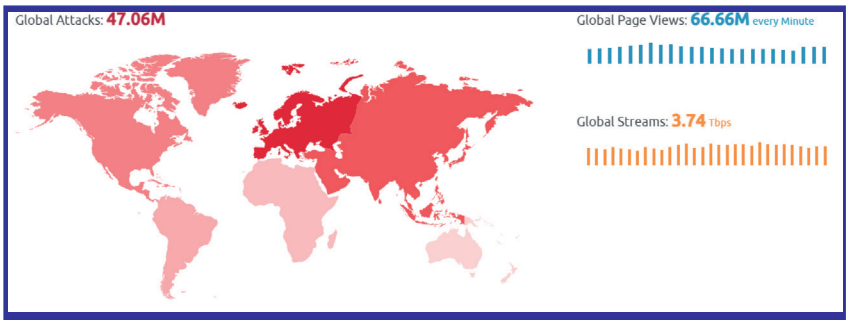
防護從天邊開始

■文：徐俊毅

Akamai 全球最大的 CDN 服務商之一，同時號稱擁有全球最大數量的物聯網節點設備。圖 1 這張來自 akamai 公司的網站截圖，清晰反映出了包括物聯網 IoT 設備在內的整個 internet 的即時資安狀況。

(注：Akamai 誕生于麻省理工學院，總部位於波士頓，在 1998 年發明 CDN 技術架構之後組建公司，據稱全世界 90% 的互聯網用戶經過 1 跳 (可以簡化為尋找最近的線路節點) 就可以找到 Akamai 伺服器，在全球 500 強企業中有 300 家是他們的客戶。)

圖 1:2021 年 1 月初當日上午 10 點左右的即時攻擊數量已經超過 4700 萬次



圖片來源 ：www.akamai.com

60 天 300 億次爬蟲請求和 60 億次惡意登陸請求

Akamai 公佈的 2020 年上半年的網路安全報告指出，在一個 60 天的週期內，他們觀測了針對全球的遊戲用戶的攻擊。總共統計到了 300 億次的敏感資訊網路爬蟲 (Web Crawler) 請求和 60 億次的惡意登陸請求。這僅僅是針對遊戲用戶的一項統計，擴展的其他行業，這個數字會更加龐大。

高密度的攻擊行為反映出，任何人、企業、機構的資料時時面臨被非法獲取，而巨量的登陸請求表明，如果你的設備使用 123456 之類的簡單登陸密碼，就意味著向全世界提供“無私”的共用內容。

攻擊方式上透過 web 應用層的攻擊比 2019 年增長了 42%，高科技公司和電商平臺是主要被攻擊對象，而越來越多網站平臺使用的 API (應用程式介面) 也成為爬蟲攻擊的重點區域，或者是獲取使用者資料，或者刺探商業機密。

遠端攻擊者採用海量攻擊的一個重要工具就是使用僵屍網路 (Botnet)。

(注：攻擊者通過各種途徑傳播僵屍程式感染互聯網上的大量主機，而被感染的主機將通過一個控制通道接收攻擊者的指令，組成一個僵屍網路。之所以用僵屍網路這個名字，是為了更形象地讓人們認識到這類危害的特點：眾多的電腦在不知不覺中如同古老傳說中的僵屍群一樣被人驅趕和指揮著，成為被有心人利用的一種工具。)

如今的僵屍網路設備已經不僅僅局限于傳統意義上電腦，包括雲、物聯網在內的各種設備，都存在被僵屍網路利用的可能性。利用僵屍網路設備，攻擊者，可以癱瘓正常的資訊系統，傳播病毒，非法獲取敏感性資料，同時還可以有效隱藏攻擊者的位置。包括電子郵件欺詐，釣魚，勒索病毒等近年來危害巨大的網路犯罪行為，後面都有僵屍網路的影子。

聯合 35 國 8 年重擊全球最大的僵屍網路 Necurs

2020 年 3 月，微軟宣佈他們成功摧毀了 Necurs，這個劫持了大量基礎設施，感染超過 900 萬台的計算設備的僵屍網路，同時獲得法院指令接管美國境內現有的 Necurs 功能變數名稱。

微軟的成功得益於 35 個國家和地區的警方以及私人科技公司的一致行動。核心技術是微軟破解了 Necurs 僵屍網路生成新功能變數名稱的演算法 –DGA，這種自動化快速生成的功能變數名稱可以使得僵屍網路的郵件發送服務逃避現有的黑名單檢測技術，提高垃圾郵件的到達率，達到分發惡意軟體的目的。

微軟負責客戶安全和信任的副總裁湯姆．伯特表示：“我們能夠準確預測 (Necurs) 未來 25 個月生成的 600 萬個功能變數名稱。破解技術能夠阻止 Necurs 控制者利用這些功能變數名稱註冊網站，進而阻止他們的網路犯罪行為。“

Necurs 在 2012 年被首次發現，在過去的這些年，Necurs 透過大量發送垃圾郵件，為灰色世界分發惡意軟體，加密劫持軟體以及勒索軟體，2017 年的統計顯示他們已經可以做到每小時發送 500 萬封電子郵件。有報告指出全球 90% 的惡意軟體傳播都是透過了他們的垃圾郵件分發實現的。

儘管微軟宣佈他們搗毀了這個僵屍網路，但實際上在 2015 年，FBI 和 NCA 就聯合行動打擊過 Necurs，只是很快他又復活，並用於傳播勒索病毒。所以長期來看，針對僵屍網路的行動遠遠沒有結束。

物聯網設備是薄弱環節

來自 ARM 的資料顯示，從雲端到邊緣，採用 ARM 核心的設備已經超過 1000 億個，並且隨著物聯網的發展，到達萬億數量級也不會等太久。物聯網設備數量龐大，安全等級參差不齊，而且有很多設備真的是遠在天邊，因此是網路攻擊的重災區。

綜合 Gartener，Strategy，Cisco 等公司的資料發現，早在 2011 年，全球的 5 億個左右的 IoT 設備中，大部分都是不具備安全防護能力或者低防護能力的設備，但隨著 IoT 設備安全性漏洞頻發，僵屍網路的興起，IoT 設備的安全等級也在迅速提升，到了 2017 年，全球一半左右的 IoT 設備具備了較強的安全防護能力，2020 年全球物聯網設備已經到達 500 億這個數量等級，這其中 9 成以上的設備裝備了安全防護功能。但從另一個角度來看，防護能力較弱的 IoT 設備仍然是以億為單位進行計量的。

越來越多傳統企業在工業和關鍵基礎設施環境中使用的 IoT，數位轉型增加了這些環境中的連線性和設備數量，從而導致更高的資安風險。在這些應用場景中，很多物聯網 IoT 設備和協定是多年前設計的，缺乏加密、增強式驗證和加固的軟體堆疊等防範風險的能力。這些設備一旦遭遇攻擊，可能會對公司造成重大影響，包括安全事件、代價高昂的生產停機時間，以及竊取有關專有配方和製造工藝的資訊等敏感智慧財產權。

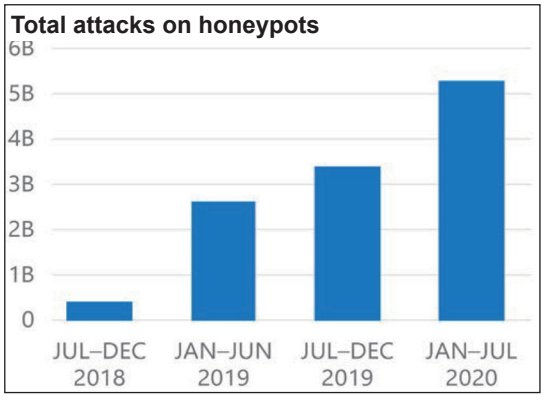
為了收集有關遠端終端機、路由器和物聯網設備攻擊的情報，微軟威脅情報中心 (MSTIC) 在 Azure 和一系列其他雲提供商上部署了 (honeypots) 蜜罐 (旨在類比網路犯罪分子的可能目標)。蜜罐使用各種已知協議與攻擊者進行交互。整個公司的安全團隊分析這些資料，以發現新的趨勢和新出現的威脅。

僅 2020 年上半年，針對這些物聯網蜜罐的攻擊相比 2019 年下半年增長了 35%，整個 2020 年針對物聯網設備的攻擊數量將超過前 5 年的總和。在他們一項分析中發現，攻擊者利用物聯網設備估計的遠端升級功能，獲取了 root 許可權，從而讓這家 IP 攝像頭數百萬台設備的視頻資訊可能被攻擊者獲取。

針對已知協議的攻擊中，Telnet 這種未經加密的明文傳輸協定和弱密碼讓攻擊者能夠輕易得手。

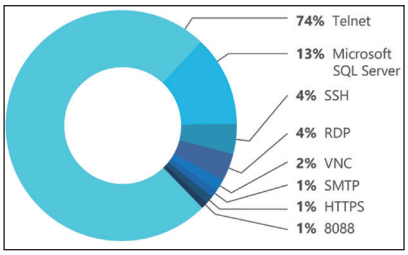
除了從遠端發動攻擊，由於 IoT 設備無所不在的特性，很多攻擊從遠端變成了本機攻擊。攻擊者直接攻擊 IoT 設備的關鍵晶片，由此獲得他們想要的資料，而這部分正是 IC 製造商們正在進行的晶片硬體安全升級的工作。 CTA

圖 2：2020 年前 7 個月 MSTIC 在 Azure 雲端部署的“蜜罐”收到超過 50 億次攻擊



資料來源： Microsoft_Digital_Defense_Report_2020 www.microsoft.com

圖 3：眾多傳輸協議中 telnet 成為攻擊重點



資料來源： Microsoft_Digital_Defense_Report_2020 www.microsoft.com