 PM — 0

The LockBit ransomware gang has again started using encryptors based on other operations, this time switching to one based on the leaked source code for the Conti ransomware.

Since its launch, the LockBit operation has gone through numerous iterations of its encryptor, starting with a custom one and moving to LockBit 3.0 (aka LockBit Black), which is derived from the BlackMatter gang's source code.

This week, cybersecurity collective VX-Underground first reported that the ransomware gang is now using a new encryptor named 'LockBit Green,' based on the leaked source code of the now-disbanded Conti gang.

num_samples	6243
num_families	1440
num_functions	6995154
num_pichashes	1464810

Query Sample

Drop file or click here to import

45c317_lockbit_green.exe

- (•) **Unmapped**
- ( ) **Dumped**

Minhash Matching: Standard

Submit

[1] https://www.bleepingcomputer.com/news/security/lockbit-ransomware-goes-green-uses-new-conti-based-encryptor/
[2] lockbit green: 45c317200e27e5c5692c59d06768ca2e7eeb446d6d495084f414d0f261f75315

Best Family Matches

total: 1070, showing: 1 - 10

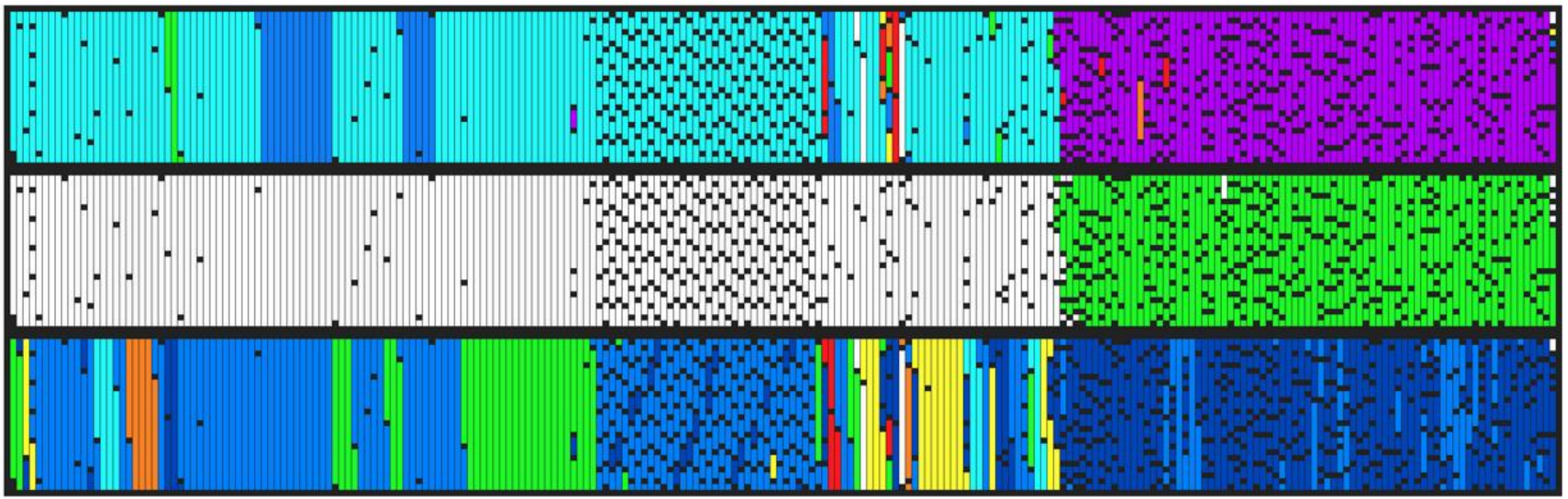
	Version		SHA256	Filename	Bitness	FNs	Min#	Pic#	Lib	Direct		Frequency	
win.meow		2172	222e2b91	222e2b91f5...3_unpacked	32	702	461	126	220	66	71	41	53
win.conti	2021-02-04	5041	a5751a46	a5751a4676...6_unpacked	32	736	516	183	256	59	58	28	36
win.scarecrow		6199	bcf49782	bcf49782d7...a_unpacked	32	653	582	271	334	61	51	27	32
win.lockergoga	2019-03-18	4517	edae201c	c97d9bbc80...0x00400000	32	7847	369	311	352	26	1	3	0
win.void		1460	2fd1863e	2fd1863eb3...c_unpacked	32	7123	366	312	351	26	1	3	0
win.bandook		4792	fabce973	fabce973a9...7_unpacked	32	3229	363	306	349	25	1	3	0

Best Family Matches

total: 1070, showing: 1 - 10

	Version		SHA256	Filename	Bitness	FNs	Min#	Pic#	Lib	Direct		Frequency	
win.meow		2172	222e2b91	222e2b91f5...3_unpacked	32	702	461	126	220	66	71	41	53
win.conti	2021-02-04	5041	a5751a46	a5751a4676...6_unpacked	32	736	516	183	256	59	58	28	36
win.scarecrow		6199	bcf49782	bcf49782d7...a_unpacked	32	653	582	271	334	61	51	27	32

Showing: foreign family match frequency, library matches, best foreign family match scores.

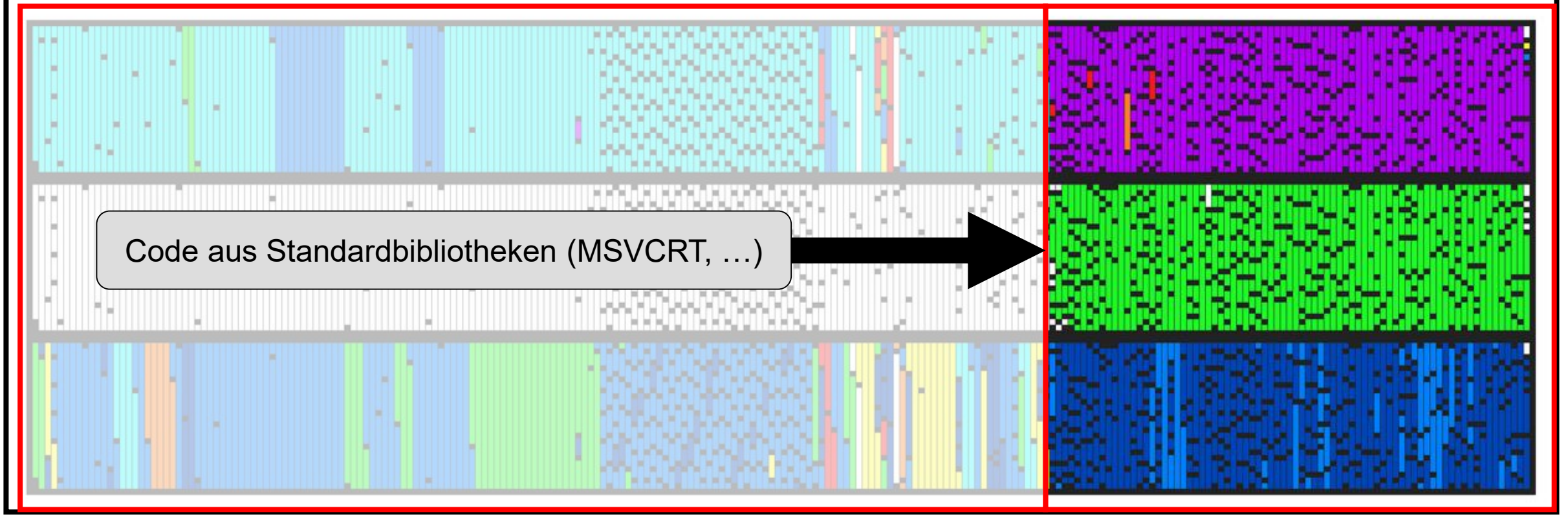


Best Family Matches

total: 1070, showing: 1 - 10

	Version		SHA256	Filename	Bitness	FNs	Min#	Pic#	Lib	Direct		Frequency	
win.meow		2172	222e2b91	222e2b91f5...3_unpacked	32	702	461	126	220	66	71	41	53
win.conti	2021-02-04	5041	a5751a46	a5751a4676...6_unpacked	32	736	516	183	256	59	58	28	36
win.scarecrow		6199	bcf49782	bcf49782d7...a_unpacked	32	653	582	271	334	61	51	27	32

Showing: foreign family match frequency, library matches, best foreign family match scores.

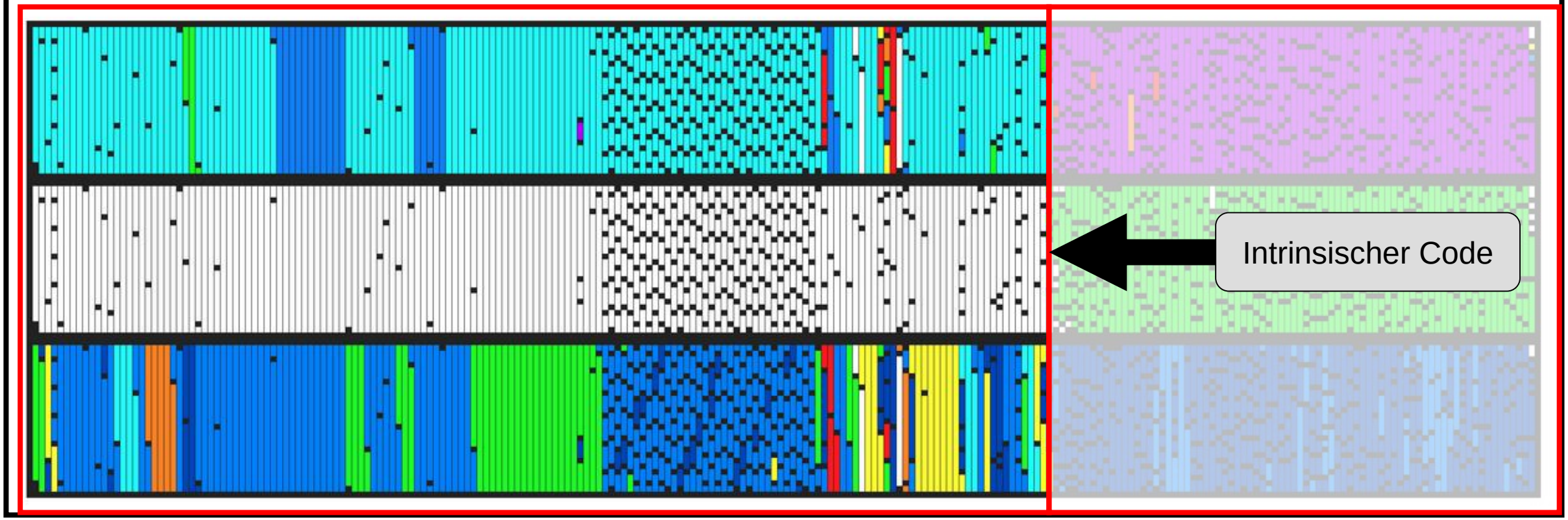


Best Family Matches

total: 1070, showing: 1 - 10

	Version		SHA256	Filename	Bitness	FNs	Min#	Pic#	Lib	Direct		Frequency	
win.meow		2172	222e2b91	222e2b91f5...3_unpacked	32	702	461	126	220	66	71	41	53
win.conti	2021-02-04	5041	a5751a46	a5751a4676...6_unpacked	32	736	516	183	256	59	58	28	36
win.scarecrow		6199	bcf49782	bcf49782d7...a_unpacked	32	653	582	271	334	61	51	27	32

Showing: foreign family match frequency, library matches, best foreign family match scores.



[1] conti: a5751a46768149c5ddf318fd75afc66b3db28a5b76254ee0d6ae27b21712e266

Function CFGs

Show Cycles | Show Loops | Show Loop Boundaries | Enable Tooltip

go to top

lockbit
@0x401730

conti
@0x10017a0

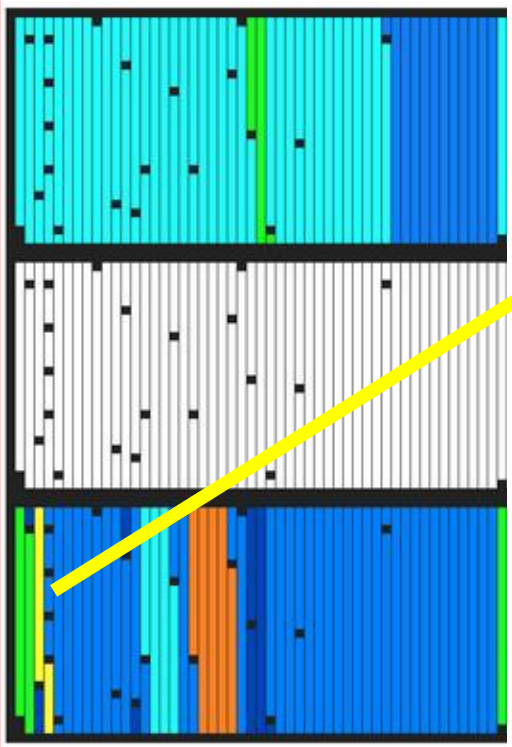
Best Family Match

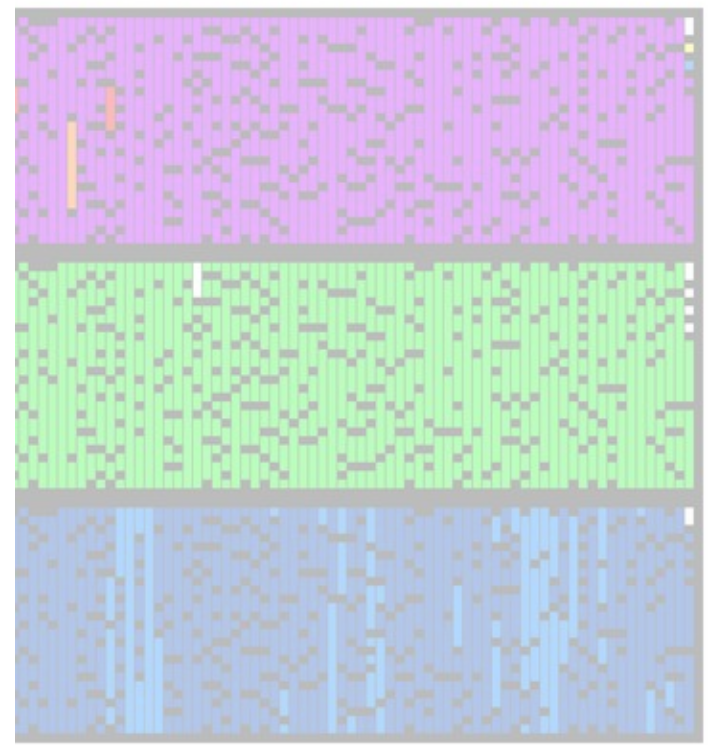
total: 1070, showing: 1 - 10

	Version
win.meow	
win.conti	2021-02-
win.scarecrow	

Min#	Pic#	Lib	Direct		Frequency	
461	126	220	66	71	41	53
516	183	256	59	58	28	36
582	271	334	61	51	27	32

Showing: foreign family match freque





Zusammenfassung

Zusammenfassung

- Vorstellung Malpedia
  - Ursprung und Konzept
- Nutzungsaspekte
  - Integration
  - Statistische Auswertungen
  - Automatisierte Regelerstellung
  - Codeähnlichkeitsanalysen

[1] https://twitter.com/stvemillertime/status/1515011501446377484

Fraunhofer FKIE

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Daniel Plohmann
daniel.plohmann@fkie.fraunhofer.de

@push_pnx
@malpedia

Fraunhofer FKIE