He is everywhere

A tale of Lazarus and his family

2023-10-17, @lazarusholic

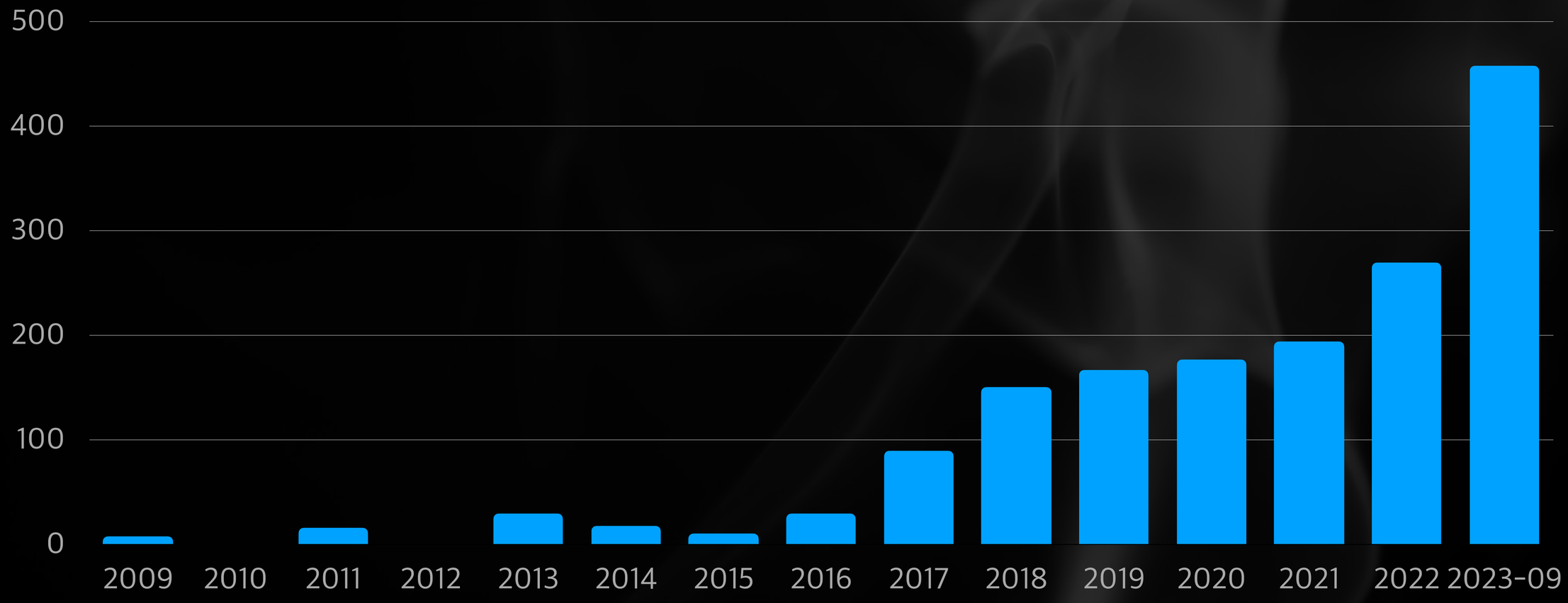
JeongGak Lyu, Financial Security Institute

금융보안원
FINANCIAL SECURITY INSTITUTE

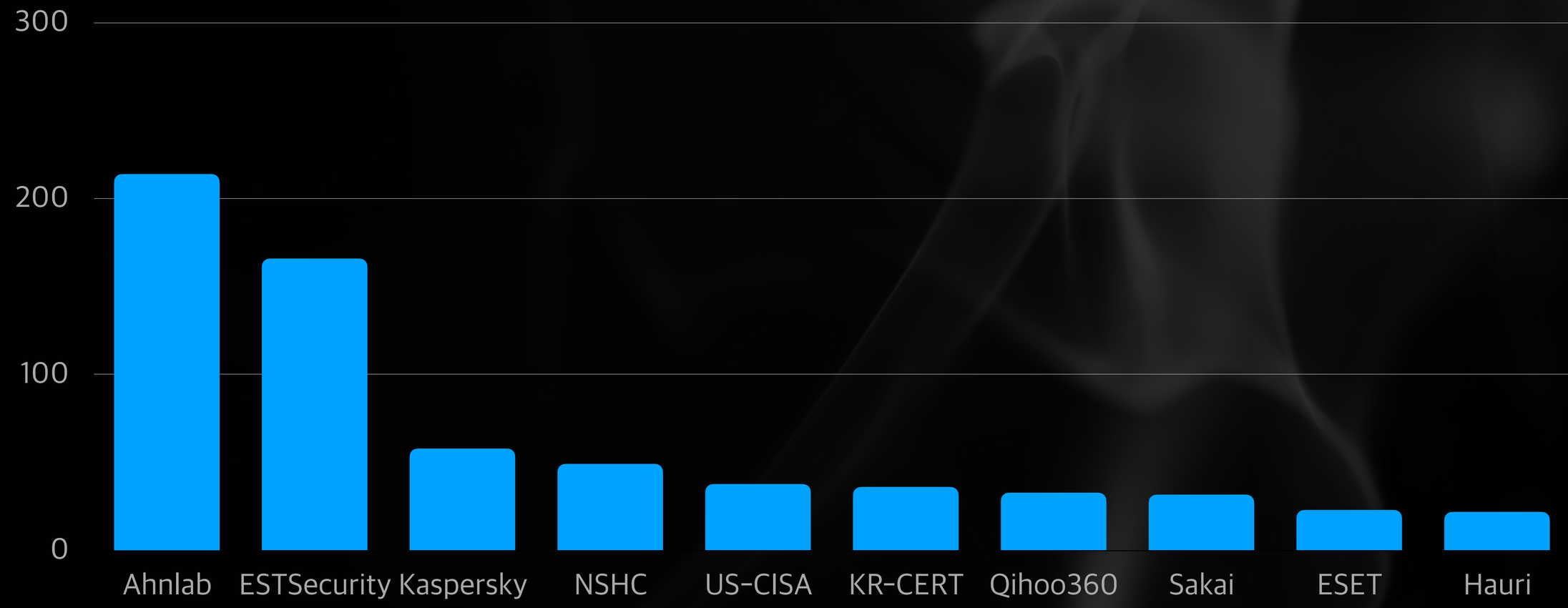
Who are Lazarus and his family?

- Behind Infamous Cyber Incidents
- Democratic People's Republic of Korea(DPRK, North Korea) stated-sponsored Threat Actors
- Most Wanted Threat Actors in the World

of posts by year



Top 10 authors



Lazarus by the numbers

Posts

1,638

Authors

329

Aliases
(Associated Groups)

143

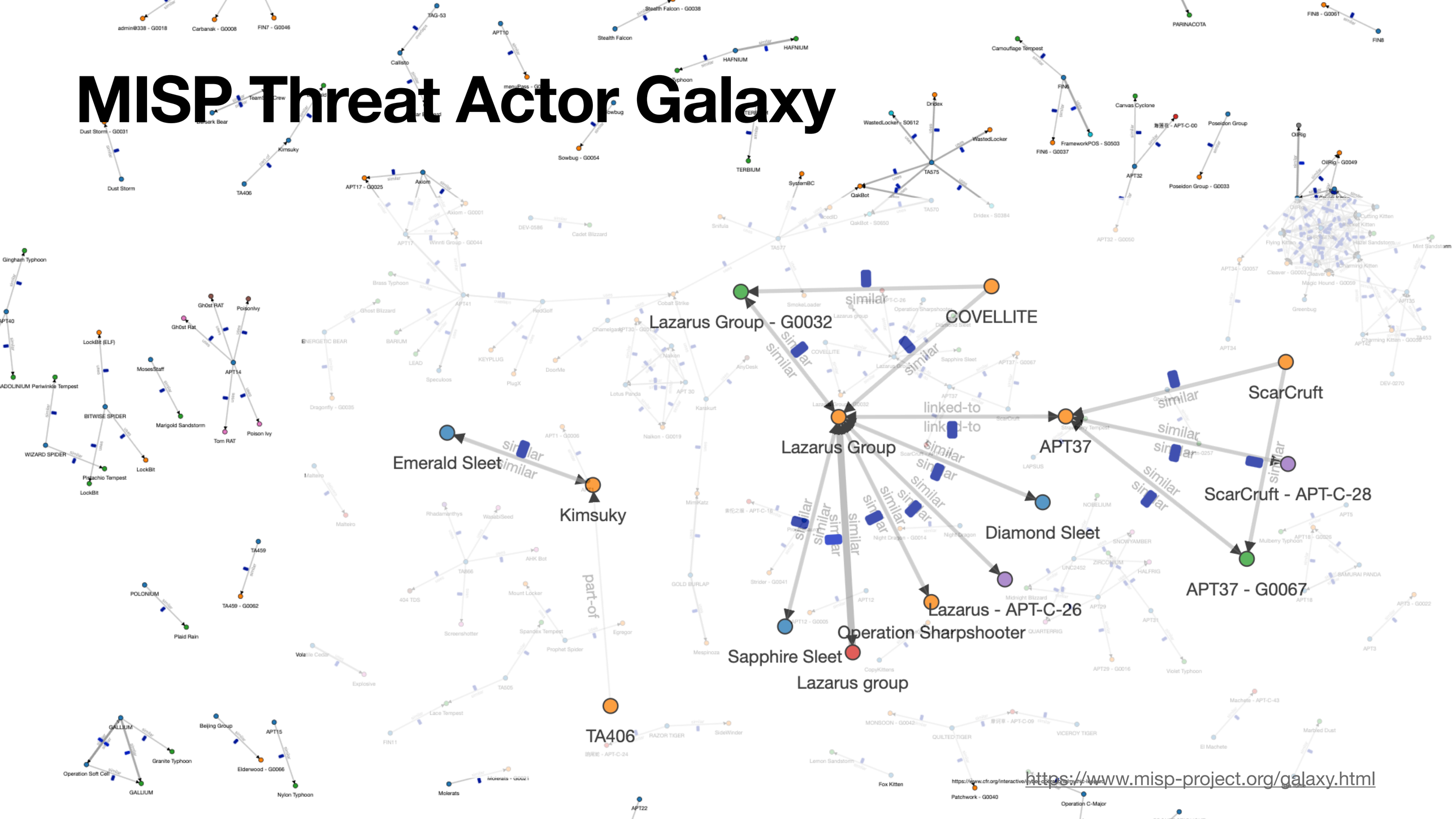
Notable Activities

109

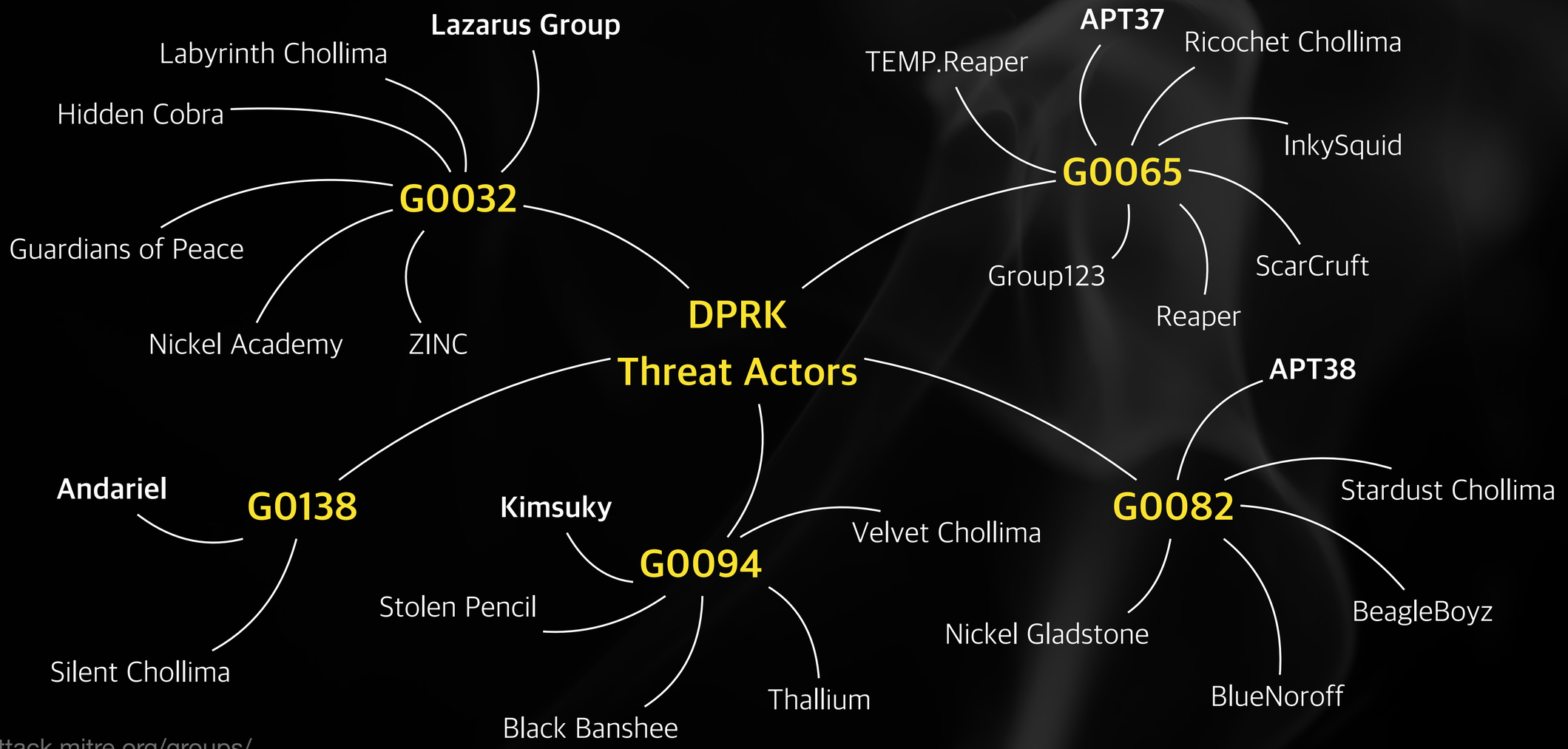
Victim Countries

57

MISP Threat Actor Galaxy

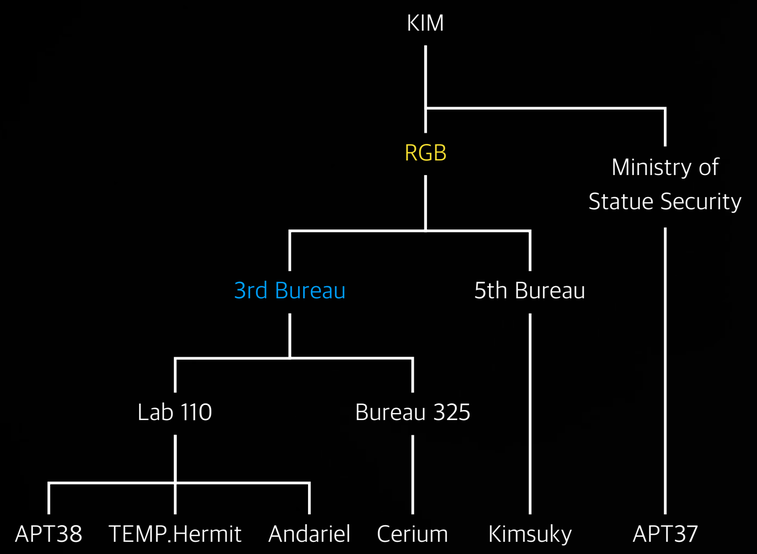


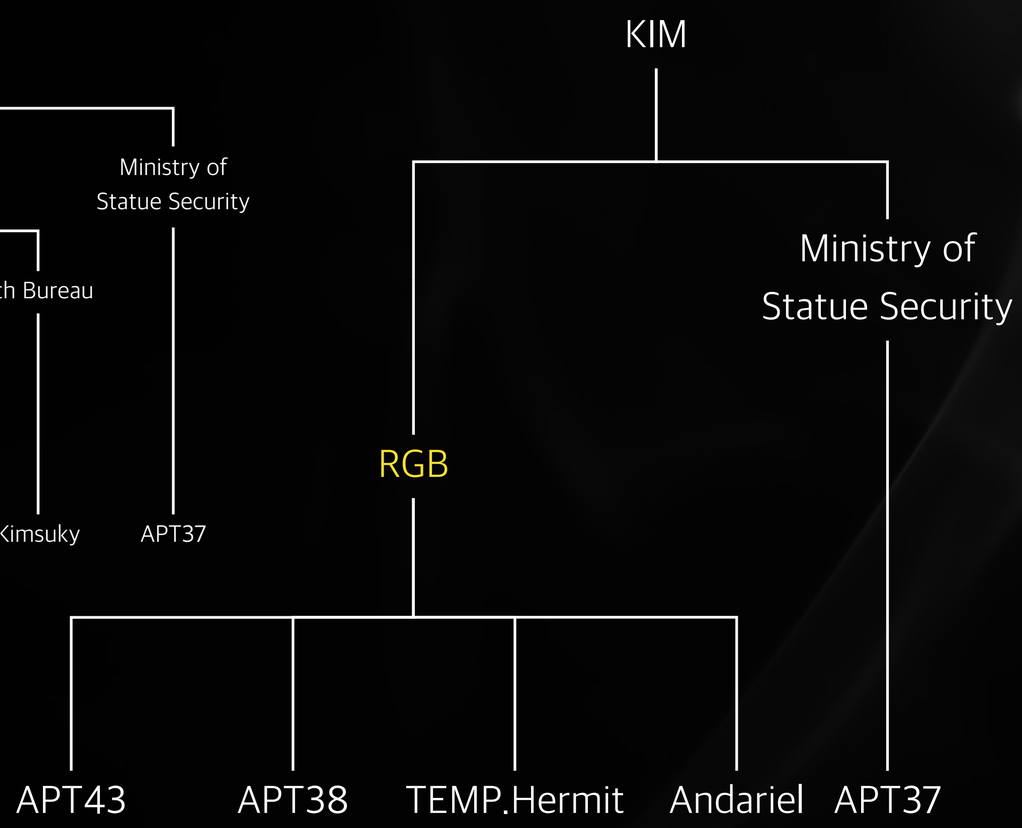
MITRE ATT&CK Groups



https://attack.mitre.org/groups/

Mandiant

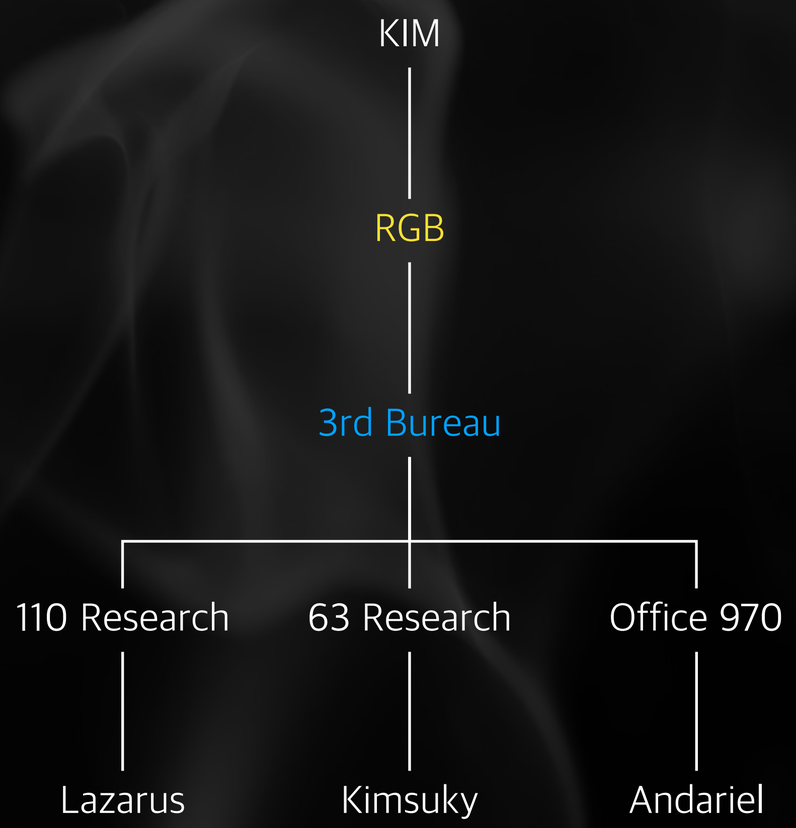




https://www.mandiant.com/resources/mapping-dprk-groups-to-government

https://www.mandiant.com/resources/blog/north-korea-cyber-structure-alignment-2023

UN Security Council



https://undocs.org/Home/Mobile?FinalSymbol=S%2F2023%2F171

Naming conventions: Simple

- Qihoo360: APT-C-[N]
- Cisco Talos: Group[N]
- Elastic: REF[N]
- IBM: ITG[N], Hive[N]
- Mandiant: APT[N], UNC[N]
- Microsoft: Element Name(Deprecated)
- NSHC: Sector[A][N]
- Proofpoint: TA[N]
- Recorded Future: TAG-[N]
- Secureworks: CTG-[N]
- Thales Group: ATK[N]
- Qianxin: APT-Q-[N]

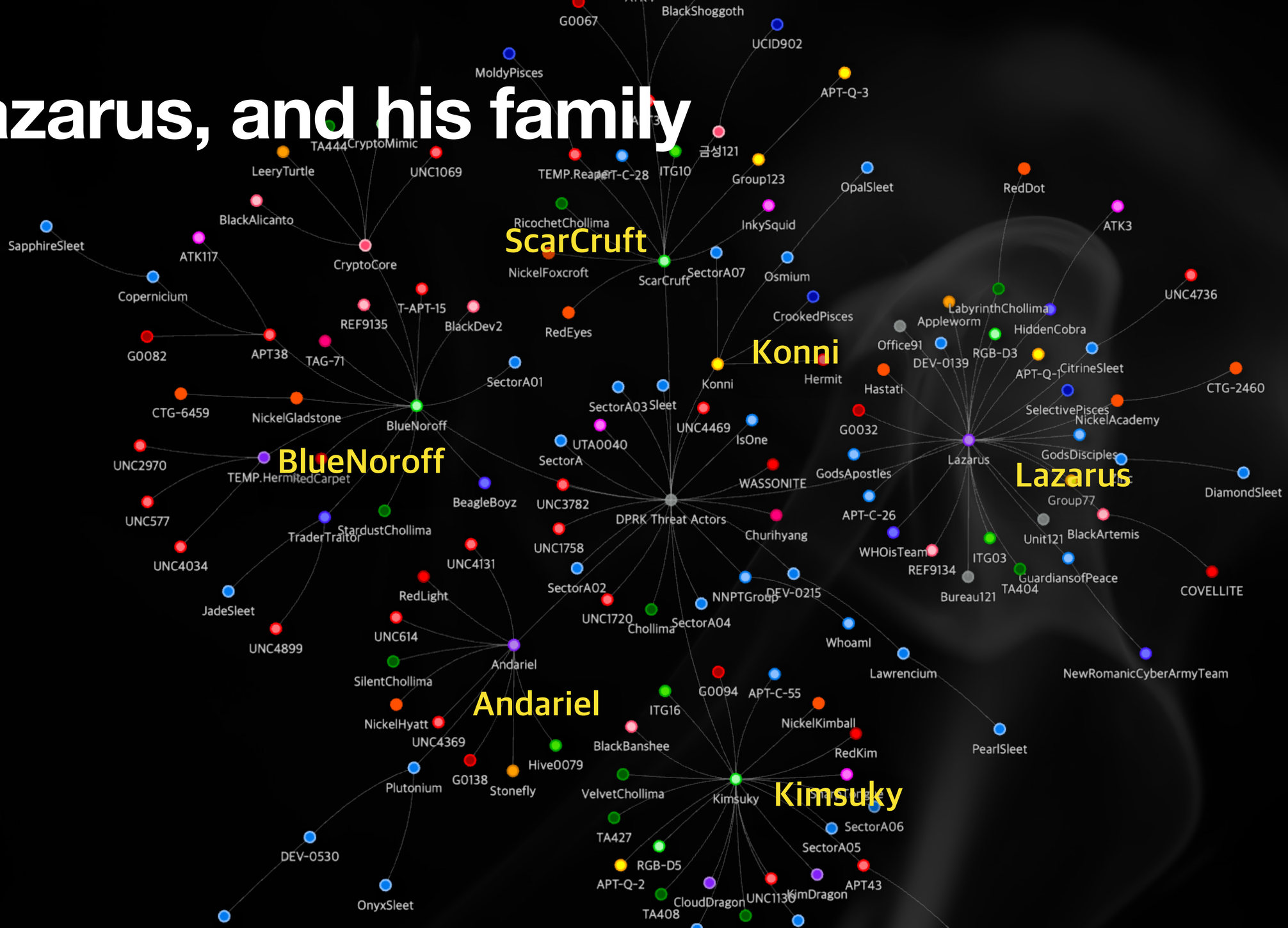
Naming conventions: State-sponsored

	China	DPRK	Iran	Russia
Crowd Strike	Panda	Chollima	Kitten	Bear
Microsoft	Typhoon	Sleet	Sandstrom	Blizzard
NSHC	SectorB	SectorA	SectorD	SectorC
Paloalto Networks	Taurus	Pisces	Serpens	Ursa
PWC	Red	Black	Yellow	Blue
Secureworks	Bronze	Nickel	Cobalt	Iron

Naming conventions: DPRK

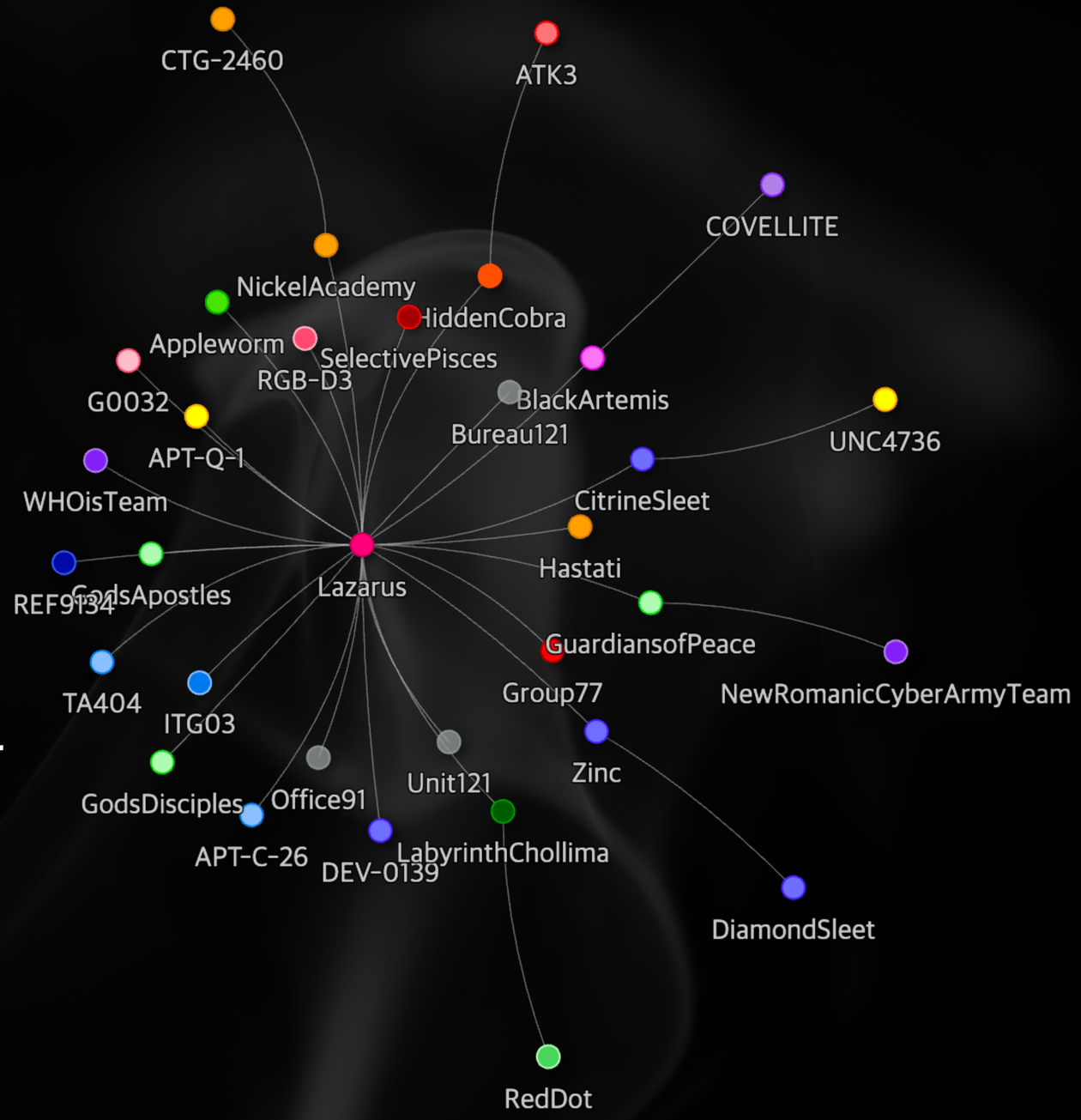
- Ahnlab: Red [Dot | Eyes]
- CrowdStrike: [Labyrinth | Ricochet | Silent | Startdust | Velvet] Chollima
- KRCERT: Red [Carpet | Kim | Light]
- Microsoft: [Citrine | Diamond | Emerald | Jade | Onyx | Opal | Pearl | Ruby | Sapphire] Sleet
- NSHC: SectorA[01 - 07]
- Paloalto Networks: [Crooked | Moldy | Selective] Pisces
- PWC: Black [Alicanto | Artemis | Banshee | Dev2 | Shoggoth]
- Secureworks: Nickel [Academy | Foxcroft | Hyatt | Kimball]

Lazarus, and his family



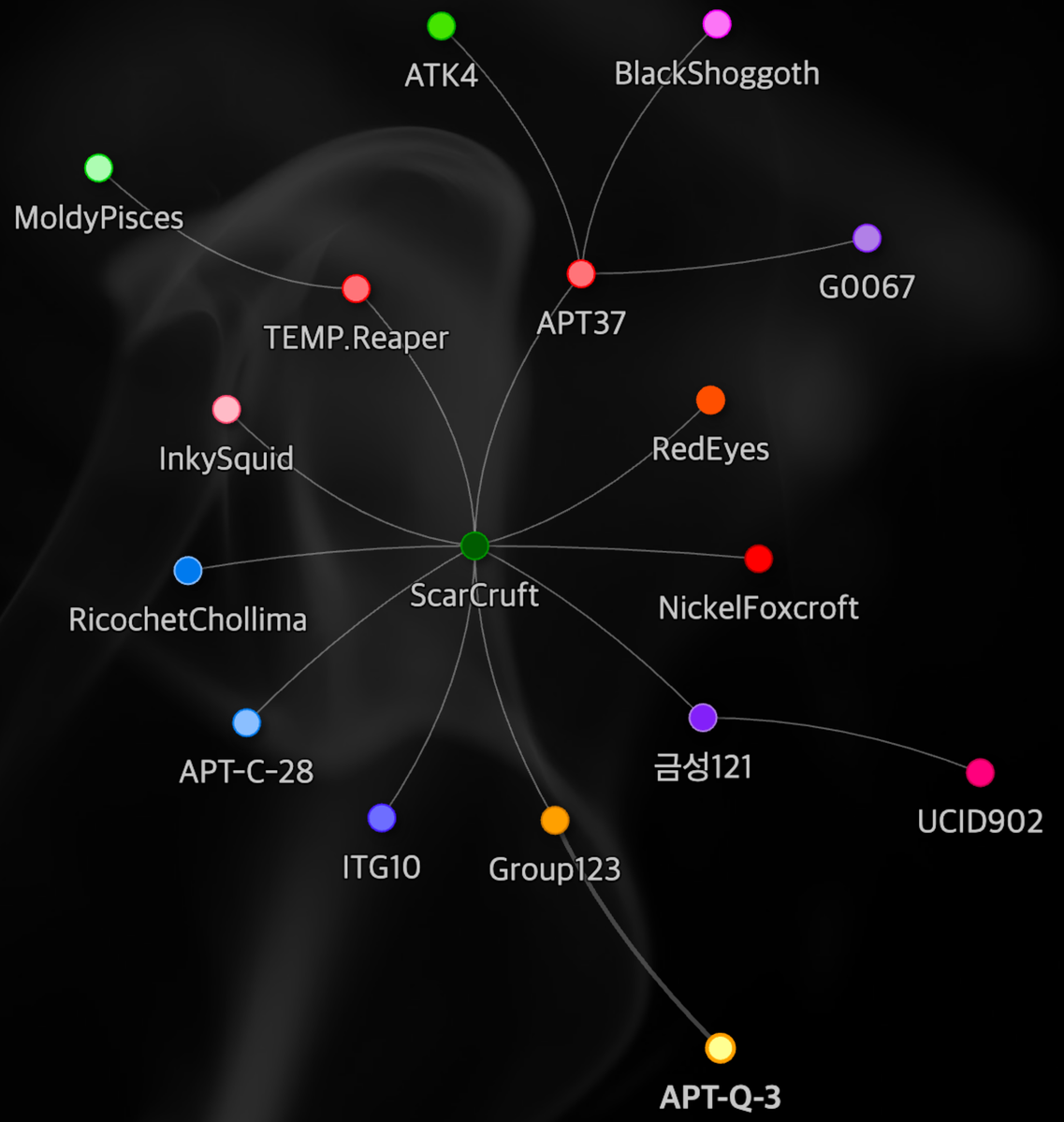
Lazarus, G0032

- Named by Novetta, 2016-02-24
  - Presumably affected by “God’s Apostles” in operation Blockbuster
  - Returned from the dead in the Bible
- Represent the entire DPRK threat actor



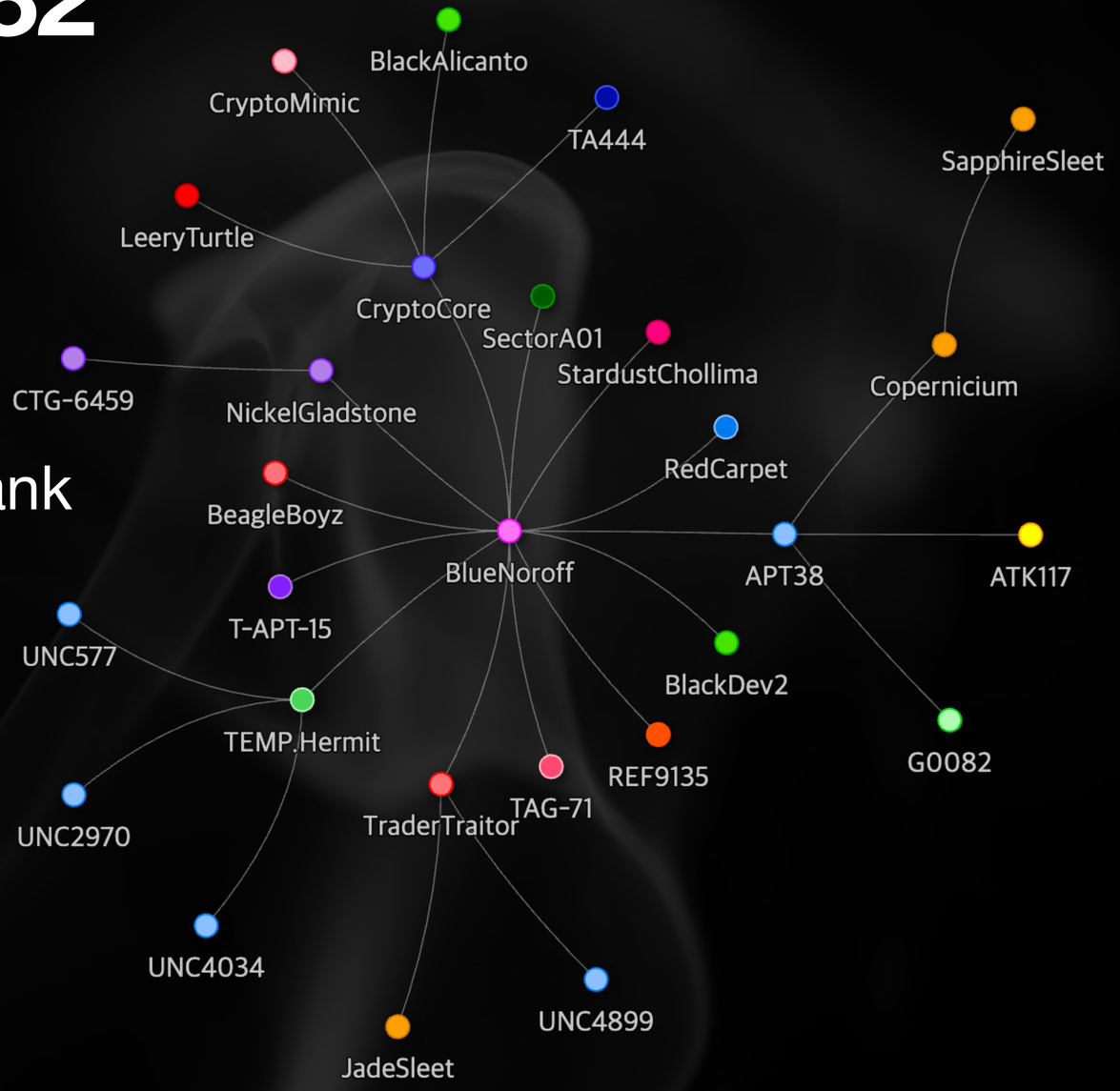
ScarCurft, APT37, G0067

- Named by Kaspersky, 2016-06-17
  - Variations on the malware repository domain, “scarcroft[.]net”
- Targeted the North Korean defectors



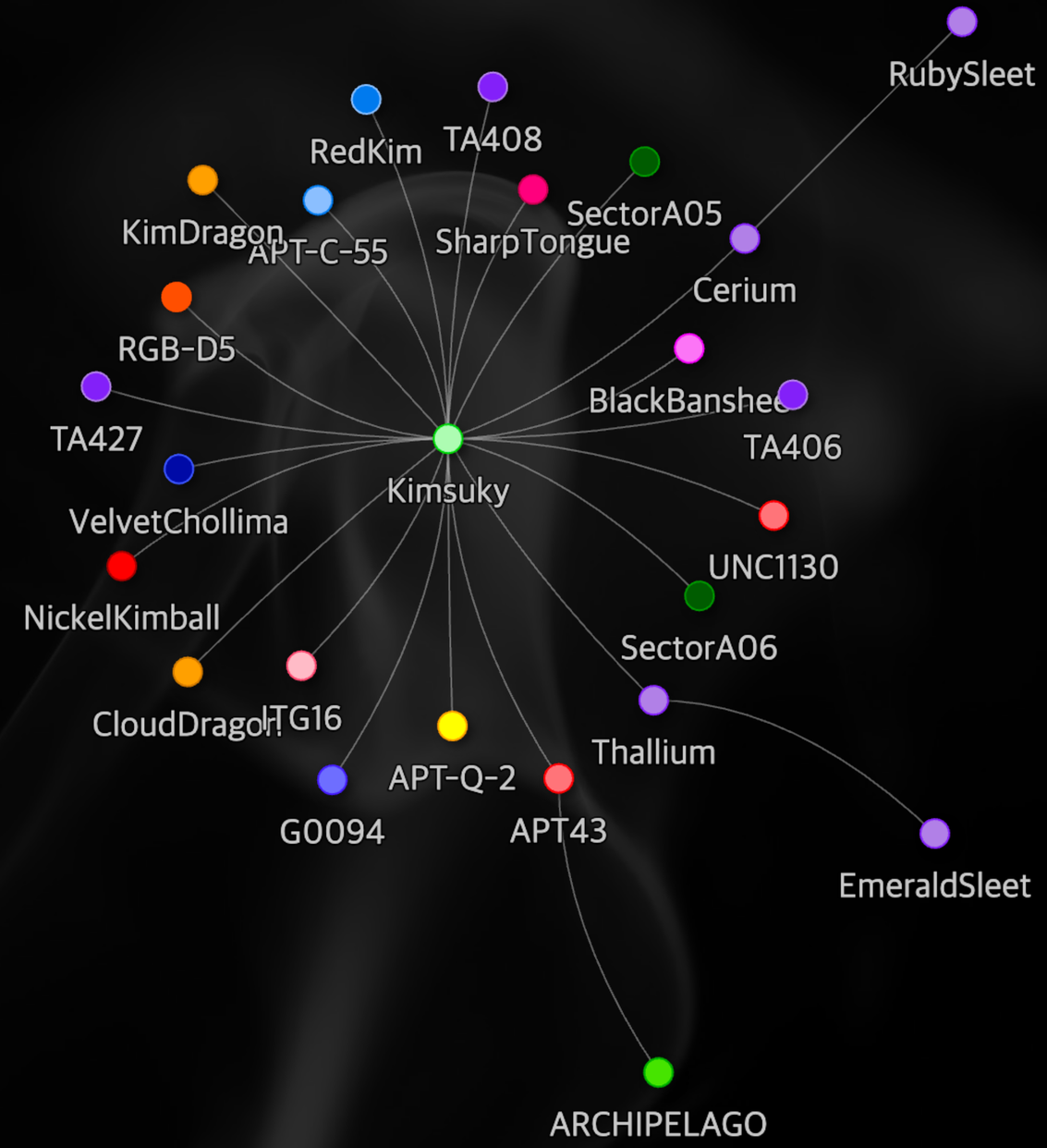
BlueNoroff, APT38, G0082

- Named by Kaspersky, 2017-04-03
  - Variations on the malware filename, “nroff_b.exe” in Bangladesh Central Bank Heist
- Follow the money



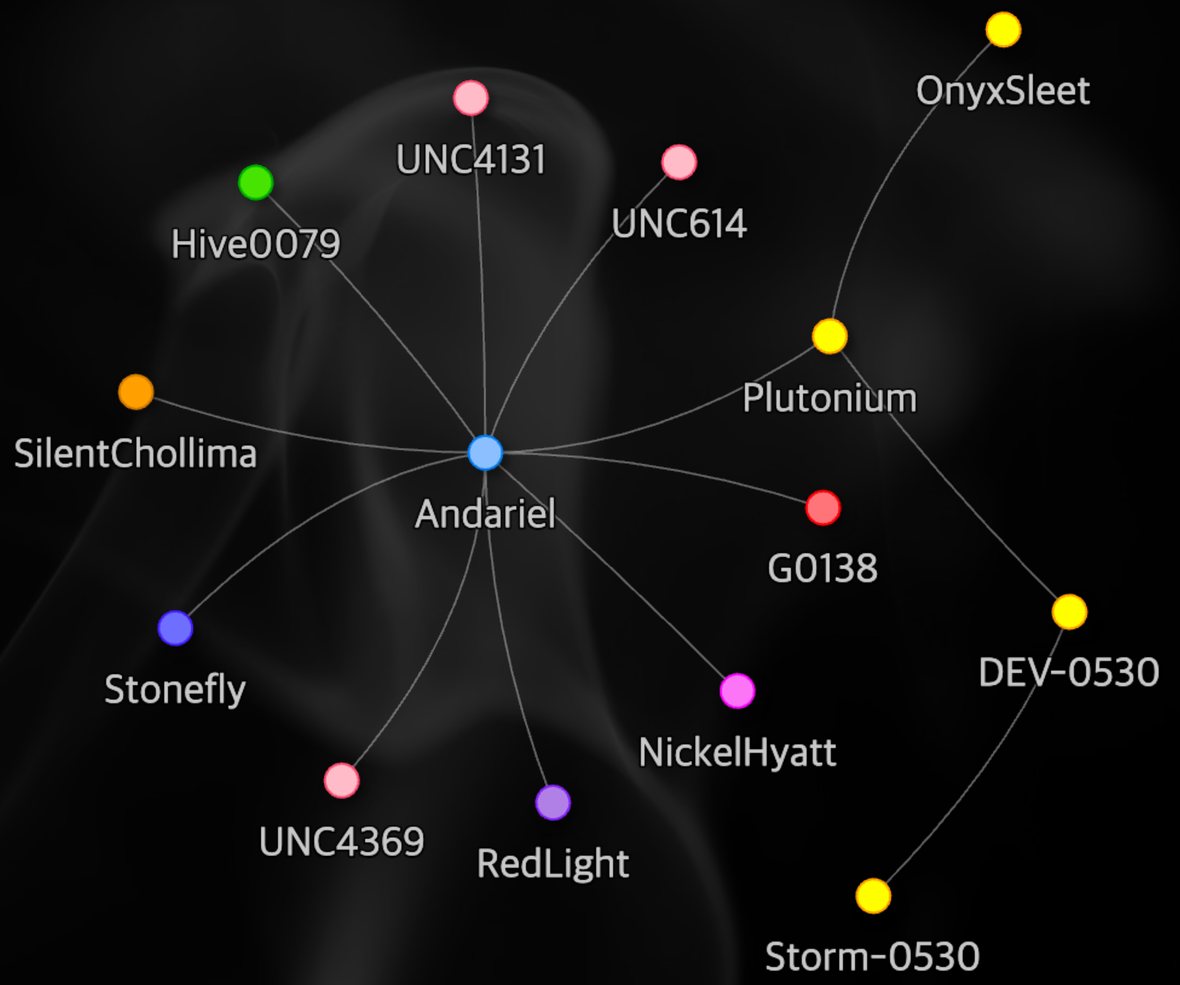
Kimsuky, APT43, G0094

- Named by Kaspersky, 2013-09-11
  - Russianized version of the email sender name, “kimsukyang”(김숙양)
  - Initially announced as an operation code name
- “The king of the spear-phishing”



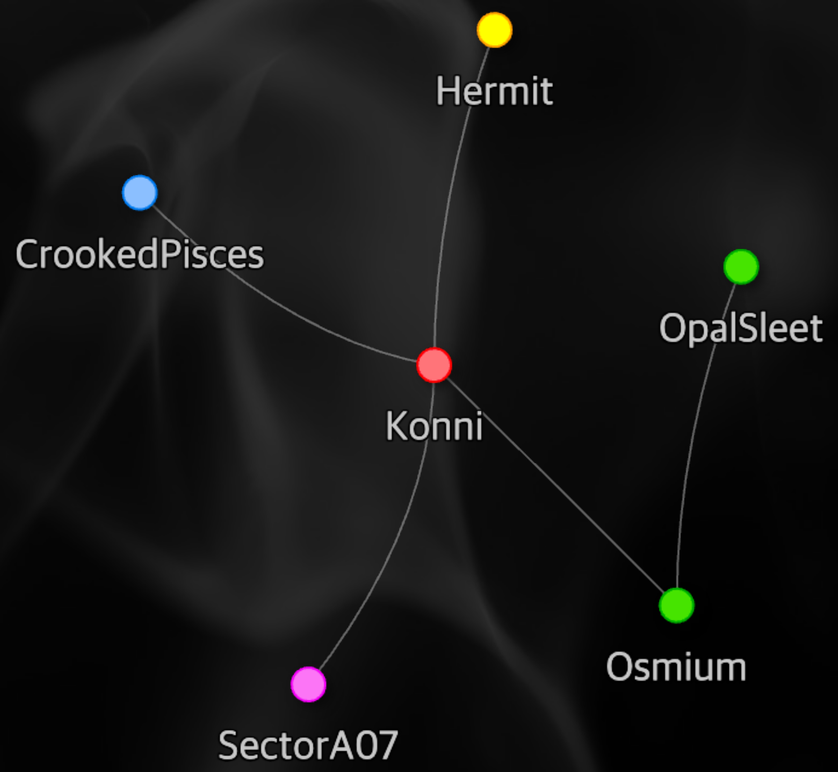
Andariel, G0138

- Named by FSI, 2017-07-27
  - The act 1 boss character in the game, Diablo II
- Exploit centralized management software
- Targeted U.S. healthcare with ransomware

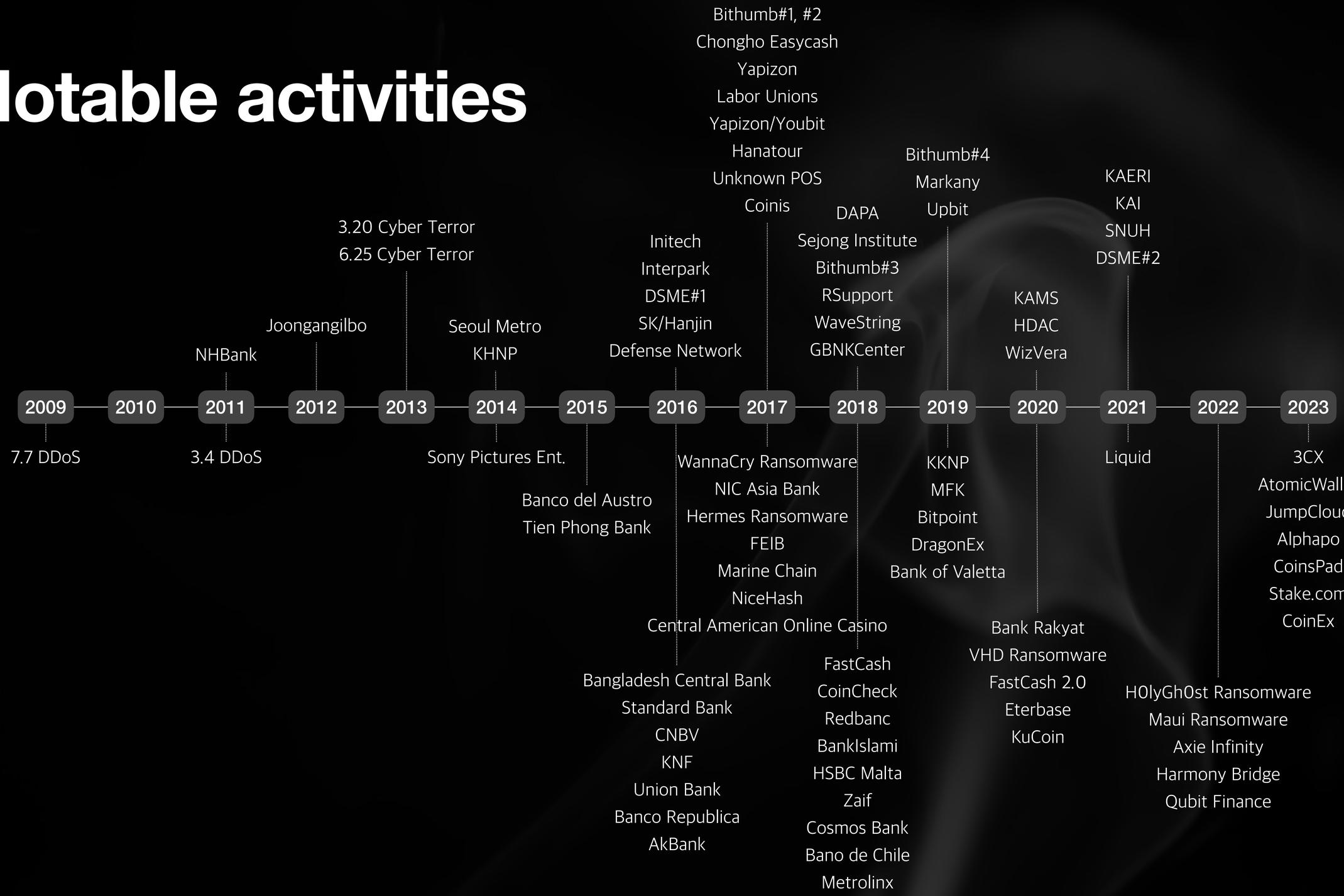


Konni

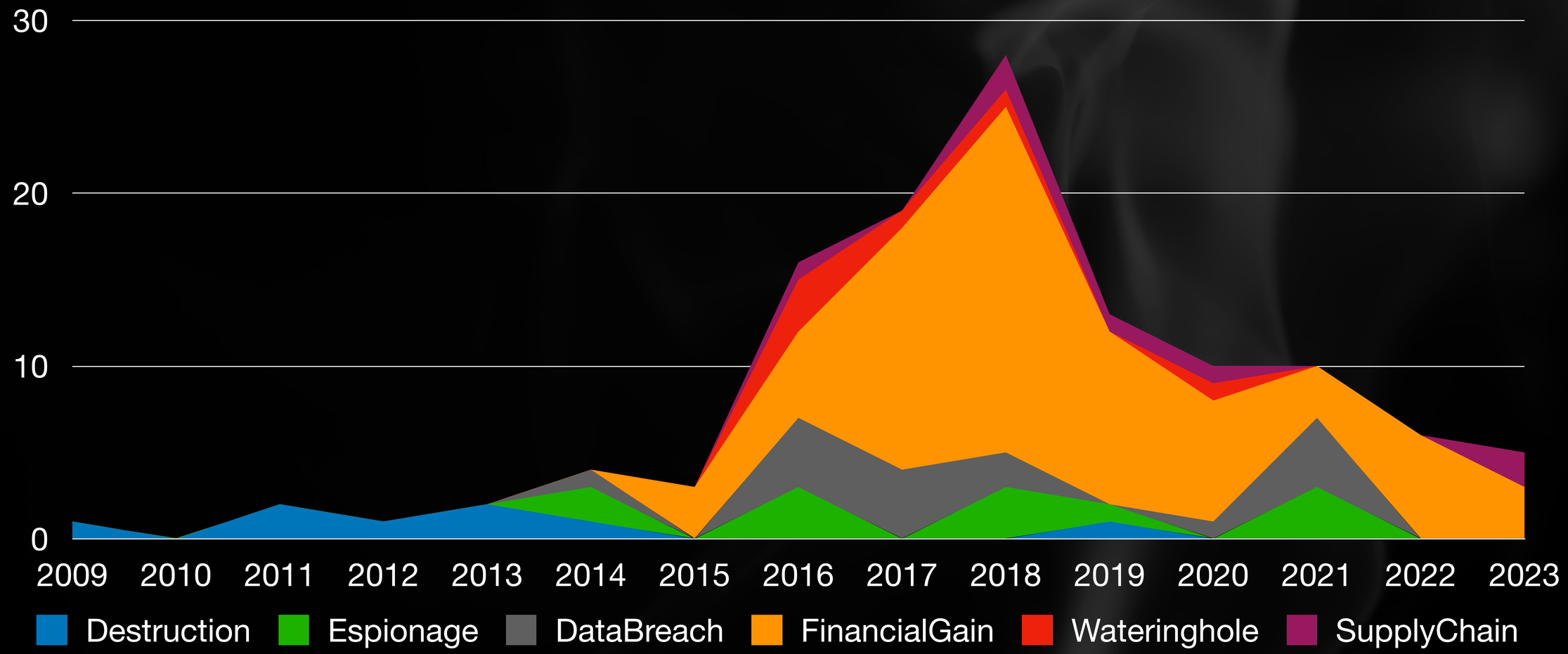
- Named by Cisco Talos, 2017-05-03
  - Initially Introduce as a malware family name
- Spear phishing targeting South Korea



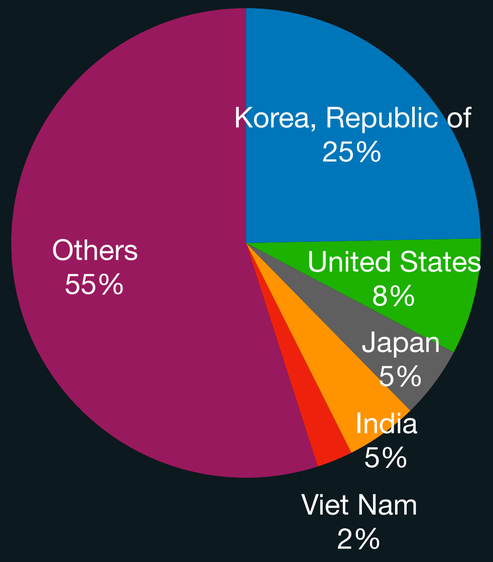
Notable activities



Notable activities by motivation

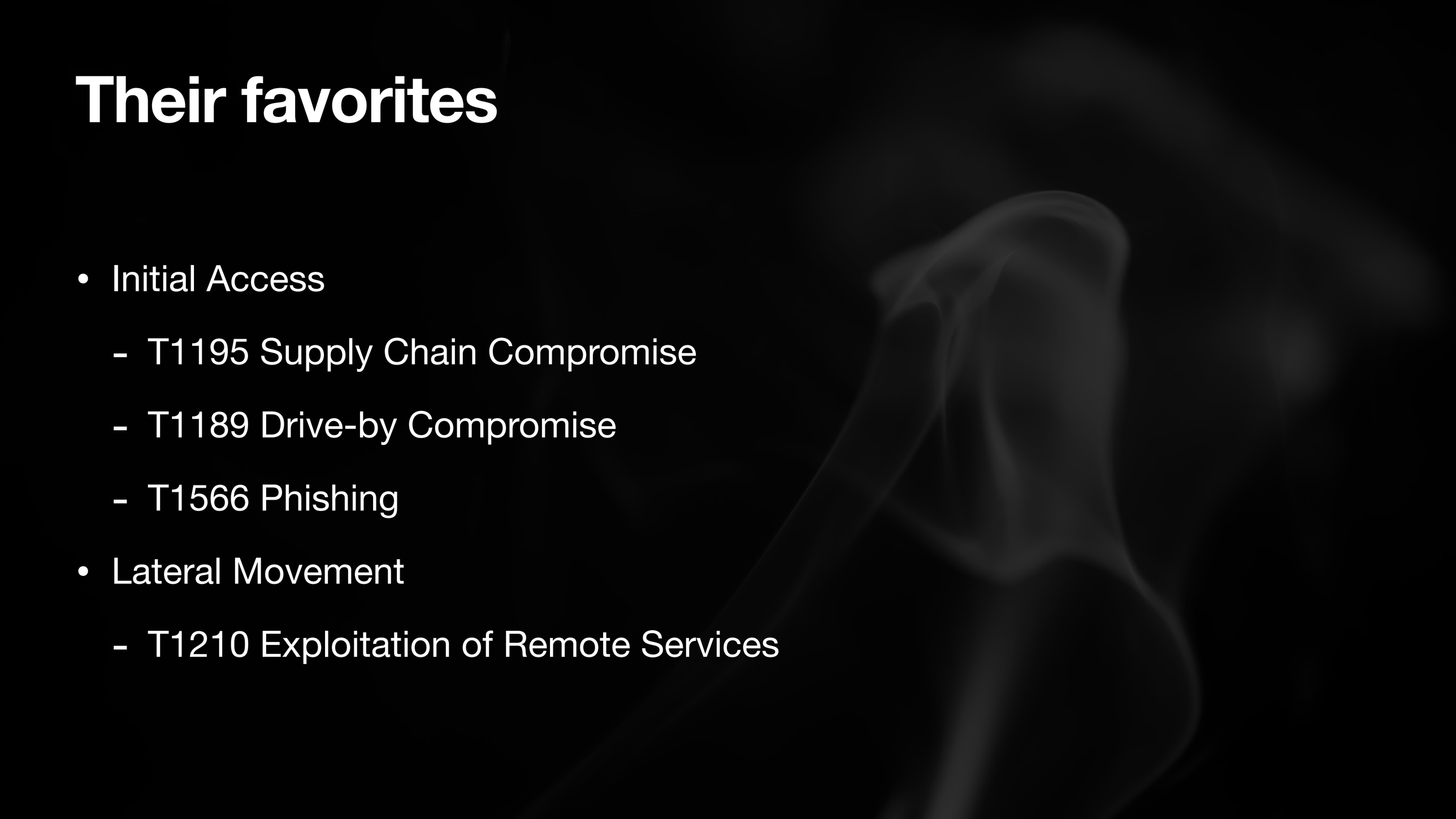


Worldmap


Korea, Republic of
25%
United States
8%
Japan
5%
India
5%
Viet Nam
2%
Others
55%

Their favorites

- Initial Access
  - T1195 Supply Chain Compromise
  - T1189 Drive-by Compromise
  - T1566 Phishing
- Lateral Movement
  - T1210 Exploitation of Remote Services



Is he everywhere?

@lazarusholic

https://lazarus.day

Background Images: Unsplash Marek Piwnicki