May 29, 2018

Hacking Healthcare

TLP White

We start with a recent breach coming out of an LA nonprofit and then address a new study that found users are failing (surprised?) to update their devices with the necessary patches and updates. We then discuss a new standards-setting process issued by NIST for biomedical imaging and artificial intelligence. We conclude with another SamSam ransomware attack and a discussion about a recent report addressing the impact ransomware attacks continue to have on the healthcare industry. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Breach in LA County.*** 211 LA County ("211"), a nonprofit dedicated to providing information and referrals for health and human services to people in LA County,[1] accidentally exposed 3.2 million files containing personally identifiable information ("PII") of LA County's abuse and crisis victims due to a misconfigured Amazon Web Services ("AWS") S3 storage bucket.[2]

   According to Amazon, S3 is a cloud service that allows users to "store and retrieve any amount of data, at any time, from anywhere on the web"[3] and buckets are used to store and upload the data – e.g., photos, videos, documents, etc. – to the cloud.[4]

   UpGuard, a cyber-resilience company,[5] discovered the misconfiguration on March 14, 2018 and although not all files were publicly accessible, those that were contained thousands of rows of PII including (1) employee access credentials; (2) email addresses; (3) home addresses; (4) phone numbers; (5) birthdates; and (6) sensitive call notes discussing abuse and suicidal distress.[6] 211 maintains a single database for all of its reports which, according to UpGuard, makes the database a "crown jewel" for attackers. As of April 24, 2018, the bucket is no longer accessible.

[1] https://www.211la.org

[2] https://www.darkreading.com/cloud/la-county-nonprofit-exposes-32m-pii-files-via-unsecured-s3-bucket/d/d-id/1331875

[3] https://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html

[4] https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html

[5] https://www.upguard.com

[6] https://www.upguard.com/breaches/la-county-211-hotline

2. ***Failure to Update.*** According a study released by Duo Security, a security provider,[7] users are running outdated smartphone and computer devices.

   The study found that 90 percent of over 10.7 million Android devices are running outdated operating systems and only 8 percent are running the latest security patch.[8] The large gap is likely because Android users do not always receive updates from their carriers and/or phone manufactures. For example, Android OS is installed onto many different devices – e.g., Samsung and LG smartphones – which places the onus on many manufactures to send updates to users. Hackers, aware of this, take advantage and frequently attack outdated Android devices. The study also found that 56 percent of iOS devices are running outdated software.

   Not surprisingly, the same study reported that 74 percent of MacOS and 85 percent of ChromeOS computers are not running the latest operating systems either. However, according to Duo Security, an outdated Chrome computer is not comparable to other computers because ChromeOS automatically updates on every restart. Meaning, an outdated ChromeOS is likely only a few weeks behind while another outdated platform may be many months behind.

3. ***AI and Medical Decision-Making.*** Experts from the medical imaging and artificial intelligence ("AI") communities recently gathered in a two-day workshop focused on opportunities for high-tech in the future of medical decision-making.[9] Workshop participants included medical specialists such as radiologists, medical imaging device manufacturers, researchers, data scientists and federal agency representatives. During the workshop, participants presented a shared vision of creating a "diagnostic cockpit" which would provide medical experts with the data needed to diagnose and treat patients while using AI to conduct data analysis on provide behind the scenes support to medical experts. By harnessing patient data, such as genetic information, medical history and high-resolution imaging data and integrating the information with AI technology, medical experts can improve the quality of diagnostics. Better diagnostics means better patient outcomes and reduced health care costs. It can't get much better than that.

   In order to make the diagnostic cockpit dream a reality, there is a need for standards to ensure that medical imaging devices output data in a standardized format. While there is an existing standard, known as Digital Imaging and Communication in Medicine, there is a need for a standard that can account for larger and more complex data streams.

[7] https://duo.com/about

[8] https://www.cyberscoop.com/android-updates-out-of-date-duo-security/

[9] https://www.nist.gov/blogs/taking-measure/next-big-health-care-merger-biomedical-imaging-and-artificial-intelligence

The purpose of the workshop was to identify the standards needed to integrate big medical data with artificial intelligence, including new data formats, imaging protocols, performance metrics, human/computer interfaces and data visualization techniques. According to NIST, "[s]tandardization at scale will fuel machine learning and create new generations of analytics and diagnostic models."[10]

4. ***Ransomware Attacks Won't Let Up.*** The healthcare sector continues to face attacks due to a ransomware strain known as SamSam. Most recently, Allied Physicians of Michiana ("Allied Physicians") a healthcare provider group, discovered a SamSam attack on their network, and immediately shut the network down in an effort to protect patient data and other components of the network.[11] Fortunately, Allied Physicians took swift action, working with their incident responder to restore the data on their network without facing significant disruptions to patient care.

   Allied Physicians are part of a larger ransomware trend in the healthcare sector. Recent data from security firm Proofpoint indicated that the number of healthcare ransomware attacks significantly increased in the third quarter of 2017, outpacing all other types of cyberattacks against healthcare companies.[12] And it is not just SamSam that the healthcare sector has to worry about. There are several other malware strains that have been targeting healthcare, including a banking trojan known as "The Trick" that tricks payment systems to redirect to a counterfeit site with a correct URL and deceivingly genuine digital certificate.

Congress –

Tuesday, May 29:
--No relevant hearings

Wednesday, May 30:
--No relevant hearings

Thursday, May 31:
--No relevant hearings

Conferences and Webinars –

--Health IT Summit – Minneapolis, MN (6/13) <https://vendome.swoogo.com/2018-Minneapolis-Health-IT-Summit>

[10] https://www.nist.gov/blogs/taking-measure/next-big-health-care-merger-biomedical-imaging-and-artificial-intelligence

[11] http://www.healthcareitnews.com/news/samsam-hackers-hit-indianas-allied-physicians-michiana

[12] https://healthitsecurity.com/news/healthcare-ransomware-attacks-soared-in-q3-2017

--Biotech / Pharmaceutical Security Workshop - Dublin, Ireland (6/21) <https://nhisac.org/events/nhisac-events/medical-device-and-pharmaceutical-security-workshop-dublin/>

--Health IT Summit – Nashville, TN (6/28) <https://vendome.swoogo.com/2018-Nasvhille-HITSummit>

--Health IT Summit – Denver, CO (7/12) <https://vendome.swoogo.com/2018-Denver-HITSummit>

--Health IT Summit – St. Petersburg, FL (7/24) <https://vendome.swoogo.com/StPetersburg-HITSummit-2018>

--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>

--Biotech/Pharma Security Workshop at Gilead Sciences, Foster City, CA (8/29) <https://nhisac.org/events/nhisac-events/biopharma-workshop-at-gilead-sciences-foster-city-ca/>

--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>

--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29) <https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –

-- **Wired's Predictions for Bots, Blockchains, Crispr, and More**
<https://www.wired.com/story/predictions-bots-blockchain-and-more>

-- **Inside the Takedown of a Notorious Malware Clearinghouse**
<https://www.wired.com/story/inside-scan4you-takedown/>

-- **Another perspective on state election security**
<https://www.politico.com/newsletters/morning-cybersecurity/2018/05/21/another-perspective-on-state-election-security-224517>

-- **YubiKey arrives on iOS**
<https://www.cyberscoop.com/yubikey-ios-apple/>

-- **Senators want National Guard on call for cyberattacks**
<https://www.cyberscoop.com/cyber-defenders-act-national-guard-maria-cantwell-joe-manchin/>

-- **North Korean Defectors Targeted with Malicious Apps on Google Play**
<https://www.darkreading.com/threat-intelligence/north-korean-defectors-targeted-with-malicious-apps-on-google-play/d/d-id/1331856>

-- **Phishing Email Ironically Provides a List of Scammers You Should Avoid**
< https://www.bleepingcomputer.com/news/security/phishing-email-ironically-provides-a-list-of-scammers-you-should-avoid/>

-- **Google to Delete 'Secure' Label from HTTPS Sites**
<https://www.darkreading.com/cloud/google-to-delete-secure-label-from-https-sites/d/d-id/1331851>

-- **Using chrome://settings/cleanup to Scan for Unwanted Software Using Chrome**

May 29, 2018

<https://www.bleepingcomputer.com/tips/web-browsers/using-chrome-settings-cleanup-to-scan-for-unwanted-software-using-chrome/>
-- **DHS secretary says she hasn’t seen assessment that Russia interfered to help Trump win**
<http://thehill.com/policy/cybersecurity/388759-dhs-secretary-says-she-hasnt-seen-assessment-that-russia-interfered-to>

Contact us: follow @NHISAC and email at contact@nhisac.org