Ransomware Actors Target Healthcare

Threat Bulletins | TLP:WHITE | Alert ID : 830a8770 | Aug 08, 2023, 04:07 PM

Health-ISAC has observed multiple incidents involving ransomware threat actors attacking healthcare and medical research facilities around the globe. These victims include multiple subsectors within healthcare, including mental health.

Threat actors have successfully infiltrated victims in the healthcare industry by sending them infected files disguised as ultrasound images or other medical documents for a patient seeking a remote consultation.

In August 2023, Rhysida ransomware threat actors disrupted patient care across multiple hospital locations associated with Prospect Medical Holdings, including Waterbury Hospital. Prior to this incident, Rhysida attacked Haemokinesis LTD, a biomedical research laboratory based in Australia.

For specific details on the Rhysida incident, please review the HC3 Alert available here. The HC3 Sector Alert has also been attached in PDF format for ease of reference.

Additional Info

While threat actors often claim they do not target healthcare organizations, in practice, threat actors do not hesitate to target healthcare organizations.

Health-ISAC has observed threat actors encrypting healthcare provider networks and attempting to extort the providers by threatening to leak sensitive, stolen patient information. In more than one observance, healthcare organizations have refused to pay the ransom and the threat actors have leaked protected health information (PHI). The threat actors then wait weeks to months before removing the data and stating they are no longer extorting the victim due to the correlation to healthcare delivery.

Ransomware affiliates have been observed formally apologized for attacking children's hospitals stating these actions violated their rules. These apologies were made only after encrypting networks associated with healthcare delivery.

No observations have been made of threat actors establishing initial access, discovering they are within healthcare infrastructure, and exiting as they claim.

In June 2023, threat actors compromised patient data, including mammogram images, Social Security numbers, birth dates, and medical history, and made the data public on the internet.

In July 2022, 2.6 million patients had their data leaked after OneTouchPoint was compromised by ransomware affiliates. OneTouchPoint serves many healthcare organizations, and the breach had an impact on many large care providers.

In March 2022, data belonging to 2 million patients was exposed after a threat actor gained access to protected health information (PHI) associated with Shields Health Care Group.

Incident Date

Aug 08, 2023, 11:59 PM

Reference | References

Krebs on Security
Forbes
Healthcareinfosecurity
Wired

Tags

Rhysida, DICOM, Ransomware

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments:

Please email us at contact@h-isac.org

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP “Share Threat Intel” Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories:

For guidance on disabling this alert category, please visit the Knowledge Base article CSAP "Alert Categories" Toggle Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base

Knowledge Base:

Check out our Knowledge Base for HITS integration documentation. https://health-isac.cyware.com/webapp/user/knowledge-base/f4b0c136/