

### Seongsu Park

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

### **Focus Area**

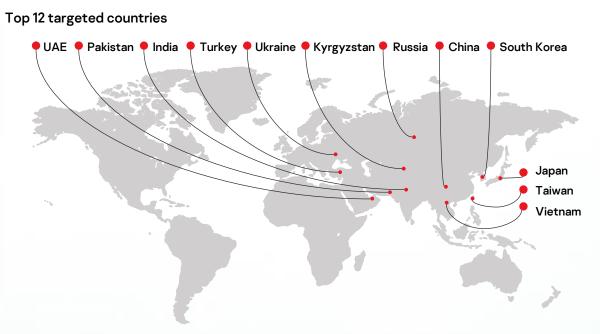
- Investigative Research
- Reversing Malware
- Digital Forensics
- Threat Intelligence



## 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.





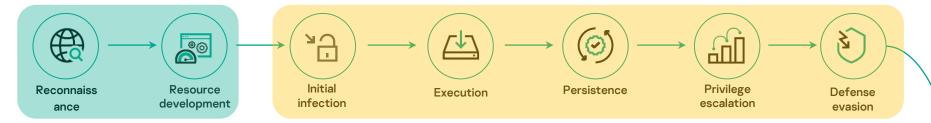
**GREAT** 

kaspersky

MITRE ATT&CK Framework

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

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control	Abuse Elevation Control Mechanism (4)	Adversary-in- the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in- the-Middle (3)	Application Layer	Automated Exfiltration (1)	Account Access Removal
Scanning IP Blocks  Vulnerability Scanning	Acquire Infrastructure (8)	Exploit Public- Facing Application	Command and Scripting	Additional Cloud Credentials	Mechanism (4) Setuid and Setgid	Setuid and Setgid	LLMNR/NBT- NS Poisoning		Internal Spearphishing	LLMNR/NBT- NS Poisoning	Protocol (4) Web Protocols	Traffic Duplication	Data Destruction
Wordlist Scanning	Domains DNS Server	External Remote Services	Interpreter (9) PowerShell	Additional Email Delegate	Bypass User Account Control	Bypass User Account Control	and SMB Relay  ARP Cache	Email Account	Lateral Tool Transfer	and SMB Relay  ARP Cache		Data Transfer Size Limits	Data Encrypted for Impact
Gather Victim Host Information (4)	Virtual Private Server	Hardware Additions	AppleScript	Permissions Additional Cloud	Sudo and Sudo Caching	Sudo and Sudo Caching	Poisoning	Cloud Account  Application Window	Remote Service	Poisoning  DHCP Spoofing	Mail Protocols	Exfiltration Over	Data Manipulation (3)
Hardware Software	Server	II Phishing (3)	Windows Command Shell	Roles SSH Authorized	Elevated Execution with Prompt	Elevated Execution with Prompt	Spoofing	Discovery  Browser Information	Session Hijacking (2)	Archive	DNS	Alternative Protocol (3)	Stored Data Manipulation
Firmware	Botnet	Spearphishing Attachment	Unix Shell	Keys	Access Token	Access Token Manipulation (5)	Password	Discovery  Cloud Infrastructure	SSH Hijacking	Data (3)	Through Removable Media	Exfiltration Over	Transmitted Data
Client Configurations	Web Services Serverless	Spearphishing Link	Visual Basic Python	Device Registration BITS Jobs	Manipulation (5) Token	Token Impersonation/Theft	Guessing Password	Discovery	RDP Hijacking Remote	Archive via Utility	Data Encoding (2)	Symmetric Encrypted Non-C2	Manipulation Runtime Data
Gather Victim Identity Information (3)	Malvertising	Spearphishing via Service	JavaScript	Boot or Logon Autostart	Impersonation/Theft Create Process with	Create Process with Token	Cracking Password	Cloud Service Dashboard Cloud Service Discovery	Services (7)	Archive via Library	Standard Encoding	Protocol Exfiltration	Manipulation  Defacement (2)
Credentials Email Addresses	Compromise Accounts (3)	Replication Through	Network Device CLI	Execution (14)  Registry Run Keys /	Token Make and	Make and Impersonate Token	Spraying Credential	Cloud Storage Object Discovery	Desktop Protocol	Archive via Custom Method	Non-Standard Encoding	Over Asymmetric Encrypted	Internal Defacement
Employee Names	Social Media Accounts	Removable Media  Supply Chain	Cloud API Container	Startup Folder Authentication	Impersonate Token Parent PID Spoofing	Parent PID Spoofing	Stuffing Credentials	Container and Resource Discovery	SMB/Windows Admin Shares	Audio Capture	Data Obfuscation (3)	Non-C2 Protocol	External Defacement
Gather Victim Network Information	Email Accounts Cloud Accounts	Compromise (3)	Administration Command	Package Time Providers	SID-History Injection	SID-History Injection BITS Jobs	from Password Stores	Debugger Evasion	Distributed Component Object Model	Automated Collection	Junk Data	Exfiltration Over Unencrypted	II Disk Wipe (2)
Domain Properties	Compromise	Software Dependencies	Deploy Container	Winlogon Helper	Boot or Logon Autostart	Build Image on Host	Keychain	Device Driver Discovery		Browser Session Hijacking	Steganography	Non-C2 Protocol	Disk Content Wipe
DNS		Exploitation for Client Execution	DLL	Execution (14)	Debugger Evasion	Securityd	Domain Trust Discovery	VNC	Clipboard Data	Protocol Impersonation	Exfiltration Over	Disk Structure	



Preperation phase

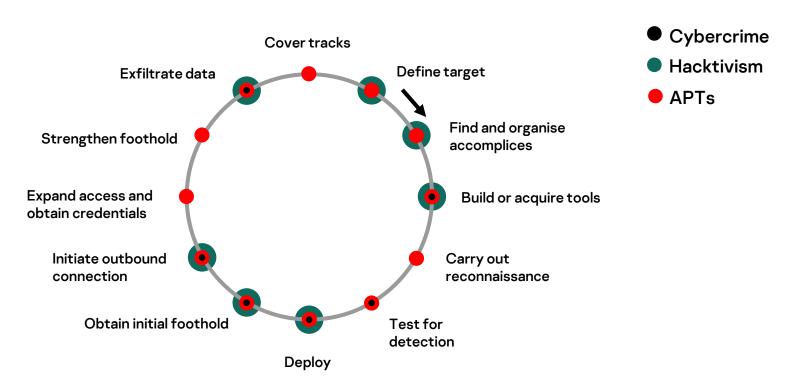
Implant malicious object phase



Complete objectives phase

Post-exploitation phase

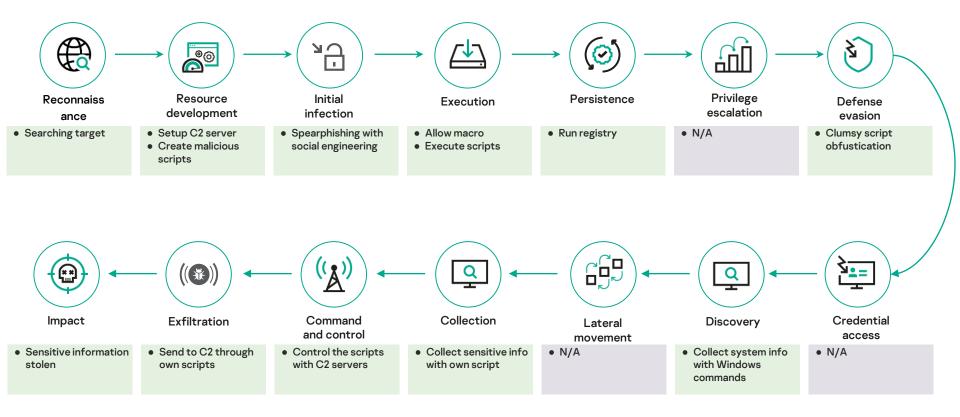
# The threat life-cycle



**GREAT** 

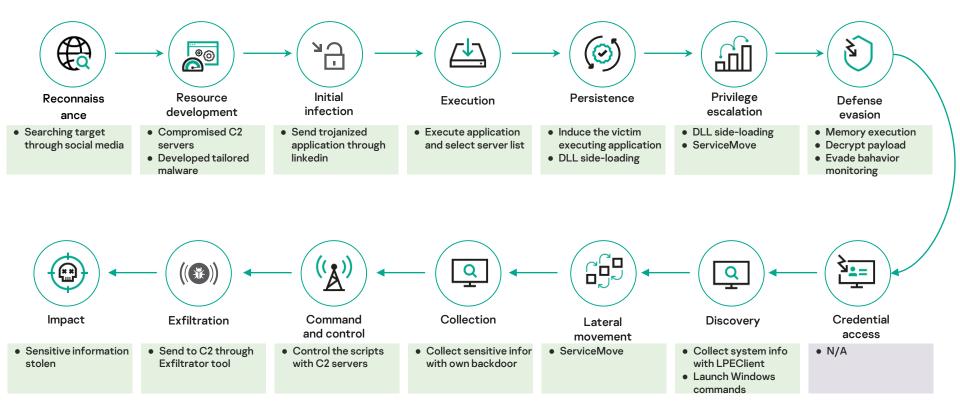
kaspersky

### Operation GoldDragon: Targeting North Korea-related individuals



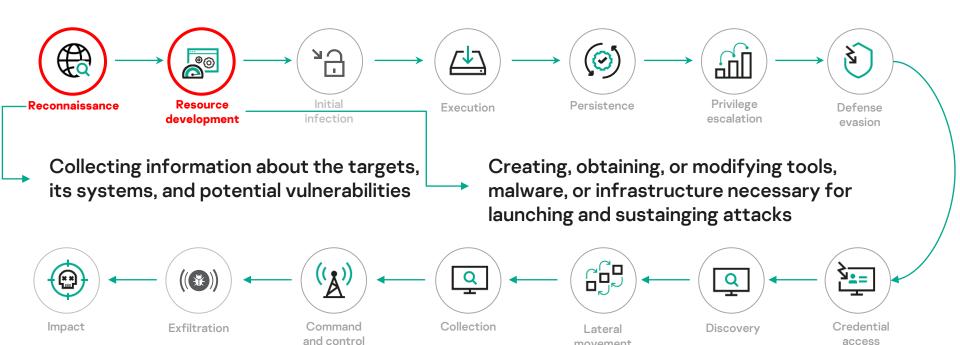
APT attack case - Lazarus

### Operation DreamJob: Targeting employees of defense contractor and nuclear engineer









movement

#### **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.



Al in Reconnaissance

## 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:

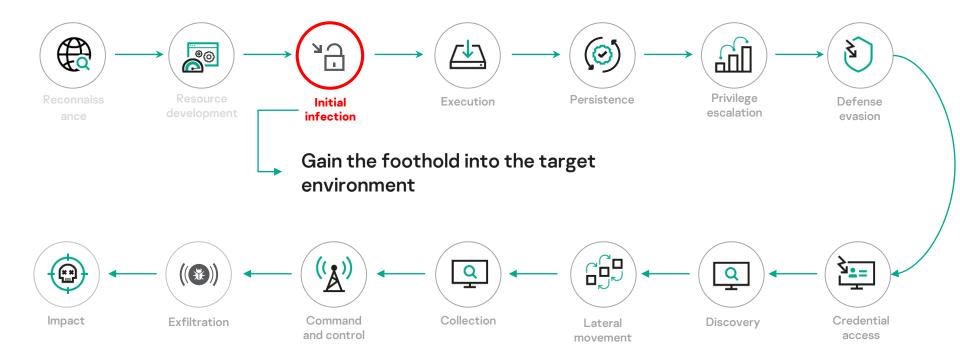
Al can be utilized in creating or acquiring tools

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

## Infrastructure Acquisition:

Al can assist in automating tasks related to building attack infrastructure

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



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



Al in Initial Access

# Most effective infection vector:

Effectively find the best entrypoint into target network

# **Social Engineering:**

Craft highly convincing and personalized phishing messages



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

....



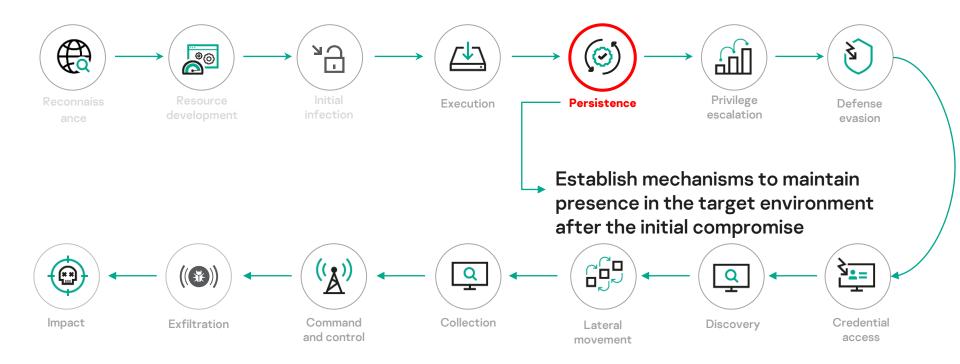
Al in Execution

# Al-chosen command and scripting interpreter:

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

# Al-Enhanced Social Engineering Techniques:

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



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

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



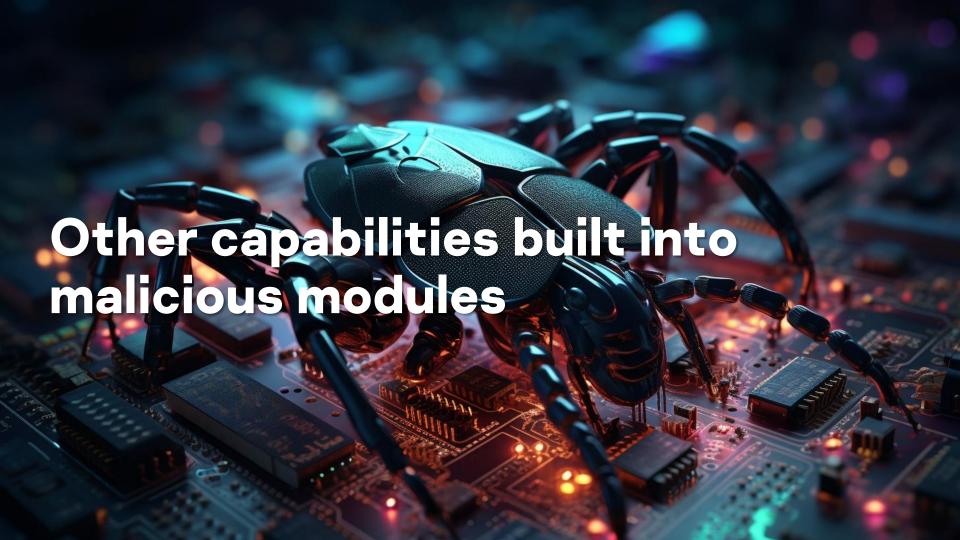
Al in Persistence

## **Boot or Log-on Scripts:**

Creating the most suitable script to execute the malware based on user behaviour analysis

# **Registry Manipulation:**

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







# Identification of vulnerable system components:

Utilize Al algorithms to scan the target environment for known vulnerabilities that can be exploited for privilege escalation

# **Al-Guided Social Engineering:**

Combine Al-enhanced social engineering with privilege escalation to manipulate users into granting higher privileges

Al in Defence Evasion

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

Al-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:**

Al 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:**

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

# Al-assisted automated network mapping and scanning:

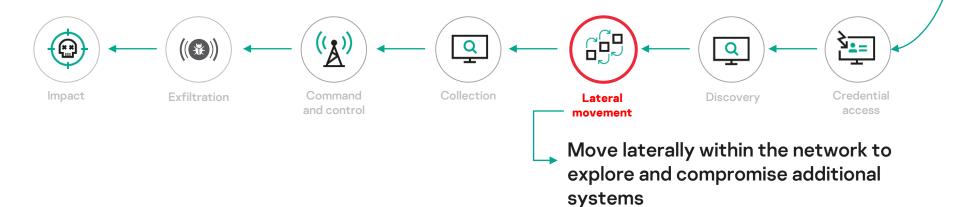
Explore and map the target network infrastructure to identify available systems, devices, services, and potential vulnerabilities

# Al-guided identification of highvalue target assets:

Analyze data and patterns within a target environment to determine which assets, data, or systems hold the greatest value for the attacker







APT actors in APAC in 2023

- 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
```

Al in Lateral Movement

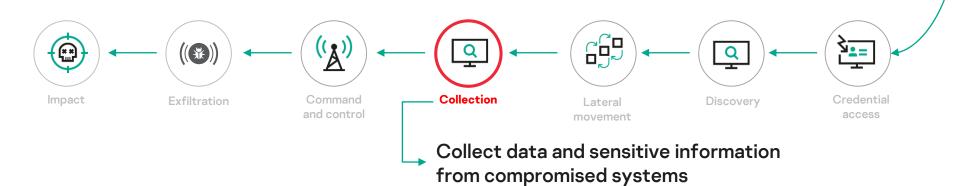
# Al-optimized lateral movement patterns to avoid detection:

Explore and map the target network infrastructure to identify available systems, devices, services, and potential vulnerabilities

### Mimic user behaviour:

Al can assist in mimicking user behaviour in the lateral movement phase to blend in with usual network activities of the system 33





APT actors in APAC in 2023



Screen Capture: Take screenshots to gather information





Screen Capture: Take screenshots to gather information



Data from local systems:

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



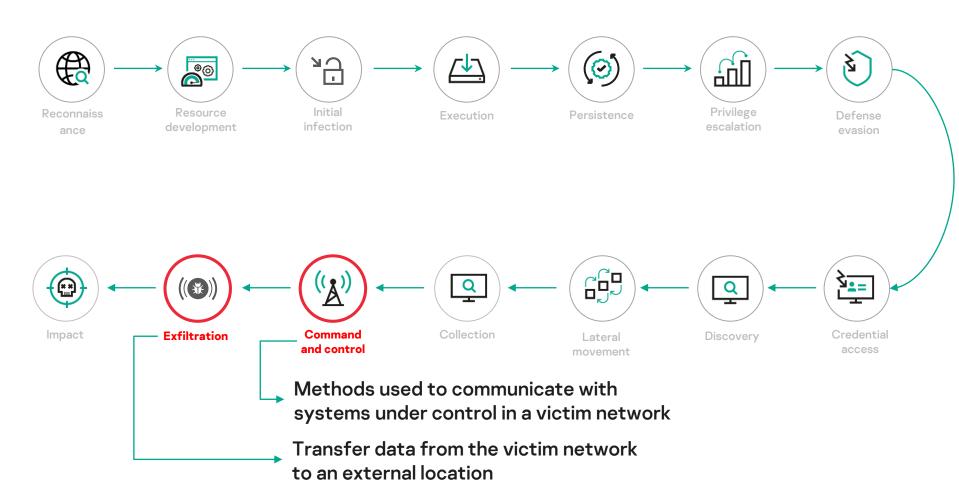
AI in Collection

### Al-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

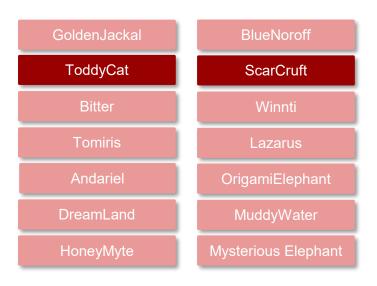
### Automated data classification and selection using Al algorithms:

Analyze, categorize, and choose most relevant data sets from extracted data



APT actors in APAC in 2023

# Exfiltration Over Web Service: Exfiltration to Cloud Storage



APT actors in APAC in 2023

Exfiltration Over Web Service: Exfiltration to Cloud Storage

**Exfiltration Over C2 Channel** 



Enhancing the stealthiness, resilience, and adaptability of communication techniques

Al 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

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

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

Al can be used in various stages of a cyber attack Al can be used by attackers in the **reconnaissance** phase of the attack to profile the victims more efficiently.

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

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

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



## Threat Intelligence

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

- Previously published researches
- Previously seen TTP's
- Scrap loC'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

