CYBER UPDATE

SCS AGENCY INSURANCE

Ransomware Actors Shifting Away From Big-game Hunting to Smaller Targets: Coveware

Ransomware actors shifted to more "mid-game hunting" in the third quarter (Q3) of 2021, resulting in fewer large ransom payments and more lower payments made by middle-market organizations, according to recent data from Coveware, an incident response and ransomware negotiation firm.

The average ransom payment amount stayed around the same level between the second quarter (Q2) and Q3 at $139,739, but the median amount jumped over 50% to $71,674, the firm reports. Both statistics are down significantly from the first quarter (Q1) of 2021.

"Ever since the pipeline attacks this spring, we have seen statistical evidence and intelligence showing that ransomware actors are trying to avoid larger targets that may evoke a national political or law enforcement response," Coveware notes. "Middle-market companies that are not systemically important may not offer up the largest ransoms, but are more cost-effective to attack and may still provide a sizable payment if the company is caught without the proper defenses and backup assets."

In Q3, small professional services firms bore the brunt of attackers' efforts, followed by public entities and health care. Firms suffering ransomware events in Q3 were predominantly in the small to middle market range, with 43.6% of attacks at firms with 101 to 1,000 employees and 34.7% at firms with 11 to 100 employees. Long-term beliefs that they aren't targeted for attacks can make smaller businesses even more vulnerable.

"This fundamental misconception of how ransomware attacks are manufactured leads companies to believe they will never be struck by lightning," Coveware noted. "What they do not realize is that this type of thinking actually makes them a lightning rod for attacks."

Ransomware actors remain dedicated to data exfiltration as a tactic to pressure victim companies into paying. Coveware found 83.3% of Q3 attacks involve the theft of corporate data, up 3% from Q2.

According to the firm, paying still isn't the best idea; it states that victims should assume data will not be destroyed by the threat actor and may be sold, misplaced, traded or kept for future extortion attempts. A promise of deletion in exchange for payment also doesn't extinguish any legal or contractual notification requirements on the part of organizations.

"Even if the threat actor deletes a volume of data following a payment, other parties that had access to it may have made copies so that they can extort the victim in the future," Coveware noted.

The report shows that despite a host of government initiatives, the extortion economy brings in new players every day; threat actors show no signs of stopping, even as they shift targets. Coveware noted that for cybercriminals, ransomware is still too lucrative and easy to deploy to quit.

"This past quarter has seen an unprecedented amount of domestic and international activity from government and law enforcement to counter the operations of ransomware actors," Coveware indicated. "Despite these initiatives, ransomware actors continue peppering enterprises with more attacks than ever. What we are doing is not working, at least not yet."