8th IEEE European Symposium on Security and Privacy on Workshop on Active Defense and Deception

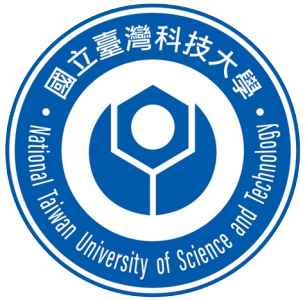
From Prey to Predator: A Use Case for Using Active Defense to Reshape the Asymmetrical Balance in Cyber Defense

Pei-Yu Huang, Washington University in St. Louis

Yi-Ting Huang, National Taiwan University of Science and Technology

Yea li Sun, National Taiwan University

Meng Chang Chen, Academia Sinica



Outline

- Main Idea
- Background & Related Work
- Use Case
- Proposed Active Defense Implementations
- Conclusion
- Future Work
- Q & A

Outline

- Main Idea
- Background & Related Work
- Use Case
- Proposed Active Defense Implementations
- Conclusion
- Future Work
- Q & A

Main Idea

- Cyber-security defenses predominantly rely on a **passive** approach of waiting for adversaries to match predefined rules.
- Active defense involves actively engaging with adversaries to **observe, affect, and elicit** attack behaviors by providing deceptive information.
- We analyzed the TTPs used in a real-world cyber-attack based on the MITRE ATT&CK® framework.
- Then, using the identified TTPs and mapped to the MITRE Engage™ framework, we **identified potential use cases for implementing active defense** as a countermeasure.

Outline

- Main Idea
- Background & Related Work
- Use Case
- Proposed Active Defense Implementations
- Conclusion
- Future Work
- Q & A

What is Active Defense?

With traditional "passive" defense, the attacker only needs to be right once

- **Secure Perimeters**
- **Secure Internal Network**
- **The IP and data within the domain are genuine, and once they are stolen, the attacker wins**

Under active defense techniques, the attacker only needs to be wrong once

- **Secure Perimeters**
- **Secure Internal Network**
- **Not all IPs and data are genuine. Once stolen, there is no guarantee that the attacker wins**

Source: https://engage.mitre.org/

Components of Active Defense

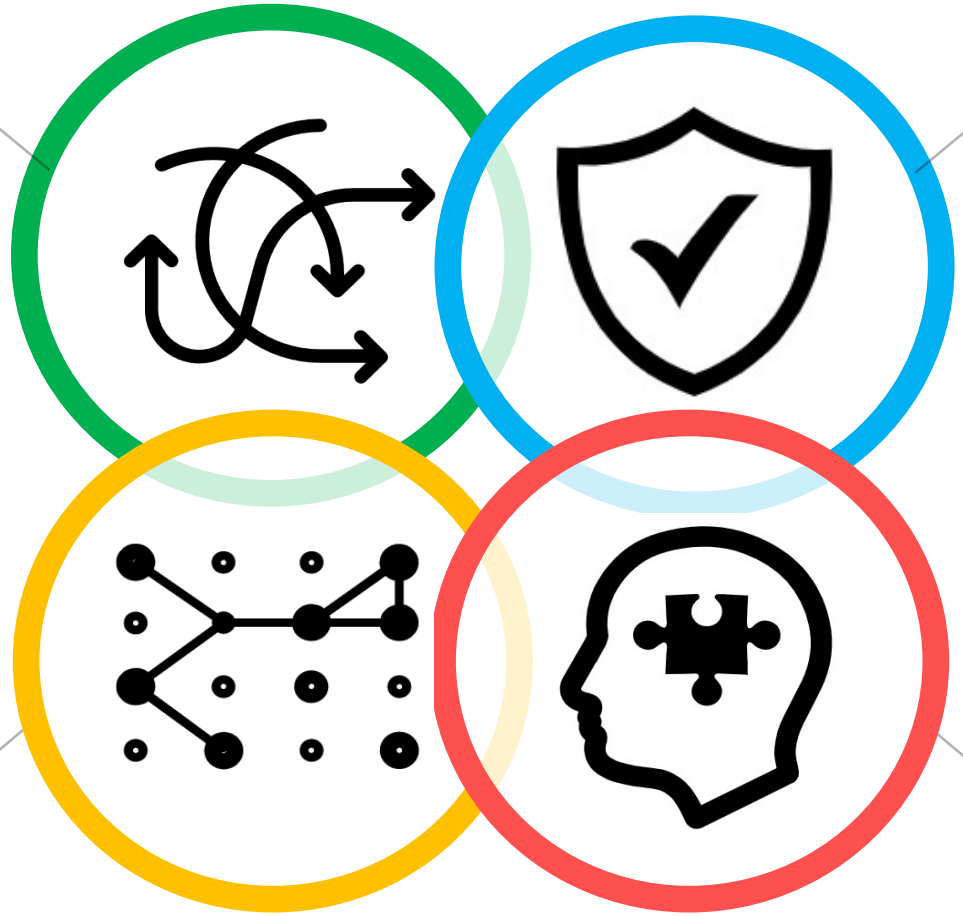
- **Cyber Denial**
  - **Prevent or impair** the adversary's ability to conduct operations
  - **Limit** their movements and collection efforts
  - **Diminish the effectiveness** of their capabilities.
- **Cyber Deception**
  - Intentionally **reveal deceptive facts** and **fictions** to **mislead** the adversary
  - **Conceal critical facts** and **fictions** to prevent the adversary from taking appropriate actions

Active Defense (Adversary Engagement)

- Cyber denial + Cyber deception
- **Negatively impact the adversary**
  - To **expose** adversaries on the network
  - To **elicit** intelligence to learn more about their attack Tactics, Techniques, and Procedures (TTPs)
  - To **affect** the adversary by **impacting** their ability to operate

What can Active Defense do?

Reduce attackers' accuracy in distinguishing between genuine and fake systems.

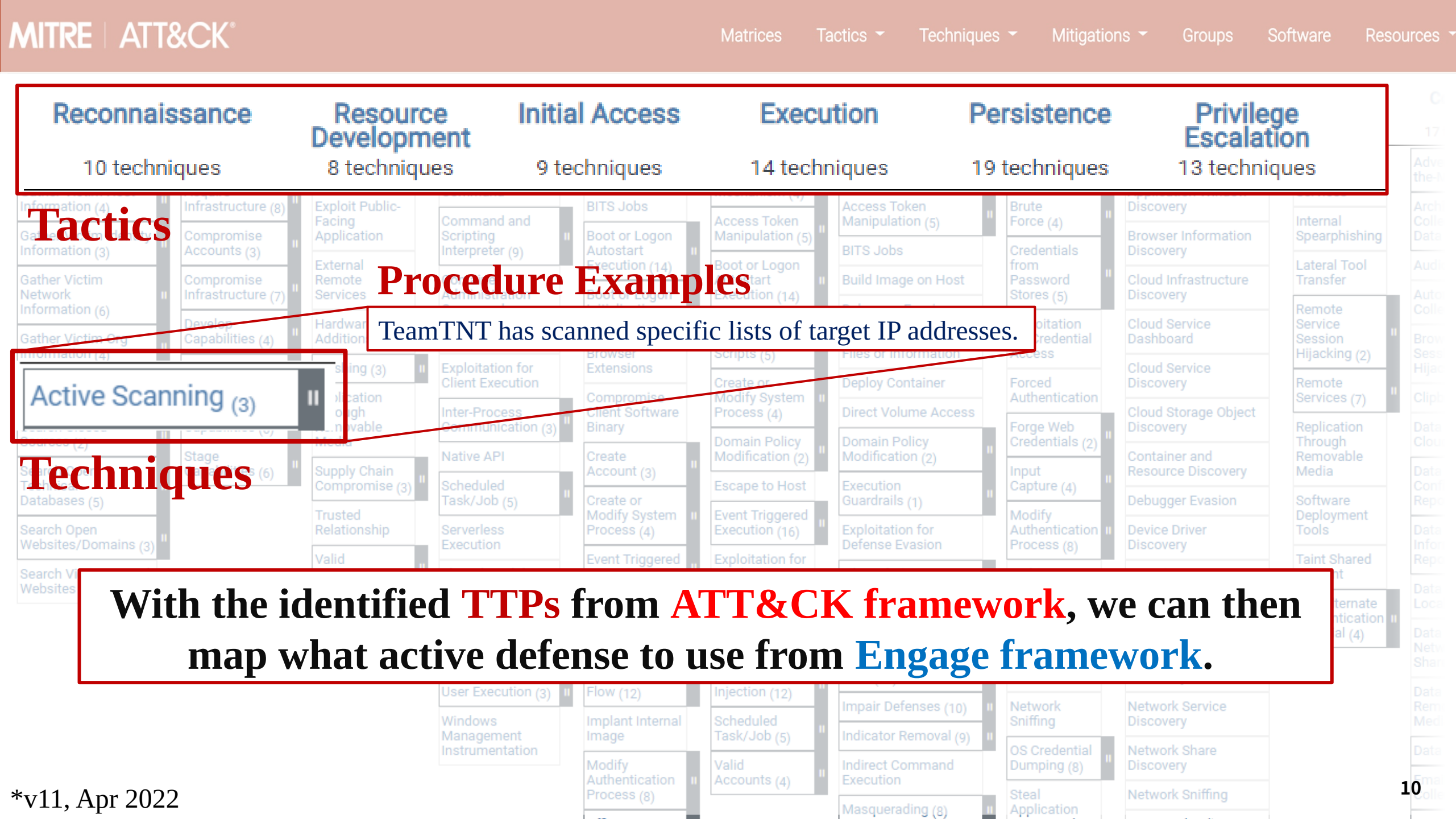


Increase the chance of detecting intrusion in real-time.

Increase the time and cost required for attackers and add complexity.

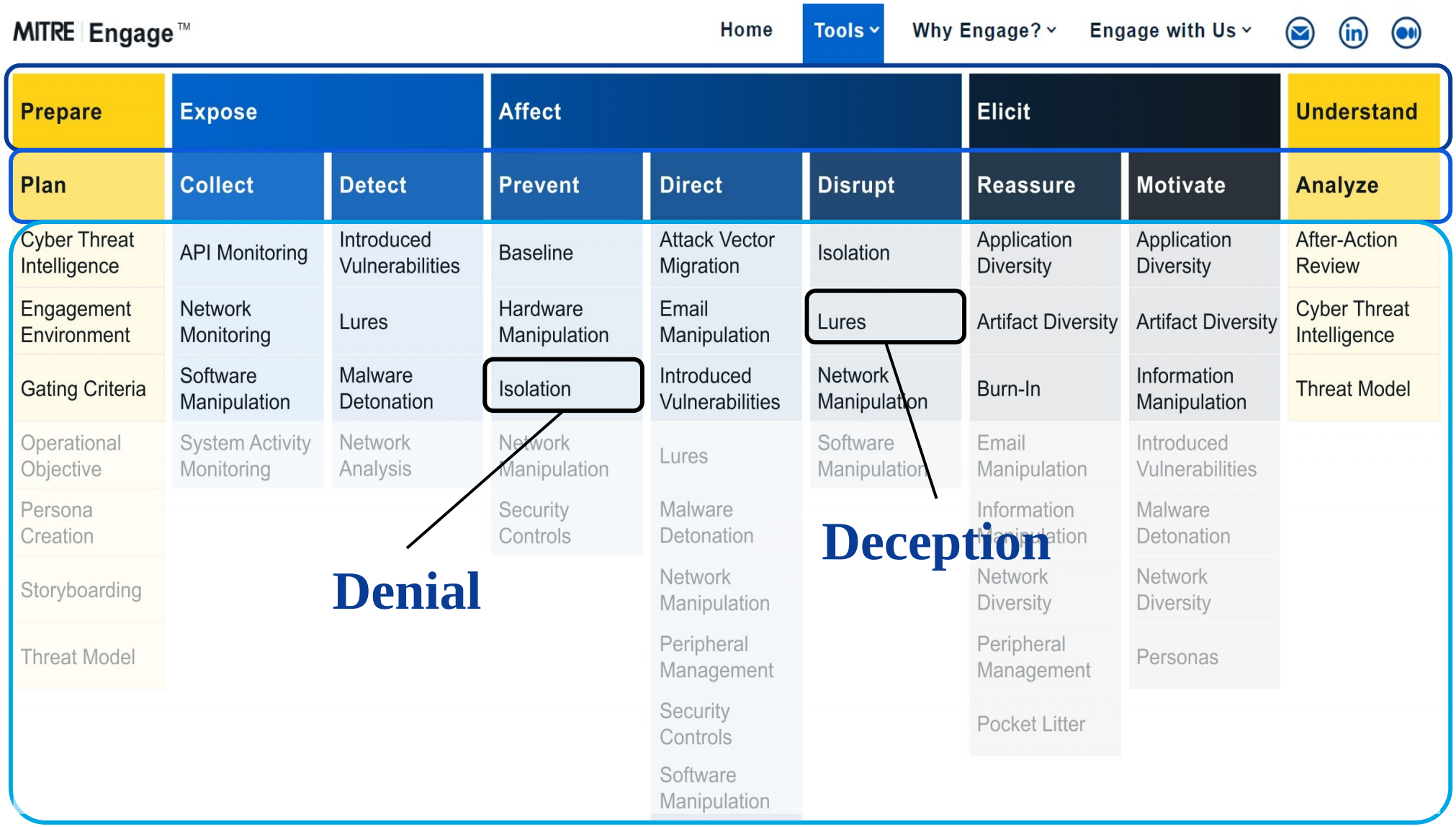
Even if deception are not actually deployed, as long as attackers believe there are, desired effect can still be achieved.

Source: Ferguson-Walter, Kimberly J., Dana S. LaFon, and T. B. Shade. "Friend or faux: deception for cyber defense." Journal of Information Warfare 16, no. 2 (2017): 28-42. and Ferguson-Walter, Kimberly, Temmie Shade, Andrew Rogers, etc. "The Tularosa Study: An Experimental Design and Implementation to Quantify the Effectiveness of Cyber Deception." No. SAND2018-5870C. Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2018.


MITRE | ATT&CK
Matrices
Tactics
Techniques
Mitigations
Groups
Software
Resources
Reconnaissance
10 techniques
Resource Development
8 techniques
Initial Access
9 techniques
Execution
14 techniques
Persistence
19 techniques
Privilege Escalation
13 techniques
Tactics
Procedure Examples
TeamTNT has scanned specific lists of target IP addresses.
Active Scanning (3)
Techniques
With the identified TTPs from ATT&CK framework, we can then map what active defense to use from Engage framework.

*v11, Apr 2022

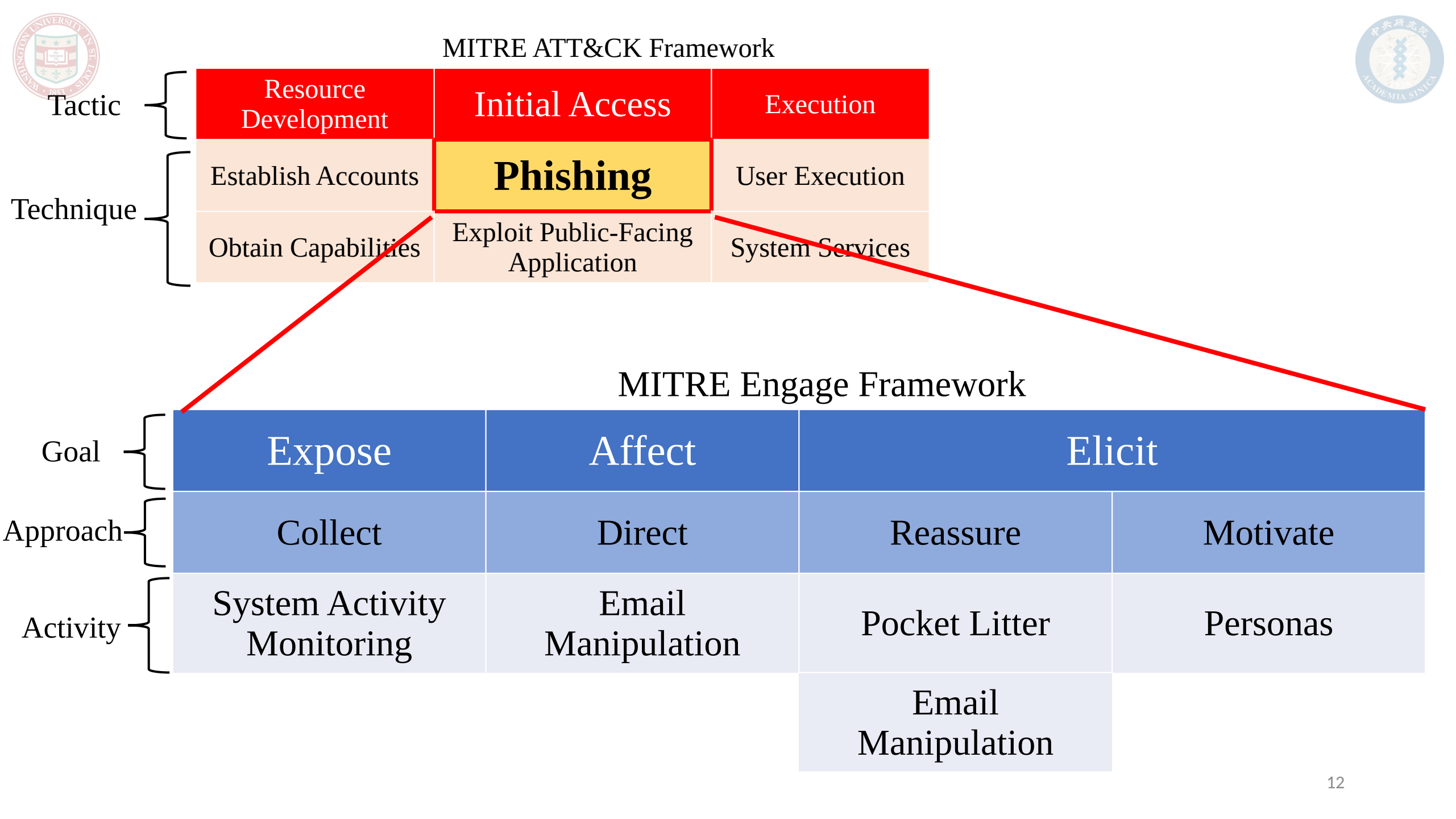
MITRE Engage Framework



5 Goals

9 Approaches

31 Activities


MITRE ATT&CK Framework
Tactic
Technique
Resource Development
Initial Access
Execution
Establish Accounts
Phishing
User Execution
Obtain Capabilities
Exploit Public-Facing Application
System Services
MITRE Engage Framework
Goal
Approach
Activity
Expose
Affect
Elicit
Collect
Direct
Reassure
Motivate
System Activity Monitoring
Email Manipulation
Pocket Litter
Personas
Email Manipulation

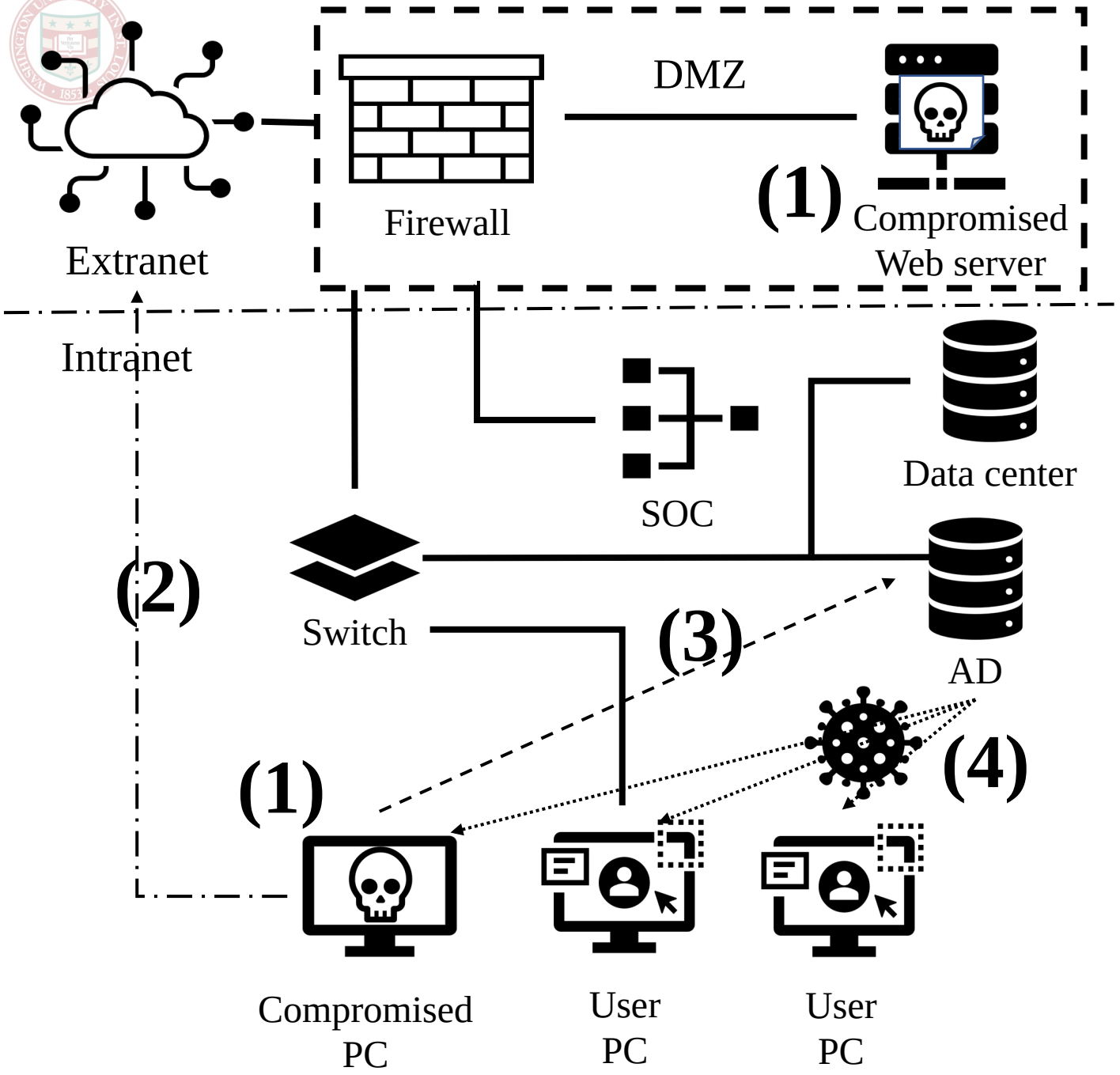
Outline

- Main Idea
- Background & Related Work
- Use Case
- Proposed Active Defense Implementations
- Conclusion
- Future Work
- Q & A

Use Case: Cybersecurity Incident at CPC Taiwan

- In May 2020, the Chinese Petroleum Corporation (CPC) in Taiwan, a natural gas corporation, fell victim to a ransomware.
- Disrupted electronic transaction applications for half a month.
- A targeted attack on **Active Directory (AD)**
- We analyzed the tactics and techniques used in this incident based on the ATT&CK framework, and we identify possible active defense implementations based on the Engage framework.

Source: https://www.ithome.com.tw/news/139331



(1) Initial Access

- T1190: Exploit Public-Facing Application
- T1566: Phishing

(2) Command and Control (C2)

- T1021: Remote Services
- T1071: Application Layer Protocol

(3) Discovery

- T1049: System Network Connections Discovery
- T1018: Remote System Discovery
- T1016.001: System Network Configuration Discovery: Internet Connection Discovery
- T1046: Network Service Discovery

(3) Credential Access & Collection

- T1550: Use Alternate Authentication Material
- T1056: Input Capture

(4) Persistence & Privilege Escalation

- T1053.003: Scheduled Task/Job

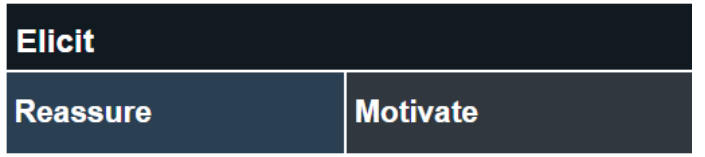
(4) Impact

- T1486: Data Encrypted for Impact

Outline

- Main Idea
- Background & Related Work
- Use Case
- Proposed Active Defense Implementations
- Conclusion
- Future Work
- Q & A

Initial Access: Exploiting Web Server



- Application Diversity
  - Mixes **decoy web servers** that mimics the legitimate server

- Network Manipulation
  - Decoy web server interacts with the adversary and alert the security team

- Introduced Vulnerabilities
  - **Redirect** the adversary from the real server and gather information about their capabilities and resources
  - **Reveal** targeting preferences, available capabilities, or even to influence future targeting decisions

Discovery

Expose	
Collect	Detect

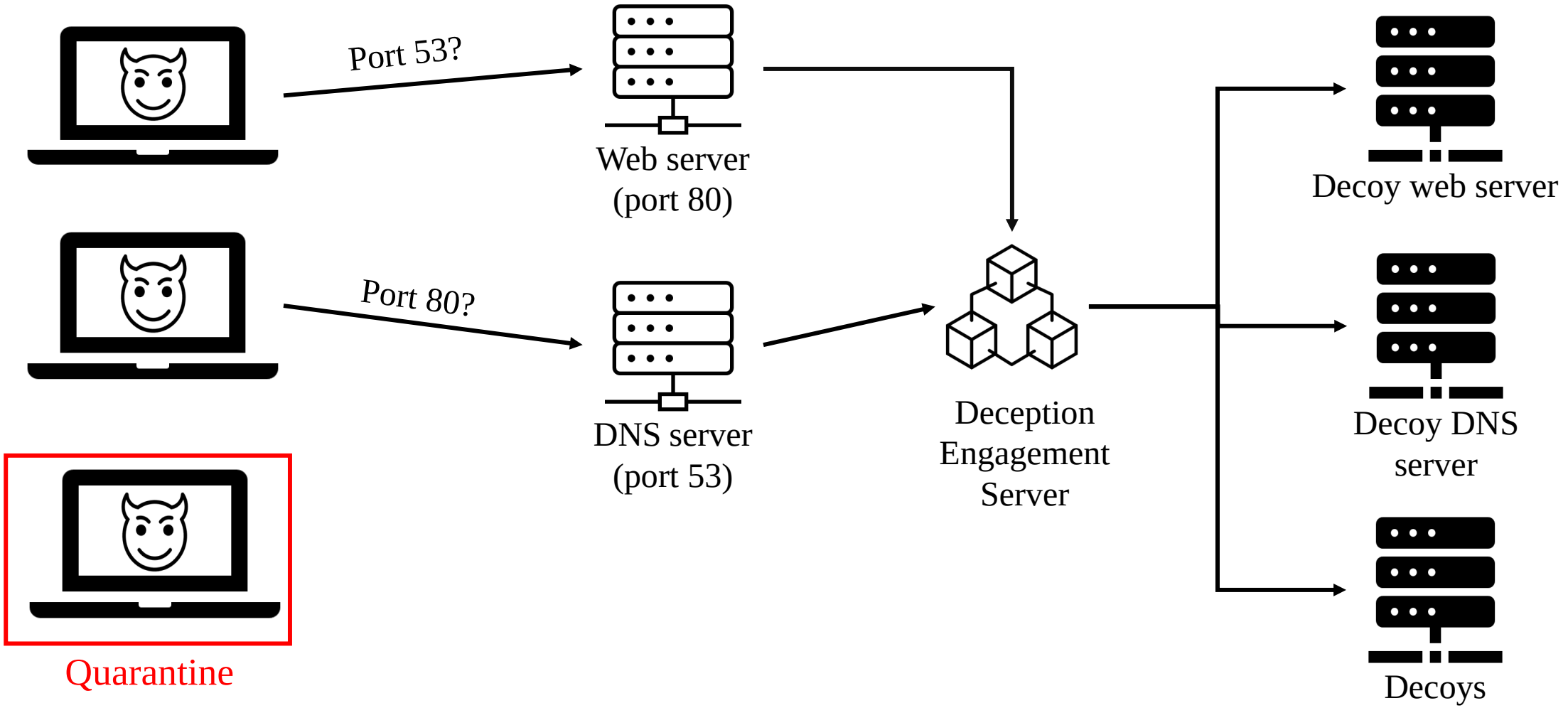
Affect		
Prevent	Direct	Disrupt

Elicit
Reassure

- Software Manipulation
  - **Decoy Endpoint**
  - **Decoy AD**
- Pocket Litter
  - Decoys provides fake information, such as IP addresses and domain account names
- Network Manipulation
  - Install a module at the endpoints that monitor any scans directed to **a closed port**
  - Scans sent to a non-existent device or service are deemed suspicious

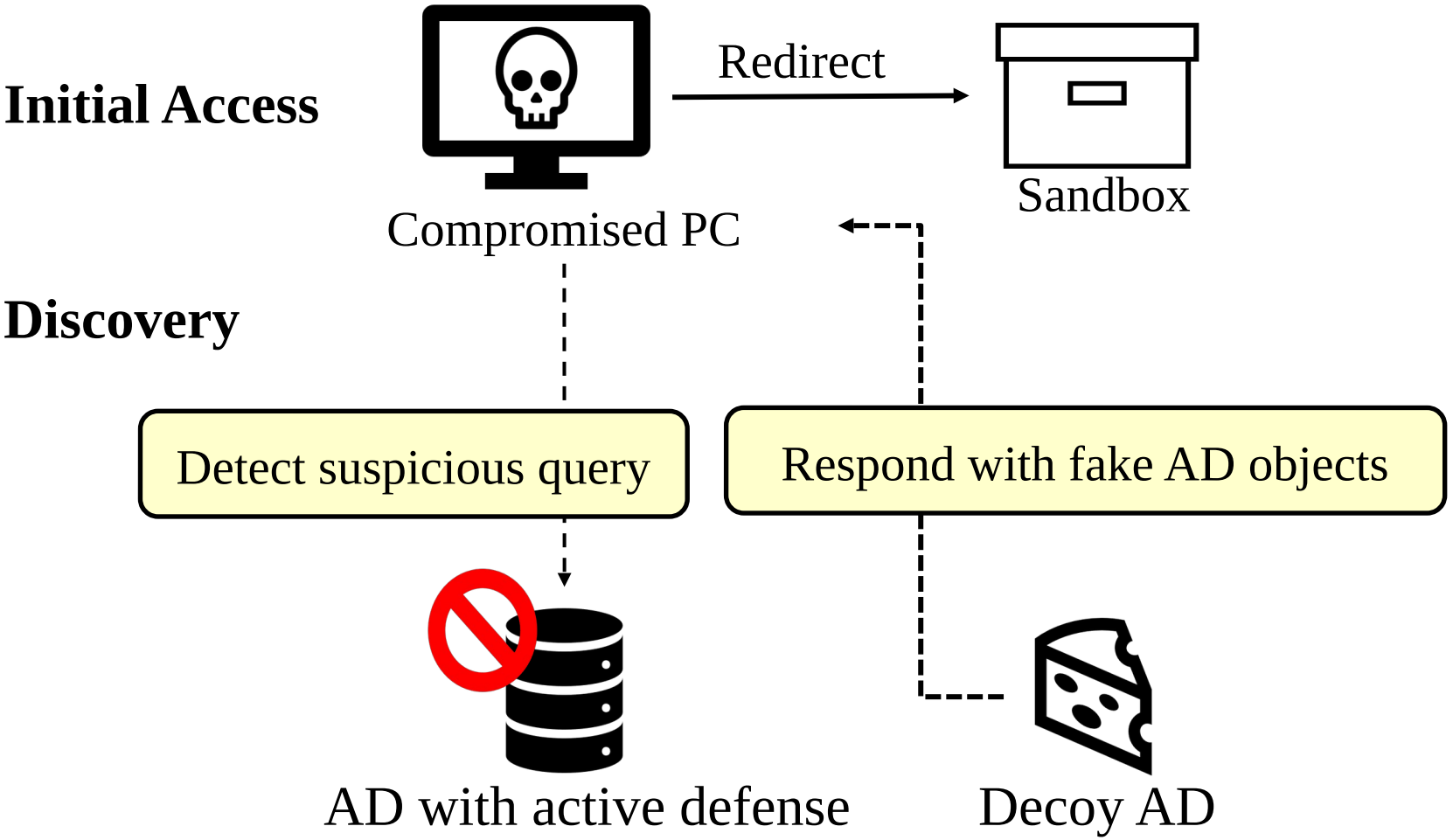
Affect		
Prevent	Direct	Disrupt

Decoy Endpoint: Obfuscating Ports Scans



Source: Sentinel.com

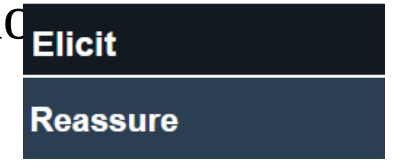
Decoy AD: Active Directory Intercept on endpoint



Source: Sentinel.com

Credential Access & Collection

- Information Manipulation
  - Place fake credentials
    - Usernames, passwords, and access keys by extracting password hash from either memory or hard disks (e.g., account manager or password/shadow file).
- Security Controls
  - Alter security controls to make the system **more or less vulnerable** to attack.
  - **Modifying** Group Policies, disabling or enabling autorun for remo… tightening or relaxing system firewalls.
- Pocket Litter
  - Browsing history, pictures, installed software, and connection history.
  - Decoy files **mixed** with non-essential real files and encrypted using base64 or Advanced Encryption Standard (AES)



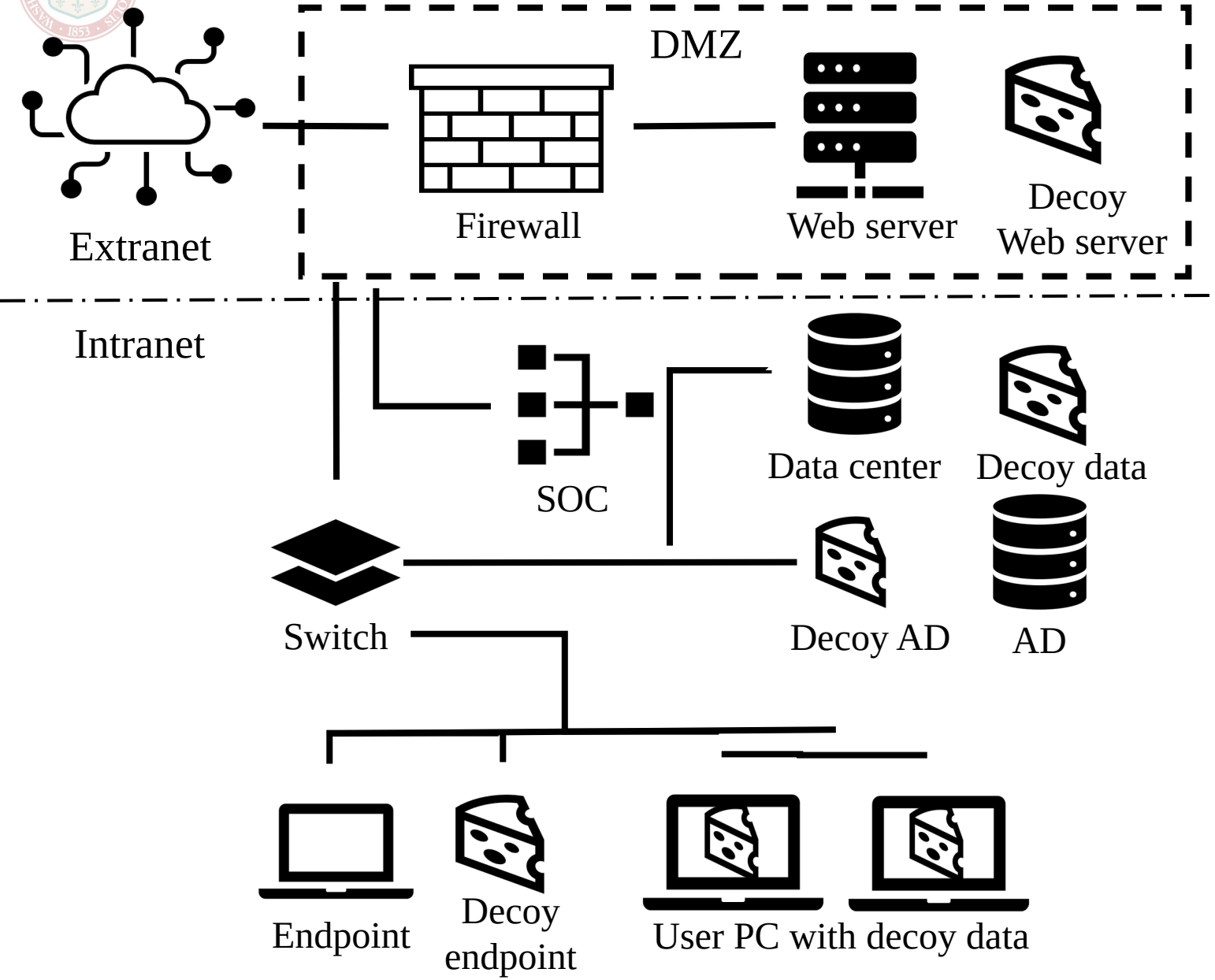
Impact- The last resort

Elicit	
Reassure	Motivate

- Artifact Diversity
  - Display various system artifacts, such as browser cookies, directories.
  - Any decoy files are modified means that ransomware has been executed.

Elicit	
Reassure	Motivate

- Information Manipulation
  - Redirected to a VM and isolated from the system network.
  - The VM would contain decoy files, such as .doc, .xlsx, .pdf, and .mp4, are included, **exceeding the quantity of actual files by one hundred times.**
  - Slow down encryption rate and create the appearance that it is still carrying out its intended function.



Initial Access

- EAC0006: Application Diversity
- EAC0016: Network Manipulation
- EAC0023: Introduced Vulnerabilities

Discovery

- EAC0011: Pocket Litter
- EAC0014: Software Manipulation
- EAC0016: Network Manipulation

Credential Access & Collection

- EAC0011: Pocket Litter
- EAC0015: Information Manipulation
- EAC0018: Security Controls

Impact

- EAC0015: Information Manipulation
- EAC0022: Artifact Diversity

Outline

- Main Idea
- Background & Related Work
- Use Case
- Proposed Active Defense Implementations
- Conclusion
- Future Work
- Q & A

Conclusion

- With CPC's APT attack scenario, we examined attack techniques employed based on ATT&CK framework.
- We proposed various active defense strategies utilizing denial and deception techniques based on Engage framework.
- Active defense **enhances the overall security posture of the internal network.**
- Active Defense is still a relatively novel concept, but the adoption of engagement, denial, and deception by the defensive side is undoubtedly becoming a prominent future trend.

Outline

- Main Idea
- Background & Related Work
- Use Case
- Proposed Active Defense Implementations
- Conclusion
- Future Work
- Q & A

Future Work

- Currently, we are working with Acer on the implementations
  - Interface
  - Report systems
- Gathering real-life data to evaluate the effectiveness of the implementations.
- Further research would focus on **resource requirements**, operational overheads, and potential scalability challenge.

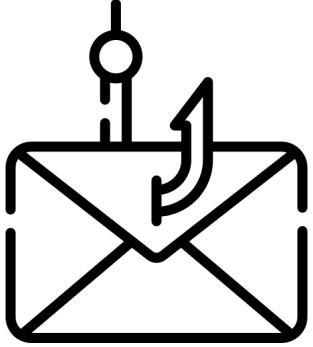
Q & A

Contact info:
Pei Yu, Huang h.peiyu@wustl.edu
Yi-Ting Huang ythuang@mail.ntust.edu.tw

Thank you!

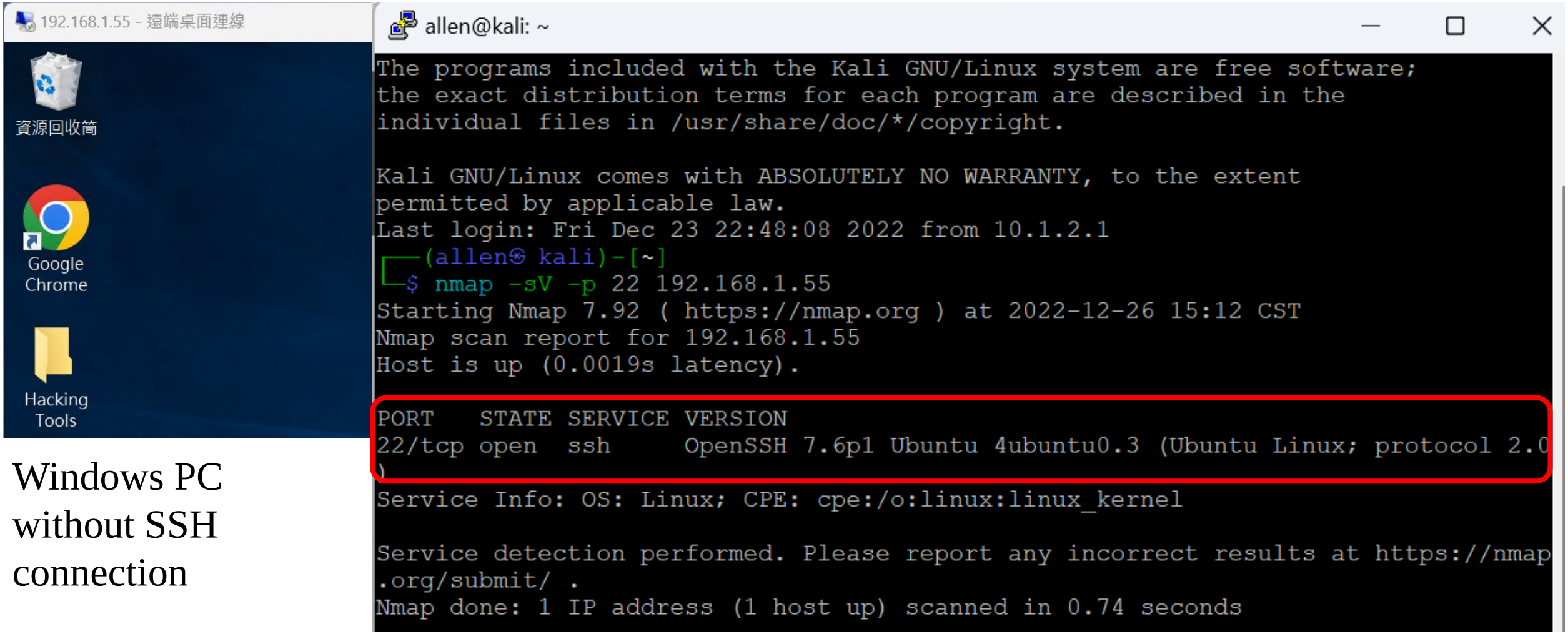
Appendix

Initial Access: Phishing Attack



- EAC0009: Email Manipulation
  - **Decoy emails** are placed on orphan pages
  - When decoy emails receive any messages, block the associated email addresses and IPs to prevent employees from viewing them.
- EAC0012: Persona
  - A **fake employee profile** on a social media platform like LinkedIn, complete with a decoy email address.
- EAC0011: Pocket Litter
  - Hobbies, personal, professional interactions, profile data, and updates

Appeared as Linux OS with SSH open for connection



Windows PC without SSH connection

Severity	Attack Phase	Timestamp	Attacker	Service	Target IP	Target OS	Description	Interface
Very High	Deceptive Credentials	15:24:02 01-18-2023	192.168.1.55 (55-Attivo Client.orange.com.tw)	WINLOGON	192.168.1.65 (AttivoDC.orange.com.tw)	Windows 2012-64	**Deceptive Credential Usage** (Windows Logon Success : WinEvtLog; 2023 Jan 18 07:23:58 WinEvtLog: Security: AUDIT_SUCCESS(4624): Microsoft-Windows-Security-Auditing: (no user): no domain: Windows2012-64.attivo.com: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: Windows2012-64$ Account Domain: attivo Logon ID: 0x3E7 Logon Type: 10 Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-1119950612-2432843808-2512486669-1106 Account Name: **attivoadmin** Account Domain: attivo Logon ID: 0x5D8EDB Logon GUID: {4E3F0FA8-8976-5FFE-F99C-71D5E1170E31} Process Information: Process ID: 0x724 Process Name: **C:\WINDOWS\SYSTEM32\WINLOGON.EXE** Network Information: Workstation Name: Windows2012-64 Source Network Address: **192.168.1.55** Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe o)	

Potential Utilized Attack Techniques

Initial Access

- T1190: Exploit Public-Facing Application
- T1566: Phishing

Command and Control

- T1021: Remote Services
- T1071: Application Layer Protocol

Discovery

- T1049: System Network Connections Discovery
- T1018: Remote System Discovery
- T1016.001: System Network Configuration Discovery: Internet Connection Discovery
- T1046: Network Service Discovery

Credential Access & Collection

- T1550: Use Alternate Authentication Material
- T1056: Input Capture

Persistence & Privilege Escalation

- T1053.003: Scheduled Task/Job

Impact

- T1486: Data Encrypted for Impact