August 28, 2018

Hacking Healthcare

TLP White

We start with a Louisiana decryption case and potential repercussions of compelled decryption in the healthcare industry. We also discuss a resurgence of the Mirai malware. We conclude by shedding some light on the Apache Struts vulnerability and the multi-stakeholder coordinated vulnerability disclosure process. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Compelled Decryption v. Fifth Amendment Protection.*** Like many areas of the law that impact new technologies, the doctrine around compelled decryption is murky to say the least. Fundamentally, the dispute centers around whether individuals can be compelled to unlock their own digital devices as part of criminal investigation, or whether they can protect themselves from self-incrimination under the Fifth Amendment.

   A case that is currently underway in Louisiana is grappling with this debate in conjunction with a fatal college fraternity hazing incident.[1] The prosecutors in that case requested a judge to compel one of the defendants, a Louisiana State University student, to provide his cell phone passcode. The prosecution would like to access communications with the victim sent via the GroupMe app. However, the courts are split on whether forcing the defendant to provide their passcode is "testimonial" i.e. would result in compelling the defendant to provide statements that would help the prosecution build a case against him in much the same way that an incriminating statement would.

   A law professor commenting on the case noted that the defendant "had a choice and chose not to use fingerprint access because he wanted more security from government intrusion." Hard to say whether a college student had the foresight to anticipate potential government intrusion such that it influenced his decision regarding security features.

[1] https://arstechnica.com/tech-policy/2018/08/prosecutor-suspect-must-give-up-his-phones-passcode-in-fatal-hazing-case/

2. ***Mirai on the Rise.*** Mirai is back! Ok, so it never really left, but this summer the malware has resurfaced and has been detected on more types of devices and platforms than previous iterations. The original author of this variant, known as "Sora," had supposedly moved on to develop other versions of the Mirai malware. This has led analysts to posit that other malware authors stepped in and decided to improve Sora by creating variants of their own. One enterprising developer decided to compile Sora with a utility that allows the malware to spread to a significant number of platforms, including on Android devices.

   The Sora variant is not the only version of Mirai to resurface. Researchers have noticed a steady increase in the number of Mirai attacks over the last twelve months. One explanation for this increase is failure to patch outdated devices, a challenge the healthcare sector is particularly familiar with as many devices are older and expensive to patch and/or replace. Vulnerabilities such as Mirai and others like it have a tendency to linger, and to pop back up over time – often more destructive than the first version as we are seeing with this Sora variant.

3. ***Speaking of Resurging Vulnerabilities.*** In other blast from the past news, last week the Apache Software Foundation released software updates for a critical vulnerability in Apache Struts.[2] Apache Struts is a web component infamous for its role in the 2017 Equifax breach, which led to the exposure of personal information belonging to 147 million Americans. Shortly after last week's update was released, researchers discovered computer code posted online that essentially gives bad actors a step-by-step guide to accessing unpatched servers by using only a web browser, making it even more challenging for companies using the application to manage the impact of the vulnerability.[3]

   The potential impact of this exploit is significant. An estimated 65% of fortune 100 companies use Apache Struts and are thus vulnerable to this threat if left unpatched. Large scale vulnerabilities like the Apache Struts vulnerability highlight the importance of the multi-stakeholder coordinated vulnerability process in responding to and managing large-scale, multi-party vulnerability disclosure incidents.

   As is the case with Mirai as we previewed above, large-scale vulnerabilities often occur in multiple rounds, meaning that the disclosure process is often repeated several times for any given vulnerability.

   How the global industry deals with these types of vulnerabilities is the subject of considerable ongoing debate.

[2] https://cwiki.apache.org/confluence/display/WW/S2-057

[3] https://krebsonsecurity.com/2018/08/experts-urge-rapid-patching-of-struts-bug/

August 28, 2018

Congress –

<u>Tuesday, August 28</u>:
--No relevant hearings.

<u>Wednesday, August 29</u>:
--Oversight hearing to examine the Food and Drug Administration, focusing on leveraging cutting-edge science and protecting public health (Senate Committee on Health, Education, Labor, and Pensions).[4]

<u>Thursday, August 30</u>:
--No relevant hearings.

Conferences, Webinars, and Summits –

--NH-ISAC Blended Threats Exercise Series – No. CA (8/28) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--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/>
--Basic Best Practices in Cybersecurity – Abilene, KS (8/29) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-kansas-3/>
--NH-ISAC Radio member-to-member discussion: Cybersecurity Design Engineering for Medical Devices – find link in Member email (8/31 Noon ET)
--Basic Best Practices in Cybersecurity – Granite Falls, MN (9/5) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-granitefalls-mn/>
--NH-ISAC Blended Threats Exercise Series – DE (9/10) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--ICS Security Workshop – Cork, Ireland (9/20) <http://www.cvent.com/events/booz-allen-nh-isac-ics-security-workshop/event-summary-098b4a1a7bca4da78550a3883853b1d6.aspx>
--Basic Best Practices in Cybersecurity – Nashville, TN (9/21) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-nashville/
--Health IT Summit – Raleigh, NC (9/27) <https://nhisac.org/events/>
--NH-ISAC Blended Threats Exercise Series – GA (10/2) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--NH-ISAC Blended Threats Exercise Series – MD (10/4) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>
--Information Sharing Turns 20: Learn more at Borderless Cyber USA – Washington, DC (10/4) <https://nhisac.org/events/nhisac-events/information-sharing-turns-20-learn-more-at-borderless-cyber-usa/>

[4] https://www.senate.gov/committees/hearings_meetings.htm

--HSCC Joint Cyber Working Group Meeting – Nashville, TN (10/9-11) <https://nhisac.org/events/nhisac-events/hscc-joint-cyber-working-group-meeting/>

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

--Biotech/Pharma Security Workshop – Tokyo, Japan (10/17) <https://nhisac.org/events/nhisac-events/biotech-pharma-security-workshop-tokyo/>

--CSS - "Table Stakes" in the Development and Deployment of Secure Medical Devices – Minneapolis, MN (10/22) <https://nhisac.org/events/nhisac-events/css-3/>

--Summit on Third-Party Risk – Leesburg, VA (10/24-26) <https://nhisac.org/events/nhisac-events/summit-on-third-party-risk/>

--NIST Cybersecurity Risk Management Conference – Baltimore, MD (11/4-6) <https://www.nist.gov/cyberframework>

--Health IT Summit – Beverly Hills, CA (11/8-9) <https://vendome.swoogo.com/2018-BeverlyHills>

--NH-ISAC Blended Threats Exercise Series – So. CA (11/19) <https://nhisac.org/events/nhisac-events/blended-threats-exercise-series/>

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

Sundries –

-- **Do we need a 'cyber 911?' A former FBI cyber agent thinks so.** <https://www.cyberscoop.com/andre-mcgregor-cyber-911-fedtalks/>

-- **DNC says phishing incident was a false alarm** <https://www.bleepingcomputer.com/news/security/academics-discover-new-bypasses-for-browser-tracking-protections-and-ad-blockers/>

--**Lazarus Group Deploys Its First Mac Malware in Cryptocurrency Exchange Hack** <https://www.bleepingcomputer.com/news/security/lazarus-group-deploys-its-first-mac-malware-in-cryptocurrency-exchange-hack/>

--**Idle Android Phones Send Data to Google Ten Times More Often Than iOS Devices to Apple** <https://www.bleepingcomputer.com/news/google/idle-android-phones-send-data-to-google-ten-times-more-often-than-ios-devices-to-apple/>

--**7 Serious IoT Vulnerabilities** <https://www.darkreading.com/iot/7-serious-iot-vulnerabilities/d/d-id/1332616>

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