How AI can be used by attackers and defenders?

Seongsu Park,
Lead security researcher @ GREAT

kaspersky

Seongsu Park

- Kaspersky, Global Research and Analysis Team
- Lead security researcher
- Tracking targeted attacks focused on APAC
- Tracking Korean-speaking actors

Focus Area

- Investigative Research
- Reversing Malware
- Digital Forensics
- Threat Intelligence

APT threat landscape 2022

Kaspersky's Global Research and Analysis Team (GReAT) is well-known for the discovery and analysis of the most advanced cyberthreats. According to our data, in 2022 the top APT targets were governments and the most significant threat actor was Lazarus.

Top 10 targets

- Government
- Military
- Diplomatic
- IT companies
- Educational
- Telecommunications
- Media
- Software Development
- Manufacturing
- Logistics

Top 10 significant threat actors

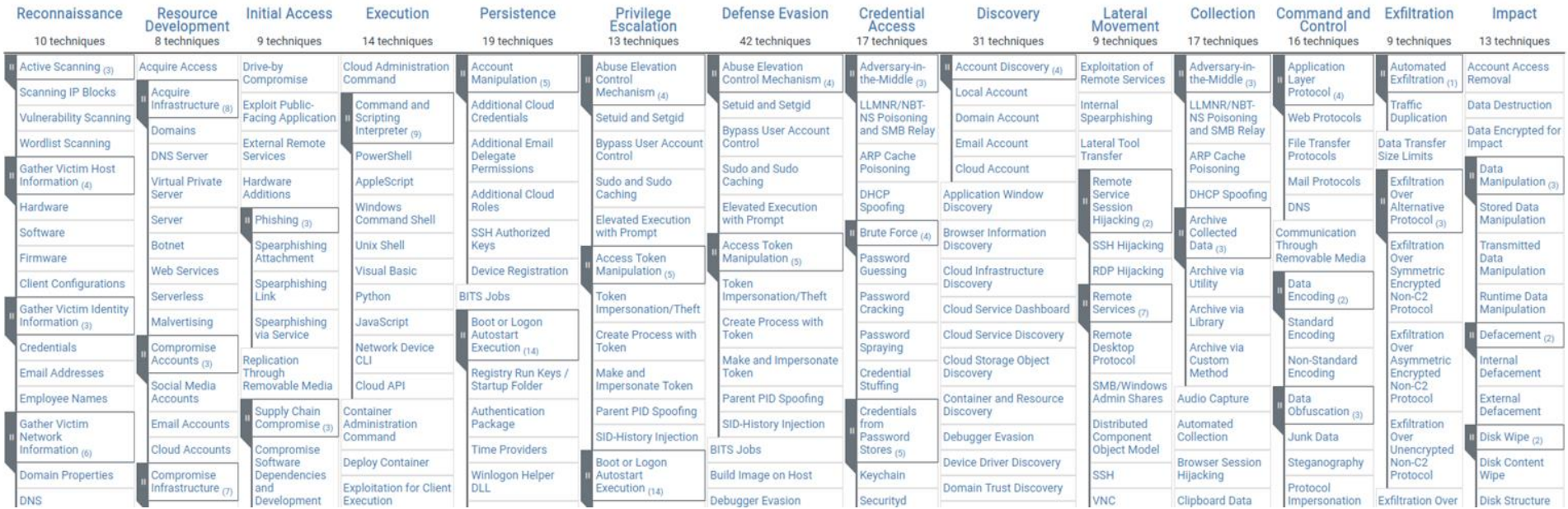
1. Lazarus
2. APT10
3. Kimsuky
4. ZexCone
5. Tomiris
6. Ghostwriter
7. DeathStalker
8. BitterAPT
9. SideCopy
10. Gelsemium

Top 12 targeted countries

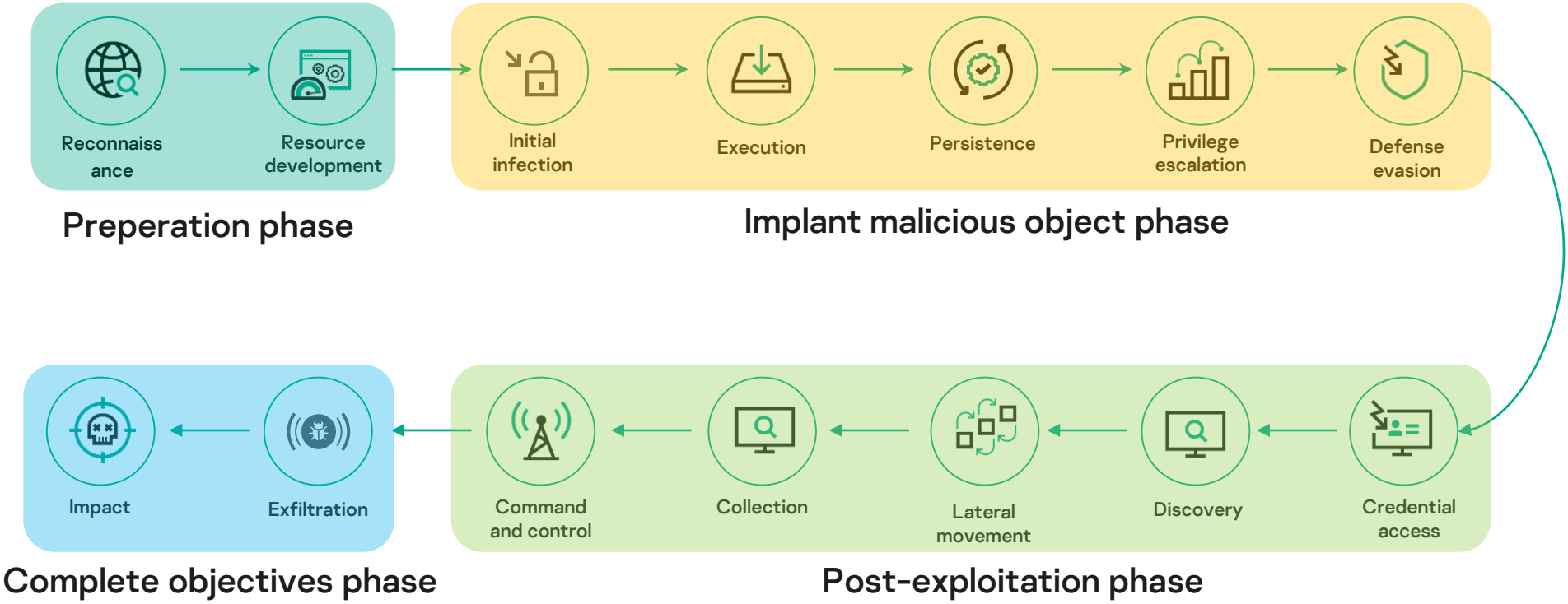
GREAT

kaspersky

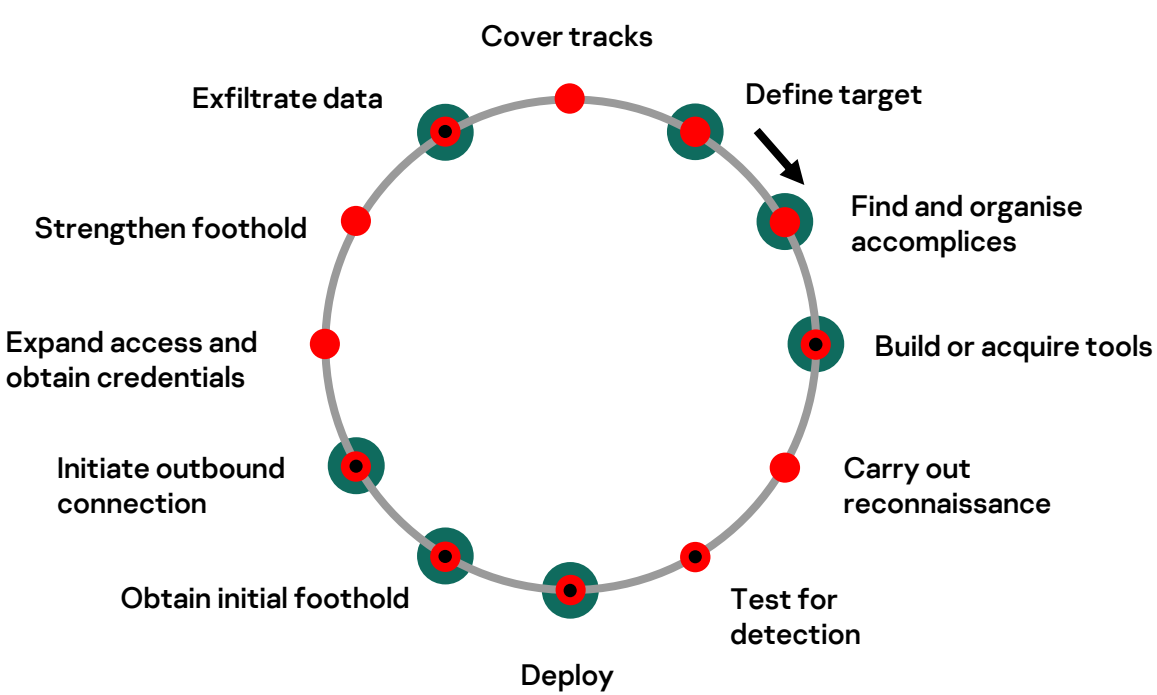
ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge



MITRE ATT&CK phase



The threat life-cycle

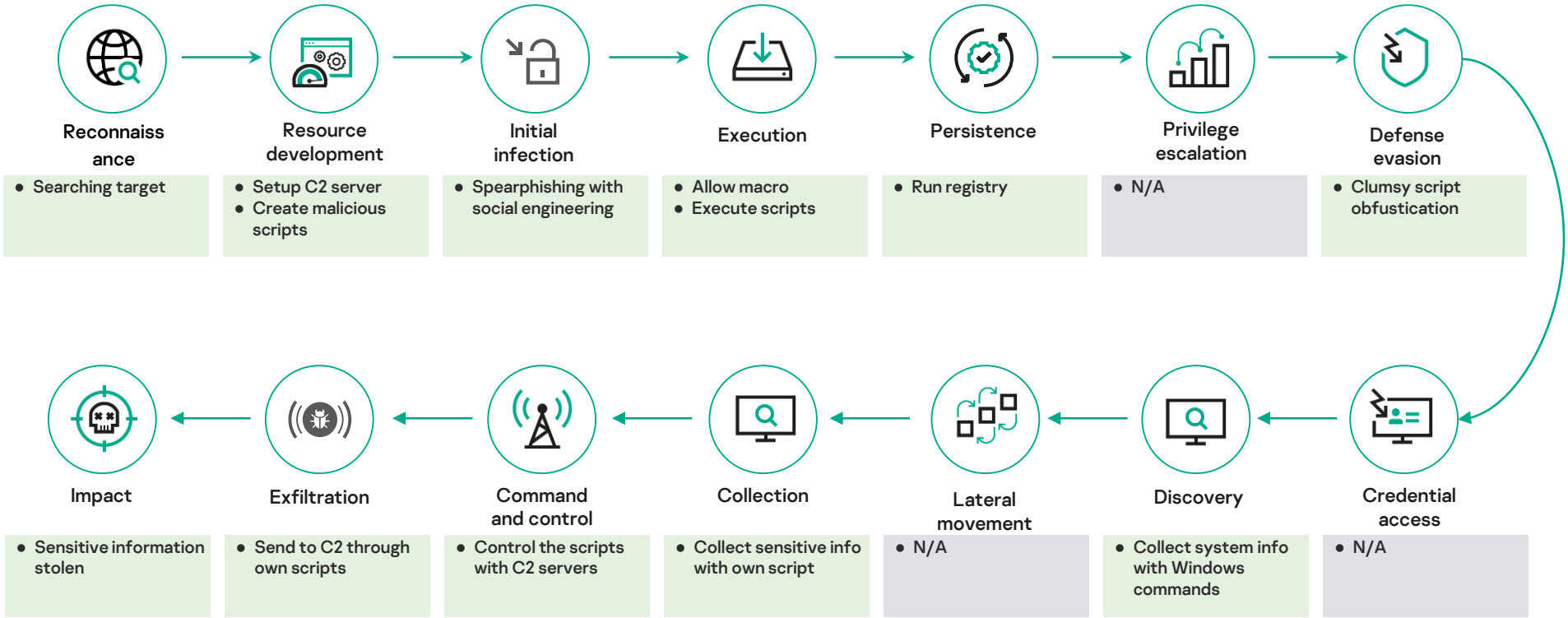


GREAT

kaspersky

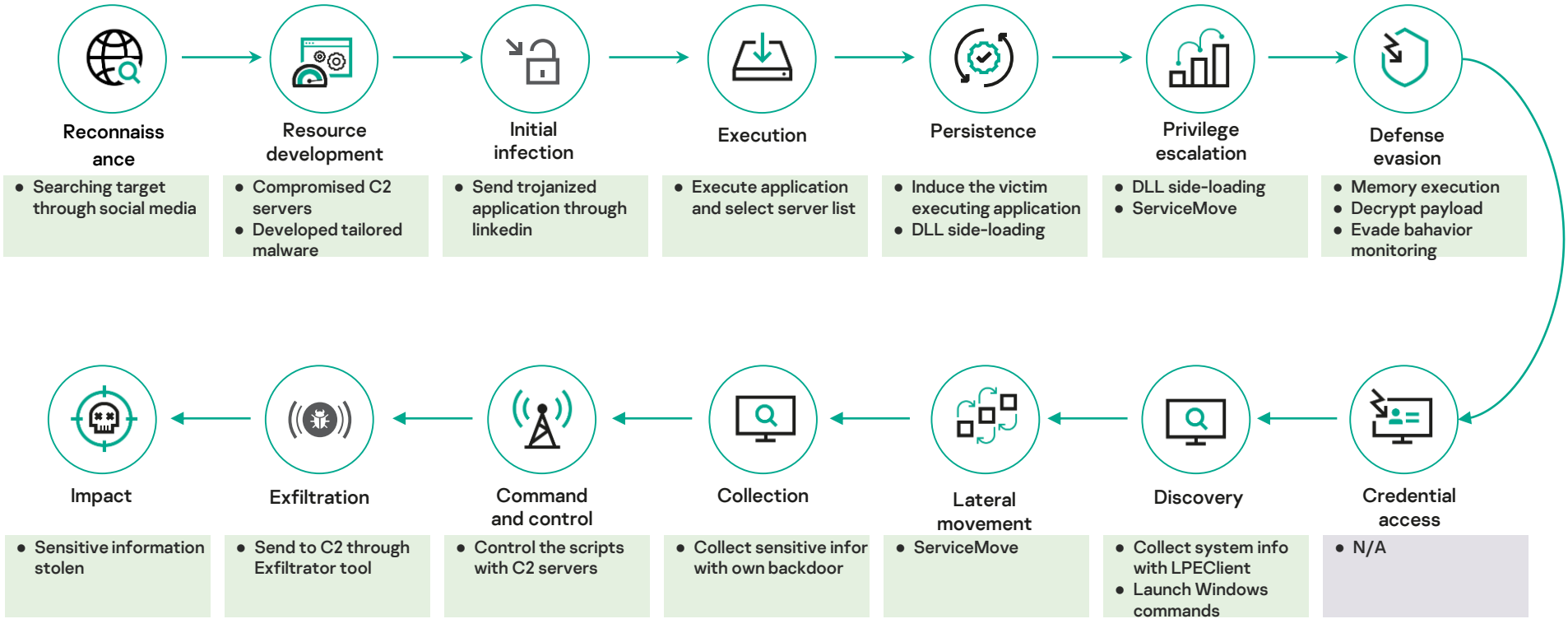
APT attack case - Kimsuky

Operation GoldDragon: Targeting North Korea-related individuals



APT attack case - Lazarus

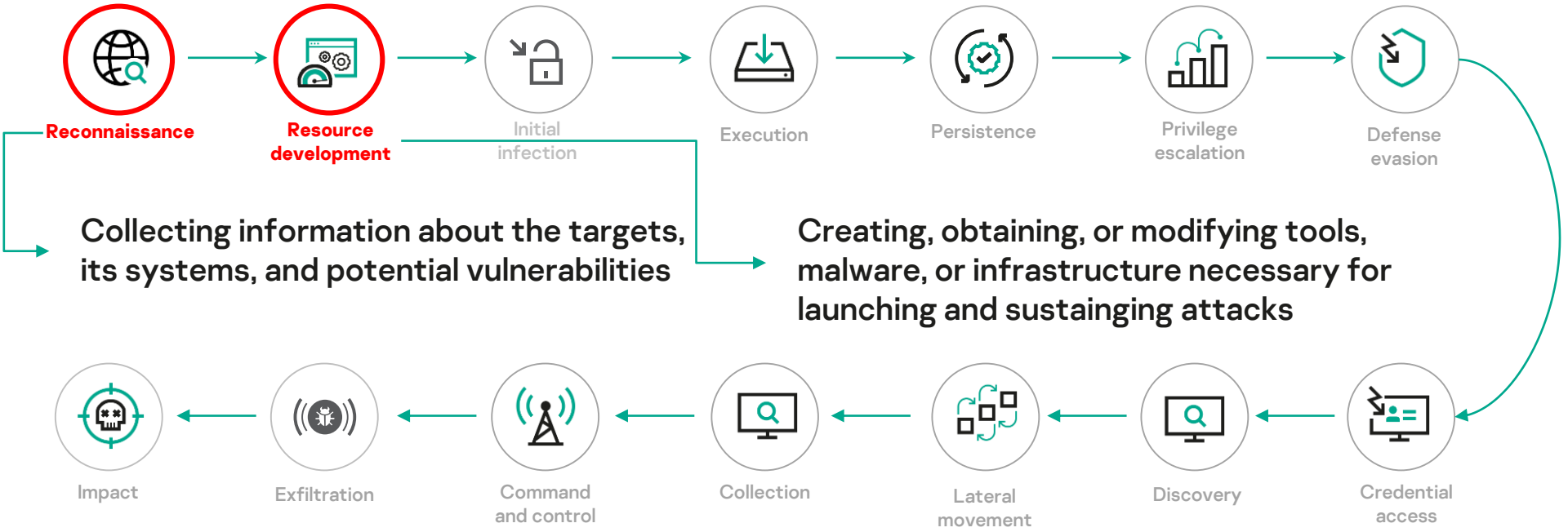
Operation DreamJob: Targeting employees of defense contractor and nuclear engineer




How artificial intelligence can support threat actors?

APT actors in APAC in 2023

APT attack process: Reconnaissance, Resource development



APT actors in APAC in 2023

Acquire Infrastructure: Domains
Acquisition of domains with a preference for Namesilo as a provider.

Acquire Infrastructure: Virtual Private Server
Acquisition of VPS with a preference for BLNWX as a provider.

Establish Accounts: Social Media Accounts
Creates social media accounts such as LinkedIn, Whatsapp, and Telegram to contact targets.

Compromise Infrastructure: Web Services
Compromised vulnerable Wordpress websites uploading actor's scripts.

- GoldenJackal
- ToddyCat
- Bitter
- Tomiris
- Andariel
- DreamLand
- HoneyMyte
- BlueNoroff
- ScarCruft
- Winnti
- Lazarus
- OrigamiElephant
- MuddyWater
- Mysterious Elephant

Find potential targets:
Automating the analysis of data from various sources such as online databases and social media platforms

Understand each potential target:
Collect information about the target's personnel, systems and applications used in their environment

Find potential entry points:
Employees details, third-party relationships, Network architecture and vulnerable systems and softwares

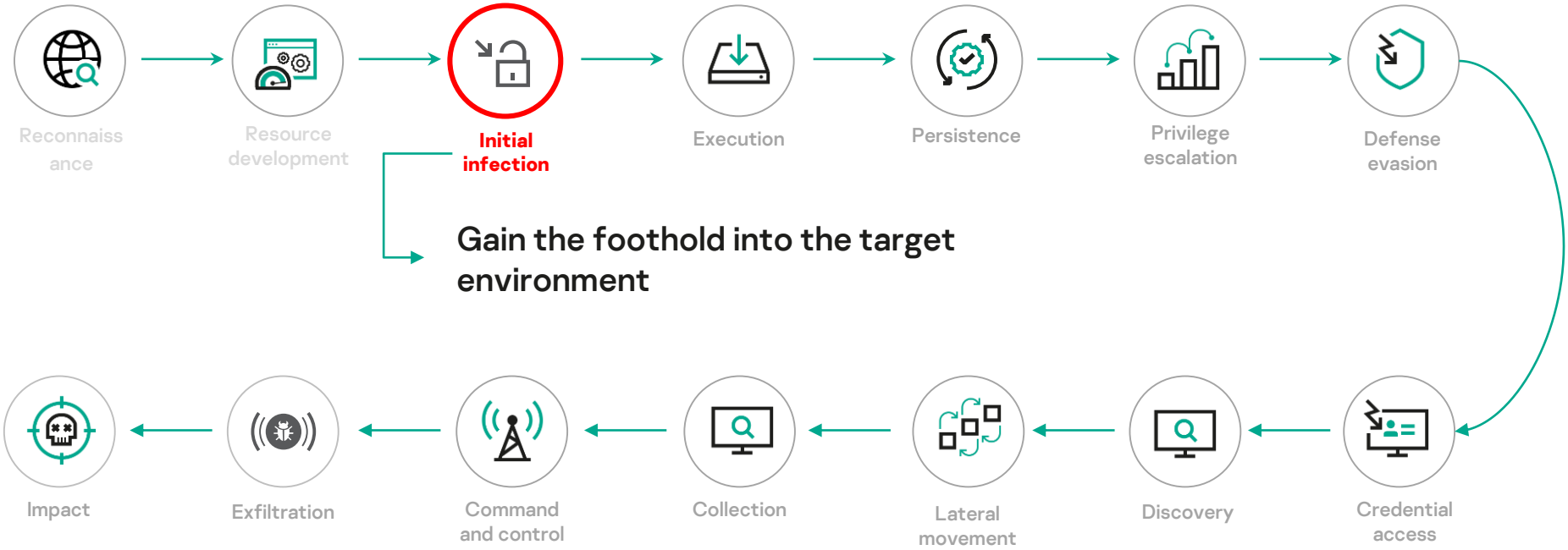
Malware Development:
AI can be utilized in creating or acquiring tools

- Automation of exploit development
- Development of advanced malware
- Gathering tools from various sources more effectively

Infrastructure Acquisition:
AI can assist in automating tasks related to building attack infrastructure

- Purchase of network infrastructure
- Creation of accounts
- Compromising network infrastructure
- Compromising accounts

APT attack process: Initial infection

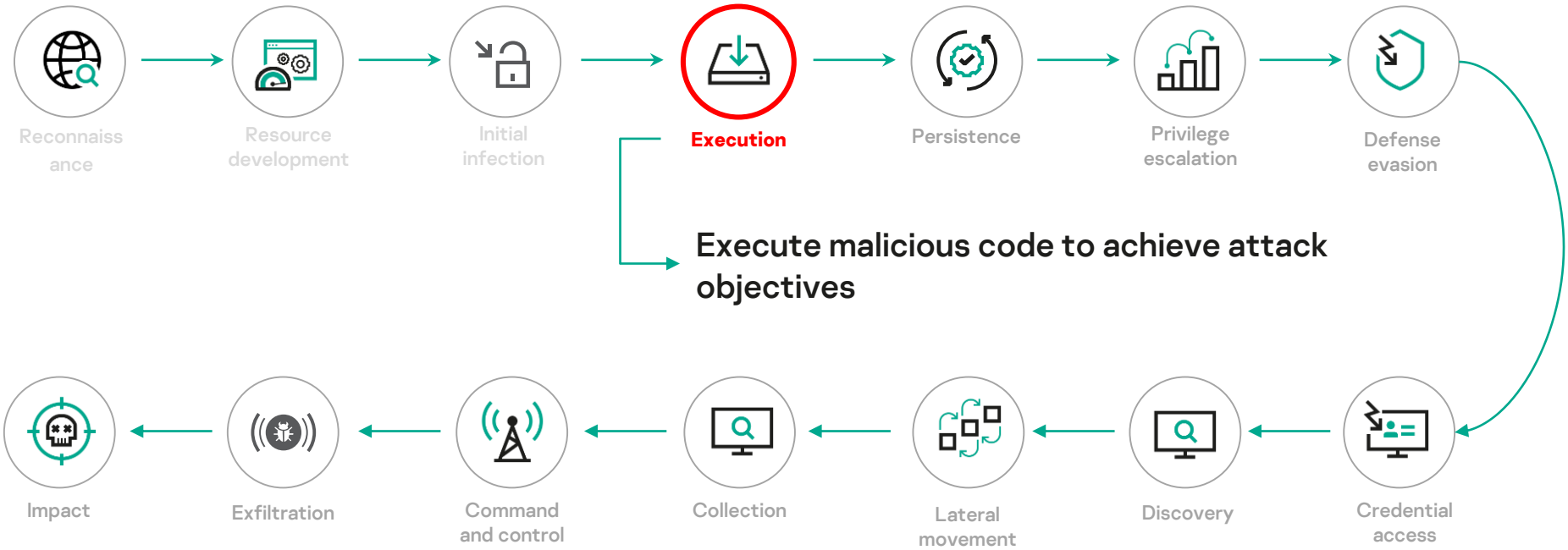


Spearphishing is still the most common initial access tactic for a lot of APT actors

Most effective infection vector:
Effectively find the best entrypoint into target network

Social Engineering:
Craft highly convincing and personalized phishing messages

APT attack process: Execution



APT actors in APAC in 2023

Command and Scripting Interpreter: PowerShell
Command and Scripting Interpreter: Windows Command Shell
Command and Scripting Interpreter: AppleScript
Command and Scripting Interpreter: Visual Basic
Command and Scripting Interpreter: Python
Scheduled Task/Job
Exploitation for Client Execution
User Execution: Malicious File
....

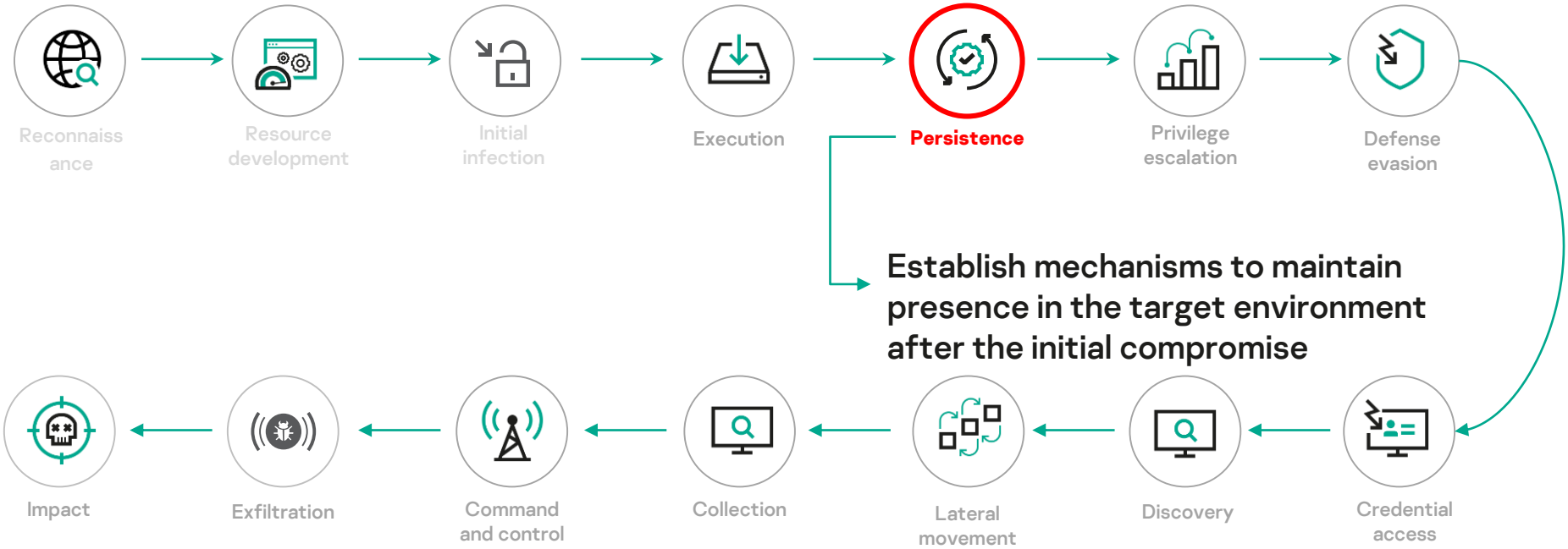
AI-chosen command and scripting interpreter:

Analyzing the target environment, understanding system characteristics, and selecting the most suitable options for running malicious scripts or commands

AI-Enhanced Social Engineering Techniques:

AI-driven social engineering techniques could increase the likelihood of users interacting with malicious files, enhancing the success of the execution phase

APT attack process: Persistence

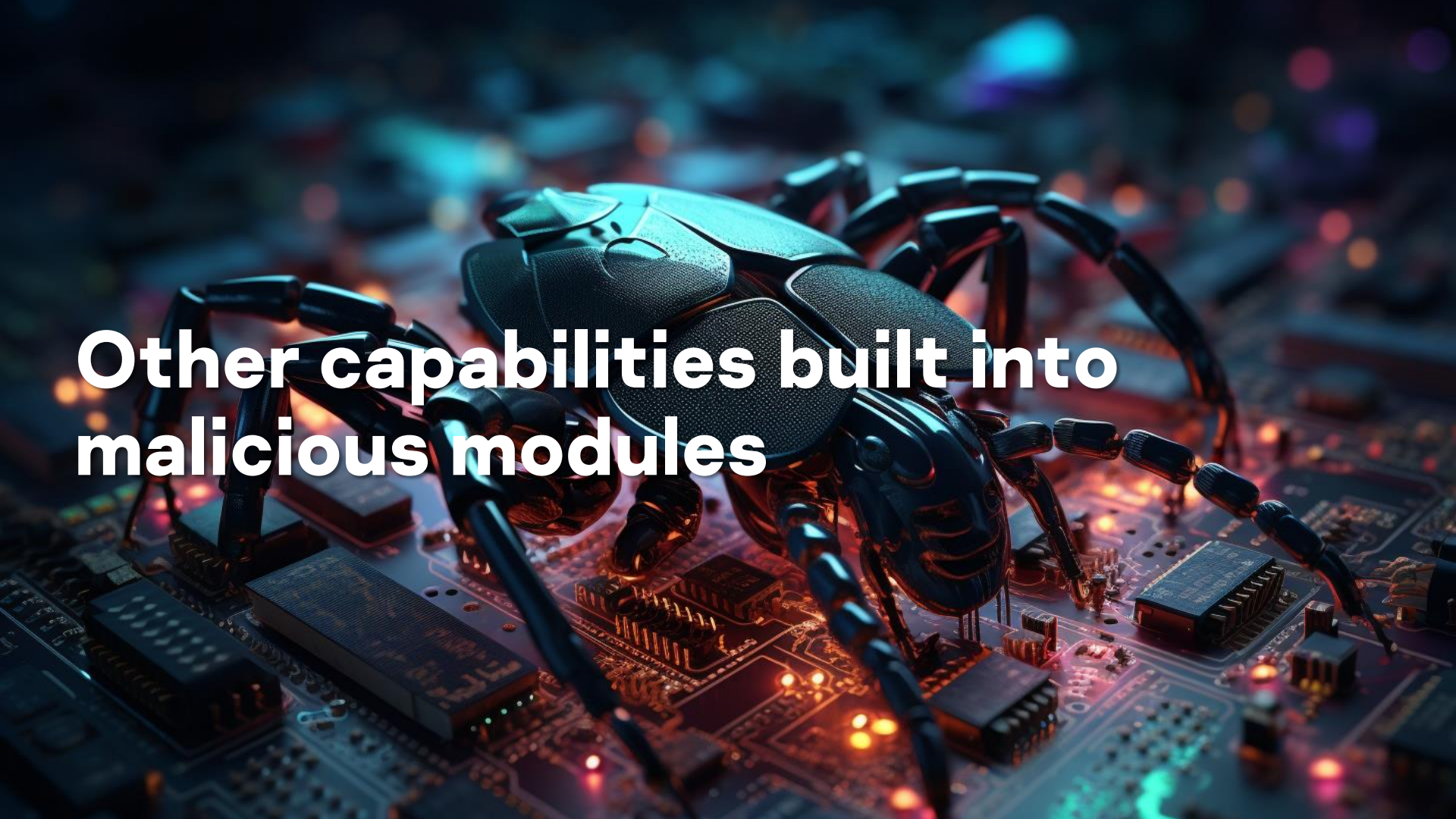


The most common techniques among APT actors to achieve persistence are:

- Scheduled Tasks
- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

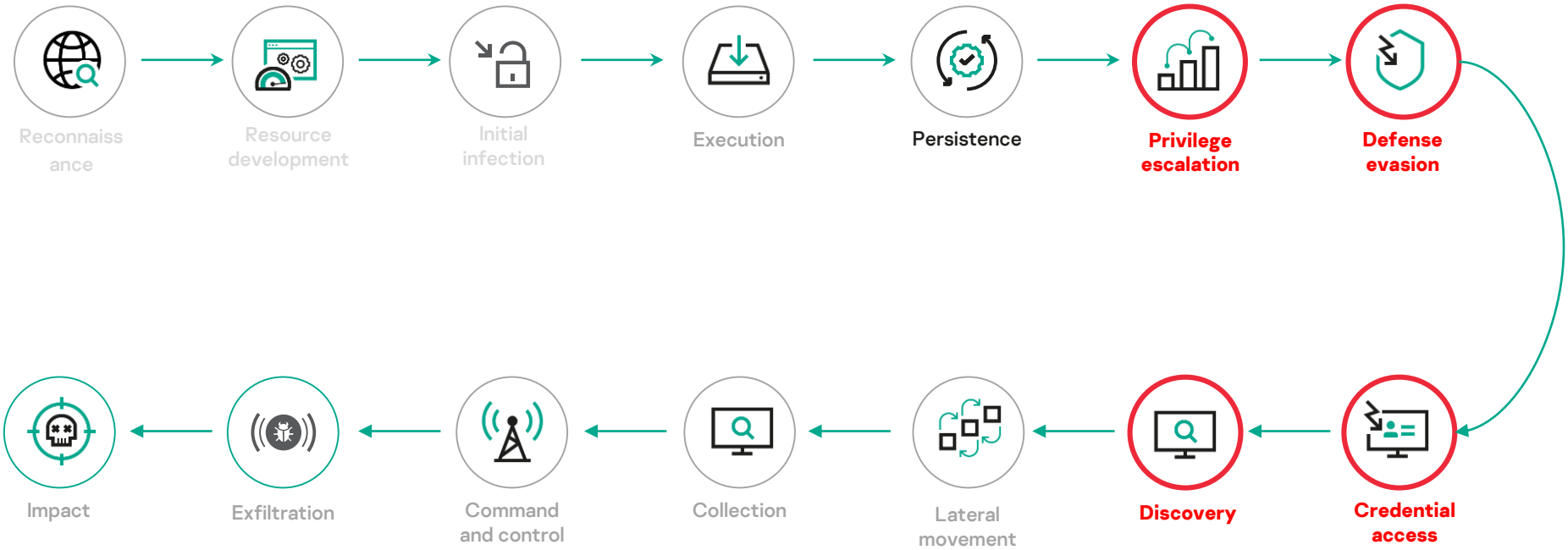
Boot or Log-on Scripts:
Creating the most suitable script to execute the malware based on user behaviour analysis

Registry Manipulation:
Apply AI-guided techniques to manipulate Windows Registry entries to update persistence registry keys and evade detection



Other capabilities built into malicious modules

APT attack process: Post-exploitation



Identification of vulnerable system components:
Utilize AI algorithms to scan the target environment for known vulnerabilities that can be exploited for privilege escalation

AI-Guided Social Engineering:
Combine AI-enhanced social engineering with privilege escalation to manipulate users into granting higher privileges

AI-generated code obfuscation for evading signature-based detection: Dynamically change the code structure of malware to avoid getting detect by signature-based security measures

AI-based detection of security monitoring to avoid detection: Analyzing patterns, behaviors, and data indicative of security activities to strategically adjust tactics to bypass these monitoring efforts

Brute-Force Attacks:
AI can enhance traditional brute-force attacks by intelligently selecting likely passwords based on patterns, dictionaries, and previous breaches, increasing the chances of successful access

Password Guessing:
AI algorithms can analyze patterns in user behavior, social media activity, and personal information to make educated guesses about passwords, increasing the likelihood of success

AI-assisted automated network mapping and scanning:
Explore and map the target network infrastructure to identify available systems, devices, services, and potential vulnerabilities

AI-guided identification of high-value target assets:
Analyze data and patterns within a target environment to determine which assets, data, or systems hold the greatest value for the attacker

Lateral Movement and C2 communication

APT attack process: Persistence

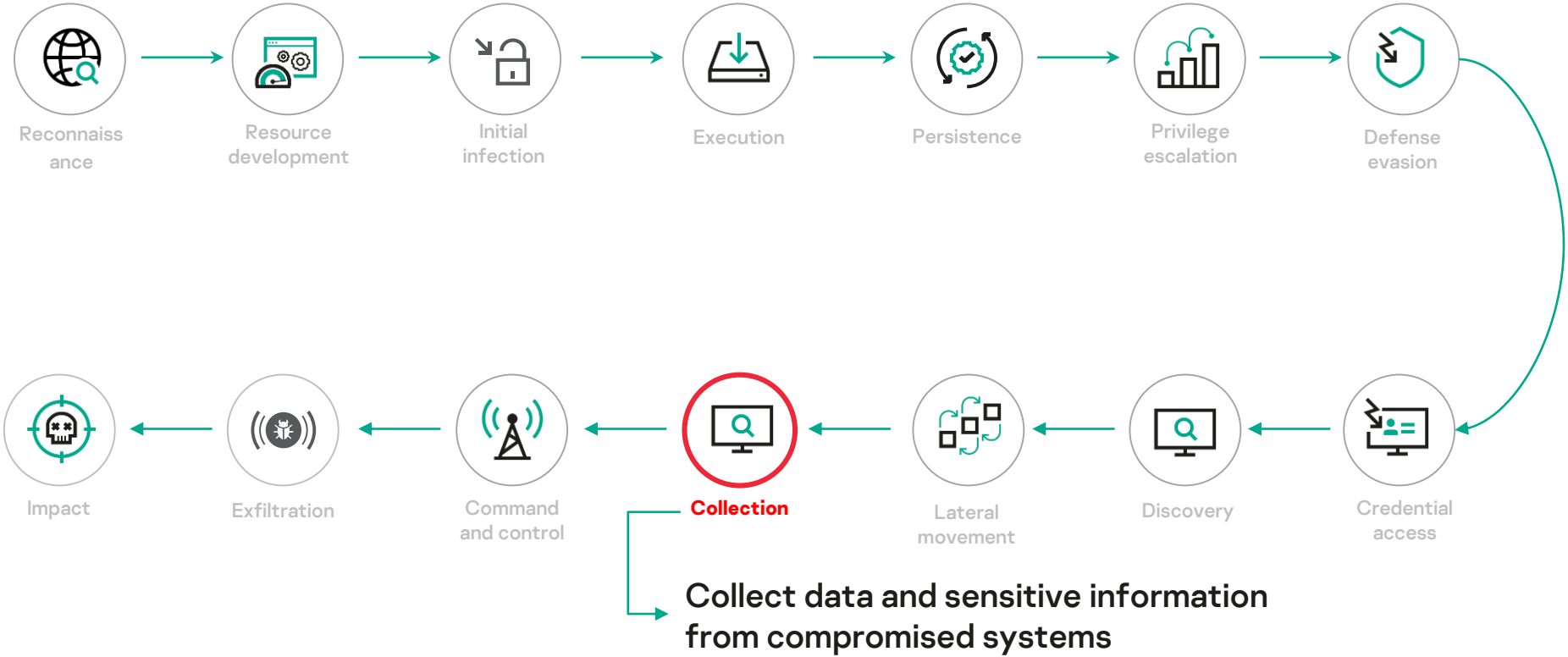
- Compromised user credentials are used to distribute malware across the infrastructure
- The tools were launched on the attacked systems as scheduled tasks


```
schtasks /s <remote_ip> /tn tpcd /u <user_name> /p <user_password> /create /ru system /sc
DAILY /tr "c:\programdata\intel\csd.exe letgo 30" /f

schtasks /run /s <remote_ip> /tn tpcd /u <user_name> /p <user_password> /i

schtasks /delete /s <remote_ip> /tn tpcd /u <user_name> /p <user_password> /f
```

AI-optimized lateral movement patterns to avoid detection:
Explore and map the target network infrastructure to identify available systems, devices, services, and potential vulnerabilities

Mimic user behaviour:
AI can assist in mimicking user behaviour in the lateral movement phase to blend in with usual network activities of the system

APT attack process: Persistence



APT actors in APAC in 2023

Screen Capture:
Take screenshots to gather information

GoldenJackal	BlueNoroff
ToddyCat	ScarCruft
Bitter	Winnti
Tomiris	Lazarus
Andariel	OrigamiElephant
DreamLand	MuddyWater
HoneyMyte	Mysterious Elephant

APT actors in APAC in 2023

Screen Capture:
Take screenshots to gather information

Data from local systems:

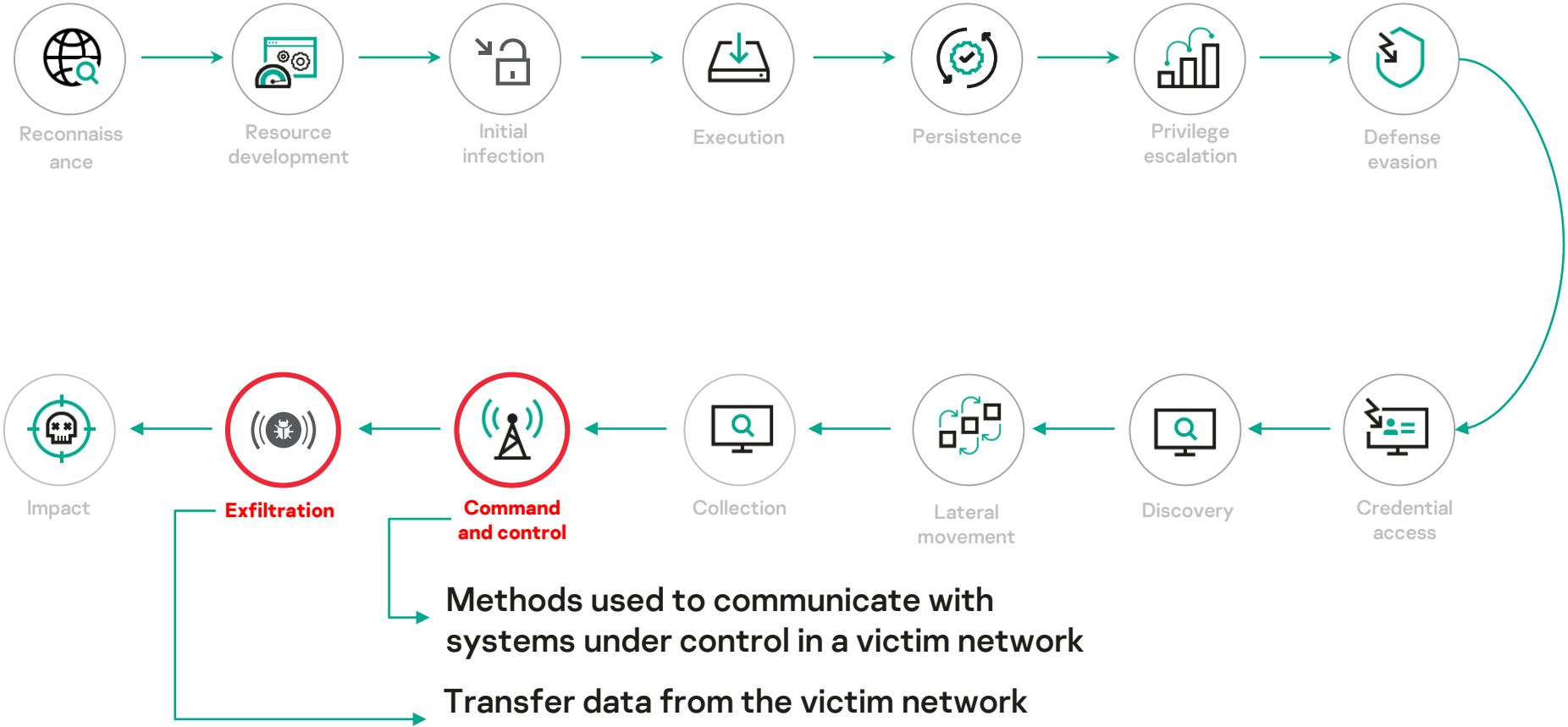
- Collect files and information from local system
- Archive collected data

GoldenJackal	BlueNoroff
ToddyCat	ScarCruft
Bitter	Winnti
Tomiris	Lazarus
Andariel	OrigamiElephant
DreamLand	MuddyWater
HoneyMyte	Mysterious Elephant

AI-guided extraction of specific types of sensitive data:
Identify, locate, and retrieve specific types of valuable or sensitive information from within a compromised system or network

Automated data classification and selection using AI algorithms:
Analyze, categorize, and choose most relevant data sets from extracted data

APT attack process: Command and Control, Exfiltration



Exfiltration Over Web Service: Exfiltration to Cloud Storage

Exfiltration Over Web Service: Exfiltration to Cloud Storage

Exfiltration Over C2 Channel

GoldenJackal	BlueNoroff
ToddyCat	ScarCruft
Bitter	Winnti
Tomiris	Lazarus
Andariel	OrigamiElephant
DreamLand	MuddyWater
HoneyMyte	Mysterious Elephant

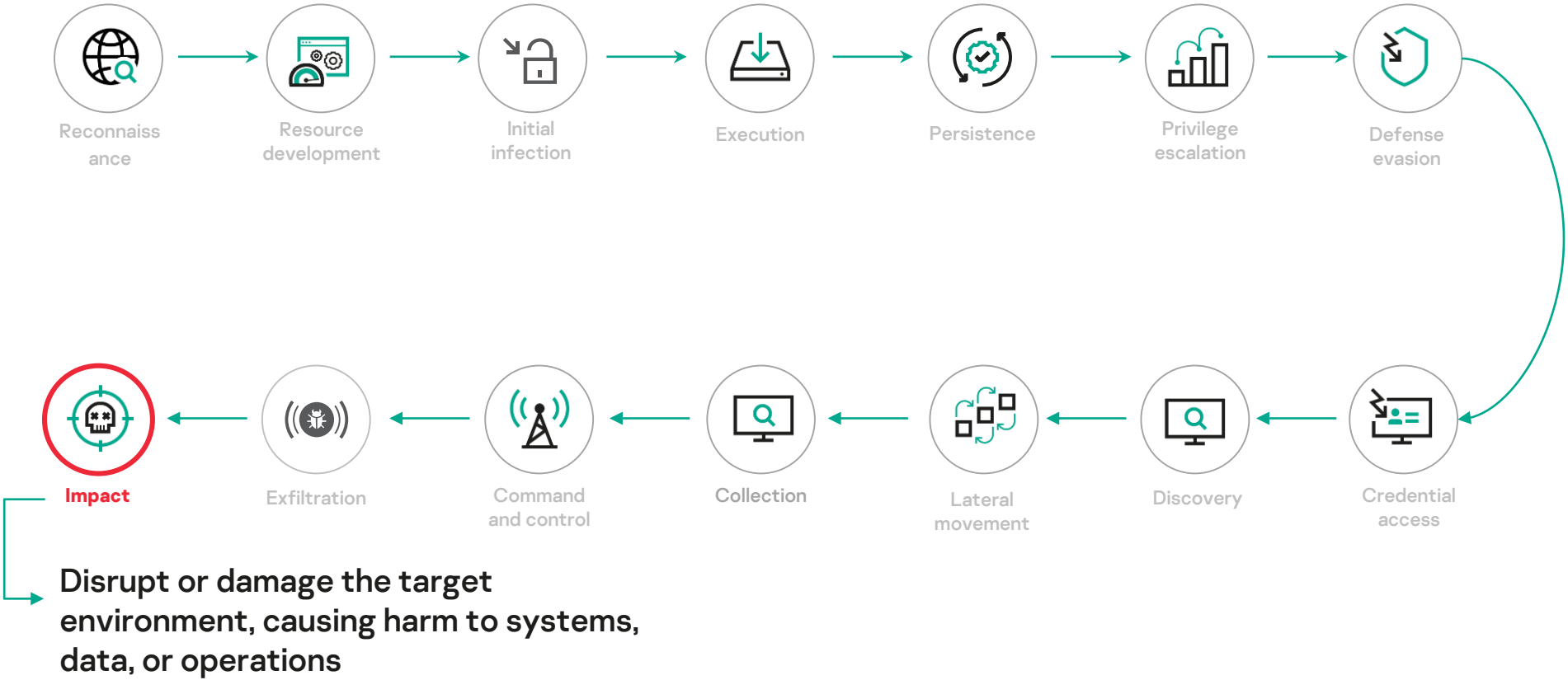
Enhancing the stealthiness, resilience, and adaptability of communication techniques

AI can help to identify the **most suitable communication channel** to exfiltrate data for each victim

Mimic normal user behaviors and interactions to avoid triggering behavioral anomaly detection systems

Dynamically adjust the frequency, timing, and protocols used for C2 communication

APT attack process: Persistence



Disrupt or damage the target environment, causing harm to systems, data, or operations

AI can assist in maximizing the attack impact by enhancing the effectiveness and efficiency of attackers actions

- Choose essential strategies to generate a substantial influence
- AI-assisted target selection to distrupt or wipe
- Maximize damage of company’s reputation

AI can be used in various stages of a cyber attack

AI can be used by attackers in the **reconnaissance** phase of the attack to profile the victims more efficiently.

AI can be used for **social engineering** purposes such as generating more convincing spear phishing emails or fake websites.

AI can be utilized to develop **malware components** with more sophisticated features.

AI can be used to facilitate **exfiltration** of data from victim machines.


How artificial intelligence can support defenders?

Threat Intelligence

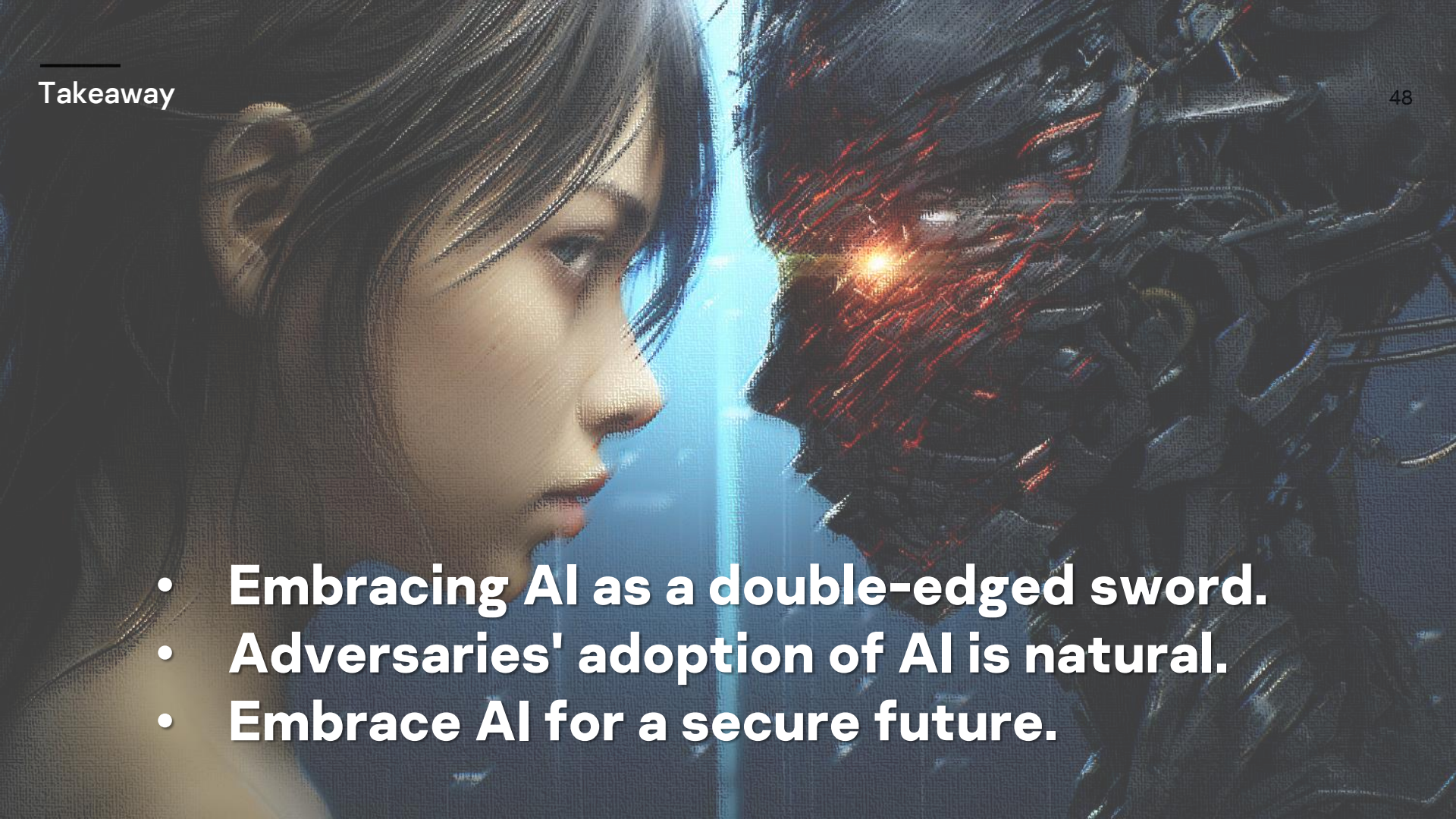
Gathering relevant information about a threat actor is important for researching a threat actor

- Previously published researches
- Previously seen TTP's
- Scrap IoC's
- Craft Threat Hunting Queries
- Develop a Threat Hunting Hypothesis
- Deobfuscate malicious scripts
- Query code of malware to boost analysis
- Create a script for automation

Incident Response

It is important to understand available threat information from security devices to speed up investigation

- Suggest anomaly in provided set of logs
- Understand a security event log
- Generate how a particular security event log may look like
- Suggest steps to looks for initial implant like web shell
- Create useful script to boost analysis



- Embracing AI as a double-edged sword.
- Adversaries' adoption of AI is natural.
- Embrace AI for a secure future.


Question?
@unpacker
seongsup4rk@gmail.com
GREAT
kaspersky