November 16th, 2021

TLP White

This week, *Hacking Healthcare* begins by examining how a Tesla over-the-air update went awry and how the incident could have larger implications for the healthcare sector. Next, we call out the risk of holiday phishing scams and why this year may be worse than most. Finally, we break down what to make of the recent announcement from Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency (CISA), that she will be appointing hackers to a new cybersecurity advisory committee.

Welcome back to *Hacking Healthcare*.

1. **Tesla Update Fiasco's Implications for Healthcare**

   A Tesla over-the-air software update gone awry is drawing scrutiny from United States federal regulators around safety oversight while simultaneously touching off a debate over the risks and rewards of an over-the-air update model versus a more traditional recall model. That debate may have significant implications for the healthcare sector as medical devices become ever more connected and cyber threats proliferate.

   On October 23, Tesla pushed out an over-the-air software update to a portion of its vehicles. Notably, it was reported that vehicles were not chosen at random but rather that the update was made optional to a select group of "volunteers who Tesla monitoring show had high safety records."[1] The following day, Tesla began receiving reports that the emergency braking system was unintentionally activating and that the forward collision warning system was not operating as intended. Tesla acknowledged that these malfunctions increased the "risk of a rear-end collision from a following vehicle."[2]

Tesla reportedly "investigated the reports and took actions to mitigate any potential safety risk," all within a "matter of hours."[3] These actions included canceling the update to vehicles that had yet to install it, disabling the affected braking and collision warning systems on vehicles that had installed the update, or rolling back the update.[4] According to Tesla, by the end of the day it had "deterministically reproduced the condition, identified the root cause, and developed software release 2021.36.5.3 as a correction solution."[5] Tesla then tested and validated that the update appeared to effectively fix the issue, and it began pushing out the updated software fix the next morning.

Tesla reported the fault to the National Highway Traffic Safety Administration (NHTSA) on October 29th, which is in line with federal rules that require known defects to be reported within five days, and ordered a full recall on all affected models.[6] Since then, NHTSA has stated it plans to "continue its conversations with Tesla to ensure that any safety defect is promptly acknowledged and addressed according to the National Traffic and Motor Vehicle Safety Act."[7]

Action & Analysis

2. Phish for the Holidays

The holiday season is also phishing season for many cyber criminals who attempt to take advantage of anxious shoppers and busy end-of-year schedules. Over the years, CISA and other government agencies have warned of an increase in "emails and ecards containing malicious links or attachments infected with malware" that may be related to "requesting support for fraudulent charities or causes" or online shopping.[8] While holiday-related phishing attacks are nothing new, the risk to organizations may be higher than usual, with large percentages of employees still working remotely and the line between work and personal life increasingly blurring.

With ecommerce sales continuing to increase yearly, individuals are spending more time than ever shopping sales and tracking package deliveries.[9] At the same time, many individuals are experiencing an end-of-year work crunch that leads to additional stress and weariness. This mixture creates an environment ripe for cyber criminals looking to take advantage with well-crafted phishing emails designed to look like great holiday deals or urgent package delivery messages.[10] What makes this year even more worrisome is the large percentage of employees working remotely, many of whom have increasingly become accustomed to mixing work and personal life.

When the blurring of work and personal life includes using work devices for shopping and personal emails, the cyber risk to organizations increases. Studies released earlier in

the year highlighted how significant an issue this has already become, with HP finding that "70% of office workers surveyed admit to using their work devices for personal tasks" and almost 30% have "let someone else use their work device."[11]

Action & Analysis

3. CISA to Welcome Hackers to Cybersecurity Advisory Committee

In an interesting development that will likely raise a few eyebrows, CISA Director Jen Easterly announced that she will "use her discretion to put members of the hacking community on a new federal advisory committee at the Department of Homeland Security."[12] The move will likely be viewed as controversial to some, but it may have significant implications for legitimizing that community and it could begin a formal process of tapping an underutilized resource.

Speaking at an event last week, Director Easterly announced that she would continue to reach out to the hacking community and that she would adding "some folks [to] our soon to be announced Cybersecurity Advisory Committee."[13] She continued by stating that she wants to "ignite the power of hackers and researchers and academics" to combat the apparent dominance of offense over defense in cyberspace.[14]

The advisory committee to which these hackers will be appointed was only recently officially established, and its primary purpose is broadly described as "to develop, at the request of the CISA Director, recommendations on matters related to the development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the Agency."[15] Exactly how many members of the hacker community will be invited to participate, and how their presence and advice will be received by the committee's other members, will be interesting to see.

Action & Analysis

Congress

Tuesday, November 16th:
- House of Representatives - Committee on Oversight and Reform: "Cracking Down on Ransomware: Strategies for Disrupting Criminal Hackers and Building Resilience Against Cyber Threats"

Wednesday, November 17th:

November 16th, 2021

- House of Representatives - Committee on Homeland Security: "A Whole-of-Government Approach to Combatting Ransomware: Examining DHS's Role."

- House of Representatives - Select Subcommittee on the Coronavirus Crisis: "Combating Coronavirus Cons and the Monetization of Misinformation"

Thursday, November 18th:
- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

EU –

Conferences, Webinars, and Summits –

https://h-isac.org/events/

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

---

[1] https://finance.yahoo.com/news/tesla-fact-recall-software-upends-110000596.html?guccounter=1

[2] https://static.nhtsa.gov/odi/rcl/2021/RCLRPT-21V846-7836.PDF

[3] https://static.nhtsa.gov/odi/rcl/2021/RCLRPT-21V846-7836.PDF

[4] https://static.nhtsa.gov/odi/rcl/2021/RCLRPT-21V846-7836.PDF

[5] https://static.nhtsa.gov/odi/rcl/2021/RCLRPT-21V846-7836.PDF

[6] https://finance.yahoo.com/news/tesla-fact-recall-software-upends-110000596.html?guccounter=1

[7] https://finance.yahoo.com/news/tesla-fact-recall-software-upends-110000596.html?guccounter=1

---

[8] https://us-cert.cisa.gov/ncas/current-activity/2019/11/08/holiday-shopping-phishing-and-malware-scams

[9] https://www.digitalcommerce360.com/article/us-ecommerce-sales/

[10] https://krebsonsecurity.com/2021/11/tis-the-season-for-the-wayward-package-phish/

[11] https://www.securitymagazine.com/articles/95177-study-reveals-growing-cybersecurity-risks-driven-by-remote-work

[12] https://www.nextgov.com/cybersecurity/2021/11/cisa-director-appoint-hackers-cybersecurity-advisory-committee/186776/

[13] https://www.nextgov.com/cybersecurity/2021/11/cisa-director-appoint-hackers-cybersecurity-advisory-committee/186776/

[14] https://www.nextgov.com/cybersecurity/2021/11/cisa-director-appoint-hackers-cybersecurity-advisory-committee/186776/

[15] https://public-inspection.federalregister.gov/2021-24254.pdf?utm_source=federalregister.gov&utm_medium=email&utm_campaign=pi+subscription+mailing+list