Homeland Security

Daily Open Source Infrastructure Report 11 December 2014

Top Stories

- CHARGE Anywhere stated December 9 that attackers had gained access to its network using a previously unknown and undetected piece of malware and were able to capture payment card data from some unencrypted communications. – *Securityweek* (See item **6**)
- A winter storm in the Northeast caused hazardous road conditions for several States and prompted at least 300 school closures or delays in New Hampshire December 9. – *Associated Press* (See item **18**)
- Researchers identified and analyzed a cyber-espionage campaign that appears similar to the RedOctober campaign dubbed Cloud Atlas or Inception Framework that has been targeting the devices of specific users in a number of industry sectors in several countries via spearphishing. – *Softpedia* (See item **22**)
- A December 10 fire at the Gatewood Apartments complex in Dallas left 2 people dead, 3 others injured, and triggered the evacuation of about 300 individuals from the facility. – *Reuters* (See item **33**)

Fast Jump Menu

Energy Sector

1. *December 10, ABC News* – (National) **Nor'easter leaves thousands without power.** Approximately 25,000 customers across a number of Northeast States remained without power December 10 following a severe winter storm December 9 that produced several inches of rain, strong wind gusts, frigid temperatures, and snow. Source: http://abcnews.go.com/US/noreaster-leaves-thousands-power/story?id=27494193

For additional stories, see items **22** and **23**

[Return to top]

Chemical Industry Sector

2. *December 10, CNN* – (West Virginia) **US charges company president with deception in Elk River chemical spill.** The former president of Freedom Industries Inc., the company responsible for a January chemical spill that contaminated the water supply for 300,000 individuals, was charged by the FBI for bankruptcy fraud, wire fraud, and lying under oath during bankruptcy proceedings in an effort to protect his personal assets, according to an FBI complaint that was filed December 8.
Source: www.cnn.com/2014/12/10/justice/west-virginia-chemical-spill-case/index.html

For another story, see item **23**

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

3. *December 9, Associated Press* – (International) **Moldova: 7 arrested suspected of uranium smuggling.** Authorities in Moldova stated December 9 that they arrested 7 people for allegedly smuggling 7 ounces of uranium-238 mixed with uranium-235 worth around $2 million. An investigation aided by the FBI found that the suspects were part of an alleged smuggling group that had specialized knowledge of radioactive materials and how to prevent their detection while in transit from Russia.
Source: https://news.yahoo.com/moldova-7-arrested-suspected-uranium-smuggling-121352584.html

[Return to top]

Critical Manufacturing Sector

4. *December 9, Reuters* – (International) **Nissan recalls about 470,000 SUVs, cars for possible fuel leaks.** Nissan Motor Co. announced December 9 that it is recalling 470,000 vehicles globally, including 143,000 in North America, due to the potential for fuel pressure sensors to have been insufficiently tightened during production, posing a fuel leak and fire risk. Models affected in the U.S. include model year 2012-2014

Nissan Juke, 2012-2013 Infiniti M56 and QX56, and 2014-2015 Infiniti Q70 and QX80 vehicles.
Source: http://www.reuters.com/article/2014/12/09/us-nissan-recall-idUSKBN0JN1JH20141209

5. *December 9, U.S. Consumer Product Safety Commission* – (International) **Lenovo recalls computer power cords due to fire and burn hazards.** Lenovo announced a recall for around 544,000 Lenovo LS-15 AC power cords in the U.S. and Canada due to the potential for the power cords to overheat, posing fire and burn hazards.
Source: http://www.cpsc.gov/en/Recalls/2015/Lenovo-Recalls-Computer-Power-Cords/

For another story, see item **23**

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Financial Services Sector

6. *December 9, Securityweek* – (International) **Hackers breached payment solutions provider CHARGE Anywhere: Undetected since 2009.** Electronic payment solutions provider CHARGE Anywhere stated December 9 that attackers had gained access to its network as early as November 2009 using a previously unknown and undetected piece of malware and were able to capture payment card data from some communications that did not have encryption. The company discovered the compromise September 22 and an investigation found that network traffic capture occurred between August 17 and September 24.
Source: http://www.securityweek.com/hackers-breach-payment-solutions-provider-charge-anywhere-numerous-merchants-affected

For another story, see item **22**

[Return to top]

Transportation Systems Sector

7. *December 10, WCBS 2 New York City; Associated Press* – (New York) **Some ferry service resumes after flooding leaves hundreds stranded on Fire Island.** Fire Island Ferries resumed limited service December 10 after 400 people were stranded on Fire Island in New York December 9 due to flooding caused by a winter storm. Ferry service to Fire Island from Sayville remained suspended through December 11.
Source: http://newyork.cbslocal.com/2014/12/10/hundreds-stranded-on-fire-island-after-flooding-forces-suspension-of-ferry-service/

8. *December 9, Rochester Democrat and Chronicle* – (New York) **DOT closes Brockport's Park Ave.-Fayette St. bridge.** The New York Department of Transportation closed the Park Avenue-Fayette Street Bridge over the Erie Canal in Brockport December 8 until further notice after an inspection revealed that the bridge's carrying capacity was below minimum thresholds. Inspectors are evaluating what repairs are required.
   Source: http://www.democratandchronicle.com/story/news/2014/12/09/dot-bridge-brockport/20130413/

9. *December 9, WCBS 2 New York City; Associated Press* – (New Jersey) **Exchange Place, WTC PATH stations to reopen on weekends after Sandy repairs.** Exchange Place and World Trade Center stations on the Port Authority Trans-Hudson line will resume weekend service December 20 after trains were halted for nearly a year to install a new signal system and repair damage from Superstorm Sandy. Officials stated that corroded metal was replaced and approximately 280,000 square feet of metal tunnel surfaces and equipment were cleaned of salt residue left by the storm.
   Source: http://newyork.cbslocal.com/2014/12/09/exchange-place-wtc-path-stations-to-reopen-on-weekends-after-sandy-repairs/

10. *December 9, WDIV 4 Detroit* – (Michigan) **Woman accused of stealing mail: I was bored.** A Detroit mail processing center employee was charged December 8 for allegedly stealing 1,600 to 2,000 pieces of mail since October and pocketing between $1,000 and $1,500 in cash from the mail after an investigation began when a customer brought in mail that was found scattered on the side of Interstate 94 near the post office.
    Source: http://www.clickondetroit.com/news/woman-accused-of-stealing-mail-i-was-bored/30131118

For another story, see item **23**

[Return to top]

Food and Agriculture Sector

11. *December 10, Business Wire* – (National) **Del Monte Fresh Produce N.A., Inc. voluntarily recalls fresh cut fruit containing Gala red apple in a few States in north east US because of possible health risk.** Del Monte Fresh Produce N.A., Inc., announced December 10 a recall of fresh fruit products containing Gala red apples grown in Pennsylvania due to possible Listeria monocytogenes contamination. The recall includes a total of 3,051 consumer packages that were distributed to several retailers in the northeastern region of the U.S.
    Source: http://www.businesswire.com/news/home/20141209006788/en/3378129/Del-Monte-Fresh-Produce-N.A.-Voluntarily-Recalls

12. *December 9, U.S. Food and Drug Administration* – (National) **Global Garlic Inc. recalls De Mi Pais products Cuajada Fresca (Fresh Curd) and Cuajada Olanchana (Fresh Curd) because of possible health risk.** The U.S. Food and Drug Administration announced December 9 that Miami-based Global Garlic, Inc., issued a

recall for 12-ounce De Mi Pais Cuajada Fresca (Fresh Curd) and Cuajada Olanchana (Fresh Curd) products due to possible Listeria monocytogenes contamination. The products were sent to distributors and retailers in Florida, Louisiana, Tennessee, and North Carolina between April and October.
Source: http://www.fda.gov/Safety/Recalls/ucm426345.htm

13. *December 9, U.S. Department of Labor* – (Nebraska) **Latino worker dies following exposure to nitrogen in tanker truck at Michael Foods' Big Red Farms facility in Wakefield, Nebraska.** The Occupational Safety and Health Administration cited Michael Foods Inc., for five serious safety violations, including nitrogen exposure hazards, following an inspection of the company's Big Red Farms facility in Wakefield that was initiated after a June worker fatality. Proposed penalties total $30,900.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=27093

For another story, see item **23**

[Return to top]

Water and Wastewater Systems Sector

14. *December 10, WDSU 6 New Orleans* – (Louisiana) **Water main break forces boil order for neighborhoods in Slidell.** A boil water advisory was issued for portions of the city of Slidell December 9 until further notice which included parts of Bayou Liberty, Camellia Drive, and Palm Lake, among others, due to a water main break.
Source: http://www.wdsu.com/news/local-news/new-orleans/water-main-break-forces-boil-order-for-neighborhoods-in-slidell/30155252

15. *December 10, Associated Press* – (Florida) **7 injured after Jacksonville sewage plant fire.** Five contractors and two workers were transported to an area hospital with injuries after a fire broke out at a JEA sewage plant in Jacksonville, Florida, December 9 and released hydrogen sulfide gas into the air. The building and a nearby shopping center were evacuated while crews worked to contain the blaze.
Source: http://www.wctv.tv/news/headlines/7-Injured-after-Jacksonville-Sewage-Plant-Fire-285334101.html

16. *December 9, Marietta Daily Journal* – (Georgia) **Reported sewer overflow caused by grease.** An estimated 140 gallons of sewage discharged into a tributary of Noses Creek in Marietta December 5 following an overflow caused by grease in Cobb County. Crews flushed the line to remove the grease and cleared the spill area.
Source: http://mdjonline.com/view/full_story/26215751/article-Reported-sewer-overflow-caused-by-grease

[Return to top]

Healthcare and Public Health Sector

17. *December 9, WXIA 11 Atlanta* – (Georgia) **Ex-Grady hospital employee convicted of embezzlement.** The former payroll director for Grady Memorial Hospital Corporation in Atlanta was found guilty December 9 for stealing more than $480,000 from the hospital by making 134 fraudulent payments to himself by replacing fired employees' bank account numbers with his own from January 2008 to June 2011, in addition to adding vacation and severance pay for former employees to his personal bank account.
Source: http://www.11alive.com/story/news/local/downtown/2014/12/09/donald-thomas-convicted-embezzlement/20134863/

[Return to top]

Government Facilities Sector

18. *December 9, Associated Press* – (New Hampshire) **Northeast dealing with heavy rains, snow, wind.** A winter storm moving through the Northeast caused hazardous road conditions for several States and caused at least 300 school closures or delays in New Hampshire December 9 due to snow, freezing rain, and sleet.
Source: http://www.msn.com/en-us/news/other/northeast-dealing-with-heavy-rains-snow-wind/ar-BBgx4lH

19. *December 9, KMOV 4 St. Louis* – (Missouri) **Water main break forces 3 Fox schools to close.** Fox Elementary, Middle, and High schools in St. Louis were all closed December 9 due to a water main break on a school campus. Crews reported to the scene to repair the break.
Source: http://www.kmov.com/news/local/Water-main-break-closes-3-schools-in-Fox-School-District-Tuesday-285191471.html

20. *December 9, Las Vegas Review-Journal* – (Nevada) **Fumes from NLV graffiti cleanup prompts evacuation of welfare building.** The State of Nevada Division of Welfare and Supportive Services building in Las Vegas was evacuated and employees were sent home after graffiti removal behind the building led to complaints of light-headedness which prompted the evacuation of the facility and several other businesses December 9. One person was transported to an area hospital and two others were treated on-site while crews ventilated the building.
Source: http://www.reviewjournal.com/news/las-vegas/fumes-nlv-graffiti-cleanup-prompts-evacuation-welfare-building

21. *December 9, Buffalo News* – (New York) **Fire at ECC North closes campus for the day.** Eerie Community College's North Campus in New York was evacuated and classes were cancelled December 9 due to a fire in Bretschger Hall that caused extensive damage to the electrical system.
Source: http://www.buffalonews.com/city-region/fire-at-ecc-north-closes-campus-for-the-day-20141209

For another story, see item **22**

[Return to top]

Emergency Services Sector

Nothing to report

[Return to top]

Information Technology Sector

22. *December 10, Softpedia* – (International) **Red October cyber spy op goes mobile via spear-phishing.** Researchers with Blue Coat and Kaspersky Lab identified and analyzed a cyber-espionage campaign that appears similar to the RedOctober campaign dubbed Cloud Atlas or Inception Framework that has been targeting the Android, iOS, and BlackBerry devices of specific users in the government, finance, energy, military, and engineering sectors in several countries via spearphishing. The malware appears to primarily be designed to record phone conversations and can also track locations, monitor text messages, and read contact lists.
Source: http://news.softpedia.com/news/Red-October-Cyber-Spy-Op-Goes-Mobile-Via-Spear-Phishing-467099.shtml

23. *December 10, Securityweek* – (International) **Trihedral fixes vulnerability in SCADA monitoring and control software.** Trihedral Engineering Ltd., released software updates for its VTScada (VTS) supervisory control and data acquisition (SCADA) software to close a vulnerability that could be used by an unauthenticated attacker to crash VTS servers. The software is used in industries including the energy, chemical, manufacturing, agriculture, transportation, and communications sectors.
Source: http://www.securityweek.com/trihedral-fixes-vulnerability-scada-monitoring-and-control-software

24. *December 10, Softpedia* – (International) **Flash Player 16.0.0.235 fixes remote code execution bug exploited in the wild.** Adobe released patches for six vulnerabilities in its Flash Player software, including a vulnerability reported by a researcher that could allow arbitrary code to be executed on affected systems. The arbitrary code execution vulnerability has been observed being exploited in the wild and all users were advised to update their versions of Flash Player as soon as possible.
Source: http://news.softpedia.com/news/Flash-Player-16-0-0-235-Fixes-Remote-Code-Execution-Bug-Exploited-in-the-Wild-467030.shtml

25. *December 10, Securityweek* – (International) **SQL injection, other vulnerabilities found in InfiniteWP admin panel.** A researcher with Slik identified and reported several vulnerabilities in the InfiniteWP administration application for WordPress Web sites, including SQL injection vulnerabilities that could be used by an unauthenticated attacker to gain control of WordPress sites.
Source: http://www.securityweek.com/sql-injection-other-vulnerabilities-found-infinitewp-admin-panel

26. *December 10, Securityweek* – (International) **Flaw in AirWatch by VMware leaks info in multi-tenant environments.** VMware released an update for its AirWatch enterprise mobile management and security platform December 10 that closes vulnerabilities that could allow a user that manages a deployment in a multi-tenant environment to view the statistics and organizational information of another tenant.
Source: http://www.securityweek.com/flaw-airwatch-vmware-leaks-info-multi-tenant-environments

27. *December 10, Securityweek* – (International) **Recursive DNS resolvers affected by serious vulnerability.** The Computer Emergency Response Team Coordination Center (CERT/CC) reported December 9 that recursive Domain Name System (DNS) resolvers are vulnerable to an issue where a malicious authoritative server can cause them to follow an infinite chain of referrals, leading to a denial of service (DoS) state.
Source: http://www.securityweek.com/recursive-dns-resolvers-affected-serious-vulnerability

28. *December 10, Securityweek* – (International) **Third-party bundling made IBM products most vulnerable: Study.** Secunia released a report on security vulnerabilities disclosed between August and October and found that vulnerabilities increased by 40 percent compared to the previous year to a total of 1,841 vulnerabilities in the 20 most vulnerable products, among other findings. The report also found that Google Chrome had the largest number of disclosed security issues, and that IBM was the most vulnerable vendor due to products being bundled with third-party software.
Source: http://www.securityweek.com/third-party-bundling-made-ibm-products-most-vulnerable-study

29. *December 9, Securityweek* – (International) **Microsoft releases critical IE security update on Patch Tuesday.** Microsoft released its monthly Patch Tuesday round of updates for its products December 9, which included 7 security bulletins addressing 24 vulnerabilities. Three vulnerabilities were considered critical and affected Internet Explorer, Microsoft Word and Office Web Apps, and the VBScript scripting engine.
Source: http://www.securityweek.com/microsoft-releases-critical-ie-security-update-patch-tuesday

30. *December 9, Threatpost* – (International) **New version of Destover malware signed by stolen Sony certificate.** Researchers at Kaspersky Lab identified a new variant of the Destover malware used in an attack on Sony Pictures Entertainment that uses a stolen, legitimate certificate from Sony. The malware is basically identical to previous versions except for the use of a certificate.
Source: http://threatpost.com/new-version-of-destover-malware-signed-by-stolen-sony-certificate/109777

31. *December 9, SC Magazine* – (International) **SEO poisoning campaign ensnares several thousand websites, security expert finds.** A webmaster identified and researchers from Websense and High-Tech Bridge confirmed that several thousand legitimate Web sites hosted on GoDaddy and other services had been compromised to

improve the search engine optimization (SEO) ranking of other sites by inserting links into the legitimate sites. GoDaddy stated that the company was investigating the issue. Source: http://www.scmagazine.com/thousands-of-websites-compromised-by-seo-poisoning/article/387453/

For another story, see item **5**

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@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: http://www.it-isac.org

[Return to top]

Communications Sector

See item **23**

[Return to top]

Commercial Facilities Sector

32. *December 10, WSOC 9 Charlotte* – (North Carolina) **20 displaced after south Charlotte apartment fire.** Twenty residents were displaced following a December 9 fire at the Oak Park Apartments complex in Charlotte. Investigators believe that food left unattended on a stove was the source of the blaze which caused about $65,000 in damage to several apartment units.
Source: http://www.wsoctv.com/news/news/local/firefighters-respond-apartment-fire-south-charlott/njPgB/

33. *December 10, Reuters* – (Texas) **Two die in Dallas fire at senior apartment complex: reports.** A December 10 fire at the Gatewood Apartments assisted-living senior apartment complex in Dallas left 2 people dead, 3 others injured, and triggered the evacuation of about 300 individuals from the facility. Authorities are investigating the source of the blaze that trapped residents on balconies and prompted the rescue of several individuals with limited mobility.
Source: http://www.reuters.com/article/2014/12/10/us-usa-texas-fire-idUSKBN0JO1EZ20141210

34. *December 10, Associated Press* – (New York) **Security stepped up after Brooklyn Jewish center stabbing.** Police shot and killed a man who stabbed a student inside the library of the Chabad-Lubavitch headquarters in the Brooklyn area of New York City December 9. Additional security measures were added at the headquarters following the attack.
Source: http://www.foxnews.com/us/2014/12/10/security-stepped-up-after-jewish-

center-stabbing-mentally-ill-suspect-shot-dead/

35. *December 9, KDKA 2 Pittsburgh* – (Pennsylvania) **3 hospitalized after Wilmerding apartment complex carbon monoxide leak.** Residents from an 18-unit apartment complex in Wilmerding were evacuated and 3 residents were hospitalized following a carbon monoxide leak December 9 that affected about half of the complex's units. The structure was red-tagged and cannot reopen until the issue is resolved and the gas company performs a camera inspection.
Source: http://pittsburgh.cbslocal.com/2014/12/09/3-hospitalized-after-wilmerding-apartment-complex-carbon-monoxide-leak/

36. *December 9, Associated Press* – (Wisconsin) **Franklin man charged with arson in apartment fire.** A Milwaukee County man was arrested and charged December 9 for allegedly setting fire to an apartment building in Franklin, Wisconsin, December 1 which caused more than $400,000 in damage to the structure.
Source: http://www.wsaw.com/home/headlines/Franklin-man-charged-with-arson-in-apartment-fire-285201741.html

For additional stories, see items **6** and **15**

[Return to top]

Dams Sector

37. *December 9, Aiken Standard* – (South Carolina) **Flash flood watch canceled, Langley Dam deemed "stable".** A flash flood warning for the Langley Dam area in South Carolina was lifted December 9 after the dam was deemed stable by inspectors following structural concerns in November that prompted the continual draw down of water and the flash flood watch.
Source:
http://www.aikenstandard.com/article/20141209/AIK0101/141209448/1004/flash-flood-watch-canceled-langley-dam-deemed-stable

38. *December 8, KIRO 7 Seattle* – (Washington) **Emergency repairs to Skagit River levee as storm approaches.** Crews worked December 8 to complete emergency repairs to the Skagit River levee near downtown Mount Vernon, Washington, and complete a new floodwall before river levels rise after a rain storm November 28 sent the Skagit River to the flood stage and damaged a portion of the levee.
Source: http://www.kirotv.com/news/news/emergency-repairs-skagit-river-levee-storm-approac/njN6x/

[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 10 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) 942-8590
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.