The Datagram newsletter

June, 2016 Volume 1, No. 6

From the Chair...

Your system has been compromised. Data is leaking from it like water from a hose. Now what? Corey White from Cylance, our April speaker, suggested that you begin to investigate how a hacker entered the system not by looking at failed logons but by looking at successful ones. The failed logons can be used to determine a pattern, but successful logons cause the damage.

The question is reduced to which logon allowed the system to be penetrated and what means where used to extract data. Now this isn't as clear in practice as it seems in theory. A high school hacker, hormones all atwitter, seeks instant gratification. Breach a site, extract data or do mischief, and leave.

Professionals are more circumspect. Breach a site, leave little bits of malware, then leave. At some future time, they use the malware to upload information. If the professional hackers are particularly clever, a 'future time' does not involve a logon; that is, the malware uses a timer to start itself. The search for a successful logon then becomes an historical search over large quantities of logins.

We've discovered when something occurred; now what do we do? A breach supported by malware requires that it be discovered. Jase Kasperowicz from Crowd Strike discussed this at the Cal Poly SWIFT seminar on May 7th.

Continued on page 2

Next meeting:

June 22, 2016

6:00 PM Exec Com Meeting
6:30 - 7:00 PM Networking
7:00 - 8:00 PM Meeting
Dinner: $10 (cash only)

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

Presenter: Michael Lipsey, Cisco

This Month's Topic

Michael Lipsey from CISCO will be our June speaker. He will introduce us to the notion of Secure Branch Design, the ability to provide secure internet connectivity within an enterprise of remote servers. The discussion will address end-to-end security, the ability to have an internet dialog in which each end of the conversation is assured that dialog is secure, reliable, and correct. The design will address features required to allow security of end points over an insecure transmission medium. The CISCO book describing their approach is at http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg/

Free Cybersecurity Training

Are you interested in getting some free cybersecurity traing? If so, go to https://training.safecode.org.

About the Speaker

Michael Lipsey, CCIE#42683, is a Systems Engineer within Cisco's California Enterprise organization. He has over 20 years in the industry with most of his focus being on Enterprise Routing and Switching and Security architectures.

Prior to joining Cisco, he held engineering roles within a variety of different types of organizations, including manufacturing, educational, service provider, retail, search engines, and entertainment. In these roles, he has been able to develop an insight into the importance of secure wide-scale networking to support an organization's business objectives.

Contact Information

Web site: cssig.brats.com

Meetup.com/CyberSecuritySIG

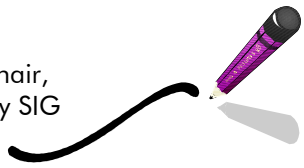
Newsletter Editor:
stargazer@stargazerpub.com

From the Chair, Cont'd.

How do you discover malware? Let's look at a simple case where the malware was 'hidden' amongst the OS system files. A typical hacker approach is to rename the malware the same as some needed OS executable and to put the executable into another directory. In practice, this means that if we know the name and location of all legitimate OS files, then a listing of all files within the OS directory (or the whole disk) and a search for files with similar or the same names as known OS files will discover them. That is, if <fileA> is in <directoryA> and if <fileA> is also discover-ed in any other directory, it is probably malware. This activity gets more complicated when multiple versions of an OS needs be considered.

Art

(reluctant) Chair,
CyberSecurity SIG



May Meeting Report: Crytography: Using Mathematics to Keep a Secret

by Carol J. Amato & Alice Silverberg, PhD

Many people worry about the safety of their data in the Cloud. According to Dr. Alice Silverberg, Professor of Mathematics and Computer Science at the University of California, Irvine, they are right to worry. She presented a very interesting talk on Fully Homomorphic Encryption (FHE), a new method that can ensure data safety.

FHE makes use of the greater storage capacity and computational power of the Cloud while not letting the Cloud know anything about the data itself; in other words, information can be sent, but the Cloud cannot decrypt it. For example, FHE would allow hospitals to send data to the Cloud. The Cloud could then perform computations on the data and send the results to the patient or healthcare provider, but the Cloud wouldn't know what the data is even though it does the computations. The decryption is done at the patient or user end.

Rivest, Adleman, and Dertouzos devised the concept of FHE in 1978, shortly after the invention of the RSA encryption scheme, but it remained an unsolved problem for years. In 2009, Craig Gentry wrote his PhD dissertation on a solution he found to do an arbitrary number of additions and multiplications through the use of ideal lattices and ring theory.

Security comes from its structure as a lattice; that is, security is based on the presumed difficulty of some lattice problem, such as the problem of finding a good basis for a lattice in a high dimensional space. The data is converted to lattice points. Silverberg described one scenario this way: Let's say Bob wants to send data for computation. He has a private key and a public key. His private key is a good basis for the lattice. His public key is a bad basis for the same lattice. Bob encrypts the data with the public key and sends it to the Cloud. The Cloud does the computations and sends the result back to Bob, who decrypts it with his private key. A limitation is that both the sender and receiver must have the same FHE system in place.

Kansas Hospital Hit with Ransomware

Kansas Heart Hospital in Wichita was hit with ransomware in May. The hospital paid the ransom, though President Dr. Greg Duick would say only that it was "a small amount." Despite this, the attackers hit again. Duick stated that the hospital had a plan for such an event and implemented it so that patients' treatment was not affected.

WPAD Vulnerability

For those of you who use Microsoft's Windows browsers. WPAD is enabled by default on all Microsoft Windows operating systems and Internet Explorer browsers allowing a man-in-the-middle vulnerability.

Solution

US-CERT encourages users and network administrators to implement the following recommendations to provide a more secure and efficient network infrastructure:

1. Consider disabling automatic proxy discovery/configuration in browsers and operating systems during device setup if it will not be used for internal networks.

2. Consider using a fully qualified domain name (FQDN) from global DNS as the root for enterprise and other internal namespace.

3. Configure internal DNS servers to respond authoritatively to internal TLD queries.

4. Configure firewalls and proxies to log and block outbound requests for wpad.dat files.

5. Identify expected WPAD network traffic and monitor the public namespace or consider registering domains defensively to avoid future name collisions.

File a report with ICANN if your system is suffering demonstrably severe harm as a consequence of name collision by visiting https://forms.icann.org/en/help/name-collision/report-problems.

Upcoming Webcast

Join the SecureWorks CISO Intel team on Thursday, June 9th, at 11 AM PT as they walk you through their time spent in the Underground, tracking hackers in numerous forums and marketplaces all over the world. To register, go to https://webinar.darkreading.com/2110?keycode=CAA1AC&elqTrackId=266d00b906bf419caf9ef0b3cff01d72&elq=ed81c0b4f93d49e6be66b133da784a68&elqaid=4889&elqat=1&elqCampaignId=3570

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	Mark Wich
Web Design	Jo3 McCarthy
Audio-Visual	Mark Wich

Whitepaper Discusses Trends for 2016

Tableu.com has posted a whitepaper discussing the trends in Big Data for 2016. To get a copy, go to http://get.tableau.com/asset/top-8-trends-big-data-2016.html?cid=70132000001HBws&ls=Advertisement&lsd=Google%20Display%20-%20Similar%20Audience%20-%20Big%20Data%20Trends%202016&adgroup=Small%20Business%20-%20Big%20Data&kw=big%20data%20platform&adused=98816373495&distribution=content&creative=freeway&gclid=CP2W35D8kc0CFQ8yaQodv5cNqA