
# 香港保安觀察報告

## 2019 第四季度

發佈日期: 2020 年 1 月 31 日
最後更新日期: 2020 年 4 月 29 日

# 更正啟示

本中心於初版報告中漏報了 Nymaim，Virut，ZeroAccess，Pushdo，Nivdort，Bedep 和 Core-bot 殭屍電腦的安全事件數量，引致以下內容出錯：

- 於表 2 和圖 4 中，將殭屍電腦安全事件的總數 7,878，誤算為 6,831。
- 於圖 12 和表 3 的主要殭屍網絡數量中，漏報了排名第 3 的 786 宗 Nynaim 安全事件，和排名第 6 的 175 宗 Virut 安全事件。
- Nynaim 的季度數量足以讓其擠身五大主要殭屍網絡之中 (圖 13 和表 4)。

謹此更正。

# 前言

## 掌握狀況提高網絡安全

現今，有很多具備上網功能的數碼設備 (例如個人電腦、智能手機、平板裝置等)，在用戶不知情下被入侵，令儲存在這些設備內的數據，每天要面對被盜取和洩漏，及可能被用於進行不同形式的犯罪活動的風險。

《香港保安觀察報告》旨在提高公眾對香港被入侵系統狀況的認知，從而作出更好的資訊保安選擇。這份季度報告提供的數據聚焦在被發現曾經遭受或參與各類型網絡攻擊活動 [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] 的香港系統，其定義為處於香港網絡內，或其主機名稱的頂級域名是「.hk」或「. 香港」的系統。

## 善用全球保安資訊力量

本報告是香港電腦保安事故協調中心 (HKCERT) 和全球各地資訊保安研究人員共同合作的成果。很多資訊保安研究人員具有偵測針對他們或其客戶攻擊的能力，有些會把攻擊來源的可疑 IP 地址或惡意活動網絡連結的數據資料收集起來，並提供給其他資訊保安機構，以改善互聯網的整體安全。他們會遵守良好的作業守則，在分享數據前，先刪除個人身份資料。

HKCERT 建立 Information Feed Analysis System (IFAS) 系統，收集和匯聚這些的數據，對有關香港的資料進行分析。數據的來源 (附錄 1) 廣泛和可靠，可以持平地反映香港的資訊保安情況。

HKCERT 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：

表 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。 |

## 更好的資訊帶來更好的服務

HKCERT 將來會加入更多有價值的數據來源以進行更深入的分析，持續改善報告內容，亦會探討如何最有效利用這些數據提升 HKCERT 的服務。請以電郵（***hkcert@hkcert.org***）反饋閣下的意見。

### 報告的局限

本報告的數據來自多個途徑，他們有不同的來源、收集週期和表達方式，各自亦存有局限，因此數據只宜作為參考，不宜用作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

# 目錄

# 報告概要

2019 第四季度，有關香港的唯一的網絡攻擊數據共有 9,911 個。數據是從 IFAS[1]系統的 11 個來源收集所得[2]，而並不是來自 HKCERT 所接獲的事故報告。

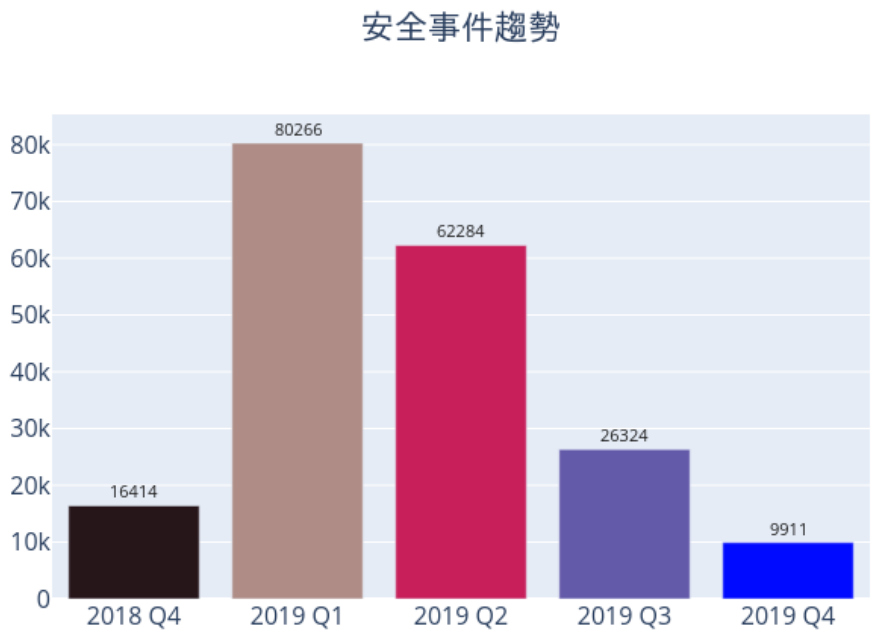


圖 1: 安全事件趨勢

表 2: 安全事件趨勢

| 事件類別 | 2018 Q4 | 2019 Q1 | 2019 Q2 | 2019 Q3 | 2019 Q4 |
|---|---|---|---|---|---|
| 網頁塗改 | 590 | 318 | 532 | 1,120 | 591 |
| 釣魚網站 | 365 | 289 | 1,306 | 849 | 257 |
| 惡意程式寄存 | 8,152 | 72,201 | 48,892 | 17,273 | 1,185 |
| 殭屍網絡（殭屍電腦） | 7,307 | 7,458 | 11,554 | 7,078 | 7,878 |
| 殭屍網絡控制中心 (C2) | 0 | 0 | 0 | 4 | 0 |

去到 2019 年最後一季，各項的保安事故皆回落到較低水平，本季度共有 9,911 宗安全事故，較上一季減少接近三分之二。其中以惡意程式寄存事件的跌幅最明顯，下跌了超過 93%，而釣魚網站事件同樣錄得七成的跌幅。

[1]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
[2]請參考附錄 A: 資料來源

# 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:

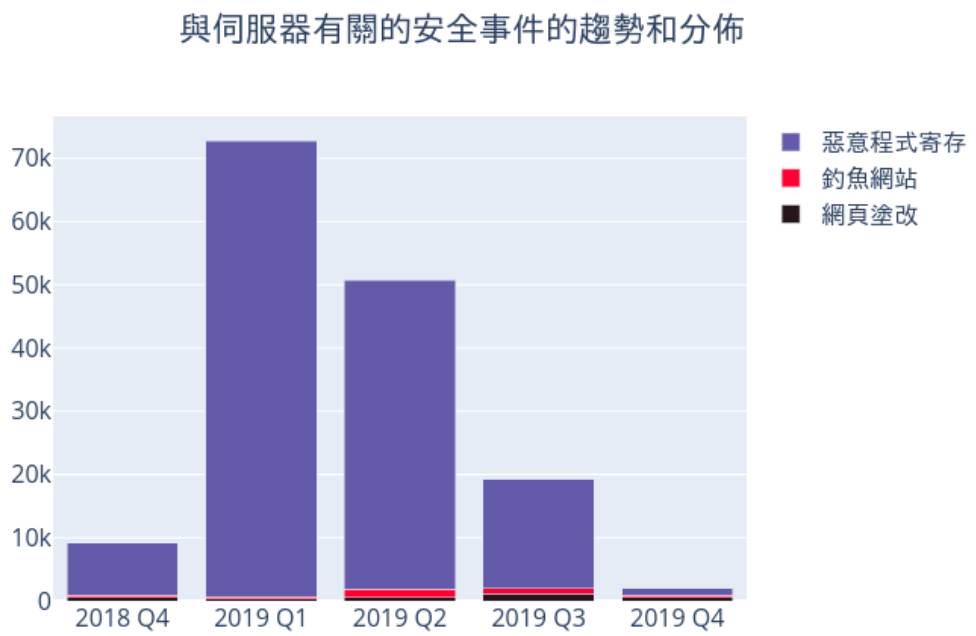


圖 2: 與伺服器有關的安全事件的趨勢和分佈

表 2 顯示，惡意程式寄存事件的總數在 2019 年第一季升到 72,201 宗的高位後，持續回落至本年度的最低，僅 1,185 宗；與此同時，所涉及的惡意程式寄存 IP 地址的數目亦大幅下跌至 63 個 (見圖 9)，是自 2018 年第一季以來，首次錄得雙位數字。
釣魚網站事件亦有近 600 宗的跌幅，而所涉及的釣魚網站事件 IP 地址數目同時從上一季的 196 個減少至 55 個 (見圖 7)。經分析數據後，可發現這些釣魚攻擊除主要針對 Apple iCloud 外，針對 eBay 的釣魚事件亦相對增加，當中有機會是由於年末為購物的熱門季節，黑客會增加對著名的網上購物平台品進行釣魚攻擊。

本季的網頁塗改事件和所涉及的 IP 地址分別下跌近一半和 36%。利用 Zone-H 和 Shodan[3]進行更深入的分析後，發現這些 IP 地址的所屬伺服器當中，約四分之一仍存在保安漏洞，部分更使用已終止支援服務 (EOS) 的作業系統，相信是導致網頁塗改事故的主因。

*HKCERT* 促請系統和應用程式管理員加強保護伺服器

- 避免黑客入侵已知漏洞，為伺服器安裝最新修補程式及更新
- 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
- 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攻擊

[3]Shodan 是一個針對互聯網連接設備的搜索引擎: https://www.shodan.io/

# 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，受影響的主要是個人電腦。

## 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:

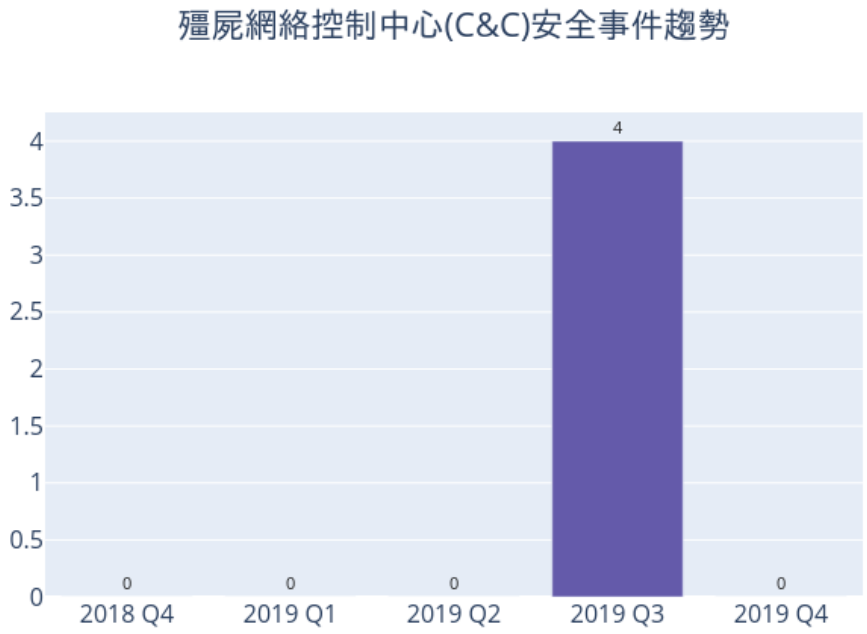


圖 3: 殭屍網絡控制中心 (C&C) 安全事件的趨勢

今季未有接獲殭屍網絡控制中心的事件報告。

## 殭屍電腦安全事件

以下為殭屍網絡（殭屍電腦）安全事件的趨勢:

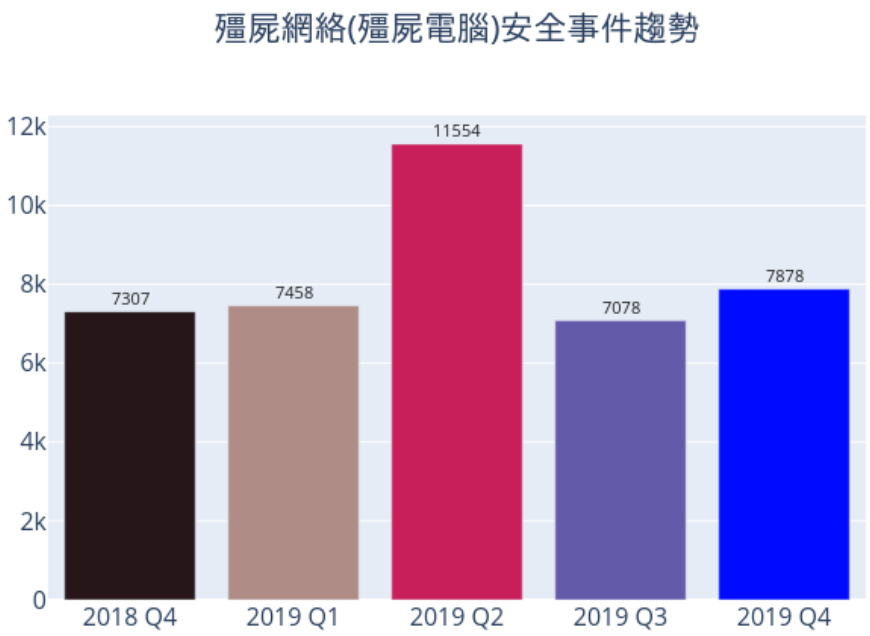


圖 4: 殭屍電腦安全事件的趨勢

香港網絡內的殭屍網絡（殭屍電腦）在 2019 年第四季度上升了 11.3%，800 宗。雖然大部分的事件都呈跌勢，當中更以 WannaCry 的跌幅最明顯，下降一半，達 354 宗，但 Nymaim 及 Avalanche 則有明顯增加，分別上升了 6 倍和 3 倍以上（見表 3）。Avalanche 為一個服務多種惡意軟件家族的網絡犯罪寄存平台，黑客可利用該平台發送各式各樣的惡意軟件（如 Nymaim、Gamarue、Tinba 和 Matsnu 等）。經分析後，發現由十一月底至十二月試圖連接到 Avalanche sinkhole 的唯一 IP 數量持續偏高，與 Nymaim sinkhole 所顯示的升幅趨勢一致。此外，比對前三季 Avalanche 的數據，惡意軟件 Nymaim 和 Matsnu 的升幅最為明顯，兩者皆為木馬程式，並有機會被用作發動勒索軟件攻擊的跳板。

*HKCERT* 促請使用者採取以下措施，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
- 不要使用盜版的 Windows 系統，多媒體檔案及軟件
- 不要使用沒有安全更新的 Windows 系統及軟件

自 2013 年 6 月，本中心一直跟進接獲的保安事故，並主動接觸本地互聯網供應商以清除殭屍網絡。清除殭屍網絡的行動仍在進行，針對幾個主要的殭屍網絡家族，包括 Avalanche, Pushdo, Citadel, Ramnit, ZeroAccess, GameOver Zeus, VPNFilter 及 Mirai。
HKCERT 呼籲一般用戶加入清除殭屍網絡行動，確保個人電腦並沒有被惡意程式控制或受感染，保護個人資料以提高互聯網的安全性。

使用者可根據 *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

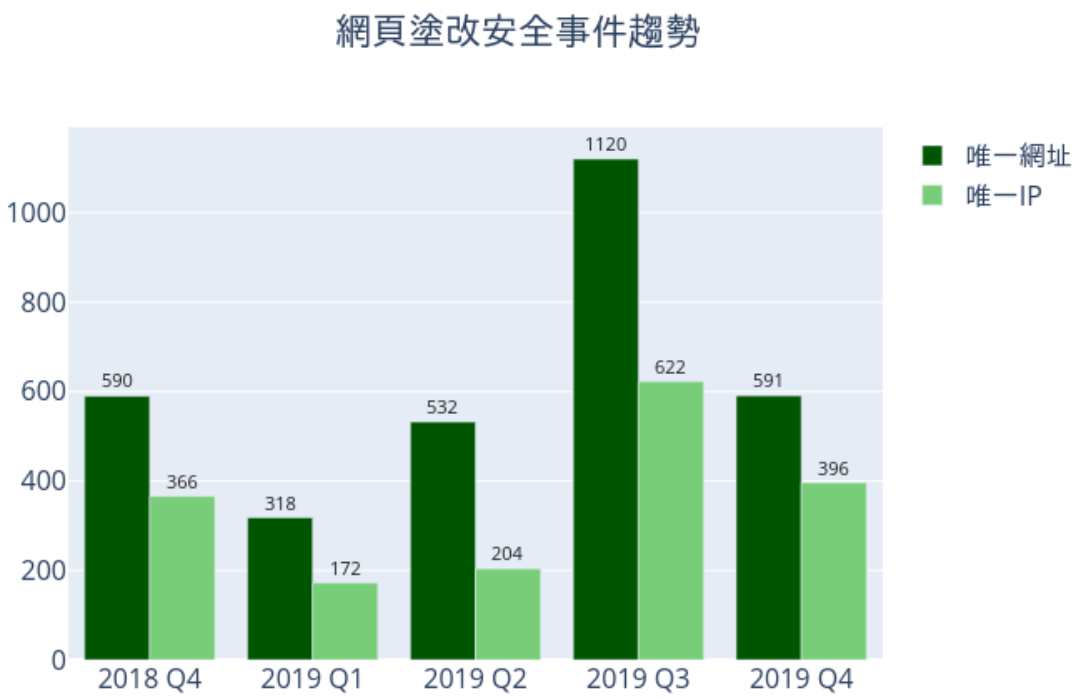


圖 5: 網頁塗改安全事件趨勢

甚麼是網頁塗改?

- 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。

有甚麼潛在影響？

- 破壞網站原本內容
- 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


圖 6: 網頁塗改全事件唯一網址/IP 比率

甚麼是唯一網址/IP 比率？

- 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，更能反映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

# 2 釣魚網站

## 2.1 數據統計

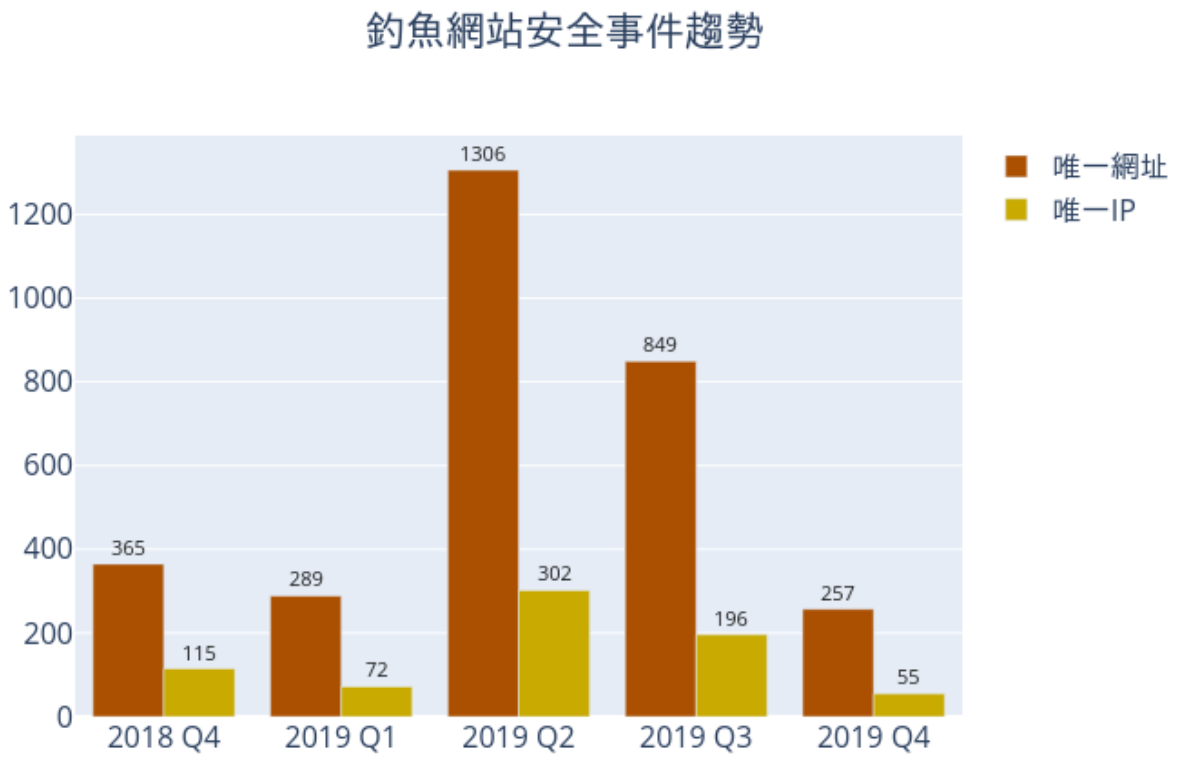


圖 7: 釣魚網站安全事件趨勢

甚麼是釣魚網站?

- 釣魚網站是冒充一個合法網站，以達到詐騙的目的。

有甚麼潛在影響？

- 訪客的個人資料可能被盜取，而導致金錢上的損失。
- 不能存取網站原來的內容
- 合法網站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。

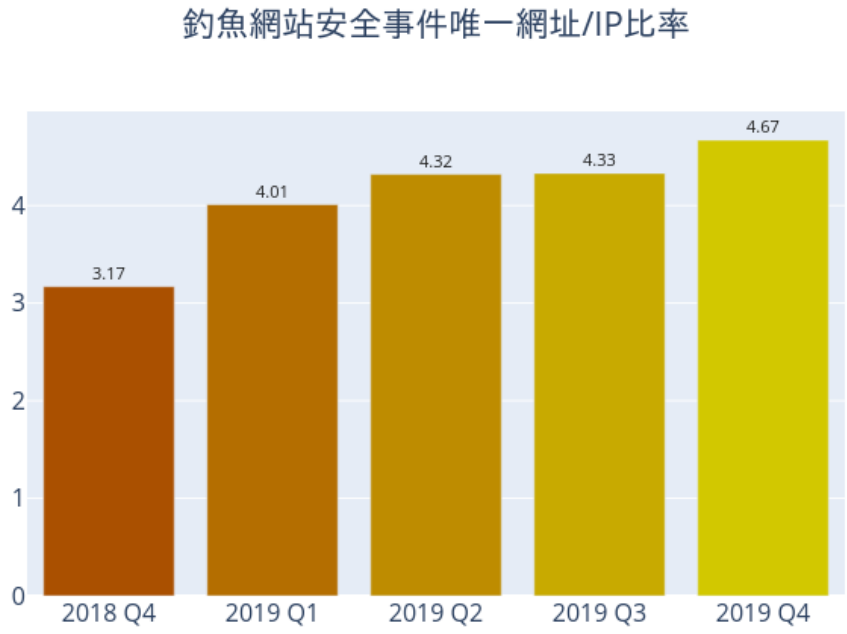


圖 8: 釣魚網站安全事件唯一網址/IP 比率

甚麼是唯一網址/IP 比率？

- 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，更能反映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：

- CleanMX - phishing
- Phishtank

# 3 惡意程式寄存

## 3.1 數據統計

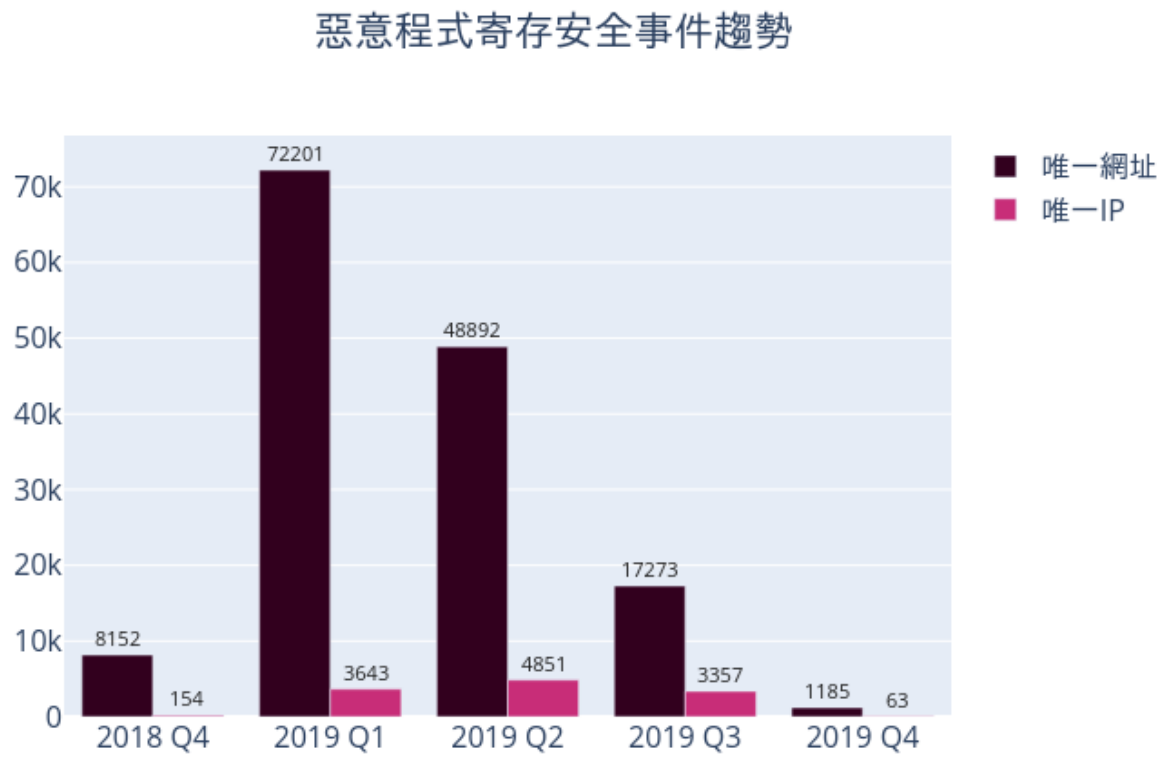


圖 9: 惡意程式寄存安全事件趨勢

甚麼是惡意程式寄存?

- 惡意程式寄存是透過網站散播惡意程式

有甚麼潛在影響？

- 訪客可能下載及安裝惡意程式，或執行網頁的惡意程式碼，導致其裝置被黑客入侵
- 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，用作其他攻擊或犯罪活動

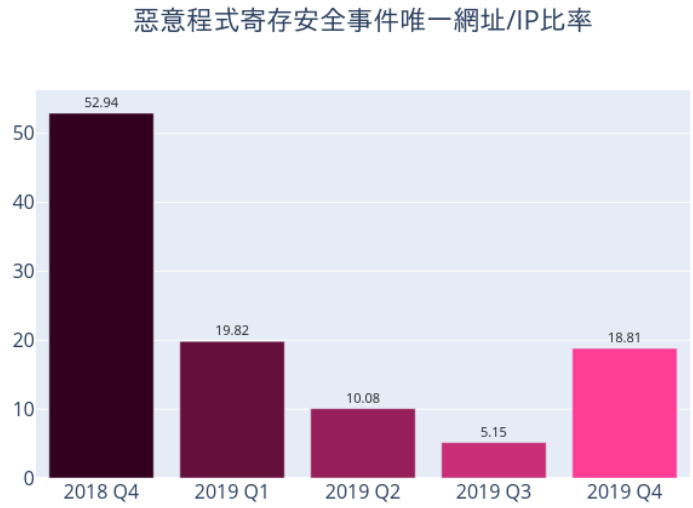


圖 10: 惡意程式寄存安全事件唯一網址/IP 比率

甚麼是唯一網址/IP 比率？

- 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

比率能反映甚麼？

- 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，更能反映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
- CleanMX - Malware
- Malc0de
- MalwareDomainList

# 4 殭屍網絡

## 4.1 殭屍網絡控制中心 (C&C)

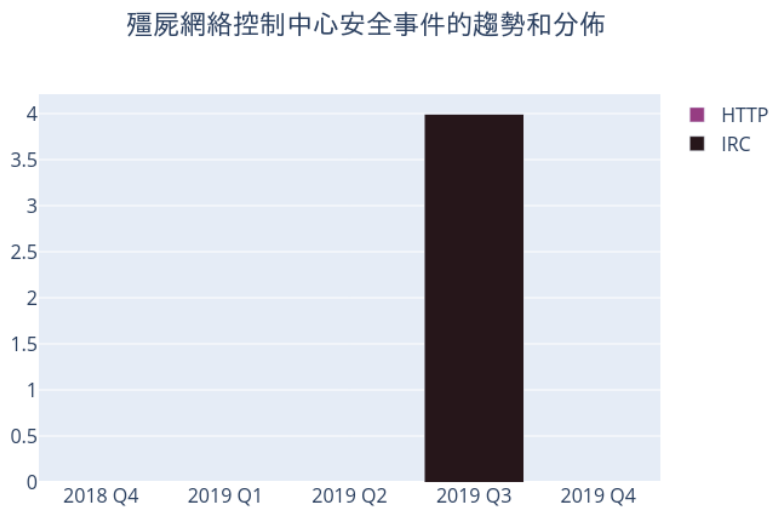


圖 11: 殭屍網絡控制中心安全事件的趨勢和分佈

甚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

有甚麼潛在影響？

- 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：

- Shadowserver - C&Cs

## 4.2 殭屍電腦

### 4.2.1 香港網絡內的主要殭屍網絡

主要殭屍網絡指在報告時間內，透過資訊來源有可觀及持續穩定的數據。
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 地址總數的最大值。換而言之，由於不是所有殭屍電腦都一定在同一天開機，因此殭屍網絡的真實規模應該比所見的數字更大。

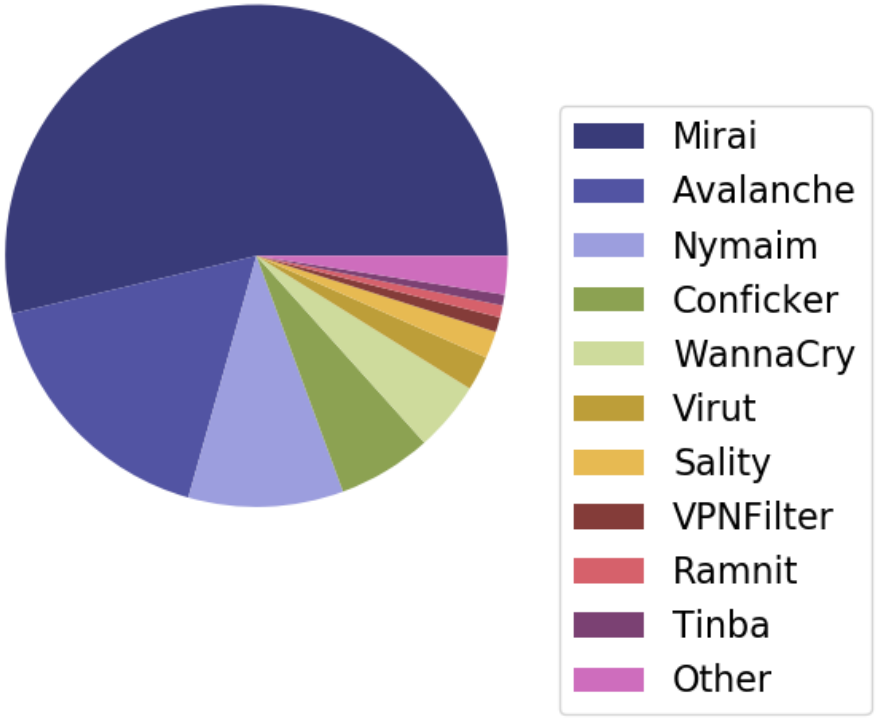


圖 12: 香港網絡內的主要殭屍網絡

表 3: 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 | → | Mirai | 4231 | -7.9% |
| 2 | ⇑ | Avalanche | 1333 | 381.2% |
| 3 | ⇑ | Nymaim | 786 | 614.5% |
| 4 | ⇓ | Conficker | 476 | -6.3% |
| 5 | ⇓ | WannaCry | 354 | -49.2% |
| 6 | ⇓ | Virut | 175 | -47.3% |
| 7 | ⇓ | Sality | 137 | -7.4% |
| 8 | → | VPNFilter | 75 | -6.2% |
| 9 | ⇑ | Ramnit | 61 | 24.5% |
| 10 | ⇓ | Tinba | 55 | -9.8% |

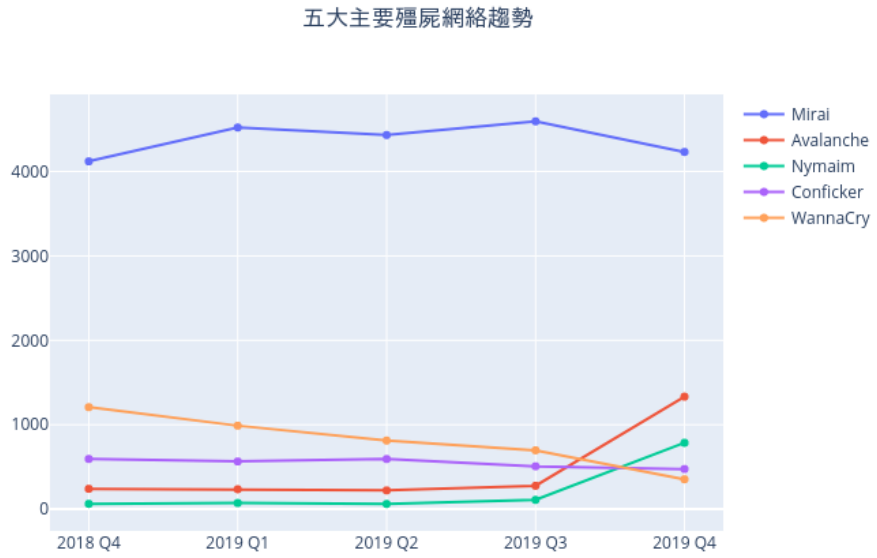


圖 13: 五大主要殭屍網絡趨勢

表 4: 五大主要殭屍網絡趨勢

| Name | 2018 Q4 | 2019 Q1 | 2019 Q2 | 2019 Q3 | 2019 Q4 |
|---|---|---|---|---|---|
| Mirai | 4,120 | 4,521 | 4,432 | 4,594 | 4,231 |
| Avalanche | 241 | 236 | 222 | 277 | 1,333 |
| Nymaim | 63 | 73 | 62 | 110 | 786 |
| Conficker | 595 | 565 | 594 | 508 | 476 |
| WannaCry | 1,208 | 989 | 813 | 697 | 354 |

甚麼是殭屍網絡?

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

有甚麼潛在影響？

- 伺服器資源被佔用，並使用於其他攻擊或犯罪活動上
- 個人資料被盜取，導致金錢損失
- 黑客有機會下指令進行其他惡意活動，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：

- 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:

表 5: IFAS 資料來源

| 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 |
| 釣魚網站 | CleanMX - Phishing | 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 | CleanMX - Malware | 2013-04 |
| 惡意程式寄存 | Malc0de | 2013-04 |
| 惡意程式寄存 | MalwareDomainList | 2013-04 |
| 殭屍網絡控制中心 (C&Cs) | Shadowserver - C&Cs | 2013-09 |
| 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 |

# B 地理位置識別方法

本中心採用以下方法去識別方網絡的地理位置是否香港。

表 6: 地理位置識別方法

| 方法名稱 | 首次使用 | 最近更新日期 |
|---|---|---|
| Maxmind | 2013-04 | 2020-04 |

# C 主要殭屍網絡

表 7: 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<br>• 寄存釣魚網站<br>• 寄存惡意程式<br>• 竊取敏感資訊 |
| Bamital | 無 | 木馬程式 | • 利用「路過式下載」(drive-by-download)<br>• 透過 P2P 網絡 | • 點擊詐騙<br>• 搜尋劫持 |
| BankPatch | • MultiBanker<br>• Patcher<br>• BankPatcher | 針對網上銀行的木馬程式 | • 透過成人網站<br>• 有問題的多媒體編解碼器<br>• 垃圾電郵<br>• 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<br>• 惡意廣告 | • 點擊詐騙<br>• 下載其他惡意軟件 |
| BlackEnergy | 無 | DDoS 木馬程式 | • 以 rootkit 技術保持隱藏<br>• 使用流程注入技術<br>• 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<br>• 按鍵記錄<br>• 截圖擷取<br>• 視訊擷取<br>• 瀏覽器中間人攻擊<br>• 勒索軟件 |
| Conficker | • Downadup<br>• Kido | 蠕蟲 | • 動態網域產生演算法 (DGA) 能力<br>• 通過 P2P 網絡進行通訊<br>• 停止安全檢測運行工具 | • 利用 Window 伺服器服務漏洞 MS08-067<br>• 暴力破解管理員密碼，在網絡上傳播<br>• 利用 Window 自動 (auto-run)，透過外置磁碟機傳播 |

表 8: 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<br>• 安裝其他惡意程式<br>• 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<br>• 發送垃圾電郵 |
| Gamarue | • Andromeda | 下載器/蠕蟲 | • 透過漏洞攻擊包<br>• 透過垃圾電郵<br>• 微軟 Word 巨集<br>• 透過外置磁碟機 | • 竊取敏感資訊<br>• 允許未經授權的存取<br>• 安裝其他惡意程式 |
| Ghost Push | 無 | 手機惡意程式 | • 透過安裝程式 | • 獲取根權限<br>• 下載其他惡意程式 |
| 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<br>• 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<br>• 發動分散式阻斷服務攻擊 (DDoS)<br>• 發送垃圾郵件 |
| Mirai | 無 | 蠕蟲 | • 利用出廠密碼 telnet | • 發動分敗式阻斷服務攻擊 (DDoS) |
| Murofet | 無 | 木馬程式 | • 透過被感染的檔案<br>• 透過漏洞攻擊包 | • 下載其他惡意軟件 |
| 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<br>• 令受害人無法存取檔案<br>• 勒索贖金 |
| Matsnu | 無 | 木馬程式 | • 透過垃圾電郵 | • 後門程式，允許未經授權的存取<br>• 鎖定受害系統<br>• 加密用戶數據<br>• 勒索贖金 |
| Palevo | • Rimecud<br>• Butterfly bot<br>• Pilleuz<br>• Mariposa<br>• 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<br>• 竊取登入認證資料及敏感資料<br>• 利用洗黑錢手法直接用銀行竊取金錢 |

表 9: 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<br>• Pandex | 下載器 | • 隱藏惡意網絡流量<br>• 動態網域產生演算法 (DGA) 能力<br>• 利用「路過式下載」(drive-by-download) 感染系統<br>• 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)<br>• 發動分散式阻斷服務攻擊 (DDoS)<br>• 發送垃圾郵件 |
| Ramnit | 無 | 蠕蟲 | • 感染檔案<br>• 透過漏洞攻擊包<br>• 公開 FTP 伺服器 | • 後門程式，允許未經授權的存取<br>• 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<br>• 通過 P2P 網絡進行通訊<br>• 透過外置磁碟機或共享傳播<br>• 停止安全檢測工具<br>• 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<br>• 通信代理<br>• 竊取敏感資料<br>• 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）<br>• 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<br>• 其他針對網上銀行的的惡意程式<br>• 發動分散式阻斷服務攻擊 (DDoS)<br>• 發送垃圾郵件 |
| Tinba | • TinyBanker<br>• Zusy | 針對網上銀行的木馬程式 | • 透過漏洞攻擊包<br>• 透過垃圾電郵 | • 竊取登入認證資料及敏感資料 |

表 10: 主要殭屍網絡

| 主要殭屍網絡 | 別名 | 性質 | 感染方法 | 攻擊/影響 |
|---|---|---|---|---|
| Torpig | • Sinowal<br>• Anserin | 木馬程式 | • 以 rootkit 技術保持隱藏 (Mebroot rootkit)<br>• 動態網域產生演算法 (DGA) 能力<br>利用「路過式下載」(drive-by-download) 感染系統 | • 竊取敏感資料<br>• 瀏覽器中間人攻擊 |
| Virut | 無 | 木馬程式 | • 透過外置磁碟機或共享傳播 | • 發送垃圾郵件<br>• 發動分散式阻斷服務攻擊 (DDoS)<br>• 詐騙<br>• 竊取資料 |
| WannaCry | • WannaCrypt | 勒索軟件 | • 於網絡中散播<br>• 利用 Windows SMB 漏洞 | • 加密用戶數據<br>• 索取贖款<br>• 數據無法復原 |
| Wapomi | 無 | 蠕蟲 | • 透過外置磁碟機或共享傳播<br>• 感染可執行檔案 | • 後門程式，允許未經授權的存取<br>• 下載其他惡意程式<br>• 改動重要檔案，導致系統不穩定<br>• 收集電腦活動數據，竊取個人資料，並令降低電腦效能 |
| ZeroAccess | • max++<br>• Sirefef | 木馬程式 | • 以 rootkit 技術保持隱藏<br>• 通過 P2P 網絡進行通訊<br>• 利用「路過式下載」(drive-by-download) 感染系統<br>• 偽裝成有效檔案 (例如: 多媒體檔案，keygen) | • 下載其他惡意程式<br>• 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<br>• 通過 P2P 網絡進行通訊<br>• 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<br>• 瀏覽器中間人攻擊<br>• 按鍵記錄<br>• 下載其他惡意程式 (例如:Cryptolocker)<br>• 發動分散式阻斷服務攻擊 (DDoS) |