# The Datagram newsletter

April, 2016 Volume 1, No. 4


## From the Chair...

The March meeting was a decidedly mixed affair. Our main speaker, Michael Lipsey from Cisco, called at the last minute to say that he could not make the presentation in time. Not wanting to miss an opportunity, I stood up and began an impromptu presentation of my latest project. Enrapt in my own presence, I failed to notice the rush of people to the door, no doubt to go to their favorite topic, CyberSecurity. With good grace and foresight, our June presenter, Carter Jones, began to talk on CyberSecurity, recapturing our audience, who gave good attention and asked intriguing questions. The slides are on our website, cssig.brats.com, and I have to say, ya' shoulda' been there.

Michael Lipsey will be our speaker on June 22, taking Carter's spot, and I think I've convinced him to provide a presentation on how to be a hacker. We hear more and more of Cyber-Attacks: active threats to the data and the sometimes successful extraction of data by the attackers. We know it can be done.

Ransomware is becoming the up and coming thing for entrepreneurs to gain a financial presence with little effort on their parts. The current hacker efforts seem directed towards our healthcare industry, where large entities' (hospitals or insurers) data are held captive until some substantial sum is given or extorted by some hacker. Of the cases reported, it is interesting that a given institution is hacked once but not twice. Either the

*Continued on page 2*

***Next meeting:***

**April 27, 2016**

**6:00 PM Exec Com Meeting**
**6:30 - 7:00 PM Networking**
**7:00 - 8:00 PM Meeting**
**Dinner: $10 (Pay and RSVP at cssig.eventbrite.com)**

**ATEP, 15445 Lansdowne Road, Tustin, CA, Room #D106**

**Presenter: Corey White, Cylance**

## This Month's topic

Corey White's presentation will be on How to Perform a Compromise Assessment.

The primary objective of a compromise assessment is to identify ongoing compromises and uncover the extent of malicious access and usage of the environment. Learn how to hunt for hosts that exhibit anomalous or suspicious behaviors and investigate related threat actor activities on hosts.

Understand what to look for in the following specific areas:

- Identify ways to determine data exfiltration and sabotage
- Identify command and control activities Identify compromised accounts
- Identify malware and persistence mechanisms
- Identify the latest techniques to compromise credentials
- Review hacking techniques used by hackers

## About the Speaker

Corey White is Vice President of Professional Services at Cylance, Inc. Prior to joining Cylance, Corey served as Director of Consulting for Foundstone and McAfee/Intel Professional Services where he was responsible for all aspects of the business for the Southwest Region.

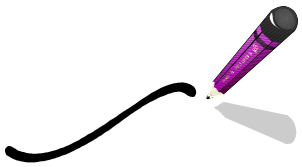
Corey is a proven security industry veteran backed by more than twenty years of success managing security practices and consulting teams, delivering on strategic projects as well as tactical assessments, penetration tests, and incident response engagements. His work encompasses virtually every industry sector, including defense, technology, government, critical infrastructure, automotive, finance, healthcare and manufacturing. Corey has a deep technical background, which has allowed him to deliver and oversee technical assessments, incident response engagements, strategic planning and risk assessments.

Corey has a degree in Computer Information Systems from the University of Louisiana at Monroe, and is a Certified Information System Security Professional (CISSP).

## From the Chair, Cont'd.

Organization has taken precautionary measures or there is some honor among thieves in not attacking the same place more than once.

The pervasiveness of these attacks and the ease which they can be inserted is a concern. Some articles on ransomware are located at P010V0RZGL02850D05uW8d3.htm and NL009ZdR00082DW1vV5053G.htm. Take a look.



*Art*

(reluctant) Chair,
CyberSecurity SIG

# March Meeting Report:

*by Carol J. Amato, Carter Jones, and Art hur Schwartz*

Thanks to Carter Jones, senior security consultant of Cigital's Irvine office, for speaking at our March meeting, when our original speaker, Michael Lipsey, was unable to. Mr. Lipsey has been rescheduled for our June 27th meeting.

Carter turned his teenage hacking skills into a consulting career in which he gets paid to hack into video games to ensure the delivered product is valid.

Carter pointed out that hacking video games touches on the same aspects of security as does hacking in any other type of industry, such as those that handle payment card information or those that have authentication services. Information can still be grabbed and sold on the black market.

Deliberately hacking a system can show if people or departments can bypass their way into parts of the network that are not otherwise open to them. He discussed recent news stories brought up by the audience of payment card processing systems erroneously tied to vendors' systems. He advised using network segmentation to help avoid these types of problems.

Carter stated that, often, end-users are sent executable files that allow attackers to reach their systems. Regarding video game security, attackers can potentially find flaws in game servers, which could allow the attacker to take over the game server. Alternatively, attackers could possibly use the game server as a relay to send data to end-users and attack them at scale.

He discussed an example threat model, which touches on various security paradigms:

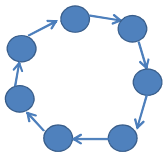
- Infrastructure security
- Web application security
- Product architecture security
- Thick client security
- Social engineering

Social engineering could involve a hacker getting a username, password, and the last four numbers of the user's credit card number and hack the system. Another way of obtaining information is via "USB drops," where an attacker puts malicious software onto a USB disk and then scatters many of these disks around parking structures or or common rest areas (such as smoking areas). People will often pick these USB sticks up and put them into their computers. When these are inserted into computers, they can often allow an attacker to gain a foothold onto the system. One method of defense against that type of attack is to remove the USB drivers so information cannot be downloaded. In any case, if a user suspects an account has been compromised, he/she should call Tech Support immediately and get his/her password changed, and follow any other steps Tech Support recommends.

The waterfall model has traditionally been used to develop software. Security expertise can be injected into each layer of this model, which involved the following: idea, specs, prototype, implementation, text, and deployment.

In this model, the development completes after delivery. The first idea is the only idea. The end result is that, in some situations, the process can take a long amount of time, even reaching multiple years, or a solution may be discovered at a point where changes are not possible.

The use of rapid development models, such as the Agile methodology, however, can result in very fast iteration cycles (as low as a few minutes.



The first idea is not the only idea. Each iteration restarts the development, and iterations can occur during each phase of the cycle. Failures detected during one cycle are folded into changes in the next cycle.

With this cyclical model, you can use IDE plugins to detect more obvious implementation errors, such as buffer overflows or SQL injections. At other stages in the cycle, you can use tools like Jenkins or other tools tp test target builds. This can help solve issues earlier on in the development process, rather than later when it can be more costly. This can apply to many types of applications from web apps to thick client to infrastructure itself. Companies like Blizzard are leading in this process.

According to members of the audience, what stands in the way of many companies adopting this new process is management's unwillingness to pay these costs up front. They have been known to wait until until there is a problem prior to taking action. This can be alleviated through clear and efficient messaging to appropriate stakeholders within an organization.

## 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 |
| Outreach | Christopher Ries<br>Mark Wich |
| Web Design | Jo3 McCarthy |
| Audio-Visual | Mark Wich |

### Contact Information

Web site: cssig.brats.com

Meetup.com/CyberSecuritySIG

Newsletter Editor: stargazer@stargazerpub.com

## University of Delaware offers Online Master's in Cybersecurity

The University of Delaware is offering an online Master of Science in Cybersecurity degree. This 30-credit program focuses on engineering of secure software and systems and students will learn from active practitioners with strong corporate and military experience. The University of Delaware is leading the field with its Cybersecurity initiative, a center for research, training, and partnerships. For more information, go to http://landing.online.udel.edu/MSCYBER-PS?utm_source=SB-IEEE&utm_medium=banner&utm_campaign=accordant.