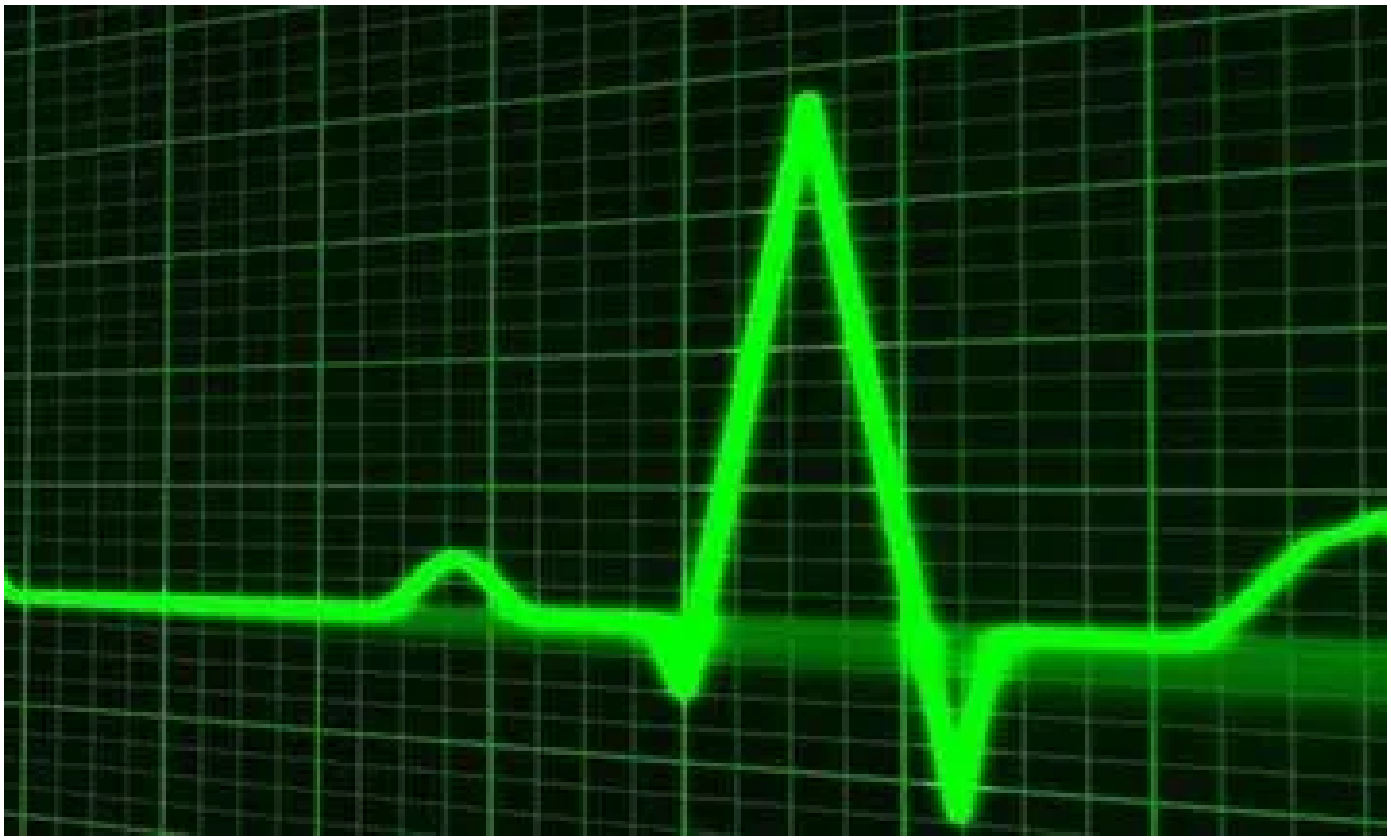
Alert
A CRA Resource

Content, Content

Cybersecurity Volunteers Defend Healthcare Organizations From Cyberattacks

D. Howard Kass April 24, 2020



Credit: Pixabay

Hundreds of cybersecurity professionals worldwide have banded together in separate groups to protect hospitals and healthcare facilities treating coronavirus (Covid-19) victims from hackers trying to steal confidential information.

One of the ad-hoc organizations calling itself the Covid-19 CTI League includes some 1,400 cybersecurity volunteers in 76 countries who work in critical

Another group, the European-based Cyber Alliance to Defend Our Healthcare, was formed by London-based C5 venture capital after a number of its clients in the United Kingdom's and Sweden's healthcare sector were hit by hackers, a report in *The Hill* said. More than a dozen information security outfits reportedly participate in the Cyber Alliance.

"There is a literal army of infosec people out in the community who are working to protect these establishments," Marc Rogers, Okta's cybersecurity executive director and a CTI League leader, told *The Hill*. "We haven't seen any catastrophic situations yet, and I'm quietly hopeful that that's because of the proactive work that all of these groups are doing."

Similarly, the Cyber Alliance's impetus came from a spike in cyber attacks directed at healthcare facilities launched by cyber gangsters and nation states, C5 founder Andre Pienaar told *The Hill*. "We decided we had to do something to help, and launched the Cyber Alliance to Defend Our Healthcare as part of a transatlantic effort to protect the crucial care provided by hospitals and clinics," he reportedly said. Ransomware has been the cyber crooks' weaponry in the hacks, with ransom demands recently to upwards of $15 million," according to Pienaar.

Collaborating with law enforcement, including the Federal Bureau of Investigation and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), is a key feature of the groups. "We have seen, and are likely going to continue to see, an increase in bad guys taking advantage of the COVID-19 pandemic to target businesses, governments and individuals alike," CISA Director Christopher Krebs told *The Hill*. CTI has helped "disseminate indicators of compromise to network defenders, improve vulnerability management in the nation's medical infrastructure, and manage supply chain risks in the medical

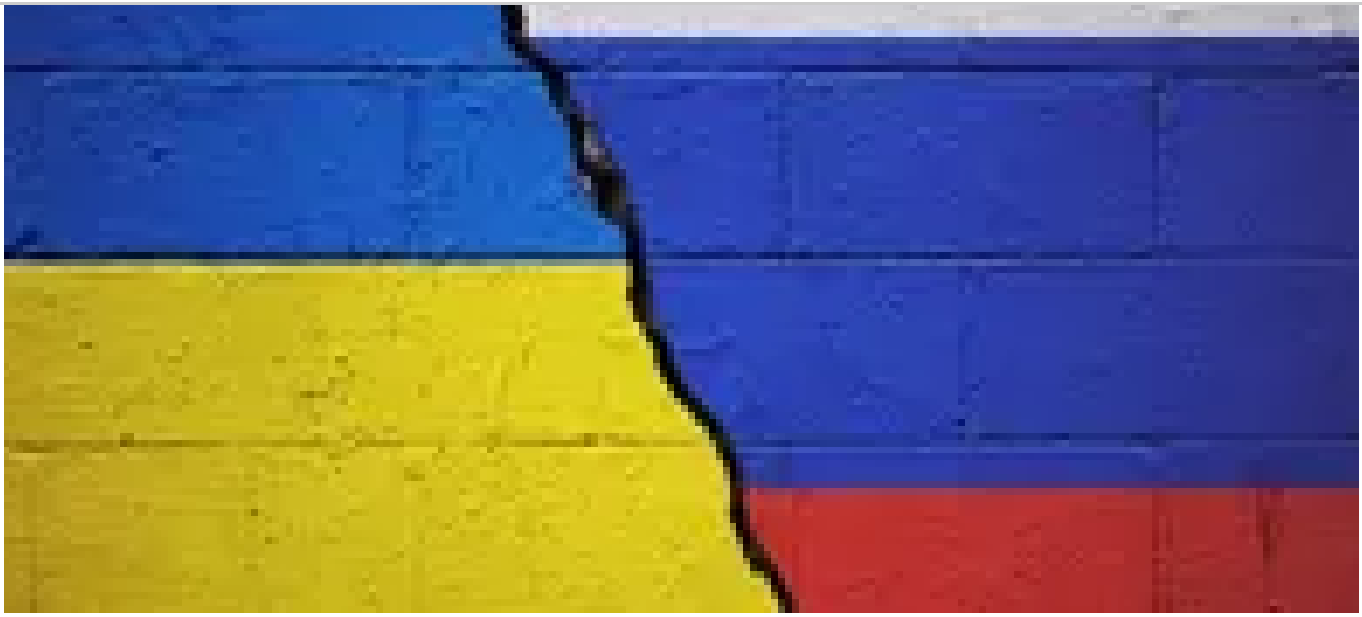
- Provide private and public threat intelligence on attacks on the healthcare sector.
- Coordinate with government agencies to increase public awareness.
- Support the National Guard to help state and local public health agencies defend against breaches.
- Convene partners in the healthcare, public health, and research sectors on cybersecurity resources needed to defend healthcare IT systems.
- Consider issuing public statements regarding hacking operations and disinformation related to the coronavirus.
- Evaluate further actions to detect and deter attacks on healthcare information technology.

“The Cybersecurity and Infrastructure Security Agency and Cyber Command are on the frontlines of our response to cybersecurity threats to our critical infrastructure,” the senators wrote. “Hospitals, medical researchers, and other health institutions need the expertise and resources your agencies have developed defending against these same sophisticated threats.

Sens. Mark Warner (D-VA), Ed Markey (D-MA), Richard Blumenthal (D-CT), David Perdue (R-GA) and Tom Cotton (R-AK) signed the letter.

D. Howard Kass

Related

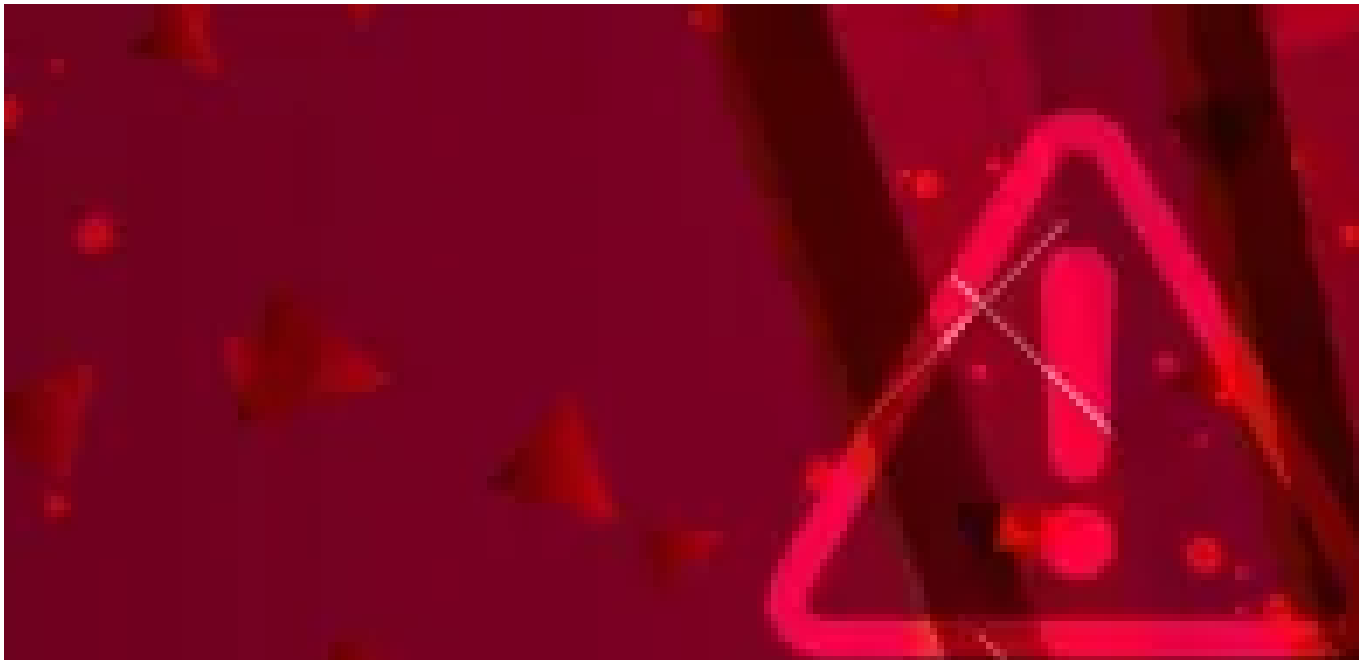


CONTENT

Russia-Ukraine War: Cyberattack and Kinetic Warfare Timeline

Jim Masters October 25, 2023

Russia's invasion of Ukraine features alleged cyberattacks. Follow this Russia-Ukraine conflict timeline for cyber & kinetic warfare updates, and guidance for MSSPs worldwide.



CONTENT

Cyber Prevention, Training Attract More Spend Than Remediation, Recovery, Execs Say

D. Howard Kass August 16, 2023

A new study by Information Services Group found that companies are more likely to spend money on cyber protection and increased training.