Header

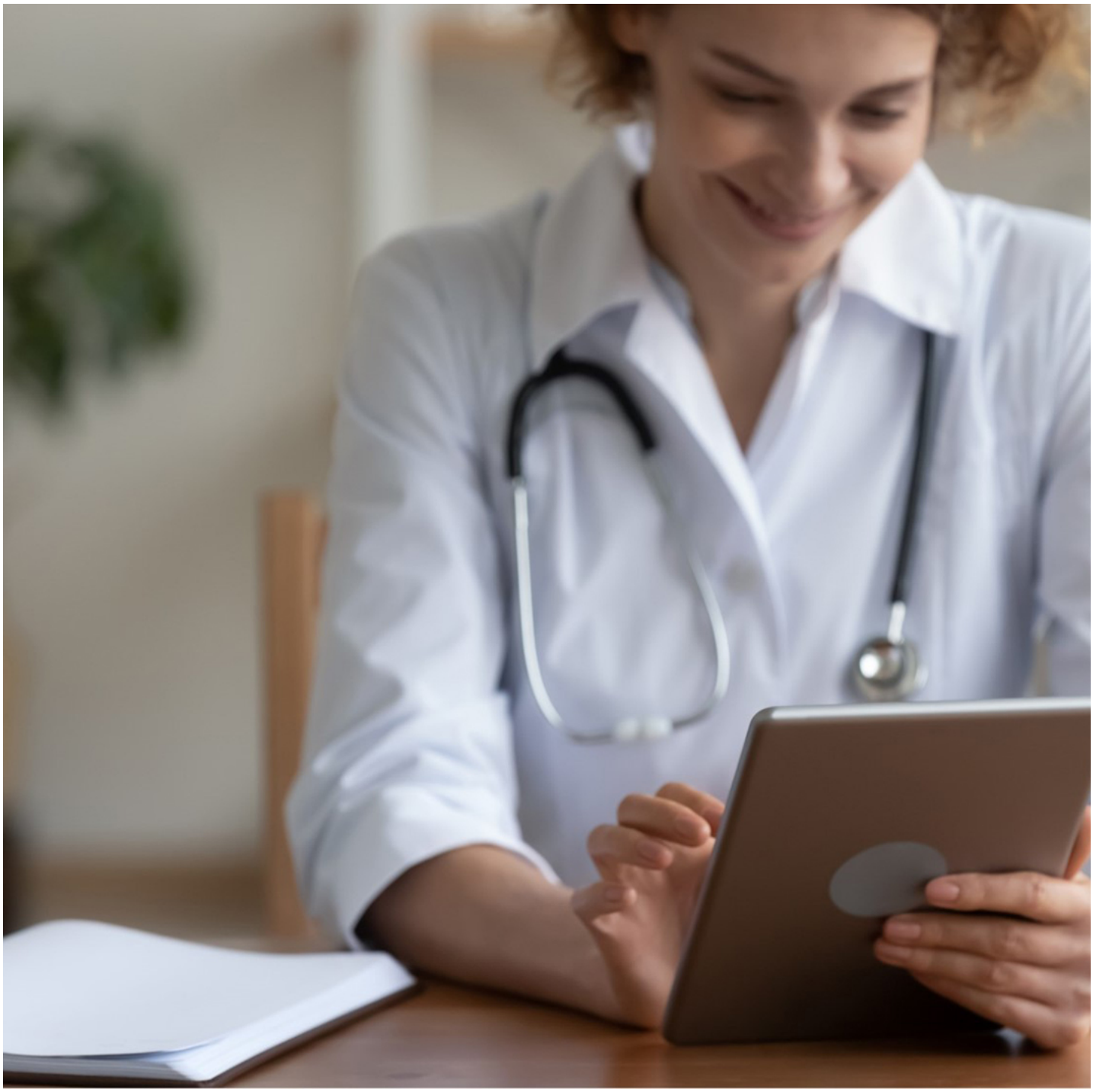
Defens
Defens

- Solution
- Features
- Use Cases
- Resources
- Pricing
- Partner Login

Buy from

Growing Collaboration Among Criminal Groups Heightens Ransomware Threat for Healthcare Sector

Growing Collaboration Among Criminal Groups Heightens Ransomware Threat for Healthcare Sector



As Healthcare Organizations are Heightened Targets for Adversaries, the CTI Weighs In

One of the most inspiring initiatives to come out of the deadly COVID-19 pandemic is The Cyber Threat Intelligence League (CTI League). Their mission, since forming in March 2020 as the virus exploded and impacted front line workers in unprecedented ways, is to “Create a safer cyber space for the medical sector and the life-saving organizations.”

The CTI League aspires to protect the medical sector and the life-saving organizations (MS-LSO) worldwide from cyber-attacks, supplying reliable information, reducing the level of threat, supporting security departments, and neutralizing cyber threats, according to their website.

Recently, the League published a report warning healthcare organizations to “expect increase in ransomware and 'triple extortion' attacks.”

This global volunteer emergency response center for healthcare organization said in a report that they expect ransomware attacks and activities, including the trading and selling of databases containing protected health information (PHI) to increase in 2021.

They defined "Triple Extortion Attacks” as those involving the use of ransomware, data theft, and distributed denial-of-service (DDoS) attacks to extort money from healthcare entities.

The League says it tracked increased demand in 2020 for backdoor access to healthcare along with an increase in the number of brokers leaking, acquiring, and selling that access.

They wrote about COVID-19-themed campaigns continuing to be a central part of phishing, social engineering scams, and information campaigns as society continues to deal with the chaos and uncertainty associated with Work-From-Home, testing and vaccine programs.

Even as new variants of the COVID-19 virus continue to morph, Sean O'Connor, leader of the CTI League's Dark team, warned healthcare organizations to expect attacks in 2021 to grow.

A major factor is the growing communication and collusion within the cybercriminal ecosystem on ransomware attacks targeting the healthcare sector.

The CTI League includes more than 1,500 cybersecurity expert volunteers from around the world who are working to help healthcare organizations deal with cyberthreats as the pandemic continues to rage. It serves as a central hub for collecting then sharing threat information to not only healthcare and health insurance companies, but law enforcement, government agencies, and network operators as well.

"In one year of the CTI League, we understand how vulnerable and, accordingly, how targeted the healthcare sector is," Ohad Zaidenberg, founder and executive of the League wrote.

Where does browser and web isolation fit in?

With remote working, more healthcare information technology employees and employees of healthcare insurance companies, including their contact centers, are using their home computers and smartphones to get work done. As part of that, they are using browser-based communications applications, and are using browsers to search for information.

Especially in times of great chaos and stress, employees may unintentionally open and engage with emails, accidentally clicking on links to fake websites or on malicious content embedded into hacked legitimate websites.

Cyber criminals are sophisticated and well-funded, and it is incumbent on every IT and OT team, every CIO and CISO in the healthcare information world to be aware of and to mitigate risk. While we are starting to see the light at the end of the COVID-19 tunnel, we have a long way to go, especially as new strains of the virus emerge.

Sadly, bad actors strike when society is at its most vulnerable, but with awareness and action, we can stop them in their tracks, and protect the information – whether private patient information or extremely valuable scientific information – from falling into the wrong hands and causing further damage beyond the pandemic itself.
