NH-ISAC Daily Security Intelligence Report – July 12, 2018

This information is marked TLP GREEN: Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community.

BREACH REPORT

Deceased Patient Data Being Sold on Dark Web

It is no shocker medical records are a prime target for cybercriminals. But less intuitive is the market for medical records of the deceased on the dark web. We took a closer look at the reason behind this strange trend. Here is what we found.

First off, despite best efforts, stolen medical records – of the living — for sale on black markets remain a huge problem. In fact, Cynerio is still seeing continued growth in the number of incidents of patient medical record breaches from hacking and unauthorized access to healthcare systems...


CRIME and INCIDENT REPORT

Ransomware Attack on Cass Regional Shuts Down EHR

Missouri-based Cass Regional Medical Center is currently recovering from a ransomware attack that struck its communication system and shut its staff out of its Meditech electronic health record system on Monday.
Hackers hit the health system around 11 a.m. Monday, and officials opted to turn off the EHR to prevent unauthorized access. Officials said there appears to be no evidence that patient data was breached.

Currently, recovery efforts are about 50 percent complete, officials said in the most recent update. Cass Regional did not immediately respond to a request for comment...


(additional companion article below)

**Hospital Diverts Ambulances Due to Ransomware Attack**

A ransomware attack forced a Missouri county medical center to divert ambulances carrying trauma and stroke patients to other facilities as the critical access hospital continues to recover.

The ransomware attack Monday impacted the enterprise IT infrastructure, including the electronic health records system, at Harrisonville, Mo.-based Cass Regional Medical Center, which includes 35 inpatient beds and several outpatient clinics, a spokeswoman tells Information Security Media Group...

https://www.healthcareinfosecurity.com/hospital-diverts-ambulances-due-to-ransomware-attack-a-11193

[Follow up] Hacker Steals Military Docs Because Someone Didn’t Change a Default FTP Password

A hacker is selling sensitive military documents on online hacking forums, a security firm has discovered.

Some of the sensitive documents put up for sale include maintenance course books for servicing MQ-9 Reaper drones, various training manuals describing comment deployment tactics for improvised explosive device (IED), an M1 ABRAMS tank operation manual, a crewman training and survival manual, and a document detailing tank platoon tactics...


ICS Security: 'The Enemy Is in the Wire'
Threats to industrial control systems are real and frightening. The government is taking steps to keep us safer in the future, but there are near-term steps you can take right now.

"The enemy is in the wire." During the Vietnam War, this call would ring out to alert everyone that the enemy was in the perimeter of fortifications. In our cyber world, we've known this for years; however, the call rang frighteningly true in May of this year...


Ukraine Security Service Stops VPNFilter Attack at Chlorine Station

The facility's process control system and emergency-detection system were infected, Interfax Ukraine reports. Ukraine's SBU Security Service reportedly detected and shut down a cyberattack that used VPNFilter malware on network equipment in a chlorine station that supplies water treatment and sewage plants.

Interfax-Ukraine reported that the LLC Aulska station in Auly was hit with a VPNFilter infection intended to disrupt operations at the chlorine station...


China-Based TEMP.Periscope APT Targets Cambodia’s Elections

Security researchers at FireEye have uncovered a large-scale Chinese phishing and hacking campaign aimed at Cambodia’s elections. The hackers distributed a remote access trojan (RAT) and data exfiltration operation targeting the poll.

The experts from FireEye attributed the attacks to an APT group tracked as TEMP.Periscope that targeted in past operations American engineering and maritime operations...

https://securityaffairs.co/wordpress/74378/intelligence/temp-periscope-cambodia.html

Engineer Found Guilty of Stealing Navy Secrets via Dropbox Account

A jury trial found a former engineer at a Navy contractor guilty of stealing trade secrets regarding Navy projects by uploading the files to his personal Dropbox account.

The man, Jared Dylan Sparks, 35, of Ardmore, Oklahoma, worked as an electrical engineer for LBI, Inc., a company authorized to build unmanned underwater vehicles (drones) for the US
Navy’s Office of Naval Research, and weather data-gathering buoys for the National Oceanic and Atmospheric Administration (NOAA). Sparks worked for LBI from January 2010 to December 2011, when he left for a similar position at Charles Rivers Analytics (CRA), another Navy contractor...


**NEWS REPORT**

**Insider Health Data Security Threats Bigger Concern than External**

Many healthcare professionals are more concerned about insider threats to health data security than external breaches, according to a survey by HIMSS on behalf of SailPoint. There is an acute level of concern about the threats posed by insiders. On a scale of 1 to 10, the mean score for the level of concern of respondents was 8.2.

Among respondents who implemented or managed cybersecurity solutions for their organization, 43 percent said that insider threats were of greater concern than external threats. Another 35 percent were equally concerned about insider threats and external threats to data security, according to the survey of 101 healthcare professionals, a copy of which was provided to HealthITSecurity.com...


**Outdated DoD IT Jeopardizes National Security: Report**

*Failure to Modernize Legacy DoD Systems is Putting U.S. National Security in Jeopardy, Report Claims*

In a new study titled 'Innovation Imperative: The Drive to Modernize DoD', Meritalk queried 150 federal IT managers working in Department of Defense (DoD) organizations. The stated objective was "to understand the state of their IT infrastructure and applications." This was to include levels of satisfaction, an indication of where missions are being met or missed, and what should be done next.

In fact, this report is solely about DoD IT managers' attitude towards cloud migration -- which is perhaps unsurprising since the survey was underwritten by AWS and Red Hat...
Google Enables "Site Isolation" Feature for 99% of Chrome Desktop Users

Google has secretly enabled a security feature called Site Isolation for 99% of its desktop users on Windows, Mac, Linux, and Chrome OS. This happened in Chrome 67, released at the end of May.

Site Isolation isn't a new feature per-se, being first added in Chrome 63, in December 2017. Back then, it was only available if users changed a Chrome flag and manually enabled it in each of their browsers.

The feature is an architectural shift in Chrome's modus operandi because when Site Isolation is enabled, Chrome runs a different browser process for each Internet domain...

VULNERABILITY REPORT

Multiple Bugs Found in QNAP Q'Center Web Console

QNAP said in a security advisory that it has fixed the issues in Q'Center Virtual Appliance, and urged customers to update to the latest version.

Researchers found an array of high severity vulnerabilities in network storage vendor QNAP’s web console, which could enable an authenticated attacker to gain privileges and execute arbitrary commands on the system...

New Spectre 1.1 and Spectre 1.2 CPU Flaws Disclosed

Two security researchers have revealed details about two new Spectre-class vulnerabilities, which they've named Spectre 1.1 and Spectre 1.2.

Just like all the previous Meltdown and Spectre CPU bugs variations, these two take advantage of the process of speculative execution—a feature found in all modern CPUs that has the role of improving performance by computing operations in advance and later discarding unneeded data...
Hackers Can Chain Multiple Flaws to Attack WAGO HMI Devices

Germany-based industrial automation company WAGO has patched several vulnerabilities in its e!DISPLAY 7300T Web Panel human-machine interface (HMI) products that can be chained to take control of affected devices.

The security holes, discovered by researchers at security consultancy SEC Consult and rated “high severity,” include multiple reflected and one stored cross-site scripting (XSS) vulnerabilities (CVE-2018-12981), unrestricted file upload and file path manipulation issues (CVE-2018-12980), and an incorrect default permissions flaw (CVE-2018-12979)...

https://www.securityweek.com/hackers-can-chain-multiple-flaws-attack-wago-hmi-devices