NH-ISAC Daily Security Intelligence Report – July 17, 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

LabCorp’s Network Security Breach May Have Exposed PHI of Millions

After recently dodging a legal bullet over an alleged HIPAA violation, LabCorp is now facing a network security breach that forced the North Carolina-based laboratory diagnostics firm to shut down its IT network, possibly placing PHI of millions of people at risk.

In a July 16 statement, LabCorp said it detected suspicious activity during the weekend of July 14-15 on its IT network. It took systems offline, which affected test processing and customer access to test results...


Thousands of Patient Records Held for Ransom in Ontario Home Care Data Breach, Attackers Claim

The detailed medical histories and contact information of possibly tens of thousands of home-care patients in Ontario are allegedly being held for ransom by thieves who recently raided the computer systems of a health-care provider.
CarePartners, which provides home medical care services on behalf of the Ontario government, announced last month that it had been breached. It said only that personal health and financial information of patients had been "inappropriately accessed," and did not elaborate further…


Thousands of Mega Logins Dumped Online, Exposing User Files

Thousands of credentials for accounts associated with New Zealand-based file storage service Mega have been published online, ZDNet has learned.

The text file contains over 15,500 usernames, passwords, and files names, indicating that each account had been improperly accessed and file names scraped.

Patrick Wardle, chief research officer and co-founder at Digita Security, found the text file in June after it had been uploaded to malware analysis site VirusTotal some months earlier by a user purportedly in Vietnam...

https://www.zdnet.com/article/thousands-of-mega-logins-dumped-online-exposing-user-files/

Telefonica Breach Leaves Data on Millions Exposed

Hackers exploited a flaw at Spanish operator Telefonica early Monday and likely exposed all the personal data of millions of the company's customers.

Identity and payment information – including land line and mobile numbers, national ID numbers, addresses, banks, names and records of calls and other data – was exposed, although there is no evidence that any of the data was used in fraudulent activity, according to a report in Telecompaper, which cited El Espanol..


CRIME and INCIDENT REPORT

North Korean Hackers Launch New ActiveX Attacks

A new series of reconnaissance attacks targeting ActiveX objects has been associated with the North Korean-linked Andariel group, a known branch of the notorious Lazarus Group.
In May, the group was observed exploiting an ActiveX zero-day vulnerability in a series of attacks on South Korean targets, mainly for reconnaissance purposes. A script injected into compromised websites would identify the visitors’ operating system and browser and check for ActiveX and running plugins from a specific list of ActiveX components if Internet Explorer was detected...


Samsung Service Centers in Italy Targeted in Malware Campaign

Security researchers have discovered ongoing malware campaigns targeting Samsung service centers in Italy, campaigns that appear to be the counterparts of attacks that have previously targeted similar electronics service centers in Russia this year.

These malware campaigns are nothing out of the extraordinary, and the only thing that remains a mystery is their purpose and end goal...


Crooks Deployed Malicious Eslint Packages That Steal Software Registry Login Tokens

Crooks compromised an ESLint maintainer’s account last week and uploaded malicious packages that attempted to steal login tokens from the npm software registry. npm is the package manager for JavaScript and the world’s largest software registry.

ESLint is open source “pluggable and configurable linter tool” for identifying and reporting on patterns in JavaScript, it was created by Nicholas Zakas.

https://securityaffairs.co/wordpress/74497/hacking/malicious-eslint-packages.html

‘LuminosityLink RAT’ Author Pleads Guilty

A 21-year-old Kentucky man has pleaded guilty to authoring and distributing a popular hacking tool called “LuminosityLink,” a malware strain that security experts say was used by thousands of customers to gain unauthorized access to tens of thousands of computers across 78 countries worldwide..

Federal prosecutors say Colton Ray Grubbs of Stanford, Ky. conspired with others to market and distribute the LuminosityLink RAT, a $40 Remote Access Tool that made it simple for buyers to
hack into computers to surreptitiously view documents, photographs and other files on victim PCs. The RAT also let users view what victims were typing on their keyboards, disable security software, and secretly activate the webcam on the target’s computer...


NEWS REPORT

Patient Safety Concerns Driving Medical Device Security Investment

Medical device security and patient data privacy are two of the areas in which the healthcare industry is investing to curb the costs of adverse patient safety events, according to a study by Frost & Sullivan.

Other areas of investments include medication safety, antibiotic resistance, patient diagnostics safety, sepsis prevention, and emergency department (ED) admissions...


SCADA/ICS Dangers & Cybersecurity Strategies

_Nearly 60% of surveyed organizations using SCADA or ICS reported they experienced a breach in those systems in the last year. Here are four tips for making these systems safer._

A large number of government agencies and private organizations have SCADA (supervisory control and data acquisition) or industrial control systems (ICS). The benefits of these technologies come with significant security challenges. In a recent survey by Forrester commissioned by Fortinet, nearly six in 10 surveyed organizations using SCADA or ICS indicate that they experienced a breach in those systems in the past year...


VULNERABILITY REPORT

Microsoft Releases Windows 10 Cumulative Update KB4345421

Windows 10 cumulative update KB4345421 bumps the OS build to 17134.166, and it is exclusively focused on non-security fixes - security updates are typically rolled out on Patch
Tuesday, unless they are included in an out-of-band release that Microsoft uses to address a major security vulnerability in its products.

There are four different changes in this update, and one of them is a fix for a BSOD caused on some systems after installing the July 2018 Patch Tuesday cumulative update. Microsoft says that some devices running network monitoring workloads encountered a 0xD1 Stop error, and installing this new update should resolve this behavior...


Researchers Show How to Manipulate Road Navigation Systems With Low-Cost Devices

Researchers have developed a tool that poses as GPS satellites to deceive nearby GPS receivers. The kit could be used to deceive receivers used by navigation systems and suggest drivers the wrong direction.

“we explore the feasibility of a stealthy manipulation attack against road navigation systems. The goal is to trigger the fake turn-by-turn navigation to guide the victim to a wrong destination without being noticed.” reads the research paper published by the experts. “Our key idea is to slightly shift the GPS location so that the fake navigation route matches the shape of the actual roads and trigger physically possible instructions.”..

https://securityaffairs.co/wordpress/74509/hacking/navigation-systems-hack.html

EJB

Operations

National Health ISAC (NH-ISAC)

Global Situational Awareness Center

226 North Nova Road, Suite 391

Ormond Beach, Florida 32174

www.nhisac.org
twitter.com/NHISAC