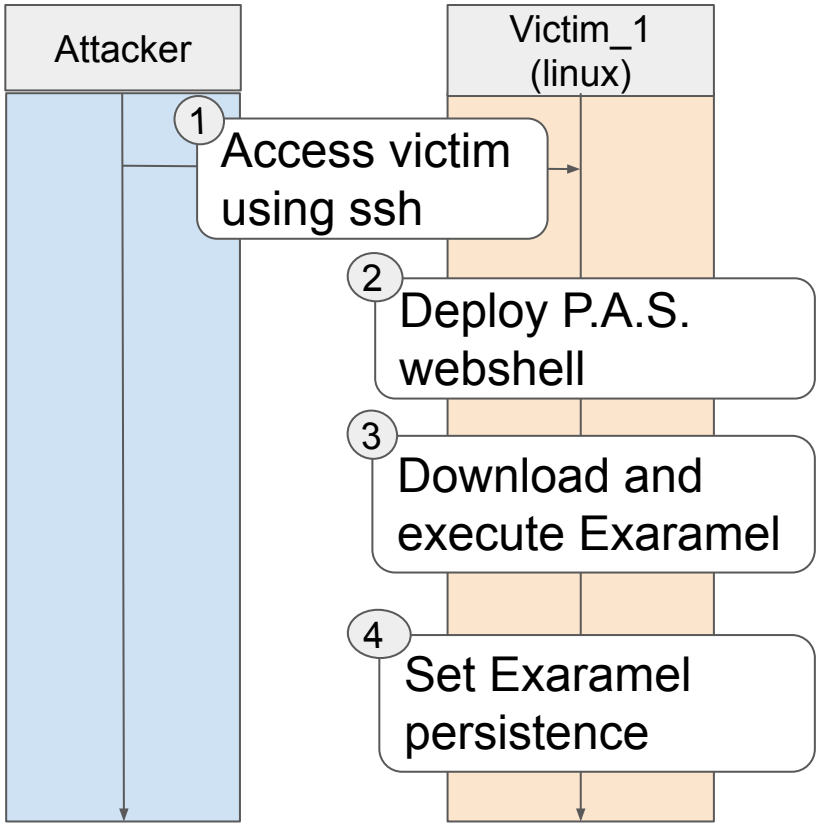
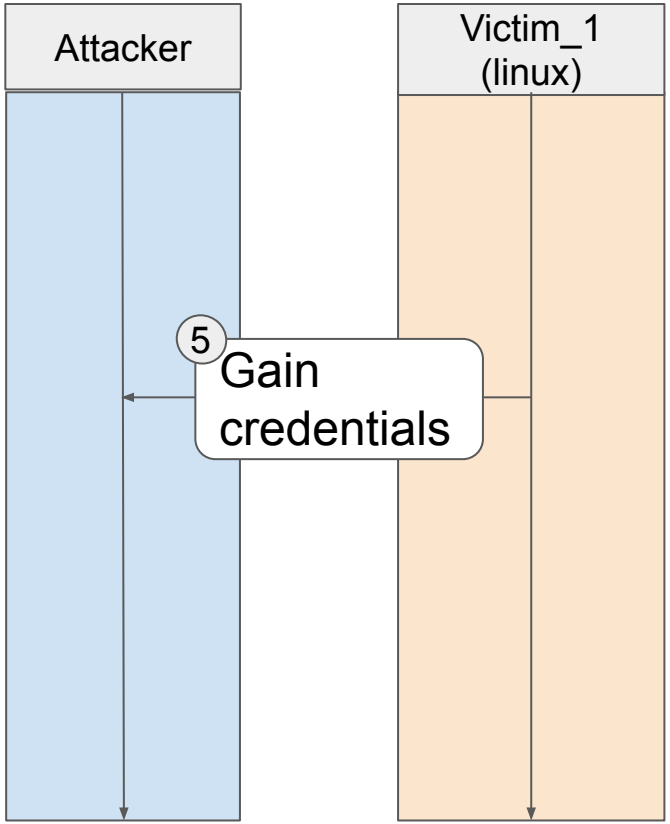
Wizard_spider&Sandworm
攻擊串鏈流程圖

Sandworm



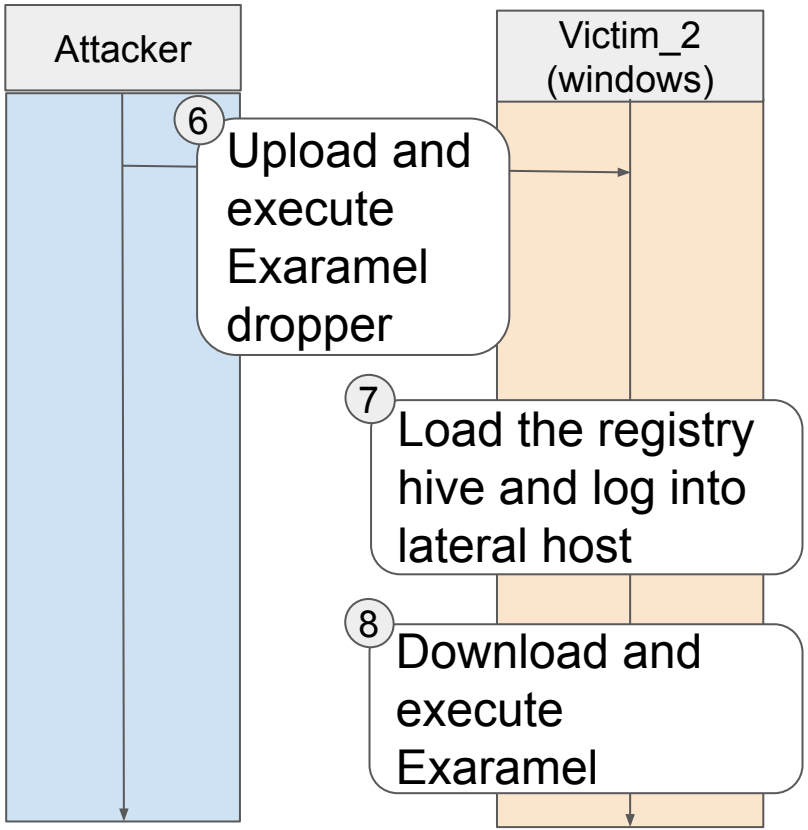
步驟	實作方法
access victim using ssh	ssh password guessing, zero day exploit… etc
Deploy P.A.S. webshell	用 scp 將 P.A.S. webshell 複製到 victim_1's /var/www/html, 使其可透過 httpd service 呼叫
Download and execute Exaramel	用 P.A.S. webshell curl 下載 exaramel service 用 chmod +x 讓 exaramel 可被執行, 透過有 root 權限的 SUID program 執行 (ex. /bin/backup)
Set Exaramel persistence	透過修改 linux crontab 定期執行 systemd 指令來確保 exaramel service 持續被運行

Sandworm



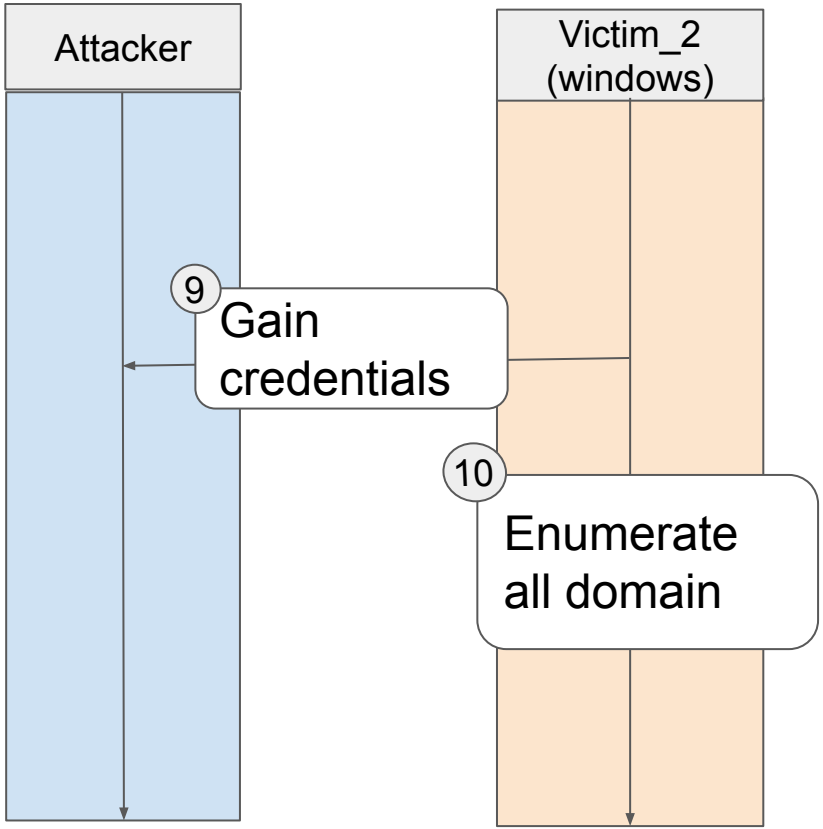
步驟	實作方法
gain credentials	用 curl 指令控制 P.A.S. webshell 執行 “whoami” (username)、 ”uname -a” (OS version)、 ”ls -lsahR / ” (file structure)、 cat /etc/passwd (user informations)、 cat /etc/shadow (encrypted password)、 cat /home/username/.bash_history (unsecured credentials)。 另外還要回傳 ssh key, 因為一開始可能不是透過正常的 ssh 登入 victim_1 (ex. zero day exploit)。

Sandworm



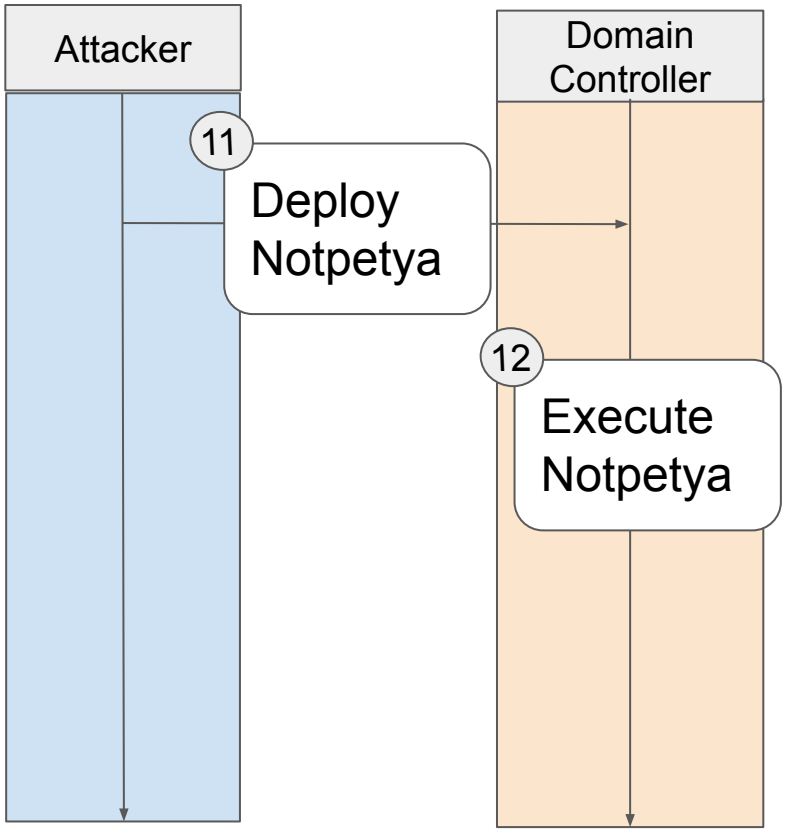
步驟	實作方法
Upload and execute Exaramel dropper	使用 step 5 獲得的 credentials 來透過 SMB channel 上傳 exaramel dropper 到 lateral host
Load the registry hive and log into lateral host	把 current user 的 registry hive 透過 bind-shell over SMB load 到 lateral host, 並使用 RDP 登入
Download and execute Exaramel	用 RDP session下載 Exaramel 並透過 rundll32.exe 執行

Sandworm



步驟	實作方法
Gain credentials	透過上傳 credentials dumper.exe 並執行，來下載所有 user 的 credentials
Enumerate all domain	透過執行 dsquery.exe 來 enumerate domain，尋找出 Domain Controller

Sandworm



步驟	實作方法
Deploy Notpetya	從 step 9 獲得的 domain admin credentials 透過 RDP 登入 Domain Controller，並下載 Notpetya
Execute Notpetya	透過 RDP 用 rundll32.exe 執行 Notpetya。 Notpetya 會 launch 一個叫 Restart 的 schedule，該 schedule 會針對 C:\ 進行 recursive encrypt，接著留下 ransom note C:\README.txt 後，繼續尋找其他的相鄰 IP copy and execute，最後 reboot。

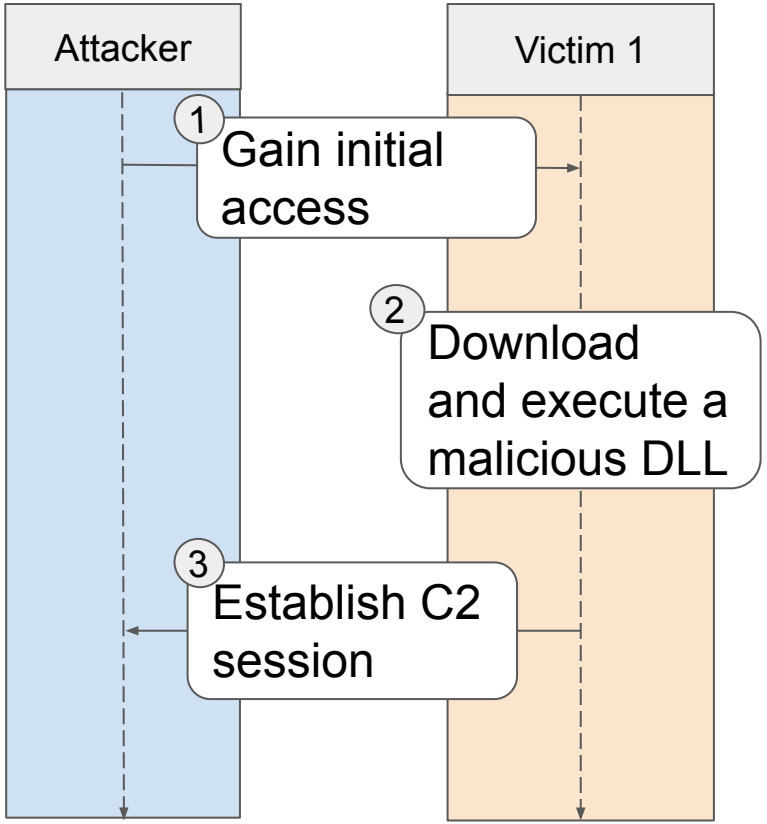
Step	Title	Category/Technique	Description	Explanation
1	Access victim using SSH	Initial Access T1190	Exploit Public-Facing Application	Sandworm identifies a vulnerability in an open source tool, Weirdingway.
		Credential Access T1110.001	Brute Force (Password Guessing)	Use password guessing to access by SSH
2	Deploy P.A.S webshell	Lateral Movement T1021.004	Remote Services (SSH)	Log into the host via SSH and deploy the PAS webshell.
3	Download and execute Exaramel	Persistence T1505.003	Server Software Component (Web Shell)	Download Exaramel using webshell.
		Privilege Escalation T1548.001	Abuse Elecation Control Mechanism (Setuid and Setgid)	Make Exaramel executable by escalating privilege.

Step	Title	Category/Technique	Description	Explanation
4	Set Exaramel persistence	Persistence T1053.003	Scheduled Task/Job (Cron)	Ensure continuous execution of Exaramel.
		Persistence T1543.002	Create or Modify System Process (Systemd Service)	Ensure continuous execution of Exaramel.
5	Gain credentials	Persistence T1505.003	Server Software Component (Web Shell)	Execute commands using webshell.
		Discovery T1083	File and Directory Discovery	Obtain credential to Gammu host.
6	Upload and execute Exaramel dropper	Lateral Movement T1021.002	Remote Services (SMB/Windows Admin Shares)	Use acquired credential to interact with SMB channel.
		Lateral Movement T1570	Lateral Tool Transfer	Upload through SMB channel to lateral host.

Step	Title	Category/Technique	Description	Explanation
7	Load the registry hive and log into lateral host	Lateral Movement T1021.002	Remote Services (SMB/Windows Admin Shares)	Load registry hive of current user to lateral host.
		Lateral Movement T1021.001	Remote Services (Remote Desktop Protocol)	Log into the Gammu host using RDP session.
8	Download and execute Exaramel	Persistence T1547.014	Boot or Logon Autostart Execution (Active Setup)	Install Exaramel when the user logs in.
		Defense Evasion T1218.011	System Binary Proxy Execution (Rundll32)	Execute Exaramel.
9	Gain credentials	Command and Control T1105	Ingress Tool Transfer	Upload credential dumper through Exaramel C2 channel.
		Collection T1119	Automated Collection	Collect credential of all the users.
		Exfiltration T1041	Exfiltration Over C2 Channel	Exfiltrate the credential through Exaramel C2 channel.
		Defense Evasion T1070	Indicator Removal	Cleanup artifacts.

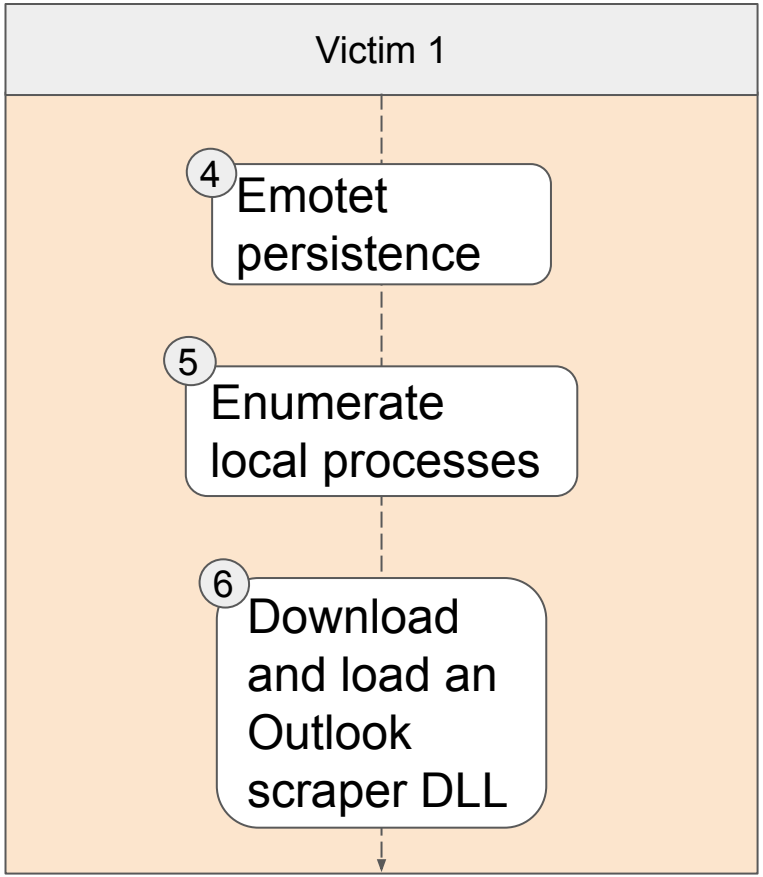
Step	Title	Category/Technique	Description	Explanation
10	Enumerate all domains	Discovery T1482	Domain Trust Discovery	Find Domain Controller.
11	Deploy NotPetya	Lateral Movement T1021.001	Remote Services (Remote Desktop Protocol)	Log into Domain Controller using RDP session.
		Command and Control T1105	Ingress Tool Transfer	Upload NotPetya over RDP channel .
12	Execute NotPetya	Defense Evasion T1218.011	System Binary Proxy Execution (Rundll32)	Execute NotPetya.

Wizard_spider



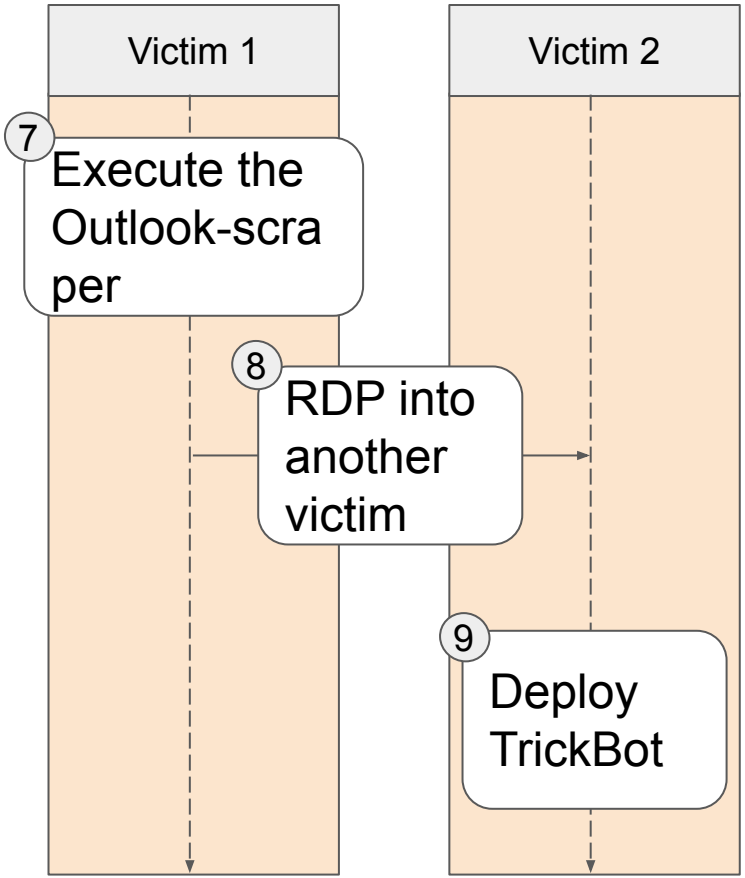
Steps	Detailed process
Gain initial access	Send a phishing mail to victim, which include a malware “Emotet” masquerading as a benign word document.
Download and execute a malicious DLL	The word document contains obfuscated VBA macros that downloads and executes a malicious DLL.
Establish C2 session	The malicious DLL establishes a C2 session with the adversary control server. Note that the malicious DLL is based on Emotet.

Wizard_spider



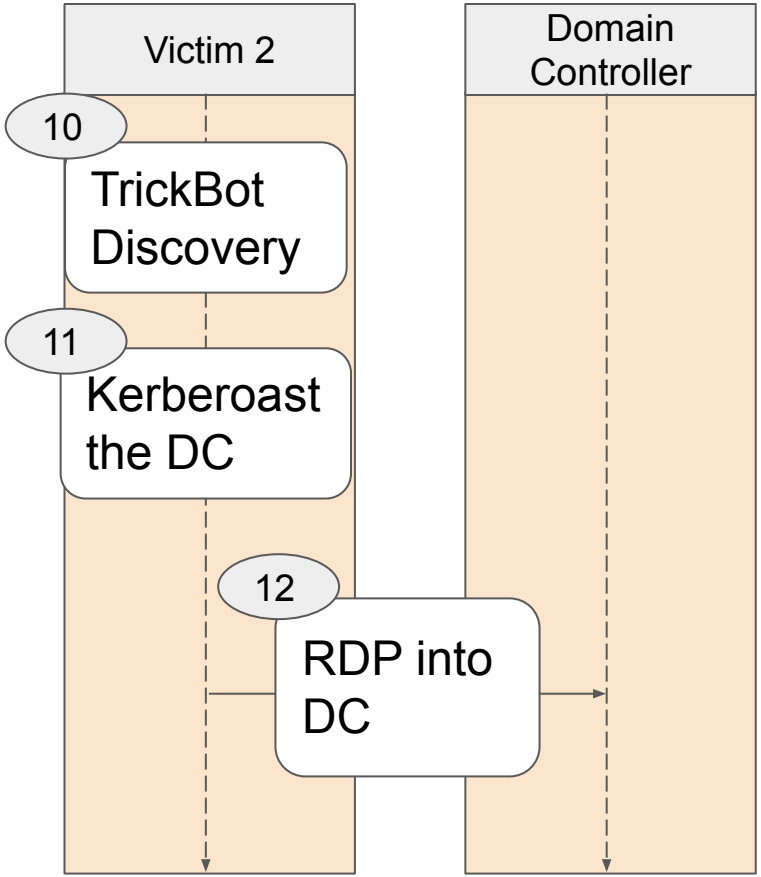
Steps	Detailed process
Emotet persistence	Establish registry persistence by adding the registry key. The registry key is written using the RegSetValueExA WinAPI function.
Enumerate local processes	Enumerate local processes using WinAPI functions: CreateToolhelp32Snapshot and Process32First.
Download and load an Outlook scraper DLL	Download and load an Outlook scraper DLL using the LoadLibraryW and GetProcAddress functions.

Wizard_spider



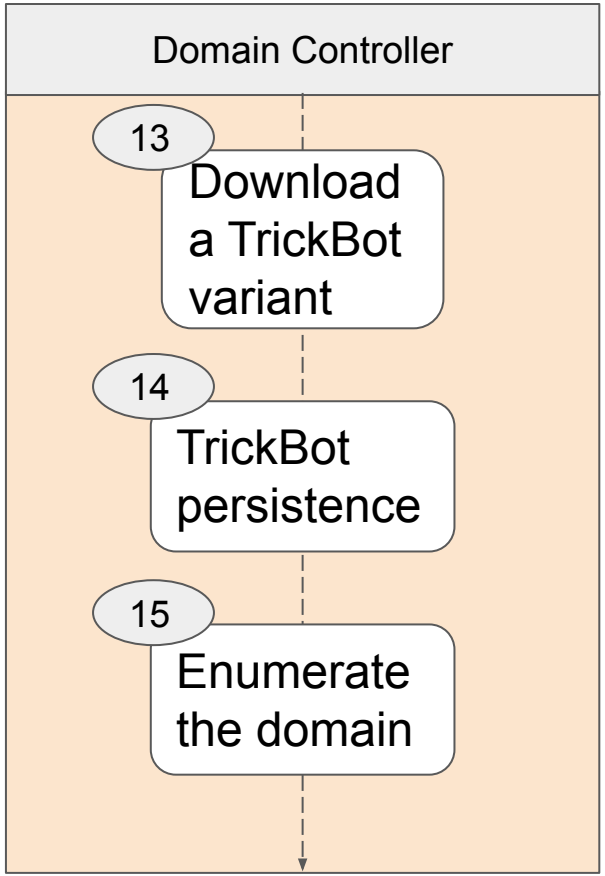
Steps	Detailed process
Execute the Outlook-scraper	Execute the Outlook-scraper to dump emails and contacts. One of the emails contains credentials for another user, which will be used in the next step.
RDP into another victim	Use the credentials gained from the last step to RDP into victim2
Deploy TrickBot	Upload and execute a malicious EXE based on TrickBot. Trickbot is uploaded to target using an RDP-mounted network share. Once executed, Trickbot calls back to the C2 server over HTTP.

Wizard_spider



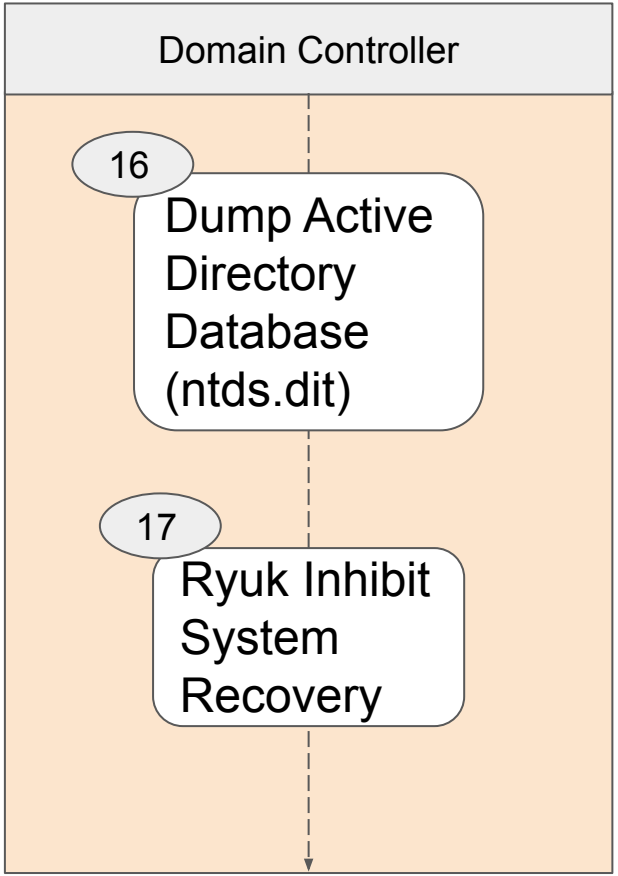
Steps	Detailed process
TrickBot Discovery	Use TrickBot to perform detailed system discovery. We can see TrickBot executing shell commands. Trickbot executes commands via the C standard library function, system().
Kerberoast the DC(Domain Controller)	Perform Kerberoasting using a public tool, Rubeus. Through Kerberoasting, we can obtain encrypted credentials for the domain admin. Crack the credentials offline for after usage.
RDP into DC	Lateral Movement to Domain Controller.

Wizard_spider



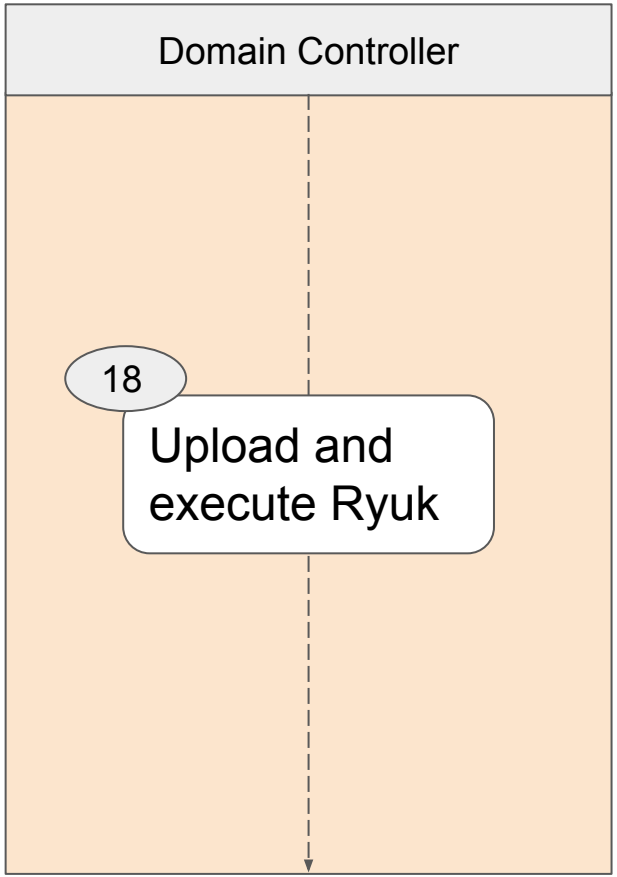
Steps	Detailed process
Download a TrickBot variant	Dowload a TrickBot variant to the DC using PowerShell's Invoke-WebRequest command.
TrickBot persistence	Establishe registry persistence to execute Trickbot when user logs in.
Enumerate the domain	Enumerate the domain using the adfind utility.

Wizard_spider



Steps	Detailed process
Dump Active Directory Database (ntds.dit)	Create a volume shadow copy to collect the active directory database (**ntds.dit**). Use vssadmin to create the shadow copy. Exfiltrate the shadow copy files using an RDP-mounted network share.
Ryuk Inhibit System Recovery	Mount the C$ share of victim2 on DC. Upload two files to disk: **kill.bat** and **window.bat**. These files are used to stop specific services and delete backups prior to encrypting the system.

Wizard_spider



Steps	Detailed process
Upload and execute Ryuk	Upload: RDP-mounted network share Execute: CMD Ryuk will first gain SeDebugPrivilege. Then, inject its own executable into a remote process, notepad.exe, via WriteProcessMemory and CreateRemoteThread WinAPI calls. From the remote process, Ryuk will encrypt files on DC recursively. Next, Ryuk encrypts files on victim2 at *C$\Users\Public*, which is mounted on DC as Z:

Step	Title	Category/Technique	Description	Explanation
1	Gain initial access	Execution T1204.002	User Execution (Malicious File)	Rely user to open the Word doc to enable the macro.
		Execution T1059.005	Command and Scripting Interpreter (Visual Basic)	The VB script is embedded into the Word doc.
2	Download and execute a malicious DLL	Command and Control T1105	Ingress Tool Transfer	Download Emotet.
		Defense Evasion T1027	Obfuscated Files or information	Make the VBA macros hidden in Word doc hard to be discovered.
		Execution T1047	Windows Management Instrumentation	Abuse WMI to execute Rundll32.
		Defense Evasion T1218.011	System Binary Proxy Execution (Rundll32)	Abuse rundll32.exe to proxy execution of Emotet.

Step	Title	Category/Technique	Description	Explanation
3	Establish C2 session	Command and Control T1071.001	Application Layer Protocol (Web Protocols)	Establish C2 connection with the adversary control server.
		Command and Control T1573.001	Encrypted Channel (Symmetric Cryptography)	Use AES to encrypt the channel with symmetric key.
4	Emotet persistence	Privilege Escalation T1547.001	Boot or Logon Autostart Execution (Registry Run Keys/Startup Folder)	Use Emotet to modify a registry key using a WinAPI function to gain persistence.
5	Enumerate local processes	Discovery T1082	System Information Discovery	Enumerate local process.
		Discovery T1057	Process Discovery	Enumerate local process.
6	Download Outlook scraper DLL	Command and Control T1105	Ingress Tool Transfer	Download an Outlook scraper DLL using Win API functions.

Step	Title	Category/Technique	Description	Explanation
7	Execute the Outlook scraper	Credential Access T1552	Unsecured Credentials	Search for credentials that is not saved securely.
		Collection T1114.001	Email Collection (Local Email Collection)	Collect emails and contacts from the client, including credentials from another user.
8	RDP into another victim	Lateral Movement T1021.001	Remote Services (Remote Desktop Protocol)	RDP into the Toto host.
9	Deploy TrickBot	Command and Control T1105	Ingress Tool Transfer	Upload TrickBot to the Toto host using an RDP-mounted network share.
		Command and Control T1071.001	Application Layer Protocol (Web Protocols)	TrickBot calls back to the C2 server over HTTP.
		Command and Control T1071.001	Non-Standard Port	Use non-standard port to establish HTTP connection.

Step	Title	Category/Technique	Description	Explanation
10	TrickBot Discovery	Initial Access T1078.002	Valid Accounts (Domain Accounts)	Collect credentials of a domain account.
		Discovery T1082	System Information Discovery	Collect information from the victim.
		Discovery T1007	System Service Discovery	Collect information from the victim.
		Discovery T1087.001, T1087.002	Account Discovery (Local Account) (Domain Account)	Collect information from the victim.
		Discovery T1016	System Network Configuration and settings	Collect information from the victim.
		Discovery T1049	System Network Connections Discovery	Collect information from the victim.
		Discovery T1482	Domain in Trust Discovery	Collect information from the victim.
		Discovery T1069	Permission Groups Discovery	Collect information from the victim.

Step	Title	Category/Technique	Description	Explanation
11	Kerberoast the DC	Command and Control T1105	Ingress Tool Transfer	Download Rubeus in the victim host.
		Credential Access T1558.003	Steal or Forge Kerberos Tickets (Kerberoasting)	Obtain encrypted credentials for the domain admin.
12	RDP into DC	Lateral Movement T1021.001	Remote Services (Remote Desktop Protocol)	RDP into Domain Controller.
13	Download a TrickBot variant	Command and Control T1105	Ingress Tool Transfer	Download TrickBot variant in DC.
14	TrickBot persistence	Privilege Escalation T1547.004	Boot or Logon Autostart Execution (Winlogon Helper DLL)	Install a registry key to execute TrickBot when the user logs in.
15	Enumerate the domain	Discovery T1069.002	Permission Groups Discovery (Domain Groups)	Enumerate the domain and map the network

Step	Title	Category/Technique	Description	Explanation
16	Dump Active Directory Database	Credential Access T1003.002	OS credential Dumping (Security Account Manager)	Create a volume shadow copy to collect the active directory database.
		Credential Access T1003.003	OS credential Dumping (NTDS)	Create a volume shadow copy to collect the active directory database.
17	Ryuk Inhibit System Recovery	Defense Evasion T1222.001	Windows File and Directory Permissions Modification	Ryuk will launch icacls command to delete access-based restrictions on files and directories
		Command and Control T1105	Ingress Tool Transfer	Uploads two files that stop specific services.
		Impact T1489	Service Stop	Use these two files to stop specific services.
		Impact T1490	Inhibit System Recovery	Delete backups.

Step	Title	Category/Technique	Description	Explanation
18	Upload and execute Ryuk	Command and Control T1105	Ingress Tool Transfer	Deploy Ryuk ransomware to the Toto host.
		Defense Evasion T1134	Access Token Manipulation	Ryuk will gain SeDebugPrivilege itself.
		Discovery T1057	Process Discovery	Enumerate all running processes.
		Privilege Escalation T1055.002	Process Injection (Portable Executable Injection)	Ryuk will inject notepad.exe via two WinAPI calls.
		Discovery T1083	File and Directory Discovery	Find files to encrypt.
		Impact T1486	Data Encrypted for Impact	Encrypt data to ask for ransom.

Similarities	Differences
Implant backdoor and ensure its connection (C2 channel)with the attacker’s host.	Clickbait user or use zero-day exploit.
Collect credentials.	Whether deleting backups and inhibit victims to do system recovery.
Lateral movement into next victim.(until find DC)	
Execute ransomware.	