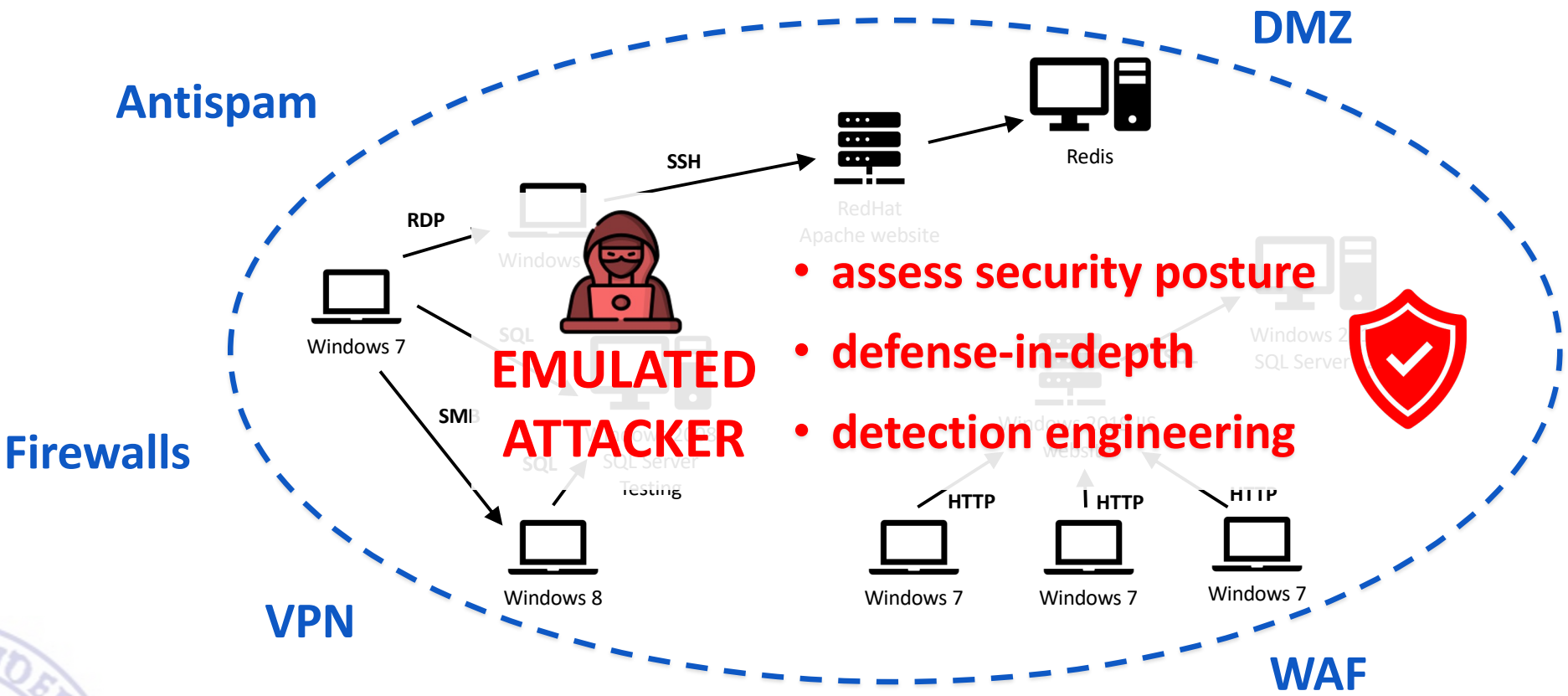
Automating Adversary Emulation of Advanced Persistent Threats

Roberto Natella – Università degli Studi di Napoli Federico II

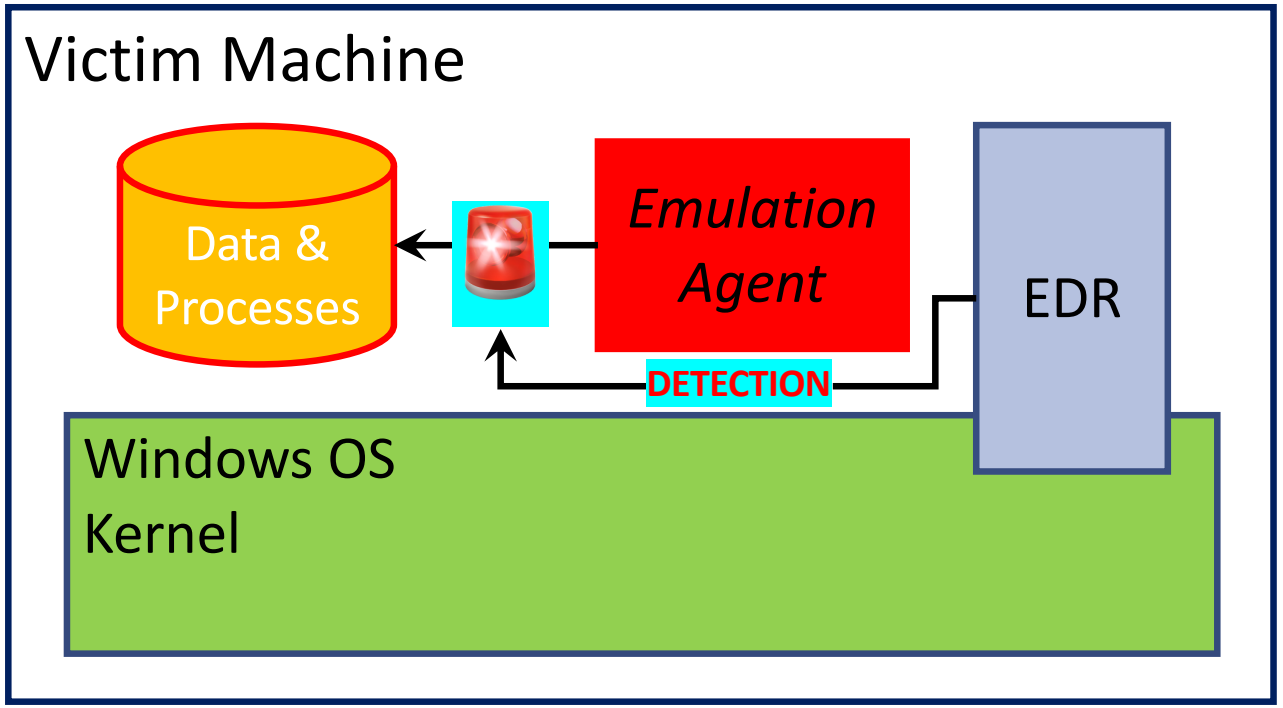
Advanced Persistent Threats (APTs)

- **Calculated** attacks against high-value targets
- Steal information, sabotage infrastructure
- **Stealthy**, can hang around for months/years

Adversary Emulation



Adversary emulation – pain points



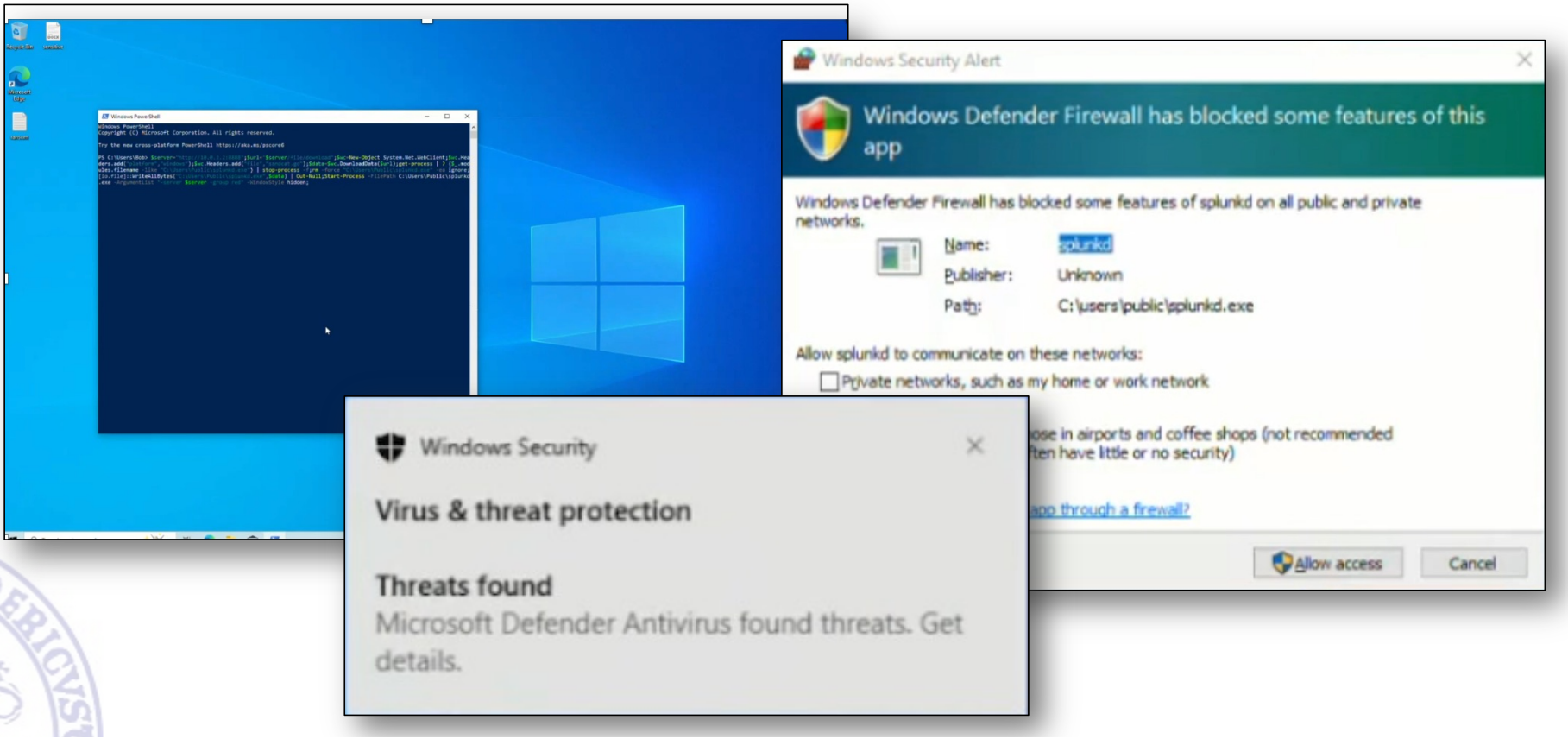
Cumbersome to deploy

Lack anti-detection abilities of real attackers

Easily noticed by defenders

Adversary emulation – pain points

splunkd.exe (impersonates a malicious executable)



Our solution: Laccolith

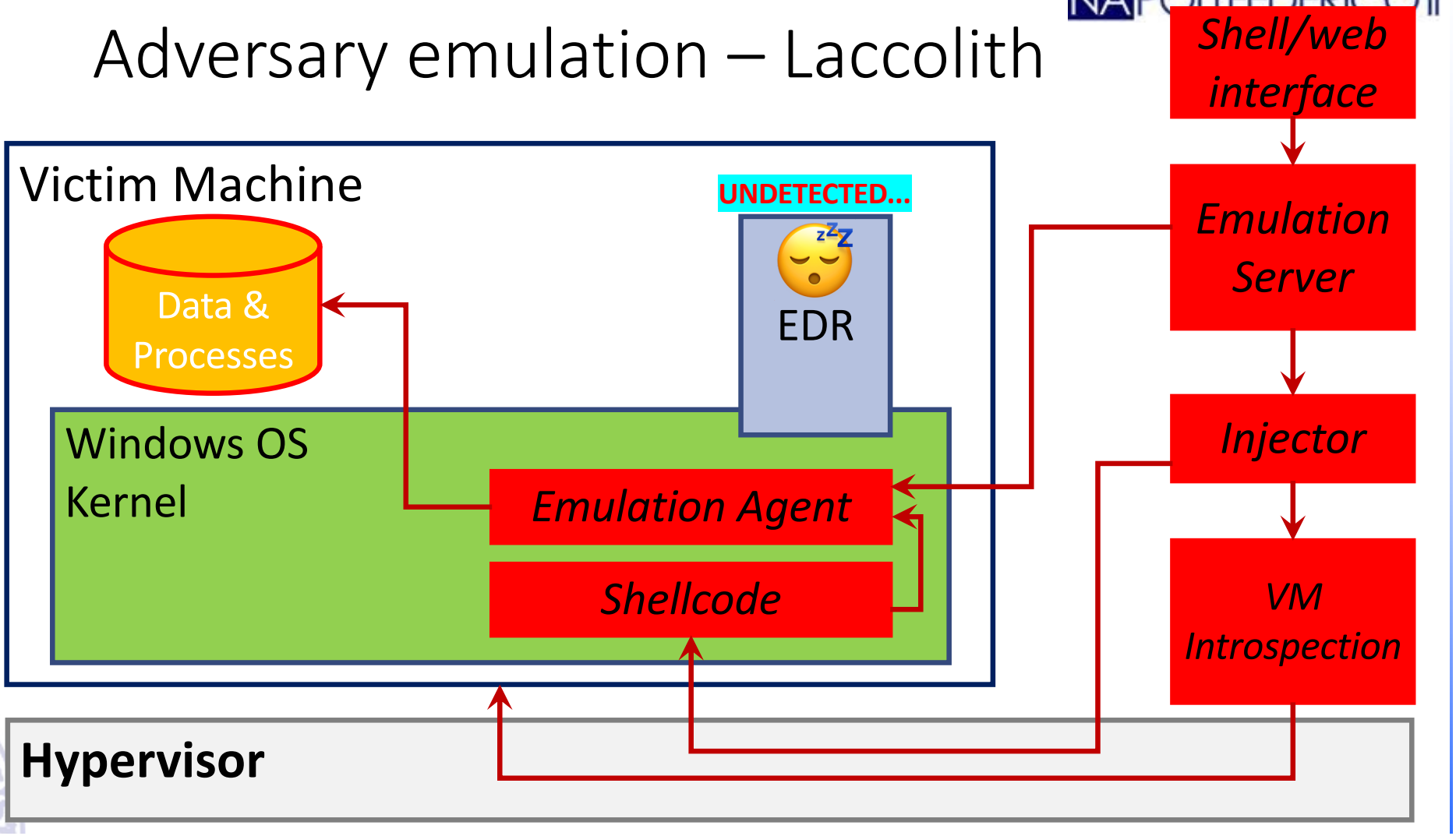
Hypervisor-based Adversary Emulation

Evades EDR products (like real attackers do!)

Support for sophisticated **attacker profiles**

As in volcanic phenomena, we inject **malicious actions from the lower layers** of the software stack.

Adversary emulation – Laccolith



Anti-detection - Laccolith

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

undetected activities ("execution progress")

Profile	Windows Defender	Avast	AVG	Kaspersky	Avira
Thief	3/3	3/3	3/3	3/3	3/3
Op-2	4/4	4/4	4/4	4/4	4/4
Ransomware	5/5	5/5	5/5	5/5	5/5
Shares Hunter	7/7	7/7	7/7	7/7	7/7

Comparison with CALDERA

undetected activities ("execution progress")

Profile	Windows Defender	Avast	AVG	Kaspersky	Avira
Discovery	9/9	9/9	9/9	9/9	9/9
Hunter	14/14	14/14	14/14	14/14	14/14
Ch					
Colle					
Enum					
Nosy N					
Signed Binary					
Super Spy	11/11	11/			
Undercover	1/2	1/2	1/2	1/2	2/2
Stowaway	1/2	1/2	1/2	1/2	2/2
Worm	1/9	1/9	1/9	1/9	9/9
You Shall (Not) Bypass	2/4	2/4	2/4	1/4	1/4
Ransomware	5/5	5/5	5/5	5/5	5/5

CALDERA (open-source adversary emulation tool) is **unable to evade EDRs**

Caldera Profile	Detected Ability
Undercover	Install PowerShell Core 6
Stowaway	Inject Sandcat into Process
Worm	Run PowerKatz
You Shall (Not) Bypass	Wow64log DLL Hijack
You Shall (Not) Bypass	Bypass UAC Medium

Laccolith – Commercial developments

- Laccolith is being incorporated into a **commercial product** for adversary emulation
  - Support for multiple hypervisors and guest OSes
  - Integration with cyber-ranges and other products
  - Curated repository of APTs
- New university spin-off (**Secureware s.r.l.**)