October 31, 2017

TLP White

Today we are digging into WannaCry and the [grim] Reaper. Enjoy, *Hacking Healthcare:*

Hot Links –

1. **After-action on NHS WannaCry** – The UK's National Audit Office just concluded a review of NHS preparedness and response to WannaCry. The report finds no negative impacts on patient health and safety – some trusts had to reschedule appointments, 5 had to divert emergency visits to other hospitals, and a few trusts were able to continue receiving patients despite the impact of the incident knocking some systems offline.

   NHS trusts were vulnerable to the attack due to poor patch management in Windows 7 systems and use of devices running XP. Unsurprisingly, those trusts that had absorbed the operations of other hospitals through mergers struggled with integrating patch management.

   The government's NHS Digital team had conducted on-sight inspections ahead of the attack (88 of 236 trusts had been inspected; none passed). In the inspections, NHS found that most hospitals had "not identified cybersecurity as a risk to patient outcomes, and had tended to overestimate their readiness to manage a cyber attack."

   The report also finds that there was not an effective system for NHS trusts to report the attack and its impact to the government. Despite NHS developing national incident response plans, they had never been tested at a local level.

2. **The grim "Reaper"** – just in time for Halloween a new botnet is being built. "Reaper" has been described as a spookier implementation of the IoT botnet concept, which was made famous by Mirai. Reaper infects IoT devices not just by exploiting default usernames and passwords (like Mirai), but also by taking advantage of known vulnerabilities to compromise unpatched IoT devices. The holiday period has been the witching hour for black hats over the past few years (especially if your black hat has a national emblem on it). With Reaper and other botnets lurking out there, should we expect large scale deployment around the holidays? It may be for hire. Some say we shouldn't worry.

3. **Please use multifactor authentication** – Javelin's 2017 State of Authentication Report has some sad numbers – only 35 percent of the 400 companies surveyed require MFA for their employees. Even worse, only 5 percent require MFA for both customers and employees. Of course, adoption of any new security technology is difficult, but there are so many good options on the market that actually improve user experience. I find it hard to believe that doctors and nurses really enjoy typing a user name and password and would resist change if shown a more user friendly authentication technology. Please get in touch with any thoughts on effective MFA implementation in clinical environments. We will be happy to document any good examples in future versions of the newsletter.

Congress –

Tuesday, October 31:

--Hearings to examine extremist content and Russian disinformation online, focusing on working with tech to find solutions (Senate Judiciary)

Wednesday, November 1:

--Hearings to examine social media influence in the 2016 United States elections. (Senate Intelligence)

--Russia Investigative Task Force Open Hearing with Social Media Companies (House Intelligence)

--Hearing: "Data Security: Vulnerabilities and Opportunities for Improvement" (House Financial Services)

Conferences and Webinars –

--Business E-mail Compromise (BEC) Workshop – Somerville, MA (NH-ISAC) (11/3)
--Business E-mail Compromise (BEC) Workshop – Kansas City, MO (NH-ISAC) (11/7)
--Biotec/Pharma Security Workshop at MSD, Prague (NH-ISAC) (11/7)
--Business E-mail Compromise (BEC) Workshop – Los Angeles, CA (NH-ISAC) (11/8)
--Health IT Summit – Los Angeles, CA (NH-ISAC) (11/9)
--Cyber Outbreak TTX (NH-ISAC) (11/27)
--NH-ISAC Fall Summit – Cyber Rodeo (11/28-30)
--Regional Healthcare Cybersecurity Summit – Cincinnati, OH (NH-ISAC) (12/7)
--Health IT Summit – Dallas (NH-ISAC) (12/14)

Sundries –

--The Cyberlaw Podcast: Interview with Tom Bossert (LawFare)

October 31, 2017

--Bossert promises new national cybersecurity strategy (CyberScoop)
--NIST-led group drafts report for interagency review on IoT risks (Inside Cybersecurity)
--Telemedicine Is Forcing Doctors to Learn 'Webside' Manner (Wired)
--Ransomware Ripping Through Russia and Ukraine Uses Stolen NSA Code (Daily Beast)
--Merck profit beat clouded by NotPetya attack, shares dip (CNBC)
--Leaked NSA tools were once again used in a global ransomware attack (CyberScoop)
--Another broadband merger: CenturyLink gets FCC approval to buy Level 3 (Ars)
--What Are Basic, Essential Healthcare Cybersecurity Measures? (HealthITSecurity)
--Congress is blowing its shot at real NSA reform (the Verge)

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