UNMASKED

CYBRARY.IT

FEBRUARY 2018 | EDITION 4

TAKING THE MYSTERY OUT OF CYBER SECURITY

IN THIS ISSUE

EDITOR'S NOTE

Healthcare is an industry which has been getting a lot of unwanted attention in the realm of cyber. As more medical devices become connected to the growing network of IoT devices, the risk for those using those devices increases.

Often, medical staff do not have any **cyber security** training and can fall victim to phishing and social engineering.

That being said, we want professionals in every industry to know that Cybrary has resources available for them, like a **HIPAA Course** for healthcare professionals.

Cybrary's own Kathie Miley, who has held a HIPAA certification will be speaking at this year's **HIMSS conference** on March 7th in Las Vegas. If you're in the healthcare profession, we urge you to attend and listen to her message on the value of training for those in the industry.

Olivia Lynch **(@Cybrary_Olivia)** is the Marketing Manager at Cybrary. Like many of you, she is just getting her toes wet in the field of cyber security. A firm believer that the pen is mightier than the sword, Olivia considers corny puns and an honest voice essential to any worthwhile blog.

CYBRARY

CYBER SECURITY NEWS

#CRYPTOMINING

Yes, every company is susceptible to cryptocurrency mining, even Tesla. And with new headlines emerging each day, it seems the tactics are becoming more complex.

In this latest incident, it appears Tesla's AWS account was breached by hackers who leveraged it's computing power for their own benefit. Discovered by security researchers at RedLock, the hackers were allegedly able to access the administration portal for Tesla's Kubernetes account, which was not password protected. Because that makes sense. It was there that credentials for the Tesla AWS environment were stored, in addition to an Amazon S3 bucket with sensitive data regarding Tesla cars. While it is not yet clear how much profit the hackers gained from their crypto mining scheme, the

tactics they used for hiding the true IP address of the mining-pool server behind a CloudFlare hosted IP address points at the lengths adversaries are taking to make their crypto mining efforts successful.

RedLock reported the issue to Tesla who has since handled the problem. Although no customer data was exposed, drivers of Tesla vehicles should be concerned about hackers gaining control of their largely computerized vehicles. This very concern is top of mind for CEO Elon Musk who said, "I think one of the biggest concerns for autonomous vehicles is somebody achieving a fleet-wide hack." Let's hope Tesla makes some immediate changes to the security of their passwords.

Dive into the world of autonomous cars in this popular blog 'Self-driving Cars: An Introduction.'

#CRASHED

It's rare we see Apple on red alert, but after the discovery of a vulnerability known as "one character to crash your iPhone," which was widely publicised, the company rushed to roll out a fix.

Officially known as CVE-2018-4124, this bug leverages the Telugu language, a widely-spoken Indian language. The font-rendering of Telugu seemed to be too complex for both iOS and macOS, specifically when devices tried to process a Telugu character formed by combining four elements of the writing system. "Unusual combinations of characters sometimes cause much more

"We maintain a bug bounty program to encourage this type of research, and we addressed this vulnerability within hours of learning about it. The impact seems to be limited to internally-used engineering test cars only, and our initial investigation found no indication that customer privacy or vehicle safety or security was compromised in any way."

-Tesla statement

programmatic trouble than you'd expect, as when six ill-chosen characters brought Apple apps down, back in 2013," writes Naked Security. This because was particularly worrisome because a notification containing the character would cause the main iOS window to crash and restart continuously. That means abusers could easily copy and paste the character into a message, crashing the phone of the recipient.

That said, Apple needed a solution quickly and has since released an update that should remedy the bug for all its operating systems and devices, including TVs, watched, tablets, phones, and Macs. Users will need to update to iOS 11.2.6 or macOS High Sierra 10.13.3 Supplemental updates. In a brief of the bug, Apple said the flaw occurred via "A memory corruption issue that was addressed through improved input validation." While this may not have seemed too serious of an issue to some, Motherboard contributor Joseph Cox pointed out that the symbol could crash Apple's networking application by typing it in the name to the wi-fi network.

"A Twitter user with the symbol in their screenname 'liked' one of my tweets late on Thursday night. Shortly after the notification popped into my feed, my Twitter app on iOS became briefly unresponsive before crashing"
-Joseph Cox

Are iPhones Safe from Virus Attacks? This blog has the answer.

#PHISHING

Another day, another email scam. The latest wave is business email compromise (BEC) campaigns targeting Fortune 500 company employees meant to convince the victims to complete fraudulent wire transfers.

According to researchers, this dangerous new trend originated

in Nigeria and is attractive to criminals because these campaigns are fairly simple to conduct. Based on phishing and social engineering tactics, criminals will take over a trusted users email account and target companies that conduct international wire transfers. The campaigns have been targeting retail, healthcare, and financial markets primarily and show no signs of slowing down. One report predicts that BEC attacks will result in over $9 billion in losses in 2018, up from $5.3 billion at the end of 2016. "Organizations need to focus on implementing technical controls to mitigate BECs and also on training employees to spot the signs of phishing emails and suspicious activity," said Sean Cavanaugh, senior incident response analyst at IBM X-Force.

The emails used during this particular BEC campaign take advantage of publicly available company information and contain an attached link that looks like a business document that redirects targets to a fraudulent DocuSign portal. The portal prompts the target to authenticate with their

email provider or business user credentials. Since the targeted user accounts were not protected with multi-factor authentication, attackers could directly log into those accounts without compromising the organization's internal network while evading detection. With the businesses' web portals, hackers had a view into Accounts Payable personnel with the ability to wire payment. Details of targeted companies have not been released, but everyone is encouraged to use catution when opening emails.

Explore phishing campaigns in-depth. Read The 5 Phases of a Phishing Attack

"Although BEC scams are not new, the examples described here detail how attackers used stolen email credentials and sophisticated social engineering tactics without compromising the corporate network to defraud a company"
-X-Force report

FACT BYTE

Cybercrime costs businesses close to $600 billion or 0.8 percent of the global GDP

-The Economic Impact of Cybercrime- No Slowing Down Report

MEET THE CYBRARIAN

Gina Palladino

Owner of Silver Tree Consulting for over 14 years, Gina has expanded her services beyond that of marketing consulting work to also help individuals go further in their careers. She's written numerous posts on Cybrary about career development and plans to teach a resume writing course on the site soon.

One of her most popular posts, **'How Do You Turn Your IT or Cybersecurity Hobby into a Career?'** offers guidance for those looking to transition into cyber. Gina says, "Essentially, they like to understand, build and un-build (reverse engineer) all kinds of things, including non-tech items." Does this describe you? Read more for insight.

READ MORE

TEACH ON CYBRARY

SECURITY+ BUNDLE

If you're looking to get Security+ certified, Bundles on Cybrary are a great way to help you achieve that goal. Backed by CompTIA, this package offers a virtual lab, practice exam, and an exam voucher (US residents only) for the best deal on exam study materials.

CompTIA CERTIFIED

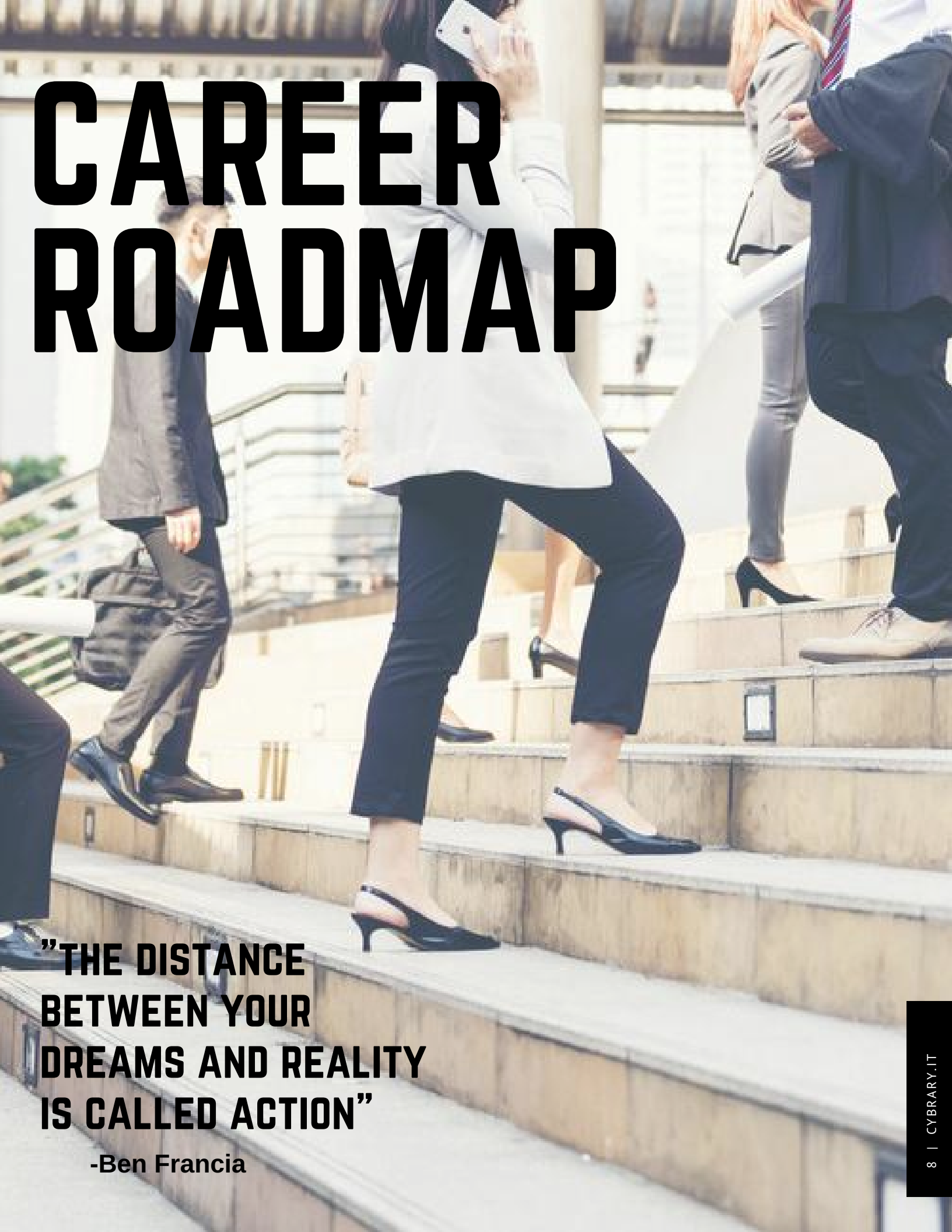
Get Certified

ESCALATE

'Escalate' your security skills with the immersive assessment environment from Point3 Security. For less than the cost of a bootcamp, Escalate offers 24/7, hands-on-keyboard, capture-the-flag tasks with a live mentor. Users are provided with learning in advanced subjects including malware reverse engineering and network security monitoring, among others.

ESCALATE
A POINT3 SECURITY ECOSYSTEM

Level-Up your Skills



CAREER ROADMAP

"THE DISTANCE BETWEEN YOUR DREAMS AND REALITY IS CALLED ACTION"

-Ben Francia

GET THE CISO PERSPECTIVE

The Chief Information Security Officer (CISO) is an essential part of every organization. They serve as a senior-level executive responsible for establishing and maintaining the vision of an enterprise and making sure all information and technology assets are protected.

Cybrary's CISO training course is useful for IT professionals looking to move up in their organization as well as current CISOs who would like to renew their certification and/or stay on top of the latest trends within the industry. Among the key topics, you'll learn how to implement the proven best practices that make for successful cyber security leadership.

Start CISO Course

Cognizant Information Security Engineer

Required Knowledge & skills

Follow the track of an industry leader's job description. Click the buttons below to view courses and supplemental materials that will put you on the path to this career

Ability to look across multiple systems and networks to troubleshoot security issues	Security+
Experience with security reporting and communication of effectiveness of security controls	CYBRScore
Create and engineer systems or procedures to solve complex problems	Certified Ethical Hacker
Work with IDS/IPS, access control, and antivirus solutions	Network Security Tools
Provide technical consultation and insight in Identity and Access Management	Access Control

Career Path Beta Program

Cybrary Career Paths is a new program with the main goal of accelerating your journey to a successful technical career by providing training for technical positions with industry leaders like Cognizant.

Apply Today

Cisco 2018
Annual Cybersecurity Report

MAKING CONNECTIONS

THE EVOLUTION OF MALWARE

"The advent of network-based ransomware cryptoworms eliminates the need for the human element in launching ransomware campaigns. And for some adversaries, the prize isn't ransom, but obliteration of systems and data, as Nyetya—wipe malware masquerading as ransomware—proved. Self-propagating malware is dangerous and has the potential to take down the Internet, according to Cisco threat researchers," the report states.

Read the Blog

Download the ACR