勒索初上

除了付贖金，還能做些什麼？

TEAMT5
杜浦數位安全

角色介紹

杜浦數位安全 執行長

蔡松廷

勒索初上

杜浦數位安全 研究員

亞拉岡

勒索初上

Our Team

Persistent Cyber Threat Hunters

- Found in 2017
- Taipei, Taiwan
- Security Experts

TEAMT5

- 300+ IR cases
- 100+ Customers
- 30+ Partners

勒索軟體持續造成鉅額損失

FACT in 2021

- **$6 trillion**: damages from cybercrime (BlackFog)
- **$102.3M** ransomware transactions per month (US Treasury Department)
- **$4.62M** cost of a ransomware breach (IBM)
- **$4.24M** cost of a data breach (IBM)
- **$1.85M** solving a ransomware attack (Sophos)
- Kaseya, Colonial pipeline, Delta Electronics, etc.

Breaches keep happening &
damages keep increasing.

當勒索來臨時?

勒索軟體事件應變

TEAMT5
杜浦數位安全

技術面

隔離感染、控制損害

收集資料、詳細調查

有效復原、持續營運

管理面

損害評估計算

勒索贖金談判

對外關係經營

勒索事件應變 Tips

TEAMT5
杜 浦 數 位 安 全

被勒索後，可以做什麼

TEAMT5 杜浦數位安全

1 快速隔離

- 判定有什麼系統被感染，並且立刻隔離
- 如果有不能斷網的機器，就將其暫時關機
- 暫時透過GPO設定，“Block all connections”，阻擋擴散

2 檢傷分類

- 透過企業持續營運計畫(BCP)進行復原
- 死亡(想辦法復原)，中重症(優先恢復)，輕症(先放著)

3 尋求協助

- 初步了解情況並記錄，聯繫內外部團隊以加快恢復
- 主管機關、司法調查單位、保險機構

4 證據收集

- 針對重點機器(server)進行Memory dump、Image、Log的收集
- 過濾及收集可疑的指令、IP

5 找尋紀錄

- 清查防毒軟體、EDR、IPS等，試圖找到初期攻擊的跡象

被勒索後，可以做什麼

TEAMT5 杜浦數位安全

6 處理一般主機

- 如還沒被加密的與加密到一半的主機(先行斷網)，待釐清勒索軟體的感染流程與移除惡意程式後再行連網
- 使用不同於原始的防毒掃描工具再清查一次
  - Microsoft Safety Scanner*

7 處理DC

- Domain Admin的密碼都改過一遍
- Krbtgt密碼更改兩次(間格十小時)
- 清查Domain Admin及其他高權限Group底下是否有被新增的未知帳號

8 備份還原

- 從離線備份還原資料
- 分階段復原服務，從必要服務到全部恢復
- 剩餘資料備份與系統重建

9 尋找家族

- 透過加密後文件的附檔名與勒索文件，尋找中獎的勒索軟體是哪個家族
- 或許有現成的解密工具(機率低)
- 如果有被發成報告或新聞，可以知道該家族慣用的入侵手法來源

*https://docs.microsoft.com/en-us/microsoft-365/security/intelligence/safety-scanner-download?view=o365-worldwide

司法調查單位、事件處理團隊想要的資料

1. 還原的執行檔 (exe)
2. 被加密的檔案與勒索說明文件 (ransom note)
3. 記憶體傾印檔 (memory dump) 與受感染的硬碟Image
4. 惡意程式樣本
   - 勒索軟體、後門、駭客工具等
5. Log (Windows event log, 防火牆log, Exchange log……)
6. 有在系統執行過的 Powershell script
7. 在入侵時間被新增到 AD 的機器或帳號
8. 勒索細節
   - 攻擊者使用的 email，勒索金額，虛擬貨幣錢包地址，與攻擊者的交涉過程紀錄

如何與事件調查團隊合作

確認受害範圍

- 受害電腦總數、受害網域、受影響服務

重點機器取證(Reg, Log, $MFT……)

- Windows
  - https://github.com/CyberDefenseInstitute/CDIR
  - Exchange IIS log/ mail log
- Linux
  - https://github.com/tclahr/uac

啟用命令列程序稽核

- Event log 4688

防火牆log

流量監控log

TEAMT5
杜 浦 數 位 安 全

清查攻擊者擁有什麼

被竊取的資料

- 尋找近期新增之 zip, tar, rar 等檔案，過濾是否是攻擊者所打包
- 尋查端點是否有建立 tunnel 或是 port forward 的工具
- 尋查 Megatools, dropbox 等雲端應用程式資料夾
  - 有些駭客會不慎留存一些 config 檔案，可以上去看看他們偷了啥

被compromised的帳號

- 透過 event log，確認駭客使用過哪些帳號進行橫向移動或是安裝檔案

用了什麼工具

- 駭客工具 : mimikatz, Rubeus, Impacket, LOLBAS……
- 後門程式 : CobaltStrike, Metasploit, TrickBot……

如果要查，要看什麼呢?

TEAMT5
杜浦數位安全

檢查是否有異常行為

- 大量登入異常Event log (密碼噴灑攻擊)
  - Event log id : 4624, 4625
- 異常之高權限操作行為

檢查是否有新增高權限的帳號或是新被加入domain的機器

- 如有，就可以從帳號或是機器著手回溯源頭

檢查是否有異常的註冊機碼(registry)

- 清除惡意程式persistence的機制

檢查是否有異常的頻寬用量

- 確認從哪台端點發出，以推測是什麼資料遭竊取

檢查是否有安裝異常的應用程式或服務

- PSEXEC、Anydesk

理出攻擊時間線(Timeline)

找出攻擊源頭

強健體魄

Conti leaks

教戰守則(Hacker's quickstart guide)

- IoT devices are a major initial attack surface.
  - Printers, routers, smart firewalls, PLCs
- RDP is recommended as an "initial backdoor.
  - Legitimate services such as VPN and RDP help to achieve an “ideal backdoor”
- Active Directory / Domain Controllers are often the primary target before achieving persistence

預防橫向移動

對於一般主機的防火牆規則設定(Windows Firewall)，阻擋inbound 連線

- SMB (TCP/445, TCP/135, TCP/139)
- 遠端桌面(TCP/3389)
- WinRM/Remote PowerShell (TCP/80, TCP/5985, TCP/5986)
- WMI

考慮評估全域停用WinRM功能

禁用SMB v1

評估在”一般PC”上禁止系統共用

- ADMIN$(預防PsExec), C$, IPC$

防火牆設定

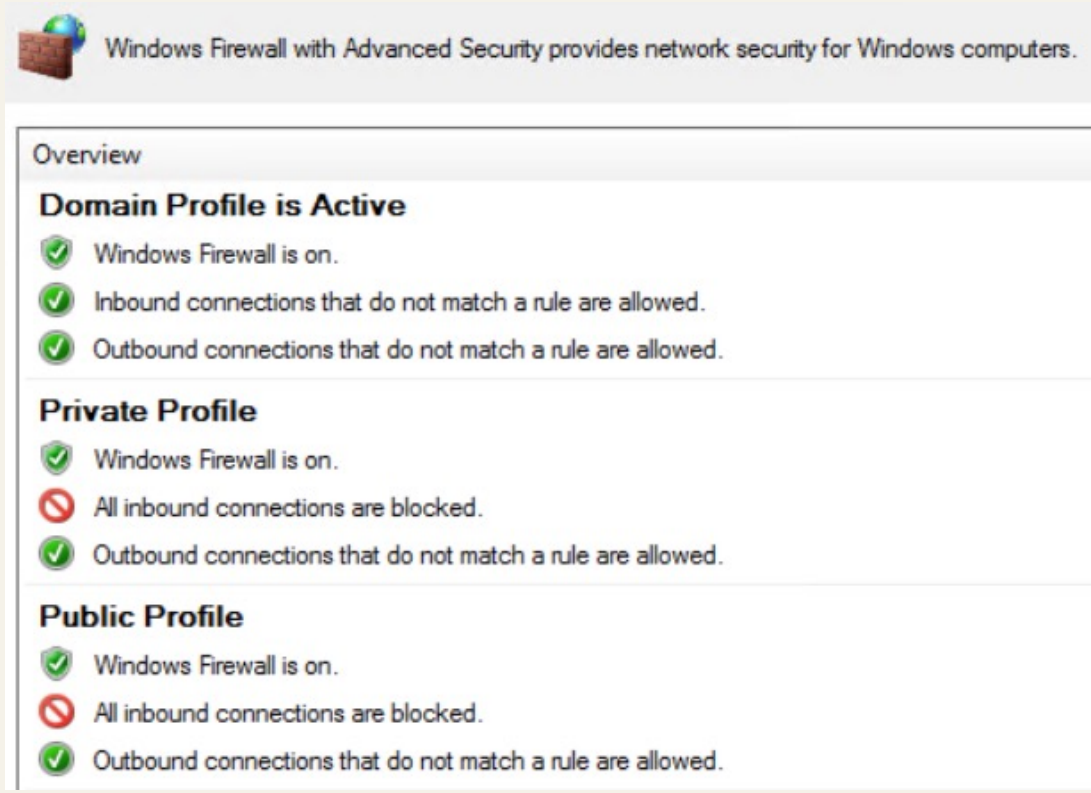
TEAMT5 杜浦數位安全

一般PC或是工作站(server)

- 如果可以，阻擋所有Inbound連線(暴力)，對於需要的(AD, File server或其他應用)開白名單IP
  - 阻擋是針對私人(Private)與公用(Public)設定檔的部分，Domain的話是不阻擋，只有對黑名單的連線進行阻擋
- 如果不行，至少對smb, rdp, WMI, WinRM, powershell阻擋inbound的連線

阻擋常被利用的合法執行檔的對外連線

- powershell.exe
- bitsadmin.exe
- csript.exe
- wscript.exe
- certutil.exe
- …



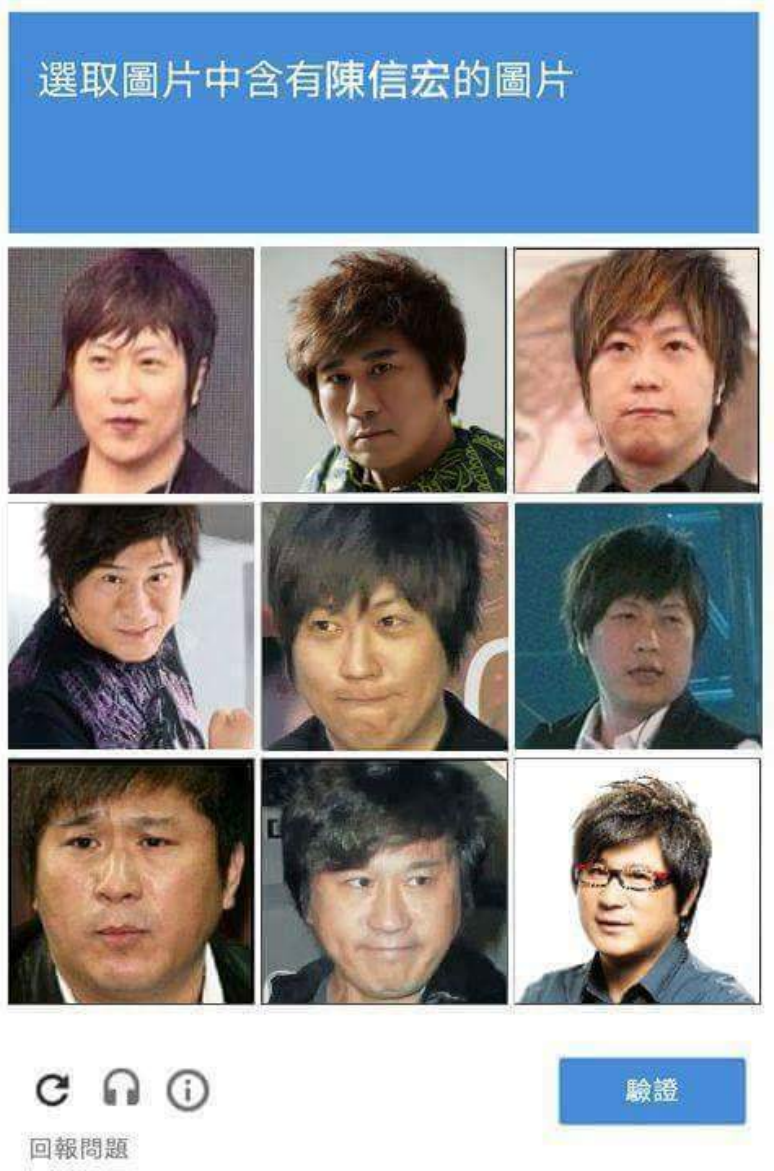
RDP保護

TEAMT5
杜浦數位安全

遠端桌面閘道(Remote Desktop Gateway)

如果不行

- 啟用多重要素驗證(Multi-Factor Authentication)
  - RADIUS
- 利用網路級身份驗證(Network Level Authentication)
  - 預防暴力破解
- 受限管理模式(Restricted Admin mode)
- 限制高權限帳號透過RDP登入
  - 高權限domain帳號
  - Local admin



AD保護 – (第一劑疫苗) 

1. **預防 local admin 遭利用 (見後續簡報介紹)**
   - (透過GPO設定，不能讓本地帳號登入到domain的電腦)
2. **限縮 Domain Admin 的權限**
   - 分離特權帳號與普通帳號
   - 確保 Domain Admin 只能登入許可的工作站，避免 credential 留在普通電腦中
3. **RDP 限制**
   - 如果要RDP AD的話請用跳板機
     (設定全部機器/帳號都不能RDP AD，另外開白名單)
   - PAW(Privileged Access Workstation)
4. **Domain Admin 帳號設定**
   - 帳號都加到”Protected User”群組
   - 將帳號設定為“sensitive & cannot be delegated”
   - 評估啟用智慧卡登入

AD保護 – (第一劑疫苗) 

5. Domain驗證的一般使用者不能有加機器到 domain (Add workstations to domain) 的權限 (預防 KrbRelayUp 攻擊)
6. 停用 Wdigest 驗證
   - “SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\ UseLogonCredential” 設定為 0
7. 啟用 SMB 簽署 (SMB Signing)
8. 啟用 LDAP 簽署(LDAP Signing)
9. 不要在 AD 上安裝第三方的程式，如果有使用 Solution 就例外
10. 限制網頁瀏覽的功能於 AD 中
    - AppLocker
11. 限制 DC 的網路連線
    - 透過外部防火牆設定阻擋 DC 對外網 internet 的 outbound 連線

TEAMT5 杜浦數位安全

預防Local admin遭濫用 – LAPS (option1)

1. 為了方便管理，很多企業的 Local Admin 密碼都一樣
2. LAPS(Local Administrator Password Solution)，微軟內建
3. 如果沒有導入其他帳號管理 solution，強烈建議使用
4. 刪除默認的擴展權限(Extended Rights)
   - 設定只有AD可讀，因為密碼是用明文儲存
5. 透過GPO設定密碼複雜度及定期更新密碼
6. 確保LAPS的讀取權限

TEAMT5
杜 浦 數 位 安 全

預防Local admin遭濫用 (option2)

S-1-5-113	NT AUTHORITY\Local account	All local accounts
S-1-5-114	NT AUTHORITY\Local account and member of Administrators group	All local accounts with the administrator privileges

1. 透過GPO限制Local Admin權限預防橫向移動，請禁用以下權限

- SeDenyNetworkLogonRight
- SeDenyBatchLogonRight
- SeDenyServiceLogonRight
- SeDenyRemoteInteractiveLogonRight
- SeDebugPrivilege

2. 啟用使用者帳戶控制和遠端限制(UAC restrictions)

TEAMT5 杜浦數位安全

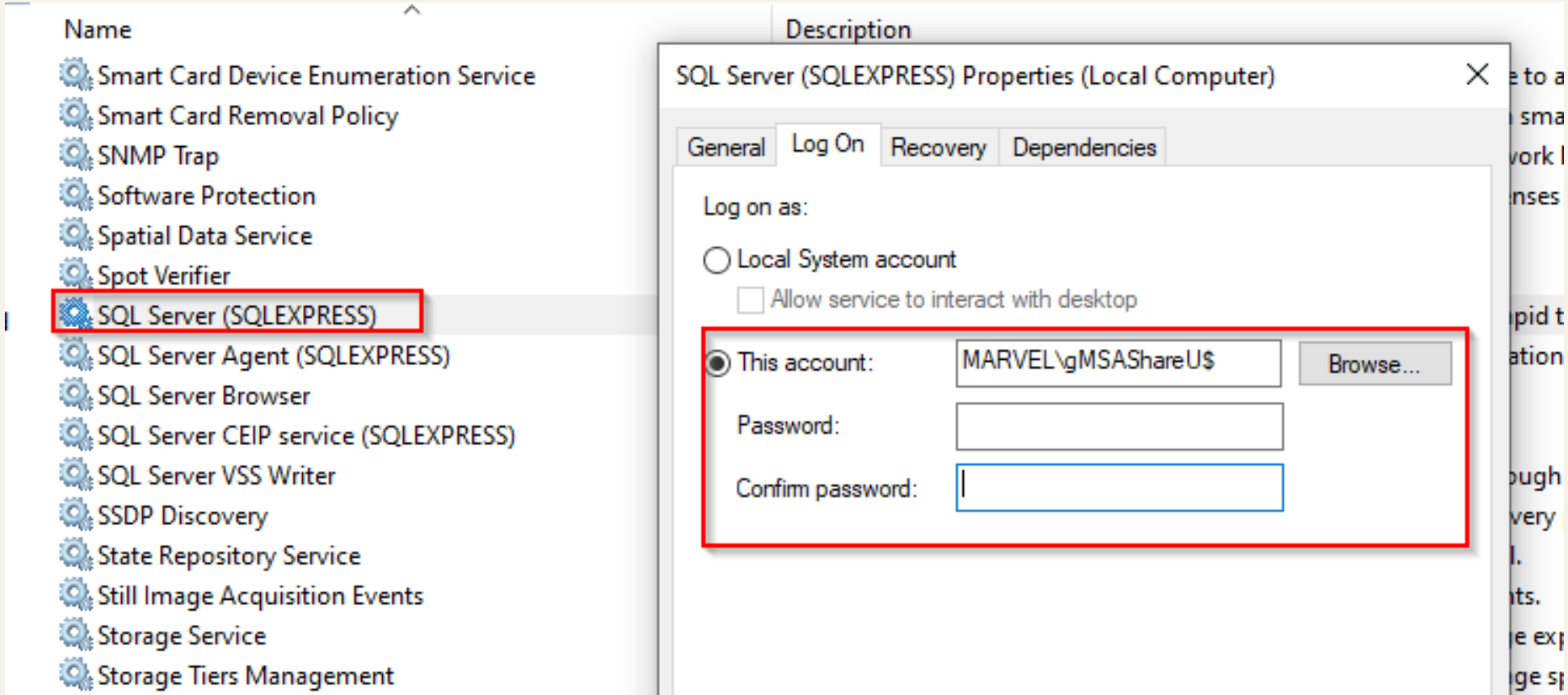
AD保護 – (第二劑疫苗) 

1. 老生常談 – 有重大 CVE 的時候，趕快上 patch
2. 將服務帳號啟用保護群組受管理的服務帳戶 (gMSA)
   - 常用服務:IIS application pool, Exchange service, Scheduled Tasks
   - 請控管好可以管理 gMSA 的帳號
3. 確保Domain電腦都是使用 NTLMv2 與 Kerberos 驗證, 請停用 LM/NTLMv1
4. 每半年將 krbtgt 密碼更改兩次，或是有 Domain admin 帳號離開也要改
5. Admin 工作站與 DC
   - 停用”NetBIOS over TCP/IP”
   - 停用LLMNR
   - 停用WPAD

TEAMT5
杜 浦 數 位 安 全

保護群組受管理的服務帳戶

- Group Managed Service Accounts(gMSA)
- 每三十天自動更新超強密碼(240-byte)
- 可部屬至多台伺服器，支援load balance

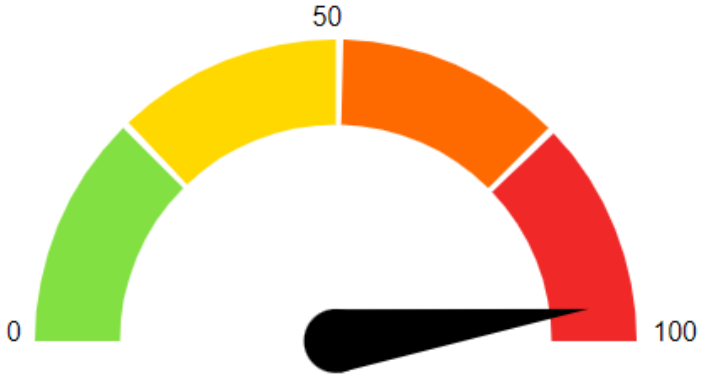


AD 健檢

TEAMT5 杜浦數位安全

- Ping Castle*
- Bloodhound**

Indicators

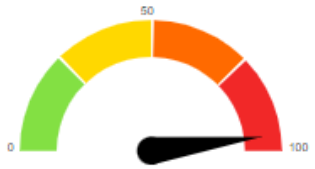


Domain Risk Level: 96 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

Compare with statistics

Privacy notice



Stale Object : 96 /100

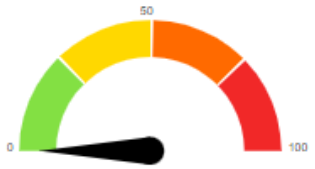
10 rules matched

It is about operations related to user or computer objects

Privileged Accounts : 40 /100

3 rules matched

It is about administrators of the Active Directory



Trusts : 0 /100

0 rules

It is about Directories

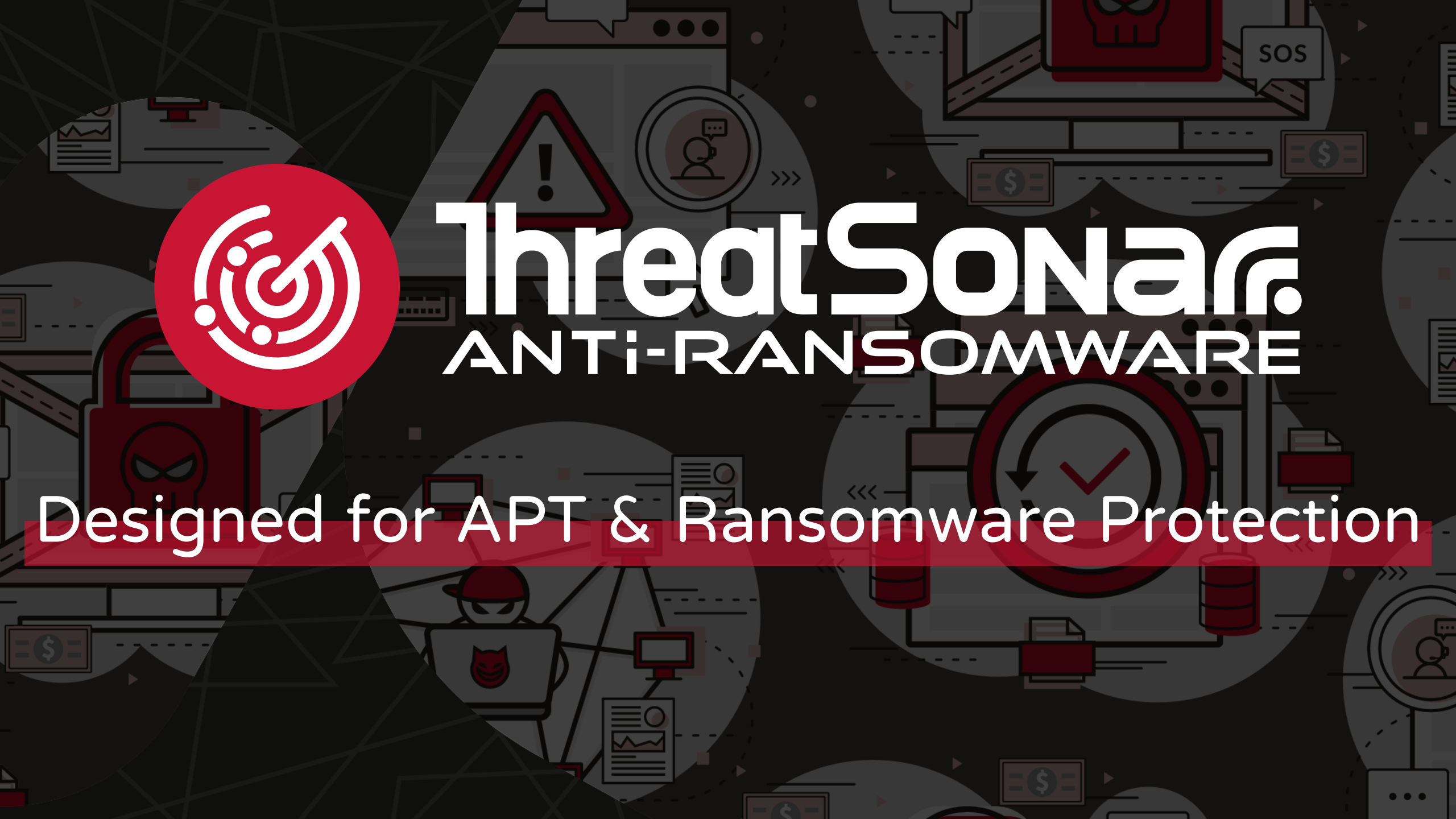
Anomali

It is about

Pre-Built Analytics Queries

- Find all Domain Admins
- Find Shortest Paths to Domain Admins
- Find Principals with DCSync Rights
- Users with Foreign Domain Group Membership
- Groups with Foreign Domain Group Membership
- Map Domain Trusts
- Shortest Paths to Unconstrained Delegation Systems
- Shortest Paths from Kerberoastable Users
- Shortest Paths to Domain Admins from Kerberoastable Users
- Shortest Path from Owned Principals
- Shortest Paths to Domain Admins from Owned Principals
- Shortest Paths to High Value Targets

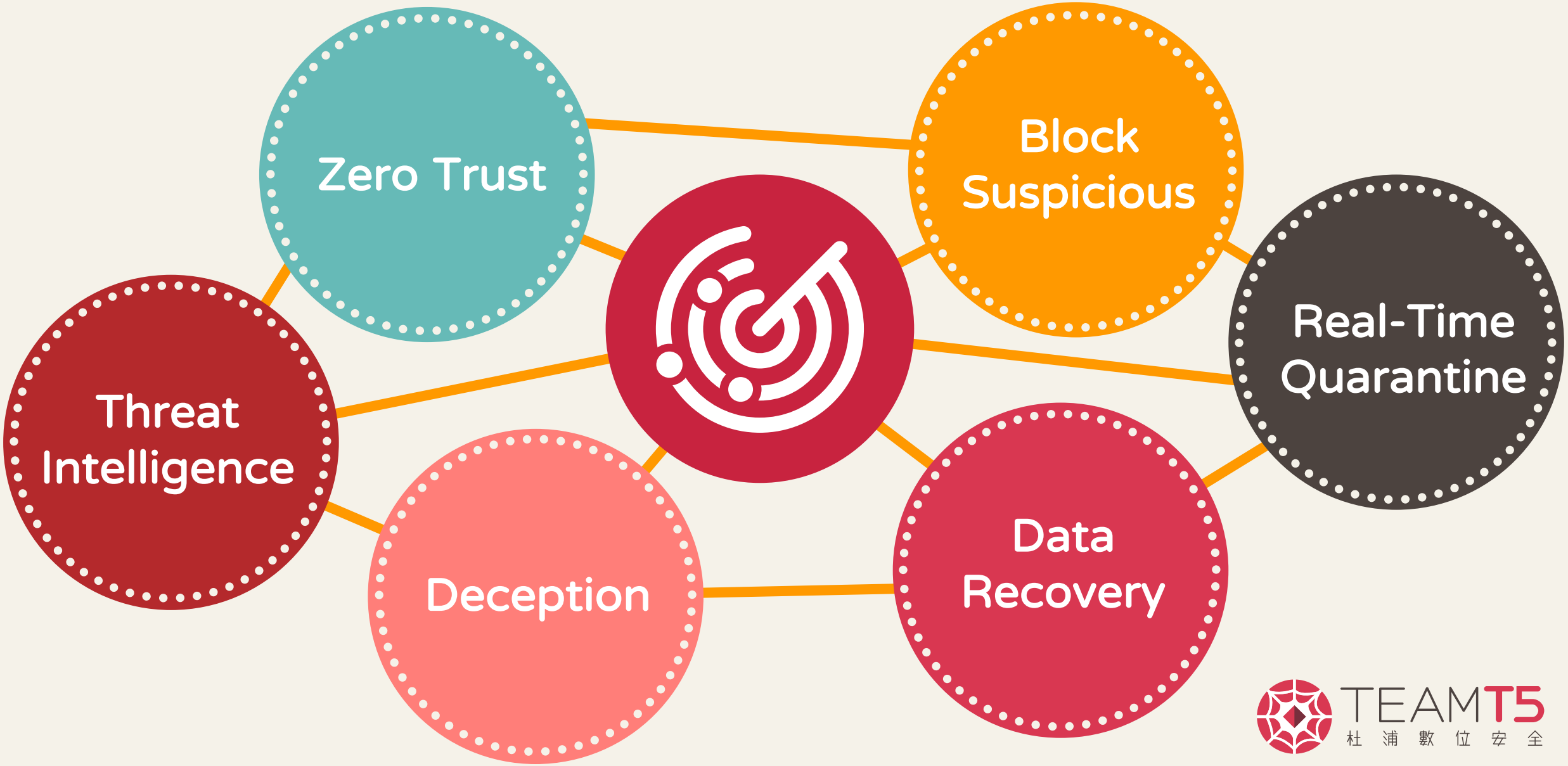
*https://pingcastle.com/
** https://github.com/BloodHoundAD



ThreatSonar ANTI-RANSOMWARE

Designed for APT & Ransomware Protection

ThreatSonar Anti-Ransomware



TEAMT5
杜 浦 數 位 安 全

聯絡我們

tt@teamt5.org

Facebook

Twitter

Linkedin

Instagram

TEAMT5

杜 浦 數 位 安 全

Persistent Cyber Threat Hunters