Unmasking APTs: Addressing Attribution Challenges in Evolving Attack Landscape

Aakanksha Saha, Jorge Blasco, Lorenzo Cavallaro, Martina Lindorfer

Researcher at TU Wien

Masters from University of Utah

Previously: Red Teamer @ MSFT

Passionate about ML and security

Enjoy Stargazing

Roadmap

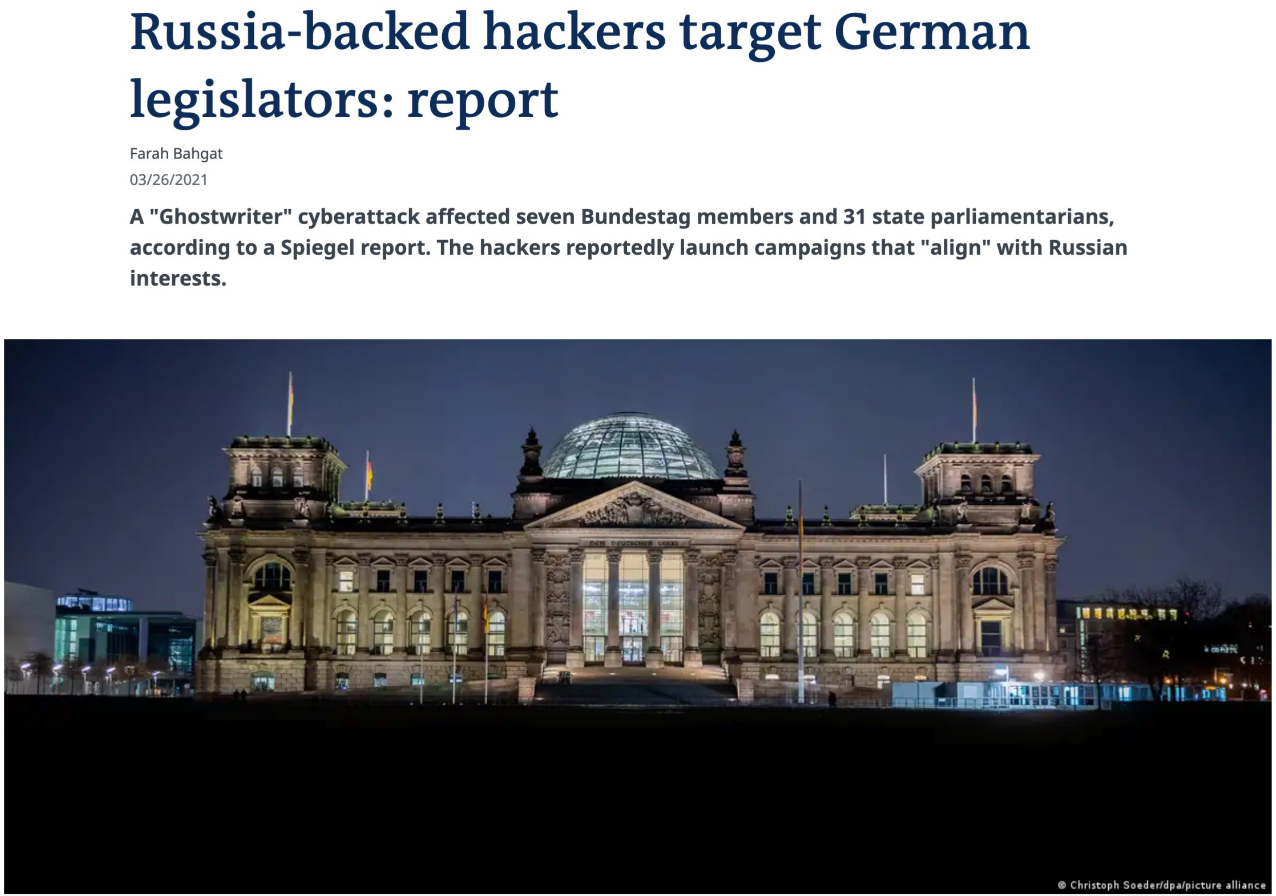
APT vs. Commodity

APT and its Attribution

Attribution challenges

ADAPT System

Next Steps



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.

© Christoph Soeder/dpa/picture alliance

DW Germany, 2021

Targeted vs. commodity malware

- Specific vs. Indiscriminate targeting
- Tailored tactics vs. Generic tactics
- Specific objective vs. Maximize potential profits

APTs are typically **well-funded, experienced teams of cybercriminals** that **target high-value organizations for specific objective** of data theft or espionage

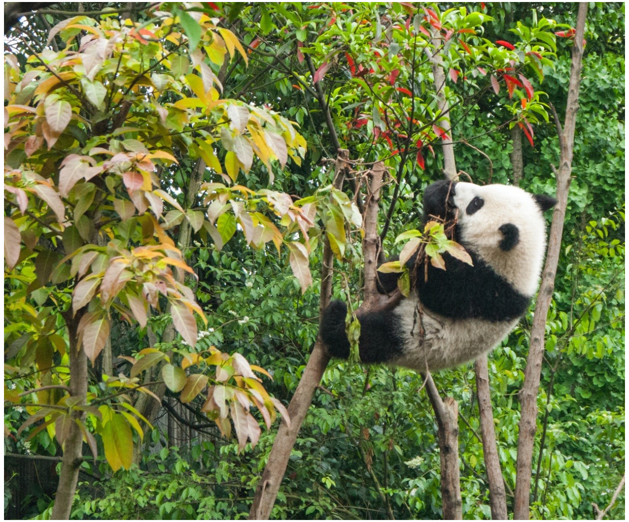
Hardy et al. Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware, Usenix, 2014

What is (AP)threat attribution?

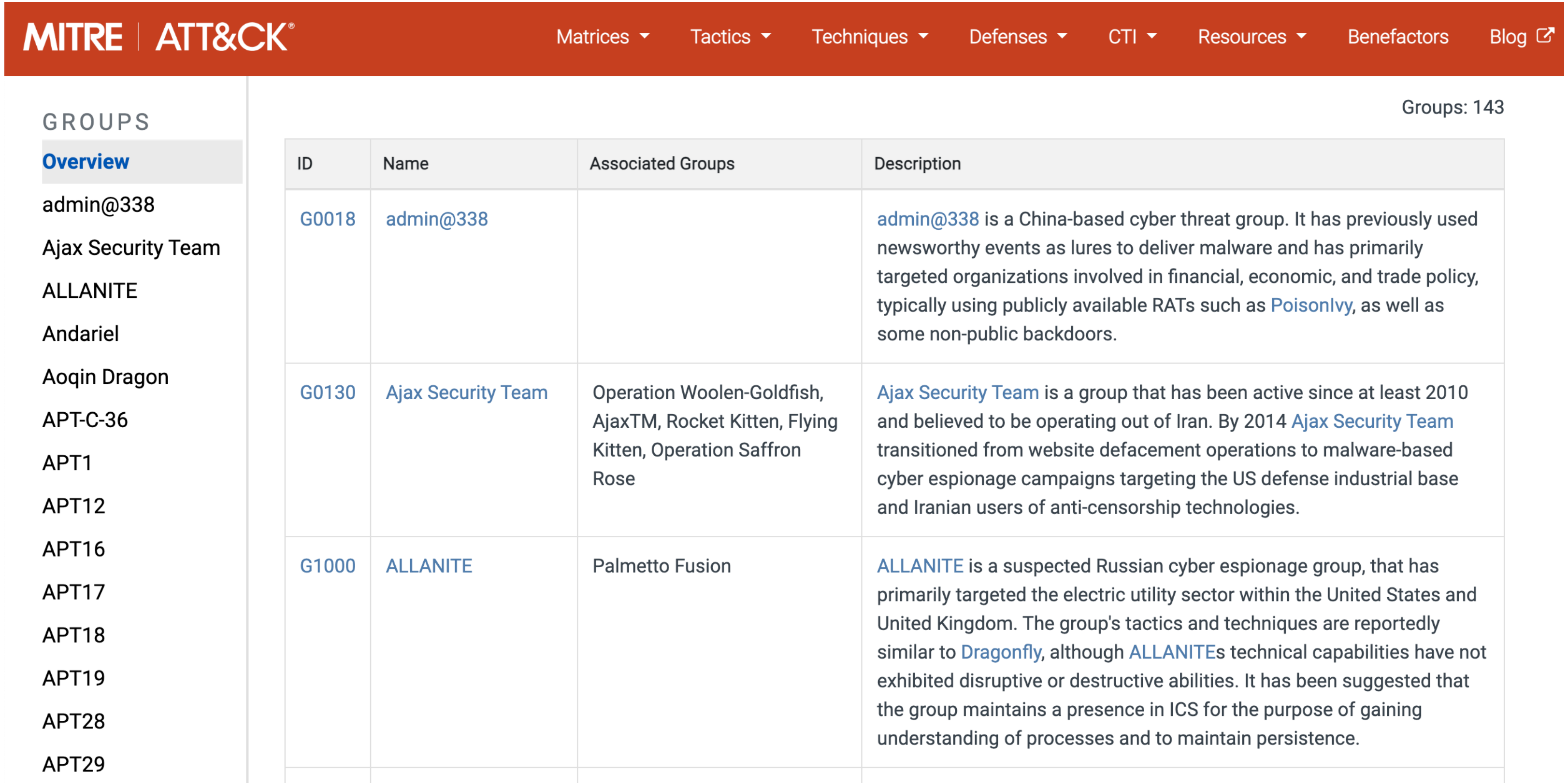
Associate a cyber-attack to an attacker

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).



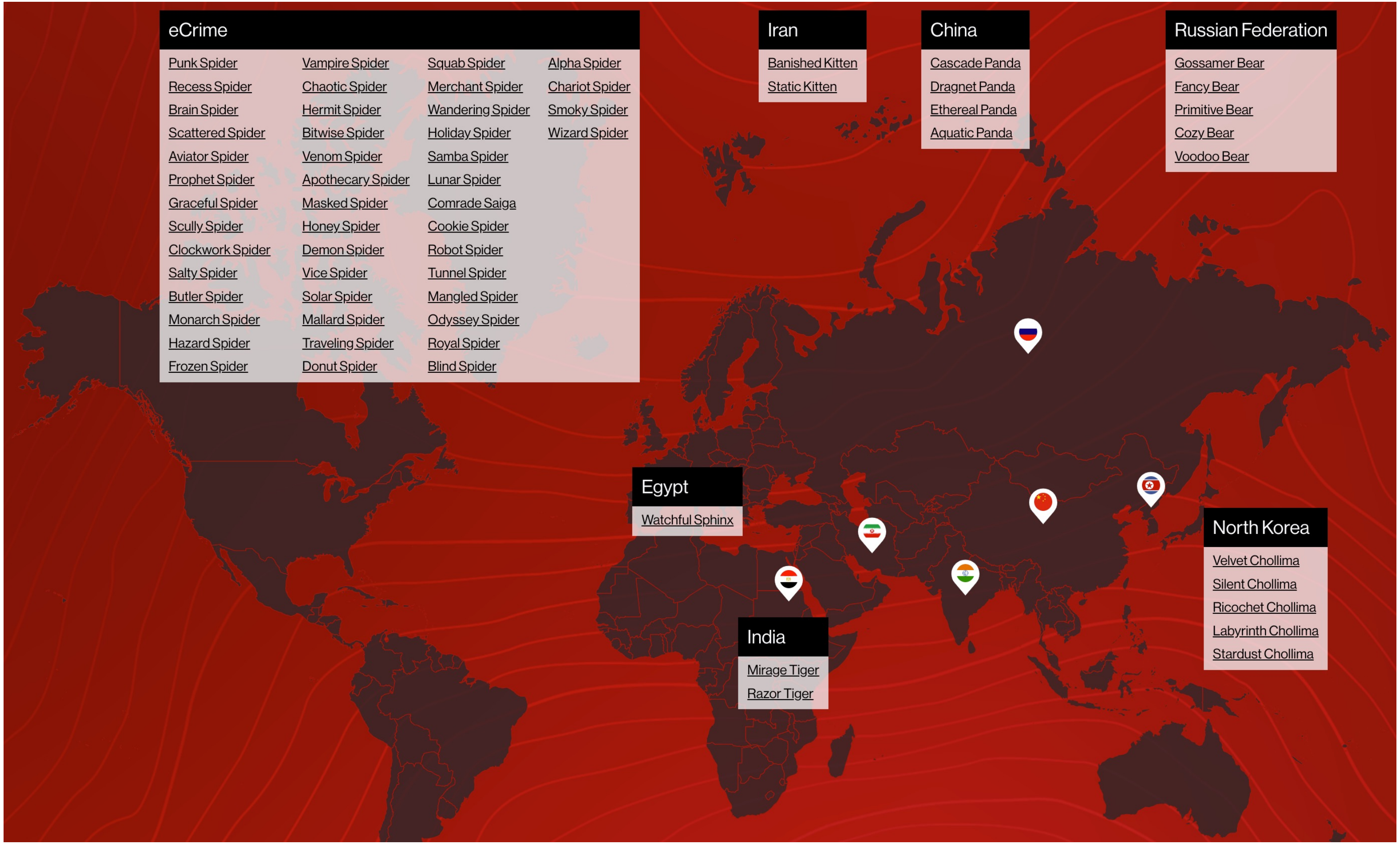
So far..?



Groups: 143

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.
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.
G1000	ALLANITE	Palmetto Fusion	ALLANITE is a suspected Russian cyber espionage group, that has primarily targeted the electric utility sector within the United States and United Kingdom. The group's tactics and techniques are reportedly similar to Dragonfly, although ALLANITEs technical capabilities have not exhibited disruptive or destructive abilities. It has been suggested that the group maintains a presence in ICS for the purpose of gaining understanding of processes and to maintain persistence.

MITRE Groups



eCrime

- Punk Spider
- Recess Spider
- Brain Spider
- Scattered Spider
- Aviator Spider
- Prophet Spider
- Graceful Spider
- Scully Spider
- Clockwork Spider
- Salty Spider
- Butler Spider
- Monarch Spider
- Hazard Spider
- Frozen Spider
- Vampire Spider
- Chaotic Spider
- Hermit Spider
- Bitwise Spider
- Venom Spider
- Apothecary Spider
- Masked Spider
- Honey Spider
- Demon Spider
- Vice Spider
- Solar Spider
- Mallard Spider
- Traveling Spider
- Donut Spider
- Squab Spider
- Merchant Spider
- Wandering Spider
- Holiday Spider
- Samba Spider
- Lunar Spider
- Comrade Saiga
- Cookie Spider
- Robot Spider
- Tunnel Spider
- Mangled Spider
- Odyssey Spider
- Royal Spider
- Blind Spider
- Alpha Spider
- Chariot Spider
- Smoky Spider
- Wizard Spider

Iran

- Banished Kitten
- Static Kitten

China

- Cascade Panda
- Dragnet Panda
- Ethereal Panda
- Aquatic Panda

Russian Federation

- Gossamer Bear
- Fancy Bear
- Primitive Bear
- Cozy Bear
- Voodoo Bear

Egypt

- Watchful Sphinx

India

- Mirage Tiger
- Razor Tiger

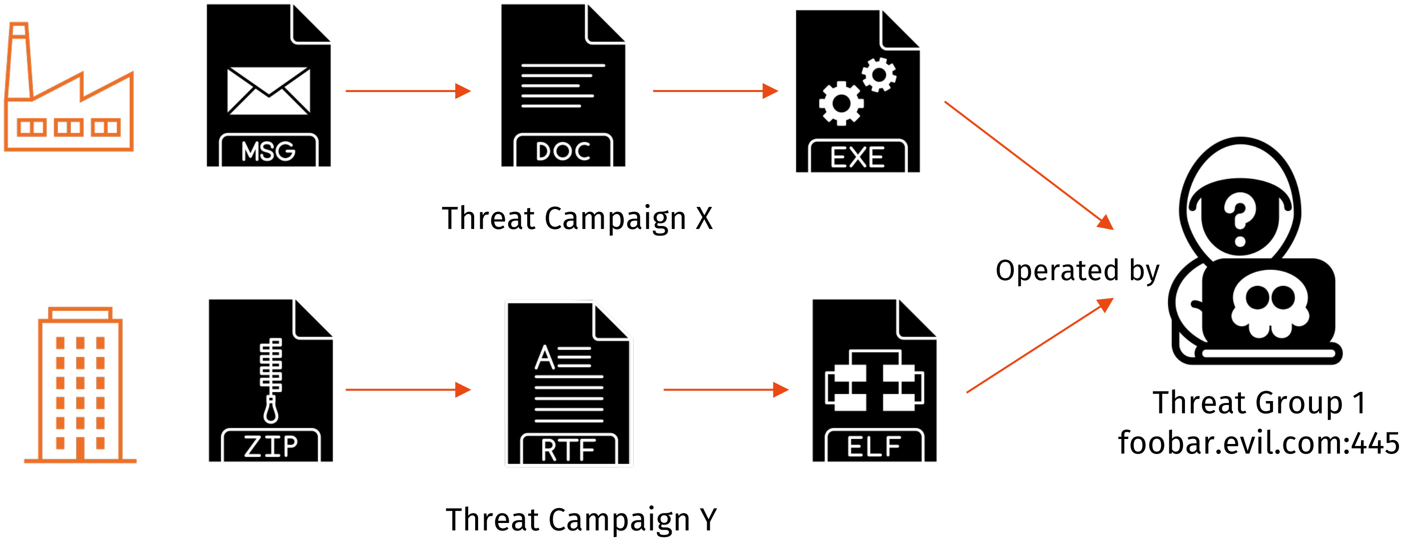
North Korea

- Velvet Chollima
- Silent Chollima
- Ricochet Chollima
- Labyrinth Chollima
- Stardust Chollima

CrowdStrike Adversaries

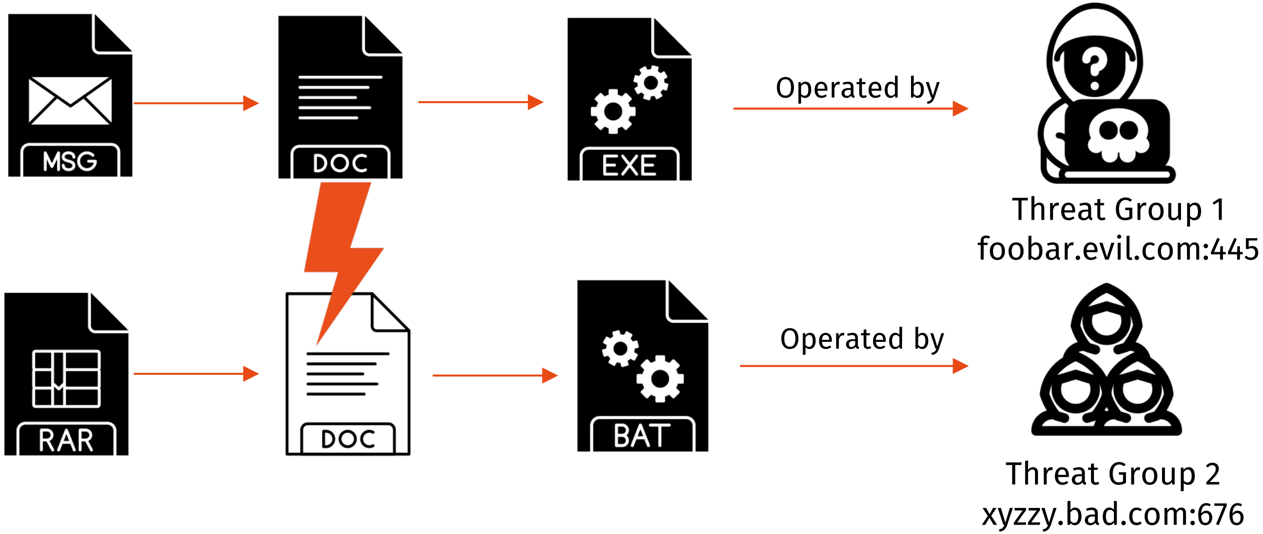
Attribution is challenging!

Campaign variation



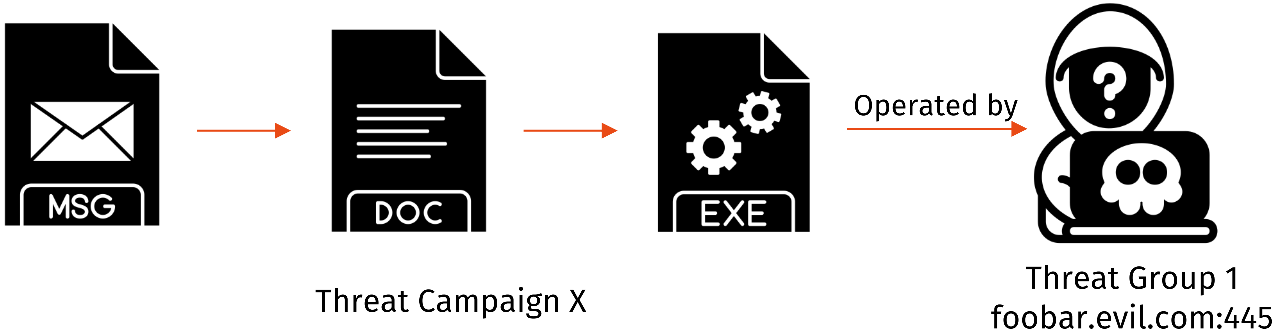
- Incomplete understanding of adversary with vendors tracking groups from varied campaign perspectives [AT&T AlienLabs, 2021]

Shared similarity



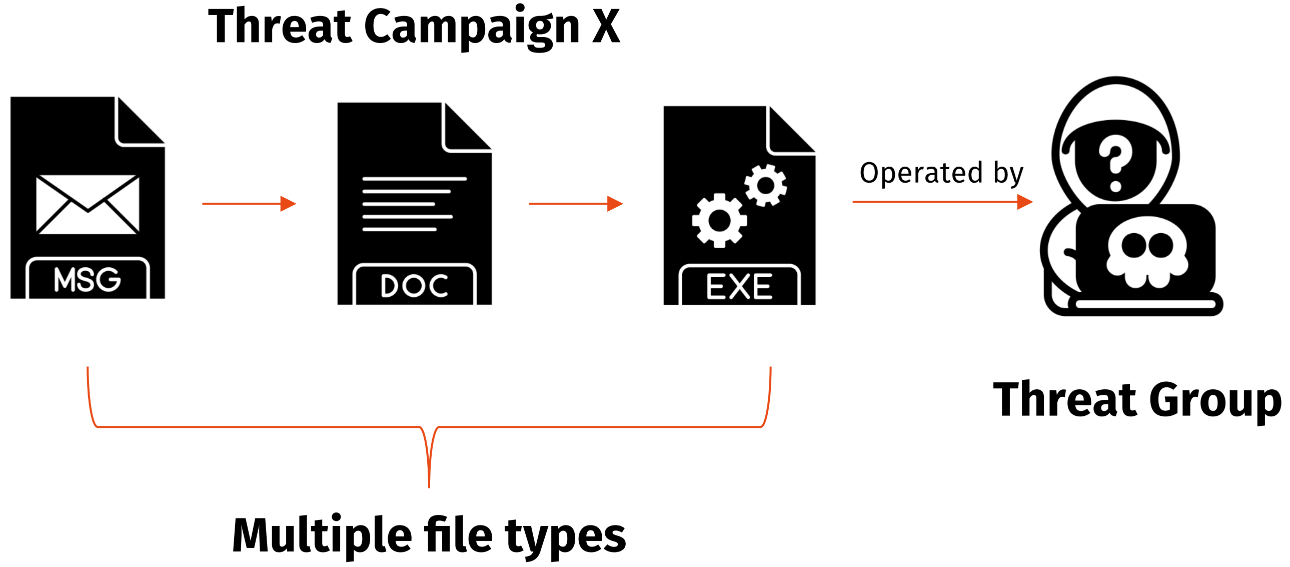
- Adoption of shared similarities, false flags and collaboration between subgroups results in inconsistent and erroneous attribution [Mandiant, 2023]

Heterogeneous files in attack chain

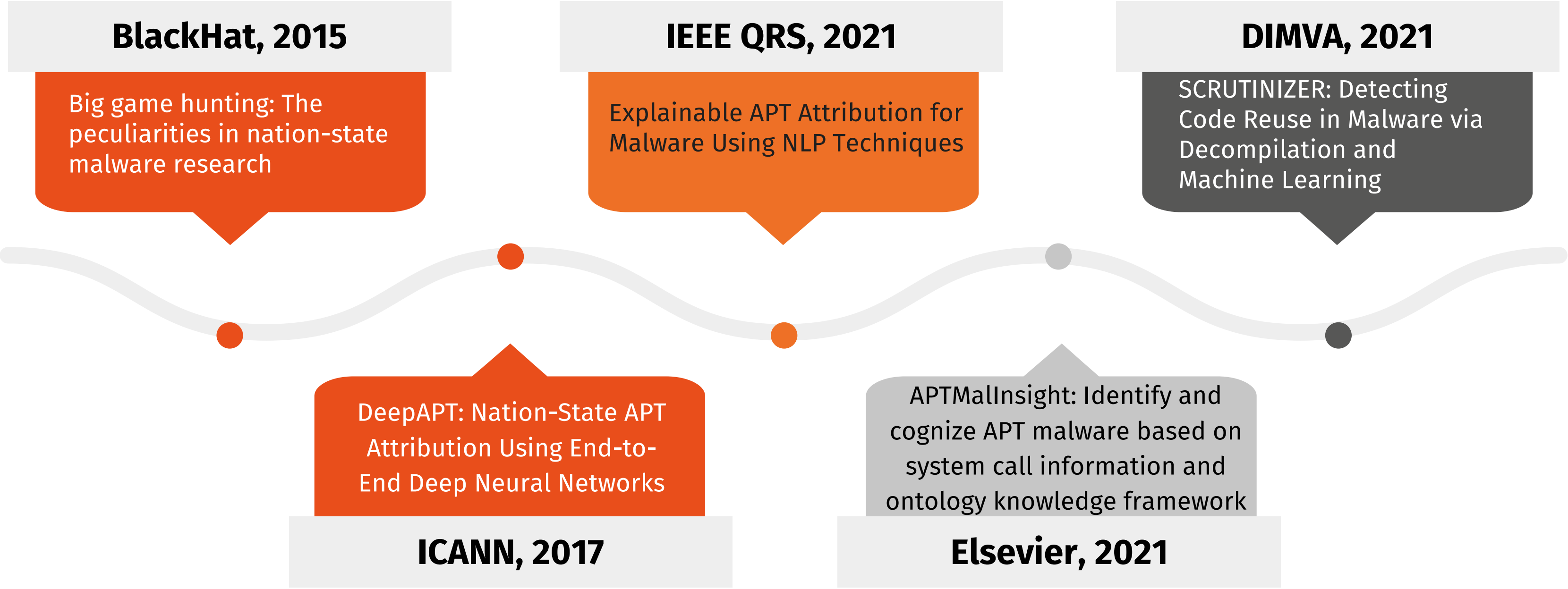


- Manual analysis of heterogenous files to identify the threat group [Mandiant, 2022]

Putting it all together



Malware based attribution research



BlackHat, 2015

Big game hunting: The peculiarities in nation-state malware research

ICANN, 2017

DeepAPT: Nation-State APT Attribution Using End-to-End Deep Neural Networks

IEEE QRS, 2021

Explainable APT Attribution for Malware Using NLP Techniques

Elsevier, 2021

APTMalInsight: Identify and cognize APT malware based on system call information and ontology knowledge framework

DIMVA, 2021

SCRUTINIZER: Detecting Code Reuse in Malware via Decompilation and Machine Learning

Approach ADAPT
Attribution of Diverse APT Samples

Campaign Attribution

Identify characteristics of attack

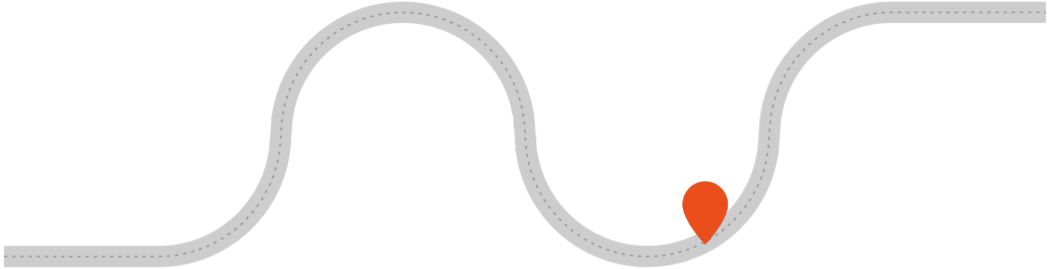
+ Prioritization of detection and mitigation

Group Attribution

Identify characteristics of attacker

+ Aid forensic investigation and indictments

ADAPT Data Collection

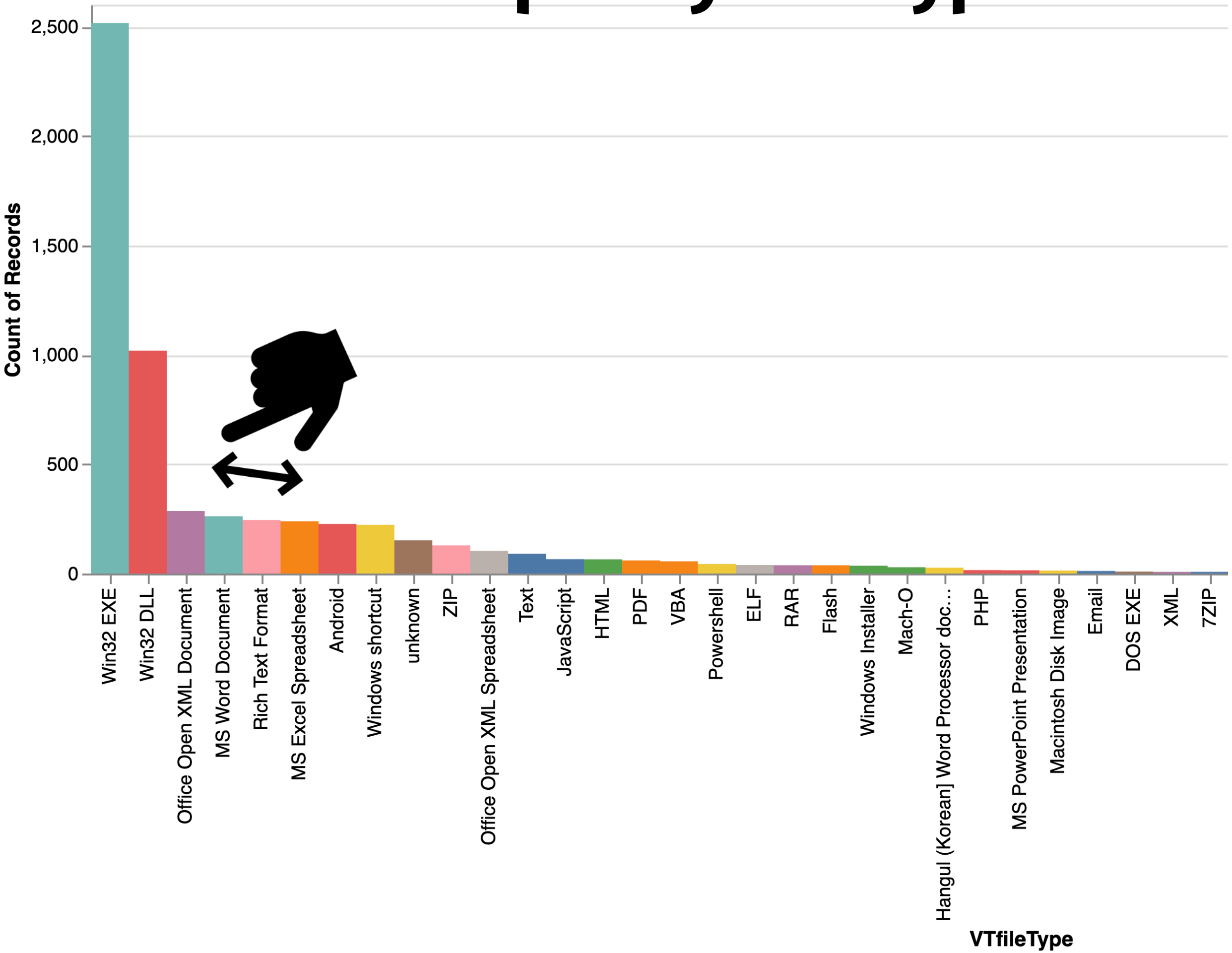


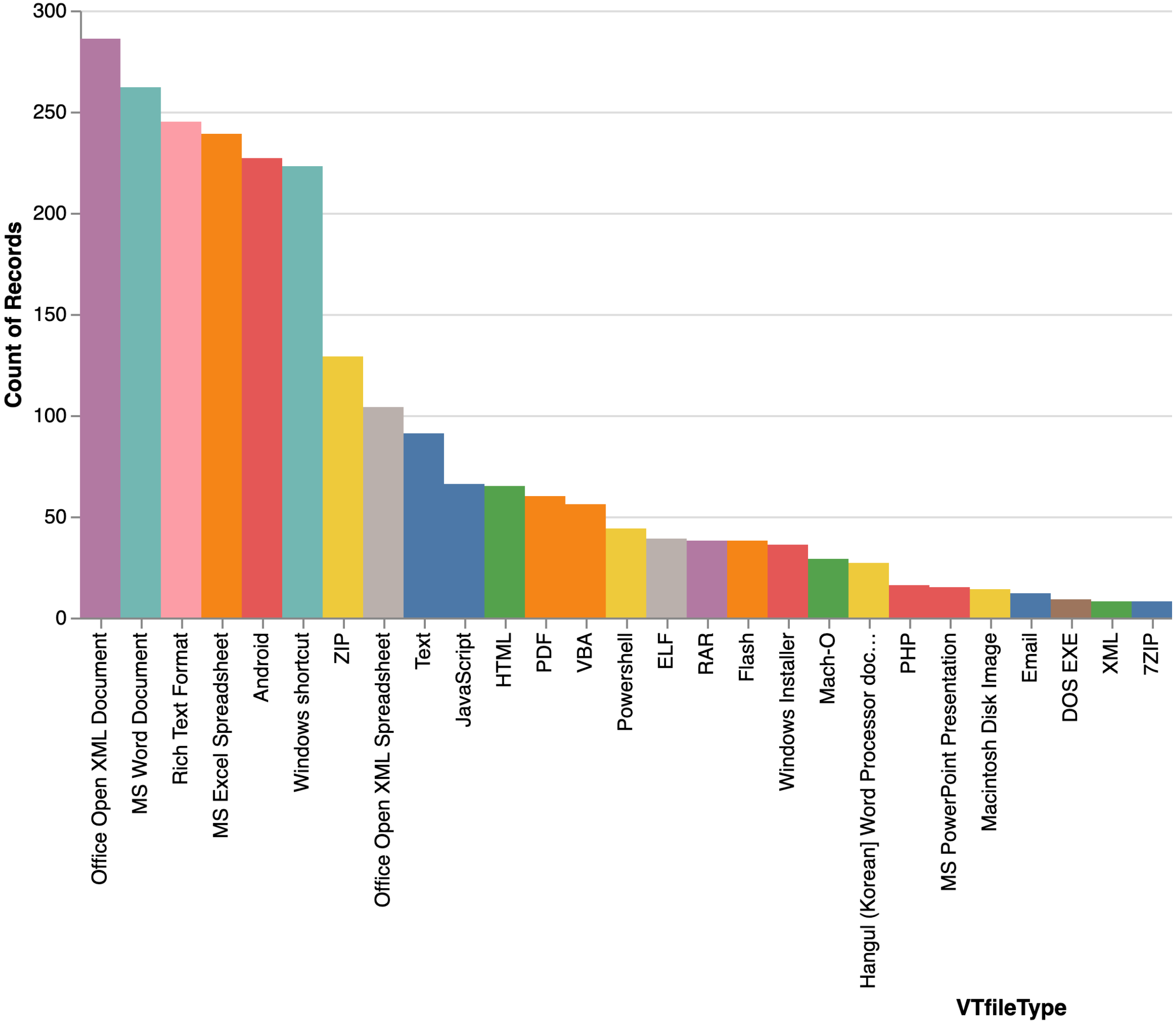
APT dataset

VIRUSTOTAL

- 6,455 samples (SHA256)
- 22+ file types
- 172 APT groups

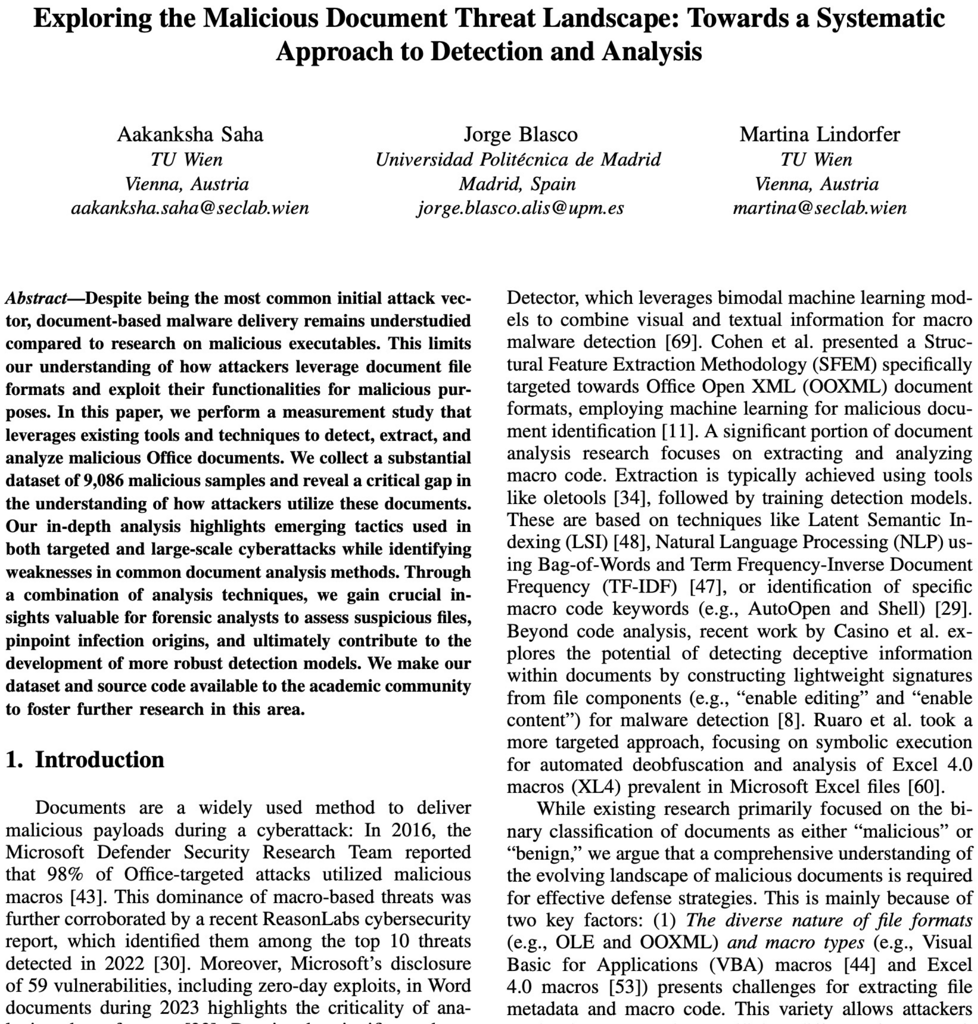
Dataset quality: Filetype





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

WORMA, Euro S&P Workshop, 2024



Exploring the Malicious Document Threat Landscape: Towards a Systematic Approach to Detection and Analysis

Aakanksha Saha
TU Wien
Vienna, Austria
aakanksha.saha@seclab.wien

Jorge Blasco
Universidad Politécnica de Madrid
Madrid, Spain
jorge.blasco.alis@upm.es

Martina Lindorfer
TU Wien
Vienna, Austria
martina@seclab.wien

***Abstract*—Despite being the most common initial attack vector, document-based malware delivery remains understudied compared to research on malicious executables. This limits our understanding of how attackers leverage document file formats and exploit their functionalities for malicious purposes. In this paper, we perform a measurement study that leverages existing tools and techniques to detect, extract, and analyze malicious Office documents. We collect a substantial dataset of 9,086 malicious samples and reveal a critical gap in the understanding of how attackers utilize these documents. Our in-depth analysis highlights emerging tactics used in both targeted and large-scale cyberattacks while identifying weaknesses in common document analysis methods. Through a combination of analysis techniques, we gain crucial insights valuable for forensic analysts to assess suspicious files, pinpoint infection origins, and ultimately contribute to the development of more robust detection models. We make our dataset and source code available to the academic community to foster further research in this area.**

1. Introduction

Documents are a widely used method to deliver malicious payloads during a cyberattack: In 2016, the Microsoft Defender Security Research Team reported that 98% of Office-targeted attacks utilized malicious macros [43]. This dominance of macro-based threats was further corroborated by a recent ReasonLabs cybersecurity report, which identified them among the top 10 threats detected in 2022 [30]. Moreover, Microsoft's disclosure of 59 vulnerabilities, including zero-day exploits, in Word documents during 2023 highlights the criticality of ana-

Detector, which leverages bimodal machine learning models to combine visual and textual information for macro malware detection [69]. Cohen et al. presented a Structural Feature Extraction Methodology (SFEM) specifically targeted towards Office Open XML (OOXML) document formats, employing machine learning for malicious document identification [11]. A significant portion of document analysis research focuses on extracting and analyzing macro code. Extraction is typically achieved using tools like oletools [34], followed by training detection models. These are based on techniques like Latent Semantic Indexing (LSI) [48], Natural Language Processing (NLP) using Bag-of-Words and Term Frequency-Inverse Document Frequency (TF-IDF) [47], or identification of specific macro code keywords (e.g., AutoOpen and Shell) [29]. Beyond code analysis, recent work by Casino et al. explores the potential of detecting deceptive information within documents by constructing lightweight signatures from file components (e.g., "enable editing" and "enable content") for malware detection [8]. Ruaro et al. took a more targeted approach, focusing on symbolic execution for automated deobfuscation and analysis of Excel 4.0 macros (XL4) prevalent in Microsoft Excel files [60].

While existing research primarily focused on the binary classification of documents as either "malicious" or "benign," we argue that a comprehensive understanding of the evolving landscape of malicious documents is required for effective defense strategies. This is mainly because of two key factors: (1) *The diverse nature of file formats* (e.g., OLE and OOXML) *and macro types* (e.g., Visual Basic for Applications (VBA) macros [44] and Excel 4.0 macros [53]) presents challenges for extracting file metadata and macro code. This variety allows attackers

Dataset quality: Group label

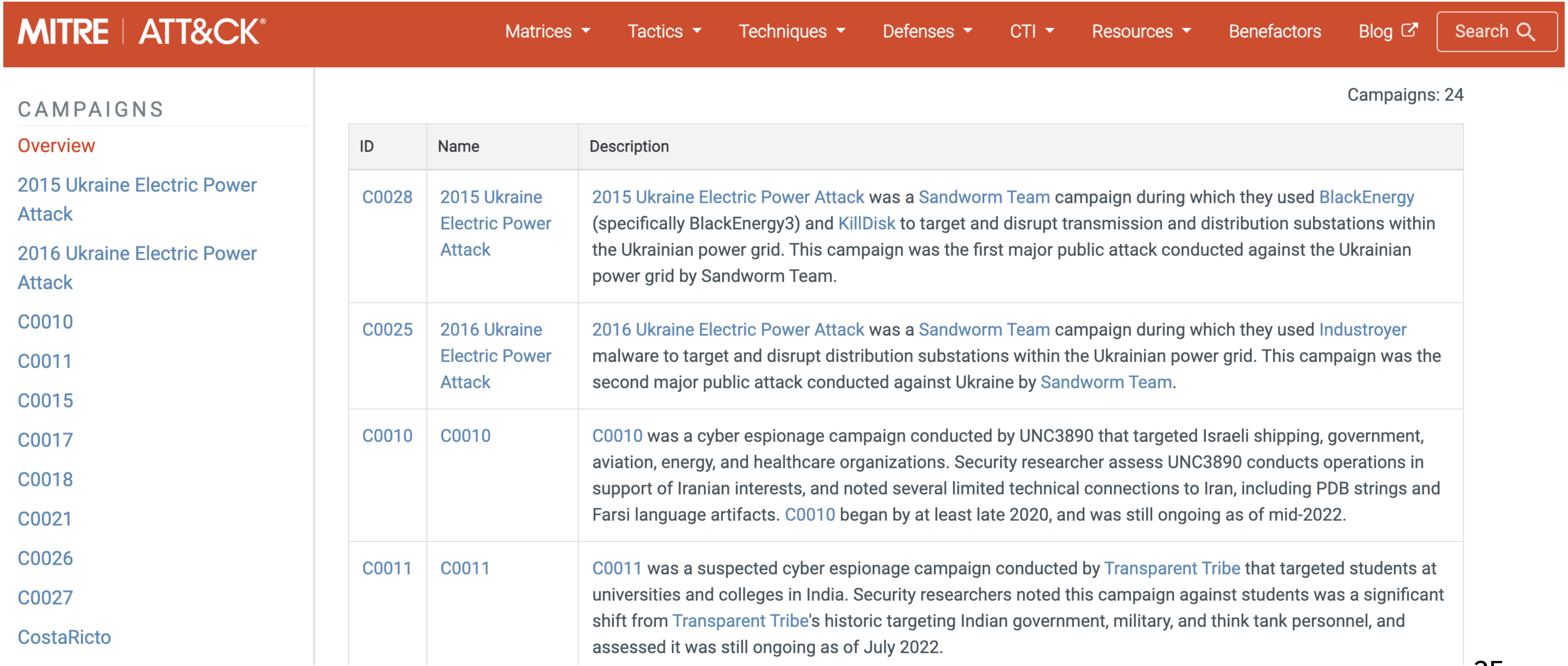
2,260 (35.01%) have more than 1 label

Threat Group Label	Number of Aliases	Number of Sample
Lazarus	29	527
Gamaredon	11	446
Transparent Tribe	9	403
APT41	16	278
Turla	21	203
APT28	23	169
APT29	15	224

Dataset (re)-labeling

- Malpedia Threat Actor Inventory and MITRE to resolve conflicts
- Standardize aliases
- Consistent naming convention
- Non-unique names and non-APT samples

Campaign Labeled Dataset



CAMPAIGNS

Overview

2015 Ukraine Electric Power Attack

2016 Ukraine Electric Power Attack

C0010

C0011

C0015

C0017

C0018

C0021

C0026

C0027

CostaRicto

Campaigns: 24

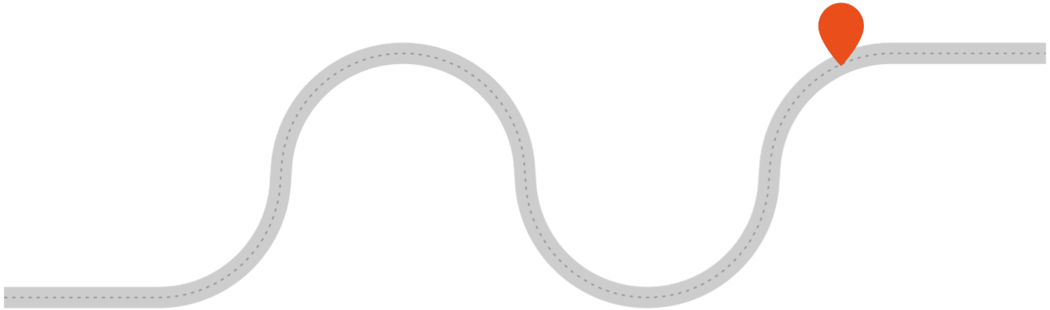
ID	Name	Description
C0028	2015 Ukraine Electric Power Attack	2015 Ukraine Electric Power Attack was a Sandworm Team campaign during which they used BlackEnergy (specifically BlackEnergy3) and KillDisk to target and disrupt transmission and distribution substations within the Ukrainian power grid. This campaign was the first major public attack conducted against the Ukrainian power grid by Sandworm Team.
C0025	2016 Ukraine Electric Power Attack	2016 Ukraine Electric Power Attack was a Sandworm Team campaign during which they used Industroyer malware to target and disrupt distribution substations within the Ukrainian power grid. This campaign was the second major public attack conducted against Ukraine by Sandworm Team.
C0010	C0010	C0010 was a cyber espionage campaign conducted by UNC3890 that targeted Israeli shipping, government, aviation, energy, and healthcare organizations. Security researcher assess UNC3890 conducts operations in support of Iranian interests, and noted several limited technical connections to Iran, including PDB strings and Farsi language artifacts. C0010 began by at least late 2020, and was still ongoing as of mid-2022.
C0011	C0011	C0011 was a suspected cyber espionage campaign conducted by Transparent Tribe that targeted students at universities and colleges in India. Security researchers noted this campaign against students was a significant shift from Transparent Tribe's historic targeting Indian government, military, and think tank personnel, and assessed it was still ongoing as of July 2022.

To help the community…

- 6,134 samples assigned to 92 groups
- 230 samples, 17 APT groups, 22 APT campaigns

** The standardized group-labeled dataset is available at https://anonymous.4open.science/r/ACM-7FC0/*

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.

📊 Conducted 15 (+3) interviews with participants from diverse industries, expertise, and locations.

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

CYSEC
CYBERSECURITYCENTER

UNIVERSIDAD POLITÉCNICA DE MADRID

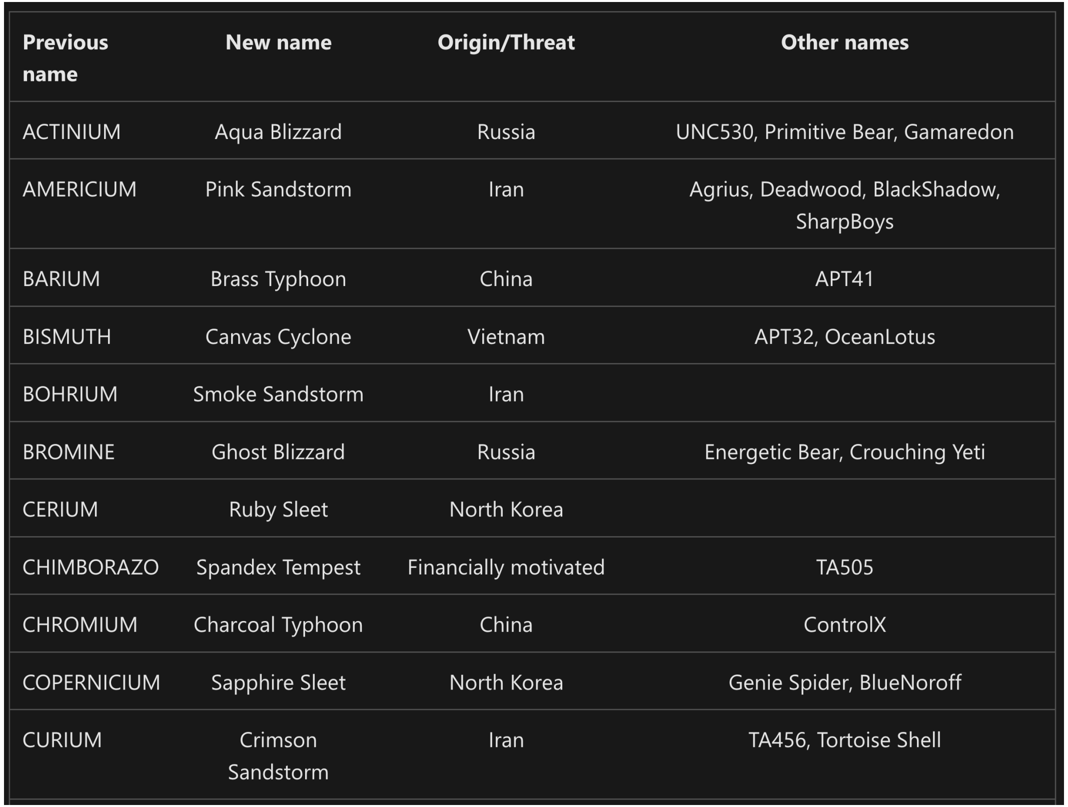
UCL

References

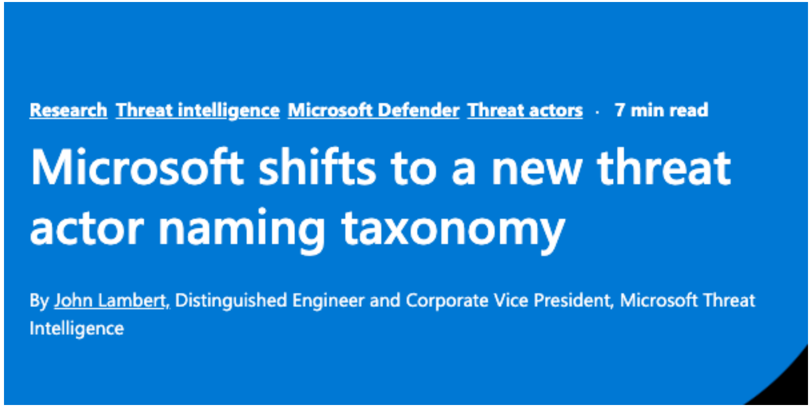
[1] https://securityaffairs.com/116001/apt/german-parliament-bundestag-russia-hackers.html
[2] https://www.mandiant.com/resources/blog/unc2452-merged-into-apt29
[3] https://www.mandiant.com/resources/blog/north-korea-cyber-structure-alignment-2023
[4] https://cybersecurity.att.com/blogs/labs-research/a-global-perspective-of-the-sidewinder-apt
[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/

Dataset quality: Group label

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



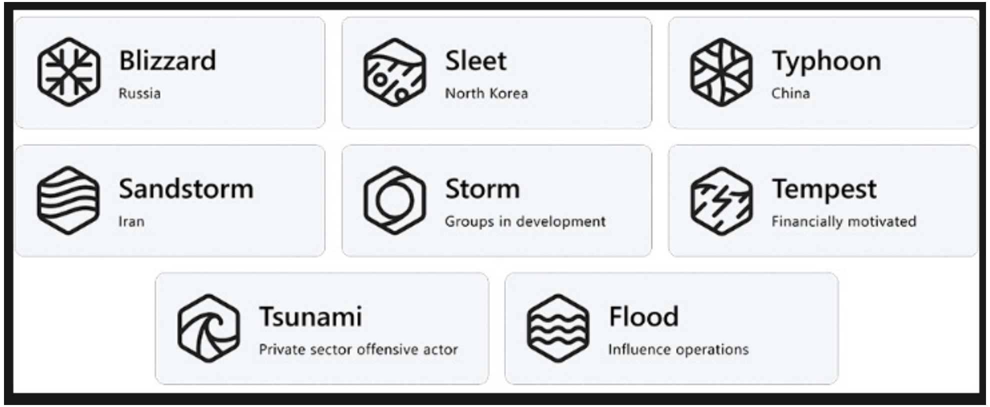
Previous name	New name	Origin/Threat	Other names
ACTINIUM	Aqua Blizzard	Russia	UNC530, Primitive Bear, Gamaredon
AMERICIUM	Pink Sandstorm	Iran	Agrius, Deadwood, BlackShadow, SharpBoys
BARIUM	Brass Typhoon	China	APT41
BISMUTH	Canvas Cyclone	Vietnam	APT32, OceanLotus
BOHRIUM	Smoke Sandstorm	Iran	
BROMINE	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



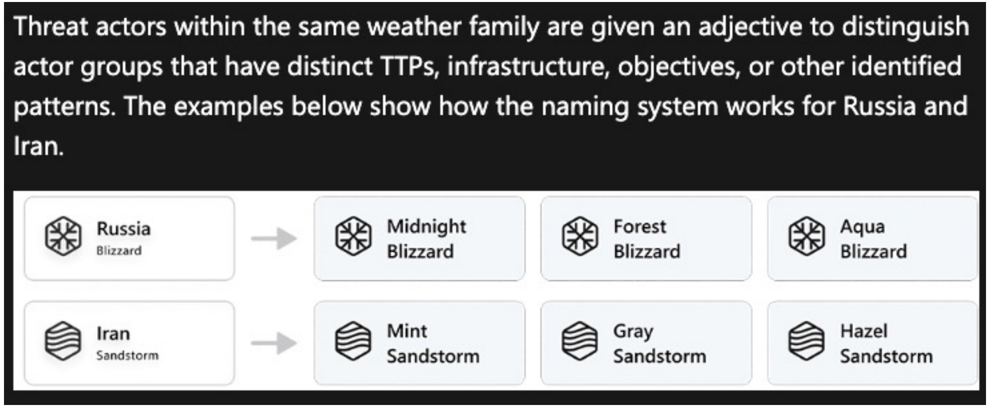
Research Threat intelligence Microsoft Defender Threat actors · 7 min read

Microsoft shifts to a new threat actor naming taxonomy

By John Lambert, Distinguished Engineer and Corporate Vice President, Microsoft Threat Intelligence



Blizzard	Russia
Sleet	North Korea
Typhoon	China
Sandstorm	Iran
Storm	Groups in development
Tempest	Financially motivated
Tsunami	Private sector offensive actor
Flood	Influence operations



Threat actors within the same weather family are given an adjective to distinguish actor groups that have distinct TTPs, infrastructure, objectives, or other identified patterns. The examples below show how the naming system works for Russia and Iran.

Russia Blizzard	→	Midnight Blizzard	Forest Blizzard	Aqua Blizzard
Iran Sandstorm	→	Mint Sandstorm	Gray Sandstorm	Hazel Sandstorm