

# ICS-CERT MONITOR



October, November, December 2013



## NCCIC

NATIONAL CYBERSECURITY AND  
COMMUNICATIONS INTEGRATION CENTER

### CONTENTS

INCIDENT RESPONSE ACTIVITY  
SITUATIONAL AWARENESS  
ICS-CERT NEWS  
RECENT PRODUCT RELEASES  
OPEN SOURCE SITUATIONAL  
AWARENESS HIGHLIGHTS  
UPCOMING EVENTS  
COORDINATED VULNERABILITY  
DISCLOSURE

This product is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this product or otherwise.

#### Contact Information

For any questions related to this report or to contact ICS-CERT:  
Email: [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov)  
Toll Free: 1-877-776-7585

#### I Want To

- Report an ICS incident to ICS-CERT
- Report an ICS software vulnerability
- Get information about reporting

#### Downloading PGP/GPG Keys

<http://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT.asc>

#### Joining the Secure Portal

ICS-CERT encourages U.S. asset owners and operators to join the Control Systems compartment of the US-CERT secure portal. Send your name, telephone contact number, email address, and company affiliation to [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov) requesting consideration for portal access.

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: <https://forms.us-cert.gov/ncsd-feedback/>

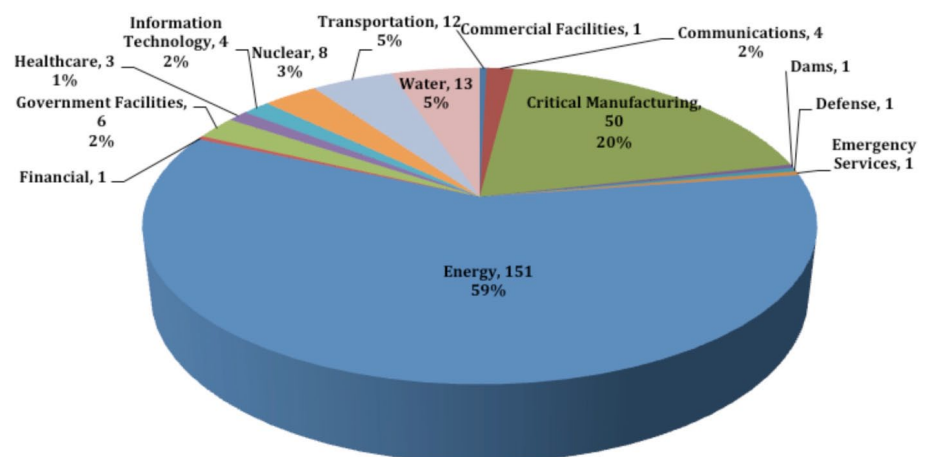
## INCIDENT RESPONSE ACTIVITY

### TRENDS IN INCIDENT RESPONSE IN 2013

#### OVERVIEW

ICS-CERT continued its cyber incident response and risk reduction mission in 2013 by responding to an increasing number of incidents (footnoted) targeting our Nation's critical infrastructure. It's important to note that all incident reporting to ICS-CERT is done on a voluntary basis. As such, the statistics highlighted below are not representative of the actual activity occurring across all sectors. ICS-CERT strives to conduct outreach to all sectors to build relationships of trust and encourage reporting of cyber incidents. The following incident attributes have been tracked and are being shared for greater community awareness.

In 2013, ICS-CERT responded to 256 incidents reported either directly from asset owners or through other trusted partners. The majority of these incidents were initially detected in business networks of critical infrastructure organizations that operate industrial control systems (ICS). In each case, ICS-CERT evaluates the incident to determine the presence and extent of the intrusion with a focus on identifying lateral movement into the control environment or ex-filtration of sensitive ICS information from the business network. Common initial infection vectors were unauthorized access of Internet facing devices, scanning and probing of publicly accessible assets, malware transfer via removable media, exploitation of software/hardware vulnerabilities, and spear-phishing attacks. Because reporting of cyber incidents is done on a voluntary basis, it is estimated that many more incidents are occurring but are not reported. In addition, based on previous incident response efforts, ICS-CERT assesses that many incidents are not detected due to a lack of sufficient detection or logging capabilities.



a. Encompasses Scans and Probes, Malware, (D)DoS, Network Penetrations, and Unauthorized Access



## INCIDENT RESPONSE ACTIVITY - Continued

### SECTORS

Of the 256 reported incidents, 59 percent, or 151 incidents, occurred in the energy sector, which exceeded all incidents reported in other sectors combined. The trusted relationship that ICS-CERT has with many industry partners, especially in the energy sector, combined with an increase in awareness and reporting, is likely responsible for the increase in reported incidents from energy sector partners. Another sector of note is critical manufacturing, where 50 incidents (20 percent) were reported, several of which targeted organizations that produce ICS devices and software. This highlights the continued interest in control systems by malicious actors as well as the possibility of threat actors looking for opportunities to exploit vulnerabilities in the supply chain.

### ATTRIBUTES

Of the 256 cyber incidents, ICS-CERT determined that:

- 79 organizations were either confirmed or suspected to be compromised
- 57 were determined to be “not compromised,” and
- 120 were indeterminate or unknown.

For many of the incidents that were categorized as “suspected” to be compromised, the detection capabilities and log records were inadequate to positively determine if threat actors were able to penetrate the network and maintain a presence. This underscores the importance of maintaining system and network logs, which are essential for ensuring detection and response capabilities, especially during the course of investigating an incident.

ICS-CERT assisted multiple organizations that were the victims of “watering hole” attacks. Watering hole attacks involve attackers compromising one or more legitimate Web sites with malware in an attempt to target and infect visitors to those sites. In several instances, ICS-CERT was concerned that the Web sites involved may have been selected to target critical infrastructure asset owners. Working with the targeted Web site owners to identify potential victims of the compromised sites. ICS-CERT assisted over 50 critical infrastructure organizations to ensure they were aware of the potential compromise from the watering hole sites and possible attacker lateral movement across networks. ICS-CERT also released alerts and provided indicators of compromise to the critical infrastructure community to aid in detection of and recovery from any infections.

Other common initial infection vectors included spear-phishing, Structured Query Language (SQL) injection, and exploitation of externally facing Web services. In general, sophisticated threat actors are capable of employing techniques to successfully compromise networks, move laterally across networks and zones, evade detection, and establish footholds to maintain a presence.

Common motivations include data exfiltration of intellectual property, reconnaissance and industrial espionage, economic sabotage, and positioning for possible future exploitation or attack activity.

Most notably, ICS-CERT responded to a major cyber intrusion campaign from an emerging threat actor targeting 40 critical infrastructure organizations. The majority of these were in the energy sector; however, critical manufacturing and several other sectors were also targeted. The characteristics of this cyber activity included new tactics, which presented new threats for critical infrastructure asset owners. Details of the tactics and techniques were provided in two alerts that were released to Secure Portal members.

In addition to the detailed alerts, ICS-CERT kicked off an “Action Campaign” in partnership with the Federal Bureau of Investigation, Department of Energy, Energy Sector –Information Sharing and Analysis Centers, Transportation Security Administration, and others to provide classified briefings to private sector critical infrastructure organizations across the country. ICS-CERT conducted 14 briefs in major cities throughout the United States, briefing over 750 personnel involved in the protection of energy assets and critical infrastructure. ICS-CERT continues to track this activity, provide support to organizations, and will issue updates and new alerts as needed.

A summary of the 2013 cyber incidents would not be complete without highlighting the continuing concern over the number of vulnerable Internet facing control system devices and remote login sites. ICS-CERT continues to notify and work with organizations that have unprotected devices accessible via the Internet, as researchers report findings from search engine type tools such as Shodan and Every Routable IP Project (ERIPP).

As we head into 2014, ICS-CERT continues to encourage asset owners to remain vigilant of today’s cyber threats in an ever evolving landscape. This vigilance should include enhanced detection, monitoring, and response capabilities, so that incidents can be detected and properly thwarted or mitigated quickly.

ICS-CERT also encourages organizations to report incidents so that they can be tracked, correlated, and shared back (anonymized) with the rest of the community for greater awareness. Reducing risk and protecting the Nation’s infrastructure requires coordination and partnerships across our entire society from private sector to government and law enforcement partners.



## INCIDENT RESPONSE ACTIVITY - Continued

### ICS-CERT ASSESSMENTS

The ICS-CERT supported onsite assessments to strengthen the cybersecurity posture of 15 critical infrastructure control systems owners, operators, and control systems manufacturers located in Arizona, California, New Jersey, New York, and Texas. Organizations in the Energy, Transportation Systems, Nuclear Reactors, Materials & Waste sector, and Water sector hosted the assessments.

### NUCLEAR POWER PLANT BENEFITS FROM NAVV

ICS-CERT receives requests and conducts assessments at critical infrastructure sites. A recent development in assessment capabilities is a technical evaluation of control system network traffic called a Network Architecture Verification and Validation (NAVV). In November, a NAVV was performed at a power plant in the nuclear sector as an extension of a scheduled network architectural review. The NAVV tool captured over 60 gigabytes of network traffic from its isolated network. ICS-CERT analyzed the network traffic to:

- Verify the accuracy of the ICS network diagram.
- Support the identification of potential rogue devices or unexpected data communications.
- Analyze data flows and ensure that boundary protection devices were working as designed.
- Identify opportunities or areas to improve zoning and perimeter protections.

The NAVV identified where network traffic was attempting to connect to devices or external addresses; fortunately, the security devices denied the connections. This analysis identified an improper configuration and potentially unknown system communications that needed to be investigated and removed or reconfigured to fully protect its environment.

Site			Service	
Quarter	Month	Year	Description	Type
1	October	2013	Transportation Utility	Onsite CSET
1	October	2013	Transportation Utility	Design Arch Rev
1	October	2013	Water Utility	Onsite CSET
1	October	2013	Transportation Utility	NAVV
1	October	2013	Water Utility	Onsite CSET
1	November	2013	Water Utility	Onsite CSET
1	November	2013	Water Utility	Onsite CSET
1	November	2013	Transportation Utility	Onsite CSET
1	November	2013	Nuclear Facility	Design Arch Rev
1	November	2013	Nuclear Facility	NAVV
1	December	2013	Energy Utility	Design Arch Rev
1	December	2013	Water Utility	Onsite CSET
1	December	2013	Water Utility	Design Arch Rev
1	December	2013	Energy Utility	Design Arch Rev
1	December	2013	Energy Utility	NAVV

The NAVV is one of three types of onsite cybersecurity assessments offered by ICS-CERT. Other onsite assessments include a Cyber Security Evaluation Tool (CSET®) and a Design Architecture Review (DAR.) The CSET® is used to evaluate an organization's cybersecurity level, against nationally recognized standards, policies and guidelines, which exist within a control or business system network, and provides recommendations for improving the system's cybersecurity posture.

The CSET® implements a simple, transparent process that can be used effectively by all sectors to perform an evaluation of any Industrial Control System. The DAR is a "deep-dive" comprehensive evaluation and discovery process, focusing on defense-in-depth strategies associated with an asset owner's specific control system network. The DAR evaluates network access/egress, design, configuration, applications and rules. It also provides a robust evaluation of system interdependencies, vulnerabilities and mitigation options.

## SITUATIONAL AWARENESS

### APPLICATION WHITELISTING IN AN ICS ENVIRONMENT (PART 2 OF 2)

This is the second in a two-part series. Part 1, "Benefits and Limitations of Application Whitelisting," was published in the [July/August/September edition](#) of the Monitor.

### CHALLENGES OF APPLICATION WHITELISTING

Application Whitelisting (AWL) is simple in concept, but the implementation of AWL technologies can be challenging for systems administrators, because they are forced to determine what applications are authorized and should be allowed to execute. This is particularly true on end points that continually require new applications. Both the creation and the maintenance of the whitelist

## SITUATIONAL AWARENESS - Continued

policy can place a burden on the system administrator. However, the maintenance burden is generally less in ICS environments than with the more dynamic IT network. The effectiveness of AWL also varies based on the true understanding of the applications executing within the environment. During the initial creation of the whitelist, it is possible to whitelist unintentionally a malicious file already present on the system or block the execution of a required program. Either scenario could lead to an adverse impact on a system.

Other challenges include:

- Limited system resources on end points of legacy systems.
- Because of the high availability requirements of ICS environments, the implementation of memory protection can be more complicated and riskier in an ICS environment. A memory protection rule/policy designed under normal operating conditions could unintentionally block valid operations used to restore a system from an abnormal state, potentially resulting in a loss of availability.
- Patches and updates may modify existing whitelisted applications or introduce new executables that require review and authorization.

### *Approaches to Overcoming AWL Challenges.*

The following sections describe a possible approach to help system administrators ease the burden of implementing and maintaining an AWL solution.

**Choose Systems to Protect.** Choose a small subset of critical systems most important to protect. Servers and systems used in an ICS environment work well with whitelisting, because the applications do not change as frequently compared to traditional corporate workstations. AWL technology is not available for field devices, but computers that have access to field devices should be protected.

**Create New Baseline of Systems.** Start with a fresh operating system that is patched and has all newly installed required applications (gold image). A gold image for the system may already be created for backup purposes or other policies. If one does not exist, create one in this step.

**Create Initial Policy from Baseline.** The initial whitelisting policy should be created from the gold image of the system. This provides the greatest chance of success at allowing only legitimate applications to execute while denying unauthorized applications from executing.

**Start in Monitor-Only Mode.** When AWL is first introduced to a system, it is best to use it in monitor-only mode (nonblocking), so an administrator can see how the policy is working without blocking any legitimate applications. This allows for tuning without impacting the availability of services.

**Run in Test Environment.** If available, first implement AWL in a test environment. Implementing AWL technology in a test environment allows the technology and policies to be thoroughly tested before introducing it into a production environment.

**Add Trusted Mechanisms** (if necessary). Each whitelisting vendor's recommended settings offer the best security protection. It may not be possible to run with all these settings for a number of reasons. For example, it may cause system updates and legacy applications to stop working properly. In such cases, an administrator can evaluate what is necessary to allow the system to be fully operational and maintainable. This will differ from organization to organization. Such changes may include allowing a trusted folder for system updates, turning off memory protection, and other various custom settings. In general, it is best to change as few of the whitelisting vendor's recommended settings as possible. However, it is better to have AWL installed with some additional allowed trusted mechanisms than to run without the technology. Each organization must determine how best to balance operational efficiency and security.

**Run in Secure-Mode (If Possible).** After establishing confidence in monitor-only mode, an administrator can switch to secure-mode to get the desired security benefits of AWL. In cases where it is not possible to switch to secure-mode, AWL is still extremely useful to install and run in monitor-only mode to provide administrators with visibility into the executables that end points on the network are trying to execute.

**Monitor and Tune System.** After switching to secure-mode, it is important to continue to monitor and tune the system in order to validate the effectiveness of the policy and ensure that operational enhancements and modifications are functioning as intended.

**Repeat Steps with New Batch of Systems.** Repeat all the steps with a new batch of systems to integrate AWL throughout the enterprise.

## CONCLUSIONS

This two-part series illustrates the benefits, limitations, and challenges of including AWL within an ICS environment. These benefits include reducing risk on end points, increasing ability to monitor executables on systems, and improving regulatory compliance. The predictable and unchanging nature of control systems provides the ideal environment for AWL, which can provide an effective way to help secure hosts. The limitations and challenges of AWL are also presented to help owners and operators more effectively develop a plan for implementation. While whitelisting cannot completely prevent malicious cyber activity, it can limit the scope of an intrusion and provide organizations another tool to assist in defending their network.





### SHOULD APPLICATION WHITELISTING REPLACE ANTIVIRUS SOLUTIONS?

AWL and antivirus solutions are best applied in combination and are not mutually exclusive. In general, antivirus technologies provide two key benefits that AWL solutions typically do not provide.

- Antivirus alerts if a malicious file is discovered.
- Antivirus provides heuristics that can help against trusted application attacks.

If an organization must remove antivirus from real-time monitoring, it is recommended to scan periodically with an antivirus solution to flag dropped malicious files.

### CAN APPLICATION WHITELISTING ALLOW DELAYED PATCHING?

By its nature, AWL does not protect against exploits that target vulnerabilities within trusted applications. Many updates provide fixes to vulnerabilities within these trusted applications.

Thus, in general, whitelisting does not protect the system from this kind of attack and is not a substitute for regular updates.

AWL should be considered as one layer in a defense-in-depth strategy for securing ICS (Figure 2). No one solution can provide complete protection. While risk of system compromise cannot be entirely eliminated, the attack surface of the system can be greatly reduced.

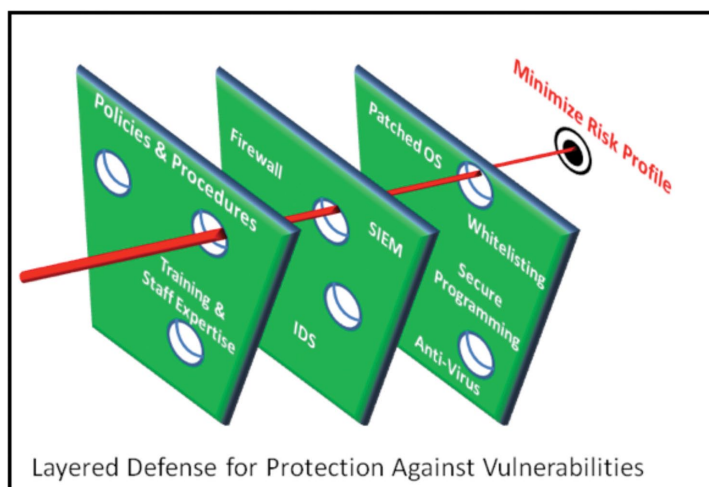


Figure 2. Minimizing risk through a defense-in-depth strategy

### DESTRUCTIVE MALWARE IN A CONTROL SYSTEM ENVIRONMENT

In the high consequence environment of industrial control systems, what you don't know could have an impact on more than just the bottom line. The risk of malware that contains a destructive payload poses a direct threat to the operations of an organization. These payloads could potentially impact the availability of critical assets and information. Organizations must continually assess their infrastructure and subsequent security controls in order to validate their capacity to actively prepare for and respond to such an event.

As evidenced by "Shamoon," officially known as W32.DistTrack, and the recent CryptoLocker ransomware, the risks associated with destructive malware are an enterprise reality. While various system entry points may be utilized as the initial infection vector, organizations must validate mechanisms within their infrastructure that could permit a destructive payload to be distributed to a large scope of systems, potentially undetected.

At the core of proactively preparing for such an event within an enterprise, a strong focus must be garnered toward recovery and reconstitution planning. This process begins by performing a Business Impact Analysis (BIA). The BIA will reinforce an organization's proficiency to create awareness regarding its infrastructure, critical applications and data elements, operational interdependencies, and areas of potential weaknesses. This assessment can then be used to identify security controls and defensive postures that must be enforced, reassessed, or redefined to ensure effectiveness.

The scope of security controls to be considered for both detection and prevention measures should not only encompass computer network defense best practices, but also include risk mitigation strategies. These strategies are focused on securing and monitoring enterprise components, especially those that could be used as a mass distribution vector, impacting a large-scale of assets required for operations. Security defenses should not only be focused at the perimeter of an organization, but also include security controls, segmentation, access control, and monitoring within the infrastructure boundary.

Combined with recovery and reconstitution planning, an organization must test its detection and response capabilities, and exercise its continuity of operations processes. Without a practical validation regarding the effectiveness of the incident response detection, prevention, containment, and restoration capabilities coupled with validation for the effectiveness of implemented security controls, a true measurement of an organization's computer network defense posture cannot be substantiated. ICS-CERT and US-CERT have provided additional guidance and



## SITUATIONAL AWARENESS - Continued

recommendations regarding preparation for a destructive malware attack.

### ICS-CERT NEWS

#### CSET® 6.0 PROVIDES NEW CAPABILITIES

As a significant piece of the ICS-CERT proactive portfolio CSET® (Cyber Security Evaluation Tool) continues to support, educate, and guide critical infrastructure asset owners. The tool uses a combination of recognized standards and a step-by-step wizard to guide users through a systematic analysis of their cybersecurity posture. CSET® has been rapidly accepted as a standard for many critical infrastructure asset owners in establishing their own cybersecurity baselines and processes.

The CSET® coaches asset owners through an assessment process. During this process, cybersecurity implementers and management personnel are taken step by step through a series of concepts and ideas. While considering each concept, the assessment team reviews its individual processes from a cybersecurity perspective. The team discovers the system's own unique environmental risks and weaknesses while being introduced to new concepts and principles of cybersecurity.

New standards incorporated into CSET® 6.0 include:

- CNSSI 1253,
- ICS Overlay,
- CNSSI ICS Overlay Update,
- NEI 08-09,
- NISTIR 7628,
- INGAA,
- NIST SP800-53 R4 Appendix J,
- NIST SP800-53 R4, and
- NIST SP800-82.

To accommodate more mature cybersecurity processes, CSET® will provide the capability for current CSET® users to employ their past and current assessments to evaluate their investment in an established cybersecurity process. This allows users to establish a baseline assessment and then incorporate follow-on assessments to trend and compare their overall cybersecurity improvement. Users will be able to drill down into specific areas to view trending in areas such as account management, password-management, defense-in-depth, or least user privileges. This information may then be used to justify spending on particular areas of vulnerability,

prioritize work, and determine the return on investment for cybersecurity-related spending.

New functionality in CSET 6.0 includes:

- Video tutorials will be available on YouTube.
- Component questions have been tuned to better reflect the latest concerns and issues in control system-related cybersecurity.
- High-level concept questions help users to better understand and navigate the assessment.
- Assessors may assign different portions and sections of an assessment to those most competent in an area and merge all the pieces back together to create a single assessment.
- Assessors responsible for cybersecurity of a large organization are now able to combine assessments from different divisions or departments to see an overall picture and summary for the organization to understand common challenges, or see individual needs in different departments.
- Establish a baseline to better understand the evolution of an organization's cybersecurity posture and trend changes in following assessments.

#### We Want To Hear From You



A key aspect of our mission is providing relevant and timely cybersecurity information products and services to industrial control system (ICS) stakeholders. As we develop and prepare new products, we need and want your input, both good and bad. Please contact us with your comments, concerns, and ideas for ways we can better serve you. Your feedback is welcomed, so we can work together to meet the security challenges facing the ICS community.

If you want to see an important or pertinent topic addressed in this forum, please send your suggestions to:  
[ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov).

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL:  
<https://forms.us-cert.gov/ncsd-feedback/>



## RECENT PRODUCT RELEASES

### ALERTS

[ICS-ALERT-13-304-01](#) Nordex NC2 – Cross-Site Scripting Vulnerability, 10/31/2013

[ICS-ALERT-13-259-01](#) Mitsubishi MC-WorkX Suite Insecure ActiveX Control, 9/16/2013

[ICS-ALERT-13-256-01](#) WellinTech KingView ActiveX Vulnerabilities, 9/13/2013

### ADVISORIES

[ICSA-13-352-01](#) NovaTech Orion DNP3 Improper Input Validation Vulnerability, 12/18/2013

[ICSA-13-347-01](#) Siemens COMOS Privilege Escalation, 12/13/2013

[ICSA-13-346-01](#) Cooper Power Systems Improper Input Validation Vulnerability, 12/12/2013

[ICSA-13-346-02](#) Cooper Power Systems Cybectec DNP3 Master OPC Server Improper Input Validation, 12/12/2013

[ICSA-13-340-01](#) RuggedCom ROS Multiple Vulnerabilities, 12/6/2013

[ICSA-13-338-01](#) Siemens SINAMICS S/G Authentication Bypass Vulnerability, 12/4/2013

[ICSA-13-337-01](#) Elecsys Director Gateway Improper Input Validation Vulnerability, 12/3/2013

[ICSA-13-329-01](#) Triangle Research Nano-10 PLC Improper Input Validation, 11/25/2013

[ICSA-13-291-01A](#) DNP3 Implementation Vulnerability, 11/21/2013

[ICSA-13-297-01](#) Catapult Software DNP3 Driver Improper Input Validation, 11/19/2013

[ICSA-13-297-02](#) GE Proficy DNP3 Improper Input Validation, 11/19/2013

[ICSA-13-295-01](#) WellinTech KingView ActiveX Vulnerabilities, 10/22/2013

[ICSA-13-282-01A](#) Alstom e-Terracontrol DNP3 Master Improper Input Validation, 10/21/2013

[ICSA-13-289-01](#) Cisco ASA and FWSM Security Advisories, 10/16/2013

[ICSA-13-276-01](#) Invensys Wonderware InTouch Improper Input Validation Vulnerability, 10/9/2013

[ICSA-13-095-02A](#) Rockwell Automation FactoryTalk and RSLinx Vulnerabilities, 10/7/2013

[ICSA-13-277-01](#) Philips Xper Buffer Overflow Vulnerability, 10/4/2013

[ICSA-13-274-01](#) Siemens SCALANCE X-200 Authentication Bypass Vulnerability, 10/3/2013

[ICSA-13-259-01](#) Emerson ROC800 Multiple Vulnerabilities, 9/26/2013

[ICSA-12-018-01B](#) Schneider Electric Quantum Ethernet Module Hard-Coded Credentials, 9/23/2013

[ICSA-13-231-01B](#) Sixnet Universal Protocol Undocumented Function Codes, 9/17/2013

[ICSA-13-254-01](#) Siemens SCALANCE X-200 Web Hijack Vulnerability, 9/11/2013

[ICSA-13-252-01](#) SUBNET Solutions Inc. SubSTATION Server DNP3 Outstation Improper Input Validation, 9/9/2013

[ICSA-13-248-01](#) ProSoft Technology RadioLinx ControlScape PRNG Vulnerability, 9/5/2013

[ICSA-13-213-04A](#) MatrikonOPC SCADA DNP3 Master Station Improper Input Validation, 8/29/2013

[ICSA-13-240-01](#) Triangle MicroWorks Improper Input Validation, 8/28/2013

### OTHER

[July/August/September 2013–ICS-CERT Monitor](#)

Follow ICS-CERT on Twitter: @icscert

## OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

### **FBI, Homeland Security and Counterterrorism Center Declare Cyber-Attacks Bigger Threat than Terrorism** 2013-11-26

Cyber-attacks, not terrorist ones, will be the greater threat in the coming years to the United States, according to federal officials at three agencies charged with protecting the nation.

At a recent hearing of the Senate homeland security and government affairs committee, the heads of the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS) and National Counterterrorism Center (NCTC) told lawmakers that cyber-attacks were likely to surpass terrorism as a domestic danger over the next decade.

<http://www.allgov.com/news/us-and-the-world/fbi-homeland-security-and-counterterrorism-center-declare-cyber-attacks-bigger-threat-than-terrorism-131126?news=851762>

### **NATO Launches ‘Largest Ever’ Cyber-Security Exercises** 2013-11-26

NATO has kicked off Cyber Coalition 2013, the largest ever exercise of its kind intended to thwart massive, simultaneous attacks on member states and their allies. The three-day exercise, based at the 27 member alliance’s cyber defense center in Estonia, will include participants from over 30 European states.

“With around 100 participants in Tartu [Estonia] and over 300 in national capitals from 32 nations, Cyber Coalition 2013 is the largest exercise of its kind in terms of participating countries,” NATO said in a statement.

<http://rt.com/news/nato-cyber-exercises-estonia-344/>

### **Threat Grows for Cyber-Physical Systems** 2013-11-21

The rapid adoption of commercial firmware and software for cybersystems serving the critical infrastructure is increasing vulnerabilities that potentially could lead to devastating system failures, according to a report issued by a cybersecurity organization. In some cases, these diverse systems also are threatened by their legacy nature, which is a barrier to implementing necessary cybersecurity measures.

<http://www.afcea.org/content/?q=node/11993>

### **Inventorying Cyber-Assaults in U.S.** 2013-11-08

The Cybersecurity Public Awareness Act of 2013, S. 1638, would require national security and federal law enforcement agencies to report to Congress on attacks on federal networks, investigations

of cybercrime and impediments to public awareness of common cybersecurity threats.

The bill also includes provisions that would boost awareness of threats against federal agencies, the military, the nation’s critical infrastructure and publicly traded companies.

<http://www.inforisktoday.com/inventorying-cyber-assaults-in-us-a-6201>

<http://www.gpo.gov/fdsys/pkg/BILLS-113s1638is/pdf/BILLS-113s1638is.pdf>

### **Why NERC Will Attack the Grid November 13 (and What it Could Mean for Utilities)** 2013-11-07

The North American Electric Reliability Council (NERC) is about to launch a simulated attack on the U.S. power grid. The drill will begin with a series of simulated attacks, both physical and cyber. Scheduled to last 36 hours, the “war games” will climax with a simulated national emergency.

[http://www.smartgridnews.com/artman/publish/Technologies\\_Security/Why-NERC-will-attack-the-grid-November-13-and-what-it-could-mean-for-utilities-6152.html/](http://www.smartgridnews.com/artman/publish/Technologies_Security/Why-NERC-will-attack-the-grid-November-13-and-what-it-could-mean-for-utilities-6152.html/)

### **Interview: Mark Weatherford and Cybersecurity for Critical Infrastructure** 2013-11-06

With NIST recently unveiling its ‘Preliminary Cybersecurity Framework’ for critical infrastructure, Drew Amorosi reaches into the vault before his live interview with The Chertoff Group’s Mark Weatherford during today’s Infosecurity Virtual Conference.

<http://www.infosecurity-magazine.com/view/35479/interview-mark-weatherford-and-cybersecurity-for-critical-infrastructure/>

### **Training the Cyber Workforce to Handle New Threats** 2013-11-05

Agencies are getting fresh advice on how to address a perennial weak link in cybersecurity: People.

Agencies are required to have educational and training programs for workers, and the National Institute of Standards and Technology has released a draft revision of Special Publication 800-16, A Role-Based Model for Federal Information Technology/Cyber Security Training.

<http://gcn.com/articles/2013/11/05/cyber-training-nist.aspx>

[http://csrc.nist.gov/publications/drafts/800-16-rev1/draft\\_sp800\\_16\\_rev1\\_2nd-draft.pdf](http://csrc.nist.gov/publications/drafts/800-16-rev1/draft_sp800_16_rev1_2nd-draft.pdf)





## OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS - Continued

### Hackers' Next Target? Maybe Your Facility's Control Systems 2013-11-04

Flash back to Super Bowl XLVII when the entire Superdome was plunged into darkness. Did someone merely flip a switch? Forget to pay the bill? Or was it something more serious? In our post-9/11 world, terrorism immediately comes to mind. In the end, Entergy New Orleans, a unit of Entergy that supplies power to the Superdome, said a relay device had failed, calming most conspiracy theories.

<http://www.cnn.com/id/101163690/page/1>

### Presidential Proclamation -- Critical Infrastructure Security and Resilience Month, 2013 2013-10-31

Over the last few decades, our Nation has grown increasingly dependent on critical infrastructure, the backbone of our national and economic security. America's critical infrastructure is complex and diverse, combining systems in both cyberspace and the physical world -- from power plants, bridges, and interstates to Federal buildings and the massive electrical grids that power our Nation. During Critical Infrastructure Security and Resilience Month, we resolve to remain vigilant against foreign and domestic threats, and work together to further secure our vital assets, systems, and networks.

<http://www.whitehouse.gov/the-press-office/2013/10/31/presidential-proclamation-critical-infrastructure-security-and-resilienc>

### US Cyber Security Framework Developed 2013-10-31

A standards body in the US has published a draft cyber security framework for businesses operating in the telecoms, energy, transport and other critical infrastructure industries.

<http://www.out-law.com/en/articles/2013/October/us-cyber-security-framework-developed/>

### Security Meets the Enemy, and It's the Users 2013-10-25

It is no shock to learn that end users and IT security people often do not see eye to eye. If the security shop had its way, everything would be locked down, and there would be no end users. Users see security as an impediment to doing their jobs. And a recent survey indicates that the divide between users and defenders could be undermining federal cybersecurity.

...with 50 percent of the threat coming from insiders, either intentionally or accidentally, bridging the gap between users and defenders is becoming more important to the security of government networks and systems.

<http://gcn.com/blogs/cybereye/2013/10/end-users.aspx>

<http://www.meritalk.com/cybersecurityexperience>

[http://www.meritalk.com/pdfs/cyber-security-experience/MeriTalk\\_Cyber\\_Security\\_Experience\\_Press\\_Release.pdf](http://www.meritalk.com/pdfs/cyber-security-experience/MeriTalk_Cyber_Security_Experience_Press_Release.pdf)

### Indonesia Overtakes China as Top Source of Cyber Attack Traffic 2013-10-18

Indonesia has overtaken China to become the number one source of cyber attack traffic, according to a report by internet monitoring company Akamai.

<http://www.abc.net.au/news/2013-10-18/an-indonesia-overtakes-china-as-top-source-of-cyber-attack-traf/5032428>

### US Power Plants at Risk 2013-10-18

Power plants in the US and Canada could be at risk of being taken over by cyber attackers, following the discovery of 25 new security vulnerabilities in the protocols used in their critical infrastructure systems.

<http://www.itweb.co.za/index.php?id=68283>

<http://bits.blogs.nytimes.com/2013/10/18/electrical-grid-called-vulnerable-to-power-shutdown/>

### Project SHINE' Illuminates Sad State Of SCADA/ICS Security On The Net 2013-10-16

A global Internet-scanning project focused on finding SCADA/ICS equipment and systems accessible via the public Internet is discovering some 2,000 to 8,000 new exposed devices each day.

Project SHINE, which has been gathering data on SCADA/ICS devices from SHODAN for a year-and-a-half, has identified more than 1 million unique IP addresses thus far, according to Bob Radvanovsky, one of the researchers behind it. "I would say one-fourth or one-third of them are devices that could be vulnerable to malware attacks ... and buffer overflows, cross-site scripting, things of that nature," he says. "[And] we feel the majority are misconfigured or improperly configured."

<http://www.darkreading.com/vulnerability/project-shine-illuminates-sad-state-of-s/240162739>

## OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS - Continued

### **The Long Shadow Of Saudi Aramco**

**2013-10-14**

“Before, we had insecure systems, and it didn’t really matter because we didn’t think of ourselves as a target. No one really knew about it,” says an engineer for a U.S. oil and gas company, who spoke on the condition of anonymity. “Now that we are a hot spot, it necessitates a closer look.”

Big changes in the threat landscape for the energy industry -- think Stuxnet and Saudi Aramco -- have changed the game, especially for the oil and gas industry, which increasingly is finding itself a target by nation-state threats as well as plain-old malware attacks.

The data-destruction attack last year on Saudi Aramco’s internal corporate network that left the oil and natural gas giant having to replace hard drives on some 30,000 or so Windows machines continues to haunt the industry, which witnessed a major player getting hit in a big way.

<http://www.darkreading.com/attacks-breaches/the-long-shadow-of-saudi-aramco/240162634>

### **Cyberthreats Grow More Ominous: Former NSA Chief**

**2013-10-11**

“I think that people need to understand that in the last 12 months there’s been a qualitative change,” said Craig Mundie, senior adviser to the CEO at Microsoft. “The threats are moving to destructive attacks. Unlike conventional weapons, every time someone shoots one of these weapons, the bad guys get to watch it, then clone it.” Gen. Michael Hayden, former director of both the National Security Agency and the CIA, told attendees that U.S. computer networks -- not just government systems, but corporate systems and ordinary citizens’ computers -- face layers of threats.

<http://www.informationweek.com/government/security/cyberthreats-grow-more-ominous-former-nsa/240162556>

### **Microsoft Releases Best Practices for Developing a National Strategy for Cybersecurity**

**2013-10-04**

On Friday, Microsoft released a new white paper entitled Developing a National Strategy for Cybersecurity: Foundations for Security, Growth, and Innovation. This publication is based on lessons learned from customers and governments around the world, and is intended to aid governmental efforts to develop national cybersecurity strategies that set a clear direction to establish and improve cybersecurity for government, academia, enterprises, consumers and the ICT companies who serve those communities.

Cybersecurity issues have developed into significant national-level problems that now require government consideration, including the

protection of assets, systems and networks vital to the operation and stability of a nation and the livelihood of its people.

[http://blogs.technet.com/b/microsoft\\_on\\_the\\_issues/archive/2013/10/04/microsoft-releases-best-practices-for-developing-a-national-strategy-for-cybersecurity.aspx](http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/10/04/microsoft-releases-best-practices-for-developing-a-national-strategy-for-cybersecurity.aspx)

[http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing\\_a\\_National\\_Strategy\\_for\\_Cybersecurity.pdf](http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing_a_National_Strategy_for_Cybersecurity.pdf)

<http://gcn.com/blogs/cybereye/2013/10/global-cybersecurity.aspx>

### **Hackers-For-Hire Group Targeting Government Assets, Report Says**

**2013-09-30**

An analysis of attacks against high-value targets, including government agencies and contractors, has revealed a large and sophisticated organization of professional hackers for hire, say Symantec researchers.

The Hidden Lynx group, located in China, dates to at least 2009 and has been involved several high-profile campaigns, including Operation Aurora, which compromised a number of high-tech companies and government contractors. Although many of the breaches have been reported, a single professional organization’s wide involvement in them had not been documented, said Symantec researcher Liam O Murchu.

<http://gcn.com/articles/2013/09/30/hackers-for-hire.aspx>

[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/hidden\\_lynx.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf)

### **Research detects dangerous malware hiding in peripherals**

**2013-09-26**

A Berlin researcher has demonstrated the capability to detect previously undetectable stealthy malware that resides in graphics and network cards.

Patrick Stewin’s proof of concept demonstrated that a detector could be built to find the sophisticated malware that ran on dedicated devices and attacked direct memory access (DMA).

[http://www.scmagazine.com.au/News/358265\\_research-detects-dangerous-malware-hiding-in-peripherals.aspx](http://www.scmagazine.com.au/News/358265_research-detects-dangerous-malware-hiding-in-peripherals.aspx)

### **Destructive Attacks On Oil And Gas Industry A Wake-Up Call**

**2013-09-23**

A recent Council on Foreign Relations report warns that future cyberattacks on the oil and gas industry could threaten the competitiveness of the U.S. oil and gas industry, pointing to the



## OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS - Continued

Saudi Aramco, Qatar RasGas, and cyberespionage attacks on Chevron and other U.S. oil companies, as warning shots.

While intrusions previously focused on the theft of intellectual property and business strategies, the malware attack on Saudi Aramco reflects a worrying qualitative change toward attacks with the potential for causing physical disruptions to the oil and gas supply chain.

<http://www.darkreading.com/attacks-breaches/destructive-attacks-on-oil-and-gas-indus/240161700>

### **Too Long Passwords Can DoS Some Servers** **2013-09-17**

The discovery of a vulnerability in popular open source web application framework Django has recently demonstrated that using a long password is not always the best thing to do.

Django does not impose any maximum on the length of the plaintext password, meaning that an attacker can simply submit arbitrarily large -- and guaranteed-to-fail -- passwords, forcing a server running Django to perform the resulting expensive hash computation in an attempt to check the password.

<http://www.net-security.org/secworld.php?id=15591>

### **Hacker Group Found in China, Linked to Big Cyberattacks: Symantec** **2013-09-17**

Computer security experts have discovered a group of highly sophisticated computer hackers operating for hire, a U.S. computer security firm said on Tuesday, and it linked the group to some of the best-known cyber-espionage attacks out of China in recent years.

Symantec Corp said the hacker group, which it dubbed "Hidden Lynx," was among the most technically advanced of several dozen groups believed to be running cyber espionage operations out of China.

<http://www.reuters.com/article/2013/09/17/us-cyberattacks-china-idUSBRE98G0M720130917>

### **Hospitals to upgrade computers in response to security risk** **2013-09-09**

Confidential information should be protected by multiple layers of security. A hacker ought to be detected when they have breached the top layer. If there are four of five layers of protection, for example, and each layer takes a hacker several days to penetrate, then the system can defend itself for long enough to work out how to get the hacker out of the network.

Hospital districts have started a large scale upgrading operation due to the problem. Tens of thousands of computers will be upgraded to a newer version of Windows by next spring.

[http://yle.fi/uutiset/hospitals\\_to\\_upgrade\\_computers\\_in\\_response\\_to\\_security\\_risk/6820718](http://yle.fi/uutiset/hospitals_to_upgrade_computers_in_response_to_security_risk/6820718)

## DOCUMENT FAQ

### **What is the publication schedule for this digest?**

ICS-CERT publishes the ICS-CERT Monitor when an adequate amount of pertinent information has been collected.

ICS-CERT provides this newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets. The public can view this document on the ICS-CERT Web page at: [http://www.us-cert.gov/control\\_systems/ics-cert/](http://www.us-cert.gov/control_systems/ics-cert/).

Please direct all questions or comments about the content, or suggestions for future content, to ICS-CERT at: [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov).



## UPCOMING EVENTS



### March

**Industrial Control Systems  
Cybersecurity (301) Training (5 days)  
North American Partners**

**CLOSED**

March 10–14, 2014  
Idaho Falls, Idaho

[Course Description and Registration](#)

### April

**Industrial Control Systems  
Cybersecurity (301) Training (5 days)  
North American Partners**

April 7 - 11, 2014  
Idaho Falls, Idaho

[Course Description and Registration](#)

### June

**Industrial Control Systems  
Cybersecurity (301) Training (5 days)  
International Partners**

June 9 - 13, 2014  
Idaho Falls, Idaho

[Course Description and Registration](#)

## COORDINATED VULNERABILITY DISCLOSURE

ICS-CERT actively encourages researchers and ICS vendors to use a coordinated vulnerability disclosure process when possible. Ideally, this coordinated disclosure process allows time for a vendor to develop and release patches, and for users to test and deploy patches prior to public vulnerability disclosure. While this process is not always followed for a variety of reasons, ICS-CERT continues to promote this as a desirable goal.

Bridging the communication gap between researchers and vendors, as well as coordinating with our CERT/CC and US-CERT partners, has yielded excellent results for both the researchers and vendors. To learn more about working with ICS-CERT in this coordinated disclosure process, please contact ICS-CERT at [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov) or toll free at 1-877-776-7585.

### RESEARCHERS Assisting ICS-CERT with products that were published OCTOBER/NOVEMBER/DECEMBER.

ICS-CERT appreciates having worked with the following researchers:

- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-13-352-01 NovaTech Orion DNP3 Improper Input Validation Vulnerability, 12/18/2013
- Siemens ProductCERT, ICSA-13-347-01 Siemens COMOS Privilege Escalation, 12/13/2013
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-13-346-01 Cooper Power Systems Improper Input Validation Vulnerability, 12/12/2013
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-13-346-02 Cooper Power Systems Cybectec DNP3 Master OPC Server Improper Input Validation, 12/12/2013
- Siemens ProductCERT, ICSA-13-340-01 RuggedCom ROS Multiple Vulnerabilities, 12/6/2013
- Siemens ProductCERT, ICSA-13-338-01 Siemens SINAMICS S/G Authentication Bypass Vulnerability, 12/4/2013
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-13-337-01 Elecsys Director Gateway Improper Input Validation Vulnerability, 12/3/2013
- Researcher Wei Gao of IXIA, ICSA-13-329-01 Triangle Research Nano-10 PLC Improper Input Validation, 11/25/2013





## COORDINATED VULNERABILITY DISCLOSURE - Continued

- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-13-291-01A DNP3 Implementation Vulnerability, 11/21/2013
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-13-297-01 Catapult Software DNP3 Driver Improper Input Validation, 11/19/2013
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-13-297-02 GE Proficy DNP3 Improper Input Validation, 11/19/2013
- Independent researcher Blake, ICSA-13-295-01 WellinTech KingView ActiveX Vulnerabilities, 10/22/2013
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-13-282-01A Alstom e-Terracontrol DNP3 Master Improper Input Validation, 10/21/2013
- Cisco, ICSA-13-289-01 Cisco ASA and FWSM Security Advisories, 10/16/2013
- Independent researchers Timur Yunusov, Alexey Osipov, and Ilya Karpov of the Positive Technologies Research Team, ICSA-13-276-01 Invensys Wonderware InTouch Improper Input Validation Vulnerability, 10/9/2013
- Researcher Carsten Eiram of Risk Based Security, ICSA-13-095-02A Rockwell Automation FactoryTalk and RSLinx Vulnerabilities, 10/7/2013
- Independent researcher Billy Rios, ICSA-13-277-01 Philips Xper Buffer Overflow Vulnerability, 10/4/2013
- Researcher Eireann Leverett of IOActive, ICSA-13-274-01 Siemens SCALANCE X-200 Authentication Bypass Vulnerability, 10/3/2013
- Researchers Dillon Beresford, Brian Meixell, Marc Ayala, and Eric Forner of Cimation, ICSA-13-259-01 Emerson ROC800 Multiple Vulnerabilities, 9/26/2013
- Independent researcher Rubén Santamarta, ICSA-12-018-01B Schneider Electric Quantum Ethernet Module Hard-Coded Credentials, 9/23/2013
- Researchers Kyle Stone and Mehdi Sabraoui, ICSA-13-231-01B Sixnet Universal Protocol Undocumented Function Codes, 9/17/2013
- Researcher Eireann Leverett of IOActive, ICSA-13-254-01 Siemens SCALANCE X-200 Web Hijack Vulnerability, 9/11/2013
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-13-252-01 SUBNET Solutions Inc. SubSTATION Server DNP3 Outstation Improper Input Validation, 9/9/2013
- Researchers Lucas Apa and Carlos Mario Penagos Hollman of IOActive, ICSA-13-248-01 ProSoft Technology RadioLinx ControlScape PRNG Vulnerability, 9/5/2013
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-13-213-04A MatrikonOPC SCADA DNP3 Master Station Improper Input Validation, 8/29/2013
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-13-240-01 Triangle MicroWorks Improper Input Validation, 8/28/2013



### RESEARCHERS CURRENTLY WORKING WITH ICS-CERT IN 2013

ICS-CERT appreciates the following researchers who continue to work with us to resolve exploits:

Aaron Patterson	Eireann Leverett	Mehdi Sabraoui
Aaron Portnoy	Eric Forner	Michael Toecker
Alexey Osipov	Eric Wustrow	Nadia Heninger
Andrew Brooks	Gleb Gritsai	Neil Smith
Anton Popov	Hisashi Kojima	Nin3
Artem Chaykin	Ilya Karpov	Postive Technologies Security
Arthur Gervais	J. Alex Halderman	Reid Wightman
Billy Rios	Joel Langill	Roman Ilin
Bob Radvanovsky	John Adam Crain	Rubén Santamarta
Brendan Harris	Jon Christmas	Ryan Green
Brian Meixell	Juan Vasquez	Sergey Bobrov
Carlos Mario Penagos Hollmann	Jürgen Bilberger	Sergey Gordeychick
Carsten Eiram	Kuang-Chun Hung (ICST)	Shawn Merdinger
Cesar Cerrudo	Kyle Stone	Terry McCorkle
Christopher Scheuring	Lucas Apa	Timur Yunusov
Christopher Sistrunk	Luigi Auriemma	Wei Gao
Dale Peterson	Marc Ayala	Zakir Durumeric
Dillion Beresford	Mashahiro Nakada	

