Homeland Security

INTELLIGENCE ASSESSMENT

(U//FOUO) Cyber Targeting of the US Emergency Services Sector Limited, But Persistent

24 September 2015

Office of Intelligence and Analysis

IA-0285-15

Homeland Security
Office of Intelligence and Analysis

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

INTELLIGENCE ASSESSMENT

24 September 2015

(U//FOUO) Cyber Targeting of the US Emergency Services Sector Limited, But Persistent

(U//FOUO) Prepared by the Office of Intelligence and Analysis (I&A) and Multi-State Information Sharing and Analysis Center (MS-ISAC).

(U) Scope

(U//FOUO) This *Assessment* provides an overview of cyber threat actors targeting the US emergency services sector (ESS) and their associated tactics, techniques, and procedures (TTPs). The intent of this *Assessment* is to provide federal, state, local, tribal, and private sector stakeholders awareness of potential cyber threats to the ESS to help identify threats and design countermeasures to protect against future cyber operations.

(U//FOUO) This *Assessment* is based on a review of cyber attacks against the ESS between February 2012 and May 2015. We expect ESS systems and networks to remain targets of cyber actors beyond the information cut-off date, as ESS communications and networked systems continue to evolve and are increasingly accessible through cyber means.

(U) Key Judgments

(U//FOUO) Cyber targeting of the ESS will likely increase as ESS systems and networks become more interconnected and the ESS becomes more dependent on information technology for the conduct of daily operations—creating a wider array of attack vectors for cyber targeting.

(U//FOUO) We judge criminal hackers are the most prominent cyber actors targeting the ESS, as criminal hackers are prone to announcing attacks to increase visibility and support for their cause.[*] This is further evidenced by the numerous attacks against state and local networks, particularly law enforcement, in response to perceived social and legal injustices.

(U//FOUO) Cybercriminal targeting of the ESS for financial gain using tactics and techniques such as telephony-denial-of-service (TDoS) and ransomware to extort funds from victims likely will persist, as cybercriminals continue to see ESS entities as lucrative targets for extortion, as well as popular targets for nuisance-level attacks.[†,‡,§]

(U//FOUO) There is no reporting to indicate state-sponsored actors are actively targeting ESS networks.

---

[*] (U//FOUO) DHS defines criminal hackers as individuals or groups that commit a crime by illegally accessing or altering systems, often in furtherance of an ideological goal.

[†] (U//FOUO) DHS defines cybercriminals as individuals or groups that carry out illegal activities on computer networks, such as carding schemes, ransom and extortion, theft of personally identifiable information, and account information to facilitate fraud.

[‡] (U) A TDoS attack occurs when malicious actors seek to overwhelm an agency's phone system by flooding the agency's telephone switches with repeated calls from spoofed numbers, clogging lines, and inhibiting real callers from connecting.

[§] (U) Ransomware is malware that prevents victims from using their computers until they pay a ransom.

(U) Cyber Threats Against the Emergency Services Sector

(U//FOUO) Cyber targeting of the ESS will likely increase as ESS systems and networks become more interconnected and the ESS becomes more dependent on information technology for the conduct of daily operations—creating a wider array of attack vectors for cyber targeting. Independent researchers have already reported on the widespread availability of vulnerabilities and attack vectors for critical hardware and software that is used in this sector extensively. Such vulnerable systems include call-center communications-management software, closed-circuit TV camera systems, interactive voice response systems, and emergency alert systems—particularly wireless emergency alert systems.[1,2] Current and historic cyber threats against the sector primarily have been limited to low-level exploitation and attacks—such as data theft, denial-of-service (DoS) attacks, website defacements, and spear phishing—on individual targets from multiple adversaries, including criminal hackers, cybercriminals, and state-sponsored actors. While most malicious activity affecting the ESS serves as a nuisance, according to MS-ISAC, such activity has the potential to disrupt or endanger first responder activities by severing access to critical information systems, slowing system resources, and degrading the integrity of data.[3]

(U) Emergency Services Sector Overview

(U) The ESS comprises a system of preparedness, response, and recovery elements forming the nation's first line of defense in response to both man-made and natural threats.[4] The sector provides life-safety and security services across the nation through a first-responder community that comprises federal, state, local, tribal, territorial, and private sector partners.[5]

- *(U) Five disciplines make up the ESS: law enforcement, fire and emergency services, emergency medical services, emergency management, and public works.[6]*
- *(U) The ESS also includes organizations with specialized capabilities, such as hazardous materials; search and rescue; explosive ordnance disposal; special weapons, tactics, and tactical operations; aviation; and public-safety answering points (PSAPs).[7]*
- *(U) During the past decade, ESS has become increasingly dependent on cyber-supported assets, systems, and functions to carry out its missions—including databases, communications equipment, control systems, navigation systems, management systems, and security systems.*

(U) Criminal Hackers Most Prominent Cyber Actors

(U//FOUO) We judge criminal hackers are the most prominent cyber actors targeting the ESS, as criminal hackers are prone to announcing attacks to increase visibility and support for their cause. This is further evidenced by the numerous attacks against state and local networks, particularly law enforcement, in response to perceived social and legal injustices. Criminal hackers attempting to gain support for their political agenda—or to exact retribution for perceived social or legal injustices—have shown repeated interest in targeting the ESS. We assess, however, that their capabilities limit them to low-level cyber operations, such as DoS attacks, website defacements, and doxing (publishing of personally identifiable information), often attacking targets of opportunity.

- (U//FOUO) TeamBerserk—in support of its political agenda that the "security of our Nation needs to be inspected and made better"—announced on associated Twitter and Pastebin accounts in January 2014 that it leaked 54MB of compressed sensitive documents stolen from the networks of multiple fusion centers, according to US media reporting and DHS open source reporting.[8,9] Team Ghostshell, another criminal hacker group, claimed responsibility in December 2012 for compromising DHS, FBI, the Federal Reserve, Interpol, and other government and private sector networks, according to media reporting, to apparently highlight these organizations' security weaknesses.[10]

- (U) AntiS3curityOPS in May 2012 took credit for disrupting access for several hours to the websites of the Chicago City Council and Chicago Police Department as part of the group's activity against a NATO summit, according to US media reporting.[11,12]

- (U) X-Blackerz, Inc., CabinCr3W, LulzKnights, and AntiSec are criminal hackers responsible for stealing and leaking significant amounts of sensitive data from law enforcement during the last three years, according to media and law enforcement reports, in response to perceived injustices by the US Government and state and local law enforcement. The victims include law enforcement agencies in Florida, Hawaii, Michigan, New York, and West Virginia.[13-20]

(U//FOUO) Criminal Hacking Related to Perceived Police Brutality

(U) The below examples are representative of the high-visibility, low-level cyber operations used by criminal hackers to gain support for their causes.

» *(U) Multiple criminal hackers have targeted a variety of police departments and municipalities nationwide with DoS and doxing attacks in reaction to perceived incidents of police brutality, according to a December 2014 joint law enforcement bulletin by the California State Threat Assessment Center, MS-ISAC, and the Northern California Regional Intelligence Center (NCRIC).*

(U) In late November 2014, criminal hackers associated with the Anonymous collective targeted the City of Cleveland with a DoS attack in response to an officer-involved shooting. Although the city's public-facing website was taken offline, communications were not affected, according to US media reporting.[21] Reporting provides no indication how long the city's website was offline.

(U//FOUO) A number of DDoS attacks specifically targeting state and local government or law enforcement websites have had the likely unintended consequence of impacting emergency call centers and dispatch communications, such as 911 communications systems.

» (U) The hacker collective Anonymous claimed responsibility for a 9 March 2015 DDoS attack on the City of Madison, Wisconsin in response to a recent officer-involved shooting in the city.[22] The hour-long attack intermittently affected some police, fire, and medical dispatch services; as well as city government Internet and e-mail communications, and online payment services, according to US media reporting.[23]

» (U) Unknown criminal hackers on 20 December 2014 accessed the Indianapolis emergency 911 system that dispatches police, fire, and EMS vehicles across the city, according to local news media. The attack lasted several days and managed to slow systems, but due to network redundancies, public safety was never compromised, and the city was able to continue to dispatch vehicles on time.[24]

(U) Cybercriminals Pose Persistent Threat

(U//FOUO) Cybercriminal targeting of the ESS for financial gain using tactics and techniques such as TDoS and ransomware to extort funds from victims likely will persist, as cybercriminals continue to see ESS entities as lucrative targets for extortion, as well as popular targets for nuisance-level attacks. Cybercriminals usually do not seek to cause damage or disruption to systems or networks because this would potentially impede their ability to exploit those systems for profit.[25]

» (U) A Nevada county sheriff's department and a Wisconsin police department in mid-May 2015 were victims of ransomware attacks that encrypted both departments' shared folders.[26,27] According to MS-ISAC analysis of the incidents, the networks of both departments likely became infected when a user from each department accessed the same probable legitimate website that had been compromised.[28,29] There was no evidence of additional infections on either department's system nor data exfiltration attempts.[30,31]

» (U//FOUO) A municipal city and several local public-safety agencies in Southern California in early June 2014 were infected by ransomware, resulting in the compromise of more than 100 computers and 10 servers, according to reporting from the NCRIC, Orange County Intelligence Assessment Center, and MS-ISAC.[32]

» (U//FOUO) A local fire department in Northern California and a law enforcement agency in Southern California in late May 2014 were infected by ransomware, resulting in the compromise of at least one computer and one server in each location, making vital information unavailable, according to the same reporting.[33]

» (U) TDoS attacks in early 2013 affected approximately 600 critical government phone systems nationwide, including 200 PSAPs. Following floods of subsequent calls over a period of days or weeks, the attackers demanded payment of $5,000 to cease the TDoS, according to US media reporting.[34]

(U) Nuisance-Level Attacks Considered Negligible

(U) The ESS has been targeted by unknown threat actors, many of whom probably were cybercriminal pranksters, causing primarily nuisance-level attacks.

» (U//FOUO) An unidentified male on 29 January 2014 called the emergency room (ER) of an Ohio-based hospital and asked to speak with an ER employee. After being told the employee was not available, the caller became enraged and began cursing and yelling. After being disconnected due to his unruly behavior, the caller recontacted the ER approximately 100 times through 30 January 2014, causing a disruption of vital ER communications, according to a state fusion center analyst with first- and second-hand access to the information.[35]

» (U) A server belonging to a county regional public-safety communications agency in a Northwestern state was breached in mid-January 2014, exposing 6,000 medical-response records from three regional fire departments and personnel data on 231 full-time and volunteer firefighters, according to a local media report.[36]

» (U) A Wisconsin local police department reported in September 2013 that its Twitter account had been hacked, and unauthorized tweets were being sent from the account, including many laced with profanities, according to a US media report.[37]

» (U) Tornado siren systems in two cities in a mid-western state were compromised in July 2013. According to a press report, in one instance the siren was activated by what officials determined was a likely cyber attack using radio signals containing a unique code. Local police reported that an illicit copy of the signal likely was crafted and broadcast to activate the sirens.

» (U) Local emergency alert systems in Montana, Michigan, New Mexico, Utah, and California were compromised in February 2013 when unknown attackers used default credentials to send messages warning local residents of zombie attacks, according to media reports.[38] The default credentials allowed the actors to take control of systems at local TV stations and override current broadcasts with the false emergency messages.[39,40,41]

» (U) An unknown actor in February 2012 used a worm to infect a mid-western regional information system, forcing it to shut down, according to local media reports.[42] The incident affected approximately 200 different agencies, including police departments and others who use the system to check criminal information, such as warrants, criminal histories, mug shots and other records. The cause of the infection was unknown.[43]

(U) Nation-States Show Lack of Activity Against Emergency Services Sector

(U//FOUO) There is no reporting to indicate state-sponsored actors are actively targeting ESS networks.

(U) Appendix A: Recommended Spear-Phishing and Malware Mitigation and Protection Measures

(U) Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.

(U) Maintain up-to-date antivirus software, and keep operating systems and software up-to-date with the latest patches.

(U) Be cautious about *all* e-mails received, including those purported to be from "trusted entities," and be careful when opening links within those messages.

(U) Do not input personal information or login credentials in pop-up windows or links within an e-mail, and do not open attachments or click on links in unsolicited e-mails—access the links by navigating to the organization's website directly.

(U) Look for uniform resource locators that do not match a legitimate site, but appear to be associated with the site through small spelling variations or different domain names (.com vice .net).

(U) Be wary of downloading files from unknown senders. Malicious code can be embedded in commonly e-mailed files, such as .doc, .pdf, .exe, and .zip; and be particularly cautious of double file extensions (evil.pdf.exe).

(U) Only download software from trusted sites, and enable the feature to scan e-mail attachments before downloading and saving them to a system or network.[44,45]

(U) Source Summary Statement

(U//FOUO) The analysis in this *Assessment* related to criminal hacker activity is based on highly reliable DHS reporting acquired from a local law enforcement officer with first-hand access to the information, FBI reporting obtained from US government and law enforcement officers, and fusion center reporting and analysis. The analysis related to cybercriminal activity is based on highly reliable DHS, MS-ISAC, and fusion center reporting. Analysis related to criminal hacker and cybercriminal activity is supported by US media reporting that comprehensively covers criminal hacker and cybercriminal activities and largely corroborates one another. We have **high confidence** in our assessments of criminal hacker and cybercriminal activities targeting the ESS based on highly reliable DHS, FBI, MS-ISAC, and fusion center reporting; extensive corroborating media reporting; the open nature of these activities; and criminal hacker propagandizing. We have low confidence in our overall assessment of the threat to the sector, as we have few examples of malicious cyber activity beyond common cybercrime and criminal hacker activities.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

(U) Tracked by: HSEC-1.2.1, HSEC-1.2.2, HSEC-1.2.3, HSEC-1.3.1, HSEC-1.5

[1] (U); APTA Control and Communications Working Group; *APTA*; "Securing Control and Communications Systems in Transit Environments"; 30 JUL 2010; pg 6; Recommended practice.
[2] (U); McGregor, John; *SEI*; "Best Practices in Wireless Emergency Alerts"; FEB 2014; pg 24; Article.
[3] (U); MS-ISAC; "Common Cyber Threats to Public Safety Organizations"; JUN 2015; pg 1; Cyber Intel Advisory.
[4] (U); DHS; "Emergency Services Sector Specific Plan: An Annex to the National Infrastructure Protection Plan"; 2010; pg i; Sector specific plan.
[5] (U); DHS; "Emergency Services Sector Specific Plan: An Annex to the National Infrastructure Protection Plan"; 2010; pg i; Sector specific plan.
[6] (U); DHS; "Emergency Services Sector Specific Plan: An Annex to the National Infrastructure Protection Plan"; 2010; pg i; Sector specific plan.
[7] (U); DHS; "Emergency Services Sector Specific Plan: An Annex to the National Infrastructure Protection Plan"; 2010; pg i; Sector specific plan.
[8] (U); Paganini, Pierluigi; *Security Affairs*; "Team Berserk Announced a Leak of Document Data from DHS Fusion Center"; 20 JAN 2014; www.securityaffairs.co/wordpress/21414/hacking/teamberserk-hacked-dhs-fusion-center.html; accessed on 12 MAY 2014; Article.
[9] (U//FOUO); DHS; DHS-OS-0104-14, 171837Z JAN 14; DOI 17 JAN 2014; (U//FOUO); TeamBerserk Hacking Group Hacks California Fusion Center; Extracted information is U//FOUO; Overall document classification is U//FOUO.
[10] (U); Gonsalves, Antone; *CSO*; "Ghost Shell Takes Credit for Extensive Hack of Government Private Websites"; 27 AUG 2014; www.csoonline.com/article/2132606/data-protection/ghostshell-takes-credit-for-extensive-hack-of-government--private-websites.html; accessed on 10 MAY 2014; Article.
[11] (U); Nick and Eric Johnson; *Chicago Tribune*; "Anonymous Affiliate Claims Hacked Chicago Police Site as NATO Opens"; 20 MAY 2012; www.articles.chicagotribune.com/2012-05-20/business/sns-rt-nato-summitcyber-attack1e8gk2d1-20120520_1_nato-summit-web-site-web-attack; accessed on 09 MAY 2014; Article.
[12] (U); Musil, Steven; *CNET*; "Hacktivists Claim Take Down of Chicago Police Web Site"; 20 MAY 2012; www.cnet.com/news/hacktivists-claim-takedown-of-chicago-police-web-site/; accessed on 09 MAY 2014; Article.
[13] (U); Lincoln, Mileka; *Hawaii News Now*; "Hawaii Police Department Security Breach Appears to be Linked to Anti-American Hacking Campaign"; 06 MAY 2013; www.hawaiinewsnow.com/story/22176979/hpd-security-breach-appears-to-be-linked-to-anti-american-hacking-campaign; accessed on10 MAY 2014; Article.
[14] (U); Walker, Danielle; *SC Magazine*; "OpUSA Hacktivist Campaign Failed to Produce Much Mayhem"; 08 MAY 2013; www.scmagazine.com/opusa-hacktivist-campaign-failed-to-produce-much-mayhem/article/292528/; accessed on 10 MAY 2014; Article.
[15] (U); Crum, Travis; *West Virginia Gazette*; "Hackers Group Posts Police Chief's Information Online"; 07 FEB 2012; www.wvgazette.com/News/201202070284; accessed on 08 MAY 2014; Article.
[16] (U); Roberts, Paul; *Threat Post*; "CabinCr3w Hacker Arrested by FBI"; 04 APR 2012; www.threatpost.com/cabincr3w-hacker-arrested-fbi-040412/76403; accessed on 09 MAY 2014; Article.
[17] (U); Goodin, Dan; *ARS Technica*; "Feds Charge Self-Confessed Anonymous Member After Tracking His Digital Footprints"; 4 APR 2012; www.arstechnica.com/business/2012/04/feds-charge-self-confessed-anonymous-member-after-tracking-his-digital-footprints; accessed on 09 MAY 2014; Article.
[18] (U); Eördögh, Fruzsina; *Daily Dot*; "Anonymous Off Shoot Cabincr3w Disbands"; 17 APR 2012; www.dailydot.com/news/anonymous-offshoot-cabincr3w-disbands/; accessed on 09 MAY 2014; Article.
[19] (U); Ragan, Steve; *Security Week*; "AntiSec Targets Michigan Law Enforcement Agency"; 16 APR 2012; www.securityweek.com/antisec-targets-michigan-law-enforcement-agency; accessed on 08 MAY 2014; Article.
[20] (U); Kouvacs, Eduard; *SOFTPEDIA*; "AntiSec Hackers Leak 40 GB of Data from Lake County Sheriff's Office"; 28 APR 2012; www.news.softpedia.com/news/AntiSec-Hackers-Leak-40-GB-of-Data-from-Lake-County-Sheriff-s-Office-266784.shtml; accessed on 07 MAY 2014; Article.
[21] (U); *Newsnet5 Cleveland*; "Anonymous claims responsibility for taking down Cleveland's website after Tamir Rice shooting"; 24 NOV 2014; www.newsnet5.com/news/local-news/cleveland-metro/anonymous-claims-responsibility-for-taking-down-Clevelands-website-after-Tamir-Rice-shooting; accessed on 27 APR 2015; Article.
[22] (U); WKOW.com; "UPDATED: A group called Anonymous claim responsibility for cyber attack"; 25 MAR 2015; http://www.wkow.com/story/28325831/2015/03/09/emergency-government-systems-in-dane-county-threatened-by-cyber-attack; accessed on 16 APR 2015; Article.
[23] (U); WKOW.com; "UPDATED: A group called Anonymous claim responsibility for cyber attack"; 25 MAR 2015; http://www.wkow.com/story/28325831/2015/03/09/emergency-government-systems-in-dane-county-threatened-by-cyber-attack; accessed on 16 APR 2015; Article.
[24] (U); Jeremy Brilliant; *WTHR*; "Hackers target Indianapolis 911 center"; 16 FEB 2015; http://www.wthr.com/story/27897557/hackers-target-indianapolis-911-center; accessed on 16 APR 2015; Article.

[25] (U); DHS; iSIGHT Partners; Threat Analysis Report; INTEL-1162876; 5 NOV 2014; DOI UNK; "CryptoWall Characteristics, Operations and Outlook"; Extracted information is UNCLASSIFIED; Overall Classification is UNCLASSIFIED.
[26] (U); MS-ISAC; FA-20140515; 28 MAY 2015; DOI UNK; "Forensic Analysis Report: Mineral County Sheriff, NV"; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.
[27] (U); MS-ISAC; FA-20140515; 28 MAY 2015; DOI UNK; "Forensic Analysis Report: Village of Pleasant Prairie"; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.
[28] (U); MS-ISAC; FA-20140515; 28 MAY 2015; DOI UNK; "Forensic Analysis Report: Mineral County Sheriff, NV"; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.
[29] (U); MS-ISAC; FA-20140515; 28 MAY 2015; DOI UNK; "Forensic Analysis Report: Village of Pleasant Prairie"; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.
[30] (U); MS-ISAC; FA-20140515; 28 MAY 2015; DOI UNK; "Forensic Analysis Report: Mineral County Sheriff, NV"; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.
[31] (U); MS-ISAC; FA-20140515; 28 MAY 2015; DOI UNK; "Forensic Analysis Report: Village of Pleasant Prairie"; Extracted information is UNCLASSIFIED; Overall document classification is UNCLASSIFIED.
[32] (U//FOUO); DHS; NCRIC/CIN/OCIAC; Joint Situational Advisory; 10 JUN 2014; DOI UNK; (U//FOUO); "New Ransomware 'CryptoWall' Rapidly Infecting Systems Across the United States"; Extracted information is U//FOUO; Overall document classification is U//FOUO.
[33] (U//FOUO); DHS; NCRIC/CIN/OCIAC; Joint Situational Advisory; 10 JUN 2014; DOI UNK; (U//FOUO); "New Ransomware 'CryptoWall' Rapidly Infecting Systems Across the United States"; Extracted information is U//FOUO; Overall document classification is U//FOUO.
[34] (U); Jackson, William; GCN; "Phone DoS Attacks in Extortion Scam Target Government Offices"; 03 APR 2013; www.gcn.com/articles/2013/04/03/phonedos-attacks-extortion-scam-target-gov-offices.aspx; accessed on 14 MAY 2014; Article.
[35] (U//FOUO); DHS; IIR 4 014 0006 14; 271740Z MAR 14; DOI 24 FEB 2014; (U//FOUO); IIR 4 014 0006 14/OH - TELEPHONY DENIAL OF SERVICE (TDoS) Attack Against An Ohio Community Hospital Disrupts Emergency Room Communications; Extracted information is U//FOUO; Overall document classification is U//FOUO.
[36] (U); KOMO Staff; *KOMOnews.com*; "Security Breach Exposes 6,000 King County Medical Records"; 13 JAN 2014; www.komonews.com/news/local/Security-breach-exposes-6000-King-Co-medical-records-240033631.html; accessed on 21APR 2014; Article.
[37] (U); Kottke, Colleen; *FDL Reporter*; "Fond du Lac Police Twitter Account Hacked"; 30 SEP 2013; www.fdlreporter.com/article/20130930/FON0101/309300245/?nclick_check=1; accessed on 23 APR 2014; Article.
[38] (U); Zetter, Kim; *Wired*; "This Is Not a Test: Emergency Broadcast Systems Proved Hackable"; 12 JUL 2013; www.wired.com/threatlevel/2013/07/eas-holes/; accessed on 25 APR 2014; Article.
[39] (U); Ollmann, Gunter; *Dark Reading*; "Hacking the Emergency Alerting System: More EAS Devices Vulnerable Now Than When Vendors were Alerted in January"; 15 JUL 2013; www.darkreading.com/attacks-breaches/hacking-the-emergency-alerting-system/d/d-id/1140113; accessed on 24 APR 2014; Article.
[40] (U); Greenberg, Adam; *SC Magazi*ne; "Alerts of "Rising Dead" Still Exploitable on EAS"; 18 OCT 2013; www.scmagazine.com/alerts-of-rising-dead-still-exploitable-on-eas/article/316996/; accessed on 25 APR 2014; Article.
[41] (U); Zetter, Kim; *Wired*; "This Is Not a Test: Emergency Broadcast Systems Proved Hackable"; 12 JUL 2013; www.wired.com/threatlevel/2013/07/eas-holes/; accessed on 25 APR 2014; Article.
[42] (U); *Toledo News Now*; "NORIS Computer System Shut Down over Virus"; 24 FEB 2012; www.toledonewsnow.com/story/17011513/noris-computer-system-shut-down-over-virus; accessed on 26 APR 2014; Article.
[43] (U); *Toledo News Now*; "NORIS Computer System Shut Down over Virus"; 24 FEB 2012; www.toledonewsnow.com/story/17011513/noris-computer-system-shut-down-over-virus; accessed on 26 APR 2014; Article.
[44] (U); MS-ISAC; "Protect Yourself from Email Phishing Attacks"; APR 2013; http://msisac.cisecurity.org/newsletteres/2013-04.cfm; accessed 24 JUN 2015; Cybersecurity tips newsletter.
[45] (U); DHS; US-CERT; Alert TA14-295A; "Crypto Ransomware"; 22 OCT 2014; https://www.us-cert.gov/ncas/alerts/ta14-295A; accessed 24 JUN 2015; Alert.