Unmasking APTs: An Automated Approach for Real-World Threat Attribution

Aakanksha Saha, Jorge Blasco, Lorenzo Cavallaro, Martina Lindorfer

TU WIEN

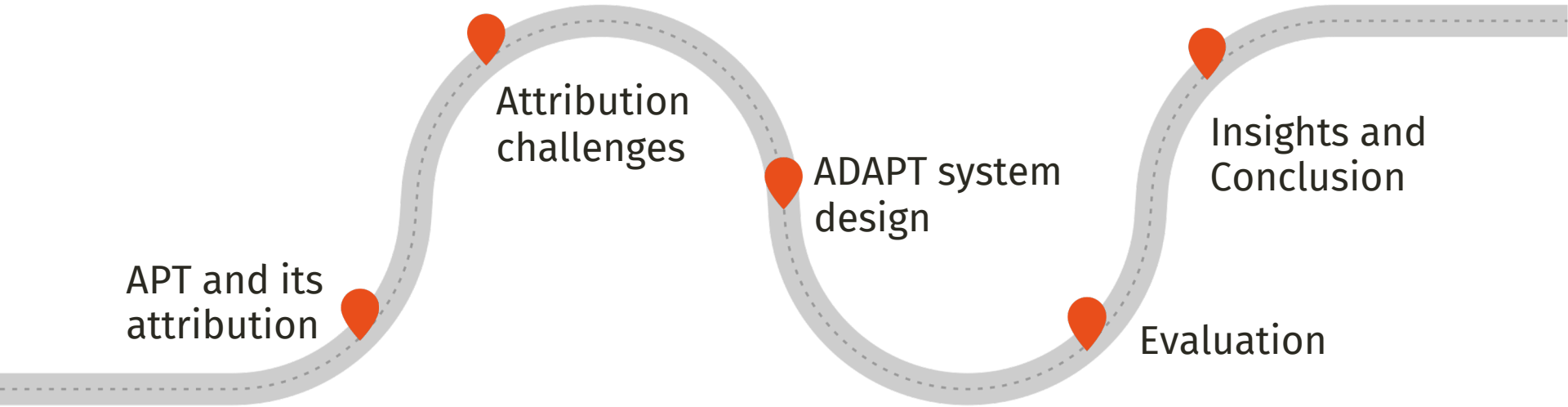
S&P Security & Privacy

UNIVERSIDAD POLITÉCNICA DE MADRID

UCL

Researcher at TU Wien
Masters from University of Utah
Previously: Red Teamer @ MSFT
Passionate about ML and security
Enjoy Stargazing

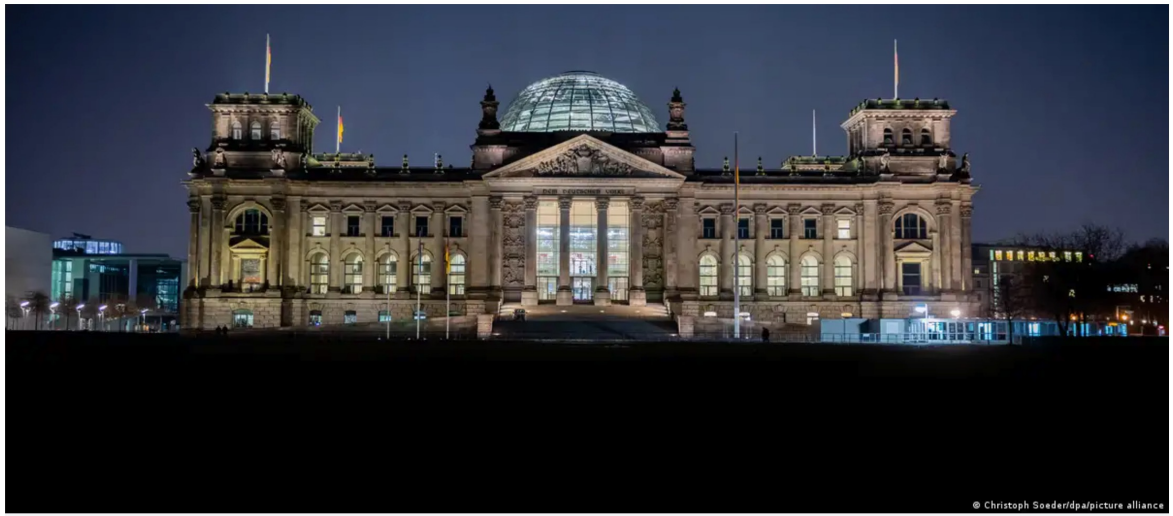
Roadmap


APT and its attribution
Attribution challenges
ADAPT system design
Evaluation
Insights and Conclusion

Russia-backed hackers target German legislators: report

Farah Bahgat
03/26/2021

A "Ghostwriter" cyberattack affected seven Bundestag members and 31 state parliamentarians, according to a Spiegel report. The hackers reportedly launch campaigns that "align" with Russian interests.



Sophisticated attacks against specific targets

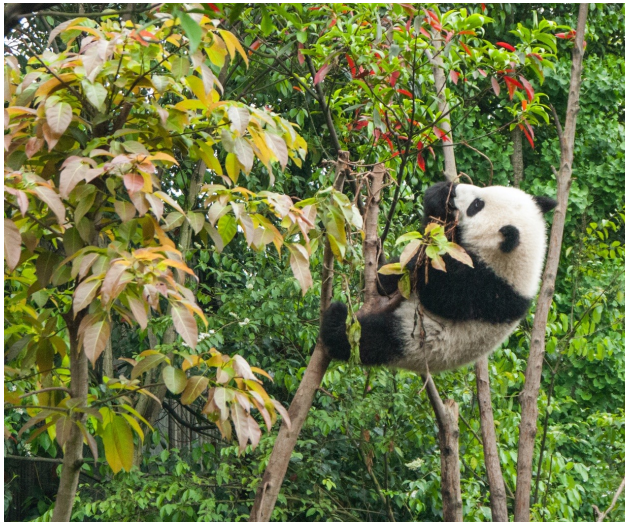
Experienced teams of cybercriminals

What is (AP)threat attribution?

Associate a cyber-attack to an attacker

Analysts link the activity to a known threat actor/group

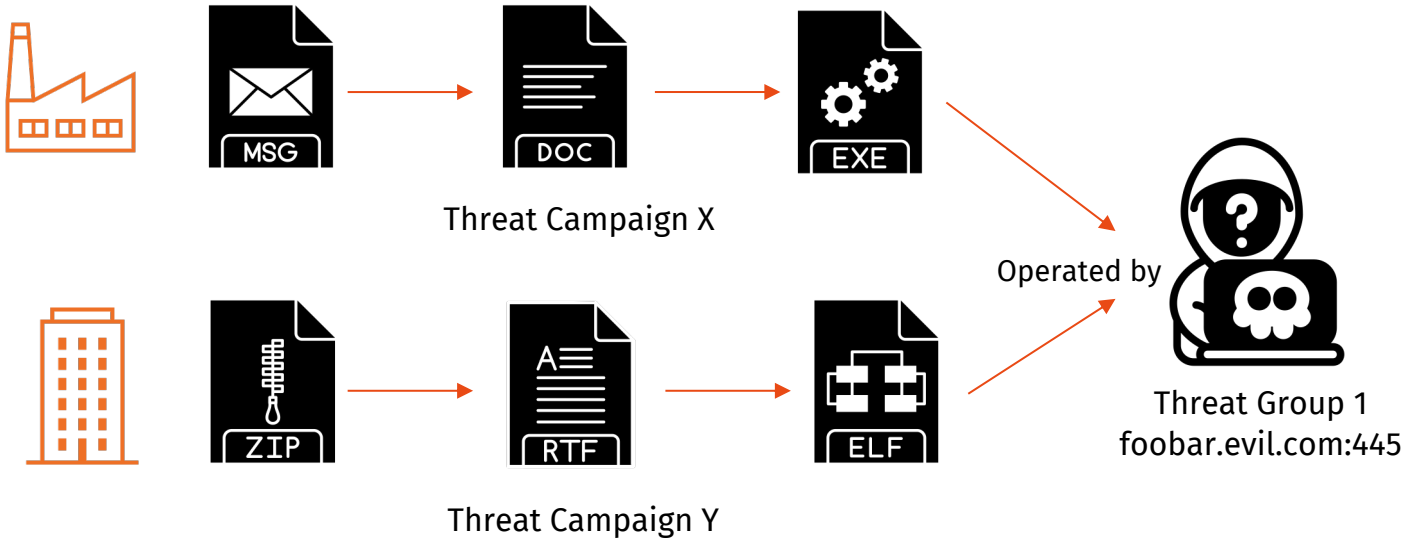
In October 2020, the Council of the European Union announced sanctions imposed on Russian military intelligence officers, belonging to the 85th Main Centre for Special Services (GTsSS), for their role in the 2015 attack on the German Federal Parliament (Deutscher Bundestag). The 85th Main Centre for Special Services (GTsSS) is the military unit of the Russian government also tracked as APT28 (aka Fancy Bear, Pawn Storm, Sofacy Group, Sednit, and STRONTIUM).



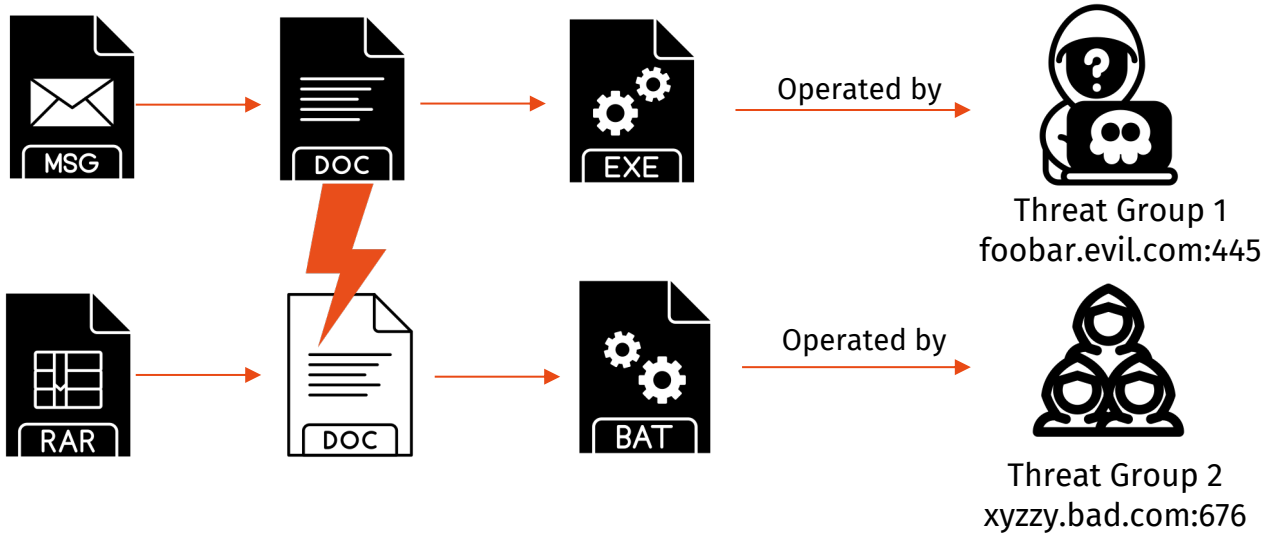
Attribution is challenging!

Campaign variation



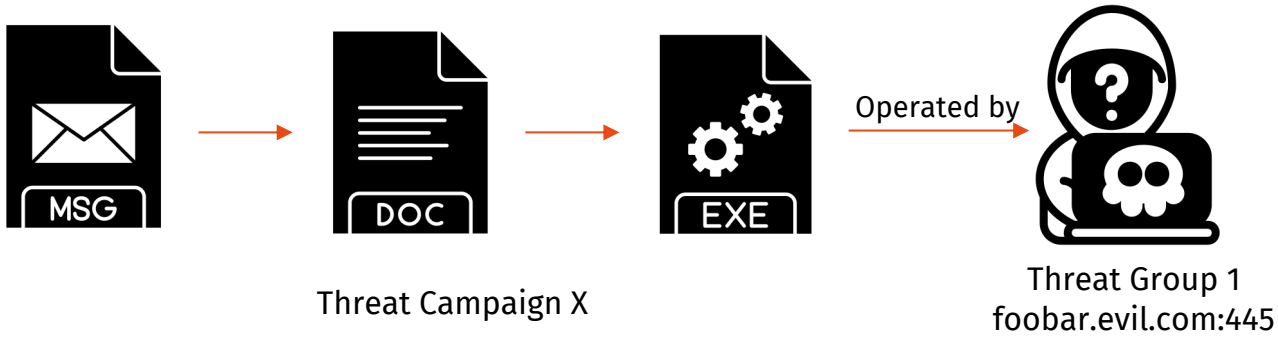
- Incomplete understanding of adversary with vendors tracking groups from varied campaign perspectives [AT&T AlienLabs, 2021]

Shared similarity



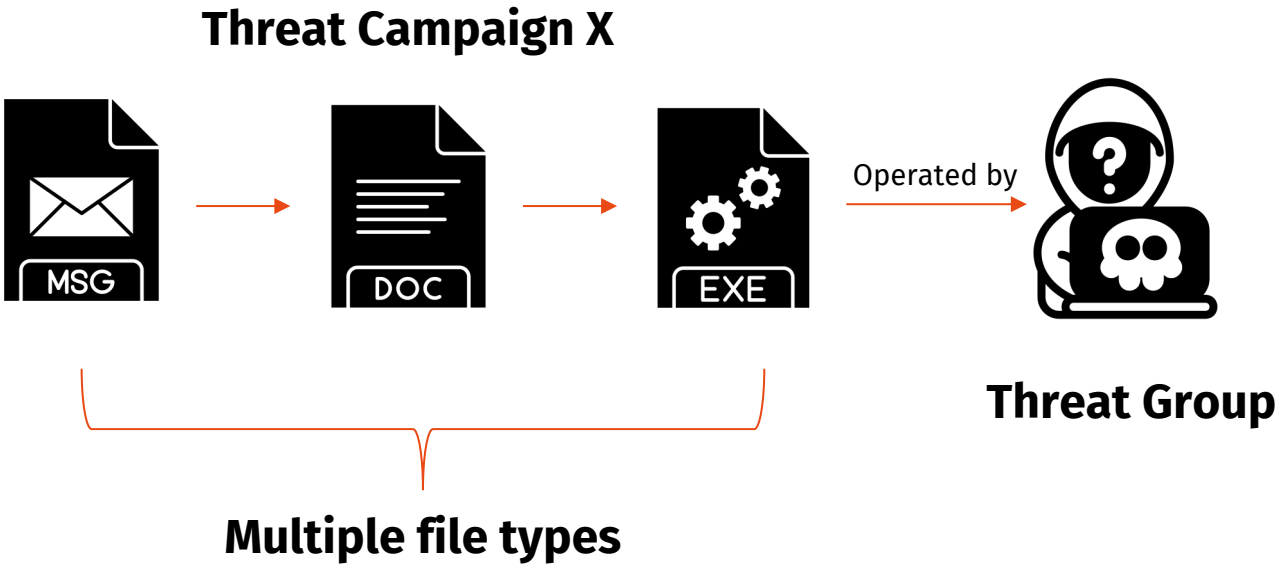
- Adoption of shared similarities, false flags and collaboration between subgroups results in inconsistent and erroneous attribution [Mandiant, 2023]

Heterogeneous files in attack chain



- Manual analysis of heterogenous files to identify the threat group [Mandiant, 2022]

Putting it all together



Approach ADAPT
Attribution of Diverse APT Samples

Campaign Attribution

Identify characteristics of attack
+ Prioritization of detection and mitigation

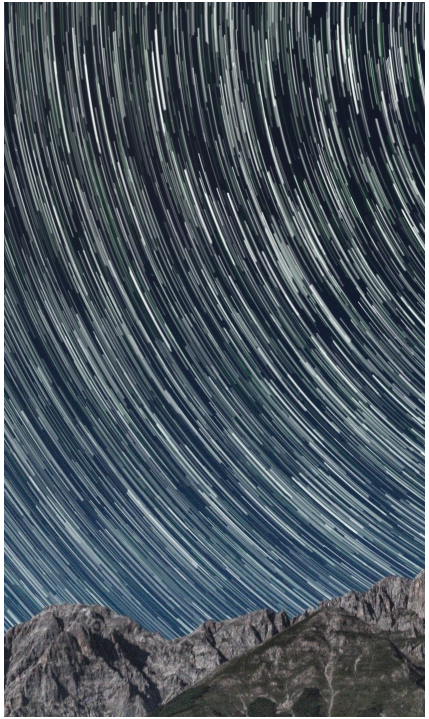
Group Attribution

Identify characteristics of attacker
+ Aid forensic investigation and indictments

ADAPT system design

Dataset Collection

Feature Extraction



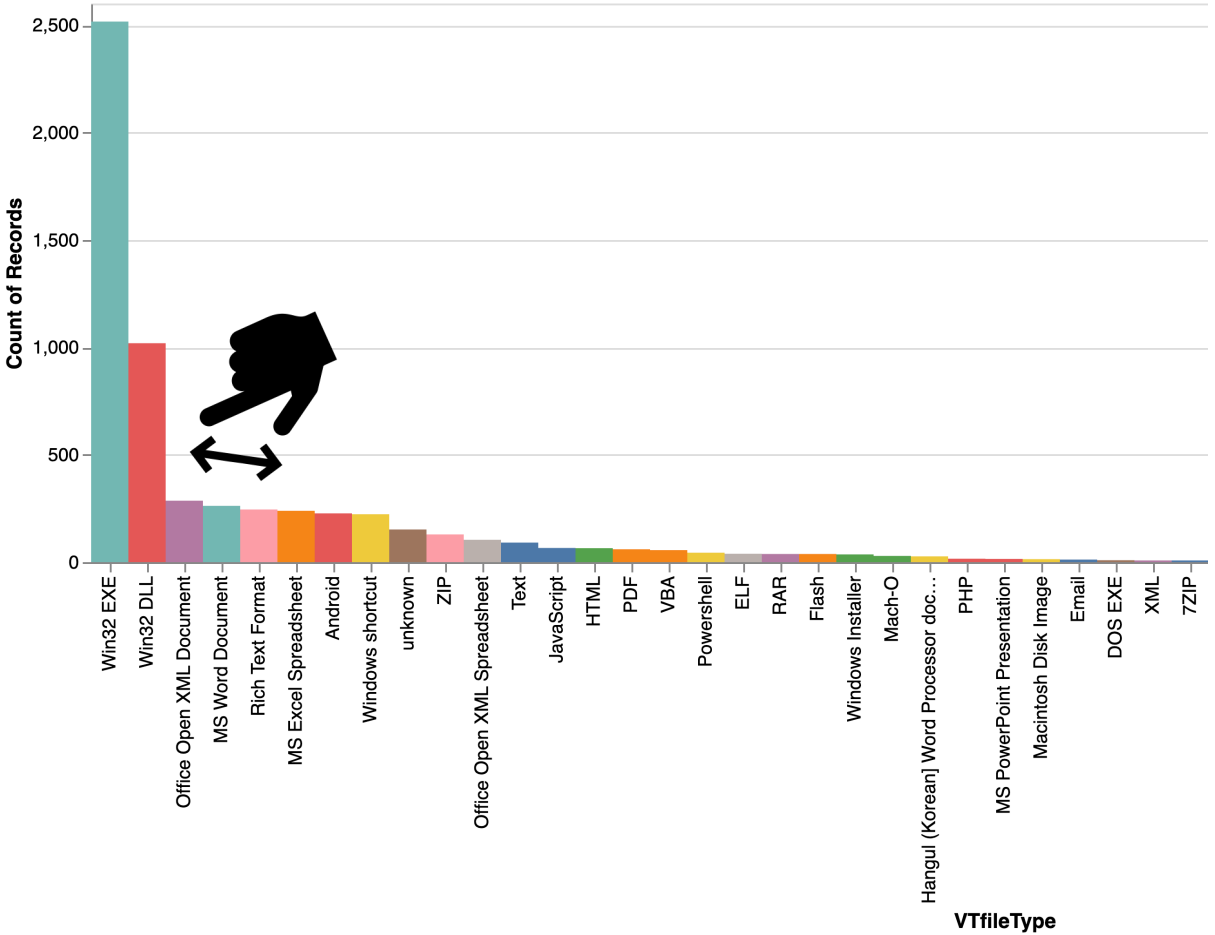
Feature Transformation

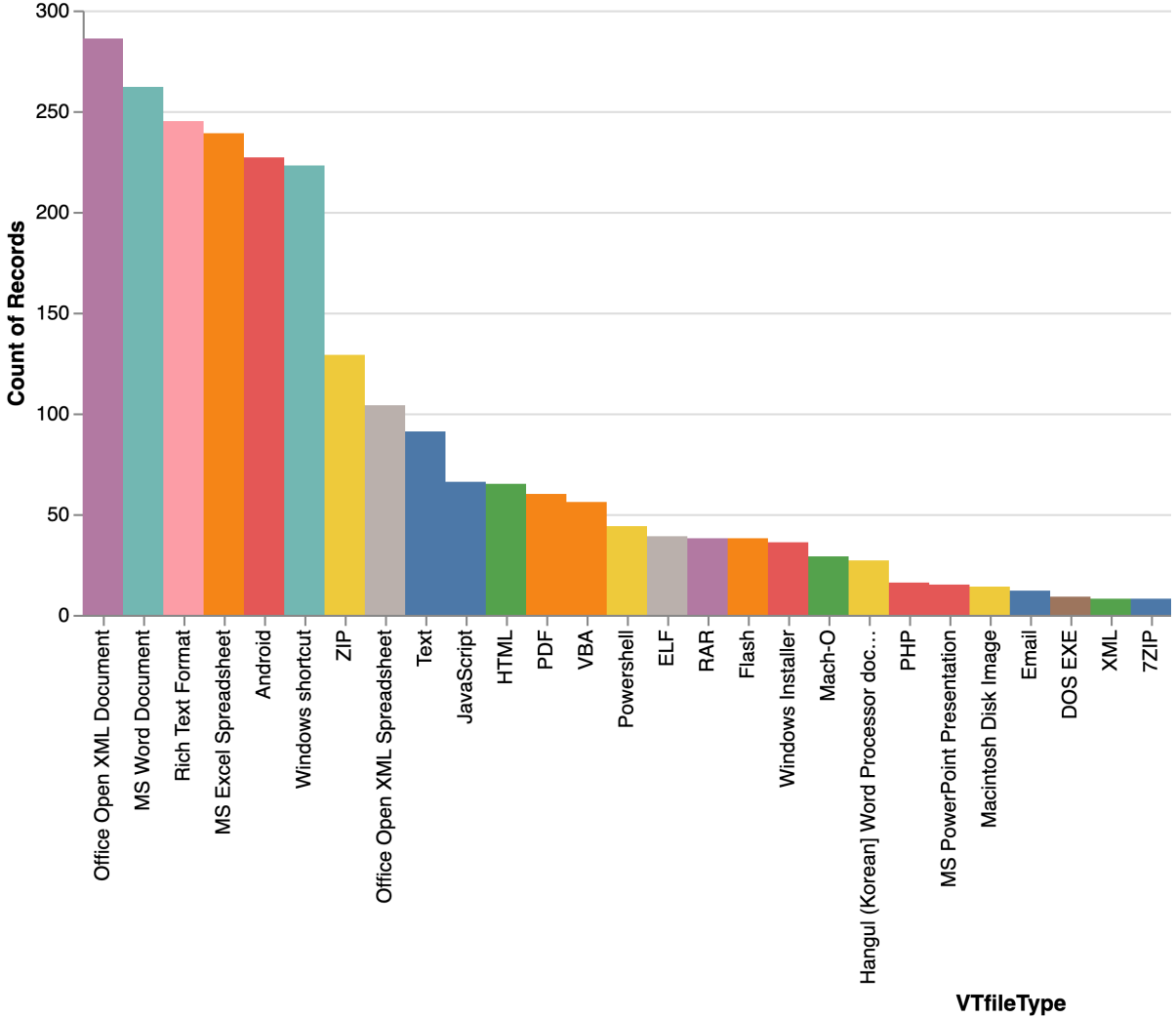
Clustering

APT dataset

- 6,455 samples
- 22+ file types
- 172 APT groups

Dataset quality: Filetype




Count of Records
300
250
200
150
100
50
0
Office Open XML Document
MS Word Document
Rich Text Format
MS Excel Spreadsheet
Android
Windows shortcut
ZIP
Office Open XML Spreadsheet
Text
JavaScript
HTML
PDF
VBA
Powershell
ELF
RAR
Flash
Windows Installer
Mach-O
Hangul (Korean) Word Processor doc...
PHP
MS PowerPoint Presentation
Macintosh Disk Image
Email
DOS EXE
XML
7ZIP
VTfileType

Dataset quality: Group label

2,260 (35.01%) have more than 1 label

Previous name	New name	Origin/Threat	Other names
ACTINIUM	Aqua Blizzard	Russia	UNC530, Primitive Bear, Gamaredon
AMERICIUM	Pink Sandstorm	Iran	Agrius, Deadwood, BlackShadow, SharpBoys
BARIUM	Brass Typhoon	China	APT41
BISMUTH	Canvas Cyclone	Vietnam	APT32, OceanLotus
BOHRIUM	Smoke Sandstorm	Iran	
BROMINE	Ghost Blizzard	Russia	Energetic Bear, Crouching Yeti
CERIUM	Ruby Sleet	North Korea	
CHIMBORAZO	Spandex Tempest	Financially motivated	TA505
CHROMIUM	Charcoal Typhoon	China	ControlX
COPERNICIUM	Sapphire Sleet	North Korea	Genie Spider, BlueNoroff
CURIUM	Crimson Sandstorm	Iran	TA456, Tortoise Shell

Dataset (re)-labeling

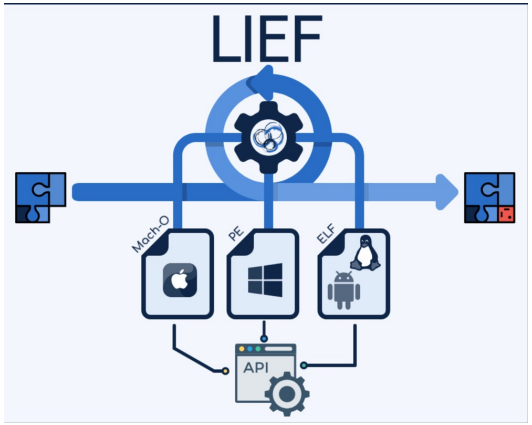
- Standardize aliases
- Consistent naming convention
- Non-unique names and non-APT samples

6,134 samples assigned to 92 groups

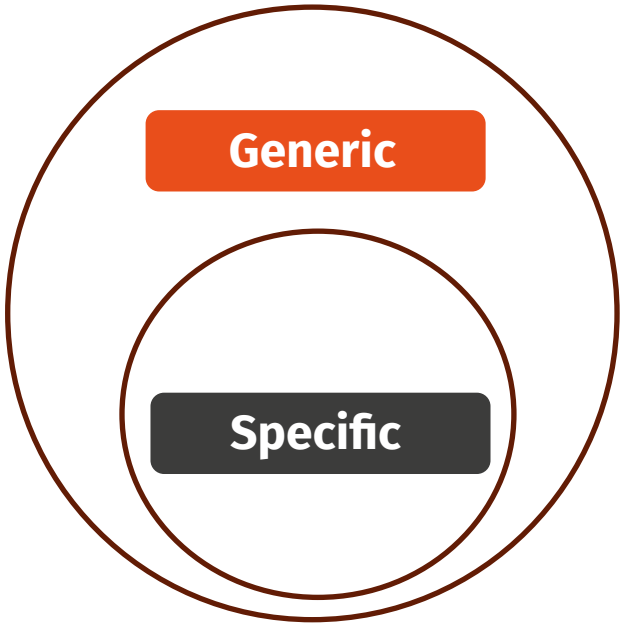
** The standardized group-labeled dataset is available at https://anonymous.4open.science/r/ADAPT-41F7/*

Feature extraction

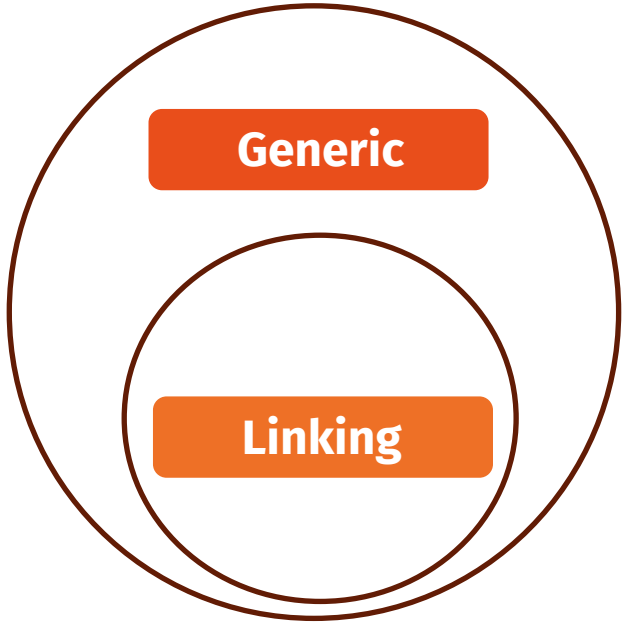
Static analysis to extract features from heterogeneous files*



Feature categories and attribution tasks



Campaign Attribution



Group Attribution

Linking attributes

[^]*?@[^]*?\.[^]*

censys


```
{'URL': ['https://sapp-f347f.firebaseio.com'],
 'ipaddress': [],
 'FilePath_1': [],
 'FilePath_2': ['/res/color/abc_hint_foreground_material_dark
  '/res/drawable/abc_item_background_holo_light.xml',
  '/res/drawable/abc_seekbar_tick_mark_material.xml',
  '/res/layout/notification_template_custom_big.xml',
  '/res/drawable/abc_dialog_material_background.xml',
  '/res/layout/notification_template_icon_group.xml',
  '/res/color/abc_secondary_text_material_light.xml',
  '/res/drawable/abc_cab_background_internal_bg.xml',
  '/res/layout/notification_media_cancel_action.xml'],
 'md5': ['000ddbb75d10a939b54a7ceea5f12563',
  'b855daec971a9da0f2b4d5f935e195a3'],
 'sha1': [],
 'sha256': [],
 'Ethereum': [],
 'Bitcoin': [],
 'EmailAddress': ['android@android.com'],
 'SlackToken': [],
 'RSAprivatekey': [],
 'SSHDSAprivatekey': [],
 'SSHECprivatekey': [],
 'PGPprivatekeyblock': [],
 'GitHub': [],
 'GenericAPIKey': [],
 'GoogleAPIKey': ['AIzaSyDjITMkuXq8V0cUt1PNGydH3uQ3GebImB8'],
```

```
  "ip": "157.90.197.123",
  "autonomous_system": {
      "bgp_prefix": "157.90.0.0/16",
      "asn": 24940,
      "description": "HETZNER-AS",
      "name": "HETZNER-AS",
      "country_code": "DE"
  },
```

```
"subdomains": [
    "www.binance.com"
],
"issuer_dn": "C=CN, ST=ZJ, L=HZ, O=Internet Widgits Pty Ltd",
"fingerprint_sha256": "9e4dcf9d3e4bdfebd76ed1bcdba8ea33d827e69fda45dec0f0e54d62e0dfb53e",
"issuer_organization": [
    "Internet Widgits Pty Ltd"
```

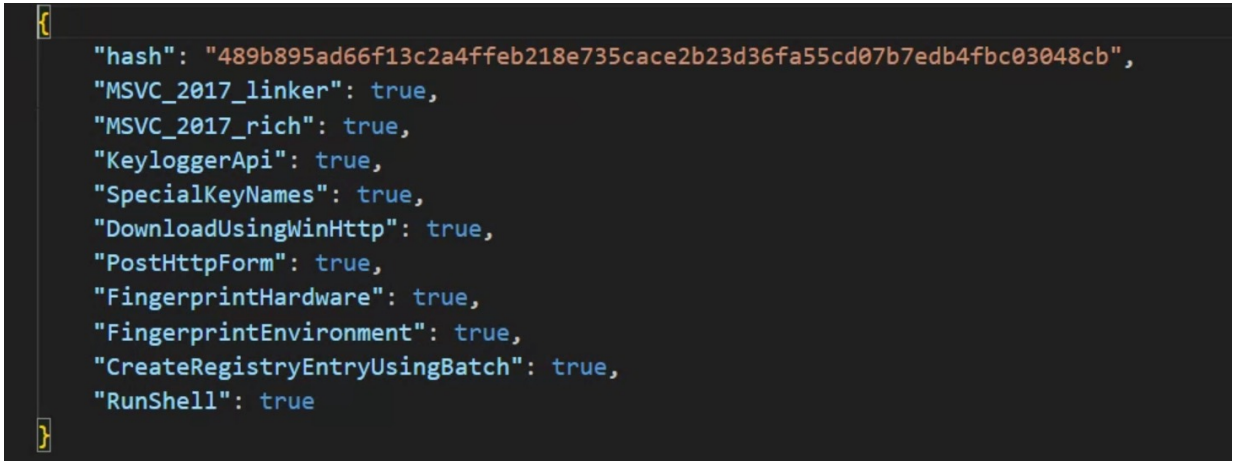
Feature transformation

- Normalization
- One-hot encoding
- String vectorization
- Word embedding

- EXE:ResourceLanguage = DOCX:LanguageCode = “Language”
- PDF:Author = XML:Creator = “Author”

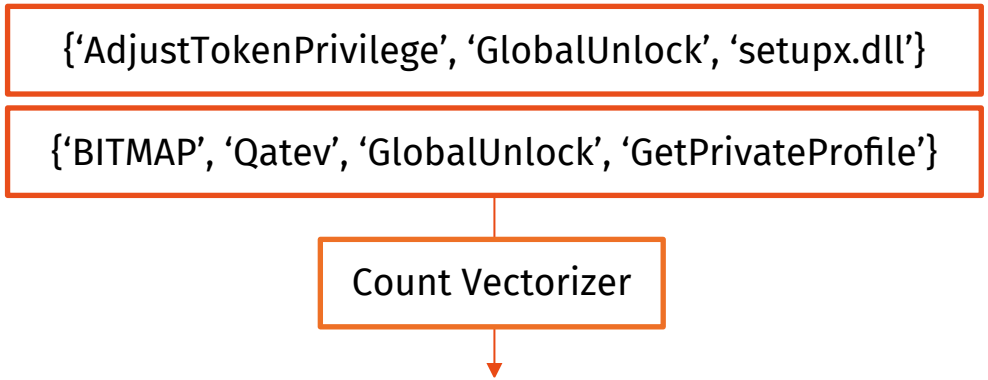
Feature transformation

- Normalization
- One-hot encoding
- String vectorization
- Word embedding



Feature transformation

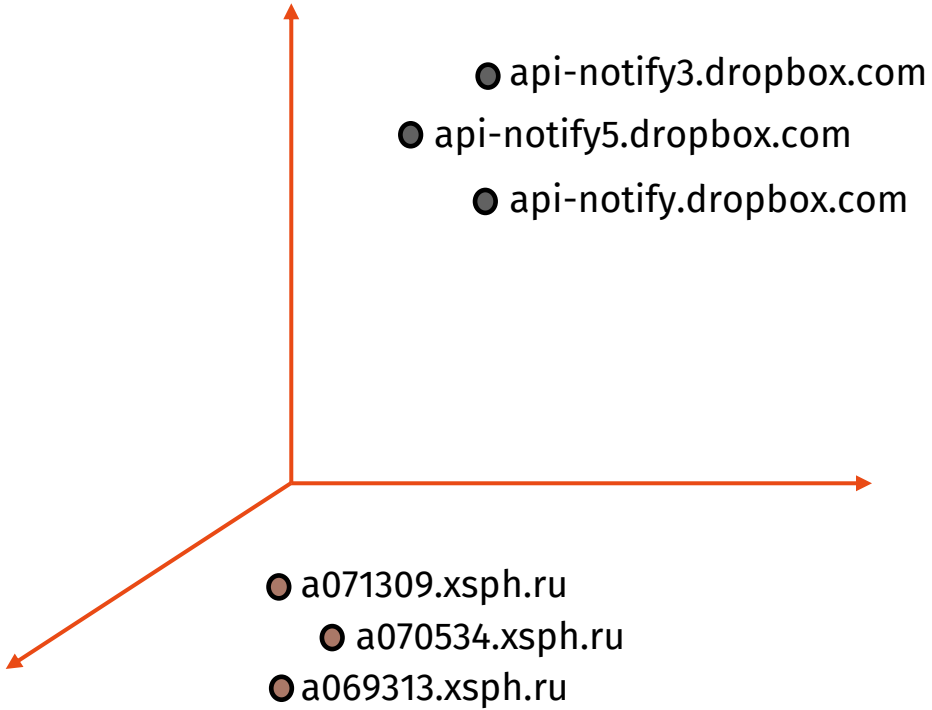
- Normalization
- One-hot encoding
- String vectorization
- Word embedding



Adjust Token Privilege	Global Unlock	setupx.dll	BITMAP	Qatev	GetPrivate Profile
1	1	1	0	0	0
0	1	0	1	1	1

Feature transformation

- Normalization
- One-hot encoding
- String vectorization
- Word embedding

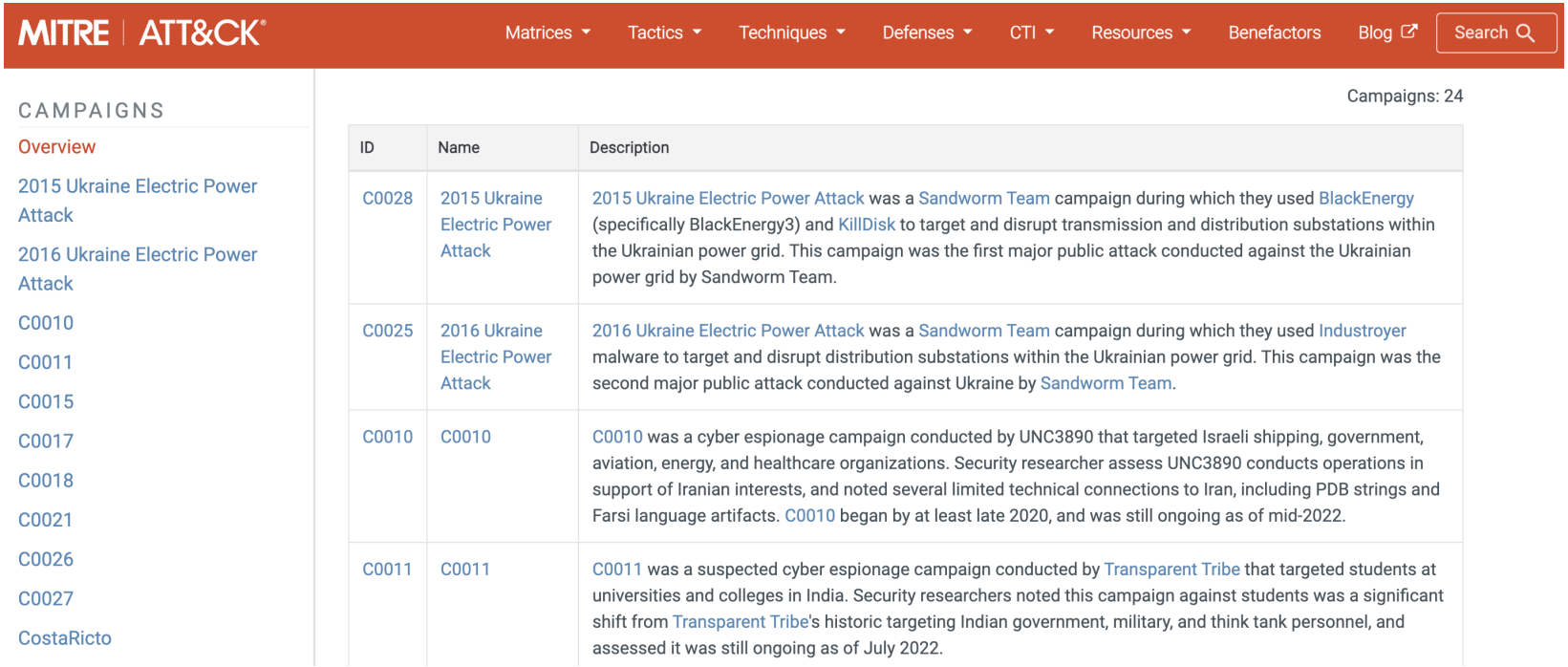


Modeling and clustering

Lack of standardized ground truth labels
- Multiple group labels for ~35% samples
- No dataset for threat campaigns

Unsupervised Agglomerative Clustering
- **APT Campaign** attribution for executable and document files
- **APT Group** attribution for all files

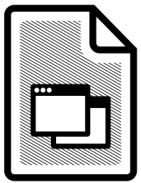
Evaluation



Evaluated the performance of ADAPT on a reference dataset from MITRE

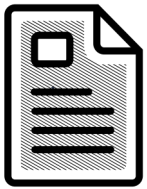
Evaluation: Quantitative

Campaign



Precision : 0.91
Recall: 0.90
F1-score: 0.90

Campaign



Precision: 0.98
Recall: 0.97
F1-score: 0.97

Group

Precision: 0.84
Recall: 0.80
F1-score: 0.78

Evaluation: Qualitative

Advisory: APT29 targets COVID-19 vaccine development

July 2020

JPCERT CC®

JPCERT/CC Eyes

Top > List of “Malware” > Malware “WellMess” Targeting Linux and Windows

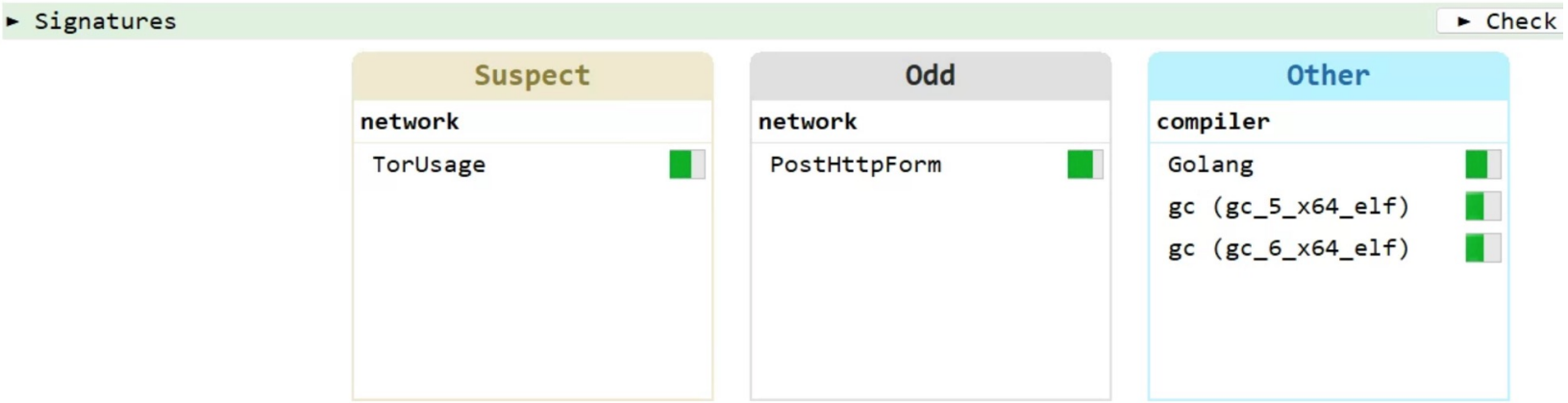
朝長 秀誠 (Shusei Tomonaga)

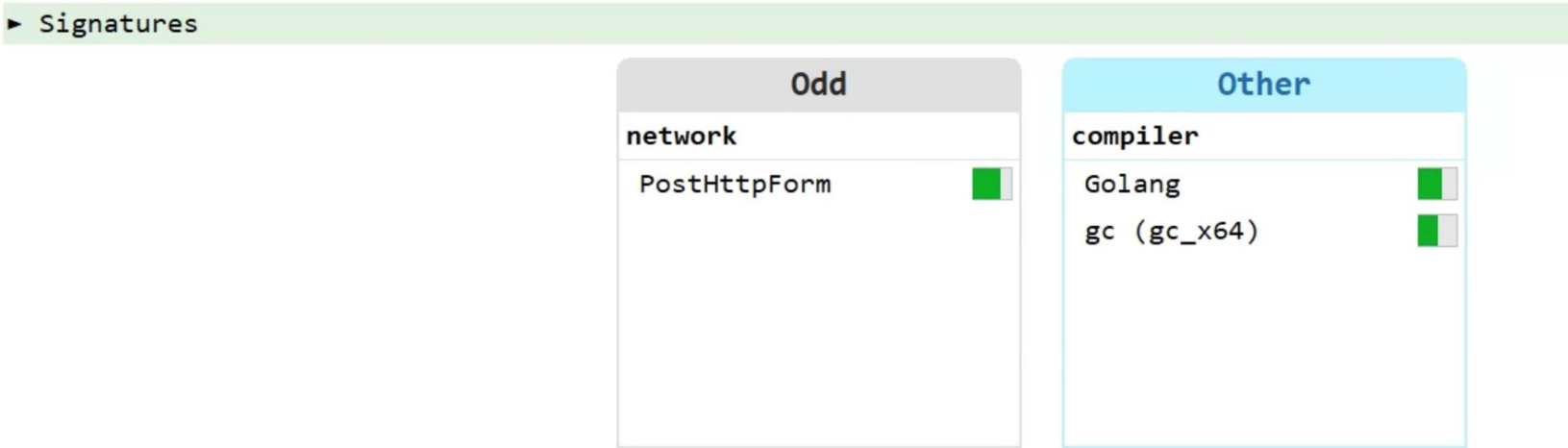
July 6, 2018

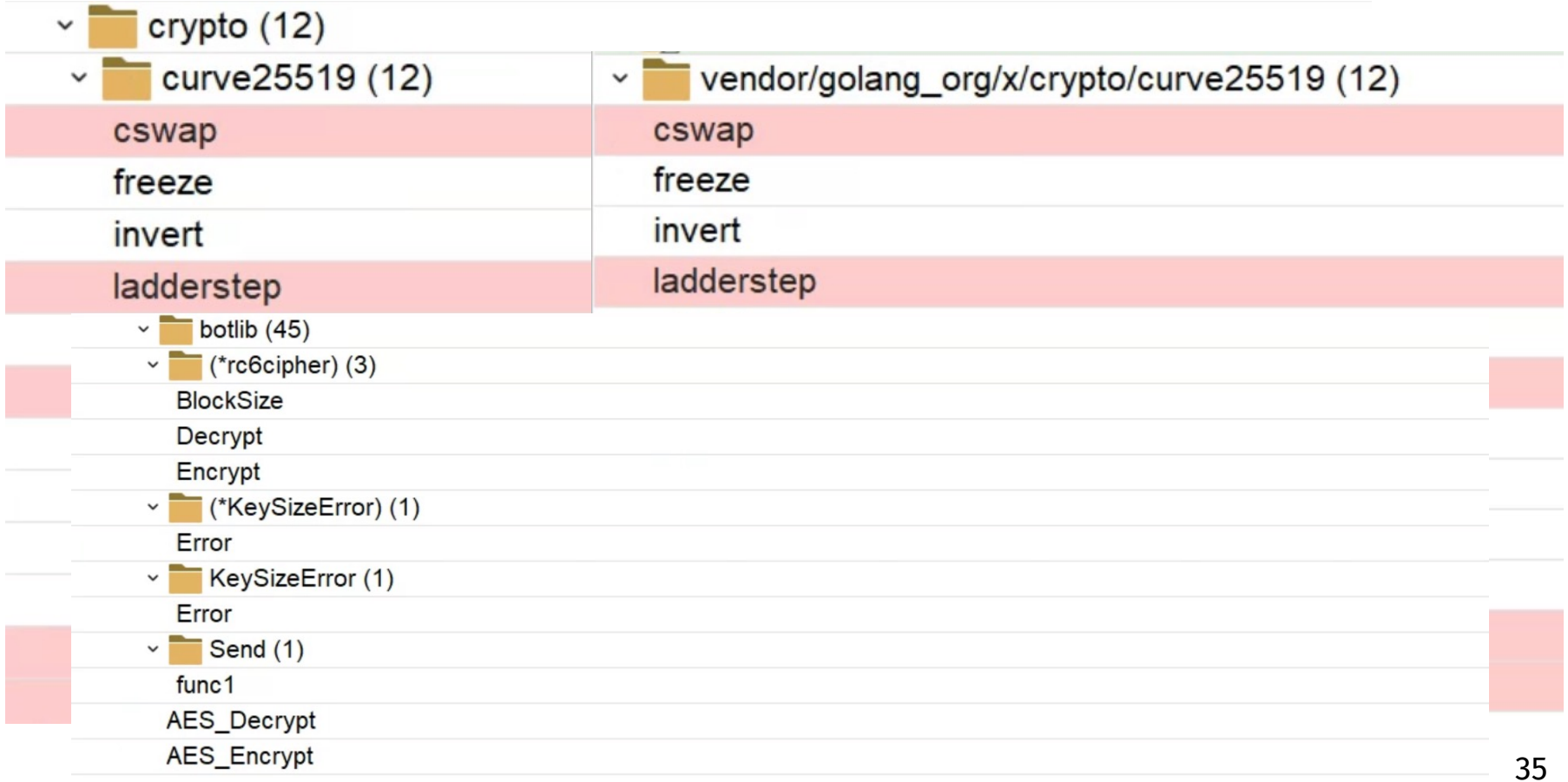
Malware “WellMess” Targeting Linux and Windows

ADAPT...

- Successfully attributes samples belonging to Wellmail and Wellmess campaigns since 2017 to the same entity
- Streamlines and automates the process of extracting and clustering key patterns such as...


► Signatures
► Check
Suspect
network
TorUsage
Odd
network
PostHttpForm
Other
compiler
Golang
gc (gc_5_x64_elf)
gc (gc_6_x64_elf)


► Signatures
Odd
network
PostHttpForm
Other
compiler
Golang
gc (gc_x64)


crypto (12)
curve25519 (12)
cswap
freeze
invert
ladderstep
vendor/golang_org/x/crypto/curve25519 (12)
cswap
freeze
invert
ladderstep
botlib (45)
(*rc6cipher) (3)
BlockSize
Decrypt
Encrypt
(*KeySizeError) (1)
Error
KeySizeError (1)
Error
Send (1)
func1
AES_Decrypt
AES_Encrypt

What’s next?

ADAPT 2.0

- Gain invaluable insights from real-world defenders – that's YOU! 🛡️
- Explore how YOU, as analysts, skillfully identify malicious activities and untangle complexities. 🕵️

Attributing APTs: Expert Insights

Intrigued? Learn more about our study here!

https://secpriv.wien/adapt/

Key Highlights

- Systematic attribution approach by disassociating campaign attribution and group attribution
- Considering the diverse array of file types in the evolving APT landscape is promising
- Effective knowledge exchange between academia and industry can lead to impactful research outcomes

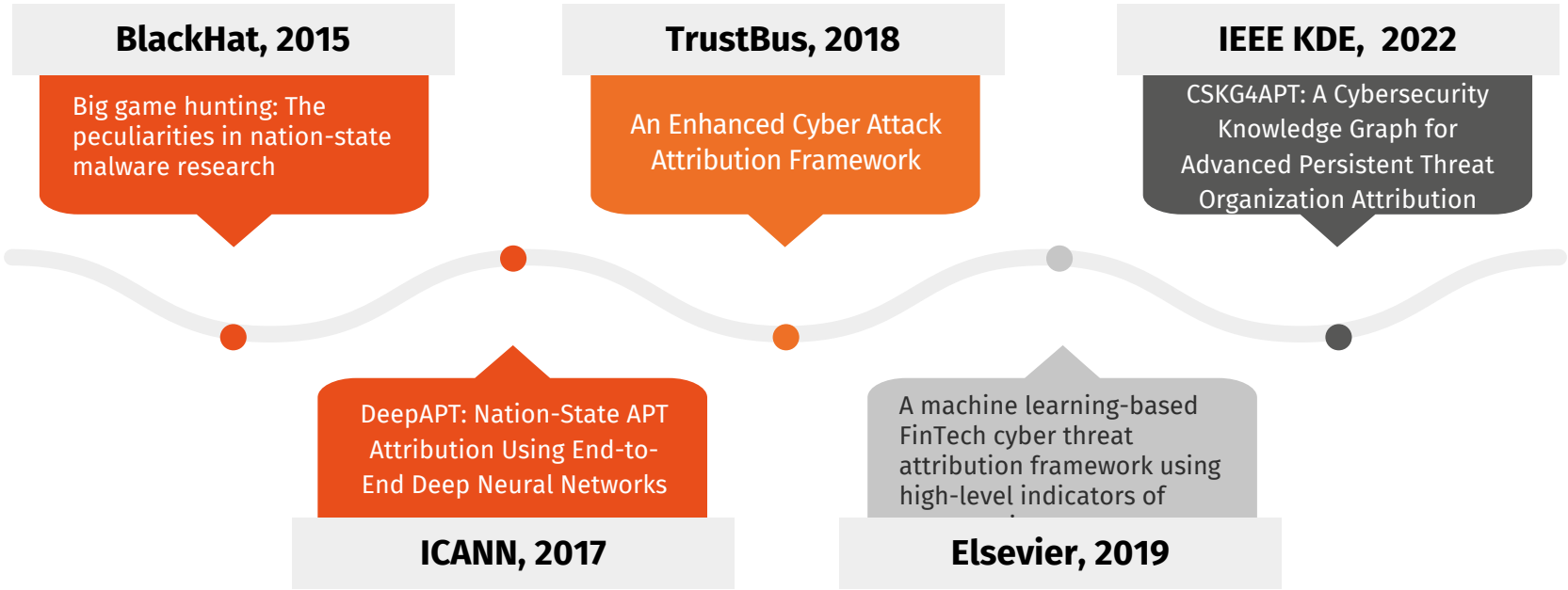
TU WIEN

S&P Security & Privacy

UNIVERSIDAD POLITÉCNICA DE MADRID

UCL

State-of-the art research



References

[1] https://securityaffairs.com/116001/apt/german-parliament-bundestag-russia-hackers.html
[2] https://www.mandiant.com/resources/blog/unc2452-merged-into-apt29
[3] https://www.mandiant.com/resources/blog/north-korea-cyber-structure-alignment-2023
[4] https://cybersecurity.att.com/blogs/labs-research/a-global-perspective-of-the-sidewinder-apt
[5] https://blog.talosintelligence.com/whats-with-shared-vba-code/
[6] https://machinelearningmastery.com/why-one-hot-encode-data-in-machine-learning/
[7] https://scikit-learn.org/stable/modules/generated/sklearn.feature_extraction.text.CountVectorizer.html
[8] https://huggingface.co/sentence-transformers
[9] https://scikit-learn.org/stable/modules/generated/sklearn.cluster.AgglomerativeClustering.html#
[10] https://attack.mitre.org/campaigns/
[11] https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf
[12] https://blogs.jpcert.or.jp/en/2018/07/malware-wellmes-9b78.html
[13] https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
[14] https://attack.mitre.org/groups/