December 19, 2017

TLP White
Happy Holidays – fingers crossed none of them are interrupted by incident response duty. Here's hoping for a pass on the worst recent tradition, the major holiday breach (Target, Sony, etc.).

Until then, check out an updated events section with lots of 2018 workshops. Sign-up for a few and enjoy this week's *Hacking Healthcare:*

Hot Links –

1. ***12 days of hacking*** – Welcome to witching season for cyber-crime. The 12 days of Christmas hacking is upon us. Target hit us (just three years ago?) and ushered in a new season when it came to the scale of cyber-crime. But it isn't only credit card fraud – the last couple of holidays have seen a major nation-state hack: think DPRK doxing Sony and Russia turning off the power in Ukraine.

2. ***Triton Malware –*** We have seen a pernicious form of malware announce itself. Triton – which was discovered by FireEye – appears to target certain industrial control systems manufactured by Schneider Electric. Reports indicate the malware targeted operational systems in the middle east oil and gas industries, but these products are used in other heavy industries and manufacturing processes.

   The malware looks to cause havoc by enabling a coordinated manipulation of automated safety systems and human machine interfaces that allow operators to monitor industrial operations. So turn off the safety failures and emergency shutdown process before manipulating an operators view, prompting the employee to send damaging commands to the systems. Or perform a "denial-of-view" attack – giving operators a sense that everything is all right – while simultaneously launching a separate attack on the functioning of the plant.

   This is also a good reminder of the power of information sharing. Getting details of this malware to manufacturers and operators helps drive awareness and create actionable mitigations.

3. ***National Security Strategy*** – The Trump Administration released its National Security Strategy on Monday[1]. This document, which is required by Congress of all Presidents, is intended to guide the Trump Administration's foreign policy and national security agenda for the next three years.

   Cybersecurity takes a front seat in the strategy. And while it is organized as one of the headline priorities, there isn't much *new* stuff in here. There's a reaffirmation of bringing cyber-criminals to justice and improving defensive capabilities alongside offensive tools.

   We do get a slightly narrower focus on critical infrastructure – "Health and Safety" are ranked among the top 6 areas of focus – alongside energy and power, banking and finance, national security, communications, and transportation. There's also a commitment to more and better information sharing and partnership with the private sector.

   In short, the new National Security Strategy has quite a bit to like in it. The key will be successful implementation, which always requires more money and better execution.

4. ***WannaCry*** – The release of the new National Security Strategy (NSS) coincides with the U.S. government attributing the WannaCry attack to the government of North Korea.[2] Since the NSS makes a point of saying they will hold bad actors accountable, should we expect some action from the USG?

   I made the case a couple months back that we should be going after North Korean criminals as part of a larger effort to increase pressure on the Kim regime.[3]

5. ***Kaspersky does not go gently*** – Kaspersky filed a lawsuit against DHS, which contests that DHS should have given Kaspersky time to respond to DHS allegations before publicly calling for the products to be removed from Federal networks.[4] This took place against the backdrop of the President signing a law to codify the prior DHS action against Kaspersky.[5]

6. ***Multifactor reminder*** – Another reminder about the value of basic security measures on critical systems and functions. This one coming out of a security firm in Holland, which had its DNS account compromised and its web-certificates were reissued. This enabled

[1] https://www.whitehouse.gov/issues/national-security-defense/
[2] https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html?tid=pm_pop
[3] https://www.lowyinstitute.org%2Fthe-interpreter%2Fcyber-crime-north-korea-s-billion-dollar-soft-spot
[4] https://arstechnica.com/tech-policy/2017/12/kaspersky-sues-dhs-over-federal-blacklist/
[5] https://www.bleepingcomputer.com/news/government/trump-signs-bill-banning-kaspersky-products-on-government-computers/

the attackers to view encrypted web-traffic including user credentials. According to Ars[6], the company acknowledged that multi-factor authentication could have prevented the breach and mitigated its impact. Also, Facebook[7] (and other sites) are vulnerable to an old man-in-the middle attack. MFA helps there too…

Congress – Congress needs to finish up some business – most notably passing a budget and reconciling the tax legislation, before it heads home for the holidays. No hearings of interest this week.

Conferences and Webinars –

--Health IT Summit – San Diego, CA (2/1) <https://vendome.swoogo.com/san-diego-hitsummit-2018/>
--Medical Device Workshop at Philips Healthcare – Andover, MA (3/20) <https://nhisac.org/events/nhisac-events/medical-device-workshop-at-philips-healthcare-andover-ma/>
--Health IT Summit – Cleveland, OH (3/27) <https://vendome.swoogo.com/2018-Cleveland-Health-IT-Summit>
--Health IT Summit – San Francisco, CA (4/5) <https://vendome.swoogo.com/2018-San-Francisco-HIT-Summit>
--Security Workshops at Intermountain Health – Park City, UT (4/24) <https://nhisac.org/events/nhisac-events/security-workshop-at-intermountain-park-city-ut/>
--2018 NH-ISAC Spring Summit – Sawgrass, FL (5/14-17) <http://www.marriott.com/hotels/travel/jaxsw-sawgrass-marriott-golf-resort-and-spa/>
--Health IT Summit – Philadelphia, PA (5/21) <https://vendome.swoogo.com/2018-Philly-HITSummit>
--Health IT Summit – Minneapolis, MN (6/13) <https://vendome.swoogo.com/2018-Minneapolis-Health-IT-Summit>
--Health IT Summit – Nashville, TN (6/28) <https://vendome.swoogo.com/2018-Nasvhille-HITSummit>
--Health IT Summit – Denver, CO (7/12) <https://vendome.swoogo.com/2018-Denver-HITSummit>
--Health IT Summit – St. Petersburg, FL (7/24) <https://vendome.swoogo.com/StPetersburg-HITSummit-2018>
--Health IT Summit – Boston, MA (8/7) <https://vendome.swoogo.com/2018-Boston-Health-IT-Summit>
--Health IT Summit – Seattle, WA (10/22) <https://vendome.swoogo.com/2018-Seattle-HITSummit>

[6] https://arstechnica.com/information-technology/2017/12/hackers-steal-security-firms-secret-data-in-brazen-domain-hijack/
[7] https://www.forbes.com/sites/thomasbrewster/2017/12/12/robot-hack-exploits-encryption-weaknesses-in-major-websites-facebook-patches/#3639cd915cc4

December 19, 2017

--2018 NH-ISAC Fall Summit – San Antonio, TX (11/26-29)
<https://www.destinationhotels.com/la-cantera-resort-and-spa>

Sundries –

--How a Dorm Room Minecraft Scam Brought Down the Internet
<https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/>
--"There will be a [Senate] vote" to reinstate net neutrality, Schumer says
<https://arstechnica.com/tech-policy/2017/12/there-will-be-a-senate-vote-to-reinstate-net-neutrality-schumer-says/>
--Standing in Data-Breach Actions: Injury in Fact? <https://www.lawfareblog.com/standing-data-breach-actions-injury-fact>
--Five things CIOs can do as IoT adoption turns into a nightmare
<https://www.helpnetsecurity.com/2017/12/18/cio-tips-iot/>
--Unauthorized Server Access Creates Data Security Concern for 47K <
https://healthitsecurity.com/news/unauthorized-server-access-creates-data-security-concern-for-47k>
--$2.3M OCR Settlement Reached for 21st Century Oncology Data Breach
<https://healthitsecurity.com/news/2.3m-ocr-settlement-reached-for-21st-century-oncology-data-breach>
--MA Reaches Settlement Following Medicaid Data Breach
<https://healthitsecurity.com/news/ma-reaches-settlement-following-medicaid-data-breach>
--Security Planner: How to Protect Yourself < https://www.lawfareblog.com/security-planner-how-protect-yourself>
--New letter: Top Uber officials engaged in illegal wiretapping, shady spycraft
<https://arstechnica.com/tech-policy/2017/12/new-letter-top-uber-officials-engaged-in-illegal-wiretapping-shady-spycraft/>

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