



UNIVERSITÀ DEGLI STUDI DI NAPOLI  
FEDERICO II

itee<sup>PhD</sup>  
information technology  
electrical engineering



Vittorio Orbinato

# A Cyber Threat Intelligence-driven Framework for Adversary Emulation

Tutor: prof. Domenico Cotroneo  
Cycle: XXXVI

co-Tutor: prof. Roberto Natella  
Year: Third

# Background information

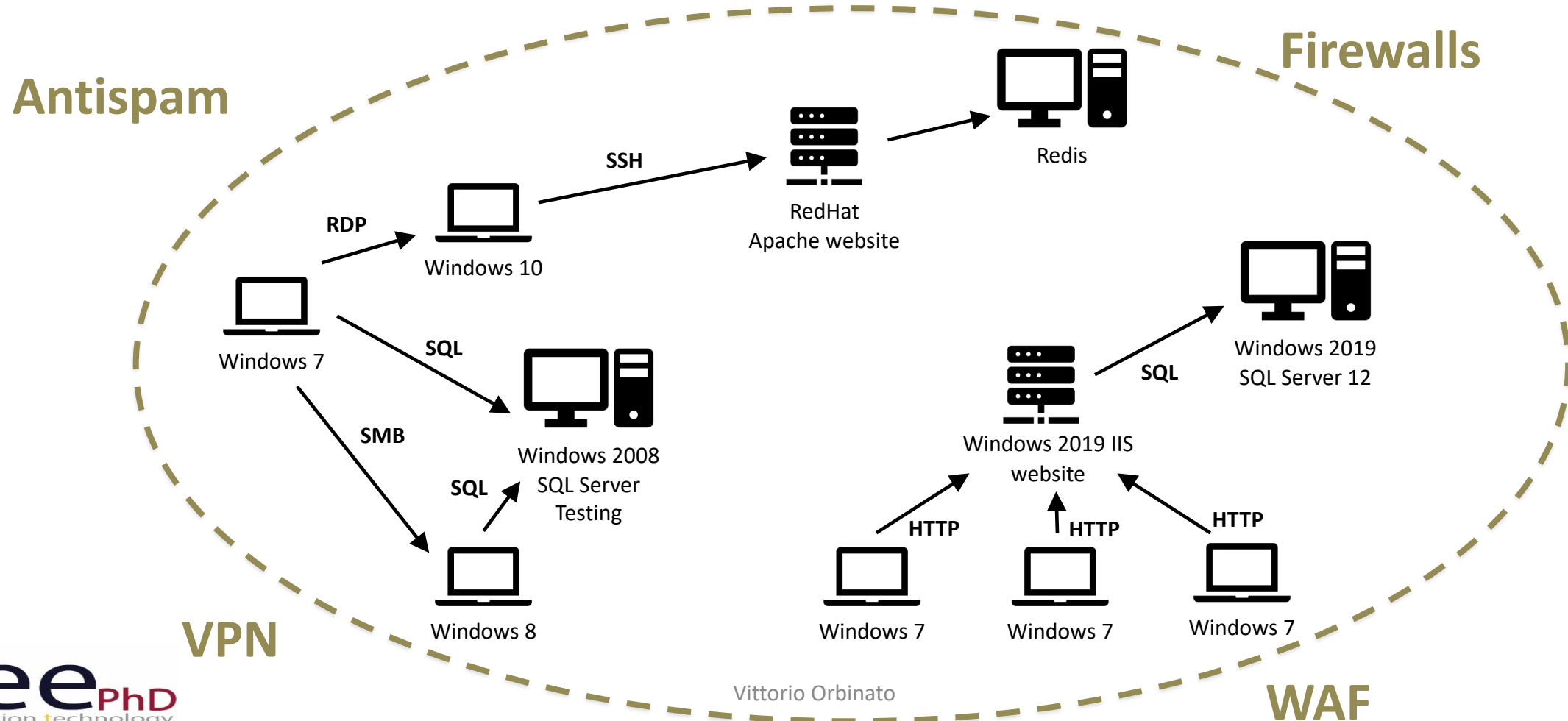
- MSc degree: Computer Engineering
- Research group: DESSERT
- PhD start date – end date: 01/11/2020 – 31/10/2023
- Scholarship type: MUR PON (“Dottorati Innovativi con Caratterizzazione Industriale”)
- Partner company: System Management S.p.A.
- Periods abroad: 18/05/2022 – 19/12/2022 @ University of Coimbra, Portugal
- Periods in company: 01/03/2022 – 30/04/2022, 01/01/2023 – 30/06/2023 @ System Management S.p.A., Napoli, Italy

# Summary of study activities

- Ad-hoc Courses:
  - Scientific programming and visualization with Python
  - Strategic Orientation for STEM Research and Writing
  - Virtualization Technologies and their Applications
- M.Sc. Degree Courses:
  - Intelligenza Artificiale
  - Data Management
- Ph.D. Schools:
  - 5G International PhD School

# Research area

My research field concerns **proactive security paradigms** for security assessment and training. In particular, the focus of my research is **Adversary Emulation**.



# Research results

My research activity led to the following results:

- Definition of a CTI-driven approach for Adversary Emulation
- Design and development of a realistic solution for Adversary Emulation

# Research products

## Published conference papers

[C1]	V. Orbinato, <i>A next-generation platform for Cyber Range-as-a-Service,</i> <b>2021 IEEE 32<sup>nd</sup> International Symposium on Software Reliability Engineering Workshops (ISSREW) ,</b> Wuhan, China, Oct. 2021, pp. 314-318, 2021
[C2]	P. Liguori, E. Al-Hossami, V. Orbinato, R. Natella, S. Shaikh, D. Cotroneo, B. Cukic, <i>EVIL: Exploiting Software via Natural Language,</i> <b>2021 IEEE 32<sup>nd</sup> International Symposium on Software Reliability Engineering (ISSRE) ,</b> Wuhan, China, Oct. 2021, pp. 321-332, 2021
[C3]	V. Orbinato, M. Barbaraci, R. Natella, D. Cotroneo, <i>Automatic Mapping of Unstructured Cyber Threat Intelligence: An Experimental Study,</i> <b>2022 IEEE 33<sup>rd</sup> International Symposium on Software Reliability Engineering (ISSRE) ,</b> Charlotte, North Carolina, Oct./Nov. 2022, pp. 181-192, 2022

# Research products

## Under review

[J1]	V. Orbinato, M. C. Feliciano, D. Cotroneo, R. Natella, <i>Laccolith: Hypervisor-Based Adversary Emulation with Anti-Detection</i> , <b>IEEE Transactions on Dependable and Secure Computing (TDSC)</b>
[J2]	V. Casola, A. De Benedictis, C. Mazzocca, V. Orbinato, <i>Secure Software Development and Testing: a Model-based Methodology</i> , <b>Computers &amp; Security, Elsevier</b>
[C4]	V. Orbinato, F. C. Grasso, R. Natella, D. Cotroneo, <i>Vulnerability Prediction on Binary Code via Neural Decompilation</i> , <b>The 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)</b>

# PhD thesis overview: Problem

My research activity was focused on addressing the two main problems of Adversary Emulation:

- Lack of integration with Cyber Threat Intelligence (CTI)
- Emulation solutions not representative of actual attackers and scenarios



# PhD thesis overview: Objective

The objective of the thesis is to define a comprehensive framework for CTI-driven Adversary Emulation that enables:

- **Automatic extraction of attack techniques from CTI documents to generate APT emulation plans**
- **Realistic emulation of APTs**

# PhD thesis overview: Methodology

The following methodology was applied to address the problems of Adversary Emulation:

- Literature analysis
- Experimental evaluation of state-of-the-art solutions
- Design and development of the proposed solution
- Experimental evaluation to assess effectiveness of the solution

# PhD thesis

My PhD thesis presents two main contributions:

1. Automatic CTI Analysis to Generate Emulation Plans
2. A Novel Solution for Adversary Emulation with Anti-Detection

# Contribution 1:

## Automatic CTI Analysis to Generate Emulation Plans

# Problem: Lack of integration with CTI

- APTs are highly skilled and resourceful, making it challenging to replicate their tactics and techniques accurately.
- Adversary Emulation should be driven by Cyber Threat Intelligence, i.e., information on the capabilities and intents of attackers and the techniques adopted in their campaigns.

# Problem: Lack of integration with CTI

CTI still comes in unstructured forms: extracting relevant information from unstructured documents requires manual effort.

All threat groups generally follow a broad operational framework known as the Attack Lifecycle. While the phases of the Attack Lifecycle — from initial compromise to privilege escalation to maintaining presence and completing the mission — are remarkably consistent, the specific TTPs used vary widely based on a group's skills, motivations and ultimate goals.

1 After gaining access with valid credentials, we observed FIN6 leveraging components of the Metasploit Framework to establish their foothold. For example, in one case, FIN6 used a Metasploit PowerShell module to download and execute shellcode and to set up a local listener that would execute shellcode received over a specific port. Similarly, FIN6 used at least two downloaders called HARDTACK and SHIPBREAD (apparent variations on Metasploit payloads) to establish backdoor access to the compromised environment. Both of these tools are configured to connect to remote command

and control (CnC) servers and download and execute shellcode. FIN6 generally used either registry run keys or Windows scheduled tasks in order to establish persistence or these tools.

2

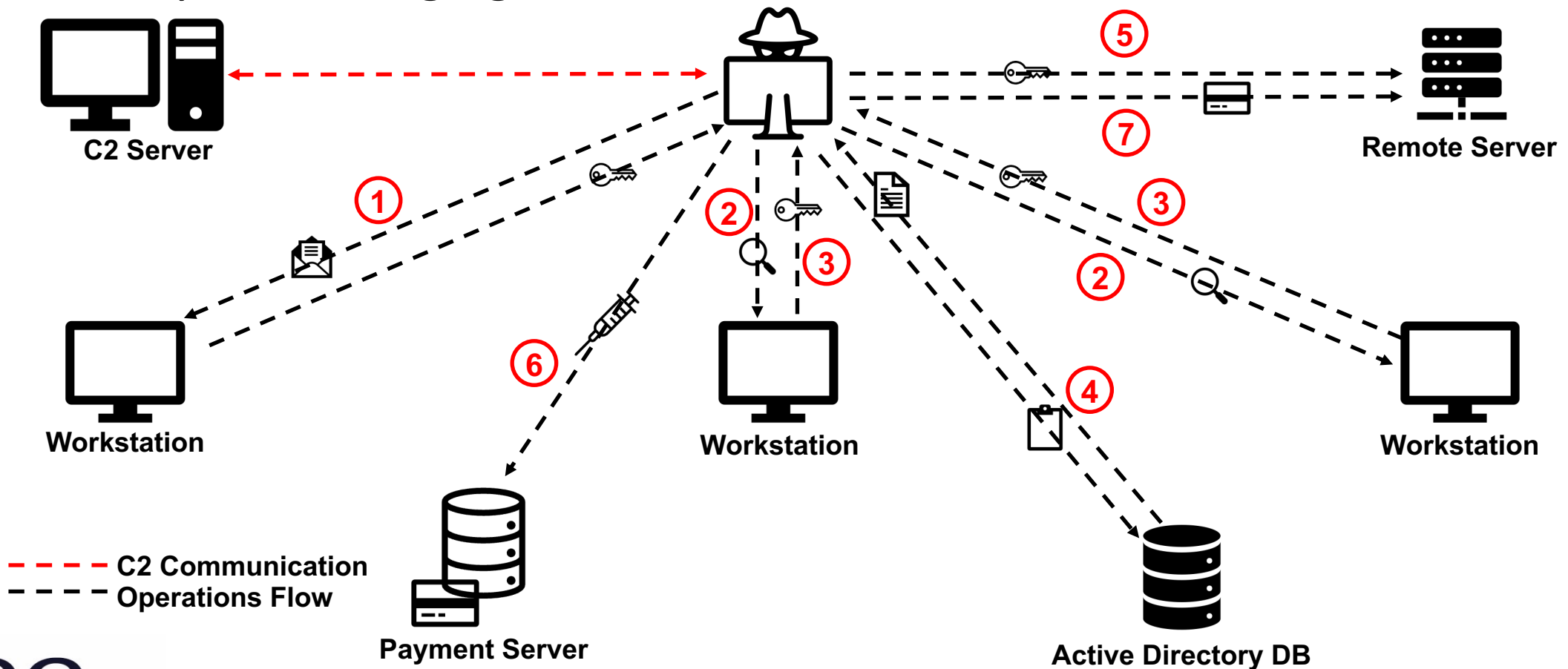
Once their accesses were established with preferred backdoors FIN6 used additional public utilities such as Windows Credentials Editor for privilege escalation and credential harvesting. Additional privilege escalation tools exploited Microsoft Windows vulnerabilities in an attempt to compromise privileged account credentials on various hosts. The tools targeted CVE-2013-3660, CVE-2011-2005 and CVE-2010-4398, all of which could allow local users to access kernel-level privileges.<sup>2</sup> Continuing their use of Metasploit-related tools, FIN6 also used Metasploit's PsExec NTDSGRAB module to obtain a copy of the Active Directory database (ntds.dit). Access to this file would allow them to extract password hashes from the file and crack them offline.

3

4

# Problem: Lack of integration with CTI

Replicating the tactics and techniques employed by advanced threat actors accurately is challenging.



# Existing literature

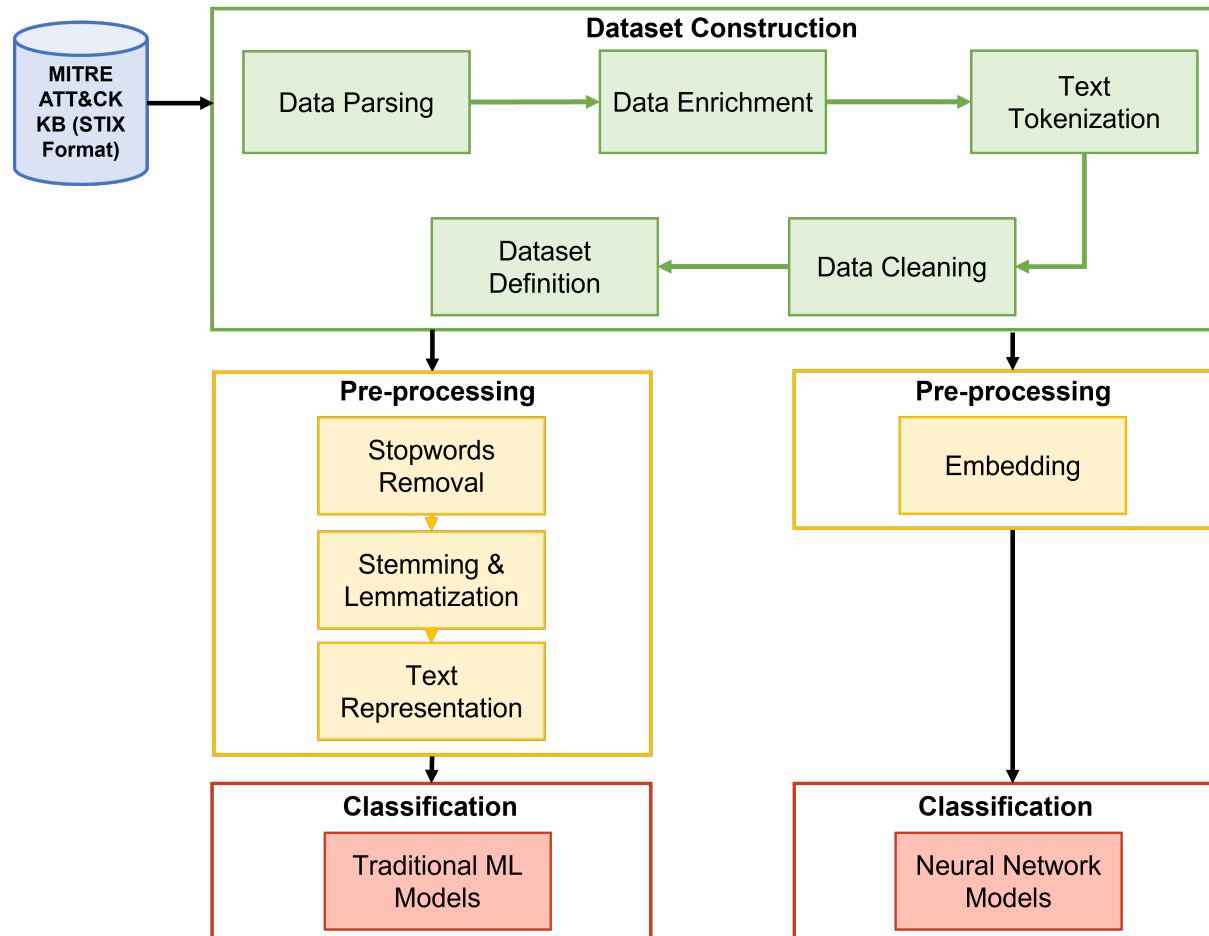
The existing literature lacks the capability to extract information about the specific actions performed by APTs, useful to replicate their behavior.

Work	Categorization	Standardized taxonomy
TIM [1]	Attack categories	None
EXTRACTOR [2]	System entity names + actions	None
TTPDrill [3]	Threat actions	MITRE ATT&CK
ActionMiner [4]	Low-level actions	None
Ampel et al. [5]	Tactics	MITRE ATT&CK



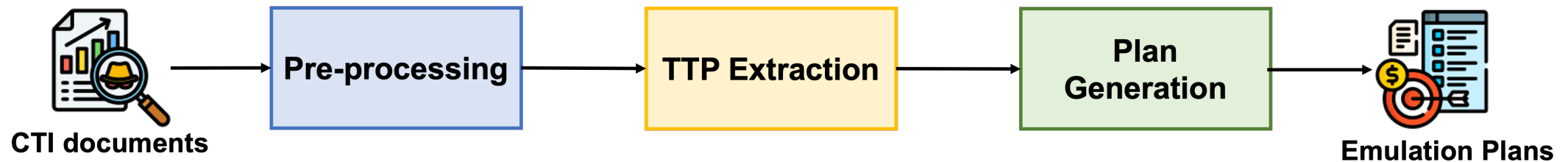
# Contribution

- Experimental study on the automatic classification of Cyber Threat Intelligence



# Contribution

- **CTI-driven pipeline for Adversary Emulation**
  - Automatic extraction of attack techniques from unstructured CTI
  - Generation of emulation plans to replicate APTs



# Results

- **CTI-driven pipeline to generate Adversary Emulation plans**
  - Tested on real-world CTI documents
  - Compared with emulation plans manually produced by security experts

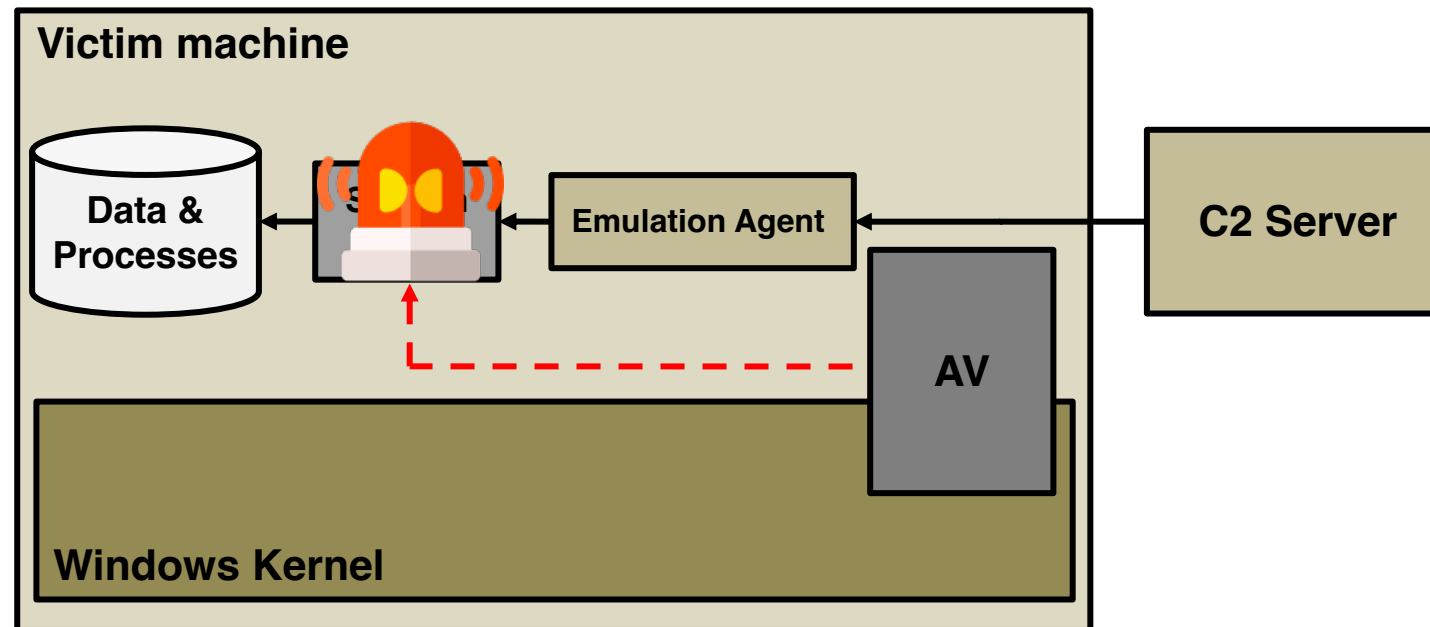
<b>APT</b>	<b>TP/Actual techniques</b>
Carbanak	75%
FIN6	62%
FIN7	28%
MenuPass	85%
Sandworm	40%
WizardSpider	45%

# Contribution 2:

## A Novel Solution for Adversary Emulation with Anti-Detection
















# Problem: Non-representative emulation solutions

- Current solutions are not capable of realistically emulating actual attackers and attack scenarios



# State-of-the-art solutions

- Limited capability to emulate complex realistic attacks

Tool	C2 Server	Complex Attacks	ATT&CK Tactics Coverage				Needs Pre-Installed Agent	Anti-detection
CALDERA	✓			✓	✗			
Atomic Red Team	✗	✗		✓	✗			
Red Team Automation	✗			✓	✗			
APTSimulator	✗			✓	✗			
Infection Monkey	✓			✓	✗			
Metta	✗			✓	✗			
DumpsterFire	✗			✓	✗			
Invoke-Adversary	✗	✗		✓	✗			
Sliver	✓	✗		✓	✗			

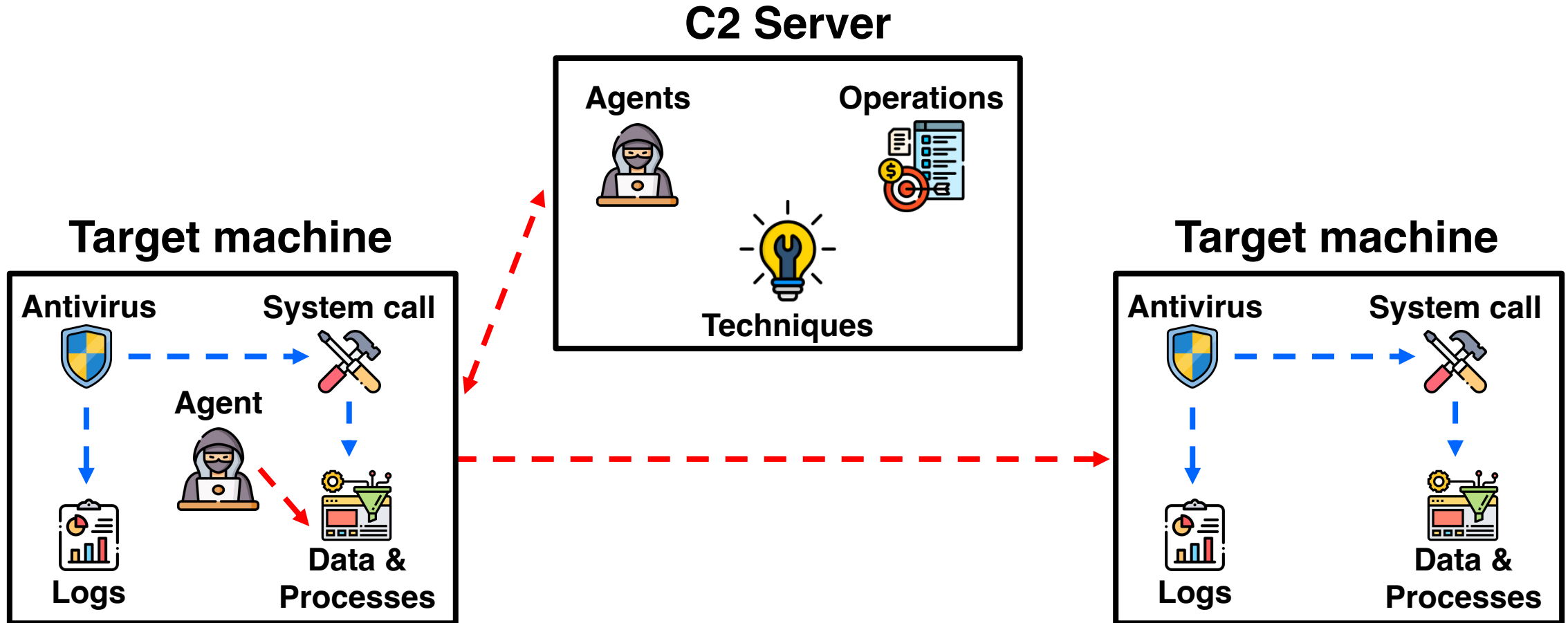
Key:

	Built-in		Collection		Execution		Lateral Movement
	Custom		Credential Access		Exfiltration		Persistence
			Defense Evasion		Impact		Privilege Escalation
			Discovery		Initial Access		

Vittorio Orbinato

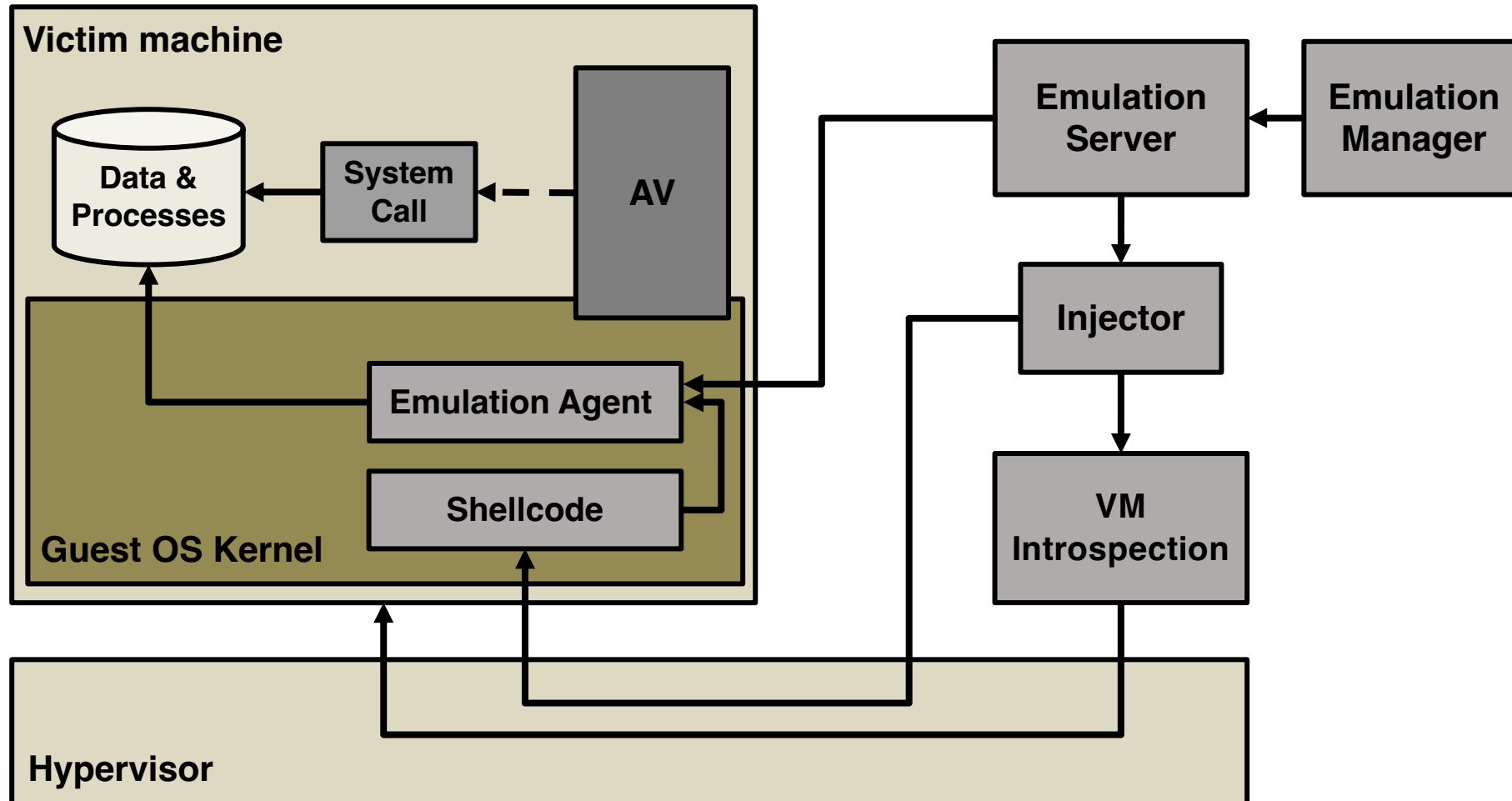
# Contribution

- Experimental evaluation of Adversary Emulation solutions



# Contribution

- Novel solution for Adversary Emulation with anti-detection





# Conclusions

- The integration of CTI into Adversary Emulation practices enables the emulation of APTs
- Adversary Emulation solutions need to overcome the drawbacks of the traditional command-and-control architecture to offer realistic emulation
- For this purpose, a novel solution was devised

# References

- [1] You et al., *TIM: threat context-enhanced TTP intelligence mining on unstructured threat data*, Cybersecurity, Springer, 2022
- [2] K. Satvat et al., *Extractor: Extracting Attack Behavior from Threat Reports*, 2021 IEEE European Symposium on Security and Privacy, 2021
- [3] Husari et al., *TTPDrill: Automatic and Accurate Extraction of Threat Actions from Unstructured Text of CTI Sources*, 33rd Annual Computer Security Applications Conference, 2017
- [4] Husari et al., *Using Entropy and Mutual Information to Extract Threat Actions from Cyber Threat Intelligence*, 2018 IEEE International Conference on Intelligence and Security Informatics, 2018
- [5] Ampel et al., *Linking Common Vulnerabilities and Exposures to the MITRE ATT&CK Framework: A Self-Distillation Approach*, 2021 ACM Conference Knowledge Discovery and Data Mining, 2021

Thank you for your attention