September 2015

Bits & Bytes–Hot off the Digital Grill

Silent Shield's Monthly Newsletter on Digital Forensics & Cybercrime

Louisiana State Attorney General's Investigators Win Silent Shield Sponsored Digital Crime Scene Challenge

Investigators from the Louisiana State Attorney General's Office took top honors at the second annual Digital Crime Scene Challenge sponsored by Silent Shield, which was held during the 27th annual Crimes Against Children Conference (CACC) in Dallas, TX, Aug. 10-13. The Louisiana investigators topped all of the other three-member teams vying to collect and identify evidence and utilize computer-based forensics tactics to formulate an investigative strategy within a designated time frame. The winning team from last year's Challenge, officers with the Edmond, Oklahoma Police Department's Internet Crimes Against Children task force, came in at a close second place.

This year's Challenge represented an expansion from the first year's Challenge, with expanded investigation times and a larger playing field to accommodate the increased number of registered teams. The first annual Challenge drew registration and extensive interest from all conference participants, necessitating the need for an expanded challenge. Jim Persinger, chief executive officer and managing partner of Silent Shield said, "We are evaluating this year's Challenge to determine what improvements we can help make for 2016."

The Digital Crime Scene Challenge is open to all CACC registered agency or business attendees who are devoted to solving crimes against children. The Challenge is designed to provide participants with hands-on experience in proper legal procedures, from applying for search warrants to conducting suspect interviews. The inaugural challenge and

Continued on Next Page

Silent Shield Upgrades Field Search

Silent Shield, LLC is pleased to announce it will release an "interim" upgrade to its Field Search program during third quarter 2015. The "interim" release resolves existing bugs and provides users with easier management of internet histories. The "interim" upgrades will resolve minor issues and serve users until the release of Field Search Version 5 later this year or in early 2016.

Field Search is used by more than 15,000 law enforcement agencies, probation offices and the military as a triage tool that examines computer files to quickly identify elements that may be related to an investigation. Designed to operate from a thumb drive or computer hard drive, Field Search is used to scan internet histories and search for specific text and images. Searches allow for bookmarking and the program is equipped with a built-in report generator that allows extraction of specific files in PDF, HTML or RTF format, or the extraction of an entire list of files into an Excel spreadsheet.

The program is offered free to law enforcement, and over 5,000 law enforcement, probation office and military personnel have been trained in its use. For more information about Field Search, contact Silent Shield at: http://www.silentshield.com/contact-us/, or by calling 1-(678) 838-4243. Existing users will be notified when Version 5 is released.

Participants at the 27th Annual Crimes Against Children Conference held Aug. 10-13, in Dallas, TX, stopped by the Silent Shield exhibitor booth to examine CATIE® software and test their digital sleuthing skills with Silent Shield's new Simulator program. Pictured demonstrating the software is Silent Shield Partner and Director of Business Development Evelyn Bishop-Persinger.

Challenge, *from Page 1*

this year's expansion were devised by Matthew Dunn, Supervisory Special Agent with the U.S. Department of Homeland Security's Immigration and Customs Enforcement. Agent Dunn developed a fact pattern and related scoring system for the Challenge. Teams were given the opportunity to apply for and execute a faux search warrant, search the suspect's "room" for evidence, catalog findings, hypothesize about unknown elements regarding the crime, and determine what steps needed to be taken to then successfully bring charges.

Each winning investigator was awarded a licensed edition of Silent Shield's Capture and Track Investigative Evidence (CATIE®) software, Google tablets and paid registration to the 2016 Crimes Against Children Conference, during which they will have the opportunity to defend their winning title.

In addition to sponsoring the Digital Crime Scene Challenge, Silent Shield hosted an exhibitor booth at the CACC, which drew more than 3,800 attendees devoted to protecting children, combatting child abuse and capturing child predators. The Silent Shield booth showcased the company's full suite of digital forensic investigative tools. In addition, Silent Shield's Simulator, which tests the skills of cybercrime and digital investigators in real time, was available to challenge each attendee's skills, which were tracked by the Simulator, and the top scores were posted on the booth's public monitor for all to see. Silent Shield's booth also featured two computer systems that allowed attendees to actually witness and experiment with CATIE® to personally experience how CATIE® helps law enforcement manage cases and track evidence.

Silent Shield develops hardware devices and software applications primarily for use by law enforcement to assist with online, offline and real-time investigations, and specializes in the development of digital forensics investigative tools that keep pace with the rapid rise of new computer technology. CATIE® is customizable software available only to law enforcement, that provides tools that track, trace, protect, preserve, catalog and report investigative evidence recovered online, offline or in real time. The software was developed to increase productivity of investigations by offering a streamlined alternative to the myriad and disconnected processes for collecting digital evidence.

CATIE® SOFTWARE
COMMAND HOW YOU INVESTIGATE

Planes, Trains & Automobiles Definitely Vulnerable to Hacking!

How's this for scary? You're driving along the highway in your new Jeep Cherokee at about 70 m.p.h. when the air vents start blasting maximum chilled air, the radio switches on and begins blaring Kanye West at full volume, and then the windshield wipers start wiping…all without you touching a control knob. And then the accelerator stops working, making your Jeep slow to a crawl while the r.p.m.s continue to climb. You regain control of the car after turning the ignition on and then off, but then, after moving forward again, the brakes fail to engage and you roll out-of-control into a ditch.

Yep, scary. But not only scary, but also true, as this is what a test driver went through earlier this summer when computer security researchers successfully took control of a Jeep by hacking into its entertainment system via the Fiat Chrysler mobile data network, "Uconnect." During this test hack the researchers also proved that they could abruptly engage the brakes, kill the engine while it was running in lower speeds, and take control of steering when the car is in reverse. The researchers, who are perfecting their ability to take complete control of the steering, also showed that they can take control of the vehicle from anywhere in the country, as well as remotely keep track of its location.

That test hack led Fiat Chrysler on July 24, to issue a safety recall of 1.4 million of its vehicles in the U.S. to install upgrades in the software of affected vehicles. Following the recall, the National Highway Traffic Safety Administration issued a memo warning that an estimated 2.8 million Harmon International car audio systems installed primarily in Mercedes-Benz, BMW, Subaru and Volvo vehicles could also be vulnerable to a similar style hack. Meanwhile, Senators Ed Markey and Richard Blumenthal have introduced legislation designed to establish new digital security standards for the automobile industry.

With so many "Internet-connected" automobiles apparently vulnerable to hacking, it begs the question: what other vehicles that rely on onboard computer systems and wireless/Internet communication might be at risk?

Airplanes? Yep, the friendly skies might certainly turn scary if a hacker gets control of an aircraft's onboard computers, which, according to the U.S. General Accounting Office (GAO) is a

Continued on Page 6

Cybercrime by the Numbers!

Significant numbers relating to cybercrime and cybersecurity

Word's Largest Digital Data Thefts

1. The Drinkman Five: Four Russians and one Ukrainian, allegedly led by Vladimir Drinkman, were charged in July 2013 with hacking into computer networks and stealing 160 million customer credit and debit card numbers since 2005. The hack, which relied on SQL injection malware, affected 17 businesses and led to losses of more than $300 million. Drinkman and another suspect are in federal custody, while three others remain at large.

2. Adobe Attack: In October 2013 it was revealed that hackers gained access to Adobe's networks and stole email addresses and passwords for 150 million users, along with credit card data for almost three million of them. The nature of the hack has not been publicly revealed, and the investigation is ongoing.

3. eBay attack: eBay in May 2014 announced that hackers stole user names, encrypted passwords, email addresses and other personal data affecting 145 million of its customers. The attackers reportedly used compromised employee login information to gain access, and the investigation is ongoing.

4. Target Target announced in January 2014 that hackers accessed its network and stole 40 million credit and debit card numbers as well as 70 million customer email addresses. The hack was reportedly initiated via credentials from one of Target's contractors, and the investigation is ongoing.

5. Home Depot: Home Depot announced in September 2014 that hackers managed to steal 53 million customer email addresses, and 56 million credit and debit card numbers from its system. The retailer disclosed that the hackers used a vendor's login information to access the network and install malware on its self-checkout systems. The investigation is ongoing.

Ashley Madison Data Breach Likely to Lead to Increase in Hacktavism

Hacktavism reared its head in a big way this summer when a group calling itself the "Impact Team" stole the user data of a purported 39-million or so infidelity seeking customers of the Ashley Madison website, which is devoted to helping people have extramarital affairs. While the data breach is proving to be not quite as large as originally thought, millions of people have been affected and the company will be hard pressed to survive the fallout and related legal action.

The Impact Team announced its hack on July 15 by warning the company to immediately shut down their websites or face the public release of their customer database. The hackers claimed to be morally outraged by the Website's facilitation of affairs, but seemed to be especially angered by the company's flawed "delete" policy, in which members were charged $19 to delete their profiles and personal information. This reportedly netted the company $2 million in 2014; however, the paid "delete" function did not work as advertised, and former members' information remained on the site.

The hackers made good on their threat on July 21, with the release of over 60 gigabytes worth of customer data, which was confirmed to be valid by Aug. 18. In a message included with the release, the Impact Team stated: "We have explained the fraud, deceit, and stupidity of ALM and their members. Now everyone gets to see their data . . . Too bad for ALM, you promised secrecy but didn't deliver."

The release was thought to contain information about almost 39-million customers, but that number continues to decline as more and more accounts turn out to be fake. In fact, the female membership, described by some analysts as only comprising about five to 10 percent of the entire membership, apparently includes a small army of "fembots" which actively engaged in flirtatious communication with the real men on the site in order to encourage their continued payment for using the Website. According to one data analyst, it appears that Ashley Madison devoted a significant portion of its software development on "refining their fembot army, to make it seem that woman are active on the site." The reasons for this, according to the analyst, was that "the number of real woman was vanishingly small, or because they didn't want men to hook up with real women and stop buying credits from the company."

The scope of the data breach and revelations such as the above alleged fraud will undoubtedly continue to emerge in the weeks ahead. Real men, and perhaps a few real women, will be outed for their philandering bent. Some reputations will be smeared, jobs perhaps lost and families destroyed. And

Continued on Next Page

***Madison,** from Page 4*

a morally deficient–and perhaps fraudulent–company might be destroyed.

While the hacktavist(s) in this case are trying to lay claim to the moral high ground, the hack remains a criminal act and the hackers should be charged for the breach and data theft. Unfortunately, the size and publicity of this case of hacktavism will undoubtedly lead to an increase in cyber attacks based on moral, political and social beliefs.

As for the hacker(s), the hunt is on! Ashley Madison parent company Avid Life Media has offered a $500,000 reward for information leading to the arrest and conviction of the perpetrator(s). However, please be advised that because Avid Life is a Canadian company, the award amount only adds up to about $377,000 in U.S. dollars. Moreover, by the time any case reaches the courts, the company could very well be in difficult financial straits and be unable to pay the reward money.

Of course, the challenge alone of finding the hacker may be enough to stir public action. Anti-virus software pioneer John McAfee reportedly claims to have narrowed down the field of suspects to being a lone, female, former Avid Life employee. No word yet on whether any impending award money may be coming his way.

NSA Transitioning Crypto to Head Off Quantum Computing Threat

The U.S. National Security Agency (NSA) has issued warnings that current cryptography used to protect email, online transactions and computerized records of all kinds may soon be rendered obsolete by quantum computing. In an update to its web page on Suite B Cryptography–www.nsa.gov/ia/programs/suiteb_cryptography–the NSA advises U.S. agencies and businesses that have not yet transitioned their computer security to the NSA's "Suite B" cryptographic algorithms, to hold off while the agency strategizes a transition to quantum resistant crypto. The August 19th update follows moves by the British NSA counterpart, Government Communications Headquarters, to encourage public sector research into developing quantum-resistant crypto systems.

The theoretical capabilities of quantum computing include the ability to instantly find the prime factors of extremely large numbers, and the rapid computing of discrete logarithm mod primes and discrete logs over elliptical curves. Current cryptography relies in large part on the difficulty of computing these factors and on the belief that crypto based on these modes cannot be deciphered by today's computers.

While quantum computing remains in the theoretical realm, the moves by these security agencies suggest that they might be concerned that quantum computing may be closer to reality than most experts think. Current forecasts for the implementation of quantum computing range from 10 to 50 years, with the former now seeming more likely to some experts with the revelation that NSA has begun working on quantum resistant algorithms.

The Aug. 19 update states that NSA's goal is to "provide cost effective security against a potential quantum computer. We are working with partners across the [U.S. government], vendors and standards bodies to ensure there is a clear plan for getting a new suite of algorithms that are developed in an open and transparent manner that will form the foundation of our next Suite of cryptographic algorithms."

While the guidance essentially advises the use of the same regimen of algorithms and key sizes that have been recommended for years, it suggests that those considering its Suite B, defer development. "For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition."

***Hacking,** from Page 3*

distinct possibility. According to an April 14, GAO report–*FAA Needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to NextGen*–it is theoretically possible for someone with just a laptop to implant a virus into flight control computers, take over the warning or navigation systems, or even commandeer an aircraft.

Noting that the nation is currently upgrading its air traffic control system to use Internet-based technology on both ground systems and in the air, the report concludes that avionics are definitely at risk. "Modern communications technologies, including IP connectivity, are increasingly used in aircraft systems, creating the possibility that unauthorized individuals might access and compromise aircraft avionics systems," according to the report. While the report does not specifically diagram potential hacks, and notes that someone would have to bypass a firewall between the Wi-Fi system and the rest of the plane's electronics, "because firewalls are software components, they could be hacked like any other software and circumvented."

In response to the GAO report, the acting Federal Aviation Administration's (FAA) assistant secretary for administration, Keith Washington, said the agency has "already initiated a comprehensive program to improve the cybersecurity defenses of the National Airspace System infrastructure, as well as other FAA-mission-critical systems. We are significantly increasing our collaboration and coordination with cyber intelligence and security organizations across the federal government and in the private sector."

We trust that the FAA has pushed this onto the priority list, as a security expert claimed that same month that he had been able to successfully take control of a plane in flight via its onboard entertainment system, and in June, Poland's LOT airline grounded 10 flights due to a cyber attack that temporarily paralyzed the airline's on-the-ground systems.

Trains? Trains do not appear to have been on the radars of potential hackers, perhaps due to their perception as a low-tech form of transportation. But as the world's rail systems get more technical and rail components make more use of digital technologies, they too could become subject to more interest. While we have not heard of any successful cyber attacks against U.S. rail systems, a suspected attack against a northwest rail company in 2011 made clear that railway systems were vulnerable to such attacks.

In a memo determining that the incident was not a cyber-attack, the Transportation Safety Administration noted that the incident highlights how railway supervisory and control data acquisition systems (SCADA) are at risk. A cyber security expert who examined the incident determined that it proved that all elements of SCADA are vulnerable, including switches, signals, crossing lights, transformers, engine monitors, and sensors. More recently, the United Kingdom's rail system was warned by cyber security experts earlier this year that a planned upgrade to its digital signaling system could make its trains vulnerable to remote hacking, hijacking and crashing.

Remote hacking, hijacking and crashing!–Apparently not just in the movies anymore.

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 forensics tools exclusively 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.