NetApp Ransomware Protection

Ransomware Detection: Techniques and Best Practices

June 16, 2022 | Topics: Cloud Backup, Data Protection, Elementary, Ransomware Protection, Security

What Is Ransomware Detection?

Threat actors use malicious software (malware) to infect computer systems and perform certain malicious actions. Ransomware is a special type of malware that aims to infect computer systems, encrypt files, and then demand ransom in exchange for decryption keys.

Ra
ran
bet
pro

In t

Ransomware Detection Techniques

Below are the most common ransomware detection techniques: signature-based detection, behavioral detection, and deception-based detection.

To better understand the types of ransomware that can affect your systems, read our guide to ransomware types

Signature-Based Ransomware Detection

A signature is a unique hash computed based on the content of a specific file. Signature-based ransomware detection takes a sample of ransomware code, computes the hash, and compares it with known file signatures. This enables fast static analysis of files in the environment, and is useful for detecting known ransomware strains.

Traditional antivirus software uses this technique to capture data from executables, and determine the likelihood that a specific executable is ransomware. Security teams can also use freely available tools like the Windows PowerShell `Get -FileHash` command to get the hash value of a file and compare it to known malware samples.

Signature-based ransomware detection technology is a line of defense—it can

help find known threats, but cannot identify new types of ransomware. Another concern is that ransomware is becoming evasive, and attackers update malware files to bypass detection. Also, ransomware executable files can be encrypted to make them undetectable by static analysis.

However, signature-based analysis is still widely used and is effective at stopping known, commonly used ransomware.

Behavior-Based Detection Methods

Security professionals and tools use behavior-based detection methods that analyze new behaviors, comparing it to historical data to discover indicators of compromise. Here are three common methods:

File System Changes

One way to identify ransomware is to search for abnormal file executions, including too many file renames. For example, hundreds of files renamed within a short period should raise an alert. Other suspicious file behaviors are new copies of files with greater entropy than the original file (which may indicate encryption), unusual encryption operations performed in the operating system, suspicious file extensions, and suspicious enumeration of files.

Data Traffic Analysis

Data traffic can indicate ransomware attacks. For example, files transferred to suspicious file-sharing sites could indicate an attack. Increased data transfer volumes are also a sign of suspicion. Ransomware needs network connectivity to off-site servers to exchange decryption keys and get command and control instructions.

Although it is helpful, this detection method can generate false positives and demands analysis. At the same time, attackers could use legitimate file-sharing

sites or servers hosted on legitimate IP addresses, and remain undetected.

API Calls

Another approach for detecting ransomware is to examine API calls in an operating system, looking for suspicious commands, or legitimate commands executed in an unusual volume or context.

As an example, many ransomware programs use operating system APIs such as GetTickCount to see the amount of time a system has been running. If the operating system has been running for a short time, this can be a clue that the ransomware is running in a VM, and so it does not undertake any malicious activity to avoid detection. When an executable makes calls to these APIs, it is a warning sign of evasive malware.

Deception-Based Detection

Ransomware often uses advanced techniques and strategies to invade organizations and compromise endpoints. However, recognizing that the main goal of ransomware is to encrypt files, an effective method to detect ransomware is to create a “bait” (also known as honeypot)—fake files, purposely created and placed in a visible location in the network to lure attackers.

As soon as ransomware identifies these fake files and attempts to encrypt them, the attacker exposes their methods and intentions, and can be stopped by security tools. This is a strong counter-attack strategy—convincing ransomware to trigger an alarm and attack harmless targets to reveal its criminal intent.

Many vendors provide commercial deception solutions (or offer these as a feature in broader endpoint security products). These solutions let an organization automatically create fake networks and distribute attractive baits that are indistinguishable from traffic and resources found on the organization’s real network. These fake networks seamlessly integrate with existing IT/OT

infrastructure to attract ransomware.

In addition to being an effective detection tool, cyber deception solutions have the additional advantage that they reveal the attacker's techniques, tools, and procedures (TTPs). This provides valuable information about the attacker, which can be combined with contextual threat intelligence, enabling effective mitigation strategies.

Best Practices for Early Ransomware Detection

Here are some practices to help you successfully identify an attack before it is too late:

- **Strong visibility—**understand east-west traffic activity in your network to gain insight into unauthorized lateral movements. Such lateral movement could be ransomware attempting to spread. Good visibility will give you an edge with defense, letting you discover possible attack vectors to critical applications using your IT assets.
- **Segmentation policies—**if you have existing segmentation policies, they should be based on the normal communication flow you observed between assets within your environment. Configure policies to provide an alert if anything outside normal activity occurs. This approach will provide you with an early warning of uncommon activity, so you can look into it further and take action if required.
- **Intrusion detection systems (IDS) and malware detection tools—**use these to help you identify operators' attempts to propagate ransomware. This approach uses predefined signatures and rules for known exploits or more automated or general anomaly detection.
- **Deception tools—**establishing baits, lures, or a distributed deception platform. These tools should identify unauthorized lateral movement and

help discover an active breach with high-fidelity incidents.

How Can You Remove Ransomware?

When you experience a ransomware attack, you will not always be able to stop the attack or retrieve your data. However, you can apply remediation techniques that will be successful in some, though not all, cases.

One approach is to reboot the system in safe mode and install anti-malware to scan your machine and restore it to a pre-infection state. Another option is to restore your system from backups stored on separate drives or disks, media or location. You can reformat your disk to restore the system from an older backup in cloud-based systems as an example.

If you use Windows, you can utilize the System Restore function to restore your device and system files to a specified point in time before infection. However, you need to enable System Restore before the attack occurs to allow it to identify a safe point to restore. Windows will enable System Restore by default.

Here is a set of general steps you can take to identify and remove ransomware:

- **Create system backups -** ensure you create a backup for every important file. In the event of a ransomware attack, your system backups will let you restore any files that you cannot recover.
- **Preserve the evidence -** do not delete ransomware files before you identify them. Ensure your cleanup and system optimization tools keep the infection intact for investigation.
- **Use anti-malware -** isolate and quarantine any malware files and verify that the attacker does not have a backdoor to access your system in the future.
- **Identify the attack technique -** determine the type of ransomware files and encryption methods used. You can use ransomware recovery and decryptor tools to identify what ransomware the attacker used.

- **Decrypt the files-** use a ransomware recovery solution to identify and decrypt the ransomware files. However, decrypting the files might not always be possible depending on the ransomware techniques used.

Learn more about NetApp's Fully Managed Backup-as-a-Service solution

NetApp Ransomware Protection Solution

NetApp Ransomware Protection is a comprehensive set of data-centric capabilities **that allows you** to protect your data estate with a **Zero Trust** approach from the inside out. It enables you to map and classify your data, detect abnormal user activity, manage access, and avoid costly downtime **using** rapid backup and restore. IT teams can **apply** these advanced defense mechanisms to strengthen cyber resiliency and make sure the most critical data stays protected.

Semion Mazor
Product Evangelist