SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE EVER EVOLVING AND HIGHLY CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog Feb 2021

Topics covered in this issue:

- Dr. Kevin Fu appointed as acting director of cybersecurity at FDA CDRH
- Cloudstrike publishes 2021 global threat report

FDA CDRH appoints Kevin Fu as acting director of cybersecurity

February 2021 featured a number of significant developments in regards to cybersecurity, and specifically regarding medical device cybersecurity and the cybersecurity of the healthcare sector. The most notable development was the appointment of Kevin Fu to the role of acting director of medical device cybersecurity within the FDA's Center for Devices and Radiological Health on February 1st, 2021 (Cherry, 2021). This post was created on January 1st of 2021, and is a 12-month appointment. The position was created as part of an initiative by the previously-mentioned CDRH's Office of Strategic Partnership & Technology Innovation, which assists the CDRH as it regulates over 6,500 different medical device product categories (U of M, 2021). Kevin Fu is a computer science researcher and the founder of the Archimedes Center for Medical Device Cybersecurity, and has a unique and comprehensive background in medical device cybersecurity, including his current position as a professor at the University of Michigan.

In an interview with the University of Michigan immediately after his appointment, Dr. Fu spoke about the current state of medical device cybersecurity, the challenges faced by medical device developers, and his plans for developing a significant and robust strategy for enhancing medical device security. In the interview, Dr. Fu stated that in recent years medical devices have increasingly come to rely on both the cloud and software, and that this reliance on software presents a modern challenge as software "…wears out much faster than mechanical components". Dr. Fu also highlighted the fact that ensuring medical device developers, stakeholders, and users keep legacy software updated and patched is a "huge challenge". Another primary challenge to medical device cybersecurity broached by Dr. Fu is the sheer number of adversaries mounting attacks on medical devices and healthcare providers-Dr. Fu stated that a decade ago, attacks of the current magnitude were largely "theoretical", but that in the current climate there are "hundreds of hospitals shut down because of ransomware".

Dr. Fu offered some insight into his plans for the post during the interview. Dr. Fu indicated that one of the major causes for concern regarding medical device cybersecurity occurs during the development process. According to Dr. Fu, there are many stakeholders and constituencies involved in the early design stage of medical devices, but security experts are not brought in until later in the process, and are expected to "sprinkle magic security pixie dust" to rectify any security issues.

John Ward – Cyberblog Feb 2021

It is evident that Dr. Fu believes that security experts should be brought into the device and/or software development cycle much earlier than they currently are in most situations, in order to preempt any security preventable security flaws.

Dr. Fu also plans to focus on education as a means to improve medical device cybersecurity. Dr. Fu is a proponent of multi-disciplinary education, and suggested a five-year program which would culminate in a master's degree. Dr. Fu proposed that this education track would combine biomedical engineering, software engineering, and public policy education, and feature a component that would teach students to work collaboratively with experts outside of the computer science field. As an example, Dr. Fu stated that his graduate students attend live surgeries so that they can see the real-world application of medical devices and medical software, as well as the effects they have on patient care.

A press release issued by the University of Michigan focused on Dr. Fu's experience in the field, and indicated that he is "one of the few computer scientists to regularly brief leaders in the White House and Congress" (U of M, 2021). The implication in this observation is that Dr. Fu's experience in briefing decision makers and stakeholders who are not experts in the field could present an opportunity for effective and consequential communication. This is a vital and often-overlooked component of successful governmental-public sector communication-a knowledgeable and credentialed expert in a critical infrastructure sector who is able to effectively and efficiently communicate with the men and women who are responsible for setting policy.

Dr. Fu's appointment as acting director of medical device cybersecurity is an important development in a modern landscape rife with adversaries and ever-advancing techniques. As the world moves becomes more interconnected via the Internet of Things, is also becomes more vulnerable to threats. Of all the critical infrastructure thus exposed to greater digital risk, the healthcare industry offers the greatest risk for acute physical damage, making the need for a coherent and agile cybersecurity policy and leadership structure paramount. The proliferation of ransomware attacks on the healthcare industry detailed later in this report, indicate that the threat is only evolving. Medical devices that are insufficiently secured are at great risk for manipulation and/or encryption by malicious actors, and can serve as entry points for these malicious actors onto vital healthcare networks.

John Ward – Cyberblog Feb 2021

CrowdStrike's 2021 Global Threat Report

American cybersecurity company CrowdStrike's 2021 Global Threat Report details just how pervasive ransomware attacks have become and offers a concerning forecast of how they will continue to develop. This report was touched upon in the previous month's report by this author for Ward Sciences and Consulting LLC, but a deeper examination serves to illuminate the threat landscape of a digitally connected world, both in a broad sense and specifically as it relates to the healthcare industry and the cybersecurity of medical devices. CrowdStrike currently has identified 149 named adversaries, whose actions they track around the globe (CrowdStrike, 2021). They are also currently aware of 29 "clusters", who are adversaries who have been detected performing "targeted intrusion activity", but have not left behind a coherent enough trail of evidence for them to be assigned an identity.

As mentioned in the previous blog by this author for Ward Sciences and Consulting LLC, there were several major trends in eCrime that developed in 2020 and are expected to continue to become more prevalent. Chief among these trends is the consolidation of ransomware resources into targeting a smaller amount of high-value targets, referred to in CrowdStrike's report as Big Game Hunting (BGH). This is a move away from the more traditional ransomware model, where perpetrators in the past mostly focused on a greater number of attacks on a larger number of targets, many of whom were of moderate-to-low value. Crowdstrike also observed a developing trend of two-part ransomware attacks, moving beyond simple encryption and denial of accessibility of files to also threatening to release those files to the public. The final major developing trend of ransomware attacks is the proliferation of resource-sharing hubs, where cyber criminals exchange expertise, consulting services, techniques, tools and products.

To help quantify their data and make it accessible, CrowdStrike has developed what they call the "eCrime Index" (ECX). This tool assigns a computed value which assesses the current state of eCrime. It is similar to how global financial markets are measured, displayed as a graph with a numerical value representing the threat of eCrime. An interested party can access the ECX via the website adversary.crowdstrike.com, and monitor the current level of eCrime activity and risk, and compare it to previous time periods-CrowdStrike's stated purpose for this tool is to "identify notable changes that can be further investigated".

John Ward – Cyberblog Feb 2021

In the report's "Threat Hunting Overview" section, CrowdStrike reports that interaction intrusion activity- "intrusions involving the use of hands-on keyboard techniques", have increased fourfold in the past two years, as monitors by the CrowdStrike Falcon Overwatch team. The report also states that eCrime intrusions (including ransomware) made up 79% of interactive intrusion campaigns in 2020. The other 21% interactive intrusion campaigns are "targeted intrusions", which are those intrusions committed by state-sponsored groups, often for political or espionage purposes. These figures make it evident that while "cyberwar" and "cyberespionage" between nation-states and their suspected proxies and affiliates dominate the headlines and discussion of cybersecurity, cyber criminals are often the more likely perpetrators, with simple financial profit often their primary motivation.

The CrowdStrike report has a great deal to say about the cybersecurity trends of the healthcare industry in 2020, as well as that industry's outlook for the future. As expected, the COVID-19 pandemic proved to be a catalyst for increased targeting of the healthcare sector and development/adoption of certain techniques by digital perpetrators . The healthcare sector was a victim of both targeted and eCrime intrusions during 2020, as the pandemic heightened the stakes in an industry that is already a particularly vulnerable target, as an attack on the healthcare industry has the potential to have patients face "a disruption of critical care facilities" and a "disruption of critical functions" (CrowdStrike, 2021). While these are the same potential consequences of any industry being digitally intruded upon, in the healthcare industry the stakes could be life and death.

Of particular note in the CrowdStrike report was the focus on a unique phenomenon in eCrime intrusions of the healthcare industry. Because of the pandemic and the potential harm that could be caused by disruption of services, CrowdStrike reported that several known adversaries publicly announced that they would not be targeting "frontline healthcare industries". Several other entities also stated that they would quickly rectify any unintentional infections in the healthcare industries, and at least once proved true to their word in the case of a German hospital in September of 2020.

However, this "noble criminal" posture proved in many cases to be a façade, one which could have significant ramifications in the future. CrowdStrike Intelligence reported that during the pandemic in 2020, 18 BGH ransomware families infected 104 healthcare organization, including at least one group that had publicly stated that they wouldn't. False proclamations of leniency of this nature could have potentially, and in the future may potentially, serve as a catalyst for healthcare organizations to be lulled into a false sense of security, reducing their monitoring/vigilance/protections against such threats.

John Ward – Cyberblog Feb 2021

REFERENCES CITED AND RELATED CYBER RESOURCES OF INTEREST

1. Cherry, G. (2021, February 01). U-Michigan professor appointed to FDA medical device security post. Retrieved February 10, 2021, from https://news.engin.umich.edu/2021/02/u-michigan-professor-appointed-to-fda-medical-device-security-post/

2. Corbet, S. (2021, February 18). France to Boost CYBERDEFENSE after Hospital malware attacks. Retrieved February 20, 2021, from https://apnews.com/1e552ec92cffe3edf78b07355be9eda6

3. Kevin FU Fills new leadership position at FDA's Center for devices and Radiological Health, OVERSEEING medical device security. (2021, February 1). Retrieved February 13, 2021, from https://cse.engin.umich.edu/stories/kevin-fu-fills-new-leadership-position-at-fdas-center-for-devices-and-radiological-health-overseeing-medical-device-security

4. Nussbaum, A. (2021, February 17). Bloomberg.com. Retrieved February 20, 2021, from https://www.bloomberg.com/news/articles/2021-02-17/france-s-macron-boosts-cyber-security-spending-after-attacks

5. Sanger, D. (2021, February 24). After Russian Cyberattack, looking for answers and Debating retaliation. Retrieved February 28, 2021, from https://www.nytimes.com/2021/02/23/us/politics/solarwinds-hack-senate-intelligence-russia.html

6. Tucker | AP, B. (2021, February 24). Tech firms say there's little doubt Russia behind major hack. Retrieved February 25, 2021, from https://www.washingtonpost.com/business/technology/tech-firms-say-theres-little-doubt-russia-behind-major-hack/2021/02/23/b93e8256-764e-11eb-9489-8f7dacd51e75_story.html

Copyright (C) 2022 by Ward Sciences and Consulting LLC. Visit our website at www.Wardsciences.com