CISO MAG

beyond cybersecurity

Volume 5 | Issue 02 | February 2021

BUZZ

Joe Biden Prioritizes Cybersecurity on His First Day in Office

KNOWLEDGE HUB

The Wild Evolution of Ransomware

UNDER THE SPOTLIGHT

“Relying heavily on firewalls does nothing against determined adversaries”

RANSOMWARE

A PANDEMIC PLAGUING THE DIGITAL WORLD

Corinium
connected thinking

MEDIA PARTNER

CISO MAG
beyond cybersecurity

9-10 February 2021

CISO Online A/NZ

Australia & New Zealand's Leading Online Event for Information Security Executives

- Future of Cyber
- Predict
- Prevent
- Respond
- Strengthen
- People
- Strategy

www.ciso-anz.coriniumintelligence.com | info@coriniumintel.con

Susie Costa,
SVP, Head of Security Management,
Sumitomo Mitsui Banking

Asaf Ahmad,
CISO APAC,
Fire & Rescue NSW

Jason Elrod,
Executive Director of Cybersecurity & Investigations,
Sutter Health

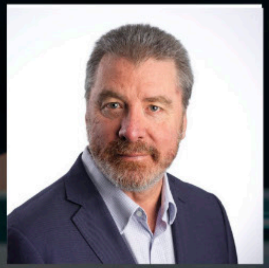
Garry Bentlin,
CSO,
TransGrid

Greg Sawyer,
Director, Cybersecurity Program,
CAUDIT

John Ellis,
CISO,
Bupa A/NZ

Narelle Devine,
CISO Asia Pacific,
Telstra

Chetan Prasad,
CISO,
Office of the Auditor-General, NZ


Rob Wiggan,
Associate Director Information,
QUT

Karthick Vankayala
Manager, Indentity & Cybersecurity
Macquarie Group

SECURE YOUR FREE PLACE

www.ciso-anz.coriniumintelligence.com | info@coriniumintel.com

CYBER WORLD

MARCH 2ND 2021
VIRTUAL CONGRESS
Join Free with Code: **CMVIP**
(T&Cs Apply)

Join Us at Cyber World Congress: 24-Hour Virtual Cyber Security Event on March 2nd!

The inaugural Cyber World Congress takes place virtually on March 2nd as a unique large-scale event to keep the cyber security community connected across the globe. As a worldwide 24-hour event, it will follow the sun by starting with speakers from the APAC region through to the Middle East & Africa, Europe, LatAm, finishing in North America. Join us online to hone your skills in areas including:

- *Securing the Modern Enterprise in a Digital World*
- *A People-Focused Approach to Security*
- *Modern Cyber Resilience for Today's Digital Environment*
- *Incident Response & Business Continuity in a Complex Threat Landscape*
- *Forward-Thinking Cyber Security for the Next Wave of Digitalisation*
- *And, more!*

CPD CERTIFIED
The CPD Certification Service

Speakers include CISOs, CSOs, and Heads of IT Security at: Sodexo, Standard Chartered Bank, Fossil Group and more...

Ashish Khanna
CISO
The Oberoi Group

Allan Tay
APAC Head of IT Security
Sodexo

Dr. Erdal Ozkaya
Regional CISO
Standard Chartered Bank

Kerissa Varma
CISO
Old Mutual

James Hamon
CISO, UK Financial Ombudsman Service

Andrea Szeiler
Global CISO
Transcom

Felipe García
CISO
Scotiabank

Julio Padilha
CSO/CISO, Sodexo Benefits & Rewards Services

Marty Ray
CISO
Fossil Group, Inc.

Liana Bailey-Crimmins
CISO
CalPERS

This is a one-of-a-kind opportunity for cyber security leaders across the globe to come together and safeguard their assets. View the agenda & secure your place for FREE using the discount code: CMVIP at: world.cyberseries.io/register/ (T&Cs apply.)

CISO MAG
beyond cybersecurity

Volume 5 | Issue 02
February 2021

President & CEO
Jay Bavisi

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

Senior Feature Writer
Augustin Kurian
augustin.k@eccouncil.org

Feature Writer
Rudra Srinivas
rudra.s@eccouncil.org

Technical Writer
Mihir Bagwe
mihir.b@eccouncil.org

Feature Writer
Pooja Tikekar
pooja.v@eccouncil.org

Web Developer
Mohammed Nadeem
mohammed.n@eccouncil.org

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

Director of Marketing
Nandakishore
nandakishore.p@eccouncil.org

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

Senior Director
Raj Kumar Vishwakarma
rajkumar@eccouncil.org

Deputy Business Head
Jyoti Punjabi
jyoti.punjabi@eccouncil.org

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

Digital Marketing and Design
Rajashakher Intha
rajashakher.i@eccouncil.org

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

Image credits: Shutterstock
Illustrations, Cover & Layouts by: Rajashakher Intha

* 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

MR. PRESIDENT, THE PROBLEM IS MUCH WORSE THAN YOU THINK

Brian Pereira
Editor-in-Chief

During a break at Camp David in 1983, President Ronald Reagan and his wife Nancy sat down to watch the evening movie *WarGames*, and was perplexed with what he saw.

WarGames (1983) is an American Cold War, science fiction technology film. David Lightman, a high school student, uses his IMSAI 8080 computer and modem to dial into systems of gaming companies in Sunnyvale, California. While war dialing numbers, David accidentally connects to WOPR (War Operation Plan Response), a supercomputer at NORAD (North American Aerospace Defense Command) — that's programmed to run war simulations.

Asking for a list of games, he stumbles upon a game with a strange name: "Global Thermonuclear War." When asked for the password, he is unable to proceed further. He asks two friends for help, who explain the concept of a backdoor password and they suggest finding a password hint in the first game in the list: "Falken's Maze." David learns that Stephen Falken was an early artificial-intelligence researcher, and he guesses correctly that Falken's dead son's name (Joshua) is the password.

David starts playing the game, takes the role of the Soviet Union, and playfully targets American cities. The computer starts a simulation that shows incoming nuclear missiles from the Soviet Union on the gigantic displays at NORAD. This shocks the military personnel as they believe it is an actual nuclear attack. The simulation escalates into something bigger, as the supercomputer takes the game to the next level. It "launches" a full-scale attack from the Soviet Union, with Soviet bombers and submarines, apart from multiple missiles. Thankfully, that was all a simulation or War Game, as everyone later realizes.

The following week, amid a meeting with military personnel, President Reagan asked if anyone had watched the movie. He then turned to General John W. Vessey, the then chairman of Joint Chiefs of Staff, and asked if this was possible.

General Vessey responded, "Mr. President, the problem is much worse than you think."

That led to the introduction of the first National Security Directive on Computer Security.

Fiction becomes Reality

Fast forward to 2020. We witnessed a large-scale attack dubbed "SolarWinds" that targeted numerous computers belonging to the U.S. government and private enterprises. Instead of nuclear missiles, the attackers dropped packages of malware on nearly 18,000 organizational networks in the U.S. and around the globe. Clearly, it was the largest cyberattack ever. The malware, which was reportedly activated in May 2020, was only detected in December, nearing the Christmas holidays. Technically speaking, only a few minutes of intrusion is enough to exfiltrate critical data if the attackers hit the bull's eye in the first go. Here, the attackers monitored the networks for nearly 6 – 9 months; so, imagine the amount of critical data they might have laid their hands on! And although Moscow denied any involvement, the White House task force said that Russia is likely behind the hack.

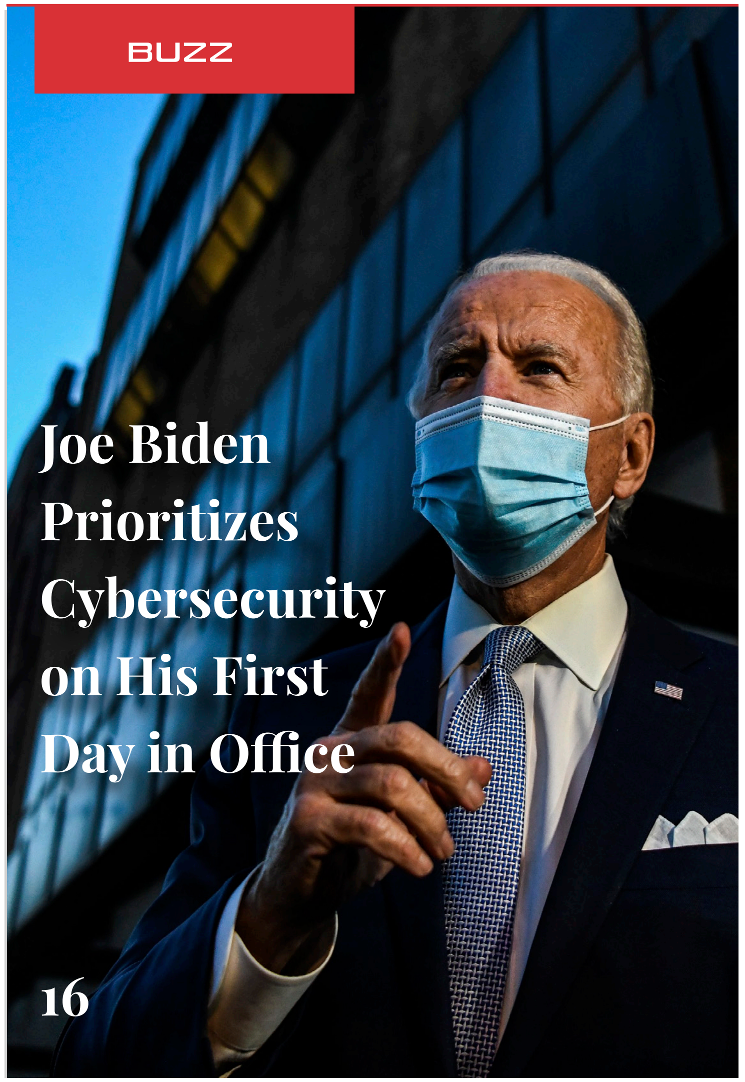
Biden has now ordered the U.S. intelligence agencies to provide him with an assessment of the SolarWinds cyberattack. History repeats itself, only this time, it's not science fiction.

The industry and government must get together to fight the dark forces of Cyberspace.

Please write to us at editorial@eccouncil.org

INDEX

Contents



Nicholas Palmer
VP-Global Sales,
Group-IB

“The thing about AI and machine learning is that it’s used by bad actors as well”

Apart from cyberattacks on the health care sector and phishing and ransomware campaigns targeting employees working remotely, 2020 also witnessed an increased surge in bot attacks. Bot attacks have also gained popularity due to their success rate compared to other vectors of cyberattacks. To discuss more about bot attacks during 2020 and the best mitigation strategies, we have **Nicholas Palmer**, **Vice President** of **Global Sales**, **Group-IB**. Since the beginning of his journey with Group-IB, Palmer has progressed through the company from a key account manager to become Head of Group-IB’s Global Business with teams reporting to him spanning Singapore, Malaysia, Vietnam, Spain, South Africa, Italy, UAE, the U.K., and the Netherlands. He is also a regular speaker at industry events such as RSA, INTERPOL World, FS-ISAC summits, CyberCrimeCon, and many others.

In an interview with **Augustin Kurian** from *CISO MAG*, Palmer reflects on the bot attacks in 2020 and their success rates. He also talks about API security and the tools that hackers favor for attacks. The latter part of the interview has interesting insights on the Group-IB’s fraud hunting platform and “smart” bot protection.

Which were the massive bad bot attacks of 2020 that had your attention? Do you believe those could have been prevented? If yes, how?

In 2020, bad bot attacks were plentiful: threat actors resorted to bots frequently to automate the process of conducting fraud, which offered them greater outreach and, hence, higher capitalization of their crimes. The application range of bot attacks is impressive, with bots generating about 30% of Internet traffic. Cybercriminals often leverage bots to compromise users' online accounts and steal their payment or personal data. There are also several known cases of bots being used as a means of unfair competition — to generate hundreds of negative comments or paid ads-clicking.

In terms of scope, the e-commerce sector was often targeted by bad bots. This was due to the proportion of valuable content available on e-commerce websites, both without authentication, such as pricing and scope, and in users' accounts; the lack of appropriate protection measures; or their ineffectiveness against bot threats. Group-IB has observed a number of large-scale bot-attacks aimed at getting access to users' reward points in online stores, their travel miles, or even personal data. Such attacks were characterized by the high intensity of requests, totaling up to 90% of all website traffic at some point. Apart from direct financial losses, bot attacks can create inconvenience for legitimate users who might have problems accessing the website.

Most of these incidents could have been prevented if a proper mechanism for checking all the requests and their source was in place. The thing about AI and machine learning is that it's used by not only good guys but by bad actors as well. To shield against advanced bot attacks, one should not only analyze the source of requests, the frequency of requests from the same IP address, but also behavioral parameters like whether the request was generated by a browser or some tool like Selenium, to imitate user activity, and if it is the result of the user's activity in a mobile or web app.

According to your research, three out of 100 user sessions at banking and e-commerce portals worldwide appeared to be fraudulent, with malware attacks, social engineering, and bot activity as the top three threats for users of e-commerce and banking portals. Following the same chronology, among these top three threats, which sees the maximum rate of success?

These three attack vectors compete in effectiveness, and we often see that one attack vector serves as a continuation to another. We have recently seen online fraud with the use of a Trojan utilizing the Android Accessibility Service for the bot-generated money transfers in mobile banking. In addition, sometimes it is difficult to distinguish between these three vectors.

Bots, however, have been gaining popularity lately with the highest success rate. It relies less on the human factor. In addition, tools for bot development are becoming more unified, diversified, and effective, reducing the entry threshold for conducting bot attacks.

While there are automated bots that snatch the best deals and win giveaways, there are also dangerous ones that break into online accounts, steal users' payment and personal data, and abuse APIs while imitating human behavior. Do you think the cybersecurity industry is giving enough to API security?

We have seen a number of huge portals that have to deal with bad bots because of outdated and irrelevant security solutions. API abuse is something that is on the rise. While more and more financial institutions and services for banks utilize APIs to fill their apps with data, fraudsters are taking advantage of this. As a result, businesses need to analyze requests to their API. Every business owner should ask themselves these questions: Can they detect illegitimate API requests versus real ones? Can they spot automated behaviors on the API and link those requests to certain individuals? And do they have the technical capabilities to do so?

Which are the most frequently used tools in bot attacks that cybercriminals use to imitate user actions for credential stuffing or brute-force purposes? Do you think traditional fraud detection solutions find it difficult to spot them?

A combination of Selenium Library and Headless Chrome is among the most common tools used by fraudsters to imitate human activity. These tools are usually employed by app developers for testing.