僵屍網络仍是持久的網络威脅

CenturyLink 在 2017 年每天追蹤到 1.04 億個僵屍網络單一攻擊目標

美通社络易斯安那州門羅 2018 年 4 月 17 日電 – CenturyLink, Inc. (NYSE: CTL) 最新發佈的一份威脅報告指出，企業、政府和消費者需更加小心僵屍網络帶來的風險。

2017 年，CenturyLink 威脅研究實驗室平均每天跟蹤到 195,000 起由僵屍網络引起的威脅，受影響的單一目標平均達到 1.04 億個，包括伺服器、電腦、手持設備或其它聯網設備，等等。

CenturyLink 威脅研究實驗室主管 Mike Benjamin 表示：「僵屍網络是不法份子用來盜取敏感數據和發起 DDoS 攻擊所依賴的基本工具之一。透過分析全球僵屍網络攻擊趨勢和方法，我們能夠更好地預測和應對新的威脅，從而保護我們自己以及客戶的網络。」

閱讀 CenturyLink 2018 年威脅報告：
http://lookbook.centurylink.com/threat-report

主要發現

- 具有強大或快速發展 IT 網络和基礎設施的地區仍將是網络犯罪活動的主要來源。
  - 按 2017 年全球惡意網络通信量來算，亞太區排名前五的國家和地區是中國大陸、韓國、日本、印度和香港。
  - 亞太地區指令和控制伺服器（積聚並監督著僵屍網络）託管量排名前五的國家和地區是中國大陸、韓國、日本、印度和香港。
- 儘管具有強大通訊基礎設施的國家各地區會在不知不覺中為互聯網 DDoS 攻擊提供頻寬，但他們同時也是最大的受害者之一（按攻擊指令量來計算）。
  - 僵屍網络攻擊流量最大的五大目標國家是美國、中國、德國、俄羅斯和英國。
  - 受連累的主機或僵屍網络數量最多的五個亞太國家和地區是中國大陸、印度、日本、臺灣和韓國。
- Mirai 病毒及其變種一直是新聞報導的重點，但在 2017 年，CenturyLink 威脅研究實驗室發現了影響著更多受害者的 Gafgyt 攻擊，其攻擊持續時間也更長。

重要事實

- CenturyLink 每天收集 1140 億份網络流量記錄，每天捕捉到超過 13 億起安全事件，並持續監測 5000 個已知的 C2 伺服器。

- CenturyLink 每天回應和平息約 120 起 DDoS 攻擊，每月刪除近 40 個 C2 網络。
- CenturyLink 威脅意識的範圍和深度源自其全球 IP 主幹網，它是全球最大的主幹網之一。這個至關重要的基礎架構為 CenturyLink 的全球營運提供支持，並為其綜合安全解決方案系列提供信息，包括威脅監測、安全性記錄檔監督、DDoS 緩解以及基於網络的安全解決方案。

更多資源

- 聽聽 Mike Benjamin 在 CenturyLink 2018 年威脅報告中的關鍵見解：https://youtu.be/3U1aIJqejjs
- 瞭解 CenturyLink 如何以更廣泛的潛在威脅信息讓網络情報更進一步發展：http://news.centurylink.com/2018-04-03-CenturyLink-takes-cyber-intelligence-to-the-next-level-with-expanded-view-of-threatscape
- 探討 IDC 報告： 利用網络安全保護聯網企業：http://idcdocserv.com/US43638618

CenturyLink 簡介

CenturyLink (NYSE: CTL)是服務于全球性企業客戶的美國第二大通信服務提供者。公司在 60 多個國家擁有客戶，高度重視客戶體驗，致力於通過滿足客戶對安全可靠的連接不斷增長的需求，成為全球最佳網络公司。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络和資訊技術，並提供有助於保護客戶業務的網络管理服務和網络安全解決方案。

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