Data Breach Today
Prevention. Response. Notification. TODAY
https://www.databreachtoday.com/

Business Continuity Management / Disaster Recovery , Cybercrime , Fraud Management & Cybercrime

Ransomware: Average Ransom Payout Increases to $41,000

Sodinokibi and GlobeImposter Gangs Target Larger Victims, Coveware Warns

Mathew J. Schwartz (euroinfosec) • November 1, 2019

Ransom payments (mean in red): From July to September 2019, victims paid an average of $41,198 for the promise of a decryption key. (Source: Coveware)

Ransomware continues to be highly profitable for criminals.

See Also: Unlocking IAM - Balancing Frictionless Registration & Data Integrity

For the third quarter of this year, the average ransom amount paid was $41,198, an increase of 13 percent compared to the second quarter and a nearly six-fold increase from the third quarter of 2018, according to ransomware incident response firm Coveware. The five most-targeted industries in the third quarter were professional services, the public sector, healthcare, software services and retail.

"The rate of increase has plateaued, reflecting resistance to paying by victims who are increasingly finding new ways to restore and recreate data, rather than pay," Coveware says in a new report. "Ryuk continued to make headlines, and other similar Hermes variants like DopplePaymer and I-Encrypt became more prevalent, suggesting that threat actors are rotating through different kits."

Coveware's findings are based on anonymized data collected from ransom payments made by its clients and clients of its business partners. "We don't publish the underlying numbers - as we are private company - but it's in the high hundreds," Coveware CEO Bill Siegel tells Information Security Media Group (see: *Ransomware Gangs Practice Customer Relationship Management*).

Top three ransomware strains, together with average ransom paid by victims, when they pay (Source: Coveware)

Siegel says that one surprise from the research is how much ransomware continues to evolve, with many more groups adapting network intrusion techniques previously used by nation-states' advanced persistent threat groups or only the most advanced cybercrime gangs.

"The year-over-year changes are the most stark," he says. "Ransomware has gone from being an autonomous threat that companies tried to deflect at their perimeter to being a targeted threat where the methods of intrusion and attack are closer to that of APTs than spam campaigns. It puts a lot of pressure on CISOs to have a multilayered approach."

Under the Gun: IT Service Providers

Coveware says the increase in ransomware payments is due to increased ransom demands being made by attackers who wield Ryuk, with the average demand increasing from $267,742 in Q2 to $377,026 in Q3.

Another driver: Both Sodinokibi and GlobeImposter "are targeting large managed service providers and large enterprises with million-dollar-plus demands," Coveware reports. "The size, sophistication and cost of these attacks, along with lower overall payment rate, indicates that threat actors are willing to invest significant time and expense for the prospect of a higher payoff" (see: *Texas Ransomware Responders Urge Remote Access Lockdown*).

Top industries targeted by ransomware attackers (Source: Coveware, Q3 2019)

Increasingly, attackers using GlobeImposter, Netwalker, Hidden Tear and Snatch are targeting larger organizations seeking a larger payoff, Coveware says.

Target: Remote Desktop Protocol

Coveware says 51 percent of the intrusions its customers experienced in the third quarter traced to attackers accessing its network stolen remote desktop protocol credentials, which remain easy and inexpensive to procure on cybercrime marketplaces. Another 39 percent of ransomware outbreaks traced to phishing and 8 percent to a software vulnerability exploited by attackers (see: *Software Bugs: Gotta Catch 'Em All?*).

Ideally, ransomware victims can wipe systems and restore them from offline backups. But some organizations don't keep up-to-date backups. And some have seen their backups get crypto-locked by attackers.

In some cases, victims can avail themselves of free decryptors from the No More Ransom project. But free decryptors don't exist for every strain of ransomware.

Bitcoin continues to be the dominant virtual currency being demanded by attackers, with Coveware saying that 99 percent of all payments get made using bitcoins.

Paying a Ransom: Just the Beginning

When organizations do choose to pay their ransomware attackers, there are no guarantees that they'll receive a decryption tool, or that it will work.

Coveware notes, however, that from July to September, 98 percent of the companies it worked with that paid a ransom did receive a working decryption tool, a slight increase from the prior three-month period. It notes that some threat actors are reliable, while others - especially those using Rapid and Dharma ransomware - often default after being paid.

Just because victims receive a decryptor, however, doesn't mean they're getting all of their data back. In the third quarter, "victims who paid for a decryptor successfully decrypted 94 percent of their encrypted data," Coveware says, which was a slight improvement from the second quarter.

Simply put, some ransomware decryptors are much better than others, and it often has to do with the quality of the crypto-locking code first used against victims. High-quality, professional-looking code tends to encrypt systems in a way that can be decrypted, while poor-quality coding and more amateur operators tend to use software that generates errors while it works, meaning that it doesn't successfully encrypt all files before it erases all unencrypted files from a victim's hard drive.

"For example, Mr. Dec Ransomware had an abysmal data recovery rate, around 30 percent," Coveware says. "This is due to the caustic nature of the payload, mixed with the relatively amateur threat actors that use it. The result is sadly predictable. On the other hand, 'Mamba' ransomware has an almost 100 percent data recovery rate. Mamba actors use full disk encryption after gaining a persistence in the network rather than black market encryption malware. Since the full disk encryption software they use is commercially manufactured, rather than black market manufactured, it tends to cause less damage."

Red Flags for Victims

Cybercrime remains a business, and Coveware's Siegel says attackers who don't provide working decryptors are shooting themselves in the foot. That's because ransomware victims are well aware of whether a gang has a history of defaulting on their promises after they've been paid.

Most prevalent ransomware strains (Source: Coveware, Q3 2019)

"It's a major red flag when we point out a bad track record to a victim, and absolutely impacts the decision to pay or not pay," he says. "That is the essence of why it is important to collect this information. While the broad averages give the appearance of a safe decision, the materiality of the decision requires close scrutiny of the actor's history. If they or the type of ransomware they are using have a poor track record, victims often don't consider paying to be a viable option, nor should they."

About the Author

Mathew J. Schwartz

Executive Editor, DataBreachToday & Europe

Schwartz is an award-winning journalist with two decades of experience in magazines, newspapers and electronic media. He has covered the information security and privacy sector throughout his career. Before joining Information Security Media Group in 2014, where he now serves as the executive editor, DataBreachToday and for European news coverage, Schwartz was the information security beat reporter for InformationWeek and a frequent contributor to DarkReading, among other publications. He lives in Scotland.

© 2019 Information Security Media Group, Corp. https://www.databreachtoday.com/ Toll Free: (800) 944-0401