Quarter of Healthcare Ransomware Victims Forced to Halt Operations

Trend Micro research reveals supply chains are key source of risk

DALLAS, Oct. 11, 2022 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today revealed that 86% of global healthcare organizations (HCOs) that have been compromised by ransomware suffered operational outages.

To find out more, visit: https://www.trendmicro.com/explore/glrans

Most (57%) global HCOs admit being compromised by ransomware over the past three years, according to the study. Of these, 25% say they were forced to completely halt operations, while 60% reveal that some business processes were impacted as a result.

On average, it took most responding organisations days (56%) or weeks (24%) to fully restore these operations.

Trend Micro research reveals 86% of global healthcare organizations compromised by ransomware suffered outages.

Ransomware is not only causing the healthcare sector significant operational pain. Three-fifths (60%) of responding HCOs say that sensitive data was also leaked by their attackers, potentially increasing compliance and reputational risk, as well as investigation, remediation and clean-up costs.

Respondents to the study also highlight supply chain weaknesses as a key challenge. Specifically:

- 43% say their partners have made them a more attractive target for attack
- 43% say a lack of visibility across the ransomware attack chain has made them more vulnerable
- 36% say a lack of visibility across attack surfaces has made them a bigger target

The good news is that most (95%) HCOs say they regularly update patches, while 91% restrict email attachments to mitigate malware risk. Many also use detection and response tools for their network (NDR) endpoint (EDR) and across multiple layers (XDR).

However, the study also highlights potential weaknesses, including:

- A fifth (17%) don't have any remote desktop protocol (RDP) controls in place
- Many HCOs don't share any threat intelligence with partners (30%), suppliers (46%) or their broader ecosystem (46%)
- A third (33%) don't share any information with law enforcement
- Only half or fewer HCOs currently use NDR (51%), EDR (50%) or XDR (43%)
- Worryingly few respondents are able to detect lateral movement (32%), initial access (42%) or use of tools like Mimikatz and PsExec (46%)

"In cybersecurity we often talk in abstractions about data breaches and network compromise. But in the healthcare sector, ransomware can have a potentially very real and very dangerous physical impact," said Bharat Mistry, Technical Director at Trend Micro.

"Operational outages put patient lives at risk. We can't rely on the bad guys to change their ways, so healthcare organisations need to get better at detection and response and share the appropriate intelligence with partners to secure their supply chains."

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

For further information: Media Contact: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

https://newsroom.trendmicro.com/2022-10-11-Quarter-of-Healthcare-Ransomware-Victims-Forced-to-Halt-Operations