



OpenText Announces 2021 Webroot BrightCloud® Threat Report

4/20/2021

Data demonstrates 34.4% YoY increase in overall phishing activity with massive spikes during the early months of the COVID-19 pandemic

WATERLOO, ON, April 20, 2021 /PRNewswire/ -- **OpenText™** (NASDAQ: OTEX), (TSX: OTEX), today announced the release of the 2021 Webroot BrightCloud® Threat Report. Webroot's unparalleled sixth generation machine learning security platform provides unique data insights into the timing, tactics and technologies that threat actors used over the past year.

Phishing activity increased significantly in the first few months of 2020, taking advantage of pandemic-induced product shortages and increased usage of streaming services. For the first time, eBay topped the list of brands most targeted for impersonations, with 31.1% of all phishing attacks in the month of February impersonating eBay. In March, phishing activity surged among streaming services YouTube (3,064%), Netflix (525%) and Twitch (337%).

"Gathered from over 285 million real-world endpoints and sensors, and leveraging the extensive BrightCloud network of industry-leading partners, this year's Threat Report clearly shows how cybercriminals are willing and able to evolve their tactics to exploit collective human interest and current events," said Prentiss Donohue, Executive Vice President, SMB/C Sales, OpenText. "The findings underscore the need for users and businesses of all sizes to enact a multi-layered approach to data security and protection given the persistent creativity of cybercriminals."

Download the full 2021 Webroot BrightCloud® Threat Report [here](#) .

Notable Report Findings:

- Phishing:
 - Attacks increased 510% from January to February alone
 - The top five phishing targets of the year were eBay, Apple, Microsoft, Facebook and Google
 - By the end of 2020, 54% of phishing sites used HTTPs. Use of HTTPS varies considerably based on the

industry being targeted and is most heavily used when spoofing cryptocurrency exchanges (70% of the time), ISPs (65%), and gaming (62%)

- Malware
 - 86.1% of malware is unique to a single PC
 - 83% of Windows® malware hides in one of four locations. One of which, %appdata%, saw the infection rate jump 59.2% YoY
 - Consumer devices saw twice as many malware infections when compared to business devices
- Infection Rates by Country and Industry
 - At 2.3%, Japan had the lowest PC infection rate per region, followed by the United Kingdom (2.7%), Australasia (3.2%) and North America (3.7%)
 - In Europe, home devices were more than three times as likely to encounter an infection as business devices (17.4% versus 5.3%)
 - Based on reported data, Health Care and Social Assistance (down 41.4% from the YoY average) led in terms of industries with the lowest infection rates, while the highest industry infection rates were seen by Wholesale Trade, Mining/Oil/Gas and Manufacturing
- Mobile and Android
 - Of the total threats detected on Android™ devices in 2020, Trojans and malware accounted for 95.9%, an increase from 92.2% in 2019
 - Outdated operating systems accounted for nearly 90% of Android infections
 - Malware for Android-based IoT devices is increasing, underscoring the importance of securing all Android devices beyond just smartphones and tablets

Methodology:

The threat intelligence, trends and details presented in the 2021 Webroot BrightCloud® Threat Report are based on data continuously and automatically captured by the Webroot® Platform, which is the proprietary machine learning-based architecture that powers all Webroot protection and BrightCloud® services. This data comes from over 285 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 advanced 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](https://www.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.

Copyright © 2021 Open Text. All Rights Reserved. Trademarks owned by Open Text. One or more patents may cover this product(s). For more information, please visit <https://www.opentext.com/patents>.

OTEX-G

View original content to download multimedia:<http://www.prnewswire.com/news-releases/opentext-announces-2021-webroot-brightcloud-threat-report-301272522.html>

SOURCE Open Text Corporation