Blueliv.

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 S21sec
- Malware and Threat Analysis
- Gathering intelligence from botnets & actors
- Relations with industry peers and LEAs

@EternalToDo

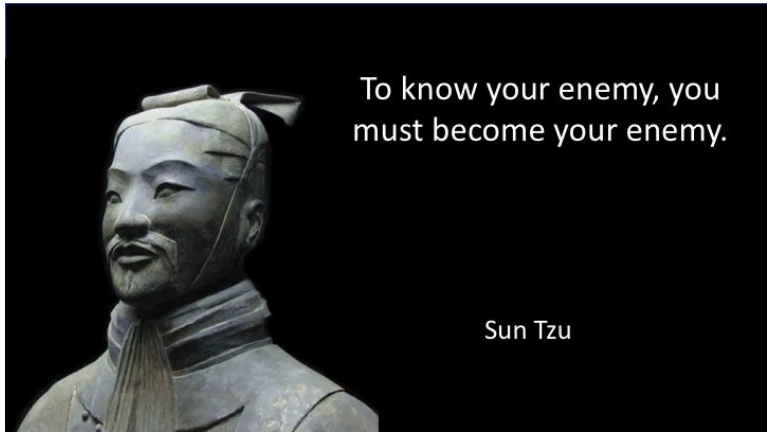
AGENDA

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

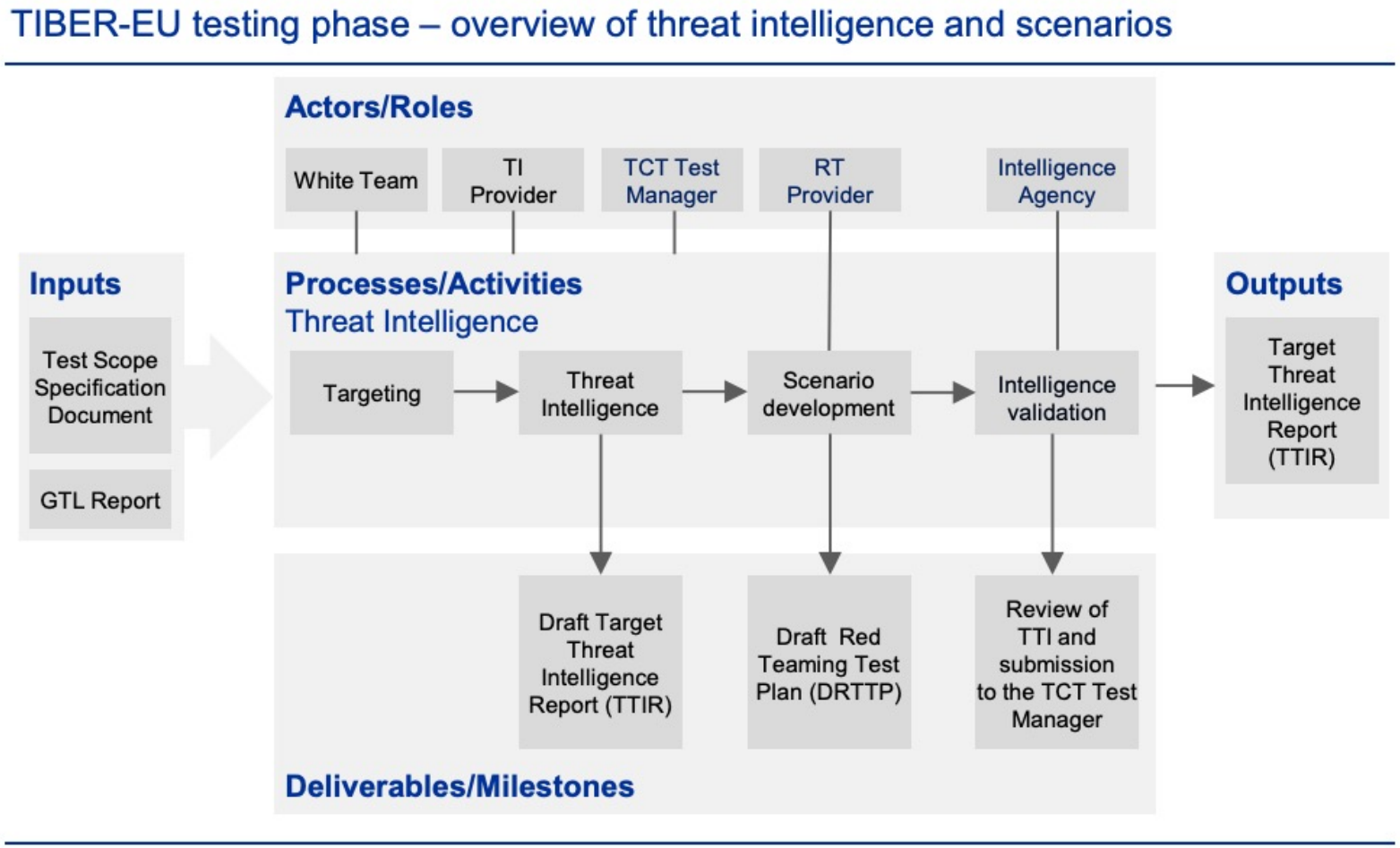
TIBER-EU BASICS

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



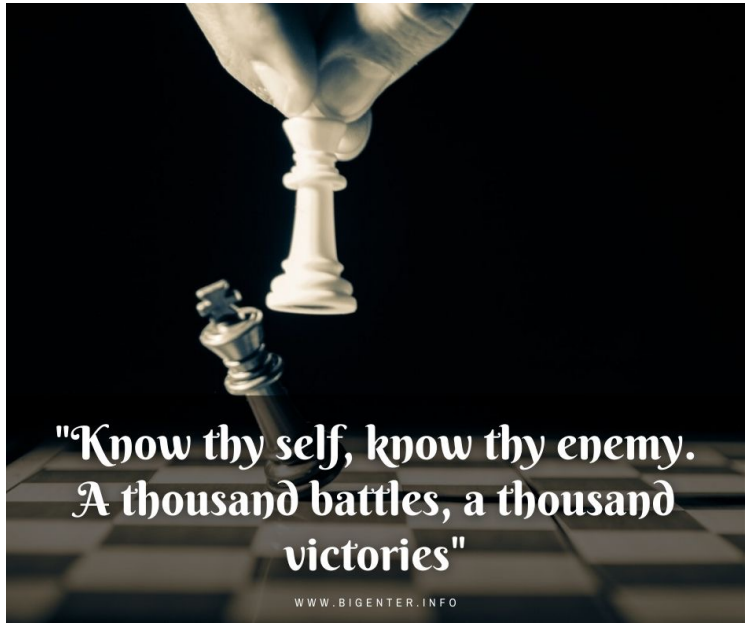
TIBER-EU BASICS



TIBER-EU BASICS

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

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


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

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/josemiguelesparza

@EternalTodo

jose.esparza@blueliv.com