REN-ISAC Daily Watch Report
2017-06-23
SHARING GUIDELINES: This report can be shared within -closed-
communities of cyber security practitioners. It must NOT be shared
publicly.

Handler: Sheryl Swinson (REN-ISAC) and other credits[A]

CRITICAL NOTICES

Nothing to report.

UPCOMING

Nothing to report.

FOLLOW-UPS

Nothing to report.

VULNERABILITIES AND EXPLOITS (only items of particular note)

Siemens Patches Vulnerabilities in SIMATIC CP, XHQ

https://threatpost.com/siemens-patches-vulnerabilities-in-simatic-cp-xhq/126513/

Siemens patched two vulnerabilities in products commonly found in industrial control system setups this week. If exploited the flaws could allow an attacker to perform administrative actions or gain read access to sensitive data on affected systems.

Siemens patched one issue (.PDF) on Tuesday and the other on Thursday (.PDF) this week. ICS-CERT, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team, warned of the flaws on Friday.

Vulnerability Spotlight: Multiple Vulnerabilities in InsideSecure MatrixSSL

http://blog.talosintelligence.com/2017/06/matrixssl-multiple-vulns.html

MatrixSSL is a TLS/SSL stack offered in the form of a Software Development Kit (SDK) that is geared towards application in Internet of Things (IOT) devices and other embedded systems. It features low resource overhead and supports many different embedded platforms. It also features FIPS 140-2 compliant cryptography making it suitable for use in high security environments. Talos recently discovered multiple vulnerabilities in MatrixSSL version 3.8.7b including two remote code execution (RCE) vulnerabilities as well as an information disclosure vulnerability.

The New and Improved MacOS Backdoor From OceanLotus
https://researchcenter.paloaltonetworks.com/2017/06/unit42-new-improved-macos-backdoor-oceanlotus/

Recently, we discovered a new version of the OceanLotus backdoor in our WildFire cloud analysis platform which may be one of the more advanced backdoors we have seen on macOS to date. This iteration is targeted towards victims in Vietnam and still maintains extremely low AV detection almost a year after it was first discovered. Despite having been in the wild for an extended period of time, the operation appears to still be active. During our analysis, we were able communicate directly with the command and control server as recently as early June 2017.

While there seem to be similarities to an OceanLotus sample discovered in May 2015, a variety of improvements have been made since then. Some of the improvements include the use of a decoy document, elimination of the use of command line utilities, a robust string encoding mechanism, custom binary protocol traffic with encryption, and a modularized backdoor.

Debian:

[DSA 3894-1] Graphite2 Security Update
https://lists.debian.org/debian-security-announce/2017/msg00154.html

[DSA 3895-1] Flatpak Security Update
https://lists.debian.org/debian-security-announce/2017/msg00155.html

[DSA 3896-1] Apache2 Security Update
https://lists.debian.org/debian-security-announce/2017/msg00156.html

---

Debian LTS:

[DLA 998-1] C-Ares Security Update
https://lists.debian.org/debian-lts-announce/2017/06/msg00027.html

[DLA 999-1] OpenVPN Security Update
https://lists.debian.org/debian-lts-announce/2017/06/msg00028.html

---

Red Hat:

[RHSA-2017:1574-01] Moderate: Sudo Security update
https://www.redhat.com/archives/rhsa-announce/2017-June/msg00054.html

---

SUSE:

[SUSE-SU-2017:1660-1] Important: Security Update For Tomcat

http://lists.suse.com/pipermail/sle-security-updates/2017-June/002971.html

[SUSE-SU-2017:1661-1] Moderate: Security Update for OpenSSH-Openssl1
http://lists.suse.com/pipermail/sle-security-updates/2017-June/002972.html

[SUSE-SU-2017:1662-1] Moderate: Security Update for Php5
http://lists.suse.com/pipermail/sle-security-updates/2017-June/002973.html

[SUSE-SU-2017:1663-1] Moderate: Security Update for Wireshark
http://lists.suse.com/pipermail/sle-security-updates/2017-June/002974.html

[SUSE-SU-2017:1664-1] Moderate: Security Update for Wireshark
http://lists.suse.com/pipermail/sle-security-updates/2017-June/002975.html

---

Ubuntu:

[USN-3339-1] OpenVPN Vulnerabilities
https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-June/003918.html

---

VIRUSES, WORMS, and MALWARE (only items of particular note)

Fake DDoS Extortions Continue. Please Forward Any Threats You Have Received.
https://isc.sans.edu/forums/diary/Fake+DDoS+Extortions+Continue+Please+Forward+Us+Any+Threats+You+Have+Received/22550/

The SANS Technology Institute continues to receive reports about DDoS extortion e-mail. These e-mails are essentially spammed to the owners of domains based on whois records. They claim to originate from well-known hacker groups like "Anonymous" who have been known to launch DDoS attacks in the past. These e-mails essentially use the notoriety of the group's name to make the threat sound more plausible. But there is no evidence that these threats originate from these groups, and so far there has not been a single case of a DDoS being launched after a victim received these e-mails.

New Android Marcher Variant Posing as Adobe Flash Player Update
https://www.zscaler.com/blogs/research/new-android-marcher-variant-posing-adobe-flash-player-update

Marcher is sophisticated banking malware that steals users' financial information, such as online banking credentials and credit card details. We have observed Marcher evolving over time, using new tricks and payload delivery mechanisms. As we reported about previous encounters with this malware, the authors are using new techniques to spread infections, such as pornographic lures and the hype around new games.

In a recent wave, we are seeing the malware payloads disguised as Adobe Flash player. Upon opening the dropper URL, the user will be

prompted by a message saying the device's Flash Player is out of date, and the malware "Adobe_Flash_2016.apk" will be dropped on the user's device. The malware will also guide the user to disable security and allow third-party apps to install, as shown in the screen below.

PHISHING, SOCIAL ENGINEERING and IDENTITY THEFT

Barclays Bank customers Targeted by Phishers
https://blog.malwarebytes.com/cybercrime/2017/06/barclays-bank-customers-targeted-phishers/

Today we have a phish targeting customers of Barclays Bank.

HACKS, ATTACKS, AND DATA THEFT/LOSS

Two Men Arrested for Hacking Microsoft
https://www.bleepingcomputer.com/news/security/two-men-arrested-for-hacking-microsoft/

British police announced today they arrested two suspects part of an international group that hacked into Microsoft's network.

The two suspects are a 22-year-old man from Lincolnshire and a 25-year-old man from Bracknell. The South East Regional Organized Crime Unit (SEROCU) arrested the two this morning, searched their homes for evidence, and seized a number of devices.

Ouch! UK Govt's Cyber Essentials Scheme Suffers Data Breach Due to Configuration Error
https://www.grahamcluley.com/ouch-uk-govts-cyber-essentials-scheme-suffers-data-breach-due-configuration-error/

The UK Government's Cyber Essentials digital security scheme has suffered a data breach caused by a configuration error in a software platform.

On 21 June, companies received word of the incident from Dr. Emma Philpott, chief executive at the Information Assurance for Small and Medium Enterprises (IASME) Consortium. One of the scheme's Accreditation Bodies, IASME has incorporated Cyber Essentials into its information assurance standard. Suppliers wanting to secure contracts for work involving government data must therefore work with a Certification Body licensed by IASME or another Accreditation Body to achieve Cyber Essentials accreditation.

PRIVACY

Gmail Will No Longer Scan E-mails for Ad Personalization

https://arstechnica.com/gadgets/2017/06/gmail-will-no-longer-scan-e-mails-for-ad-personalization/

Google has announced it will no longer scan e-mail messages for ad personalization. Previously, in the consumer version of Gmail, Google's computers would scan the contents of every e-mail message to determine a relevant ad to show. The scanning "feature" has been turned off for Google Apps for Education and GSuite accounts for some time, but now Google says that "consumer Gmail content will not be used or scanned for any ads personalization after this change."

The Google announcement is available at:
https://blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/

Giving People More Control Over Their Facebook Profile Picture

https://newsroom.fb.com/news/2017/06/giving-people-more-control-over-their-facebook-profile-picture/

Part of our goal in building global community is understanding the needs of people who use Facebook in specific countries and how we can better serve them. In India, we've heard that people want more control over their profile pictures, and we've been working over the past year to understand how we can help.

Today, we are piloting new tools that give people in India more control over who can download and share their profile pictures. In addition, we're exploring ways people can more easily add designs to profile pictures, which our research has shown helpful in deterring misuse. Based on what we learn from our experience in India, we hope to expand to other countries soon.

REPORTS, PAPERS, AND PRESENTATIONS

FBI: Reported Internet-Enabled Crime Losses Hit $1.3 Billion

http://www.govinfosecurity.com/fbi-reported-internet-enabled-crime-losses-hit-13-billion-a-10033

Reported losses due to internet crime last year totaled $1.3 billion, according to the FBI's Internet Complaint Center, or IC3. The report calls out four increasingly seen types of scams: business email compromise, aka CEO fraud or email account compromise; ransomware; tech-support fraud; and extortion.

The findings, however, include a big caveat, in that the Department of Justice estimates that only 15 percent of internet-related crime gets reported to authorities.

Download a PDF of the full report directly at:
https://pdf.ic3.gov/2016_IC3Report.pdf

AUDIO/PODCAST
==========

ISC StormCast for Friday, June 23rd 2017 (~ 12 min.)
https://isc.sans.edu/podcastdetail.html

- Obfuscating Without XOR
- Airbnb OAUTH Token Theft
- Critical Drupal Vulnerability
- Auditing Docker Containers

How PayPal Protects Billions of Transactions (~ 15 min.)
http://www.govinfosecurity.com/interviews/how-paypal-protects-billions-transactions-i-3627

How does PayPal, one of the world's largest internet payment companies with over 203 million active users, maintain a fraud loss rate of just .032 percent? Guru Bhatt, PayPal's general manager of technology and head of engineering, says it comes down to a combination of sophisticated automation, machine learning, and human insight.

In an in-depth interview with Information Security Media Group, Bhatt shares what it takes to create an effective self-learning model that leverages machine learning to track and mitigate fraud, and how it is supported by a team of over 2000 risk analysts .

Paul's Security weekly #518 Trey Forgety, NENA (~38 min.)
https://securityweekly.com/2017/06/23/psw518trey/

Trey Forgety is the Director of Government Affairs and Information Security Issues at the National Emergency Number Association. He worked with the White House to develop policy for a nationwide LTE network for public safety, known as FirstNet. Trey joins us to discuss emergency response systems and the future of crisis communications.

Threatpost News Wrap, June 23, 2017 (~24 min.)
https://threatpost.com/threatpost-news-wrap-june-23-2017/126503/

Mike Mimoso and Chris Brook discuss the news of the week, including Citizen Lab's latest report, WannaCry hitting Honda, GhostHook, and Fireball.

TOOLS AND TIPS
==========
Nothing to report.

ARTICLES AND OTHER
==========

The Week in Ransomware - June 23rd 2017
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-23rd-2017-a-fricken-1-million-dollar-ransom-payment/

What a crazy week. The biggest news is that we had a hosting company who actually paid a 1 million dollar (think Dr. Evil) ransomware payment. We then had the return of Locky, which at one point was the preminent ransomware being distributed. We will have to wait and see if it can become king of the hill again.

Other than that, it has mostly been small ransomware variants being released that will probably never make it into any real distribution.

Cyber News Rundown: Edition 6/23/17
https://www.webroot.com/blog/2017/06/23/cyber-news-rundown-edition-62317/

- WannaCry Shuts Down Honda Production Plant
- Web Host Pays Out $1 Million Ransom
- NSA Malware Installing Cryptocurrency Miners
- Mac® Computers Becoming Focal Point for Attackers
- WannaCry Found on Australian Traffic Cameras

NEWS
=======

Germany Just Gave Cops More Hacking Powers to Get Around Encryption
https://motherboard.vice.com/en_us/article/gyp7em/germany-just-gave-cops-more-hacking-powers-to-get-around-encryption

Cops are getting comfortable with hacking. Already, agencies across the world are using malware or other techniques to identify child pornographers, bomb hoaxers, and stalkers.

But, in the continuing battle over the proliferation of easy-to-use encryption, German lawmakers want to go further. On Thursday, the Bundestaag—the German parliament—passed legislation authorizing the country's law enforcement to use malware in a wider range of investigations, including drug trafficking.

"Police must be able to do what terrorists and criminals can already do today," Johannes Fechner from the SPD, a Center-left party which forms part of the current government, said during a debate before the vote.

What a crazy week. The biggest news is that we had a hosting company who actually paid a 1 million dollar (think Dr. Evil) ransomware payment. We then had the return of Locky, which at one point was the preminent ransomware being distributed. We will have to wait and see if it can become king of the hill again.

Other than that, it has mostly been small ransomware variants being released that will probably that will probably never make it into any real distribution.

UPCOMING CONFERENCES, WORKSHOPS, TRAINING, ETC.
==========

CALL FOR PAPERS:

Hackfest.ca CFP
Jun 15, 2017 End of round 1
Sep 30, 2017 End of round 2
https://hackfest.ca/en/cfp/

BSides Wellington 2017
Aug 27, 2017 CFP closes
https://www.papercall.io/bsideswlg2017

MACIS 2017 CFP
September 3, 2017 - CFP closed
Vienna, Austria
https://macis2017.sba-research.org/

EVENTS:

Hack in Paris
June 19 - 23, 2017
Paris, France
https://hackinparis.com/

SANS DFIR Summit
June 22 - 23, 2017
Austin, TX
https://www.sans.org/event/digital-forensics-summit-2017

BrrCon
June 23, 2017
Minneapolis, MN
https://brrcon.com/

BSides MSP
June 24 - 25, 2017
St. Paul, MN
https://www.bsidesmsp.org/

Nuit Du Hack XV
June 24 - 25, 2017
Paris, France

https://www.nuitduhack.com/en

Community College Cyber Summit (3cs)
June 28 - 30, 2017
National Harbor, Maryland
https://www.my3cs.org/

BSides Chicago
July 15, 2017
Chicago, IL
https://bsideschicago.org/

Black Hat USA
July 22-27, 2017
Las Vegas, NV
https://www.blackhat.com/us-17/

BSides Las Vegas
July 25 - 26, 2017
Las Vegas, NV
https://www.bsideslv.org/

DEF CON 25
July 27 - 30, 2017
Las Vegas, NV
https://www.defcon.org/

SANS Security Awareness Summit
August 2 - 3, 2017
Nashville, TN
https://www.sans.org/event/security-awareness-summit-2017

26th USENIX Security Symposium
August 16 - 18, 2017
Vancouver, BC
https://www.usenix.org/conference/usenixsecurity17

(ISC)Â² Security Congress 2017
September 25-27, 2017
Austin, Tx
http://blog.isc2.org/isc2_blog/2016/09/2017-security-congress.html

M3AAWG General Meeting (members)
October 2-5, 2017; training October 2
Toronto, CA
https://www.m3aawg.org/upcoming-meetings

Hackfest.ca 2017
Oct 31 - Nov 4, 2017
Quebec City, QC, CA
https://hackfest.ca/en/

MACIS 2017
November 15-17, 2017
Vienna, Austria
https://macis2017.sba-research.org/

BSides Wellington

November 23-24, 2017
Wellington, NZ
https://bsides.nz/

REFERENCES
==========

[A] CREDITS

Thanks to the following individuals for contribution to the Daily Report:

Sarah Bigham (REN-ISAC), writer
Sheryl Swinson (REN-ISAC), writer
Chris O'Donnell (REN-ISAC), writer
Doug Pearson (REN-ISAC), editor

Research and Education Networking ISAC
24x7 Watch Desk: +1(317)274-7228
soc@ren-isac.net