HC3: Analyst Note

October 13, 2021 TLP: White Report: 202110131200

Health Sector Ransomware Trends for Third Quarter 2021

Executive Summary

Ransomware remains a major threat to the health sector worldwide, with many healthcare organizations operating legacy technology with limited security resources. Health or medical clinics continue to be the most frequently affected sub-industry by ransomware followed by healthcare industry services and hospitals. The HC3 CTI team assesses that these trends are likely to continue through 2021.

Report

The HC3 conducted a review of ransomware activity tracked for the third quarter (Q3) of 2021 (July 1 to September 30) and derived a few insights. The team was able to identify ten major ransomware groups affecting healthcare organizations as well as the sub-industries within the healthcare sector impacted most by ransomware for Q3 2021. It is important to note that this data is based on a sample of ransomware incidents derived from a variety of sources (including media reports, ransomware blog leak sites, and information shared by federal partners) and that the findings may not encompass all ransomware incidents affecting healthcare entities, as many go unreported.

In total 68 ransomware incidents impacting healthcare organizations worldwide occurred during Q3. HC3 found that about 63% of these ransomware incidents impacted the U.S. health sector while 37% impacted healthcare organizations outside the United States. The top countries impacted by these ransomware incidents in the health sector outside the U.S. included France, Brazil, Thailand, Australia, and Italy. In the United States, the states experiencing the most ransomware incidents included California, Florida, Illinois, Michigan, Texas, Arizona, Indiana, Maryland, New York, and Georgia. It is important to note that some states may experience more incidents due to their size and population.

The table in Figure 1 shows the top ten ransomware groups impacting healthcare organizations globally (including the United States). Conti, Avaddon, and REvil/Sodinokibi ransomware-as-as-service (RaaS) groups were responsible for impacting the most healthcare organizations worldwide.

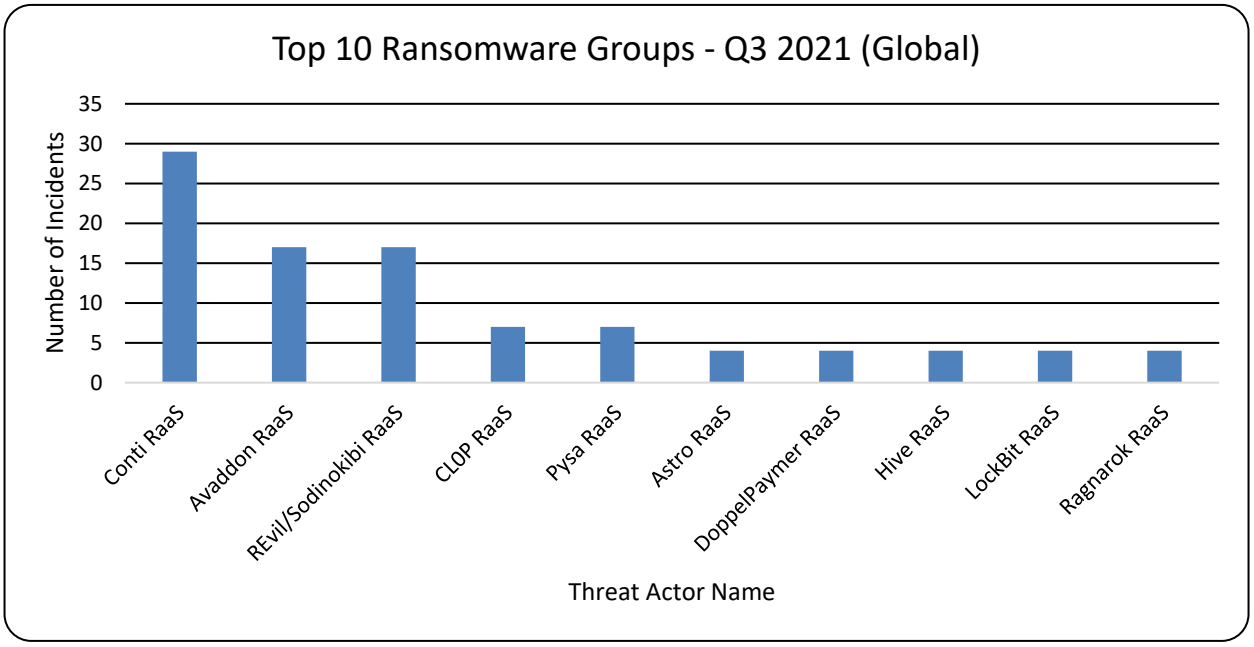

Figure 1

HC3: Analyst Note

October 13, 2021 TLP: White Report: 202110131200

The top ten ransomware groups impacting healthcare organizations in the United States alone is somewhat comparable to the global findings, although a few ransomware groups stood out. While the Avaddon RaaS was the second most observed group targeting the health sector globally, this group was only identified impacting one healthcare organization in the United States for Q3 2021. Furthermore, the Hive ransomware group claimed the compromise of four healthcare entities all located in the United States, including hospitals and medical centers.

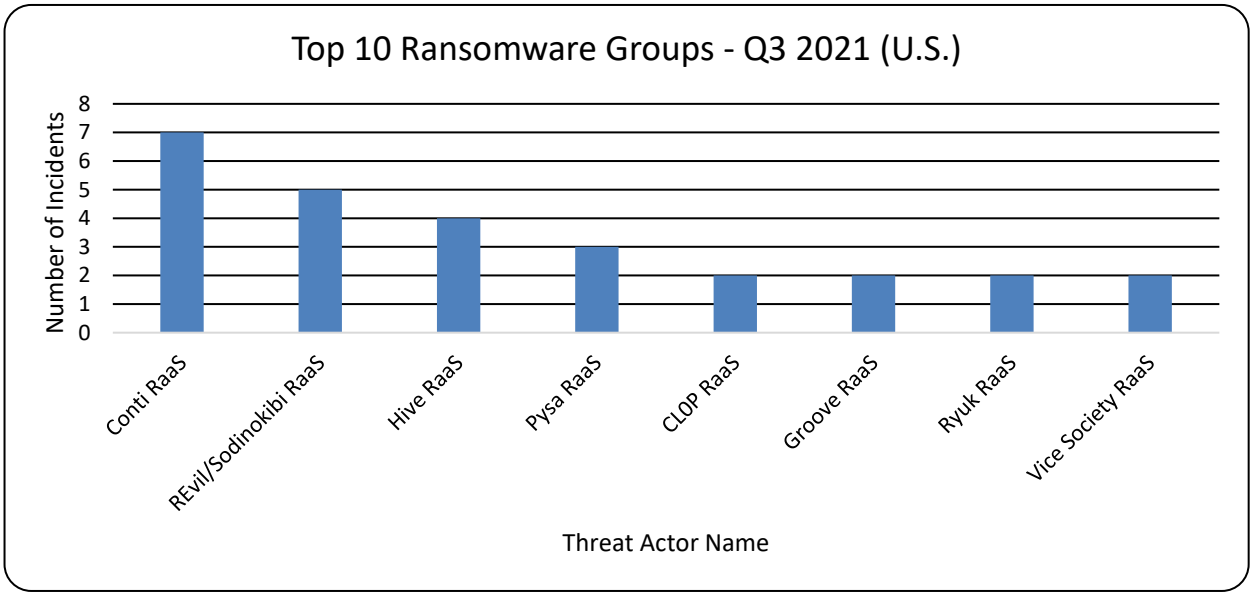

Figure 2

The sub-industries within the health sector that were most impacted by ransomware in the United States remains somewhat consistent with HC3's findings from the first half of 2021. Health or medical clinics and healthcare industry services organizations remained the most impacted types of healthcare entities by ransomware during the third quarter. At least 20 health centers or medical clinics experienced a ransomware attack and Conti was the ransomware group responsible for impacting the most health centers or clinics in the United States.

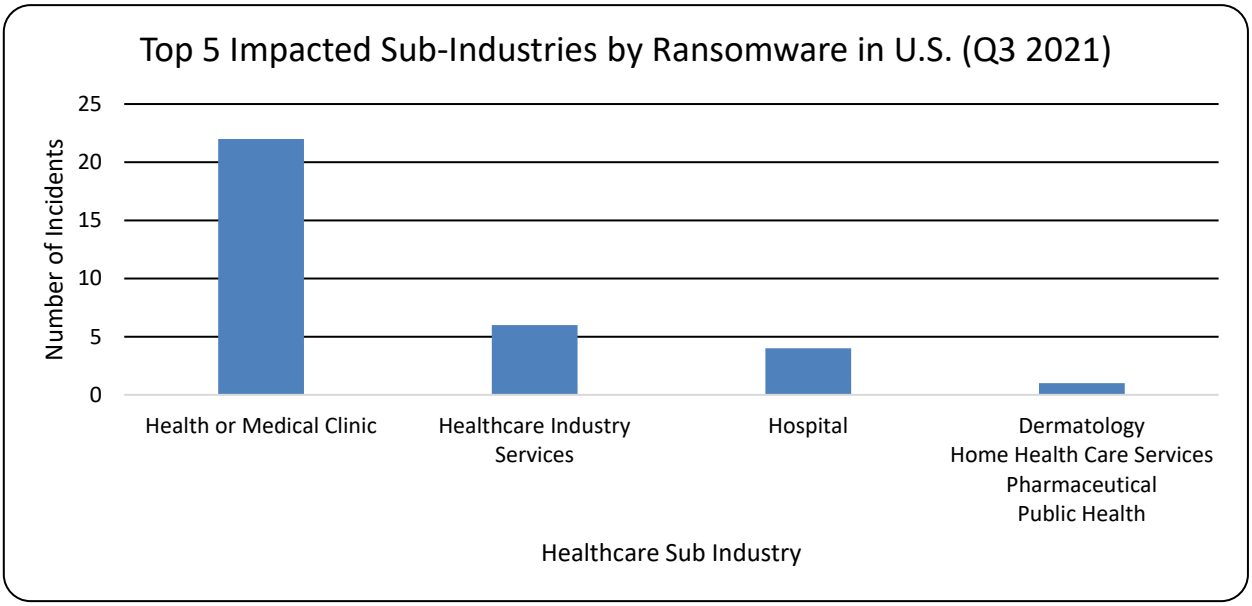

Figure 3

HC3: Analyst Note

October 13, 2021 TLP: White Report: 202110131200

Analyst Comment

HC3 assesses the Hive ransomware operators are likely to continue to target healthcare organizations specifically in the United States while the Vice Society ransomware group are likely to continue to target the health sector both in the United States and abroad. Furthermore, both the Hive and Vice Society ransomware groups surfaced in June 2021, following a trend of ransomware groups rebranding in attempts to evade law enforcement and takedown efforts. HC3 assesses that this trend is likely to continue, especially as ransomware groups attempt to compromise and extort healthcare entities with ransomware.

References

McKeon, Jill. "Hive Ransomware Continues to Attack Healthcare Providers," 23 September 2021. https://healthitsecurity.com/news/hive-ransomware-continues-to-attack-healthcare-providers

Walter, Jim. "Hive Attacks | Analysis of the Human-Operated Ransomware Targeting Healthcare," 23 August 2021. https://www.sentinelone.com/labs/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/

Ilascu, Ionet. "Hive ransomware attacks Memorial Health System, steals patient data," 16 August 2021. https://www.bleepingcomputer.com/news/security/hive-ransomware-attacks-memorial-health-system-steals-patient-data/

Greig, Jonathan. "Ransomware groups continue assault on healthcare orgs as COVID-19 infections increase," 11 September 2021. https://www.zdnet.com/article/ransomware-groups-continue-assault-on-healthcare-orgs-as-covid-19-infections-increase/

Abrams, Lawrence. "United Health Centers ransomware attack claimed by Vice Society," 24 September 2021. https://www.bleepingcomputer.com/news/security/united-health-centers-ransomware-attack-claimed-by-vice-society/

Michael Gillespie @demonslay335, Twitter. https://twitter.com/demonslay335/status/1403109032014061568

Jerich, Kat. "FBI issues alert about Hive ransomware," 2 September 2021. https://www.healthcareitnews.com/news/fbi-issues-alert-about-hive-ransomware

Dept. of Health and Human Services, HC3, "Ransomware Trends 2021," 3 June 2021. https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback