August 30, 2017

TLP White

Policy Analysis – Who does what

After looking at the roles and responsibilities of different Federal agencies during incident response, we thought it might help to step back and provide an overview of the agencies themselves and the cyber capabilities and authorities they each possess.

You can break down the government's cyber mission into defensive and offensive authorities and responsibilities. Most of the funding and attention is directed towards defensive capabilities, and as such, that's what we'll focus on here.

The Department of Homeland Security serves as the government's lead agency for cybersecurity. DHS' cyber mission is primarily defensive in nature and based out of the National Protection and Programs Directorate (NPPD), which supports U.S. government agencies and critical infrastructure organizations. This support is extended through network defense capabilities, information sharing efforts, and incident response assistance.

DHS mostly channels its external cyber mission through the National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC, which NH-ISAC has a partnership with, serves as the hub for much of the agency's external cyber mission. It serves as a physical watch center and space for personnel from critical infrastructure companies and ISACs to congregate and collaborate during an incident, as well as providing the technical infrastructure to connect the federal government with its external partners day-to-day (i.e., through the Automated Indicator Sharing program).

DHS also invests in applied R&D through the Science & Technology Directorate, performs intelligence analysis and assessments through the Office of Intelligence and Analysis, investigates cyber-crime (mainly financial crimes) through the U.S. Secret Service, and supports incident response planning and operations through FEMA. The U.S. Coast Guard serves as the sector specific agency for ports.

The FBI is the primary agency responsible for investigating Federal computer crimes. The FBI conducts this work out of its criminal division and the field offices that are located throughout the country. Many field offices have cyber task forces with Special Agents and analysts specifically dedicated to cyber-crime. The FBI also has responsibility for investigating threats to national security, which includes cyber-threats from foreign governments and non-government actors (i.e., terrorists, trans-national organized crime). The cybersecurity focus of the national security division has increased in recent years, with some notable cases being developed with their support. FBI also runs the National Cyber-Forensics & Training

Alliance in Pittsburgh, which utilizes public-private partnership to develop threat-specific analysis and mitigation.

The Department of Justice directs the FBI's investigatory resources and decides which FBI cases the U.S. government will prosecute. DOJ has civil, criminal, and national security divisions that each have lawyers who bring cyber-related cases to court. DOJ also provides policy counsel to the White House and executive branch agencies. This is done through the Office of Legal Counsel which advises on the legality of policy developed and implemented by agencies.

Next week we'll look at the distinct roles that HHS plays in cybersecurity, as well as the other agencies around the government, including those which conduct offensive cyber operations.

Hot Links –

--DE Data Breach Notification Law Includes Medical Information (Health IT Security) – Delaware's governor recently signed a law modifying the requirements for data breach notifications. Included in the definition of personal information, subject to protection under the law, are a person's medical history and health insurance policy numbers. Protection and notification requirements under this new law are in line with current best practice and consistent with requirements under HIPAA.

--HIMSS releases its 2017 Cybersecurity Survey – some of the findings here are significant: 62 percent of all healthcare organizations utilize the NIST Framework, but those who employ a CISO (or equivalent senior leader) utilize the NIST Framework at a rate of 95 percent. 71 percent of respondents indicate that cybersecurity commands its own budget line; and more than 50 percent of organizations say that they have at least 1 cybersecurity professional for every 500 staff members, a ratio that has been identified as optimal for high risk organizations. Read the 5 key takeaways from HIMSS.

--AHA Urges Reduced Data Sharing Barriers in HIPAA Regulations (Health IT Security)
--FBI Arrests Suspect in OPM Hack (The Hacker News) (the Register)
--Members of Trump's cybersecurity council resign in protest (the Verge)
--Hospitals must band together to beat hackers (Healthcare IT News)
--Google mistake is the root cause of Internet Outage in Japan (Security Affairs)

The Week Ahead –

Administration activity –
--HHS Secretary Price declares public health emergency in response to Hurricane Harvey
--HHS continues support in Texas and Louisiana in response to Hurricane Harvey

--Cybersecurity was NOT on the agenda when Secretary Price visited Japan and Vietnam last week.

Congressional Activity – The House and Senate return from recess next week. A (now-postponed) hearing to look at the future of FEMA would have been interesting. We'll update you when that gets re-scheduled.

Conferences and Webinars –
--HIPAA and Personal Devices (webinar) (9/5)

August 30, 2017

--Basic Best Practices in Cybersecurity – Minnesota (NH-ISAC) (9/6)
--Medical Device Workshop at Medtronic – Mounds View, MN (NH-ISAC) (9/7)
--HIMSS Healthcare Security Forum (9/11-13)
--Billington CyberSecurity Summit (9/13)
--Basic Best Practices in Cybersecurity - Alabama (NH-ISAC) (9/15)
--Biotec/Pharma Security Workshop at MSD, Prague (NH-ISAC) (11/7)
--NH-ISAC Fall Summit – Cyber Rodeo (11/28-30)

Reports –
--2017 U.S. State and Federal Government Cybersecurity report (Security Scorecard)
--2017 U.S. State of Cybercrime (CSO)
--2017 HIMSS Cybersecurity Survey
--2017 State of Enterprise Digital Defense Report (RiskIQ)
--Survey: One Quarter of Healthcare IT Security Pros Cite Little Confidence in Ability to Manage Digital Threats (IDG Connect)

Speeches –
--Remarks by Sen. John McCain at ASU Cybersecurity Conference

Sundries –
August Vacation reading:
--The Hotel Room Hacker (Wired)

Breaches:
--NHS Lanarkshire recovers from ransomware attack (Computer Weekly)
--St. Mark's Ransomware Attack Could Affect 33K Patients (Health IT Security)
--OIG Notes NC Potential Medicaid Data Security Vulnerabilities (Health IT Security)
--New Mexico Medicaid Data Security Requires Improvements (Health IT Security)

Op-eds:
--Show the proof, or cut it out with the Kaspersky Lab Russia rumors (CSO)

New Book:
--Review: Securing the Internet of Things (HelpNet)

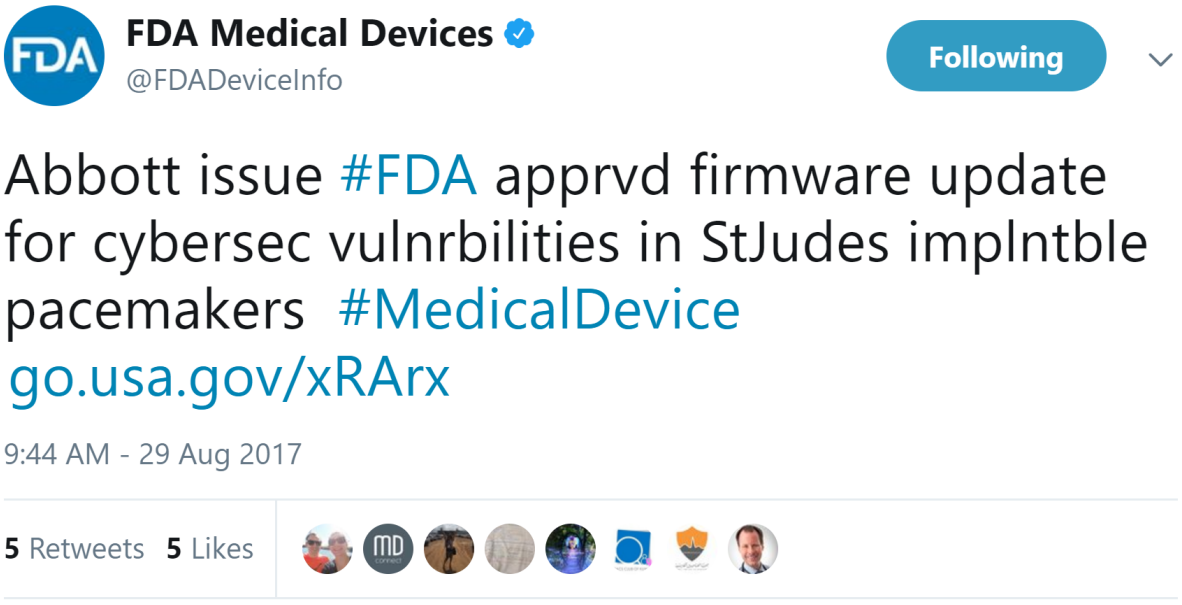
Tech:
--Android Oreo: What's new on the security front (HelpNet)
--Malware rains on Google's Android Oreo parade (naked security)
--Google Introduces App Engine Firewall (SecurityWeek)

Threats:
--Massive Android DDoS Botnet Derailed (Dark Reading)
--Defray Ransomware Used in Selective Attacks Against Multiple Sectors (Security Week)
--Proofpoint analysis of DEFRAY
--Floodwaters, phishing scams rise as Hurricane Harvey hammers South Texas (SC)

August 30, 2017

Network defense and vulnerabilities:
--Leak of >1,700 valid passwords could make the IoT mess much worse (Ars)
--Thousands of IoT Devices Impacted by Published Credentials List (Security Week)
--Maintaining PHI Security with Specialized mHealth App Usage (Health IT Security)
--How HIPAA Regulations Can Ease Information Blocking (Health IT Security)
--Cybersecurity: An Asymmetrical Game of War (Dark Reading)
--Global DMARC adoption still slow, it's open season for phishers (HelpNet)
--Don't like Mondays? Neither do attackers (CSO)
--Disaster recovery vs. security recovery plans: Why you need separate strategies (CSO)
--Living in an Assume Breach world (HelpNet)
--Cracking Active Directory Passwords or "How to Cook AD Crack" (SANS)
--Cybersecurity world faces 'chronic shortage' of qualified staff (the Register)

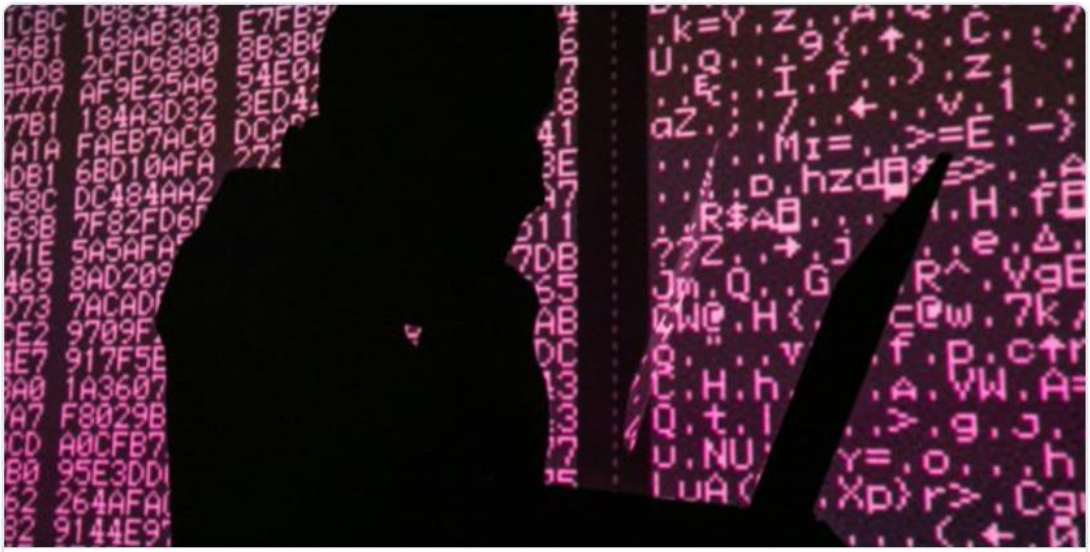
(In)Secure Takes – Twitter's best from the week



August 30, 2017

Malware Unicorn @malwareunicorn · Aug 28

Spreading the malware research love in Teen Vogue



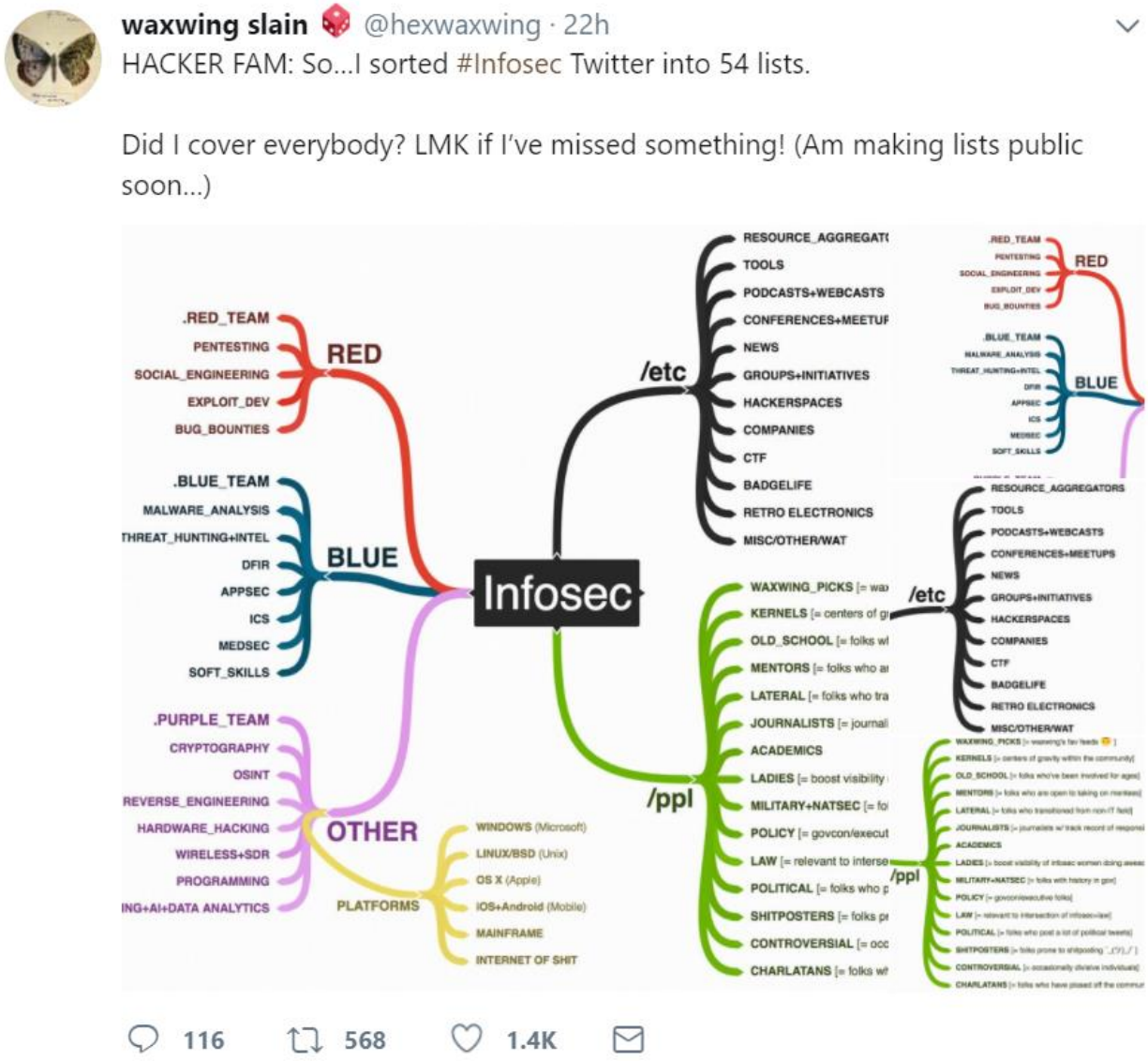
4 Reasons Being a Hacker Is the Best Job You Haven't Considered

It's not all dark rooms and hoodies.

teenvogue.com

82 1.1K 2.0K

August 30, 2017



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