Blurred Lines of Cyber Threat Attribution:

The Evolving Tactics of North Korean Cyber Threat Actors

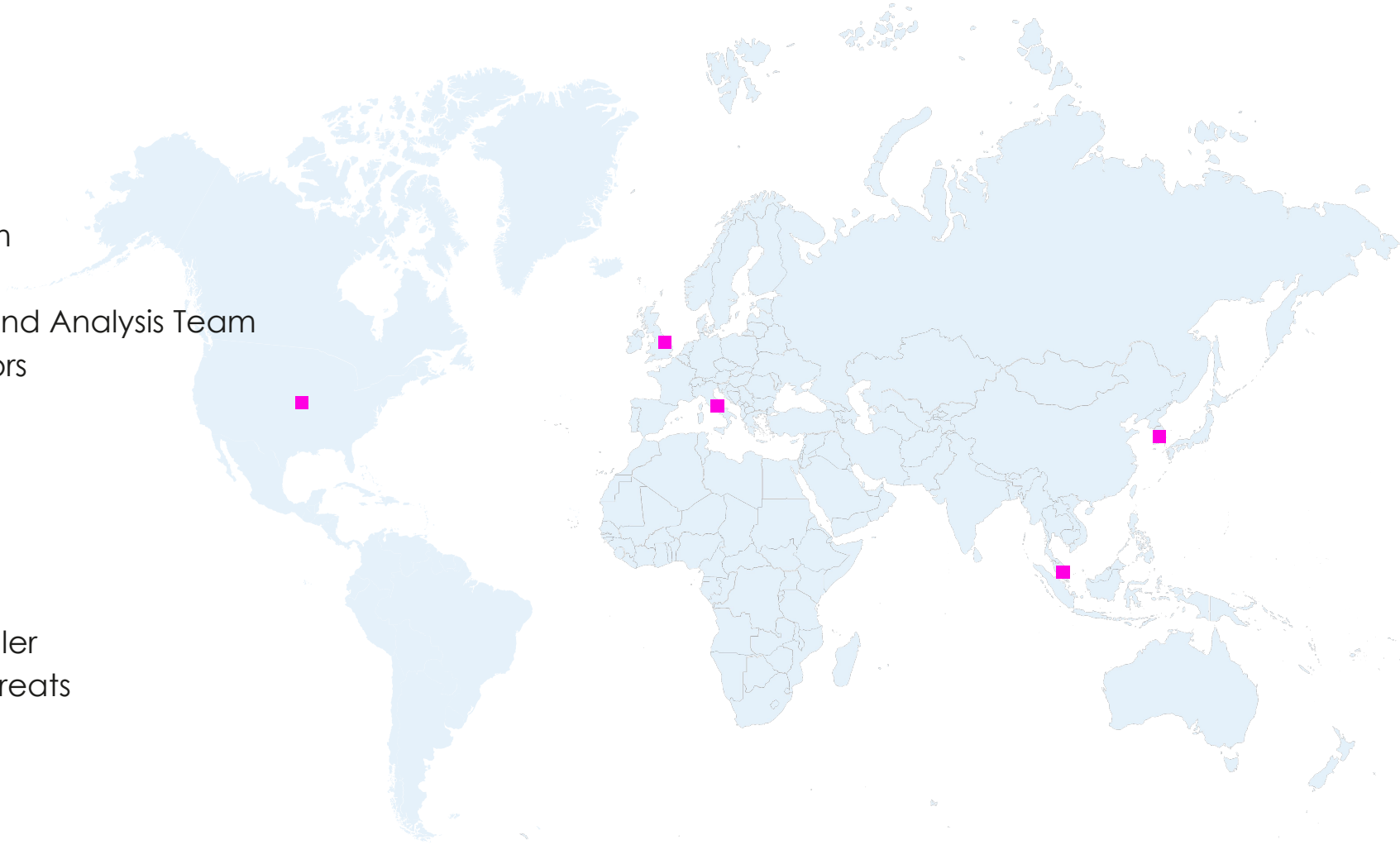
Seongsu Park, Staff Threat Researcher
APT Research

Adversary Village at DEF CON 33

Introduction

Seongsu Park

- Zscaler, ThreatLabZ, APT Research Team
- Staff Threat Researcher
- Formerly, Kaspersky, Global Research and Analysis Team
- Mostly tracking North Korea threat actors



APT Research Team

- Global threat intelligence team of Zscaler
- Tracking and analyzing global cyber threats
- Analyzing novel attack techniques

Attribution in Cyber Threat Intelligence

- Cyber Threat Intelligence (CTI) is evidence-based knowledge about adversaries' motivations, capabilities, and tactics that enables informed security decisions.
- Attribution is the process of identifying the actors responsible for cyber attacks by analyzing technical indicators, tactics, and strategic context.
- Attribution requires both technical evidence and analytical judgment to determine who is behind an attack and why they conducted it.

Challenges in Accurate Cyber Threat Attribution

False Flags

Attackers deliberately plant misleading evidence

Shared Infrastructure

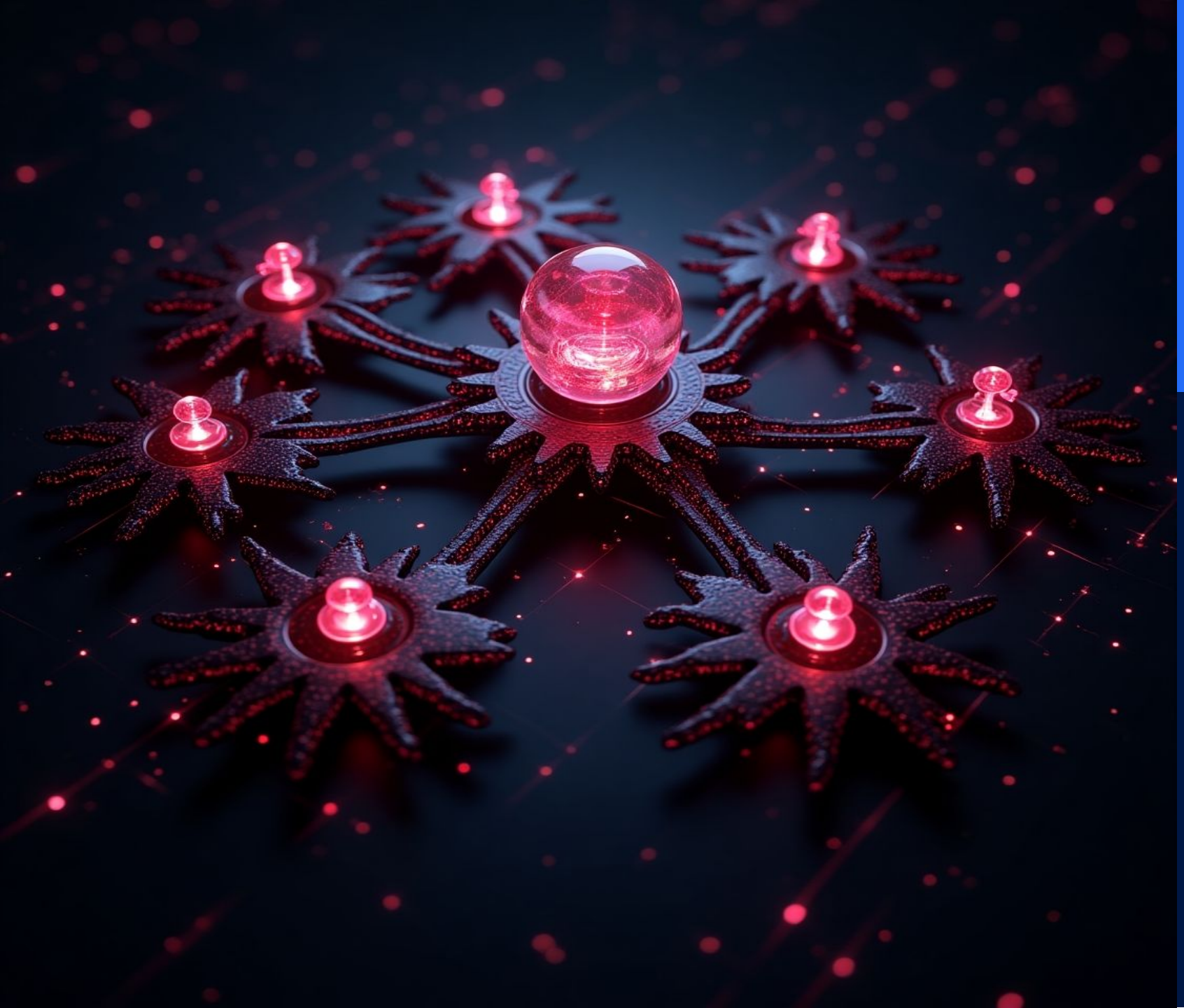
Multiple threat actors using the same tools and hosting services

Anonymization Tools

Use of VPNs, Tor, and proxies to hide true origin

Code and Tool Reuse

Reuse public malware and tools



Case #1

The Rise of Umbrella Groups: A Structured Expansion

Lazarus group

Historical events of Lazarus group

1

2007: Initial Recognition

Sony Pictures breach established Lazarus group as a significant threat actor with potential nation-state backing

2

2014: Sony Pictures hack

WannaCry ransomware outbreak demonstrated expanded capabilities and willingness to cause widespread disruption

3

2017: WannaCry ransomware outbreak

Lazarus Group splinters into specialized operational units with distinct focuses: financial crime, espionage, and intelligence gathering

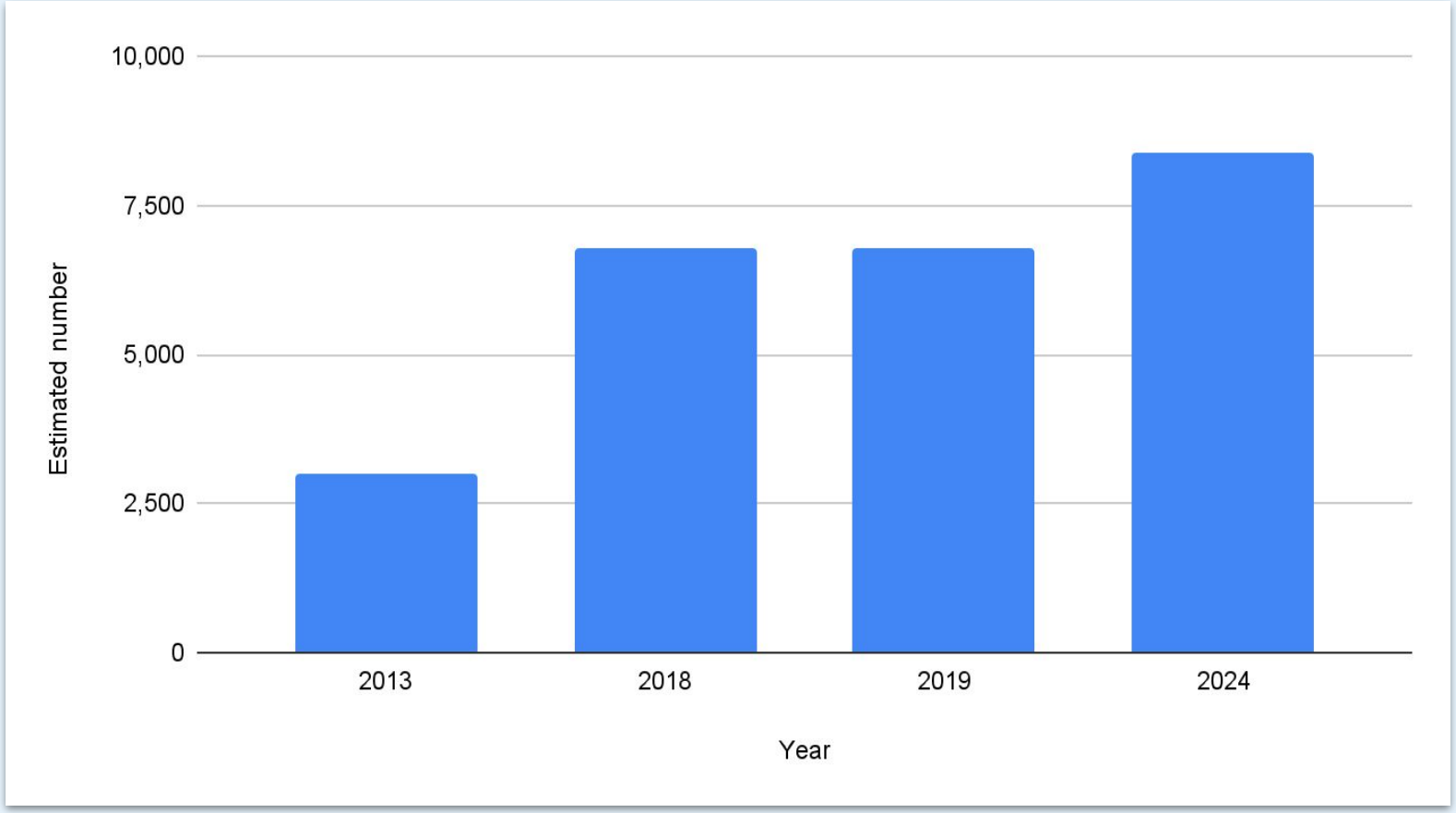
4

2019-2023: Global cryptocurrency theft campaigns

Growth of North Korea's Cyber Army

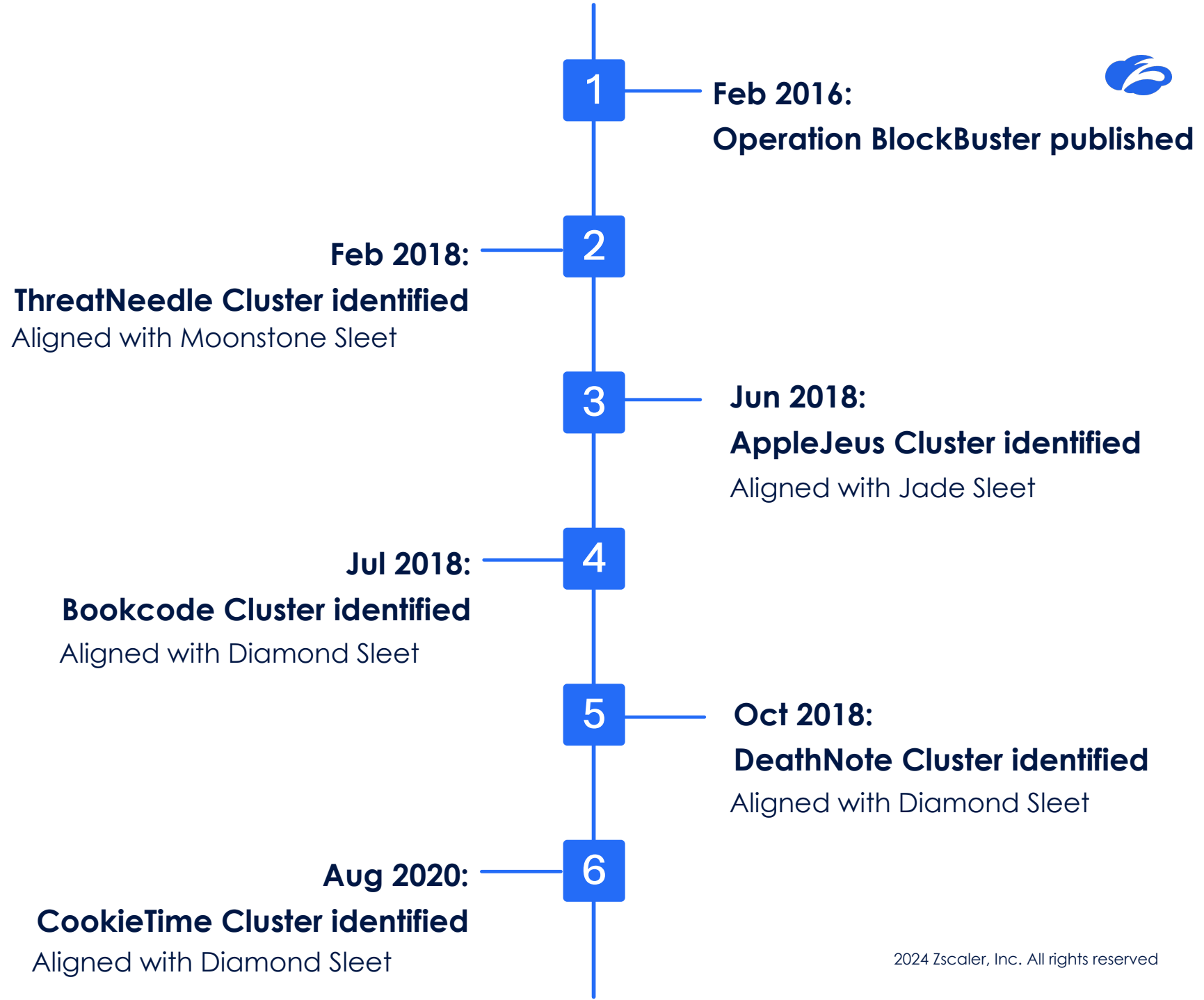
- The number of cyber operatives has increased consistently each year, indicating a deliberate and ongoing expansion.
- Between 2013 and 2018, the size of the cyber force approximately doubled, highlighting a sharp escalation in recruitment and training efforts.

- **Number of Cyber Army of DPRK from Korea Defence White Paper**



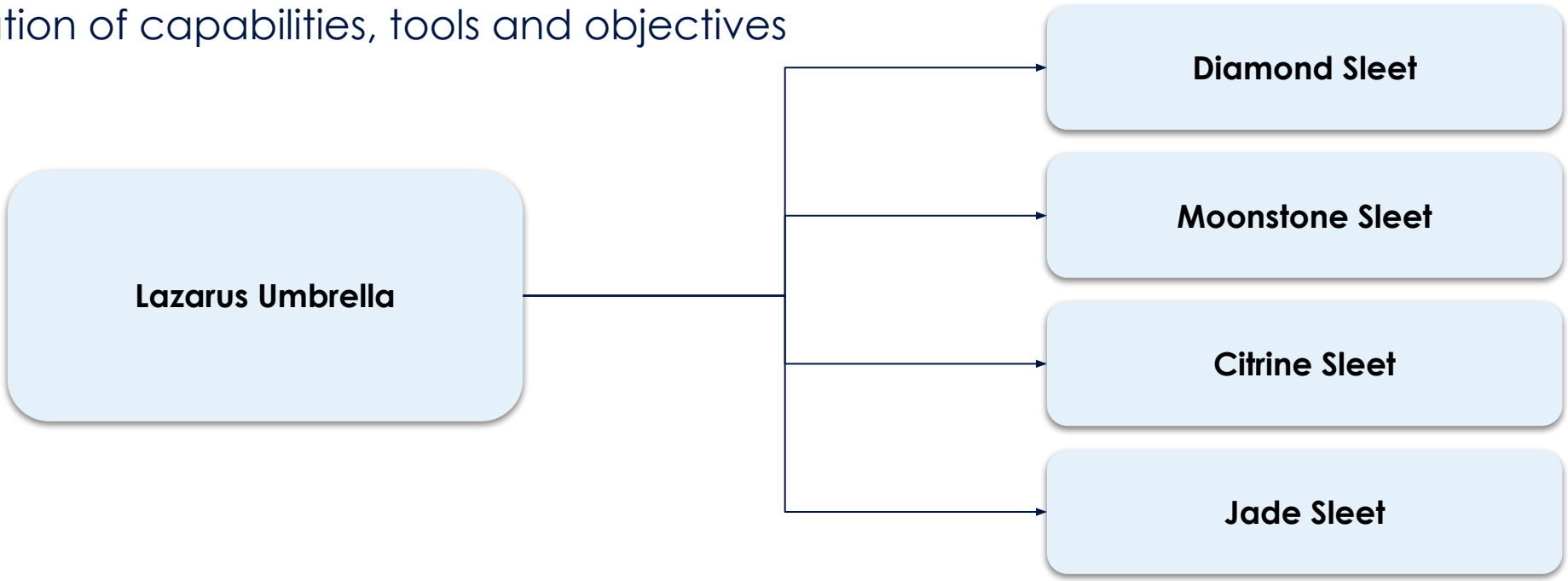
Expansion of Lazarus group

- Since 2018, multiple sub-clusters within the Lazarus group have been identified, indicating a more complex and decentralized operational structure.
- The majority of these sub-groups remain active, continuing to engage in diverse cyber operations across the globe.



Expansion of Lazarus group

Diversification of capabilities, tools and objectives



Connections

- Identified within the same victim environment
- Many code similarities observed across samples
- Shared toolsets and post-exploitation techniques
- Overlapping command-and-control (C2) infrastructure

Differences

- Distinct Tactics, Techniques, and Procedures (TTPs)
- Divergent targeting objectives and operational focus

Expansion of Kimsuky group

Multi-cluster of Kimsuky group

- Published: 2013
- Also Known As: APT43, Emerald Sleet, Velvet Chollima
- Initial activity: Focused on cyber espionage attack

	BabyShark	AppleSeed	httpSpy	FPSpy	MillionOK
Tools	Various scripts	Custom backdoor	httpSpy/PEBBLEDASH, Golang malware	FPSpy, KLogger	AiTM phishing Kits
Primary Objective	Surveillance	Intelligence gathering	Intelligence gathering	Intelligence gathering	Financial profits
Main Targets	Individual related to DPRK regime	Enterprise, Government, Defense, and so on	Defense sector, Heavy-industry	Entities related to DPRK regime	Individual investors

The Rise of Umbrella Groups: A Structured Expansion

Key Takeaways

Threat actors are evolving into structured, multi-cluster entities

- North Korea has restructured its cyber capabilities from a single group (e.g., Lazarus) into multiple operational sub-clusters, each tasked with distinct mission profiles such as cyber espionage, financial intrusion, and strategic intelligence collection.
- Subgroups are structured similarly to enterprise teams, functionally organized to support distinct national strategic goals.

TTP-Based clustering is essential for accurate attribution

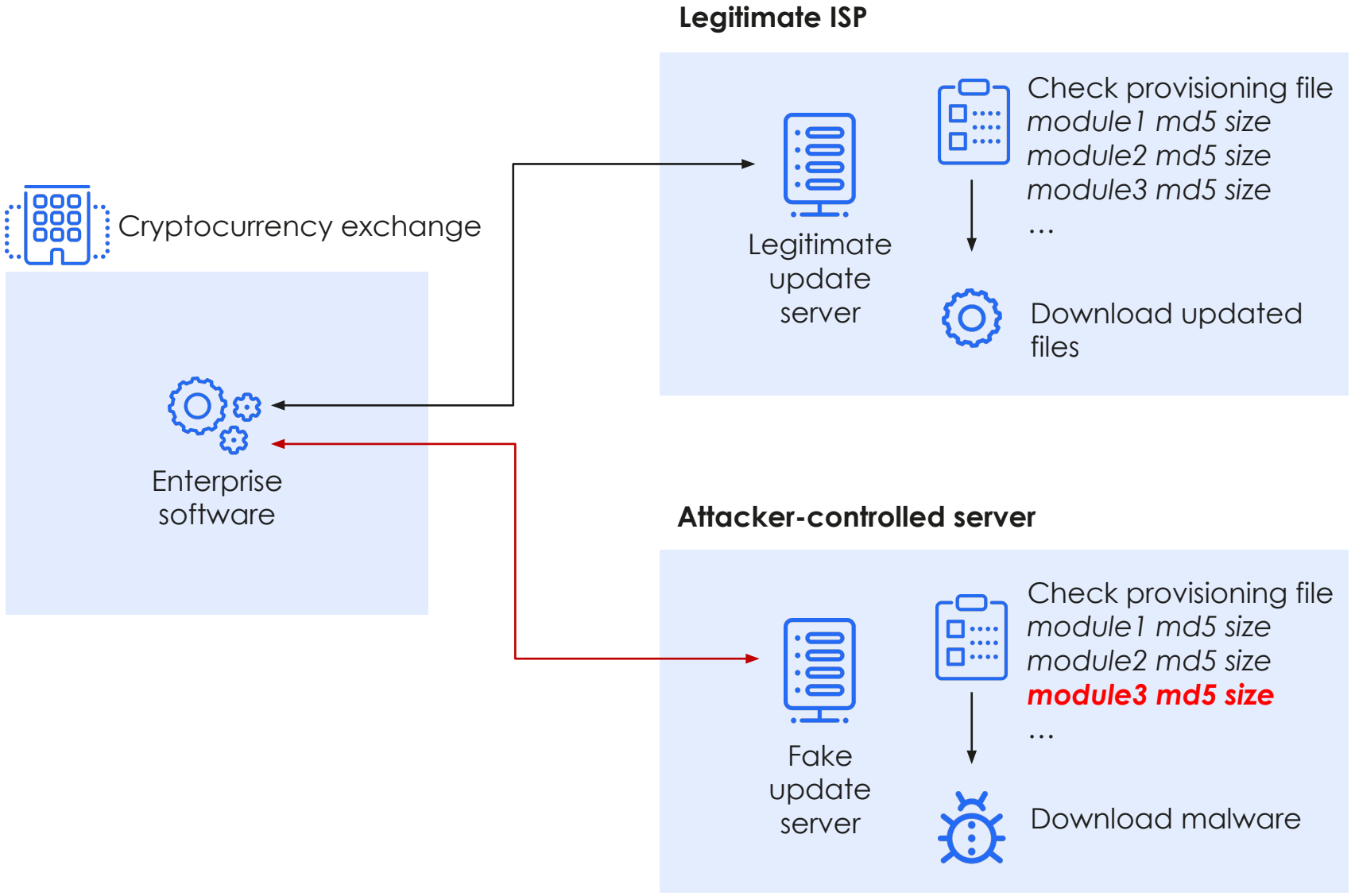
- Profiling threat actors by consistent TTPs allows analysts to decompose umbrella groups into distinct sub-clusters, each with identifiable technical and behavioral traits.
- This granularity enhances attribution accuracy, supports proactive threat hunting, and enables tailored detection and response strategies aligned to specific adversary behaviors.

Case #2

Inter-Group Collaboration: The Blurring of Attribution

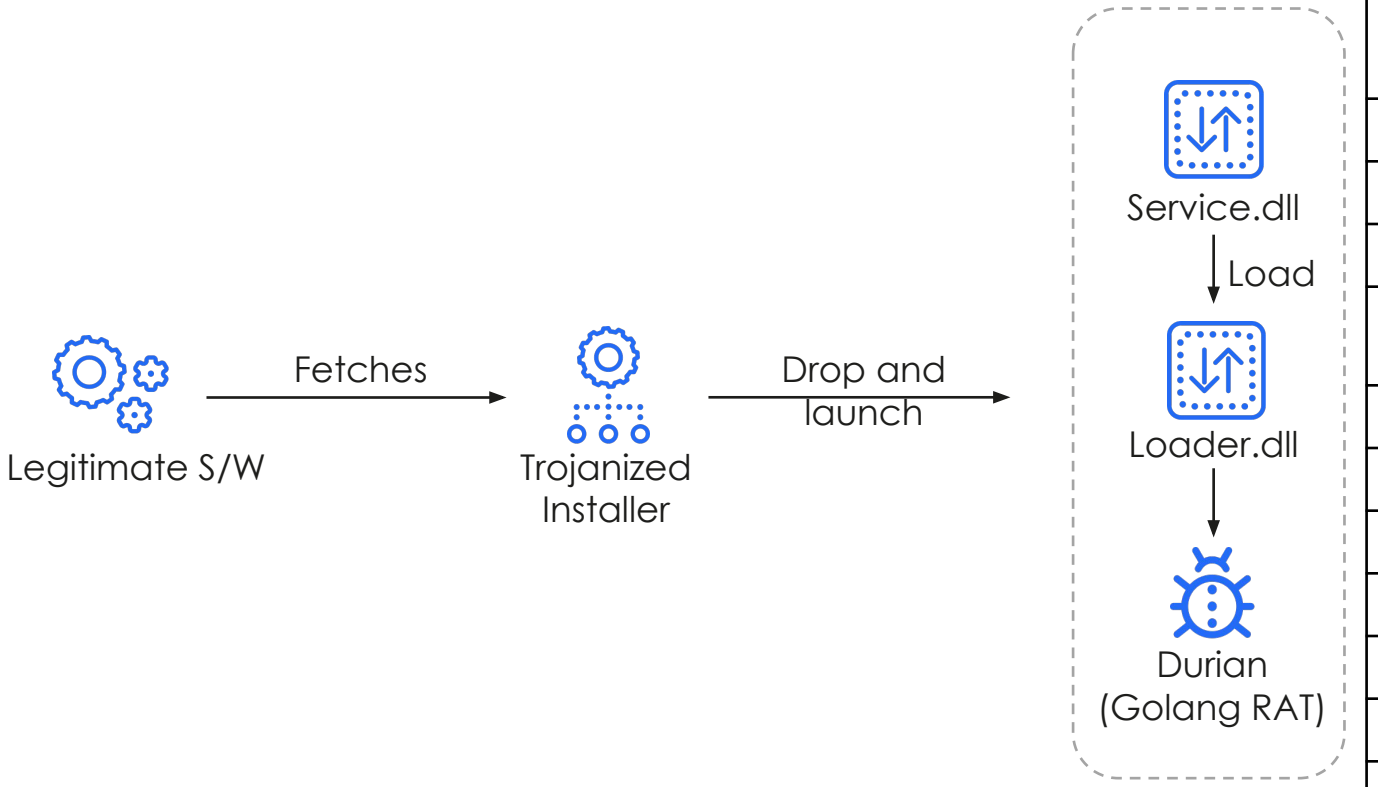
Supply-Chain attack

- Identified in late 2023.
- Malware was delivered via a legitimate security product.
- The attacker manipulated the software update mechanism somehow.



Cryptocurrency targeting attack

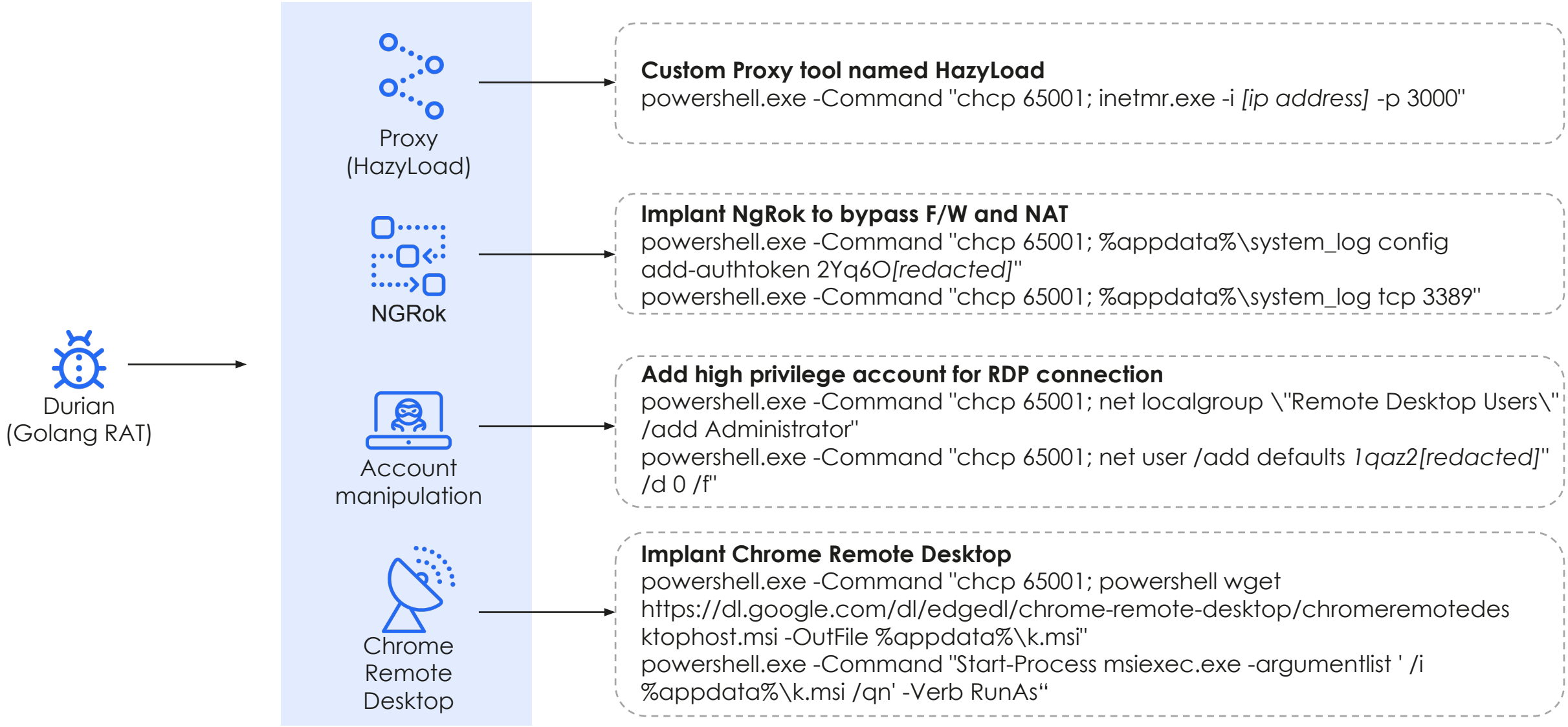
Implatanted malware



Index	Command name	Description
0	ProcessCommand_Hibernate	Enter sleep mode.
1	ProcessCommand_Interval	Set Sleep interval.
2	ProcessCommand_ExecuteJob	Execute command with "powershell.exe -Command "chcp 65001; [command]" format.
3	ProcessCommand_Ls	Enumerate a list of files and directories.
4	ProcessCommand_Drives	Gather disk information.
5	ProcssCommand_UploadStart	Received a file from the C2 server.
9	ProcessCommand_DownloadStart	Upload a file from victim to C2 server.
7	N/A	Write file.
8	N/A	Close file.
12	ProcessCommand_MakeDir	Create a new directory.
13	ProcessCommand_Remove	Remove the directory.
14	ProcessCommand_Execute	Execute delivered command.
15	N/A	Exit
16	ProcessCommand_SelfDelete	Remove itself with the Windows command: cmd.exe /c ping 127.0.0.1 -n 4 && del /f /q [module path]

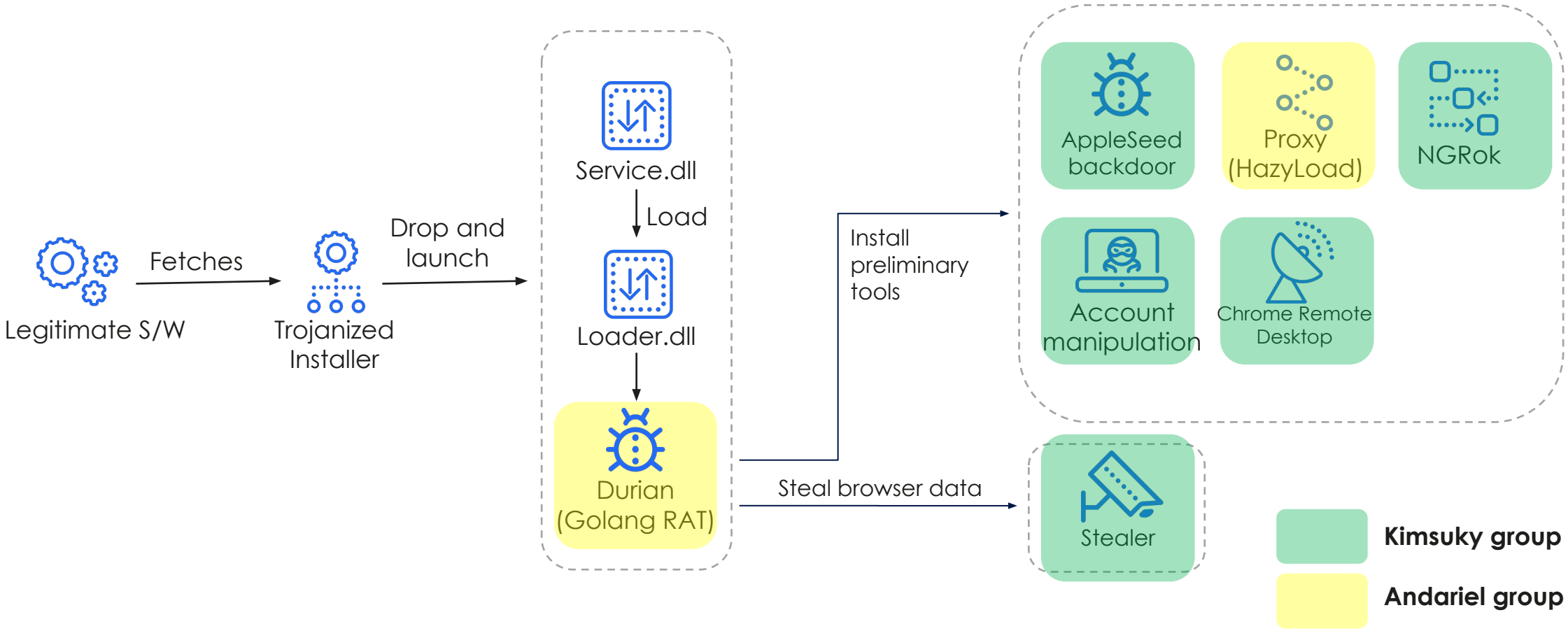
Cryptocurrency targeting attack

Post-exploitation process: Installed preliminary tools



Cryptocurrency targeting attack

Summary of infection chain and known connection



Inter-Group Collaboration: The Blurring of Attribution

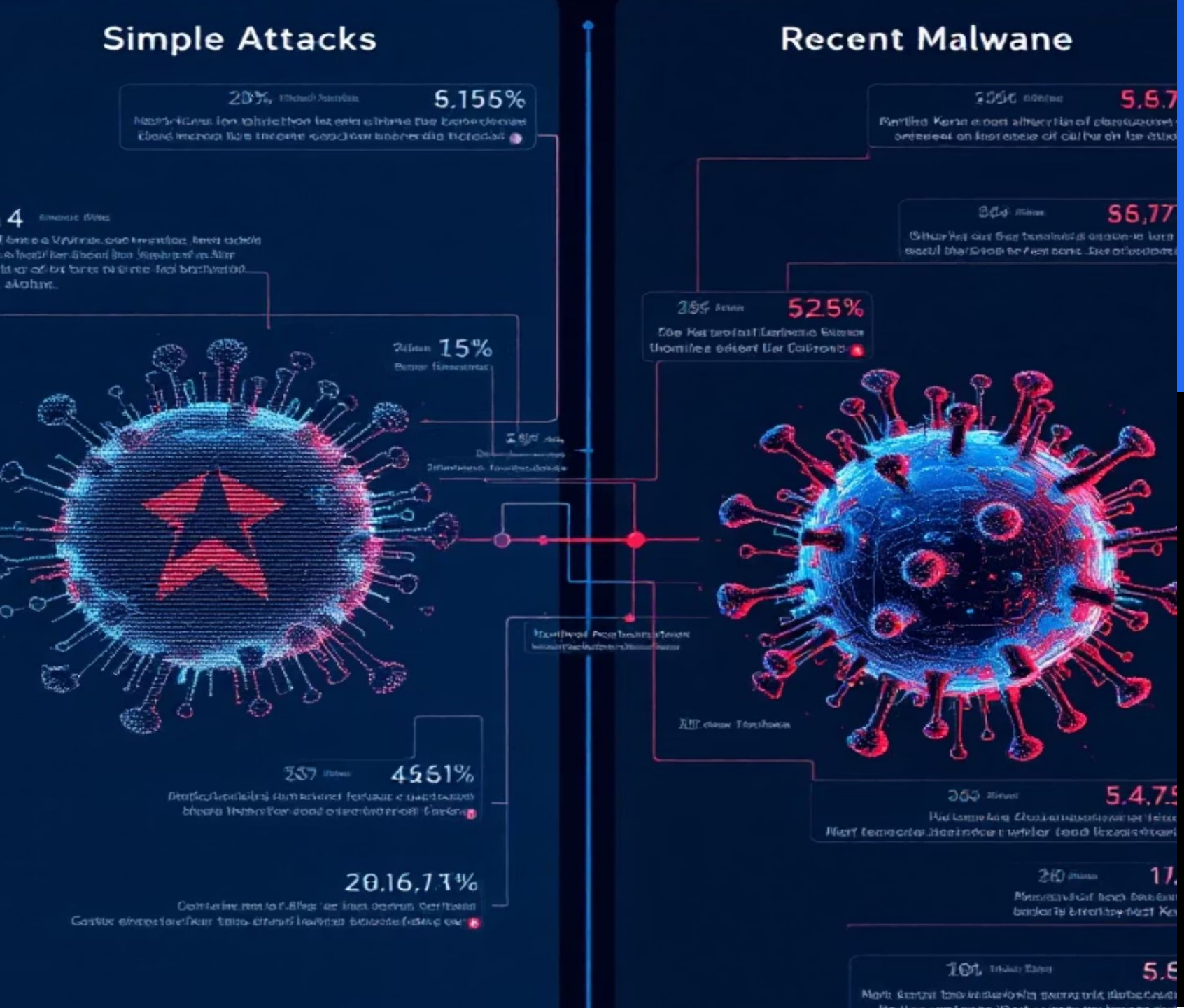
Key Takeaways

Hybrid operations reveal multi-group involvement within single intrusions

- Incident analysis increasingly reveals that DPRK threat groups like Andariel and Kimsuky may operate collaboratively across different phases of a single campaign, blurring conventional attribution lines.
- These hybrid operations indicate shared tools, intelligence, or coordinated handoffs, challenging the assumption that a single group owns the entire intrusion lifecycle.

DPRK cyber units are coordinating to achieve shared objectives

- Previously siloed threat actors are now coordinating their efforts, aligning distinct capabilities to achieve shared operational goals.
- This inter-group collaboration reflects a unified, mission-oriented strategy where multiple units converge on targets with complementary roles to maximize effectiveness and impact.

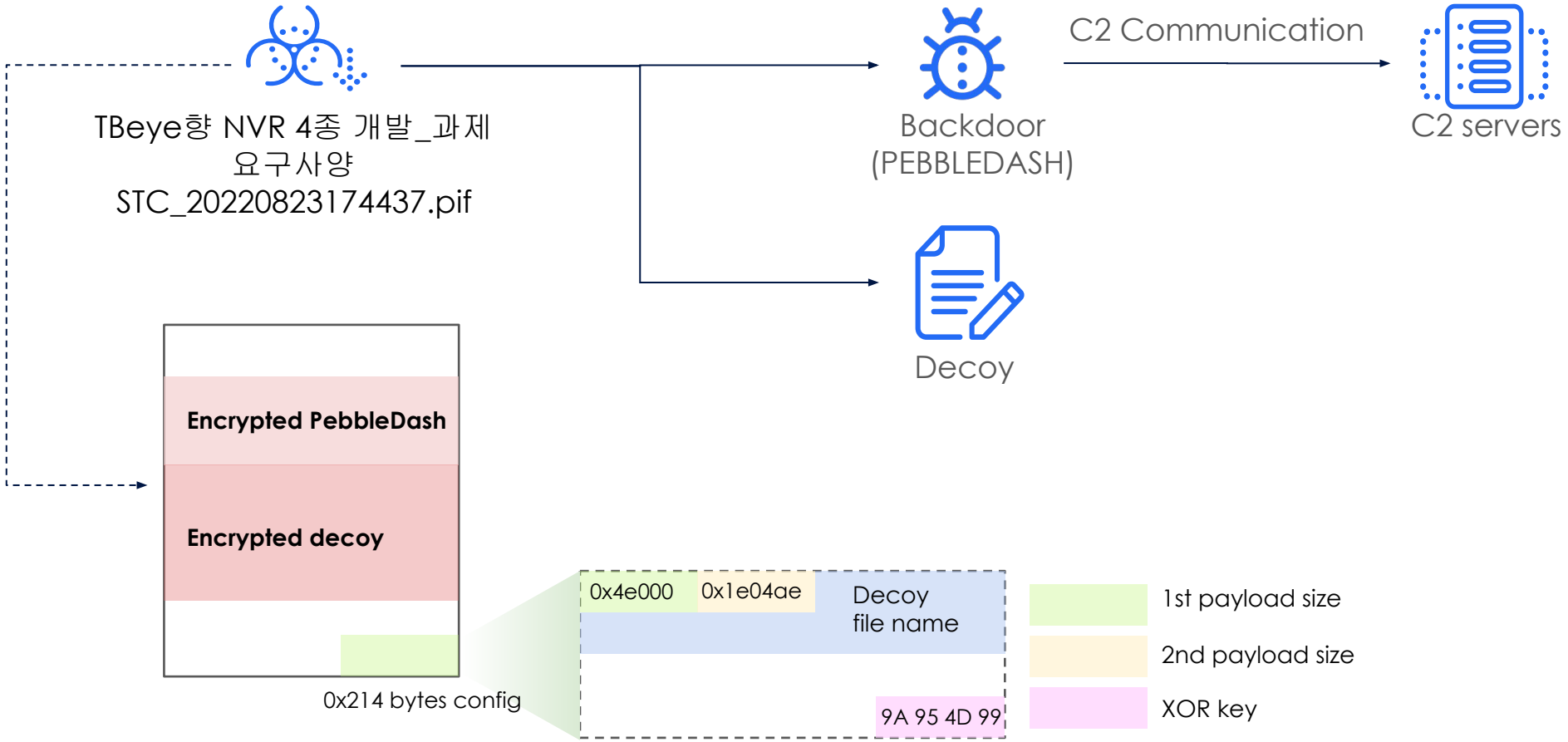


Case #3

Reshuffling Tools and Personnel: Attribution Pitfalls

Initial PEBBLEDASH research

- In August 2022, a suspicious malware was discovered deploying a known implant called PEBBLEDASH.
- The payload had previously been attributed to the Lazarus Group by CISA, based on earlier campaigns.
- Ambiguous points: Initial infection vector and C2 infrastructure deviated from the Lazarus's tradecraft and operational patterns.



Initial PEBBLEDASH research

Early stage confusion on attribution

Connection with Lazarus group

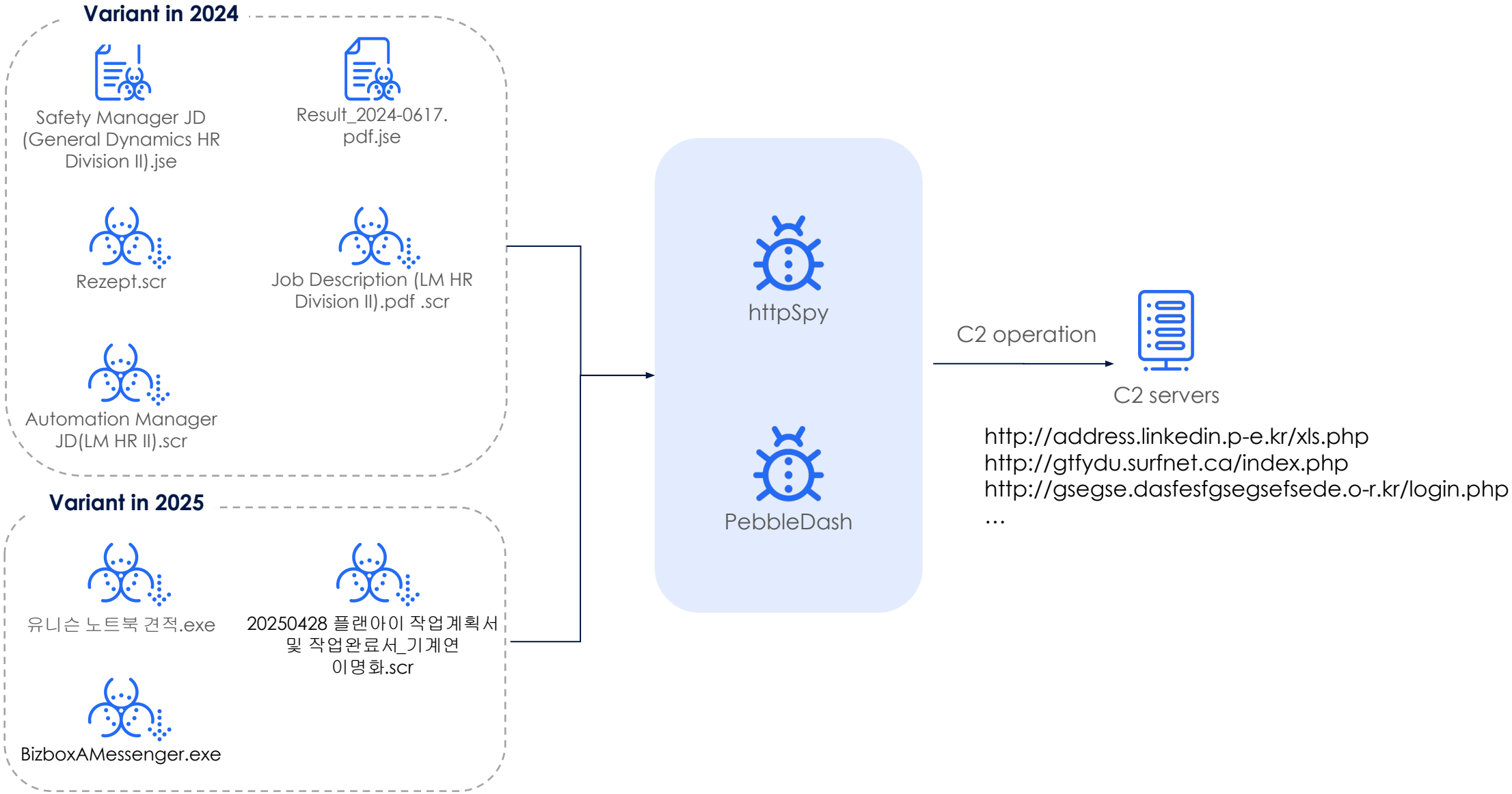
- PEBBLEDASH shares a highly similar configuration and execution structure with legacy malware samples previously attributed to the Lazarus Group.
- The malware was formally attributed to Lazarus Group by CISA
- The defense sector, a long-standing target of Lazarus operations, was among the primary targets in this campaign.

Connection with Kimsuky group

- The C2 domain used in this case `address.linkedin.p-e[.]kr` has been historically associated with the Kimsuky, suggesting possible overlap.
- PEBBLEDASH contained a previously unused key string, which was identical to one used in past Kimsuky malware for decrypting embedded strings, indicating potential code reuse or cross-group development.

Ongoing Campaign Activities

Heavily targeted defence sectors



C2 Investigation

Attribution hints toward Kimsuky based on C2 analysis

Example of email content

```
{
    template: "contents/content (test).php",
    subject: "금주 업무보고 드립니다.", (This week's work report.)
    content: " 오늘 상담드립니다. 참고하시기 바랍니다.", (Please note)
    from: "백업센터" (Backup center)
}
```

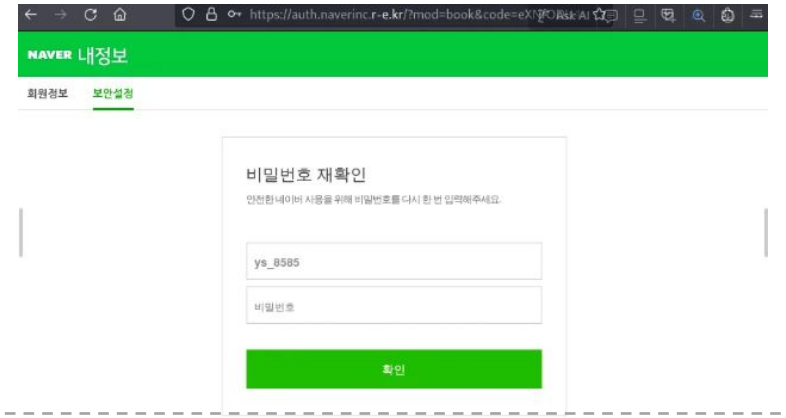
Mis-configured C2 server

Index of /

Name	Last modified	Size	Description
chaos.php	2025-04-03 01:58	1.6K	
chaos_old.php	2025-04-03 01:58	4.2K	
chaos_subject.php	2025-04-03 01:58	1.5K	
contents/	2025-04-03 01:59	-	
resend_.php	2025-04-21 12:27	4.6K	
tinyurl.php	2025-04-03 01:58	3.0K	
url.txt	2025-04-23 14:39	10K	

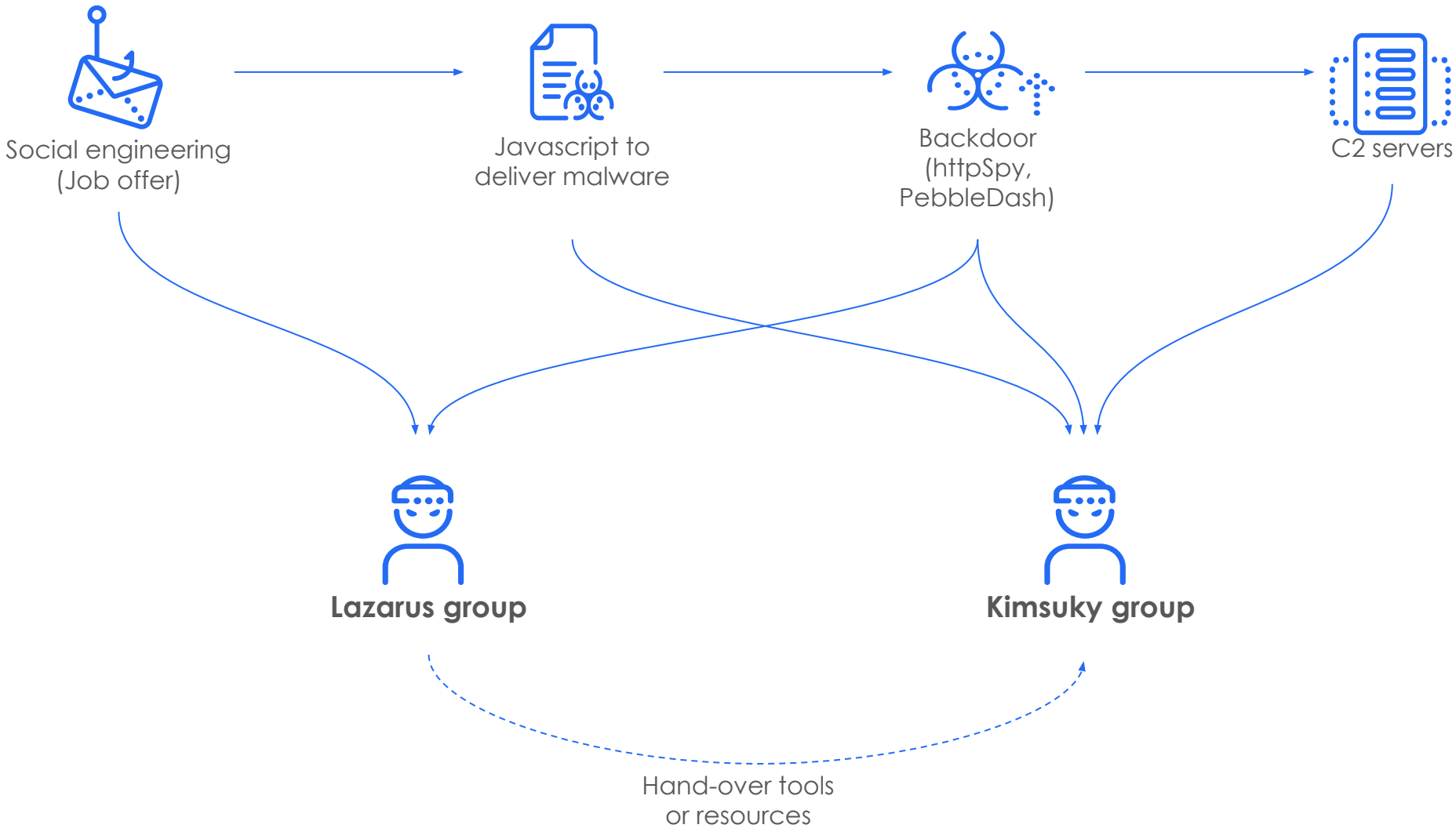
More than 400 shorten URLs for phishing

Shorten URLs	Original URLs	Email ID
hxxps://buly[.]kr/uTnE2J	hxxps://secure[.]naverdomain[.]r-e[.]kr/?mod=book&code=dG1na[redacted]=&back=security&c9GRB=ooMjtMFYnpcTd3FUV3u2AaFkWSoVwj	tm[redacted]05
hxxps://buly[.]kr/FLXvf9J	hxxps://secure[.]naverdomain[.]r-e[.]kr/?mod=book&code=Y2hhaX[redacted]&back=security&qfH3b=vsmjhYs9KCL6veD4FjsOONXcOCsp5R	chairman_[redacted]
hxxps://buly[.]kr/ESy8l3Z	hxxps://secure[.]naverdomain[.]r-e[.]kr/?mod=book&code=a2FyZX[redacted]&back=security&R50FF=vwcYEtU9bkbwm7dAvU26rEMCiERTYy	kar[redacted]00



Summary

Attribution of this campaign



Reshuffling Tools and Personnel: Attribution Pitfalls

Key Takeaways

Tool reuse across DPRK units signals internal resource reallocation

- The reemergence of PEBBLEDASH malware indicates either reassignment of developers or intentional tool sharing among DPRK cyber units.
- Such cross-unit reuse reflects an adaptable operational model, where tools are shared assets, not unique group signatures, complicating attribution based solely on malware origin.

Attribution requires full-chain analysis beyond malware

- As malware tools are reused across threat actors, attribution based solely on tool signatures risks misclassification.
- Effective attribution requires analyzing the full attack chain including delivery, behavior, and post-exploitation to accurately identify threat actors and track evolving tactics.

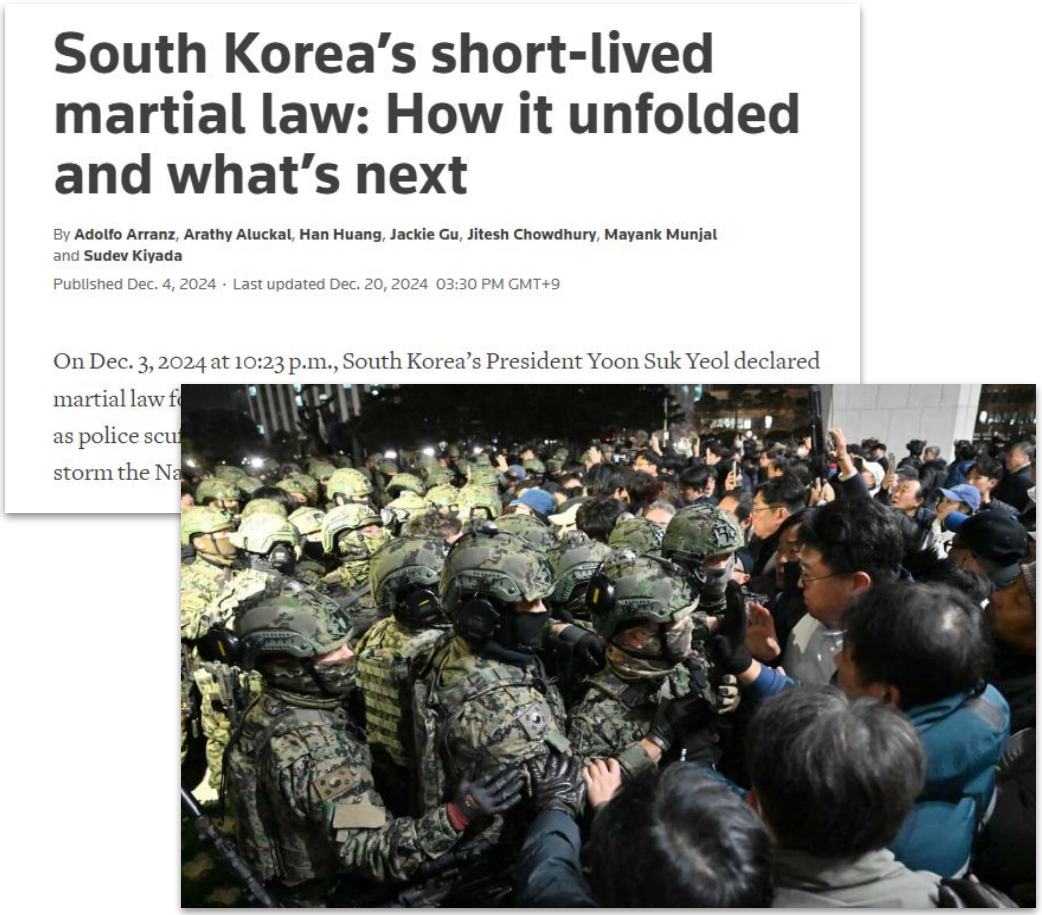
Case #4

Emergence of New Actors: The Unpredictable Variable

Quickly adopted Social Engineering attack

Political issue and quickly adapt it for social engineering attack

- On 3 December 2024, at 22:27 KST, the then-president of South Korea, declared martial law.

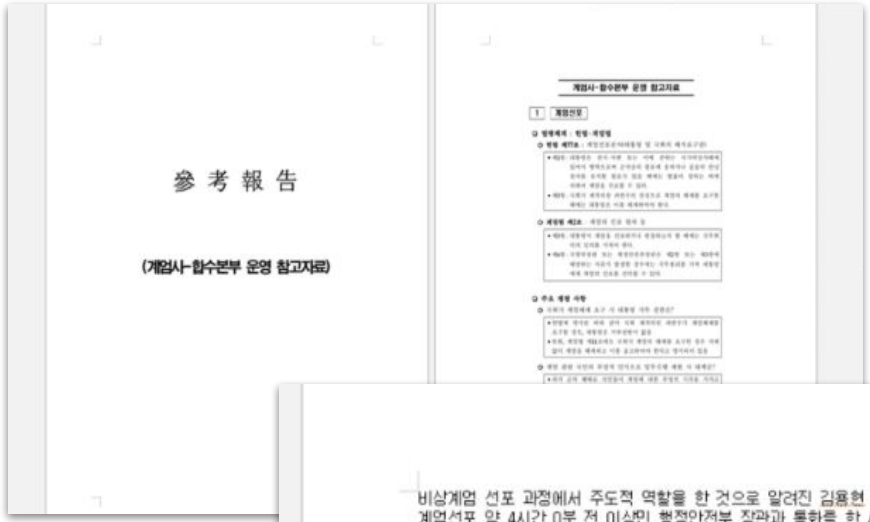

South Korea's short-lived martial law: How it unfolded and what's next

By Adolfo Arranz, Arathy Aluckal, Han Huang, Jackie Gu, Jitesh Chowdhury, Mayank Munjal and Sudev Kiyada

Published Dec. 4, 2024 · Last updated Dec. 20, 2024 03:30 PM GMT+9

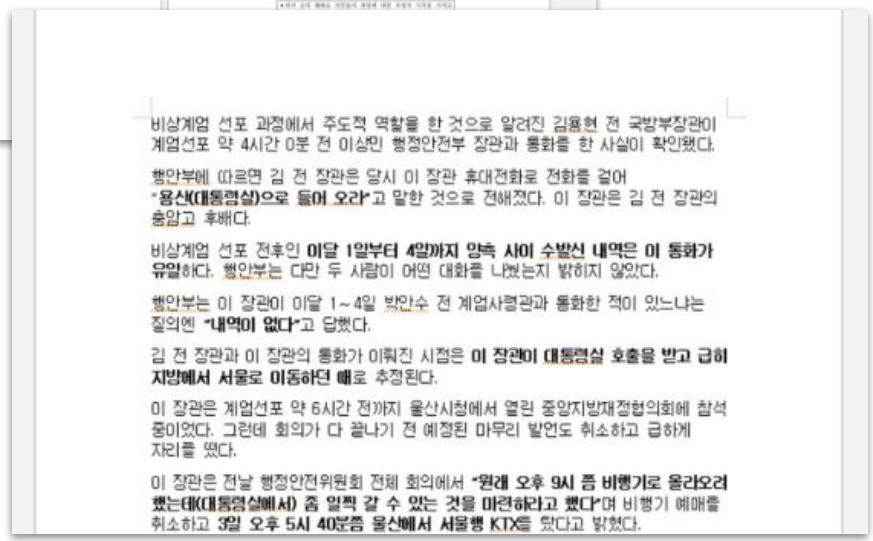
On Dec. 3, 2024 at 10:23 p.m., South Korea's President Yoon Suk Yeol declared martial law f
as police scu
storm the Na

- On December 8, 2024, a spear-phishing campaign was launched using the related content.


參 考 報 告

(계엄사-합수본부 운영 참고자료)

Reference Materials for the Operation of the Joint Investigation Headquarters of the Martial Law Command


비상계엄 선포 과정에서 주도적 역할을 한 것으로 알려진 김용현 전 국방부장관이 계엄선포 약 4시간 0분 전 이상민 행정안전부 장관과 통화를 한 사실이 확인됐다.

행안부에 따르면 김 전 장관은 당시 이 장관 휴대전화로 전화를 걸어 "**용산(대통령실)으로 들어 오라**"고 말한 것으로 전해졌다. 이 장관은 김 전 장관의 충암고 후배다.

비상계엄 선포 전후인 **이달 1일부터 4일까지 양측 사이 수발신 내역은 이 통화가 유일**하다. 행안부는 다만 두 사람이 어떤 대화를 나눴는지 밝히지 않았다.

행안부는 이 장관이 이달 1~4일 박안수 전 계엄사령관과 통화한 적이 있느냐는 질의엔 "**내역이 없다**"고 답했다.

김 전 장관과 이 장관의 통화가 이뤄진 시점은 **이 장관이 대통령실 호출을 받고 급히 지방에서 서울로 이동하던 때**로 추정된다.

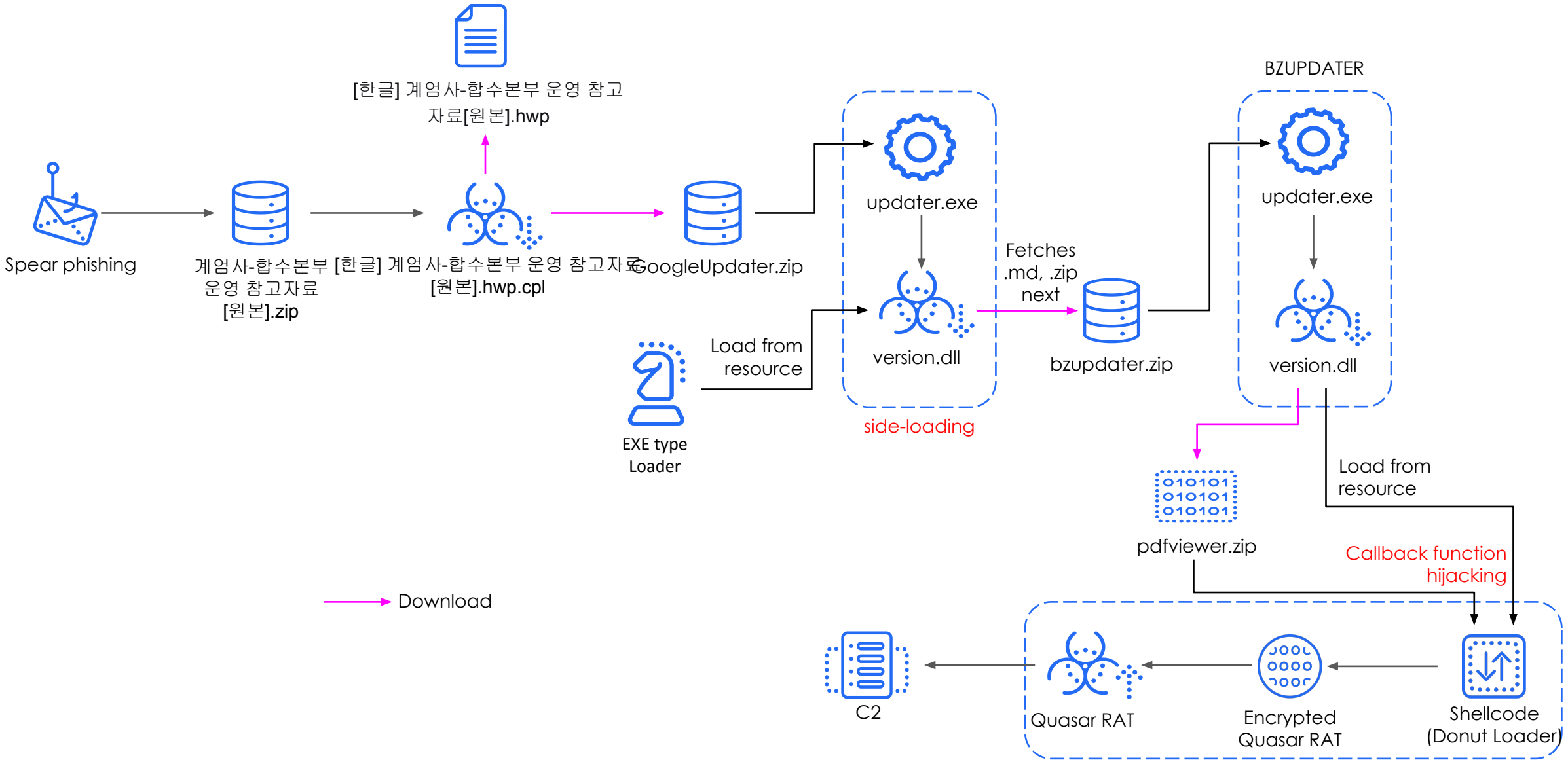
이 장관은 계엄선포 약 6시간 전까지 울산시청에서 열린 중앙지방재정협의회에 참석 중이었다. 그런데 회의가 다 끝나기 전 예정된 마무리 발언도 취소하고 급하게 자리를 뜬다.

이 장관은 전날 행정안전위원회 전체 회의에서 "**원래 오후 9시 쯤 비행기로 올라오려 했는데(대통령실에서) 좀 일찍 갈 수 있는 것을 마련하라고 했다**"며 비행기 예매를 취소하고 **3일 오후 5시 40분쯤 울산에서 서울행 KTX**를 탔다고 밝혔다.

The content of the '30-second call' 4 hours before martial law

Infection Chain

Sophisticated chain with public tools and techniques



An Unprecedented Infection Chain and Limitation

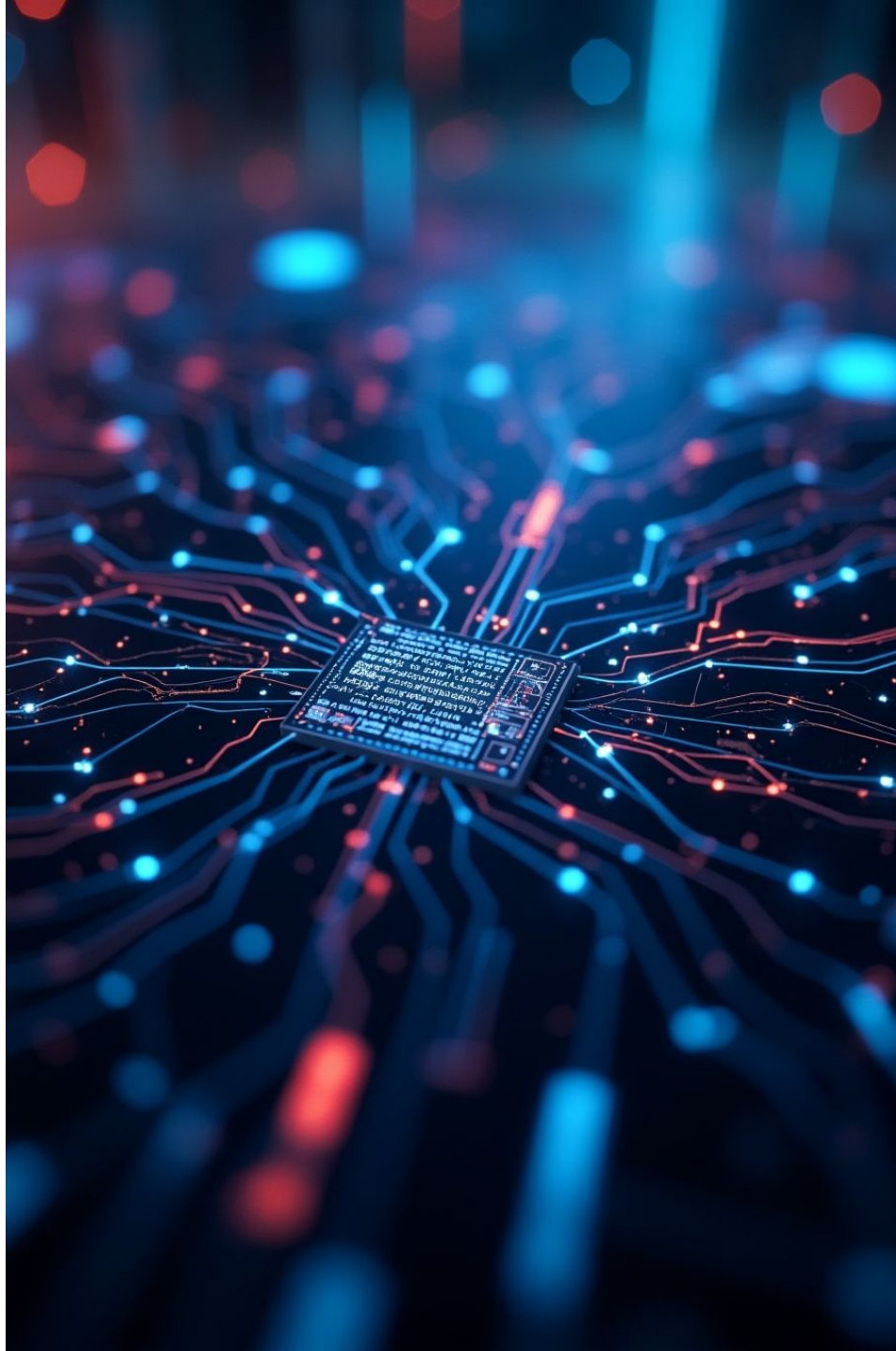
Intriguing points

Uses a known information stealer as its core component

- Adopted Taurus Stealer code introduced since mid 2020.
- Developed and sold by the “Predator the Thief” group on underground forums and used by this campaign suddenly.
- Most of the samples are already detected by the majority of antivirus

Utilized publicly available tools, Donut Loader and Quasar RAT

- Donut Loader is used to generate shellcode that loads and executes Windows payloads in memory with parameters.
- The final payload used to control the victim is the publicly available Quasar RAT



Understanding Attribution with Limited Evidence

Working path

- Malware has a PDB path with the internal name is `**Sewiz**`.
- Malware build path:
  F:\2024**work**\Sewiz\Sewiz\Release\DllProxy.pdb

Familiar with Korean

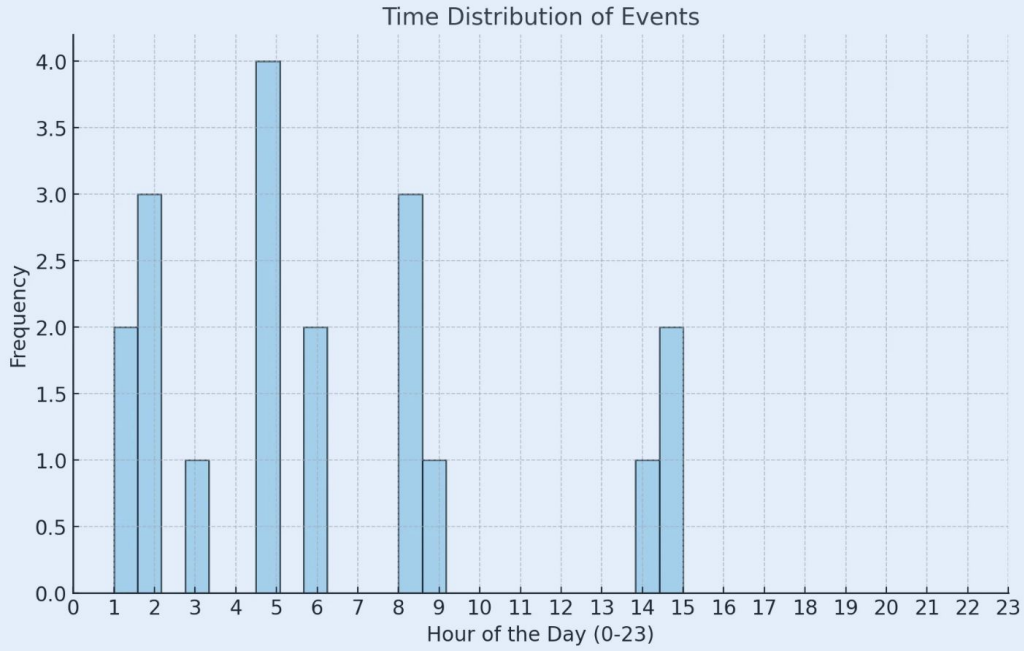
- Korean resource

9e94126e8a26efd10b2a5b179d64be90	VERSION.DLL	Contained KOREAN Resources
ca93591a9441a2ade70821f67292d982	VERSION.DLL	Contained KOREAN Resources

- Utilized BandiZip for side-loading

Timezone

- Working time zone: GMT +8 ~ +9



Emergence of New Actors: The Unpredictable Variable

Key Takeaways

State-Backed threat actors can emerge without prior attribution footprints

- The emergence of a previously untracked group in December 2025 shows that state-backed cyber units can surface without clear lineage or historical overlap.
- These actors lack behavioral baselines, making attribution difficult and pushing analysts to rely on contextual clues such as geopolitical timing and strategic intent.

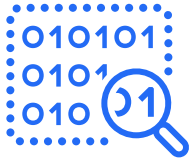
Attribution bias toward known actors can lead to misclassification

- Analysts often default to attributing novel incidents to known threat groups, introducing attribution bias that can obscure the emergence of new actors or structural changes within existing ones.
- Accurate attribution in such cases demands restraint from premature conclusions and a focus on objective indicators including novel tooling, targeting patterns, and operational context.

Takeaways

The structure of threat actors are evolving like modern teams

- Expanding in size with specialized subgroups
- Dynamically re-allocating tools and personnel across units
- Collaborating across teams to achieve shared objectives
- Introducing new members or units



Full-context based conclusion is the key

- Hit-and-run style defense never works
- Need to understand full-context of threats
- Diversify defense points

Cooperation with other industry

- Each sector has different strength
- Cooperation is essential to cope with the latest cyber threats

Thank you

spark@zscaler.com

@unpacker