20TH ANNIVERSARY OF THE IT-ISAC

2 DECADES OF COLLABORATIVE INFORMATION SHARING AND ANALYSIS

MISSION:

Our mission is to grow a diverse community of companies that leverage information technology and have in common a commitment to cyber-security. We serve as a force multiplier that enables *collaboration* and *sharing* of relevant, actionable cyber threat information and effective security policies and practices for the benefit of all.

WHAT WE DO:

We go beyond information sharing by focusing on four key actions: *Innovate, Share, Analyze, and Collaborate.* We have established a one-of-its kind forum which assembles some of the brightest minds from the world's leading IT companies to minimize threats, manage risk, and respond to cyber incidents.

INNOVATE

- Pioneered the functions "based approach" to sector-wide risk management, which is now being applied by DHS through its "National Critical Functions" approach.
- Provided the road map for a joint industry-government operations center, which is now the DHS NCCIC.
- Developed and piloted a concept of operations for information sharing across industry and government.
- Driving the development of a Coordinated Vulnerability Disclosure program within the Elections Industry.
- Founder of the National Council of ISACs and IT Sector Coordinating Council.
- Won ISAO Standards Organization's Hall of Fame award for contributions to the information sharing community.

SHARE

- Partnership with TruSTAR intelligence management platform provides members enhanced analytics and enables members to use automation to receive and share indicators.
- Distribute our Daily Open Source product to global information community.
- Leverage the National Council of ISACs to share intelligence across the critical infrastructure community.

ANALYZE

- Provide members tactical & strategic intelligence needed to manage threats to their enterprises.
- Weekly VEAR report provides detailed information on significant but not widely publicized vulnerability exploits.
- Leverage TruSTAR platform to connect individual indicators to specific incidents, threat actors, and campaigns.
- Develop incident specific analytic reports on high profile attacks, exploits and vulnerabilities.

COLLABORATE

- Engage analysts from leading global technology companies through the IT-ISAC Technical Committee.
- Develop industry leading white papers on emerging security topics.
- Discuss common security issues unique to the food and agriculture or elections industries through our Special Interest Groups.
- Leverage global network of subject matter experts across the critical infastructures through the National Council of ISACs.

ORGANIZATIONAL MILESTONES

2000

Dec. IT leaders establish the IT-ISAC

2001

July IT-ISAC goes "operational" with a contract with ISS to provide 24/7 operational support

2002

May Established formal MOUs with Financial Services. Electricity, Energy, and Telecom ISACs

2003

National Council of ISACs is established

June IT-ISAC helps establish the ISAC Council, now known as National Council of ISACs

Aug. IT-ISAC launches cross sector coordination through the ISAC Council

2005

Aug. IT-ISAC Hires First Executive Director

April IT-ISAC participates in DHS TopOff 3 Excercise

2006

Jan. IT-Sector Coordinating Council (IT-SCC) forms and recognizes the IT-ISAC as the sector's official information sharing mechanism

Feb. IT-ISAC coordinates the IT-Sector's participation in DHS' first Cyber Storm excercise

Dec. Released an updated and revised ConOps to members

2008

Jun. IT-ISAC enters an information sharing MOU with InfraGard

2009

Aug. IT Sector Working Group, chaired by the IT-ISAC, releases IT Sector Baseline Risk Assessment which identified a functions based approach to managing critical functions

2011

Apr. IT-ISAC participates in National Level Excercise

2012

Dec. IT-ISAC is the first organization to sign a CRADA agreement with U.S. Department of Homeland Security

2013

Oct. IT-ISAC forms Food & Ag SIG

2018

Aug. IT-ISAC creates Elections Industry SIG

Sep. IT-ISAC is awarded ISAO Standards Hall of Fame Award

Nov. IT-ISAC is appointed to DHS ICT Supply Chain Risk Management task force

2015

Sep. IT-ISAC deploys automated information sharing capability

2016

Mar. IT-ISAC joins DHS AIS program

2019

Apr. DHS release of critical functions list

Nov. MOU with ICT-ISAC Japan

INCIDENT RESPONSE MILESTONES

The IT-ISAC participated in the response to various cyber security incidents over the years. Below you will find a sampling of pertinent incidents that have occured over the last 20 years. Our analysts researched events, fact checked sources, and leveraged members input to provide reliable reports to our member companies.

2001

- July — IT-ISAC responds to Code Red Attack
- Sep. — IT-ISAC responds to NIMDA

2003

- 2003 — Hacktivist group, "Anonymous" is formed

2004

- Oct. — Hackers called 'Titan Rain,' steal important information from NASA and military lab networks

2006

- May — Biggest web defacement in Web History by iSKORPiTX

2008

- July — Issued joint bulletin with FS and Comm ISACs on Kaminsky DNS Cache Poisoning
- Sep. — IT-ISAC and other ISACs deploy to DHS NICC for first time for hurricane response

2009

- Apr. — IT-ISAC responds to Conficker Worm

2010

- Sep. — Stuxnet launched

2011

- 2011 — Beginning of Iranian DDoS attacks against Wall Street
- Mar. — APT actors steal token credentials from RSA.

2012

- Aug. — Attack on Saudi Aramco fries thousands of machines

2013

- Mar. — Spamhaus is attacked by the largest DDoS attack in history

2014

- 2014 — Yahoo data breach
- Mar. — Office of Personnel Management data breach
- Nov. — North Korea attacks SONY Picture Studios

2015

- Dec. — Black Energy 2015, considered to be the first known successful cyberattack on a power grid

2016

- Aug. — Shadow Brokers campaign revealed
- Nov. — Foreign powers use IT to interfere in elections

2017

- Jan. — Heartbleed bug puts hundreds of thousands of servers at risk
- May — WannaCry ransomware attacks 200,000+ Windows computers

2018

- Jan. — Meltdown and Spectre exploit critical vulnerabilities in computing devices

2019

- Jan. — DNS hijacking impacts govt. domains, telecommunications and infrastructure
- May — Turla Group employs Microsoft exchange BackDoor

CONNECT WITH US:

@it-isac

linkedin.com/company/it-isac/

703-385-4969

P.O. Box 471
Manassas, VA 20108

membership@it-isac.org

it-isac.org