CyberSense®
Powered by Index Engines

The Power of CyberSense’s Machine Learning

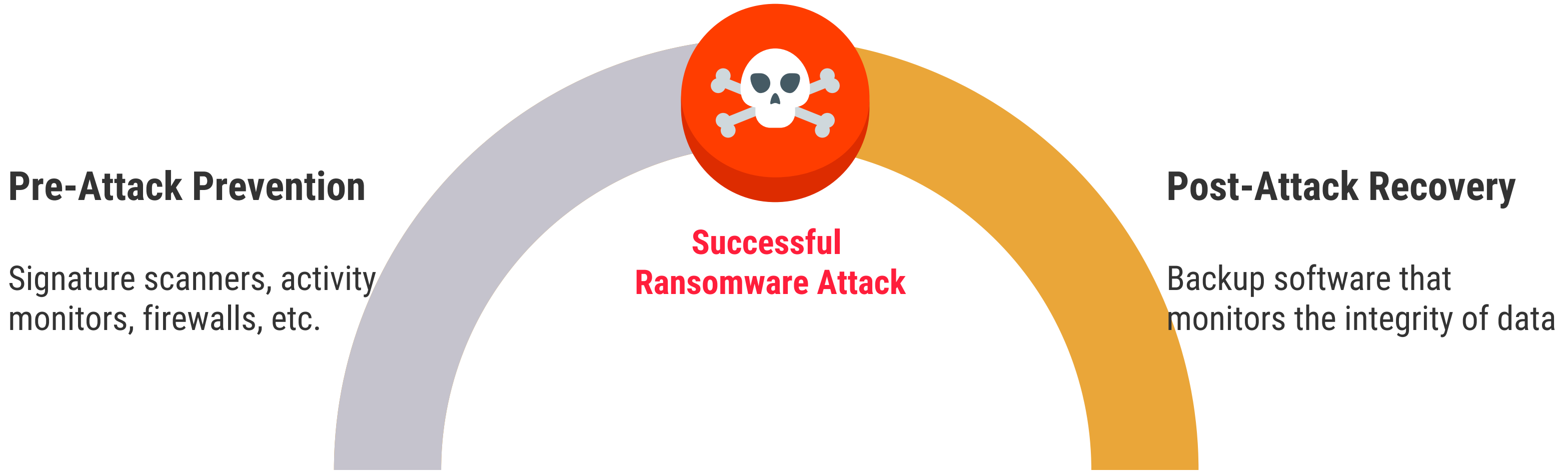
There are many products on the market today that are focused on preventing a ransomware attack: firewalls to stop viruses from entering, scans that detect unusual activity and signatures of common malware, and more. These pre-attack products are critical in supporting a cyber resiliency strategy; however, these products are just the first piece of the puzzle.

What happens when these solutions fail, and an attack is successful? How does an organization detect, diagnose and recover quickly?

This is where CyberSense fits into the tech stack. CyberSense is a post-attack product that is focused on data resiliency and does not replace the ransomware prevention approaches of the pre-attack products but is a last line of defense that helps determine what data has been corrupted, and what backups are good in order to facilitate a clean and rapid recovery when prevention fails.

The traditional pre-attack security solutions that focus on cyber resiliency are critical but not 100% effective. Cyber criminals are using new and innovative approaches to circumvent these solutions, therefore, it is critical to focus on data resiliency in order to have a reliable post attack recovery plan.   Some backup software vendors have responded by adding capabilities to their data protection software. Most of these are basic capabilities that have been added on in order to check a data resiliency box on a buyer’s guide.

CyberSense is a new and disruptive approach that relies on comprehensive inspection of file and database contents using over 200 analytics, as well as powerful machine learning models that have been trained on thousands of ransomware variants. This approach has proven to be far more robust in detecting corruption due to a cyberattack, even when new, more sophisticated variants are deployed.



Pre-Attack Prevention

Signature scanners, activity monitors, firewalls, etc.

Successful Ransomware Attack

Post-Attack Recovery

Backup software that monitors the integrity of data

Lets take a look at BianLian, a new variant that appeared on VirusTotal in August 2022. This new variant utilizes the Google Go programming language for portability across OS platforms, so the ransomware authors only need to write the ransomware once and can then run it on Windows, Linux, Solaris, etc. allowing them to get to market quickly across a range of targets.

The BianLian variant encrypts inside a file and adds a new file extension. For encryption, the malware divides the file content into 10 bytes chunks. First, it reads 10 bytes from the original file, then encrypts the bytes and writes the encrypted data into the target file. Dividing the data into small chunks is a method to evade detection by Anti-Virus products. Read more here.

What BianLian shows us is that the community of bad actors are getting smarter, using advanced technology, and outsmarting existing and traditional security tools. Let’s look at some approaches that are becoming less effective against these new variants.

1. Many data protection vendors have added signature-based scanning tools to their backups to find known malware. This was easy to do and allowed them to add a cyber check box to their offering.

   Scanning for signatures is commonly performed in the production environment by pre-attack security tools, however backup software vendors have also embraced this traditional approach. The question to ask here is if the malware was not detected using the current signature watchlist in production, then why do you think you will have any success in scanning your backups with these same signatures?

   Based on a recent security report from WatchGuard, over half of malware (57.8%) evades signature detection. And with new variants, such as BianLian, they are being designed to evade signature-based approaches. A simple change in the encryption algorithm will change the signature of any variant. This is why signatures have to be updated on a continual basis, a never ending and less successful battle.

   Signature-based scanning has some value with backup data during restoration, such as scanning for known malware with a known signature to avoid restore the malware after an attack. However, thinking that scanning backups with known malware signatures will provide data resiliency is providing a false hope.

2. The use of concepts such as metadata analysis and data thresholds have also become commonplace for backup software vendors.   These are not difficult to implement and provide some level of data integrity, but they can be easily outsmarted by bad actors using more advanced approaches.

Examples of metadata analysis includes scanning for extensions known to be used when data is corrupted, such as appending .encrypted or .lol onto a file. In the case of BianLian this will be a new extension that may not be known by the scanner and will be passed over. These scanners will need to be frequently updated to support the latest variants, which are continually changing to evade this simple approach. Or if the analysis is simply tracking a large number of files that have a change in extension this could easily generate a false positive as there are normal activities that may also generate this event.

In addition to metadata, the use of threshold analysis has been added to detect unusual behavior. Using thresholds, an analysis can be performed to determine if the number of files created or modified daily is outside the norm. If so, this will trigger an alert.

In addition to metadata and threshold analysis is there is analysis of file entropy, looking to see if the modified files show increases in entropy which would represent possible encryption. For those using metadata analysis where the entropy is calculated on the whole file and not pieces/chunks of the internal contents, this will only detect extreme encryption of the entire file.

BianLian is taking a more stealth approach to circumvent this approach. BianLian is performing intermittent encryption, not full file encryption, inside the file to avoid detection. This is purposely done to evade these lightweight analysis tools that are looking for obvious thresholds or changes in metadata properties or entire file encryption.

3. CyberSense takes a fundamentally different approach to detecting corruption due to ransomware. An approach that is not easily circumvented by bad actors who are growing smarter and deploying more advanced techniques. Without any updates, CyberSense detected the BianLian variant when it appeared on VirusTotal.com.

CyberSense looks for unusual patterns of behavior based on analysis of file and database content. This includes metadata properties which are a limited set of statistics that are available, something other vendors have implemented, however, CyberSense goes deeper and looks at hundreds of content statistics across the entire set of files and databases contained in each backup, which no other vendor is performing.

> With the volumes of advanced metadata and content analytics, fed to machine learning that has been trained on all the common approaches that are utilized to corrupt data, a new and advanced variant such as BianLian is easily detected.   Others need to update their software to detect new variants. CyberSense is designed to be smarter and more advanced so that with no updates to the analytics or machine learning is needed to detect a new variant like BianLian.

Leveraging the power of machine learning, with over 200 advanced metadata and content analytics, to detect new variants are no match for CyberSense. The fundamentally different and advanced approach provides a more confident data resiliency strategy that will ensure confidence that when corruption occurs, it can be detected regardless of the approach used, and an intelligent and rapid recovery process can be executed. Relying on techniques that constantly need to be updated and modified to support new variants is a thing of the past.

Content based analysis of files and databases combined with advanced machine learning is the only way forward to deliver confidence that data is protected from the most sophisticated cyber threats.

Learn more at www.indexengines.com/cybersense or contact us at info@indexengines.com