香港保安觀察報告

2013 年第四季度

前言

認知保安狀況 提高網絡安全

現今有很多「隱形」殭屍電腦， 在使用者還不知道的情況下，被攻擊者入侵及控制。這些電腦上的數據可能每天都被盜取及暴露，而電腦則被利用進行各種的犯罪活動。

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」，以便公眾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：

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

Table of Content 目錄

報告概要

本報告是 2013 年第四季季度報告。

在此期間共有 12,536 宗與香港有關的安全事件。數據是經 IFAS[1] 系統由 19 個來源[2]收集得來。它們並非來自 HKCERT 所收到的事故報告。

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:

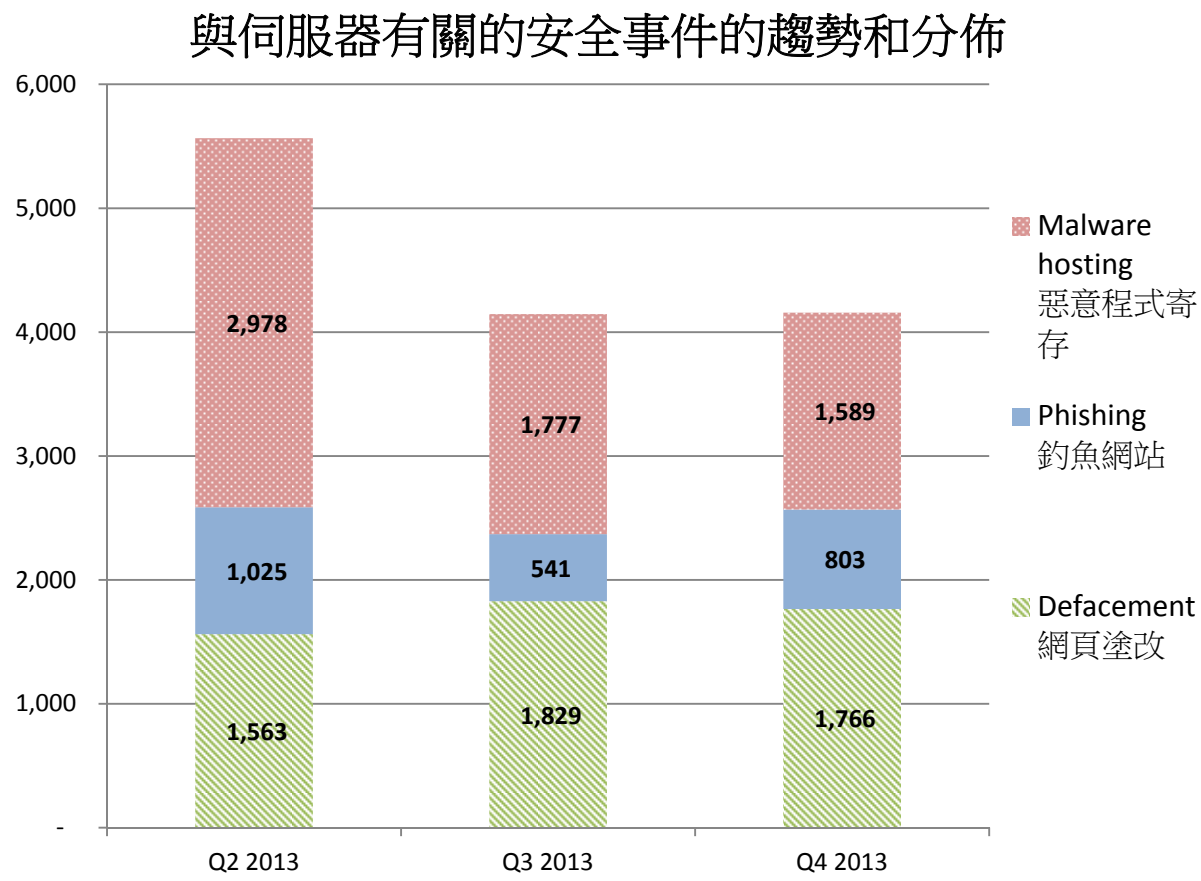


圖 1 – 與伺服器有關的安全事件的趨勢和分佈

[1] 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

[2] 參照附錄 1 -資料來源

有關伺服器的安全事件的數量，自 2013 年第三季開始下降，並在 2013 年第四季保持穩定。

惡意程式寄存安全事件的數量連續三個季度有下降趨勢。網頁塗改攻擊的數量在本季度與上季度相若，但相對於第一季的數量仍為略高。釣魚網站攻擊數量顯著在本季度增多，比較上季多出 48%。釣魚網站攻擊的數量在 2013 年 11 月和 12 月有明顯增多 (圖 2)，這很可能與年尾的節日，例如感恩節和聖誕節有關。當大量消費者在網上購買節日禮物時，網絡犯罪分子亦看準這個時機，設下大量的釣魚網站，以竊取消費者賬戶和憑證。

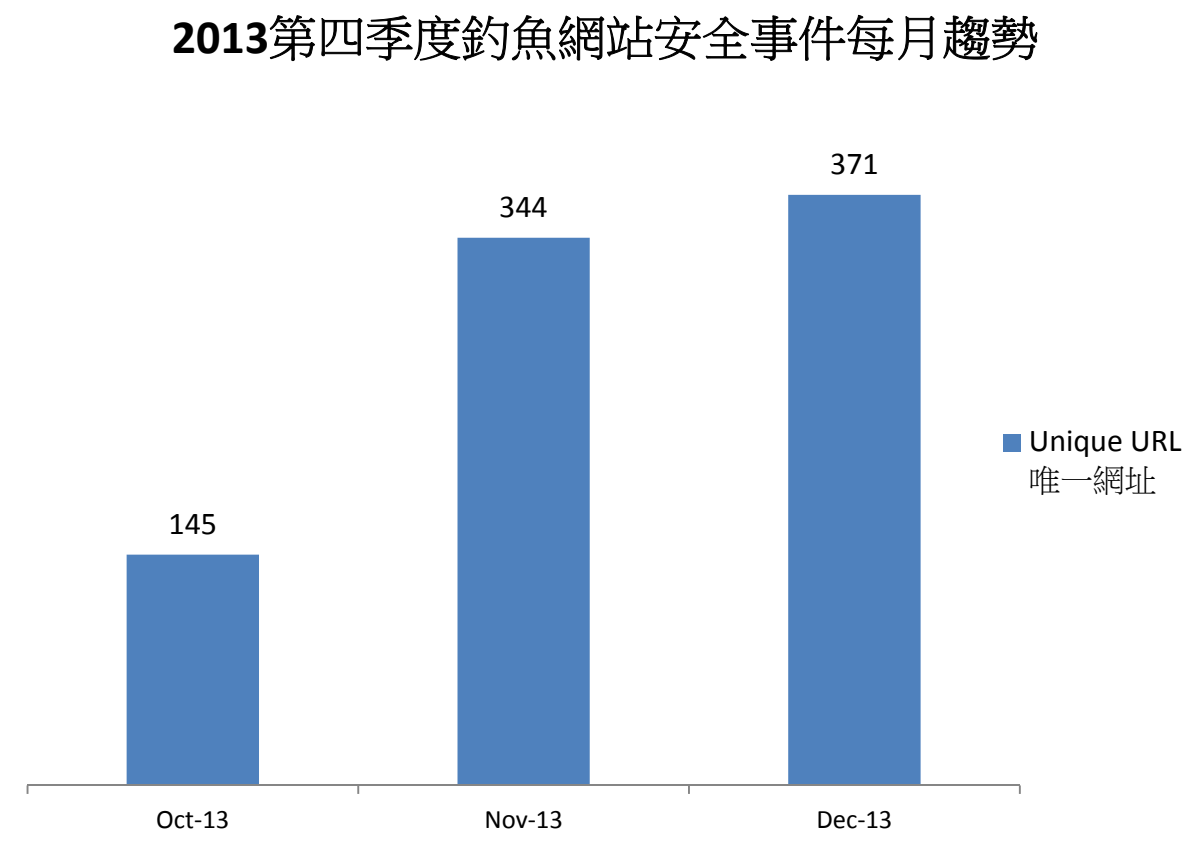


圖 2 - 2013 第四季度釣魚網站安全事件每月趨勢

由 HKCERT 以往處理有關伺服器的事故報告的經驗觀察到，大概 50%有關伺服器的事故報告，都是由於管理員都沒有好好管理其伺服器或應用程式，讓網絡犯罪分子有機可乘，利用漏洞入侵，使系統或應用程式成為他們犯罪的平台。

HKCERT 促請系統和應用程式管理員保護好伺服器

- 為伺服器安裝最新修補程式及更新，以避免已知漏洞被利用
- 更新網站應用程式和插件至最新版本
- 按照最佳實務守則來管理使用者帳戶和密碼
- 必須核實客戶在網上應用程式的輸入，及系統的輸出

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:

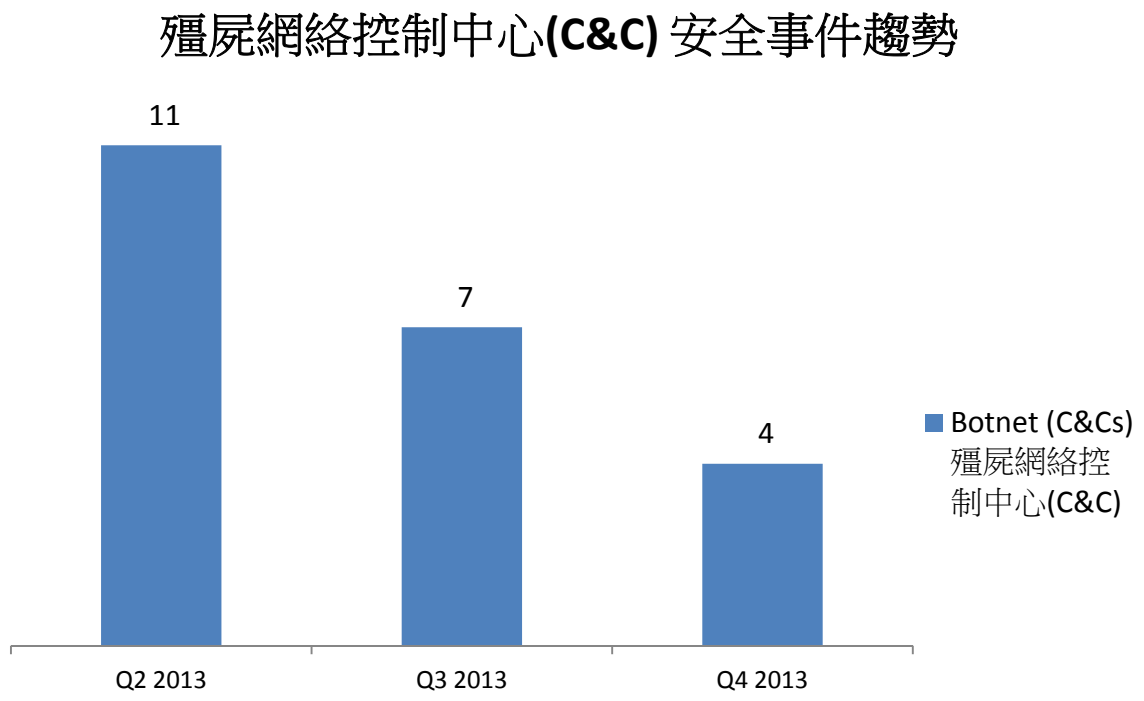


圖 3 – 殭屍網絡控制中心(C&C)安全事件的趨勢

殭屍網絡控制中心的數字連續三個季度都有減少。

本季有 4 個殭屍網絡控制中心的報告。其中兩個被確定為 Zeus 的殭屍網絡控制中心，另外兩個是 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:

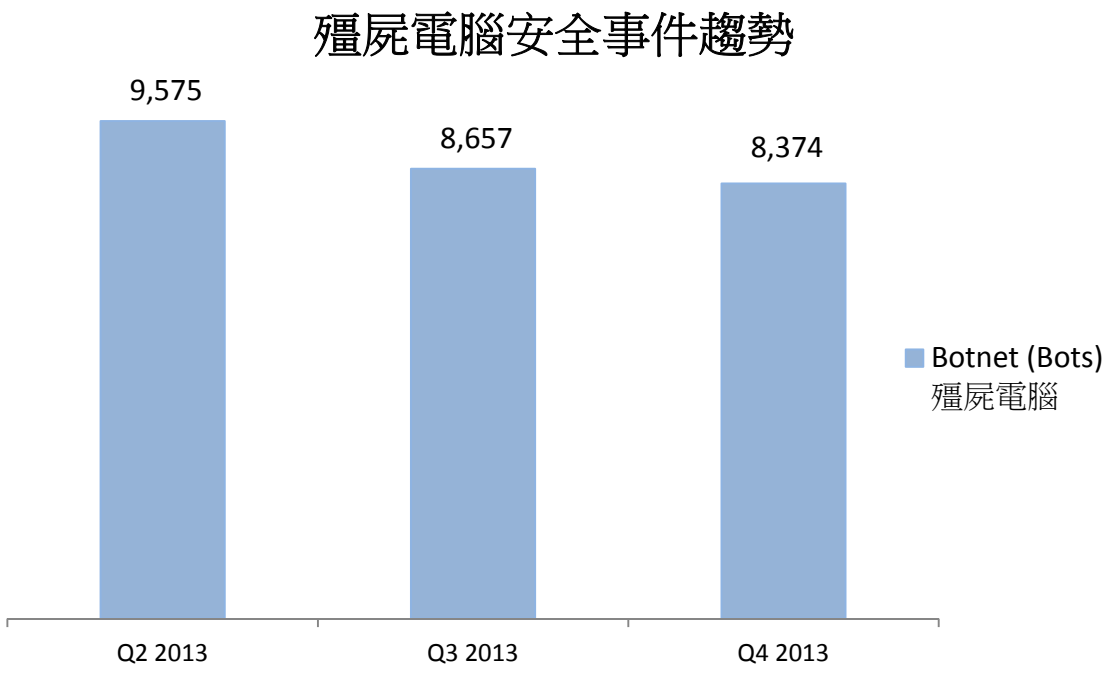


圖 4 -殭屍電腦安全事件的趨勢

殭屍電腦安全事件連續三個季度都有減少。

在 2013 年第四季，Conficker 是香港最多的殭屍電腦，一共有 3,175 部電腦被感染。此數字指在 2013 年第四季，感染 Conficker 的電腦在線最多的一天，一共有 3,175 部。Conficker 自 2008 年被發現以來，感染率仍然很高。其中原因可能是用戶未有為系統安裝修補程式，或是在使用盜版的 Windows 系統以致無法更新修補程式，而且沒有安裝有效的保安防護工具。一些研究顯示，針對身份認證的攻擊是 Conficker 最常用的攻擊方法，其次是利用 Window 系統漏洞和自動運行(auto-run)[3]。微軟安全研究報告（SIR）第 12 卷指出，透過破解管理員密碼入侵系統的共佔了 54%至 89%，透過的 Window 系統漏洞來入侵系統的只佔 19%至 43%，而透過自動運行來入侵系統的只佔 1%- 11%。Conficker 具備了一個小字典，用來進行暴力攻擊以破解管理員密碼，然後進一步在網絡上傳播到其他的電腦。

[3]據微軟安全情報報告（SIR），第 12 卷，出版日期 2011 年 12 月，針對身份認證的攻擊佔 54%至 89%，透過的 Window 系統漏洞來入侵系統的只佔 19%至 43%，而透過自動運行來入侵系統的亦只佔 1%- 11%。(http://www.microsoft.com/security/sir/archive/default.aspx)

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
- 在 Windows 系統停用自動運行功能[4]
- 停止使用盜版的 Windows 系統，多媒體檔案及軟件
- 注意 Windows XP 的支援將在 2014 年 4 月結束，須把操作系統更新/升級，保證繼續有安全更新的支援

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

[4]如何在 Windows 中更正「停用自動執行登錄機碼」增強功能, Microsoft, Knowledge Base
http://support.microsoft.com/kb/967715/zh-tw

1. 網頁塗改

1.1 數據統計

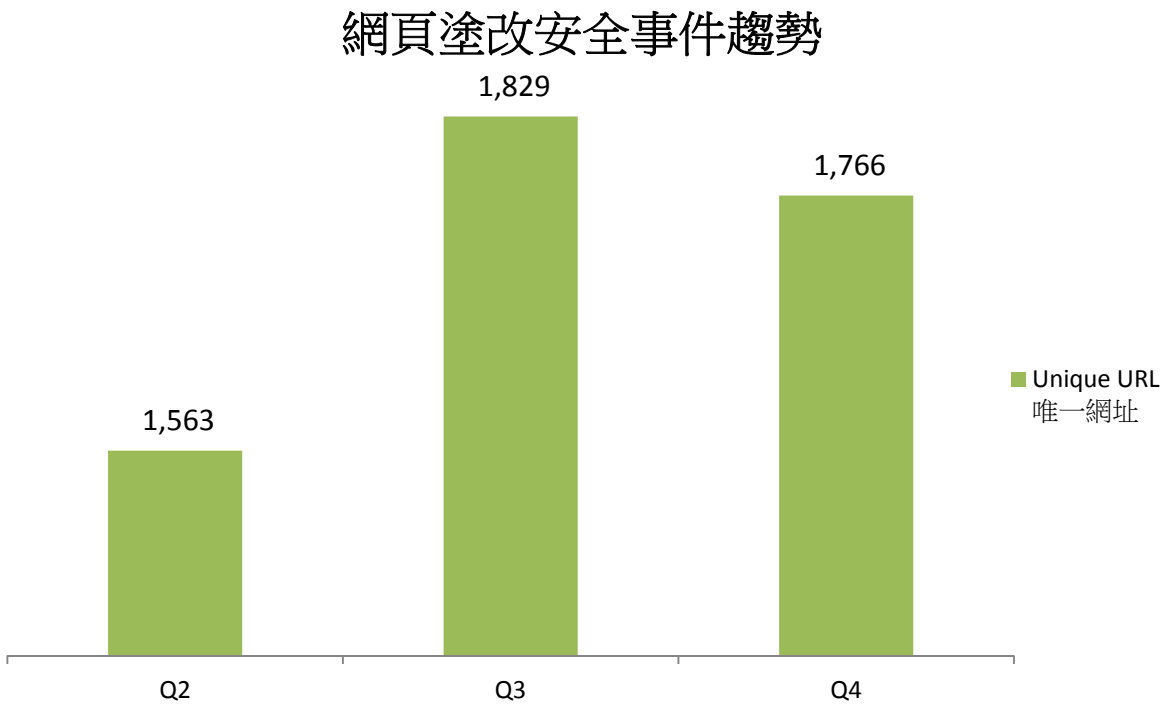


圖 5 – 網頁塗改全事件趨勢

	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

資料來源:

- Zone-H

2. 釣魚網站

2.1 數據統計

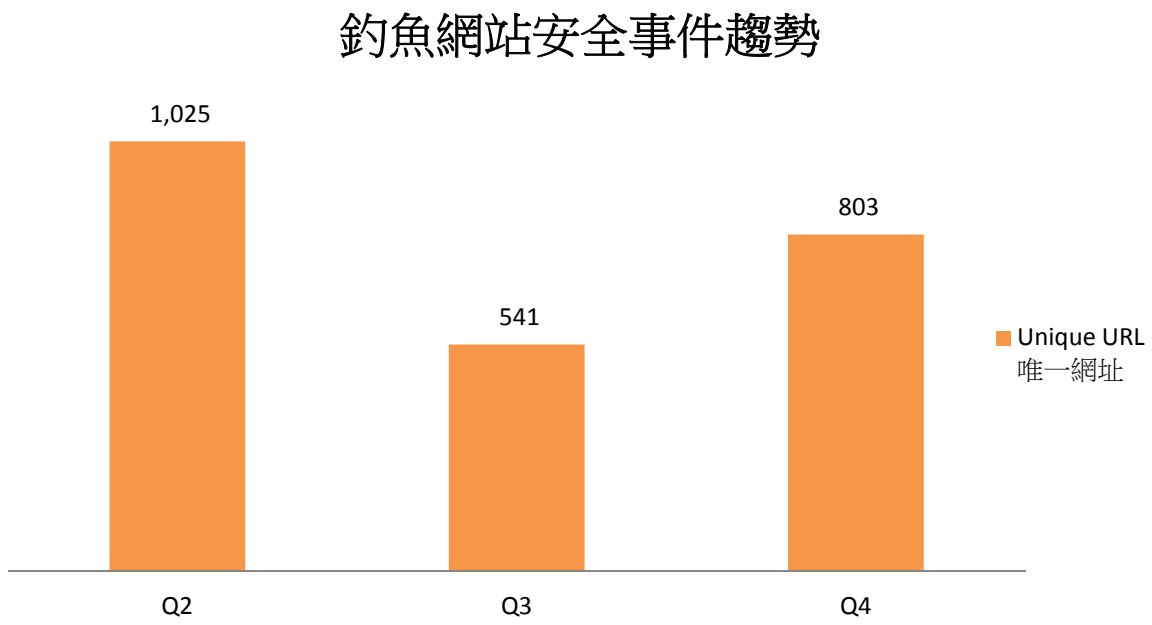


圖 6 – 釣魚網站安全事件趨勢

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。

資料來源:

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

3. 惡意程式寄存

3.1 數據統計

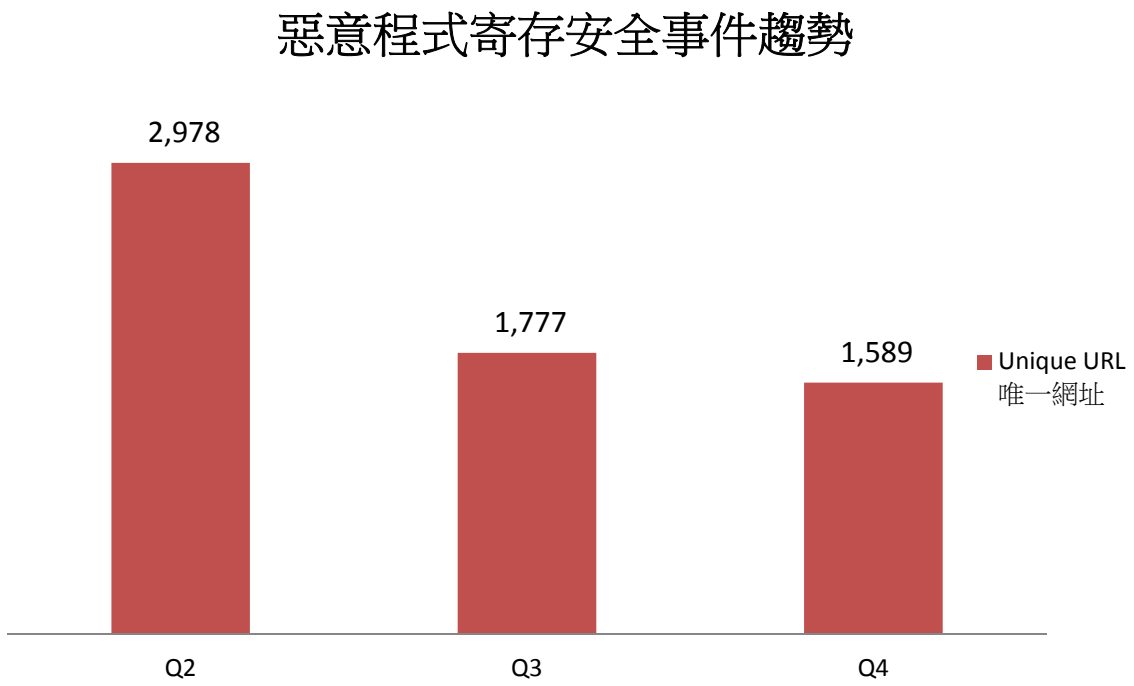


圖 7 – 惡意程式寄存安全事件趨勢

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。

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)

4.1.1 香港網絡內的主要殭屍網絡控制中心(C&C)

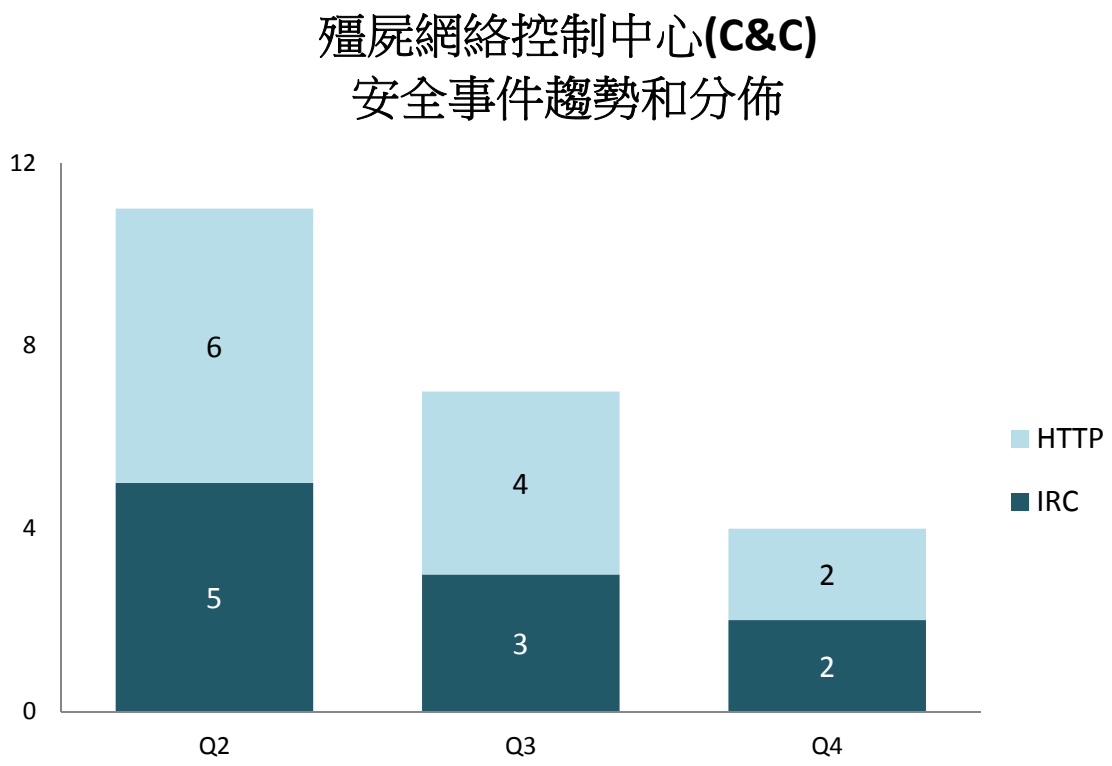


圖 8 – 殭屍網絡(控制中心)安全事件的趨勢和分佈

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。

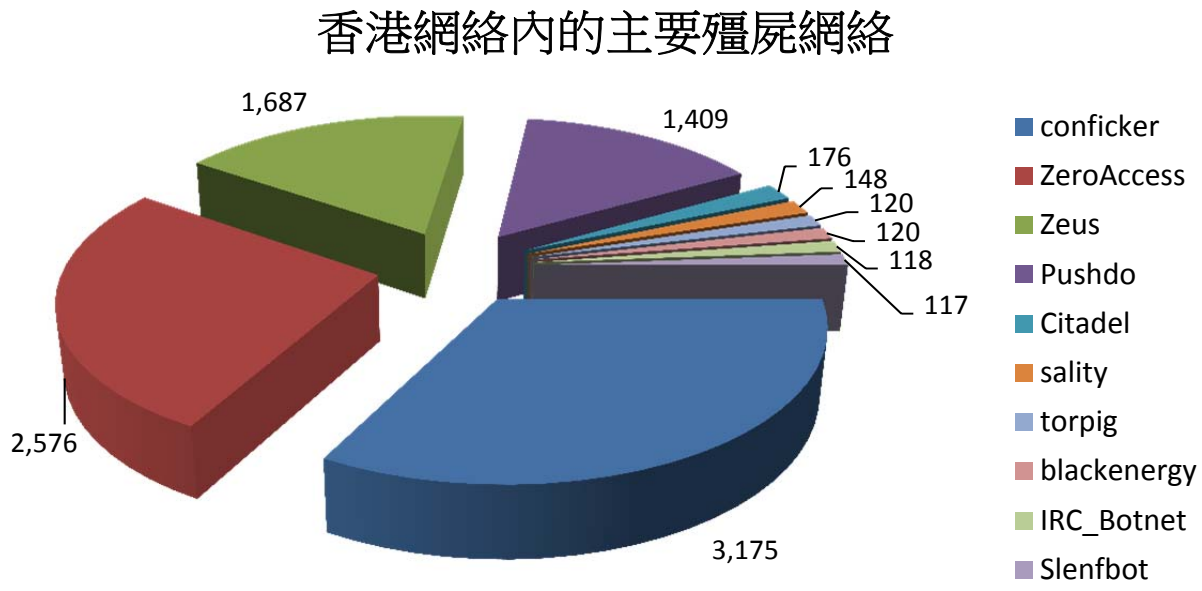
資料來源:

- 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[5]

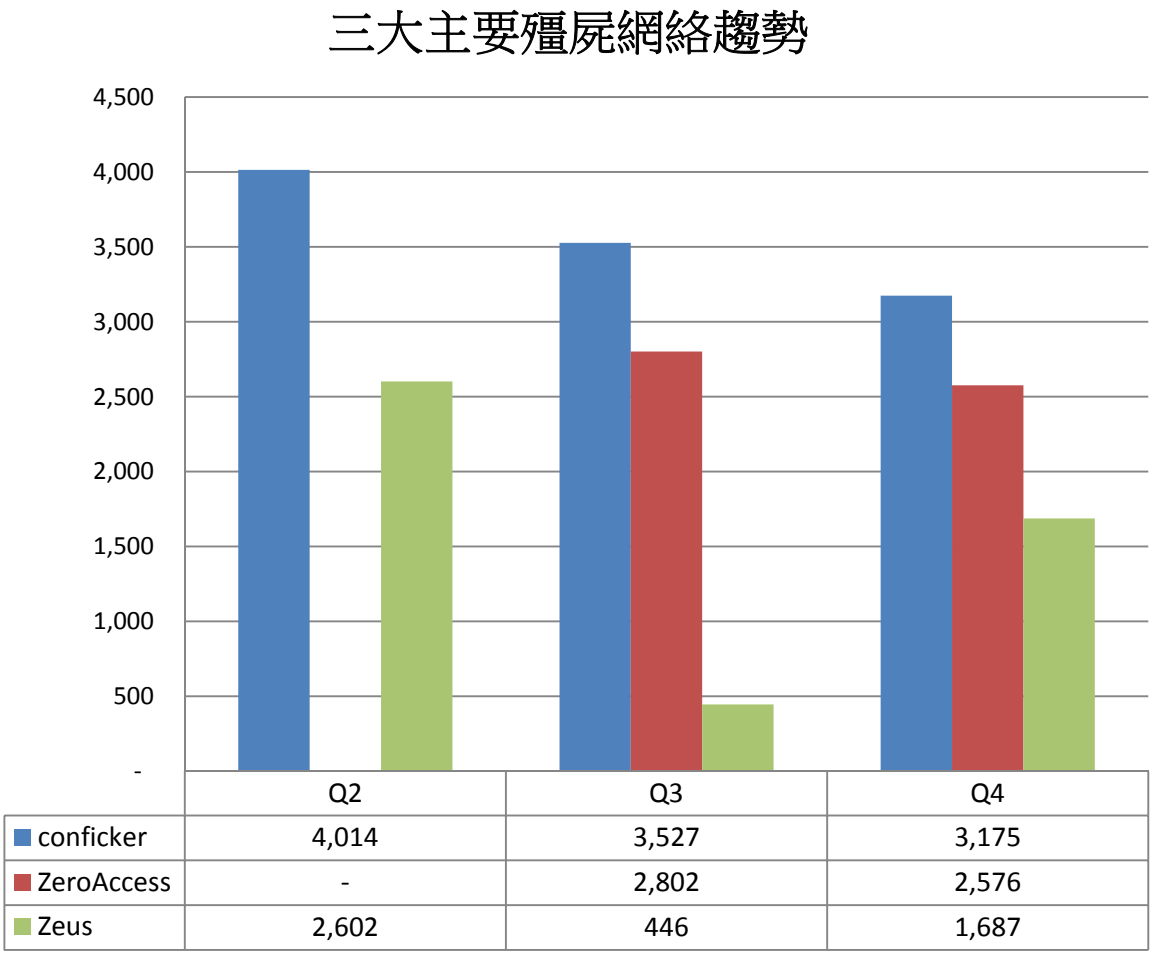
殭屍網絡的規模是計算在報告時間內，每天嘗試連接到殭屍網絡的唯一 IP 地址的總數的最大值。換句話說，因為不是所有殭屍電腦都一定在同一天開機，殭屍網絡的真實規模應該比所見的數字更大。



排名	殭屍網絡名稱	唯一 IP (本季每天內最高數字)
1	conficker	3,175
2	ZeroAccess	2,576
3	Zeus	1,687
4	Pushdo	1,409
5	Citadel	176
6	sality	148
7	torpig	120
8	blackenergy	120
9	IRC_Botnet	118
10	Slenfbot	117

圖 9 – 香港網絡內的主要殭屍網絡的殭屍電腦數量

[5]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。



	Q2	Q3	Q4
conficker	4,014	3,527	3,175
ZeroAccess	-	2,802	2,576
Zeus	2,602	446	1,687

圖 10 -三大主要殭屍網絡趨勢

*注意: 有關 ZeroAccess 的感染數據自 2013 年第三季才穩定，因此未能與 2013 年第二季作直接比較。

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，由於被惡意軟件感染而成為殭屍電腦。當被感染後，惡意軟件會用盡方法隱藏，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。
- 黑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

附錄 1 – 資料來源

以下是資料的來源:

網絡攻擊類別	資料來源	首次使用日期
網頁塗改	Zone - H	2013-04
釣魚網站	ArborNetwork: Atlas SRF-Phishing	2013-04
釣魚網站	CleanMX – Phishing	2013-04
釣魚網站	Millersmiles	2013-04
釣魚網站	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	Sacour.cn	2013-04
殭屍網絡控制中心(C&C)	Abuse.ch: Zeus Tracker – C&Cs	2013-04
殭屍網絡控制中心(C&C)	Abuse.ch: SpyEye Tracker – C&Cs	2013-04
殭屍網絡控制中心(C&C)	Abuse.ch: Palevo Tracker – C&Cs	2013-04
殭屍網絡控制中心(C&C)	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
殭屍電腦	Shadowserver - microsoft_sinkhole	2013-08

附錄 2 – 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	2013-10-29

附錄 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
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 自動運行 (auto-run)，透過外置磁碟機傳播
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

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的惡意軟件(例如: Zeus 和 Spyeye) • 發動分散式阻斷服務攻擊(DDoS) • 發送垃圾郵件
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） • 下載其他惡意軟件
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軟件 • 發動分散式阻斷服務攻擊(DDoS) • 發送垃圾郵件
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)感染系統	• 竊取敏感資料 • 瀏覽器中間人攻擊
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)	• 下載其他惡意軟件 • 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 • 利用「路過式下載」(drive-by-download)感染系統 • 通過 P2P 網絡進行通訊	• 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 • 下載其他惡意軟件(例如: Cryptolocker) • 發動分散式阻斷服務攻擊(DDoS)