November 2015

Bits & Bytes–Hot off the Digital Grill

Silent Shield's Monthly Newsletter on Digital Forensics & Cybercrime

Silent Shield's Upcoming Release of Field Search Expected to Easily Parse and Examine Microsoft Edge

Silent Shield is pleased to report that the latest version of its triage tool, Field Search, will provide, among other enhancements and features, easy analysis and parsing of Microsoft's new web browser, "Edge." Field Search Version 5 passed alpha testing and is in its final testing phase, which is expected to conclude over the next few weeks. Silent Shield plans to release the latest version of Field Search mid December 2015.

Edge eventually will replace Microsoft Internet Explorer and compete with other browsers such as Google Chrome and Firefox. The latest upgraded edition of Edge, which is included with Microsoft's Windows 10 operating system, was released earlier this month.

Security experts have expressed concerns about how Edge may impact data searches conducted using existing forensic tools because Edge integrates with Microsoft's online platforms, and supports cache files, pictures and bookmarks on a single file for storage and sharing on OneDrive, Microsoft's Cloud-based storage "system." The latest version of Field Search was designed to address these "nuances" and is expected to have scan, retrieve, pars3 and repor relevant Edge data faster than existing forensic triage tools.

Field Search is used by more than 15,000 law enforcement agencies, probation officers and military personnel as a triage tool to examine computer files to quickly identify elements potentially related to an investigation or probation violation. Designed to operate from a thumb drive or computer hard drive, Field Search can be used to scan Internet histories and search for specific text and images among other features. Field Search also allows for bookmarking and is equipped with built-in reporting 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: www.silentshield.com or call (678) 838-4243. Existing Field Search users will be notified when Version 5 is released.

Score 1,004 "Rescues" for the Good Guys, 2,394 Worldwide Arrests!

Child exploitation investigators with the Department of Homeland Security U.S. Immigration and Customs Enforcement (ICE) division announced this month that they had identified and rescued 1,004 victims of child sexual abuse and online exploitation so far this year. Special Agents with ICE's Homeland Security Investigation (HSI) Department also arrested or assisted in the arrest of 2,394 child predators worldwide so far this year, through human trafficking investigations, including the production and distribution of online child pornography and child sex tourism.

HSI has analyzed more than 7,500 *TERABYTES* of data seized through search warrants to date this year, which equates to almost 100 years of high definition video. More than half of the data analyzed was related to child exploitation investigations, and HSI notes that the amount of child exploitation data collected through search

Continued on Next Page

Good Guys, *from Page 1*

warrants is increasing by approximately 40 percent per year, a staggering incremental percentage.

HSI is one of the worldwide leaders in the fight against sexual exploitation of children and the pursuit and apprehension of such criminals. The department is a prime collaborator in Operation Predator, a worldwide initiative to protect children from sexual predators.

As part of the initiative HSI:

- Participates in all 50 states, and 11 local enforcement agencies, Internet Crimes Against Children Task Forces across the U.S.
- Operates the National Victim Identification Program, which combines the latest technology with traditional investigative techniques to rescue victims of child exploitation.
- Works with Interpol's working group that locates new child sexual abuse materials on the Internet and refers cases to the countries from which the material is believed to originate.
- Assigns Special Agents to work with Interpol, foreign governments, and law enforcement agencies to coordinate on child crimes that cross borders.
- Works in partnership with the National Center for Missing and Exploited Children and other federal agencies to help solve cases, make arrests, and rescue potential victims.
- Is chair and founding member of the Virtual Global Taskforce, which joins law enforcement agencies, non-governmental organizations and private sector partners around the world to fight child exploitation information and images that travel over the Internet.

Since its inception in 2003, Operation Predator has resulted in HSI arrests of more than 14,000 suspects for crimes against children.

NIST Seeks Input On Mobile Devices, Cloud Security

The National Cybersecurity Center of Excellence is seeking public comments on the National Institute of Standards and Technology's (NIST) draft guide, *Mobile Device Security: Cloud and Hybrid Builds*. The draft guide, released earlier this month, offers information on how commercially available technologies can meet organizational needs to secure sensitive information accessed by and/or stored by mobile devices.

Organizational adoption of mobile devices without policies and management infrastructure designed to keep data secure "increases the opportunities for attackers to breach sensitive enterprise data," according to the guide's executive summary. The "How To" guide offers demonstrations of standards-based, commercially available cyber security technologies, which helps organizations save research and proof of concept costs.

The executive summary notes that the information technology

Continued on Next Page

FBI Warns About EMV Card Vulnerability

Last month the FBI issued a warning that hundreds of millions of "EMV" credit cards being issued (as replacements for traditional magnetic strip credit cards) may still be vulnerable to exploitation. While EMV cards provide greater security than traditional cards, "no technology eliminates fraud and cybercriminals will continue to look for opportunities to steal payment information," notes the Oct. 13th public service announcement.

One of the biggest security threats to the new EMV cards is the fact that they still include the magnetic strip and its related information, which is necessitated simply because not all merchants have upgraded to EMV technology. Thus data on EMV cards can still be stolen if a merchant has not upgraded to an EMV terminal and his magnetic strip reader has been infected or compromised with data-capturing malware. Additionally, the EMV chips do not prevent lost or stolen cards from being used in stores, nor does the EMV chip prevent the stealing of information from online or telephone purchases.

The FBI urges consumers using EMV cards to utilize merchants with EMV technology whenever possible, and reminds consumers and merchants alike to handle EMV cards with the same level of security and precaution used for traditional credit cards.

NSIT, *from Page 2*

environment is undergoing dramatic change with the increasing popularity of smartphones, tablets, and other high powered and "rapidly maturing" mobile devices. Such devices have similar functional capabilities as traditional information technology, particularly with mobile (cloud) computing, but security controls "have not kept pace with security risks that mobile devices can pose."

The guide is designed to demonstrate how security can be supported throughout the mobile device "lifecylce," and offers information that:

- Identifies security characteristics that need to be addressed to reduce the risk of data breach from mobile device storage and cloud-based access.
- Maps security characteristics to standards and best practices.
- Provides a detailed example solution, with instructions for implementers and security engineers, on installing, configuring and integrating the solution into existing information technology infrastructures.
- Points to mobile devices and enterprise management systems that meet identified security characteristics.
- Provides an example solution suitable for organizations of all sizes, along with an accompanying evaluation.

The comment period is open until January 8, 2016. Reviewers can access the document and submit comments by going to: www.nccoe.nist.gov.

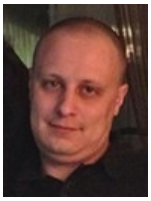
Cybercrime by the Numbers!

FBI's Top Most Wanted Cyber Criminals

Most everyone is familiar with or has at least heard of the FBI's Top Ten Most Wanted list, which was first officially released in 1950 and has thus far led to the capture of 471 criminals. But did you know the FBI also has a "Cyber's Most Wanted" criminal list?

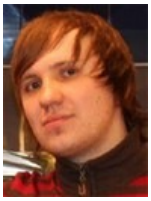
There are more than 10 of these most wanted cyber criminals and, if you happen to run across one of them, the rewards being offered for their capture and conviction can rise up to $3 million. Below are five of the most wanted, so if you see any of these suspects, or otherwise have information that might be connected to their respective cases, please contact your nearest FBI field office, or go to: tips.fbi.gov.

Joshua Samuel Aaron—numerous charges relating to an alleged scheme that combined the computer theft of customer information with stock manipulation. Aaron allegedly hacked into several U.S. company data bases and accessed information relating to millions of customers. Reward: none set yet.



Evgeniy Mikhailovich Bogachev—alleged operation of racketeering scheme that utilized malicious software that infected more than one million computers and led to the loss of more than $100 million. Reward: up to $3 million.

Nicolae Popescu—alleged operation of an Internet fraud scheme that bilked purchasers of vehicles and other merchandise for products that did not exist. The scheme relied on fraudulent online payment services, U.S. bank accounts opened under false passports, and wire transfers of proceeds. Reward: up to $1 million.



Alexsy Belan—alleged identity theft, computer intrusion and computer-related fraud in connection with the breach of three major e-commerce company computer systems leading to the theft of personal data and passwords of millions of accounts. Reward: up to $100,000.

Viet Quoc Nguyen—alleged computer intrusion and wire fraud conspiracy related to hacking into email service providers to steal information and marketing data on millions of email addresses, and the launching of spam attacks on many of these stolen addresses. Reward: no information provided by Bureau.

"Zero Day" $1 Million Bug Bounty Awarded, New Bounties Offered

Computer hackers successfully broke into Apple's recently released iOS9 system and were awarded the $1 million reward offered by Zerodium, the start-up cybersecurity company that offered the world's largest "bug bounty." The company reported that one team submitted a full chain of exploits that took advantage of a series of zero-day vulnerabilities leading to a remote and untethered jailbreak of the iOS 9.1 and 9.2. The anonymous team apparently submitted its data just hours before the Oct. 31 deadline expired.

Zerodium is now offering "premium rewards" to security researchers who disclose their original and unreported zero-day exploits affecting the world's most widely used operating systems, software and/or devices. The company is marketing its "Exploit Acquisition Platform" as exclusive, noting that while other bug bounty programs accept almost any kind of vulnerability, it only focuses on high risk vulnerabilities with fully functional exploits, and will "pay the highest rewards on the market."

As reported in the October issue of Bits & Bytes, Zerodium is only a few months old, but has quickly emerged as the leading purchaser of zero-day vulnerabilities. Zerodium, and companies like it serve as hacker middlemen who seek out such vulnerabilities in order to sell them to the highest bidding company or government before they become public. A zero-day vulnerability is called such because the application developer has zero days in which to plan a response once the flaw becomes known.

Meanwhile, Microsoft has revamped its bug bounty program by offering $100,000 prizes for anyone turning in mitigation bypass techniques. The company believes that such techniques are "much more valuable than learning about individual bugs because insight into exploitation techniques can help us defend against entire classes of attacks as opposed to a single bug." In an effort to make sure that "white hat" legitimate responders earn the rewards, organizations and people must pre-register with Microsoft before the company will accept technical write-ups and proof of concept code for consideration.

Of course, despite the expanding bounties being offered, many in the computing world believe the U.S. government is the biggest purchaser of zero-day vulnerabilities, and point to the U.S. National Security Agency's contract with zero-day exploit vendor Vupen Security, incidentally whose founders also launched Zerodium.

Digital Forensics Market Expected to More than Double, Reach $5 Billion by 2021, According to Report

A recently issued report forecasts that the global digital forensics market is expected to more than double in the next six years, rising from an estimated $2.03 billion in 2015 to almost $5 billion by 2021. The report—*Digital Forensics Market: Global Industry Analysis, Size, Share, Growth, Trends and Forecast 2015-2021*—attributes the strong growth to rapid advances in forensic technology, increasing affordability of the technology, and strong growth in the key sectors that utilize forensic technology.

The report, issued by global research and consultancy firm "Transparency in Markets," segments the digital forensics market into six types—computer forensics, network forensics, cloud forensics, mobile device forensics, database forensics, and "others"—with computer forensics accounting for more than 30 percent of the overall market. These forensic types are primarily used by seven distinct sectors of the economy, such as law enforcement, healthcare, banking, information technology, and defense, among others.

DHS Key Player in Cyber Forensics Support for Law Enforcement

While most people know that the U.S. Department of Homeland Security (DHS) is a key player in efforts to enhance cybersecurity in both the public and private sectors, many do not realize that the department also focuses on enhancement of cyber forensic tools and strategies for the nation's law enforcement agencies. Such efforts are carried out by DHS's Cyber Security Division (CSD), which established the Cyber Forensics Working Group in 2008 that is comprised of representatives from federal, state and local law enforcement agencies.

These representatives meet biannually to help guide the division's work by examining potential gaps in digital forensic capabilities in order to prioritize technology development, and test and evaluate new technologies. Among issues examined by the group are mobile device forensics, GPS forensics, first responder crime-scene computer triage, high-speed data capture, deep packet inspection, gaming system live capture, data acquisition and analysis, and law enforcement technology information exchange.

As stated on the CSD website —www.dhs.gov/science-and-technology/csd-forensics— criminal activity increasingly relies on computers and portable media devices, and such devices "frequently contain vital evidence, including user information, call logs, location, text messages, email, images and audio and video recordings."

However, because new technologies, both in hardware and software, are released at such a rapid pace, law enforcement has a "significant challenge" keeping up with the technology and its use by criminals. Because potential evidence contained on digital devices can make or break an investigation, law enforcement needs "updated tools to address the changing technology," which is where the working group comes into play.

CSD is also researching better methods to forensically acquire data from information and entertainment systems of vehicles seized during law enforcement investigations, and works to increase the capabilities of the existing open source digital forensics tool, "Autopsy."

While law enforcement agencies nationwide benefit from the work carried out by CSD, the Department of Homeland Security benefits as well, do to its extensive use of of digital forensic tools (as reported in "Score 1,004 Rescues for the Good Guys, 2,394 Worldwide Arrests" on page 1 of this edition of Bits & Bytes).

Smartphone App Scores One for the Good Guys!

A Michigan couple, who absconded during a federal child pornography investigation, turned themselves in earlier this month after being profiled on the U.S. Immigration and Customs Enforcement (ICE) "Operation Predator" smartphone app.

Authorities had been seeking the pair since charges were laid on Oct. 23, but had been unable to locate them. The "Operation Predator" app resulted in several tips regarding the pair's whereabouts, and the couple surrendered within a week of being added to to the system.

"The public pressure put on fugitives through traditional and social media has proved once again to be a game changer," said ICE Homeland Security Investigations Special Agent Marion Miller.

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.