CenturyLink 宣佈推出新的威脅研究與營運子公司 Black Lotus Labs

Black Lotus Labs 發現僵屍網絡 Necurs 在全球廣泛傳播多工具僵屍網絡隱藏技術

美通社路易斯安那州門羅 2019 年 2 月 28 日電 CenturyLink, Inc.(NYSE:CTL)正在分享其新的威脅研究和營運子公司 Black Lotus Labs 發現的 Necurs 僵屍網絡的情報，致力於進一步幫助保護互聯網免受惡意網絡和軟件的傷害。

在這裡體驗互動多渠道新聞稿：https://www.multivu.com/players/English/8238355-centurylink-black-lotus-labs/

Black Lotus Labs 的使命是利用 CenturyLink 的網絡**透明**度來幫助保護客戶和保障互聯網安全。Black Lotus Labs 透過追蹤和擾亂 Necurs 這樣的僵屍網絡方式實現這一點，Necurs 是一種在全球範圍內被廣泛傳播的垃圾郵件和分發系統，它最近展示了一種隱藏技術，既可以避開檢測，又可以悄悄地滋生更多僵屍網絡。

閱讀 Black Lotus Labs 有關 Necurs 的報告詳情：網址。

Black Lotus Labs 負責人 Mike Benjamin 表示：「Necurs 是一種多工具僵屍網絡，從以垃圾郵件的形式提供銀行特洛伊木馬和勒索軟體業務，再到開發代理服務，以及擁有加密貨幣挖礦和分散式拒絕服務(DDoS)功能。特別值得一提的是，Necurs 會定期隱藏以避免被發現，重新出現向受感染的主機發送新命令後，然後再次隱藏。這項技術是 Necurs 能夠擁有 50 多萬僵屍網絡的原因之一。」

主要發現

——從 2018 年 5 月開始，Black Lotus Labs 觀察到，包括 Necurs 在內的三種最活躍的僵屍網絡類群會有規律地出現持續停工期，大約運行三周，停工兩周。

——Necurs 的大約 570,000 個僵屍網絡在全球廣泛分佈，大約一半分佈在以下國家，按流行程度排列：印度、印尼、越南、土耳其和伊朗。

——Necurs 使用域名生成演算法(DGA)混淆其操作，並避免卸載。不過，DGA 是一把雙刃劍：由於 Necurs 將使用的 DGA 域名是事先已知的，安全研究人員可以使用諸如轉接 DGA 域名、解析 DNS 和網絡流量等方法來評估僵屍網絡以及指揮和控制(C2)基礎設施。

——除了通知潛在受感染設備的其他網絡所有者之外，CenturyLink 還採取措施減少 Necurs 對客戶的風險，保護互聯網安全。

更多資源

- 瞭解 TheMoon 如何演變為服務代理：http://news.centurylink.com/2019-01-31-TheMoon-Illustrates-Evolving-Threat-of-IoT-Botnets.
- 瞭解更多關於 Mylobot 的第二階段攻擊的信息：http://news.centurylink.com/2018-11-14-Mylobot-botnet-delivers-one-two-punch-with-Khalesi-malware.
- 瞭解 Satori 僵屍網絡如何盯上新目標：http://news.centurylink.com/2018-10-29-Satori-botnet-resurfaces-with-new-targets.

CenturyLink 簡介

CenturyLink(NYSE: CTL)是服務於全球性企業客戶的美國第二大通訊服務提供商。公司在 60 多個國家擁有客戶，高度重視客戶體驗，致力於透過滿足客戶對安全可靠的連接不斷增長的需求，成為全球最佳網絡公司。作為客戶值得信賴的合作夥伴，CenturyLink 幫助他們管理日益複雜的網絡和信息技術，並提供有助於保護客戶業務的網絡管理服務和網絡安全解決方案。

圖標——https://mma.prnewswire.com/media/134213/centurylink_logo.jpg

聯繫人：Stephanie Walkenshaw, 電話：+1 720-888-3084, 電郵：stephanie.walkenshaw@centurylink.com