OpenText Security Solutions Announces Nastiest Malware of 2022

10/3/2022

Analysis Reveals the Emergence of Triple Extortion and a Possible End to the Hacker Holiday

WATERLOO, ON, Oct. 3, 2022 /PRNewswire/ -- **OpenText™** (NASDAQ: OTEX), (TSX: OTEX), today announced the Nastiest Malware of 2022, a ranking of the year's biggest cyber threats. For the fifth year running, OpenText Security Solutions' threat intelligence experts combed through the data, analyzed different behaviors, and determined which malicious payloads are the nastiest. Emotet regained its place at the top, reminding the world that while affiliates may be taken down, the masterminds are resilient. LockBit evolved its tactics into something never seen before: triple extortion. Analysis also revealed an almost 1100% increase in phishing during the first four months of 2022 compared to the same period in 2021, indicating a possible end to the "hacker holiday," a hacker rest period following the busy holiday season.

"The key takeaway from this year's findings is that malware remains center stage in the threats posed towards individuals, businesses, and governments," said Muhi Majzoub, EVP and Chief Product Officer, OpenText. "Cybercriminals continue to evolve their tactics, leaving the infosec community in a constant state of catch-up. With the mainstream adoption of ransomware payloads and cryptocurrency facilitating payments, the battle will continue. No person, no business—regardless of size—is immune to these threats."

While this year's list may designate payloads into different categories of malware, it's important to note many of these bad actor groups contract work from others. This allows each group to specialize in their respective payload and perfect it.

2022 Nastiest Malware

Emotet remains the most successful botnet in existence, following a brief shutdown last year. Its job is to send malspam campaigns to billions of emails a day. It creates a foothold on a victim's computer, with follow-up malware that will then move laterally and compromise the rest of the environment before bringing in the final payload of ransomware.
LockBit is this year's most prolific and successful ransomware group. While the group has been around for about

three years as a ransomware-as-a-service (RaaS) group, they continue to advance their tactics. In addition to taking data, holding it for ransom and threatening to leak it, triple extortion adds a third layer: a distributed denial-of-service (DDoS) attack on an entire system to completely lock it down.

Conti, a RaaS malware, has been on the Nastiest Malware radar for quite some time. In February, Conti released a statement of support on their leak site for the Russian government. Shortly after a twitter account, **Conti leaks**, leaked Conti's internal chats dating back almost two years resulted in the dismantling of their leak site and command and control servers. Conti has since rebranded into multiple operations, most notably HelloKitty, BlackCat, and BlackByte.

Qbot (AKA Qakbot), possibly the oldest info-stealing trojan, still receives updates today. It moves throughout the network and infects the entire environment while "casing the joint" to allow access to as much data as possible to exfiltrate for extortion and to prepare for the final stage of ransomware payloads.

Valyria is another strain of a used-to-be banking trojan turned into malspam botnet with email attachments, turned into malicious scripts that starts an infection chain typically resulting in ransomware. The tricky part about Valyria is the complexity of the components and its ability to evade detection.

Cobalt Strike and Brute Ratel are adversarial attack simulation tools. Cobalt Strike is a pen testing tool designed by white hats; Brute Ratel was created for red teams. The purpose of these tools is to help teams simulate attacks to understand the tactics hackers use, determine security gaps, and make the appropriate changes. Not surprising, Cobalt Strike, and now Brute Ratel, are frequently used by the bad guys.

To learn more about the findings of this year's Nastiest Malware analysis, visit **Webroot Community**.

About OpenText Security Solutions

As attack surfaces expand, OpenText Security Solutions help organizations of every size achieve cyber resilience with Webroot Security, Carbonite Data Management, BrightCloud® Threat Intelligence, and EnCase Digital Forensics and Threat Response. With a united front of best practices paired with layered solutions, we prevent, detect, and restore small, mid-sized and enterprise business operations in the event of a cybersecurity attack.

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-security-solutions-announces-nastiest-malware-of-2022-301638296.html**

SOURCE Open Text Corporation