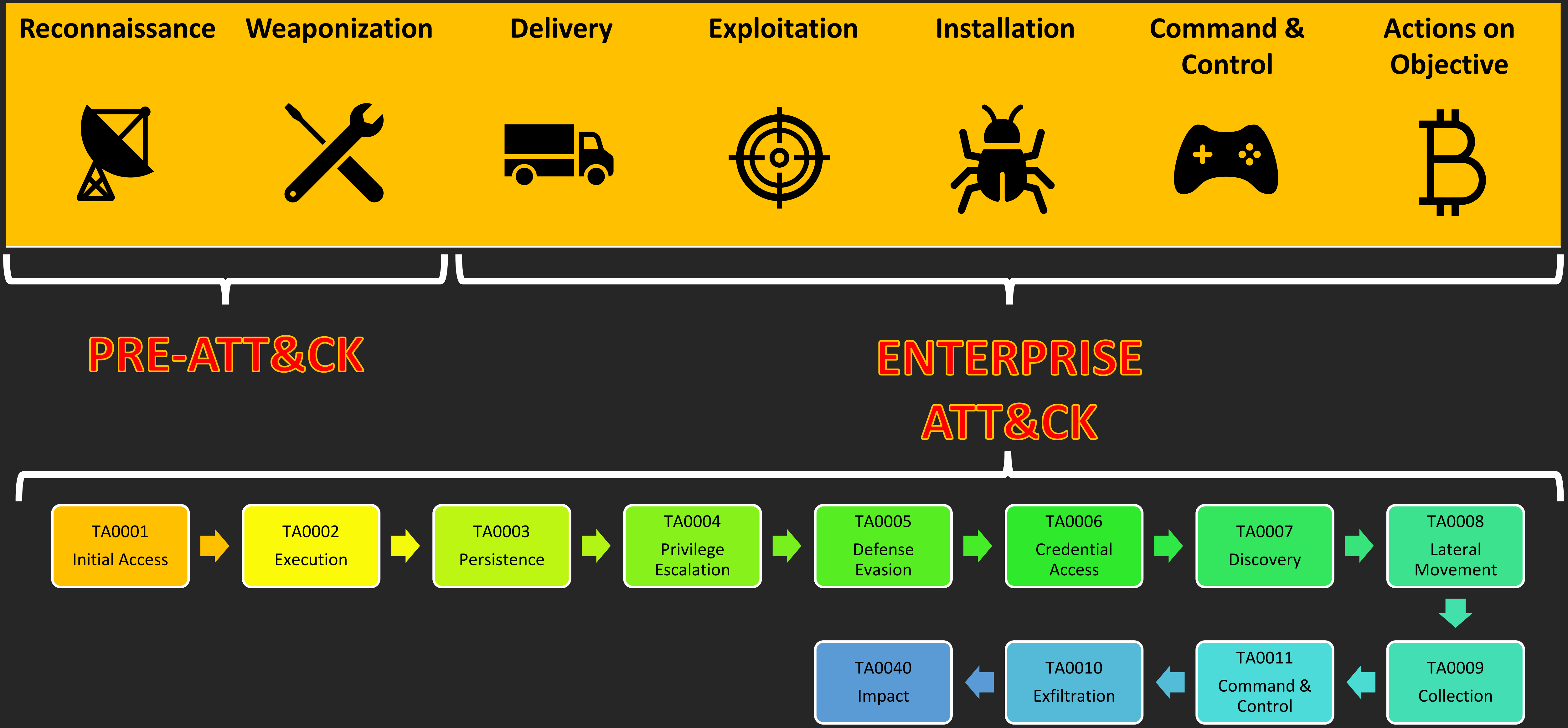
Cyber Kill Chain and MITRE ATT&CK



Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command & Control

Actions on Objective

PRE-ATT&CK

ENTERPRISE ATT&CK

TA0001 Initial Access

TA0002 Execution

TA0003 Persistence

TA0004 Privilege Escalation

TA0005 Defense Evasion

TA0006 Credential Access

TA0007 Discovery

TA0008 Lateral Movement

TA0009 Collection

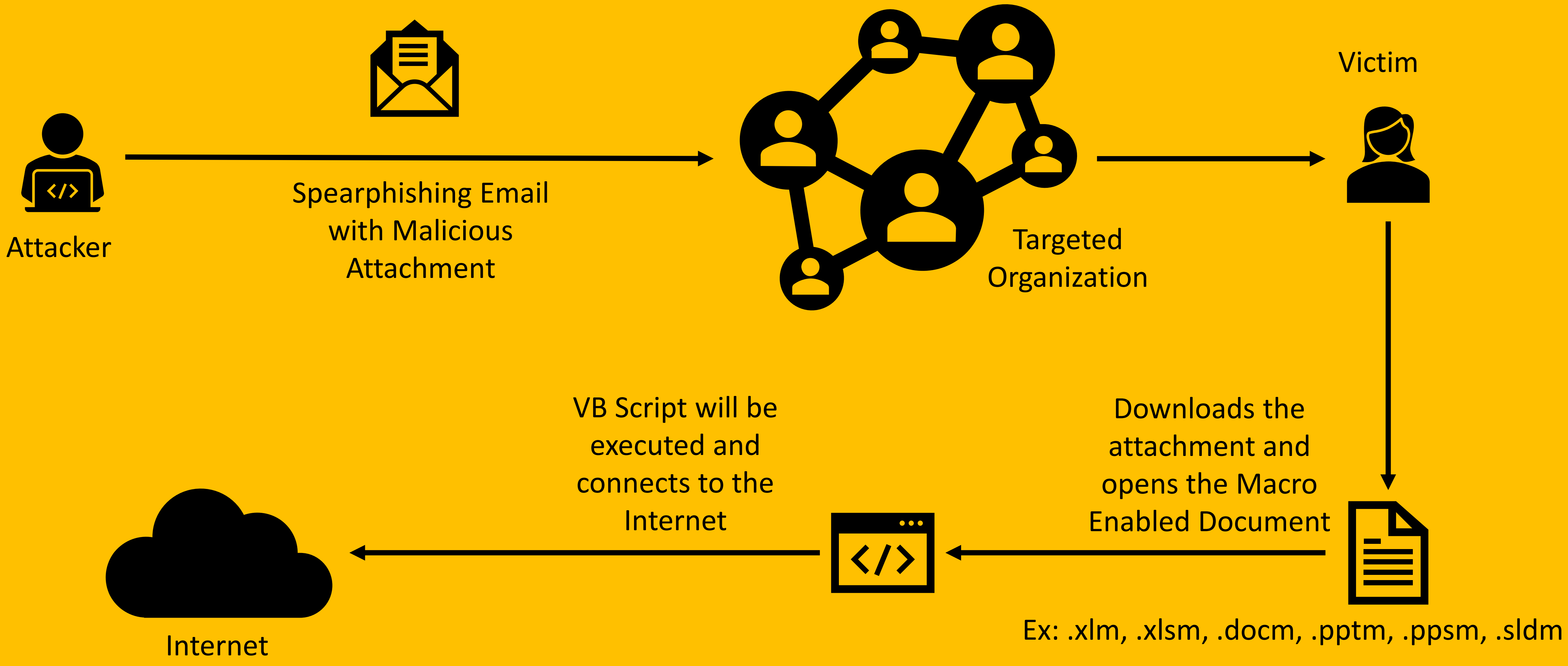
TA0011 Command & Control

TA0010 Exfiltration

TA0040 Impact

TA0001 - Initial Access

T1193 - Spearphishing Attachment (Windows)



Attacker

Spearphishing Email with Malicious Attachment

Targeted Organization

Victim

Downloads the attachment and opens the Macro Enabled Document

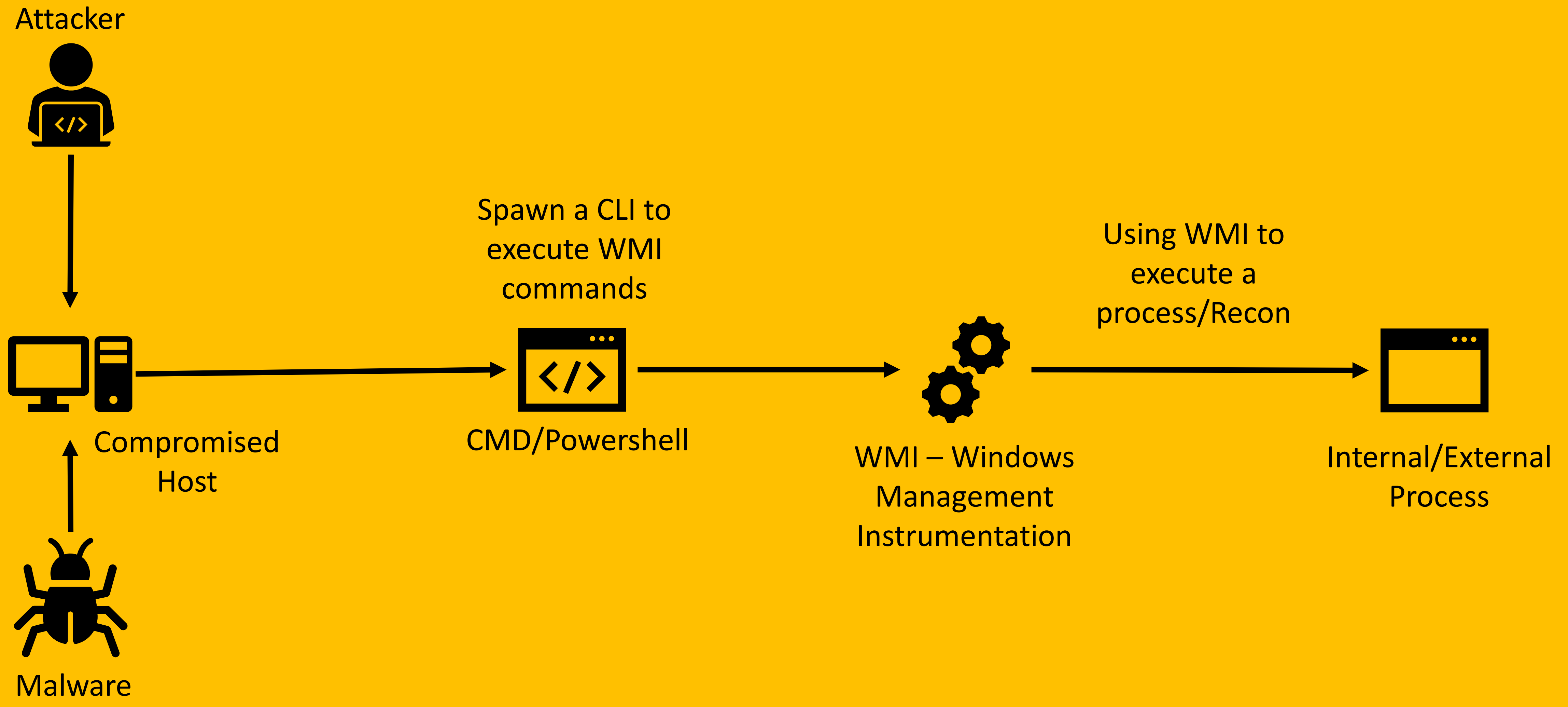
Ex: .xlm, .xlsm, .docm, .pptm, .ppsm, .sldm

VB Script will be executed and connects to the Internet

Internet

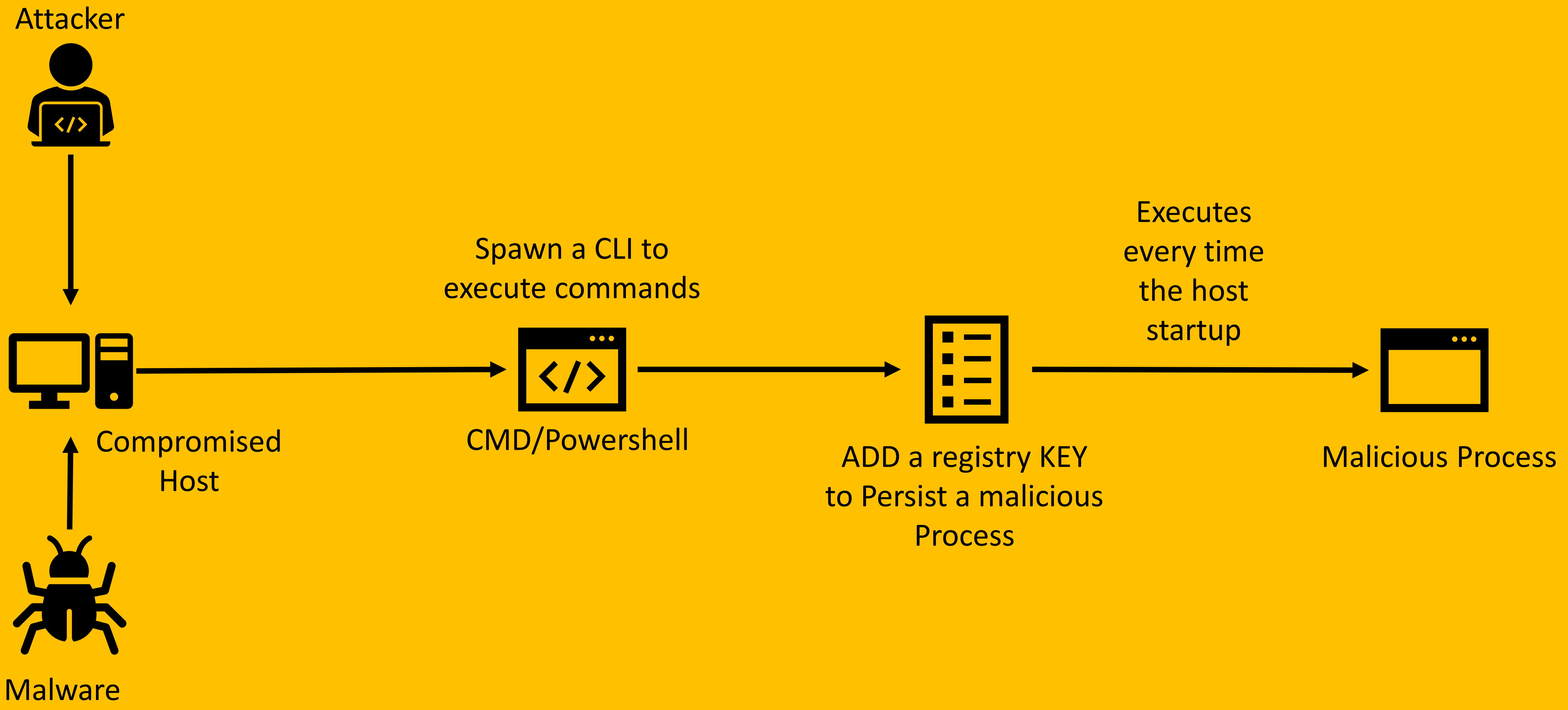
TA0002 - Execution

T1047 - Windows Management Instrumentation (Windows)


Attacker
Spawn a CLI to execute WMI commands
Using WMI to execute a process/Recon
Compromised Host
CMD/Powershell
WMI – Windows Management Instrumentation
Internal/External Process
Malware

TA0003 - Persistence

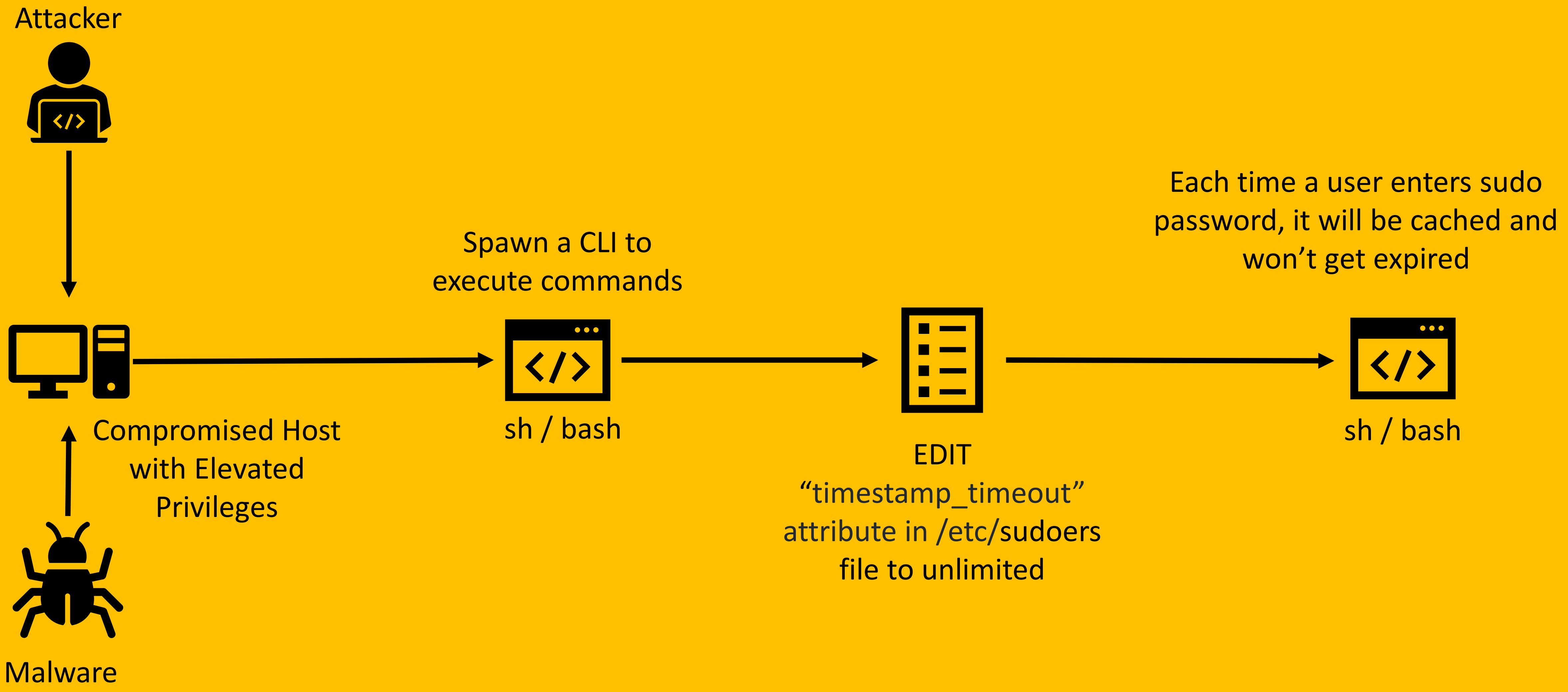
T1060 - Registry Run Keys / Startup Folder (Windows)



Attacker
Spawn a CLI to execute commands
Executes every time the host startup
Compromised Host
CMD/Powershell
ADD a registry KEY to Persist a malicious Process
Malicious Process
Malware

TA0004 - Privilege Escalation

T1206 - Sudo Caching (Linux)



Attacker

Compromised Host with Elevated Privileges

Malware

Spawn a CLI to execute commands

sh / bash

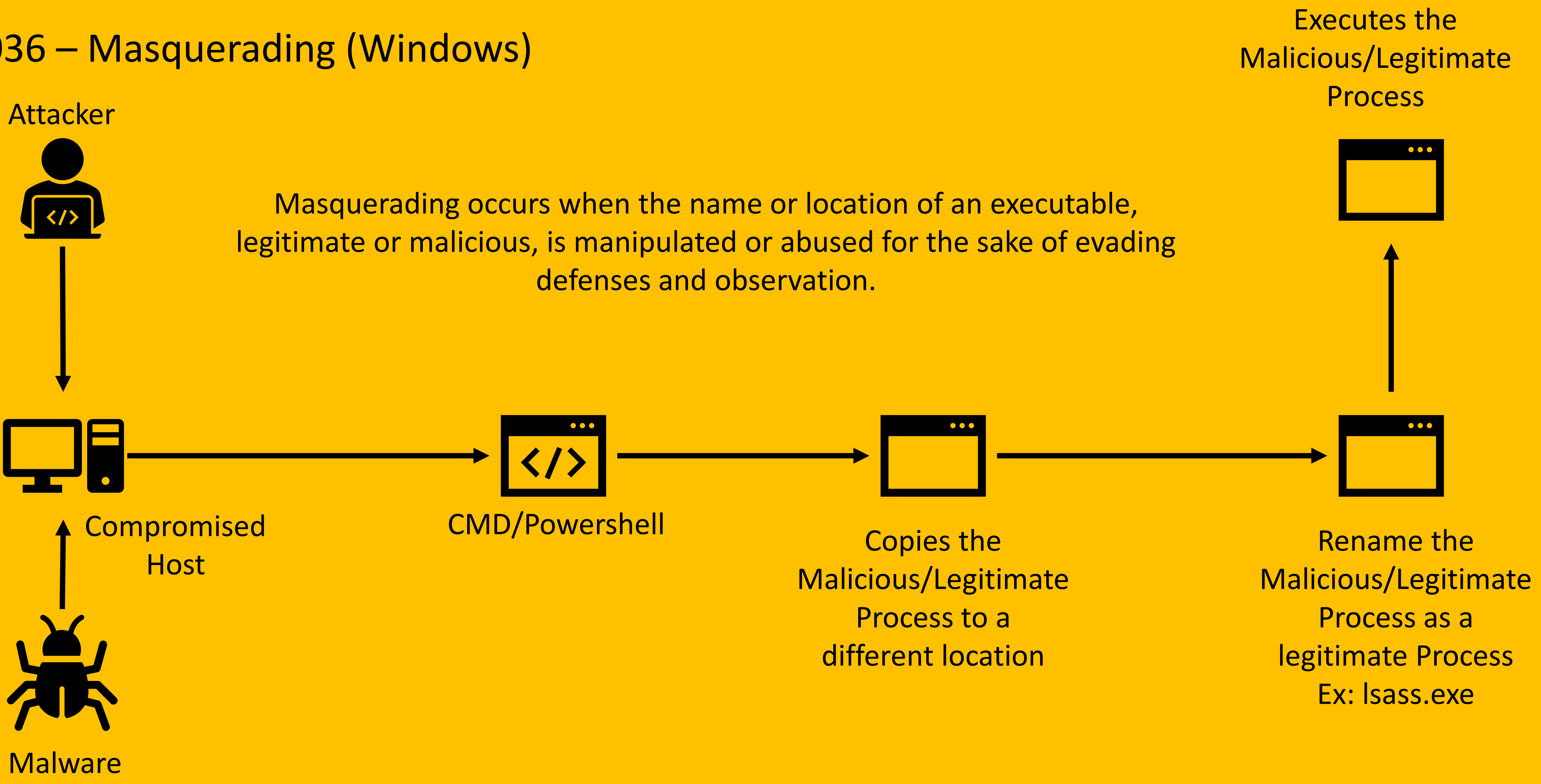
EDIT “timestamp_timeout” attribute in /etc/sudoers file to unlimited

Each time a user enters sudo password, it will be cached and won’t get expired

sh / bash

TA0005 - Defense Evasion

T1036 – Masquerading (Windows)



Masquerading occurs when the name or location of an executable, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation.

Attacker

Compromised Host

Malware

CMD/Powershell

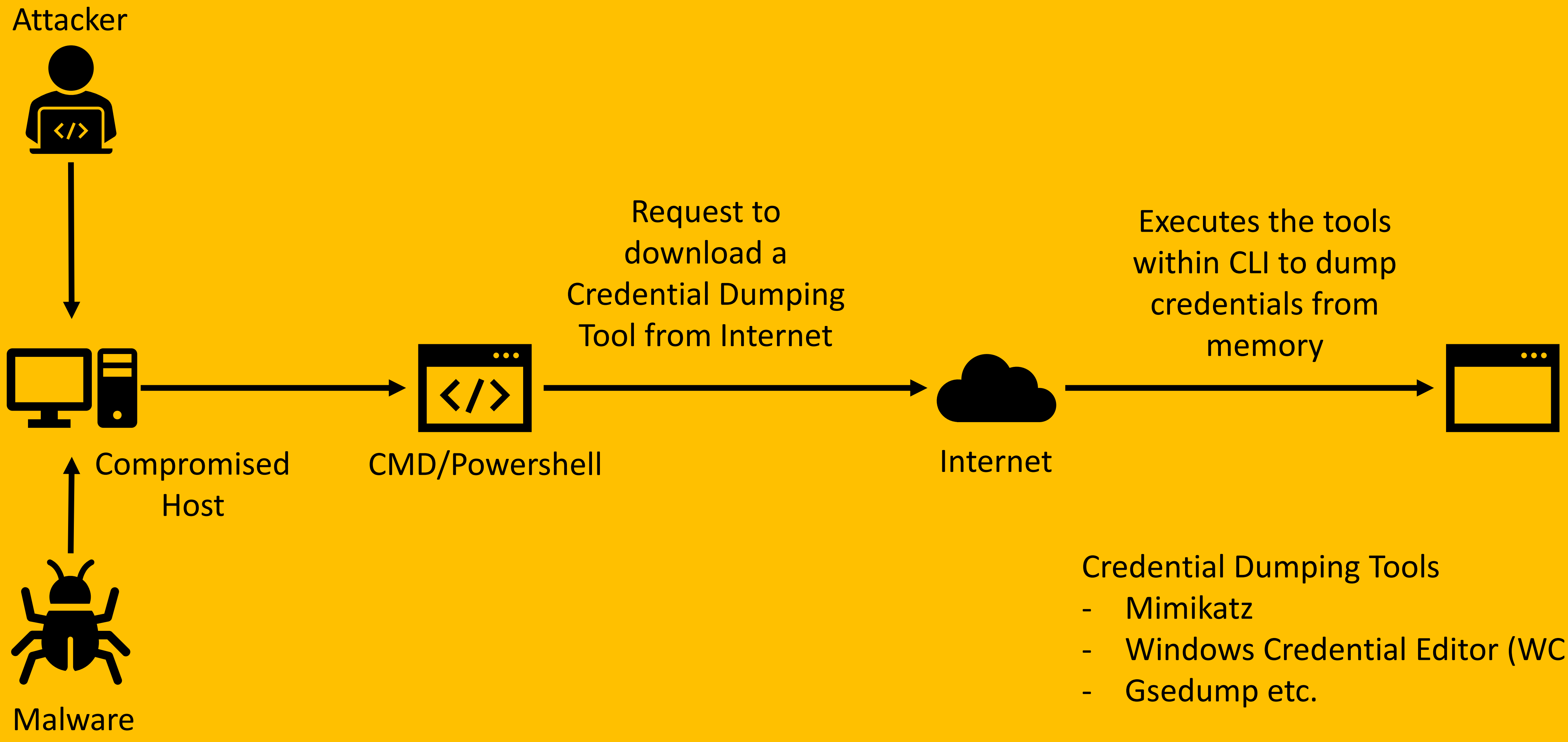
Copies the Malicious/Legitimate Process to a different location

Rename the Malicious/Legitimate Process as a legitimate Process Ex: lsass.exe

Executes the Malicious/Legitimate Process

TA0006 - Credential Access

T1003 - Credential Dumping (Windows)



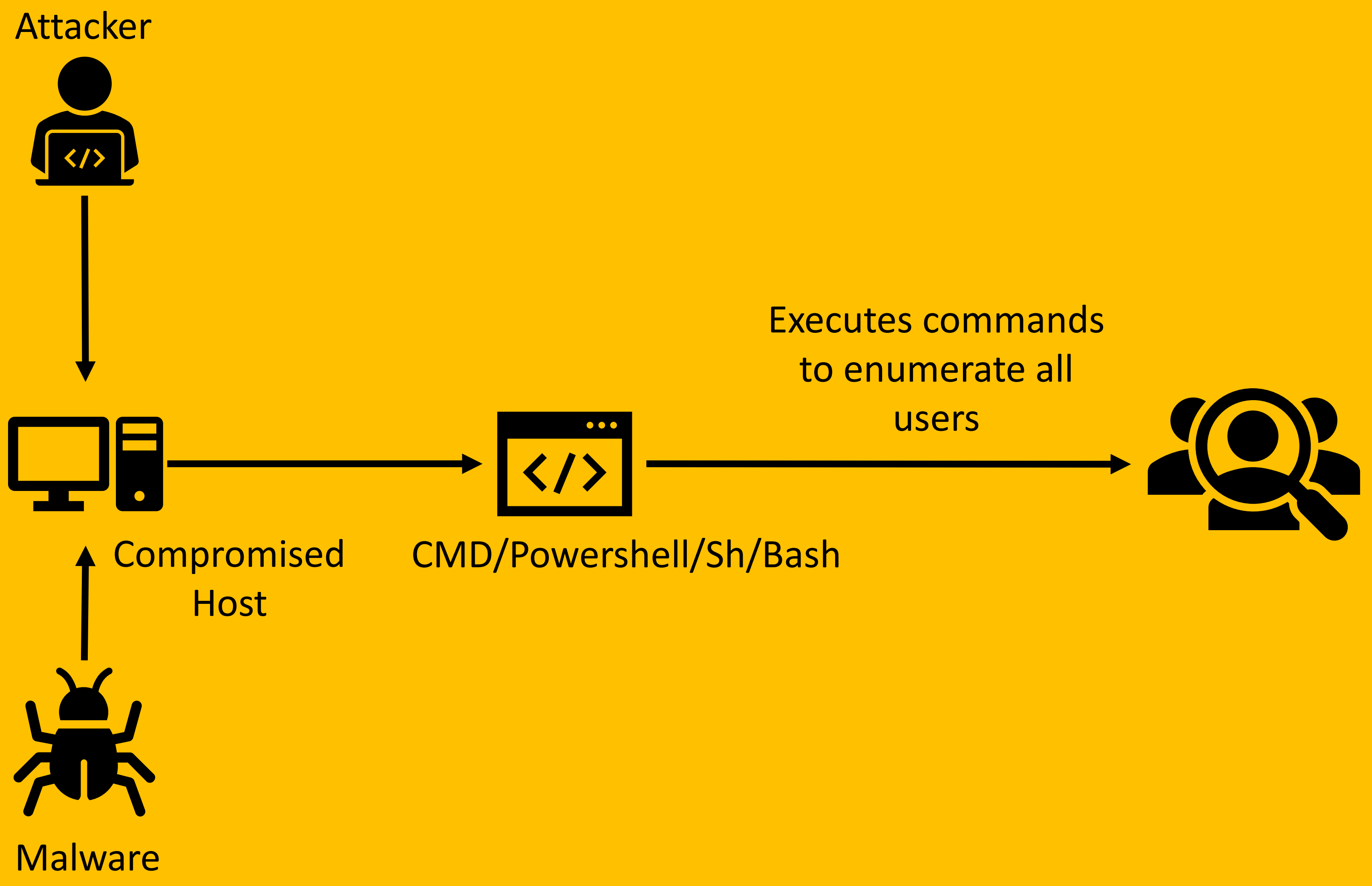
Attacker
Request to download a Credential Dumping Tool from Internet
Executes the tools within CLI to dump credentials from memory
Compromised Host
CMD/Powershell
Internet
Malware

Credential Dumping Tools

- Mimikatz
- Windows Credential Editor (WCE)
- Gsedump etc.

TA0007 - Discovery

T1087 - Account Discovery (Windows / Linux)



Attacker

Compromised Host

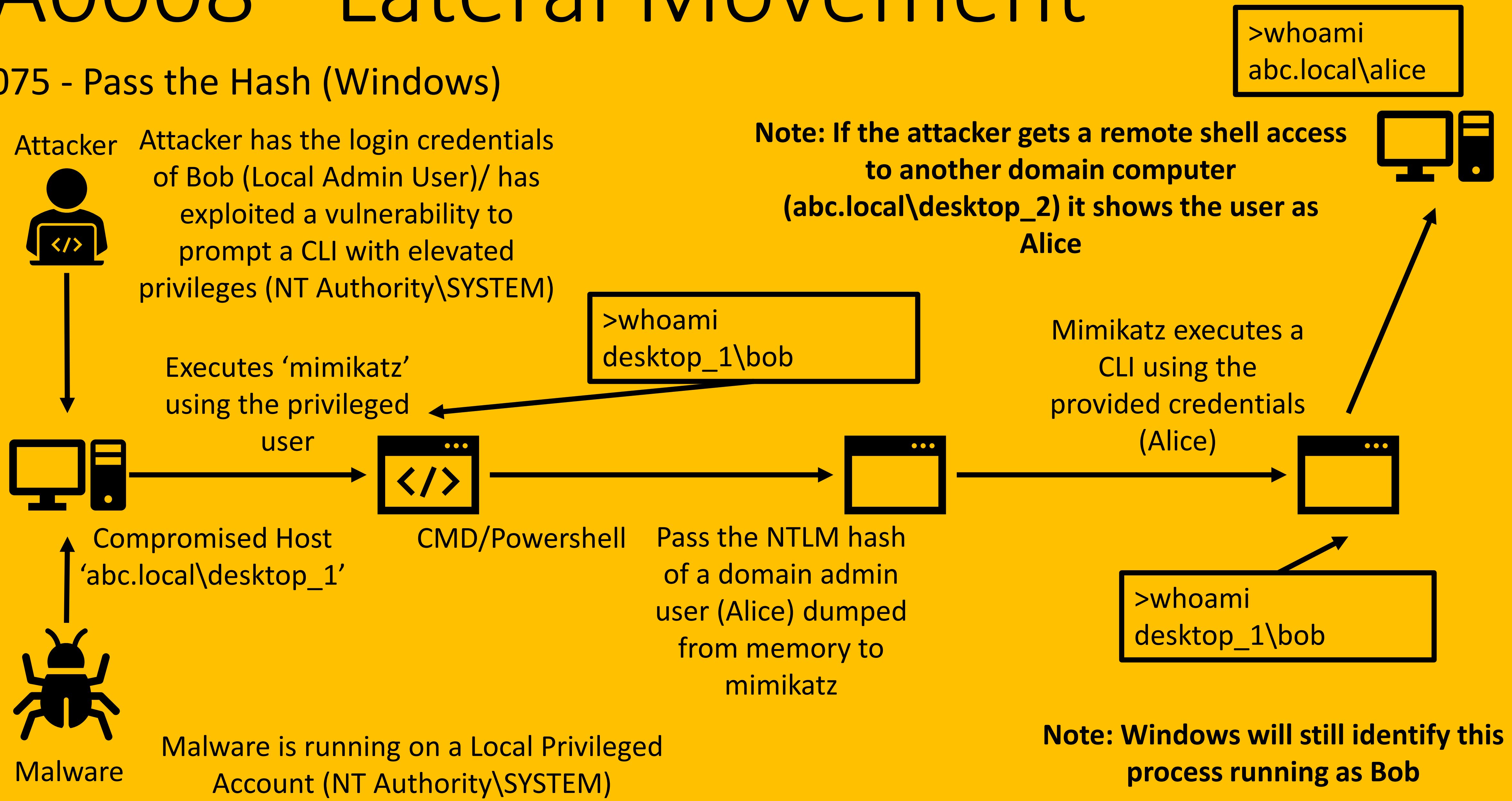
CMD/Powershell/Sh/Bash

Executes commands to enumerate all users

Malware

TA0008 - Lateral Movement

T1075 - Pass the Hash (Windows)



Attacker

Attacker has the login credentials of Bob (Local Admin User)/ has exploited a vulnerability to prompt a CLI with elevated privileges (NT Authority\SYSTEM)

Compromised Host ‘abc.local\desktop_1’

Malware

Malware is running on a Local Privileged Account (NT Authority\SYSTEM)

Executes ‘mimikatz’ using the privileged user

```
>whoami
desktop_1\bob
```

CMD/Powershell

Pass the NTLM hash of a domain admin user (Alice) dumped from memory to mimikatz

Mimikatz executes a CLI using the provided credentials (Alice)

```
>whoami
desktop_1\bob
```

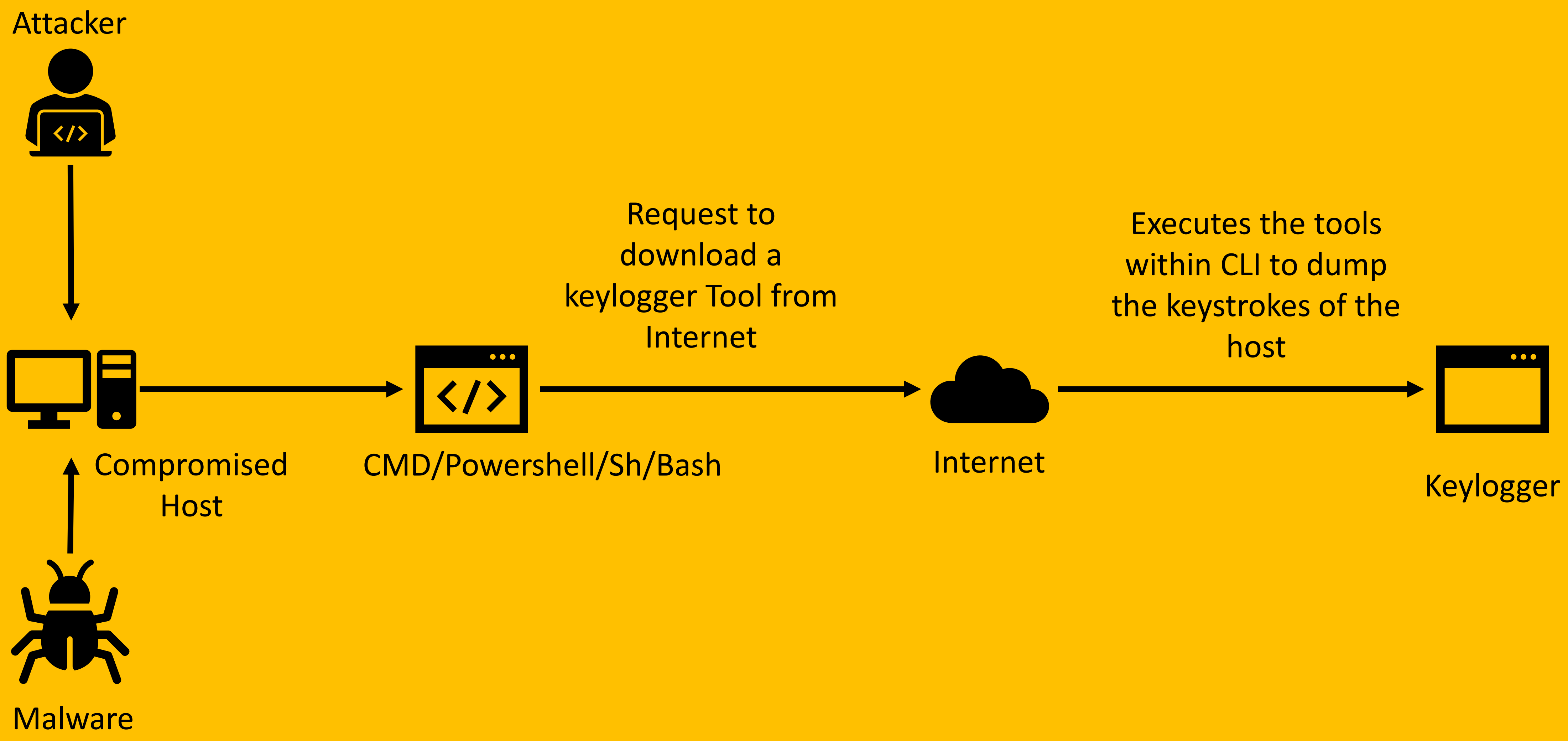
Note: Windows will still identify this process running as Bob

```
>whoami
abc.local\alice
```

Note: If the attacker gets a remote shell access to another domain computer (abc.local\desktop_2) it shows the user as Alice

TA0009 - Collection

T1056 – Keylogging (Windows / Linux)



Attacker

Compromised Host

Malware

CMD/Powershell/Sh/Bash

Request to download a keylogger Tool from Internet

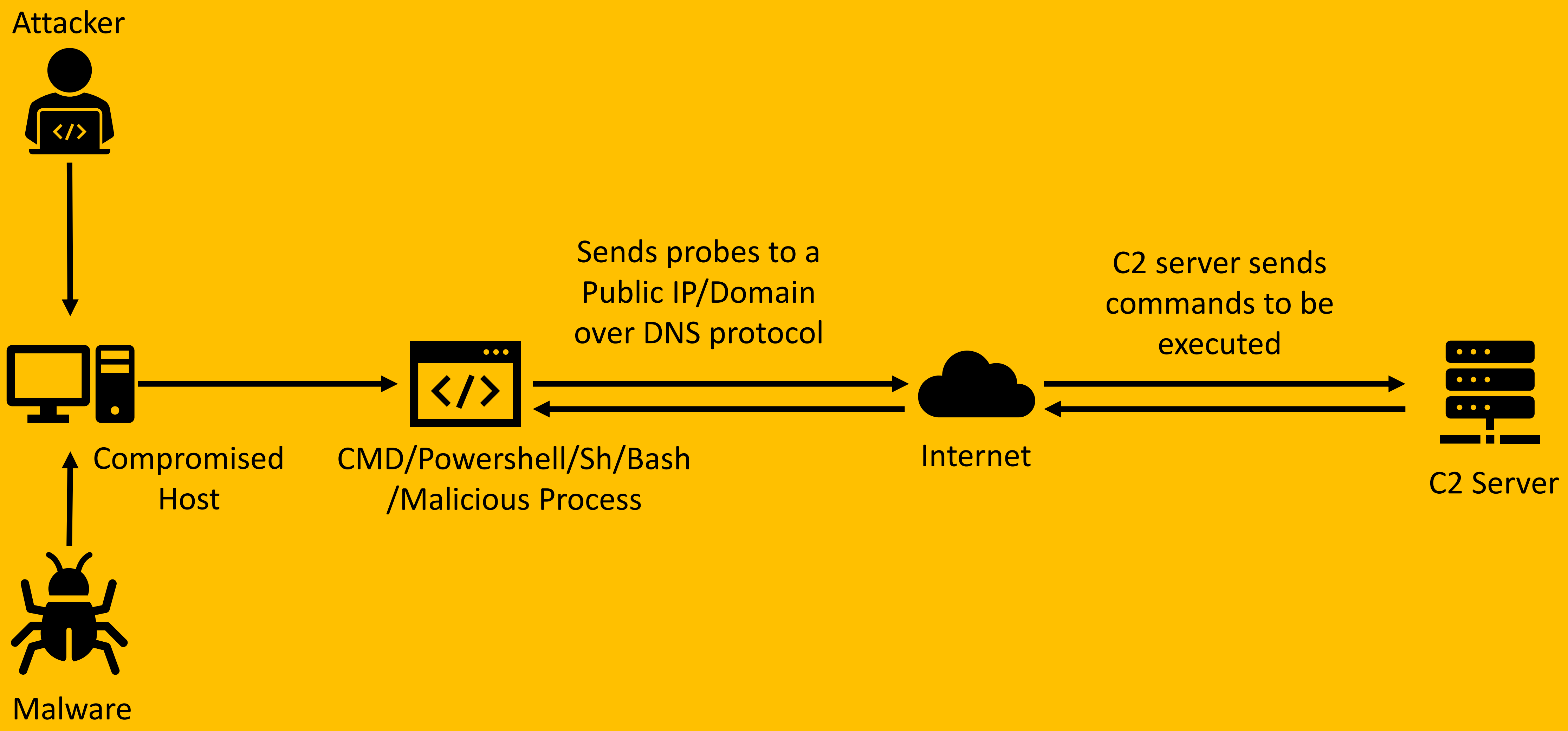
Internet

Executes the tools within CLI to dump the keystrokes of the host

Keylogger

TA0011 - Command & Control

T1071 – DNS (Windows / Linux)



Attacker

Compromised Host

Malware

CMD/Powershell/Sh/Bash /Malicious Process

Sends probes to a Public IP/Domain over DNS protocol

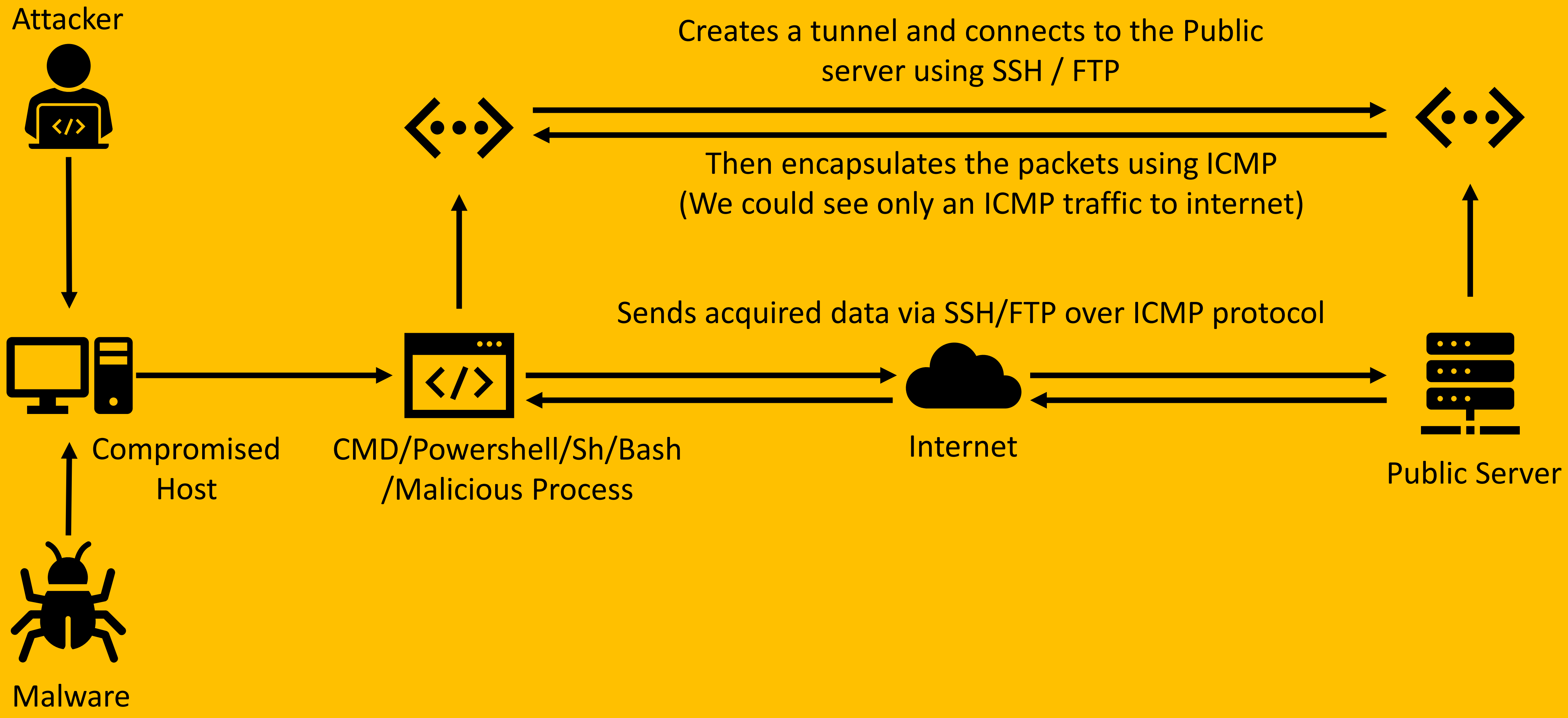
Internet

C2 server sends commands to be executed

C2 Server

TA0010 - Exfiltration

T1048 - Exfiltration Over Alternative Protocol (Windows / Linux)



Attacker

Creates a tunnel and connects to the Public server using SSH / FTP

Then encapsulates the packets using ICMP
(We could see only an ICMP traffic to internet)

Sends acquired data via SSH/FTP over ICMP protocol

Compromised Host

CMD/Powershell/Sh/Bash /Malicious Process

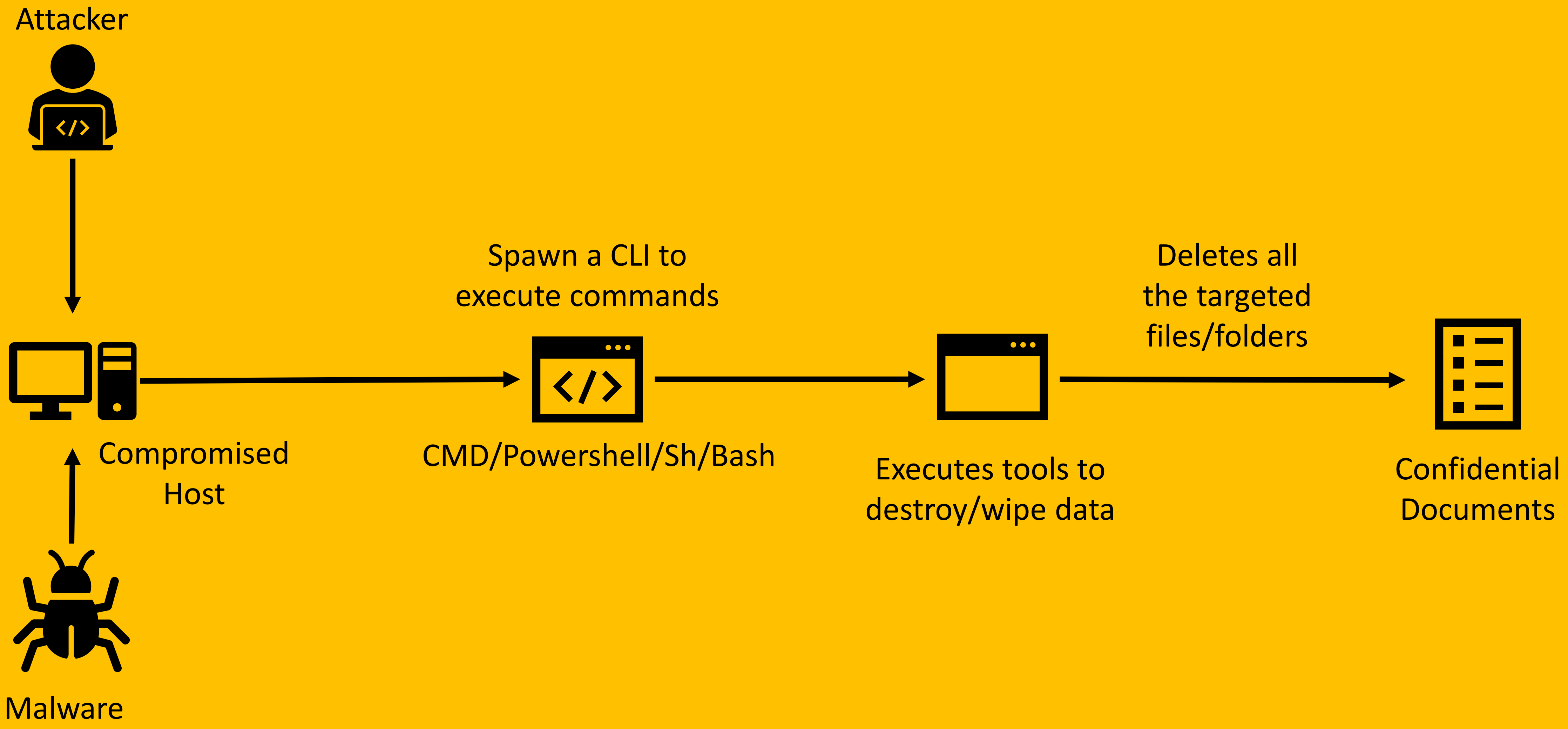
Internet

Public Server

Malware

TA0040 - Impact

T1485 - Data Destruction (Windows / Linux)



Attacker

Compromised Host

Malware

Spawn a CLI to execute commands

CMD/Powershell/Sh/Bash

Executes tools to destroy/wipe data

Deletes all the targeted files/folders

Confidential Documents