opentext™

OpenText Cybersecurity's 2024 Threat Hunter Perspective Shows Collaboration Between Nation-States and Cybercrime Rings to Inflict More Damage

2024-09-27

Adversaries are taking advantage of weak security fundamentals and a lack of countermeasures to carry out cyberattacks

WATERLOO, ON, Sept. 27, 2024 /PRNewswire/ -- OpenText™ (NASDAQ: OTEX), (TSX: OTEX) today released the results of its **2024 Threat Hunter Perspective**. The report found that the collaboration and coordination taking place between nation-states and cybercrime rings to target global supply chains and further geopolitical motives has become a signature trend in the threat landscape.

For CISOs, the question isn't whether attacks will happen, but what form they'll take and how enterprises can prepare. According to **Cybersecurity Ventures**, the cost of cybercrime is projected to reach $9.5 trillion in 2024 and is expected to increase to $10.5 trillion by 2025. To understand the current threat landscape, CISOs need to know not just the types of threats but also who is behind them, when they might occur, why they're happening, and how they're executed. Connecting these dots helps threat hunters gain a clearer picture of the risks organizations face, enabling more effective preparation and response.

"Our threat intelligence and experienced threat hunting team have found that nation-states are not slowing down and, as notable events like the U.S. presidential election get closer, every organization in the global supply chain needs to be on high alert for advanced and multiple cyberattacks," said Muhi Majzoub, executive vice president and chief product officer, OpenText. "Based on the report's findings, enterprises need to be prepared for large-scale attacks, making adversarial signals, threat intelligence and defense capabilities more important than ever."

Highlights from this year's report, which explores comprehensive findings from OpenText threat intelligence and hunters on the front lines of cybersecurity, include:

- Organized crime rings are supporting attacks by nation-states—possibly through direct collaboration or coordination—by attacking the same targets at the same time.
    - Russia has been seen to collaborate with malware-as-a-service gangs including Killnet, Lokibot,

    Ponyloader and Amadey.
  - China has entered into similar relationships with the Storm0558, Red Relay, and Volt Typhoon cybercrime rings, typically to support its geopolitical agenda in the South China Sea.
  - The top threats include Killnet (DDoS attacks), Lokibot (info-stealing malware) and Cobalt Strike (penetration testing tool used by APT groups)

- Attackers are keyed in on specific events, especially major holidays, military aid to Ukraine, turning the upcoming U.S. presidential election into a time of imminent peril. Nation-states also target specific days of the week for cyberattacks:
  - Russian cyberattack activity typically follows a Monday through Friday schedule with spikes within 48 hours of an adversarial announcement.
  - Chinese attacks don't follow a set schedule, though any data exfiltration is typically slated for Friday afternoons or Saturdays, when it's more likely to be missed, with the data broken into smaller chunks to further reduce suspicion.

- Evasion, misdirection and masquerading are helping adversaries get around defenses designed for direct attacks. Many attacks are taking advantage of weak security fundamentals, with victims increasing their vulnerability by not taking basic countermeasures.
  - Nations with weaker cyber defense infrastructure, like the Democratic Republic of Congo, Argentina, Iran, Nigeria, Sudan, Venezuela and Zimbabwe, have all been compromised, broadening the range of potential sources for a large-scale attack.
  - Global supply chains offer another indirect means of inflicting damage where the attacker might target the operations of a port or transportation network to disrupt a military aid shipment to have an indirect but significant impact on the primary target.

Additional Resources:

- To read the full report and methodology, click **here**.
- For further insights into the report, read our **blog post**.

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™ is the leading Information Management software and services company in the world. We help organizations solve complex global problems with a comprehensive suite of Business Clouds, Business AI, and Business Technology. For more information about OpenText (NASDAQ/TSX: OTEX), please visit us at **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. Readers are cautioned not to place undue reliance upon any such forward-looking statements, which speak only as of the date made. 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. Further, readers should note that we may announce information using our website, press releases, securities law filings, public conference calls, webcasts and the social media channels identified on the Investors section of our website (**https://investors.opentext.com**). Such social media channels may include the Company's or our CEO's blog, Twitter account or LinkedIn account. The information posted through such channels may be material. Accordingly, readers should monitor such channels in addition to our other forms of communication.

OTEX-G

View original content to download multimedia:**https://www.prnewswire.com/news-releases/opentext-cybersecuritys-2024-threat-hunter-perspective-shows-collaboration-between-nation-states-and-cybercrime-rings-to-inflict-more-damage-302260809.html**

SOURCE Open Text Corporation