UNMASKED

CYBRARY.IT

FEBRUARY 2018 | EDITION 3

TAKING THE MYSTERY OUT OF CYBER SECURITY

IN THIS ISSUE

EDITOR'S NOTE

At Cybrary, we're dedicated to helping our users get the training they need to start or advance in their careers. With a career-focused approach in mind, we understand that it can sometimes be difficult to know whether or not you're qualified for a job just based on a description.

In cybersecurity and IT specifically, the uptime in getting hired to actually working on necessary tasks is almost immediate; at least for most major organizations. But what if you had a way of completing training prior to getting hired based on a specific job description?

With our new beta program, Cybrary Career Paths, now you can. With this program, Cybrary is accelerating your journey to a successful technical career by providing training for technical positions with industry leaders like Cognizant.

Apply Today! Space is limited.

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

Another day, another headline about cryptocurrency miners operating in stealth where they shouldn't be. It seems over 4,200 websites were infected by a Monero cryptocurrency miner via Browsealoud.

Of the infected sites were UK and US government websites which use Browsealoud, a hosted accessibility service, to read website content aloud for the visually impaired. While no customer data was compromised or lost, an investigation by Browsealoud developer, Texthelp, is underway. CTO and data security officer for Texthelp, Martin McKay, said, "Texthelp has in place continuous, automated security tests for Browsealoud, and these detected the modified file and as a result, the product was taken offline." It appears the exploit was only active for 4 hours

after being discovered by security researcher Scott Helme. Helme was prompted by a friend to investigate after that individual received an antivirus software warning on the UK Information Commissioner's office website.

A closer look revealed Browsealoud had been compromised by hackers who altered its hosted JavaScript files. According to Helme, hosted assets are a prime target and can be used to infect thousands of websites. While it's unclear how much Monero was generated from this scheme, it is clear that the attack could have been prevented using 'subresource integrity.' Recently, cryptomining has risen in commonality ass cryptocurrency has risen in popularity.

To learn more about the recent Monero botnet, read last week's edition of UNMASKED.

#MALWARE

Sure, 'Olympic Destroyer' would be a cool name for one of the Winter Olympians, but unfortunately, it's the name of malware behind a recent attack against this year's Games in PyeongChang.

Initially deployed during the Games' opening ceremony on February 9th, this malware strain was credited with disrupting broadcasts and taking down the official Winter Olympics website. It's believed that the attack's purpose was to take down systems rather than steal information, but details surrounding the attack are continuing to unfold.

"It was pretty alarming to realize that they were running a crypto miner on their site, their whole site, every single page. … I quickly realized though that this script, whilst present on the ICO website, was not being hosted by the ICO, it was included by a 3rd party library they loaded."
-Scott Helme

Researchers from Cisco Talos, upon further analysis, believe the malware wipes files on shared network drives, rather than targeted single endpoints, as they initially thought. "Olympic Destroyer's goal is to make systems unusable by deleting shadow copies, event logs and trying to use PsExec & WMI to further move through the environment," the researchers wrote. This malware also includes a binary which allows user credentials to be easily stolen.

Perhaps most terrifying is that the author of this malware appears to have direct connections inside of the Games. Based on the technical details, that person intimately knew the infrastructure including usernames, the domain server names, and passwords. We're holding our breath on the discovery of who is behind this attack, but motivations among hackers for targeting the Olympics are pretty clear. In the meantime, researchers will be monitoring the binaries associated with the attack, as it seems each new attack adds credentials to the existing code. These new credentials can in turn be used on newly infected systems via propagation.

"Disruption is the clear objective in this type of attack and it leaves us confident in thinking that the actors behind this were after embarrassment of the Olympic committee during the opening ceremony"
-Cisco Talos researchers

For an inside look at new strains of malware, read 'Fileless Malware.'

#VULNERABILITIES

February may be the month of love for most, but for Microsoft, it's the month of vulnerabilities. The company recently patched 14 considered critical but left a Skype vulnerability unpatched.

Among the flaws addressed this month, Microsoft patched issues

mostly in the Edge browser and Outlook client. One of the most severe bugs identified is a memory corruption vulnerability (CVE-2018-0852) in Outlook which can be exploited to achieve remote code execution. "The end user targeted by such an attack doesn't need to open or click on anything in the email – just view it in the Preview Pane. If this bug turns into active exploits – and with this attack vector, exploit writers will certainly try – unpatched systems will definitely suffer." Hackers have been actively moving towards bugs that can be exploited without a user opening or clicking on anything, which is especially dangerous.

In addition to the vulnerabilities that are being handled by Microsoft, the service Skype, which they own, has a bug that will not be patched in the near future. This bug could potentially allow attackers to gain full control of the host machine by granting system-level privileges to a local, unprivileged user. In order to fix this flaw, Microsoft would be required to perform a significant software rewrite. So, until the

company is ready to issue a completely new version of Skype, users are warned to proceed with caution. Unfortunately, Skype has been dealing with a few security flaw recently. Those who have it installed on their computers are advised to run updated anti-virus software.

Check out the results of a previous Patch Tuesday from Microsoft, read this previous edition of UNMASKED.

""The exploitation of this preferential search order would allow the attacker to hijack the update process by downloading and placing a malicious version of a DLL file into a temporary folder of a Windows PC and renaming it to match a legitimate DLL that can be modified by an unprivileged user without having any special account privileges."
-HackerNews report

FACT BYTE

People ranked security as the highest priority for logging in to the majority of applications, particularly when it came to money-related apps.

-The IBM Security: Future of Identity Study

MEET THE CYBRARIAN

Dave Tuckman

Dave, President and Owner of Golden State Web Solutions (GSWS), has always been a big supporter of Cybrary. Recently, he passed his CISM certification exam using our free CISM course. In a blog post discussing his studying strategies, Dave offers great advice for those preparing for any exam.

His biggest takeaway from the experience- Practice real test simulation exams. "As it gets closer to your exam date, take some tests under conditions that mimic the actual exam – for example, four hours to answer 150 questions. That will build your mental calluses for the big exam."

Start CISM Course

Browse Practice Tests

Network Operations and Security

In the Network Operations and Security Course by Michael Redman, students will get a thorough deep dive into network operations, focusing on core concepts that will help them pass the Network+ exam. You will learn about Ethernet basics, TCP/IP, and wireless networking.

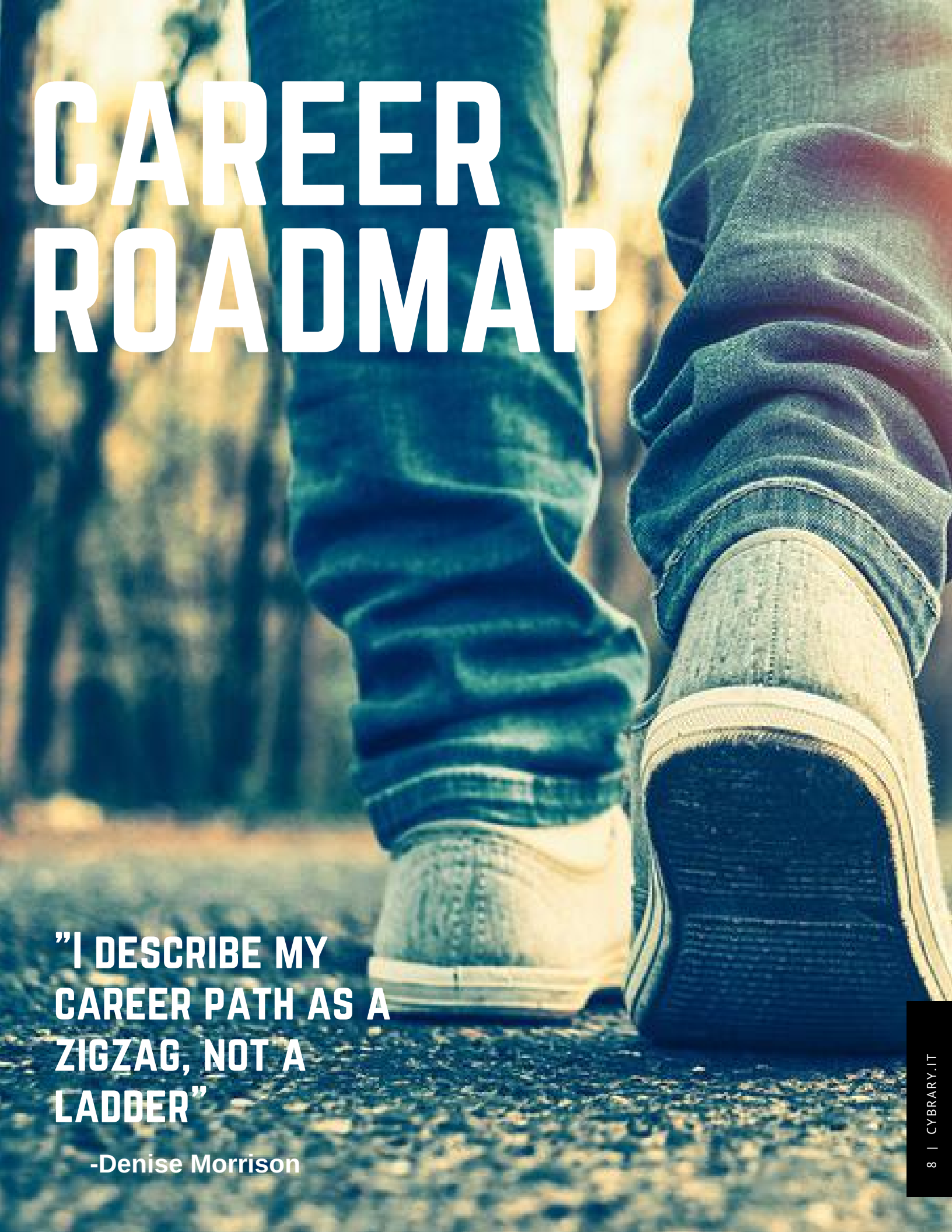
Dive Into the Course

CompTIA CySA+ Virtual Lab

The CompTIA Cybersecurity Analyst CS0-001 Virtual Lab will prepare you to plan and execute critical security measures to protect key networks and systems from attacks.

Professionals looking to gain an understanding of different security tools and practices will benefit from The CompTIA CySA+ Lab.

Enter a Virtual World



CAREER ROADMAP

"I DESCRIBE MY CAREER PATH AS A ZIGZAG, NOT A LADDER"

-Denise Morrison

TRAINING IS TRENDING

Employee Training Tops List of Financial CISO Priorities

“The bottom line is that employees must be held responsible and accountable for cybersecurity training and they need to understand the basics of cyber hygiene – it’s not just the job of the CISO or IT security teams anymore."
-Cybrary COO, Kathie Miley

Read Full Article

Cognizant Soc Analyst

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

Configure and use threat detection tools	CySA+
Develop protection plans for incident response	Incident Response
Perform data analysis and interpret the results to identify vulnerabilities	Malware Analysis
Work with IDS/IPS, access control, and antivirus solutions	Network Security Tools
Develop secure networks, identify breaches in real-time and respond to an attack	CASP

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

MAKING CONNECTIONS

What Can the winter olympics Teach Us About Cyber Security?

"Although the Olympics are a global, highly publicized event with an especially complex attack surface, it appears that the trend towards more layered security leveraging multiple vendors and devices will only continue to grow. Practitioners should prepare to defend their organizations as though this was already the case; closely examining vendors and aligning policies to ensure ultimate protection and pinpointing exactly who is responsible for the security of IoT devices."

Read More

Explore the Blog