The Datagram newsletter

September 2016 Volume 1, No. 9

From the Chair...

Ransomware is an ever increasing and pernicious presence in the computer world. Ransomware can be categorized as 'locked screen,' 'encryption,' and 'app denial,' where the locked screen prevents computer use by presenting a persistent image on the monitor, encryption encrypts files and makes them inaccessible, and app denial prevents users from accessing specific apps. Ransomware is introduced onto a computer the same way as other malware and is an ubiquitous presence in the same way.

Once a computer is infected, it becomes unusable until a fee (the 'ransom') is paid. Payment in Bitcoins seems to be the medium of choice. The nature of the threat places users with high data content at a potential threat and, if the data is used as an integral part of a business, at considerable financial loss. The criminals extort money with little risk. They become rich without work.

Current ransomware attacks seemed focused on encrypting files rather than denying access. Although, in time, the encryption algorithms are discovered, the discovery has little effect on the immediate needs of a business in its normal operations. And so businesses can't wait for a discovery of a means to decrypt their files and are forced to pay a ransom.

As a subset of malware, ransomware suffers the same difficulties in mediation as viruses, trojans and the like. This month, the CyberSecurity Web Site, cssig.brats.com->INFOSec->

Continued on page 2

Next meeting:

September 28, 2016

6:30 PM Networking and dinner
7:00 - 8:00 PM Presentation
8:00 - 8:30 PM Q & A
8:30 - 9:00 PM More networking

Dinner: FREE

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

Presenter: Joshua Garcia

This Month's Topic:

Joshua Garcia, assistant project scientist, will present "Lightweight, Obfuscation-Resilient Detection and Family Identification of Android Malware." The number of malicious Android apps is increasing rapidly. Detecting and removing malware apps is insufficient, since they can damage or alter other files or settings, install additional applications, etc. To determine such behaviors, a security analyst can significantly benefit from identifying the family to which an Android malware belongs. Techniques for detecting Android malware and determining their families lack the ability to handle certain obfuscations that aim to thwart detection. Moreover, some prior techniques face scalability issues, preventing them from detecting malware in a timely manner.

To address these challenges, Garcia will discuss a novel machine learning-based Android malware detection and family identification approach, RevealDroid, that operates accurately and efficiently without the need to perform

Continued in Column 3

About the Speaker

Joshua Garcia is an Assistant Project Scientist at the Institute for Software Research at UC-Irvine and the Software Engineering and Analysis Lab (SEAL) at UCI's Department of Informatics. His current research interests include mobile security, testing, and analysis—and addressing problems of software architectural drift and erosion. Before joining UCI, he was a Postdoctoral Research Fellow at George Mason University's Department of Computer Science. He received three degrees from the University of Southern California: a B.S. in computer engineering and computer science, an M.S. in computer science, and a Ph.D. in computer science. His industrial experience includes software-engineering or research positions at the NASA-JPL, the Southern California Earthquake Center, and Xerox Special Information Systems. ■

complex program analyses or to extract large sets of features. On a dataset of 51,496 malicious and benign apps, RevealDroid achieves an accuracy of 91%. For 18,065 malicious apps from 68 families, RevealDroid can identify the malware family with an accuracy of 87%. ■

Contact Information

Web site: cssig.brats.com

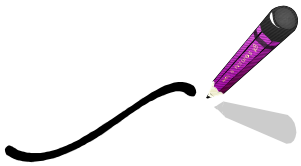
Meetup.com/CyberSecuritySIG

Newsletter Editor:
stargazer@stargazerpub.com

From the Chair, Cont'd.

Articles, has been augmented with a number of articles, theses, and commercial offerings bearing on ransomware. Techniques are presented to discover and/or isolate ransomware infected machines on a network and to discover means to disinfect an infected machine. The articles show that this is an active field of research and that some niggling progress has been made, but that there is no solution at this time to absolute detection and elimination.

If you have some thoughts and experience with ransomware, we would like to hear about it.



Art

(reluctant) Chair,
CyberSecurity SIG

August Meeting Report: We Lost The Battle Against Intrusion — Are We Left to Raise Our Hands in Defeat?

by Carol J. Amato

Our August meeting focused on cybersecurity espionage hacks. Speaker Aaron Sramek stated that security vulnerabilities were first detected in 1988 and that a Gartner report claims that, today, 44% of malware intrusions happen on top of security solutions in place. The original exploitation programs focused on memory corruption, which made exploitation harder but not impossible.

In 2016, selling zero-day malware on the black market is big business, and companies sell to countries good and bad for millions of dollars without a care for any of the repercussions.

"So what are we to do?" asked Sramek. "Should we give up?"

Sramek's answer is no, despite the fact that constant patching can't catch up. Many of these attacks come from countries such as Russia and Ukraine.

He cited the example of the Sandworm virus, which attacked a PowerPoint vulnerability. The original patch was flawed. Not only could attackers bypass it, but McAfee virus protection didn't detect it.

As of this year, security software will be judged on how well it can prevent zero-day vulnerabilities. Companies, however, have to be aware that they will always be compromised, and they have to work under the assumption that malware is inside their systems. The next step, then, is to go from detection to blocking.

Sramek's company, EnSilo, has developed security software that blocks ransomware at the communication steps and at file points and isolates it. Companies should not give up trying to head off these attacks. ■

Your Phone Can Be Easily Hacked

by Carol J. Amato

Many people argue over which phone is best: Iphone or Android. According to a report repeated on the September 4th episode of *60 Minutes*, that argument is moot when it comes to hacking, as both types are just as vulnerable.

Since some of the world's best hackers are in Germany, Sharyn Alfonsi, a *60 Minutes* correspondent, went to Berlin to interview Dr. Karsten Nohl, the head of Security Research Labs. During the day, the lab advises Fortune 500 companies on computer security. At night, the team looks for vulnerabilities in the devices we use every day—smartphones USB sticks, and SIM cards—so they can warn the public about the risks. Right now, they are concentrating on mobile phone networks.

With just a phone number, Nohl claimed he could get into Alfonsi's phone and retrieve all her transactions (including credit card numbers), track her location, see where she went, which people she met and when, see who she calls and what they say, and read her texts.

To test this claim, *60 Minutes* sent an off-the-shelf iPhone to Representative Ted Lieu of California along with the telephone number registered to it. Lieu agreed to use the phone knowing it would be hacked. Alfonsi called from Berlin and Nohl hacked in.

How did he do it? By exploiting a security flaw in the Signaling System Seven (SS7), the global network that connects phone carriers, though he admitted that some were easier to hack than others. He recorded the congressman's calls and tracked his movements in Washington and back in California. Lieu admitted that this was "immensely troubling."

John Hering, who cofounded the mobile security company, Lookout, when he was 23, has developed a free app that scans mobile phones for malware and alerts users when the phones are attacked. According to Hering, there are only two types of companies and people: those who have been hacked and realize it and those who have been hacked and don't.

He claims that most phone hacks are not via SS7 but via spoofing, explaining that people install malicious applications and willingly give up their passwords every day.

60 Minutes contacted the cellular phone trade association, which claimed that SS7 attacks could not happen on a U.S. network but are only a problem on foreign ones. The hacking of Lieu's *60 Minutes* phone, however, proved exactly the opposite.

The problem is that the world's intelligence agencies don't want this flaw

Continued on page 3

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.

Phone Hacks, *Continued from page 2*

fixed. Lieu stated that the people who know about it and aren't doing anything to recify it should be fired. Adds Hering, "We live in a world where we cannot trust the technology that we use."

To read the full transcript of this story, please go to http://www.cbsnews.com/news/60-minutes-hacking-your-phone/ ■

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!