CyberSecDome added values from a pilot OTE Group

Fotis Stathopoulos
fstathopoulos@ote.gr

Info Day Athens

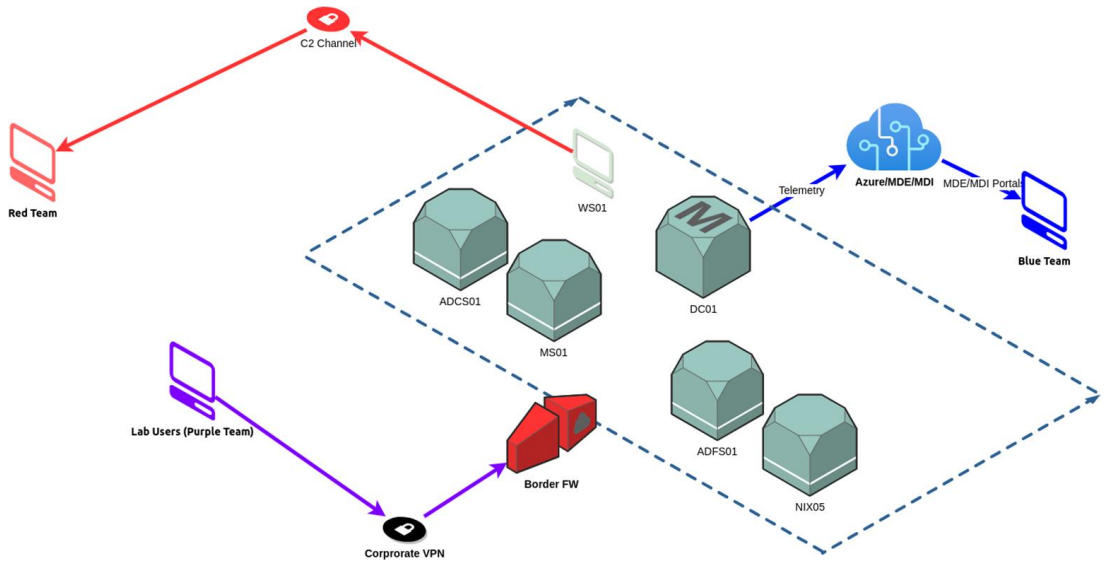
4th December 2024

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101120779

OTE Pilot: Responsibilities

OTE Responsibilities :

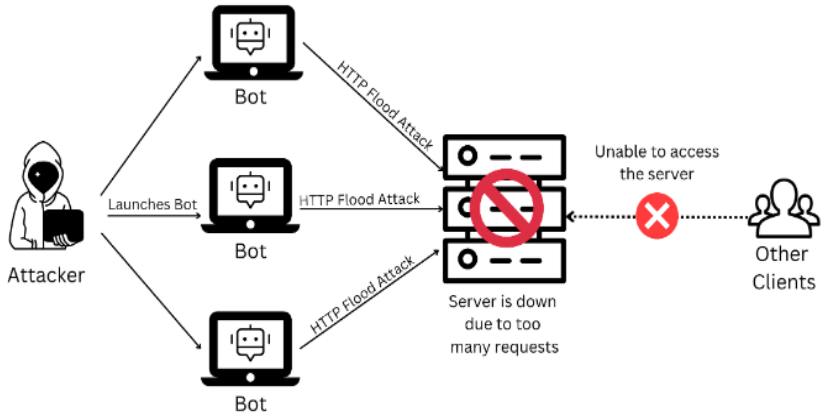
- Provide **Infrastructure**
- Provide/execute **use case attack scenarios**
- **Test the security tools** developed by the project consortium
  - IDPS tool, Automatic Pentest tool, Risk Assessment tool, Prophesy (SIEM)
- **Evaluate** the CyberSecDome platform



OTE Pilot: Use Cases

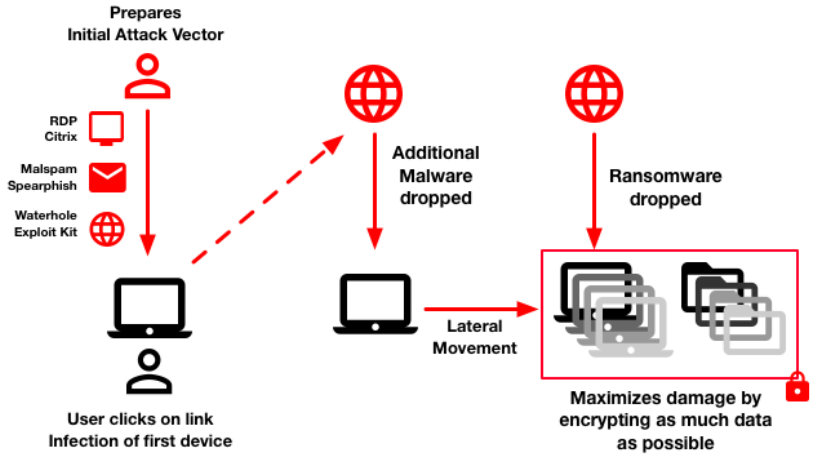
Use Case #01: DDoS attack scenario

Layer 7 DDoS attack (or application attack) that will target a specific service instead of an entire network. This type of DDoS is becoming increasingly more common than broad network attacks.



Use Case #02: Ransomware attack scenario

Crypto ransomwares encrypts all or some files on a computer and demands a ransom from the victim in exchange for a decryption key. Some newer variants also infect shared, networked and cloud drives. Crypto ransomware spreads through various means, including malicious emails, websites and downloads



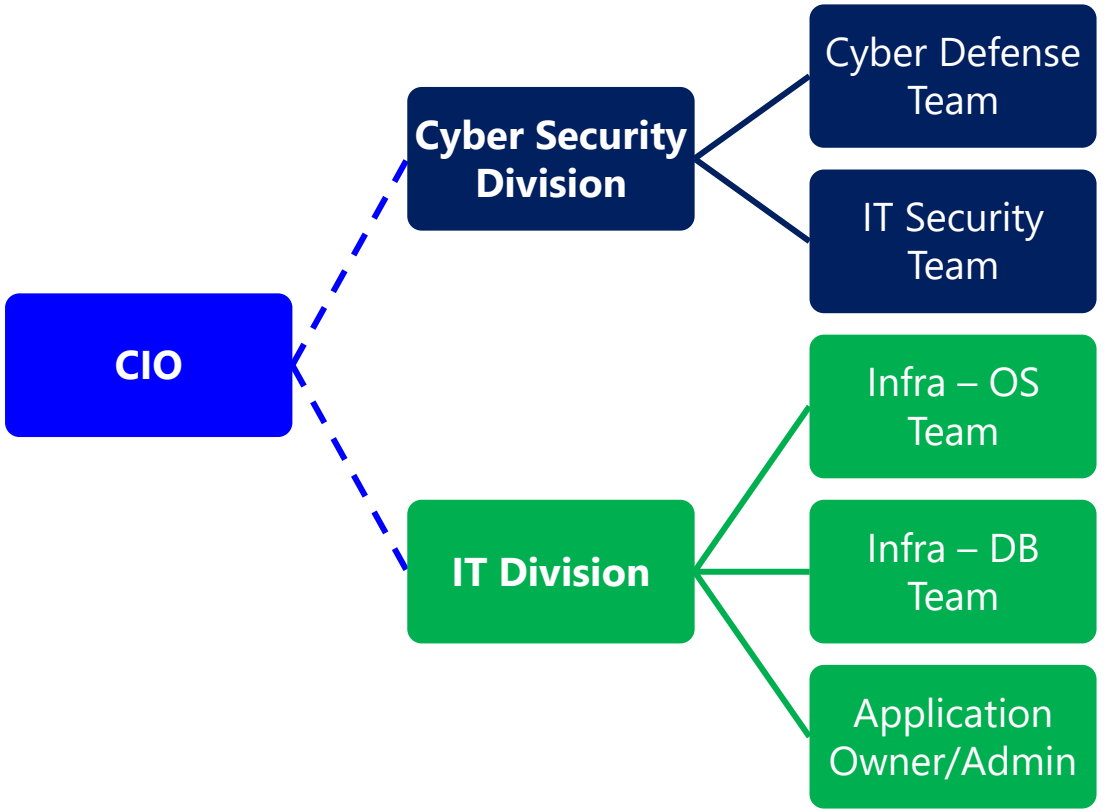
OTE Pilot: Use Cases Roles

Attacker - orchestrate the attack

Cyber Defense Team - identify, assess and respond to the incident

IT Security Team - take actions for stopping the attack

Infra Administrator (OS/DB/APP) - apply mitigation actions, if necessary, according to guidelines given by IT Security Team



OTE Pilot: Assets

Scenario	Assets	Security & digital infrastructure	Related processes
Use Case #01: DDoS attack	○ Target Web Server ○ Web Application	○ DDoS Protection Mechanism ○ Web Application Firewall ○ SIEM (Security Information and Event Management)	OTE's Security Incident Management Process
Use Case #02: Ransomware attack	○ Servers ○ Workstations	○ Anti-Malware Mechanisms ○ EDR (End point Detection and Response) ○ SIEM (Security Information and Event Management)	OTE's Security Incident Management Process

OTE Pilot: Benefits

OTE Benefits:

- **Strengthen our security posture against new types of cyber-attacks** by using up-to-date detection and prediction tools
- **Improve our cybersecurity systems in specific directions**:
  - Reduce the amount of time to detect an incident
  - Reduce the downtime during an incident
  - Improve the absolute number of reported incidents

Contact

Fotis Stathopoulos
fstathopoulos@ote.gr

Dimitris Papanikas
dpapanikas@ote.gr