OpenText Empowers Businesses to Better Understand Threat Intelligence and Strengthen Cyber Resiliency

3/28/2022

2022 BrightCloud® Threat Report shows ransomware remains largest cyber threat to SMBs as phishing activity spikes with 770% increase

WATERLOO, ON, March 28, 2022 /PRNewswire/ -- **OpenText™** (NASDAQ: OTEX), (TSX: OTEX) announces the **2022 BrightCloud® Threat Report** which outlines key data points and trends affecting small and large businesses worldwide, as well as individuals in the new hybrid, inter-connected world. This year's report provides in-depth analysis, market insights, trend data, and predictions for what lies ahead as organizations move toward strengthening their cyber resiliency posture in the face of ever-increasing cyberattacks and cyber warfare.

Remote and hybrid work environments, along with rapidly shifting world affairs, continues to alter how we interact and presents new security challenges that opens lucrative avenues for bad actors. Last year, phishing attacks escalated across email, text, and other communications platforms and new high-risk malicious URLs were found hiding behind proxy avoidance and anonymizers. Alternatively, while browser-based cryptojacking may have practically disappeared, cryptomining malware shifted into mainstream as cybercriminals continue looking for ways to compromise data and personal information.

"Businesses' ability to prepare for and recover from threats will increase as they integrate cyber resilience into their technologies, processes, and people," said Mark J. Barrenechea, OpenText CEO & CTO. "With security risks escalating worldwide and a persistent state of 'unprecedented' threats, compromises are inevitable. This year's findings reiterate the need for organizations to deploy strong multi-layered security defenses to help them remain at the heart of cyber resilience and circumvent even the most creative cybercriminals."

Key Report Highlights:

Phishing & Impersonated Companies:

- 770% overall phishing activity spike during the month of May 2021

- January – April 2021 saw a mere 9% of phishing activity
- 54% of all detected phishing URLs in 2021 were from top-targeted brands: Apple, Facebook, YouTube, Microsoft, and Google
- TO NOTE: eBay fell from being #1 impersonated brand in 2020, dropping out of the top 10 completely in 2021 as pandemic-related shortages eased.

Malware:

- 86.3% of malware is unique to a single PC; consistent YOY
- 83% of Windows malware hides in one of four locations, noting that %appdata% saw a 46% decrease from the prior year, and %desktop% saw a 40% increase from the prior year
- TO NOTE: The number of malware files reaching Webroot-protected Windows endpoints dropped 58% between 2020 and 2021.

Infection Rates by Industry:

- Manufacturing registered 54% above average in 2021
- Public Administration saw 41% rise above average in 2021
- Finance and Insurance were 22% below average in 2021
- TO NOTE: Manufacturing was the industry most likely to be infected in 2021 based on a willingness to pay ransoms to prevent supply chain disruptions. The 2021 Colonial Pipeline incident was reminiscent of the damage and chaos from the 2017 NotPetya ransomware by Russian nation state attackers on the Ukrainian supply chain. We expect to see more attacks targeting manufacturers and supply chains in 2022.

Infection Rates by Region:

- Japan, United Kingdom, North America, and Australia saw infection rates drop by 51% since the year prior
- United States held the largest number of malicious IP addresses and convictions (24.3%)
- TO NOTE: Netherlands had the highest number of convictions per bad IP address (average 526), meaning that each malicious IP address in the Netherlands performed more malicious activity on average than the average malicious IP address in other countries.

"Cyber resiliency is a top proactive priority for organizations worldwide," said Craig Robinson, IDC Program Director, Security Services. "Better understanding the known threats will play a key role in building and maintaining a strong layered security approach."

Download the full 2022 BrightCloud® Threat Report **here**.

Methodology:

The threat intelligence, trends and details presented in the 2022 BrightCloud® Threat Report are based on data continuously and automatically captured by BrightCloud® 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.

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/opentext-empowers-businesses-to-better-understand-threat-intelligence-and-strengthen-cyber-resiliency-301511087.html**

SOURCE Open Text Corporation