ATT&CK Community Workshop

Purple Teaming with Attack Flow

Denise Tan

Overview

1. Visualizing results in a heatmap
2. Different approach to interpreting results
3. Utilizing Attack Flow for Purple Teaming
4. Key takeaways from Attack Flow
5. Attack Flow Builder

Profile of Fictional Company

“QuestLab Inc.”

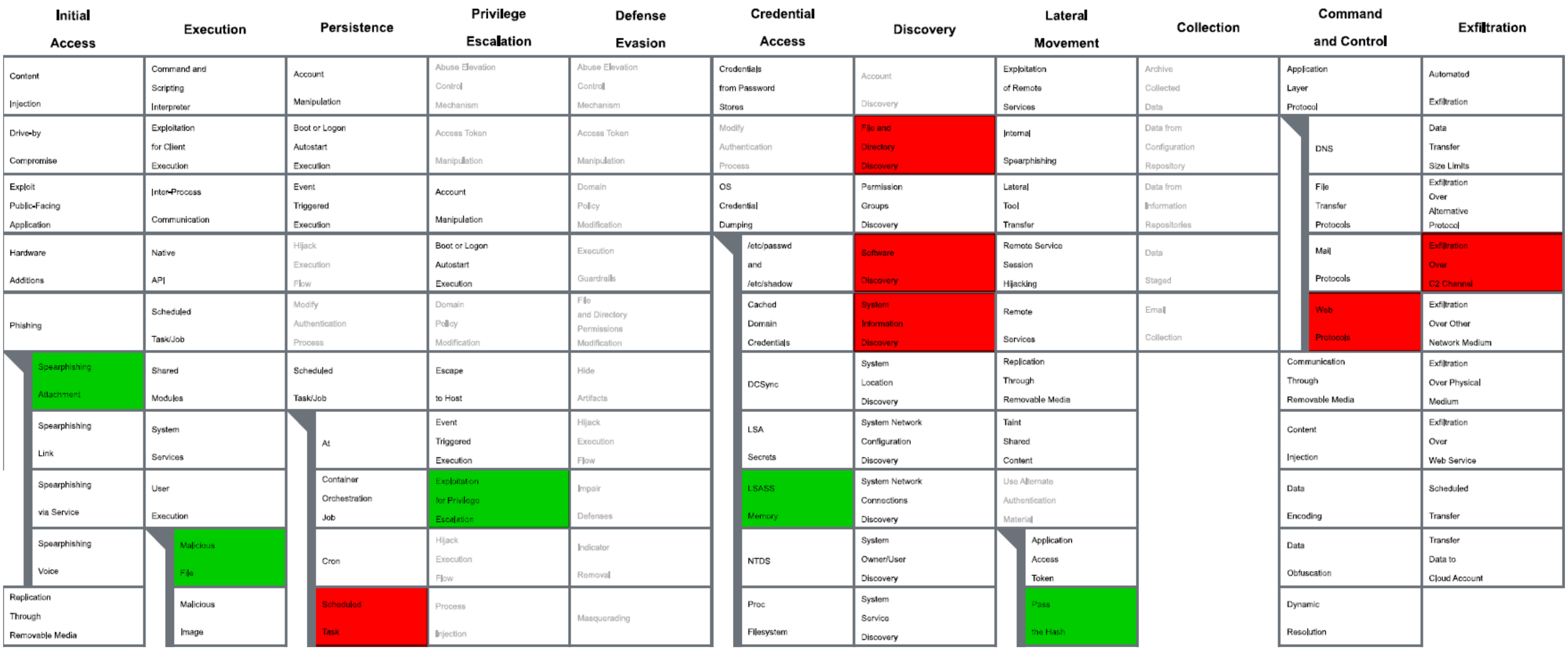
Research Institute with <20 employees

Security stack
Microsoft 365 Business Premium

- EDR: Defender for Business
- Firewall: Windows Defender Firewall

Email
Microsoft Outlook

Traditional Approach: Visualizing Results in Heatmap



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Content Injection	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Credentials from Password Stores	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration
Drive-by Compromise	Exploitation for Client Execution	Boot or Logon Autostart Execution	Access Token Manipulation	Access Token Manipulation	Modify Authentication Process	File and Directory Discovery	Internal Spearphishing	Data from Configuration Repository	DNS	Data Transfer Size Limits
Exploit Public-Facing Application	Inter-Process Communication	Event Triggered Execution	Account Manipulation	Domain Policy Modification	OS Credential Dumping	Permission Groups Discovery	Lateral Tool Transfer	Data from Information Repositories	File Transfer Protocols	Exfiltration Over Alternative Protocol
Hardware Additions	Native API	Hijack Execution Flow	Boot or Logon Autostart Execution	Execution Guardrails	/etc/passwd and /etc/shadow	Software Discovery	Remote Service Session Hijacking	Data Staged	Mail Protocols	Exfiltration Over C2 Channel
Phishing	Scheduled Task/Job	Modify Authentication Process	Domain Policy Modification	File and Directory Permissions Modification	Cached Domain Credentials	System Information Discovery	Remote Services	Email Collection	Web Protocols	Exfiltration Over Other Network Medium
Spearphishing Attachment	Shared Modules	Scheduled Task/Job	Escape to Host	Hide Artifacts	DCSync	System Location Discovery	Replication Through Removable Media		Communication Through Removable Media	Exfiltration Over Physical Medium
Spearphishing Link	System Services	At	Event Triggered Execution	Hijack Execution Flow	LSA Secrets	System Network Configuration Discovery	Taint Shared Content		Content Injection	Exfiltration Over Web Service
Spearphishing via Service	User Execution	Container Orchestration Job	Exploitation for Privilege Escalation	Impair Defenses	LSASS Memory	System Network Connections Discovery	Use Alternate Authentication Material		Data Encoding	Scheduled Transfer
Spearphishing Voice	Malicious File	Cron	Hijack Execution Flow	Indicator Removal	NTDS	System Owner/User Discovery	Application Access Token		Data Obfuscation	Transfer Data to Cloud Account
Replication Through Removable Media	Malicious Image	Scheduled Task	Process Injection	Masquerading	Proc Filesystem	System Service Discovery	Pass the Hash		Dynamic Resolution	

Note:

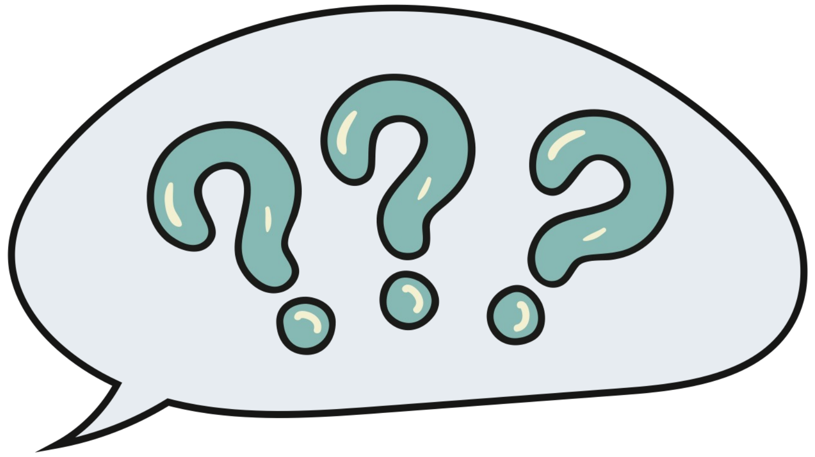
- Highlighted techniques are based on APT29's campaigns
- Heatmap generated via MITRE ATT&CK Navigator

Traditional Approach: Visualizing Results in Heatmap

Initial Access	Execution	Persistence	Privilege Escalation	Credential Access	Discovery	Lateral Movement	Command & Control	Exfiltration
🟩 Phishing: Spearphishing Attachment	🟩 User Execution: Malicious File	🟥 Scheduled Task/Job	🟩 Exploitation for Privilege Escalation	🟩 OS Credential Dumping: LSASS Memory	🟥 File and Directory Discovery	🟩 Pass the Hash	🟥 Application Layer Protocol: Web Protocols	🟥 Exfiltration Over C2 Channel
					🟥 Software Discovery			
					🟥 System Information Discovery			

Traditional Approach: Visualizing Results in Heatmap

Initial Access	**Execution**	**Persistence**	**Privilege Escalation**	**Credential Access**	**Discovery**	**Lateral Movement**	**Command & Control**	**Exfiltration**
🟩 Phishing: Spearphishing Attachment	🟩 User Execution: Malicious File	🟥 Scheduled Task/Job	🟩 Exploitation for Privilege Escalation	🟩 OS Credential Dumping: LSASS Memory	🟥 File and Directory Discovery	🟩 Pass the Hash	🟥 Application Layer Protocol: Web Protocols	🟥 Exfiltration Over C2 Channel
					🟥 Software Discovery			
					🟥 System Information Discovery			



Traditional Approach: Visualizing Results in Heatmap

Initial Access	Execution	Persistence	Privilege Escalation	Credential Access	Discovery	Lateral Movement	Command & Control	Exfiltration
🟩 Phishing: Spearphishing Attachment	🟩 User Execution: Malicious File	🟥 Scheduled Task/Job	🟩 Exploitation for Privilege Escalation	🟩 OS Credential Dumping: LSASS Memory	🟥 File and Directory Discovery	🟩 Pass the Hash	🟥 Application Layer Protocol: Web Protocols	🟥 Exfiltration Over C2 Channel
					🟥 Software Discovery			
					🟥 System Information Discovery			

However...

It may not be realistic to colour every cell green!

Traditional Approach: Visualizing Results in Heatmap

Initial Access	Execution	Persistence	Privilege Escalation	Credential Access	Discovery	Lateral Movement	Command & Control	Exfiltration
🟩 Phishing: Spearphishing Attachment	🟩 User Execution: Malicious File	🟥 Scheduled Task/Job	🟩 Exploitation for Privilege Escalation	🟩 OS Credential Dumping: LSASS Memory	🟥 File and Directory Discovery	🟩 Pass the Hash	🟥 Application Layer Protocol: Web Protocols	🟥 Exfiltration Over C2 Channel
					🟥 Software Discovery			
					🟥 System Information Discovery			

However...

It may not be realistic to

colour every cell green!

Other limitations:

Views techniques in an atomic manner

Lacks context - dependencies exist between each technique

Traditional Approach: Visualizing Results in Heatmap

Initial Access	Execution	Persistence	Privilege Escalation	Credential Access	Discovery	Lateral Movement	Command & Control	Exfiltration
🟩 Phishing: Spearphishing Attachment	🟩 User Execution: Malicious File	🟥 Scheduled Task/Job	🟩 Exploitation for Privilege Escalation	🟩 OS Credential Dumping: LSASS Memory	🟥 File and Directory Discovery	🟩 Pass the Hash	🟥 Application Layer Protocol: Web Protocols	🟥 Exfiltration Over C2 Channel
					🟥 Software Discovery			
					🟥 System Informati Discov			

However...

It may not be realistic to colour every cell green!

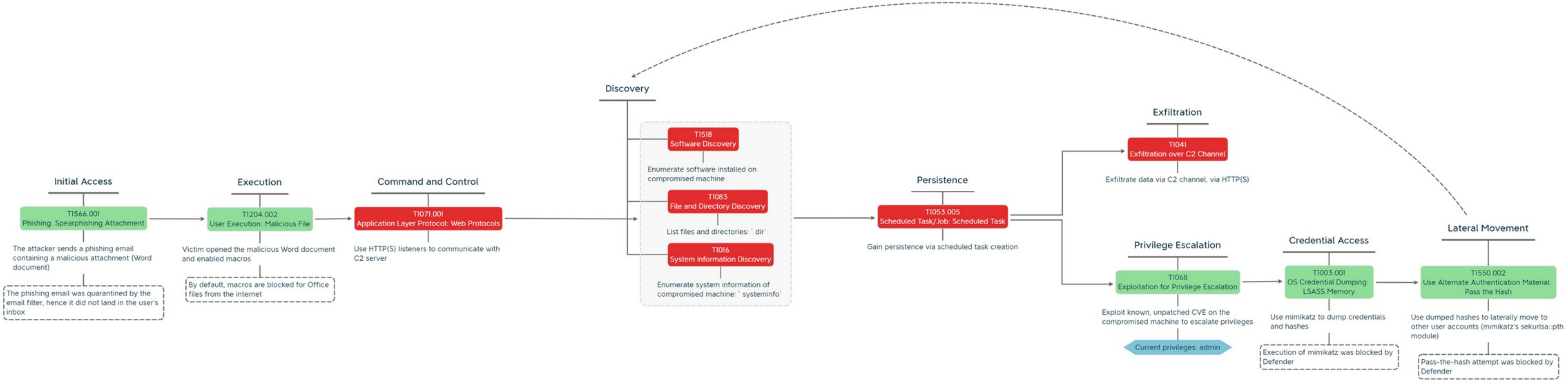
Given QuestLab's limited security budget, how should we choose what to fix?

Other limitations:

- Views techniques in an atomic manner
- Lacks context - dependencies exist between each technique

Heatmap vs Attack Flow

Initial Access	Execution	Persistence	Privilege Escalation	Credential Access	Discovery	Lateral Movement	Command & Control	Exfiltration
🟩 Phishing: Spearphishing Attachment	🟩 User Execution: Malicious File	🟥 Scheduled Task/Job	🟩 Exploitation for Privilege Escalation	🟩 OS Credential Dumping: LSASS Memory	🟥 File and Directory Discovery	🟩 Pass the Hash	🟥 Application Layer Protocol: Web Protocols	🟥 Exfiltration Over C2 Channel
					🟥 Software Discovery			
					🟥 System Information Discovery			



T1566.001
Phishing: Spearphishing Attachment

The attacker sends a phishing email containing a malicious attachment (Word document)

The phishing email was quarantined by the email filter, hence it did not land in the user's inbox

T1204.002
User Execution: Malicious File

Victim opened the malicious Word document and enabled macros

By default, macros are blocked for Office files from the internet

T1071.001
Application Layer Protocol: Web Protocols

Use HTTP(S) listeners to communicate with C2 server

T1518
Software Discovery

Enumerate software installed on compromised machine

T1083
File and Directory Discovery

List files and directories: ` dir`

T1016
System Information Discovery

Enumerate system information of compromised machine: ` systeminfo`

T1053.005
Scheduled Task/Job: Scheduled Task

Gain persistence via scheduled task creation

T1041
Exfiltration over C2 Channel

Exfiltrate data via C2 channel, via HTTP(S)

T1068
Exploitation for Privilege Escalation

Exploit known, unpatched CVE on the compromised machine to escalate privileges

Current privileges: admin

T1003.001
OS Credential Dumping: LSASS Memory

Use mimikatz to dump credentials and hashes

Execution of mimikatz was blocked by Defender

T1550.002
Use Alternate Authentication Material: Pass the Hash

Use dumped hashes to laterally move to other user accounts (mimikatz's sekurlsa::pth module)

Pass-the-hash attempt was blocked by Defender

What is Attack Flow?

Accurate reflection of security posture

Sequences of adversary behavior

TTPs in the context of adversary campaigns

Heatmap vs Attack Flow

Heatmap vs Attack Flow

Heatmap vs Attack Flow

Heatmap

Heatmap vs Attack Flow

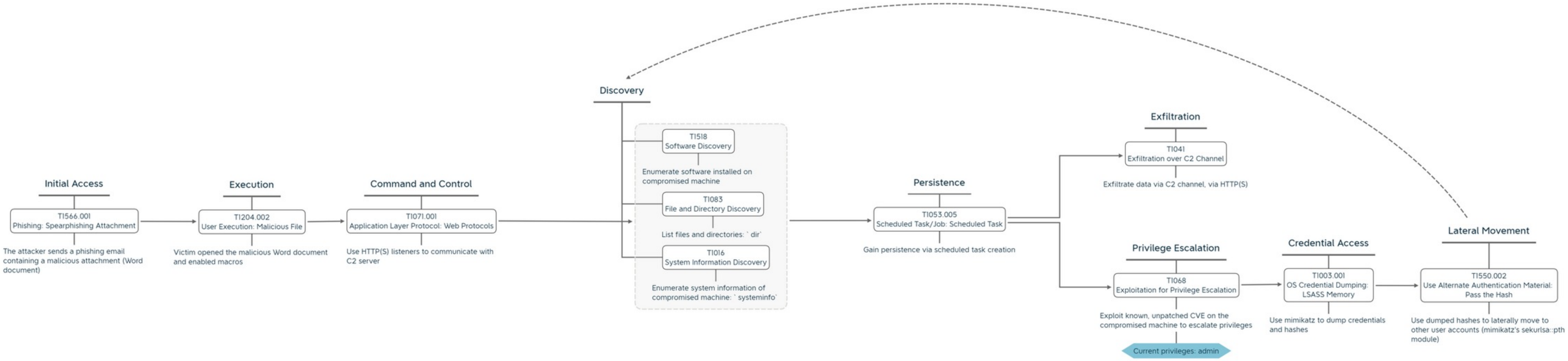
Heatmap

Heatmap vs Attack Flow

Heatmap

Attack Flow

Pre-Exercise: Attack Flow



Initial Access

T1566.001
Phishing: Spearphishing Attachment

The attacker sends a phishing email containing a malicious attachment (Word document)

Execution

T1204.002
User Execution: Malicious File

Victim opened the malicious Word document and enabled macros

Command and Control

T1071.001
Application Layer Protocol: Web Protocols

Use HTTP(S) listeners to communicate with C2 server

Discovery

T1518
Software Discovery

Enumerate software installed on compromised machine

T1083
File and Directory Discovery

List files and directories: ` dir`

T1016
System Information Discovery

Enumerate system information of compromised machine: ` systeminfo`

Persistence

T1053.005
Scheduled Task/Job: Scheduled Task

Gain persistence via scheduled task creation

Exfiltration

T1041
Exfiltration over C2 Channel

Exfiltrate data via C2 channel, via HTTP(S)

Privilege Escalation

T1068
Exploitation for Privilege Escalation

Exploit known, unpatched CVE on the compromised machine to escalate privileges

Current privileges: admin

Credential Access

T1003.001
OS Credential Dumping: LSASS Memory

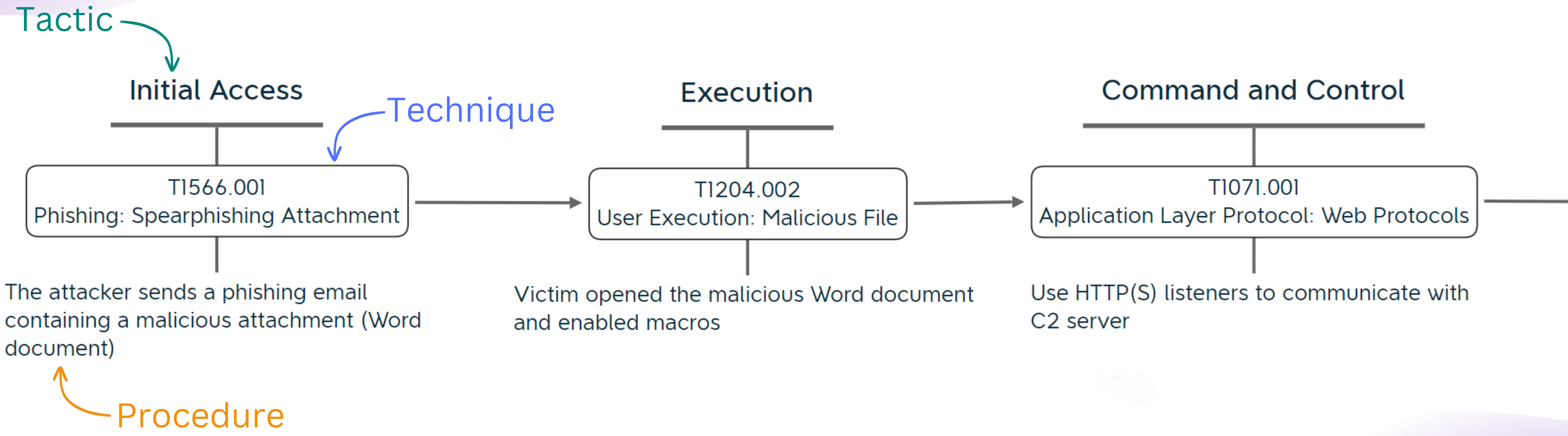
Use mimikatz to dump credentials and hashes

Lateral Movement

T1550.002
Use Alternate Authentication Material: Pass the Hash

Use dumped hashes to laterally move to other user accounts (mimikatz's sekurlsa::pth module)

Start of Campaign



Tactic

Technique

Procedure

Initial Access

T1566.001
Phishing: Spearphishing Attachment

The attacker sends a phishing email containing a malicious attachment (Word document)

Execution

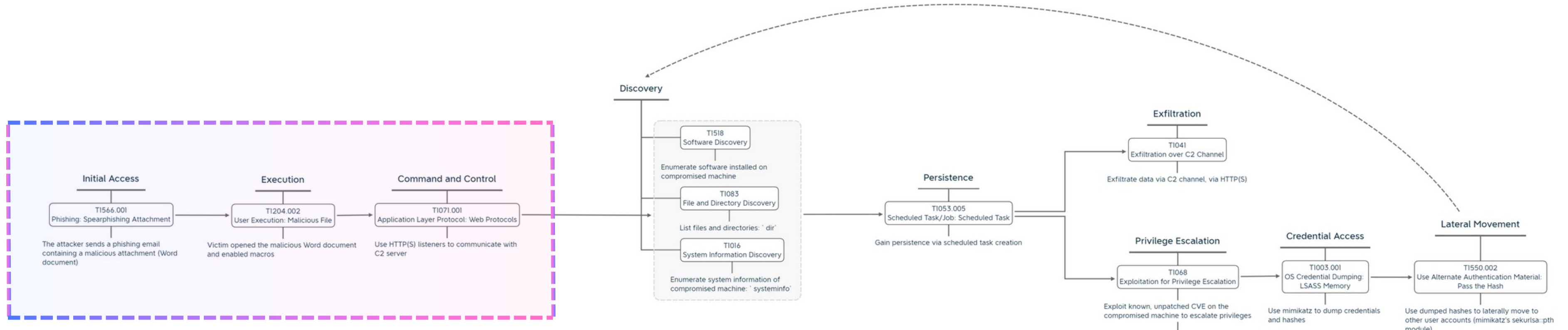
T1204.002
User Execution: Malicious File

Victim opened the malicious Word document and enabled macros

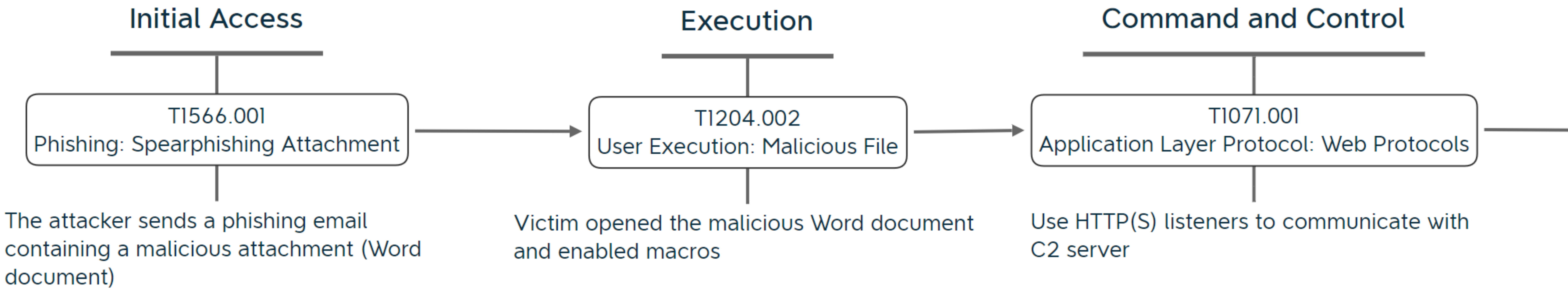
Command and Control

T1071.001
Application Layer Protocol: Web Protocols

Use HTTP(S) listeners to communicate with C2 server


Initial Access
T1566.001
Phishing: Spearphishing Attachment
The attacker sends a phishing email containing a malicious attachment (Word document)
Execution
T1204.002
User Execution: Malicious File
Victim opened the malicious Word document and enabled macros
Command and Control
T1071.001
Application Layer Protocol: Web Protocols
Use HTTP(S) listeners to communicate with C2 server
Discovery
T1518
Software Discovery
Enumerate software installed on compromised machine
T1083
File and Directory Discovery
List files and directories: ` dir`
T1016
System Information Discovery
Enumerate system information of compromised machine: ` systeminfo`
Persistence
T1053.005
Scheduled Task/Job: Scheduled Task
Gain persistence via scheduled task creation
Exfiltration
T1041
Exfiltration over C2 Channel
Exfiltrate data via C2 channel, via HTTP(S)
Privilege Escalation
T1068
Exploitation for Privilege Escalation
Exploit known, unpatched CVE on the compromised machine to escalate privileges
Current privileges: admin
Credential Access
T1003.001
OS Credential Dumping: LSASS Memory
Use mimikatz to dump credentials and hashes
Lateral Movement
T1550.002
Use Alternate Authentication Material: Pass the Hash
Use dumped hashes to laterally move to other user accounts (mimikatz's sekurlsa::pth module)

Start of Campaign



Initial Access

T1566.001
Phishing: Spearphishing Attachment

The attacker sends a phishing email containing a malicious attachment (Word document)

Execution

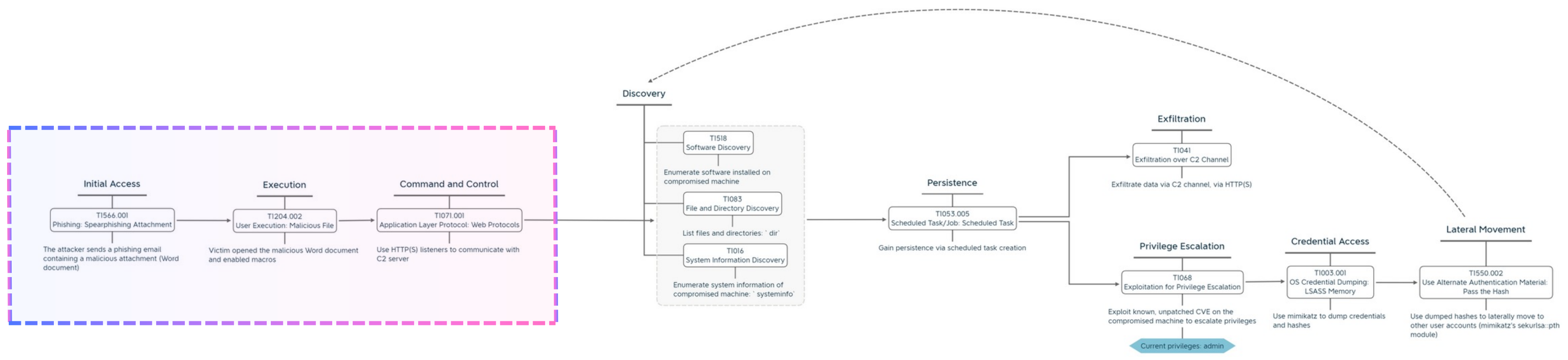
T1204.002
User Execution: Malicious File

Victim opened the malicious Word document and enabled macros

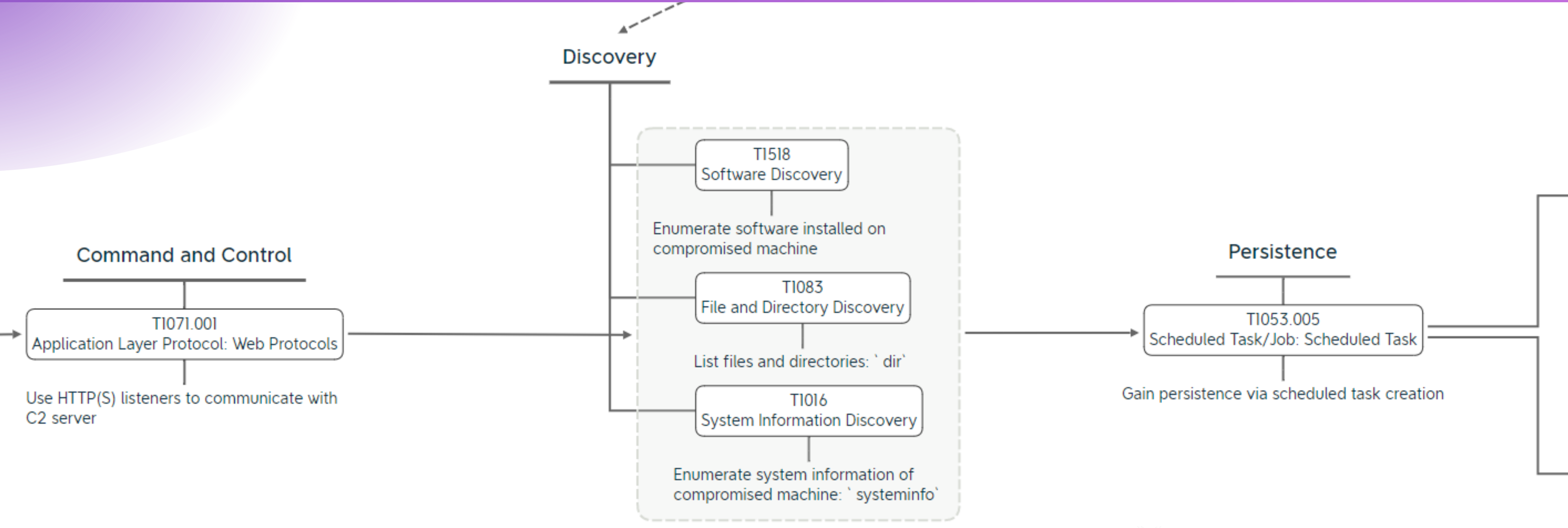
Command and Control

T1071.001
Application Layer Protocol: Web Protocols

Use HTTP(S) listeners to communicate with C2 server


Initial Access
T1566.001
Phishing: Spearphishing Attachment
The attacker sends a phishing email containing a malicious attachment (Word document)
Execution
T1204.002
User Execution: Malicious File
Victim opened the malicious Word document and enabled macros
Command and Control
T1071.001
Application Layer Protocol: Web Protocols
Use HTTP(S) listeners to communicate with C2 server
Discovery
T1518
Software Discovery
Enumerate software installed on compromised machine
T1083
File and Directory Discovery
List files and directories: `dir`
T1016
System Information Discovery
Enumerate system information of compromised machine: `systeminfo`
Persistence
T1053.005
Scheduled Task/Job: Scheduled Task
Gain persistence via scheduled task creation
Exfiltration
T1041
Exfiltration over C2 Channel
Exfiltrate data via C2 channel, via HTTP(S)
Privilege Escalation
T1068
Exploitation for Privilege Escalation
Exploit known, unpatched CVE on the compromised machine to escalate privileges
Current privileges: admin
Credential Access
T1003.001
OS Credential Dumping: LSASS Memory
Use mimikatz to dump credentials and hashes
Lateral Movement
T1550.002
Use Alternate Authentication Material: Pass the Hash
Use dumped hashes to laterally move to other user accounts (mimikatz's sekurlsa::pth module)

Middle of Campaign



Discovery

T1518
Software Discovery

Enumerate software installed on compromised machine

T1083
File and Directory Discovery

List files and directories: ` dir`

T1016
System Information Discovery

Enumerate system information of compromised machine: ` systeminfo`

Command and Control

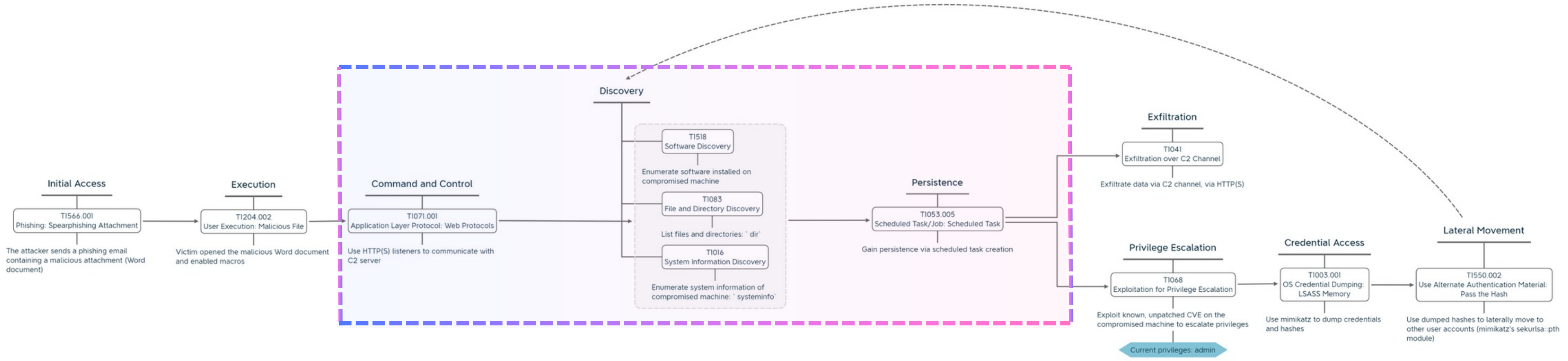
T1071.001
Application Layer Protocol: Web Protocols

Use HTTP(S) listeners to communicate with C2 server

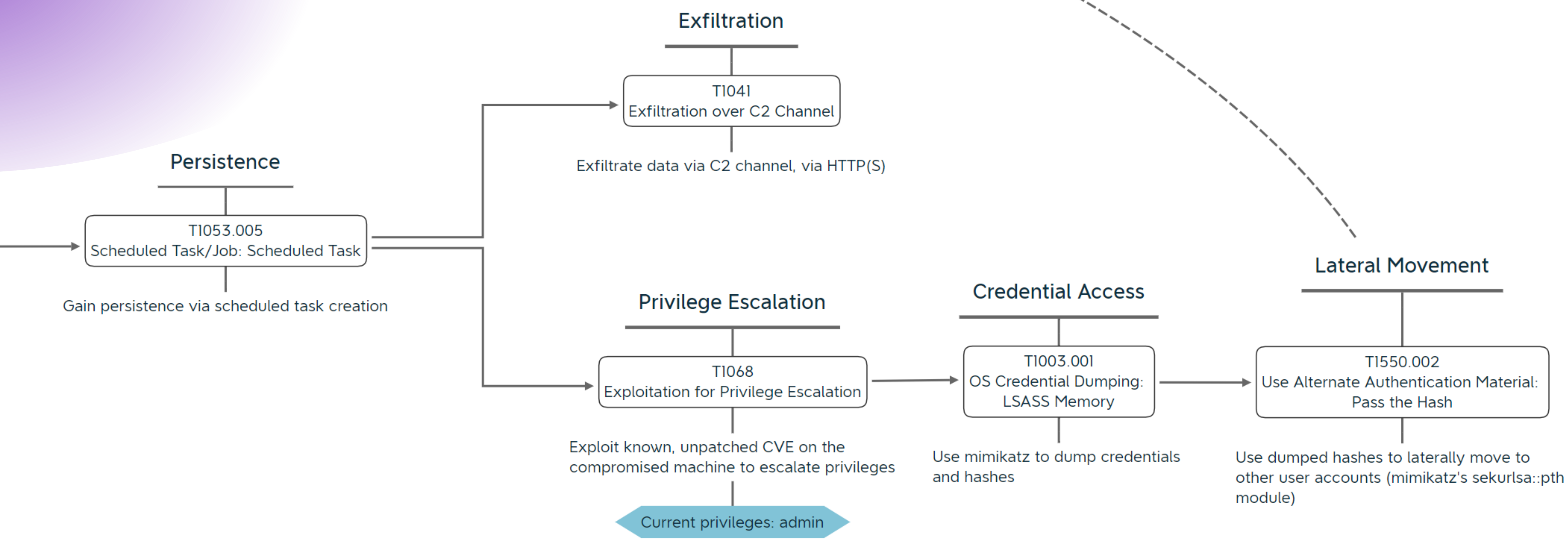
Persistence

T1053.005
Scheduled Task/Job: Scheduled Task

Gain persistence via scheduled task creation


Initial Access
T1566.001
Phishing: Spearphishing Attachment
The attacker sends a phishing email containing a malicious attachment (Word document)
Execution
T1204.002
User Execution: Malicious File
Victim opened the malicious Word document and enabled macros
Command and Control
T1071.001
Application Layer Protocol: Web Protocols
Use HTTP(S) listeners to communicate with C2 server
Discovery
T1518
Software Discovery
Enumerate software installed on compromised machine
T1083
File and Directory Discovery
List files and directories: ` dir`
T1016
System Information Discovery
Enumerate system information of compromised machine: ` systeminfo`
Persistence
T1053.005
Scheduled Task/Job: Scheduled Task
Gain persistence via scheduled task creation
Exfiltration
T1041
Exfiltration over C2 Channel
Exfiltrate data via C2 channel, via HTTP(S)
Privilege Escalation
T1068
Exploitation for Privilege Escalation
Exploit known, unpatched CVE on the compromised machine to escalate privileges
Current privileges: admin
Credential Access
T1003.001
OS Credential Dumping: LSASS Memory
Use mimikatz to dump credentials and hashes
Lateral Movement
T1550.002
Use Alternate Authentication Material: Pass the Hash
Use dumped hashes to laterally move to other user accounts (mimikatz's sekurlsa::pth module)

End of Campaign



Exfiltration

T1041
Exfiltration over C2 Channel

Exfiltrate data via C2 channel, via HTTP(S)

Persistence

T1053.005
Scheduled Task/Job: Scheduled Task

Gain persistence via scheduled task creation

Privilege Escalation

T1068
Exploitation for Privilege Escalation

Exploit known, unpatched CVE on the compromised machine to escalate privileges

Current privileges: admin

Credential Access

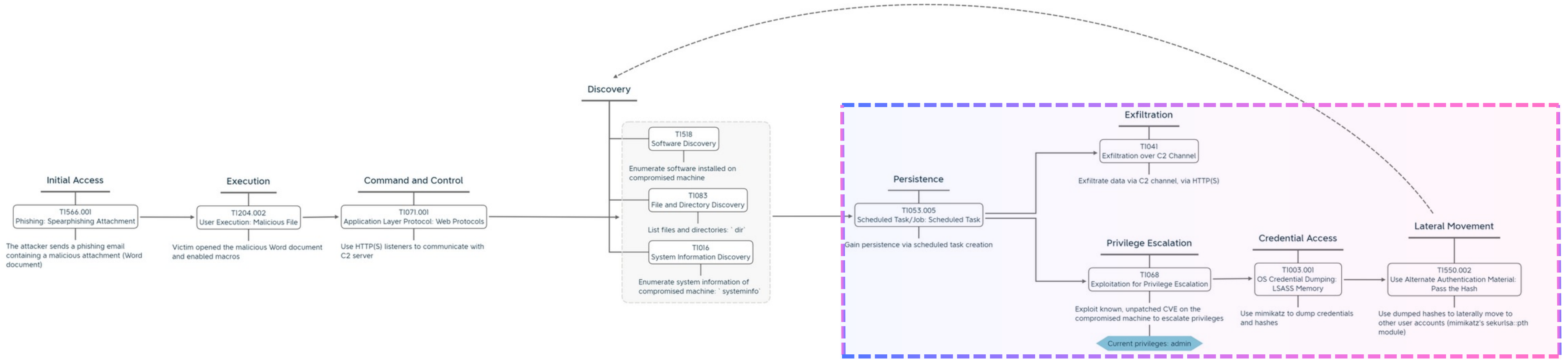
T1003.001
OS Credential Dumping: LSASS Memory

Use mimikatz to dump credentials and hashes

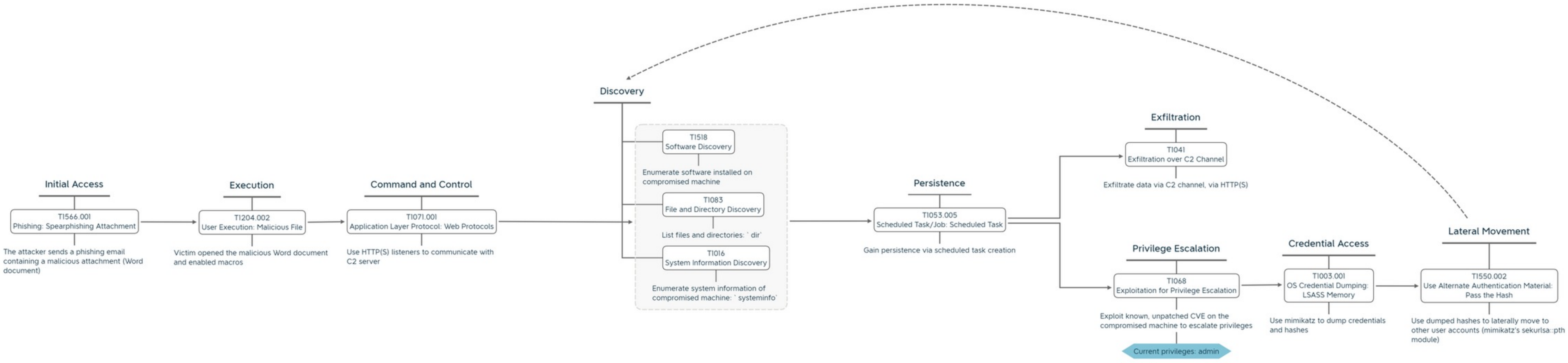
Lateral Movement

T1550.002
Use Alternate Authentication Material: Pass the Hash

Use dumped hashes to laterally move to other user accounts (mimikatz's sekurlsa::pth module)


Initial Access
T1566.001
Phishing: Spearphishing Attachment
The attacker sends a phishing email containing a malicious attachment (Word document)
Execution
T1204.002
User Execution: Malicious File
Victim opened the malicious Word document and enabled macros
Command and Control
T1071.001
Application Layer Protocol: Web Protocols
Use HTTP(S) listeners to communicate with C2 server
Discovery
T1518
Software Discovery
Enumerate software installed on compromised machine
T1083
File and Directory Discovery
List files and directories: ` dir`
T1016
System Information Discovery
Enumerate system information of compromised machine: ` systeminfo`
Exfiltration
T1041
Exfiltration over C2 Channel
Persistence
T1053.005
Scheduled Task/Job: Scheduled Task
Privilege Escalation
T1068
Exploitation for Privilege Escalation
Credential Access
T1003.001
OS Credential Dumping: LSASS Memory
Lateral Movement
T1550.002
Use Alternate Authentication Material: Pass the Hash
Current privileges: admin

Iterative Cycle



Initial Access

T1566.001
Phishing: Spearphishing Attachment

The attacker sends a phishing email containing a malicious attachment (Word document)

Execution

T1204.002
User Execution: Malicious File

Victim opened the malicious Word document and enabled macros

Command and Control

T1071.001
Application Layer Protocol: Web Protocols

Use HTTP(S) listeners to communicate with C2 server

Discovery

T1518
Software Discovery

Enumerate software installed on compromised machine

T1083
File and Directory Discovery

List files and directories: ` dir`

T1016
System Information Discovery

Enumerate system information of compromised machine: ` systeminfo`

Persistence

T1053.005
Scheduled Task/Job: Scheduled Task

Gain persistence via scheduled task creation

Exfiltration

T1041
Exfiltration over C2 Channel

Exfiltrate data via C2 channel, via HTTP(S)

Privilege Escalation

T1068
Exploitation for Privilege Escalation

Exploit known, unpatched CVE on the compromised machine to escalate privileges

Current privileges: admin

Credential Access

T1003.001
OS Credential Dumping: LSASS Memory

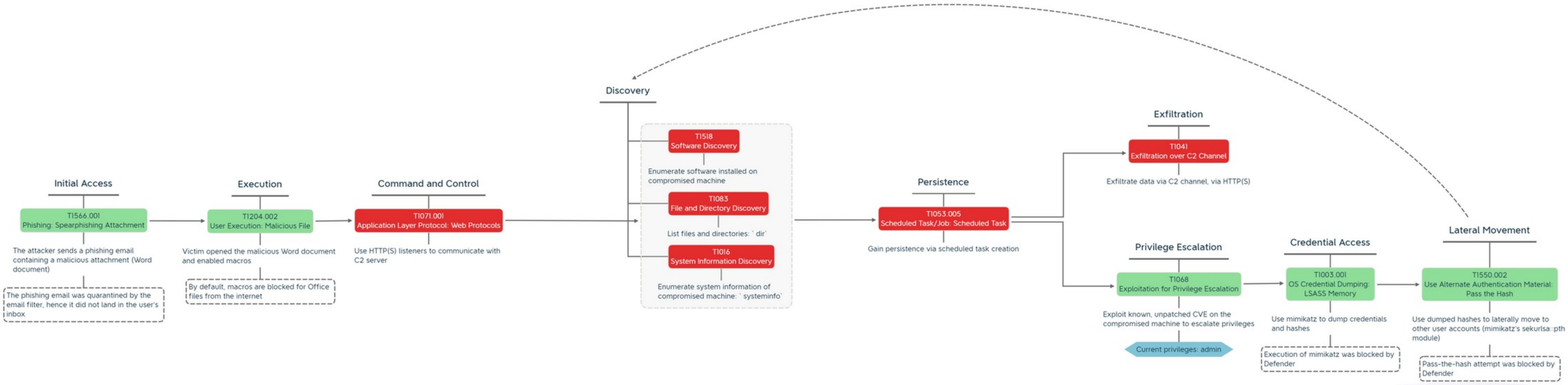
Use mimikatz to dump credentials and hashes

Lateral Movement

T1550.002
Use Alternate Authentication Material: Pass the Hash

Use dumped hashes to laterally move to other user accounts (mimikatz's sekurlsa::pth module)

Post-Exercise: Defensive Controls



Initial Access

T1566.001
Phishing: Spearphishing Attachment

The attacker sends a phishing email containing a malicious attachment (Word document)

The phishing email was quarantined by the email filter, hence it did not land in the user's inbox

Execution

T1204.002
User Execution: Malicious File

Victim opened the malicious Word document and enabled macros

By default, macros are blocked for Office files from the internet

Command and Control

T1071.001
Application Layer Protocol: Web Protocols

Use HTTP(S) listeners to communicate with C2 server

Discovery

T1518
Software Discovery

Enumerate software installed on compromised machine

T1083
File and Directory Discovery

List files and directories: ` dir`

T1016
System Information Discovery

Enumerate system information of compromised machine: ` systeminfo`

Persistence

T1053.005
Scheduled Task/Job: Scheduled Task

Gain persistence via scheduled task creation

Exfiltration

T1041
Exfiltration over C2 Channel

Exfiltrate data via C2 channel, via HTTP(S)

Privilege Escalation

T1068
Exploitation for Privilege Escalation

Exploit known, unpatched CVE on the compromised machine to escalate privileges

Current privileges: admin

Credential Access

T1003.001
OS Credential Dumping: LSASS Memory

Use mimikatz to dump credentials and hashes

Execution of mimikatz was blocked by Defender

Lateral Movement

T1550.002
Use Alternate Authentication Material: Pass the Hash

Use dumped hashes to laterally move to other user accounts (mimikatz's sekurlsa::pth module)

Pass-the-hash attempt was blocked by Defender

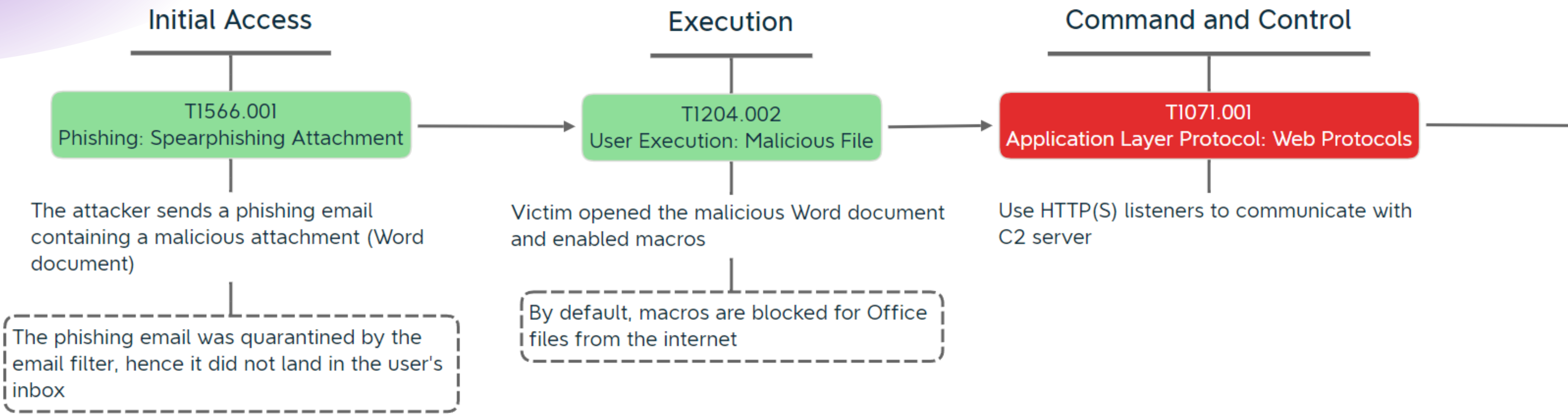
Legend

Green: TTP with defensive control

Red: TTP without defensive control

Dotted rectangle: Defensive control

Defensive Controls: Start of Campaign



Initial Access

T1566.001
Phishing: Spearphishing Attachment

The attacker sends a phishing email containing a malicious attachment (Word document)

The phishing email was quarantined by the email filter, hence it did not land in the user's inbox

Execution

T1204.002
User Execution: Malicious File

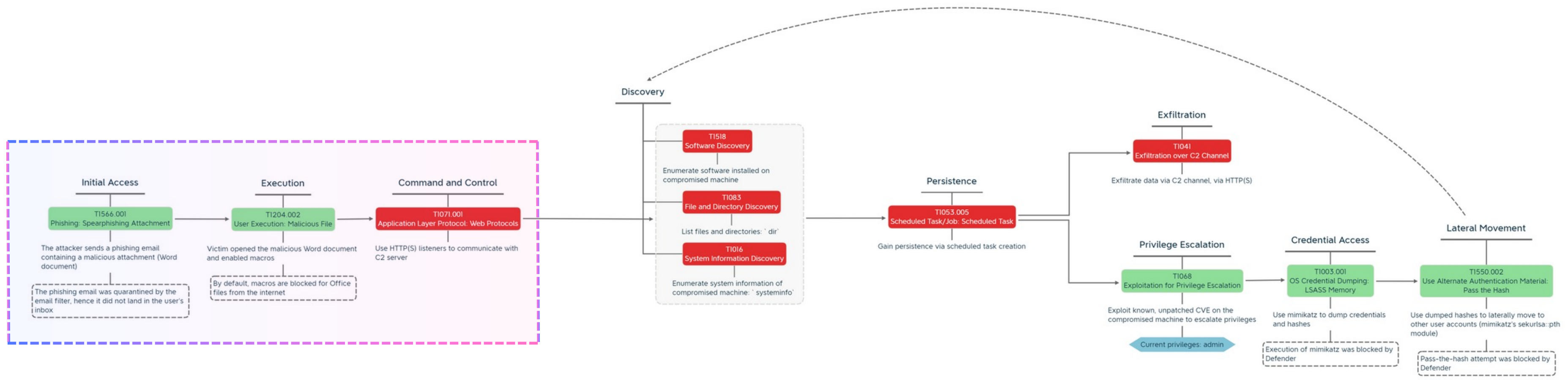
Victim opened the malicious Word document and enabled macros

By default, macros are blocked for Office files from the internet

Command and Control

T1071.001
Application Layer Protocol: Web Protocols

Use HTTP(S) listeners to communicate with C2 server



Initial Access

T1566.001
Phishing: Spearphishing Attachment

The attacker sends a phishing email containing a malicious attachment (Word document)

The phishing email was quarantined by the email filter, hence it did not land in the user's inbox

Execution

T1204.002
User Execution: Malicious File

Victim opened the malicious Word document and enabled macros

By default, macros are blocked for Office files from the internet

Command and Control

T1071.001
Application Layer Protocol: Web Protocols

Use HTTP(S) listeners to communicate with C2 server

Discovery

T1518
Software Discovery

Enumerate software installed on compromised machine

T1083
File and Directory Discovery

List files and directories: ` dir`

T1016
System Information Discovery

Enumerate system information of compromised machine: ` systeminfo`

Persistence

T1053.005
Scheduled Task/Job: Scheduled Task

Gain persistence via scheduled task creation

Exfiltration

T1041
Exfiltration over C2 Channel

Exfiltrate data via C2 channel, via HTTP(S)

Privilege Escalation

T1068
Exploitation for Privilege Escalation

Exploit known, unpatched CVE on the compromised machine to escalate privileges

Current privileges: admin

Credential Access

T1003.001
OS Credential Dumping: LSASS Memory

Use mimikatz to dump credentials and hashes

Execution of mimikatz was blocked by Defender

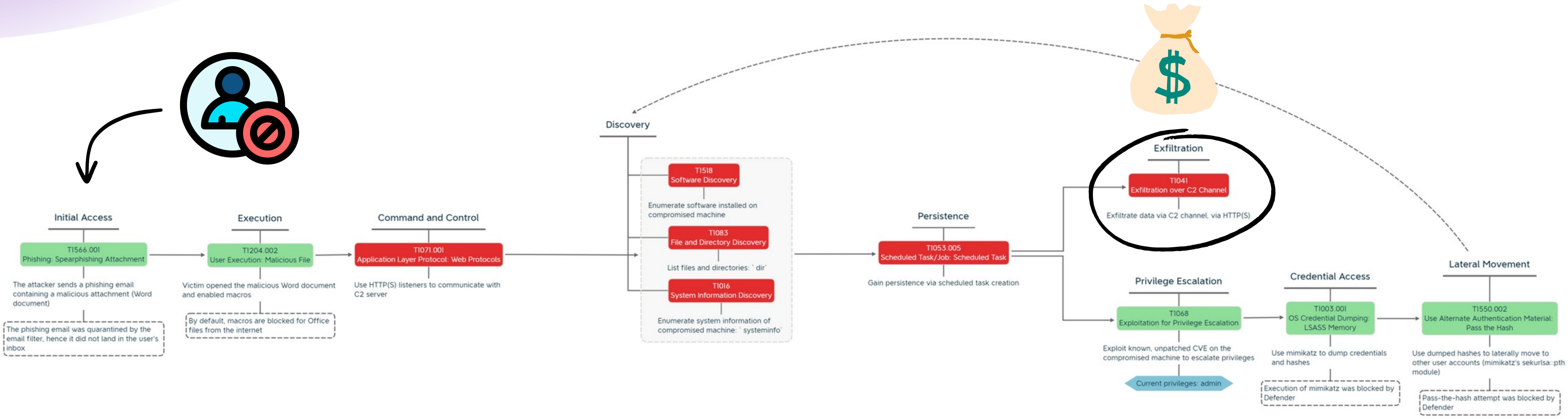
Lateral Movement

T1550.002
Use Alternate Authentication Material: Pass the Hash

Use dumped hashes to laterally move to other user accounts (mimikatz's sekurlsa::pth module)

Pass-the-hash attempt was blocked by Defender

Defense-in-depth



Initial Access

T1566.001
Phishing: Spearphishing Attachment

The attacker sends a phishing email containing a malicious attachment (Word document)

The phishing email was quarantined by the email filter, hence it did not land in the user's inbox

Execution

T1204.002
User Execution: Malicious File

Victim opened the malicious Word document and enabled macros

By default, macros are blocked for Office files from the internet

Command and Control

T1071.001
Application Layer Protocol: Web Protocols

Use HTTP(S) listeners to communicate with C2 server

Discovery

T1518
Software Discovery

Enumerate software installed on compromised machine

T1083
File and Directory Discovery

List files and directories: ` dir`

T1016
System Information Discovery

Enumerate system information of compromised machine: ` systeminfo`

Persistence

T1053.005
Scheduled Task/Job: Scheduled Task

Gain persistence via scheduled task creation

Exfiltration

T1041
Exfiltration over C2 Channel

Exfiltrate data via C2 channel, via HTTP(S)

Privilege Escalation

T1068
Exploitation for Privilege Escalation

Exploit known, unpatched CVE on the compromised machine to escalate privileges

Current privileges: admin

Credential Access

T1003.001
OS Credential Dumping: LSASS Memory

Use mimikatz to dump credentials and hashes

Execution of mimikatz was blocked by Defender

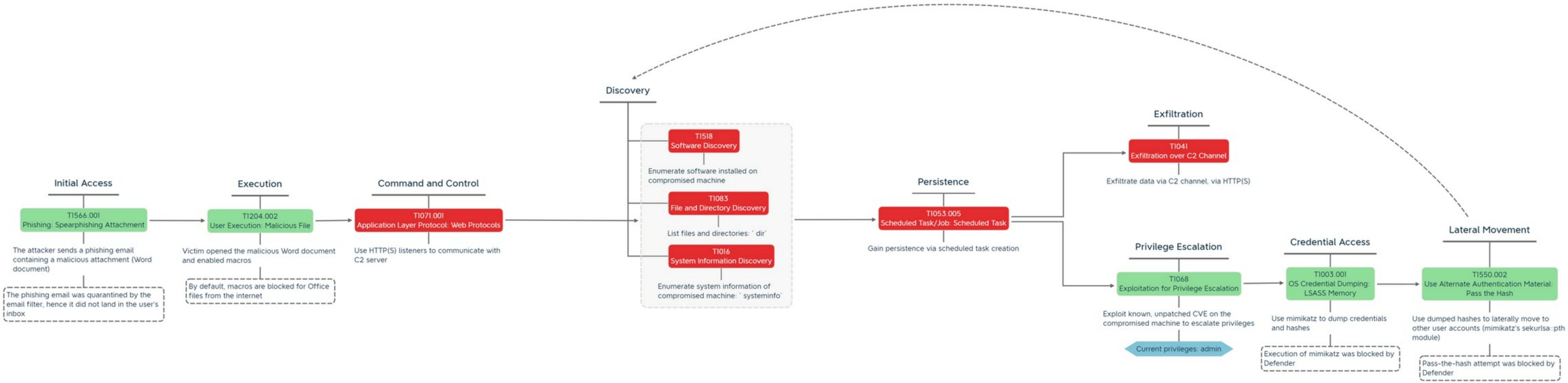
Lateral Movement

T1550.002
Use Alternate Authentication Material: Pass the Hash

Use dumped hashes to laterally move to other user accounts (mimikatz's sekurlsa::pth module)

Pass-the-hash attempt was blocked by Defender

Key Takeaways from Attack Flow



Initial Access

T1566.001
Phishing: Spearphishing Attachment

The attacker sends a phishing email containing a malicious attachment (Word document)

The phishing email was quarantined by the email filter, hence it did not land in the user's inbox

Execution

T1204.002
User Execution: Malicious File

Victim opened the malicious Word document and enabled macros

By default, macros are blocked for Office files from the internet

Command and Control

T1071.001
Application Layer Protocol: Web Protocols

Use HTTP(S) listeners to communicate with C2 server

Discovery

T1518
Software Discovery

Enumerate software installed on compromised machine

T1083
File and Directory Discovery

List files and directories: ` dir`

T1016
System Information Discovery

Enumerate system information of compromised machine: ` systeminfo`

Persistence

T1053.005
Scheduled Task/Job: Scheduled Task

Gain persistence via scheduled task creation

Exfiltration

T1041
Exfiltration over C2 Channel

Exfiltrate data via C2 channel, via HTTP(S)

Privilege Escalation

T1068
Exploitation for Privilege Escalation

Exploit known, unpatched CVE on the compromised machine to escalate privileges

Current privileges: admin

Credential Access

T1003.001
OS Credential Dumping: LSASS Memory

Use mimikatz to dump credentials and hashes

Execution of mimikatz was blocked by Defender

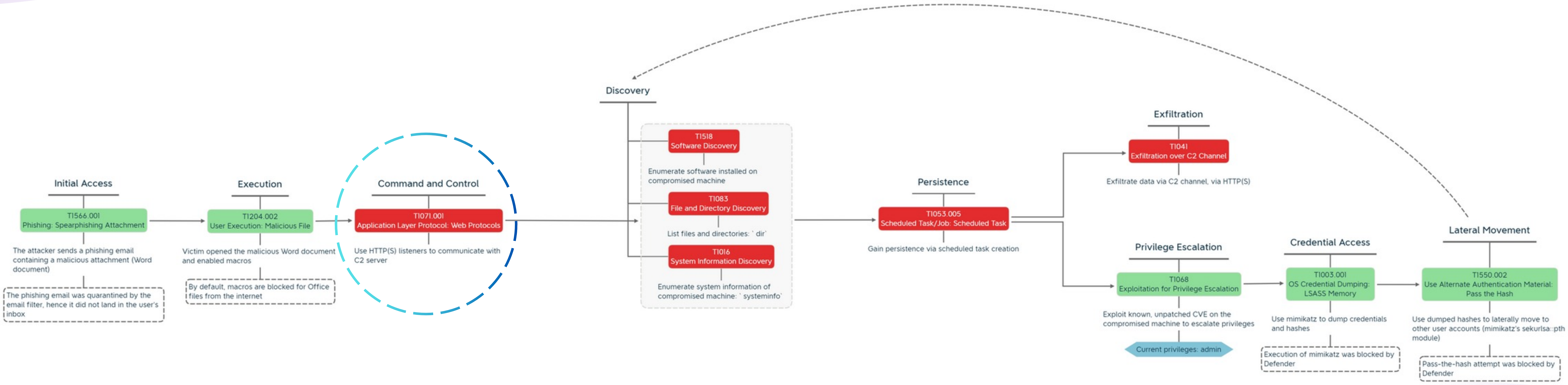
Lateral Movement

T1550.002
Use Alternate Authentication Material: Pass the Hash

Use dumped hashes to laterally move to other user accounts (mimikatz's sekurlsa::pth module)

Pass-the-hash attempt was blocked by Defender

Key Takeaways from Attack Flow



Initial Access

T1566.001
Phishing: Spearphishing Attachment

The attacker sends a phishing email containing a malicious attachment (Word document)

The phishing email was quarantined by the email filter, hence it did not land in the user's inbox

Execution

T1204.002
User Execution: Malicious File

Victim opened the malicious Word document and enabled macros

By default, macros are blocked for Office files from the internet

Command and Control

T1071.001
Application Layer Protocol: Web Protocols

Use HTTP(S) listeners to communicate with C2 server

Discovery

T1518
Software Discovery

Enumerate software installed on compromised machine

T1083
File and Directory Discovery

List files and directories: ` dir`

T1016
System Information Discovery

Enumerate system information of compromised machine: ` systeminfo`

Persistence

T1053.005
Scheduled Task/Job: Scheduled Task

Gain persistence via scheduled task creation

Exfiltration

T1041
Exfiltration over C2 Channel

Exfiltrate data via C2 channel, via HTTP(S)

Privilege Escalation

T1068
Exploitation for Privilege Escalation

Exploit known, unpatched CVE on the compromised machine to escalate privileges

Current privileges: admin

Credential Access

T1003.001
OS Credential Dumping: LSASS Memory

Use mimikatz to dump credentials and hashes

Execution of mimikatz was blocked by Defender

Lateral Movement

T1550.002
Use Alternate Authentication Material: Pass the Hash

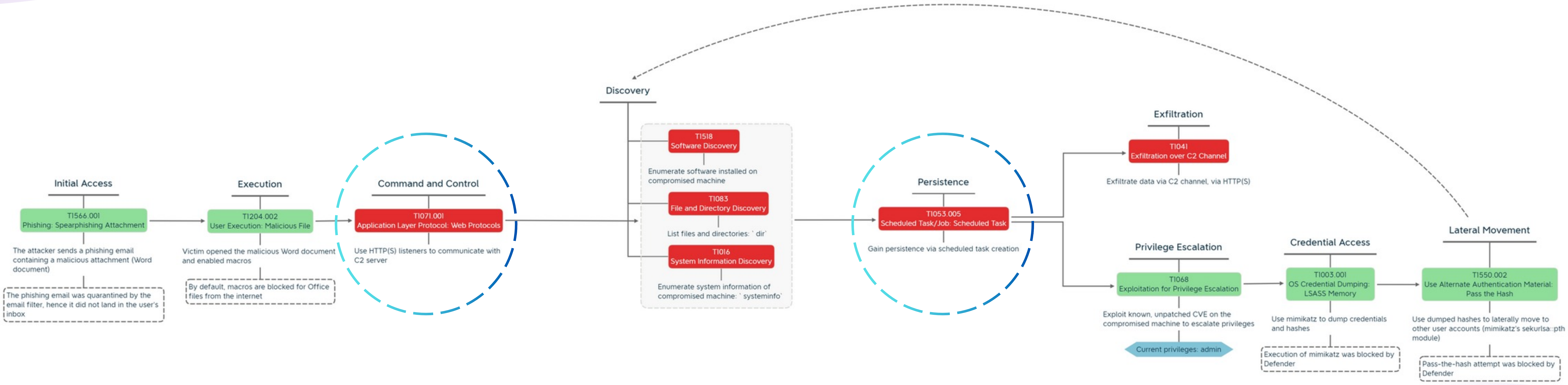
Use dumped hashes to laterally move to other user accounts (mimikatz's sekurlsa::pth module)

Pass-the-hash attempt was blocked by Defender

Instead of trying to implement defensive measures for every technique...

- Focus on techniques at the start of the flow

Key Takeaways from Attack Flow



Initial Access

T1566.001
Phishing: Spearphishing Attachment

The attacker sends a phishing email containing a malicious attachment (Word document)

The phishing email was quarantined by the email filter, hence it did not land in the user's inbox

Execution

T1204.002
User Execution: Malicious File

Victim opened the malicious Word document and enabled macros

By default, macros are blocked for Office files from the internet

Command and Control

T1071.001
Application Layer Protocol: Web Protocols

Use HTTP(S) listeners to communicate with C2 server

Discovery

T1518
Software Discovery

Enumerate software installed on compromised machine

T1083
File and Directory Discovery

List files and directories: ` dir`

T1016
System Information Discovery

Enumerate system information of compromised machine: ` systeminfo`

Persistence

T1053.005
Scheduled Task/Job: Scheduled Task

Gain persistence via scheduled task creation

Exfiltration

T1041
Exfiltration over C2 Channel

Exfiltrate data via C2 channel, via HTTP(S)

Privilege Escalation

T1068
Exploitation for Privilege Escalation

Exploit known, unpatched CVE on the compromised machine to escalate privileges

Current privileges: admin

Credential Access

T1003.001
OS Credential Dumping: LSASS Memory

Use mimikatz to dump credentials and hashes

Execution of mimikatz was blocked by Defender

Lateral Movement

T1550.002
Use Alternate Authentication Material: Pass the Hash

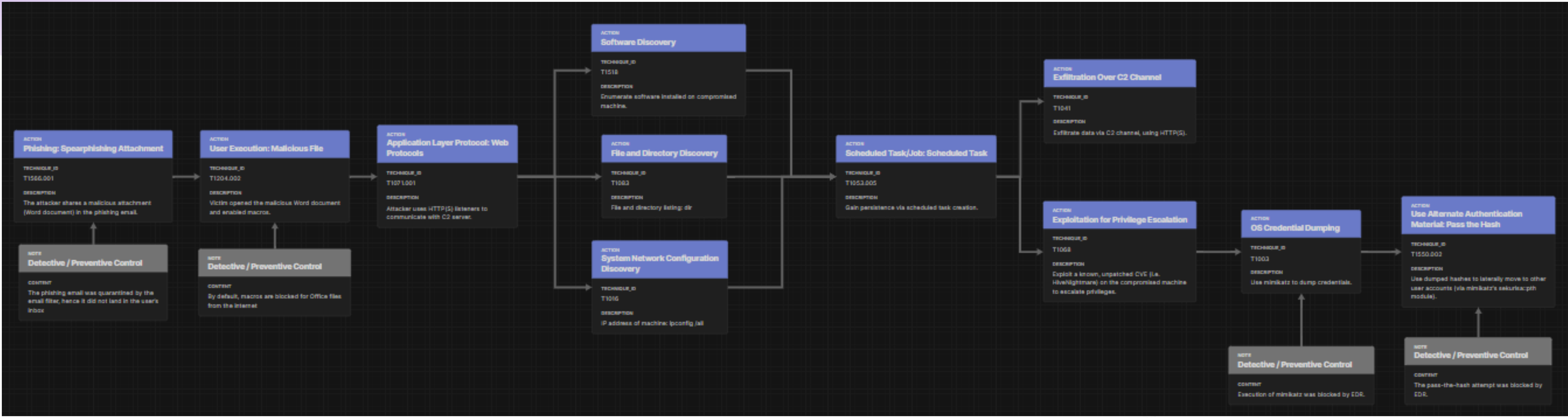
Use dumped hashes to laterally move to other user accounts (mimikatz's sekurlsa::pth module)

Pass-the-hash attempt was blocked by Defender

Instead of trying to implement defensive measures for every technique...

- Focus on techniques at the start of the flow
- Address chokepoints in the flow

MITRE CTID’s Attack Flow Builder



ACTION
Phishing: Spearphishing Attachment
TECHNIQUE_ID
T1566.001
DESCRIPTION
The attacker shares a malicious attachment (Word document) in the phishing email.

NOTE
Detective / Preventive Control
CONTENT
The phishing email was quarantined by the email filter, hence it did not land in the user's inbox

ACTION
User Execution: Malicious File
TECHNIQUE_ID
T1204.002
DESCRIPTION
Victim opened the malicious Word document and enabled macros.

NOTE
Detective / Preventive Control
CONTENT
By default, macros are blocked for Office files from the internet

ACTION
Application Layer Protocol: Web Protocools
TECHNIQUE_ID
T1071.001
DESCRIPTION
Attacker uses HTTP(S) listeners to communicate with C2 server.

ACTION
Software Discovery
TECHNIQUE_ID
T1518
DESCRIPTION
Enumerate software installed on compromised machine.

ACTION
File and Directory Discovery
TECHNIQUE_ID
T1083
DESCRIPTION
File and directory listing: dir

ACTION
System Network Configuration Discovery
TECHNIQUE_ID
T1016
DESCRIPTION
IP address of machine: ipconfig /all

ACTION
Scheduled Task/Job: Scheduled Task
TECHNIQUE_ID
T1053.005
DESCRIPTION
Gain persistence via scheduled task creation.

ACTION
Exfiltration Over C2 Channel
TECHNIQUE_ID
T1041
DESCRIPTION
Exfiltrate data via C2 channel, using HTTP(S).

ACTION
Exploitation for Privilege Escalation
TECHNIQUE_ID
T1068
DESCRIPTION
Exploit a known, unpatched CVE (i.e. HiveNightmare) on the compromised machine to escalate privileges.

ACTION
OS Credential Dumping
TECHNIQUE_ID
T1003
DESCRIPTION
Use mimikatz to dump credentials.

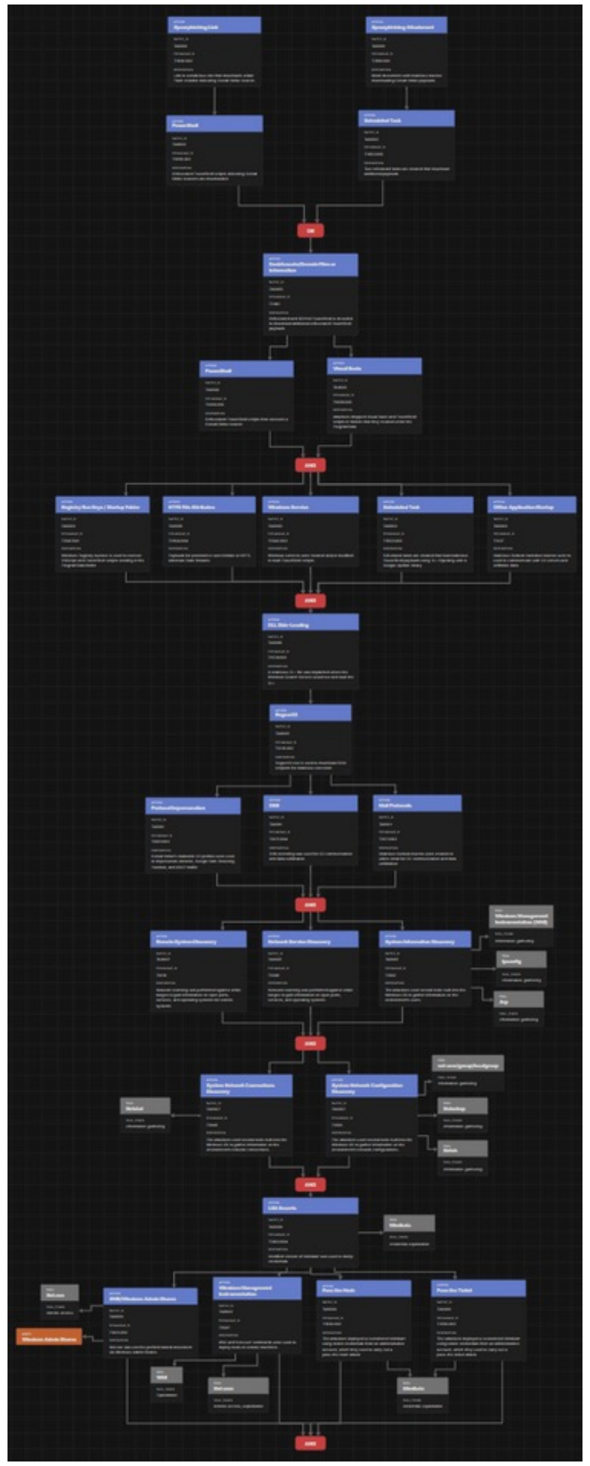
NOTE
Detective / Preventive Control
CONTENT
Execution of mimikatz was blocked by EDR.

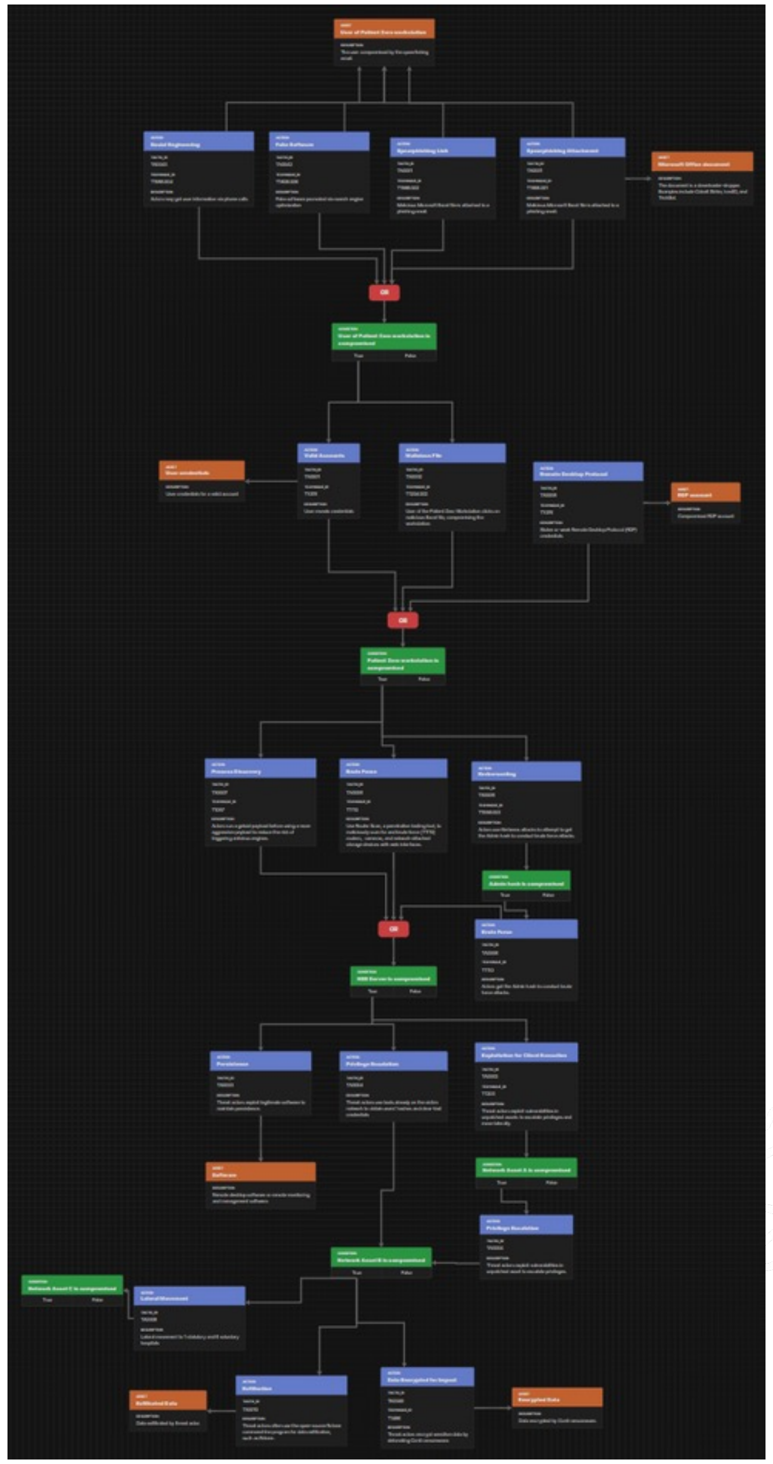
ACTION
Use Alternate Authentication Material: Pass the Hash
TECHNIQUE_ID
T1550.002
DESCRIPTION
Use dumped hashes to laterally move to other user accounts (via mimikatz's sekurlsa::pth module).

NOTE
Detective / Preventive Control
CONTENT
The pass-the-hash attempt was blocked by EDR.

Access Attack Flow Builder at: https://center-for-threat-informed-defense.github.io/attack-flow/ui/

More Examples of Attack Flows

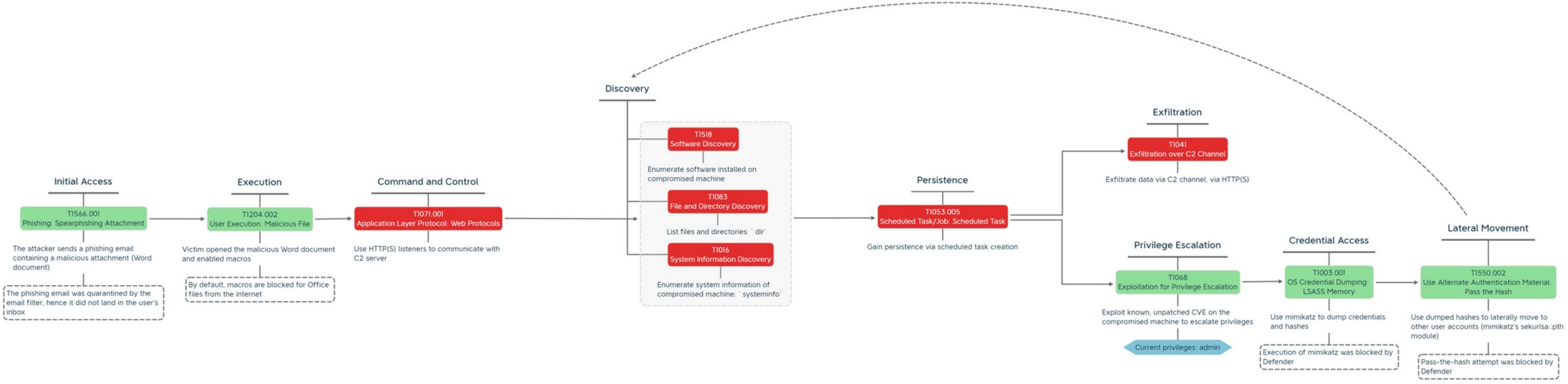




- Attack Flows from MITRE CTID’s corpus
- Access them at: https://center-for-threat-informed-defense.github.io/attack-flow/example_flows/

Heatmap vs Attack Flow

Initial Access	**Execution**	**Persistence**	**Privilege Escalation**	**Credential Access**	**Discovery**	**Lateral Movement**	**Command & Control**	**Exfiltration**
🟩 Phishing: Spearphishing Attachment	🟩 User Execution: Malicious File	🟥 Scheduled Task/Job	🟩 Exploitation for Privilege Escalation	🟩 OS Credential Dumping: LSASS Memory	🟥 File and Directory Discovery	🟩 Pass the Hash	🟥 Application Layer Protocol: Web Protocols	🟥 Exfiltration Over C2 Channel
					🟥 Software Discovery			
					🟥 System Information Discovery			


Initial Access
T1566.001
Phishing: Spearphishing Attachment
Execution
T1204.002
User Execution: Malicious File
Command and Control
T1071.001
Application Layer Protocol: Web Protocols
Discovery
T1518
Software Discovery
T1083
File and Directory Discovery
T1016
System Information Discovery
Persistence
T1053.005
Scheduled Task/Job: Scheduled Task
Exfiltration
T1041
Exfiltration over C2 Channel
Privilege Escalation
T1068
Exploitation for Privilege Escalation
Current privileges: admin
Credential Access
T1003.001
OS Credential Dumping: LSASS Memory
Lateral Movement
T1550.002
Use Alternate Authentication Material: Pass the Hash

The attacker sends a phishing email containing a malicious attachment (Word document)

The phishing email was quarantined by the email filter, hence it did not land in the user's inbox

Victim opened the malicious Word document and enabled macros

By default, macros are blocked for Office files from the internet

Use HTTP(S) listeners to communicate with C2 server

Enumerate software installed on compromised machine

List files and directories: ` dir`

Enumerate system information of compromised machine: ` systeminfo`

Gain persistence via scheduled task creation

Exfiltrate data via C2 channel, via HTTP(S)

Exploit known, unpatched CVE on the compromised machine to escalate privileges

Use mimikatz to dump credentials and hashes

Execution of mimikatz was blocked by Defender

Use dumped hashes to laterally move to other user accounts (mimikatz's sekurlsa::pth module)

Pass-the-hash attempt was blocked by Defender

Conclusion

Heatmap

Attack Flow

helps us to allocate resources more efficiently

Thank you