EIGHTBELLS

vDPI

Real-time Unified Network Threat Management

Eight Bells

Who We Are | What We Do

- Research and Development Company based in Nicosia
- Technology focused in multi-disciplinary areas of research
- Cyber-Security, 5G, Smart-Grids, AI, Networks
- Emmanouil Kafetzakis, Co-Founder, Principal Analyst
- Ioannis Giannoulakis, Co-Founder, Principal Analyst
- Marios Spinthiras, Chief Technology Officer

Ransomware Attacks

What are Ransomware attacks?

- Cyber-extortion designed to hold data hostage for money.

- A form of Malware that infects a device and encrypts its data.

- Prevents user from accessing data until a ransom is paid.

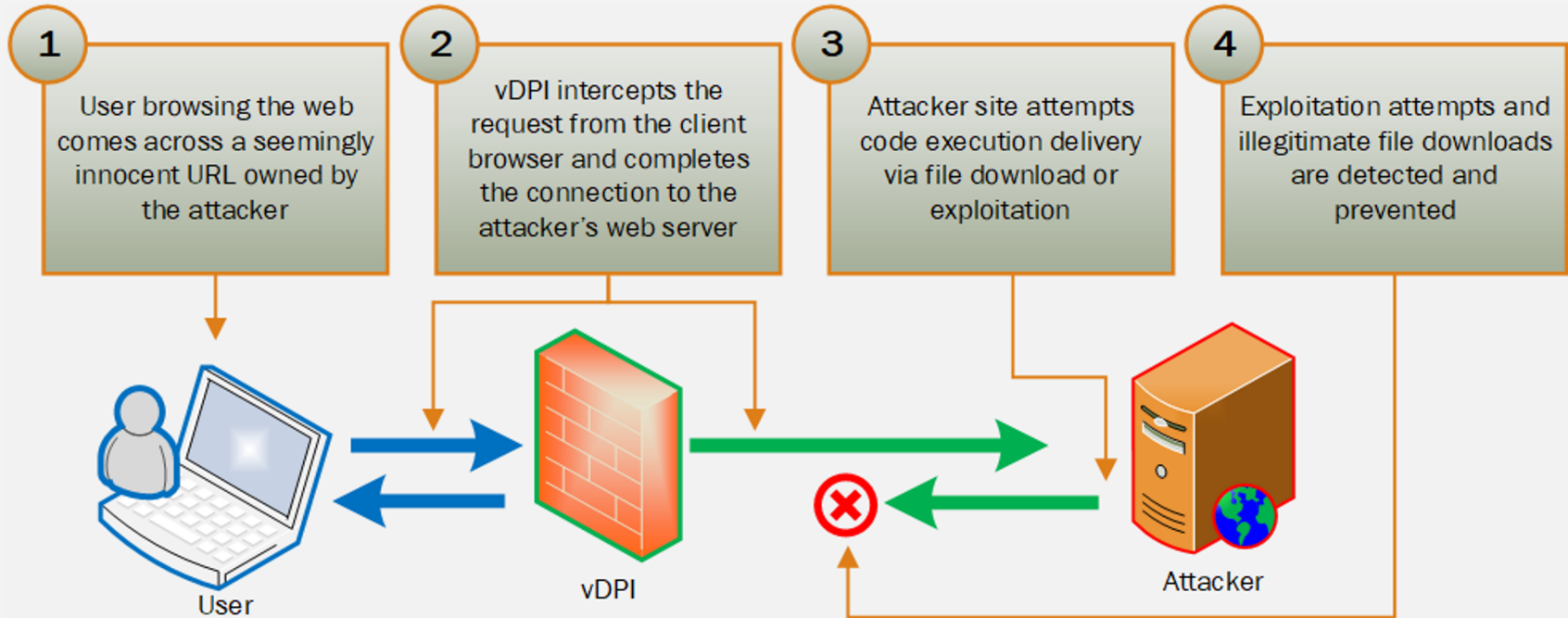- Time based. If ransom is not paid data may be lost.

Ransomware Attacks

The Anatomy of a Ransomware Attack

- **Web**: User file downloads and Browser exploitation.

- **Mail**: Attachment Executable and Exploit Downloads.

- **Laterally**: Infected device infects other nearby devices.

- **Tor**: Downloaded during infection stage to notify Attacker.

Infection via Web

How Ransomware is detected and prevented

1 User browsing the web comes across a seemingly innocent URL owned by the attacker

2 vDPI intercepts the request from the client browser and completes the connection to the attacker's web server

3 Attacker site attempts code execution delivery via file download or exploitation

4 Exploitation attempts and illegitimate file downloads are detected and prevented
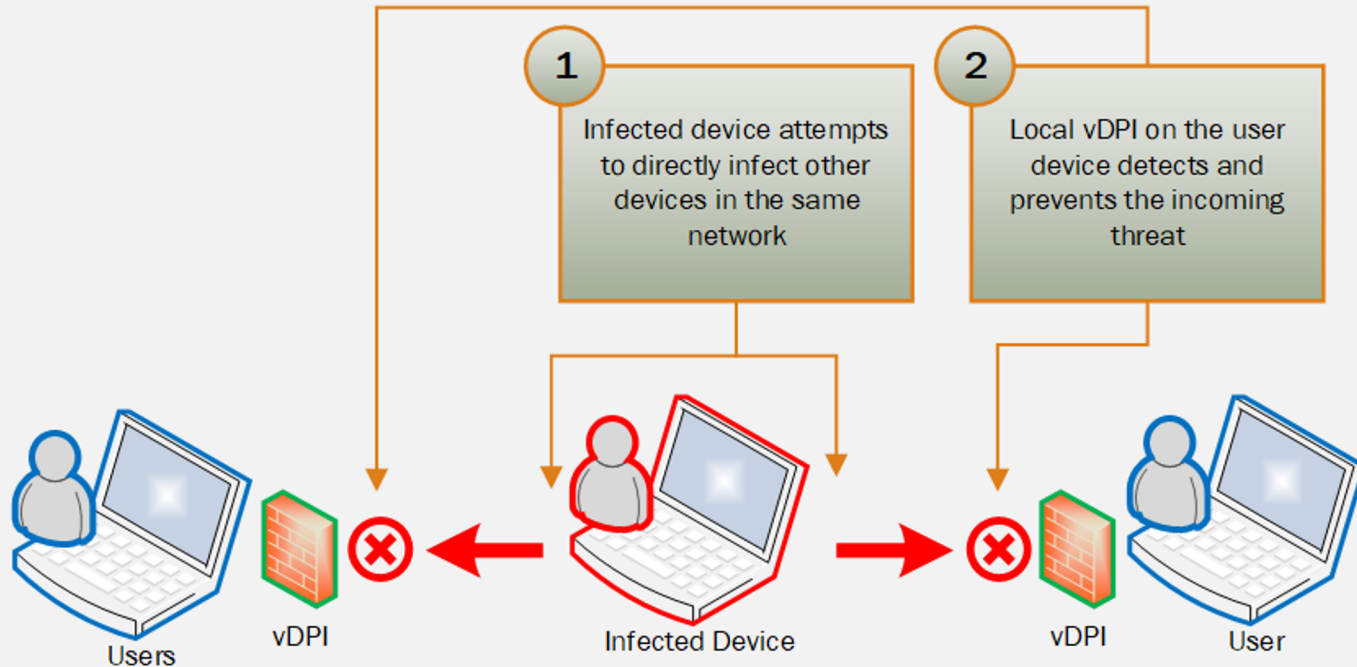
User

vDPI

Attacker

Infection via Email

How Ransomware is detected and prevented
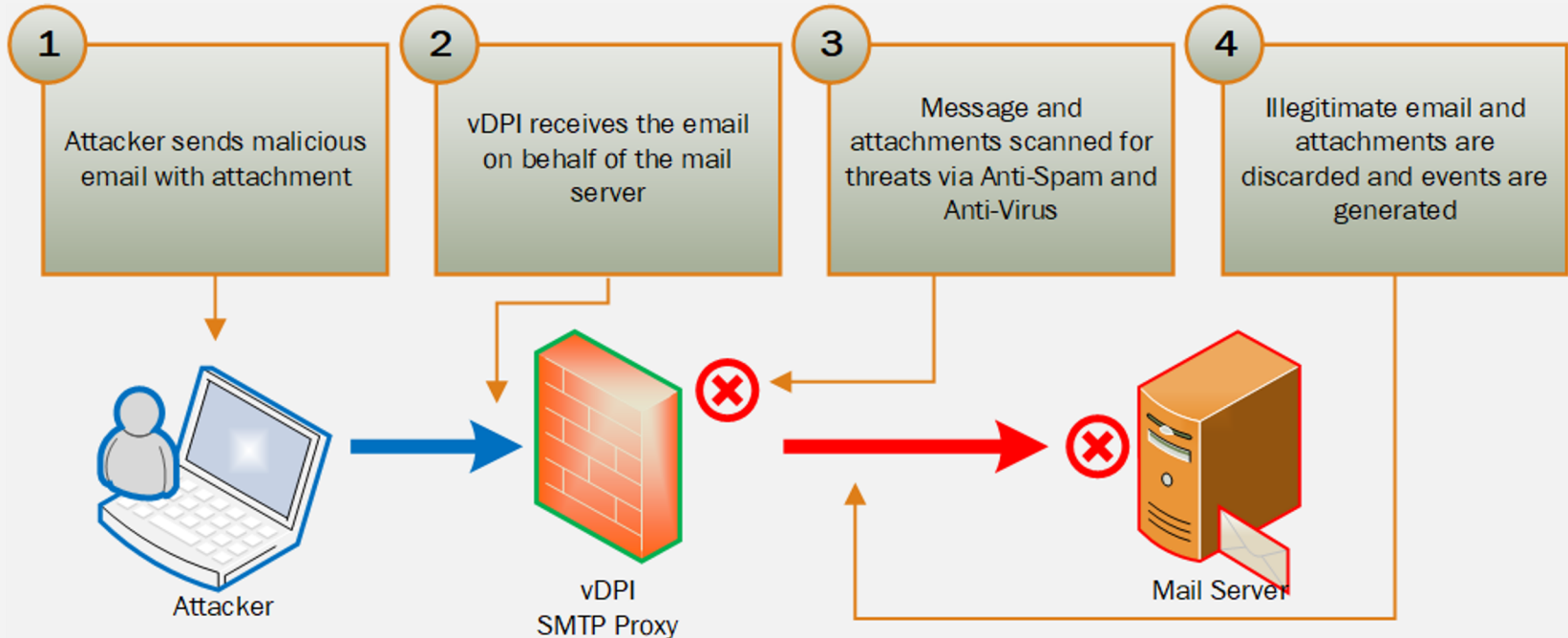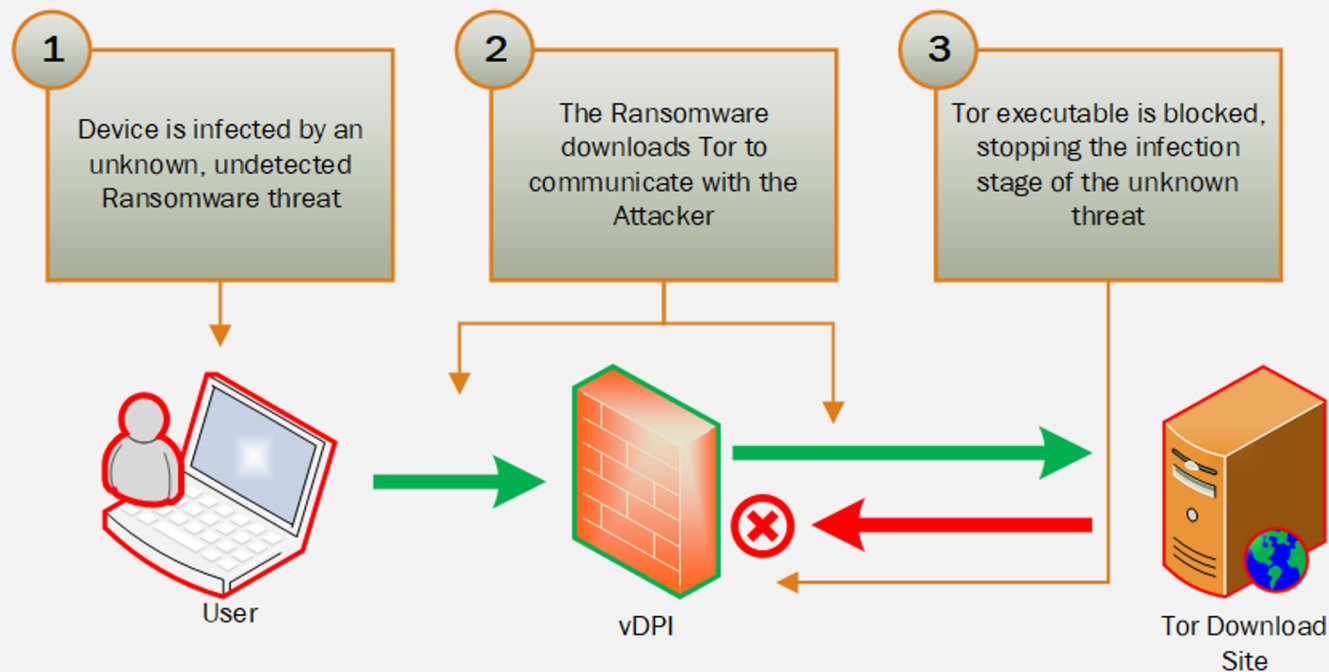
Infection via Lateral movement

How Ransomware is detected and prevented

Tor Activity

How Ransomware is detected and prevented

vDPI UTM Security Appliance

Real-time Unified Network Threat Management

- Situated in the middle and edge of the network for full protection

- Network-wide Threat Detection and Prevention (NIDS/NIPS/NSM)

- Advanced (Layer 2-7) Policy Enforcing Firewall

- Unified Events, Alerts and Reports Web Console