UNMASKED

CYBRARY.IT

FEBRUARY 2018 | EDITION 2

TAKING THE MYSTERY OUT OF CYBER SECURITY

IN THIS ISSUE

EDITOR'S NOTE

We'd like to thank all of our users for helping us to win the **Cyber Security Excellence Best Education Provider Award** for the third year in a row. This great honor is just another example of how the Cybrary community comes together to do something powerful. We truly appreciate the constant support and contributions.

In 2018, it is our goal to continue expanding our catalog of free courses so that everyone, everywhere, has the resources they need to be competent and confident. But again, we need your help in doing so.

Anyone can create a course on Cybrary and those who do not only help the community and showcase their skills, but they can also make money. The only qualification needed is that you have knowledge to share. If you are interested in teaching on Cybrary, you can submit your content **here.** Someone from the Cybrary team will be in touch once you do!

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

#CYBERCRIME

The US Justice Department recently indicted 36 people in what's being called one of the largest cyber ring takedowns.

Started by a Ukranian national, Svyatoslav Bondarenko, the cyber ring known as 'Infraud,' which operated under the slogan of "In Fraud We Trust" was a forum that allowed cybercriminals to buy and sell a variety of personally identifiable information (PII) including social security numbers and passwords. This ring is said to have generated those involved more than $530 million over the past 7 years. Of the 36, 13 defendants were arrested in the United States after a Las Vegas grand jury indictment was unsealed. "Over the course of the Infraud Organization's seven-year history, its members targeted more than 4.3 million credit cards, debit cards, and

bank accounts held by individuals around the world and in all 50 States," says the Assistant Attorney General, so needless to say, this is a big win in the realm of cybercrime.

While the unsealed indictment does not indicate that Infraud members committed any data breaches, it does confirm that with over 10,900 members, it was a premier destination for illegal online activity that provided an escrow service that members could use to transact business using digital currencies. The indicted individuals are being charged with racketeering and fraud among other charges and could serve upwards of 20 years in prison.

If you're curious about what are the laws governing cybercrime, read this blog 'Cybercrime and Punishment: Who's Actually Paying the Price?' to dive in.

#CRYPTOMINING

Cryptocurrency is the new, popular kid in town, but too bad crypto-mining is making it the bully as demand continues to rise. In two different cases, malware has leveraged the power of victims devices to mine more currency.

Kaspersky researchers discovered fake antivirus and porn Android apps infected with malware used to mine Monero. It appears this malware also has the capability to launch DDoS attacks and perform other malicious tasks. Dubbed 'ADB.Miner,' the Android malware uses

"Today's indictment and arrests mark one of the largest cyberfraud enterprise prosecutions ever undertaken by the Department of Justice. As alleged in the indictment, Infraud operated like a business to facilitate cyberfraud on a global scale."
-Acting Assistant Attorney General John P. Cronan

the same scanning code as Mirari and can scan a wide-range of Ip-addresses to find vulnerable devices including smartphones, and even smart TVs. For those unfamiliar ADB, Android Debug Bridge is "a command-line tool that helps developers debug Android code on the emulator and grants access to some of the operating system's most sensitive features."

It appears the infection began on January 21st of this year, but according to researchers, there has been a recent uptick in the number of attacks, with the highest number of infection in China (40%) and South Korea (31%). So far, over 7,400 unique IP-addresses have been detected mining Monero, which translates to over 5,00 devices.

Similarly, researchers at Bitdefender have found a custom-built malware dubbed 'Operation PZChao' which has the ability to mine Bitcoin, steal passwords, and provide remote access to hackers. In this case, it seems the malware is the work of Chinese hacking group Iron Tiger, and is meant to target organizations in the United States and Asia.

"The payloads deployed by the threat actors are diversified and include capabilities to download and execute additional binary files, collect private information and remotely execute commands on the system"
-Bitdefender researchers

Another case of crypto mining? Read 'Monero Mining Software Found on Oil Transport Company's Systems' from Tripwire.

#SOURCECODE

Sharing is caring, but in the case of source code, not so much. It appears source code for a core component of the iPhone's operating system, iBoot, which controls the phone's security checks has been leaked on GitHub.

To be more specific, the iBoot essentially acts as the BIOS of an iPhone, which ensures that the kernel and systems files are adequately signed by Apple and are not modified in any way whenever you turn on your phone. With the source code leak, this could allow "hackers and researchers to discover currently unknown zero-day vulnerabilities to develop persistent malware and iPhone jailbreaks." At this time, it is not clear if the code is totally authentic, who released the code online, and how that person was able to get the code in the first place. A closer look reveals that it is from a version of iOS 9, of which some parts of the code is still used by iOS 11, but not all.

Some are citing this as 'the biggest leak in history,' although it seems the source code was previously shared on Reddit months ago. In the past, Apple has shared portions of code for macOS and iOS, but iBoot code is particularly security sensitive. According to Motherboard, they say "the company treats iBoot as integral to the iOS security system and classifies secure boot

components as a top-tier vulnerability in its bug bounty program, offering $200,000 for each reported vulnerability." While it's clear this code can pose a security risk, it's important to note that newer iPhones ship with 'Secure Enclave' which offers protection against many of the potential issues from the leaked code. At the time of writing, Apple had not commented on the issue, but we can assume with its removal from GitHub, plenty got their hands on it.

For a look at how GitHub tries to combat security issues, read this previous edition of UNMASKED.

""This is the SRC for 9.x. Even though you can't compile it due to missing files, you can mess with the source code and find vulnerabilities as a security researcher. It also contains the bootrom source code for certain devices."
-tweet from a security expert

FACT BYTE

THE U.S. INFORMATION TECHNOLOGY (IT) SECTOR POSTED MODEST JOB GAINS TO START 2018, BUT HIRING FOR CORE TECHNOLOGY POSITIONS WAS STRONG IN OTHER INDUSTRIES

-CompTIA

MEET THE INSTRUCTOR

MICHAEL REDMAN

Michael has delivered courses using materials and content he has developed to support civil service and DoD cybersecurity professionals pursuing certifications such as CISSP, CISM, Security+, LInux+ and others. To date, in excess of 300 individual students have been mentored with an astonishing 93% successfully achieving their certification goals.

His leadership style demonstrates his understanding that each individual is critical to the security posture of the systems, networks, and enclaves they are a part of. Among his current courses offered on Cybrary, one of the most popular is **Vulnerabilities, Application Data, and Host Security**. Stay tuned for many more courses from Michael coming soon.

START COURSE NOW

Ethical Hacking from Scratch

Learn how to hack networks, wireless, applications, and websites as well as bypass different security layers. This course demonstrates how to compromise computers, crack passwords, crash systems, and compromise applications in any organization.

Dive Into the Course

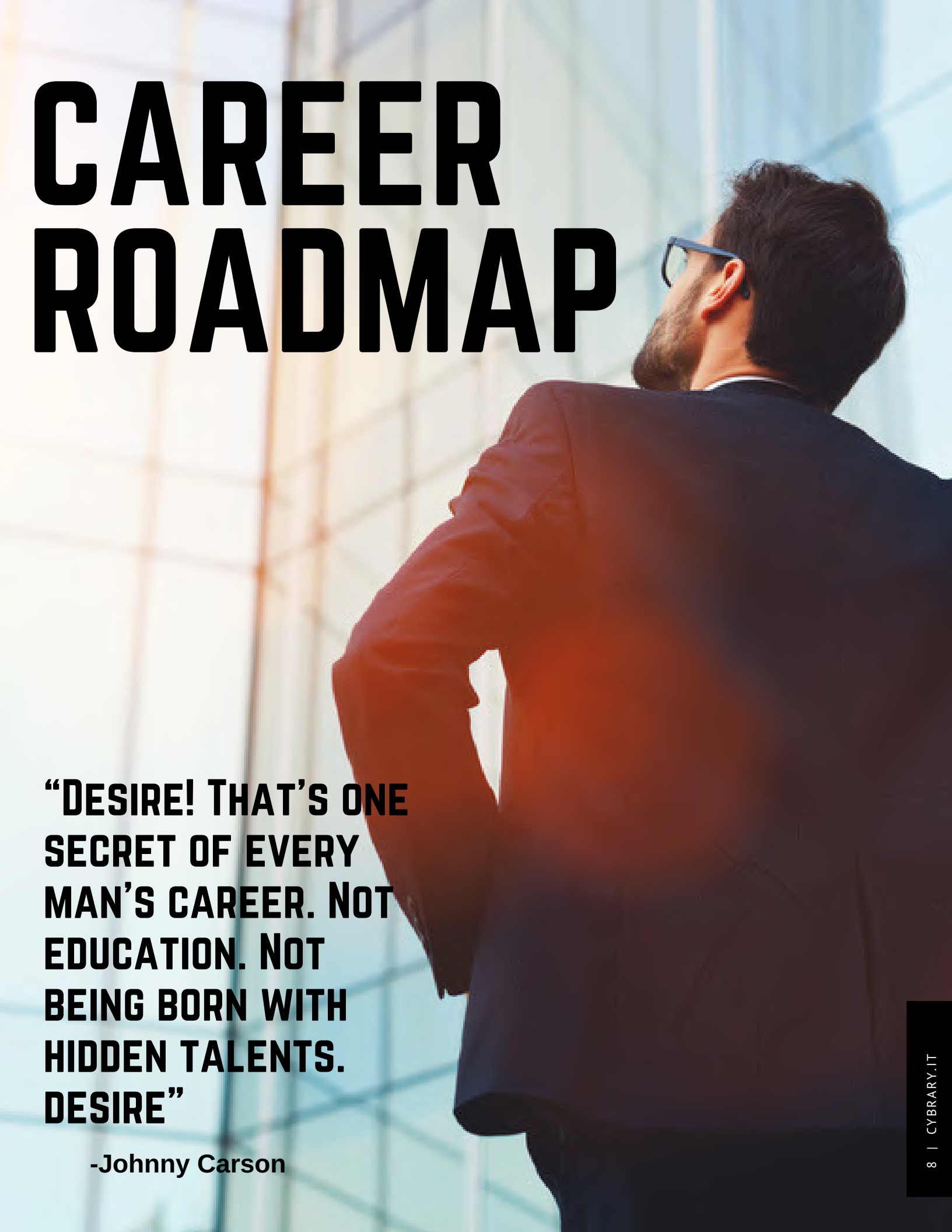
CompTIA CySA+ Exam Voucher

The CompTIA CySA+ certification verifies the skills required to use threat detection tools, perform data analysis and identify vulnerabilities.

Enjoy a less stressful testing experience when you purchase a CompTIA CySA+ exam voucher from Cybrary and locate your nearest testing center. (US Only)

Schedule Your Exam

CAREER ROADMAP



"Desire! That's one secret of every man's career. Not education. Not being born with hidden talents. Desire"

-Johnny Carson

TRENDING SKILLS

SOFTWARE ENGINEERING

“As someone new to web development, my advice to those starting out as well is that there are many others in the same position as you. The community, both online and in your local cities, are huge. Don’t be afraid to ask questions, join a meet-up, and review someone else’s code to make sense of it for yourself (**Don’t plagiarize!**). That’s how you learn and grow."

Continue Reading

Teach a Software Engineering Course

MANTECH CNO DEVELOPER

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

Program in languages such as Python	**Python**
Ensures software security standards are met	**Secure Coding**
Designs, develops, documents, tests, and debbugs applications software	**CSSLP**
Analyzes system capabilities to resolve problems	**Security Misconfigurations**
Knowledge of Linux/Unix/Windows administration, and system configuration	**Linux Fundamentals**
Program in languages such as C#	**C# Programming**
Independently develops hardware or software alongside other developers on the same project	**Software Development Fundamentals**

MAKING CONNECTIONS

What Can Football Teach Us About Cyber Security?

"If football players just talked about football while sitting around a table or practiced against fake, cardboard cutouts of the opposition, they wouldn't win. Your security analysts need real practice too. That practice needs to be on your real, production network leveraging your real security controls, processes and people against real attacks."

Read More

Explore the Blog