May 19th, 2020

TLP White

This week, Hacking Healthcare begins by examining what to expect from two federal agencies formally naming China as a culprit in ongoing cyber espionage against healthcare organizations. Next, we highlight new research that emphasizes just how important identity is to organizational cybersecurity and what the H-ISAC is doing to help members interested in taking an identity-centric approach to cybersecurity. Lastly, we briefly examine why it's not so easy to counter the COVID-19 social media misinformation that may be harming mitigation and response efforts.

Reminder: H-ISAC Member Only Monthly Threat Brief: H-ISAC members are encouraged to join this month's Threat Brief Webinar on May 26th at 12:00pm EST. Topics include adversaries targeting healthcare, Ransomware as a Service, mitigating threats to healthcare workers, RDP vulnerabilities, and the upcoming FTC review of the Health Breach Notification rule. The webinar is free for H-ISAC members and details are sent out on the members listserver. Welcome back to *Hacking Healthcare*.

1. **U.S. Formally Accuses China of COVID-19 Research Hacks**: On May 13th, the Federal Bureau of Investigation ("FBI") and the Department of Homeland Security's ("DHS") Cybersecurity and Infrastructure Security Agency ("CISA") released a joint Public Service Announcement ("PSA") to "raise awareness" regarding Chinese government affiliated entities targeting COVID-19 research.[1] In response, the People's Republic of China's ("PRC") Ministry of Foreign Affairs spokesperson denied the accusation stating "It is immoral to target China with rumors and slanders in the absence of any evidence."[2]

   The PSA outlines how the FBI is investigating the "targeting and compromise of U.S. organizations conducting COVID-19-related research by PRC-affiliated cyber actors," and that "These actors have been observed attempting to identify and illicitly obtain valuable intellectual property (IP) and public health data related to vaccines, treatments, and testing from networks and personnel affiliated with COVID-19-related research." [3] As a result, both CISA and the FBI are urging all organizations likely to be affected to ensure that they are properly supporting and implementing appropriate cybersecurity safeguards.

   Recommendations include:

- Assume that press attention affiliating your organization with COVID-19 related research will lead to increased interest and cyber activity.
- Patch all systems for critical vulnerabilities, prioritizing timely patching for known vulnerabilities of internet-connected servers and software processing internet data.
- Actively scan web applications for unauthorized access, modification, or anomalous activities.
- Improve credential requirements and require multi-factor authentication.
- Identify and suspend access of users exhibiting unusual activity.

For more information on this subject, have a look at the whitepaper the Healthcare and Public Health Sector Council recently release on Health Industry Cybersecurity Protection of Innovation Capital.[4]

And don't forget that hackers more often than not are taking advantage of known vulnerabilities and weaknesses, as noted recently by US-CERT in Alert (AA20-133A) Top 10 Routinely Exploited Vulnerabilities.[5] We know that patching can be challenging, but it's one of the most impactful things you can do to improve your security posture.

Analysis & Action

H-ISAC Membership Required

2. **New Research Highlights the Importance of Identity in Cybersecurity:** Last week, the Identity Defined Security Alliance ("IDSA") released a report entitled *Identity Security: A Work in Progress*. The report, which was based on a survey of IT security and identity professionals, looked to examine "the risks endangering enterprise identities and explore why some companies are doing better at securing those identities than others."[6] Their findings give an interesting glimpse at the evolution of identity-centric approaches to cybersecurity.

   Among the key facts and figures, IDSA found that 94% of those surveyed have had an identity related breach, and 79% said such a breach occurred in the past two years.[7] Additionally, two thirds of respondents highlighted phishing as the most common cause of identity related breaches and an astounding 99% believed that their identity related breach was preventable.[8] Lastly, a significantly fewer number of companies that adopt a "forward-thinking" security culture have experienced an identity related breach in the past year when compared to organizations with "reactive" security cultures.[9]

   The 14-page document goes on to detail how confident organizations are at securing various aspects of identity, which kind of identities were most likely to be compromised, and what each company could have done to lower the likelihood of an identity related

breach. Their report wraps up with several pages outlining the progress being made within industry to adopt identity-centric approaches and highlighting benefits that survey respondents perceive to have gained from it. The report is freely available on the IDSA website.

Analysis & Action

H-ISAC Membership Required

3. **The State of COVID-19 Misinformation:** While malicious cyber actors continue to target the healthcare sector for ransom or valuable COVID-19 research, a more visible threat to COVID-19 response efforts is delivered daily to the general population worldwide. Social media sites like Twitter and Facebook, and video sharing platforms like YouTube and TikTok, are contending with wide-spread medical misinformation. Effectively countering the false narratives and unscientific advice that is routinely posted to these platforms is proving to be a challenge. One example of this has been the incorrect statements that 5G wireless towers are responsible for the spread of COVID-19[10]. Unfortunately, it isn't hard to envision a situation where misinformation like this could implicate hospitals, laboratories, or their personnel.

   To be fair, Twitter is making efforts to label and warn its users of content that includes misleading or disputed medical information, and Facebook is doing the same in partnership with over 60 fact checking organizations.[11, 12] Despite these efforts, there seems to be an entrenched and pervasive amount of COVID-19 conspiracy theories and misinformation on social media sites. Unfortunately, this state of affairs seems unlikely to change in the near future due to significant logistical, technical, legal, and political reasons.

   Freedom of speech, the various mediums involved, and the sheer volume of COVID-19 misinformation that is created daily poses legal, political, logistical, and technical challenges that are difficult at best.

   Analysis & Action

   H-ISAC Membership Required

Congress –

Tuesday, May 19th:
- No relevant hearings

Wednesday, May 20th:
- House – Committee on Education and Labor – "Examining the Federal Government's Actions to Protect Workers from COVID-19"

Thursday, May 21st:
- No relevant hearings

May 19th, 2020

International Hearings/Meetings –

EU –

- No relevant hearings

Conferences, Webinars, and Summits –

--H-ISAC Virtual Training: Securing Medical Device Infrastructure on a Shoestring Budget – Virtual (5/20/2020)
https://h-isac.org/hisacevents/h-isac-virtual-training-securing-medical-device-infrastructure-on-a-shoestring-budget/
--H-ISAC Monthly Member Threat Briefing – Webinar (5/26/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-8/
-- H-ISAC Virtual Security Workshop – Webinar (5/27/2020)
https://h-isac.org/hisacevents/nz-virtual-workshop/
--Shared Solution Webinar: Managed Threat Detection for the Rest of Us – Webinar (5/28/2020)
https://h-isac.org/hisacevents/managed-threat-detection-for-the-rest-of-us/
H-ISAC Shared Solutions: Adapting Your Third-Party Program to Rapidly Changing Times (TLP White) – Webinar (6/2/2020)
https://h-isac.org/hisacevents/h-isac-shared-solutions-adapting-your-third-party-program-to-rapidly-changing-times-tlp-white/
--Identity for the CISO – Becoming 'Identity-Centric' – Webinar (6/3/2020)
https://h-isac.org/hisacevents/identity-for-the-ciso/
-- An H-ISAC Framework for CISOs to Manage Identity – Webinar (6/10/2020)
https://h-isac.org/hisacevents/framework-for-cisos-to-manage-identity/
-- Life as a CISO by Axonius
https://h-isac.org/hisacevents/life-as-a-ciso-axonius/
--AAMI Exchange – New Orleans, LA (6/12/2020-6/15/2020)
https://h-isac.org/hisacevents/aami-exchange/
--H-ISAC 2020 Inaugural APAC Summit – Singapore (6/23/2020-6/25/2020)
https://h-isac.org/summits/apac-summit-2020/
H-ISAC Monthly Member Threat Briefing – Webinar (6/30/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-9/
--Healthcare Cybersecurity Forum - Mid-Atlantic – Philadelphia, PA (7/17/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426497
--Healthcare Cybersecurity Forum - Rocky Mountain – Denver, CO (7/20/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426499
--Healthcare Cybersecurity Forum – Southeast – Nashville, TN (9/9/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426517
--H-ISAC Security Workshop - Greenwood Village, CO (9/16/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-greenwood-villiage-co/
--Healthcare Cybersecurity Forum – Northeast – Boston, MA (9/22/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/427126
--H-ISAC Cyber Threat Intel Training - Titusville, FL (9/22/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-titusville-fl/

--H-ISAC Security Workshop - Forchheim, Germany
https://h-isac.org/hisacevents/h-isac-security-workshop-forchheim-germany/
--Summit on Security & Third Party Risk – National Harbor, MD (9/28/2020-9/30/2020)
https://h-isac.org/hisacevents/summit-on-security-third-party-risk/
--Healthcare Cybersecurity Forum – Texas – Houston, TX (10/8/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840
--CYSEC 2020 – Dubrovnik, Croatia (10/27/2020 – 10/28/2020)
https://h-isac.org/hisacevents/cysec-2020-croatia/
--H-ISAC Security Workshop - Mounds View, MN (10/27/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-buffalo-ny/
--Healthcare Cybersecurity Forum - Pacific Northwest – Seattle, WA (10/28/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428886
--H-ISAC Security Workshop - Seattle, WA – (10/29/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-seattle-wa-2/
--Healthcare Cybersecurity Forum – California – Los Angeles, CA (11/12/2020)
https://h-isac.org/hisacevents/healthcare-cybersecurity-forum-california-2/
--H-ISAC Security Workshop - Paris, France (11/18/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-paris-france/

Sundries –

--US Commerce Department tightens screws on Huawei export controls
https://www.cyberscoop.com/huawei-export-controls-commerce-department/
--Researchers expose new malware designed to steal data from air-gapped networks
https://www.cyberscoop.com/eset-ramsay-air-gap-malware/
-- IoT security: How these unusual attacks could undermine industrial systems
https://www.zdnet.com/article/iot-security-how-these-unusual-attacks-could-undermine-industrial-systems/
-- Paying the Ransom Can Double Ransomware Attack Recovery Costs
https://healthitsecurity.com/news/paying-the-ransom-can-double-ransomware-attack-recovery-costs

Contact us: follow @HealthISAC, and email at contact@h-isac.org

[1] https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf.pdf
[2] https://www.cyberscoop.com/coronavirus-vaccine-china-hacking-dhs-fbi/
[3] https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf.pdf
[4] https://healthsectorcouncil.org/hic-pic/
[5] https://www.us-cert.gov/ncas/alerts/aa20-133a
[6] https://www.idsalliance.org/wp-content/uploads/2020/05/Identity-Security-A-Work-in-Progress.pdf
[7] https://www.idsalliance.org/wp-content/uploads/2020/05/Identity-Security-A-Work-in-Progress.pdf
[8] https://www.idsalliance.org/wp-content/uploads/2020/05/Identity-Security-A-Work-in-Progress.pdf
[9] https://www.idsalliance.org/wp-content/uploads/2020/05/Identity-Security-A-Work-in-Progress.pdf
[10] https://arstechnica.com/tech-policy/2020/05/prepare-for-cell-tower-attacks-by-5g-covid-19-conspiracy-theorists-us-warns/

[11] https://www.cyberscoop.com/twitter-coronavirus-false-information-warning/
[12] https://about.fb.com/news/2020/04/covid-19-misinfo-update/