The IECA Cyber Bulletin

Volume 2 • Issue 4 • April 2017

WikiLeaks Dishes Massive CIA Leak

Web publisher WikiLeaks has disclosed a massive breach of material from the US Central Intelligence Agency (CIA). The trove of information, which is being called "Vault 7" was apparently leaked by a CIA insider. It contains highly classified materials including documents detailing methods of hacking smart phones, TVs, Internet routers, and computers. It also apparently includes several million lines of code for viruses, Trojan horses, zero day exploits, and other malware. As usual, WikiLeaks plans to publish the material gradually. So more is expected to break in the coming months.

The big news from Vault 7 so far is the fact that the CIA is operating its own hacking operations on the level of the US National Security Agency (NSA). Also revealed were tools that allowed the CIA to mimic hacking "fingerprint" characteristics of other nations. It seems to have occurred to nobody in the press to ask how this affects recent allegations of Russian "fingerprints" on the DNC hack.

WikiLeaks editor-in-chief Julian Assange called the breach a "historic act of devastating incompetence", noting that the cache of cyber weapons was being passed around "out of control" by contract hackers. The FBI has reportedly tasked a special mole-hunting team to isolate the leak. The probe is expected to focus on outside CIA contractors.

Assange has been holed up in the Ecuadorian embassy since 2012. The world doesn't seem to have quite made up its mind whether the organization he founded is a hero or a villain. Nonetheless, it bears remembering that the "crime" in this case was committed by whoever leaked the material. It is unlikely that anybody would question the rights of the press had the leakers given the material to The Washington Post, instead of WikiLeaks.

DOJ Dismisses Child Porn Case

An attorney for the US Department of Justice said that the government would file a motion to dismiss the charges in their case against Jay Michaud, one of 135 people under prosecution in connection with the Playpen case. The FBI used a hacking exploit it termed a "network investigative technique" (NIT) to isolate the identities of Playpen users on The Onion Router (TOR) network. US District Judge Robert Bryan ordered the government to disclose their NIT to support how Michaud's identity was determined. The government responded by classifying the source code of the NIT exploit. In taking this action, the government is choosing to protect their investigative methods, over a successful prosecution of a single case. The impact this will have on any of the other cases is not yet clear. Dismissing the charges without prejudice will allow the case to be tried again should the situation change.

Radio Station Air Signals Hacked

More than a dozen low power frequency modulation (LPFM) radio stations were apparently hacked, and caused to play an anti-Trump song, shortly after the inauguration. Attackers took advantage of weaknesses in the transmitters, which all used Barix Exstreamer products. Barix warned its customers in 2016 that the remote login interface of these devices is very vulnerable to attack if exposed to the Internet. Yet many operators ignored the guidance, and left themselves vulnerable to attack.

Arby's Acknowledges Data Breach

Arby's Restaurant Group, Inc. issued a statement in January acknowledging that it had been the victim of a malware attack targeting customer credit and debit card

(continued on the reverse)

(continued from page 1)
information. The breach affected only corporate-owned Arby's stores, not franchise partners. However, the breach may have affected upwards of 1,000 stores. The malware targeted the point of sale system, and Arby's says their team has isolated and eradicated the malware. Arby's said they had delayed notifying the public at the request of the FBI.

Geek Squad Spying for the FBI

Court filings recently unsealed from the case of US vs. Rettenmaier seem to make it clear that Best Buy's Geek Squad has been acting on the FBI's behalf to search through customers' computers for evidence of possible crimes. When first asserted by Rettenmaier attorney James Riddet, the situation was denied by both the Bureau and Best Buy. Assistant US Attorney M. Anthony Brown initially called the claim "wild speculation", and Best Buy vice president Jeff Haydock claimed that the discovery of evidence in the case was inadvertent. He said when they discovered something, Best Buy, "had an obligation to contact law enforcement."

New documents have been released which seem to put the lie to these claims. Multiple FBI documents show that Geek Squad employees routinely snooped for the Agency, and were "under the direction and control of the FBI." Attorneys in the case have asserted that the FBI is expressly using the arrangement to rifle through customer systems without any probable cause. They also argue that in using the company to conduct its fishing expeditions, and by rewarding Geek Squad employees with a $500 bounty on evidence of possible criminality, the Agency has in effect made Geek Squad an unofficial wing of the FBI. While we are still awaiting key rulings in the case, this situation should serve as a wake up call to anybody who uses outside computer maintenance or repair. If you have sensitive data on your computer, you really need to think twice before granting access to outside personnel. You don't necessarily know who's agenda they're pursuing.

Elon Musk Touts Brain Interface

Billionaire and serial entrepreneur Elon Musk, founder of SpaceX, Solar City, and PayPal, among others, tweeted in January that he is working on something he calls "neural lace". This lace would offer the means of interfacing computers directly with human thoughts and feelings. In a later tweet, Musk said that this interface is the thing that really matters for humanity to achieve symbiosis with machines. In March, Musk announced the formation of a new company, called Neuralink, to focus on the technology. He expects that first steps will include implanted electrodes designed to treat epilepsy and depression.

While we do not quibble with Elon Musk's obvious success, or the potential importance of this neural lace, the development makes us very nervous in light of the present cyber threat environment. Everything from light bulbs to bio-medical devices are being targeted, and few products are able to bear up under concerted attack. We wouldn't advise you to connect that sort of environment to your brain anytime soon.

CloudBleed Bug Leaks User Data

The coding of the reverse proxies that are the core of the CloudFlare service were recently found to contain a bug that causes temporary memory to be dumped. Unfortunately, these temporary memory buffers were not scrubbed before they were returned to the system. So an attacker can use the technique to access indeterminate amounts of memory from conversations with prior clients. This is quite serious, in that unsanitized memory could give access to anything that was part of any client HTTPS conversations handled by that particular HTTPS proxy. This might include passwords, session cookies, or handshake parameters from the Transport Layer Security (TLS) association. The problem was triggered by the presence of a specific set of unbalanced HTML tags. CloudFlare now claims to have addressed the problem.

Please visit our website at www.ieca.com.

The IECA Cyber Bulletin is published monthly as a service to our clients and the security community at large.