September 5, 2018

TLP White

We start with a glimpse at a special flavor of cyber extortion and then discuss a letter from Congress about an important cybersecurity related program. We conclude with an update on California privacy legislation as the California legislative session comes to an end. Welcome back to *Hacking Healthcare:*

Hot Links –

1. ***Cyber Extortion Threatens More Than Your Wallet.*** Cybercriminals have found many ways to use extortion in the cyber environment, threatening to steal data or to reveal compromising content in exchange for a sum of money, typically in bitcoin. Recently, companies are facing threats to their most valuable asset: their reputation. CheapAir, a flight price comparison website, found itself on the receiving end of such a reputational extortion scheme.[1] The hackers, which refer to themselves as STD Company, explain that "[o]nce we complete our job, even if your site remains on Google, you can be sure that all first page would be full of negative results about your company…." The email goes on to state STD Company's plans to create thousands of negative reviews on consumer websites TrustPilot and RipOff report, in addition to threatening to leave thousands of negative posts and replies on CheapAir's social media accounts.

   CheapAir has taken the position that it will not pay "these cyber thugs." However, the company is still forced to devote significant time and resources to combating STD Company's efforts.

   Both Twitter and Facebook have been active in this area, developing tools and features to help limit these types of attacks

   Twitter CEO Jack Dorsey is scheduled to testify before Congress on Wednesday September 5, 2018 along with Facebook COO Sheryl Sandberg on foreign influence

[1] https://motherboard.vice.com/en_us/article/8xbpdb/scammers-review-bomb-twitter-bots-instagram-fake-reviews-cheapair-std-company

operations' use of social media platforms.[2] Additionally, Dorsey is scheduled to testify alone in a hearing about how the company's algorithms work to filter out abuse and Twitter's decision-making process when it blocks certain content and accounts from appearing on its site.[3]

Facebook has been taking similar approaches to Twitter, but for many, these approaches begin to encroach on free speech rights. As such, Congress will likely continue to focus on these issues in the months to come, particularly in light of the upcoming election cycle.

2. ***Congress Makes CVE Program Recommendations.*** In March 2017, the House Committee on Energy and Commerce ("committee") began an investigation into the Common Vulnerabilities and Exposures ("CVE") program. The investigation was conducted in response to reports that the CVE program was having a difficult time fulfilling its purpose and meeting stakeholder needs, taking several weeks or months to process CVE number requests, and in some cases rejecting them altogether for being "out of scope."[4] Following the conclusion of the investigation, committee leadership sent a letter to the Department of Homeland Security ("DHS")[5] and the MITRE Corporation[6] (entities responsible for administering the CVE program) that identifies irregular funding and failure to conduct regular audits as the root causes for the CVE program's shortcomings.

   After reviewing the documentation, the committee made two recommendations. First, the committee recommended that DHS should transition the CVE program to a dedicated Program, Project or Activity ("PPA") line item in its annual budget. Currently, the CVE program relies on a contract-based funding model. This inconsistent source of funding forces the CVE program to focus on short-term goals rather than long term thinking. Second, the committee recommended that both DHS and MITRE perform biennial reviews of the program to ensure program stability and effectiveness. In the letters, the committee noted that during the investigation the committee found limited documentation to demonstrate regular reviews of the CVE program. The committee suggested that regular program reviews would help the CVE to catch and address the types of administrative problems which have led to current failures, and would help the program adapt to evolving stakeholder needs.

---

[2] https://www.intelligence.senate.gov/hearings/open-hearing-foreign-influence-operations%E2%80%99-use-social-media-platforms

[3] https://energycommerce.house.gov/news/press-release/ec-announces-twitter-ceo-jack-dorsey-will-testify-september-5th/

[4] https://energycommerce.house.gov/wp-content/uploads/2018/08/082718-DHS-Recommendations-for-CVE-Program.pdf

[5] https://energycommerce.house.gov/wp-content/uploads/2018/08/082718-DHS-Recommendations-for-CVE-Program.pdf

[6] https://energycommerce.house.gov/wp-content/uploads/2018/08/082718-MITRE-Recommendations-for-CVE-Program.pdf

3. ***The Battle Continues Over the CA Privacy Bill.*** Despite the passage of AB 375 earlier this summer, California lawmakers have been working on a new bill, SB 1121 in an effort to fix some of the shortcoming of the original bill.[7] AB 375 was designed to give consumers more control over what data companies collect about them and how it is used. It was written and passed very quickly in the hopes of staving off an aggressive ballot initiative which would have had sweeping impacts for anyone doing business on the internet. SB 1121 was originally supposed to address typos and technical errors in AB 375, pushing more substantive changes to next year's legislative session. However, industry groups have been hard at work over the last few weeks, urging legislators to address more substantive changes to AB 375 vis-à-vis SB 1121, including changes to definitions of key terms and changes to the bill's scope. Consumer groups have also been active in the last few weeks, criticizing the bill in its current form for not providing a private right of action, leaving enforcement up to the Attorney General. The issue of providing a private right of action was part of the California ballot initiative that was at the root of this political hubbub earlier this year. California Attorney General Xavier Becerra recently proposed a list of changes of his own, which includes restoration of the private right of action

   One thing that both industry and consumer groups can agree upon is that the bill needs work. With only a few days left in California's legislative session, the battle over the future of consumer privacy in California and beyond will undoubtedly continue into 2019. These efforts are occurring in parallel with efforts to pass federal privacy legislation, which if passed would preempt California's law. And of course, the outcome of the upcoming federal mid-term elections will also play a part in shaping the course of consumer privacy in the years to come. For now, as the California legislative session comes to an end, groups on both sides of the debate over California privacy will retreat and regroup, and are scheduled to reconvene in early 2019.

Congress –

Tuesday, September 4:
--No relevant hearings.

Wednesday, September 5:
--Hearing entitled, "Reusable Medical Equipment: Continuing to Examine VHA's Sterile Processing Problems" (House Subcommittee on Oversight and Investigations).[8]
--Hearing entitled, "Opportunities to Improve Health Care" (House Subcommittee on Health).[9]

[7] https://www.wired.com/story/california-privacy-bill-tech-lobbying/
[8] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108637
[9] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108643

Thursday, September 6:
--Joint hearing entitled, "Understanding Cybersecurity Threats to America's Aviation Sector" (House Subcommittee on Cybersecurity and Infrastructure Protection & House Subcommittee on Transportation and Protective Security).[10]
--Hearing entitled, "Examining Federal Efforts to Ensure Quality of Care and Resident Safety in Nursing Homes" (House Subcommittee on Oversight and Investigations).[11]

Conferences, Webinars, and Summits –

--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/>
--Basic Best Practices in Cybersecurity – Nashville, TN (9/21) <https://nhisac.org/events/nhisac-events/basic-best-practices-in-cybersecurity-nashville/
--H-ISAC Radio: Cloud Security-Member discussions (9/24) Find listen-in link in member email
--ICS Security Workshop – Cork, Ireland (9/25) <http://www.cvent.com/events/booz-allen-nh-isac-ics-security-workshop/event-summary-098b4a1a7bca4da78550a3883853b1d6.aspx>
--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/>
--HSCC Joint Cyber Working Group Meeting – Nashville, TN (10/9-11) <https://nhisac.org/events/nhisac-events/hscc-joint-cyber-working-group-meeting/>
--Biotech/Pharma Security Workshop – Tokyo, Japan (10/17) <https://nhisac.org/events/nhisac-events/biotech-pharma-security-workshop-tokyo/>
--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>
--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>

[10] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108646
[11] https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108648

--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 –

--**Germany launches new cybersecurity research agency modeled after DARPA**
<https://www.cyberscoop.com/germany-cybersecurity-research-agency-modeled-after-darpa/>
--**Google's FIDO Based Titan Security Key Now Available for $50 USD**
<https://www.bleepingcomputer.com/news/google/googles-fido-based-titan-security-key-now-available-for-50-usd/>
--**ES&S security lead: We trust our process over DEF CON village findings**
<https://www.cyberscoop.com/chris-wlaschin-ess-def-con-voting-village-election-security/>
--**6 Reasons Security Awareness Programs Go Wrong** <https://www.darkreading.com/threat-intelligence/6-reasons-security-awareness-programs-go-wrong/d/d-id/1332644/>
--**'Celebgate' Hacker Heading to Prison**
<https://www.darkreading.com/application-security/celebgate-hacker-heading-to-prison/d/d-id/1332701>

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