The Datagram newsletter

October 2016 Volume 1, No. 10

From the Chair...

Bring your funny hats and noise-makers! We have a one-year anniversary this month. We have grown from 8 to 160. That's about 39% per month. Come along. At this month's meeting, there will be cake and the ATEP Dean, Corine Doughty, has agreed to cut the first slice. Dean Doughty provided a place to meet and a parking lot to park in. '

We've learned some things from you. You like very technical meetings (Dr. Silverberg on Encryption) and Workshops (Sam Browne). We plan to use this information in the coming year to try to engineer a meeting place with something to meet for.

Some of you are regular attendees. Thanks. For those who haven't attended, come on by. We don't bite. If you want to talk to someone, talk to us. There's always someone interested in what you have to say. And if you feel that that someone is not present, speak to any of the CyberSecurity SIG executive committee members. We love to talk so much so that you may have to quiet us.

And for those who have come by once or only occasionally, what have we done wrong? We want you. If we're not quite doing it for you, we can change. Tell us. There is a forum at cssig.brats.com or Meetup.com/CyberSecuritySIG for your comments. What you say may change what we do.

Normally, we have November and December as blackout months, November because Thanksgiving would

Continued on page 2

Next meeting:

Ocober 26, 2016

6:30 PM Networking and dinner
7:00 - 9:00 PM Workshop

Bring your laptops

Dinner: FREE

ATEP, 15445 Lansdowne Road, Tustin, CA, Room #D106 (Room number subject to change)

Workshop Leader: Jo3 McCarthy

This Month's Topic: Introduction To Penetration Testing: A Workshop

For October's meeting, we're going to have another workshop. Joe McCarthy will be handing out flash drives with Kali Linux on it, and teaching us how to ethically destroy the universe. Joe is one of our own. A dynamic speaker who has appeared before. Joe knows the mechanics of CyberSecurity. The How's, To's and Where's.

This session will be hands-on, so bring your laptops. Attendees will be provided with bootable USB drives which have a Kali Linux image. We will be exploring the basics of penetration testing. By the end of the session, attendees will be able to find systems on a network, identify potential targets and learn about various exploits that could be used to compromise the target systems. ■

About the Speaker

Jo3 McCarthy is a senior software developer at Lantern Credit in Newport Beach. He has been developing software for decades. He has worked for various companies of various sizes from startups to Fortune 500s. He has a very strong interest in hacking and cybersecurity. He holds a Bachelor's degree in Information and Computer Sciences from The University of California, Irvine. ■

CSX 2016 North America

Join thought leaders, experts, and professionals at all levels of cybersecurity at the CSX 2015 North America conference October 17-19 in Las Vegas.

For complete information and to register, go to http://www.isaca.org/cyber-conference.

Contact Information

Web site: cssig.brats.com

Meetup.com/CyberSecuritySIG

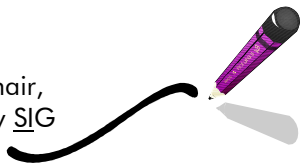
Newsletter Editor:
stargazer@stargazerpub.com

From the Chair, Cont'd.

be the day following the meeting and December because we would be meeting somewhere during the Christmas holidays. This year we will have a two-hour seminar conducted by TEKSystems, our sponsor, which is a professional placement organization, on December 7th. A meeting announcement will be sent about mid-month November to tell you the wheres and whens. Please attend and come prepared to talk. This may be your chance for an opportunity.

Art

(reluctant) Chair,
CyberSecurity SIG



September Meeting Report:

Lightweight, Obfuscation-Resilient Detection and Family Identification of Android Malware

by Carol J. Amato

Android malware was the subject of our October general meeting. Joshua Garcia, Assistant Project Scientist at UCI's Institute for Software Research, gave a very informative and interesting presentation on the issues plaguing this platform.

Android has 67% of the mobile/tablet market, with 1.8 billion android devices sold to date. As of September of 2016, there were 24,000 unique Android device models and 20 versions of the OS.

What makes Android software so vulnerable? Despite its success, Garcia stated, mobile systems open themselves to third-party app developers, resulting in massive software ecosystems. In December of 2009, there were nearly zero applications. By February of 2016, there were over two million. Add to that the fact that the typical app developer is 12 years old. These amateur developers don't have the expertise to ensure that their apps will be safe from easy hacking.

As a result, many of the apps are low quality, no longer functional, unmaintained or abandoned, and now malicious because they can be hacked.

In addition, Android has a permissions model that asks for your permission before installing an app. If you don't give it, the app won't load or won't work correctly.

Most apps have an inadequate permissions model. Sometimes, a hacker can make two apps work together to get around the permissions model with the intent to hijack and spoof. One malware family includes GingerMaster, the first Android malware to use a root exploit on Android 2.3 (Gingerbread), and Droid Jack, which allows anyone to take ownership of a phone to remotely control and update it. Removing this malware can often damage the device.

Obfuscation allows code to be installed and people don't know it's there. For this reason, Garcia stated that people should beware of Chinese phones, which are often repackaged.

Native code is installed near the hardware and can cause problems. Android malware propagates quickly.

Mr. Garcia gave a thorough overview of RevealDroid, the machine learning-based software his group at UCI is developing for malware detection and family identification of android malware. It allows the user to load the apps from the phone onto a computer then into RevealDroid.

The Department of Homeland Security website lists apps that have already been analyzed and cleared. Check this website to see if the apps you use are listed.

Mr. Garcia was kind enough to send us the slides from this presentation. You can download them from the CyberSecurity SIG website at www.cssig.brats.com. ■

INTERFACE-OC 2016 IT Conference

The IIBA-OC and INTERFACE cordially provide you, your staff, peers, and colleagues with a complimentary admission to the INTERFACE-Orange County 2016 IT Conference at the Anaheim Marriott on October 20, 2016, from 8:30 AM to 4:45 PM.

The keynote speaker is Chris Roberts, Counter Threat Intelligence and Cybersecurity Expert. Other highlights include solutions-based presentations by Centrify, Darktrace, Fortinet, Kaspersky Lab, Stortagecraft, Tintri, WatchGuard, Symantec, Blue Coat, and more.

Lunch will be served as well as an afternoon reception. There is a charge for parking, however: $24/self and $29/Valet.

To register, go to http://www.interfacetour.com/evites/oca/iiba-oc.htm. ■

3rd Annual LA Cybersecurity Summit

The 3rd Annual Cybersecurity Summit will be held at Loyola Marymount University on October 22, 2016, from 8:30 AM to 3:00 PM in honor of the National Month of Cybersecurity Awareness.

Registration, networking, and vendor setup is from 8:30 AM to 9:30 AM. The opening ceremony starts at 9:30 AM with Dr. Dennis W. Draper, Dean of the LMU School of Business, as the keynote speaker.

Other distinguished speakers include Dr. Merhdad S. Sharbaf, Mitchell Sherman of EastWest Bank, Kevin Von Keyserling of Cerified Security Solutions, and Congresswoman Loretta Sanchez.

For detailed information, map, and registration, go to https://www.eventbrite.com/e/third-annual-los-angeles-cyber-security-summit-2016-silicon-beach-tickets-25885191304 ■

Place Your Ads in The Datagram

Do you have information about an academic program, seminar, workshop, symposium, presentation, or job listing related to cybersecurity? Consider placing an ad in The Datagram.

Ads are currently FREE and will be published for three months, after which they are renewable. They will appear simultaneously on the CyberSecuritySIG's website at cssig.brats.com for maximum exposure.

Submit a camera-ready, business-card-sized (3.5" x 2") .jpg file to Carol Amato, at stargazer@ stargazerpub

Have suggestions for what you would like to see in the newsletter?

Send them to Carol J. Amato at stargazer@stargazerpub.com.

Request for Articles

This newsletter is open for article or information submission by all members of the CyberSecurity SIG. If you have something to say or leads on information that would be of benefit to the SIG, the members would love to read it.

Articles must be a maximum of 500 words and concern some aspect of cybersecurity. Submit them double-spaced via a .doc, .docx, or .rtf file to Carol J. Amato, Newsletter Editor, at stargazer@stargazerpub.com.

Speakers Requested

If you know of an expert in cybersecurity who is willing to speak to our CyberSecurity SIG, please contact our program chair, Angela Young, at angela.y@email.com.

2016 CyberSecurity SIG Executive Committee

Chair	Arthur Schwarz
Co-Chair	Gora Datta
Treasurer	Brandon Young
Programming	Angela Young
Newsletter	Carol J. Amato
Web Design	Jo3 McCarthy
Audio-Visual	Open

TEKsystems

Thank you!

Our sincerest thanks to Ashley Groothuis of TEKsystems for sponsoring our food and beverages for the rest of the year. This means dinner will be free to everyone through December. Thanks again so much to Ashley Groothuis and TEKsystems!