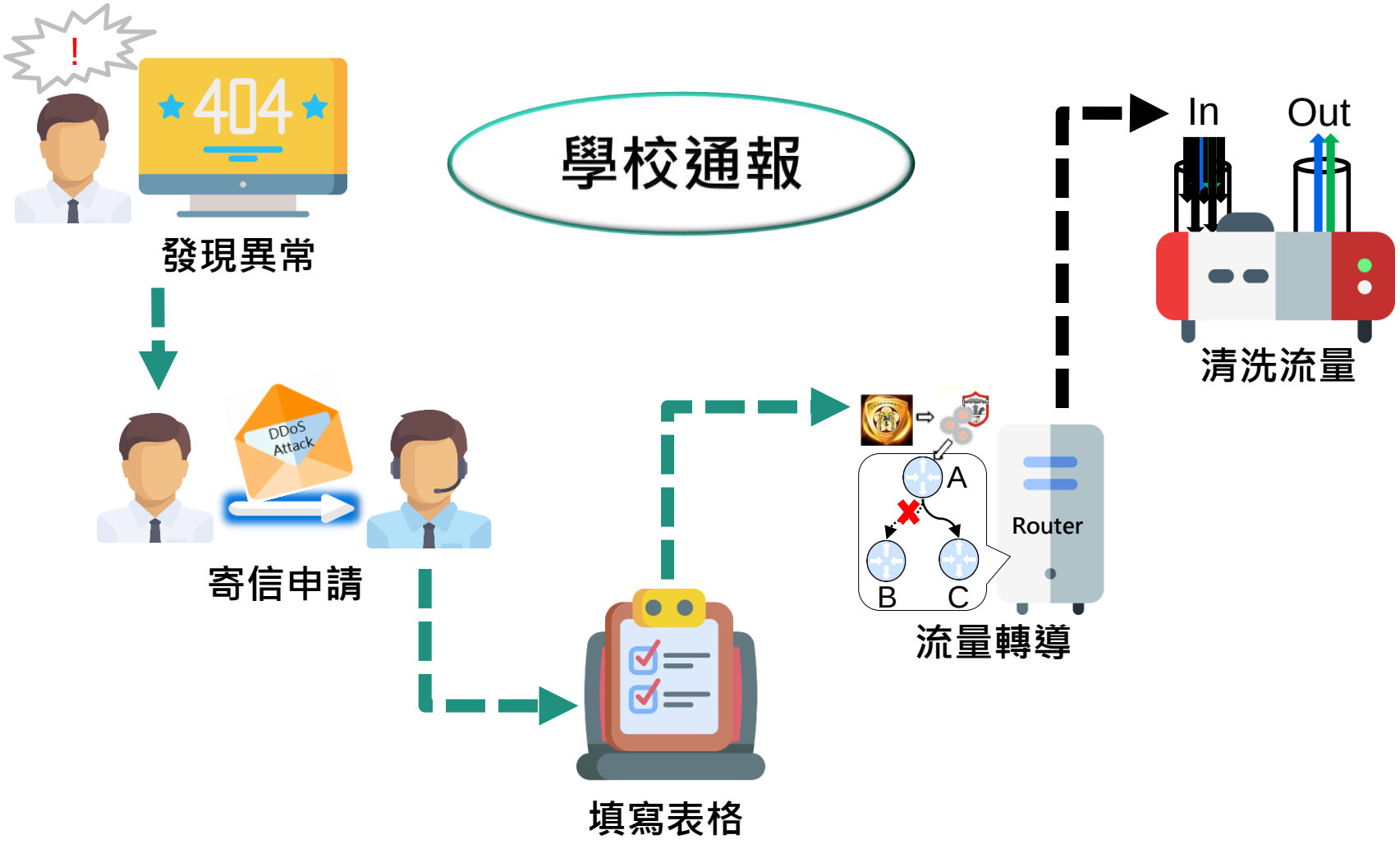
區網網管會議

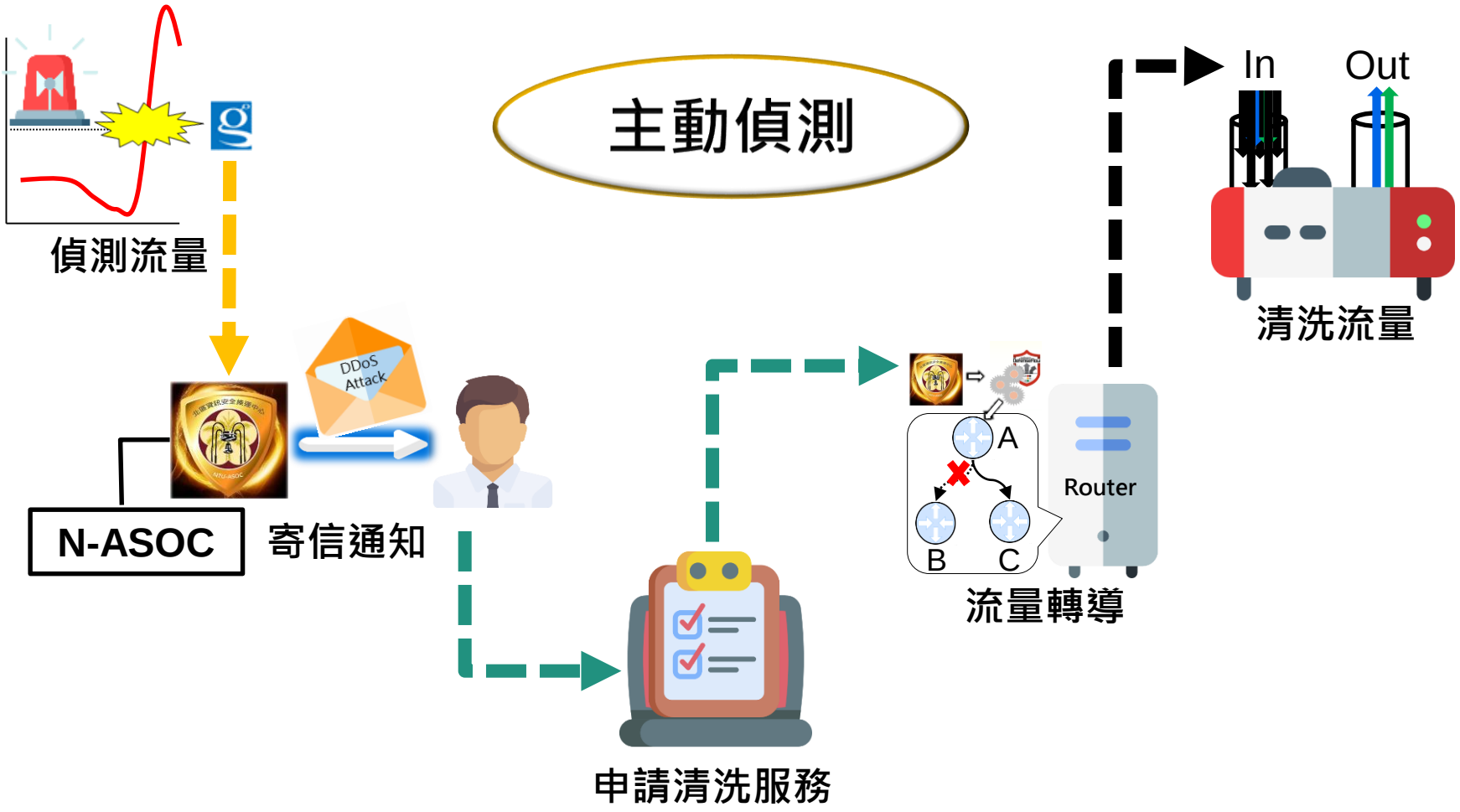
臺灣大學計資中心
李美雯

DDoS攻擊通報流程

DDoS攻擊偵測與通報架構



DDoS攻擊偵測與通報架構



Zerologon漏洞

漏洞描述

- **Windows AD Server** 遠端協定漏洞，編號 CVE-2020-1472
- 該漏洞能夠使駭客繞過身分驗證機制，進而完全掌控AD SERVER
- 該漏洞已出現大量Mimikatz 、Powershell、Python**攻擊腳本**，微軟也偵測到相關攻擊行為
- 美國官方也於今年9月18日發布緊急命令，要求政府機關需於三天內安裝Windows 安全性更新修補該漏洞

影響範圍

- 啟用Active Directory套件之Windows Server
- Samba 4.7以下版本

可能受影響的作業系統(有安裝Active Directory套件的情況下)
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server 2019
Windows Server 2019 (Server Core installation)
Windows Server, version 1903 (Server Core installation)
Windows Server, version 1909 (Server Core installation)
Windows Server, version 2004 (Server Core installation)

漏洞分析

- CVE-2020-1472 存在於 AD的客戶端驗證 AES-CFB8加密演算法的**初始參數**中

- AES-CFB8 演算法透過客戶端傳送的Client challenge 與 Session Key計算身分驗證用的**credential 參數**，而漏洞存在於當**Client challenge皆為0**時則會有1/256的機率造成**credential參數也皆為0**，使得能夠輕易地被暴力破解。

建議防護措施

1. 透過windows Update 安裝修補程式
2. 到官方網站下載並安裝最新版的韌體(根據作業系統版本下載更新)

Security Updates

To determine the support life cycle for your software version or edition, see the Microsoft Support Lifecycle.

Product	Platform	Article	Download	Impact	Severity	Supersedence
Windows Server 2008 R2 for x64-based Systems Service Pack 1		4571729	Monthly Rollup	Elevation of Privilege	Critical	4565524
		4571719	Security Only			
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)		4571729	Monthly Rollup	Elevation of Privilege	Critical	4565524
		4571719	Security Only			
Windows Server 2012		4571736	Monthly Rollup	Elevation of Privilege	Critical	4565537
		4571702	Security Only			
Windows Server 2012 (Server Core installation)		4571736	Monthly Rollup	Elevation of Privilege	Critical	4565537
		4571702	Security Only			
Windows Server 2012 R2		4571703	Monthly Rollup	Elevation of Privilege	Critical	4565541
		4571723	Security Only			
Windows Server 2012 R2 (Server Core installation)		4571703	Monthly Rollup	Elevation of Privilege	Critical	4565541
		4571723	Security Only			
Windows Server 2016		4571694	Security Update	Elevation of Privilege	Critical	4565511
Windows Server 2016 (Server Core installation)		4571694	Security Update	Elevation of Privilege	Critical	4565511
Windows Server 2019		4565349	Security Update	Elevation of Privilege	Critical	4558998
Windows Server 2019 (Server Core installation)		4565349	Security Update	Elevation of Privilege	Critical	4558998
Windows Server, version 1903 (Server Core installation)		4565351	Security Update	Elevation of Privilege	Critical	4565483
Windows Server, version 1909 (Server Core installation)		4565351	Security Update	Elevation of Privilege	Critical	4565483
Windows Server, version 2004 (Server Core installation)		4566782	Security Update	Elevation of Privilege	Critical	4565503

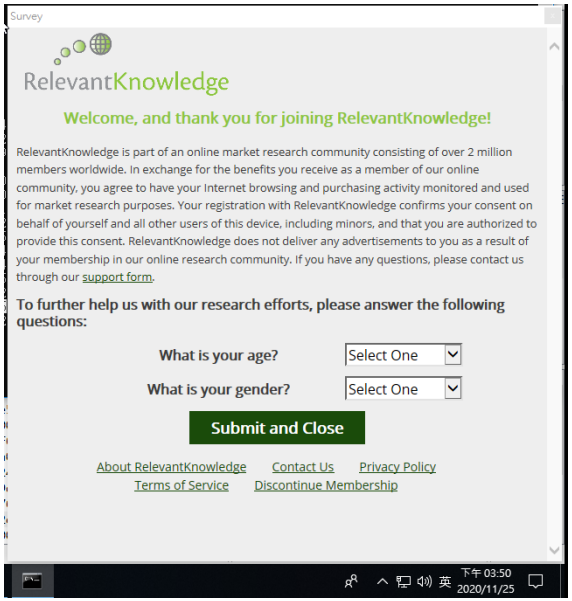
資料來源：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

Relevantknowledge 廣告軟體

惡意程式描述

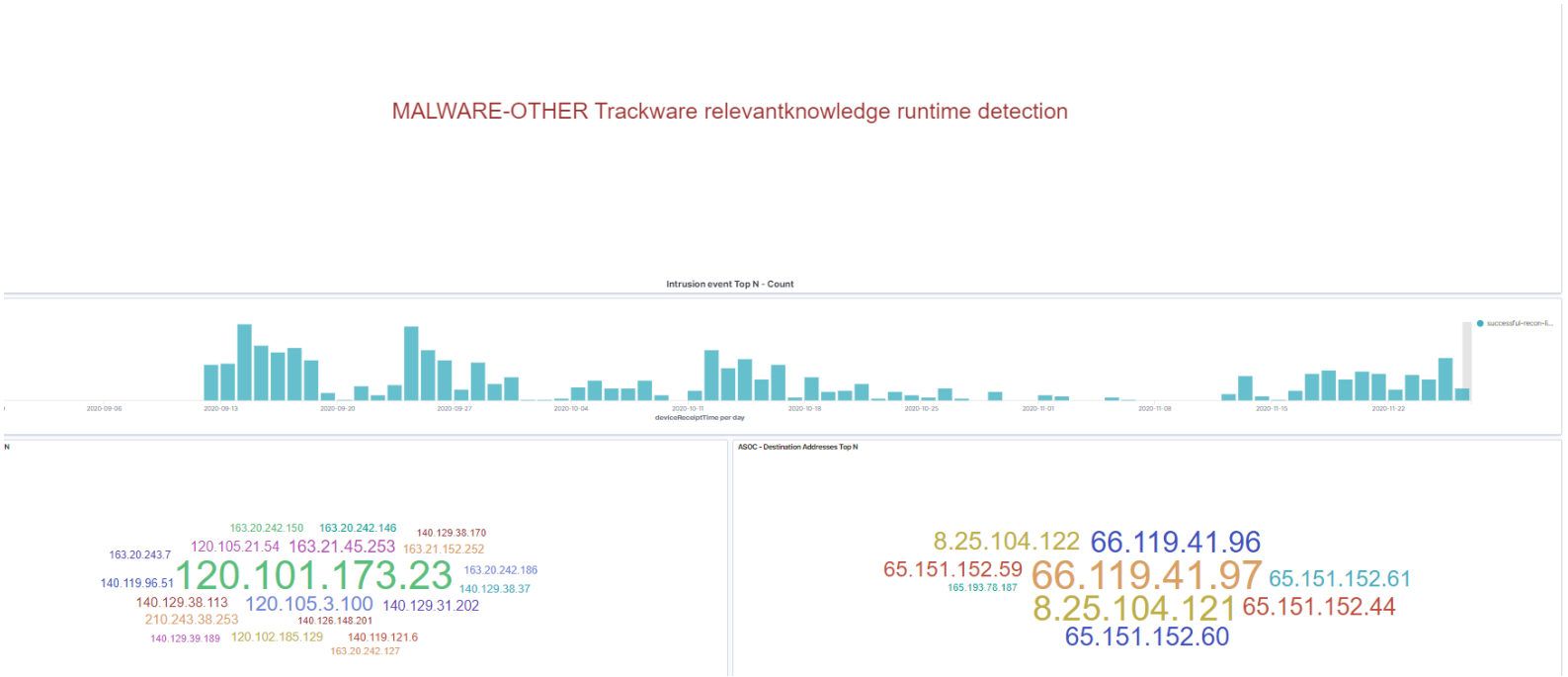
Netsetter公司旗下的**Relevantknowledge軟體**

- ✓ 用來偵測裝置上網與連線習慣，並透過該公司架設的OSS Proxy傳輸使用者的相關資訊
- ✓ 該軟體會依照使用者搜尋字串跳出廣告，綁架網頁等



事件觸發情形

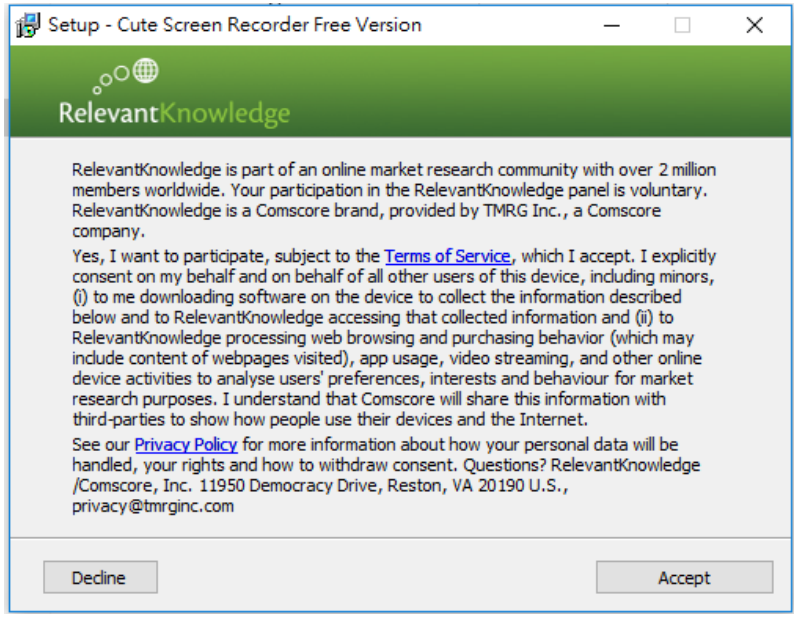
近幾個月學術網路內部遭安裝 Relevantknowledge 廣告軟體的情形愈發嚴重，從ELK統計圖表中可發現從9月開始各區網轄下IP陸續出現該廣告軟體的連線行為。

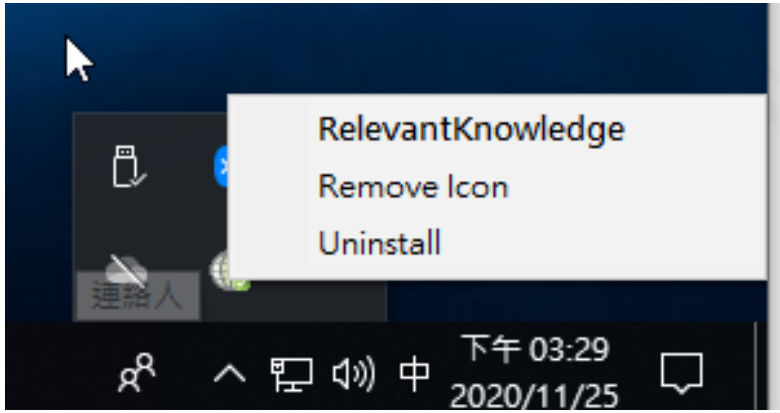


安裝途徑

該程式經常封裝於免費的共享軟體中，例如免費錄音程式Cute Screen Recorder 等，使用者於安裝過程中會出現以下畫面

若選擇Accept 則RelevantKnowledge將成功安裝並於下次設備重啟時自動啟動於Windows右下角工作列。





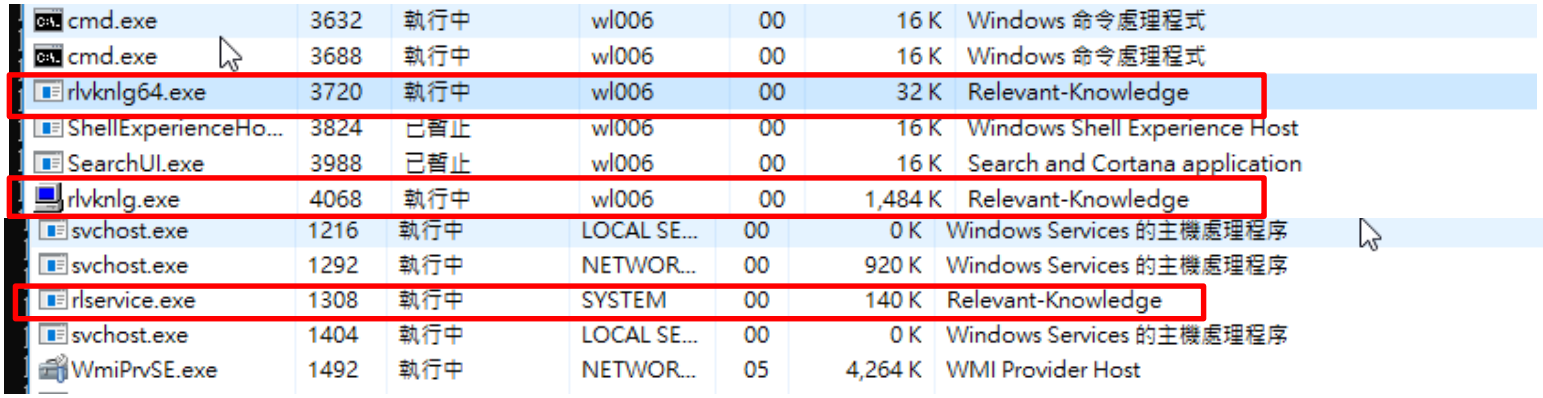
異常行為

該軟體預設安裝於C:\Program Files (x86)\ Relevantknowledge 目錄中，並於系統登陸檔中建立以下機碼以確保設備重啟時執行該程式：

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder \Start Menu\Programs\RelevantKnowledge
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "RelevantKnowledge"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "OSSProxy" rlvknlg.exe
- HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache Data "RelevantKnowledge"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ {d08d9f98-1c78-4704-87e6-368b0023d831}
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\ FirewallPolicy\StandardProfile\AuthorizedApplications\List "c:\program files\relevantknowledge\rlvknlg.exe:*:Enabled:rlvknlg.exe"

建立處理程序

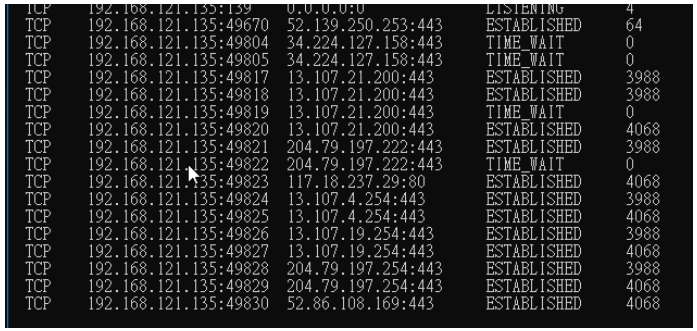
該程式建立三個處理程序
rlvknlg64.exe、rlvknlg.exe、rlservice.exe



cmd.exe	3632	執行中	wl006	00	16 K	Windows 命令處理程式
cmd.exe	3688	執行中	wl006	00	16 K	Windows 命令處理程式
rlvknlg64.exe	3720	執行中	wl006	00	32 K	Relevant-Knowledge
ShellExperienceHo...	3824	已暫止	wl006	00	16 K	Windows Shell Experience Host
SearchUI.exe	3988	已暫止	wl006	00	16 K	Search and Cortana application
rlvknlg.exe	4068	執行中	wl006	00	1,484 K	Relevant-Knowledge
svchost.exe	1216	執行中	LOCAL SE...	00	0 K	Windows Services 的主機處理程序
svchost.exe	1292	執行中	NETWOR...	00	920 K	Windows Services 的主機處理程序
rlservice.exe	1308	執行中	SYSTEM	00	140 K	Relevant-Knowledge
svchost.exe	1404	執行中	LOCAL SE...	00	0 K	Windows Services 的主機處理程序
WmiPrvSE.exe	1492	執行中	NETWOR...	05	4,264 K	WMI Provider Host

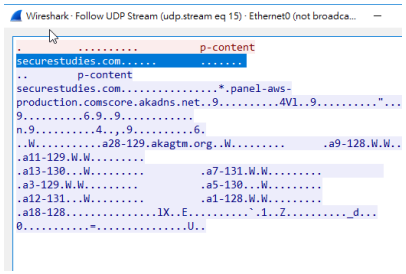
對外連線

1. 從netstat 檢視TCP網路連線行為，可發現處理程序PID 4068 rlvknlg.exe 對複數的外部IP建立80、443 PORT ，包含複數的Microsoft Azure雲端服務IP



TCP	192.168.121.135:139	0.0.0.0:0	LISTENING	4
TCP	192.168.121.135:49670	52.139.250.253:443	ESTABLISHED	64
TCP	192.168.121.135:49804	34.224.127.158:443	TIME_WAIT	0
TCP	192.168.121.135:49805	34.224.127.158:443	TIME_WAIT	0
TCP	192.168.121.135:49817	13.107.21.200:443	ESTABLISHED	3988
TCP	192.168.121.135:49818	13.107.21.200:443	ESTABLISHED	3988
TCP	192.168.121.135:49819	13.107.21.200:443	TIME_WAIT	0
TCP	192.168.121.135:49820	13.107.21.200:443	ESTABLISHED	4068
TCP	192.168.121.135:49821	204.79.197.222:443	ESTABLISHED	3988
TCP	192.168.121.135:49822	204.79.197.222:443	TIME_WAIT	0
TCP	192.168.121.135:49823	117.18.237.29:80	ESTABLISHED	4068
TCP	192.168.121.135:49824	13.107.4.254:443	ESTABLISHED	3988
TCP	192.168.121.135:49825	13.107.4.254:443	ESTABLISHED	4068
TCP	192.168.121.135:49826	13.107.19.254:443	ESTABLISHED	3988
TCP	192.168.121.135:49827	13.107.19.254:443	ESTABLISHED	4068
TCP	192.168.121.135:49828	204.79.197.254:443	ESTABLISHED	3988
TCP	192.168.121.135:49829	204.79.197.254:443	ESTABLISHED	4068
TCP	192.168.121.135:49830	52.86.108.169:443	ESTABLISHED	4068

2. 從連線封包內容也可發現，其不斷查詢securestudies.com等Domain name 並發出請求。




```
GET /oss/images/RKicon.ico HTTP/1.1
Accept: */*
Accept-Language: x-ns1Y2bB8hAGNxP,x-ns2rfbMxcVGQb2
X-OSSProxy: OSSProxy 1.3.338.320 (Build 338.320 Win32 en-us)(Apr  9 2020 18:44:54)
Content-Type: application/x-www-form-urlencoded
X-B: RelevantKnowledge
X-M: 147698416
X-H: 53706135
User-Agent: OSSProxy 1.3.338.320 (Build 338.320 Win32 en-us)(Apr  9 2020 18:44:54)
Host: rules.securestudies.com
Cache-Control: no-cache
```

建議處理措施

經測試微軟的Windows Defender 並無法偵測此廣告軟體。
其餘常見防毒軟體皆可完整根除此廣告軟體，且不影響免費軟體的使用

Avast 防毒軟體偵測結果

手動清除步驟

1. 開啟工作管理員並結束rlvknlg64.exe、rlvknlg.exe、rlservice.exe等處理程序
2. 移除C:\Program Files (x86)\ Relevantknowledge 目錄
3. 於開始選單右鍵=>執行輸入regedit 進入登陸編輯器並刪除下機碼

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu\Programs\RelevantKnowledge
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "RelevantKnowledge"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce"OSSProxy" rlvknlg.exe
- HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache Data "RelevantKnowledge"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{d08d9f98-1c78-4704-87e6-368b0023d831}
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\
- FirewallPolicy\StandardProfile\AuthorizedApplications\List"c:\program files\relevantknowledge\rlvknlg.exe:*:Enabled:rlvknlg.exe"

Q & A