Bitcoin ransomware targets MongoDB, impacts over 10,500 databases - ET CIO

Some victims have already paid ransom to recover their files, while other exposed installs are being erased and held for ransom.Ashwani Mishra | ETCIO | January 09, 2017, 09:17 IST

19

Malware that scrambles data and demands a ransom to decode it — increased 6,000 percent in 2016 as compared to 2015, a study from IBM Security had revealed in December last year.

In such a scenario, when a company places open, unauthenticated and exposed data stores by the thousands, it was only a matter of time for hackers to do what they do best.

Around 10,500 website databases of MongoDB have been hijacked in the last few days by attackers who are now demanding hefty ransoms for the data to be restored.

Andreas Nilsson, Director of Product Security at MongoDB wrote in the company's blog, "Recently, there have been reports of malicious attacks on unsecured instances of MongoDB running openly on the internet. The attacker erased the database and demanded a ransom be paid before restoring it."

Nilsson writes, "If you don't have a backup or are otherwise unable to restore the data, unfortunately your data may be permanently lost. You should assume that the attacker has a copy of all data from the affected database(s). Follow your internal security procedures for a data breach."

Though he has also suggested various security measures to diagnose and respond to the attack, it is a lesson that's coming in too late.

Various groups are behind the attack and their demand ranges from as low as 0.15 Bitcoin to a full Bitcoin. The message from the attackers states that administrators should mail them the proof of ownership before the files are restored. For those left without backups can take consolation from Nilsson's blog.

As reported in the media, so far around 11 victims have paid the ransom in order to recover their files.

It seems that attackers performed a mass-scan to find unprotected MongoDB databases, post which the sites were accessed and data was held for ransom.