CISO MAG

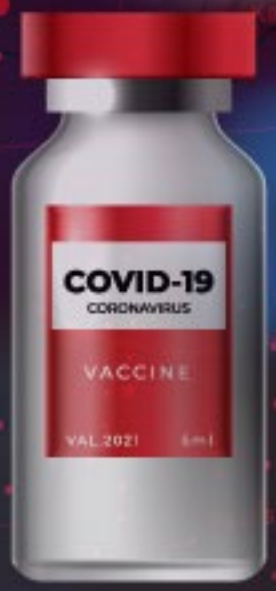
beyond cybersecurity

Volume 5 | Issue 04 | April 2021

"My biggest concern is sabotage of the vaccine either through propaganda or manipulation"

Heath Renfrow
CISO, Conversant Group / Former CISO, United States Army Healthcare

UNDER THE SPOTLIGHT 20



Protecting the COVID-19 Vaccine Supply Chain from 'Cold'-hearted Phishers

INSIGHT 28

5 Critical Responsibilities of a CISO, Post-COVID-19

58 KNOWLEDGE HUB

ADVERSARIES ON A VACCINE TRAIL

CISO MAG
beyond cybersecurity

Volume 5 | Issue 04
March 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

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
Rajashakher Intha
rajashakher.i@eccouncil.org

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

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

Image credits: Shutterstock & Freepik
Illustrations, 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

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

LEVERAGING FUD FOR OPPORTUNITY

It would not be an exaggeration to say that COVID-19 vaccines are the most sought-after commodity today. In February, the UN announced that more than 130 countries don't have a single COVID-19 vaccine, while 10 countries have already dispersed 75% of all vaccines. In recent weeks, countries announced their second and third lockdowns, acknowledging another COVID-19 wave of infections.

Vaccine producers are working overtime to produce enough vaccine doses to fulfill government commitments and timelines. While pharmaceutical companies stepped up their production schedules to develop and test vaccines, adversaries tracked the news and devised campaigns to leverage the momentum generated by news coverage. They capitalize on the fear, uncertainty, and doubt (FUD) of people to spread misinformation and to plan attack vectors. The result: phishing campaigns with vaccine themes, malware attacks for exfiltration of sensitive and personal information, and clinical trial data. Fake websites purporting to offer (mis)information about vaccine distribution. There are attacks on supply chains and networks of Pharma companies too.

ATTACKS ON PHARMA NOT NEW

But the attacks are not new to this industry. They happened even before the onset of the pandemic. Pharma companies were targeted whenever they were mentioned in the news. For instance, in early 2019, many Indian pharma companies were applying for FDA licenses for manufacturing – and then exporting drugs to the U.S. The FDA mandated certain policies for these companies to protect their intellectual property and infrastructure. A security researcher quoted in our cover story confirms these companies were attacked then but they did not report it. The attacks caught the media's attention only when the pandemic set in, last year.

And it's not just India.

According to a report by Cyfirma that was shared with Reuters, the target countries are U.S., U.K., India, Japan, Australia, South Korea, Italy, Spain, Germany, Brazil, Taiwan, and Mexico.

#VAXFRAUD, FAKE WEBSITES, PHISHING

Adversaries are also capitalizing on the fear and anxiety of citizens who are anxiously waiting for an appointment for their vaccine shots. Fake websites and fraudulent social media posts are their channels of deceit and misinformation. Scammers consistently use social media platforms to market themselves. These criminals impersonate legitimate pharmaceutical companies or lie about being able to sell vaccines. Social media platforms are also being used to sell fraudulent vaccines or drive people to phishing sites that can steal their money or credentials, sell them a potentially deadly product, or move the scam offline through private messaging.

Consumers are also facing the fury of adversaries, in the form of targeted phishing attacks. In an analysis conducted between October 2020 and January 2021, Barracuda researchers witnessed a 26% increase in the number of these phishing attacks, including a 12% spike in November 2020, following the announcement of the availability of vaccines by pharmaceutical companies like Pfizer and Moderna.

In the months ahead we can expect more attacks on pharma companies. Phishing attacks will become more sophisticated and targeted. And there will be tens of thousands of new fraudulent websites.

To counter this, security researchers advise governments and pharma companies to take a "defense in depth" strategy and view the situation holistically, to safeguard all stakeholders.

Read more about this in the feature articles, interviews, and the cover story within this issue.

INDEX

Contents

COVER STORY 36

Adversaries on a Vaccine Trail

EC-Council CodeRed
Tackling the Skills Gap through Commitment, Collaboration, and Change
06 CAMPUS CORNER

BUZZ 08

Chinese Hacking Group RedEcho Targets Indian Power Sector

KNOWLEDGE HUB 58

5 Critical Responsibilities of a CISO, Post-COVID-19

TABLE TALK 68

McAfee Reveals the Unknown About Babuk Ransomware

John Fokker
John Fokker, Head of Cyber Investigations and Principal Engineer
McAfee

UNDER THE SPOTLIGHT 20

"My biggest concern is sabotage of the vaccine either through propaganda or manipulation"

Heath Renfrow
CISO, Conversant Group / Former CISO, United States Army Healthcare

INSIGHT 28

Protecting the COVID-19 Vaccine Supply Chain from 'Cold'-hearted Phishers

KICKSTARTER

74 In ByteChek, Companies Can Find the "X" Factor for Cybersecurity Compliance

82 REWIND

EC-Council CodeRed

Tackling the Skills Gap through Commitment, Collaboration, and Change

Security leaders have been talking about the global cybersecurity skills shortage for years, urging people to upskill and join this growing industry. However, despite various initiatives, it appears that this gap is only growing.

For many years, cyberattacks have made headlines for causing irreversible damage to - organizations, both financially and, more importantly, to their reputation. With the onset of the pandemic, more and more businesses, big and small, have begun to shift to a digitized platform, leaving cyberspace, increasing their vulnerability and dependence on cybersecurity capability. With such a drastic shift initiated so rapidly, upskilling and bridging the growing cybersecurity skills gap has become of paramount importance.

With a vision to create a skilled cybersecurity workforce and provide continuous online learning to millions of students across the country, **EC-Council,** the world's leading cybersecurity certification body, has announced cost-effective course bundle solutions to empower learners with future-ready cybersecurity skills. As a part of this initiative, courses from EC-Council's leading-edge continuous learning platform - **CodeRed**, have been made available to students and faculty via **EC-Council Academia**. Students have access to the latest and most relevant cybersecurity courses developed by world-leading practitioners. The new box bundles provide a curated collection of critical, vetted, cost-effective solutions for selective learning that gives organizations, educators, and individuals a chance to advance without accessing the entire course library.

They will be able to develop skills in a wide range of topics, including defending against cyberbullying, conducting reconnaissance for cybersecurity, adopting security and privacy in data, cybersecurity basics for summer learning - university edition, and cybersecurity basics for summer learning - high school edition.

Organizations, educators, and individuals can now access these pre-curated course bundles created based on various job skills by CodeRed's expert content team. It's an affordable way to get a premium education and improve one's skills. This initiative and the new updates and offerings on CodeRed will inspire more professionals and aspirants to upskill and join the cybersecurity field.

In addition, EC-Council has also announced a series of updates to its flexible, continuous learning platform. These changes will keep its users connected to the platform's engaging content, instructional strategies, and professional learning resources wherever learning is taking place, and give them an even more robust, secure, and reliable learning experience.

Among the updates to CodeRed's learning platform is the introduction of 40 new courses in the following categories - Network Security, Data Science, Information Security, Secure Programming, and Cloud Computing.

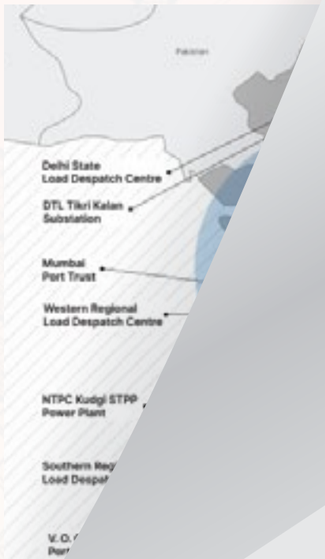
CHINESE HACKING GROUP REDECHO TARGETS INDIAN POWER SECTOR

Brian Pereira
Editor-in Chief
CISO Mag

Rudra Srinivas
Feature Writer
CISO Mag

Relations between India and China deteriorated after troops from both sides engaged in a skirmish along the LAC (line of actual control) in May 2020. While diplomacy and multiple rounds of talks involving both sides have thwarted a direct war, cyber espionage operations from state-sponsored attackers continue to disrupt organizations in India. Cybersecurity experts uncovered a Chinese hacking group's cyber campaign targeting India's power grid and transmission sector. It is being widely speculated whether a grid failure and power outage in Mumbai October, may have been caused b same group (See box).

Research from security firm **F Future** found a China-link



actor group dubbed **RedEcho**, targeted 10 Indian power sector companies and two seaports since early last year. The latest attack occurred on February 28, 2021. Recorded Future's threat research team **Insikt Group,** uncovered a subset of the servers that share some common tactics, techniques, and procedures (TTPs) with several previously reported Chinese state-sponsored groups.

In its report – "China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions" Recorded Future cites geopolitical d heightened border clashes sian neighbors as the s The report post-

SUBSCRIBE NOW
TO READ THE FULL ISSUE

cisomag.eccouncil.org

SCAN AND STAY UPDATED WITH
REAL TIME CYBERSECURITY NEWS