



How to effectively use ATT&CK in the context of TIBER-EU

Jose Miguel Esparza

Seventh EU MITRE ATT&CK® Community Workshop

June 2021



WHO AM I?

- Jose Miguel Esparza
- Head of Threat Intelligence at [Blueliv](#)
 - Ex Fox-IT and S2Isec
- Malware and Threat Analysis
- Gathering intelligence from botnets & actors
- Relations with industry peers and LEAs



AGENDA

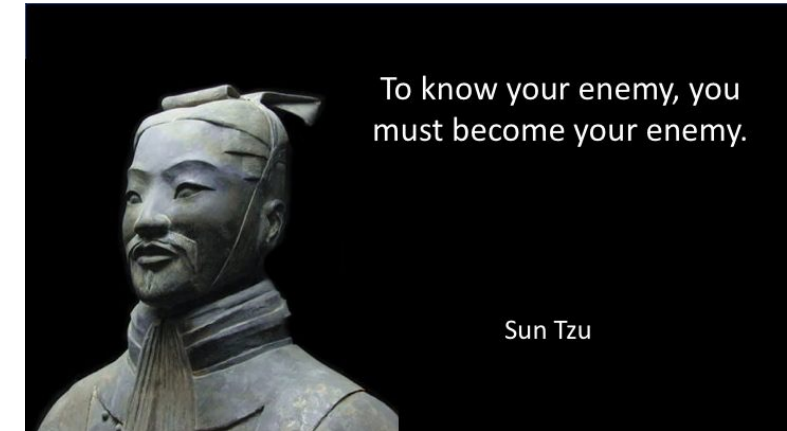
- TIBER-EU basics
- Adversaries and TTP prioritization
- Real use-case
- Conclusions

TIBER-EU BASICS



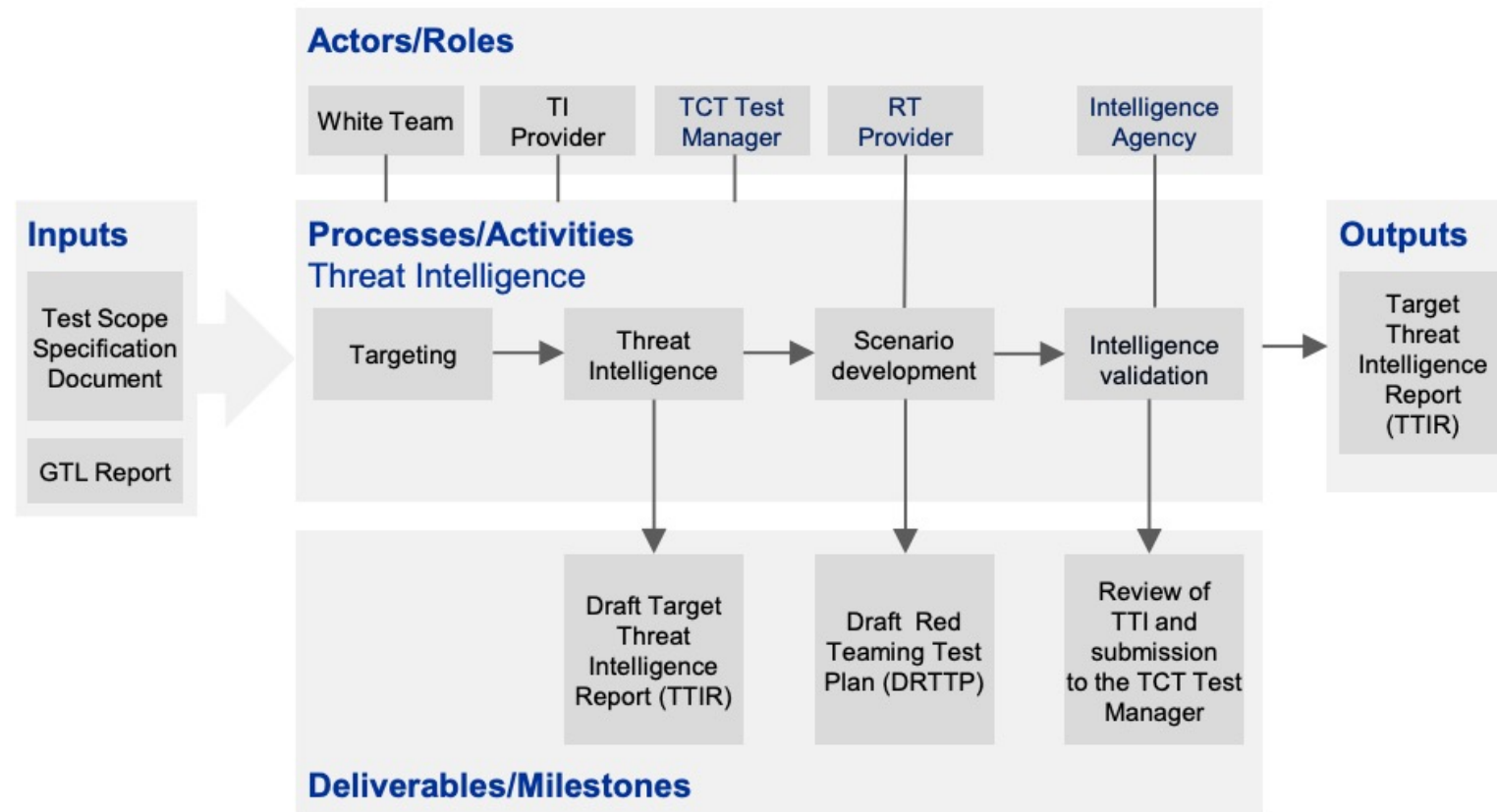
TIBER-EU BASICS

- Framework developed by the ECB
 - Similar to CBEST in UK
- Threat Intelligence insights as input for red teams
- Mimic TTPs of real-life threat actors
- Focusing on financial and critical sectors
 - But applicable to any sector
- Improve the protection, detection and response of tested entities



TIBER-EU BASICS

TIBER-EU testing phase – overview of threat intelligence and scenarios



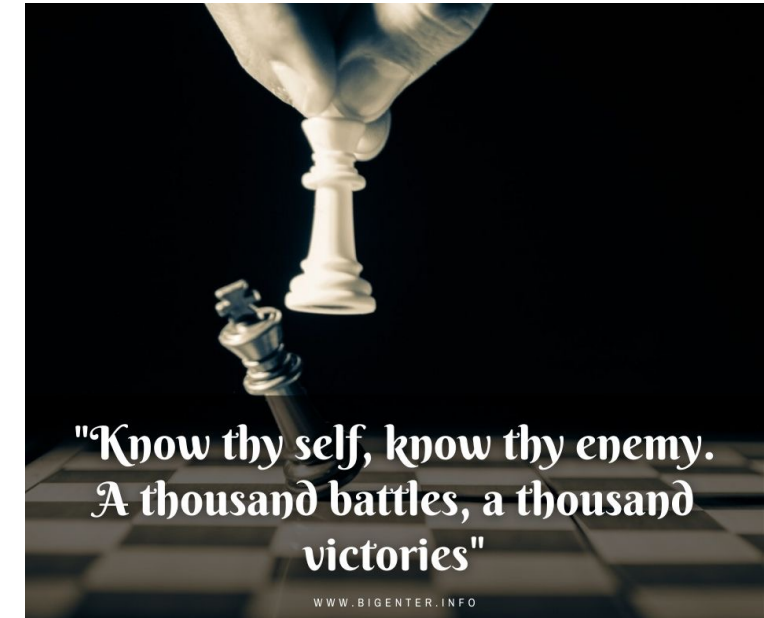
TIBER-EU BASICS

TIBER-EU testing phase – overview of threat intelligence and scenarios



ADVERSARIES AND TTP PRIORITIZATION

- Not all threat actors will attack you
- Knowing your potential adversaries is critical
- Knowing the most used TTPs is key too
- Objective: defend effectively against them!



ADVERSARIES AND TTP PRIORITIZATION: TIPS

- You need to build a Threat Actor Knowledge Base (KB)
 - New campaigns and targets
 - Tools used by them
 - TTPs based on ATT&CK
- This Knowledge Base must be continuously updated!
 - Own investigations
 - Community and public research

ADVERSARIES AND TTP PRIORITIZATION: TIPS

- Use the Threat Actor KB to prioritize
 - Adversaries
 - Filter per sector and country/region targeted
 - Score those actors based on potential impact
 - TTPs
 - Score ATT&CK techniques based on adversaries and most used in campaigns



REAL USE-CASE: RANSOMWARE GROUPS

- Let's score ransomware groups based on number of victims targeted
- Let's keep in mind their sophistication
- Let's score ATT&CK techniques based on usage in campaigns

REAL USE-CASE: RANSOMWARE GROUPS

- Example (actor score)
 - Trickbot Group
 - High sophistication: 5 points
 - High impact: 5 points
 - Total: 10 points
 - Babuk Team
 - Medium sophistication: 3 points
 - High impact: 5 points
 - Total: 8 points

The screenshot displays the CONTI NEWS website interface. At the top, there is a logo and the text 'CONTI NEWS'. Below this is a search bar and links for 'Web mirror' and 'Tor mirror'. The main content area features three news articles, each with a title, URL, location, and a brief description. At the bottom of each article is a progress bar indicating the percentage of data published (5%, 20%, and 100% respectively) and a 'READ MORE' link.

"NATIONAL LOUIS UNIVERSITY"
www.nl.edu
 122 S. Michigan Ave.
 Chicago, IL 60603
 National Louis University has a downtown Chicago campus, and Illinois campuses in Lisle and Wheeling. Our Florida Campus is located in one of Tampa's major business districts.
 NLU's downtown Chicago campus is located Michigan Avenue occupies five floors of the historic Peoples Gas Building and several floors in the Gage Building. Our Florida Campus was established in 1988 and located in one of Tampa's major business districts, NLU's Florida Campus serves students in 13 counties in central Florida. We also have Illinois campuses in Lisle, the North Shore (Skokie) and Wheeling.
 PUBLISHED 5%
 June 01, 2021 643 READ MORE »

"FUNBREAK"
funbreak.fr
 28 rue Nicolai
 69007 Lyon
 Created 12 years ago by a former president of BDE (Bureau des Etudiants), FunBreak has become the leader in festive stays for young people and students in France. Composed of a team of 8 people, all between 22 and 33 years old, we strive to offer only quality stays and services by responding to the demand of 18-30 year olds. Service, security, supervision and professionalism are the strengths of our agency.
 PUBLISHED 20%
 June 01, 2021 8970 READ MORE »

"TEMMELOGISTIK CENTER"
tlc.co.at
 Temmel Logistik Center GmbH
 Industriestraße 2
 84094 Elsendorf | Deutschland
 Tel. +43 (0) 316 - 40 77 66 - 0
 TLC - Temmel Logistik Center ist ein top-professioneller Dienstleister für die Automobil- und produzierende Industrie. Wir verfügen über viele Jahre Erfahrung und höchste Kompetenz in den Arbeitsbereichen Montage, Nacharbeit, Qualitätskontrolle, Lager-Verwaltung und Kommissionierung - auch direkt am Bedarfspunkt bei Ihrem Kunden bzw. in Ihrer Nähe – und decken somit den gesamten Prozess der Supply Chain ab.
 PUBLISHED 100%
 June 01, 2021 591 READ MORE »

REAL USE-CASE: RANSOMWARE GROUPS

- Example (ATT&CK technique score)
 - T1133 - External Remote Services
 - Used in 5 “Trickbot Group” campaigns: 10 (actor) + 5 (campaigns)
 - Used in 3 “Babuk Team” campaigns: 8 (actor) + 3 (campaigns)
 - Total technique score: 15 + 11 = 26 points



HOW TO EFFECTIVELY USE ATT&CK IN THE CONTEXT OF TIBER-EU

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 17 techniques	Privilege Escalation 12 techniques	Defense Evasion 35 techniques	Credential Access 15 techniques	Discovery 24 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 16 techniques	Exfiltration 8 techniques	Impact 13 techniques
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/6)	Valid Accounts (1/4)	Windows Management Instrumentation	Valid Accounts (1/4)	Valid Accounts (1/4)	Valid Accounts (1/4)	Brute Force (2/4)	File and Directory Discovery	Lateral Tool Transfer	Data from Local System	Data Obfuscation (0/3)	Automated Exfiltration (0/1)	Data Encrypted for Impact
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Exploit Public-Facing Application	User Execution (2/2)	External Remote Services	Process Injection (2/11)	Process Injection (2/11)	Credentials from Password Stores (1/3)	System Information Discovery	Exploitation of Remote Services	Automated Collection	Web Service (1/3)	Exfiltration Over Alternative Protocol (3/3)	Inhibit System Recovery
Active Scanning (0/2)	Acquire Infrastructure (0/6)	External Remote Services	Scheduled Task/Job (2/6)	Scheduled Task/Job (2/6)	Exploitation for Privilege Escalation	Modify Registry	Input Capture (2/4)	Process Discovery	Remote Services (4/6)	Data from Network Shared Drive	Data Encoding (0/2)	Fallback Channels	Service Stop
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Phishing (2/3)	System Services (1/2)	Create Account (2/3)	Access Token Manipulation (2/5)	Obfuscated Files or Information (3/5)	Network Sniffing	Query Registry	Replication Through Removable Media	Email Collection (0/3)	Encrypted Channel (2/2)	Exfiltration Over Web Service (1/2)	Data Destruction
Gather Victim Identity Information (0/3)	Develop Capabilities (0/4)	Trusted Relationship	Exploitation for Client Execution	Account Manipulation (1/4)	Scheduled Task/Job (2/6)	Deobfuscate/Decode Files or Information (2/6)	Steal or Forge Kerberos Tickets (1/4)	Remote System Discovery	Taint Shared Content	Screen Capture	Protocol Tunneling	Data Transfer Size Limits	Network Denial of Service (1/2)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Drive-by Compromise	Command and Scripting Interpreter (5/8)	Browser Extensions	Create or Modify System Process (1/4)	Virtualization/Sandbox Evasion (1/3)	Unsecured Credentials (2/5)	System Network Configuration Discovery	Internal Spearphishing	Archive Collected Data (2/3)	Dynamic Resolution (2/3)	Exfiltration Over C2 Channel	Resource Hijacking
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Inter-Process Communication (2/2)	Create or Modify System Process (1/4)	Abuse Elevation Control Mechanism (1/4)	Access Token Manipulation (2/5)	Exploitation for Credential Access	Network Service Scanning	Remote Service Session Hijacking (1/2)	Data from Information Repositories (0/2)	Non-Standard Port	Exfiltration Over Other Network Medium (0/1)	Account Access Removal
Search Open Technical Databases (0/5)		Replication Through Removable Media	Native API	Office Application Startup (0/8)	Domain Policy Modification (0/2)	Indicator Removal on Host (4/6)	Forced Authentication	Network Share Discovery	Software Deployment Tools	Data Staged (0/2)	Application Layer Protocol (3/4)	Exfiltration Over Physical Medium (0/1)	System Shutdown/Reboot
Search Open Websites/Domains (0/2)		Hardware Additions	Shared Modules	BITS Jobs		Impair Defenses (3/5)	Forge Web Credentials (0/2)	System Time Discovery	Use Alternate Authentication Material (2/4)	Input Capture (2/4)	Communication Through Removable Media	Scheduled Transfer	Data Manipulation (0/3)
Search Victim-Owned Websites			Software Deployment Tools	Boot or Logon Autostart Execution (3/12)	Boot or Logon Autostart Execution (3/12)	Indirect Command Execution	Man-in-the-Middle (0/2)	Domain Trust Discovery		Man in the Browser			Defacement (0/2)
				Boot or Logon Initialization Scripts (2/5)	Boot or Logon Initialization Scripts (2/5)	Abuse Elevation Control Mechanism (1/4)	Modify Authentication Process (0/4)	Virtualization/Sandbox Evasion (1/3)		Video Capture	Ingress Tool Transfer		Disk Wipe (1/2)
				Compromise Client Software Binary	Event Triggered Execution (4/15)	BITS Jobs	OS Credential Dumping (4/8)	Peripheral Device Discovery		Audio Capture	Multi-Stage Channels		Endpoint Denial of Service (0/4)
				Event Triggered Execution (4/15)	Hijack Execution Flow (2/11)	Domain Policy Modification (0/2)	Steal Application Access Token	Permission Groups Discovery (1/3)		Clipboard Data	Non-Application Layer Protocol		Firmware Corruption
				Hijack Execution Flow (2/11)		Execution Guardrails (1/1)	Steal Web Session Cookie	System Network Connections Discovery		Data from Configuration Repository (0/2)	Proxy (2/4)		
				Pre-OS Boot (1/5)		Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery		Data from Removable Media	Traffic Signaling (0/1)		
				Server Software Component (2/3)		Rootkit		System Service Discovery		Man-in-the-Middle (0/2)			
				Traffic Signaling (0/1)		Signed Binary Proxy Execution (5/11)		Software Discovery (1/1)					
						Direct Volume Access		Browser Bookmark Discovery					
						File and Directory Permissions Modification (2/2)		Network Sniffing					
						Hide Artifacts (4/7)		Application Window Discovery					
						Hijack Execution Flow (2/11)		Cloud Service Dashboard					
						Modify Authentication Process (0/4)		Cloud Service Discovery					
						Modify System Image (0/2)		Password Policy Discovery					
						Network Boundary Bridging (0/1)							
						Pre-OS Boot (1/5)							
						Rogue Domain Controller							
						Signed Script Proxy Execution (0/1)							
						Subvert Trust Controls							

CONCLUSIONS

- TIBER-EU uses **Targeted** Threat Intelligence to test organizations
- ATT&CK is needed in TIBER-EU context (but tweaked better)
 - Build a Threat Actor Knowledge Base
 - Filter adversaries based on **targets**: sectors and country/region
 - Score threat actors based on **impact** and **sophistication**
 - Score ATT&CK techniques based on **usage** by attackers in **campaigns**
- Proper scores for techniques will customize ATT&CK for entities
 - Not all companies should generate the same ATT&CK matrix
 - Customized TIBER-EU scenarios

Q&A

THANK YOU!!

 <http://es.linkedin.com/in/josemiguellesparza>

 @EternalTodo

 jose.esparza@blueliv.com

