Homeland Security

Daily Open Source Infrastructure Report 17 October 2012

Top Stories

- A federal cybersecurity team warned of critical vulnerabilities in computerized control systems that attackers could exploit to sabotage or steal sensitive data from operators of the solar arrays that generate electricity in homes and businesses. – *Ars Technica* (See item **1**)
- Officials in Burlington, Washington, notified hundreds of employees and residents that their names, bank account information, and routing numbers were compromised the week of October 8 when hackers broke into city systems and stole more than $400,000 from the city's account at Bank of America. – *Computerworld* (See item **6**)
- Hackers managed to gain access to the records of at least 8,500 current and former University of Georgia employees. The university's representatives began investigating the breach October 1, after they learned the cybercriminals obtained unauthorized access through the accounts of two employees. – *Softpedia* (See item **23**)
- Researchers from Symantec reported that cybercriminals are trying to spread malware disguised as Windows help files in attacks targeting government and industry sectors. – *Softpedia* (See item **26**)

Energy Sector

1. *October 15, Ars Technica* – (National) **Solar panel control systems vulnerable to hacks, feds warn.** DHS is warning of critical vulnerabilities in a computerized control system that attackers could exploit to sabotage or steal sensitive data from operators of the solar arrays that generate electricity in homes and businesses, Ars Technica reported October 15. A slew of vulnerabilities in a variety of products, including the Sinapsi eSolar Light Photovoltaic System Monitor and the Schneider Electric Ezylog Photovoltaic Management Server, allow unauthorized people to remotely log into the systems and execute commands, warned the Industrial Controls Systems Cyber Emergency Response Team in a recent alert. Other vulnerable devices include the Gavazzi Eos-Box and the Astrid Green Power Guardian. Proof-of-concept code available online makes it easy to exploit some of the bugs. The advisory is based on a report published in September that disclosed SQL injection vulnerabilities, passwords stored in plain text, hard-coded passwords, and other defects that left the devices open to tampering. According to researchers, the vulnerable management server is incorporated into a photovoltaic products from several manufacturers. "All the firmware versions we analyzed have been found to be affected by these issues," the researchers wrote. "The software running on the affected devices is vulnerable to multiple security issues that allow unauthenticated remote attackers to gain administrative access and execute arbitrary commands," the researchers said.
Source: http://arstechnica.com/security/2012/10/solar-panel-control-systems-vulnerable-to-hacks/

For another story, see item **38**

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials and Waste Sector

2. *October 16, Nuclear Power International* – (Illinois) **Exelon begins transformer replacement at Illinois nuclear power plant.** Plant operator Exelon said two main power transformers will be replaced during Braidwood Station's refueling outage that began October 15. The Braidwood Generating Station in Will Township, Illinois, houses two reactors that generate about 2,300 MW. The transformers will be replaced as part of the station's long-term equipment reliability plan, an approach to replace major equipment before it reaches the end of its service life, Exelon said. Along with the transformer replacement, employees and supplemental workers will complete more than 13,000 tasks during the outage. The work includes performing maintenance activities and upgrading plant equipment.

Source: http://www.power-eng.com/articles/2012/10/exelon-begins-transformer-replacement-at-illinois-nuclear-power-plant.html

[Return to top]

Critical Manufacturing Sector

3. *October 16, U.S. Department of Transportation* – (National) **NHTSA recall notice - Ford Fiesta side air bags.** Ford announced October 16 the recall of 154,604 model year 2011-2013 Fiesta vehicles, manufactured from November 3, 2009 through September 21, 2012. The vehicles fail to comply with Federal Motor Vehicle Safety Standard (FMVSS) No. 208, "Occupant Crash Protection." The passenger side curtain air bag will not deploy in the event of a side impact collision when the front passenger seat is empty. Although the side curtain air bag system was designed to suppress the side curtain air bag under this scenario, that information is not explained in the owner's guide for these vehicles as required by FMVSS No.208. An occupant in the right rear seating position will not have coverage from the side curtain air bag in a side impact collision when the front passenger seat is empty, increasing the risk of injury to the right rear occupant. Ford will notify owners, and dealers will reprogram the vehicle's software free of charge so that it no longer suppresses the passenger side curtain air bag when the front passenger seat is empty.
   Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V488000&summary=true&prod_id=942768&PrintVersion=YES

4. *October 15, Rochester Democrat and Chronicle* – (New York) **OSHA cites Crosman for 23 alleged safety violations.** Crosman Corp, a manufacturer located in Bloomfield, New York, is facing proposed fines of $148,000 stemming from inspections conducted after an employee's finger was allegedly cut off by a machine in March, the Rochester Democrat and Chronicle reported October 15. The company makes airguns, rifle scopes, sights, and archery products. The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) cited Crosman for 23 alleged serious and repeat violations of workplace safety. OSHA inspectors found that procedures were not used to prevent a mechanical press from turning on while the worker was setting it up, which resulted in the amputation. The citations included 21 serious violations involving numerous machine and electrical hazards, in addition to missing guardrails on elevated areas, damaged and unstable metal storage racks, a buildup of combustible residue, and a lack of eye flushing facilities for employees working with corrosives, according to OSHA documents. OSHA also issued citations for two repeat violations: Letting lead to accumulate on surfaces, and failing to develop written procedures to make sure machines do not power up while employees are setting them up.
   Source: http://www.democratandchronicle.com/article/20121015/BUSINESS/310150043/osha-crosman?odyssey=nav|head

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

5. *October 15, WNBC 4 New York* – (New York) **FBI arrests man accused of stuffing ATMs with fake cash.** A man was arrested October 15 in connection with the counterfeit bills dispensed at two ATMs in New York City the week of October 8, authorities said. The man was arrested at Kennedy Airport after voluntarily returning to New York City from the Dominican Republic, the FBI said. He worked for a company that serviced the ATMs. He faces several charges, including embezzlement and other charges related to counterfeit currency. The amateurish fake bills were put in ATMs at two Chase branches in Manhattan to replace cash that had been stolen. The banks were short a total of some $11,000. The counterfeit bills were blank on one side. Authorities believe they were meant to trick the ATM into believing it was carrying a full complement of cash. A bank official said that the machines were able to distinguish most of the fake bills from real ones.
   Source: http://www.nbcnewyork.com/news/local/Counterfeit-ATM-Bills-Arrest-Midtown-Chase-Gene-Carlo-Pena-JFK-FBI-174268821.html

6. *October 15, Computerworld* – (Washington) **Cyberthieves loot $400,000 from city bank account.** Burlington, Washington officials notified hundreds of employees and residents that their bank account information was compromised the week of October 8 when hackers broke into city systems and stole more than $400,000 from a city account at Bank of America. Among those impacted by the breach were employees participating in Burlington’s electronic payroll deposit program and utility customers enrolled in the city’s autopay program. In an alert issued October 15, a city administrator said all autopay customers should assume that their name, bank account number, and routing number were comprised. He urged affected customers to immediately contact their bank to flag or close their accounts. All employees participating in the city’s electronic payroll deposit program were also asked to close out their old accounts and establish a new one as a result of the breach. The city first learned of the online heist October 11 when an east coast bank sought information about a series of suspicious transfers from a Burlington city account. The city immediately reviewed the activity and noticed at least three “significant transactions” from its Bank of America account to accounts at the east coast bank over a two-day period, the administrator said. The theft was from an account containing more funds, but the administrator said the city did not know why more was not taken. The account was frozen and all of the city’s money was temporarily moved out of Bank of America as a precaution. The Burlington theft came just days after security firm RSA warned of cybercriminals plotting a massive and concerted campaign to steal money from the online accounts of thousands of consumers at 30 or more major U.S. banks.
   Source:

http://www.computerworld.com/s/article/9232372/Cyberthieves_loot_400_000_from_city_bank_account

7. *October 15, Associated Press* – (Texas) **Ex-Houston attorney pleads guilty in Ponzi scheme.** A former attorney in Houston who portrayed himself as a real estate investment tycoon pleaded guilty in a $7.8 million Ponzi scheme, the Associated Press reported October 15. Federal prosecutors in Houston said the man pleaded guilty to wire fraud. Investigators said more than 20 investors were scammed. Prosecutors said the man during the past 10 years pretended to be in the real estate investment business. He used money from investors to pay his previous debts and fund his personal lifestyle. Source: http://www.businessweek.com/ap/2012-10-15/ex-houston-attorney-pleads-guilty-in-ponzi-scheme

8. *October 13, Lincoln Journal Star* – (National) **Former Cornhusker owner indicted on fraud charges.** A Boca Raton, Florida man who formerly owned several lodging properties was indicted by a federal grand jury in Illinois on 10 counts of fraud and making false statements to lenders, the Lincoln Journal Star reported October 13. The hotel owner and another Floridian are accused of using about $9 million in bank loans to refinance and remodel hotels that the owner's Shubh Hotels owned in Cincinnati, Ohio, and Boca Raton, Florida, for purposes other than those the bank intended. The hotel owner also owned hotels in Detroit, Michigan, Pittsburgh, Pennsylvania, and Lincoln, Nebraska. The indictment said the two men created false invoices in the name of the latter's remodeling firm and used false documentation of supplies to get money from the lenders that ended up in accounts they controlled at other banks. The hotel owner borrowed money in 2007 from two banks in Illinois that later failed due to bad loans.
Source: http://journalstar.com/business/local/former-cornhusker-owner-indicted-on-fraud-charges/article_c7556967-03a0-5acc-80dd-bb2c02984950.html

[Return to top]

Transportation Sector

9. *October 16, Aiken Standard* – (South Carolina) **Interstate 520 reopens after tanker truck overturns.** Interstate 520 reopened October 15 after a tanker truck filled with liquid nitrogen overturned, according to the South Carolina State Highway Patrol. The wreck happened in the westbound lanes of I-520 near Ascauga Lake Road and the I-20 interchange, and shut down traffic in both directions for about 8 1/2 hours in Aiken County. The truck exited the left side of the roadway and struck the guardrail, according to a State Highway Patrol representative. The truck re-entered the roadway and then traveled back into the median and overturned, he said. According to lieutenant of the North Augusta Department of Public Safety, the truck was carrying a full load of liquid nitrogen, but the liquid nitrogen did not leak. There were no other vehicles involved, and the cause of the crash was still under investigation. Authorities evacuated everything within a half-mile radius, including the Department of Motor Vehicles office and a gas station, and the evacuation was lifted about 3 hours after the incident. The driver was trapped inside the truck and had to be extricated by rescue crews. He

was taken to a hospital with non-life-threatening injuries. There were no other vehicles involved, and the cause of the crash was still under investigation.
Source:
http://www.aikenstandard.com/article/20121016/AIK0101/121019626/1004/interstate-520-reopens-after-tanker-truck-overturns

10. *October 16, KIRO 7 Seattle* – (Washington) **Driver of pickup dies in crash with Amtrak train.** Police were investigating a deadly train crash after an Amtrak train collided with a pickup in Pierce County, Washington, KIRO 7 Seattle reported. The train was headed from Seattle to Eugene when it crashed about 19 miles south of Tacoma October 15. After the crash, the train stopped on the track between DuPont and Steilacoom, and arrived in Lacey about 4 hours late. A spokesman for Burlington Northern Santa Fe said the truck was on the tracks about 40 yards north of the crossing at Solo Point. Amtrak said none of the 153 passengers and crew members aboard the train were hurt. Several other trains were delayed by the crash but service has since returned to normal.
Source: http://www.kirotv.com/news/news/driver-pickup-dies-crash-amtrak-train/nSdxH/

11. *October 15, Associated Press* – (Alaska) **Bad joke prompts Alaska airport evacuation.** The main terminal of Anchorage, Alaska's largest airport was evacuated for 2 hours October 14 after a man made comments about a bomb, which he later said were meant to be taken as a joke. Police at Ted Stevens Anchorage International Airport took the matter seriously and arrested on charges of making terroristic threats and disorderly conduct. The man was jailed with bail set at $5,000, an airport manager said by email. "That caused us and the airlines, the TSA, the airport police, to have to evacuate the building, the terminal," he said. Airport shuttle buses took passengers to another terminal. Police set up a roadblock on a street leading to the airport to prevent drivers from getting to the terminal. That created a long stretch of traffic along Anchorage's International Airport Road.
Source: http://www.kimatv.com/news/national/Bad-joke-prompts-Alaska-airport-evacuation-174202131.html

[Return to top]

Postal and Shipping Sector

12. *October 15, San Jose Mercury-News* – (California) **Hazmat teams search UPS truck after driver becomes ill.** After a delivery truck driver became sick October 15 outside a Fremont, California tech business, HAZMAT crews searched his vehicle and found a package with a toxic substance that could be the source of his illness. The package containing xylene, a toxic and flammable substance often used as a solvent, gave off a small contamination reading inside the cab of the vehicle, and a larger reading inside the cargo area, said the Fremont Fire battalion chief. Crews were dispatched after the driver called 9-1-1 to complain of nausea, chest tightness, and irritated eyes while making his deliveries. The UPS driver was taken to the hospital to be evaluated for his symptoms. Fire crews called in a special operations team and about 10 HAZMAT

specialists suited up in Level C protection gear to search the truck for a possible gaseous substance. The package was removed from the truck, sealed off, and taken away.
Source: http://www.mercurynews.com/breaking-news/ci_21777502/fremont-hazmat-teams-search-ups-truck-after-driver

[Return to top]

Agriculture and Food Sector

13. *October 15, U.S. Department of Agriculture Food Safety and Inspection Service* – (Louisiana; Texas) **Texas firm recalls beef and pork products produced without benefit of inspection and misbranding.** October 15, Lao Chareune Foods of Dallas recalled approximately 8,200-pounds of various beef and pork products because they were produced without being federally inspected and were misbranded. Recalled products include the "Pork Snack Stick," "Seasoned Fried Beef," "Fried Pork Skins," and "Sliced Fried Pork Ears." Each package bears the establishment number "EST. 13479" inside the United States Department of Agriculture mark of inspection. There were no printed production or expiration dates. The pork snack stick was also misbranded in that it is raw and as such cannot be labeled as a snack stick. The products were produced beginning May 22, 2012, and distributed to retail establishments in Louisiana and Texas.
Source:
http://www.fsis.usda.gov/News_&_Events/Recall_066_2012_Release/index.asp

14. *October 15, U.S. Food and Drug Administration* – (National) **Mondelez Global LLC conducts voluntary U.S. recall of Green & Black Organic Peanut and Sea Salt Milk Chocolate Bar due to possible health risk.** Mondelez Global LLC announced a voluntary national recall of the Green & Black's Organic Peanut & Sea Salt Milk Chocolate Bar, the U.S. Food and Drug Administration reported October 15. The product contains peanuts, supplied by Sunland, Inc., which may be contaminated with Salmonella. The product bears the UPC 708656100562, includes all best by dates, and was distributed to retail and specialty stores nationwide.
Source: http://www.fda.gov/Safety/Recalls/ucm324043.htm

15. *October 15, U.S. Food and Drug Administration* – (National) **Hines Nut Company, Dallas, TX announces voluntary recall of Salted Jumbo Virginia In-Shell Peanuts due to possible health risk.** Hines Nut Company Inc., of Dallas, announced a voluntary recall of its Salted Jumbo Virginia In-Shell Peanuts October 15. The peanuts were processed by Sunland, Inc. and may be contaminated with Salmonella. The product was distributed nationally to numerous large supermarket, grocery, and retail chains under the Hines or Dollar General Clover Valley label. The peanuts have best by/expiration dates from October 12, 2012, through August 27, 2013. The affected products have various packaging and includes 43 lot numbers.
Source: http://www.fda.gov/Safety/Recalls/ucm323984.htm

16. *October 11, U.S. Food and Drug Administration* – (National) **Super Store Industries recalls Lovin' Scoopful Ice Cream - Super Duper Peanut Butter Cup because of possible health risk.** Super Store Industries of Turlock, California, recalled its Lovin' Scoopful Ice Cream — Super Duper Peanut Butter Cup, October 11, due to a potential Salmonella contamination from Sunland, Inc. ingredients. The ice cream has a best by date of October 24, 2012, and was distributed at Albertsons retail stores in Oregon, Utah, Washington, Idaho, and Montana. It was also distributed to Walmart stores in Washington.
    Source: http://www.fda.gov/Safety/Recalls/ucm323942.htm

[Return to top]

Water Sector

17. *October 16, Charlotte Observer* – (North Carolina) **Arsenic in Mountain Island Lake, study says.** A Duke University-led study of coal ash contaminants, published October 15, found high levels of toxic arsenic in Mountain Island Lake, North Carolina. The study reported ash contaminants downstream of coal-fired power plant ash settling ponds in the 11 lakes and rivers sampled. It was published in the journal Environmental Science & Technology. Concentrations tended to be highest in small bodies of water, such as 2,914-acre Mountain Island Lake. Water flowing into the lake from the Riverbend power plant's ash ponds had arsenic concentrations up to nine times higher than the federal drinking water standard, the study said. It also found arsenic at levels that could harm aquatic life in water at the lake bottom. That suggests arsenic could accumulate in fish tissue, said a Duke scientist, who contributed to the study. The findings did not surprise Mecklenburg County water quality officials. The county sampled lake water near the Riverbend discharge point eight times a year since mid-2009, and detected arsenic above the state water quality standard five times, said a water quality official. Concentrations have been up to three times higher than the State standard. The Duke study also found high levels of contamination in the French Broad River in Asheville, and in Hyco and Mayo lakes near the Virginia line. Lakes Norman and Wylie were among other water bodies studied.
    Source: http://www.charlotteobserver.com/2012/10/16/3600452/arsenic-in-mountain-island-lake.html

18. *October 16, KTTN 92.3 FM Trenton/KGOZ 101.7 FM Gallatin* – (Missouri) **Gilman City placed under boil water advisory.** A precautionary boil water advisory was in effect for Gilman City, Missouri, until further notice, KTTN 92.3 FM Trenton/KGOZ 101.7 Gallatin reported October 16. The utilities superintendent said that a lightning strike October 13 damaged a Gilman City water main midway between Gilman City and Coffey, leading to the water tower being drained and a water outage for Gilman City. Repairs were made, but samples of water would need to be tested to determine whether the water was safe to drink and use for cooking. Lightning split a Farmer's Electric pole and apparently moved down a ground wire, blowing a four-foot section from the water main. Water line flushing was conducted, but water samples must be tested before the boil advisory is lifted for Gilman City. Gilman City receives its water from Harrison County Public Water Supply District Two. The district itself does not

have a boil advisory. The line damaged by lightning was a Gilman City main.
Source: http://www.kttn.com/kgozfm/modules/news/article.php?storyid=8425

19. *October 16, Cape Girardeau Southeast Missourian* – (Illinois) **Cairo water flowing again, but boil order in effect.** Water service was restored to Cairo, Illinois, October 15, after the dropping Ohio River started to cause service interruptions October 13, but a boil-water order remains in effect. Full water service was restored after crews worked through October 14, said a spokeswoman for Illinois American Water, which manages the city's water system. Water service was out for some customers, while others experienced low pressure after the Ohio River, from which the system gets its water, dropped 3-4 feet in a 48-hour period. The water service problems caused the Cairo school district to close October 15, but classes were expected to resume October 16, a receptionist at the district office said. During the service interruptions, Illinois American brought in a tanker truck, bottled water, and provided portable toilets to help those without water. A boil-water order remains in effect, which is required any time water pressure drops below a certain level. The spokesman said water customers would be notified when the order is lifted.
Source: http://www.semissourian.com/story/1903876.html

20. *October 16, Associated Press* – (Iowa) **Water alert issued for 2 Iowa cities.** Residents of Fontanelle in southwest Iowa and part of Walford, near Cedar Rapids, were asked to boil their drinking water for now, the Associated Press reported October 16. The Iowa Department of Natural Resources said a break in a large water main in Fontanelle left the city without water. Crews worked October 15 to repair the break and restore service. Breaks in pipes can allow contaminants to enter the water system. In Walford, water samples taken during routine testing in the Clover Ridge Subdivision tested positive for E. coli bacteria. Three out of four subsequent samples taken October 11 tested positive for total bacteria, but did not contain E. coli. The subdivision plans to chlorinate the wells and retest the water.
Source: http://www.kwqc.com/story/19828754/water-alert-issued-for-2-iowa-cities

For another story, see item **34**

[Return to top]

Public Health and Healthcare Sector

21. *October 15, Associated Press* – (Indiana) **Ind. doctor nabbed in Italy gets 7 years in prison.** A former Indiana surgeon arrested on a snowy Italian mountainside after five years on the run was given a seven-year prison term, nearly double the recommendation under federal sentencing guidelines, October 12 for billing insurers and patients for procedures he did not perform. The U.S. district judge said the more severe sentence was necessary because the surgeon — who disappeared just before he was charged — left a web of lawsuits, 401(k) problems for his 40 employees, and health issues for patients at his nose and sinus clinic. "The fallout from this is enormous," the judge said, noting that hundreds of patients could not access their medical records after the surgeon fled while vacationing in Greece.

Source: http://www.seattlepi.com/news/article/Ind-doctor-nabbed-in-Italy-gets-7-years-in-prison-3941740.php

For another story, see item **40**

[Return to top]

Government Facilities Sector

22. *October 16, Calaveras Enterprise* – (California) **Suspicious package found at government center.** A suspicious package found October 15 near a bus stop at the Calaveras County Government Center in California caused the Sheriff's Office to shut down the main entryway and deploy the bomb squad as a precautionary measure. The squad used a robot to get a closer look at the package, and it was X-rayed to see what was inside. A sheriff's deputy said the contents were suspicious enough for it to be destroyed on scene instead of removed. Shortly after the package was found and destroyed, the main entryway to the government center had reopened, but the bomb squad was still working in the area where the package was found surrounded by caution tape.
    Source: http://www.calaverasenterprise.com/news/article_f85378de-171b-11e2-a7da-0019bb2963f4.html

23. *October 16, Softpedia* – (Georgia) **University of Georgia hacked, at least 8,500 employees exposed.** Hackers managed to gain access to the records of at least 8,500 current and former University of Georgia employees, Softpedia reported October 16. The cybercriminals obtained access to the accounts of two employees who worked in "sensitive information technology positions." From there, the attackers were able to gain access to the details of thousands of employees, including names, Social Security numbers, and other information, University of Georgia Today reported. The university's representatives began investigating the breach October 1, after they learned the passwords of two employees were reset by an unknown actor. It was later determined that the intrusion could have occurred as early as September 28. It is believed the hackers might have been able to reset the passwords by guessing the answers to the secret questions set by the targets. All the affected individuals were notified and those who request it will benefit from credit monitoring services. The police were contacted to investigate the incident.
    Source: http://news.softpedia.com/news/University-of-Georgia-Hacked-At-Least-8-500-Employees-Exposed-299800.shtml

For more stories, see items **6** and **19**

[Return to top]

Emergency Services Sector

24. *October 16, Beckley Register-Herald* – (West Virginia) **Clear Creek fire station burglarized, vandalized.** Clear Creek, West Virginia volunteer firefighters spent

October 15 testing equipment and cleaning up the mess left when their station was broken into sometime between October 12 and October 14. The Raleigh County sheriff said someone forced their way through the firehouse door and stole equipment and assorted tools. They also took other items they thought would contain money, he said. The most troubling aspect of the break-in is that the station was vandalized. Equipment and supplies from the fire trucks and ambulance were left strewn around the station. By October 15, the Clear Creek fire chief confirmed the station was ready to respond to calls. After an inventory, the fire chief said nearly $1,300 worth of items were stolen.
Source: http://www.register-herald.com/todaysfrontpage/x699438932/Clear-Creek-fire-station-burglarized-vandalized

25. *October 15, WBOY 12 Clarksburg* – (West Virginia) **Harrison County man arrested after threatening to shoot officers.** Clarksburg, West Virginia law enforcement agencies were put on notice October 13, after a man told his family members that he wanted to shoot officers or be shot by them. His family members called the Harrison County Sheriff's department and reported that he took a shotgun and their 2002 Chevy Venture van without permission. They said when he left he was threatening to shoot officers, and said he wanted to be shot by them. The man was later stopped near the I-79 and U.S. Route 50 interchange. He is in jail, charged with petit larceny, theft of a vehicle, and driving with suspended license. His bail was set at $6,000.
Source: http://www.wboy.com/story/19816274/harrison-county-man-arrested-after-threatening-to-shoot-officers

[Return to top]

Information Technology Sector

26. *October 16, Softpedia* – (International) **Windows Help files used in attacks against industry and government sectors.** To make sure their potential victims do not suspect they are the targets of an attack, cybercriminals often rely on harmless-looking Windows Help files (.hlp) to spread pieces of malware. Symantec reports that in the past period, cyberattacks using this attack vector have been aimed at government and industry sectors. According to researchers, everything starts with a simple email which informs the recipient of a "White Paper on corporate strategic planning." In reality, the attachment is not a white paper, but a cleverly designed Windows Help file. The Help file's functionality permits a call to the Windows API, which allows the attacker to execute code and install other malicious elements. Experts emphasize the fact that this functionality exists by design, it is not an exploit. In the attacks identified so far, cybercriminals were trying to spread Trojan.Ecltys and Backdoor.Barkiofork — pieces of malware often utilized in targeted attacks against government agencies and the industry sector. Most of the threats have been identified in the United States, China, India, and France.
Source: http://news.softpedia.com/news/Windows-Help-Files-Used-in-Attacks-Against-Industry-and-Government-Sectors-299782.shtml

27. *October 16, Softpedia* – (International) **Steam browser protocol flaws allow cybercriminals to execute malicious commands.** Two security researchers from

ReVuln identified a vulnerability in the Steam Browser Protocol that could be leveraged by remote attackers to cause damage. Their research was published in a paper called Steam Browser Protocol Insecurity. The popular gaming platform uses the steam:// URL protocol in order to run, install, and uninstall games, backup files, connect to servers, and reach various sections dedicated to customers. After testing various browsers, the experts concluded that Mozilla and Safari are perfect for the "silent Stream Browser Protocol calls" needed to perform such an attack because they do not warn users before executing the external URL handler. Internet Explorer and Opera do warn users, but the "dodgy part" of the URL can be hidden by adding spaces into the steam:// URL. The researchers found that not only these Web browsers can be utilized for the calls to external protocol handlers. Steam browser and RealPlayer's embedded browser are just as susceptible to an attack. One of the attacks they demonstrated relies on the retailinstall command that designed for installing and restoring backups from a local folder. A function that is in charge of loading a splash image during this process contains an integer overflow vulnerability which could be leveraged by an attacker to run his malicious scripts. Furthermore, the researchers showed that the Steam Browser Protocol can also be used in attacks against the Source and Unreal engines. Massive multiplayer online games can be exploited via the auto-update features by leveraging a directory traversal vulnerability.
Source: http://news.softpedia.com/news/Steam-Browser-Protocol-Flaws-Allow-Cybercriminals-to-Execute-Malicious-Commands-299598.shtml

28. *October 15, Threatpost* – (International) **Oracle patch update to include 109 patches.** Oracle's quarterly Critical Patch Update, October 16 included 109 fixes. The company released fixes for security vulnerabilities across most of its enterprise products, addressing a host of remotely exploitable flaws. This comes a little more than a month after exploits of a serious zero-day vulnerability in Java were reported, as well as a critical zero-day vulnerability in Java SE. Five patches were released addressing security problems in Oracle Database Server, including one that is remotely exploitable over a network without the need for a username and password, Oracle said. Two of the patches address client-only installations.
Source: http://threatpost.com/en_us/blogs/oracle-patch-update-include-109-patches-101512

29. *October 15, Dark Reading* – (International) **Next-generation malware: Changing the game in security's operations center.** Sophisticated, automated malware attacks are spurring enterprises to shift their security technology and staffing strategies. In many new cases, augmentations to malware involves no human author, rather, it is being created by an automated program that continually tweaks known attacks in new ways, so that it will not be recognized by antivirus or intrusion prevention systems. Antivirus (AV) systems work by identifying malware through a blacklist — a database of known viruses, trojans, and other malicious code — and blocking and eradicating any code on the list. The premise of AV technology is that it is possible to identify the unique characteristics of any known malware — its "signature" — and use that signature to prevent it from penetrating the enterprise. However, with new "zero-day" malware being created constantly, AV systems often cannot keep up, and their blacklists have become bloated and slow to perform. This growing problem has spurred many vendors

— and many enterprises — to begin looking for ways to recognize malware not by how it looks — its known signature — but by how it behaves.
Source: http://www.darkreading.com/security-monitoring/167901086/security/security-management/240009058/next-generation-malware-changing-the-game-in-security-s-operations-center.html

30. *October 15, Softpedia* – (International) **Fake DHL Express Tracking Notifications bring 'good' news and malware.** A DHL Express Tracking Notification is making the rounds, landing in the inboxes of users in an attempt to trick them into infecting their computers with a piece of malware. Although DHL is one of the most commonly utilized brands by cybercriminals in their malicious campaigns, fake notifications that rely on the company's name still appear to be a success. The latest malware attack relies on emails entitled "Processing complete successfully," which urge recipients to open an attached file in order to see additional details. As in all similar schemes, the file (DHL_Express_Processing_ complete.pdf.zip) is not a detailed report, but a piece of malware identified by Sophos as Troj/BredoZp-S.
Source: http://news.softpedia.com/news/Fake-DHL-Express-Tracking-Notifications-Bring-Good-News-and-Malware-299466.shtml

31. *October 15, Softpedia* – (International) **Cybercriminals update the eBay logo in their phishing scams.** In order to ensure their malicious campaigns record a success, cybercriminals must always keep up with the changes made by the companies whose names and reputations they leverage. That is exactly what a group in charge of an eBay phishing scam did. eBay recently changed its logo and while the new one is not completely different compared to the old one, this minor detail can make the difference between a successful and an unsuccessful phishing scheme. If a user sees that it bears the old logo, it is probably a scam. However, users should still be cautious when clicking on shady links, since most criminals will surely update their pages in the upcoming period.
Source: http://news.softpedia.com/news/Cybercriminals-Update-the-eBay-Logo-in-Their-Phishing-Scams-299482.shtml

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: https://www.it-isac.org

[Return to top]

Communications Sector

Nothing to report

[Return to top]

Commercial Facilities Sector

32. *October 16, Detroit News* – (Michigan) **4 seniors hospitalized in downtown high-rise fire.** One person suffered minor burns and three others were taken to a hospital October 15 after a fire at a downtown Detroit senior high-rise apartment. Residents were evacuated from the Griswold Building Senior Apartments after the fire was reported, fire officials said. The fire, which started in a sixth-floor apartment, was downgraded from a second-alarm to a first-alarm fire within 30 minutes. Most residents were cleared to return to the building after four hours. No other major injuries were reported. The Southeastern Michigan Region Red Cross provided shelter to six residents whose apartments had water damage. Fire authorities investigated the cause of the blaze. Arson investigators were expected to survey the scene.
    Source:
    http://www.detroitnews.com/article/20121016/METRO01/210160373/1409/metro/4-seniors-hospitalized-downtown-high-rise-fire

33. *October 16, Associated Press* – (Kentucky) **Former segregated school destroyed by fire.** A black history museum located in a formerly segregated school burned and a county official suspects the fire was intentionally set. WCPO 9 Cincinnati reported the Grant County Black History Museum in Kentucky was destroyed and a nearby church was damaged in the blaze October 14. The Grant County Parks and Recreation director said the fire was a "senseless crime" and said every effort will be made to find whoever is responsible. The museum was formerly the Dry Ridge Consolidated Colored School, which closed in 1958 when Grant County School integrated.
    Source: http://www.lex18.com/news/former-segregated-school-destroyed-by-fire

34. *October 15, Associated Press* – (Mississippi) **Sewage discharge closes part of Biloxi beach.** A sewage discharge closed several miles of beach in Biloxi, Mississippi, over the weekend of October 13. A brief power failure October 13 caused the discharge at a pump station, the public works director said October 14. He did not know what caused the power failure. Sewage entered the storm drains and discharged along the beach, according to the Mississippi Department of Environmental Quality (MDEQ). The public works director said a vacuum truck was sent out immediately, and the beach was closed as a precaution. Sewage "didn't get onto the beach itself. But there's probably a drain down the road it might have reached," he said. MDEQ closed the beach from Mockingbird Lane to Edgewater Drive, and said it would lift the closure when test indicated the water is safe. That would take more than 24 hours from the October 13 notification. Experts were working out how much sewage was discharged, but at estimated it might have been 1,000 to 2,000 gallons.
    Source: http://www.katc.com/news/sewage-discharge-closes-part-of-biloxi-beach/

35. *October 15, Fosters Daily Democrat* – (New Hampshire) **Kohl's evacuated after bomb threat in Rochester.** Police in Rochester, New Hampshire, evacuated a Kohl's store October 15 in response to a bomb threat but said after their search that no explosive device was found. Rochester police and fire departments, as well as an emergency medical services (EMS) team responded after learning from an employee that an unknown person called the store and claimed a bomb was on the premises,

stated a police spokesperson. He said officials immediately evacuated the building and used a New Hampshire State Police Bomb Squad K9 unit to search the area but did not find anything. He said employees were allowed to return to the store almost three hours after the evacuation.
Source: http://www.fosters.com/apps/pbcs.dll/article?AID=/20121015/GJNEWS_01/310159959/-1/FOSNEWS

36. *October 15, Associated Press* – (Connecticut) **Historic synagogue damaged in fire.** An 85-year-old synagogue in Connecticut listed on the National Register of Historic Places was heavily damaged by a fire October 14, but firefighters were able to save the congregation's two Torah scrolls and other important items. The rabbi of the Hebrew Congregation of Woodmont said fire officials told him an electrical problem started the blaze, which destroyed the Milford synagogue's sanctuary and its ornate stained glass windows. The two Torah scrolls were somewhat damaged and will be assessed to see if they can be restored, he said.
Source: http://connecticut.cbslocal.com/2012/10/15/historic-synagogue-damaged-in-fire/

37. *October 15, WAVY 10 Portsmouth* – (Virginia) **NFD: Man threw explosives at apartment.** Officials said Norfolk, Virginia's bomb squad was on scene after a disgruntled boyfriend threw four Molotov cocktails inside of his girlfriend's apartment. According a captain with the Norfolk Fire Department, Norfolk fire and police units, as well as agents with the Alcohol, Tobacco, Firearms, and Explosive Bureau, and FBI, responded to the Beechwood Apartments in Norfolk near Naval Station Norfolk October 15. He said the investigation appears to be the result of a domestic incident between a couple. He said the suspect threw four Molotov cocktails at his girlfriend's apartment. Only one ignited, landed in the bushes and created a small fire. The woman was inside of the apartment at the time with a small child. Neither was injured. A backpack was found close to the scene and following an investigation by the bomb squad, it appeared as though the man had brought the four cocktails inside of the backpack and left it outside. A robot checked for explosives in the backpack which turned out to be empty but smelled of carbon fuel. The captain said officials were aware of the man's identity but did not make any arrests. A portion of Ogden Avenue was closed during the incident and opened back up shortly after it ended. He said residents were allowed to leave but no one was allowed to enter the apartments.
Source: http://www.wavy.com/dpp/news/local_news/norfolk/bomb-squad-on-scene-in-at-norfolk-apts

38. *October 15, KSAZ 10 Phoenix; Associated Press* – (Arizona) **Gas leak evacuates Tempe auto dealership.** Southwest Gas workers tried to close a natural gas leak in Tempe, Arizona, that caused the evacuation of a car dealership. Employees at a Suzuki dealership were evacuated October 15, but were allowed to return and all dealerships were open for business at the Tempe Autoplex. Tempe Fire Department officials considered evacuating the Acura and Toyota dealerships as a precautionary measure until Southwest Gas could contain the leak. "There has been some gas issues in the area for the last week. They have been doing some repairs doing work on the street,

apparently they either had another leak or some residual gas was caught up underground," said an official of the Tempe Fire Department. The cause of the leak was unclear.
Source: http://www.myfoxphoenix.com/story/19826390/2012/10/15/gas-leak-evacuates-several-tempe-auto-dealerships

39. *October 14, Juneau Empire* – (Alaska) **2 arrested on suspicion of operating meth lab in Hoonah.** Two people were arrested on suspicion of manufacturing methamphetamine after authorities discovered an active meth lab inside a commercial storage facility in Hoonah, Alaska, the Juneau Empire reported October 14. The Alaska Bureau of Investigation said in a dispatch that the two suspects were arrested in connection with operating the lab. They were each charged with one count of second-degree drug misconduct for being in possession of methamphetamine precursors and listed chemicals with intent to manufacture methamphetamine, the release stated. The Southeast Alaska Cities Against Drugs (SEACAD) task force processed the lab October 11 after the Hoonah Police Department requested their assistance. Four SEACAD members arrived in Hoonah and removed processed methamphetamine, various precursors, listed chemicals, and other items related to the manufacture of methamphetamine.
Source: http://juneauempire.com/local/2012-10-13/2-arrested-suspicion-operating-meth-lab-hoonah#.UH1ufm881zA

For another story, see item **33**

[Return to top]

National Monuments and Icons Sector

40. *October 15, Reuters* – (California) **Yosemite workers will be studied for disease clues.** California public health officials planned to interview and collect blood samples from up to 2,500 Yosemite National Park workers as they hunted for clues in the biggest outbreak of the deadly hantavirus in nearly two decades, a State health official said October 15. The voluntary employee screening, scheduled for October 16 and 17, was the most recent effort to shed light on the rare, mouse-borne lung disease, which infected nine park visitors and killed three. "This is a highly unusual situation," the chief of the California Department of Public Health's occupational health branch said. The U.S. Centers for Disease Control and Prevention sounded a worldwide alert about the virus over the summer, saying visitors to the popular insulated Curry Village tent cabins between June and August were at risk of contracting the disease. All but one of the nine infected visitors stayed in Curry Village in double-walled, insulated tent cabins later found to be infested with deer mice that carry the virus in their droppings, urine, and saliva. Among the lingering questions over the outbreak is why hantavirus infected park visitors while sparing employees. A 50-question survey and blood tests examined willing workers' exposure to hantavirus following a smaller pilot study in September. By October 15, 300 employees signed up. Humans have never been known to transmit the virus, which kills more than a third of those infected. People can inhale hantavirus when mice droppings mix with dust, especially in confined, poorly ventilated spaces.

Source: http://www.reuters.com/article/2012/10/16/us-usa-hantavirus-yosemite-idUSBRE89F01T20121016

[Return to top]

Dams Sector

41. *October 16, Fayetteville Observer* – (North Carolina) **Hope Mills board votes to sue builders of dam for repairs.** The Hope Mills, North Carolina Board of Commissioners voted unanimously October 15 to file a lawsuit over stalled repairs to the Hope Mills Lake dam. The lawsuit asked that the firms that designed and built the dam, which failed in June 2010 and emptied the lake, pay for its repair. "It is alleged that the estimate of the total repair of the dam is at or in excess of more than $10 million," said a spokesman for the Brough Law Firm, which represents the town. The suit names Crowder Construction, Liberty Mutual Insurance, McKim and Creed engineers, Morrison Engineers, AMEC Environmental and Infrastructure (formerly MacTec Engineering), Mosher Engineering, and an independent engineer. The board took the action after an hour-long closed session. The mayor said various dates set up for negotiations on the dam project were missed. She said the town was told that one or more of the insurance companies representing the firms would not be available to meet until January 2013 at the earliest.
Source: http://www.fayobserver.com/articles/2012/10/16/1210919?sac=fo.local

[Return to top]

NTAS
National Terrorism Advisory System
NO ACTIVE ALERTS
www.DHS.gov/alerts

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2273
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.