Hacking Healthcare

Welcome to the first edition of *Hacking Healthcare*, NH-ISAC's new weekly newsletter designed to guide you through the week in healthcare cybersecurity and policy. Every Wednesday, *Hacking Healthcare,* will bring you analysis on the latest news stories, policy developments, reports, and public remarks that impact the cybersecurity practitioner across all the different healthcare industries. We have our views on what matters, but we also want to reflect your interests – so get in touch and let the *Hacking Healthcare* team know what you want to see. Here we go…

This is the public version of the *Hacking Healthcare* newsletter. For additional in-depth analysis and opinion, become a member of the NH-ISAC.

Petya (aka GoldenEye, NotPetya)

For the second time in as many months, a ransomware attack is snaking its way around the globe. It appears that the attack started in Ukraine and has much of its impact in Europe. But there are reports that U.S. entities have also been infected, including at least 1 U.S. hospital.

Some researchers have reported that the malware resembles Petya or GoldenEye, or maybe an off-spring of one of these variants. We'll call it Petya for now since that is the standard that NH-ISAC has adopted.

Regardless of its lineage, the malware used in the current attack does seem to be relying on the ETERNALBLUE exploit to gain initial network access. Installing all of the latest Microsoft updates for the related vulnerabilitiesseems like a good first step in response. The **NH-ISAC is working hard to gather and share further information** on this attack and will keep its members informed through their incident-specific blog and AMBER list-serve.

Our first rule of thumb at *Hacking Healthcare* is that the initial policy assumptions about security incidents will be incomplete at best. At worst, those assumptions will be flat out wrong. So we'll wait until next week to opine on what the attack means for the healthcare sector now and in the future.

For now, we know that you all are head-down and working on the problem. Here are some additional resources as you respond and recover to a more secure state:

--NH-ISAC Petya Blog – NH-ISAC will post update information on their main page as further details are obtained and analytics are produced.

--NH-ISAC bulletin – This is the initial technical release from NH-ISAC on the current ransomware campaign.

--USG Ransomware Guidance – Last year, the federal government put out a short technical and policy document advising organizations on how to address ransomware threats. Not specific to this attack or ransomware variant, but still a good baseline.

--USG Ransomware Guidance for CEOs – a one-pager of the longer guidance, with the non-technical executive in mind. Not specific to this attack.

--HHS Bulletin (May 2017) – Basic info on ransomware and HHS response efforts to WannaCry.

--OCR Quick-Response Checklist – OCR's post-wanna cry guide for healthcare incident response.

--HIPAA Ransomware Fact Sheet – if you are a covered entity or business associate under HIPAA, consider your reporting requirements. As this document states: "**Unless the covered entity or business associate can demonstrate** that there is a "…low probability that the PHI has been compromised," based on the factors set forth in the Breach Notification Rule, **a breach of PHI is presumed to have occurred**."

--FDA Postmarket Guidance – FDA guidelines that inform medical device manufacturers of their obligations and abilities to patch vulnerable devices. Any devices running on top of older windows systems (XP anyone?) may be vulnerable to this attack.

Healthcare Task Force Report

We were planning on spending the week discussing this month's big policy news in the world of healthcare cybersecurity. After a year of work, the HHS Healthcare Industry Cybersecurity Task Force released its report on June 2.

The report should be viewed as a landmark release, which will inform public policy developments over the coming years. Reports such as this represent a "consensus" view of the sector's view, as well as a commitment to action on behalf of the government.

The Administration will look to show progress on implementing the recommendations. Congress, the Government Accountability Office, and agency Inspector Generals will all provide oversight and request regular updates on implementing activities.

The Task Force establishes the immediacy and scope of the sector's cyber-risk by stating that "…health care cybersecurity is a **key public health concern** that needs immediate and aggressive attention." This statement represents an evolution in thinking that is reflected in many of the task force recommendations – patient privacy is no longer the sector's only concern.

The Task Force provides **102 action items, organized into 27 recommendations and 6 imperatives**, that it believes will reduce cyber-risk within the healthcare sector. The action items have a bit for everyone across the sector.

Let's look across the different imperatives **under the light of the ongoing ransomware attack** to help give us a sense of the impact that these policy recommendations might have on security operators within the healthcare sector. We'll also note **what types of healthcare organizations might be interested** in each Imperative. (member's version only)

Healthcare news –

- New Cyberattack Spreads in Europe, Russia and U.S. (nyt)
- Schroedinger's Pet(ya) (Kaspersky)
- A new ransomware outbreak similar to WCry is shutting down computers worldwide (Ars Technica)
- Why an HHS cyber center could confuse federal efforts (FCW)
- HHS faces flak over new cyber center (CS)
- FDA Implementing Risk-Based Medical Device Regulation (HealthITSecurity)
- Anthem agrees to pay record $115M to settle data breach suit (cnet)
- Airway Oxygen Ransomware Attack May Affect PHI of 500K (HealthITSecurity)
- Google begins removing personal medical records from search results (the verge)

- FTC Data Security Enforcement Standard Center in LabMD Case (HealthITSecurity)

- Healthcare Company CoPilot Settles Data Breach with $130k Payment (healthcare informatics)

Some older takes on the healthcare task force and the subsequent hearing:

- Health Care Industry Cybersecurity Task Force Report Recommends Urgent Improvement (proviti)

- Health Care Industry Cybersecurity Task Force Report: Analysis and Recommendations (himss)

- Healthcare Cybersecurity, and HHS Response to WannaCry Ransomware, Focus of House Subcommittee Hearing (healthcare informatics)

- Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity (House E&C)

- Patient Safety, PHI Security Key in HHS Cybersecurity Role (HealthITSecurity)

- Industry Applauds HHS Cybersecurity Task Force Report (HealthITSecurity)

The Week Ahead –

It's 'Cyber Week' in Israel, but the U.S. cyber community seems to have a light week. I guess we'll all just sit around drinking code red and watching fireworks.

Events:

Healthcare Informatics - Nashville HIT Summit (June 27-28)

SharedAssessments Summit (June 28-29)

NIST 2017 Community College Cyber Summit (June 28-30)

Congressional Hearings:

Senate Intelligence Committee Hearing on RussianInterference in European Elections (10:00 AM,Wednesday, June 28)

Relevant Federal Nominations:

--Thomas G. Bowman, of Florida, to be Deputy Secretary of Veterans Affairs
--James Byrne, of Virginia, to be General Counsel, Department of Veterans Affairs

Reports –

- NIST SP 800-63 - Digital Identity Guidelines (NIST)
- FBI 2016 Internet Crime Report (FBI)
- The Hacker-Powered Security Report 2017 (hackerone)
- Principles for fair and accurate security ratings (us chamber)
- A Proposal to Enhance the Financial Sector's Participation in Classified Cyber Threat Information Sharing (INSA)
- U.S. HEALTHCARE PROVIDERS' EMAIL SECURITY IN CRITICAL CONDITION (GCA)

Sundries –

- A Cyberattack 'the World Isn't Ready For' (nyt)
- Obama's secret struggle to punish Russia for Putin's election assault (WP)
- China rolls out national cyber threat response plan (reuters)
- HOW AN ENTIRE NATION BECAME RUSSIA'S TEST LAB FOR CYBERWAR (wired)
- GOOGLE'S BIG EU FINE ISN'T JUST ABOUT THE MONEY (wired)
- UK energy industry cyber-attack fears are 'off the scale' (the guardian)
- Investigation shows DHS did not hack Georgia computers (the hill)
- Remarks by Homeland Security Advisor Tom Bossert (WH)
- Encryption debate is a top focus at five eyes meeting (CS)
- EU agrees to joint diplomatic response to cyber attacks (EU)

(In)Secure Takes – the best of social media

NH-ISAC @NHISAC · 6h

Go to NH-ISAC website for updates on the Petya ransomware. nhisac.org #NHISAC #PETYA

> **NH-ISAC is currently tracking the Petya Ransomware attack quickly spreading across Europe. Information regarding IOC's, TTP's , etc are being shared on the AMBER listserver. As appropriate, we will scrub to Green/White as soon as possible for wider distribution.**
>
> **Visit our Petya Ransomware Blog Page for up-to-date information regarding this global threat.**
>
> **Our Wannacry Updates Page will also have updates as they are made available.**

1

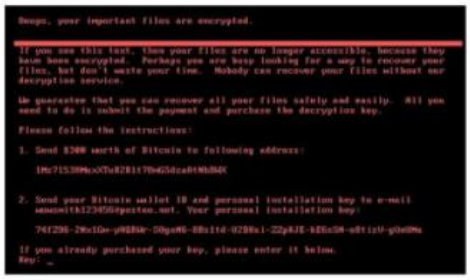
Pinned Tweet

Mikko Hypponen @mikko · 10h

There's over 30 years between these two trojans.

AIDS Information ransom trojan, from 1986

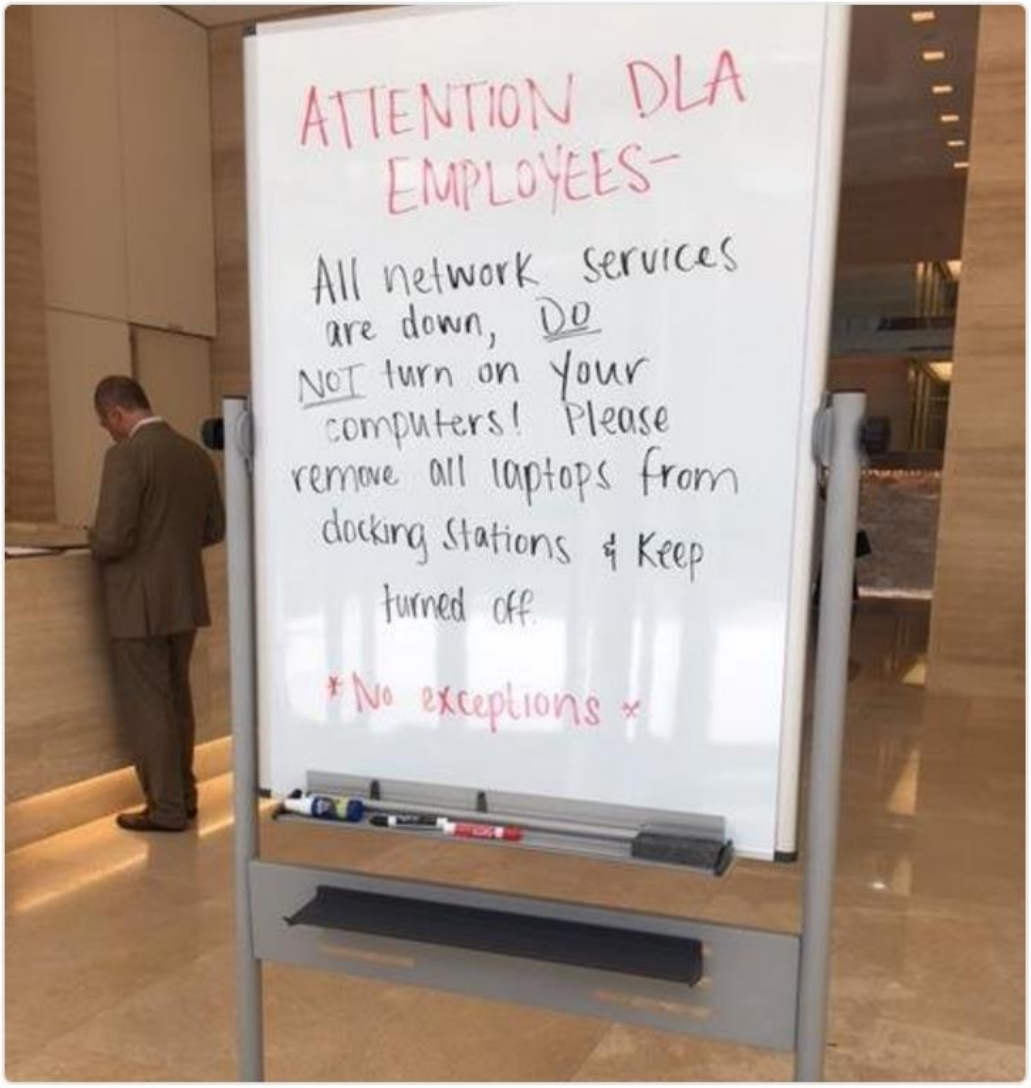
Petya ransom trojan, from 2017

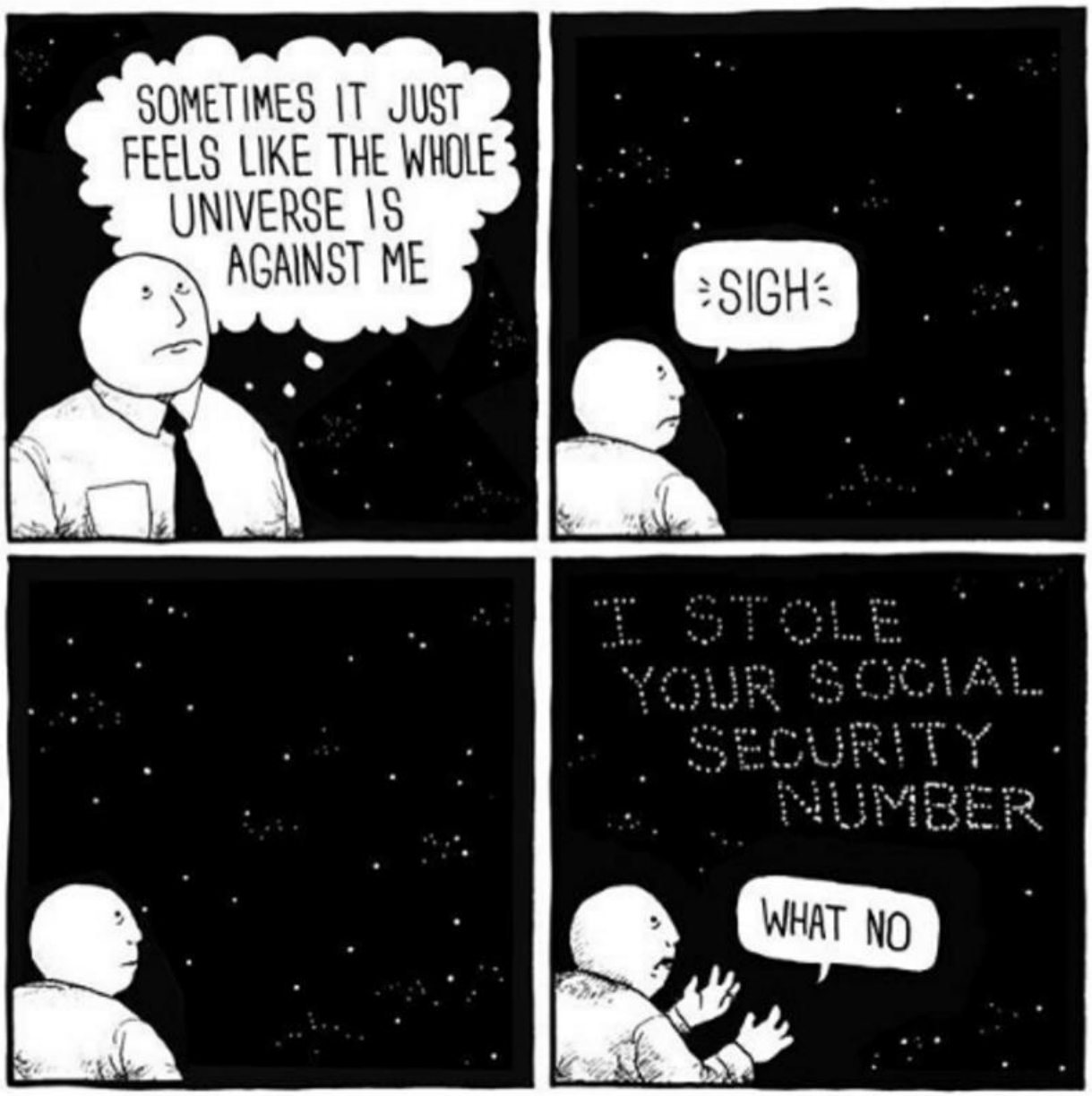


11 230 238

Eric Geller @ericgeller · 8h

A tipster sends along this photo taken outside DLA Piper's D.C. office around 10am. #Petya





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