The Attribution Story of WhisperGate. An Academic Perspective

Dr. Oleksandr Adamov

Dr. Anders Carlsson

BLEKINGE INSTITUTE OF TECHNOLOGY

vb 2025 BERLIN 24-26 Sept 2025

About us

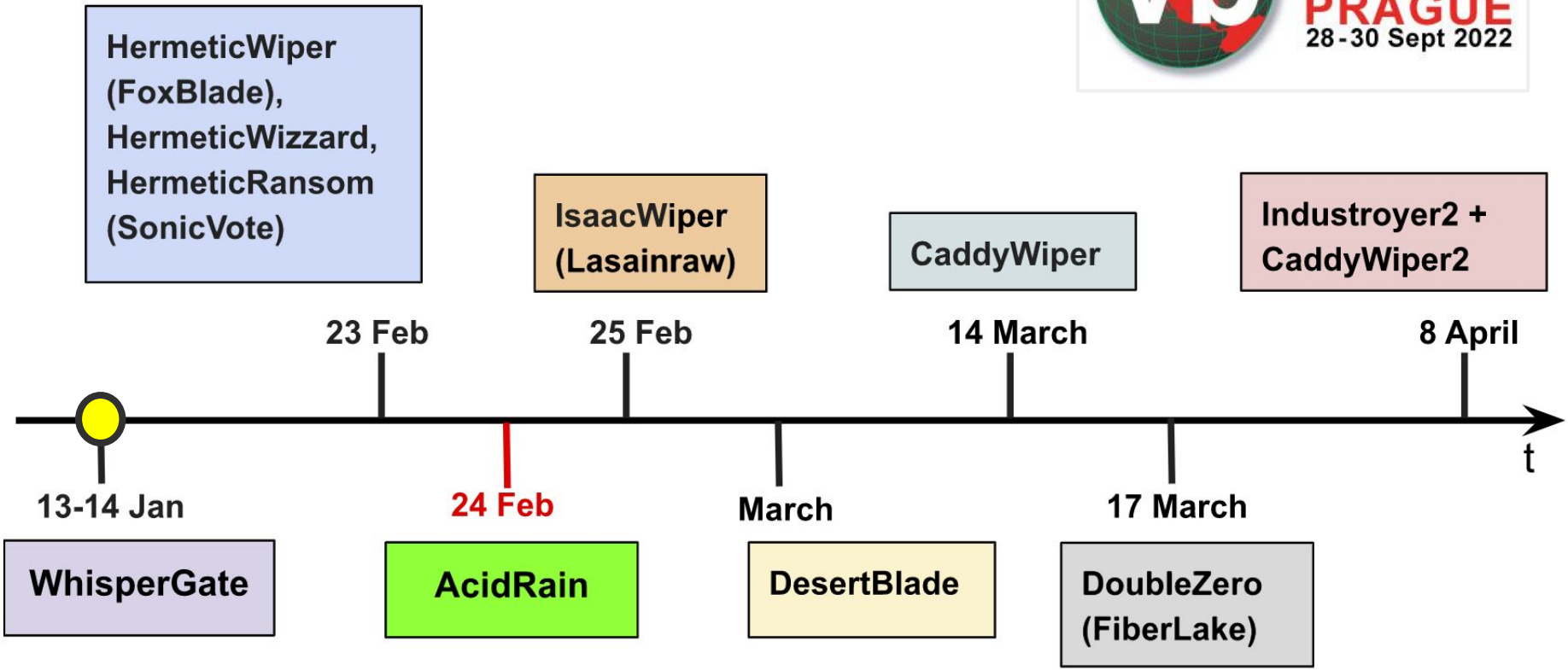
Dr. Alexander (Oleksandr) Adamov
Assoc. Professor at BTH (Sweden) and NURE (Ukraine) universities
Founder and CEO *at Nioguard Security Lab*
ada@nioguard.com
@Alex_Ad

Dr. Anders Carlsson
Senior lector at BTH (Sweden) and NURE *Kharkiv (Ukraine) universities*
Founder and CEO at Promestra Security

BLEKINGE INSTITUTE OF TECHNOLOGY

In previous episodes…

Wiper attacks in 2022



NioGuard Security Lab © 2022

WhisperGate - 2022

Date: 13-14 Jan 2022
Targets: Government infrastructure
Discovered by: CERT-UA, Microsoft
Attribution: DEV-0586 (GRU)
Platform: Windows 64/32-bit
Delivery:

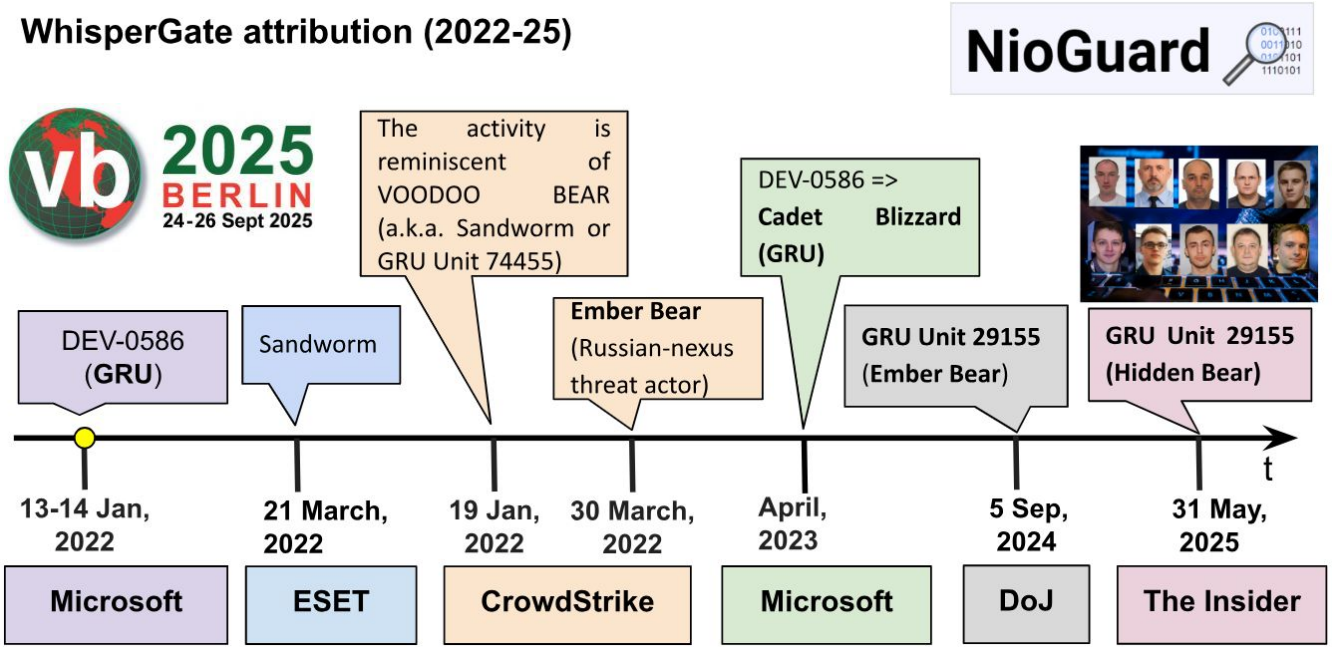
- Stage1.exe: MBR writer -> Disk wiper
- Stage2.exe: Trojan-Downloader -> Discord -> File wiper

Destruction:

- Wiping every 199th sector
- Filling files with ‘0x100000’ of ‘0xCC’ byte

NioGuard Security Lab © 2022

Storyline


WhisperGate attribution (2022-25)
NioGuard
vb 2025 BERLIN 24-26 Sept 2025
The activity is reminiscent of VOODOO BEAR (a.k.a. Sandworm or GRU Unit 74455)
DEV-0586 => Cadet Blizzard (GRU)
DEV-0586 (GRU)
Sandworm
Ember Bear (Russian-nexus threat actor)
GRU Unit 29155 (Ember Bear)
GRU Unit 29155 (Hidden Bear)
t
13-14 Jan, 2022
21 March, 2022
19 Jan, 2022
30 March, 2022
April, 2023
5 Sep, 2024
31 May, 2025
Microsoft
ESET
CrowdStrike
Microsoft
DoJ
The Insider

Who is Ember Bear?
// subgroup to GRU Unit 29155 //

BLEKINGE INSTITUTE OF TECHNOLOGY

New grouping within GRU Unit 29155 since 2021

AKA Saint Bear, *Lorec53*, *Bleeding Bear*, *UAC-0056* ,Cadet Blizzard *UNC2589*

GRU Unit 29155 mostly known as an unit specilicing on:assassination, elite sabotage disinformation operations, sow mistrust, degrade institutions. example WADA.
Major involvement in conflicts Georgia, Crimea (2014), Moldova, coup in Montenegro (2016)
Part of destabilization operations in Spain during the Catalonia independence referendum (2017) and the
assassination attempt on former Russian spy Sergei Skripal in Salisbury, UK (2018).

2021 was Ember Bear a new part of this **elite sabotage unit**
before they had no or very limited IT-skills

T

Today, GRU recrute direct [Positive Hack Days, Moscow, 2024]

BLEKINGE INSTITUTE OF TECHNOLOGY

Attribution Methods

BLEKINGE INSTITUTE OF TECHNOLOGY

***Indicators of Compromise* (IoC)**
include file hashes, IP addresses, domain names, or malware signatures left behind

***Tactics, Techniques, and Procedures* (TTPs)**
– build environment, metadata, Weaponization

Malware evolution and code similarities
There is significant code reuse

Variable names/TAG's
–"speciale name" (tag) language or cultural hints

Mistakes or slip-ups by attackers.
Attackers sometimes make operational mistakes, exposing their identity. I

***Open Source Inteligence (OSINT*)**
Follow the stolen data

Target Objective
– sectors, countries, technologies
– espionage, disruption, influence

Geopolitical context. The timing, target, and nature of an attack may align with the interests of a nation-state, offering clues to its origin.

Language and cultural indicators, such as language markers, time zones, and cultural habits

Challenge of Attribution

BLEKINGE INSTITUTE OF TECHNOLOGY

Different security vendors often give the same APT group different names (e.g., Ember Bear, Lorec53, UNC2589, UAC-0056 are the same group).

Different names Security company as ESET, CrowedStrike, Kasperskey, name both the malware and the APT group differently.

Reuse of Code parts – reused snippets, libraries, unique routines sharing of tools, infrastructure, and techniques across different APT groups, sometimes even across nations.
they steal / borrow from other APT groups - can be confusing

False Flag include information to point out other APT-group

Because of these challenges, political decision-makers require very high confidence before publicly blaming a group or government.

Attribution is therefore both a technical and a political process — and it always comes with uncertainty."

Ember Bear: Human Analysis

BLEKINGE INSTITUTE OF TECHNOLOGY

WhisperGate operation on January 13, 2022 [*CISA Cybersecurity Advisory: Russian Military Cyber Actors Target US and Global Critical Infrastructure*]:

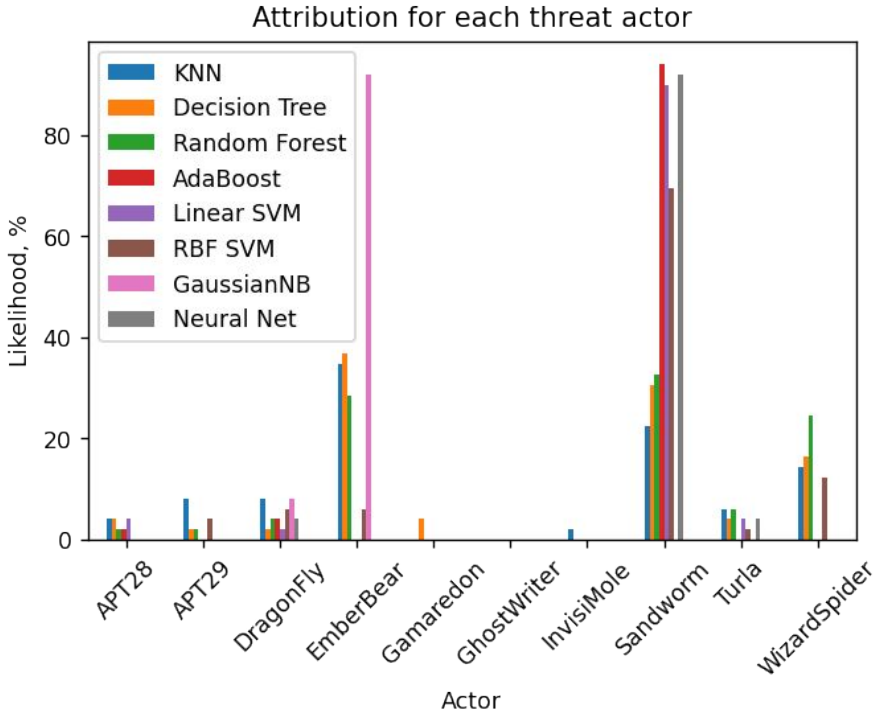
- Cluster 1:
  a. hxxps://cdn.discordapp[.]com/attachments/928503440139771947/9301086376811847 68/**Tbopbh.jpg** (a resource, e.g., payload, for stage2.exe)
  b. **saint.exe** (a downloader, **SaintBot**, as detailed by CERT-UA)
  c. Puttyjejfrwu.exe

Ember Bear's attack on the energy sector of Ukraine on Feb 1, 2022 [Palo Alto Networks, CERT-UA]:

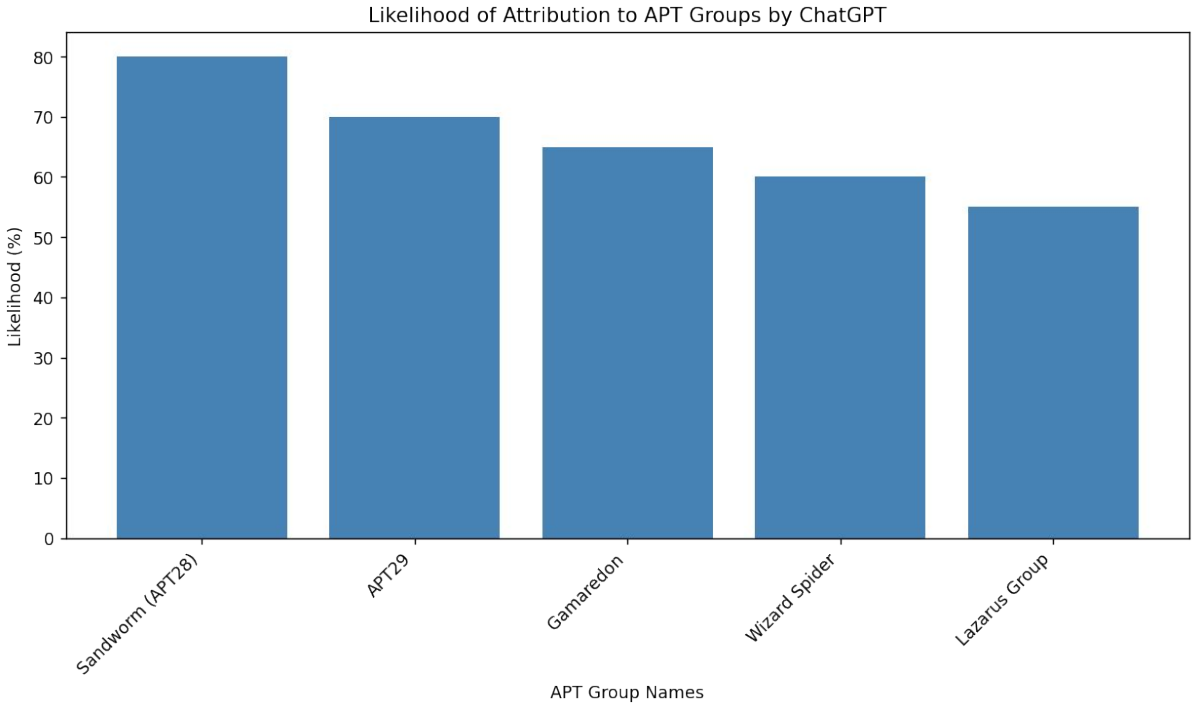
- cdn.discordapp[.]com/attachments/853604584806285335/854020189522755604/1406.exe
- cdn.discordapp[.]com/attachments/908281957039869965/908282786216017990/AdobeAcrobatUpdate.msi
- cdn.discordapp[.]com/attachments/908281957039869965/908310733488525382/AdobeAcrobatUpdate.exe
- cdn.discordapp[.]com/attachments/908281957039869965/911202801416282172/AdobeAcrobatReaderUpdate.exe
- cdn.discordapp[.]com/attachments/908281957039869965/911383724971683862/21279102.exe
- …

Attribution with Classic ML

BLEKINGE INSTITUTE OF TECHNOLOGY

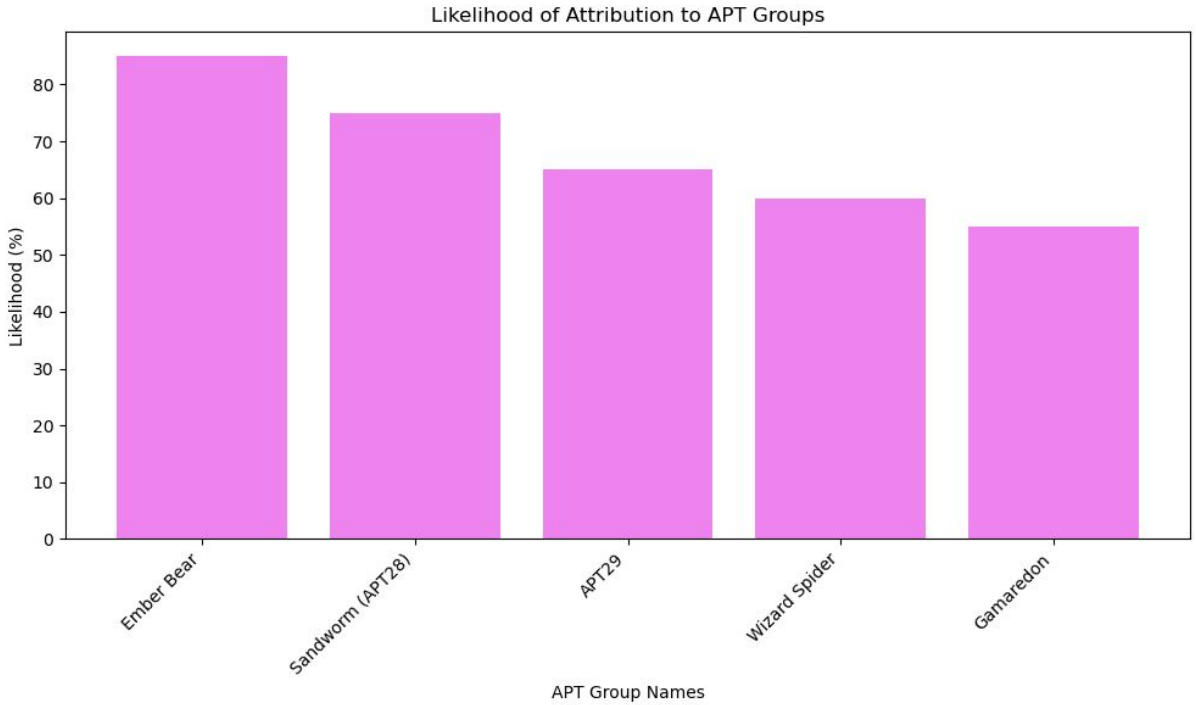


Attribution with ChatGPT: Zero-Shot

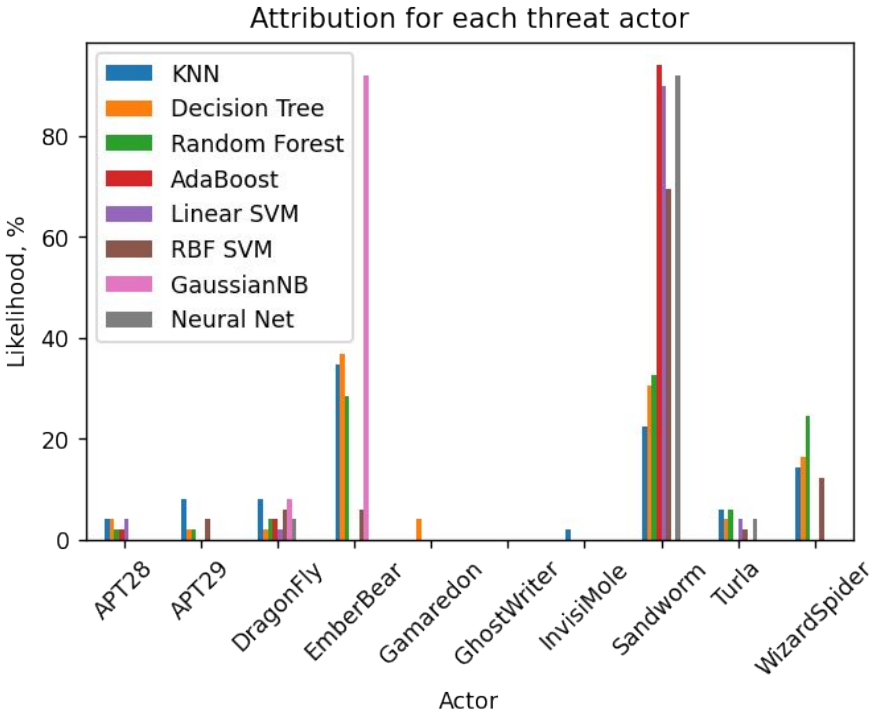


BLEKINGE INSTITUTE OF TECHNOLOGY

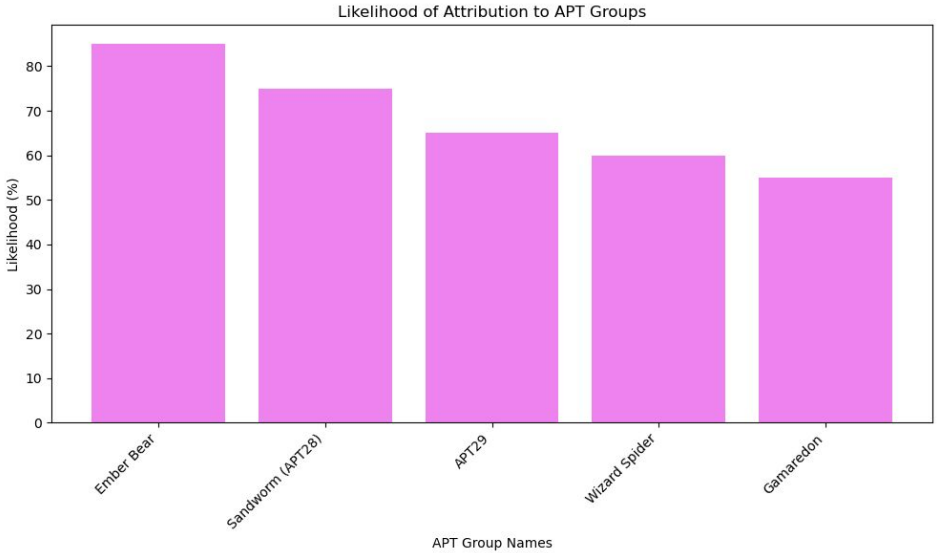
Attribution with ChatGPT: One-Shot



BLEKINGE INSTITUTE OF TECHNOLOGY



ChatGPT: One-shot results



Conclusion

BLEKINGE INSTITUTE OF TECHNOLOGY

1) The need for a **unified naming convention**
2) **GenAI** can help with:
   - ✓ new types of data and methods to be used for attribution (e.g., linguistic analysis of chat messages)
   - ✓ easier collection of indicators from heterogeneous data
   - ✓ higher accuracy of attribution

Next: (Gen)AI Agent for APT attribution (BlackHat Europe 2025)