www.esecurityplanet.com /trends/exfiltration-data-in-use-encryption/

Exfiltration Can Be Stopped With Data-in-Use Encryption, Company Says | eSecurityPlanet

Ray Fernandez ⋮ 6-7 minutes ⋮ 7/26/2022

Even the most advanced and sophisticated security tools are failing to protect against ransomware and data exfiltration, according to a new report from data encryption vendor Titaniam.

The State of Data Exfiltration and Extortion report says that despite heavy investments, more than half of organizations that experienced ransomware attacks ended up paying the ransom.

The organizations affected had solid cybersecurity measures, but nonetheless experienced significant data security failures. Titaniam also highlighted the solutions that can help leaders respond to triple threat ransomware attack trends, data theft, and extortion.

Also read: How One Company Survived a Ransomware Attack Without Paying the Ransom

Exfiltration Attacks Surge

The Titaniam report surveyed 107 organizations across the U.S. from various industries. In the past five years, 70% of these organizations reported an attack, and 40% experienced a cyberattack in the past year.

More than half—68%—of those attacked had their data exfiltrated. Additionally, 60% of these were subsequently extorted.

“Exfiltration rates are up 106% relative to 5 years ago,” the study says.

According to Titaniam, more than 75% of organizations surveyed had all three significant categories of ransomware protection:

- 78% had data security and safety measures
- 75% had prevention and detection
- 73% had backup and recovery systems

However, 60% of those attacked were forced to give in to ransom demands.

According to Titaniam, “cyber criminals are no longer limiting themselves to just encrypting entire systems—they are making sure to steal data ahead of the encryption so that they can have additional leverage on the victim.”

Also read: Best Backup Solutions for Ransomware Protection

Stolen Credentials Source of Attacks

Arti Arora Raman, founder and CEO of Titaniam, told *eSecurity Planet* that data exfiltration attacks are not typically executed by attackers hacking into networks but rather by attackers simply logging in using stolen credentials.

Titaniam CEO Arti Arora Raman

“In this type of situation, all other data security controls simply fall away, giving unfettered data access to attackers,” Raman said.

The solution? Raman says the emerging technology of choice to defend against data exfiltration and extortion attacks is *encryption-in-use*.

Also read: Homomorphic Encryption Makes Real-World Gains, Pushed by Google, IBM, Microsoft

Data Security and Encryption

Evidently, if over 70% of leaders assume they are using strong cybersecurity systems but more than half are extorted and end up paying a ransom, the need to take a deep look at how data protection is being approached is paramount, Raman said.

“We must understand that while prevention, detection, and backup are essential, no ransomware defense strategy is complete without eliminating data exfiltration. This is what would take us beyond the notions of impenetrability and towards immunity,” Raman said.

While encrypting data at rest and data in motion is common practice, data in use is almost 100% unencrypted, according to Titaniam. Furthermore, data in use is increasingly targeted due to its vulnerability, potential to hold sensitive information, and the complexity of securing it.

“Titaniam extends strong data protection that has traditionally only been available for data at rest and in transit to also cover data in use,” Raman said.

Titaniam is also NIST FIPS 140-2 certified, she added.

Titanium also offers nine other data security and privacy formats, including traditional and format-preserving encryption, vaulted and vaultless tokenization, static and dynamic as well as whole or partial data masking, redaction, and hashing. This translates to the equivalent of four other data security solutions with the addition of innovative encryption-in-use, the company claims.

Data-in-use often lives in cloud service back-ends, powering business and customer support, apps, AI, and security operations. Titanium says it has the cloud covered too, with interoperable modules that can be mixed and matched to support all varieties of cloud and hybrid architectures as well as a large variety of data platforms and applications.

Regarding performance, Raman says that unlike other encryption-in-use and tokenization providers that operate with high query and storage overhead, Titaniam requires less than 5% query and search overhead.

“This enables us to tackle large, high-performance, high-throughput datasets,” the CEO added.

Titaniam Vault, Titaniam Plugin, Titaniam Translation Service, Titaniam Proxy, and Titaniam Studio can stand alone or combine via the Platform, which provides bring your own key encryption (BYOK) and ensures that protected data can move across the enterprise.

In the event of an attack, the company produces audit-ready certification that says sensitive data retained encryption. Software-as-a-service (SaaS) companies can store and process customer data with less risk, data-intensive products can operate with fewer privacy or compliance concerns, and governments can secure their data and intellectual property.

“This means that customers can now have a dramatically superior alternative to tokenization where data can be protected but still utilized,” Raman said.

Read next: Best Encryption Software

Ray Fernandez

Ray is a Content and Communication Specialist with more than 10 years of experience. He currently works as a Senior Copywriter for Wunderman Thompson and writes as a freelance technology journalist for several tech media. His work has been published in Microsoft, Slash Gear, Screen Rant, OOSKA News, Bloomberg, and Nature Conservancy, among other places.