opentext™

2023 OpenText Cybersecurity Threat Report Reinforces Need for Multilayered Security Approach

3/29/2023

40.3% reduction in the number of devices encountering malware for those with three layers of protection versus a single layer

WATERLOO, ON, March 29, 2023 /PRNewswire/ -- **OpenText™** (NASDAQ: OTEX), (TSX: OTEX) today released the results of the 2023 OpenText Cybersecurity Threat Report which explores the latest threats and risks to the small and medium business (SMB) and consumer segments. Powered by the BrightCloud® Threat Intelligence Platform, the OpenText Cybersecurity annual report breaks down a broad range of threat activity, offers insight into the trends observed, and discusses wide-reaching impacts for industries, geographies, companies and individuals.

Threat actors doubled down on longstanding tactics while demonstrating innovation with new techniques. One notable trend from the past year was a significant increase in concealing the location of URLs hosting malware and phishing sites. The percentage of malicious URLs hidden behind a proxy or geolocation-masking service increased 36% year-over-year (YoY). Meanwhile, online cybersecurity threats continue to emerge at an alarming pace. New malicious websites come online daily, while legitimate sites are occasionally compromised and co-opted for nefarious purposes.

"Cyber bad actors, including nation-state players, continue to be persistent, innovative and effective. There is, however, some encouraging news. A decline in malware infections indicates comprehensive security measures are effective," said Prentiss Donohue, Executive Vice President, OpenText Cybersecurity. "Cybercriminals are equal opportunity offenders. Acknowledging risks and preparing accordingly with a mulitlayered approach to protecting data are recommended courses of action for businesses of every size."

Key highlights from this year's report include:

Malware

- Malware on endpoint continues to decline 16.7% YoY
- Rising geopolitical tensions continue to influence malware campaigns

- Manufacturing remains the #1 targeted industry vertical
- Analyzing high-risk URLs, on average, each malicious domain hosted 2.9 malware URLs, compared to only 1.9 phishing URLs

Phishing

- Email phishing is the primary vector for infection followed by remote desktop protocol (RDP); RDP was #1 last year
- Over 1 billion unwanted emails classified as phishing
- Spear phishing email traffic increased 16.4% YoY and now accounts for approximately 8.3% of all email traffic
- 55.5% year-over-year increase in HTTPS vs HTTP phishing attacks

Ransomware

- Double extortion from data exfiltration is commonplace in campaigns at a rate of 84%
- Median ransomware payments meteor spike to almost $200k; up from $70k last year
- Law enforcement crackdowns on ransomware saw some success but have yet to make a large impact on the overall threat ransomware poses

Infection Rates

- 28.5% of businesses with 21-100 protected endpoints encountered an infection in 2022
- For businesses between 1-20 endpoints, the rate is 6.4%
- For businesses between 101-500 endpoints the rate rose to 58.7%
- And for 501+ the rate was 85.8%

Geographic Breakdown

- The top 50,000 most-active malicious IP addresses originated from 164 countries
- The Netherlands and Germany made it into the top five, along with the US, China and Vietnam

Multi-layered defense

- 40.3% reduction in the number of devices that encountered malware for users who adopted all three layers of protection — Webroot SecureAnywhere, Webroot Security Awareness Training, and Webroot DNS Protection — versus devices using Webroot SecureAnywhere alone
- Data confirms, cyber resilience using a layered defense strategy remains the best defense against today's cybercrime landscape

To view the complete 2023 OpenText Cybersecurity Threat report, visit **2023 Threat Report**.

Methodology:

The threat intelligence, trends and details presented in the 2023 OpenText Cybersecurity Threat Report are based on data continuously and automatically captured by the BrightCloud® Threat Intelligence Platform, which is the proprietary machine learning-based architecture that powers all Webroot protection and BrightCloud® services. This data comes from over 95 million real-world endpoints and sensors, specialized third-party databases, and intelligence from end users protected by our leading technology partners like Cisco, Citrix, F5 Networks, and more. Our threat research team analyzes and interprets the data using advanced machine learning and artificial intelligence. New to this year's report is the inclusion of data from Webroot Email Security Powered by Zix.

About OpenText Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

About OpenText

OpenText, The Information Company™, enables organizations to gain insight through market leading information management solutions, powered by OpenText Cloud Editions. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit **opentext.com**.

Connect with us:

OpenText CEO Mark Barrenechea's blog

Twitter | **LinkedIn**

Certain statements in this press release may contain words considered forward-looking statements or information under applicable securities laws. These statements are based on OpenText's current expectations, estimates, forecasts and projections about the operating environment, economies and markets in which the company operates. These statements are subject to important assumptions, risks and uncertainties that are difficult to predict, and the actual outcome may be materially different. OpenText's assumptions, although considered reasonable by the company at the date of this press release, may prove to be inaccurate and consequently its actual results could differ materially from the expectations set out herein. For additional information with respect to risks and other factors which could occur, see OpenText's Annual Report on Form 10-K, Quarterly Reports on Form 10-Q and other securities filings with the SEC and other securities regulators. Unless otherwise required by applicable securities laws, OpenText disclaims any intention or obligations to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise.

OTEX-G

View original content to download multimedia:**https://www.prnewswire.com/news-releases/2023-opentext-cybersecurity-threat-report-reinforces-need-for-multilayered-security-approach-301783952.html**

SOURCE Open Text Corporation