



Research and Education Networking
Information Sharing and Analysis Center

REN-ISAC

March 2009

Contacts

Executive Director

Mark Bruhn

mbruhn@iu.edu

Director

Doug Pearson

dodpears@ren-isac.net

Principal Security Engineer

Gabriel Iovino

giovino@ren-isac.net

24x7 Watch Desk

ren-isac@ren-isac.net

+1(317)274-6630

<http://www.ren-isac.net>

ISACs in General

- Formation encouraged by U.S. Government Presidential Decision Directive 63: *Protecting America's Critical Infrastructures* (1998) and subsequently affirmed in *The National Strategy to Secure Cyberspace* (2003)
- Collect, derive, analyze, and disseminate security threat information, including:
 - the physical security of infrastructure, operations, and facilities, and
 - computing and networking infrastructures
- Provide resources to support member understanding of threats, protection, and mitigation, so that member organizations can better defend and secure their infrastructures and operations.
- Most are private-sector entities.
- Examples:
 - Communications ISAC
 - Electricity Sector ISAC
 - Emergency Management and Response ISAC
 - Financial Services ISAC
 - Highway ISAC
 - Information Technology - ISAC
 - Multi-State ISAC
 - Public Transit ISAC
 - Surface Transportation ISAC
 - Supply Chain ISAC
 - Water ISAC

The REN-ISAC:

- is an integral part of U.S. higher education's strategy to improve network security through information collection, analysis, dissemination, early warning, and response;
- is specifically designed to support the unique environment and needs of higher education and research organizations;
- and, supports efforts to protect national cyber infrastructure by participating in the formal U.S. ISAC structure.

Trust Community

- The REN-ISAC is a private, member-centered, trusted community for sharing sensitive information regarding cybersecurity threat, incidents, response, and protection, specifically designed to support the unique environment and needs of higher education and research organizations.
- Rigorous guidelines for membership and member vetting are used to engender and maintain a community of trust requisite for sharing sensitive information.

Organization

Host – Indiana University

24x7 Watch Desk is collocated with the network operations center that serves the Internet2, NLR, and international-connecting R&E networks.

Executive Advisory Group (EAG) advises regarding policies, legal issues, plans and strategies, and other non-technical aspects of REN-ISAC operations. EAG members are:

- Jack Seuss, chair University of Maryland-Baltimore County
- Rosio Alvarez Lawrence Berkeley National Laboratory
- Ken Klingenstein Internet2 & University of Colorado
- Rodney Petersen EDUCAUSE
- Marty Ringle Reed College
- Theresa Rowe Oakland University
- Bill Terry Bard College
- Brian Voss Louisiana State University
- Mark Bruhn, ex officio REN-ISAC/Indiana University
- Ken Connelly, ex officio University of Northern Iowa
- Chris Misra, ex officio University of Massachusetts Amherst
- Doug Pearson, ex officio REN-ISAC/Indiana University

Technical Advisory Group (TAG) advises regarding useful REN-ISAC products, services, and methods, guided by evaluation of member needs. Considerations include, but are not limited to: services, information products, information sharing and communication methods, relationships, technical methods to support the trust community and activities, and methods to implement and evaluate services and products. TAG members are:

- Chris Misra, co-chair University of Massachusetts Amherst
- Randy Raw, co-chair Missouri Research and Education Network
- Daniel Aldinolfi Cornell University
- Phil Deneault Worcester Polytechnic Institute
- Brian Eckman University of Minnesota
- Stephen Gill Team Cymru
- Andrew Korty Indiana University
- John Kristoff Team Cymru
- Michael Sinatra University of California Berkeley
- Joe St Sauver University of Oregon
- Gabriel Iovino, ex officio REN-ISAC/Indiana University
- Doug Pearson, ex officio REN-ISAC/Indiana University

Microsoft Analysis Team (MAT) serves as the technical interface between REN-ISAC and Microsoft for their Security Cooperation Program (SCPe) agreement. The MAT guides the objectives for the relationship, and receives, analyzes, and disseminates information shared under the partnership. MAT members are:

- Brian Smith-Sweeney, chair New York University
- David Greenberg Indiana University
- Daniel Schwalbe University of Washington
- Gabriel Iovino REN-ISAC/Indiana University
- Doug Pearson REN-ISAC /Indiana University

Membership Committee (MC) assists with the processes of vetting prospective members, maintaining membership awareness and policy compliance, and membership development. MC members are:

- Ken Connelly, chair University of Northern Iowa
- Tony Maszeroski The University of Scranton
- Keith Schoenefeld The University of Illinois at Urbana-Champaign
- Karen Swanberg University of Minnesota
- James Huval REN-ISAC/Louisiana State University
- Doug Pearson REN-ISAC/Indiana University

Supporting organizations

- Indiana University (host)
- Internet2
- EDUCAUSE
- Louisiana State University

Organizational Relationships

- Internet2
- EDUCAUSE
- Internet2/EDUCAUSE Computer & Network Security Task Force
- National ISAC Council

External contributing relationships

- Team Cymru

Membership:

Membership is open to:

- institutions of higher education,
- teaching hospitals,
- research and education network providers, and
- government-funded research organizations.

Two tiers of membership are differentiated in the degree of vetting of the prospective member representative, and the classification of sensitive information shared in the tier.

Membership guidelines are roughly:

- must be permanent staff,
- with organization-wide responsibilities for cybersecurity protection and response, and
- be nominated for membership by the CIO (tiers 1 & 2) and vouched for by two existing tier 2 members (tier 2)

<http://www.ren-isac.net/membership.html>

As of March 2009 there are 568 individuals representing 262 institutions in the REN-ISAC trust community. Figure 1 represents our member growth.

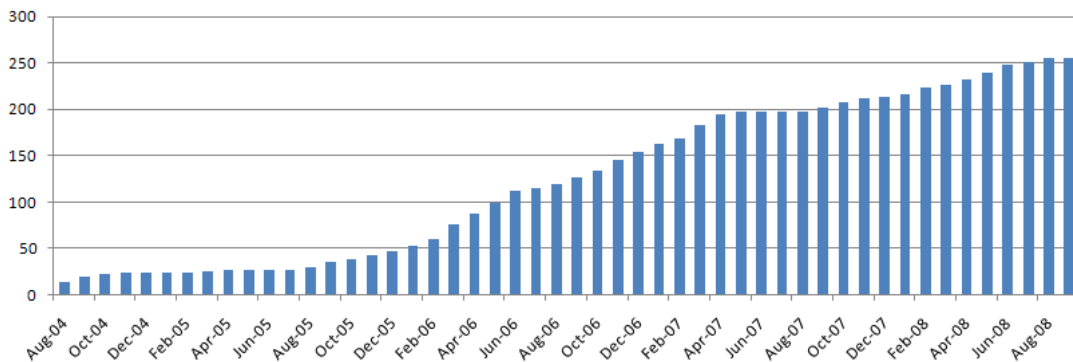


Figure 1

Member Participation

Member participation is a cornerstone of REN-ISAC. A lean central permanent staff provides a set of centrally-based services and facilitates an environment for substantial member contributions to services, tools, and organization.

Member participation takes on forms such as:

- Information sharing w/ peers

- Dedicated commitment of resources (i.e. fixed commitment of %FTE)
- Informal commitment of resources
- Daily reports authoring
- Systems administration
- Educational webcasts
- Sensor and monitor data sharing
- Tool development
- Advisory groups
- Analysis Teams

Members Contributing Substantial Resources

- Bard College (EAG)
- University of California, Berkeley (TAG)
- University at Buffalo (systems and tools)
- Cornell University (TAG)
- The University of Illinois at Urbana-Champaign (MC)
- Indiana University (host, EAG, TAG, MAT, MC)
- Louisiana State University (daily reports, EAG)
- University of Northern Iowa (MC)
- Oakland University (EAG)
- University of Oregon (TAG)
- MOREnet (TAG, TechBursts)
- New York University (MAT)
- Reed College (EAG)
- University of Massachusetts Amherst (EAG, TAG)
- University of Maryland, Baltimore County (EAG)
- University of Minnesota (TAG, MC)
- University of Scranton (MC)
- Team Cyrmu (TAG)
- University of Washington (MAT)
- Worcester Polytechnic Institute (TAG, systems)

Information Resources

The threat intelligence resources that REN-ISAC maintains are:

REN-ISAC members

Sharing incident, vulnerability, and threat information within the private trust community.

External information sharing relationships

With CERTs and private threat collection and mitigation groups, e.g. among network service providers, .edu regional groups, and other private efforts.

Direct reconnaissance

By REN-ISAC security analysts.

Other sector ISACs

Daily inter-ISAC status conference call, and other inter-ISAC communications.

Global Research NOC at IU

The Global NOC provides network operations center and engineering services for the Internet2, National LambdaRail, and international connecting research and education networks

Vendor Relationships

Microsoft / REN-ISAC Security Cooperation Program, Education

Network instrumentation and sensors

- Internet2 Abilene network backbone netflow
- REN-ISAC Shared Darknet
- SES – Security Event System (real-time mid-level event information sharing)
- Global NOC operational monitoring

Information Products

Daily Watch Report

The Daily Watch Report provides situational awareness. Sections of the report deal with critical notices, observations from REN-ISAC sensors, information regarding notable vulnerabilities, exploits, viruses, worms, malware, phishing, social engineering, identify theft, hacks, and data theft or loss. Links and abstracts are provided regarding useful reports, papers, and presentations, tools, and news.

Alerts

Alerts provide timely information concerning new or increasing threat.

Notifications

Notifications are sent regarding specific compromised or vulnerable computers, and computers involved in attacks. Private notifications are sent directly to contacts at the involved sites. A typical notification includes the IP address of the involved machine(s), timestamp, and observed activity. Example notification topics include: worm infected machines, machines that have contacted known malware sites; malware sites, botnet C&C and drones, and systems identified as vulnerable to specific threats. Direct notifications are sent to members of the EDU sector, regardless of REN-ISAC membership status.

Figure 2 illustrates the volume of REN-ISAC notifications to EDU sites July 2006 – April 2008.

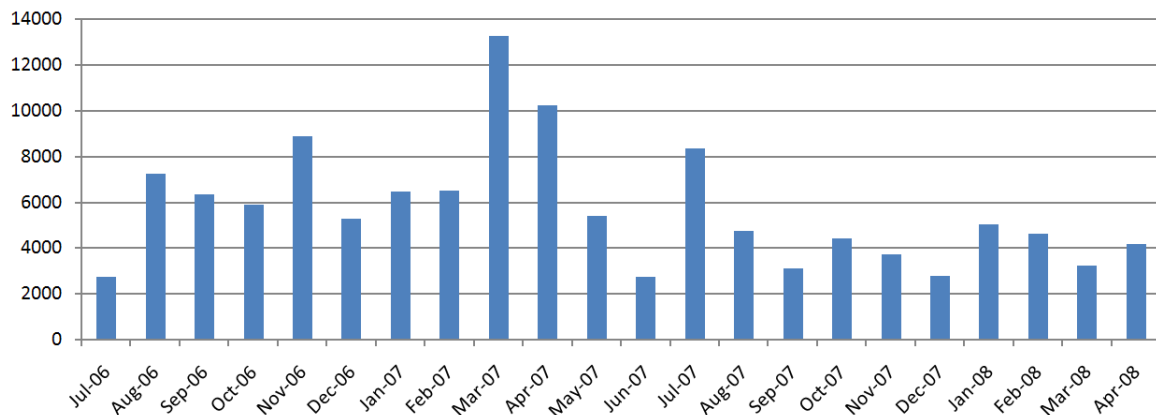


Figure 2 – Monthly Notifications

Figure 3 illustrates specifically Storm Worm notifications during the period Feb – Aug 2007. Beginning Feb 2007, a REN-ISAC member researcher infiltrated the Storm Worm P2P network and began providing a source of ongoing intelligence regarding compromised systems operating in the Storm botnet. Notifications to affected sites quickly drove down the infected population.

In mid-July the highly successful e-card vector started. Again, although success of the vector was initially strong, we were able to quickly drive down the infection. Storm-based DDoS activity began late June/early July. REN-ISAC detected and responded to approximately a dozen Storm-sourced DDoS events that transited the Internet2 network. On September 9, REN-ISAC issued an Alert, "Storm Worm DDoS Threat to the EDU Sector". On September 11, the Microsoft MSRT (Malicious Software Removal Tool) was updated for Storm on 9/11

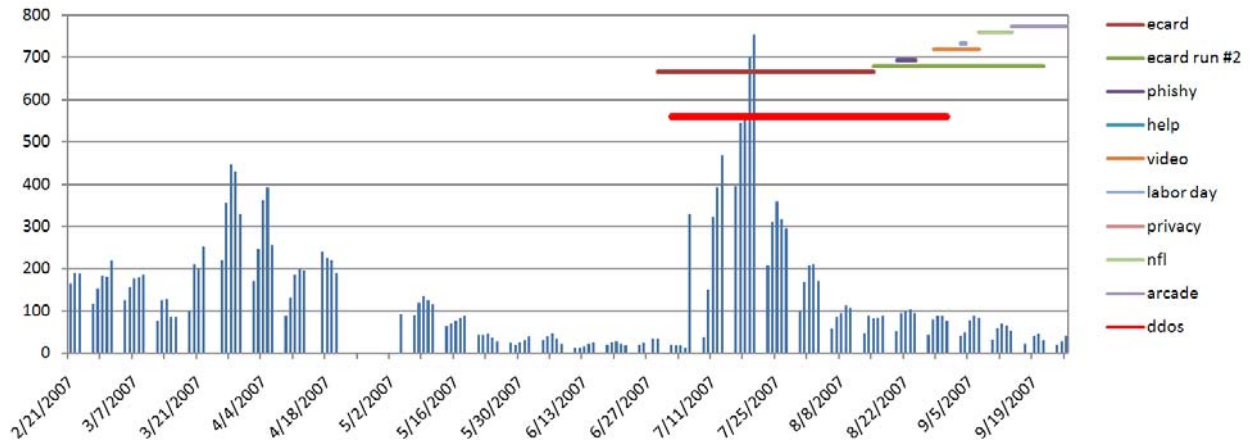


Figure 3 – Storm Worm Notifications Feb – Aug 2007

Figure 4 illustrates the number of notifications sent to EDU sites regarding botnet command and control (C&C) hosts, during the period January 2006 through March 2007. Generally, miscreants will place C&C's in perceived safe havens. In Jan 2006, EDU was a safe haven. At that time REN-ISAC undertook an aggressive effort to eradicate C&C's. The sustained reduction likely indicates that miscreants chose to place their important infrastructure in other Internet space.

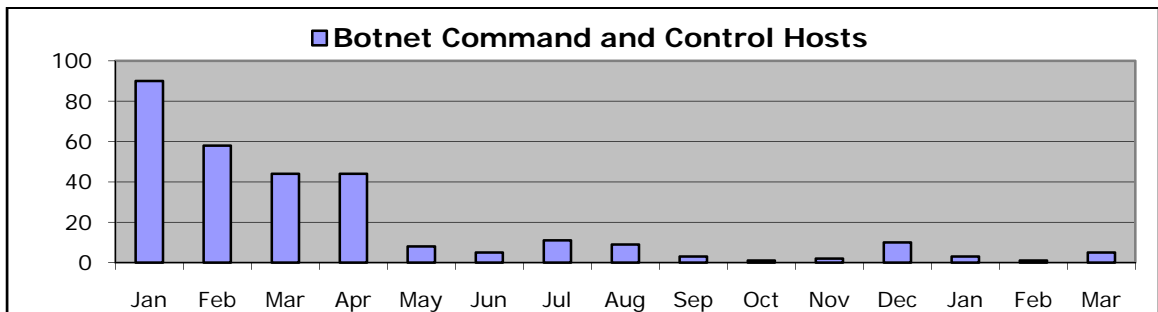


Figure 4 – Botnet Command and Control Hosts

Threat Information Resources

Threat Information Resources are datasets regarding known active sources of threat. Examples include known active botnet command and control hosts and malware sites. Data is refreshed every half hour. Members use these datasets in conjunction with their local protection and

response methods, e.g. in IP and DNS block lists, sensor signatures, and in conjunction with mining of DNS logs or netflow data for identification of local compromised machines.

Monitoring views

Publicly-accessible views of activity on common application and threat vector IP ports are published to the REN-ISAC web pages, <http://www.ren-isac.net/monitoring.html>. For example, Figure 5 illustrates activity on UDP/53 (DNS) on the Internet2 network, with three days of unusual and suspicious increased activity.

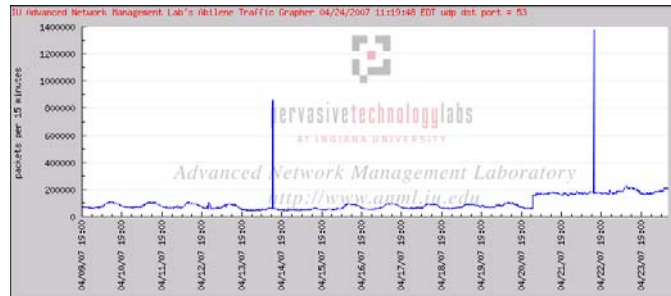


Figure 5

Education

TechBurst webcasts inform members on technical topics relevant to security protection and response. The live and archived webcasts are presented monthly by members and are open only to the trust community members – permitting discussions on sensitive topics. TechBurst examples include:

- BotNet Detection Using DNS Methods
- Netflow Advanced Topics
- DNS: Protocols, Operation and Security

Advisories inform regarding specific practices or approaches that can improve security posture. A recent example is an Advisory discussing open, recursive DNS servers, reasons why open recursive servers are bad, what sites should do about them, and links to additional sources of information.

Peer interaction, supported on IRC and mailing list, provides a substantial source of informal education.

Security exercises

REN-ISAC has participated in sector-specific exercises, e.g. with the Internet2 organization, and in national-level exercises, e.g. DHS CyberStorm II.

Tools

Tools providing direct services to the members:

- Communications
 - wiki
 - IRC
 - mailing lists
- Community Plumbing
 - web-based community-building tools to support member-contributed project development, and member subgroups for specific interest topics
- Cyber Security Registry
 - deep and rich information about site security contacts and the institutions
- Malware Analysis Infrastructure for R&E (under development)
 - malware sandbox and repository; working in cooperation and with contribution from CWSandbox; talks in progress with Norman
- SES – Security Event System (under development)
 - Provides standards-based (IDMEF and IODEF) collection, transport, storage, and representation of mid-level security event data, and aggregation and correlation, in an extensible framework. Development in cooperation with Internet2 and funded through a grant from the Department of Justice.
- RENOIR (under development)
 - Research and Education Networking Operational Incident Repository provides trust community-based sharing of incident information. Development in cooperation with the Internet2 SALSA CSI2 effort.

Monitors and sensors

- Internet2 netflow collection and analysis
 - Arbor Networks Peakflow
 - Flow-tools
 - Traffic Grapher (developed by IU Advanced Network Management Lab (ANML))
- Shared Darknet
 - Data from dispersed, member-based darknet sensors is combined to a single community resource. Notifications of observed scanning sources and reports of aggregate statistics are provided from the collected data. Development in cooperation IU ANML.

Other tools

- .edu notification system

Priorities for 2009

- Membership growth
- Facilitate various forms of member involvement and contribution
- Develop additional and strengthen existing information sharing relationships
- Assessment of current services and member needs
- Implementation of new business model (fee-based membership)
- Tool/service projects (development projects listed under Tools)