

**CISO
MAG**

beyond cybersecurity

Volume 5 | Issue 07 | July 2021

4
YEARS
ANNIVERSARY




THE INTERVIEW ISSUE

A screenshot of a Spotify web player interface. At the top left is the Spotify logo. To its right are icons for sharing, a heart (likes), and a menu. The track title "EPISODE #7" is displayed in a large, bold font, followed by the subtitle "CISO Culture is All About Focusing on the Negatives" in a smaller font. Below the text is a black and white portrait of a man with short dark hair, wearing a suit jacket over a button-down shirt. The bottom of the player features a progress bar with the time "01:12" on the left and "20:45" on the right. Below the progress bar are five circular control buttons: a double left arrow (previous), a single left arrow (previous 30s), a right arrow (play/pause), a single right arrow (next 30s), and a double right arrow (next).

A screenshot of the Spotify mobile app interface. At the top, the Spotify logo is in the upper left corner. Below it, the text 'Listen Now' is displayed in a large, bold, white font. Underneath, the episode title 'How Do We Help Small and Medium Businesses with Cybersecurity?' is shown in a bold, white font. Below the title, a short description reads: 'In this episode, Brian Pereira, Editor-in-Chief, CISO MAG interviews Chris Roberts, Researcher, Hacker, and CISO, to discuss the impact of cyberattacks on small and medium businesses.' Below the text is a red 'PLAY' button. To the right of the play button are two circular icons: a heart (like) and a three-dot menu. At the bottom of the screen is a progress bar with a white line. Below the progress bar is a row of six circular navigation icons: a double left arrow, a single left arrow, a large play button, a single right arrow, a double right arrow, and a full-screen icon. The time '01:12' is displayed on the left side of the progress bar, and '20:42' is displayed on the right side.

A screenshot of a podcast player interface. At the top left is the Spotify logo. At the top right are icons for a share menu, a heart (favorites), and a list of items. The main visual is a circular profile picture of a smiling man with a shaved head, wearing a light-colored button-down shirt. Below the photo, the text 'EPISODE # 3' is displayed in a white, spaced-out, sans-serif font. The episode title, 'How Zoom is Enhancing Security and Evolving its Product', is written in a large, bold, white sans-serif font. At the bottom, a white progress bar shows the current time as '01:12' and the total duration as '20:41'. Below the progress bar are five circular control buttons: a double left arrow (previous), a single left arrow (previous 30s), a large right arrow (play/pause), a single right arrow (next 30s), and a double right arrow (next).

Listen to the podcasts exclusively on

The Spotify logo, consisting of a green circular icon with three horizontal white lines and the word "Spotify" in white text to its right.

A promotional graphic for the CISO MAG Podcast. The background is a solid dark blue. At the top, there are two logos: on the left, the CISO MAG logo which consists of a red square containing the text 'CISO MAG' in white, with the tagline 'beyond cybersecurity' in smaller white text below it; on the right, a red microphone icon with white sound waves above it, and the word 'PODCAST' in white capital letters below the microphone. In the center of the image, the text 'LISTEN TO THE LATEST CYBERSECURITY TRENDS AND INSIGHTS BY POPULAR INDUSTRY LEADERS ON THE GO.' is written in large, white, bold, sans-serif capital letters, arranged in five lines.



 Spotify

Intel Labs' Breakthrough Research on Data Privacy and Encryption Technologies

In this episode, researchers from Intel Labs in the U.S. explain how Federated Learning and Homomorphic Encryption is driving new applications that require secure data sharing and data privacy

PLAY

A screenshot of a YouTube video player. The video title is "The Case for Virtual Cybersecurity" and it is labeled as "EPISODE #10". The video is by "Spotify", as indicated by the logo in the top left. The video features a man with glasses and a light-colored shirt. The video progress bar shows the video is at 01:12 out of 04:42. The video player controls at the bottom include a play button, a volume icon, and a full screen icon.

Listen to the podcasts exclusively on

The Spotify logo, consisting of a green circular icon with three horizontal white lines and the word "Spotify" in a green sans-serif font with a registered trademark symbol.

A screenshot of a Spotify podcast player interface. At the top left is the Spotify logo. At the top right are icons for sharing, heart, and a menu. In the center is a circular profile picture of a man with glasses. Below the picture, the text 'EPISODE # 11' is displayed. The main title 'Supply Chain Attacks and Vulnerability Disclosures' is shown in a large, bold font. At the bottom, there is a progress bar with the time '01:12' on the left and '20:41' on the right. Below the progress bar are five circular control buttons: a previous episode button (double left arrow), a previous episode button (single left arrow), a play/pause button (triangle), a next episode button (single right arrow), and a next episode button (double right arrow).

A screenshot of a Spotify podcast player. At the top left is the Spotify logo. At the top right are icons for share, heart, and a menu. The title "EPISODE #1" is centered, followed by the subtitle "How Digital Risk Management (DRM) is Changing During the Pandemic". Below this is a black and white portrait of a man with glasses, wearing a suit and tie. At the bottom is a progress bar showing "01:12" and "21:40". Below the progress bar are five circular control buttons: a previous track button, a previous track button, a play/pause button, a next track button, and a next track button.

A Spotify player interface on a dark background. At the top left is the Spotify logo. The main title 'Listen Now' is in large white font. Below it, the episode title 'CISO Culture is All About Focusing on the Negatives' is displayed in white. A description follows: 'In this episode, Adam Palmer, Chief Cybersecurity Strategist, Tenable, explains cybersecurity metrics and the CISO culture of focusing on the negatives.' Below the text is a red 'PLAY' button. To the right of the button are two circular icons: a heart and a three-dot menu. A progress bar is shown with the time '01:12' on the left and '20:42' on the right. At the bottom are five circular control buttons: a previous track button, a play/pause button (which is highlighted with a white border), a next track button, and two additional buttons for full screen and a share menu.

OUR BEST RESOURCE TO UPSKILL YOUR CYBERSECURITY TEAM'S PRODUCTIVITY

Upskill your IT teams with custom curriculum mapping, dedicated course development that targets your organization's needs, and deep analytics that always puts you in the driving seat of your team's training.

BROWSE COURSES IN YOUR FAVORITE CATEGORIES

Network Security

Secure Programming



Information Security



Data Science



Cloud Computing



CUSTOMIZATION PUSHED TO THE LIMIT

Your teams' needs are at the heart of every enterprise offering we provide so you can see real relevant results. Fast!



Create custom course
Bundles



Assign users



Track learning through
dashboard

Our top program architects help you assess the skill gaps in your teams, and then customize a learning path that addresses those gaps.

Custom
Curriculum
Mapping

Custom
Course
Development

We can even work with our industry-leading authors to create special programs just for your team.

You can also design and assign different learning paths to different groups within your organization to target specific knowledge gaps.

Assign
Personalized
Learning
Paths through
bundles

Upskill your team with
CodeRed for Enterprise







Worried About
Rising **IoT Attacks** in the
Healthcare Sector?

Join Expert-Led Webinar on

IoT Based Attacks in the Healthcare Industry: Do You Know How to Respond?

 | 15th July 2021

 | 7.30 pm IST / 8.00 am MST / 9.00 am CDT

[Register Now!](#)

Key Issues to be Addressed:

1. How is IoT used in the healthcare industry?
2. What are the major impacts of IoT in the healthcare industry?
3. Types of IoT-based attacks on healthcare devices
4. How to respond to such attacks.

Moderator:

Amol Kodag

Engineering Director – R&D, Medtronic.
Heading Cardiovascular Portfolio
at Medtronic Engineering and Innovation Center (MEIC)

Panelists:

Scott E. Augenbaum

Retired FBI Supervisory Special Agent / Cyber Division

Ricoh Danielson

Executive Cyber Security Advisor of Incident Response and
Digital Forensics at 1st Responder LLC – A Cyber Security Firm

[More Details](#)



Volume 5 | Issue 07
July 2021

President & CEO
Jay Bavisi

Editorial
Editor-in-Chief
Brian Pereira*
brian.p@eccouncil.org

Assistant Editor
Augustin Kurian
augustin.k@eccouncil.org

Sr. Feature Writer
Rudra Srinivas
rudra.s@eccouncil.org

Sr. Technical Writer
Mihir Bagwe
mihir.b@eccouncil.org

Sub Editor
Pooja Tikekar
pooja.v@eccouncil.org

Management
Senior Vice President
Karan Henrik
karan.henrik@eccouncil.org

General Manager - Marketing
Seema Bhatia
seema.b@eccouncil.org

Senior Director
Raj Kumar Vishwakarma
rajkumar@eccouncil.org

Head - Research & Content
Jyoti Punjabi
jyoti.punjabi@eccouncil.org

Publishing Sales Manager
Taruna Bose
taruna.b@eccouncil.org

Manager - Digital Marketing
Rajashakher Intha
rajashakher.i@eccouncil.org

Asst. Manager Visualizer cum Graphic Designer
Jeevana Rao Jinaga
jeevana.r@eccouncil.org

Manager – Marketing and Operations
Munazza Khan
munazza.k@eccouncil.org

Image credits: Shutterstock & Freepik
Illustrations, Survey Design, Cover & Layouts by: Jeevana Rao Jinaga

* Responsible for selection of news under PRB Act. Printed & Published by Brian Pereira, E-Commerce Consultants Pvt. Ltd.,
The publishers regret that they cannot accept liability for errors & omissions contained in this publication, howsoever caused. The opinion & views contained in this publication are not necessarily those of the publisher. Readers are advised to seek specialist advice before acting on the information contained in the publication which is provided for general use & may not be appropriate for the readers' particular circumstances. The ownership of trade marks is acknowledged. No part of this publication or any part of the contents thereof may be reproduced, stored in a retrieval system, or transmitted in any form without the permission of the publishers in writing.

EDITOR'S NOTE

FIGHTING BACK
(WE’VE HAD ENOUGH!)

The Colonial Pipeline attack on May 7 was a watershed moment in the universal fight against ransomware attacks. It was the first incident in which the ransom paid to attackers was recovered. The attack on Colonial impacted the fuel supply chain, leading to a temporary fuel shortage along the Northeast coast of the U.S. The pressure was building for Colonial Pipeline and their CEO, Joseph Blount, had to make a difficult decision – paying up. In an interview with the *Wall Street Journal*, Blount acknowledged he authorized the ransom payment of 75 Bitcoin, which is approximately \$4.4 million. A few weeks later, the Department of Justice and the FBI announced that they recovered most of the ransomware amount.

In his [blog](#) post dated June 16, Brian Krebs, Editor of **KrebsOnSecurity**, reported that the Ukraine Cyber Police arrested six people from the CLOP ransomware group. The gang reportedly extorted more than half a billion dollars from victims.

Ransomware attacks are now an everyday occurrence. A report from Cybersecurity Ventures estimated a ransomware attack on businesses every 11 seconds in 2021.

While there are numerous debates about whether impacted companies should be paying the ransom, we could soon have legislation for this. Last year, the Department of the Treasury’s Office of Foreign Assets Control (OFAC) published an advisory informing the public that the payment of ransom demanded by cybercriminals may be a violation of U.S. law.

For sure, there will be more ransomware attacks in the coming months. The adversaries see this as a lucrative opportunity, more so now, when the pandemic has office workers at home, with weak security on their home networks. Ransomware gangs are getting more organized with affiliate



Brian Pereira
Editor-in-Chief

programs. They now offer Ransomware-as-a-Service – case in point, the DarkSide ransomware group that brought Colonial Pipeline to its knees. Read more about this in “The Vulnerabilities that Open the Door to Ransomware” on page 68.

So, are we just going to sit around and watch? And become the next victim?

Isn’t it time we did something about it?

The fight against ransomware attacks goes beyond private organizations, as even governments and critical infrastructure are being attacked.

Immediately after the Colonial Pipeline attack, the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI issued a security advisory with mitigation steps to reduce the risk of compromise by ransomware attacks.

The increased involvement of APT groups who engage in cyber warfare would make it extremely difficult to contain ransomware attacks. This was on the agenda for discussion during the recent meeting between President Biden and Russian leader Vladimir Putin. There were similar discussions at the G7 meet in the U.K. in June.

Ransomware needs to be tackled on a global stage, with the involvement of governments, and organizations like Interpol, Europol, NIST, CERT, ACSC (Australia), National Cybersecurity Center (U.K.), and others.

It’s about time they banded together and fight back!

Contents

BUZZ

RANSOMWARE GETS MEATY WITH JBS ATTACK

12



INTERVIEW SPECIAL



20

"I expect security options to evolve over time with the rollout of 5G"



32

"We want to bring together incident response and security teams from every country to ensure a safe internet for all"



40

"I believe in building products and teams that are obsessed with customer success"



50

"The most hacker-resistant environment is the one that is administered from end-to-end"



60

"IoT technology will always improve but it will never be 100% secure"

INSIGHT



The Vulnerabilities that Open the Door to Ransomware

68

KNOWLEDGE HUB

How Communication Service Providers are Keeping the World Connected During COVID-19

78



86

RANSOMWARE GETS MEATY WITH JBS ATTACK

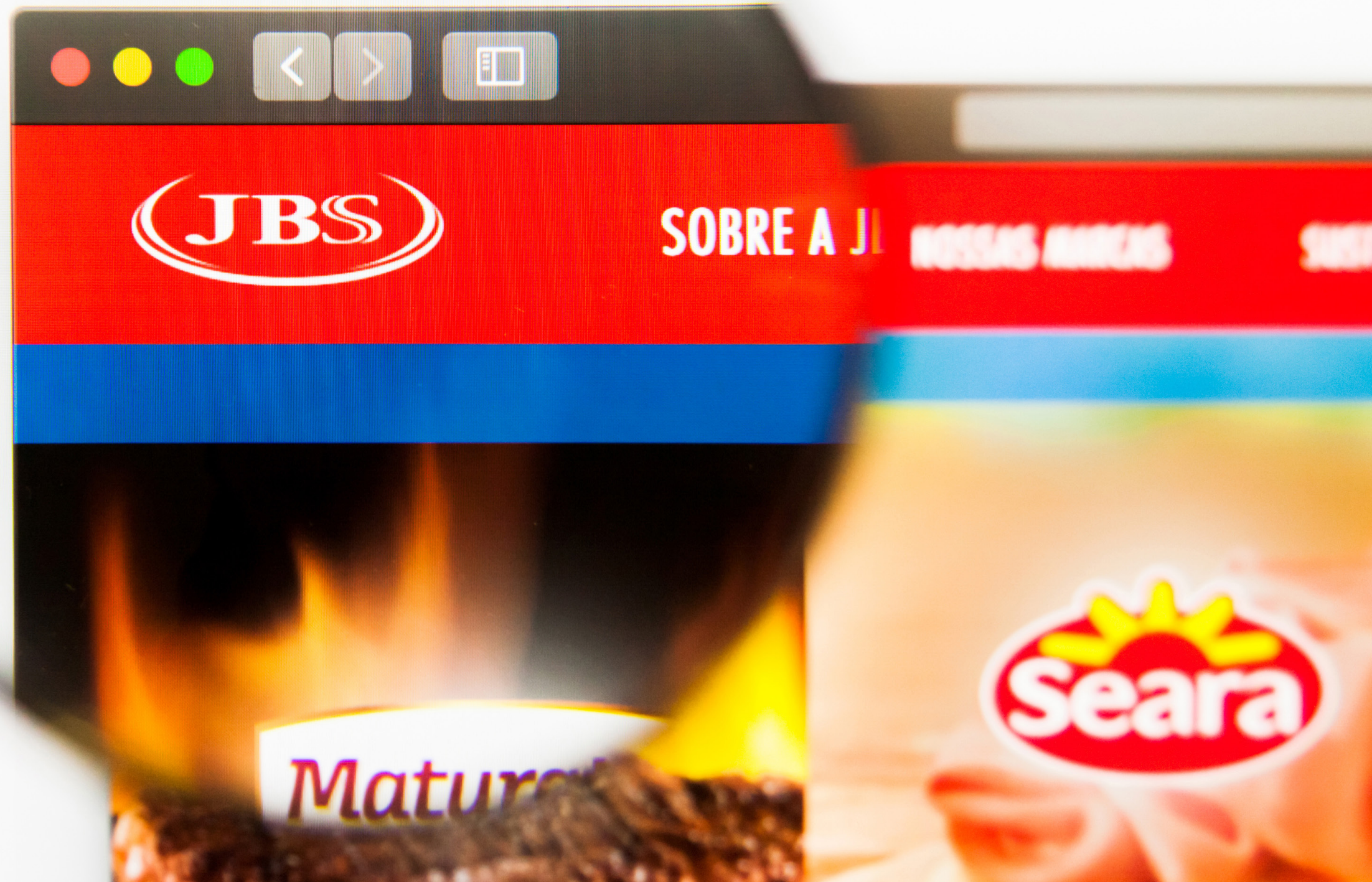
Mihir Bagwe

Sr. Technical Writer

CISO MAG

Ransomware has by far been the buzzword of 2021. Until now, ransomware attacks only appeared under the Tech section of news dailies. However, this has changed. Stories of ransomware attacks are now front page news and make it to cover stories. The modus operandi of ransomware operators has evolved over the years. They are not just looting businesses but targeting critical sectors and larger supply chains, raising the stakes for national security. Remember the [Colonial Pipeline hack](#), which virtually exhausted the entire gas supply on the East Coast? And the Babuk ransomware gang's attack on [D.C. Metropolitan Police Department](#) that acted as a roadblock for the law enforcement in the city? These attacks have grown manifold, and are found everywhere.

The dust of the Colonial Pipeline ransomware attack had just begun to settle as the U.S. Department of Justice's (DoJ) newly formed digital extortion task force [reported](#) recovering majority of the ransom paid (approximately \$2.3 million of \$4.4 million in Bitcoins) by the company to the cybercriminals. And while one company was heaving a sigh of relief, another sophisticated ransomware attack took center stage. This time, adversaries struck a meaty blow at the world's largest meat producer – JBS.





The Aftermath?

The ransomware attack on JBS' systems did not just affect its IT infrastructure; it had a ripple effect. The attack paralyzed its worldwide supply chain. It halted slaughter operations not just in the U.S. but across its units in Canada and Australia. Transactions and supplies with both – customers and suppliers – were suspended temporarily. The company issued a [press release](#) in which it deemed the incident as “organized cybersecurity attack.”

Upon discovery, JBS suspended all systems and networks that were known to be compromised and were known to have been intruded on and informed their respective law enforcement authorities in Canada, CISA and FBI.

The only silver-lining in the entire

was the fact that JBS had a data backup in place. The company issued a [statement](#) confirming that its backup servers were not affected, and thus (they were) actively working with an incident response firm to restore its systems as soon as possible.

JBS did not mention how the ransomware intruded on its systems or the perpetrators involved. But certain [news reports](#) suggested that it was the evil hand of the Russian-speaking REvil ransomware gang. The gang, the notoriously infamous gang, has been linked to many details related to the attack. Their underground network, known as “Happy Blog,” has been linked to stolen data and other cybercriminal activities.

SUBSCRIBE NOW

TO READ THE FULL ISSUE