

New Reports Show IT Ransomware Attacks Down, Cryptocurrency Mining Up

With the exception of consumer costs, downward trends are patterns to avoid in healthcare. But a new study by the cybersecurity firm Cryptonite sheds light on another area where decreased numbers are a good thing: the incidents of healthcare ransomware attacks. Those numbers are trending down lately, though some attention-grabbing attacks (like those launched against LabCorp and Allscripts) might lead consumers to believe otherwise.

The decline is substantial. The first half of 2018 saw a total of eight healthcare ransomware attacks, but in the same period in 2017, 19 attacks occurred (this according to Cryptonite's analysis of data supplied by the Health and Human Service's Office for Civil Rights [OCR]). That's a reduction of 57%.

Cyber criminals still inspired to lift personal data

However, the improvement doesn't mean healthcare IT experts should look the other way. Cryptonite President and CEO Michael Simon had this to say (as reported by "HealthITSecurity): "While 1st half 2018 shows a downtrend in the successful use of ransomware, we expect cyber criminals to continue to adjust their attack techniques to successfully targeting the IoT devices, medical devices, and mobile devices for the continued compromise of healthcare networks."

The trend may be positive, but the threat has not passed, since the motivations of bad actors still exist. Simon noted: "[Cyber criminals] are driven by the economic opportunity for the sale and ransom of these stolen data records, and that opportunity remains as strong as ever."

Regarding IT/hacking incidents overall, Cryptonite reported that the OCR said it was made aware of 59 of them in the first half of the year, compared to 140 similar events for the entirety of 2017. However, nearly 2 million healthcare records were compromised in the first half of 2018, which represents a 9% increase over the first half of 2017.

"Cyberattackers continue to target healthcare to obtain medical records they contain for sale on the dark web. Medical records still continue to provide the best and most complete data which can support identity theft and related financial fraud," said Simon.

Cryptocurrency mining on the rise

Kaspersky Lab is an endpoint security firm that recently released a report also showing a downward trend in the number of ransomware attacks in the healthcare IT world. Kaspersky reported that the ransomware incidents among users of its IT products dropped by around 30% in 2017-18 (to around 1,800,000, from around 2,600,000 in 2016-17).

Before those numbers alone foster a sense of complacency regarding the current cybersecurity climate, though, other statistics are worth looking at. Kaspersky reported that users of its IT products that were the subject of cryptocurrency miners went up substantially, by more than 44% in 2017-18 (to around 2,700,000, from around 1,900,000 the year prior).

Cryptocurrency miners in it for the long haul

The behavior of cryptocurrency miners is typically not as devastating as ransomware attacks, but the mining can wreak havoc on a healthcare company's IT system, and, because the victim is not required to be informed about the attack, the issue can be insidious and carry on for more protracted periods. So despite the positive downward trend in ransomware attacks in healthcare IT, strong, evolving cybersecurity defenses remain as imperative as ever.



Kaspersky's report read: "While ransomware can provide cybercriminals with potentially large but one-off rewards in a turbulent landscape, miners might make less money out of their victims, but through a more sustainable/longer-term model."

This article is provided for educational purposes only and is not offered as, and should not be relied on as, legal advice. Any individual or entity reading this information should consult an attorney for their particular situation. For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.