# 2020 Webroot Threat Report: Phishing Attempts Grew by 640% Last Year

February 18, 2020

**Webroot Also Observed a 125% Increase in Malware Targeting Windows 7®**

WATERLOO, Ontario, Feb. 18, 2020 /PRNewswire/ -- OpenText ™ (NASDAQ: OTEX) (TSX: OTEX) today issued the 2020 Webroot Threat Report, highlighting not only the agility and innovation of cybercriminals who continue to seek out new ways to evade defenses, but also their commitment to long-established attack methods. Most notably, Webroot observed a 640 percent increase in phishing attempts and a 125 percent increase in malware targeting Windows 7®. The report is derived from metrics captured and analyzed by Webroot's advanced, cloud-based machine learning architecture: the Webroot® Platform.

"In the cybersecurity industry the only certainty is that there is no certainty, and there is no single silver bullet solution," said Hal Lonas, Senior Vice President and CTO, SMB and Consumer, OpenText. "The findings from this year's report underline why it's critical that businesses and users of all sizes, ensure they're not only protecting their data but also preparing for future attacks by taking simple steps toward cyber resilience through a defense-in-depth approach that addresses user behavior and the best protection for network and endpoints."

**Download the full report here.**

**Notable Findings:**

- **Phishing URLs encountered grew by 640 percent in 2019.**
  - 1 in 4 malicious URLs is hosted on an otherwise non-malicious domain.
  - 8.9 million URLs were found hosting a cryptojacking script.
  - The top sites impersonated by phishing sites or cybercriminals are Facebook, Microsoft, Apple, Google, PayPal and DropBox.
  - The top five kinds of websites impersonated by phishing sites are crypto exchanges (55%), gaming (50%), web email (40%), financial institutions (40%) and payment services (32%).
- **Malware targeting Windows 7® increased by 125 percent.**
  - 93.6 percent of malware seen was unique to a single PC – the highest rate ever observed.
  - 85 percent of threats hide in one of four locations: %temp%, %appdata%, %cache%, and %windir%, with more than half of threats (54.4%) on business PCs hiding in %temp% folders. This risk can be easily mitigated by setting a Windows policy to disallow programs from running from the temp directory.
  - IP addresses associated with Windows exploits grew by 360 percent, with the majority of exploits targeting

out-of-date operating systems.

- **Consumer PCs remain nearly twice as likely to get infected as business PCs.**
  - The data reveals that regions most likely to be infected also have the highest rates of using older operating systems.
  - Of the infected consumer devices, more than 35 percent were infected more than three times, and nearly 10 percent encountered six or more infections.
  - The continued insecurity of consumer PCs underscore the risk companies face in allowing employees to connect to business networks from their personal devices.
- **Trojans and malware accounted for 91.8 percent of Android™ threats.**

Explore all the findings here.

The 2020 Webroot Threat Report presents analysis, findings and insights from the Webroot Threat Research team on the state of cyber threats. The report analyzed samples from more than 37 billion URLs, 842 million domains, 4 billion IP addresses, 31 million active mobile apps, and 36 billion file behavior records. The statistics presented in this annual threat report are derived from metrics automatically captured and analyzed by the Webroot® Platform, our advanced, cloud-based machine learning architecture. This system provides proactive protection for users and networks against both known and zero-day, never-before-seen and advanced persistent threats. Threat intelligence produced by the platform is used by Webroot® endpoint security products and by technology partners through Webroot BrightCloud® Threat Intelligence Services.

The Webroot® Platform harnesses the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide endpoint protection, network protection, and security awareness training solutions purpose built for managed service providers and small businesses. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals.  Learn more at webroot.com.

**About OpenText**
OpenText, The Information Company™, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. 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.

Copyright © 2020 Open Text. All rights reserved. OpenText is a trademark or registered trademark of Open Text. The list of trademarks is not exhaustive of other trademarks. Registered trademarks, product names, company names, brands and service names mentioned herein are property of Open Text or other respective owners.

OTEX-G

View original content to download multimedia:http://www.prnewswire.com/news-releases/2020-webroot-threat-report-phishing-attempts-grew-by-640-last-year-301006574.html

SOURCE Open Text Corporation

Ashley Stewart, OpenText, 402-910-0140, publicrelations@opentext.com