March 6, 2023

IronNet Publishes Annual Cyber Threat Intel Report

Threat Detections, Analysis, and Insights Highlight Emerging Cyber Trends and Threat Actor Evasion Techniques

MCLEAN, Va.--(BUSINESS WIRE)-- IronNet, Inc. (NYSE: IRNT) ("IronNet"), an innovative leader Transforming Cybersecurity Through Collective Defense^{SM}, today released its **2022 Cyber Threat Intel Report**, an annual report that provides an overview of events and trends impacting the cybersecurity landscape in the past year as seen and analyzed by IronNet analysts and threat hunters. The report includes an overview of significant cyber attacks and the real-world results of those attacks, cybercrime trends, the tactics and techniques threat actors have used, and 2023 predictions.

"IronNet's Annual Cyber Threat Report informs and educates our customers and the broader community about how cyber threat actors are constantly evolving their tactics to evade detection. This report complements IronNet's capabilities for enabling security teams to be more proactive in their defenses while we continue to move the community to defend against cyber threats collectively," commented Anthony Grenga, IronNet Vice President of Cyber Operations.

"We highlight several of IronNet's detections of malicious command and control (C2) infrastructure. These enhanced detections are the result of IronNet's recent launch of IronRadar, our purpose-built threat feed that uniquely identifies and tracks attacker infrastructure as it is being stood up, allowing us to block campaigns before they progress to the attack itself," noted Grenga. "Additionally, we released new features to the IronNet Collective Defense platform, adding capabilities that enable continuous automated threat hunting and detection engineering, drawing from the vast telemetry of the IronNet ecosystem and the services we offer."

Key Trends

- 2022 was busier than ever for nation-state actors, particularly the Big 4 (Russia, China, Iran, and North Korea) who consistently used cyber operations to achieve their respective strategic goals.
- The Ukraine-Russia War instigated one of the largest displays of collective cybersecurity in history, resulting in a number of collective defense actions that have impacted the war.
- Large-scale ransomware attacks led to greater cybersecurity awareness and motivated many companies to put in place mitigations in case of an attack, leading cybercriminals to alter their targeting and tactics in key new ways.
- New features added to the **IronNet Collective Defense platform** this past year enabled the detection of various malicious alerts across enterprises in the United

States, Asia, and the Middle East that previously would have appeared as more innocuous and likely overlooked.

Detection Highlights from IronRadar

As IronNet threat hunters and analysts continue their efforts in 2023, the launch of **IronRadar^{SM}** will continue to provide unique insight into many characteristics of command and control infrastructure, allowing IronNet to map the techniques, tools, and procedures (TTPs) of how threat actors are setting up their malware infrastructure for attacks —blocking the threat before the attack causes business impact or disruption.

Resources

For more information on IronNet and how we contribute to a larger collective defense effort to protect organizations, nations, and sectors from cyber attacks, please visit our website at **www.ironnet.com**.

To learn more about IronRadar, please reference the blog post **"A new weapon against Command & Control infrastructures"**, our **white paper**, and this **video**. IronRadar is now available as an annual subscription sold directly from the **Amazon Web Services ("AWS") Marketplace**. There is also a **Free Trial** option available through Marketplace to gain access to the APIs for a limited time.

About IronNet, Inc.

Founded in 2014 by GEN (Ret.) Keith Alexander, IronNet, Inc. (NYSE: IRNT) is a global cybersecurity leader that is transforming how organizations secure their networks by delivering the first-ever Collective Defense platform operating at scale. Employing a number of former NSA cybersecurity operators with offensive and defensive cyber experience, IronNet integrates deep tradecraft knowledge into its industry-leading products to solve the most challenging cyber problems facing the world today.

Forward-Looking Statements

This press release includes "forward-looking statements" within the meaning of the "safe harbor" provisions of the United States Private Securities Litigation Reform Act of 1995, including, without limitation, statements regarding IronNet's ability to educate its customers and the broader community about cyber threat actors and the company's ability to provide visibility and detection of malicious behaviors and to help defend against increased cyber threats facing the globe. When used in this press release, the words "estimates," "projected," "expects," "anticipates," "forecasts," "plans," "intends," "believes," "seeks," "may," "will," "should," "future," "propose" and variations of these words or similar expressions (or the negative versions of such words or expressions) are intended to identify forward-looking statements. These forward-looking statements are not guarantees of future performance, conditions, or results, and involve a number of known and unknown risks, uncertainties, assumptions and other important factors, many of which are outside IronNet's management's control, that could cause actual results or outcomes to differ materially from those discussed in the forward-looking statements. Important factors, among others, that may affect actual results or outcomes include: IronNet's ability to continue as a going concern; risks and uncertainties associated with a potential filing for relief under the United

States Bankruptcy Code; IronNet's inability to recognize the anticipated benefits of collaborations with IronNet's partners and customers; IronNet's ability to execute on its plans to develop and market new products and the timing of these development programs; the rate and degree of market acceptance of IronNet's products; the success of other competing technologies that may become available; the performance of IronNet's products; potential litigation involving IronNet; and general economic and market conditions impacting demand for IronNet's products. The foregoing list of factors is not exhaustive. You should carefully consider the foregoing factors and the other risks and uncertainties described under the heading "Risk Factors" in IronNet's Annual Report on Form 10-K for the year ended January 31, 2022, filed with the Securities and Exchange Commission (the "SEC") on May 2, 2022, IronNet's most recent Quarterly Report on Form 10-Q for the quarter ended July 31, 2022, filed with the SEC on September 14, 2022, and other documents that IronNet files with the SEC from time to time. These filings identify and address other important risks and uncertainties that could cause actual events and results to differ materially from those contained in the forward-looking statements. Forward-looking statements speak only as of the date they are made. Readers are cautioned not to put undue reliance on forward-looking statements, and IronNet does not undertake any obligation to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise, except as required by law.

View source version on businesswire.com:
https://www.businesswire.com/news/home/20230306005679/en/

Investor Contact: IR@ironnet.com
Media Contact: Media@ironnet.com

Source: IronNet, Inc.