Ransomware just met its match

Written By: Fran Howarth
Published: 24th March 2023
Content Copyright © 2023 Bloor. All Rights Reserved.
Also posted on: Bloor blogs

RANSOMWARE ATTACK
Your personal files are encrypted
NeuShield
How much is your data worth?

Ransomware was the most common form of malware in 2022 and is the second more prevalent cause of data breaches. The main point of ransomware is to extort victims by demanding a ransom be paid to restore data that has been rendered unavailable by attackers – and the sums involved are getting larger. Any organisation can be considered to be a legitimate target.

Traditional protections insufficient

In the battle against ransomware, traditional protections are not good enough. Far too many attacks are still getting through.

Backups can provide a defence against ransomware if an organisation has a good backup strategy in place, with multiple copies including one that is stored offsite and is immutable. But if data has already been infected with malware, even the best backup strategy can fall short. Attackers are now routinely attempting to go after backups. Alone, they are insufficient.

There are a number of techniques that are used to detect ransomware. Signature-based systems are good at detecting known threats and ransomware strains, but are ineffective against sophisticated, targeted ransomware campaigns. They also require frequent updates. Data traffic analysis can be used to detect even new strains, but are plagued with high rates of false positives and can lead to legitimate traffic being blocked.

Behavioural monitoring looks to identify anomalies upon file execution and monitor how files and processes behave to root out malicious activity. But they require time to analyse behaviour, which can result in some data being encrypted during the process. Deception techniques use honeypots and false networks to try to trick attackers.

Yet none of these techniques are watertight and some attacks will seep through.

A new kid on the block

Bloor Research was recently briefed by NeuShield, which offers an unorthodox, yet effective, solution for defending against ransomware. Its Data Sentinel mirror shielding technology works like a pane of glass that shields data. When a small endpoint agent that communicates with a web console is installed, any changes to files and data are stored on this overlay. If anything is found to be corrupted, the changes can be deleted with just one click and the underlying data is safe. These repairs are performed without the need for backups, or detecting and blocking a threat. Repairs to the files or operating system can be made quickly and effectively, greatly reducing the cost of any downtime, which is another consequence of ransomware and can also be extremely costly.

The technology also works in offline mode and can be used to protect remote systems—a necessity in this day and age. NeuShield has also released a solution for databases in its data centre edition, which it continues to develop and broaden.

Bottom line

The promise of NeuShield's technology is that not only can encrypted data be recovered without having to restore data from backups, but that it can be recovered almost instantly. Original data is never modified owing to mirror shielding capabilities, stopping ransomware in its tracks.

Share on Social Media

Share Tweet Share Pin It

Post a public comment?
You must be logged in to post a comment.

ABOUT BLOOR

Bloor is an independent research and analyst house focused on the idea that *Evolution is Essential* to business success and ultimately survival. For nearly 30 years we have enabled businesses to understand the potential offered by technology and choose the optimal solutions for their needs.

LATEST TWEETS

Bloor's @DavidN_Drhys has been catching up on developments at @puppetize, now part of @perforce. Together, they provide the basis for a strong DevOps automation platform, & David shares his thoughts following a briefing with @DNSandilands. #MutableBusiness bloorresearch.com/20…

USEFUL LINKS

Bloor Mailing List
Request an Analyst Briefing
Bloor Navigators
Site Map
Terms & Conditions
Privacy & Cookie Policy