TLP:CLEAR

37TH ANNUAL FIRST CONFERENCE

FORTRESSES OF THE FUTURE
BUILDING BRIDGES NOT WALLS

COPENHAGEN DENMARK
#FIRSTCON25

JUNE 22·27 2025

Navigating the Threat Actor Maze: A Tool for Mapping Names, Families and Insights

Dr Dave Matthews, Gen Digital (Avast/NortonLifelock), Australia

Whoami @work

> 25 years in Cyber: Engineering, Forensics and IR

Australian National University

System Administrator - Phd in Statistics

Worked – Government, Corporate, Defense, Law Enforcement, then

CROWDSTRIKE

Avast

Gen

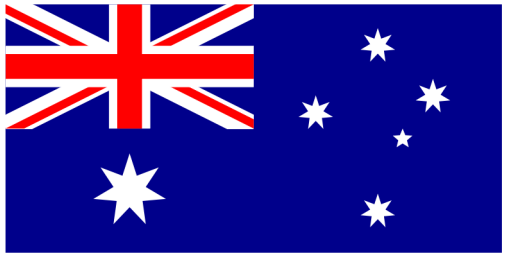
From Brisbane, Australia

Went to first FIRSTCON in 1999!

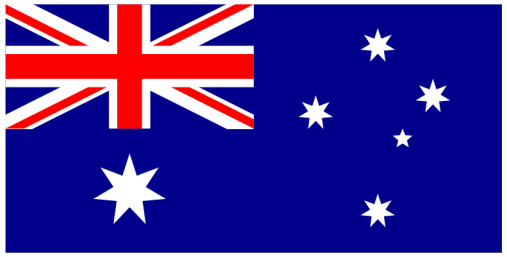
Contact details at end of talk

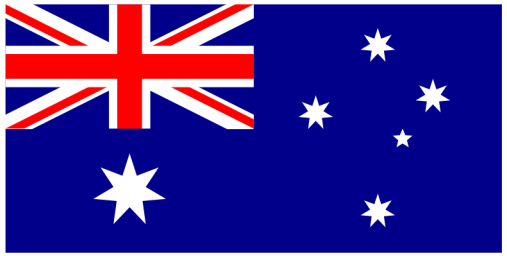
TLP:CLEAR

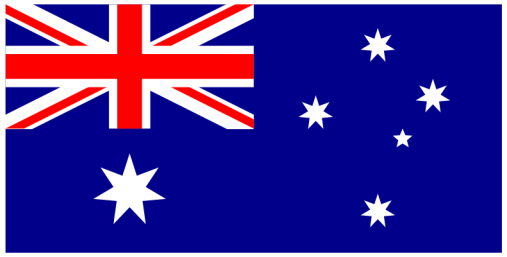
For fun I like to:



TLP:CLEAR







- Welcome To Australia!

What is my talk about?

- Based on some tools I wrote in my spare time:
- Threat Actor Naming – it is hard to keep track
- How Are Threat Actors named?
- Why should you care?
- Where can you look up details on Threat Actors?
- What does this new tool/service do and why is it useful

Threat Actor naming
- It’s hard to keep track

Threat Actors – they have so many names!

- Who has heard of the threat actor ‘Stealth Mango’?

- What about the Threat Actor ‘HoneyMyte’
  - Also known as ‘Mustang Panda’?
- How about those Microsoft naming conventions? Storm-0501?
- And MAGNALLIUM anyone?
  - Also Known As: APT 33
- How many threat actor names/aliases are there? Have a Guess – win a prize!

Why should you care?

- Do you ever read a cyber security report/news/blog that references a threat actor
- And wonder – who is that?
- Where are they from?
- What are their likely motivations?

You could just ‘search on the web’

- There are multiple places – not all data is complete
  - Where to start?
- Takes time

How are Threat Actors named?

- It is completely up to vendors and researchers
- Let's talk about the most well known
  - Some have themes:
    - **Crowdstrike**: Bears, Pandas, Chollimas and Spiders
      - Eg. Fancy Bear/APT28 – Russian based
    - **Dragos**: uses minerals, e.g. XENOTIME, ELECTRUM, CHERNOVITE
    - **Proofpoint**: uses numbered TA groups, e.g. TA505, TA542
    - **Mandiant**: uses numbered APT, FIN and UNC groups, e.g. APT1, FIN7, UNC2452
    - **Microsoft**: used to use elements, e.g. PHOSPHORUS, NOBELIUM, STRONTIUM
      - But changed – to the theme of Weather: eg. Typhoon, Sandstorm, Rain, Storm
    - **Secureworks**: uses metals like GOLD for eCrime, BRONZE for China
      - Eg. BRONZE ATLAS is APT41 – Chinese

- Confused?

Some threat actors have MANY aliases:

- North Korea's Lazarus Group: is known by more than 50 different names!

```
Threat Actor:
  Lazarus Group
Aliases:
  Alluring Pisces
  Andariel
  Appleworm
  APT 38
  APT-C-26
  APT38
  ATK 117
  ATK 3
  ATK117
  ATK3
  BeagleBoyz
  Black Alicanto
  Black Artemis
  Bluenoroff
  Bureau 121
  CageyChameleon
  Citrine Sleet
  COPERNICIUM
  COVELLITE
  CryptoCore
  CryptoMimic
  CTG-2460
  CTG-6459
  Dangerous Password
  Dark Seoul
  DEV-0139
  DEV-1222
  Diamond Sleet
  Gods Apostles
  Gods Disciples
  Group 77
  Guardians of Peace
  Hastati Group
  HIDDEN COBRA
  ITG03
  Jade Sleet
  Labyrinth Chollima
  Lazarus
  Lazarus Group
  Moonstone Sleet
  NewRomanic Cyber Army Team
  NICKEL ACADEMY
  NICKEL GLADSTONE
  Operation AppleJeus
  Operation DarkSeoul
  Operation GhostSecret
  Operation Troy
  Sapphire Sleet
  SectorA01
  Selective Pisces
  Slow Pisces
  Stardust Chollima
  Storm-0139
  Storm-1222
  T-APT-15
  TA404
  TA444
  TAG-71
  UNC4034
  UNC4736
  UNC4899
  UNC577
  Unit 121
  Whois Hacking Tea
  ZINC
```

This was what motivated me to improve things

- I like to save time.
- Don’t really like remembering information that is not useful
- I’m looking at CTI all the time – wanted a quick way of knowing more about other related research – and threat actor aliases
- Wrote some tools – can quickly use – to show info about a particular threat actor
- All you need to start with is a web browser

Where to look?

- Where are Threat Actor descriptions kept? Lots of places….
- Have initially focused on data from MISP, ETDA, MITRE, Malpedia, Microsoft
- Search data in these repositories
- As well as public sources of information from Cyber Vendors – eg. Wiz
- Problem – not all are frequently updated – and hard to link between them:
  - Some cost $$$

What is MISP?

- MISP: “**Malware Information Sharing Platform** “
  - MISP started out as a platform for technical indicator sharing
  - Very widely used and actively supported
  - Opensource Threat intelligence platform for sharing, storing and correlating IOCs
  - Uses Taxonomies to classify events and data:
    - Taxonomy for many types of data - NOT just Cyber Security

What is the MISP-Galaxy?

MISP Galaxy: represents Clusters – to describe event/attribute data)

- Many Clusters for many https://misp-galaxy.org/threat-actor/

Cluster: A knowledge base that describes type of data

- A Cluster has Key / Value pairs (Elements) that describe the data

Many Clusters defined in the MISP-Galaxy:

- Some examples:

- Software
- Tactics
- Intrusion Set
- Malware
- mitre-tool
- NACE
- NAICS
- NICE Competency areas
- NICE Knowledges
- OPM codes in cybersecurity
- NICE Skills
- NICE Tasks
- NICE Work Roles
- o365-exchange-techniques
- online-service
- Preventive Measure
- Producer
- Ransomware
- RAT
- Regions UN M49
- rsit
- Sector
- Sigma-Rules
- Dark Patterns

Attack Pattern

Cluster Examples:

- Tools

PNG Dropper
Rotexy
KingMiner
Taurus
Terra Loader
SpicyOmelette
LamePyre
DarthMiner
OSX.BadWord
OSX/Shlayer
Bushaloader
ANEL
BabyShark
StealthWorker

LONEJOGGER
PASSMARK
PENCILDOWN
PENDOWN
PUMPKINBAR
SLIMCURL
SPICYTUNA
SWEETDROP
VENOMBITE
DarkGate
DangerAds
AtlasAgent
RDP Wrapper
TightVNC
RevClient
Colibri Loader
BUSHWALK
LIGHTWIRE
CHAINLINE
FRAMESTING
IMPACKET
IODINE
ENUM4LINUX
SPAWNANT
SPAWNMOLE
SPAWNSLOTH
ROOTROT
TONERJAM
GOST

Tinba
PlugX
MSUpdater
Lazagne
Poison Ivy
SPIVY
Torn RAT
OzoneRAT
ZeGhost
Elise Backdoor
Trojan.Laziok
Slempo
PWOBot
Lost Door RAT
njRAT
NanoCoreRAT
Sakula
Hi-ZOR
Derusbi
EvilGrab
Trojan.Naid
Moudoor
NetTraveler
Winnti
Mimikatz
WEBC2
Pirpi

Cluster Examples:

- Sector (or Vertical)

Justice
Manufacturing
Maritime
Military
Multi-sector
News - Media
NGO
Oil
Payment
Pharmacy
Police - Law enforcement
Research - Innovation

Aerospace
Agriculture
Arts
Bank
Chemical
Citizens
Civil Aviation
Country
Culture
Data Broker
Defense
Development
Diplomacy
Education

Cluster Examples:

- Even, Intelligence Agencies

Secret Intelligence Service

Defence Intelligence

Government Communications Headquarters

National Crime Agency

Gangmasters and Labour Abuse Authority

Director of National Intelligence

Central Intelligence Agency

Defense Intelligence Agency

National Security Agency

National Geospatial-Intelligence Agency

Intelligence Protection Organization of Islamic Republic of Iran Army

Intelligence Organization of Army of the Guardians of the Islamic Revolution

Intelligence Protection Organization of Army of the Guardians of the Islamic Revolution

Intelligence org of FARAJA

Intelligence org of the Islamic Republic of Iran[12]

General Security Directorate (Iraq)

Iraqi National Intelligence Service

Falcons Intelligence Cell

Kurdistan Region Security Council

Intelligence and Counter-Terrorism Directorate - Ministry of Interior

Directorate of Military Intelligence (Ireland)

CIS Corps (Ireland)

Military Intelligence (Czech Republic)

Danish Security and Intelligence Service

Danish Defence Intelligence Service

Army Intelligence Center

Egyptian General Intelligence Directorate

Military intelligence and reconnaissance (Egypt)

Egyptian Homeland security

National Security Office (Eritrea)

Estonian Internal Security Service

Estonian Foreign Intelligence Service

National Intelligence and Security Service (Ethiopia)

Finnish Defence Intelligence Agency

Intelligence Division (Finland)

We use the ‘Threat Actor’ cluster

- Threat Actor
- More than 850 different threat actor
- Each of these often has aliases – links threat actor research
- Eg. Mustang Panda – also known as:

  BASIN, BRONZE PRESIDENT, HoneyMyte, Red Lich, TEMP.HEX

ShaggyPanther

Fishing Elephant

RevengeHotels

GhostEmperor

Operation Triangulation

Operation Ghoul

CardinalLizard

Ferocious Kitten

Operation Red Signature

Earth Yako

Threat Actor Cluster

- Cluster is JSON –
  - KEY: ‘synonyms’
  - KEY: ‘country’ w
- Keys of particula
- ‘uuid’ – used to t
- ‘synonyms’ – eg.
- ‘refs’ – list of pub


```
{
  "description": "This threat actor targets nongovernmental organizations using
  Mongolian-themed lures for espionage purposes.
  These campaigns involve the use of shared malware like Poison Ivy or PlugX.",
    "country": "CN",
    "refs": [
      "https://www.cfr.org/interactive/cyber-operations/mustang-panda",
      "https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-f
    ],
    "synonyms": [
      "BRONZE PRESIDENT",
      "HoneyMyte",
      "Red Lich",
      "TEMP.HEX",
      "BASIN",
      "Earth Preta",
      "..."
    ],
  "uuid": "78bf726c-a9e6-11e8-9e43-77249a2f7339",
  "value": "MUSTANG PANDA"
},
```

Data source: ETDA – (THAICERT)

- Thai Electronic Transactions Development Agency (ETDA)
  - Freely Publish their Threat Actor Encyclopedia

https://apt.etda.or.th/

Uses a different uuid for threat actors to MISP but is well structured

- Includes references from their own threat actor research
- Easily downloadable JSON – regularly updated

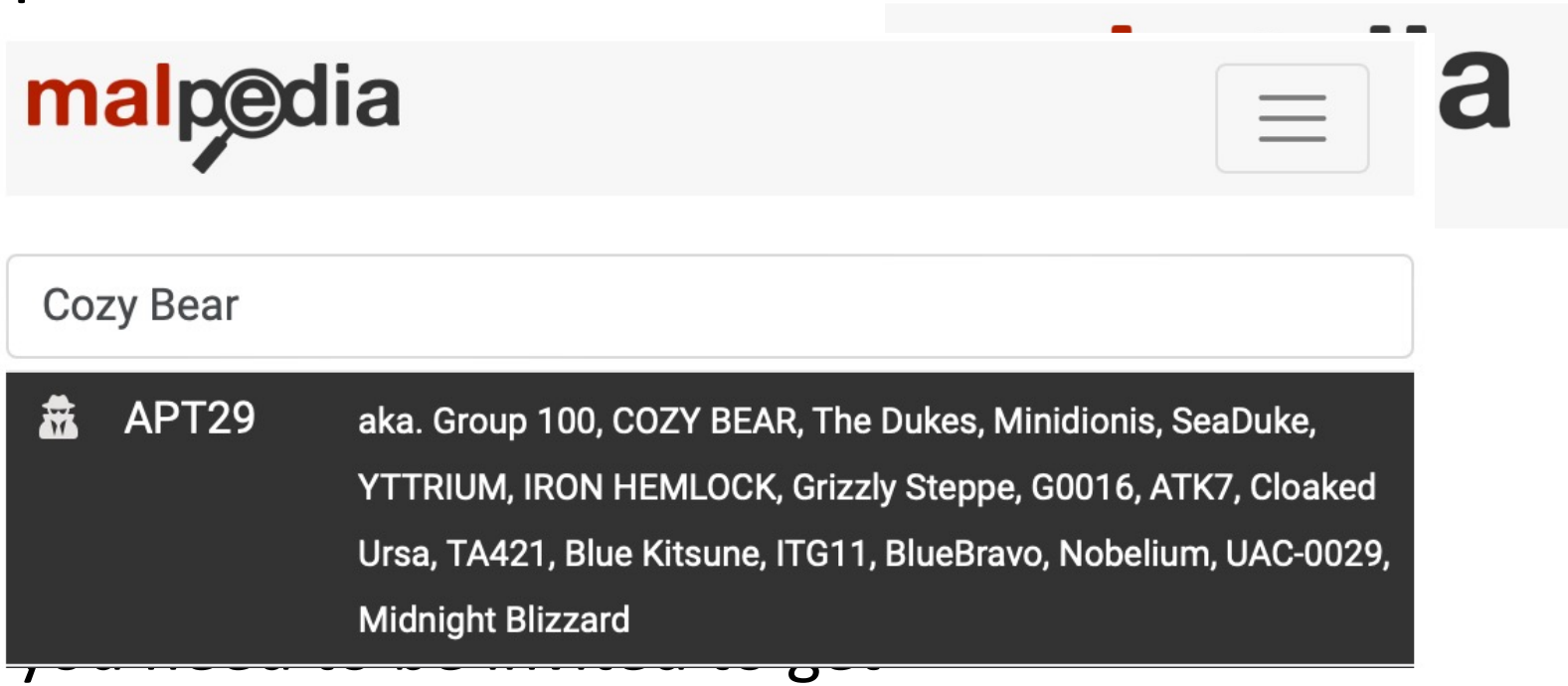
Data source: MITRE ATT&CK

MITRE | ATT&CK®

- Frameworks that categorize the TTPs used by Threat Actors
- MITRE ATT&CK groups are Threat Actors that have been observed using specific TTPs
- Data for these Threat groups is published freely for
  - Enterprise Matrix
    - Windows/macOS/Linux/Cloud and network environments
  - Mobile Matrix
    - TTPs specific to Android and iOS
  - ICS Matrix
    - Threats targeting operational technology (OT) environnetsj

Data source: Malpedia

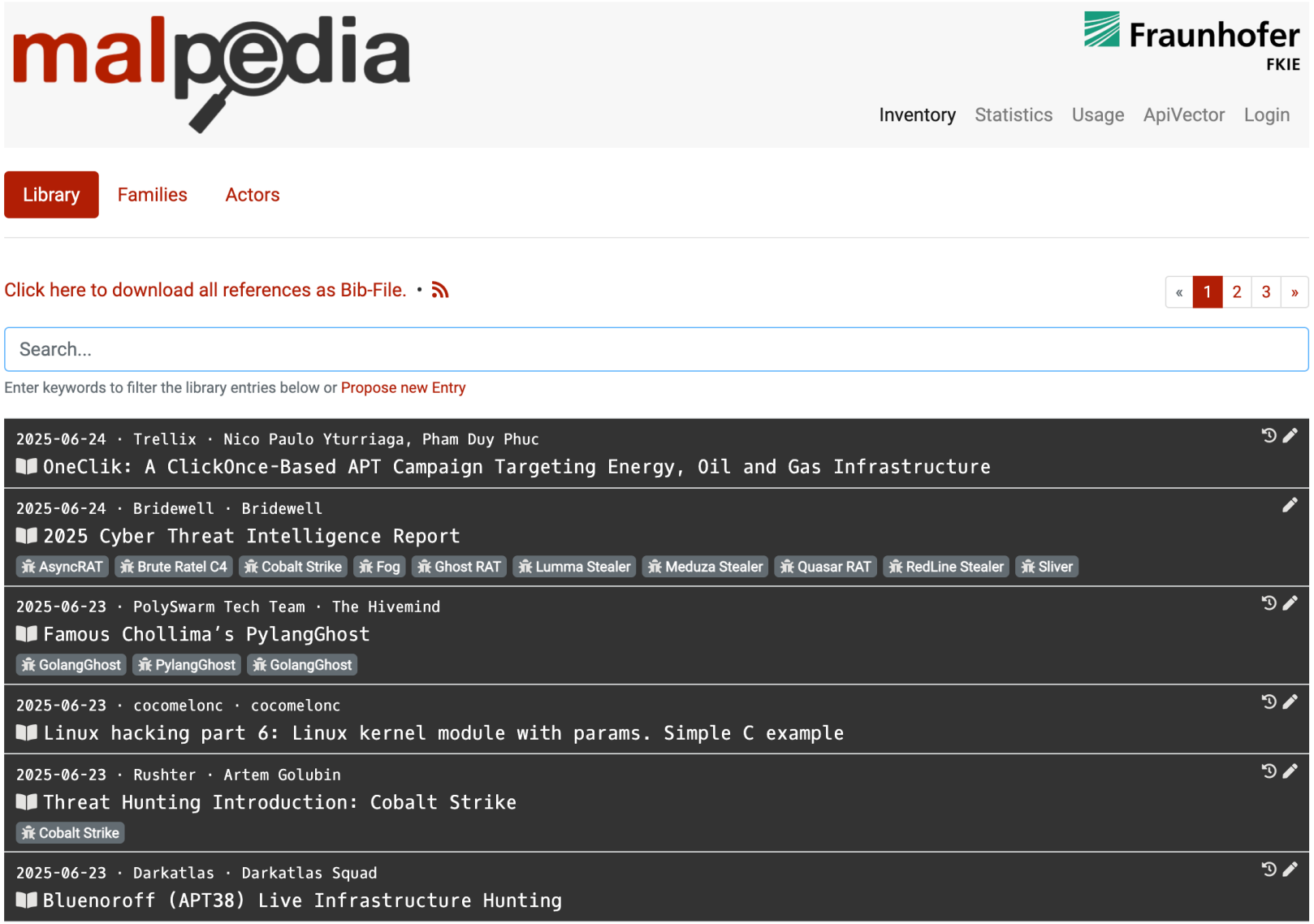
- Malpedia is hosted by Fr
- It contains malware sam
- Threat Actor data
  - Uses same ‘uuid’ as MISI
  - Has synonyms, Malware
- Invite-only Trust group – API or modification access to Malpedia by someone with account.
- Has public website to search manually with some data openly downloadable – like the full Malpedia Bibliography



TLP:CLEAR

Malpedia

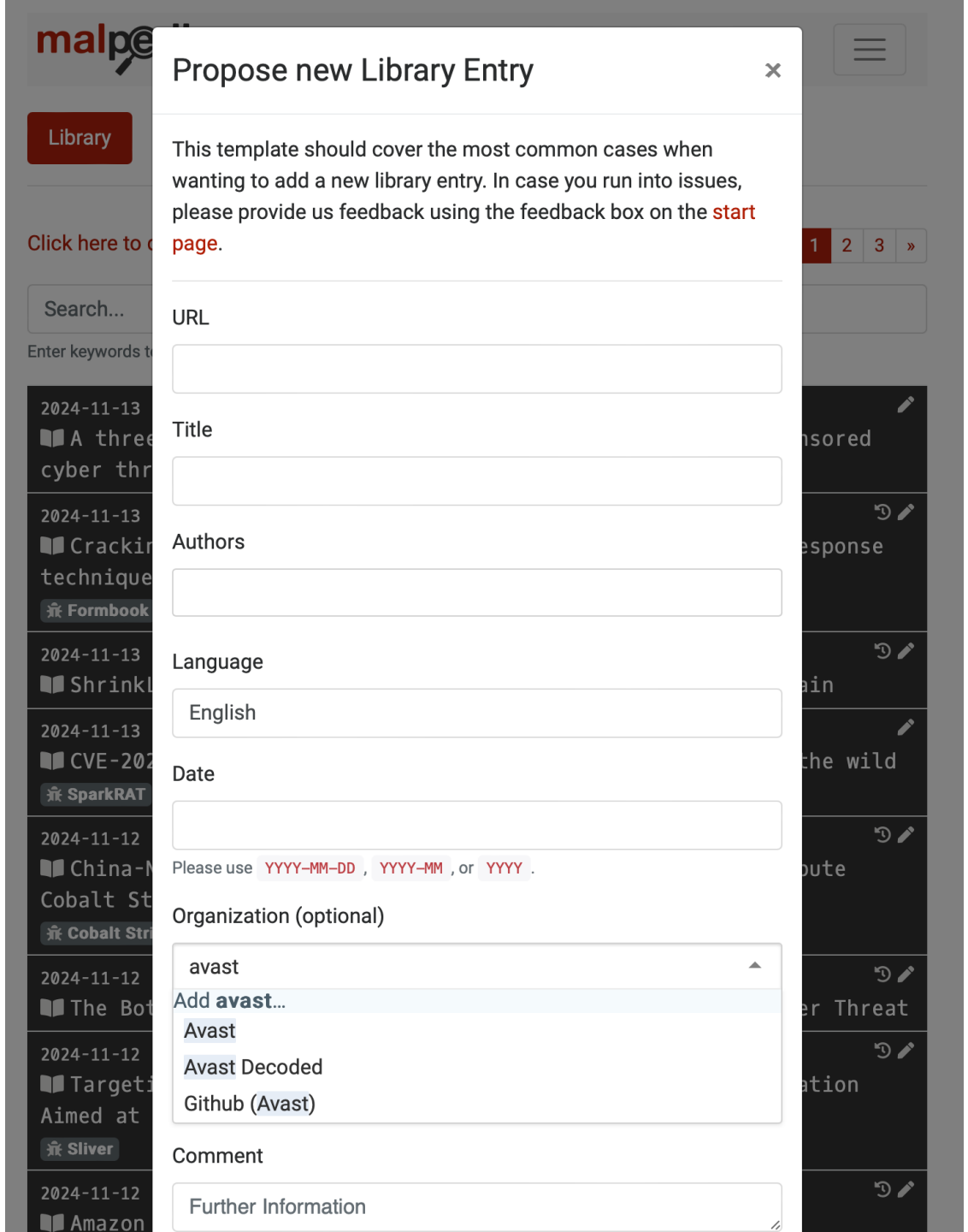
- Once you have an account – you have access to advanced features
  - Malware samples
  - Non-public yara rules
  - API access
  - Ability to suggest additional web references for Threat Actors and Malware families
  - Has good community – regular updates



TLP:CLEAR

Malpedia

- Once joined – you can also add links to websites/blogs/reports that relate to a specific Threat Actor
  - Additions are vetted and sometimes take a while



TLP:CLEAR

Microsoft

mstic / PublicFeeds / ThreatActorNaming / MicrosoftMapping.json

Code Blame 676 lines (676 loc) · 17.9 KB


```
165         },
166         {
167             "Threat actor name": "Hazel Sandstorm",
168             "Origin/Threat": "Iran",
169             "Other names": "EUROPIUM, HELIX KITTEN, COLBALT GYPSY, Crambus, OilRig, APT34"
170         },
171         {
172             "Threat actor name": "Heart Typhoon",
173             "Origin/Threat": "China",
174             "Other names": "HELIUM, AURORA PANDA, APT17, Hidden Lynx, ATG3, Red Typhon, KAOS, TG-8153, S
175         },
176         {
177             "Threat actor name": "Hexagon Typhoon",
178             "Origin/Threat": "China",
179             "Other names": "HYDROGEN, NUMBERED PANDA, Calc Team, Red Anubis, APT12, DNS-Calc, HORDE"
180         },
```


- Microsoft's Threat In
  groups that they trac
- Not as detailed as M
- A few years ago they
  - Eg. Russia is 'Blizzarc
    Private sector offens
- They publish data that aims to map between Microsoft naming and other vendors on github
  - Lacks uuids, references and the rigor that has been put into say MISP/ETDA.
  - But this is on their radar – eg. Recent 'partnership' with CrowdStrike

Many vendors don’t make it easy

- Not easy to find references for all of the vendor’s named threat actors
- Requires trawling their sites.
- Some vendors get updated in MISP/ETDA etc quickly – others not..

Some Stats

- MISP has about 850 Threat Actor groups,
  - With 1200 Threat Actor Aliases/Synonyms (eg. CozyBear is alias of APT29)
- MITRE has about 180 Threat Actor groups,
  - With 375 Threat Actor Aliases
- ETDA (ThaiCERT) has about 590 Threat Actor groups,
  - With 1190 Threat Actor Aliases
- MICROSOFT has about 135 Threat Actor groups in their github repo

Vendors agreeing on Naming?

The Newcomer's Guide to Cyber Threat Actor Naming

Florian Roth Follow 5 min read · Mar 25, 2018

440 4

I was driven by a deep frustration when I started my public "APT Groups and Operations" spreadsheet in 2015. I couldn't understand why I had to handle so many different names for one and the same threat actor.

osoft.com/en-us/security/blog/2025/06/02

CrowdStrike and Microsoft Unite to Harmonize Cyber Threat Attribution

June 02, 2025 | Adam Meyers | Executive Viewpoint • Threat Hunting & Intel

osoft.com/en-us/security/blog/2025/06/02/announcing-a-new-strategic-collaboration-to-bring-clarity-to-threat-actor-naming/

Introducing a collaborative reference guide to threat actors

Microsoft and CrowdStrike are publishing the first version of our joint threat actor mapping. It includes:

- A list of common actors tracked by Microsoft and CrowdStrike mapped by their respective taxonomies.
- Corresponding aliases from each group's taxonomy.

This reference guide serves as a starting point, a way to translate across naming systems so defenders can work faster and more efficiently, especially in environments where insights from multiple vendors are in play. This reference guide helps to:

- Joe Slowik h

"This is movement in a direction toward potential solutions. It is not a solution," Slowik added. "If nothing else, it just highlights more of what the problem actually is, that we have to have these sort of one-off agreements between different companies to say, 'OK, we'll work through our lists and figure out where things are equal to each other.'"

CYBERSCOOP

- Joe Slowik

"While it would be nice for industry to all come together mutually and agree on a way to do this, I don't think it's ever going to work," Slowik said. "Organizations will continue to maintain their own naming and classification schema for the foreseeable future. I do not see that going away, irrespective of this effort and collaboration."

Tool Time!

- Wouldn’t it be nice…
  - If there was something that could quickly
    - Lookup synonyms of a given threat actor name
    - Allow for wildcards or regular expressions – eg. APT-33 will match APT33
    - All you need is a web browser – or Commandline
  - Outputs data that is aggregated from all of these sources

How does the tool work?

- On the backend – python code – which Gathers / updates data from:
  - MISP Threat Actor Cluster on GitHub
  - ETDA Threat Actor database
  - MITRE Attack Groups
  - Malpedia
  - Microsoft Threat Actors
  - Published websites
- Has aggregated data for 1160 Threat Actor Groups (with 2269 Actor Aliases)
  3429 in total!
- Enables searching this data for:
  - Threat Actor Names/Aliases
  - Descriptions
  - References

When might this be useful?

- For example – when reading article referencing a threat actor
- Listening to a talk at Cyber Security conference
  - Want to quickly get more background on the Threat Actor
  - Other names/aliases
  - Or references to read
  - Tools / malware families used
- Even researchers searching for a new name for their new threat group!

Reality – not everyone wants to run my code

- Use the web interface: thrunter.org
- Free to use Website:
  - simple to query and search
  - Regularly updated with data

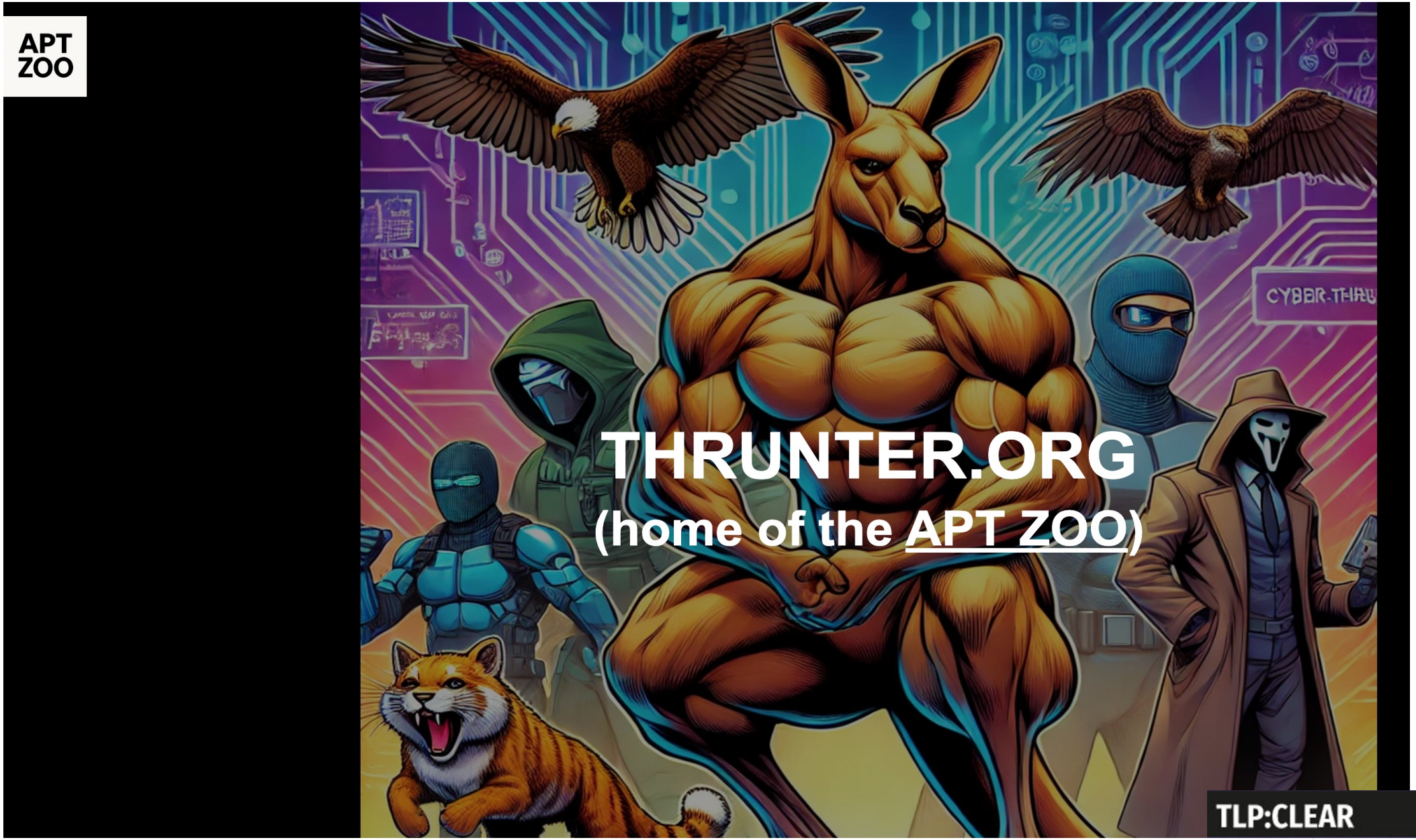
The “APT ZOO”

- https://thrunter.org

DEMO!

DEMO

Demo Backup
☺



Demo Backup ☺

aptZoo - Threat Actor Search

Search Threat Actors Names and Aliases (display Aliases/Description/References):

MUSTA

MUSTANG PANDA
Mustard Tempest

☐ **Use Regex pattern in search**

☐ **Show related Malpedia Bibliographies**

Search Descriptions / References and show matching Threat Actor information:

Search Options - choose one only:

○ **Search Descriptions of Threat Actors (eg. 'australia' will show threat actors whose description include 'Australia')**

○ **Search References/URLs of Threat Actor Reports (eg. 'silentpush' will show all threat actors who have SilentPush reports published)**

Search | Reset options

Quick Threat Actor Alias lookup:

Demo Backup
☺

aptZoo - Threat Actor Search

Search Threat Actors Names and Aliases (display Aliases/Description/References):

FIN\d$

Extra Search Options:

- [x] **Use Regex pattern in search**
- [ ] **Show related Malpedia Bibliographies**

FIN\d$

Search Descriptions / References and show matching Threat Actor information:

Search Options - choose one only:

- ○ **Search Descriptions of Threat Actors (eg. 'australia' will show threat actors whose description include 'Australia')**
- ○ **Search References/URLs of Threat Actor Reports (eg. 'silentpush' will show all threat actors who have SilentPush reports published)**

Search | Reset options

Quick Threat Actor Alias lookup:

Demo Backup ☺

Searching for Threat Actor info on 'FIN\d$' (using regex):

Searched for "FIN\d$": 6 Results Found: - FIN7, WOLF SPIDER, FIN6, FIN8, FIN5, FIN1

Result 1. Match found for Threat Actor "FIN7"

Threat Actor:
FIN7
Aliases:
Anunak
APT-C-11
ATK 32
ATK32
Calcium
Carbanak
Carbanak, Anunak
CARBON SPIDER
Coreid
ELBRUS
FIN7
G0008
G0046
GOLD NIAGARA
Gold Waterfall
ITG14
JokerStash
Navigator
Sangria Tempest
TAG-CR1

Description(s):

1. [ETDA] Carbanak is a threat group that mainly targets banks. It also refers to malware of the same name (Carbanak). It is sometimes referred to as {{FIN7}}, I
Carbanak malware and are therefore tracked separately.

(Kaspersky) From late 2013 onwards, several banks and financial institutions have been attacked by an unknown group of cybercriminals. In all these attacks, a s
and the law enforcement agencies (LEAs) involved in the investigation, this could result in cumulative losses of up to 1 billion USD. The attacks are still acti
attacks. The motivation for the attackers, who are making use of techniques commonly seen in Advanced Persistent Threats (APTs), appears to be financial gain as

Demo Backup ☺

Searching for Threat Actor info on 'FIN\d$' (using regex):

Searched for "FIN\d$": 6 Results Found: - FIN7, WOLF SPIDER, FIN6, FIN8, FIN5, FIN1

Result 1. Match found for Threat Actor "FIN7"

Threat Actor:
FIN7
Aliases:
Anunak
APT-C-11
ATK 32
ATK32
Calcium
Carbanak
Carbanak, Anunak
CARBON SPIDER
Coreid
ELBRUS
FIN7
G0008
G0046
GOLD NIAGARA
Gold Waterfall
ITG14
JokerStash
Navigator
Sangria Tempest
TAG-CR1

Description(s):

1. [ETDA] Carbanak is a threat group that mainly targets banks. It also refers to malware of the same name (Carbanak). It is sometimes referred to as {{FIN7}}, I
Carbanak malware and are therefore tracked separately.

(Kaspersky) From late 2013 onwards, several banks and financial institutions have been attacked by an unknown group of cybercriminals. In all these attacks, a s
and the law enforcement agencies (LEAs) involved in the investigation, this could result in cumulative losses of up to 1 billion USD. The attacks are still acti
attacks. The motivation for the attackers, who are making use of techniques commonly seen in Advanced Persistent Threats (APTs), appears to be financial gain as

Demo Backup
☺

Searching for Threat Actor info on 'MUSTANG PANDA'; will display any relevant Malpedia links :

Searched for "MUSTANG PANDA": 1 Results Found: - MUSTANG PANDA

Result 1. Match found for Threat Actor "MUSTANG PANDA"

Threat Actor:
  MUSTANG PANDA
Aliases:
  BASIN
  BRONZE PRESIDENT
  Camaro Dragon
  Earth Preta
  HoneyMyte
  LuminousMoth
  Mustang Panda
  PKPLUG
  Polaris
  Red Lich
  RedDelta
  Stately Taurus
  TA416
  TANTALUM
  TEMP.HEX
  Twill Typhoon
  UNC1066
  VERTIGO PANDA

Description(s):

1. [ETDA] (Kaspersky) APT actors are known for the frequently targeted nature of their attacks. Typically, they will handpick a set of targets that in turn are handled with almost surgic
vectors, malicious implants and payloads being tailored to the victims' identities or environment. It's not often we observe a large-scale attack conducted by actors fitting this profile
being noisy, and thus putting the underlying operation at risk of being compromised by security products or researchers.

We recently came across unusual APT activity that exhibits the latter trait – it was detected in high volumes, albeit most likely aimed at a few targets of interest. This large-scale and
observed in South East Asia and dates back to at least October 2020, with the most recent attacks seen around the time of writing. Most of the early sightings were in Myanmar, but it now
much more active in the Philippines, where there are more than 10 times as many known targets.

Further analysis revealed that the underlying actor, which we dubbed LuminousMoth, shows an affinity to the {{Mustang Panda, Bronze President}} (HoneyMyte) group. This is evident in both
connections, and the usage of similar TTPs to deploy the Cobalt Strike Beacon as a payload. In fact, our colleagues at ESET and Avast recently assessed that HoneyMyte was active in the s
time and common occurrence in Myanmar of both campaigns could suggest that various TTPs of HoneyMyte may have been borrowed for the activity of LuminousMoth.

2. [THRUNTER.ORG] This threat actor targets nongovernmental organizations using Mongolian-themed lures for espionage purposes.
In April 2017, CrowdStrike Falcon Intelligence observed a previously unattributed actor group with a Chinese nexus targeting a U.S.-based think tank. Further analysis revealed a wider ca
techniques, and procedures (TTPs). This adversary targets non-governmental organizations (NGOs) in general, but uses Mongolian language decoys and themes, suggesting this actor has a spe
intelligence on Mongolia. These campaigns involve the use of shared malware like Poison Ivy or PlugX.
Recently, Falcon Intelligence observed new activity from MUSTANG PANDA, using a unique infection chain to target likely Mongolia-based victims. This newly observed activity uses a series
fileless, malicious implementations of legitimate tools to gain access to the targeted systems. Additionally, MUSTANG PANDA actors reused previously-observed legitimate domains to host f

[CROWDSTRIKE] VERTIGO PANDA is China-nexus adversary that has likely been active since at least mid-2020 as a discrete operational group separate from—but adjacent to—MUSTANG PANDA. Thro
PANDA has targeted defense and government sector organizations worldwide with an emphasis on Europe, as well as likely targeting religious sector organizations and the Vatican.

3. [MITRE] [Mustang Panda](https://attack.mitre.org/groups/G0129) is a China-based cyber espionage threat actor that was first observed in 2017 but may have been conducting operations si
Panda](https://attack.mitre.org/groups/G0129) has targeted government entities, nonprofits, religious, and other non-governmental organizations in the U.S., Europe, Mongolia, Myanmar, Pa

Demo Backup ☺

Searching for Threat Actor info on 'MUSTANG PANDA'; will display any relevant Malpedia links :

Searched for "MUSTANG PANDA": 1 Results Found: - MUSTANG PANDA

Result 1. Match found for Threat Actor "MUSTANG PANDA"

Threat Actor:
MUSTANG PANDA

Aliases:
BASIN
BRONZE PRESIDENT
Camaro Dragon
Earth Preta
HoneyMyte
LuminousMoth
Mustang Panda
PKPLUG
Polaris
Red Lich
RedDelta
Stately Taurus
TA416
TANTALUM
TEMP.HEX
Twill Typhoon
UNC1066
VERTIGO PANDA

Description(s):

1. [ETDA] (Kaspersky
vectors, malicious i
being noisy, and thu

We recently came acr
observed in South Ea
much more active in

Further analysis rev
connections, and the
time and common occu

2. [THRUNTER.ORG] Th
In April 2017, Crowd
techniques, and proc
intelligence on Mong
Recently, Falcon Int
fileless, malicious

[CROWDSTRIKE] VERTIG
PANDA has targeted d

3. [MITRE] [Mustang
Panda](https://attac

References:
https://attack.mitre.org/groups/G0129
https://attack.mitre.org/groups/G1014
https://blog.checkpoint.com/securing-user-and-access/smugx-unveiling-a-chinese-based-apt-operation-targeting-european-governmental-entities-check-point-research-exposes-a-shifting-trend/
https://blog.checkpoint.com/security/check-point-research-reveals-a-malicious-firmware-implant-for-tp-link-routers-linked-to-chinese-apt-group/
https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/
https://blog.talosintelligence.com/2022/05/mustang-panda-targets-europe.html
https://blog.talosintelligence.com/mustang-panda-targets-europe/
https://blog.vincss.net/2020/03/re012-phan-tich-ma-doc-loi-dung-dich-COVID-19-de-phat-tan-gia-mao-chi-thi-cua-thu-tuong-Nguyen-Xuan-Phuc.html
https://blogs.blackberry.com/en/2022/12/mustang-panda-uses-the-russian-ukrainian-war-to-attack-europe-and-asia-pacific-targets
https://csirt-cti.net/2024/01/23/stately-taurus-targets-myanmar/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2020-0728.pdf
https://insights.oem.avira.com/new-wave-of-plugx-targets-hong-kong/
https://jsac.jpcert.or.jp/archive/2023/pdf/JSAC2023_2_LT4.pdf
https://lab52.io/blog/new-mustang-pandas-campaing-against-australia/
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW
https://research.checkpoint.com/2023/beyond-the-horizon-traveling-the-world-on-camaro-dragons-usb-flash-drives/
https://research.checkpoint.com/2023/malware-spotlight-camaro-dragons-tinynote-backdoor/
https://securelist.com/apt-luminousmoth/103332/
https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
https://thecyberwire.com/podcasts/microsoft-threat-intelligence/4/notes
https://therecord.media/indonesian-intelligence-agency-compromised-in-suspected-chinese-hack/
https://threats.wiz.io/all-actors/mustang-panda
https://threats.wiz.io/all-incidents/earth-pretas-campaign-abusing-mavinject-to-bypass-detection
https://unit42.paloaltonetworks.com/chinese-apts-target-asean-entities/
https://unit42.paloaltonetworks.com/pkplug_chinese_cyber_espionage_group_attacking_asia/
https://unit42.paloaltonetworks.com/stately-taurus-abuses-vscode-southeast-asian-espionage/
https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian-government/
https://unit42.paloaltonetworks.com/stately-taurus-targets-philippines-government-cyberespionage/
https://unit42.paloaltonetworks.com/stately-taurus-uses-bookworm-malware/
https://unit42.paloaltonetworks.com/thor-plugx-variant/
https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2023-q3-2023.pdf
https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations
https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations#When:17:14:00Z
https://www.anomali.com/blog/covid-19-themes-are-being-utilized-by-threat-actors-of-varying-sophistication#When:14:00:00Z
https://www.bitdefender.com/blog/labs/luminousmoth-plugx-file-exfiltration-and-persistence-revisited
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html
https://www.cfr.org/interactive/cyber-operations/mustang-panda
https://www.crowdstrike.com/adversaries/mustang-panda
https://www.crowdstrike.com/adversaries/vertigo-panda
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/
https://www.darkreading.com/threat-intelligence/chinese-apt-bronze-president-spy-campaign-russian-military
https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european
https://www.proofpoint.com/us/blog/threat-insight/ta416-goes-ground-and-returns-golang-plugx-malware-loader
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.secureworks.com/blog/bronze-president-targets-government-officials
https://www.secureworks.com/blog/bronze-president-targets-russian-speakers-with-updated-plugx
https://www.secureworks.com/research/bronze-president-targets-ngos
https://www.secureworks.com/research/threat-profiles/bronze-president
https://www.trendmicro.com/en_us/research/22/k/earth-preta-spear-phishing-governments-worldwide.html
https://www.trendmicro.com/en_us/research/23/c/earth-preta-cyberespionage-campaign-hits-over-200.html
https://www.trendmicro.com/en_us/research/23/c/earth-preta-updated-stealthy-strategies.html
https://www.trendmicro.com/en_us/research/23/f/behind-the-scenes-unveiling-the-hidden-workings-of-earth-preta.html
https://www.trendmicro.com/en_us/research/24/b/earth-preta-campaign-targets-asia-doplugs.html
https://www.trendmicro.com/en_us/research/24/i/earth-preta-new-malware-and-strategies.html
https://www.trendmicro.com/en_us/research/24/b/earth-preta-mixes-legitimate-and-malicious-components-to-sidestep-detection.html
https://www.welivesecurity.com/2022/03/29/mustang-panda-hodur-old-tricks-new-korplug-variant/
https://www.welivesecurity.com/2023/03/02/mqsttang-mustang-panda-latest-backdoor-treads-new-ground-qt-mqtt/
https://www.zscaler.com/blogs/security-research/latest-mustang-panda-arsenal-paklog-corklog-and-splatcloak-p2
https://www.zscaler.com/blogs/security-research/latest-mustang-panda-arsenal-toneshell-and-starproxy-p1

Malpedia had 10 unique references related to Threat Actor 'MUSTANG PANDA': (Date / URL)
[2025-03-21] https://hunt.io/blog/darkpeony-certificate-patterns
[2024-10-25] https://www.trendmicro.com/en_in/research/24/i/earth-preta-new-malware-and-strategies.html
[2024-10-18] https://www.welivesecurity.com/en/eset-research/separating-bee-panda-ceranakeeper-making-beeline-thailand/
[2024-10-09] https://hitcon.org/2024/CMT/slides/Sailing_the_Seven_SEAs_Deep_Dive_into_Polaris_Arsenal_and_Intelligence_Insights.pdf
[2024-09-11] https://hunt.io/blog/toneshell-backdoor-used-to-target-attendees-of-the-iiss-defence-summit
[2024-07-17] https://lab52.io/blog/mustang-pandas-plugx-new-variant-targetting-taiwanese-government-and-diplomats/
[2024-07-17] https://research.checkpoint.com/2023/chinese-threat-actors-targeting-europe-in-smugx-campaign/
[2024-07-17] https://go.recordedfuture.com/hubfs/reports/cta-2022-1223.pdf
[2024-07-10] https://files.speakerdeck.com/presentations/6d01e26c85a444d0a3f888e45629635f/hodur_recon2024.pdf
[2023-09-08] https://blog.sekoia.io/my-teas-not-cold-an-overview-of-china-cyber-threat/

Demo Backup

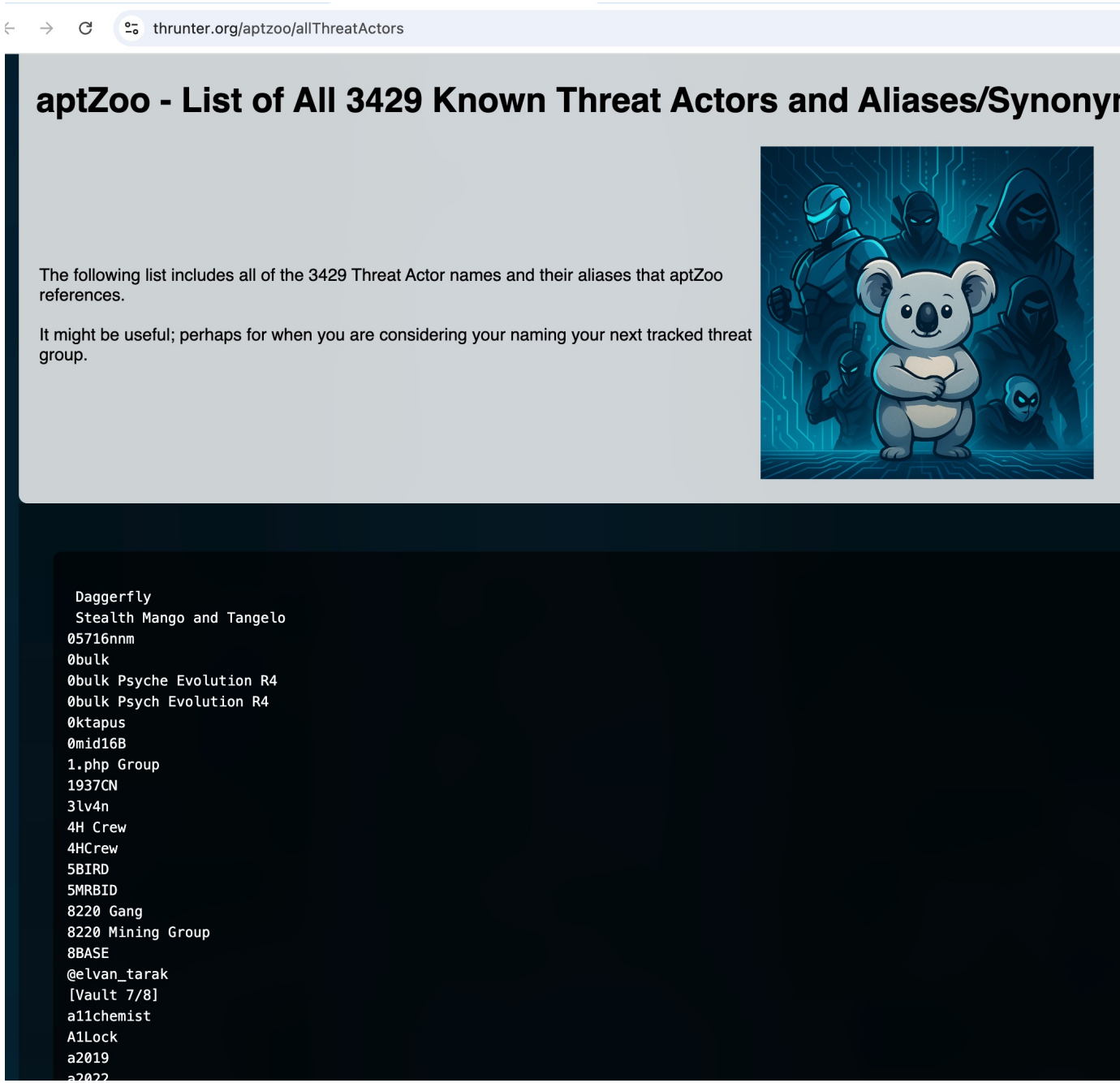
- ☺

If you are a vendor

- Perhaps check your

Next Threat actor name

Isn’t taken!



TLP:CLEAR

How does the tool work again?

- On the backend – it Gathers data from:
  - MISP Threat Actor Cluster on GitHub
  - ETDA Threat Actor database
  - MITRE Attack Groups
  - Malpedia
  - Microsoft Threat Actors
  - Thrunter.org
  - Published websites

- Enables searching this data for:
  - Threat Actor Names/Aliases
  - Descriptions
  - References

Additional Features

- You can query your own repository!
- You may have good reason to lookup your own Threat Actor repository:
- Perhaps you have internal naming for threat actors you track?
  - Referencing internal / non-published documents?
- Or you can't wait for MISP/MITRE/ETDA/Malpedia etc to update?
- You can add your own repository – where you add info of interest
- Tool will examine MISP/MITRE/Malpedia/ETDA data and merge with your own repository

Why you might want your own TA repository:

For example:

Reading an interesting blog:

SilentPush discovered a new threat actor: ‘IMP-1G’

This Threat Actor is so new – it’s not in MISP/Malpedia – you can add your own definition in your local repo.

October 10, 2024

SILENT PUSH

EXECUTIVE SUMMARY

Silent Push Threat Analysts have developed a method for locating and tracking the deployment of SMS phishing domains – a.k.a. “smishing” – from a previously unknown threat actor, who we are designating **IMP-1G**.

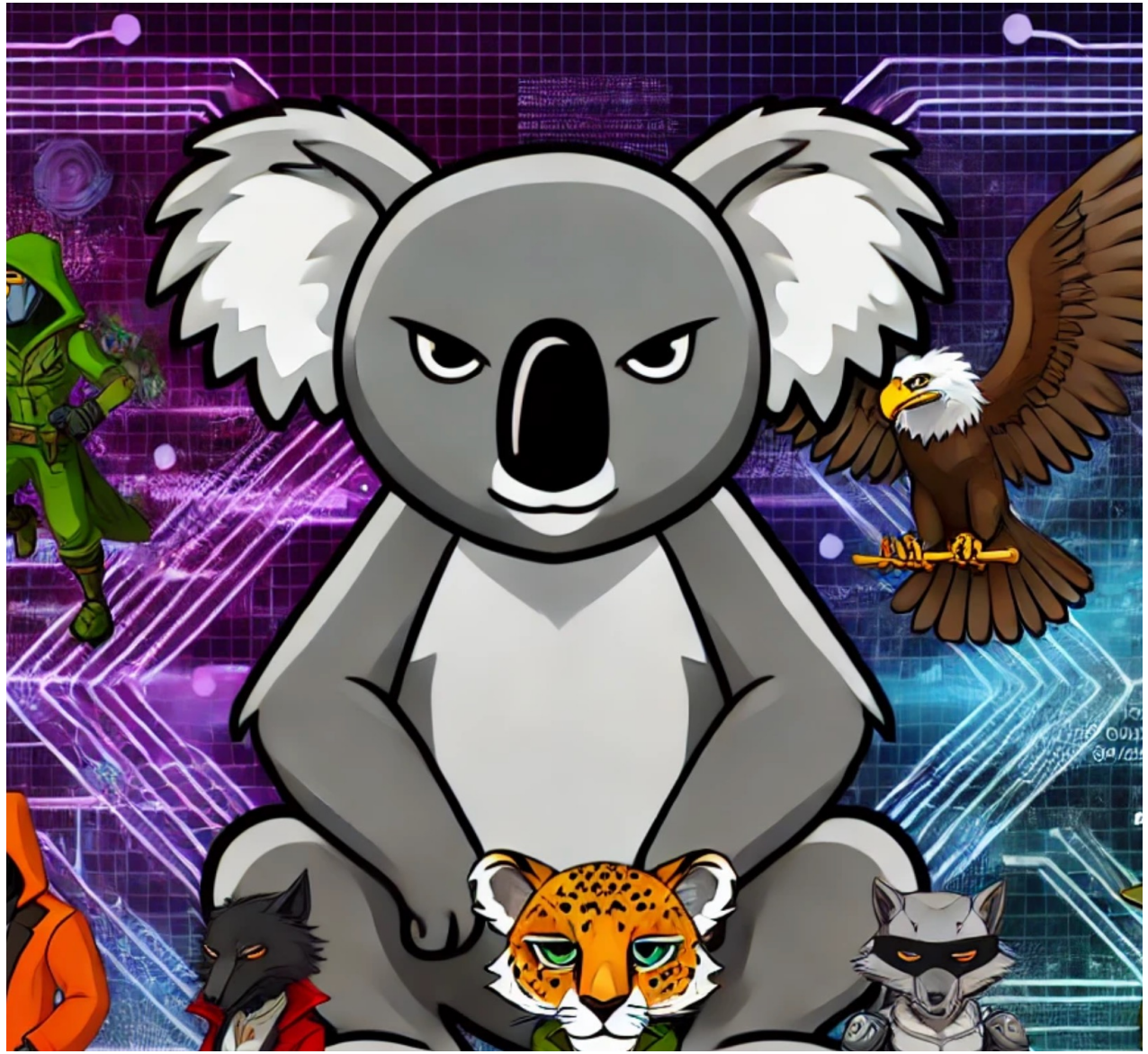
TLP:CLEAR

Or tracking unpublished threat Actors

- IRON KANGAROO?

Or tracking unpublished threat Actors

- Or KARMA KOALA?



Or for tracking your commercial Cyber Threat Intel

- Keep track of relevant links to reports in their portal

More features

- Works when you are offline/airgapped network
  - Not everyone is connected to the internet in real time…
  - Don’t have to worry about your queries being tracked

Other Lookup tools

- MISP has some software:
  - https://github.com/MISP/threat-actor-intelligence-server
  - A simple ReST server to lookup threat actors (by name, synonym or UUID) and return the corresponding MISP galaxy information about the known threat actors.
    - Has a number of limitations – not simple to install but may be useful for some
- Malpedia has a nice web interface: https://malpedia.caad.fkie.fraunhofer.de
- ORKL.eu is also great

Important!

- There are multiple names for different threat actors
- Threat actors can evolve and are fluid – members can work in different groups
- Attribution is based on different sets of telemetry - end up with multiple names for what seems to be the same threat groups.
- Important to remember - Threat groups are fluid and they evolve, they are rarely 1:1
- Threat Actor overlaps include malware samples, tools, commands, infrastructure, TTPs.

Important!

- Sean Sullivan from F-Secure once said:

“Threat Actor attribution/research is like a being a palaeontologist who has found some bones of a dinosaur:

Everyone may have a bone,
But no one has the full skeleton”

Future Work cont..

- Malware family / tooling lookup:
  - Eg. IcedID – malware typically used by threat actor LUNAR Spider
  - Malware families suffer the same problem as Threat actors
- Add more good data sources
  - Alienvault, Automating Vendor naming scraping
- Improving the data
  - lots of old reports – links are now dead
  - Eg. fireeye.com's APT reports

Challenges

- Keeping this updated
- Automated a lot of it.
  MISP/ETDA/Malpedia/MITRE are more straightforward
- Some other sources are more manual

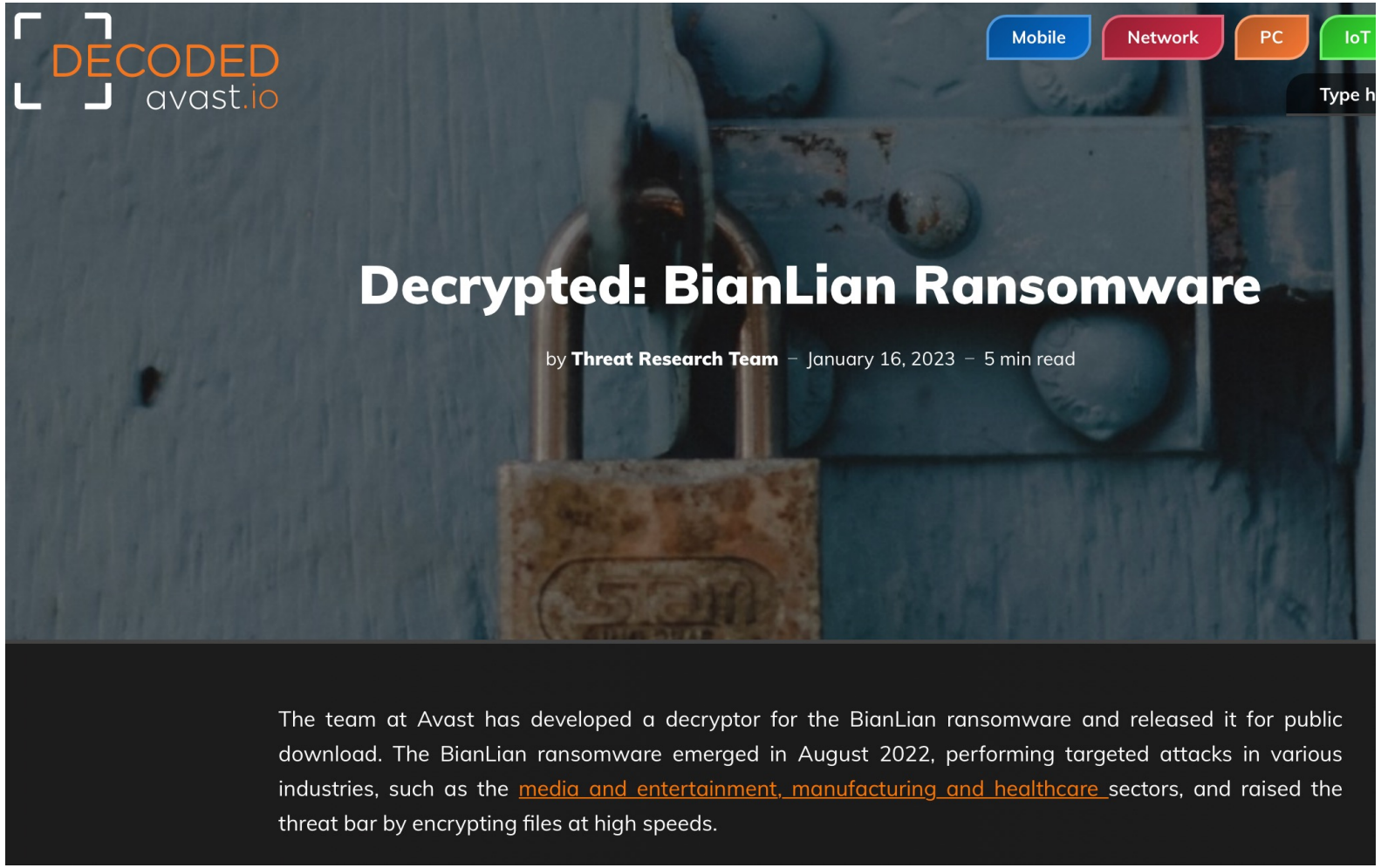
Avast (and Gen's) mission

- Two years ago - Avast joined with NortonLifelock to become Gen Digital – the new name
- Still honoring the original Avast mission:

  "Everyone has the right to have Free Cyber Security"
- We have a big responsibility – over 500 million users
- Keen to help CERTs/LE/partners
- Have helped many people with ransomware infections
- Some of our success stories are public:
- – others not….

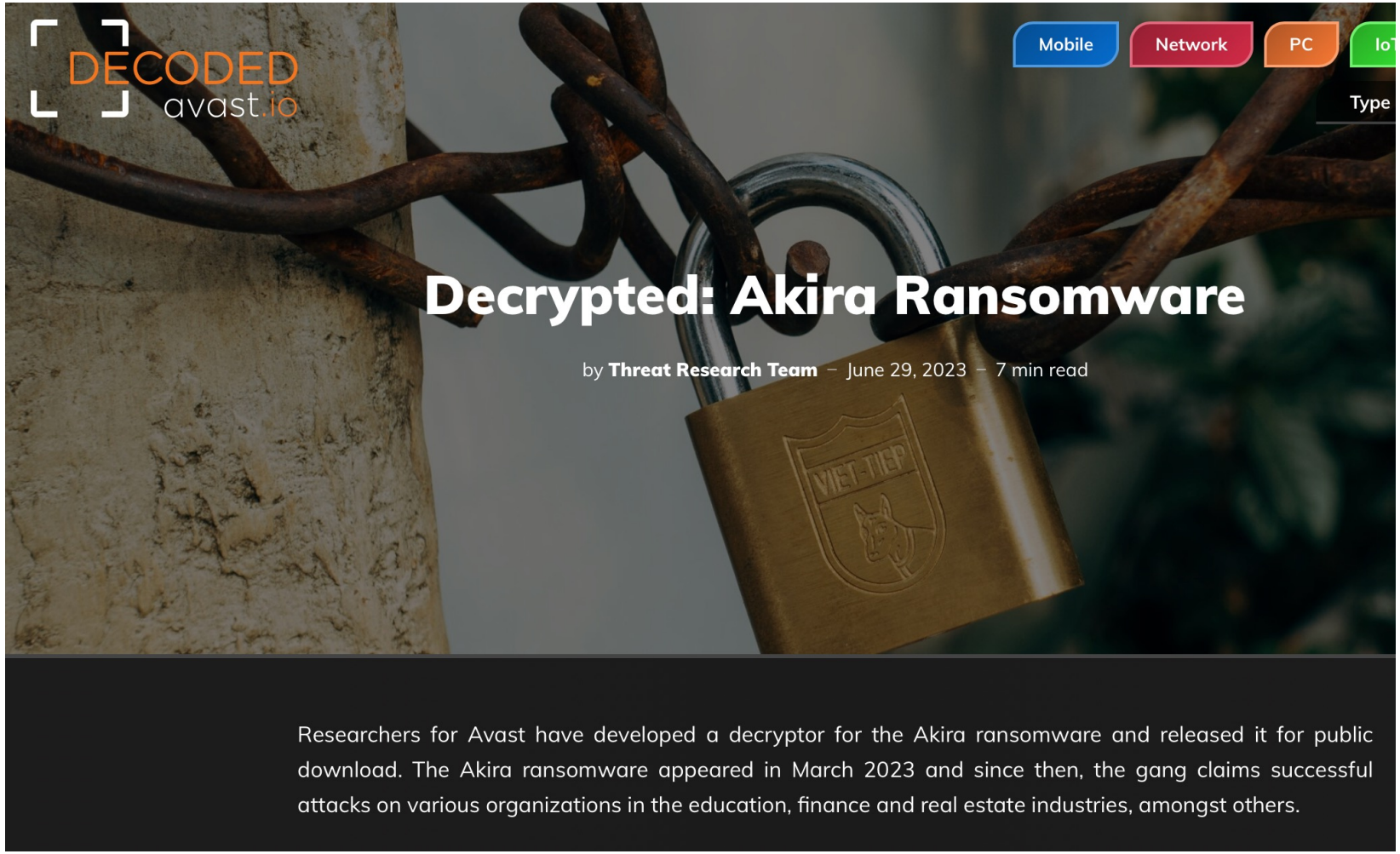
Some success stories:

- Bian Lian ransomware:



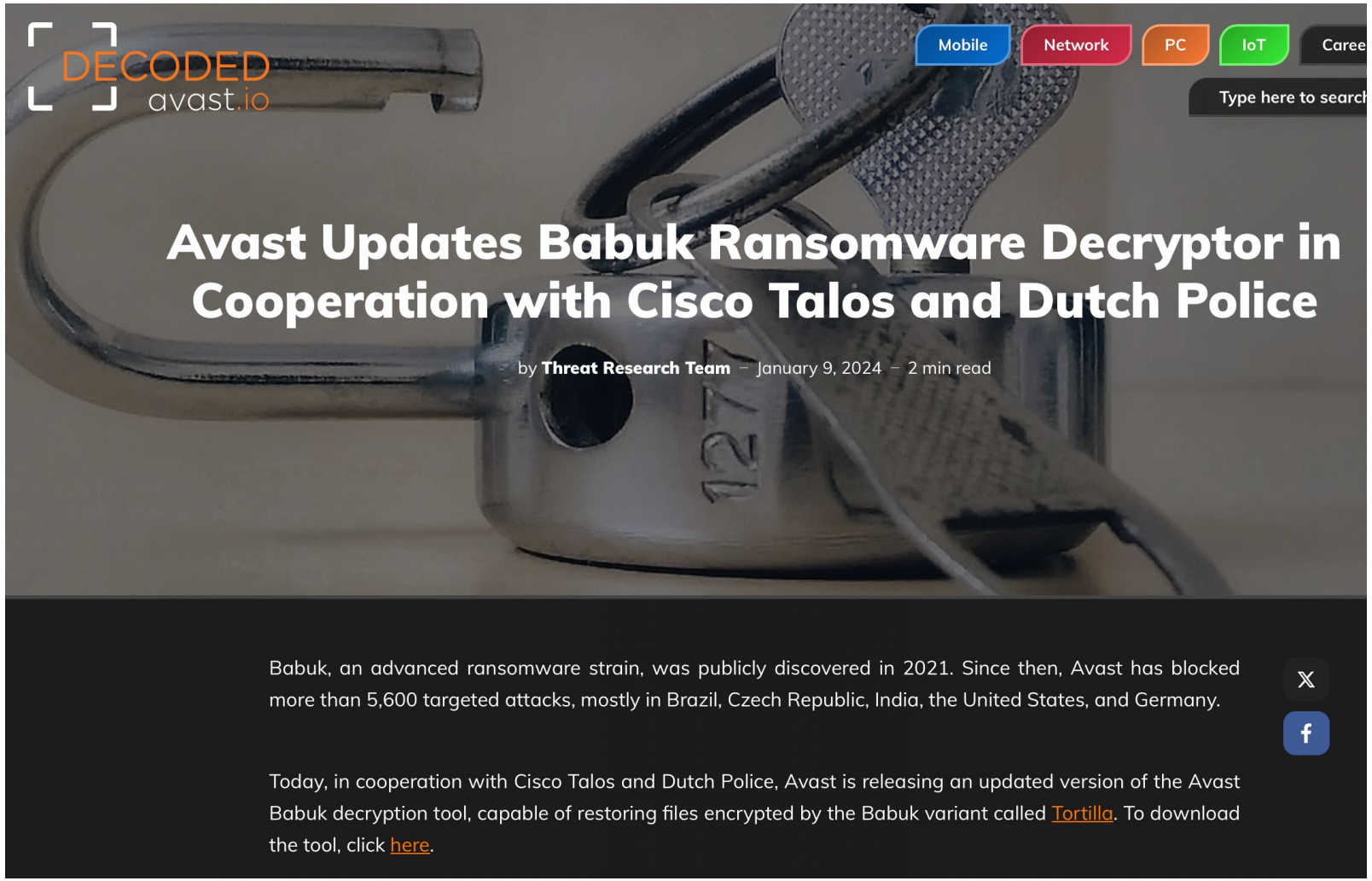
Some successes:

- Akira Ransomware:



Some successes:

- Babuk Ransomware



Some successes:

- Rhysida Ransomware

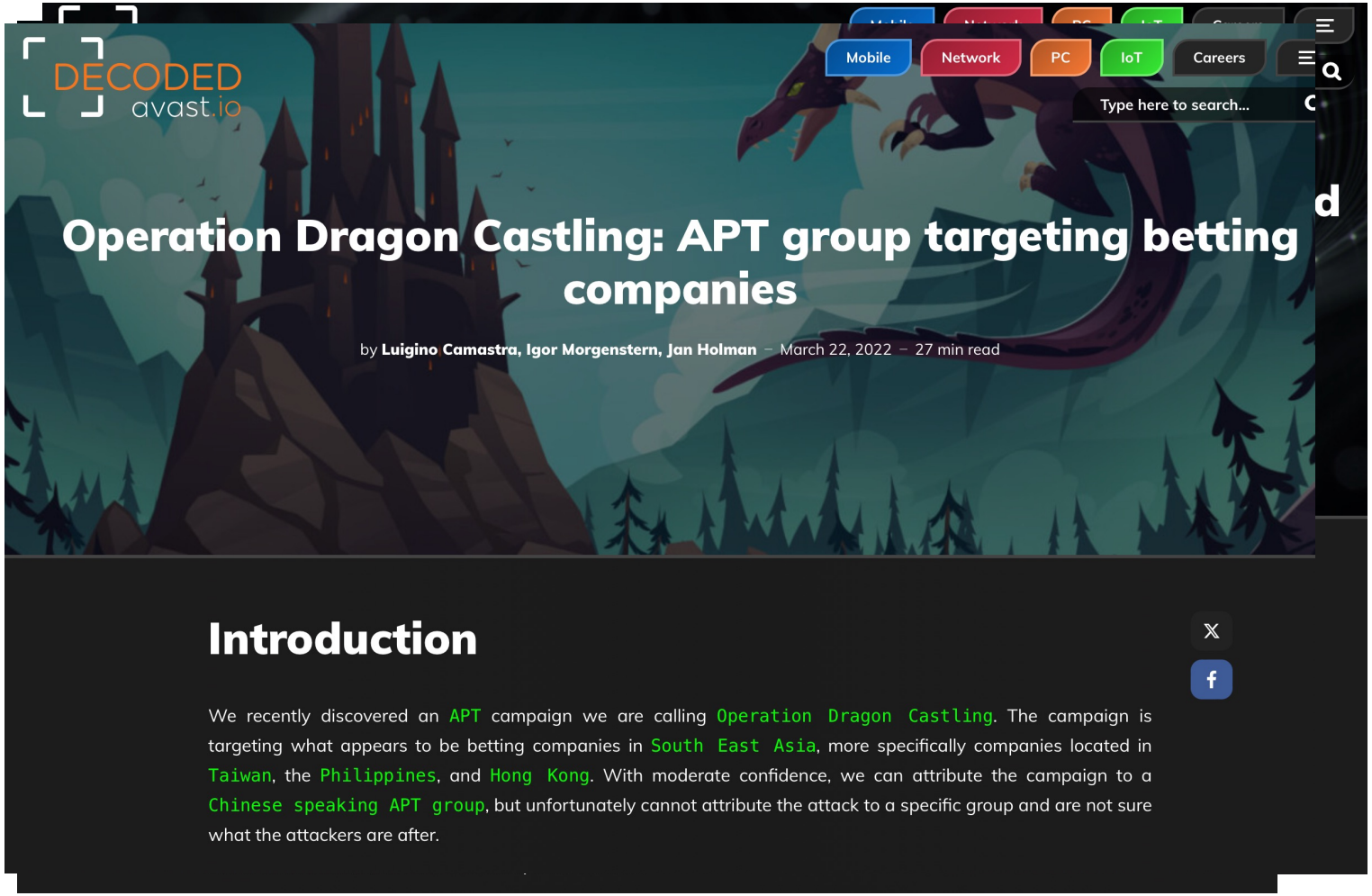
Some successes:

- HomuWitch Ransomware

Avast (and Gen Digital's) mission

- Other successful tools are not shared openly…
- Why? We don't want to alert the Threat Actors about weaknesses in their Ransomware
- Perhaps we can help….

Sometimes we share success stories



But not everything can be shared in this way

- Typically we contact a CERT
- Or use contacts in FIRST or Trusted Introducers

TF-CSIRT
Trusted Introducer

FIRST

TLP:CLEAR

Always happy to help

- If you have malware you are not sure about
- Or you're unlucky enough to get ransomware/wipers deployed
- Contact me: LinkedIn/Signal/Keybase/PGP/FIRST/Email
- Slides/code: github.com/forensicdave

Check out the APTZOO:

thrunter.org