October 2015

Bits & Bytes–Hot off the Digital Grill

Silent Shield's Monthly Newsletter on Digital Forensics & Cybercrime

Government Promotes Cybersecurity Awareness This Month

October is "National Cyber Security Awareness Month," a presidential designation made since 2003 to encourage greater knowledge about the increasingly sophisticated cyber threats posed to government, corporations and individuals, and to educate the public about cyber hygiene and security.

In acknowledgement of the federal designation, the National Security Agency (NSA) and Department of Homeland Security have set up a web page–National Cyber Security Awareness Month–devoted to educating the public about cyber security with a focus on weekly themes:

- General Cyber Security Awareness
- Creating a Culture of Cyber Security at Work
- Connected Communities: Staying Protected While Always Connected
- Your Evolving Digital Life
- Building the Next Generation of Cyber Professionals

In a statement promoting the designation, NSA director Admiral Michael S. Rogers said, "The importance of cyber security continues to grow as cyber risks increase. Recent attacks against the federal government and industry demonstrate the ongoing challenges of securely protecting networks and proprietary information. As the threats escalate and become more sophisticated, so must our vigilance and the resources we use to thwart them."

To learn more go to: https://www.nsa.gov/public_info/news_information/2015/ncsam/index.shtml

Score 18 for the Good Guys!

Eighteen Georgia residents were arrested earlier this month on charges relating to the possession, production and/or distribution of child pornography over the Internet. The arrests were made after a three-month investigation by the Georgia Bureau of Investigation's Child Exploitation and Computer Crimes Unit and the Georgia Internet Crimes Against Children Task Force.

Officers executed 24 search warrants and seized 232 digital devices as evidence. Further arrests are expected, as the investigation continues with more search warrants issued based on digital forensic evidence found thus far on the seized devices.

FBI Issues Alert on Vulnerability of "Internet of Things"

The U.S. Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) released a public service alert last month warning that the "Internet of Things" is vulnerable to cyber criminals. The Internet of Things (IoT) refers to objects and devices connected to the Internet that automatically send and/or receive data.

IoT devices are used in security systems, medical monitoring, smart appliances, fuel monitoring, lighting modules, entertainment systems, heating/air conditioning, and office equipment such as wireless printers. These devices generally connect through computer networks to exchange data with the operator, business, manufacturers, and other connected devices, mainly without requiring human interaction.

According to IC3, IoTs tend to have deficient security capabilities, and present difficulties with regard to patching vulnerabilities. Combined with a lack of consumer security awareness, these factors provide cyber criminals with opportunities to exploit the IoT devices. Unsecured or weakly secured IoTs may allow cyber criminals to

Continued on Next Page

***IoT,** from Page 1*

intrude upon private networks and gain access to devices and information attached to the networks. IoT devices with default passwords or open Wi-Fi connections are considered especially vulnerable.

IC3 warns that criminals can exploit the Universal Plug and Play protocol to gain access to many IoT devices. Because the protocol is designed to self-configure when attached to an IP address, cyber criminals can change the configuration and run their own commands on the devices.

Depending upon the device, cyber criminals can potentially use the compromised IoT to remotely facilitate attacks on other systems, steal personal information, send malicious emails, interfere with businesses transactions, perform digital eaves-dropping, interfere with physical safety, and/or overload the devices to render them inoperable.

Among consumer protection recommendations offered by IC3 are:

- Isolate IoT devices on their own protected networks
- Disable Plug and Play protocol on routers
- Purchase IoT devices from manufacturers with a proven track record of offering secure devices
- Update IoT devices with security patches when offered
- Change default passwords and only allow operation with a home network with a secured Wi-Fi router
- In devices that do not allow password changes, ensure the device providing wireless Internet has a strong password and uses strong encryption
- Use current best practices when connecting to wireless networks or connecting remotely to an IoT device

For more information visit the FBI's IC3 website at: www.ic3.gov.

"Zero Day" Company Offers $1 Million, Largest Bug Bounty Ever

A start-up cybersecurity company last month offered the largest bounty ever to anyone who can hack into a computer system. Zerodium is offering $1 million to anyone who can provide a hacking trick to break into an iPhone or iPad running on Apple's newly released iOS9 system. The hack must be made remotely via the Internet, or through a vulnerable app on the device, or by text message, and the company is prepared to pay multiple bounties for different hacks, though the payouts are capped at $3 million.

Zerodium, and companies like it, serve as hacker middlemen who seek out "zero-day" system vulnerabilities in order to sell them to the highest bidding company or government before they become public. A "zero-day" vulnerably is named such because the application developer has zero days in which to plan a response once the flaw becomes known.

According to "bug-bounty" platform vendor Bugcrowd, the average bounty is only about $200, and a $110,000 payout to a security researcher who found vulnerabilities in Google Chrome is cited as being the highest single hack payout. Bugcrowd also notes that Hewlett-Packard paid out more than $550,000 in total last march in a contest it sponsored that found vulnerabilities in a number of systems. However, the *New York Times* reported in 2013 that an iphone zero-day hack sold for a half-million dollars.

Zerodium points to Apple's iOS system as being the most secure mobile operating

Continued on Next Page

Silent Shield Offering CATIE® Training Oct. 30

Silent Shield, LLC is hosting a CATIE® training session at the Jackson, TN Police Department on Oct. 30, from 9:30 am to 12 pm. The introductory training class will demonstrate how CATIE® compares to other products, such as Camtasia, Snagit and Snipping Tool, to show how agencies can increase efficiency and productivity in cybercrime and digital forensics cases. The class will also detail the benefits of several add-on modules, such as Prosecution Package, Inventory Module and Activity Monitor.

Pre-registration is not required, but participants must present their law enforcement or government agency credentials for admittance.

***Bounty,** from Page 2*

system of all. "But don't be fooled," says a statement on the company's website announcing the bounty. "[S]ecure does not mean unbreakable, it just means that iOS currently has the highest cost and complexity of vulnerability exploitation and here's where the Million Dollar iOS 9 Bug Bounty comes into play."

While only months old, Zerodium has reportedly already acquired zero-day hacks potentially affecting Web browsers on Windows and Android. Zerodium founder Chaouki Bekrar said the company is "currently spending between $400,000 and $600,000 per month for vulnerability acquisitions, and we expect to spend around one million U.S. dollars per month before the end of this year additionally to the iOS bug bounty."

The deadline for applying for the bounty is this Oct. 31 at 6 p.m. EDT, but it may be terminated prior to this time in the event the payout total reaches $3 million. Terms of the payout dictate that the bug cannot have been reported to Apple or otherwise been publicly disclosed. For more information go to: www.zerodium.com/ios9.

Is No One Safe?–Top U.S. Spy Chief Allegedly Hacked by Teenagers

An American teenager has reportedly hacked into the personal email accounts of the U.S. spy chief and the head of U.S. security. The teenager and his accomplices, who go by the moniker "Crackas With Attitude (CWA)," contacted the *New York Post* and *Wired Magazine* in mid October to gloat about their exploits and provide evidence of their allegedly successful hack.

The hackers reportedly used "social engineering" tactics to trick Verizon employees into giving them personal information about U.S. Central Intelligence Agency (CIA) Director John Brennan, and then used this information to gain access into the director's private AOL account. CWA also claimed that it gained access to Department of Homeland Security Secretary Jeh Johnson's private Comcast account.

Among sensitive documents accessed by the hackers were Brennan's "SF-86" application that the director had filed to obtain top-secret security clearance. Brennan's account held sensitive documents because he had made the mistake of forwarding them from his work email. Other documents accessed included a spreadsheet of names and social security numbers of intelligence officials and a letter from the Senate regarding its demands that the CIA halt harsh interrogation techniques.

CWA told the *New York Post* and *Wired* that they had access to Brennan's account for three days, and that the director re-set his password three different times to regain control of his account, but that they would then "re-jack it." The hackers then called the director on his mobile phone and advised him that he had been hacked.

In describing the phone call, CWA told *Wired* that when Brennan asked what the hackers wanted they replied, "two-trillion dollars...just joking."

"How much do you really want?" Brennan, according to CWA, replied.

"We just want Palestine to be free and for you to stop killing innocent people," CWA said it

Continued on Next Page

Spy Chief, *from Page 3*

responded, at which point Brennan hung up.

The CIA director's private account has been disabled, and the FBI and other federal agencies are investigating. Details about the scope of the Homeland Security secretary's hack have not emerged, though CWA did provide the *Post* with screenshots of the account's billing pages.

A law enforcement source told the *Post* that "I think they'll want to make an example of [CWA] to deter people from doing this in the future." While noting that it's hard to believe CWA had the nerve to hack the head of the CIA, the source added that the "problem with these older-generation guys is that they don't know anything about cybersecurity."

US-EU Safe Harbor Agreement Ruled Invalid by European Court

Servers based in the U.S. that store European visitor data may be violating the law, as the European Court of Justice earlier this month invalidated the U.S.-European Union (EU) Safe Harbor Program. The EU Court ruling came in the wake of leaked files by former National Security Agency (NSA) contractor Edward Snowden's that revealed that the NSA was spying on European data held by American companies. The court essentially ruled the Safe Harbor Agreement invalid because the leak proved that American companies can't be trusted with user data.

In theory this ruling means that transferring EU customer data to U.S.-based servers is now illegal and that American companies are subject to lawsuits from Europe. However, cyber-security and legal experts are just starting to determine the ramifications of the ruling, and some U.S. companies are already protected under other EU-approved data protection agreements known as "model clauses." The U.S. Department of Commerce is expected to issue guidance on how to comply with the ruling or otherwise resolve its impact in the coming weeks. In the meantime, the Department will continue to administer the program under the original framework.

The Safe Harbor Agreement was developed by the European Commission and U.S. Commerce Department in the late 1990s to account for Europe's stricter privacy laws. These laws include provisions that prohibit sending of personally identifiable information (PII) outside of Europe unless that data is adequately protected. Safe Harbor created a streamlined program in which U.S. companies could self-certify that they were in compliance with the data protection requirements, and then be automatically protected by the agreement.

U.S. companies known to store European PII should contact their web hosting company to determine whether it has an existing model clause agreement with the EU. Absent such a clause, companies will likely have to wait for guidance from their provider and/or the Commerce Department.

For the latest Commerce Department information about Safe Harbor go to: www.export.gov/safeharbor.

Cybercrime by the Numbers!

Top Five Traditional Schools Offering Computer Forensics

George Mason University
Fairfax, Virginia

Kent State University
Kent, Ohio

Southern Utah University
Cedar City, Utah

University of Alabama
Tuscaloosa, Alabama

University of Central Florida
Orlando, Florida

Top Five Online Computer Forensics Degree Providers

Kaplan University
www.kaplanuniversity.edu

Loyola University Chicago
www.luc.edu

Penn Foster College
www.pennfoster.edu

Stevens-Henager College
www.stevenshenager.edu

Walden University
www.walden.edu

Source: Criminal Justice Degree Hub

Department of Homeland Security Considers Security Clearance Revocation for Personnel Who Fall for Phishing Emails

The Department of Homeland Security (DHS) may revoke the top-secret security clearance of high level officials who continuously fall for phishing emails. The action is being considered in the wake of revelations that some employees repeatedly fall for these scams and that even senior-level department officials are susceptible.

"Someone who fails every single phishing campaign in the world should not be holding a [top secret security clearance] with the federal government, said DHS Chief Information Security Office (CISO) official Paul Beckman, who spoke during a panel discussion at the Billington Cybersecurity Summit in Washington on Sept. 17, 2015. Such people have "clearly demonstrated that [they] are not responsible enough to responsibly handle that information," he added.

Beckman described how he sends out his own "blatant" phishing emails to test staff members, including senior managers, to see who fall for the fake scam by clicking on potentially unsafe links and inputting usernames and passwords. Employees who click and fail are forced to undergo mandatory online security training. But Beckman said a small number of employees continue to fall for the fake scams, sometimes even in the third round of phishing tests. "You'd be surprised at how often I catch these guys," he said.

DHS discussions about revocation of security clearance for repeat offenders are still in the initial stages, and CISO is currently more focused on the impacts of the recent hack of data on 22 million federal employees and contractors from the U.S. Office of Personnel Management. Among the top concerns regarding this hack is how the data could be used to create personally tailored phishing expeditions that will make government officials more susceptible to the scams.

Silent Shield Opens Satellite Office in North Georgia

Silent Shield, LLC is opening a new satellite office next month in North Georgia to provide products, support and training to sworn law enforcement and government agents. The 2,500-square-foot office is designed to offer support for Silent Shield products to law enforcement and government agents in the region encompassing North Georgia, Western North Carolina, East Tennessee, Northeast Alabama and Upstate South Carolina. Closed to the public, officers and agents can call ahead to book an appointment to review and test Silent Shield's latest digital forensic and cybercrime fighting tools, or schedule a group training session. For more information contact Silent Shield at 678-838-4243.

Score Another for the Good Guys!

The U.S. Department of Justice earlier this month announced the arrest of Andrey Ghinkul on nine counts of cybercrime-related charges that were associated with more more than $10 million dollars in cybertheft losses to U.S. banks and businesses. Ghinkul was arrested in Cyprus and the U.S. is currently seeking his extradition. The malware used in the crime–"a bonet named "Bugat"–has been "substantially disrupted," according to the DOJ.

Silent Shield, LLC
400 Galleria Parkway
Suite 1500
Atlanta, Georgia 30339 USA
(678) 838-4243

Contact:
sales@silentshield.com
info@silentshield.com

Web Site:
www.silentshield.com

Silent Shield, LLC provides cost-effective, technologically advanced cybercrime fighting and digital forensic tools for law enforcement personnel, military operations and government agencies.

Bits & Bytes–Hot of the Digital Grill is published 12 times per year by Silent Shield, LLC.