Detecting Alternate Authentication Based APT Attack via MITRE Techniques Correlation

Advisor: 謝續平 講座教授
Student: 0612213 曾振豪、0711529 陳冠儒

Outline

- Introduction
- Contribution
- Proposed scheme
- Evaluation
- Conclusion

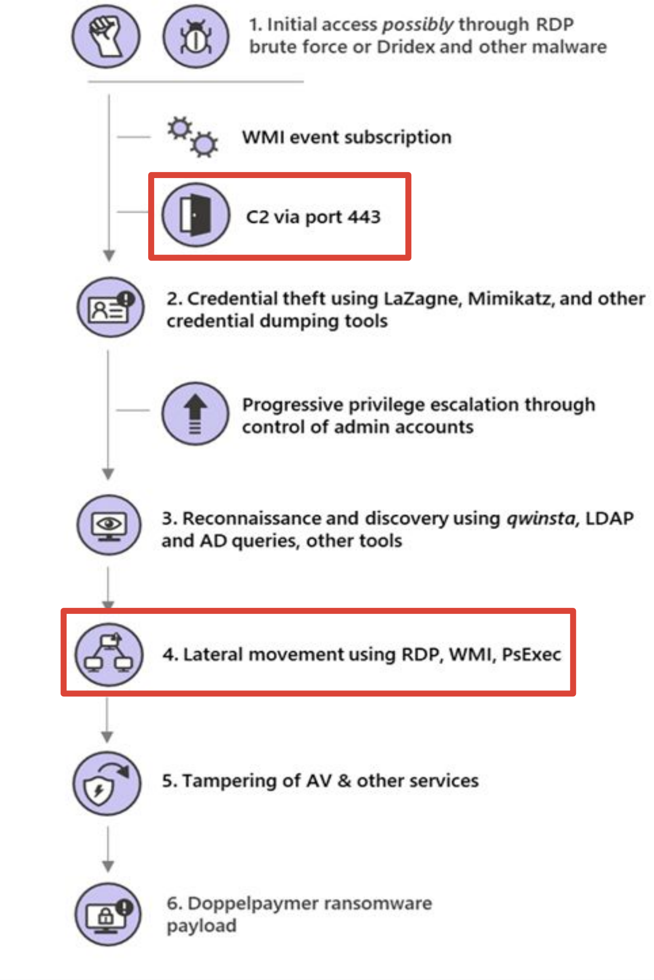
Introduction

APT

- Advanced Persistent Threat (APT) are compound network attacks that utilize multiple stages and different attack techniques.
- In MITRE ATT&CK, they described APT lifecycle as 14 steps.
    - Most attacks include Initial Access, C&C, Lateral Movement, Exfiltration.

Doppelpaymer

- DoppelPaymer is a recent ransomware attack.
- The infection process will also go through many techniques used in the APT attack.
- C&C and Lateral Movement are two of important steps in this process.



1. Initial access *possibly* through RDP brute force or Dridex and other malware

WMI event subscription

C2 via port 443

2. Credential theft using LaZagne, Mimikatz, and other credential dumping tools

Progressive privilege escalation through control of admin accounts

3. Reconnaissance and discovery using *qwinsta*, LDAP and AD queries, other tools

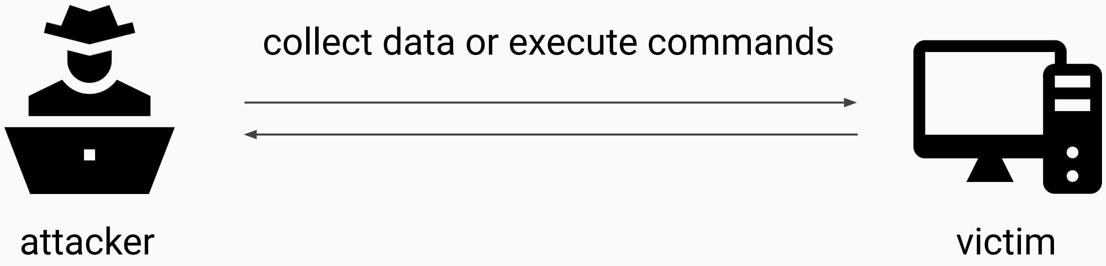
4. Lateral movement using RDP, WMI, PsExec

5. Tampering of AV & other services

6. Doppelpaymer ransomware payload

Command and Control via HTTPS

- The attacker is trying to communicate with compromised systems to control them.
- Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic.



collect data or execute commands

attacker

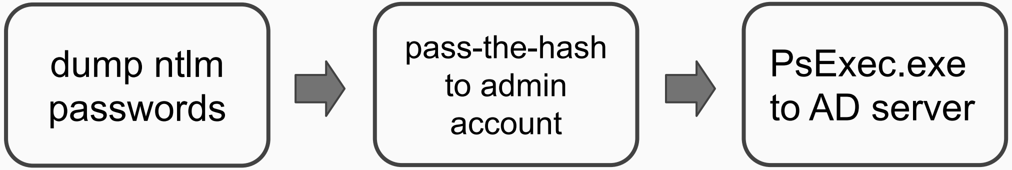
victim

Alternate Authentication

- Alternate authentication materials like password hashes and kerberos tickets are generated for SSO.
- Using alternate authentication materals, attacker can move laterally within target environment without knowing the plaintext password.
- Kerberos is the standard for remote trusted third-party authentication service for the clients and servers.
- Password authentication process:
    - winlogon.exe → accept the user’s input → lsass (Local Security Authority Subsystem Service) → SAM (Security Account Manager)

Pass the hash & Pass the ticket

- Pass the hash

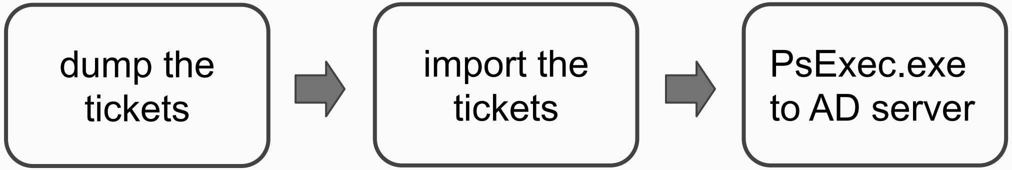


dump ntlm passwords

pass-the-hash to admin account

PsExec.exe to AD server

- Pass the ticket



dump the tickets

import the tickets

PsExec.exe to AD server

Difficulty to Detect C&C and Lateral Movement

- HTTPS-based C&C: Since HTTPS traffic is encrypted and the size is similar to normal network traffic, it’s hard to detect it.
- Pass-the-hash & Pass-the-ticket: It’s hard to distinguish it from normal service logon.

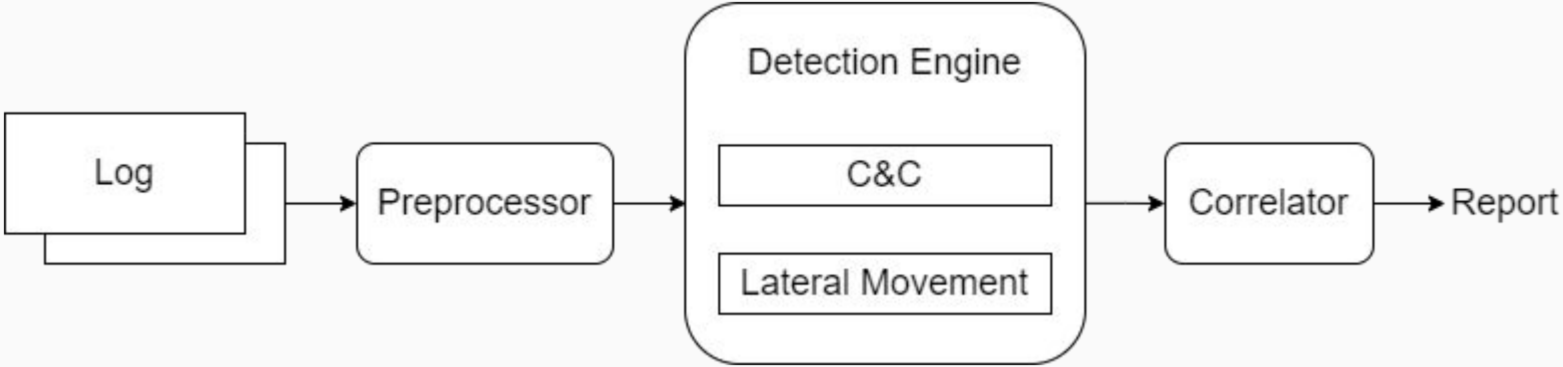
Contribution

Contribution

- Based on the reports and our results on emulation, we have discovered some useful attack features that can detect the attack flow.
- Our system can eventually be installed on the host of school or even enterprise.

Proposed Scheme

System Architecture

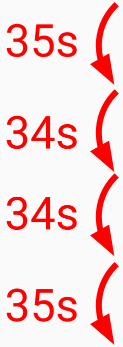


Preprocessor

- For connection logs
  - Use a whitelist to filter out logs with some multicast protocols
  - e.g. SSDP, mDNS, ...
- For Windows event logs
  - Use a whitelist to filter out normal processes which would interact with lsass memory.

C&C Feature

- During our experiment, we found that common C&C tools have a special behavior, that is, making “checkalive” connections frequently and regularly.



35s

34s

34s

35s

Timestamp	Source	Destination
14:40:26.340	<victim_IP>	<attacker_IP>
14:41:01.358	<victim_IP>	<attacker_IP>
14:41:35.289	<victim_IP>	<attacker_IP>
14:42:09.316	<victim_IP>	<attacker_IP>
14:42:44.252	<victim_IP>	<attacker_IP>

⋮

C&C Detection

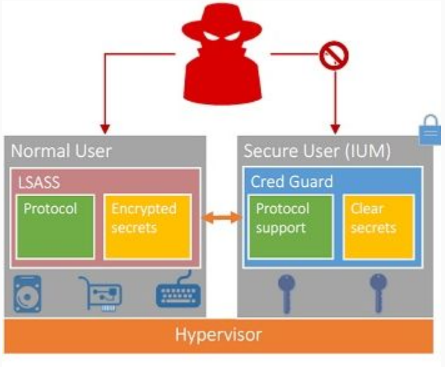
1. Calculate the time intervals of connections established to the same (IP, port).
2. Remove the outlier intervals with Z-score > 2.5 (e.g. time intervals caused by C&C control traffic).
3. Filter out the group of connections with the variance of time intervals <= 1 and # of connections >= 3.

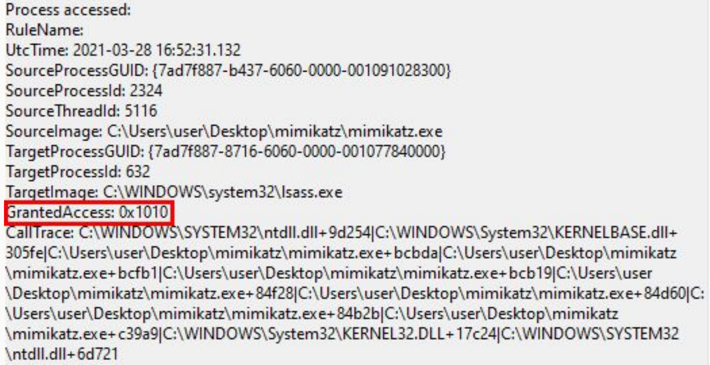
Lateral Movement Feature

- We can find the feature in the following place
    - Dumping the credentials from lsass
    - User logon with different credentials
    - Kerberos tickets request process

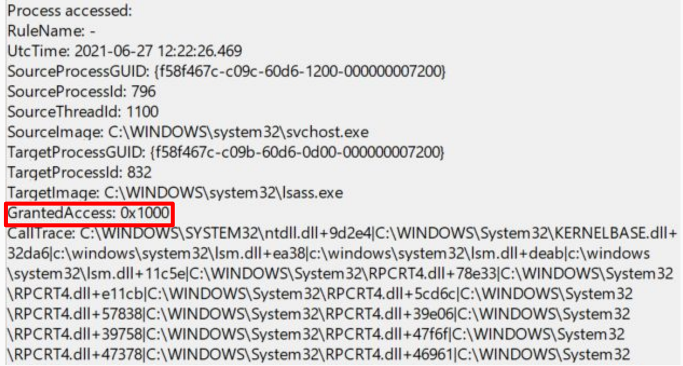
Dumping the credentials from lsass

- EID 10 (Process Access)
  - TargetImage: lsass.exe
  - GrantedAccess(process-specific access rights): 0x1010, 0x1038
    - 0x1000 : PROCESS_QUERY_LIMITED_INFORMATION
    - 0x0010 : PROCESS_VM_READ
    - 0x0020 : PROCESS_VM_WRITE
    - 0x0008 : PROCESS_VM_OPERATION





```
Process accessed:
RuleName:
UtcTime: 2021-03-28 16:52:31.132
SourceProcessGUID: {7ad7f887-b437-6060-0000-001091028300}
SourceProcessId: 2324
SourceThreadId: 5116
SourceImage: C:\Users\user\Desktop\mimikatz\mimikatz.exe
TargetProcessGUID: {7ad7f887-8716-6060-0000-001077840000}
TargetProcessId: 632
TargetImage: C:\WINDOWS\system32\lsass.exe
GrantedAccess: 0x1010
CallTrace: C:\WINDOWS\SYSTEM32\ntdll.dll+9d254|C:\WINDOWS\System32\KERNELBASE.dll+
305fe|C:\Users\user\Desktop\mimikatz\mimikatz.exe+bcbda|C:\Users\user\Desktop\mimikatz
\mimikatz.exe+bcfb1|C:\Users\user\Desktop\mimikatz\mimikatz.exe+bcb19|C:\Users\user
\Desktop\mimikatz\mimikatz.exe+84f28|C:\Users\user\Desktop\mimikatz\mimikatz.exe+84d60|C:
\Users\user\Desktop\mimikatz\mimikatz.exe+84b2b|C:\Users\user\Desktop\mimikatz
\mimikatz.exe+c39a9|C:\WINDOWS\System32\KERNEL32.DLL+17c24|C:\WINDOWS\SYSTEM32
\ntdll.dll+6d721
```

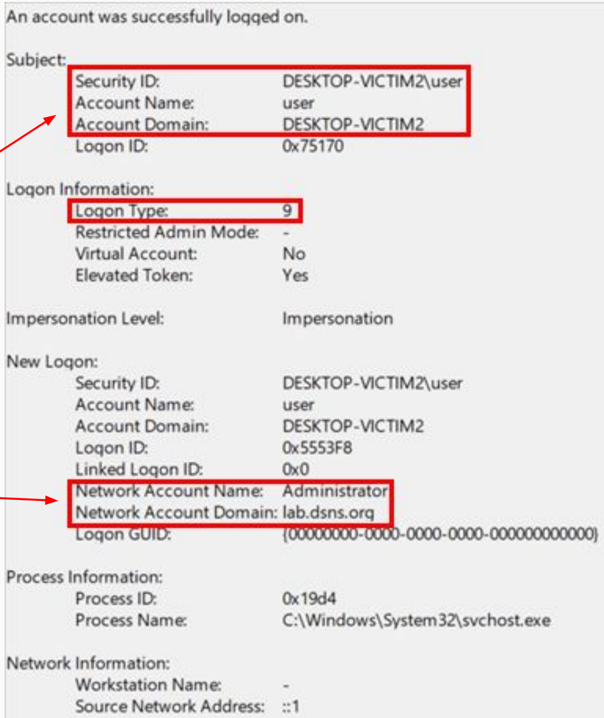


```
Process accessed:
RuleName: -
UtcTime: 2021-06-27 12:22:26.469
SourceProcessGUID: {f58f467c-c09c-60d6-1200-000000007200}
SourceProcessId: 796
SourceThreadId: 1100
SourceImage: C:\WINDOWS\system32\svchost.exe
TargetProcessGUID: {f58f467c-c09b-60d6-0d00-000000007200}
TargetProcessId: 832
TargetImage: C:\WINDOWS\system32\lsass.exe
GrantedAccess: 0x1000
CallTrace: C:\WINDOWS\SYSTEM32\ntdll.dll+9d2e4|C:\WINDOWS\System32\KERNELBASE.dll+
32da6|c:\windows\system32\lsm.dll+ea38|c:\windows\system32\lsm.dll+deab|c:\windows
\system32\lsm.dll+11c5e|C:\WINDOWS\System32\RPCRT4.dll+78e33|C:\WINDOWS\System32
\RPCRT4.dll+e11cb|C:\WINDOWS\System32\RPCRT4.dll+5cd6c|C:\WINDOWS\System32
\RPCRT4.dll+57838|C:\WINDOWS\System32\RPCRT4.dll+39e06|C:\WINDOWS\System32
\RPCRT4.dll+39758|C:\WINDOWS\System32\RPCRT4.dll+47f6f|C:\WINDOWS\System32
\RPCRT4.dll+47378|C:\WINDOWS\System32\RPCRT4.dll+46961|C:\WINDOWS\System32
```

User logon with different credentials

- EID 4624 (An account was successfully logged on)
  - Every successful attempt to logon to the local computer
  - Logon type 9 NewCredentials
    - The same local identify
    - Uses different credentials for other network connections.

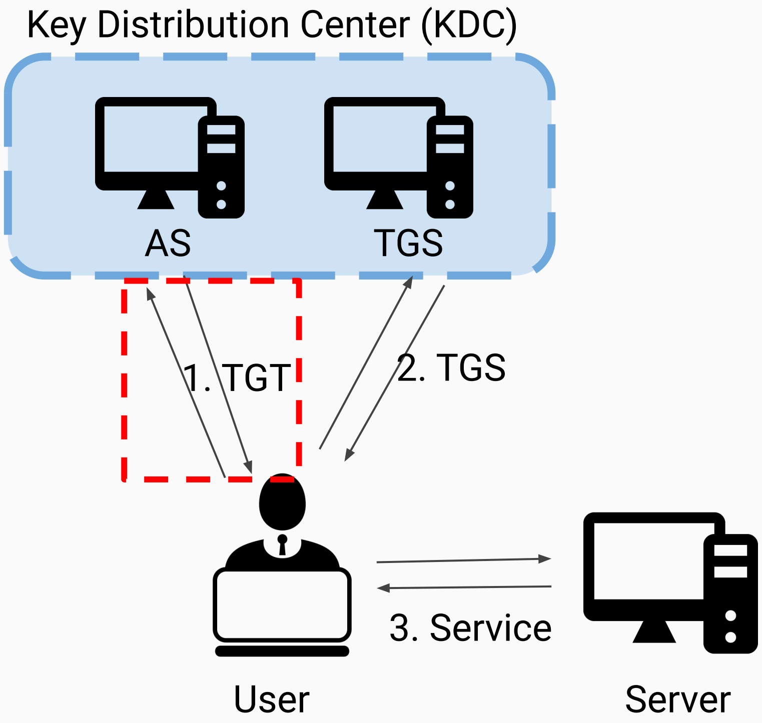
```
powershell> runas /netonly /user:<domain>\<account name> cmd
```



```
An account was successfully logged on.

Subject:
        Security ID:                DESKTOP-VICTIM2\user
        Account Name:               user
        Account Domain:             DESKTOP-VICTIM2
        Logon ID:                   0x75170

Logon Information:
        Logon Type:                 9
        Restricted Admin Mode:      -
        Virtual Account:            No
        Elevated Token:             Yes

Impersonation Level:                Impersonation

New Logon:
        Security ID:                DESKTOP-VICTIM2\user
        Account Name:               user
        Account Domain:             DESKTOP-VICTIM2
        Logon ID:                   0x5553F8
        Linked Logon ID:            0x0
        Network Account Name:       Administrator
        Network Account Domain:     lab.dsns.org
        Logon GUID:                 {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:                 0x19d4
        Process Name:               C:\Windows\System32\svchost.exe

Network Information:
        Workstation Name:           -
        Source Network Address:     ::1
```

Kerberos tickets request process

- Step 1: EID 4768 A Kerberos authentication ticket (TGT) was requested.
- Step 2: EID 4769 A Kerberos service ticket was requested.
- Pass the ticket: The attacker want to stolen the TGT ticket, so only EID 4769 will appear, EID 4768 won't appear.



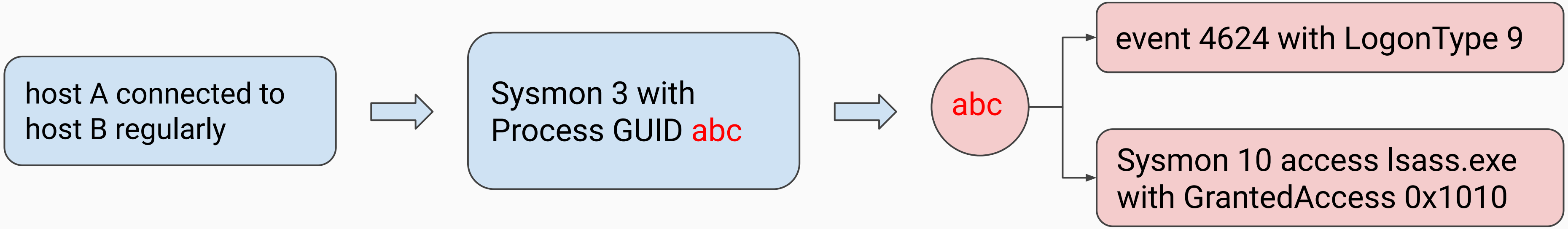
Alternative Authentication Detection

1. Collect logs of the attack we emulated with event id 1, 3, 10, 4624, 4768 and 4769.
2. Remove logs of lsass.exe which are in the whitelist.
3. Group each log based on ParentProcessGuid and ProcessGuid to build a log flow diagram.
4. If the the group of logs have
    a. EID10 grantedaccess 0x1010 and logontype 9, it may be pass the hash
    b. EID10 grantedaccess 0x1010 and no EID4768 but have EID 4769, it may be pass the ticket

Correlation

- If we try to detect C&C and lateral movement separately, there are some false positives captured by our detector.
    - e.g. services.exe connects to Microsoft regularly
- In our implementation, C&C and lateral movement are correlated by Sysmon 3 event (Network Connection).

Correlation (cont.)



host A connected to host B regularly

Sysmon 3 with Process GUID abc

abc

event 4624 with LogonType 9

Sysmon 10 access lsass.exe with GrantedAccess 0x1010

C&C detection

Network connection log on host A

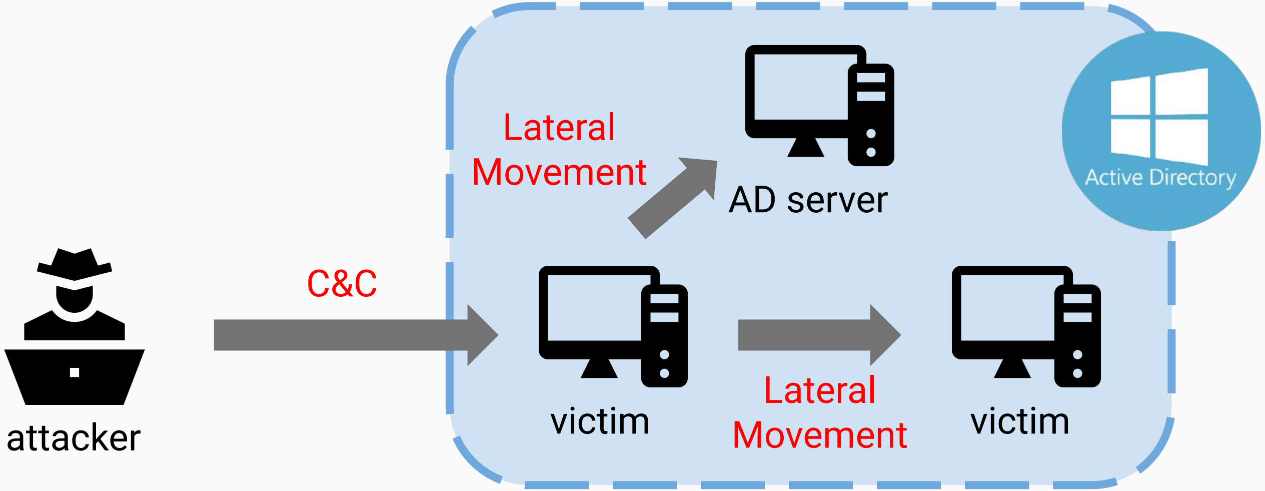
Lateral movement detection

Evaluation

- Attack Simulation Scenario
- Attack Tools
- C&C Detection Accuracy
- Lateral Movement Detection Accuracy
- Correlation Result

Attack Simulation Scenario

1. First, attacker controls one victim computer
2. Move laterally to other machines
3. Move to AD server to get the access of domain administrator



Attack Tools

- According to DoppelPaymer’s attack chain, it uses HTTPS C&C channel.
  - We choose Merlin to implement the attack.
  - Merlin is a C&C tool with HTTPS supported.
- DoppelPaymer uses Mimikatz and PsExec to perform lateral movement.
  - We use the same tools.
  - Use Mimikatz to dump hashes and tickets.
  - Use PsExec to login other computers.

Log Collection

Windows Event Log

- 795 log entries on a computer during 1 hour
- Only collect Windows event 1, 3, 10 and 4624

Network Traffic Collected by Zeek

- 2690 connections during 1 hour
- 151 of them are malicious connections

elastic stack

C&C Detection Accuracy

		Predicted	
		Normal	Malicious
Actual	Normal	2334	205
	Malicious	0	151

precision	recall	f1-score	accuracy
0.42	1	0.6	0.92

Confusion matrix and classification performance

Lateral Movement Detection Accuracy

- Can’t detect the attack via cracking password hashes

Predicted

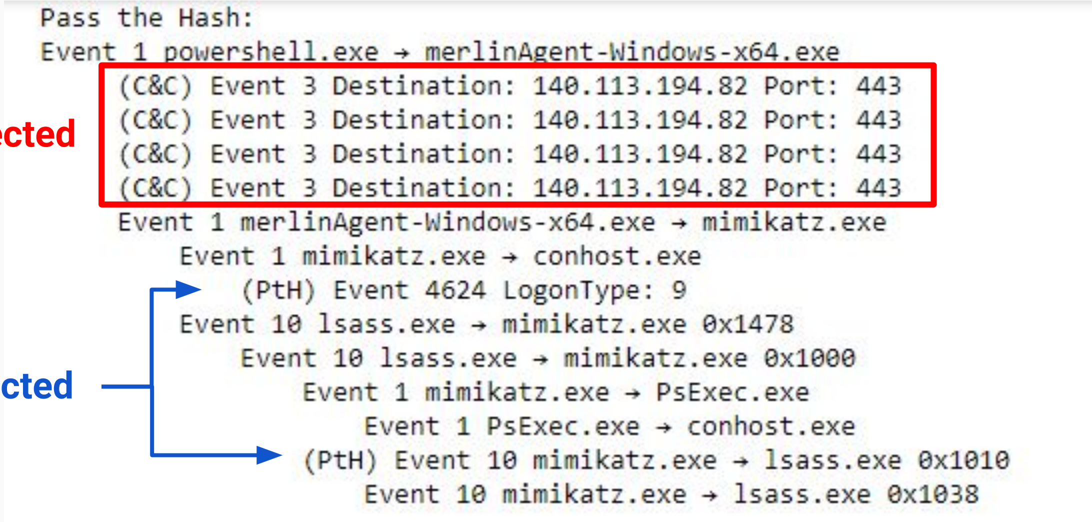
		Normal	Malicious
Actual	Normal	741	0
	Malicious	0	54

precision	recall	f1-score	accuracy
1	1	1	1

Confusion matrix and classification performance

Correlation Result

- Correlate two attack steps by Sysmon event 3



```
Pass the Hash:
Event 1 powershell.exe → merlinAgent-Windows-x64.exe
    (C&C) Event 3 Destination: 140.113.194.82 Port: 443
    (C&C) Event 3 Destination: 140.113.194.82 Port: 443
    (C&C) Event 3 Destination: 140.113.194.82 Port: 443
    (C&C) Event 3 Destination: 140.113.194.82 Port: 443
    Event 1 merlinAgent-Windows-x64.exe → mimikatz.exe
        Event 1 mimikatz.exe → conhost.exe
            (PtH) Event 4624 LogonType: 9
        Event 10 lsass.exe → mimikatz.exe 0x1478
            Event 10 lsass.exe → mimikatz.exe 0x1000
                Event 1 mimikatz.exe → PsExec.exe
                    Event 1 PsExec.exe → conhost.exe
                (PtH) Event 10 mimikatz.exe → lsass.exe 0x1010
                    Event 10 mimikatz.exe → lsass.exe 0x1038
```

C&C detected

Pass-the-Hash detected

Conclusion

Conclusion

- We refer to an important part, https-based C&C and alternate authentication of the latest ransomware Doppelpayer for research and detection.
- Finally, we use the features in network flow and logs to concatenate various behaviors in sequences become groups of logs.
- According to our detection design, we can accurately detect the https-based C&C and Pth/Ptt attacks behavoirs.

Reference

- [1]“MITRE ATT&CK®.” https://attack.mitre.org/ (accessed Jun. 16, 2021).
- [2]“人為勒索軟體攻擊 : 一場可預防的災難 ,” 微軟新聞中心 , Nov. 24, 2020. https://news.microsoft.com/zh-tw/features/threat-protection/ (accessed Jun. 16, 2021).
- [3]“Head Fake: Tackling Disruptive Ransomware Attacks,” FireEye. https://www.fireeye.com/blog/threat-research/2019/10/head-fake-tackling-disruptive-ransomware-attacks.html (accessed Jun. 16, 2021).
- [4]Karl-Bridge-Microsoft, “Process Security and Access Rights - Win32 apps.” https://docs.microsoft.com/en-us/windows/win32/procthread/process-security-and-access-rights (accessed Jun. 16, 2021).
- [5]Andy Green Updated, “Windows 10 Authentication: The End of Pass the Hash?,” Inside Out Security, Sep. 01, 2015. https://www.varonis.com/blog/windows-10-authentication-the-end-of-pass-the-hash/ (accessed Jun. 16, 2021).
- [6]Karl-Bridge-Microsoft, “Windows Events - Win32 apps.” https://docs.microsoft.com/en-us/windows/win32/events/windows-events (accessed Jun. 16, 2021).
- [7]“The Zeek Network Security Monitor,” Zeek. https://zeek.org/ (accessed Jun. 16, 2021).
- [8]“Free and Open Search: The Creators of Elasticsearch, ELK & Kibana | Elastic.” https://www.elastic.co/ (accessed Jun. 16, 2021).
- [9]R. V. Tuyl, Ne0nd0g/merlin. 2021. Accessed: Jun. 16, 2021. [Online]. Available: https://github.com/Ne0nd0g/merlin
- [10]markruss, “PsExec - Windows Sysinternals.” https://docs.microsoft.com/en-us/sysinternals/downloads/psexec (accessed Jun. 16, 2021).
- [11]B. DELPY, gentilkiwi/mimikatz. 2021. Accessed: Jun. 16, 2021. [Online]. Available: https://github.com/gentilkiwi/mimikatz