資安訊息：六月份網路安全威脅報告

2014/07/11

風險等級： 資安訊息

摘　　要： 資安事件：綜觀本月份資安新聞，備受關注焦點為壹傳媒網站包括香港網站及台灣網站，自 2014 年 6 月 18 日起兩天內共遭受 87 億次攻擊，而香港普選電子公投網站「香港民間公投投票系統」，也於 6 月 19 日當日遭受 100 億次的網站查詢，造成網站服務中斷。可參考蘋果日報發佈「壹傳媒遭中國駭　行政總裁：規模史無前例」及 iThome 發佈「蘋果日報網站遭癱瘓，緊急改以臉書發新聞」。此類攻擊事故對整體資訊安全造成威脅，請加強防範，建議進行 patch 更新、修補網站弱點及架設入侵防禦系統或網頁應用程式防火牆，降低受駭威脅。

重大弱點：微軟公佈了 7 項重大更新，Adobe 發布旗下產品(Flash Player /Air) 共 2 個弱點通告，Google 發佈 Chrome 瀏覽器共 1 個弱點通告，McAfee 發布 3 個弱點通告，WordPress 發布 3 個弱點通告，Apache 發布 2 個弱點通告，Oracle 發布 17 個弱點通告，Cisco 發佈旗下產品 29 個弱點通告，SUSE 發佈 22 項更新，Red Hat 發布 19 項更新，建議受影響的用戶盡速上網修補。

病毒狀況：防毒軟體廠商近期發現 BKDR_KULUOZ.ED 後門程式 (Microsoft 命名為 TrojanDownloader:Win32/Kuluoz.D)，該後門程式透過下載執行郵件附檔方式進行感染，可以執行來自遠端惡意攻擊者的命令，有效地攻擊被感染的系統，並竊取敏感資料。建議您勿瀏覽可疑或惡意網站以及開啟任何可疑的檔案或郵件，並更新防毒軟體病毒碼至最新版本。

網路威脅分析：經由 HiNet SOC 團隊進行網路威脅情報分析後，建議客戶可採取以下防護措施：
(1)為避免遭受駭客使用 DNS 反射性 DOS 攻擊手法，HiNet SOC 建議客戶可將 DNS 主機之向上查詢 Name Server 主機改為 HiNet DNSIP (168.95.1.1 及 168.95.192.1)，客戶之 DNS 主機僅接受來自於內部電腦查詢，並關閉外部查詢非客戶使用網域之主機名稱，以避免成為駭客利用之主機。
(2)客戶如前端流量過大造成線路頻寬滿載，可協請 ISP 業者於機房端設定僅接受信任之 DNS 系統之流量訊務，以維持對外重要服務系統運作正常。
(3)客戶如使用 OpenSSL 服務之主機系統應請盡速更新至最新版本

(OpenSSL 0.98za 或 1.0.0m 或 1.0.1h 版本)，同時針對 CVE-2014-0195 及 CVE-2014-0224 等弱點攻擊進行 IPS 設備更新，並且 CVE-2014-0224 更需注意來自於內部電腦之不正常活動情形，避免已淪為駭客操作之肉雞電腦。

(4)CryptLocker 雖然已經破獲駭客之中心機房，但 FBI 表示仍未將犯罪首腦逮捕，因此 HiNet SOC 提醒客戶仍應勿瀏覽可疑或惡意網站以及開啟任何可疑的檔案或郵件，定期備份重要檔案及更新作業系統至最新版本，並更新至最新病毒碼來降低受駭風險。

本資訊轉自教育部資安服務網