

OUCH!

您的每月安全意識通訊

暗網

概觀

您可能聽過其他人或媒體使用的“暗網”一詞，並想知道“暗網是什麼？”或“我應該做些什麼嗎？”。今天我們解釋一下暗網 (Dark Web) 是什麼以及它對您意味著什麼。

它是什麼？

暗網網站由互聯網上的系統組成，旨在安全和匿名地進行信息通信或共享。沒有單一的“暗網”；它不像 Facebook 那樣由一個組織運營。相反，Dark Web 是由不同人員管理的不同系統和網絡的集合，用於各種目的。這些系統仍然連接到 Internet 並且是 Internet 的一部分，但是您通常不會使用普通的搜索引擎找到它們。您通常還需要在電腦上使用特殊軟件來查找或訪問它們。一個例子是 Tor 項目。要訪問此 Dark Web，請下載並安裝 Tor Browser。使用 Tor 瀏覽器連接到 Web 服務器時，加密的流量也通過 Tor 傳輸到其他電腦。當它通過這些電腦時，源 IP 地址正在改變意味著當您訪問該網站時，您的在線活動是匿名的。Dark Webs 的其他例子包括 Zeronet, Freenet 和 I2P。

誰使用它？

網絡罪犯是 Dark Web 的大用戶。他們維護暗網中的網站和論壇，以便進行犯罪活動，例如購買毒品或銷售數十億字節的黑客數據 - 所有這些都是匿名和安全的。例如，當網絡犯罪分子攻擊銀行或網上購物商店時，他們會盡可能多地竊取信息，然後將這些信息賣給暗網上的其他網絡犯罪分子。

Dark Web 也有合法用途。例如，在審查猖獗的國家/地區的人們可以使用 Dark Web 網絡來共享信息，看看世界上還發生了什麼，同時保護他們的隱私並保持匿名。記者，舉報人和有隱私意識的人可以使用暗網

來增加他們的匿名性並繞過審查制度。此外，這類人群可以使用像Tor瀏覽器這樣的技術，不僅可以訪問Dark Web，還可以匿名瀏覽常規Internet。

我該怎麼辦？

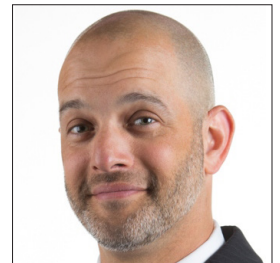
除非您有特定原因要訪問Dark Web，否則我們會提醒您不要使用它。一些暗網用於非法目的，許多網站在網絡中使用您的電腦來實現其目標，在某些情況下，您的電腦甚至可能被探測或攻擊。有些公司提供監控服務，讓您知道您的姓名或其他信息是否被網絡犯罪分子竊取並在暗網上找到，但這些服務的實際價值值得懷疑。保護自己的最佳方法是假設您的某些信息已經被網絡犯罪分子使用。因此。。



- 時刻警惕任何假裝成官方組織的電話或電子郵件，並強迫您採取行動，例如支付罰款。犯罪分子甚至可能會使用他們發現的有關您的信息來創建個性化攻擊。
- 監控您的信用卡和銀行對賬單。甚至對可能會對發生的任何交易設置每日警報。通過這種方式，您可以檢測是否發生了任何財務欺詐。如果您確實檢測到它，請立即將其報告給您的信用卡公司或銀行。
- 凍結您的信用評分。它不會影響您如何使用信用卡，這是您可以採取的最有效的步驟之一，以防止身份被盜。

客座編輯

Micah Hoffman (@WebBreacher) 是Spotlight Infosec LLC的首席研究員，也是一名認證的SANS研究所講師，以及SANS OSINT課程的作者。Micah對網絡和開源智能的熱情表現在他的項目，課件和教學風格中。



參考資料

個性化攻擊: <https://www.sans.org/u/RfW>
社會工程: <https://www.sans.org/u/Rq1>
身份盜竊: <https://www.identitytheft.gov>
信用凍結: <https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/>
Tor瀏覽器: <https://www.torproject.org/>
SANS OSINT課程: <https://sans.org/sec487>

OUCH! 由SANS Security Awareness發行刊登，遵從 Creative Commons BY-NC-ND 4.0 (創意公用授權條款4.0版)。在不更改本刊物內容的前提下，你可以自由分享此月刊或使用於你的安全意識計劃。有關翻譯或更多諮詢，請聯絡 www.sans.org/security-awareness/ouch-newsletter。編輯委員會：Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | 翻譯：巴珊珊