香港保安觀察報告

2016 第四季度

前言

認知保安狀況提高網絡安全

現今，有很多「隱形」電腦，在使用者還不知道的情況下，被攻擊者入侵及控制。在這些電腦上的數據可能每天都被盜取及暴露，並用於不同種類的犯罪活動上。香港保安觀察報告旨在提高公眾對香港被入侵電腦狀況的「能見度」，以便他們可以做更好資訊保安的決策。報告提供在香港被發現曾經遭受或參與各類型網絡攻擊活動的電腦的數據，包括網頁塗改，釣魚網站，惡意程式寄存，殭屍網絡控制中心 (C&C) 或殭屍電腦等。香港的電腦的定義，是處於香港網絡內，或其主機名稱的頂級域名是「.hk」或「.香港」的電腦。

善用全球資訊的力量

本報告是 HKCERT 和全球各地的資訊保安研究人員協作的成果。很多資訊保安研究人員具有能力去偵測針對他們或其客戶的攻擊，有些會把錄得的攻擊來源的可疑 IP 地址或惡意活動網絡連結的數據提供給其他資訊保安機構，目的是改善互聯網的整體安全。他們有良好的實務守則，在分享數據之前刪除個人身份的數據。HKCERT 建立 Information Feed Analysis System (IFAS) 系統，收集和匯聚這些寶貴的數據，對有關香港的資料進行分析。數據的來源 (附錄 1) 非常分散及可靠，可以持平地反映香港的資訊保安情況。我們會移除來自多個數據來源的重複報告，並以下面的統計指標來確保統計數據的質量：

Table 1: 網絡攻擊類型

網絡攻擊類型	統計指標
網頁塗改、釣魚網站、惡意程式寄存	在本報告所述期間，錄得有關的唯一網址的數量
殭屍網絡控制中心 (C&C)	在本報告所述期間，錄得有關的唯一 IP 地址的數量
殭屍電腦	在本報告所述期間，錄得各個殭屍網絡在季度內的同日唯一 IP 地址數量的最高值的總和。

更好的資訊，更好的服務

我們將來會加入更多的有價值的數據來源和進行更深入的分析，持續改善這報告。我們亦會探討如何利用這些數據改進我們的服務。請以電郵（***hkcert@hkcert.org***）給我們你的反饋意見。

報告的局限

本報告的數據有不同的來源，他們採用不同的收集方法、收集週期、表達方式和有各自的局限，因此數據宜作參考之用，不宜用於直接比較或視為反映現實的全貌。

免責聲明

本中心可隨時更新或修正報告，恕不另行通知。對於本報告內容及數據中出現的任何錯誤、偏頗、疏漏或延誤，或據此而採取之任何行動，本中心概不負上任何責任。對於因使用本報告內容及數據而產生的任何特殊的、附帶或相應的損失，本中心概不負上任何責任。

授權條款

Contents

1 網頁塗改 **11**
1.1 數據統計 11

2 釣魚網站 **13**
2.1 數據統計 13

3 惡意程式寄存 **15**
3.1 數據統計 15

4 殭屍網絡 **17**
4.1 殭屍網絡控制中心 (C&C) 17
4.2 殭屍電腦 18
4.2.1 香港網絡內的主要殭屍網絡[1] 18

附錄 **20**

A 資料來源 **21**

B 地理位置識別方法 **21**

C 主要殭屍網絡 **22**

[1]主要殭屍網絡指殭屍網絡在報告時間內，透過資訊來源有可觀及持續穩定的數據。

報告概要

本報告是 2016 第四季度報告。
在 2016 第四季度，有關香港的唯一的網絡攻擊數據共有 13,681 個。數據經 IFAS[2] 系統由 19 個來源收集。它們並不是來自 HKCERT 所收到的事故報告。

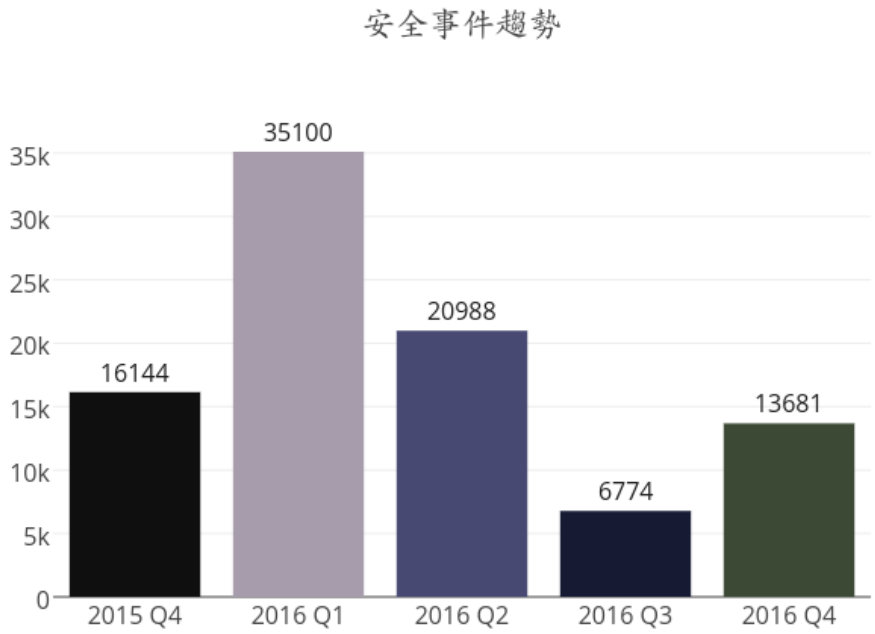

Figure 1: 安全事件趨勢

本季度安全事件大幅增加 102% 或 6,907 宗。該數字的大幅增加是由於去季的數字比平常低，上季我們一度無法從其中一個主要數據來源，CleanMX 取得數據，導致事件數字偏低。實際上，該數字仍低於前四季的平均數。

與伺服器有關的安全事件

與伺服器有關的安全事件有: 惡意程式寄存、釣魚網站和網頁塗改。以下為其趨勢和分佈:
有關伺服器的安全事件的數量在 2016 第四季度從 4,139 宗增加至 9,025 宗 (118%)。
本季寄存最多惡意程式網址的域名是 btjykjj.com。它共寄存了所有惡意程式寄存事件中的 11% 或 543 宗。驟眼看，此域名很像惡意域名：域名由看似胡亂堆砌的字母組成；管理員的電郵地址，dingchun158@gmail.com 由數百個域名共同使用。可是，細看 WHOIS 數據 [3] 會發現該域名由一間叫 “Bao Tou Shi Jiu Yuan Qu Ke Xue Ji Shu Ju” 的組織擁有，該名稱是「包頭市九原區科學技術局」的漢語拼音。該局乃中國內蒙古的

[2]IFAS - Information Feed Analysis System(IFAS) 是 HKCERT 建立的系統，用作收集有關香港的環球保安資訊來源中有關香港的保安數據作分析之用

[3]https://www.passivetotal.org/search/gaqylz.com

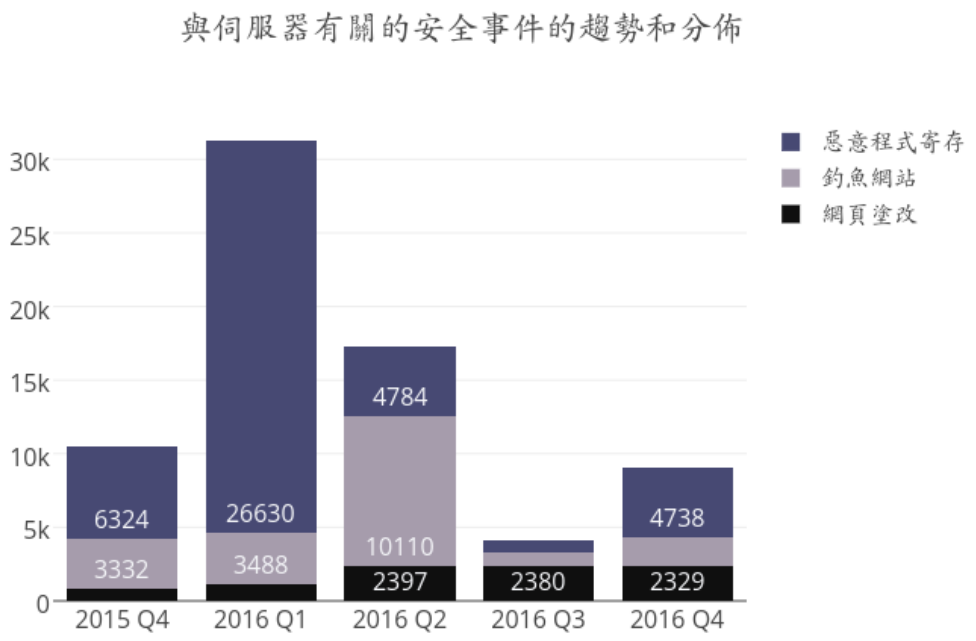

Figure 2: 與伺服器有關的安全事件的趨勢和分佈

一個政府機構，btjykjj 就是由拼音的第一個字母組成。該域名在一年前到期後沒有續期，其後便被 dingchun158@gmail.com 註冊。

我們進一步發現該域名解析出的 IP 地址同時與另外六宗惡意程式寄存事件有關，當中最少兩宗的域名疑為未有續期的正常域名，分別是 gaqylz.com，取自 “Guang An Qu Yue Lai Zhen” 的第一個字母，即「廣安區悅來鎮」的拼音，是中國四川省的一個鎮；及 hfjgg.com，取自 “He Fei Jiu Gong Ge” 的第一個字母，即「合肥九宮格」的拼音，是中國安徽省的一間裝飾工程公司。

以上個案反映網絡罪犯正尋找過期的正當域名以作惡意用途。由於它們曾經是正當域名，它們能更易騙取受害人的信任，尤其是知道背後正當組織的人。網絡用戶不應單憑域名判斷一個網址是否可信，如有懷疑，應在存取網址前進一步查核該網址。

HKCERT 促請系統和應用程式管理員保護好伺服器

- 訪問可疑網址時應核實清楚
- 在管理控制界面使用強認證，例如：雙重認證
- 獲取信息安全知識以防止社交工程

殭屍網絡相關的安全事件

殭屍網絡相關的安全事件可以分為兩類：

- 殭屍網絡控制中心 (C&C) 安全事件—涉及少數擁有較強能力的電腦，向殭屍電腦發送指令。受影響的主要是伺服器。
- 殭屍電腦安全事件—涉及到大量的電腦，它們接收來自殭屍網絡控制中心 (C&C) 的指令。受影響的主要是家用電腦。

殭屍網絡控制中心安全事件

以下將是殭屍網絡控制中心 (C&C) 安全事件的趨勢: 殭屍網絡控制中心的數字在本季

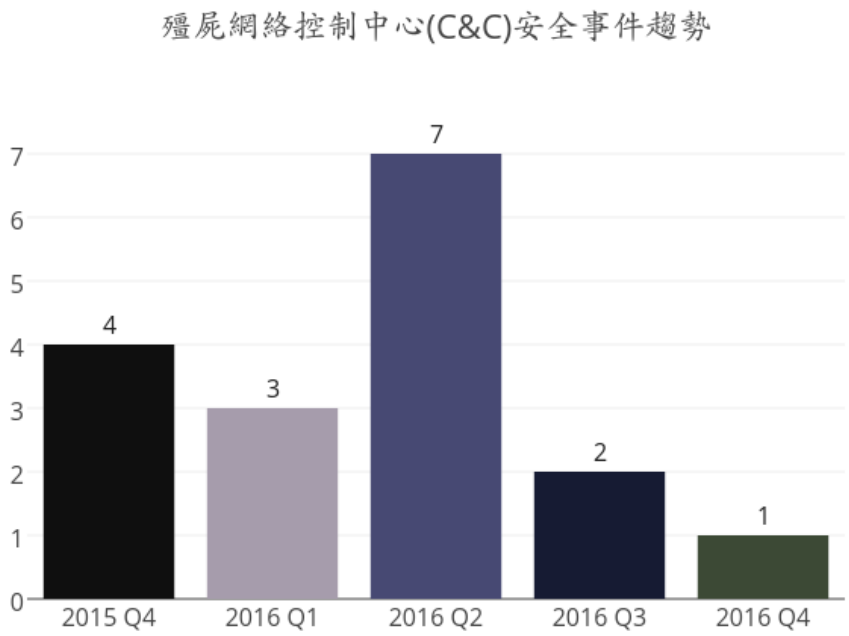

Figure 3: 殭屍網絡控制中心 (C&C) 安全事件的趨勢

減少。
本季有 1 個殭屍網絡控制中心的報告，屬 IRC 殭屍網絡控制中心。

殭屍電腦安全事件

以下為殭屍電腦安全事件的趨勢:

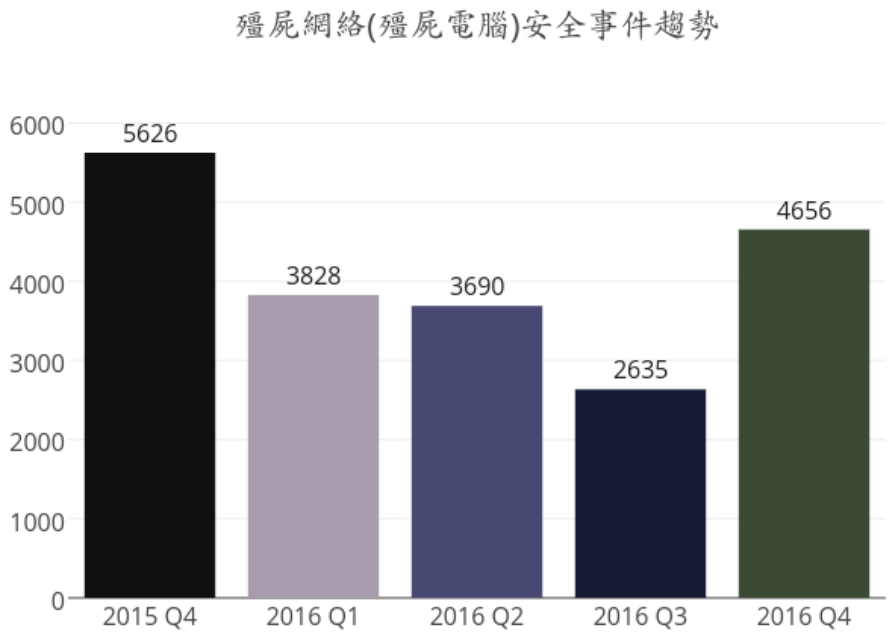

Figure 4: 殭屍電腦安全事件的趨勢

殭屍電腦安全事件在本季大幅上升 77%。兩隻新殭屍網絡，Mirai 及 Avalanche 佔所有殭屍電腦事件超過一半。

Mirai

本季，Conficker 的長期壟斷被打破。自有記錄以來，Conficker 都在統計中排第一位，遠遠拋棄其他殭屍網絡，但在本季，新殭屍網絡 Mirai 超越了它。(Figure 12).

Mirai 是一個針對物聯網設備的殭屍網絡。物聯網設備是具連接互聯網功能的設備，例如網絡攝影機、路由器及智能電視等。它們通常由缺乏保安知識的普通人操作，並且防禦薄弱，因此它們往往成為易於入侵的簡單目標。

Mirai 利用 telnet 預設密碼嘗試取得受害系統的控制來傳播。它內建一個擁有超過 60 個預設用戶名及密碼的列表 [4]，利用這個列表，Mirai 輕易地感染全球數以十萬計的設備。如有如戶把使用預設密碼的物聯網設備連著上互聯網，它很有可能在短時間內被感染。

Mirai 在九月對電腦保安博客 Brain Krebs 發動一個大型阻斷服務 (DDoS) 攻擊，該網站被超過 620Gbps 的流量攻擊。不久之後，法國寄存公司 OVH 遭到史上最大的 DDoS 攻擊 – 最高流量接近 1Tbps。[5] 不足一個月後，該殭屍網絡再對一間 DNS 服務供應商 DYN 發動另一 DDoS 攻擊。這次攻擊令 DYN 的服務癱瘓，同時令數個依賴 DYN 服務的網站亦無法連上。[6]

十一月，Mirai 攻擊了德國互聯網供應商 Deutsche Telekom 的九十萬個路由器，令其無法連線 [7]。研究人員發現這個殭屍網網的 Mirai 品種使用了一個新的傳播方法，除了

[4] https://nakedsecurity.sophos.com/2016/10/05/mirai-internet-of-things-malware-from-krebs-ddos-attack-goes-o

[5] http://www.scmagazineuk.com/ovh-suffers-11tbps-ddos-attack/article/524826/

[6] https://www.hkcert.org/my_url/en/blog/16102401

[7] https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/

使用傳統的預設備密攻擊外，它還能利用 Zyxel 及 Speedport 路由器的一個漏洞透過 TR-069 遠端管理協儀感染相關設備。
要移除這種惡意程式十分困難。Mirai 會停用 TR-069 及 telnet 所使用的端口，令互聯網供應商無法遠端修補設備上的漏洞。用戶需把路由器關掉以在記憶體中移除 Mirai，可是，由於 Mirai 一直在活躍地掃描互聯網上的設備，除非該設備接著立刻安裝修補程式，否則它可能在重新啟動後數分鐘內再受感染。
在可見將來，Mirai 會繼續是互聯網的一個主要威脅。

HKCERT 促請使用者保護好電腦，免淪為殭屍網絡的一部分。

- 立刻更改物聯網設備上的預設密碼
- 設定強密碼以防止密碼容易被破解
- 關閉所有非必要的網絡服務，尤其是 telnet
- 如非必要，不要直接把設備曝露在互聯網
- 如懷疑設備受感染，應立刻把設備從網絡中移除

Avalanche
Avalanche 是一個網絡罪犯使用的寄存平台。它在 2009 年設立，由遍佈全球的 600 台伺服器網成，主要用作部署財務犯罪軟件（如 Zeus，SpyEye），發送命令至被感染設備（例如發送詐騙電郵，清洗黑錢等）。它利用代理伺服器及雙重 “fast flux” 技術（即每 5 分鐘改變一次惡意域名使用的 DNS 及 IP 地址）以隱藏伺服器的真實位置。
一個由歐洲刑警組織領導，並由來自超過三十個國家的執法機構、司法機構及保安研究員執行的聯合行動搗破了 Avalanche 網絡犯罪寄存平台。該行動拘捕了五名疑犯，並繳獲 39 台伺服器及透過寄存供應商令 221 台伺服器下線。超過 830,000 惡意域名被充公、屏蔽或 “sinkhole”。[8]
大約 350 個香港 IP 地址受影響。HKCERT 已通知相關的互聯網供應商以接觸受影響客戶。

[8] https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international

HKCERT 促請使用者保護好電腦，免淪為殭屍網絡的一部分。

- 安裝最新修補程式及更新
- 安裝及使用有效的保安防護工具，並定期掃描
- 設定強密碼以防止密碼容易被破解
- 不要打開來歷不明的檔案

自 2013 年 6 月，本中心一直有跟進接收到的保安事件，並主動接觸本地互聯網供應商以清除殭屍網絡。現在殭屍網絡的清除行動仍在進行中，針對的是幾個主要的殭屍網絡家族，包括 Pushdo, Citadel,ZeroAccess 及 GameOver Zeus。

使用者可 *HKCERT* 提供的指引，偵測及清理殭屍網絡。

- 殭屍網絡偵測及清理指引
- https://www.hkcert.org/botnet

詳細數據

1 網頁塗改

1.1 數據統計

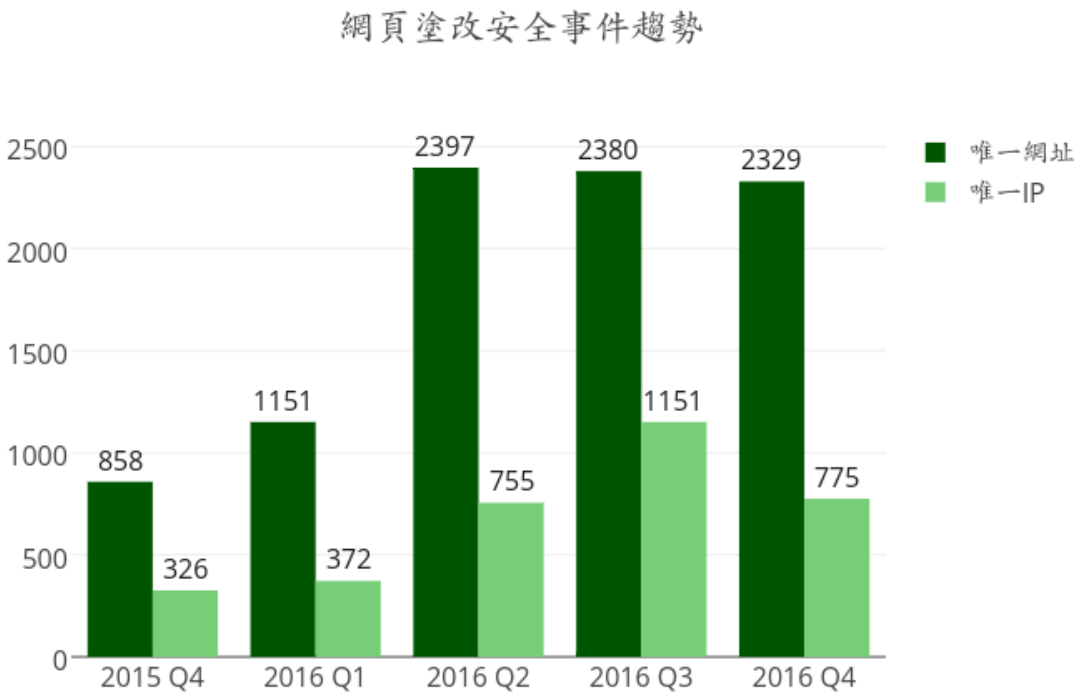

Figure 5: 網頁塗改安全事件趨勢

什麼是網頁塗改?

- 網頁塗改是在未經授權下，使用黑客攻擊方法去更改合法網站的內容。

有什麼潛在影響?

- 網站內容的完整性被破壞
- 不能存取網站原來的內容
- 合法網站的擁有者的聲譽或受損害
- 伺服器上存儲/處理的其他資訊亦有可能被黑客入侵，用作其他攻擊

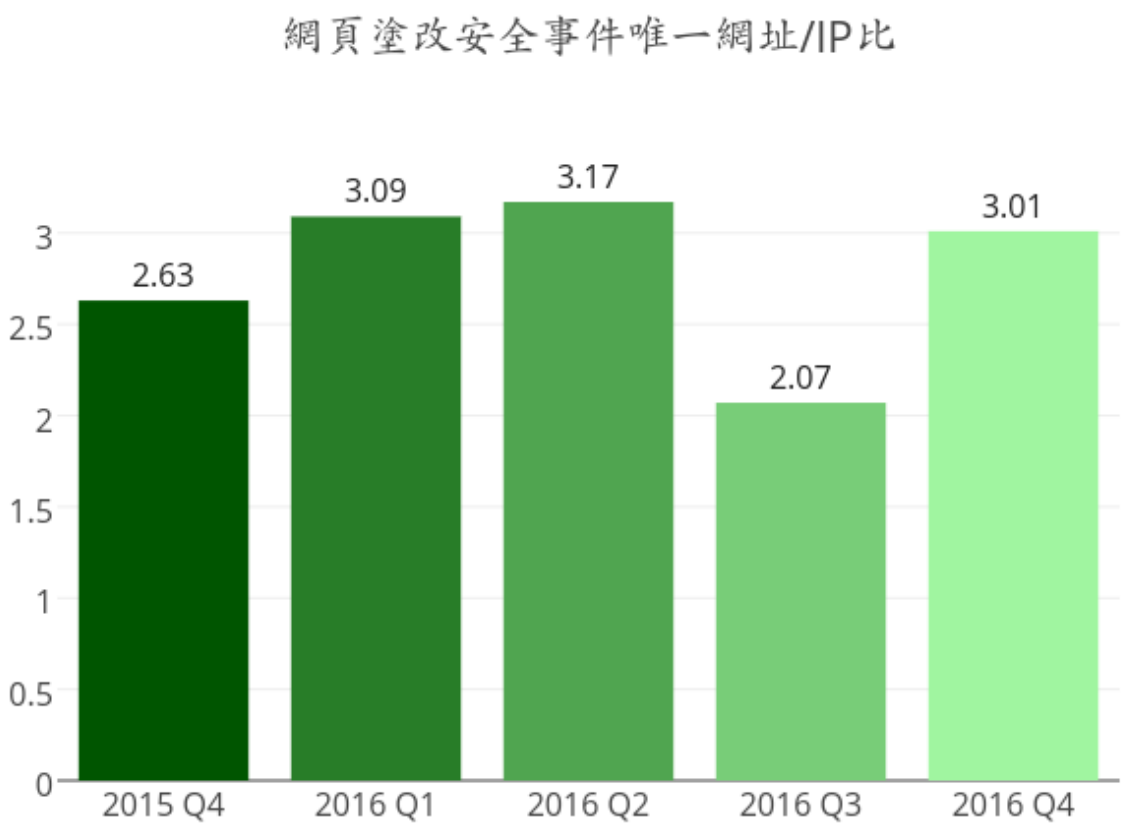

Figure 6: 網頁塗改全事件唯一網址/IP 比

甚麼是唯一網址/IP 比？

- 它是以唯一網址計算的安全事件數量除以以 IP 地址計算的安全事件數量

這個比例能顯示甚麼？

- 以唯一網址計算的安全事件數量並不能反映被入侵伺服器的數量，因為一台伺服器可能提供很多唯一網址
- 以 IP 地址計算的安全事件數量能更能關聯被入侵伺服器的數量
- 這個比例越高，代表越多大型入侵事件

資料來源：

- Zone-H

2 釣魚網站

2.1 數據統計

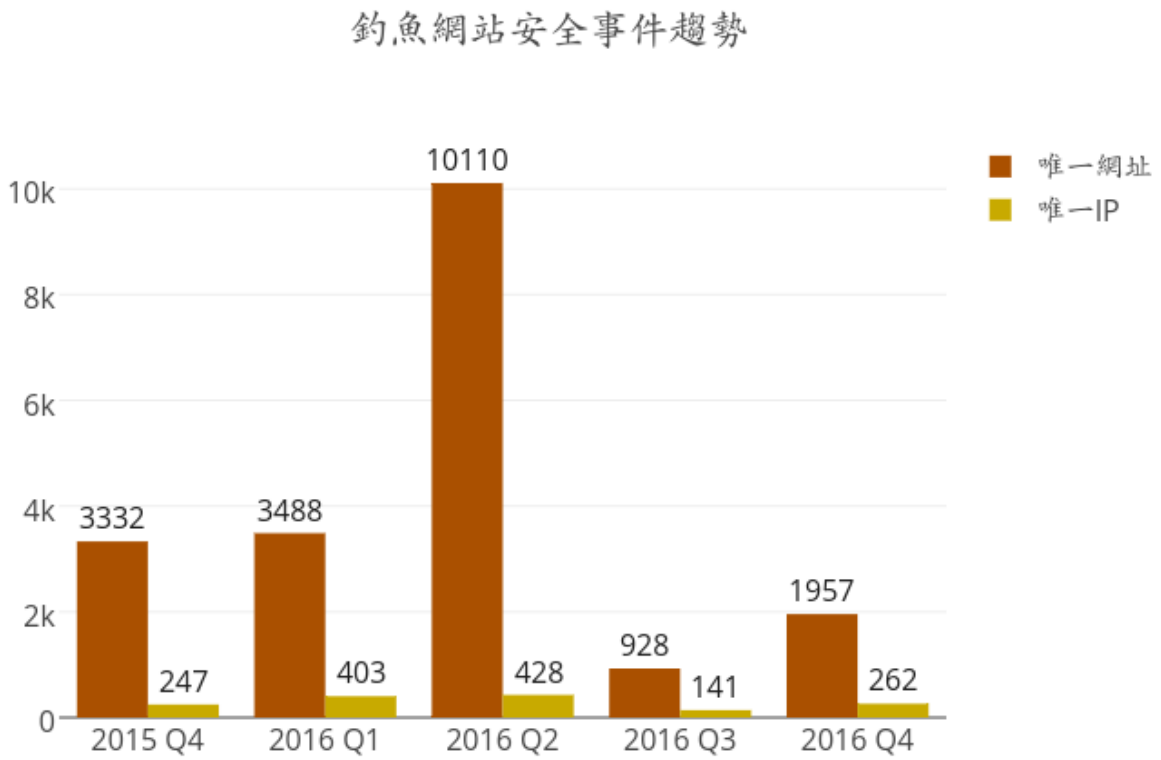

Figure 7: 釣魚網站安全事件趨勢

什麼是釣魚網站?

- 釣魚網站是冒充一個合法網站，以達到詐騙的目的。

有什麼潛在影響？

- 訪客的個人資料可能被盜取，導致金錢上的損失。
- 不能存取網站原來的內容
- 合法網站的擁有者的聲譽或受損害
- 伺服器可能被黑客進一步入侵，用作其他攻擊。

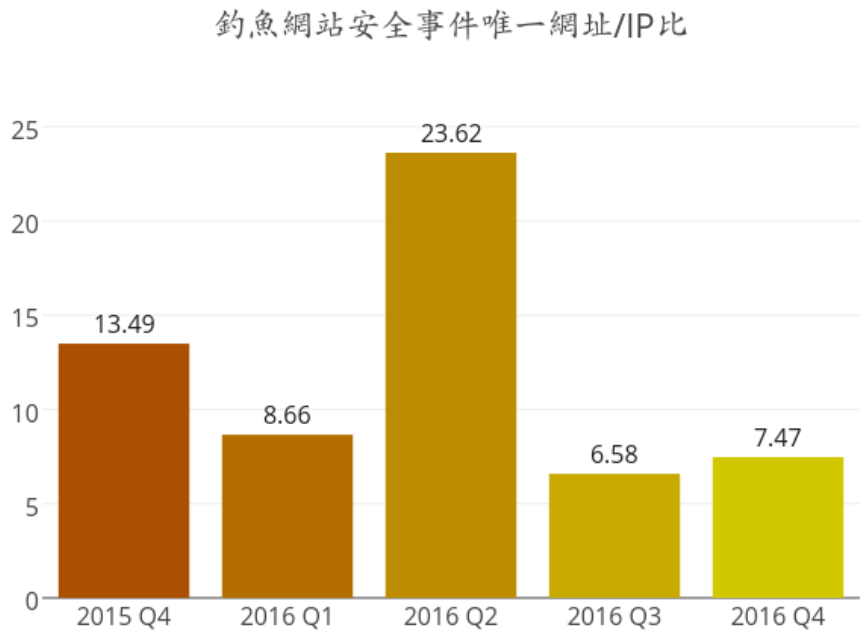

Figure 8: 釣魚網站安全事件唯一網址/IP 比

甚麼是唯一網址/IP 比？

- 它是以唯一網址計算的安全事件數量除以以 IP 地址計算的安全事件數量

這個比例能顯示甚麼？

- 以唯一網址計算的安全事件數量並不能反映被入侵伺服器的數量，因為一台伺服器可能提供很多唯一網址
- 以 IP 地址計算的安全事件數量能更能關聯被入侵伺服器的數量
- 這個比例越高，代表越多大型入侵事件

資料來源：

- ArborNetwork - Atlas SRF
- CleanMX - phishing
- Millersmiles
- Phishtank

3 惡意程式寄存

3.1 數據統計

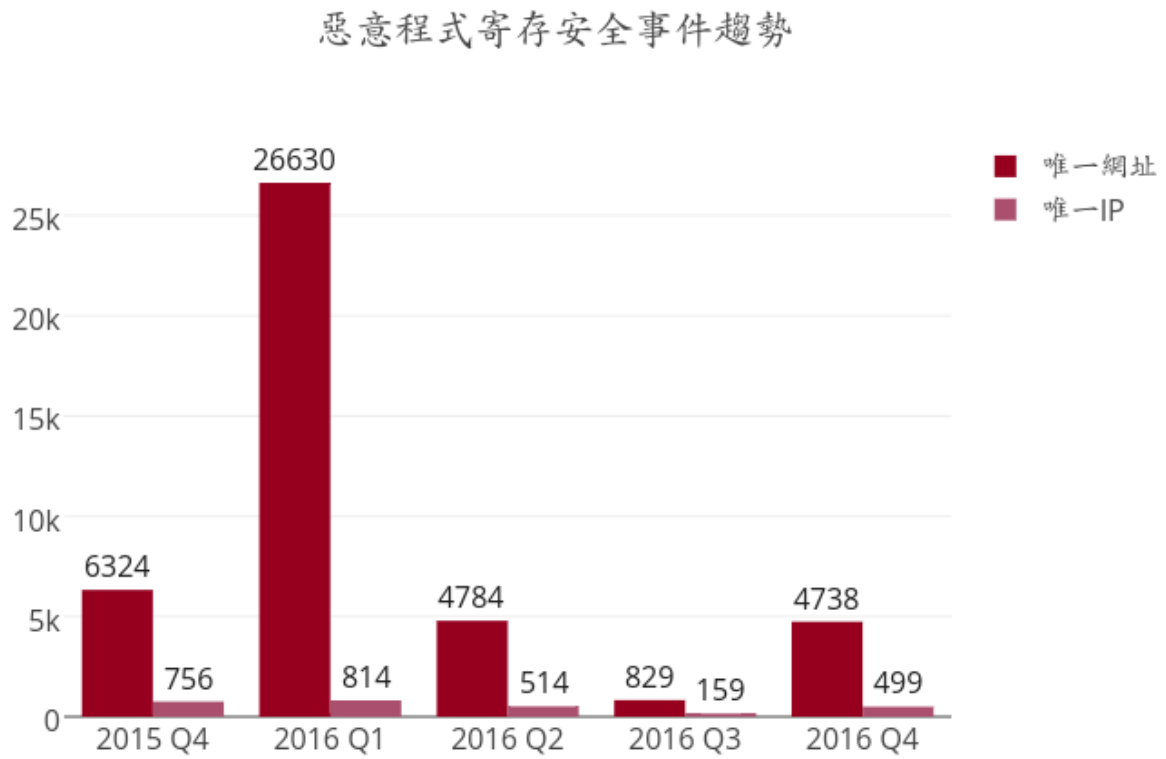

Figure 9: 惡意程式寄存安全事件趨勢

什麼是惡意程式寄存?

- 惡意程式寄存是透過網站散播惡意程式

有什麼潛在影響?

- 訪客可能下載及安裝惡意程式，或執行網頁的惡意程式碼，導致被入侵。
- 不能存取網站原來的內容
- 網站的擁有者的聲譽或受損害
- 伺服器可能被黑客進一步入侵，用作其他攻擊。

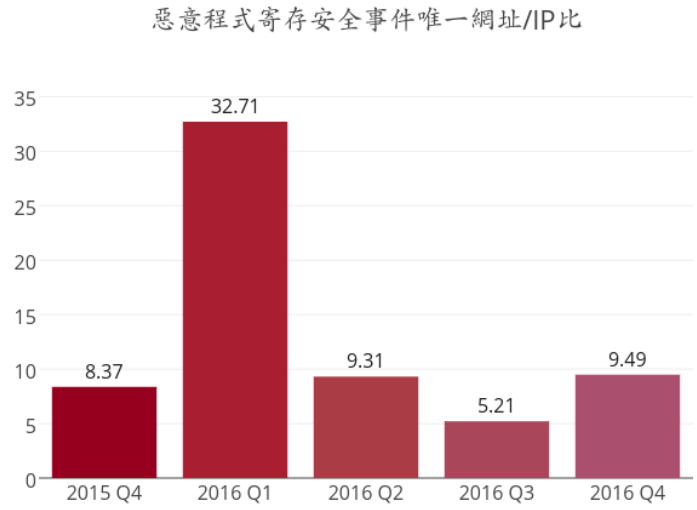

Figure 10: 惡意程式寄存安全事件唯一網址/IP 比

甚麼是唯一網址/IP 比？

- 它是以唯一網址計算的安全事件數量除以以 IP 地址計算的安全事件數量

這個比例能顯示甚麼？

- 以唯一網址計算的安全事件數量並不能反映被入侵伺服器的數量，因為一台伺服器可能提供很多唯一網址
- 以 IP 地址計算的安全事件數量能更能關聯被入侵伺服器的數量
- 這個比例越高，代表越多大型入侵事件

資料來源：

- Abuse.ch:Zeus Tracker - Binary URL
- Abuse.ch:SpyEye Tracker - Binary URL
- CleanMX - Malware
- Malc0de
- MalwareDomainList
- Sacour.cn

4 殭屍網絡

4.1 殭屍網絡控制中心 (C&C)

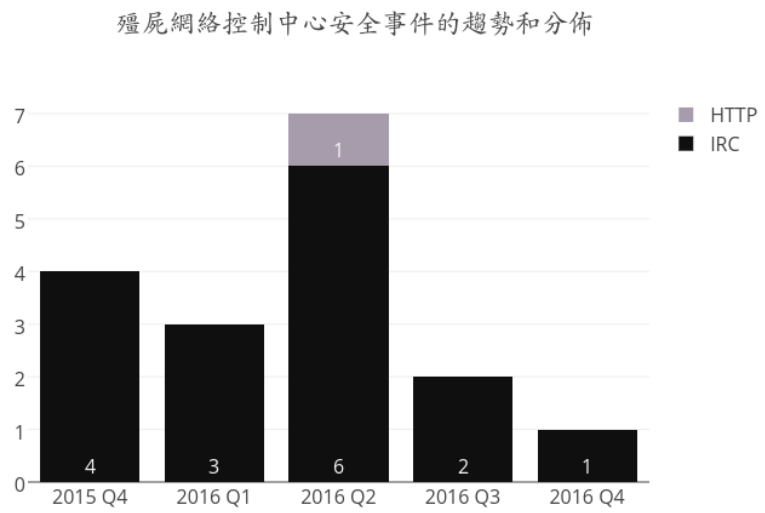

Figure 11: 殭屍網絡控制中心安全事件的趨勢和分佈

什麼是殭屍網絡控制中心?

- 殭屍網絡控制中心是網絡罪犯用來控制殭屍電腦的伺服器，通過發送命令來遙控殭屍電腦執行惡意活動，例如竊取個人信息財務信息和分散式阻斷服務攻擊。

有什麼潛在影響?

- 當很多殭屍電腦連接時，伺服器可能嚴重負荷。
- 伺服器可能收集到大量由殭屍電腦盜取的個人或財務數據。

資料來源:

- Zeus Tracker
- SpyEye Tracker
- Palevo Tracker
- Shadowserver - C&Cs

4.2 殭屍電腦

4.2.1 香港網絡內的主要殭屍網絡[9]

殭屍網絡的規模是計算在報告時間內，每天嘗試連接到殭屍網絡的唯一 IP 地址的總數的最大值。換句話說，因為不是所有殭屍電腦都一定在同一天開機，殭屍網絡的真實規模應該比所見的數字更大。

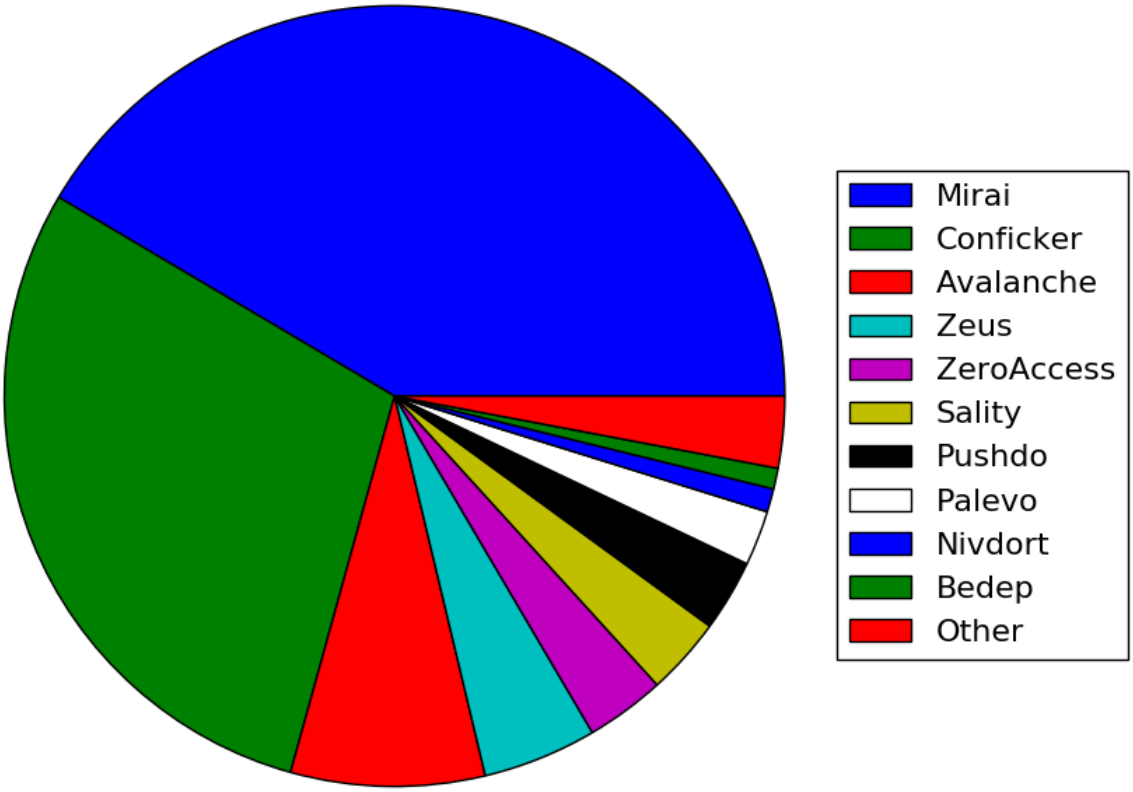

Figure 12: 香港網絡內的主要殭屍網絡

Table 2: 香港網絡內的主要殭屍網絡

排名	⇑⇓	殭屍網絡名稱	唯一 **IP** 地址	變化
1	NEW	Mirai	1932	NA
2	⇓	Conficker	1360	-6.9%
3	NEW	Avalanche	374	NA
4	⇓	Zeus	220	-21.7%
5	⇓	ZeroAccess	153	-13.1%
6	⇓	Sality	150	0.0%
7	⇓	Pushdo	138	-22.0%
8	→	Palevo	106	92.7%
9	⇓	Nivdort	45	-27.4%
10	⇓	Bedep	40	-16.7%

[9]主要殭屍網絡指殭屍網絡在報告時間內，透過資訊來源有可觀及持續穩定的數據。

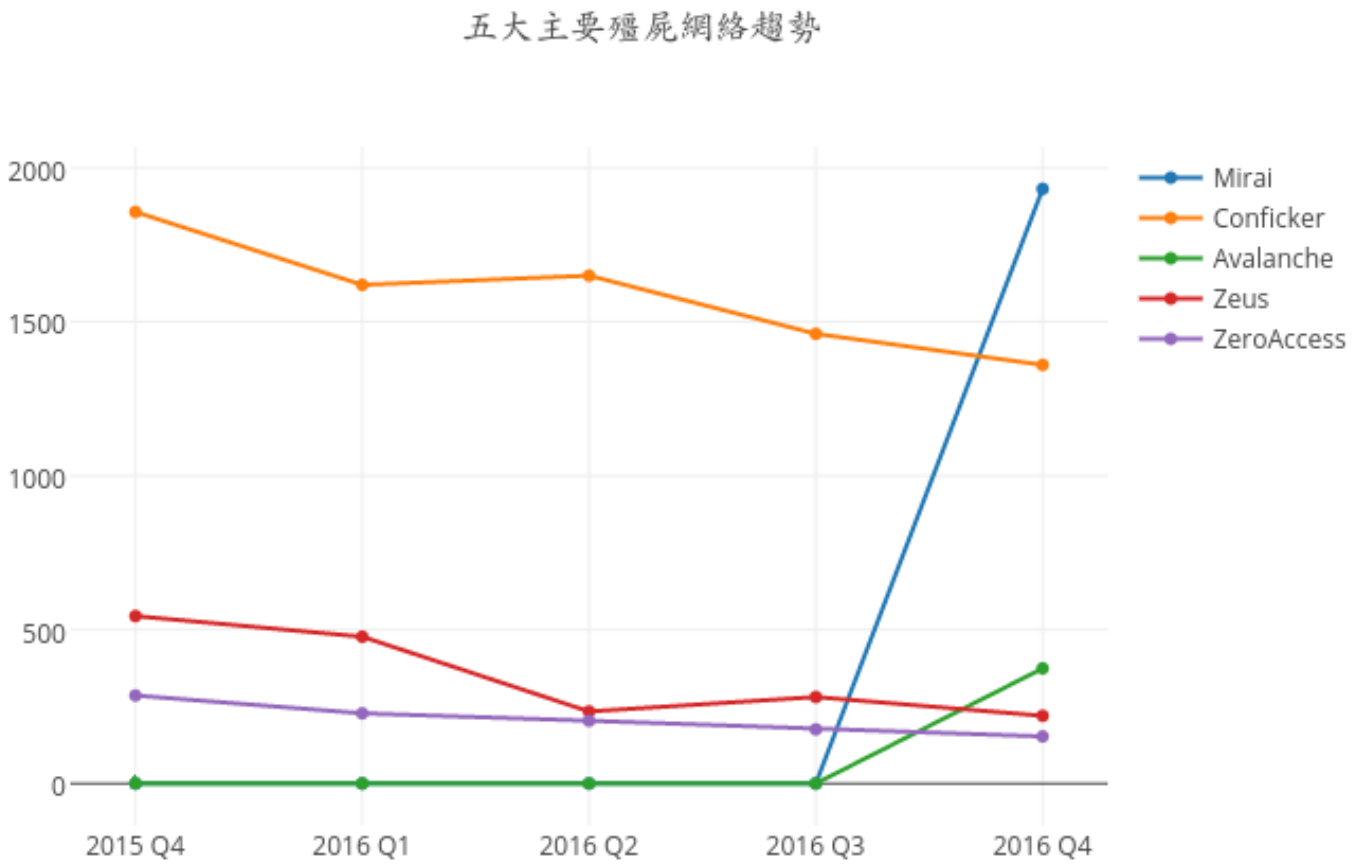

Figure 13: 五大主要殭屍網絡趨勢

Name	2015 Q4	2016 Q1	2016 Q2	2016 Q3	2016 Q4
Mirai	0	0	0	0	1932
Conficker	1857	1620	1650	1461	1360
Avalanche	0	0	0	0	374
Zeus	544	477	234	281	220
ZeroAccess	286	228	204	176	153

什麼是殭屍網絡?

- 殭屍網絡由一群殭屍電腦組成。殭屍電腦，大多數是一般的電腦，由於被惡意程式感染而成為殭屍電腦。當被感染後，惡意程式會用盡方法隱藏，並隱身連接到命令與控制服務器，得到黑客的指令，並進行攻擊。

有什麼潛在影響?

- 伺服器資源被佔用，並使用於犯罪活動上。
- 盜取個人資料被及導致金錢上損失
- 客的指令可能導致其他惡意活動，例如: 散播惡意程式和進行分散式阻斷服務攻擊 (DDoS)

資料來源：

- ArborNetwork - Atlas SRF - conficker
- ShadowServer - botnet_drone
- ShadowServer - sinkhole_http_drone
- Shadowserver - Microsoft_sinkhole

附錄

A 資料來源

以下是資料的來源:

以下是資料的來源:	資料來源	首次使用日期
網頁塗改	Zone - H	2013-04
網頁塗改	ArborNetwork: Atlas SRF-Phishing	2013-04
網頁塗改	CleanMX - Phishing	2013-04
網頁塗改	Millersmiles	2013-04
網頁塗改	Phishtank	2013-04
惡意程式寄存	Abuse.ch: Zeus Tracker - Binary URL	2013-04
惡意程式寄存	Abuse.ch: SpyEye Tracker - Binary URL	2013-04
惡意程式寄存	CleanMX - Malware	2013-04
惡意程式寄存	Malc0de	2013-04
惡意程式寄存	MalwareDomainList	2013-04
惡意程式寄存	Savour.cn	2013-04
殭屍網絡控制中心 (C&Cs)	Abuse.ch: Zeus Tracker - C&Cs	2013-04
殭屍網絡控制中心 (C&Cs)	Abuse.ch: SpyEye Tracker - C&Cs	2013-04
殭屍網絡控制中心 (C&Cs)	Abuse.ch: Palevo Tracker - C&Cs	2013-04
殭屍網絡控制中心 (C&Cs)	Shadowserver - C&Cs	2013-09
殭屍電腦	Arbor Network: Atlas SRF-Conficker	2013-08
殭屍電腦	Shadowserver - botnet_drone	2013-08
殭屍電腦	Shadowserver - sinkhole_http_drone	2013-08
Botnet (Bots)	Shadowserver - microsoft_sinkhole	2013-08

B 地理位置識別方法

我們採用以下方法去識別方網絡的地理位置是否香港。

方法名稱	最近更新日期
Maxmind	2017-1-14

C 主要殭屍網絡

Table 3: 主要殭屍網絡

主要殭屍網絡	別名	性質	感染方法	攻擊/影響
Avalanche	無	網絡犯罪包辦服務	視乎惡意軟件	• 發送垃圾郵件 • 寄存釣魚網站 • 寄存惡意程式 • 竊取敏感資訊
Bamital	無	木馬程式	• 利用「路過式下載」(drive-by-download) • 透過 P2P 網絡	• 點擊詐騙 • 搜尋劫持
BankPatch	MultiBanker Patcher BankPatcher	針對網上銀行的木馬程式	• 透過成人網站 • 有問題的多媒體編解碼器 • 垃圾電郵 • 即時通訊系統	監視特定的銀行網站並竊取用戶密碼、信用卡資料及其他敏感財務數據
Bedep	無	木馬程式	• 透過漏洞攻擊包 • 惡意廣告	• 點擊詐騙 • 下載其他惡意軟件
BlackEnergy	無	DDoS 木馬程式	• 以 rootkit 技術保持隱藏 • 使用流程注入技術 • 擁有強的加密技術和模塊化的架構	發動分散式阻斷服務攻擊 (DDoS)
Citadel	無	針對網上銀行的木馬程式	逃避及停止安全檢測工具	• 竊取銀行登入認證資料及敏感資料 • 按鍵記錄 • 截圖擷取 • 視訊擷取 • 瀏覽器中間人攻擊 • 勒索軟件
Conficker	Downadup Kido	蠕蟲	• 動態網域產生演算法 (DGA) 能力 • 通過 P2P 網絡進行通訊 • 停止安全檢測運行工具	• 利用 Window 伺服器服務漏洞 MS08-067 • 暴力破解管理員密碼，在網絡上傳播 • 利用 Window 自動 (auto-run)，透過外置磁碟機傳播

Table 4: 主要殭屍網絡

主要殭屍網絡	別名	性質	感染方法	攻擊/影響
Corebot	無	針對網上銀行的木馬程式	• 透過下載器	• 竊取敏感資訊 • 安裝其他惡意程式 • 後門程式, 允許未經授權的存取
Dyre	無	針對網上銀行的木馬程式	• 透過垃圾電郵	• 誘騙受害人致電詐騙電話號碼以竊取銀行登入認證資料 • 發送垃圾電郵
Gamarue	Andromeda	下載器/蠕蟲	• 透過漏洞攻擊包 • 透過垃圾電郵 • 微軟 Word 巨集 • 透過外置磁碟機	• 竊取敏感資訊 • 允許未經授權的存取 • 安裝其他惡意程式
Glupteba	無	木馬程式	利用「路過式下載」(drive-by-download)感染系統	• 推送內容關聯廣告 • 點擊劫持
IRC Botnet	無	木馬程式	通過 IRC 網絡進行通訊	• 後門程式，允許未經授權的存取 • 發動分散式阻斷服務攻擊 (DDoS) • 發送垃圾郵件
Mirai	無	蠕蟲	利用出廠密碼 telnet 連接	發動分敗式阻斷服務攻擊 (DDoS)
Nivdort	無	木馬程式	• 透過垃圾電郵	• 竊取登入認證資料及敏感資料
Nymaim	無	木馬程式	• 透過垃圾電郵	• 鎖定受害系統 • 令受害人無法存取檔案 • 勒索贖金
Palevo	• Rimecud • Butterfly bot • Pilleuz • Mariposa • Vaklik	蠕蟲	• 即時通訊系統, 點對點網絡及外置磁碟機	• 後門程式，允許未經授權的存取 • 竊取登入認證資料及敏感資料 • 利用洗黑錢手法直接用銀行竊取金錢

Table 5: 主要殭屍網絡

主要殭屍網絡	別名	性質	感染方法	攻擊/影響
Pushdo	• Cutwail • Pandex	下載器	• 隱藏惡意網絡流量 • 動態網域產生演算法 (DGA) 能力 • 利用「路過式下載」(drive-by-download)感染系統 • 利用瀏覽器和插件漏洞	• 下載其他針對網上銀行的惡意程式(例如: Zeus 和 Spyeye) • 發動分散式阻斷服務攻擊 (DDoS) • 發送垃圾郵件
Ramnit	無	蠕蟲	感染檔案 透過漏洞攻擊包 公期 FTP 伺服器	• 後門程式，允許未經授權的存取 • 竊取登入認證資料及敏感資料
Sality	無	木馬程式	• 以 rootkit 技術保持隱藏 • 通過 P2P 網絡進行通訊 • 透過外置磁碟機或共享傳播 • 停止安全檢測工具 • 使用多態性和遮蔽切入點（Entry Point Obscuring）技術來感染檔案	• 發送垃圾郵件 • 通信代理 • 竊取敏感資料 • 感染網絡伺服器和/或發佈計算任務來達到處理密集型任務目的（例如：破解密碼） • 下載其他惡意程式
Slenfbot	無	蠕蟲	透過外置磁碟機或共享傳播	• 後門程式，允許未經授權的存取 • 其他針對網上銀行的的惡意程式 • 發動分散式阻斷服務攻擊 (DDoS) • 發送垃圾郵件
Tinba	TinyBanker Zusy	針對網上銀行的木馬程式	• 透過漏洞攻擊包 • 透過垃圾電郵	竊取登入認證資料及敏感資料
Torpig	Sinowal Anserin	木馬程式	• 以 rootkit 技術保持隱藏 (Mebroot rootkit) • 動態網域產生演算法 (DGA) 能力 利用「路過式下載」(drive-by-download)	• 竊取敏感資料 • 瀏覽器中間人攻擊

Table 6: 主要殭屍網絡

主要殭屍網絡	別名	性質	感染方法	攻擊/影響
Virut	無	木馬程式	透過外置磁碟機或共享傳播	• 發送垃圾郵件 • 發動分散式阻斷 • 服務攻擊 (DDoS) • 詐騙 • 竊取資料
Wapomi	無	蠕蟲	• 透過外置磁碟機或共享傳播 • 感染可執行檔案	• 後門程式，允許未經授權的存取 • 下載其他惡意程式 • 改動重要檔案，導致系統不穩定 • 收集電腦活動數據，竊取個人資料，並令降低電腦效能
ZeroAccess	max++ Sirefef	木馬程式	• 以 rootkit 技術保持隱藏 • 通過 P2P 網絡進行通訊 • 利用「路過式下載」(drive-by-download)感染系統 • 偽裝成有效檔案 (例如: 多媒體檔案，keygen)	• 下載其他惡意程式 • 採礦比特幣和欺詐點擊
Zeus	Gameover	針對網上銀行的木馬程式	• 隱身技術 • 通過 P2P 網絡進行通訊 • 利用「路過式下載」(drive-by-download)感染系統	• 竊取銀行登入認證資料及敏感資料 • 瀏覽器中間人攻擊 • 按鍵記錄 • 下載其他惡意程式 (例如:Cryptolocker) • 發動分散式阻斷服務攻擊 (DDoS)