Center For Internet Security Funds No-Cost Service to Help Protect all U.S. Private Hospitals Against Ransomware

The Malicious Domain Blocking and Reporting Service is also available to all U.S. public hospitals via no-cost membership in the MS-ISAC.

EAST GREENBUSH, N.Y., Feb. 17, 2021 – The Center for Internet Security, Inc. (CIS®) is launching a no-cost ransomware protection service, Malicious Domain Blocking and Reporting (MDBR), for private hospitals in the U.S. today. CIS is fully funding this service for all private hospitals in the U.S. as part of its nonprofit mission to make the connected world a safer place. The service is already available for all public hospitals, health departments, and healthcare organizations through the Multi-State Information Sharing and Analysis Center (MS-ISAC). MS-ISAC funding for public hospitals is provided by the U.S. Department of Homeland Security's (DHS) Cybersecurity & Infrastructure Security Agency (CISA).

Ransomware has emerged as the largest cyber threat facing hospitals today, especially since the onset of the COVID-19 pandemic. Ransoms demanded from cybercriminals to unlock systems and files have exceeded millions of dollars. In some cases, patient care has even been delayed or cancelled due to locked-out digital medical records and treatment regimens.

Protecting against the threat of ransomware is now a top priority for hospitals and systems. Especially in the time of COVID, when you have to act fast and information is paramount, this new service can serve as a critical component of hospital security.

The MDBR service is being offered from CIS with the support of technology partner Akamai, the world's most trusted solution for securing and delivering digital experiences. The service leverages Akamai's Enterprise Threat Protector edge security service which proactively blocks network requests from an organization to known harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats.

MDBR can help protect hospital IT systems against ransomware attacks by stopping them before they occur. To learn more and sign up for CIS's MDBR service for U.S. private and public hospitals visit: https://www.cisecurity.org/hospitals/

"The CIS Board of Directors prioritized making MDBR service available to all public and private U.S. hospitals at no cost, through both the MS-ISAC for public hospitals, and a $1 million investment of CIS funds for private hospitals this year. CIS is fully funding this for private hospitals at no cost, and with no strings attached because it's the right thing to do and no one else is doing it at scale," said Ed Mattison, Executive Vice President of CIS Operations and Security Services. "The COVID-19 pandemic has made hospitals an even larger target for malicious cyber threats than they were already. While other commercial cybersecurity organizations are certainly supporting hospitals and hospital systems, our nonprofit status and mission focus enable us to offer this service at no cost and at scale to any hospital or system that can benefit from it," he said.

More than 1,000 U.S. State, Local, Tribal, and Territorial (SLTT) government organizations already have a successful track record using MDBR through a federally funded pilot program via the MS-ISAC.

Since its inception, and through the beginning of this year, the MDBR service has blocked more than 748 million requests for known and suspected malicious web domains, which might have resulted in a ransomware infection or other harmful cyber-attacks on SLTT organizations. MDBR provides an additional layer of cybersecurity protection that is proven, effective, and easy to deploy.

In December 2020, there were nine instances of ransomware domains being blocked by MDBR for a group of nine U.S. public health organizations already on the service through the MS-ISAC – any one of which could have resulted in a major cyber incident. Additionally, during the same month, MDBR prevented malicious requests for the following types of cyber-attacks:

- 4,200+ known malware domains
- 500+ known phishing domains
- 15 known command-and-control (C&C) domains

Recognizing the heightened cyber threat against the U.S. healthcare system and the crucial importance of protecting and maintaining patient care and operations, CIS and Akamai are offering this service at no cost to the following U.S. based health care organizations:

- Independent hospitals
- Multi-hospital systems
- Hospital-based integrated health systems – an organization, consisting of one or more hospitals plus at least one or more groups of physicians, that provides a continuum of care and that are connected to each other through joint ownership or joint management
- Post-acute patient care facilities
- Psychiatric, rehabilitation, or other specialty hospitals

CIS and Akamai encourage all U.S. hospitals to use MDBR and embrace a broader risk management approach to cybersecurity.

"Protecting the U.S. healthcare system against prevalent cyber threats should be viewed as a patient safety, enterprise risk, and strategic priority," said Mattison. "Proven cybersecurity defenses should be installed into existing enterprise, risk management, governance, and business-continuity frameworks."

MDBR is an effective and easy way to implement tools in the defense-in-depth or multi-layered approach to cybersecurity best practices that can help prevent cyber threats against hospital systems before they start.

About CIS

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously refine these standards to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial

(SLTT) government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the cybersecurity needs of U.S. elections offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

Contact: Barbara Ware
Barbara.Ware@cisecurity.org
Cell: (518) 526–4525