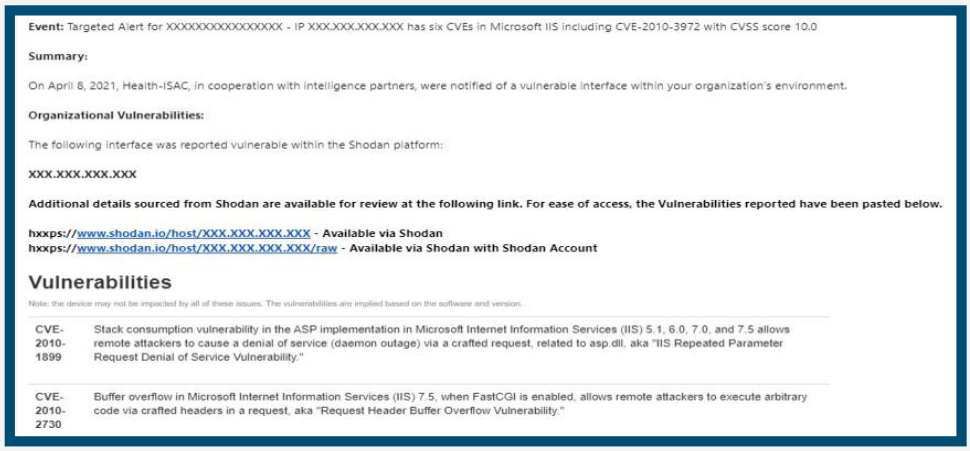
Now Hear This: Targeted Alerts Right to Your Desktop!

The TOC now has the ability to pass compromised credentials, exposed Remote Desktop Protocol (RDP) and Common Vulnerabilities and Exposures (CVEs) linked to an IP address right to your door.

In the case of exposed RDP, the TOC also passes along a screenshot and timestamp of the instance so that members can determine when the exposure occurred.



Event: Targeted Alert for XXXXXXXXXXXXXXXX - IP XXX.XXX.XXX.XXX has six CVEs in Microsoft IIS including CVE-2010-3972 with CVSS score 10.0

Summary:

On April 8, 2021, Health-ISAC, in cooperation with intelligence partners, were notified of a vulnerable interface within your organization's environment.

Organizational Vulnerabilities:

The following interface was reported vulnerable within the Shodan platform:

XXX.XXX.XXX.XXX

Additional details sourced from Shodan are available for review at the following link. For ease of access, the Vulnerabilities reported have been pasted below.

hxxps://www.shodan.io/host/XXX.XXX.XXX.XXX - Available via Shodan
hxxps://www.shodan.io/host/XXX.XXX.XXX.XXX/raw - Available via Shodan with Shodan Account

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2010-1899	Stack consumption vulnerability in the ASP implementation in Microsoft Internet Information Services (IIS) 5.1, 6.0, 7.0, and 7.5 allows remote attackers to cause a denial of service (daemon outage) via a crafted request, related to asp.dll, aka "IIS Repeated Parameter Request Denial of Service Vulnerability."
CVE-2010-2730	Buffer overflow in Microsoft Internet Information Services (IIS) 7.5, when FastCGI is enabled, allows remote attackers to execute arbitrary code via crafted headers in a request, aka "Request Header Buffer Overflow Vulnerability."

To make these targeted alerts as timely as possible, and allow you to act quickly to remediate, please ensure H-ISAC has an Intelligence POC and an up-to-date internal security distribution list for your organization. You can send the applicable information along with any questions to contact@h-isac.org.

Intelligence Island Summit in San Diego, California.
Nov 30—Dec 2, 2021

Agenda is now available!

View the agenda here or go to our website:

https://web.cvent.com/event/f1465e19-27ed-4efb-b152-15b79504f4fb/summary

Also, Registration is Now Open!

Be on the lookout for Intelligence Island Specials! This month the first 50 registrants will be entered in a raffle and three lucky winners will receive either a spa treatment or a room upgrade. Also, we are having "SS Minnow Uncharted" deals that will kick off on September 26th in honor of the day Gilligan's Island first aired.

Register here: https://h-isac.org/summits/intelligence-island-fall-2021-summit/

Top Health Related Cyber & Physical Events for September:

Colonial Pipeline Reports Data Breach after Ransomware Attack

AlphaBay Darknet Market Comes Back to Life

Microsoft Confirms New Windows Print Spooler Zero-Day Bug

Microsoft August 2021 Patch Tuesday Fixes 3 Zero-Days, 44 Flaws

US Distributor Warns of Medical Supply Shortage

Healthcare Industry Has Highest Number of Reported Data Breaches in 2021

Loopholes in Thailand's COVID-19 Vaccine Appointment Website Lead to Data Breach

PwnedPiper Critical Bug Set Impacts Major Hospitals in North America

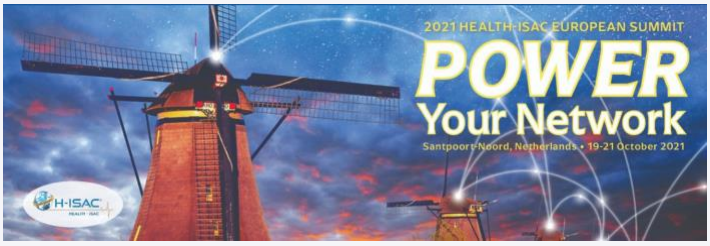
DoppelPaymer Ransomware Gang Rebrands as the Grief Group

California to Become First State Requiring Vaccines for Health Care

H-ISAC is pleased to publish a monthly member newsletter. It is designed to bring events and other important ISAC information to your attention. If there is something you would like to see included, please email: contact@h-isac.org

@H-ISAC @HealthISAC @Health-ISAC

EUROPEAN SUMMIT



Power Your Network Summit in Santpoort-Noord, Netherlands. 19-21October, 2021

Call for Papers closes September 14

Submit content here: https://h-isac.org/summits/power-your-network-2021/

Registration is open!

Register here: https://h-isac.org/summits/power-your-network-2021/

Just minutes from the beach and dunes of the North Sea, close to major cities like Amsterdam and Haarlem and located in gorgeous Zuid Kennermerland National Park, with its hundreds of kilometres of trails, the stately and historic Duin & Kruidberg Country Estate will provide the perfect environment to learn from and network with your peers.

And you won't want to miss the Summit keynote speaker, Mikko Hypponen. He led his team through some of the largest computer virus outbreaks in history.

Be sure to register today!

UPCOMING UPGRADE

The Health-ISAC Threat Intelligence Portal will be Upgraded on September 7.

The 3.0 version boasts a new look and builds in several user-requested features. Members will have new messaging abilities, multi-question polling capabilities, more complex search filters, guided walkthrough and tutorial videos, and improvements to the Doc Library that include sharing documents with other member analysts, marking favorite documents for later use, and also storage of personal threat intelligence documents prior to analyst distribution.

Look for more information coming soon. Get your questions answered on the HTIP upgrade—or any Health-ISAC product—by dropping by the "office" during a TOC Office Hour session on **Thursdays 10-12pm EST.**

CALL FOR PEER REVIEW

HHS 405(d) Aligning Health Care Industry Security Approaches

Health-ISAC members are asked to review the version 2.0 update to the Health Industry Cybersecurity Practices (HICP) publication. HHS is looking to form several 'virtual focus groups' to review the latest HICP draft and provide critical feedback. They are looking to break these focus groups into two sections: clinical and administrative staff, and IT and cyber staff.
Learn more here:
https://h-isac.org/health-industry-cybersecurity-practices-publication-peer-reviews-needed/.

HEALTH-ISAC WORKING GROUPS

New working group! **Cyber Threat Intelligence Program Development**

Looking to initiate or increase the maturity of your organization's Cyber Threat Intelligence (CTI) program? Join the CTIPD, to discuss the development of these programs within member organizations of all sizes and develop best practices and guidance to provide the tools necessary to build a CTI program tailored to your organizational needs. The CTIPD will meet biweekly starting on Wednesday the 8th of September from 12-1PM EDT. To join, reach out to contact@h-isac.org.

UPCOMING EVENTS — Or visit our Events Page https://h-isac.org/events/

NAVIGATOR WEBINARS

Building The Ransomware Security Stack in Your Organization by FireCompass
September 14 at 1pm EDT
https://h-isac.org/hisacevents/building-the-ransomeware-security-stack-in-your-organization-by-firecompass/

Top 5 Active Directory Configurations Every Healthcare Organization Should Secure by Tenable
September 15 at 1pm EDT
https://h-isac.org/hisacevents/top-5-active-directory-configurations-by-tenable/

H-ISAC HEALTH - ISAC

Health-ISAC Healthcare Cybersecurity Workshop

Hosted at Emory University Atlanta, Georgia

Monday, September 20 1-4:30pm EDT

https://h-isac.org/hisacevents/h-isac-healthcare-cybersecurity-workshop-hosted-by-emory-university/

H-ISAC HEALTH - ISAC

Exercise sponsored by ordr

Rethinking Resiliency: Virtual Exercise Series #4

Thursday, September 23 12pm EDT

https://h-isac.org/hisacevents/rethinking-resiliency-a-virtual-exercise-series-4/

H-ISAC HEALTH - ISAC

Health-ISAC Monthly Member Threat Briefing TLP AMBER

Tuesday, September 28 12pm EDT

https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-september-28-2021/