108年度

網路購物產業價值升級與環境建構計畫

電子商務資訊安全培訓

時間： 108年9月24日（二）下午 2:00

地點： 集思台大會議中心亞歷山大廳
（台北市大安區羅斯福路四段85號B1）

主辦單位 經濟部商業司

執行單位 財團法人資訊工業策進會

中華民國無店面零售商業同業公會
Chinese Non-Store Retailer Association

加入 無店面公會

※官網：
www.cnra.org.tw

※FB粉絲團：
www.facebook.com/cnra.org

電子商務資訊安全培訓

時間：108年9月24日（星期二）下午 2:00

地點：集思台大會議中心 亞歷山大廳

項次	時間	分鐘	主題	講者
1	14:00~14:15	15	致詞及合影	經濟部商業司 許福添專門委員 資策會資安所 吳建興副所長
2	14:15~14:25	10	調查局於公司資安事件中扮演之角色	法務部調查局新北市調查處 姜威廷調查官
3	14:25~15:05	40	行動資安議題與風險淺談	中華資安國際股份有限公司 邱品仁資深資安技術顧問
4	15:05~15:45	40	區塊鏈應用的資安防護	大宏數創意股份有限公司 黃重道營運長
5	15:45~15:50	5	中場休息	
6	15:50~16:30	40	API串接的資安風險	如梭世代有限公司 何宜霖技術長
7	16:30~16:45	15	網站常見的資安問題與防範	飛象資訊股份有限公司 郭泰良執行長
8	16:45~17:00	15	廠商經驗分享	匯智資訊股份有限公司 莊哲豪服務經理

中華民國無店面零售商業同業公會
Chinese Non-Store Retailer Association

電子商務信賴安全聯盟暨資安服務中心

https://bit.ly/2mphfQg

零售商業同業公會
Chinese Non-Store Retailer Association

非洲豬瘟
由你我一同防堵

非洲豬瘟
不會傳染給人

非洲豬瘟是一種可怕的豬隻傳染病，
致死率可高達100%，目前沒有藥物疫苗可以治療及預防。

萬一非洲豬瘟入侵臺灣，初估將造成至少2000億元損失。

請大家遵守以下規定，一起守護國產豬：

NO 不要自國外攜帶肉類產品入境

NO 不要自國外網購肉類產品寄送臺灣

NO 不要到國外畜牧場參觀

違規者將重罰：

違規攜帶肉類產品入境，最高將處新臺幣100萬元罰鍰。

違規輸入、網購或漁船走私肉類產品，最高可處7年以下有期徒刑得併科新臺幣300萬元以下罰金。

檢舉走私專線
0800-039-131

認識非洲豬瘟
懶人包

加入防檢局Line
查詢檢疫物規定

調查局於公司資安事件中扮演之角色

法務部調查局新北市調查處

姜威廷調查官

調查局於公司資安事件中扮演之角色

新北市調查處資通安全科
報告人：姜威廷

調查局能提供的協助

- 立案偵辦
- 現場數位鑑識（IR）
- 事件紀錄分析(靜態)
- 封包側錄分析(動態)

立案前的準備工作

- 維持現場跡證
- 準備案關資料(連線紀錄、日誌檔)
- 派員來本處製作筆錄

找調查局處理的好處

- 有效溯源，根除駭侵源頭
- 出具鑑識報告具公信力
- 完全免費

行動資安議題與風險淺談

中華資安國際股份有限公司

邱品仁資深資安技術顧問

行動資安議題與風險淺談

邱品仁
資深資安技術顧問
2019/09/24

中華資安國際

講師介紹

- **學歷:** 國立中正大學資訊工程碩士
- **專長:**
  - 資訊安全系統設計開發
  - 資安威脅情資分析
  - 資安事件回應
- **工作經歷:**
  - 中華電信數分資訊處
  - 中華電信數分資安處
  - 中華資安國際(CHT Security) - 現職
- **講師經歷:**
  - 勞保局、國泰產險、新北市環保局、法扶會、2017 Digitimes雲端資安論壇、財團法人台灣網路資訊中心、三信商銀、聯合會、彰化縣政府地政處、行政院農委會漁業署、台中歌劇院、中華郵政...等
- **國際資安認證:**
  - CISM、 ECSA,、ISO 27001:2013 LA
  - (Expired)CEH、CHFI

大綱

- 行動資安議題探討
- 行動支付相關安全議題探討
- 個人行動資安防護建議

行動資安議題探討

行動趨勢快速一覽

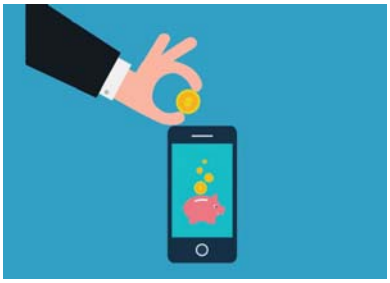
- 行動裝置
  - 2009
    - iPhone 問世
    - Android 1.1釋出
  - 2019
    - Android Q(10)　釋出
    - iPhone 11(iOS 13) 上市
- 行動網路
  - 於2003年，我們還在討論3G網路
  - 2019年，我們已經在使用4G網路，支援高達4CA/1Gbps, 5CA/900 Mbps傳輸
  - 隨著行動裝置與行動網路普及，資安的議題也隨之重要

現今的行動資安威脅

Malware
惡意程式

Phishing
釣魚/社交工程

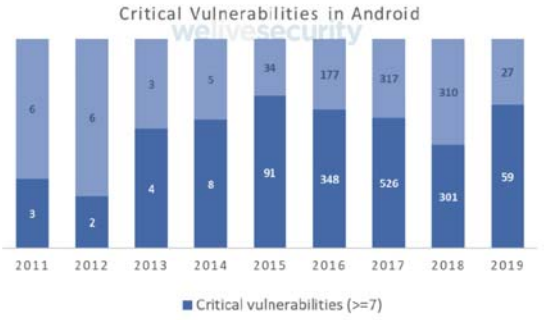
Fraud
詐騙



Vulnerability
系統安全性弱點

圖片來源: Kaspersky[1][2], Securitytoday, Fortytwo

行動裝置系統安全修補議題須受到重視



2018年，共有611個Android系統的弱點被回報，而在今年到6月的時間，有86個被提出，而其中**29%**是高危險的RCE弱點。

以今年弱點被回報的趨勢，相較於2018年，是呈現相對放緩的。

對iOS系統來說，今年已經發現了155的安全弱點，相較於去年是呈現成長的趨勢; 但是高風險弱點比數為20%左右，相較少於Android的29%。

資料來源: ESET WeliveSecurity https://www.welivesecurity.com/2019/09/05/balance-mobile-security-2019/

不修補系統弱點會有多大的風險？

Android

iOS

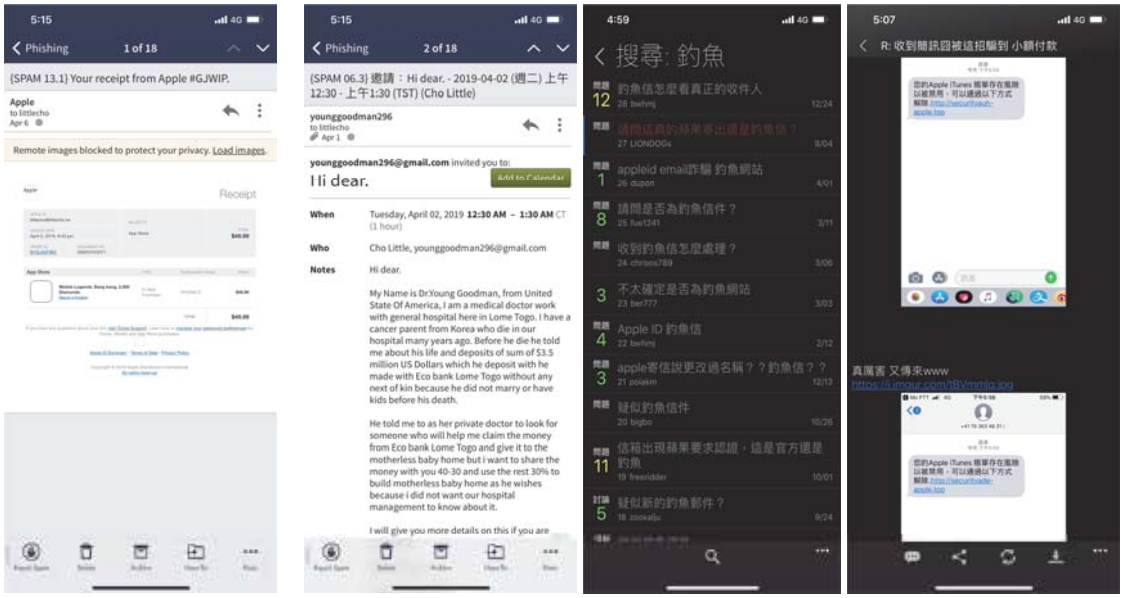
重大的系統弱點，往往都是一個網頁瀏覽，或是打開一則訊息就可被利用
即時修補系統弱點方為上策，不妨檢查一下手上的裝置版本為何？

資料來源: The Hacker News[1][2]

惡意程式威脅持續

行動裝置已成另一個資安的重戰區

釣魚/社交工程攻擊屢見不鮮

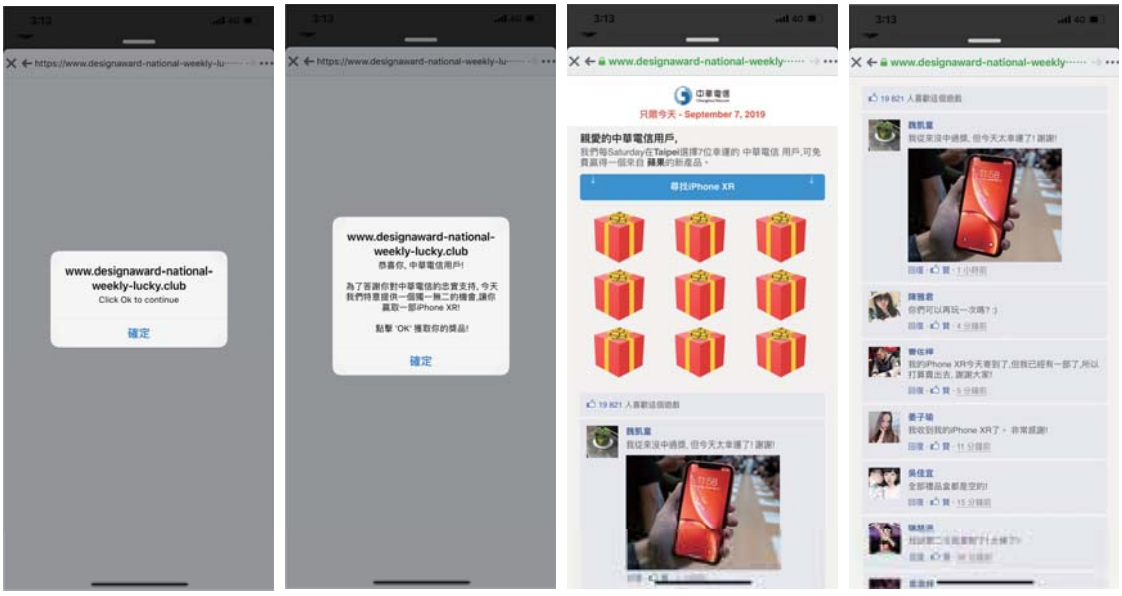


釣魚信件攻擊仍然頻繁，透過SMS傳遞的訊息讓防禦更困難

釣魚/社交工程攻擊屢見不鮮(2)

不法份子甚至可以使用遠端鎖定功能進行勒索攻擊

詐騙手法愈加細膩



使用HTTPS的安全連線，逼假亂真的Facebook留言頁面，只為詐騙個資

行動支付相關安全議題探討

行動支付逐漸普及

中華資安國際

回首過去的相關的資安議題

API或是商務邏輯的小資安錯誤，卻會造成重大的損失

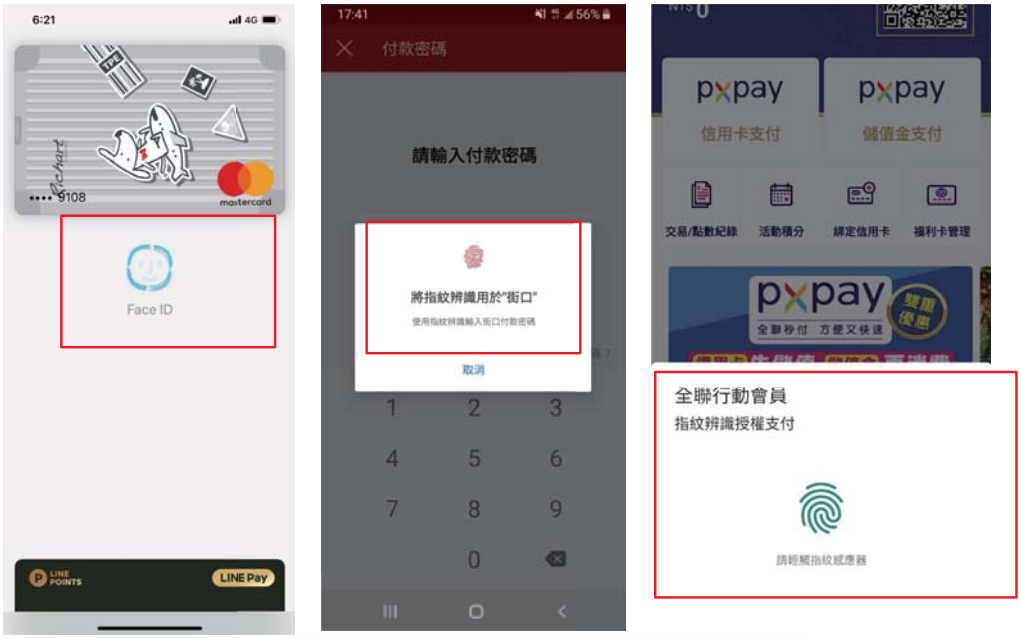
攻擊行為趨向Monetize已成為最大夢魘
與金融或是支付相關的資安議題，不可小覷。

資料來源: iThome, Ettoday新聞

行動支付中的資安防護機制

- 對於行動支付服務提供者：
  - 使用像是Secure Element的模組進行安全運算
  - 使用兩步驟驗證機制(簡訊/推播做相關行為確認)
  - 使用生物特徵驗證機制，例如：
    - 指紋
    - 臉孔辨識/虹膜辨識
  - 交易覆核機制
    - 商業流程的設計應以資安為首要考量

行動支付中的資安防護機制(2)



行動支付中的資安防護機制(3)

結合裝置的生物辨識機制與安全元件會是一個好的開始

我們面臨的資安威脅/風險

- 惡意程式感染
  - SMS轉發
  - 盜用支付資訊
  - 螢幕/鍵盤側錄
- 釣魚/社交工程
  - 透過SMS與Email
  - 透過LINE或是新興的即時通訊軟體
    - 尤其是內建轉帳功能的，更不可不慎
  - 不懷好意的廣告(Malvertising)
    - 很多都已經支援HTTPS連線
- 使用者自行破壞安全機制
  - Root/Jail break手機會使得手機更不穩定，甚至破壞原先的安全設計

個人行動資安防護建議

行動世代的資安基本功

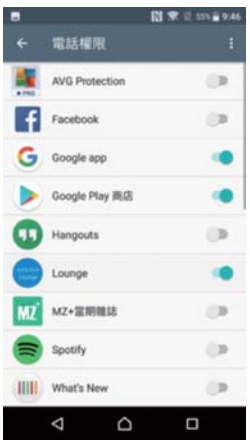
- 在你聽完這場議程後，你應該
  - 檢查你的手機是否已經安裝了最新的系統安全更新
    - Android 版本(>=7.0)
      - 安全更新編號(2019 September)
    - iOS版本 (= 12.4.1)
  - 確認手機是否啟用全機加密(Android)
    - iPhone預設已經全機加密
  - 確認是否啟用了偏弱的裝置密碼
  - 檢查你的手機App權限設定是否過度寬鬆
    - SMS讀取權限 (Android)
    - 聯絡人讀取權限 (Android/iOS)
    - 電話撥打權限 (Android)
    - 相機權限(Android/iOS)
    - 麥克風權限(Android/iOS)
    - 註冊為裝置管理員的App清單 (iOS為描述檔)

行動世代的資安基本功(2)

- 在你聽完這場議程後，你還需要記得
  - 謹慎使用公眾Wifi，使用公眾Wifi時請留意上網與相關金融操作App之安全
  - 不任意連接到不知名的充電站
  - 謹慎安裝App
    - 不從非官方App Store下載安裝App
  - 不貪小便宜，不過度好奇
    - 攻擊者往往善用小優惠或新奇的訊息誘使受害者上鉤

附錄

如何檢查相關設定？(Android)



如何檢查相關設定？ (iOS)

中華資安國際

敬請指教

中華資安國際

區塊鏈應用的資安防護

大宏數創意股份有限公司

黃重道營運長


全球首創無線金鑰加密安全溝通平台
A Service Platform
which offers best security structure to link
people and business together


OWN YOUR KEY !
安全至上 企業可以管理自己的金鑰
企業最大的資產是員工與公司的機敏資料 所有溝通與資訊傳遞都應當是以加密的形式進行溝通與傳遞 以避免競爭者取得機密或是內部機密外洩
也因為如此 市場上一直充斥著許多資安管理系統的產品與應用 其實加密資訊控管最大的關鍵在於「金鑰的管理與保護」有別於一般的資安管理服務 I.X Trio 創造了一個PKI的加密管理環境 將資料與溝通整合為一個服務平台 最後將「金鑰」的管理交由客戶
所以I.X Trio是一個真正安全無疑的企業資安解決方案

G SUITE
的整合運用

運用一：強化G Suite身份認證安全

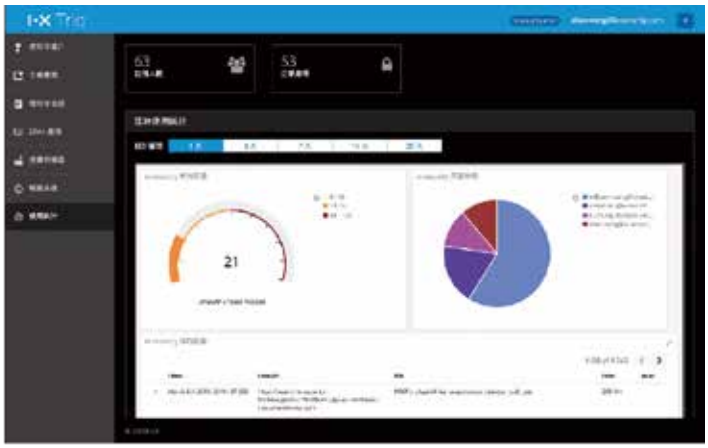
I.X Trio 的二次身份認證機制，用戶只要從手機是就可確認，提供高等級的數位簽章認證服務，不必再背一大串難記的密碼，也不需每三個月更新一次密碼。

包含 G Suite、其他雲端服務，以及VPN、ERP等內部系統，都改用 Trio 為您把關身份認證！

運用二：安全瀏覽，資料不落地

無論是用PC/Notebook, 或是手機想要瀏覽公司的Email, Google Drive以及其他公司的服務，透過 I.X Trio 的安全瀏覽器，可協助公司控管遠端存取行為，包含文件下載、內容複製、螢幕截圖等，皆受到安全瀏覽器管制！

運用三：可稽核的管理後台



Trio 提供企業稽核管理平台，以及圖像化的介面 ·

不僅所有流通資訊都已加密，更讓您可以掌握內部文件的所有流向，從上傳群組，解密瀏覽，到轉傳分享全都瞭若指掌，幫助您的團隊或企業更容易達到資料保護法規的標準。

其他運用： I.X Trio 管理其他 SAAS 的服務

- Trio 支援 SAML 認證，凡支援 SAML 的服務，都可以使用 Trio 認證身份。使用者授權登入時，會檢驗使用者金鑰簽章，並留存紀錄

- 除身份認證外，Trio 安全瀏覽器可管制雲端網頁服務檔案存取，限制下載或紀錄所有存取行為

G Suite

Slack

IBM Notes

Github

SAP® Business ByDesign

成功案例

國際法律事務所

資料不落地＆文件加密編輯＆存取權限及稽核管理

Scenario

- 保護事務所資料安全性，不允許使用個人裝置或電腦從外部連結事務所內網服務
- 事務所的資料必須不落地，保障資訊安全
- 登入以及資料存取必須可隨時稽核管理

Solution

- I.X Trio加強登入的身份認證安全
- I.X Trio的安全瀏覽器，確保資料不落地
- I.X Trio提供的圖像化稽核管理平台

新創公司或中小型企業

目前使用G Suite，缺少資安整合方案

SME & Startup

Scenario

- 公司沒有專職IT, 用 G Suite方便管理
- 需要能整合 G Suite 又能提供檔案加密，以及可稽核管理的系統
- 習慣使用SaaS的服務

Solution

- I.X Trio 透過 SAML 整合 G Suite，可以立即提升公司的登入認證安全等級
- I.X Trio 整合 Google Drive，並提供檔案下載管理，以及圖像化稽核管理平台
- I.X Trio 保護 Gmail 的附件檔案不外洩


It’s time to own
your key !
安全至上 企業可以管理自己的金鑰

API串接的資安風險

如梭世代有限公司

何宜霖技術長

ZUSO Generation

The best defense is offense.

如何嚇阻API幫助駭客竊取我們資料

API串接資安風險

Leo Ho

service@zuso.ai

ZUSO Generation

The best defense is offense.

Leo Ho

zo@zuso.ai

演講

2014 HITCON 台灣駭客年會 Speaker

2015 SITCON 學生計算機年會 Speaker

2017 OWASP Taiwan Speaker

2018 OWASP 台灣資安高峰會

專長

資安檢測

資安事件調查

駭客攻擊手法

證照

Certificated Ethical Hacker

Computer Hacking Forensic Investigator

ISO 27001 / ISO 20000 / BS 10012

10+
資安經驗

500+
防止
駭客入侵機會

10+
資安產品研發

ZUSO Generation
The best defense is offense.

API

Application Programming Interface

ZUSO Generation
The best defense is offense.

API 生態歷史

1990s->2000s

Web網站與電子商務

WebServices

傳統資安風險漏洞
Injection

2000s->2010s

雲端、社群與行動裝置

RESTful
JSON

無法預知
使用者如何使用
權限問題

2010s.....

IOT與所有連網裝置

SensorThings

複雜環境
易造成控管不當

ZUSO Generation
The best defense is offense.

OWASP API Top 10

- A1: 無效物件層級認證機制 Broken Object Level Authorization
- A2: 無效認證與授權 Broken Authentication
- A3. 過多資訊洩露 Excessive Data Exposure
- A4. 缺乏資源與限制不足 Lack of Resources & Rate Limiting
- A5. 無效權限控管 Broken Function Level Authorization
- A6. 質量配置不當 Mass Assignment
- A7. 不安全的組態設定 Security Misconfiguration
- A8. 注入攻擊 Injection
- A9. 版本控管不當 Improper Assets Management
- A10. 紀錄與監控不足 Insufficient Logging & Monitoring

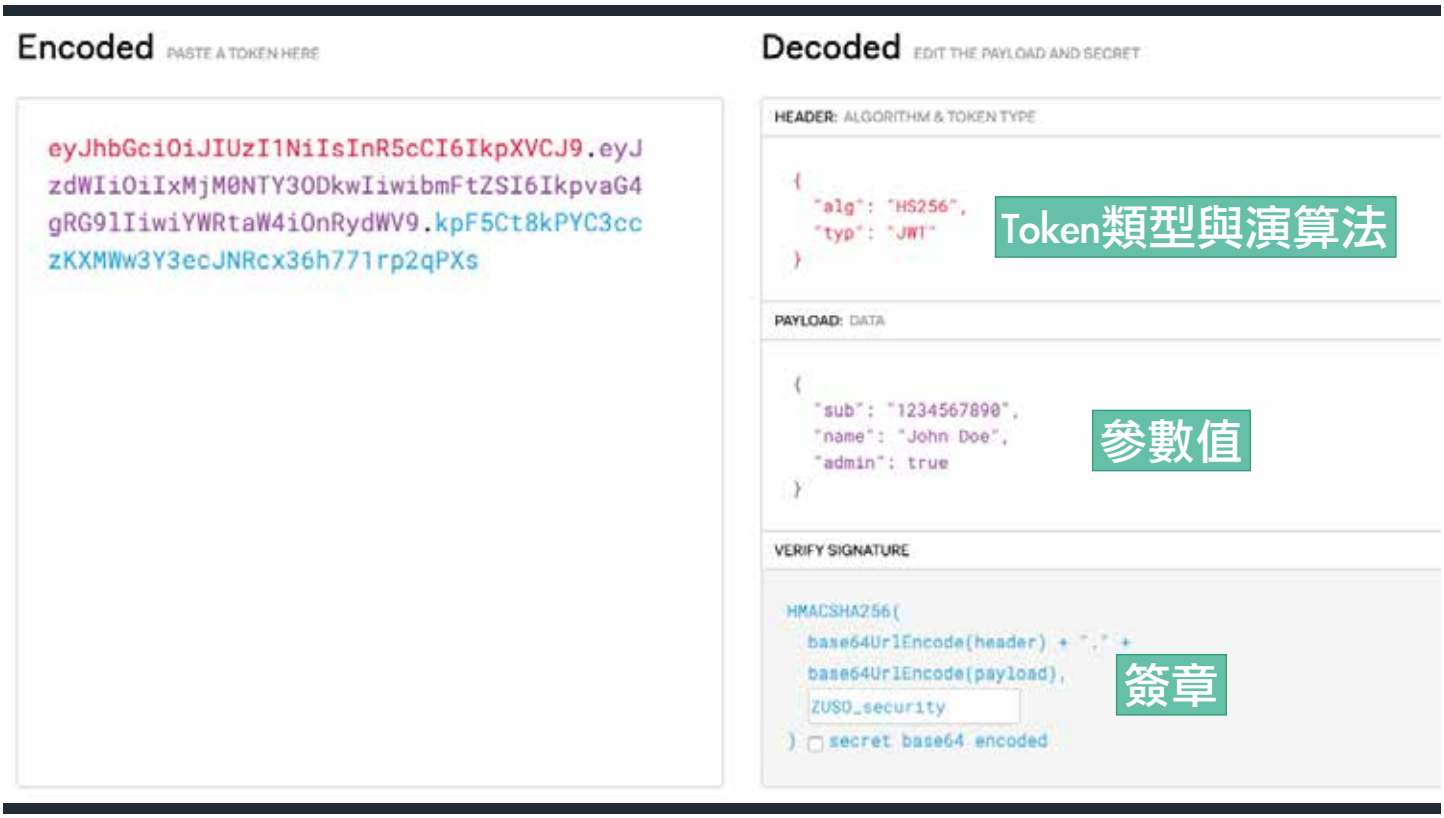
ZUSO Generation
The best defense is offense.

JWT?

Json Web Token

JWT (Json Web Token)

- 開放標準 RFC 7519
- 數位簽章可驗證傳輸資料完整性
- 簡潔
  - Size非常小，可放在POST參數、HTTP Header內傳輸
- 獨立
  - Payload可包含使用者資訊，可減少對資料庫查詢
- 認證
  - 單一登入，能夠容易跨不同Domains使用



JWT 攻擊面

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "Matt",
  "admin": true,
  "pwd" : "54987"
}
```

VERIFY SIGNATURE

```
HMACSHA256(
```

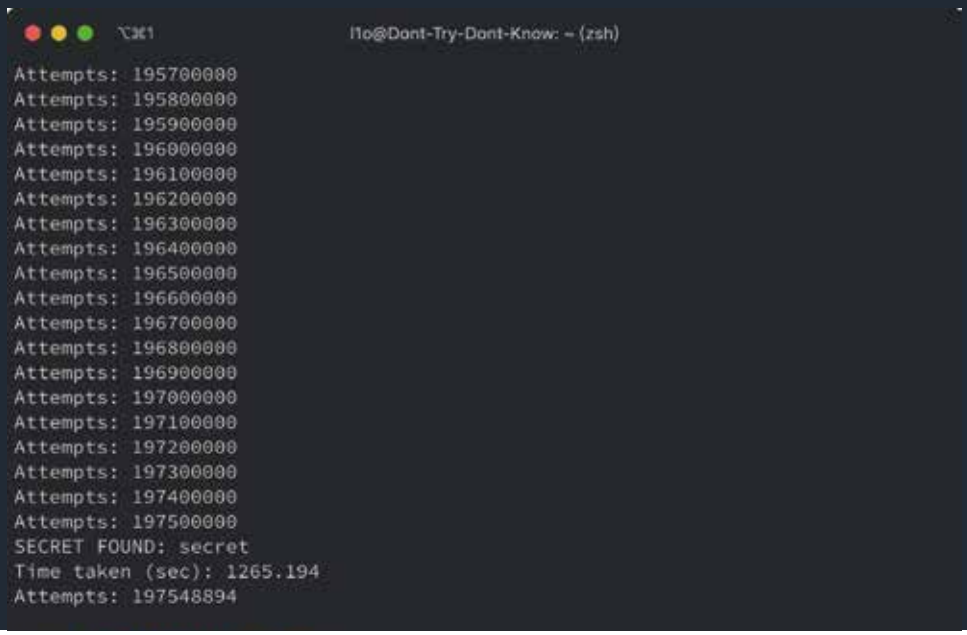
資訊洩露過多

JWT 攻擊面

演算法更改
NONE

ZUSO Generation
The best defense is offense.

JWT 攻擊面



爆破對稱式密碼

API最基本防禦策略？

- 使用HTTPS加密通道
- 限制請求次數速度，可以大致抵制多數惡意攻擊
- 做好每個功能的身份驗證
- 重視JWT安全機制與HTTP Header防禦
- 不要相信使用者所輸入
- 將身分驗證系統與敏感資料庫系統隔離
- 定期執行滲透測試，檢核API系統

ZUSO Generation
The best defense is offense.

連絡我們

Email

service@zuso.ai

Facebook

https://FB.com/ZUSOGeneration/

Website

https://zuso.ai/

ZUSO Generation
The best defense is offense.

網站常見的資安問題與防範

飛象資訊股份有限公司

郭泰良執行長

ELEPHANT Information 飛 象 資 訊

忽略資安!!!

中小企業 & 開發商

沒有概念　　人力考量　　成本考量

小電商成為目標

- 常見的主導攻擊者

1. 外部駭客
2. 內部員工

- 都是為了數據
- 信用卡欺詐
- 個資銷售

攻擊目標

1. 網站程式
2. 網站主機

主機密碼

- 密碼策略設定不嚴謹
- Root 允許登入
- SSH

飛 象 資 訊

防火牆

1. 不使用防火牆
2. 白名單防火牆
3. 應用程式防火牆

防範安裝軟體

- 實體主機或是虛擬化專屬主機（VPS）可使客戶能夠輕鬆安裝應用程式或是免費套件
- 不必要的服務接口
- 含惡意存取資料的軟體
- 記錄操作或複製你機密資料、交易的資料。

飛 象 資 訊

正確的系統設定

- 定期更新資安相關更新檔案
- 適當的檔案權限
- 伺服器設定
- X-XSS-Protection
- Content-Security-Polic
- ……

防範勝於治療

飛 象 資 訊

快速取得完整掃描報告

Thank you
Tai

飛 象 資 訊

廠商經驗分享

匯智資訊股份有限公司

莊哲豪服務經理

匯智資訊 cloudmax

資訊安全 實務分享

Cloudmax Inc.

關於我們

公司名稱：匯智資訊股份有限公司 (Cloudmax Inc.)
創立時間：1999 年 11 月
服務內容：

- 網址註冊 Domain registration
- 主機服務 Hosting
- 管理服務 Hosting Management
- 企業郵件 Email
- 數位憑證 SSL Certificate
- 資訊安全 Security
- 網站建置與行銷 Website and Marketing
- IBM、微軟、Google 等雲端服務

我們致力於提供中小企業最佳的網路解決方案，擁有 19 年豐富的產業經驗及服務超過十萬名客戶，我們了解您的需求及消費者的行為，讓我們成為您事業上的最佳助力。

19 年+ 產業經驗	服務超過 10 萬名客戶	專精 中小企業需求	了解各產業服務需求 及消費者行為
7 x 24 x 365 客服、技術雙軌支援	ISO 27001 資訊安全管理認證	擅長架構規劃、佈署 、導入及維運管理	機房、設備、資訊 安全完善規劃
Microsoft 合作夥伴	Pchome、APTG、 So-net 合作夥伴	IBM合作夥伴	國內外企業 策略聯盟

豐田子公司遭郵件詐騙攻擊，損失40億


News Release

Discovery of European subsidiary being subject of fraud

Kariya (JAPAN) September 6, 2019 Toyota Boshoku Corporation (TOKYO:3116) announce a recent case involving fraudulent payment directions from a malicious third party that has resulted in a financial loss at our European subsidiary.

Together with the European subsidiary, we became aware that the directions were fraudulent shortly after the leakage. Recognizing the high possibility of criminal activity we promptly established a team comprising legal professionals, then reported the loss to local investigating authorities. While cooperating in all aspects of the investigation, we are devoting our utmost efforts to procedures for securing/recovering the leaked funds.

We will promptly disclose any amendments to the released March 2020 earnings forecast if this incident makes such revision necessary.

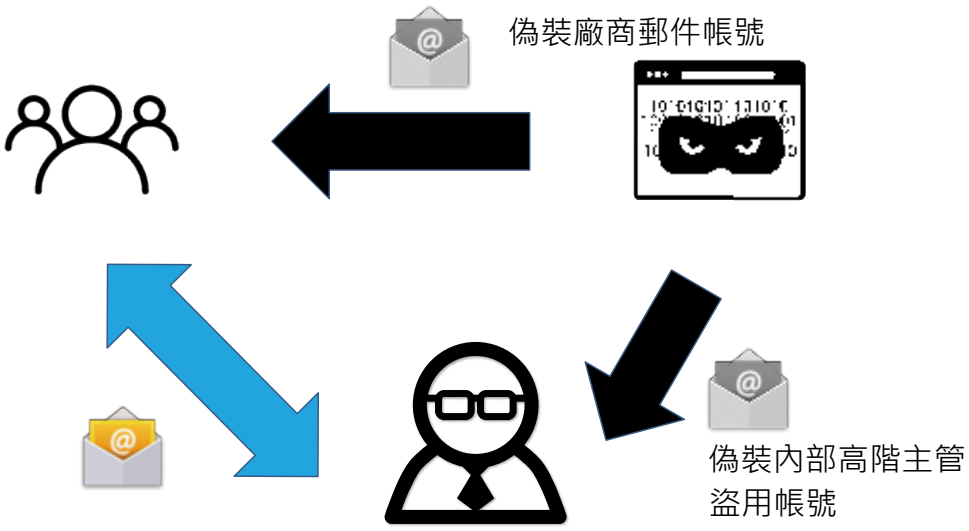
[Outline]
Expected financial loss: Approximately 4 billion yen maximum (as of 5 September)
Incident date: 14 August

To ensure the confidentiality of the investigation, we are unable to provide further details at this time. We ask for your understanding.

Contact:
TEL: +81-566-36-0301
External Affairs & Public Relations Div.
Toyota Boshoku Corporation
Available time: 8:30-17:30 Japan Time

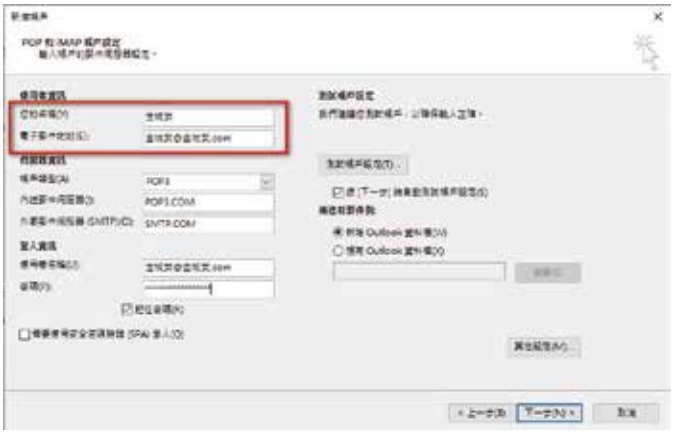
參考資料
https://www.ithome.com.tw/news/132936?fbclid=IwAR21DQh76S984AupMyy_mKcVH7VEssBz6SssEetzoAWIBa5lM1m6fZhALyg
https://www.toyota-boshoku.com/global/content/wp-content/uploads/190906e.pdf

變臉詐騙 BEC



偽裝郵件帳號手法

透過不須驗證的SMTP 伺服器



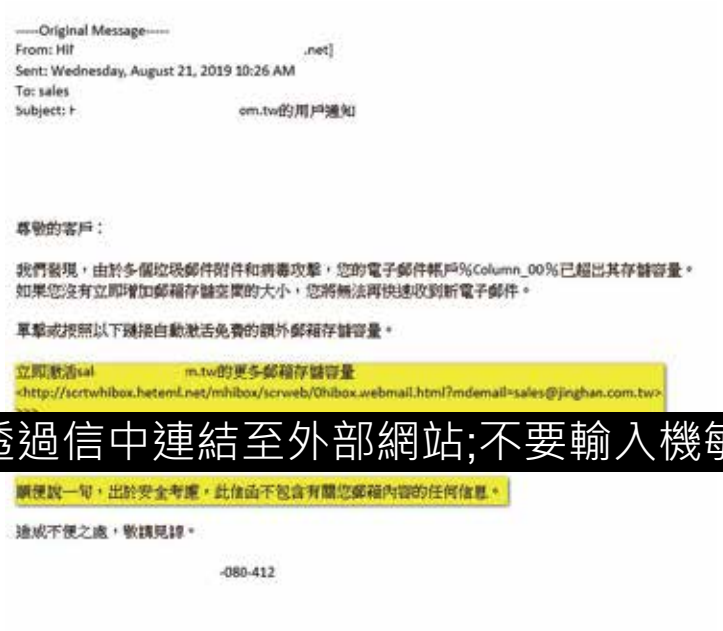
相似的網域名稱

duke.chuang@cloudmax.com.tw

duke.chuang@cioudmax.com.tw

常見的惡意郵件

釣魚郵件



不要透過信中連結至外部網站;不要輸入機敏資訊

常見的惡意郵件

域名註冊詐騙

Dear Sir/Madam,
About the “1234". We are the department of Asian Domain Registration Service in China. Here I have something to confirm with you. We formally received an application on March 9th, 2015 that a company claimed "CraTeny Company" were applying to register " 1234 " as their Net Brand and some " 1234 " Asian countries top-level domain names through our firm.

Now we are handling this registration, and after our initial checking, we found the name were similar to your company's, so we need to check with you whether your company has authorized that company to register these names. If you authorized this, we would finish the registration at once. If you did not authorize, please let us know within 7 workdays, so that we could handle this issue better.

網域註冊，不需要經過同一名稱的其他類別持有人同意

appropriate person. Thanks a lot.)

Best Regards,
Matt Fung
Senior Adviser Manager

常見的惡意郵件

搜尋引擎優化詐騙

important notice

Notice#: 896528
Date: 07/25/2019

Expiration notice

Domain: e

Expiration date: 08/02/2019

To: memowell ent co ltd|Peter Tsang,

Domain Name:	Registration Period:	Amount:	Term:
	08/15/2019 to 08/15/2020	$86.00	1 Year

Secure Online Payment

Domain Name:

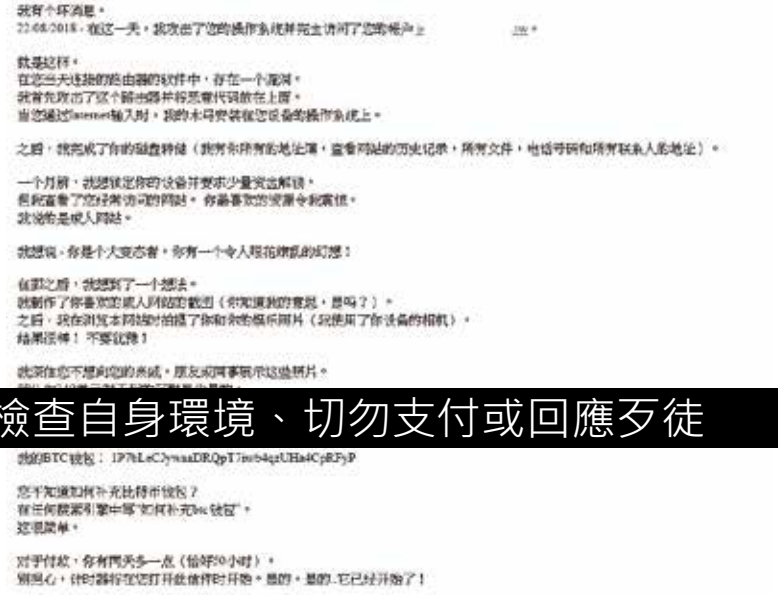
expiration notification may contain legally privileged information from the notification processing department of the Domain Seo Service Registration to our search engine traffic generator. We do not register or renew domain names. We are selling traffic generator software tools. This information is intended for the use of the individual(s) named above.
If you fail to complete your domain name registration memowell.com.tw search engine optimization service by the expiration date, may the dismissal of this search engine optimization domain name notification notice.

Process

未經身分驗證即可支付款項

常見的惡意郵件

性愛勒索詐騙



我有个坏消息。
22/08/2018，在这一天，我攻击了您的操作系统并完全访问了您的帐户。

我基础好。
在您当天连接的路由器的软件中，存在一个漏洞。
我首先攻击了这个路由器并将恶意代码放在上面。
当您通过Internet输入时，我的木马病毒将在您设备的操作系统上。

之后，我完成了你的磁盘种植（我所有所有的地址簿，查看网站的历史记录，所有文件，电话号码和所有联系人的地址）。

一个月前，我想锁定你的设备并要求少量资金解锁。
但我查看了您经常访问的网站。 你最喜欢的资源令我震惊。
我说的是成人网站。

我想说，你是个大变态者，你有一个令人难以置信的幻想！

在那之后，我想到了一个想法。
我制作了你喜欢的成人网站的屏幕截图（你知道我的意思，是吗？）。
之后，我在浏览本网站时启动了你和我的娱乐网片（我使用了你设备的相机）。
结果证明！ 不要犹豫！

我保存您不想向您的亲戚，朋友和同事展示这些照片。

我的BTC钱包： 1P7hLeCJysaaDRQpT3wb4qzUHa4CpRPyP

您不知道如何补充比特币钱包？
在任何搜索引擎中写“如何补充btc钱包”。
这很简单。

对于付款，你有两天多一点（恰好48小时）。
别担心，计时器将在您打开此信件时开始。是的，是的，它已经开始了！

檢查自身環境、切勿支付或回應歹徒

如何讓你的郵件更佳安全

如何讓你的郵件更佳安全

如何讓你的郵件更佳安全

雙/多因素驗證

無害化設置

【郵件無害化流程概念圖】

如何讓你的郵件更佳安全

關閉讀信回條

慎選郵件服務供應商

- 累積19 年、超過10萬名各產業代管經驗。
- ISO 27001 資訊安全管理認證。
- 24 小時客服工程雙軌緊急支援及系統同步監控管理。
- 微軟金級專長認證夥伴，技術能量原廠認證。
- 國家通訊傳播委員會 NCC 許可二類電信商。

Any Question ?

聯絡我們

10058 台北市中正區八德路一段 23 號 6 樓

(02) 2718-7200

(02) 2718-1922

service@cloudmax.com.tw

營業時間：

星期一～星期五　9 : 00 ~ 19 : 00

星期六　9 : 00 ~ 17 : 00

Thank you !