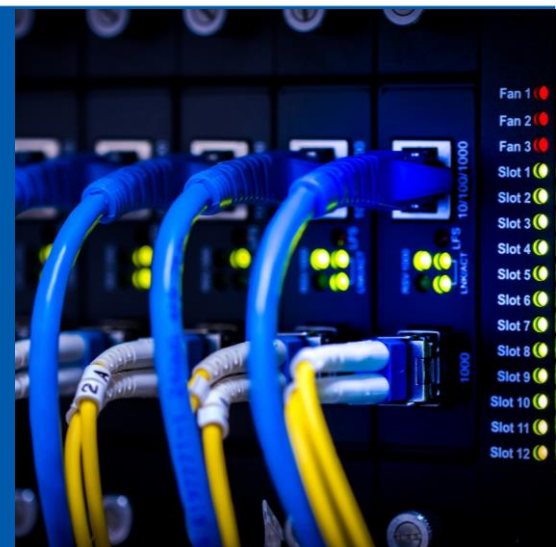
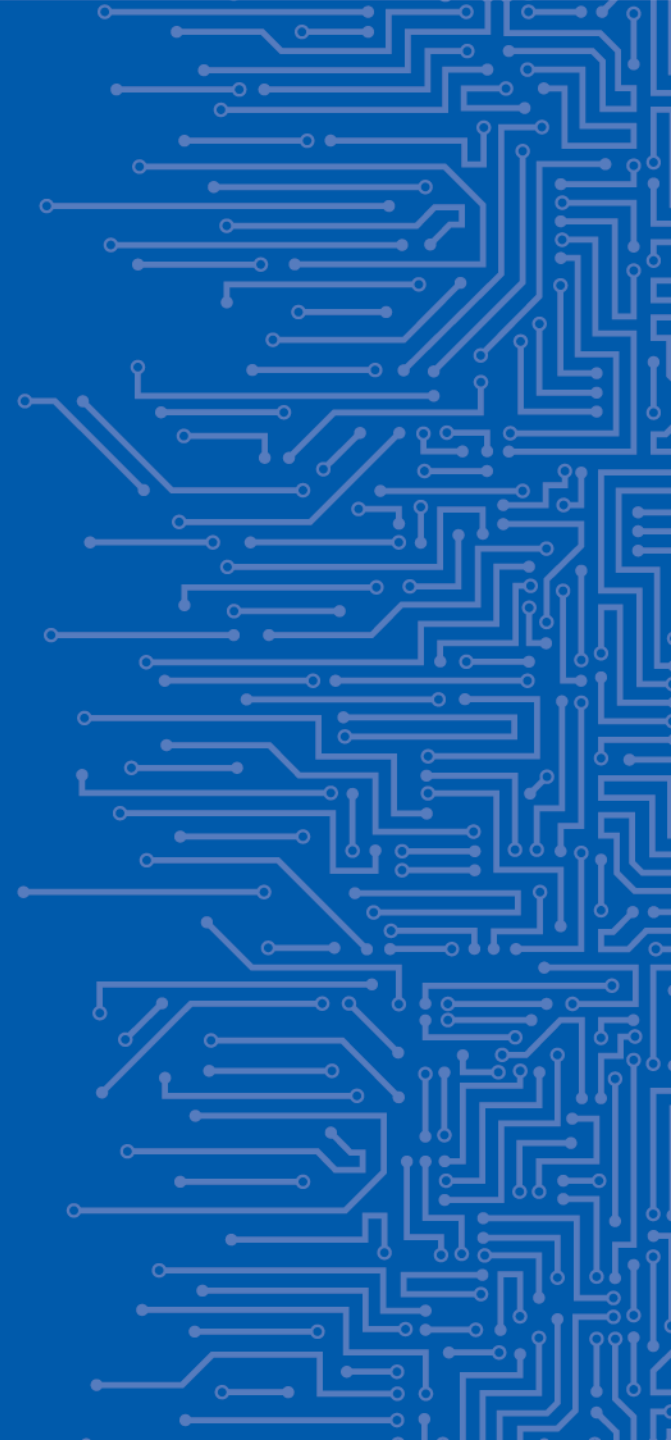


CYBER EXERCISE (ANALYSING AN ATTACK RELATED TO A SPECIFIC THREAT)

09 | 10 | 2024



INTRODUCTION TO INCIDENT HANDLING



INCIDENT HANDLING DEFINITIONS

A security **incident** encompasses a range of **events** that may indicate a threat to an organization's security.

A security **alert** is derived from security events that are logged by the systems in an organization.

Security Event: Any log message related to security, such as authentication logs, firewall logs, etc.

Security Alert: One or more events flagged by the SIEM solution as possibly suspicious. These can be either true positives or false positives.

Security Incident: A security alert that has been validated as a genuine **threat**.

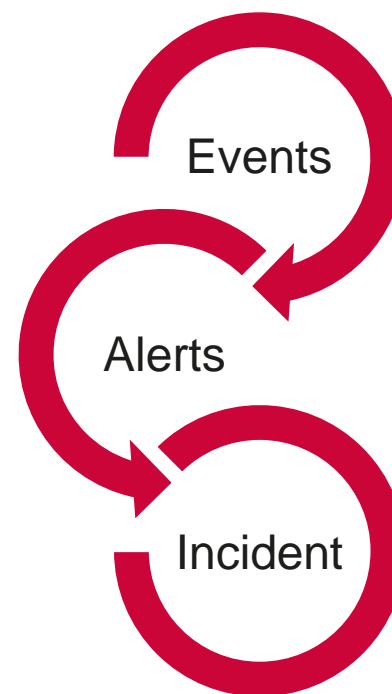
It's important to differentiate between a security incident and a **security breach**.

A **security breach** is a type of security incident that specifically involves verified unauthorized access or exploitation, impacting the confidentiality, integrity, or availability of systems, services, networks, or data. While breaches often involve data compromise, they can also encompass other forms of security compromise, such as the unauthorized usage of systems, the installation of malware, or the disruption of operational services.

INCIDENT HANDLING

Events. Alerts. Incidents. Precursors. Indicators.

- An **event** is any observable happening
 - Each log entry is an event
- **Alerts** are events which match a specific condition
- **Incidents** are violations or an imminent threat of violation of security policies
- **Indicators**
 - An incident may have occurred or is occurring.
- **Precursor**
 - An incident may occur in the future, for example a vulnerability disclosure



MANAGING INCIDENT RESPONSE



MANAGING INCIDENT RESPONSE

Planning and Preparation	Detection and Reporting	Assessment and Decision	Responses	Lessons Learned
Development and documentation of strategic IR policies	Monitor	When did the event happen?	Containment	Create an Incident Report
Establish communication guidelines	Detect	How was it discovered?	Eradication	Post-Incident monitoring
Incorporate threat intelligence feeds	Alert	Have any other areas been impacted?	Recovery	Identify preventative measures
Perform threat hunting exercises	Report	What is the scope of the compromise?		
Backups		Has the point of entry been discovered?		

DETECTING AN INCIDENT

Security Alerts

- Security **tools**
 - IDS, AV, Firewall
 - Sigma rules
 - Threat intelligence
- **Human** report
 - Helpdesk
 - System administrator
- Other **teams**
 - CSIRT
 - LEA
 - Regulatory bodies

Threat Hunting

- Sophisticated attacks have different steps
- Attackers blend in
 - Living of the Land
 - Signature bypass
 - Unknown techniques
- **Anomaly** detection
- **Correlation**
 - Human factor
 - Know your assets
 - Connecting the dots

INCIDENT REGISTRATION

Ensure completeness of the report

Incident Report



Registration



Triage



Further Process

- **When** did it start?
- **What** triggered the incident report or how was an incident detected?
- Is it a **reliable** source? Quality of the source?
- **Where** was it detected?
- **What** is the severity and impact?
- Impact on availability, integrity or confidentiality?
- PII. Safety? Criminal act?

TRIAGE (1)

Validating an Incident Before Triage



1. Is this a genuine threat or attack?
2. Was the attack successful?
3. What was the outcome of the attack on the affected system?
4. How severe is this threat?
5. Does this threat grant the attacker network access?
6. Are other systems at risk as well?

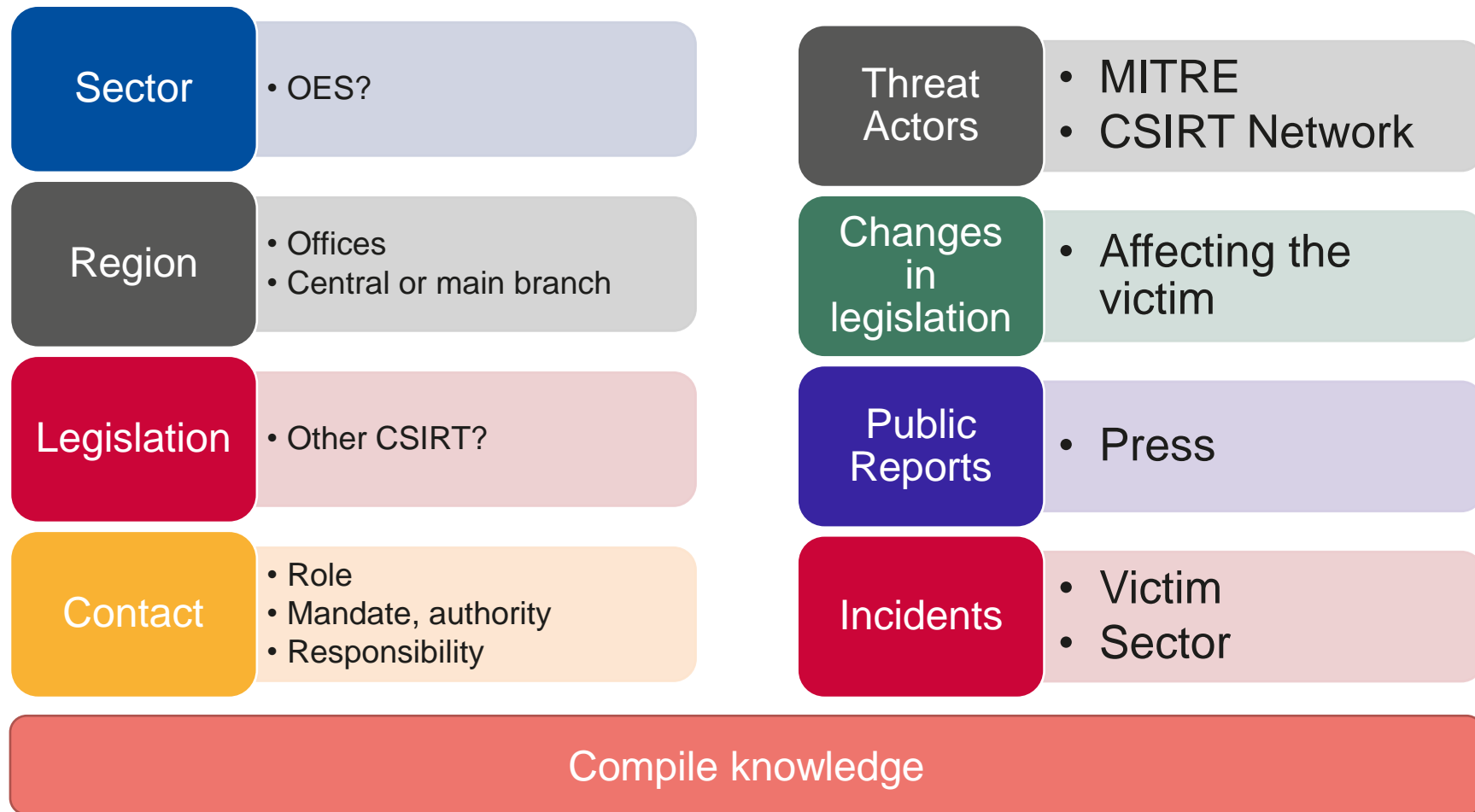
TRIAGE (2)

Not First Come First Served

- Is it really a **security incident**?
- **Relevant** for your team?
 - In your constituency?
- **Previously** reported to your team?
- What is the **impact** and **severity** of the incident?
 - Escalation, notification or legal requirements?
- **Categorize** the incident
 - After the registration, categorize the incident so you can use a correct incident response plan or playbook



VICTIM INFORMATION



PRESERVE EVIDENCE

Inform the victim first

- No reboot. Do not run security software
- Do not start or stop services or applications
- Do not change user configuration
- Do not tip off the attacker
- Assume communication is breached



Collection

- Outweigh balance between evidence collection and risk of tampering material
- Have a standard method for collecting evidence



EVIDENCE: CHAIN OF CUSTODY

Audit trail

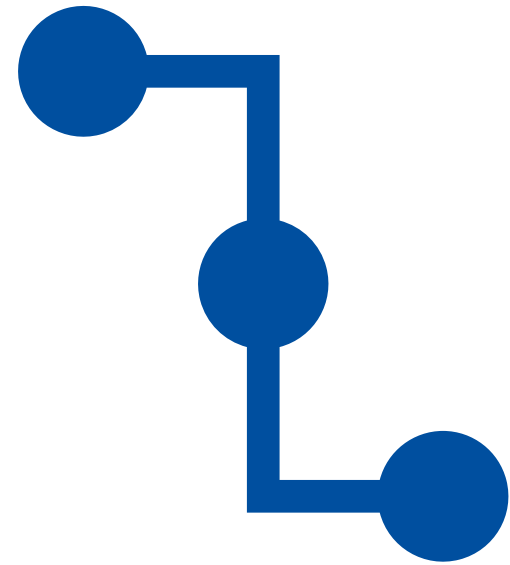
- Validating collection, storage, movement and protection of evidence.
- Was everything handled correctly?
- Is the source **known**?
- Ensure **no modifications** can take place.

Label everything

- Case and item identification. Location. Date. Tools.

Document everything

- Timestamps. Conditions. Expected outcome and actual outcome.



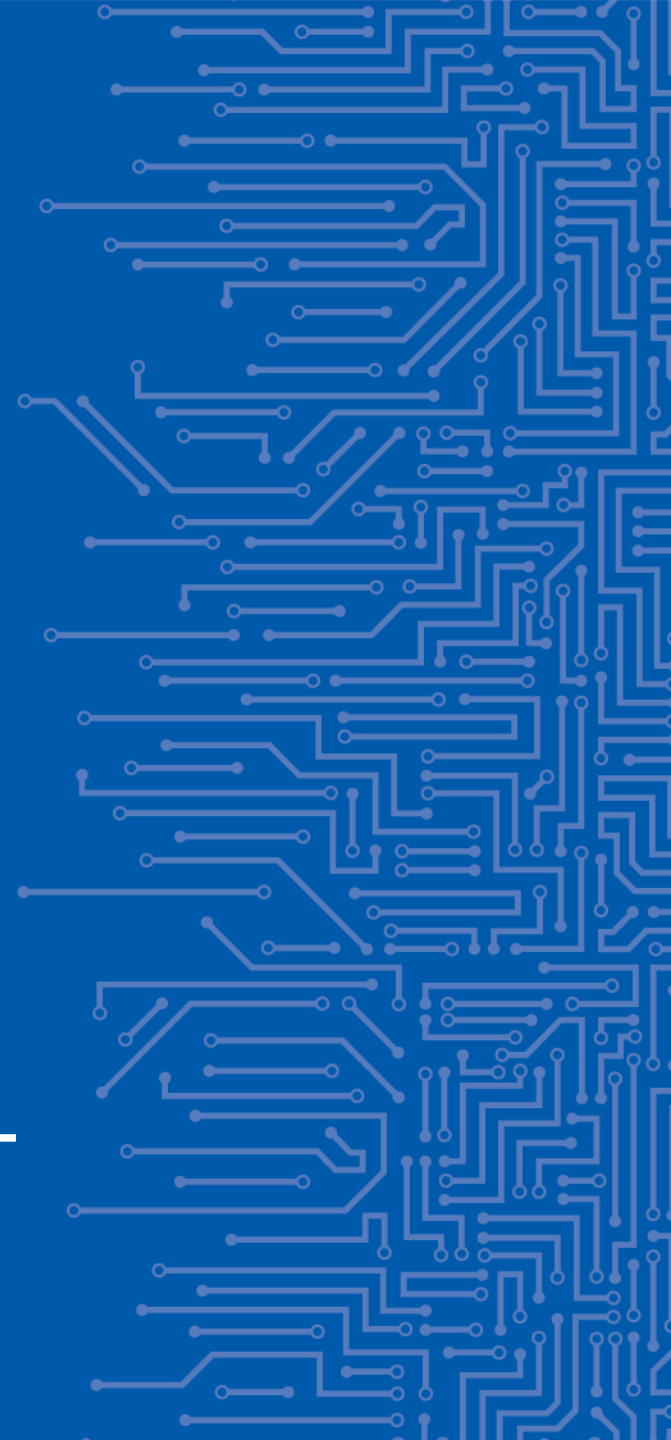
EVIDENCE: CHAIN OF CUSTODY

The O.J. Simpsons case: June 12, 1994

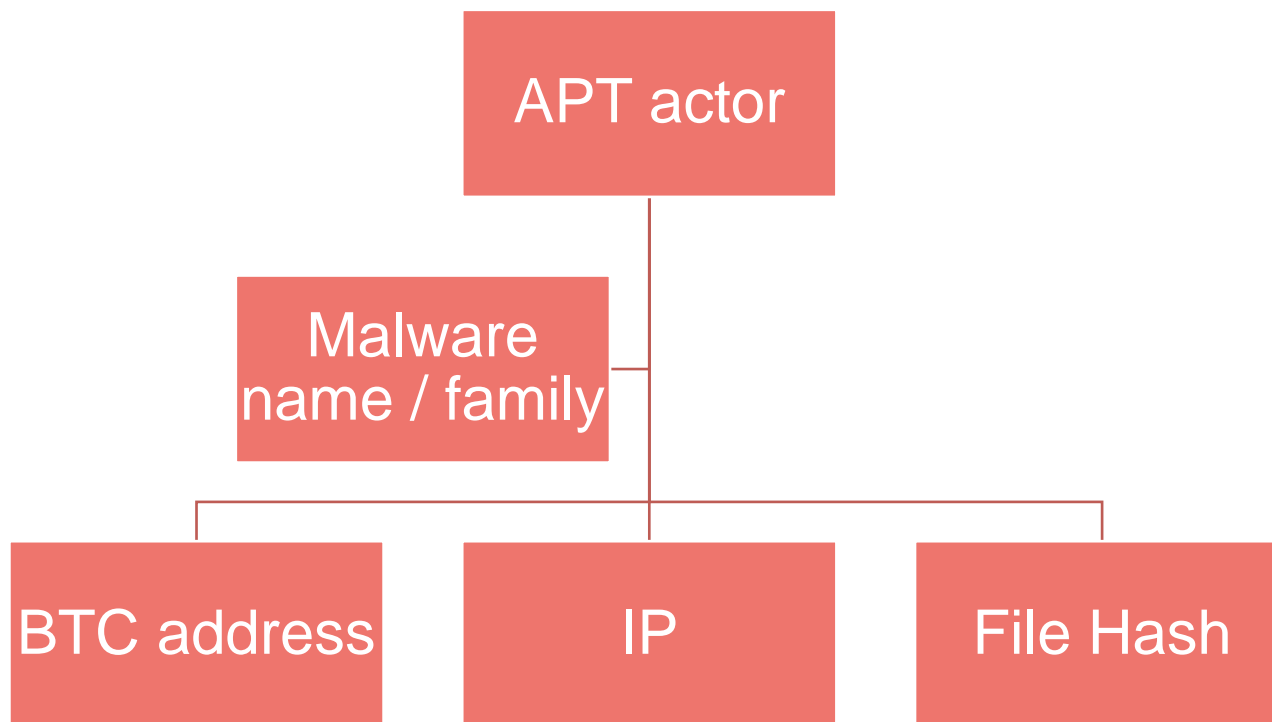
1. Sloppy forensic evidence collection
2. Cross – contaminated evidences
3. “Missing blood”
4. Holding evidence in unsecured environment
5. Fingerprint not collected



CTI AND IRANIAN THREAT ACTOR



THREAT INTELLIGENCE



DATA



SORTED



ARRANGED



PRESENTED
VISUALLY



EXPLAINED
WITH A STORY



TTPS

Tactics

- Tactics are defined as what the attacker does.

Techniques

- Techniques best describe what the attacker uses to accomplish their goal.

Procedures

- Procedures are the manner, or order, in which an attack is carried out.

ABOUT CTI

Sources:

1. Open Source (Shodan, Virus Total, Google, Malpedia)
2. Free Subscriptions
3. Paid subscriptions
4. Own data collection
5. Collaborations, memberships

Types of CTI:

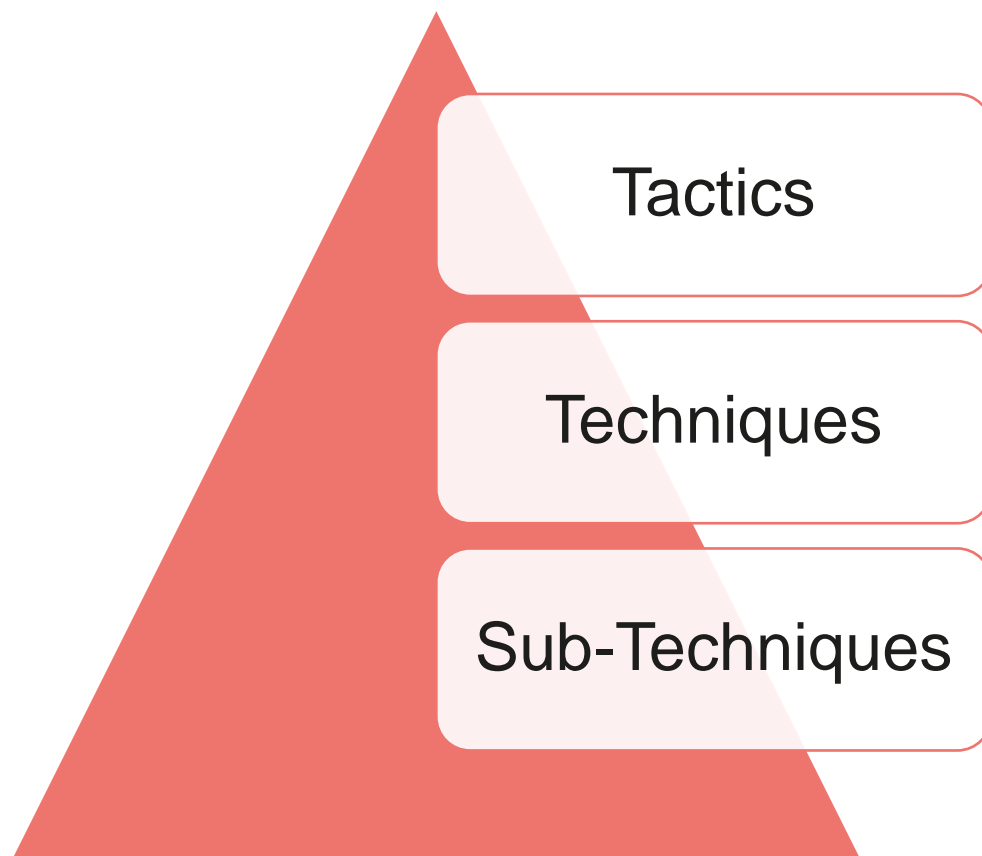
1. Strategic CTI
2. Tactical CTI
3. Technical CTI
4. Operational CTI

CTI is NOT a brainless collection of all data available!

The use of a TIP (Threat Intelligence Platform) can either help you or drive you away from your goal. Be wise.

MITRE ATT&CK OVERVIEW

The MITRE ATT&CK framework is a standardized knowledge base of Adversary Techniques, Tactics & Common Knowledge.



Techniques are categorized into 14 different tactics, which progress from pre-attack to impact and data exfiltration.

Techniques describe the actual activities an attacker might perform in order to reach their goals.

Many techniques in the MITRE ATT&CK framework consist of multiple sub-techniques that describe different ways to carry out each technique.

MITRE ATT&CK OVERVIEW

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Active Scanning (1)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Scanning IP Blocks	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (9)	Additional Cloud Credentials	Setuid and Setgid	Setuid and Setgid	LLMNR/NBNS Poisoning and SMB Relay	Local Account	Internal Spearfishing	LLMNR/NBNS Poisoning and SMB Relay	Web Protocols	Traffic Duplication	Data Destruction
Vulnerability Scanning	Domains	Exploit Public-Facing Application	PowerShell	Additional Email Delegate Permissions	Bypass User Account Control	Bypass User Account Control	Sudo and Sudo Caching	Domain Account	Lateral Tool Transfer	File Transfer Protocols	File Transfer Protocols	Data Transfer Size Limits	Data Encrypted for Impact
Wordlist Scanning	DNS Server	External Remote Services	AppleScript	Additional Cloud Roles	Sudo and Sudo Caching	Sudo and Sudo Caching	ARP Cache Poisoning	Email Account	Remote Service Session Hijacking (2)	Mail Protocols	Mail Protocols	Exfiltration Over Alternative Protocol (3)	Data Manipulation (1)
Gather Victim Host Information (4)	Virtual Private Server	Hardware Additions	Windows Command Shell	SSH Authorized Keys	Elevated Execution with Prompt	Elevated Execution with Prompt	DHCP Spoofing	Cloud Account	SSH Hijacking	DNS	DNS	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Stored Data Manipulation
Hardware	Server	Phishing (4)	Unix Shell	Device Registration	Temporary Elevated Cloud Access	Temporary Elevated Cloud Access	Brute Force (4)	Application Window Discovery	RDP Hijacking	Archive Collected Data (3)	Communication Through Removable Media	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Transmitted Data Manipulation
Software	Botnet	Spearfishing Attachment	Visual Basic	Additional Container Cluster Roles	Access Token Manipulation (3)	Access Token Manipulation (3)	Password Guessing	Browser Information Discovery	Remote Services (6)	Archive via Utility	Content Injection	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Runtime Data Manipulation
Firmware	Web Services	Spearfishing Link	Python	BITS Jobs	Token Impersonation/Theft	Token Impersonation/Theft	Password Cracking	Cloud Infrastructure Discovery	Remote Desktop Protocol	Archive via Library	Data Encoding (2)	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Defacement (2)
Client Configurations	Serverless	Spearfishing via Service	JavaScript	Boot or Logon Autostart Execution (14)	Create Process with Token	Create Process with Token	Password Spraying	Cloud Service Dashboard	SMB/Windows Admin Shares	Archive via Custom Method	Standard Encoding	Exfiltration Over Unencrypted Non-C2 Protocol	Internal Defacement
Gather Victim Identity Information (3)	Compromise Accounts (3)	Spearfishing Voice	Network Device CLI	Registry Run Keys / Startup Folder	Make and Impersonate Token	Make and Impersonate Token	Credential Stuffing	Cloud Storage Discovery	Distributed Component Object Model	Automated Collection	Non-Standard Encoding	Exfiltration Over Unencrypted Non-C2 Protocol	External Defacement
Credentials	Social Media Accounts	Replication Through Removable Media	Cloud API	Authentication Package	Parent PID Spoofing	Parent PID Spoofing	Keychain	Container and Resource Discovery	SSH	Audio Capture	Data Obfuscation (3)	Exfiltration Over C2 Channel	Disk Wipe (2)
Email Addresses	Email Accounts	Supply Chain Compromise (3)	Deploy Container	Time Providers	SID-History Injection	SID-History Injection	Securityd Memory	Debugger Evasion	VNC	Browser Session Hijacking	Junk Data	Exfiltration Over C2 Channel	Disk Content Wipe
Employee Names	Cloud Accounts	Compromise Software Dependencies and Development Tools	Exploitation for Client Execution	Winlogon Helper DLL	Account Manipulation (6)	Build Image on Host	Credentials from Web Browsers	Device Driver Discovery	Windows Remote Management	Clipboard Data	Steganography	Exfiltration Over Other Network Medium (1)	Disk Structure Wipe
Gather Victim Network Information (6)	Compromise Infrastructure (7)	Compromise Software Supply Chain	Inter-Process Communication (3)	Security Support Provider	Additional Cloud Credentials	Debugger Evasion	Windows Credential Manager	Domain Trust Discovery	Cloud Services	Data from Cloud Storage	Protocol Impersonation	Exfiltration Over Bluetooth	Endpoint Denial of Service (4)
Domain Properties	Domains	Compromise Hardware Supply Chain	Component Object Model	Kernel Modules and Extensions	Additional Email Delegate Permissions	Deofuscate/Decode Files or Information	Password Managers	File and Directory Discovery	Direct Cloud VM Connections	Data from Configuration Repository (2)	Dynamic Resolution (3)	Exfiltration Over Bluetooth	OS Exhaustion Flood
DNS	DNS Server	Trusted Relationship	XPC Services	Re-opened Applications	Additional Cloud Roles	Deploy Container	Cloud Secrets Management Stores	Group Policy Discovery	Network Service Discovery	SNMP (MIB Dump)	Fast Flux DNS	Exfiltration Over Physical Medium (1)	Service Exhaustion Flood
Network Trust Dependencies	Virtual Private Server	Valid Accounts (4)	Native API	Port Monitors	SSH Authorized Keys	Direct Volume Access	Cloud Secrets Management Stores	Log Enumeration	Network Share Discovery	Network Device Configuration Dump	DNS Calculation	Exfiltration over USB	Application Exhaustion Flood
Network Topology	Server	Default Accounts	Scheduled Task/Job (5)	Print Processors	Device Registration	Domain Policy Modification (2)	Exploitation for Credential Access	Network Sniffing	Network Service Discovery	Data from Information Repositories (3)	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Application or System Exploitation
IP Addresses	Botnet	Domain Accounts	At	XDG Autostart Entries	Additional Container Cluster Roles	Group Policy Modification	Forge Web Credentials (2)	Permission Groups Discovery (3)	Peripheral Device Discovery	Confuence	Symmetric Cryptography	Exfiltration to Code Repository	Financial Theft
Network Security Appliances	Web Services	Local Accounts	Cron	Registry Run Keys / Startup Folder	SSH Authorized Keys	Execution Guardrails (1)	Web Cookies	Domain Groups	Use Alternate Authentication Material (4)	Sharepoint	Asymmetric Cryptography	Exfiltration to Cloud Storage	Firmware Corruption
Gather Victim Org Information (4)	Serverless	Cloud Accounts	Scheduled Task	Authentication Package	Device Registration	Environmental Keying	SAML Tokens	Cloud Groups	Application Access Token	Code Repositories	Failback Channels	Exfiltration to Text Storage Sites	Inhibit System Recovery
Determine Physical Locations	Develop Capabilities (4)	Default Accounts	System Timers	Time Providers	Boot or Logon Autostart Execution (14)	Exploitation for Defense Evasion	Input Capture (4)	Process Discovery	Pass the Hash	Data from Local System	Ingress Tool Transfer	Exfiltration Over Webhook	Network Denial of Service (2)
Business Relationships	Malware	Domain Accounts	Container Orchestration Job	Winlogon Helper DLL	Registry Run Keys / Startup Folder	File and Directory Permissions Modification (2)	Keylogging	Query Registry	Pass the Ticket	Data from Network Shared Drive	Multi-Stage Channels	Scheduled Transfer	Reflection Amplification
Identify Business Tempo	Code Signing Certificates	Local Accounts	Serverless Execution	Security Support Provider	Authentication Package	Windows File and Directory Permissions Modification	GUI Input Capture	Web Portal Capture	Web Session Cookie	Data from Removable Media	Non-Application Layer Protocol	Transfer Data to Cloud Account	Resource Hijacking
Identify Roles	Digital Certificates	Cloud Accounts	Shared Modules	Kernel Modules and Extensions	Winlogon Helper DLL	Linux and Mac File and Directory Permissions	Web Portal Capture	Credential API Hooking	Local Data Staging	Data Staged (2)	Protocol Tunneling	Service Stop	
Phishing for Information (4)	Exploits	Default Accounts											
Spearfishing Service	Establish Accounts (3)												
Spearfishing Attachment	Social Media Accounts												

OILRIG, APT34, TWISTED KITTEN, CRAMBUS, HELIX KITTEN, CRIMSON

Motivation: state sponsored

Goals: espionage

Target: mainly Middle-East, but in addition:
Turkey, Albania

First sight: 2014

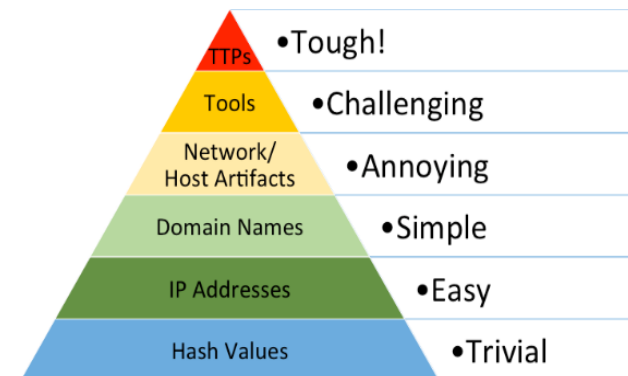
Target sectors: Academic/Research
Institutes, Commercial Aviation, Energy,
utilities & mining, Financial services,
Government & public
services, Healthcare, Industrial manufacturing,
Insurance, Transportation & logistics

APT34 has conducted reconnaissance
aligned with the strategic interests of Iran

SCENARIO

Advanced adversary

- How an adversary operates
 - TTPs: **Tools, Techniques, Procedures**
 - Not as concrete as indicators of compromise (IoCs)
- Understand current **exposure**
- Assess **detection** capabilities



MITRE
ATT&CK™

- Tactics: **Why**
- Techniques: **How**

ADVERSARY

Adversary

- OilRig

QUADAGENT x RGDoor x Helminth x POWRUNNER x OopsIE x Oilrig x +

selection controls										
layer controls										
technique controls										
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
5 items	7 items	5 items	3 items	8 items	4 items	11 items	3 items	3 items	6 items	1 items
External Remote Services	Command-Line Interface	External Remote Services	Scheduled Task	Compiled HTML File	Brute Force	Account Discovery	Remote Desktop Protocol	Automated Collection	Commonly Used Port	Exfiltration Over Alternative Protocol
Spearphishing Attachment	Compiled HTML File	Redundant Access	Valid Accounts	Deobfuscate/Decode Files or Information	Credential Dumping	Network Service Scanning	Remote File Copy	Input Capture	Custom Command and Control Protocol	
Spearphishing Link	PowerShell	Scheduled Task	Web Shell	File Deletion	Credentials in Files	Password Policy Discovery	Remote Services	Screen Capture	Fallback Channels	
Spearphishing via Service	Scheduled Task	Valid Accounts		Indicator Removal from Tools	Input Capture	Permission Groups Discovery			Remote File Copy	
Valid Accounts	Scripting	Web Shell		Obfuscated Files or Information		Process Discovery			Standard Application Layer Protocol	
	User Execution			Redundant Access		Query Registry			Standard Cryptographic Protocol	
	Windows Management Instrumentation			Scripting		System Information Discovery				
				Valid Accounts		System Network Configuration Discovery				
						System Network Connections Discovery				
						System Owner/User Discovery				
						System Service Discovery				

OILRIG

Software

ID	Name
S0360	BONDUPDATER
S0160	certutil
S0095	ftp
S0170	Helminth

Associated Group Descriptions

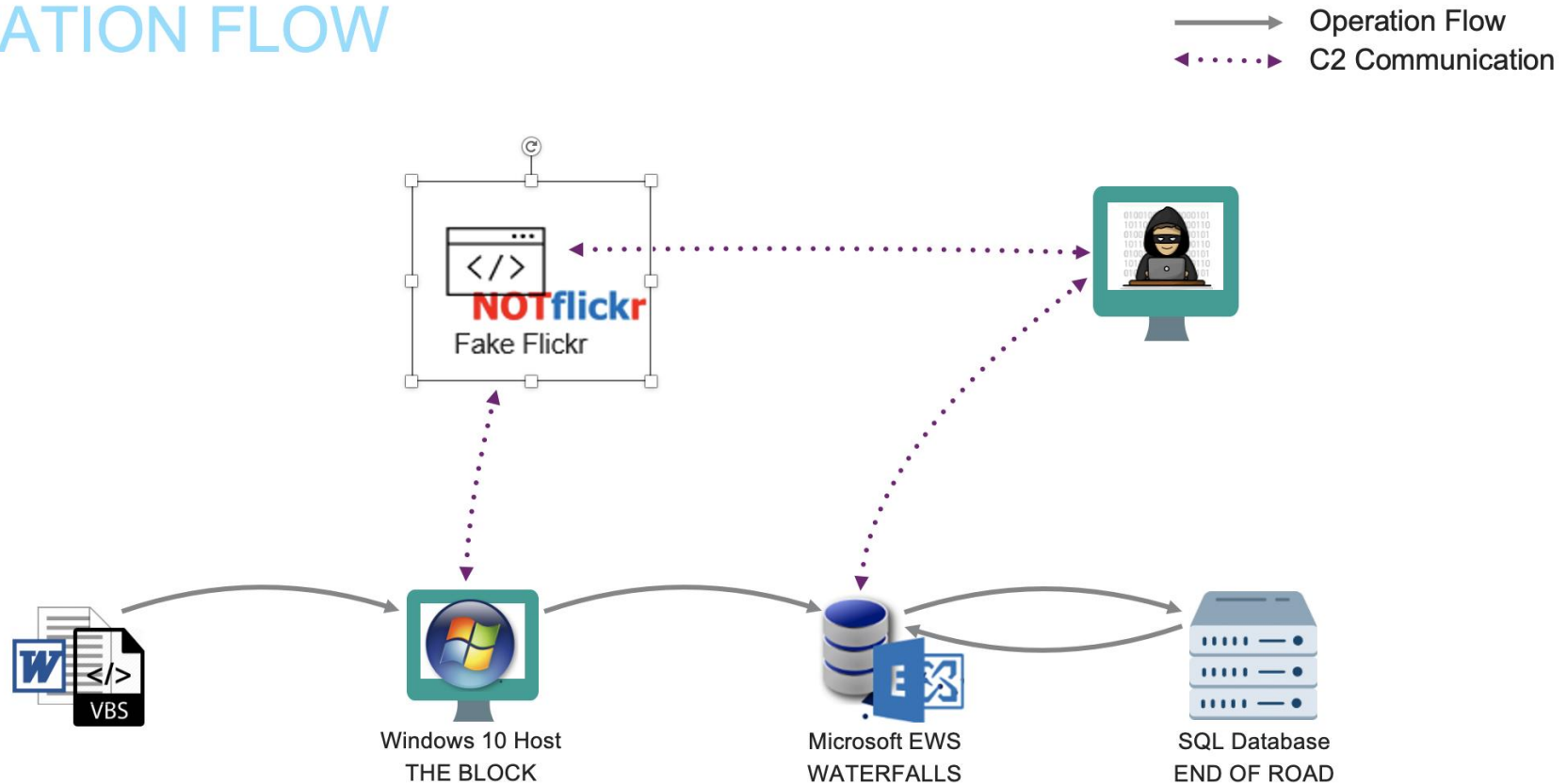
Name	Description
COBALT GYPSY	[8]
IRN2	[9]
APT34	This group was previously tracked under two distinct groups of the activity. ^{[7][6][10]}
Helix Kitten	[7][9]
Evasive Serpens	[5]

Multiple threat intelligence organisations following this group and therefore multiple names.

OPERATION FLOW

HARDTWIST

OPERATION FLOW





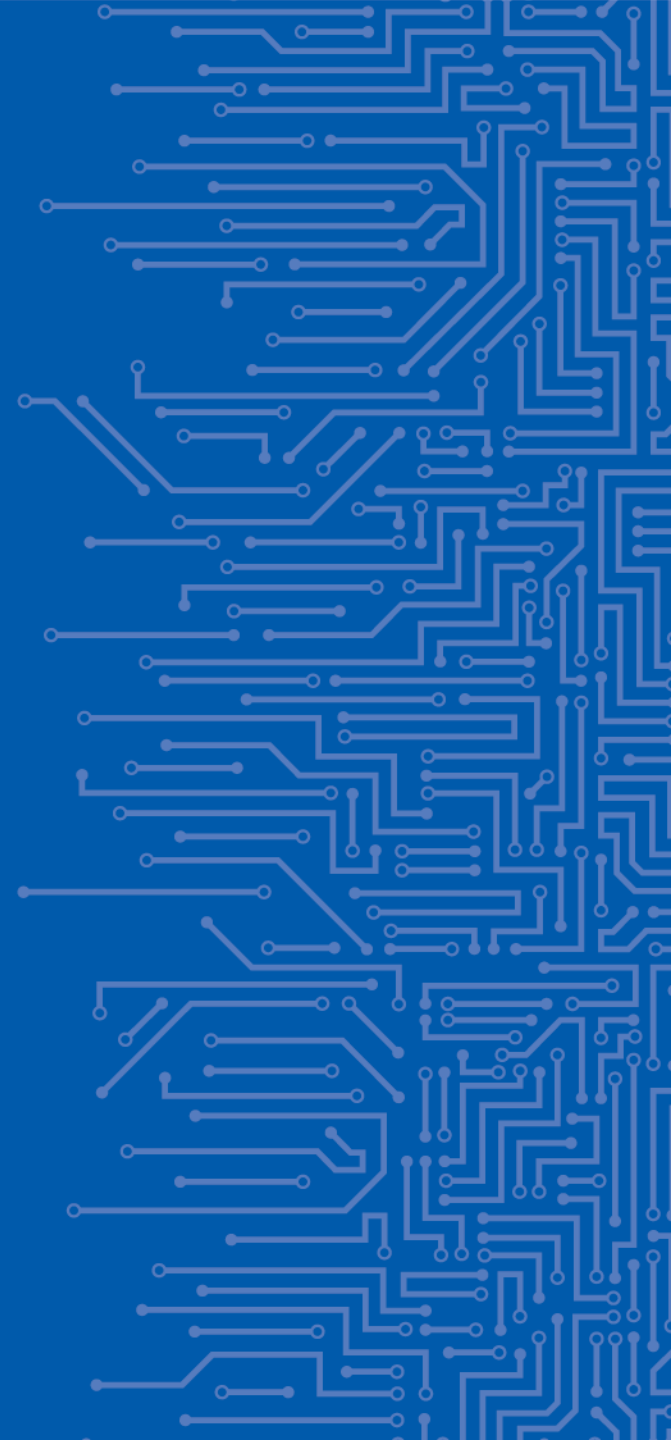
TOOLS NEEDED FOR TODAY



TOOLS

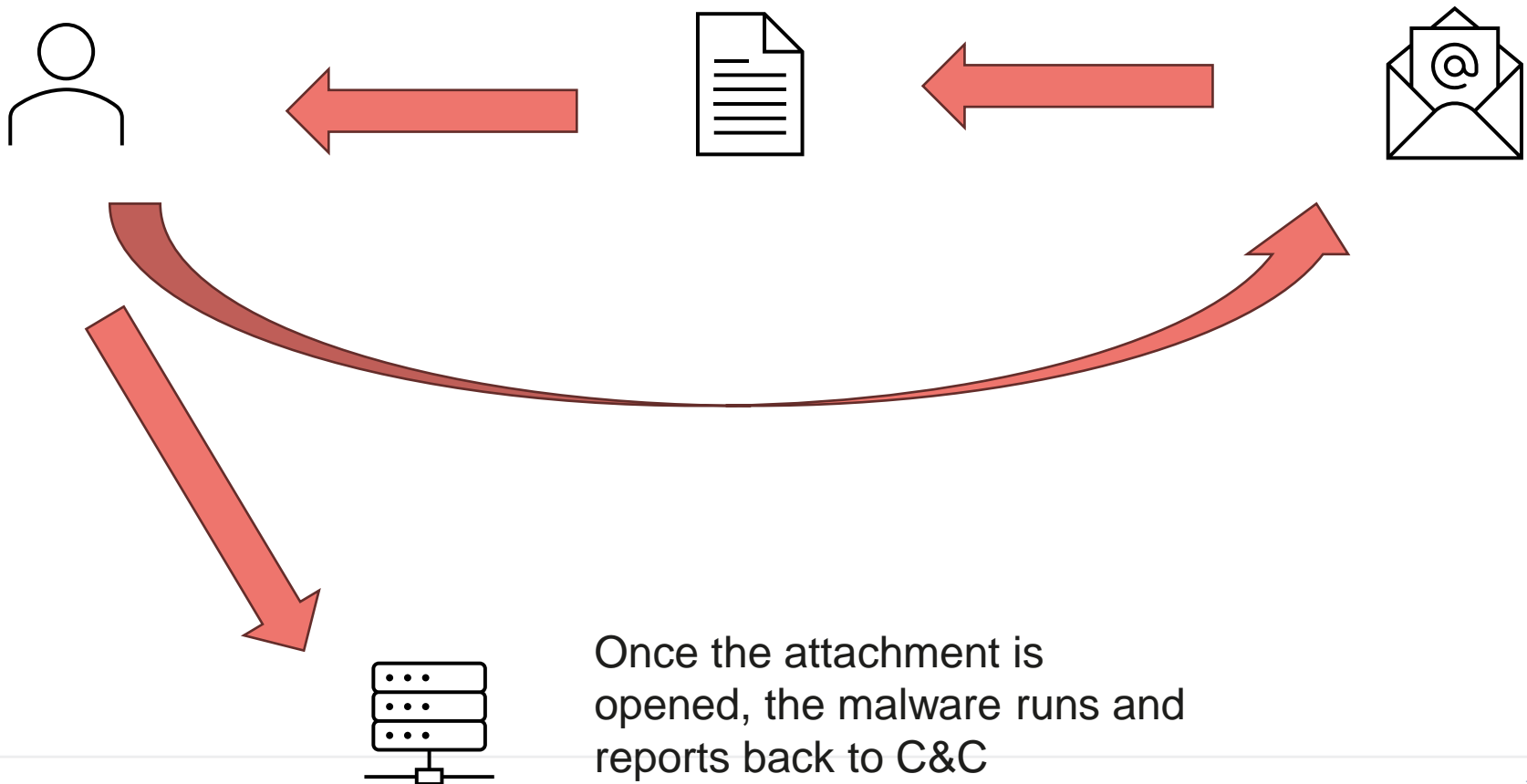
<https://github.com/Lensver65/ESDC-BP>

THE STORY



STEP 1

User receives a SpearPhishing email with a malicious attachment...



STEP 1



- Base64 encoded text → SideTwist Malware
- VBS in doc creates scheduled task, writes the base64 text to file in the localappdata\SystemFailureReporter\ directory as b.doc (file actually is executable)
- Has basic Sandbox evasion technique
- b.doc is renamed as „SystemFailureReporter.exe” and is scheduled to run every 5 minutes
- Executable connects to **X.X.X.X**

TASK 1:

Use the LINK of „[GGMS Overview.doc](#)” (from GitHub) and have it analysed with VirusTotal and HA. Do the same with the „[SideTwist.exe](#)” file

Q:

What is the verdict?



DEMO

See the macro

Demo the
weaponisation

I'm only a script
kiddie'

Start VMs

Start control
server

Execute
SideTwist
malware

Binaries are available on the server: http://192.168.0.5/marketing_materials.zip

Q: TASK 1

What are the hashes of the „b.exe” file?

- MD5: a59b8539af98a6a6df7af4a771d05ea5
- SHA-1:
0188756ec0173ba6af6c51551521997a316e588b
- SHA-256:
9a080bb47fab612597fcb8d31b85f95fc080ed23ca86f75422a73b3f632a1e06

What is the comment „jinfantes” made on VT about the file „update.xml”?

„Iran’s APT34 Returns”

Q: TASK 1

What APIs are called by SideTwist?

- GetUserNameW
- GetComputerNameW
- TerminateProcess
- OutputDebugStringW
- UnhandledExceptionFilter
- IsDebuggerPresent
- GetComputerNameExW
- GetModuleHandleW

What is the IP of the C&C server?

192.168.0.4

All Strings (252)

Interesting (127)

?.AVios_base@std@@

?.AVruntime_error@std@@

?.AVtype_info@@

/getFile/

192.168.0.4



STEP 2

Enumeration of the current user, accounts, groups, system information, network connections, processes, services, and if remote desktop is enabled.

Low privilege credential dumping

SystemFailureReporter.exe to download VALUEVAULT (the executable for which is b.exe) which is then leveraged to perform a low privilege credential dumping. SystemFailureReporter.exe then uploads the VALUEVAULT dump (named ***.dat**) back to C2 via HTTP POST request.



STEP 2

TASK 1:

Use the LINK of „[b.exe](#)” (from GitHub) and have it analysed with VirusTotal and HA

Q:

What is the verdict?

Q: TASK 2

What is the name of the file created?

What is the name of the xml file embedded in b.exe?

b.exe

PID: 7176, Report UID: 00000000-00007176

MD5: a59b8539af98a6a6df7af4a771d05ea5

SHA256: 9a080bb47fab612597fcb8d31b85f95fc080ed23ca86f75422a73b3f632a1e06

%APPDATA%\fsociety.dat

	nts	Handles	Modules	Files
OPEN				%WINDIR%\System32\netutils.dll
OPEN				%WINDIR%\System32\samlib.dll
OPEN				%WINDIR%\System32\samlib.dll
OPEN				%APPDATA%\FSOCIETY.DAT
OPEN				%APPDATA%\FSOCIETY.DAT
OPEN				%APPDATA%\FSOCIETY.DAT
CREATE				%APPDATA%\fsociety.dat

Hash:

a73f26a8d504043f785d7360e8febf2eeb8522ec873a0d4dd5d
1d4bfd1e67d3d

Name: 1.xml (among others)



STEP 3

Lateral movement

It has been discovered from the credentials dumped in Step2 that the user logged in the Victim has admin privileges on the EWS server

Installing webshell to remote server

Downloading the TWOFACE webshell (named contact.aspx) via SystemFailureReporter.exe; TWOFACE is then copied from the victim to SERVER and hidden with attrib + h.



STEP 3

TASK 1:

Use the LINK of „[contact.aspx](#)” (from GitHub) and have it analysed with VirusTotal

Q:

What is the verdict?



FINAL CHALLENGE

Create a threat report about this threat actor!

Include:

- Executive summary
- Description
- IOCs
- TTPs
- Mitre ATT&CK Framework references
- Recommendations

Target Audience:

Your SOC ppl



REFERENCES

This scenario is based on the Adversary Emulation Library created by Center for Threat-Informed Defense for education purposes.

https://github.com/center-for-threat-informed-defense/adversary_emulation_library/

Full attack scenario is available: https://github.com/center-for-threat-informed-defense/adversary_emulation_library/blob/master/oilrig/Emulation_Plan/README.md

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity

Vasilissis Sofias Str 1, Maroussi 151 24

Attiki, Greece

 +30 28 14 40 9711

 info@enisa.europa.eu

 www.enisa.europa.eu

