IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Cybersecurity

Best Practices in Next-Gen Data Protection: How to Implement Recovery-First Ransomware Detection

Michael Colby

Michael Colby
Product Marketing Manager
Infinidat

Biography

Michael Colby is a Product Marketing Manager at Infinidat (https://www.infinidat.com) and has been focused on the storage industry since the early days at NetApp, as a system engineer.

He was also an early employee at Data Domain and spent time focused on Data Protection at Data Domain and EMC. Michael has also had tenures in competitive intelligence at EMC, Dell and, most recently, Pure Storage.

Michael blogs at: https://www.infinidat.com/en/blog/ .

Keywords Ransomware attacks, Social engineering, Cyber threat detection, Artificial Intelligence (AI), Data protection
Paper type Research

Abstract

The increasing scale, sophistication, and frequency of ransomware attacks necessitate that organizations acknowledge the vulnerability of all systems and datasets, regardless of the cybersecurity measures in place. Even robust protocols such as multi-layered defences, stringent access controls, and network segmentation, may not fully eliminate risk. In the event of a ransomware attack, threat actors often encrypt organizational data and demand payment for its restoration. Addressing these incidents presents multifaceted challenges, including concerns over data integrity, tight response timelines, and complex legal implications. In this article, the author examines the importance of prompt and decisive action following a ransomware incident and explores how organizations can adopt next-generation data protection solutions that prioritize a recovery-focused approach to ransomware detection.

Introduction

The threat of a ransomware attack has never been greater. According to a recent report from S.C. Bitdefender SRL and published in SiliconANGLE, February 2025[1] was the worst month on record for ransomware attacks and “set a record for the highest number of ransomware attacks ever reported.”

Check Point Research also reported the highest increase of global cyberattacks seen in two years – a 30% increase of global cyberattacks in Q2 2024, up from Q2 2023 and now at 1,636 cyberattacks per week[2].

Similarly, Comparitech reported in their "Ransomware Roundup" for Q1 2025 that they recorded 2,190 enterprise ransomware attacks globally – an increase of 184% from ransomware attacks recorded[3] for Q1 2024. These are staggering increases.

As cyber security analysts project, the collective cost to enterprises of cyberattacks will be several trillions of pounds in 2025. Cyber security has rightly become a top concern of CEOs worldwide.

Cyber risks are increasing daily

As the crisis of ransomware and cyberattacks continues to grow, it is not a matter of if but when an organization will suffer a cyberattack or ransomware attack.

This risk increases daily because cyber criminals are not standing still – they continue to evolve and shift their tactics to find and exploit new software vulnerabilities and are doing so at an increasing rate, now using AI tools to accelerate their attack vectors.

How they attack is not a big secret. First, they find a vulnerability to gain access to internal networks. Then, they move to a phase of manual intrusion and deploy their ransomware code. During this time, they analyze compromised networks, increasing their access and rights privileges whilst they surreptitiously plant malicious code across an organization's data infrastructure.

While they may be undetected until a full-scale attack is launched, organizations are frequently already compromised before any sign of a cyberattack. This phase used to take place over weeks or months. Now, the trajectory of a cyberattack can occur in just over days or hours, from manual intrusion to ransomware code deployment and, finally, the launch of the attack on the data.

Five methods used to hide ransomware

These are just some of the methods that cyber criminals use to hide ransomware before an attack:

- **Timebomb Ransomware** – Remains dormant for a period before activating, ensuring the potential to infect backups and making them useless when needed.

- **Slow and Intermittent Encryption** – Encrypting only portions of files, over time. Slow and subtle corruption is designed to stay below the radar of threshold-based monitoring tools.

- **Maintaining Original Metadata –** Some ransomware maintains the original metadata of the files after encryption to make it difficult for basic inspections to identify the corruption based on detection of changes in file name, size, or extensions.

- **Database Corruption** – Sophisticated attacks corrupt database pages without immediate detection, enabling operations to continue unnoticed until routine maintenance reveals the issue, by which time significant data loss may have occurred.

- **Shadow Encryption** – An evolving approach of encrypting files in memory or using multiple encryption algorithms that attempts to make it nearly impossible to detect using traditional methods.

Increasingly sophisticated methods of rapidly planting the seeds of an attack and attacking data with the intent to be undiscovered, means early detection is crucial to limit the impact of such attacks. In their report[1], Bitdefender recommends that all organizations take proactive security measures to reduce the risk of exploitation.

Identify the right solution for proactive cyber threat detection

It's therefore vital that enterprises understand the importance of proactive detection and response. They need to invest in solutions that can go beyond simply detecting when an attack is activated. Notification and warning of when an attack begins is not enough – by then it's too late! Enterprises need proactive detection that operates further upstream in the process – allowing more time to respond.

Look out for these features when you are considering proactive cyber threat detection:

- Ability to perform a sophisticated AI and content analysis of every file and database in the enterprise, looking for any changes over time. This level of proactive content examination should be able to identify even subtle signs of ransomware activity.

- Ability to utilize AI powered training to monitor the actual behaviours of ransomware and how they affect data content. This includes the ability to understand patterns of corruption, encryption/decryption, and mass deletion. For instance, AI models should be trained and validated on tens of millions of data sets and real-world samples.

- Ability to utilize a collection of different machine-learning engines to allow these advanced AI models to operate independently and then perform a polling process to generate a single prediction of whether the data change is indicative of a ransomware attack.

- A training process that involves using millions of customer samples to increase the solution's detection accuracy. Plus, the entire training process should be repeated daily with hundreds of new and existing ransomware variants to ensure optimum predictive reliability.

- Final product testing conducted on 30 million completely different data sets, often from real-world customer analytics, to ensure the 99.99% accuracy is maintained before a code release.

Once you identify a next generation data protection solution like this, one that has been developed and trained following this best practice methodology, you can be assured your enterprise will be benefiting from proactive cyber threat detection. In addition, you will have the confidence of knowing that your data has integrity and that cyber criminals are not circumventing your data analytics tools, hiding their tracks, and covertly corrupting your data before launching a full-scale attack. Take this into consideration when evaluating your next data protection solution. It pays to be well informed.

Reference

[1] Riley, D. (03 June 2025), 'Bitdefender report finds 84% of major attacks now involve legitimate tools'. SilliconANGLE. Available at: https://siliconangle.com/2025/06/03/bitdefender-report-finds-84-major-attacks-now-involve-legitimate-tools/

[2] (2025) *The State of Cyber Security 2025*. Checkpoint. Available at: https://engage.checkpoint.com/security-report-2025

[3] Moody, R. (10 April 2025), Ransomware roundup: Q1 2025. Comparitech. Available at: https://www.comparitech.com/news/ransomware-roundup-q1-2025/