|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | |  | | |  | | --- | |  |  |  |  | | --- | --- | | [Cyber Security and Information Systems Information Analysis Center](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=http%3A%2F%2FtheCSIAC.com&url_id=3df6fa9231b5b4fddc7adbfaa302377532f2b0ea) | Department of Defense Defense Technical Information Center |  |  | | --- | |  |  |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | |  | | | | | |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | |  | | | | | |  | | --- | |  | | ****The Cyber Security and Information Systems (CSIAC) Information Assurance Digest**** If you would like to share your thoughts on the Information Assurance Digest or make suggestions as to what should be included, click the following link: [https://www.csiac.org/discussion/information-assurance-digest-suggestions](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fwww.csiac.org%2Fdiscussion%2Finformation-assurance-digest-suggestions&url_id=ee9674b4e4e58891bdea9373f63c784d42894682) Recent Headlines:Cyber-Security:[New Oil and Gas ISAC Opens It's Doors, Targets Cybersecurity of Critical Infrastructure](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2F2l96na%3Fid%3D65276&url_id=cfafa7fb27076d03aad6f42a8bbb20b2d6b691dc) - ONG-ISAC A secure and trusted environment for sharing cybersecurity information across the oil and natural gas industry. [Hostile State-Sponsored Hackers Breached Government Network](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Ffjuzhw%3Fid%3D65276&url_id=6d5d9bf0a5d1a060c880a6dc2cc4d1a4afe22e17) - Zdnet The UK government's secure network has come under attack from hackers controlled by a foreign state. [Groups Say Information-Sharing CISA Bill Would Threaten Individual Privacy](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fkp39wi%3Fid%3D65276&url_id=a386a1c85a8e44088e6c5dd1db950124732334fb) - ACLU A group of privacy organizations has written a letter to Congress saying that a newly released draft version of a bill, the [Cybersecurity Information Sharing Act of 2014](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=http%3A%2F%2Fwww.feinstein.senate.gov%2Fpublic%2Findex.cfm%2Ffiles%2Fserve%2F%3FFile_id%3D08de1c1b-446b-478c-84a8-0c3f35963216&url_id=df520acb7117b823c6a9a3d052ec8b2be159f1dc) (CISA), which aims to improve private and public sector sharing of cyber threat information, could pose a major risk to individuals' privacy. [Dragonfly: Western Energy Companies Under Sabotage Threat](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2F1amkw7%3Fid%3D65276&url_id=04ddba976734c4676ab174aa383be4e0bab4232b) - Symantec An ongoing cyberespionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims. [Syrian Electronic Army’s Attack on Reuters](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fhwcybx%3Fid%3D65276&url_id=6c876263195bb78a9deeacddeda34cba41988a78) - Homeland Security News Wire The Reuters site was attacked by the Syrian Electronic Army (SEA), a pro-Assad group of “hacktivists.” [The 2014 Quadrennial Homeland Security Review](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fmh8saf%3Fid%3D65276&url_id=cd088e7ca3433d32382fdb3800c60c93dd130ab3) - Department of Homeland Security This report provides a strong analytic and strategic foundation for one of my highest priorities, which is ensuring that the Department invests and operates in a cohesive, unified fashion and makes decisions that strengthen Departmental unity of effort. Cyber-Warfare:[NATO Updates Cyber Defence Policy As Digital Attacks Become a Standard Part of Conflict](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fklt0uh%3Fid%3D65276&url_id=9005e7ce2ffe4409483423ac6ea0e192697a5dc2) - Atlantic Council The Alliance is facing a new and dynamic security environment that is more strategically constraining and competitive than at any time since the end of the Cold War. Data Security:[Phishing Activity Trends Report: 1st Quarter 2014](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fjd9hj0%3Fid%3D65276&url_id=d689f934f28acac5fedd38e30ceae77b0a862d1d) - APWG The APWG Phishing Activity Trends Report analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization’s website at  [http://www.apwg.org](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=http%3A%2F%2Fwww.apwg.org&url_id=2a2ebdab804211add5cdabe46c4f184cf7af1a52), and by e-mail submissions to [reportphishing@antiphishing.org](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=http%3A%2F%2Freportphishing%40antiphishing.org&url_id=25bd075d178e4e49b208f124655af9b2286bcec9). [Marked Ghost Imaging](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fo8p30d%3Fid%3D65276&url_id=c2d77220db0f432d699c8ec00fc98c4780af09e5) - Scritation In recent years, ghost imaging has been widely applied in various areas, such as optical security. Here, we report how an object and multiple hidden marks can be simultaneously recovered by using only one rebuilt reference intensity sequence in ghost imaging. Mobile Security:[A Measurement Study of Google Play](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fnmk7ze%3Fid%3D65276&url_id=cd670d508e5137a29fde71121faeb62a7487cf45) - Columbia University We have built PlayDrone, the ?rst scalable Google Play store crawler, and used it to index and analyze over 1,100,000 applications in the Google Play store on a daily basis, the largest such index of Android applications. [Android's HijackRAT](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2F8rcev8%3Fid%3D65276&url_id=fa3fae5b5997c318c2e04d0426252907fd829df0) - Fire Eye Mobile security researchers have discovered such a malware that pretends to be a “Google Service Framework” and kills an anti-virus application as well as takes other malicious actions. [Selfmite: Attack Using SMS Worm to Increase Pay-Per-Install Income](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fg0zd81%3Fid%3D65276&url_id=d9b3f1d25bbc59a8b18bdfd110722e64a4f1c322) - Adaptive Mobile AdaptiveMobile has analysed and confirmed a new piece of malware, termed Selfmite, that is also able to propagate via SMS. Network Security:[Microsoft Advancing Encryption and Transparency Efforts](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2F3nengl%3Fid%3D65276&url_id=8e8b45a37580e1b893cb8846be2f784e3681ce64) - Technet Microsoft steps up security for its cloud products and opens a transparency center. [Pony Loader 2.0 Steals Credentials and Bitcoin Wallets: Source Code for Sale](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fbpjlit%3Fid%3D65276&url_id=fd0d9fc608b7ec4f9553ddbe3b2d5095cdb15807) - Damballa Pony Loader malware has been around for years. The source code for version 1.9 was leaked on the Internet, giving criminals the opportunity to modify it to their liking. Recently, Damballa's Threat Research team observed Pony Loader version 2.0. This variant, which ups the potential payday for criminals, is also up for sale. CSIAC Communities of Interest:[Software Assurance Community of Practice (SwA COP)](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2F7s6j0a%3Fid%3D65276&url_id=332aaab79858056393eae8b2a5cfa7c2789d08ac) - CSIAC CSIAC serves on the DoD  Software Assurance Community of Practice Working Group. For further information contact Taz Daughtrey at [hdaughtrey@csiac.org](mailto:hdaughtrey@csiac.org) [Cyber Security of Critical Infrastructure](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fyf0mjx%3Fid%3D65276&url_id=2e3cad4aedf0b5061073ad8a325c0702646e9f93) - Department of Homeland Security CSIAC serves on the EO 13636/PPD-21 Research & Development (R&D) Working Group (WG) run by DHS S&T. If you would like further information, contact Dr. Paul Losiewicz at [plosiewicz@csiac.org](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fwww.thecsiac.com%2Fresources%2Fjournals%2Fia_digest%2Fissue%2Fplosiewicz%40csiac.org&url_id=79734f2314d68b93d7bf4ba843dcdbda6e42ff4a) [The Cyber Shield Newsletter](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fklwhtj%3Fid%3D65276&url_id=4a0ffb2a82ed794a92656ad73ab40883dfe7dce7) - New Mexico CounterIntelligence Working Group (NMCIWG) The Cyber Shield is a Cyber Newsletter for Counterintelligence, IT and Security Profressionals associated with DoD and USG agencies. There are Distribution constraints. If you would like to subscribe, please contact Dr. Paul Losiewicz at [plosiewicz@csiac.org](mailto:plosiewicz@csiac.org) [Systems and Software Producibility Collaboration Environment (SPRUCE)](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2F00lzw6%3Fid%3D65276&url_id=60f15c44a28b48f78689a9028e3f6d8b66f51109) - CSIAC SPRUCE is an online collaborative Forum for describing CS and SE challenging problems, assembling cannonical data sets, and proposing models and solutions. CSIAC invites free use of this environment by the academic, defense-industrial-base, and Government user community. For more information contact Tom McGibbon at [tmcgibbon@csiac.org](mailto:tmcgibbon@csiac.org) Technical Resources:[US-CERT Bulletins](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fw8dgzg%3Fid%3D65276&url_id=6239597650119b1c4f8611c09cfd580a11c514b9) - Department of Homeland Security Bulletins provide weekly summaries of new vulnerabilities. Patch information is provided when available. [US-CERT Alerts](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2F00x6as%3Fid%3D65276&url_id=1556c80d9b9367df5a608026b3699cc018c5ccbb) - Department of Homeland Security Alerts provide timely information about current security issues, vulnerabilities, and exploits. [National Vulnerability Database](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2F30f4tk%3Fid%3D65276&url_id=7d0f68a1d0d43b40552bc2615cdebc988daa59ad) - NIST NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics. Policy Resources:[DoD Cyber Domain Resources](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2F6j8x4x%3Fid%3D65276&url_id=465afb8a360754a3b746658cf65e85538a2777a2) - DoD[Committee on National Security Systems (CNSS)](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fn0zfci%3Fid%3D65276&url_id=0d922e2b8580e49071caa9159b6807f8f76635a2) - Committee on National Security Systems[DHS Cyber Security Strategy ("Blueprint for a Secure Cyber Future", 2011)](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fbi7is6%3Fid%3D65276&url_id=1053a7e862771b9db25038a0d02d5f57ba6e1cc6) - Department of Homeland Defense[Trustworthy CyberSpace: Strategic Plan For The Federal Cybersecurity Research and Development Program](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fjcqliu%3Fid%3D65276&url_id=31a80015c8086115c372a5629bd3c79ef5ec1acb) - NITRD[DoD COI Governance and Guidance](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fq4k6g4%3Fid%3D65276&url_id=0ea0f03e5e6137268b206fc93c0eed9644707f4e) - DoD Chief Information Officer[CSIAC Information Assurance Policy Chart](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2F3o9mee%3Fid%3D65276&url_id=ffaeb3ac2976e54630c15488a3c4fea6813b45da) - CSIAC Updated 15 April 2014 Guidance:[Framework for Improving Critical Infrastructure Cybersecurity](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fya42fh%3Fid%3D65276&url_id=dafd50a3830f3889a3f3c698699ad206b804956b) - National Institute of Standards and Technology NIST Framework published 12 February 2014. [ISO Standards on Vulnerability Handling and Disclosure](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2F2m7eq8%3Fid%3D65276&url_id=a3779b027367943e4ad42b3c077d78b548850a98) - Internet Storm Center Two new ISO standards for vulnerability verification and reporting. [Administration's Strategy to Mitigate the Theft of U.S. Trade Secrets](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fqgtr5u%3Fid%3D65276&url_id=fee0106ceac5ed3f6e0bdeb5c61a8a86f18b67c2) - The White House White House Economic Cyberwarfare Strategy. [DoD Commercial Mobile Implementation Plan](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2F6eapcr%3Fid%3D65276&url_id=3ef007f082c82172476eb51c581f5fcf62f5eb02) - DoD Update to DoD Mobile Device Strategy. [CNSS Advisory Memorandum Information Assurance 01-12 6 June 2012](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Flaei0c%3Fid%3D65276&url_id=744b71da7c41b878476235e546ecbb48525b07e0) - CNSS NSA-Approved Commercial Solution Guidance. [Bring Your Own Device](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fddlpjf%3Fid%3D65276&url_id=bb3a8335fba6c63b87cf5528a75c048c317afd07) - The White House A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs - August 23, 2012. Product of the Digital Services Advisory Group and Federal Chief Information Officers Council. [GAO-13-187 Cybersecurity](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fycvsmk%3Fid%3D65276&url_id=4621a1e0cac78e49b9a19379362c6b446a523954) - Government Accountability Office National strategy, roles, and responsibilities need to be better defined and more effectively implemented. [GAO February 2013 High Risk Update](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2F5aafaj%3Fid%3D65276&url_id=df17b0d70e2e96687af8cdf31f97a9c03dc24c41) - Government Accountability Office GAO recommends assessment of government-wide material weakness in information security be upgraded to a significant deficiency for 2 consecutive years. (p.189) [DoDI 8510.01](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2F2ygr2b%3Fid%3D65276&url_id=506775052f6b11c720e675564ad490f382401a44) - DTIC Provides procedural guidance for the reciprocal acceptance of authorization decisions and  artifacts within DoD, and between DoD and other federal agencies, for the authorization and  connection of information systems (ISs). Effective 12 March 2014. [DoDI 8500.01](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fkjjldw%3Fid%3D65276&url_id=42436938d7f29c6cc0d339300b4c838140497bef) - DTIC DoDD 8500.01E (which it replaced),  DoDI 8500.02, DoDD C-5200.19, DoDI8552.01 and DTM 08-060 were all cancelled because the new DoDI 8500.01 incorporates them all. Effective 14 March 2014. [NIST announces that the Second Public Draft of Special Publication (SP) 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, has been released for public comment. (June 3, 2014)](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fssahzc%3Fid%3D65276&url_id=d831dd3d128aa1dff55feca37497d6f44d14dc93) - NIST This document provides guidance to federal departments and agencies on identifying, assessing, and mitigating Information and Communications Technology (ICT) supply chain risks at all levels in their organizations. It integrates ICT supply chain risk management (SCRM) into federal agency enterprise risk management activities by applying a multitiered SCRM-specific approach, including supply chain risk assessments and supply chain risk mitigation activities and guidance. Feedback from the last ia digest:most popular:[AT&T Confirms Serious Mobile Security Breach](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Fxw2l5z%3Fid%3D65276&url_id=d515b4ab4afd91b755cebfe134aae7861eb86afa) - Softpedia Some AT&T customers received a letter from the company informing them that some of their details have been accessed without authorization by employees of one of their service providers. [Cloud-Based POS Software- "New Target For Hackers"](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2F88wbya%3Fid%3D65276&url_id=b57c25a2cb0d75f6f65b585af50b96ca9cff6eb4) - Intel Crawler IntelCrawler, a cyber threat intelligence firm from Los Angeles, has identified new-targeted attacks on cloud-based POS software, used by grocery stores, retailers and other small businesses using web browsers like Internet Explorer, Safari, and/or Google Chrome. [Google Embraces Docker, The Next Big Thing In Cloud Computing](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fr.thecsiac.com%2Faehnnc%3Fid%3D65276&url_id=400e30ae05b63df5e3f5021f7b7901e3d82f9194) - Wired Google is putting its considerable weight behind an open source technology that’s already one of the hottest new ideas in the world of cloud computing.  The CSIAC IA Digest is a semi-weekly news summary for information assurance and software reliability professionals protecting the global information grid. It is transmitted in an HTML-formatted email and provides links to articles and news summaries across a spectrum of IA/SE/DIO/IW topics.   |  | | --- | |  | | |  | | --- | |  | | | |  | | --- | |  | |  | | --- This is an automatic message from the Cyber Security and Information Systems Information Analysis Center. To unsubscribe from this email list or other CSIAC email lists, [update your subscriptions settings](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=https%3A%2F%2Fwww.csiac.org%2Fsubscription_manager%2F%3Fid%3D65276%26e%3Dnjones%40coastline.edu&url_id=1ef4ddd5cee0ac60106b630945987a64c54642bb).   |  | | --- | |  | | |  | | |  | | --- | |  | |
| |  | | --- | | [Quanterion Solutions Incorporated.](http://click.thecsiac.com/track/click.php?u=30024433&id=4923e729e04d4cd790367395964f6557&url=http%3A%2F%2Fquanterion.com%2F&url_id=3b4777036bfee2cb4a30a9e959d099db43d7151b) Copyright © 2013 811 Court Street. Utica, NY. 13502 | | | |

http://click.thecsiac.com/track/open.php?u=30024433&id=4923e729e04d4cd790367395964f6557