DefMal Workshop
6/6/2025

The threat actor naming mess

Measured

Juan Tapiador, Universidad Carlos III de Madrid

Context

- Linking malware to campaigns (=operations) and groups (=TAs)

- Ground truth retrieved from ~15k multivendor CTI reports
  - Time
  - Victimology (geographies, sector, motivation)
  - Group
  - IoCs

Attribution is hard.

Naming is harder.

APT 9, APT 15, APT 17, APT 19, APT 26, APT 41, AXIOM, BACKDOOR DIPLOMACY, BARIUM, BEIJING GROUP, BRONZE ATLAS, BRONZE EXPORT, BRONZE FIRESTONE, BRONZE KEYSTONE, BRONZE PALACE, DEEP PANDA, ELDERWOOD, HIDDEN LYNX, KE3CHANG, NIGHTSHADE PANDA, TURBINE PANDA, WINNTI GROUP

How have we come to this?

What gets named (and renamed), and why

- Analysis workflows involve clustering together threat activity / intrusion sets.
- Clusters get names for internal cataloging and for future correlation.
- Because the process is approximately similar across vendors, naming schemes are roughly similar in structure, but each vendor has one.
- During CTI dissemination (conferences, reports, STIX, …) vendors use their internal names.

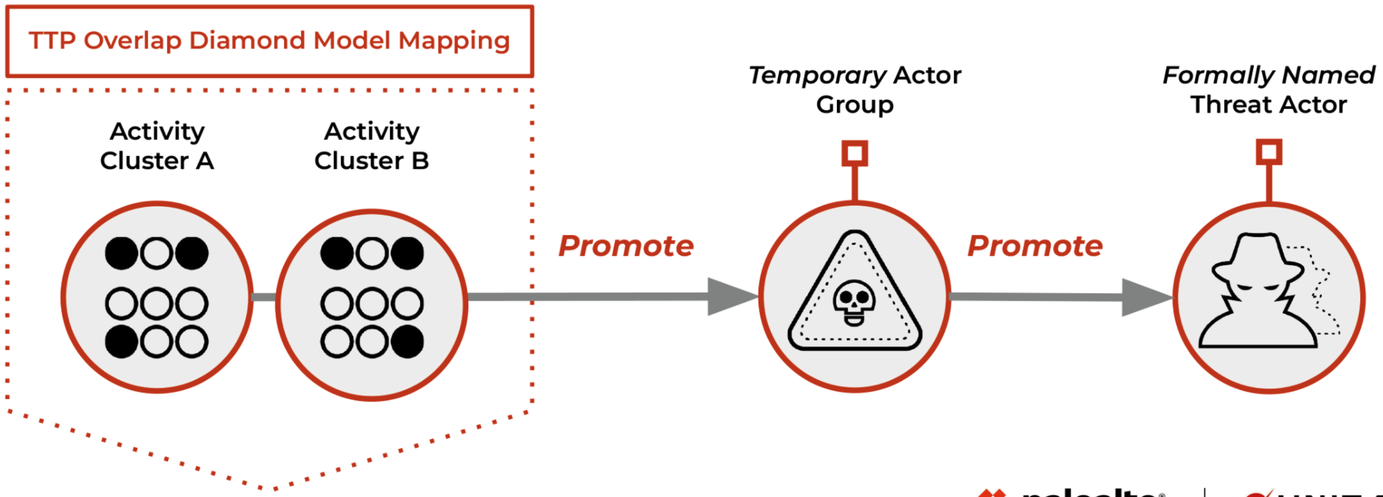
The graduation of a TA

The case of Unit 42

`CL-{CRI | STA | MIX | UNK} - ####` → `TGR-{CRI | STA | MIX | UNK} - ####`

"Graduation"

- **CL** - short for cluster
- **CRI** - short for criminal motivation
- **STA** - short for state-backed motivation
- **MIX** - short for mixed motivation
- **UNK** - short for unknown motivation



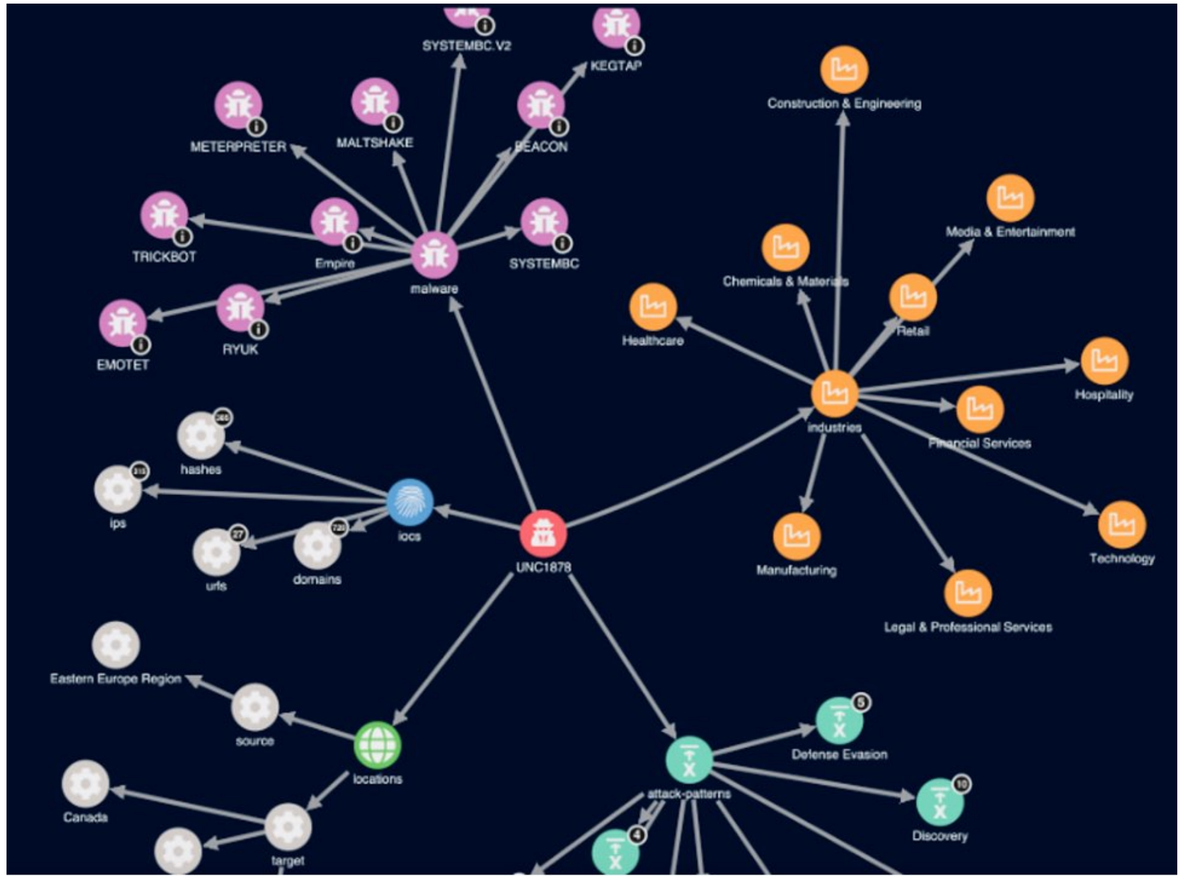
https://unit42.paloaltonetworks.com/from-activity-to-formal-naming/

paloalto NETWORKS | UNIT 42 BY PALO ALTO NETWORKS

Mandiant (FireEye, Trellis)

(FireEye)

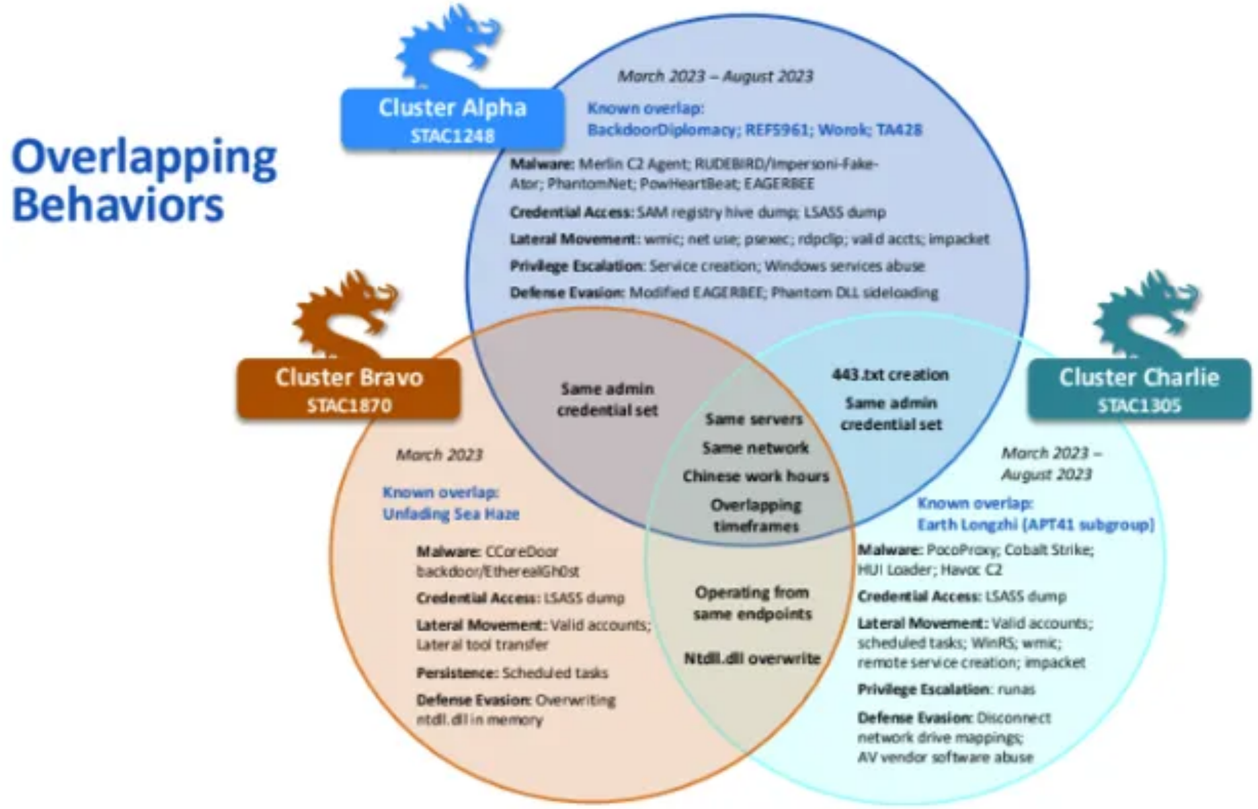
- UNC[XXXX] (e.g. UNC1878) for clusters of threat activity
- TEMP.[X] (e.g. TEMP.Periscope) for activity traced back to a TA but cannot yet claim motivations with confidence
- APT
- FIN

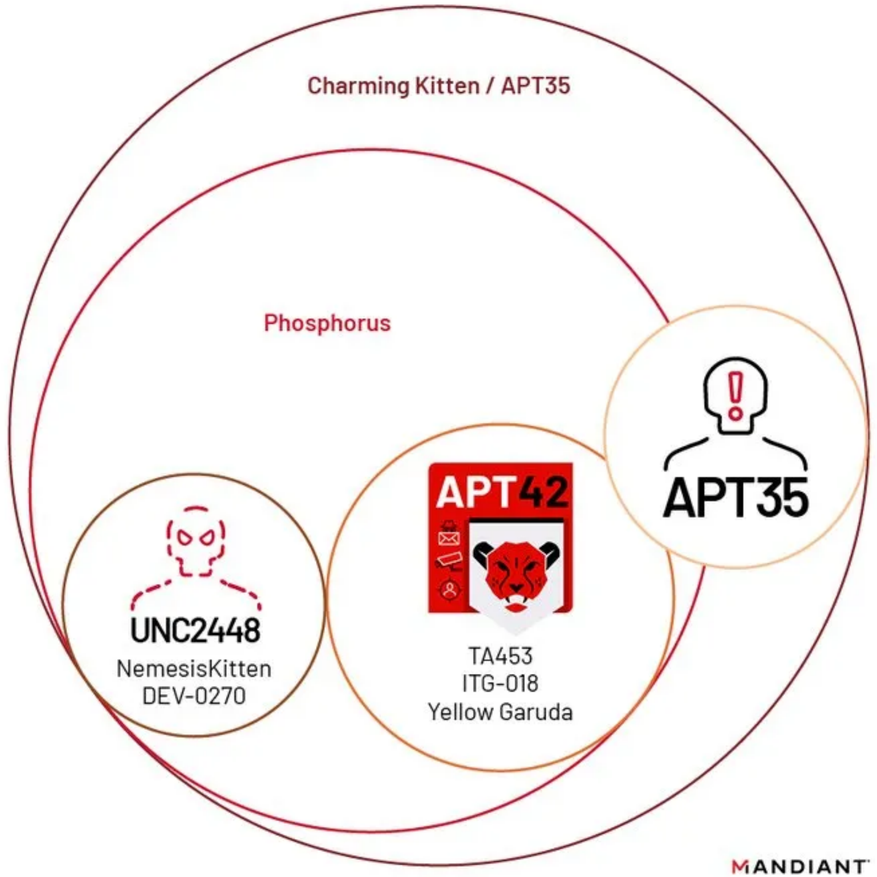


https://cloud.google.com/blog/topics/threat-intelligence/how-mandiant-tracks-uncategorized-threat-actors

Overlapping tradecraft

Or, from intrusion clusters to TAs

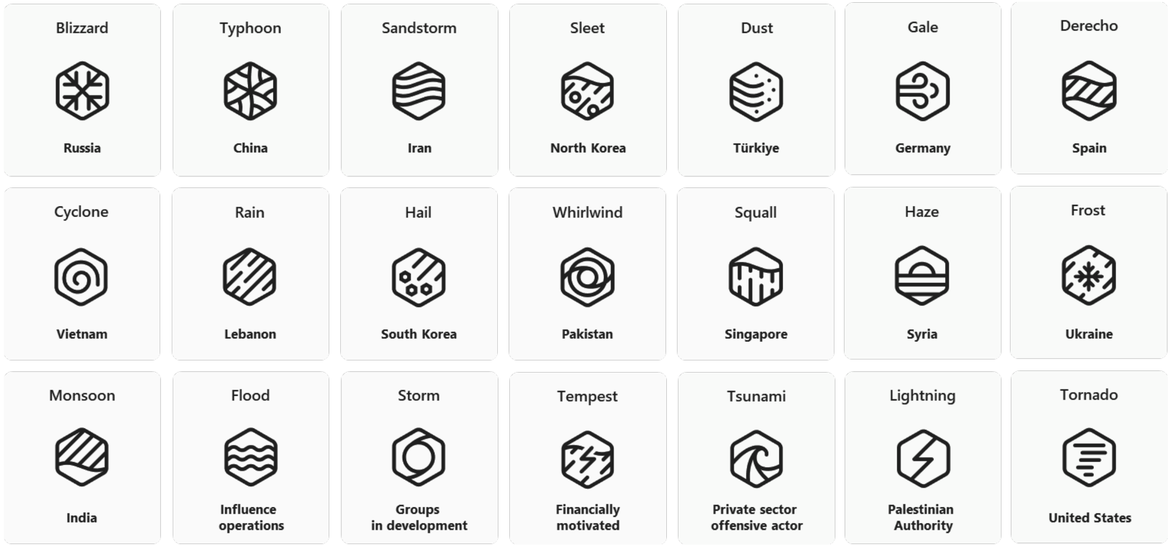




https://medium.com/@Shinigami42/what-a-cluster-how-industry-groups-and-names-threat-activity-clusters-0c65a7128162

Namespaces

MSFT naming scheme (new)



Threat actor category	Type	Family name
Nation-state	China Iran Lebanon North Korea Russia South Korea Türkiye Vietnam	Typhoon Sandstorm Rain Sleet Blizzard Hail Dust Cyclone
Nation-state	China Germany India Iran North Korea Lebanon Pakistan Palestinian Authority Russia Singapore South Korea Spain Syria Türkiye Ukraine United States Vietnam	Typhoon Gale Monsoon Sandstorm Sleet Rain Whirlwind Lightning Blizzard Squall Hail Derecho Haze Dust Frost Tornado Cyclone
Financially motivated	Financially motivated	Tempest
Private sector offensive actors	PSOAs	Tsunami
Influence operations	Influence operations	Flood
Groups in development	Groups in development	Storm

CrowdStrike naming scheme

eCrime

LIGHTNING SPIDER
HOOK SPIDER
SINFUL SPIDER
HOLIDAY SPIDER
SAMBA SPIDER
LUNAR SPIDER
OCULAR SPIDER
RADIANT SPIDER
PLUMP SPIDER
CURLY SPIDER
CHATTY SPIDER
RENAISSANCE SPIDER
PUNK SPIDER
RECESS SPIDER

BRAIN SPIDER
SCATTERED SPIDER
AVIATOR SPIDER
PROPHET SPIDER
GRACEFUL SPIDER
SCULLY SPIDER
CLOCKWORK SPIDER
SCION SPIDER
APOTHECARY SPIDER
MASKED SPIDER
HONEY SPIDER
VICE SPIDER
SOLAR SPIDER
TRAVELING SPIDER

BUTLER SPIDER
HAZARD SPIDER
FROZEN SPIDER
VAMPIRE SPIDER
BITWISE SPIDER
NIMBLE SPIDER
COOKIE SPIDER
ROBOT SPIDER
TUNNEL SPIDER
ODYSSEY SPIDER
ROYAL SPIDER
BLIND SPIDER
INDRIK SPIDER
WIZARD SPIDER

North Korea

FAMOUS CHOLLIMA
VELVET CHOLLIMA

Russian Federation

PRIMITIVE BEAR
COZY BEAR
FANCY BEAR
GOSSAMER BEAR

Iran

SPECTRAL KITTEN
STATIC KITTEN
PULSAR KITTEN

China

TREASURE PANDA
VAULT PANDA
CASCADE PANDA
KRYPTONITE PANDA
LOCKSMITH PANDA
SUNRISE PANDA
PHANTOM PANDA
VIXEN PANDA

OVERCAST PANDA
VERTIGO PANDA
AQUATIC PANDA
CIRCUIT PANDA
MUSTANG PANDA
HORDE PANDA
OPERATOR PANDA
ENVOY PANDA

Hacktivism

BOUNTY JACKAL
CRUEL JACKAL

Egypt

WATCHFUL SPHINX

Pakistan

MYTHIC LEOPARD

MITRE ATT&CK naming scheme

Groups: 170

ID	Name	Associated Groups	Description
G0018	admin@338		admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors.
G1030	Agrius	Pink Sandstorm, AMERICIUM, Agonizing Serpens, BlackShadow	Agrius is an Iranian threat actor active since 2020 notable for a series of ransomware and wiper operations in the Middle East, with an emphasis on Israeli targets. Public reporting has linked Agrius to Iran's Ministry of Intelligence and Security (MOIS).
G0130	Ajax Security Team	Operation Woolen-Goldfish, AjaxTM, Rocket Kitten, Flying Kitten, Operation Saffron Rose	Ajax Security Team is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 Ajax Security Team transitioned from website defacement operations to malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies.
G1024	Akira	GOLD SAHARA, PUNK SPIDER, Howling Scorpius	Akira is a ransomware variant and ransomware deployment entity active since at least March 2023. Akira uses compromised credentials to access single-factor external access mechanisms such as VPNs for initial access, then various publicly-available tools and techniques for lateral movement. Akira operations are associated with "double extortion" ransomware activity, where data is exfiltrated from victim environments prior to encryption, with threats to publish files if a ransom is not paid. Technical analysis of Akira ransomware indicates variants capable of targeting Windows or VMWare ESXi hypervisors and multiple overlaps with Conti ransomware.

Others (many)

Geopolitical Entanglement				
	CrowdStrike	PAN	SecureWorks	TrendMicro
China	Panda	Taurus	BRONZE	
Iran	Kitten	Serpens	COBALT	
India	Tiger	Gemini	ZINC	
Motivations				
Espionage				Earth
Financially motivated	Spider	Libra	GOLD	Water
Hacktivists	Jackal	Virgo		Wind

Mappings

Lists of aliases

- Ideally mappings between two sources:

$$\mathbf{source_A{:}name_1 = source_B{:}name_2}$$

- But in reality is more like

$$\mathbf{source_A{:}name_1 = [name_2, name_3, name_4]}$$

  It’s up to you to figure out where those names (aliases) come from.

Example: MSFT mapping


```
{
        "Threat actor name": "Diamond Sleet",
        "Origin/Threat": "North Korea",
        "Other names": "ZINC, LABYRINTH CHOLLIMA, Black Artemis, Lazarus"
},
{
        "Threat actor name": "Emerald Sleet",
        "Origin/Threat": "North Korea",
        "Other names": "THALLIUM, VELVET CHOLLIMA, RGB-D5, Black Banshee, Kimsuky, Greendinosa"
},
{
        "Threat actor name": "Fallow Squall",
        "Origin/Threat": "Singapore",
        "Other names": "PLATINUM, PARASITE, RUBYVINE, GINGERSNAP"
},
{
        "Threat actor name": "Flax Typhoon",
        "Origin/Threat": "China",
        "Other names": "Storm-0919, ETHEREAL PANDA"
},
{
        "Threat actor name": "Forest Blizzard",
        "Origin/Threat": "Russia",
        "Other names": "STRONTIUM, FANCY BEAR, Sednit, ATG2, Sofacy, Blue Athena, Z-Lom Team, Operation Pawn Storm, Tsar Team, CrisisFour, HELLFIRE, APT28"
},
{
        "Threat actor name": "Ghost Blizzard",
        "Origin/Threat": "Russia",
        "Other names": "BROMINE, BERSERK BEAR, TG-4192, Koala Team, Blue Kraken, Crouching Yeti, Dragonfly"
},
{
        "Threat actor name": "Gingham Typhoon",
        "Origin/Threat": "China",
        "Other names": "GADOLINIUM, KRYPTONITE PANDA, TEMP.Periscope, Leviathan, JJDoor, APT40, Feverdream"
},
```

Example: MISP galaxy


```
 "values": [
    {
      "description": "PLA Unit 61398 (Chinese: 61398部队, Pinyin: 61398 bùduì) is the
Military Unit Cover Designator …"
       …
       "synonyms": [
          "COMMENT PANDA",
          "PLA Unit 61398",
          "Comment Crew",
          "Byzantine Candor",
          "Group 3",
          "TG-8223",
          "Comment Group",
          "Brown Fox",
          "GIF89a",
          "ShadyRAT",
          "G0006"
        ]
     …
     "value": "APT1"
    },
```

Example: APT Groups and Operations

THE spreadsheet

- Links to naming schemes of vendors, where available.
- Lists of TA names organized by {country/regions, others, unknown}.
- Names broken down by CTI vendor namespace.
- Aliases here and there, where known.
- Useful resource.
- Unknown coverage.

Issues with existing mappings

- Source/catalog/namespace not always available for all aliases.
    - It’s up to you to find out where each alias comes from.
    - Sometimes you can only say “others.”
- Often not reciprocal
    - Source A says A:X has B:Y as an alias.
    - Source B does not say B:Y has A:X an alias.
- Sources may:
    - Change their naming scheme.
    - Split a TA into multiple subgroups, or vice versa.
    - Use different syntax conventions.

Result

ANDY GREENBERG SECURITY APR 23, 2023 7:00 AM

Hacker Group Names Are Now Absurdly Out of Control

Pumpkin Sandstorm. Spandex Tempest. Charming Kitten. Is this really how we want to name the hackers wreaking havoc worldwide?



ILLUSTRATION: JACQUI VANLIEW; GETTY IMAGES

Motivation and goals

- Gain a more empirical understanding of the problem
- Develop a tool to defragment TA names, integrating as many existing mappings as possible

Measurement

Dataset

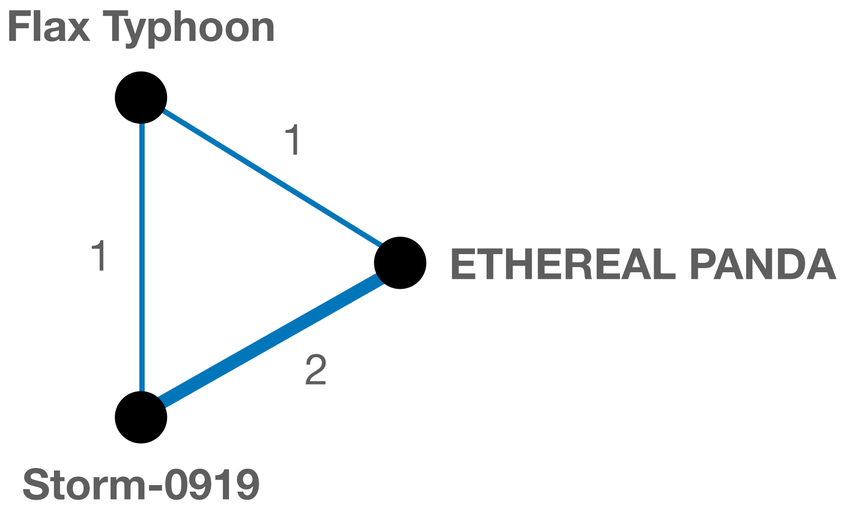
11 sources
13,371 CTI reports
1,675 TA profiles

Source	Dataset
MITRE	MITRE ATT&CK STIX Data [16]
APTnotes	APTnotes Data [4]
CyberMonitor	APT & Cybercriminals Campaign Collection [6]
ETDA	Threat Group Cards: A Threat Actor Encyclopedia [7]
Malpedia	Malpedia Collection [8]
OTX	Alienvault Open Threat Exchange [2]
Secureworks	Secureworks Threat Profiles [19]
AGRO	APT Groups and Operations [3]
ORKL	ORKL Community Contributed Content [17]
MISPGALAXY	MISP Galaxy Clusters [14]
VXUG	vx-underground Papers [20]

Threat Actor Name Alias Graph (TANAG)

```
{
  “source” = “MSTIC”
  “ta_canonical_name” = “Flax Typhoon”,
  “ta_aliases” = [“Storm-0919”, “ETHEREAL PANDA”],
  “country” = “China”,
  “reports” = [“url 1”, “url 2”, …],
  “tools” = [“tool 1”, “tool 2”, …],
   …
}
```

```
{
  “source” = “Malpedia”
  “ta_canonical_name” = “Ethereal Panda”,
  “ta_aliases” = [“Storm-0919”],
  “country” = “China”,
  “reports” = [“url 1”, “url 2”, …],
  “tools” = [“tool 1”, “tool 2”, …],
   …
}
```

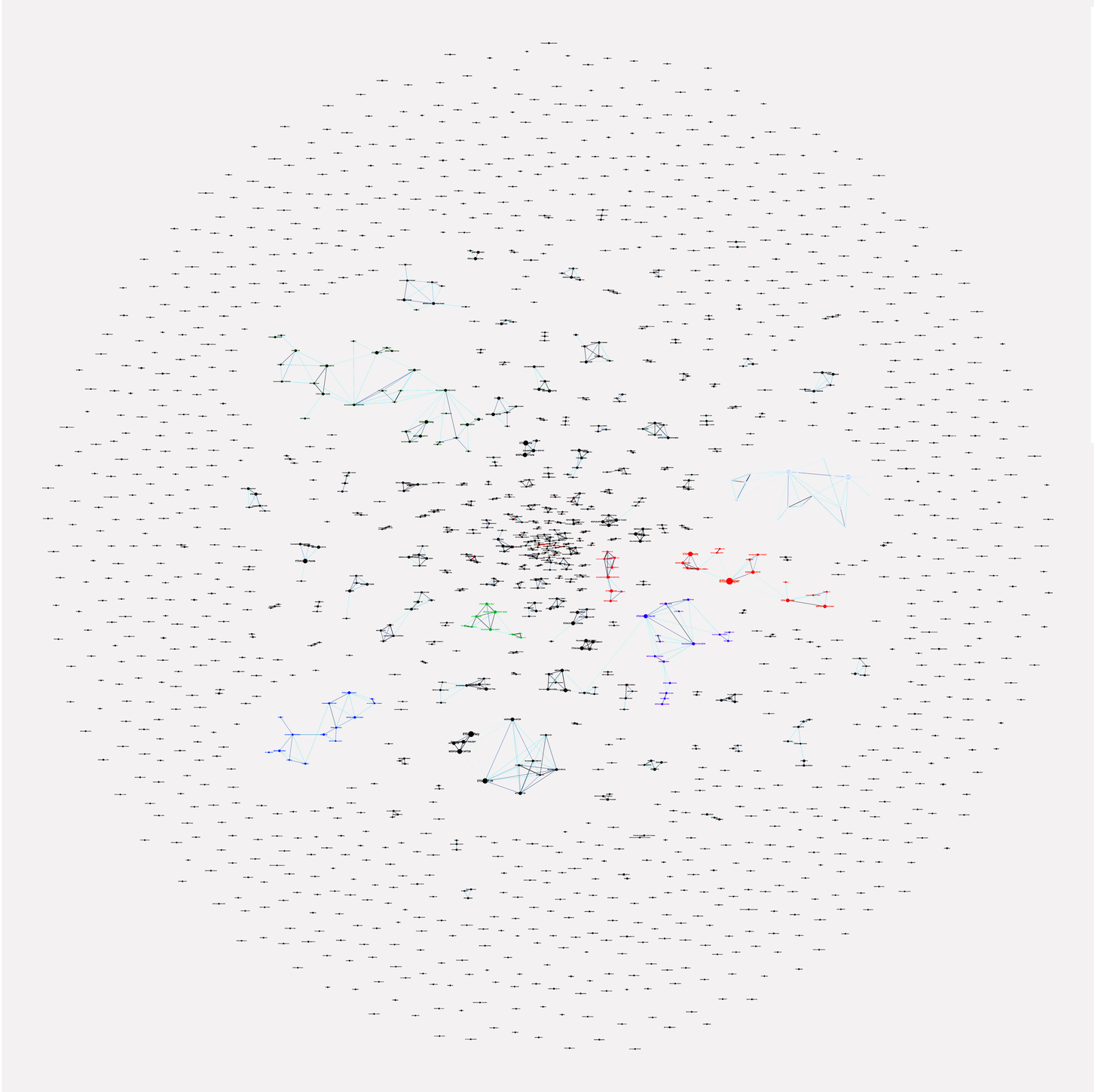


Threat Actor Name Alias Graph (TANAG)

Issues

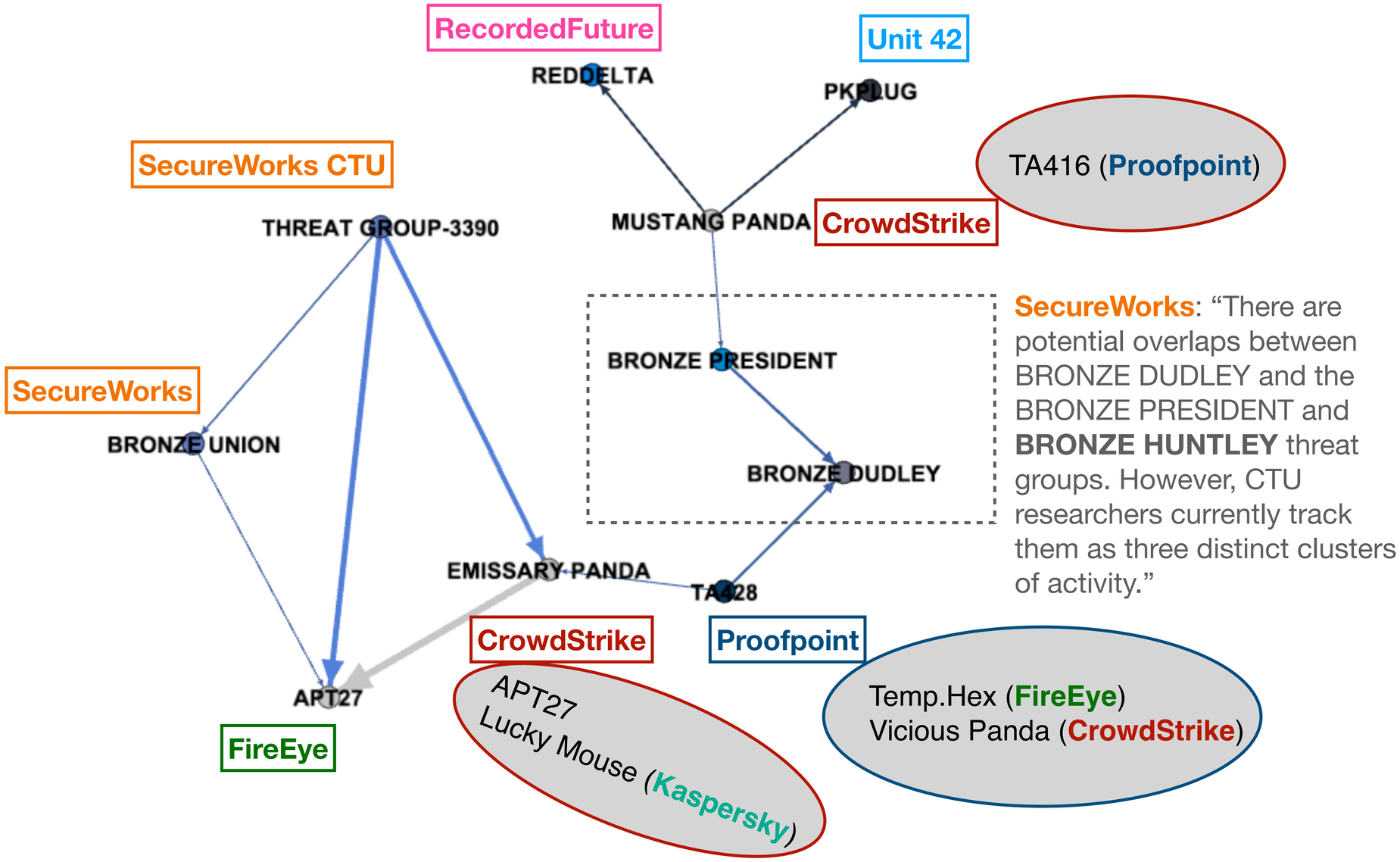
- EMISSARY PANDA vs. Emissary Panda
- APT41 vs. APT 41 vs. APT-41
- THREAT GROUP-3390 vs. Group-3390
- MACHETE vs. EL MACHETE

We match names considering identified syntax discrepancies, yet …


REDDELTA
PKPLUG
MUSTANG PANDA
THREAT GROUP-3390
BRONZE PRESIDENT
BRONZE UNION
BRONZE DUDLEY
EMISSARY PANDA
TA428
APT27
LAZARUS GROUP
ANDARIEL
TRADERTRAITOR
NICKEL HYATT
COVELLITE
SILENT CHOLLIMA
BEAGLEBOYZ
NICKEL ACADEMY
APT38
BLUENOROFF
NICKEL GLADSTONE
BACKDOORDIPLOMACY
BADIUM
BRONZE EXPORT
APT15
KE3CHANG
WINNTI GROUP
APT41
BRONZE ATLAS
BRONZE PALACE
APT 41
AXIOM
HIDDEN LYNX
BRONZE KEYSTONE
APT17
BRONZE CRESTONE
APT19
APT26
NIGHTSHADE PANDA
TURBINE PANDA
NEXUS ZETA
APT9
APT 17
DEEP PANDA
APT 19
BEIJING GROUP
ELDERWOOD

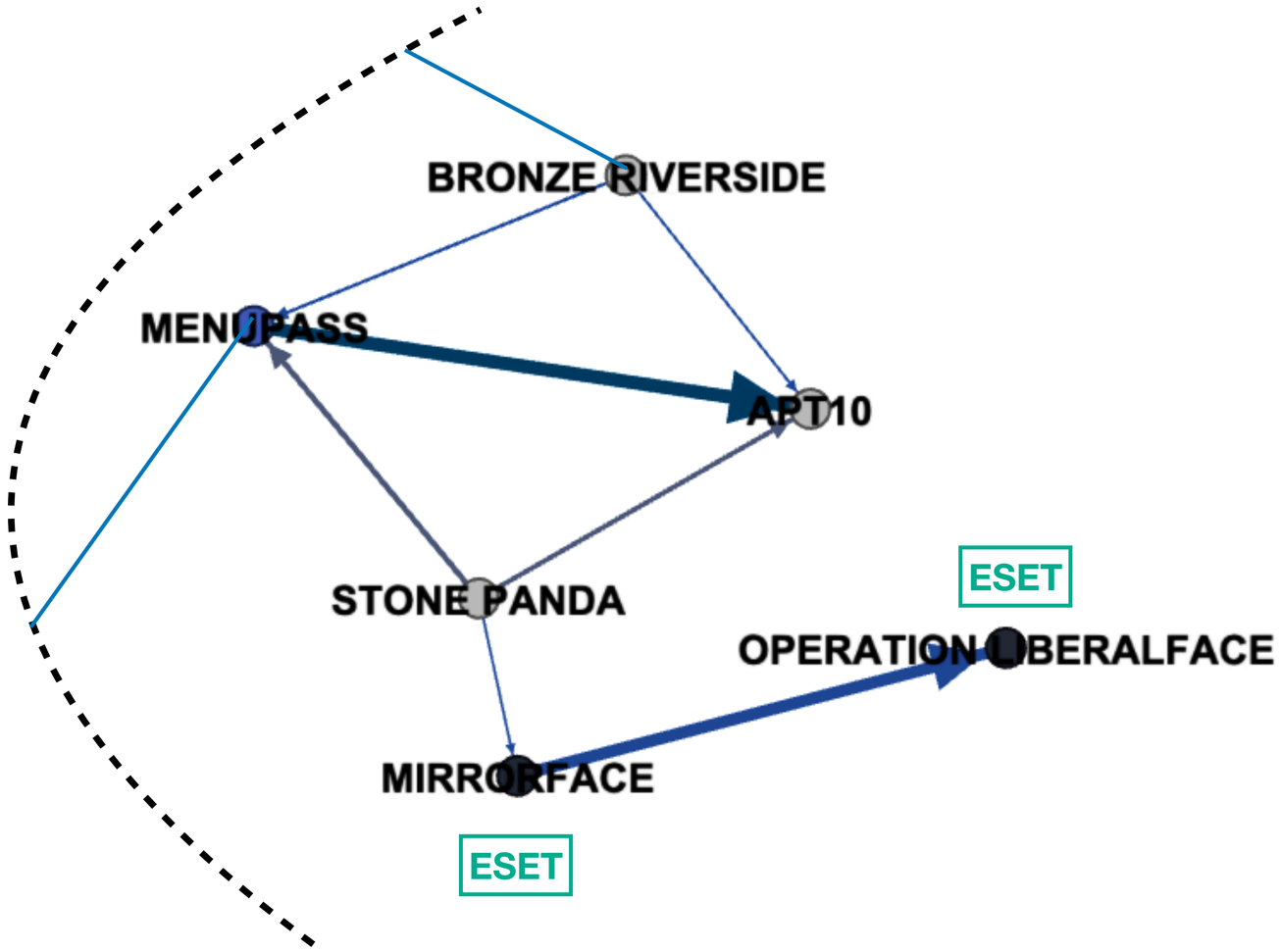
APT27

BASIN
Earth Preta
HoneyMyte
LuminousMoth
Polaris
Red Lich
Stately Taurus
TANTALUM
Twill Typhoon
Earth Smilodon
G0027
GreedyTaotie
Group 35
Iron Taurus
Iron Tiger
Red Phoenix
TEMP.Hippo
ZipToken



SecureWorks: "There are potential overlaps between BRONZE DUDLEY and the BRONZE PRESIDENT and **BRONZE HUNTLEY** threat groups. However, CTU researchers currently track them as three distinct clusters of activity."

Names conflated with operations

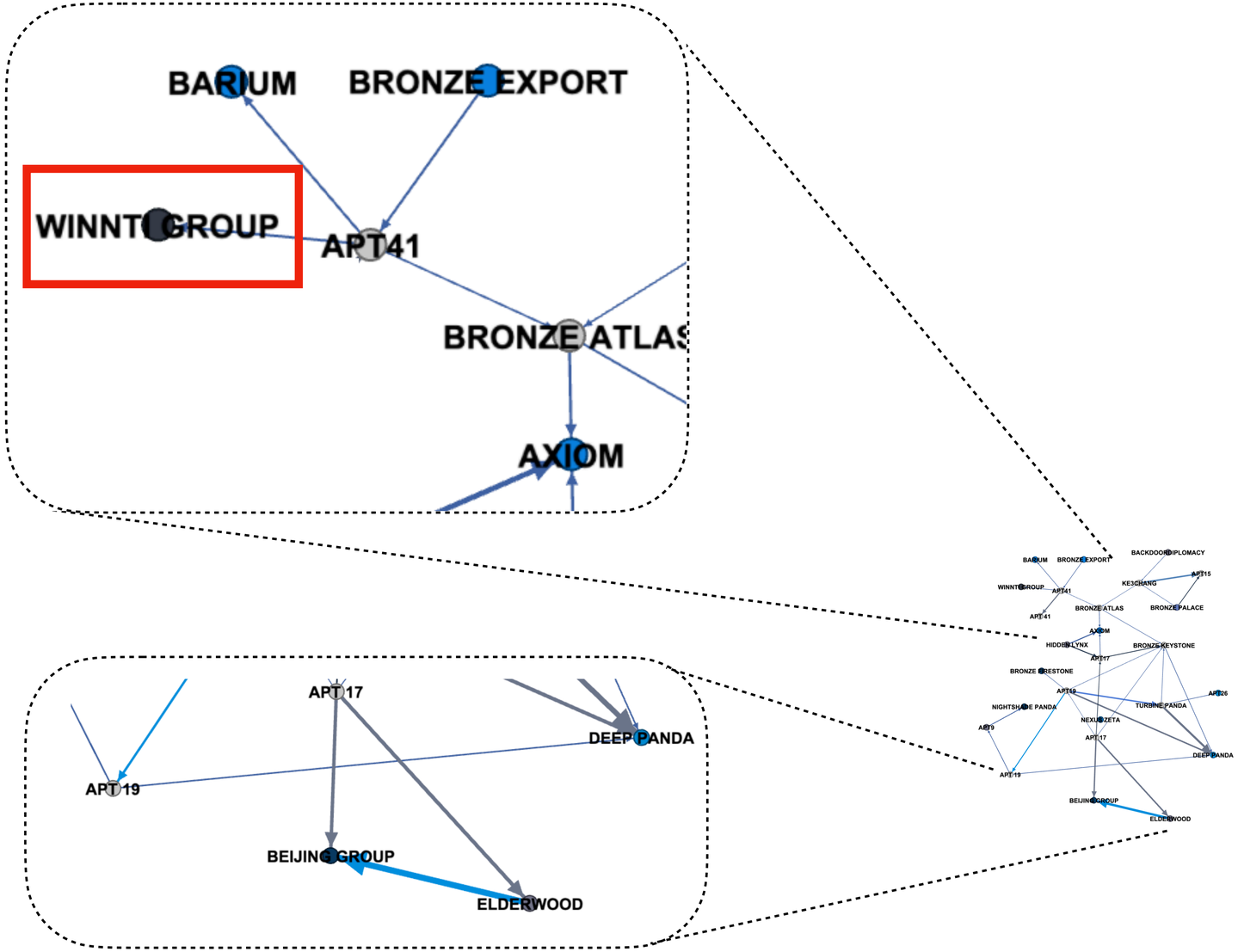


"ESET researchers discovered a **spearphishing campaign**, launched in the weeks leading up to the Japanese House of Councillors election in July 2022, **by the APT group that ESET Research tracks as MirrorFace**. The campaign, which we have named **Operation LiberalFace**, targeted Japanese political entities"

Names conflated with malware

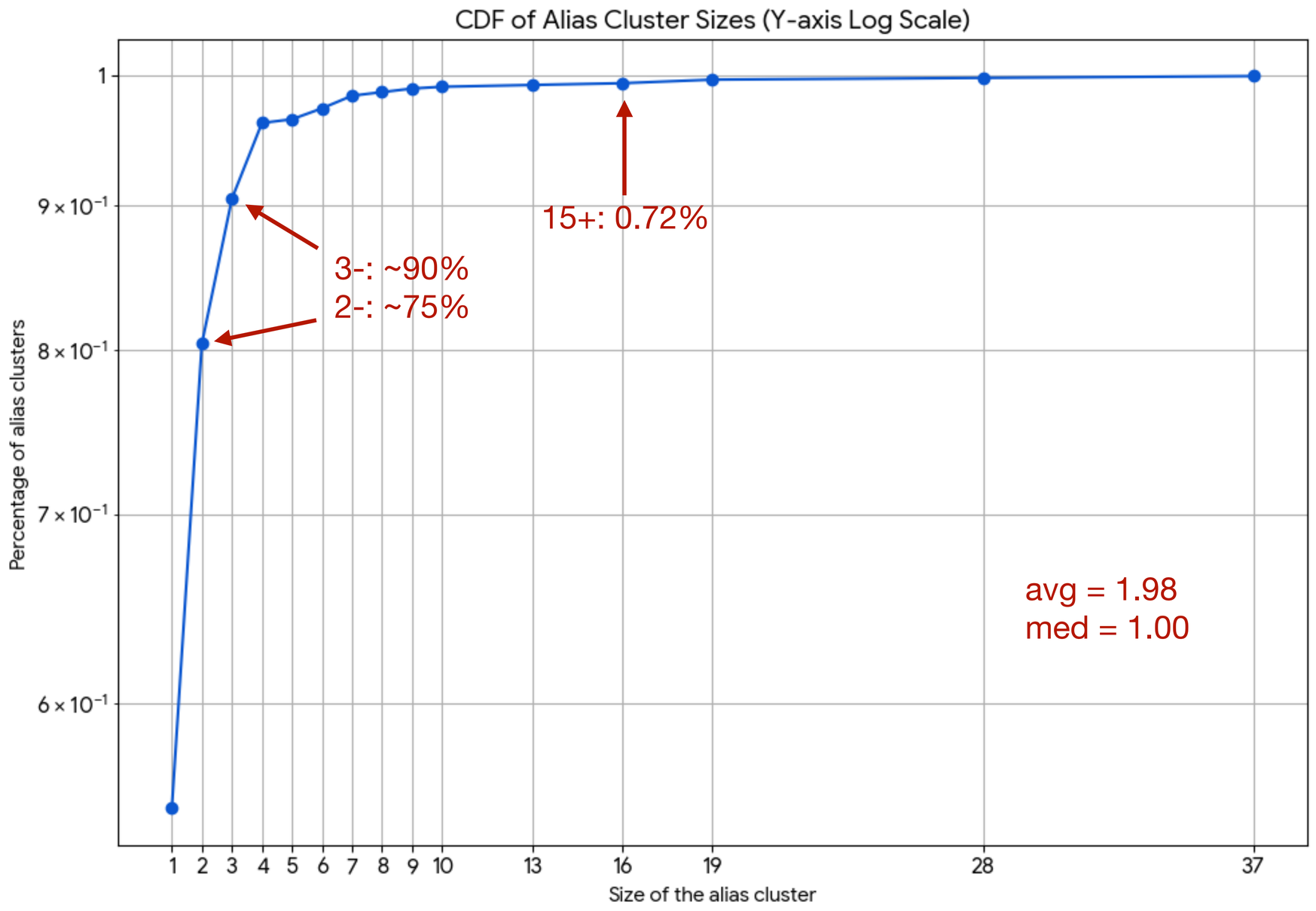
WINNTI: trojan/RAT family heavily used by a number of Chinese APT groups. Initially (2011) used to target the gaming industry and later found in in attacks targeting organizations in other sectors.

ELDERWOOD/BEIJING GROUP (PLA) and **Operation Aurora**.



What is the research question?

RQ1: alias clusters distribution


CDF of Alias Cluster Sizes (Y-axis Log Scale)
Percentage of alias clusters
1
9 × 10⁻¹
8 × 10⁻¹
7 × 10⁻¹
6 × 10⁻¹
1 2 3 4 5 6 7 8 9 10 13 16 19 28 37
Size of the alias cluster
15+: 0.72%
3-: ~90%
2-: ~75%
avg = 1.98
med = 1.00

RQ2: why?

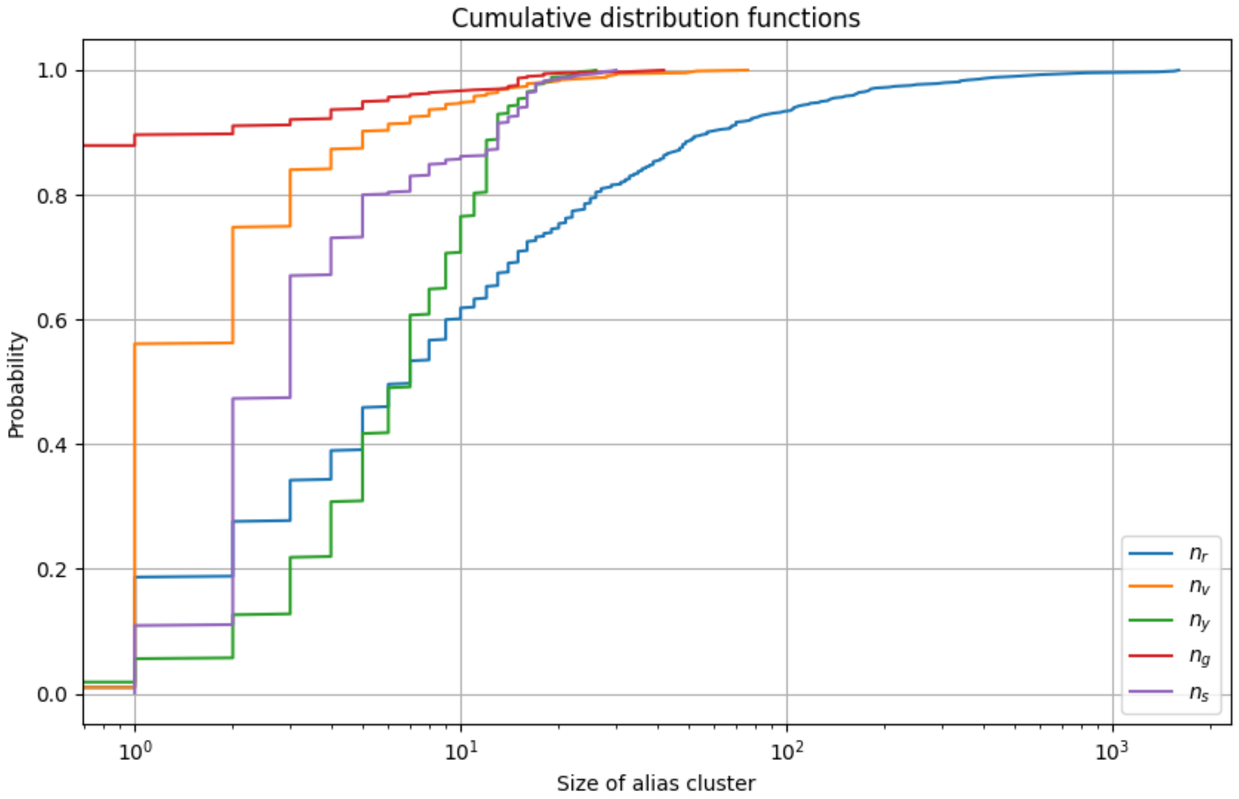
Correlation analysis: cluster features

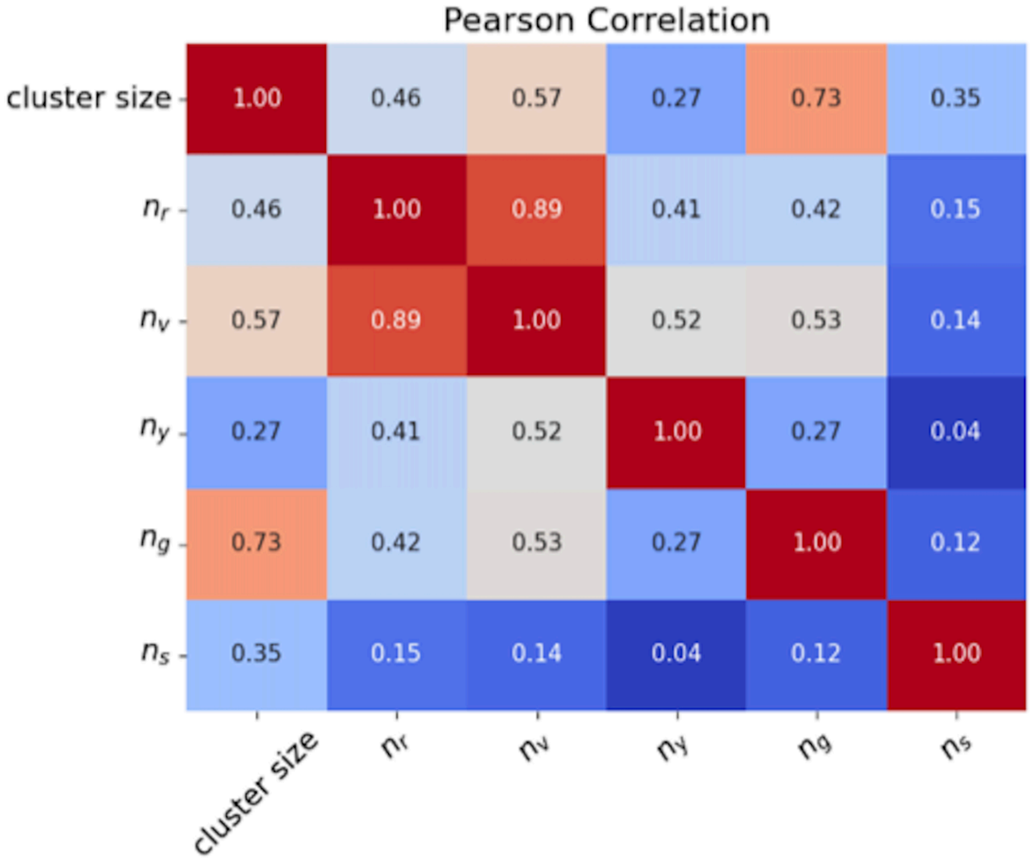
- n_r = Number of CTI reports in which any of the aliases in the cluster appear.
- n_v = Number of CTI vendors that have published a CTI report about the TA.
- n_y = Number of years that the TA has been studied (by any CTI vendor).
- n_g = Number of different geographies or world regions targeted by the TA.
- n_s = Number of victim sectors targeted by the TA.

Correlation analysis: methods

- **Linear**
  - Pearson’s correlation coefficient
- **Monotonic**
  - Spearman’s rank correlation
  - Kendall’s Tau

Correlation analysis: results

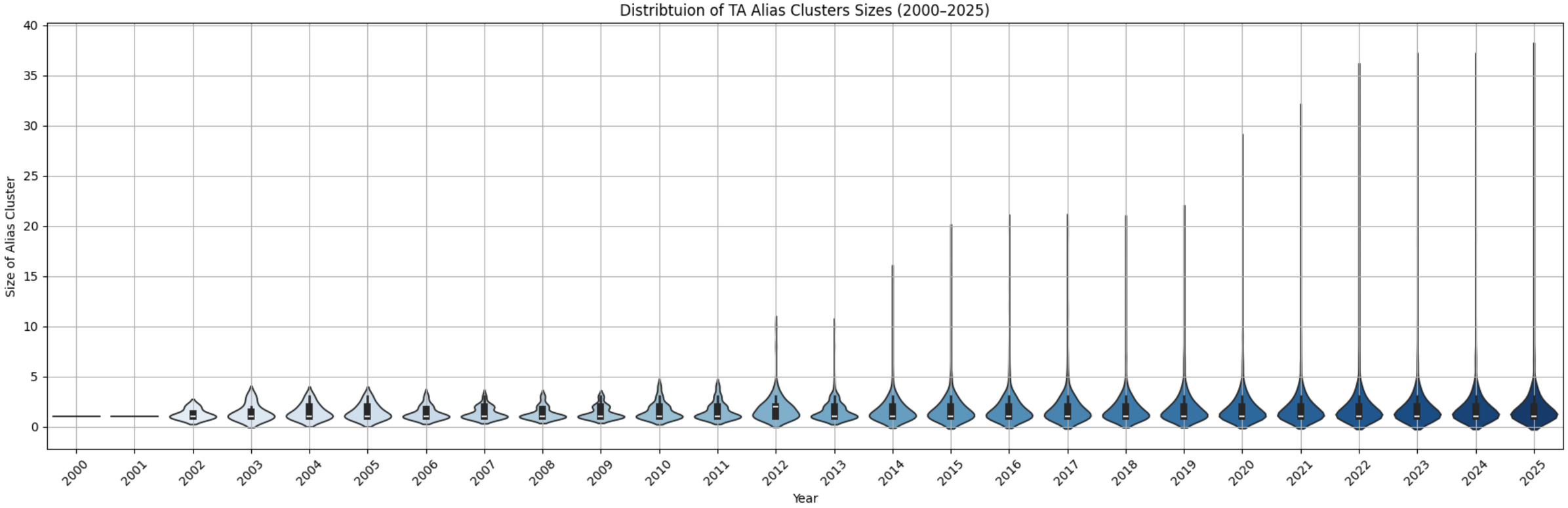




Correlation analysis: results

TA feature	Pearson	Spearman	Kendall	Interpretation
n_r	0.4615 (p=5.993e-38)	0.5096 (p=3.398e-47)	0.4200 (p=5.974e-45)	Moderate, possibly nonlinear
n_v	0.5706 (p=2.745e-61)	0.4474 (p=1.645e-35)	0.3989 (p=3.992e-34)	Fairly strong, primarily linear
n_y	0.2727 (p=2.561e-13)	0.2891 (p=7.576e-15)	0.2328 (p=1.034e-14)	Weak correlation
n_g	0.7301 (p=1.039e-116)	0.4599 (p=1.125e-37)	0.4242 (p=1.526e-34)	Very strong linear correlation
n_s	0.3463 (p=5.219e-21)	0.4112 (p=9.812e-30)	0.3504 (p=7.936e-29)	Moderate, possibly nonlinear

RQ3: evolution


Distribtuion of TA Alias Clusters Sizes (2000–2025)
Size of Alias Cluster
Year
0
5
10
15
20
25
30
35
40
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025

Solutions

MISP RFC

https://www.misp-standard.org/rfc/threat-actor-naming.html

Workgroup:	Network Working Group
Internet-Draft:	draft-00
Published:	21 December 2024
Intended Status:	Informational
Expires:	24 June 2025

Authors:	A. Dulaunoy	P. Bourmeau
	CIRCL	*Cubessa*

Recommendations on Naming Threat Actors

Abstract

This document provides advice on the naming of threat actors (also known as malicious actors). The objective is to provide practical advice for organizations such as security vendors or organizations attributing incidents to a group of threat actors. It also discusses the implications of naming a threat actor for intelligence analysts and threat intelligence platforms such as MISP [MISP-P].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Table of Contents ▲

1. Introduction
   1.1. Conventions and Terminology
2. Recommendations
   2.1. Reusing Threat Actor Names
   2.2. Uniqueness
   2.3. Format
   2.4. Encoding
   2.5. Avoid Confusing Actor Names with Malware Names
   2.6. Directory
3. Examples
4. Security Considerations
5. Acknowledgements
6. References
7. References
   7.1. Normative References
   7.2. Informative References

Authors' Addresses

It is unlikely to work

- Remember CARO
    - Syntax rules may be adopted or may be inspirational

- But 2 vendors won't be able to agree on whether they are referring to the same TA unless they share raw intelligence (telemetry)
    - Systematically, not on a case-by-case basis
- Are they willing to do it?
- Are they allowed to do it?

Naming is hard.

Correction:

Agreeing on a naming convention is hard.

Correction 2:

Adopting a naming convention is really hard.

In the meantime, we just need better mappings …

MALWARE & THREATS

Microsoft, CrowdStrike Lead Effort to Map Threat Actor Names

Microsoft and CrowdStrike are running a project that aims to align threat actor names, and Google and Palo Alto Networks will also contribute.



By Eduard Kovacs | June 3, 2025 (4:25 AM ET)

… and our tool :-)

FIN

Thank you for listening.

Questions? Comments? Thoughts?