Detecting Alternate Authentication Based APT Attack via MITRE Techniques Correlation

陳冠儒、曾振豪
指導教授：謝續平

目錄

關鍵字：APT、Alternative Authentication、C&C、Lateral Movement

壹、摘要

常常在新聞上看到「某某企業又被駭客勒索」或是「某某企業重要個資被外洩」，這些其實都是受到了 APT 攻擊。APT 攻擊是什麼呢？他的全名是 Advanced Persistent Threat，是一種針對特定組織的長期且多階段攻擊，而 MITRE 這家最強大的網路安全公司在 2015 時提出一個資安框架，讓這種多階段性的攻擊具有了更一致的標準與描述，目前他總共分成了 14 個步驟，從攻擊前的準備，到入侵，機台間的移動和最後的資料取出、破壞、勒索等等，分成了概括性的 tectics 與詳細方式的 techniques 和 sub-techniques，可以讓我們更能理解攻擊者而進行防禦。

我們這次研究的主題是關於 APT attack 中的 alternate authentication，它可以繞過正常的系統訪問以進行 lateral movement，此外在 lateral movement 前後也會有其他像是 C&C 等攻擊的發生，因此我們為了要 robust 我們的偵測方式，所以將 C&C 與 lateral movement 進行 correlation，試圖能將這種攻擊串的偵測率提高並將 false negative 及 false positive 降到最低。

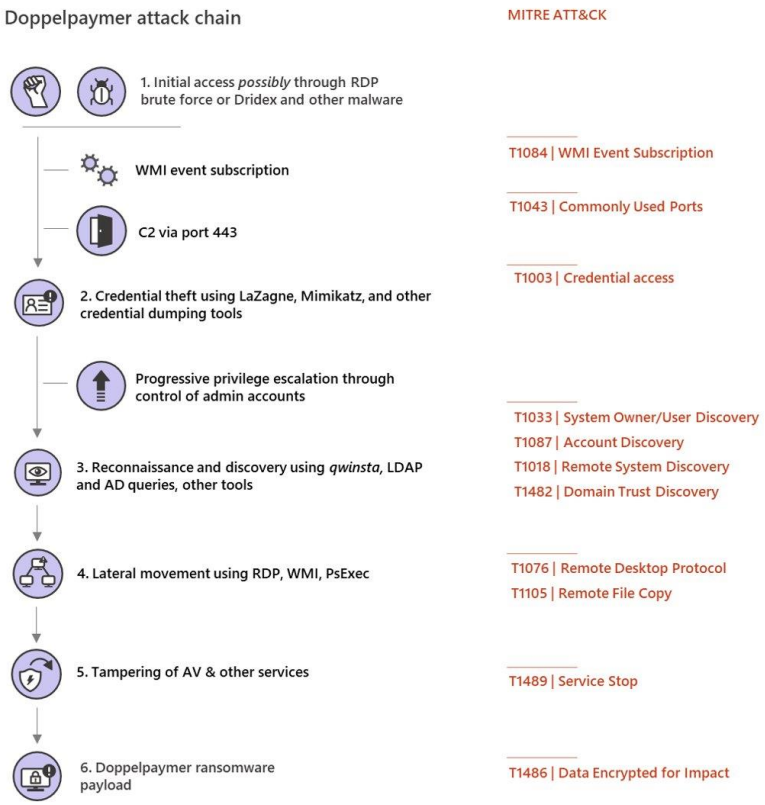
貳、研究動機與研究問題

1、研究動機

隨著科技跟網路的越來越發達，帶給人們許多的便利，卻造成網路犯罪也日趨嚴重，特別是勒索病毒的盛行，常常一波未平一波又起。 在 2017 年出現的「BitPaymer 勒索病毒」透過 Windows 的 iTunes 程式中的 zero-day exploit，可以躲避過各種防毒軟體的偵測，引入惡意程式碼，進而向使用者勒索贖金，對歐美企業產生重大影響。

而近期 2020 年，出現了一套推測從 BitPaymer 衍伸而來的 DoppelPaymer，對醫療、緊急服務與教育等機構進行過數次的攻擊，癱瘓了多次的服務，也是個影響重大的勒索軟體。這些勒索軟體常常被聚焦在他們的贖金及被裝載勒索軟體的資訊上，而忽略了他們長時間的攻擊入侵過程，在這些過程中其實都是有機會去偵測與預防的，因此我們就想從最新的勒索軟體 DoppelPaymer 開始著手，去探討 APT attack 這麼多的 technique 中，哪個環節是相對重要的。

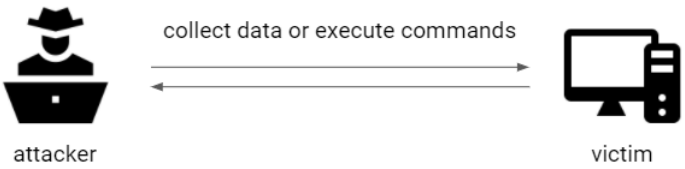
由圖一可以看到 Doppelpaymer 的感染過程會經歷 APT attack 中的許多 tachnique 步驟，像 initial access、C&C、discovery、lateralmovement、impact 等等，其中我們發現 C&C 、 credential access 和 lateral movement 是相當重要的一個環節，因為憑藉著這三個 tachnique，他可以不停地滲透擴散到整個企業系統環境中，讓感染的機器數量大大提升，因此我們最後選擇這個攻擊串來進行研究。



圖一、DoppelPaymer attack chain

2、研究問題

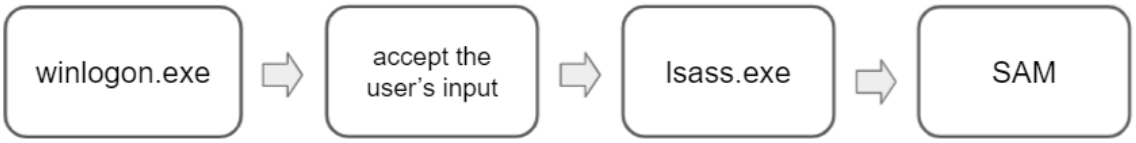
C&C 是一種攻擊者與受感染的系統通信，藉由傳送指令、payload 等方式，控制他們並蒐集資訊。攻擊者可以使用應用層協議進行通信，通過與現有流量混合來避免檢測/網絡過濾。而我們最後選擇了 https，他是一個很常被廣泛使用的 protocol，並且因為他可以加密，所以攻擊者也因此可以藉此將自己的攻擊活動隱藏在其中。



圖二、C&C attack 示意圖

Alternate Authentication attack 是一種 credential dumping 的方式，攻擊者使用替代身份驗證的材料，例如 password hashes、Kerberos tickets 等，以便不用知道明碼就可以在環境中進行 lateral movement。而 Kerberos tickets 是一個受信任的第三方遠程身份驗證服務，可以調解 client 和 server 相互間身份驗證，pash-the-ticket 就是從這個驗證過程中衍生而來的。至於這些 alternate authentication material 是哪來的呢？在用戶成功進行身分驗證後，因為他使用 SSO (single sign-on)，所以會將 host 上的活動用戶憑據存儲，用戶就無需重新輸入 domain 內的服務憑據，但也因此讓攻擊者能夠藉由竊取這些 alternate authentication material，進行 pass-the-ticket 或 pass-the-hash 等攻擊。

接下來我們來看下使用者密碼登入的過程，在 windows 一開機或從休眠喚醒時讓使用者輸入帳密的是 winlogon.exe 這支 process 在處理，他接收到密碼後會傳遞給 lsass.exe 來進行明文轉 hash value 的處理，最後傳給 SAM 這個儲存密碼的 database 來進行核對，因此在 lsass 的 memory 中會留有許多 credential，我們接下來的攻擊就會利用到這點。



圖三、Password authentication process of windows logon

那最常搭配 alternate authentication material 進行的 lateral movement attack 就是 pass-the-ticket 跟 pass-the-hash。Pass-the-hash 會先從 lsass memory 中 dump 出 ntlm hash，利用該 ntlm hash 我們可以作為 compromised-user 進行身份驗證，接著就可以利用 PsExec 將連線到一台主機；Pass-the-ticket 會先從 lsass memory 中 dump 出 Kerberos tickets，將該 tickets 緩存進 memory 中，我們也可以擁有該 compromised-uesr 的權限，而再 PsExec 連線到另一台 host。

圖四、pass-the-hash attack flow(上)，pass-the-ticket attack flow(下)

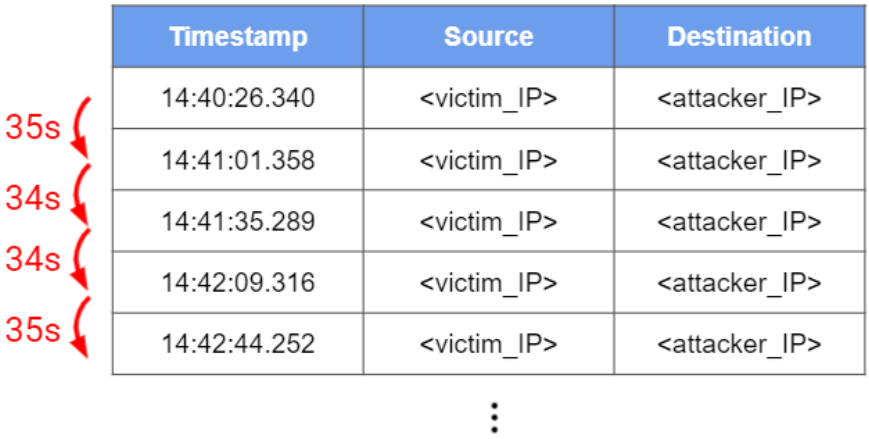
C&C 和 alternate authentication 這些攻擊在偵測方面都有他們困難的地方存在。C&C attack 時網路的流量跟 normal traffic 十分相近，故我們無法透過檢查 packet 內容的方式偵測，而 alternate authentication 他在進行 credential 的操作上，也與 normal service logon 的行為相似，因此若分別單獨看這兩個 attack 而言，都有一定的偵測困難。

參、研究方式與步驟

1.研究方法

1) C&C Feature

在我們的實驗中我們發現 C&C 會有一個很特別的現象「check-alive」，他會在一個固定的頻率下發送 connection 來確保 server 跟 client 之間的連線還存在著。



圖五、C&C checkalive connection 示意圖

2) Lateral Movement Feature

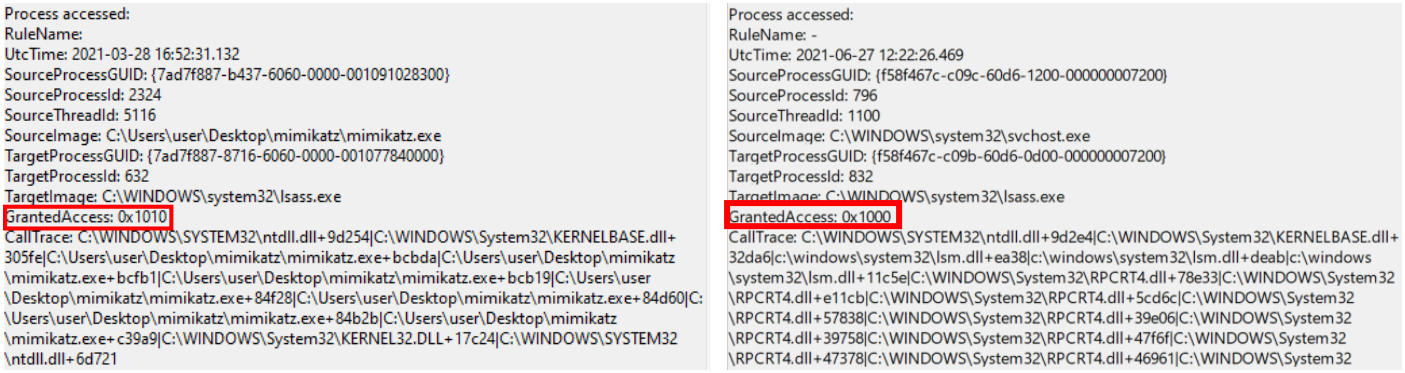
從 pass-the-hash 和 pass-the-ticket 實行過程中的 log 中，我們可以觀察到一些特點，分別是在以下幾個過程中可以發現：

a) Dumping the credentials from lsass

從 lsass.exe 這個程序中提取 credentials 時，會有 event id 10 process access 這個 log 出現，那他特別的地方是在於其中的「GrantedAccess」這項上，正常的與 lsass.exe process 進行交互的 log 這項應該會是 0x1000，但當我們使用 alternate authentication 的手法去取得 lsass.exe 中的 credentials 時，他的 GrantedAccess 會是 0x1010，因為 lsass.exe 使用了類似於 VM (virtual machine)的環境將他與其他 process 給區別了開來，所以我們除了一般的 0x1000 PROCESS_QUERY_LIMITED_INFORMATION 外，還會需要 0x0010 PROCESS_VM_READ 這個權限去讀取他。

Value	Meaning
0x1000	PROCESS_QUERY_LIMITED_INFORMATION
0x0010	PROCESS_VM_READ
0x0020	PROCESS_VM_WRITE
0x0008	PROCESS_VM_OPERATION

表一、rocess-specific access rights

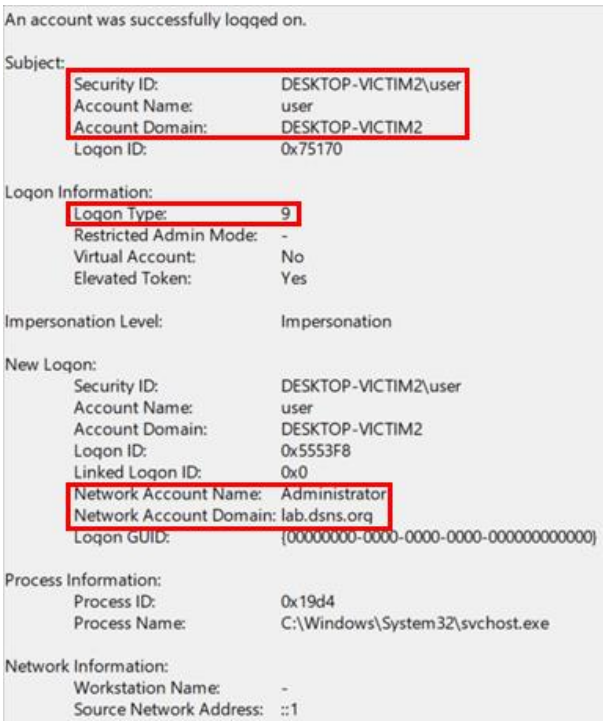


圖六、左為 compromised access lasss.exe 的 event log，右為 normal access lasss.exe 的 event log

b) User logon with different credentials

Event id 4624 An account was successfully logged on 這個 event log 當每次成功的登入到 local computer 時都會出現，但會隨著不同的登入方式而在 LogonType 的地方有所不同。

Pass-the-hash attack 因為使用 compormised-user 的 hash value 登入，所以會出現 LogonType 為 9 的 Event id 4624，這是個蠻罕見的 log，他會有與原先登入帳戶相同的 local identiy，但在 network account 卻是另一個 credential。我們從文獻與實際操作中只有發現當在 powershell 輸入指令 runas /netonly /user:<domain>\<account name> cmd 會有相同的 event log，其他情況下都不會看到，因此算是個十分罕見的特點。

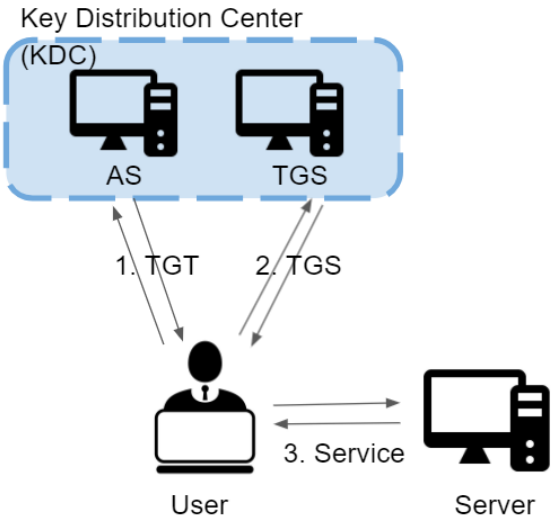


圖七、pass-the-hash 使用 compromised-user hash value 登入的 event id 4624。

c) Kerberos tickets request process

User 透過 Kerberos 來進行認證時，他與 KDC 進行交互請求 tickets 主要會經歷兩個步驟，第一個是跟 KDC 請求 TGT，這時會產生 event id 4768 A Kerberos authentication ticket (TGT) was requested 這個 event log；第二個是向 KDC 請求 TGS ticket，這時會產生 event id 4769 A Kerberos service ticket was requested 這個 evet log。

Pass-the-ticket attack 會利用 alternative authentication attack 取得 compormised-user 的 TGT，因此觀察 log 時只會看到 event id 4769 而不會看到 event id 4768。

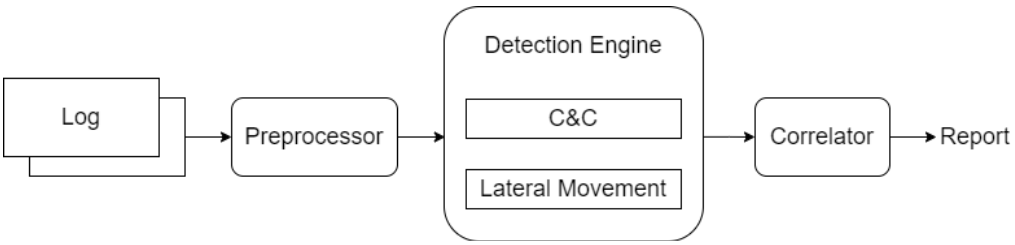


圖八、user 與 kerberos 進行交互請求 tickets

2.研究步驟

1) 系統架構

本研究的系統如圖九所示，首先將收集到的 log 經過前處理 (Preprocessor)，再把這些 log 分別交由 Detection Engine 來鑑定有無 C&C 及 Lateral Movement 的行為，最後由 Correlator 找出這兩個異常行為發生的關聯性並產出偵測報告。



圖九、系統架構示意圖

2) Preprocessor

在前處理階段，我們會使用白名單的方式將已知為正常使用所產生的 log 給過濾掉，避免這些正常使用的 log 在後續的步驟被判定為異常行為。若是針

對網路連線的 log，會將 SSDP、mDNS 等容易被誤判的正常協定流量過濾掉；若是針對 Windows 系統上的 event log，會將平常與 lsass 互動的正常程式過濾掉。

3) C&C Detection

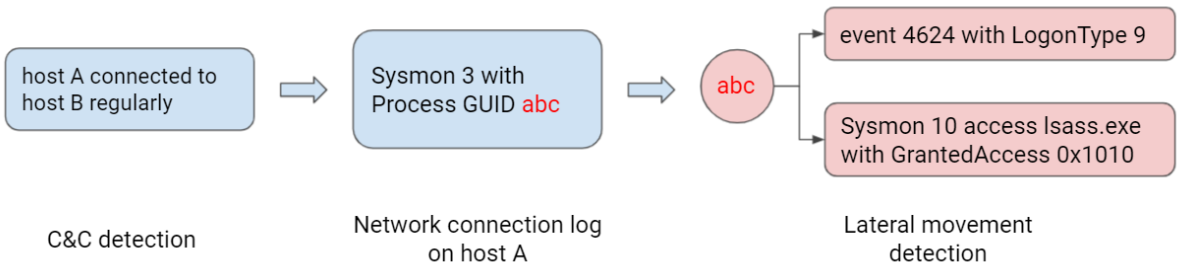
在此階段 Detection Engine 會將相同 source IP、destination IP/port 的連線歸類成同一個連線群組，並在紀錄連線群組內每次連線的時間間隔後剃除掉 Z-score 超過 2.5 的數字，原因是我們在實驗時發現當攻擊者對 C&C agent 下達指令時，check-alive 的連線以及下達指令的連線會被歸類在同個連線群組，導致 C&C feature 較不明顯，因此用 Z-score 來剔除掉下達指令的連線。處理完之後 Detection Engine 會挑出時間間隔的變異數不超過 1 且至少有 3 個連線的連線群組，並認定這些連線群組為異常連線。

4) Alternative Authentication Detection

在此階段 Detection Engine 會將跟 feature 相關的 Windows event 蒐集下來，並且利用 process GUID 將前後有觸發關係的 process 串聯起來，若串聯後的 group 中有 event-ID 10 GrantedAccess 0x1010 和 LogonType 9 出現，那它會被認為是 pass-the-hash 攻擊，而若有 event-ID 10 GrantedAccess 0x1010 和 event-ID 4769 出現且沒有 event-ID 4768 就會被認為是 pass-the-ticket 攻擊。

5) Correlation

會有此階段的原因是我們在實驗的過程中發現如果分別用 C&C 及 Lateral Movement 的 Detector 去偵測所得到的準確率不夠理想，因此我們試圖將兩個 Detector 偵測到的結果找出關聯，這樣一來就能更有信心的去認定這些異常行為其實是一連串的攻擊過程。而實作流程如圖十所示，當 C&C Detector 找到異常連線時，Correlator 會去尋找對應的 Sysmon event-ID 3 log (Network connection)，並透過這筆 log 的 process GUID 去追溯該 process 在建立了可疑連線後是否有被 Lateral Movement 也偵測到的異常行為，若有的話 Correlator 就會認定其為一連串的攻擊行為。



圖十、Correlation 流程

肆、預期結果

綜合以上所述，本計畫擬開發一套基於 alternative authentication 的 APT 攻擊串偵測系統，希望能藉由 log 分析，將 C&C feature 與 lateral movement feature 給串聯在一起，以能更加準確的檢測出攻擊行為。以下為預期完成之工作項目:

1. C&C、alternative authentication attack 文獻探討
3. 攻擊串偵測技術開發
4. 攻擊串實驗 log 及 network flow 資料收集
5. 攻擊串偵測程式測試
6. 系統展示與實驗結果分析
7. 結案報告撰寫

本計畫具體成果在實作出一套的基於 alternative authentication 的 APT 攻擊串偵測系統。該系統判斷 log 及 network flow 資料 ，輸出是否有 C&C 和 lateral movement 攻擊發生，以及是發生在何時、哪兩台電腦間。

總結來說，基於 alternative authentication 的 APT 攻擊串偵測系統利用 logs 和 network flow 等資料，將確實會發生的各種 feature 串聯，以幫助我們偵測這 C&C 和 lateral movement 這兩項攻擊，達到防止勒索軟體攻擊的最終目的。由於偵測時所消耗的資源很小，因此可以很 light weight 的安裝在學校、醫院甚至是企業的系統上協助偵測 C&C 和 lateral movement 攻擊的發生。

伍、實驗結果與分析

1.簡介

1) 環境介紹
    a) victim host
        i) 版本：Win10 Education 20H2
        ii) OS：19042.1237

    b) AD server
        i) 版本：Windows Server 2019 Datacenter Evaluation 1809
        ii) OS：17763.737

2) 工具介紹
    a) Merlin
        i) 版本：1.1.0 windows
        ii) 簡介：an open source C&C tool with HTTPS supported

    b) Mimikatz
        i) 版本：2.2.0 x64
        ii) 簡介：an open source tool for windows credential dumping

    c) PsExec
        i) 版本：2.32
        ii) 簡介：Microsoft tool 可以用來遠程執行 process

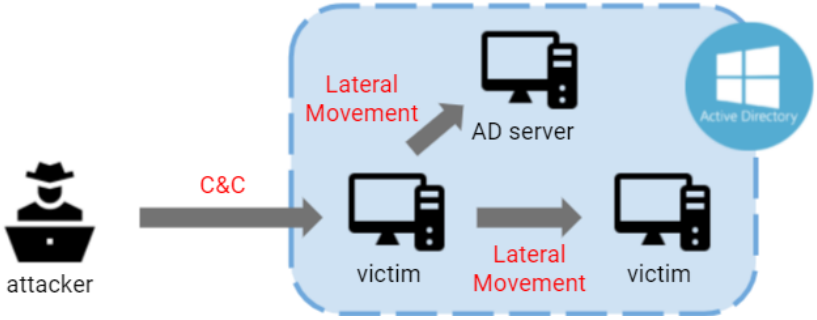
    d) Kibana
        i) 版本：7.10.2

ii) 簡介：用來收集 log 並分析

e) zeek
   i) 版本：4.1.0
   ii) 簡介：取得個電腦的 network flow 資料

2.實驗步驟

1) 攻擊步驟
   a) 首先我們假定 attacker 已經取得了一個 victim computer 的控制權，可以透過 Merlin 使用 C&C 對其下指令。
   b) 利用 victim computer 上的 Mimikatz 來取得 lsass 中的 credential。
   c) 將取得的 compromiesd-user credential 利用 Mimikatz 進行 pass-the-hash 或 pass-the-ticket。
   d) 在 compromised-user 的身分下用 PsExec lateral movement 到其他電腦。



圖十一、攻擊步驟

2) log 與 network flow 資料收集
   a) Windows Event Log
      i) 資料總數：795 log entries a computer per hour
      ii) log 處理：為避免資料太多太亂，因此我們只收集 Windows event-ID 1, 3, 10, 4624, 4768 and 4769 這幾個跟 feature 相關的 log，並傳送至 kibana 以進行後續的分析處理。

   b) Network Traffic Collected by Zeek
      i) 資料總數：2690 connections per hour
      ii) 惡意連線：151 connections per hour
      iii) Network flow 處理：透過 zeek 來蒐集 AD domain 下的所有網路連線傳輸，並傳送至 kibana 以進行後續的處理分析，其中數據又可以分為五大類：conn、dns、http、kerberos、ntlm。

3.實驗結果分析

1) C&C Detection Accuracy

   只單純看 C&C 的偵測結果的話，最終的 accuracy 為 0.92，主要是因為有一些 false positive，可能是因為他 connection 的頻率與我們定的 C&C check-alive 頻率很接近，以至於會誤判為 malicious connection。

Predicted

Actual		Normal	Malicious
	Normal	2334	205
	Malicious	0	151

precision	recall	f1-score	accuracy
0.42	1	0.6	0.92

圖十二、Confusion matrix and classification performance of C&C detection

2) Lateral Movement Detection Accuracy

只單純看 lateral movement 的偵測結果的話，最終的 accuracy 為 1，可能是因為我們的環境太乾淨了。

Predicted

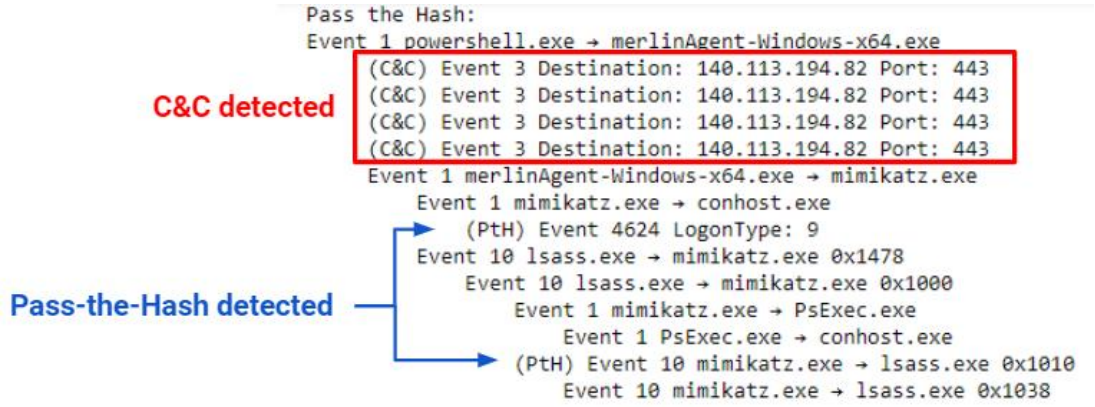
Actual		Normal	Malicious
	Normal	741	0
	Malicious	0	54

precision	recall	f1-score	accuracy
1	1	1	1

圖十三、Confusion matrix and classification performance of lateral movement detection

3) Correlation Result

透過 event-ID 3 將 C&C 和 lateral movement 的偵測結果給串聯起來，可以讓我們的偵測更加的準確，在這裡因為 lateral movement 的 accuracy 成功率是 100%，所以串聯後的結果也會是 100%。



圖十四、Correlation Result

陸、未來研究方向

這個攻擊串主要可以分成三大步驟：C&C、credential dumping、lateral movement，目前都只有針對每一步驟中較單一手法的攻擊來進行偵測，未來希望能夠將更多的途徑給考慮進去，像是不用 mimikatz 而是其他 open source tool 來進行攻擊，以能更廣泛的適應更多種的情況。

柒、參考文獻

[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