TechNews 科技新報

竊取名人 Twitter 帳號詐騙 10 萬美元黑手幕後主腦曝光！竟是位 17 歲少年

作者 雷鋒網 | 發布日期 2020 年 08 月 03 日 14:04 | 分類 社群 , 網路 , 資訊安全

據外媒消息，大規模名人 Twitter 遭駭客入侵事件水落石出，策劃者為來自佛羅里達州的 17 歲少年格雷厄姆·克拉克（Grahamlvan Clark）。

▲ 格雷厄姆·克拉克。（Source：WGNTV）

兩名同夥為英國人梅森·薛博（Mason Sheppard），以及也為佛州人的尼瑪·法茲利（Nima Fazeli）。目前三人均遭逮捕。

主謀克拉克面臨包括詐騙罪等 30 多項重罪指控，並以成年人身分接受審判。

訊息一出，有網友調侃：

如此天才少年，應該懲罰他到國家安全局工作。

但也有網友回答，天才少年沒錯，不過主要還是 Twitter 安全性太差了。

> FancyShark wrote:
> I assume he'll be getting a job with the NSA as punishment.
>
> The NSA does actually recruit talented hackers, but I doubt this kid would be a candidate. Going by the other information that we have, this is less "this 17-year-old is such a genius that he can hack Twitter" and more "Twitter's sensitive account security practices are so garbage that a 17-year-old can hack Twitter".

至於駭客如何成功駭入名人帳戶，Twitter 最新官方回覆為應是採取手機魚叉式網路釣魚攻擊（phone spear phishing attack）。FBI 調查人員針對駭客攻擊行為有詳細說明。

駭客攻擊事件回顧

7 月 15 日，Twitter 爆發史上最大規模安全漏洞事件，包括伊隆·馬斯克（Elon Musk）、比爾蓋茲（Bill Gates）、前總統歐巴馬（Barack Obama）、總統候選人民主黨喬·拜登（Joe Biden）等眾多名人等 130 個 Twitter 帳戶均遭駭客入侵。

其中 45 位名人帳戶被駭並發表比特幣募集推文。

推文內容大致相似：

我在回饋社會。所有傳送到以下地址的比特幣都會加倍寄回！如果你寄 1,000 美元，我就寄回你 2,000 美元。只有 30 分鐘。

所用推文最後全部附上駭客的比特幣錢包程式碼。

事件一出，Twitter 官方立刻採取措施，限制部分 Twitter 帳戶推文和重設密碼等功能，從規模和影響來看，這次駭客攻擊是 Twitter 史上最大安全漏洞事件。

由於這些名人帳號均有數百萬粉絲，駭客精心策劃的比特幣騙局單日就收到超過 10 萬美元比特幣。

希爾斯伯勒州州檢察長安德魯·華倫（Andrew Warren）說：

駭客利用名人 Twitter，旨在從佛州等全美國人身上偷錢。這種大規模詐欺行為是精心策劃的行動，我們絕不允許。

隨後，美國執法部門展開調查，最後將目標鎖定 17 歲克拉克、19 歲薛博和 22 歲的法茲利三人。

接受成年人審判

據調查人員介紹，他們是在 OGusers 論壇發現嫌犯的蹤跡。OGusers 是駭客論壇，有許多發文、私人訊息、IP 位址、電子郵件及眾多參與者的用戶資訊。

Twitter 事件當天，OGusers 論壇名為「Chaewon」的帳號發文，聲稱可變更與任何 Twitter 帳戶連結的電子郵件位址，價格為 250 美元，並可直接存取 2,500 美元至 3,000 美元的帳戶。如有需求可與 Discord 用戶聯繫。

與此同時，OGuser 資料程式庫顯示，名稱「Rolex」的帳戶表示，他可以控制註冊到「Rolex＃0373」的 Discord 帳戶，因此，調查人員大致鎖定了法茲利。

今年 2 月初，Chaewon 還有一項盜版影片遊戲帳戶的購買記錄，交易收付款地址正是此事件的比特幣集群（為一組錢包，可連結到個人或實體）。調查人員使用帳戶 IP 位址，連結到另一名為「Mas」的 OGuser 帳號，發現用戶使用的電子信箱地址與薛博的帳戶連結。兩位嫌犯已確定。

此外，對如何發現克拉克的犯罪路徑，研究人員沒有說明。

據 WFLA 稱，檢察長沃倫已對這名 17 歲少年提起 30 多項重罪指控，包括有組織的詐欺罪、17 項通訊詐欺罪、詐欺性使用個人資訊的犯罪案件、十項詐欺性使用個人資訊罪和未經授權存取電腦的罪名。由於事件的嚴重性，佛州法院表示，將酌情考慮以成年人標準審判。

同時，另兩名成年人也會在加州接受審查，薛博被指控串謀電匯詐欺，串謀洗錢及故意存取受保護的電腦三項罪名。 法茲利被指控協助故意存取受保護電腦。

他們是如何做到的？

Twitter 最新聲明指出，駭客透過魚叉式網路釣魚，啟動內部員工登入不安全網站，洩露 Twitter 系統的存取和管理許可權。近日，首席法官馬克·拉許（Mark Rasch）詳細說明駭客的攻擊手段。

- 駭客透過全球最大職場社交平台 LinkedIn，取得 Twitter 員工的手機號碼和其他私人聯繫資訊。
- 隨後致電員工，透過個資與員工建立信任，並確認是否為 Twitter 系統授權人員。
- 確定後將員工引到模仿 Twitter VPN 的釣魚頁面。當目標員工進入時，攻擊者便獲得存取憑證。

為了繞過 Twitter 的兩步驟身分驗證，駭客在員工將資訊輸入假 Twitter 登入頁面後幾秒內，便將憑證輸入真實 Twitter VPN。一旦員工輸入一次性密碼，攻擊者就跟著進入。

調查研究人員介紹，駭客計劃之所以成功，武和肺炎疫情有關鍵作用。首先受疫情影響，大部分員工在家辦公，個人裝置往往無法達到公司電腦的控制和存取限制程度，另外使用的 VPN 服務，可能未經全面審核，每個員工都擁有完全存取許可權。最重要的是，在家上班阻礙了員工面對面相互驗證，依賴網路或手機資訊越來越不安全。

如何預防駭客網路攻擊？調查人員表示，對於如 Twitter 等技術服務商而言，最直接方法是使用硬體或證書檢查，以確保單獨使用竊取的憑證入侵無效。另外，公司也必須加強網路監管，了解駭客社群常用的技術，並與其他公司共享訊息。

（本文由 雷鋒網 授權轉載；首圖來源：pixabay）

延伸閱讀：

- Twitter 版「無間道」：歐巴馬、蓋茲等名人帳號被盜，竟是因為有內鬼？
- 美國政商名人 Twitter 帳號集體被駭，發出比特幣兩倍券騙局

關鍵字: Twitter , 比特幣 , 駭客

0則留言 排序依據 最舊

新增回應……