Cisco Advanced Malware Protection for Endpoints

– Malicious activity protection

What you will learn

This document explains the new engine added to Cisco® Advanced Malware Protection for Endpoints as a part of AMP Connector Version 6.1.5 for Windows–Malicious Activity Protection. The paper is intended to explain the technology, as well as help assess the value, of Malicious Activity Protection as an augmentation of the current security stack available with the product. It clarifies how the engine works and provides brief guidance for Proof of Value testing and demonstrations.

Introduction

Ransomware attacks can take many different shapes and forms. Ransomware is a type of malicious software that typically attempts to encrypt the files on a victim's computer. Upon successful encryption, it demands payment before the ransomed data is decrypted and access returned to the victim. Ransomware attacks are typically carried out using a malicious payload that is distributed as a legitimate file that tricks the user into downloading or opening when it arrives as an email attachment. However, there have been examples of ransomware attacks that are propagated without user interaction. The motivation for attackers using ransomware is nearly always monetary, and unlike other types of attacks, the victim is usually notified that an attack has occurred. The victim is then given instructions on how to recover from the attack. Payment is often demanded in a virtual currency so that the cyber criminal's identity isn't easily attributed. An important point here is that paying the ransom doesn't guarantee data decryption and this also sponsors development of next generation of ransomware. Refer to the Cisco Talos™ website (talosintelligence.com) to learn more about examples of recent ransomware attacks and foundational guidelines to minimize the risks.

AMP for Endpoints Malicious Activity Protection (MAP) engine included in the AMP Connector Version 6.1.5 for Windows defends your endpoints by monitoring the system and identifying processes that exhibit malicious activities when they execute and stops them from running. Because the MAP engine detects threats by observing the behavior of the process at run time, it can generically determine if a system is under attack by a new variant of ransomware or malware that may have eluded other security products and detection technology, such as legacy signature-based malware detection. The first release of the MAP engine targets identification, blocking, and quarantine of ransomware attacks on the endpoint.

Contents

AMP for endpoints protection lattice

AMP for Endpoints protection capabilities comprise several technologies that work together to prevent, detect, and remediate malicious code at the endpoint.

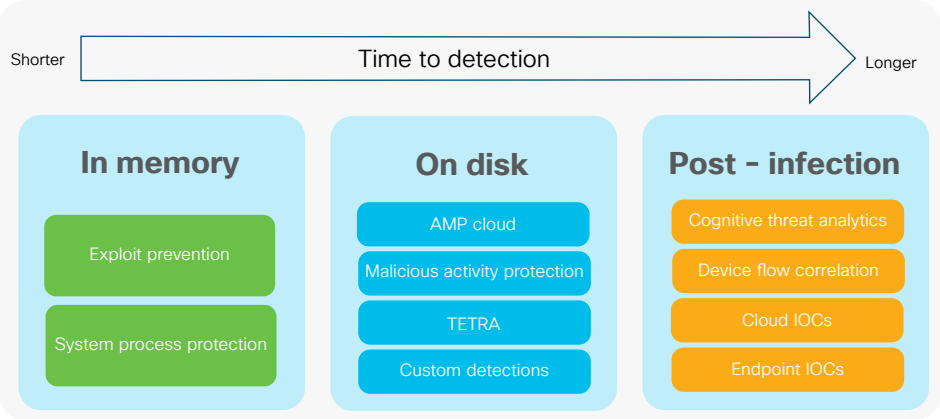
The core in-memory prevention technologies include:

- **Exploit Prevention** defends endpoints from memory injection attacks commonly used by malware and zero-day attacks on unpatched software vulnerabilities in protected processes.
- **System Process Protection** defends critical Windows system processes from being compromised through memory injection attacks by other processes.

The core on-disk detection technologies include:

- **AMP Cloud** provides access to the global intelligence database that is constantly updated and augmented with new detections and provides a great breadth of knowledge to the AMP Connector through one-to-one hash lookups, a generic signature engine, and the machine learning engine.
- **TETRA** is a traditional signature-based antivirus engine that resides on the endpoint and provides on-disk malware detection capabilities; TETRA is a part of the AMP Connector for Windows (ClamAV is an offline engine for Mac and Linux).
- **Malicious Activity Protection** provides run-time detection and blocking of abnormal behavior of a running program on the endpoint (for example, behaviors associated with ransomware).
- **Custom Detections** serve the goal of delivering robust control capabilities to the security administrator by allowing to define custom signatures and enforce blacklists.

Figure 1. AMP for Endpoints - Protection Lattice



The core post-infection detection technologies include:

- **Cognitive Threat Analytics** uses machine learning and artificial intelligence to correlate traffic generated by users to reliably identify command and control traffic, data exfiltration, and possibly unwanted applications already operating in the environment; it requires a proxy supplying weblogs or a Cisco Stealthwatch® Flow Collector supplying NetFlow.
- **Device Flow Correlation** allows to monitor network activity and determines which action the AMP Connector should take when connections to malicious hosts are detected.
- **Cloud Indication of Compromise (IOC)** is a feature that allows detecting suspicious behaviors observed on the endpoints and looks for patterns of malware and alerts on such; Cloud IOCs don't imply active blocking.
- **Endpoint IOC** is a powerful incident response tool for scanning post-compromise indicators across multiple computers and can be imported from open IOC-based files that are written to trigger on file properties.

These security features are the foundation of the overall approach to pervasive advanced malware protection. While Cisco recommends using all of these engines in conjunction with each other to leverage the full value of the product, customers can select whether to enable or disable one or another feature through a policy. MAP, which is the focus of this whitepaper, is itself just one of the important elements of functionality that AMP for Endpoints delivers. Although listed separately, these technologies work together as a detection lattice to provide improved visibility and increased control across the entire attack continuum.

Additional functionality of AMP for Endpoints, such as dynamic analysis and retrospective detection, is well described in the user guide available at docs.amp.cisco.com.

Malicious activity protection technology

The MAP engine is a behavioral-based detection engine that identifies malicious actions that are happening on the endpoint at run time. After extensive research with many variants of ransomware samples observed in the wild, the AMP for Endpoints research and development team has attributed common behaviors associated with such threats to build a rule set that is a part of the engine, residing on the AMP Connector itself.

How it works

The MAP engine constantly checks for certain changes (explained further) on the protected system to identify the processes that should be convicted when activities outlined in the behavioral rule set are matched. The following actions can be taken on processes detected by MAP, according to the policy configuration:

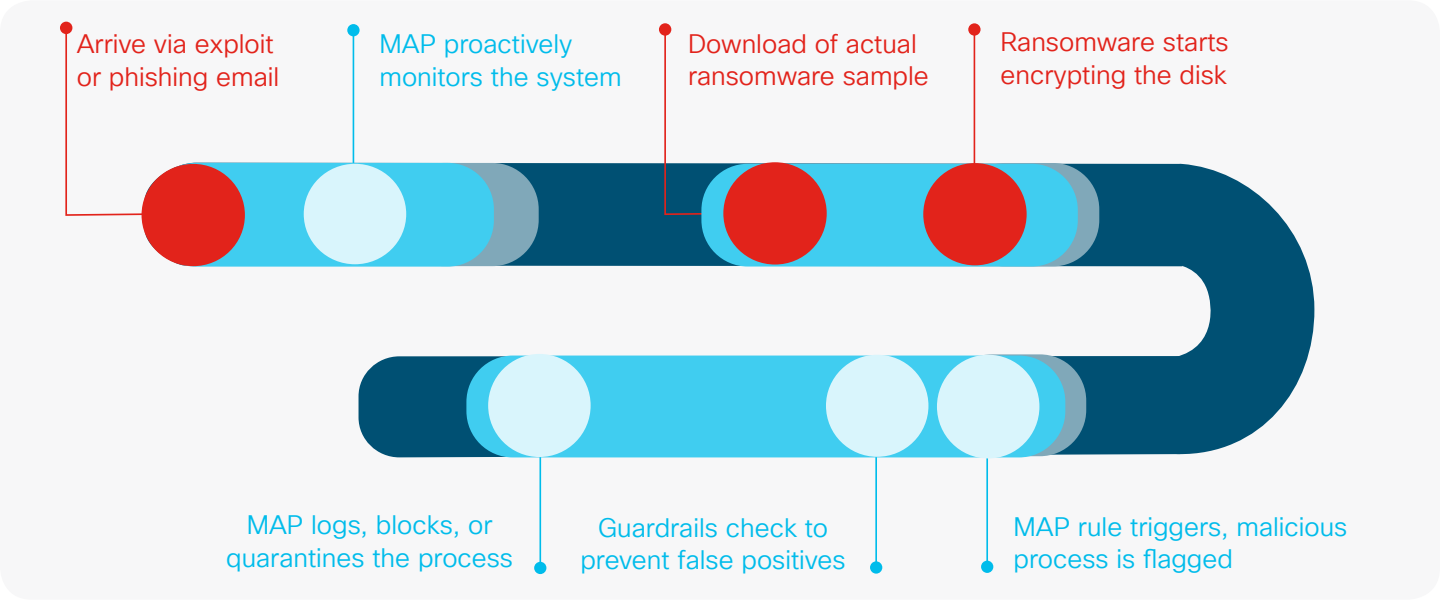
- Log the detection: In this mode, the identified malicious process is not blocked by MAP, but the detection is logged in the AMP for Endpoints console. (This is Audit mode, where no blocking or quarantine action happens, but the detection is logged.)
- Block process execution: In this mode, the malicious binary is identified and blocked, and no longer allowed to execute (similar to how the Application Blocking feature works).
- Quarantine process: This mode terminates the offending process and places the files into quarantine.

The set of detection rules in the MAP engine look for abnormalities on the system. For example, if the process reads, writes, and renames a set of files within a short span of time, then the rule can trigger to take action on that process. Alternatively, if the process reads and writes the content of a file to a different file and then deletes the original files, then the MAP engine can trigger to take action defined in the policy. These are just a couple of examples of rules present in the rule set. Rules are internal for developers and are never exposed to users, as well as not configurable by users. AMP for Endpoints engineering and research teams are continuously assessing techniques used by malware and ransomware in the wild to enhance the anticipated protection levels.

To combat false-positive detections, processes that are identified by the MAP engine as exhibiting malicious activity are checked against guardrails to prevent accidental blocking or quarantine of legitimate applications and operating system components.

Although the AMP Connector can detect and prevent ransomware from completely compromising data on the system, it is possible that some files will be encrypted by the offending process until the MAP engine determines that the process meets the criteria for being labeled as malicious. The AMP Connector will report files that were modified by the offending process so they can be quickly restored from backups, if necessary. This file history information lives in the MAP event shown in the AMP for Endpoints console.

Figure 2. MAP engine detection flow



MAP is a part of the AMP for Endpoints Connector for Windows. Refer to the release notes for details on the supported operating systems.

Performance and compatibility

Performance impact is a large part of the endpoint security selection criteria. AMP for Endpoints adds little overhead to system performance. Enabling the MAP engine does not imply a significant performance penalty or changes to the end user experience. The anticipated increase in CPU utilization associated with enabling the MAP engine is around 5%, and the memory, disk, and network performance impact is close to zero.

Compatibility with software installed on the endpoint is an essential aspect of any endpoint security solution. The MAP engine doesn't specifically have any known compatibility issues with third-party security software. Please refer to the AMP for Endpoints user guide for compatibility details around known issues.

Exclusions

Legitimate applications used in a customer environment that exhibit behavior similar to ransomware may need to be excluded from MAP monitoring. A simple example is archiving software. Process exclusions can be applied to prevent AMP for Endpoints from monitoring applications, and optionally their child processes, for the presence of malicious activity by the MAP engine. Note that child processes created by an excluded process are not excluded by default.

In general, exclusions can also be used to resolve conflicts with other security products or mitigate performance issues by excluding directories containing large files that are frequently written to, such as databases. Please refer to the AMP for Endpoints user guide for further details.

See it in action

Although MAP is an engine capable of generically stopping ransomware at run time (without regards to the exploitation vector, propagation abilities, hash of the sample, targeted files, file extensions, etc.), it may be helpful for testing purposes to relate to several examples of attacks that may be blocked or quarantined by the engine. Testing was performed using infrastructure automated for testing using different virtualization environments, as well as bare-metal machines with supported operating systems. AMP for Endpoints engineering and research teams are continuously evaluating techniques used by ransomware authors to enhance the protection levels.

Some of the ransomware families that were blocked or quarantined at run time by MAP include SamSam, WannaCry, JigSaw, Jaff, Cerber, TeslaCrypt, CryptoFortress, and many others.

Because the MAP engine uses behavior-based protection to look for activities, it is impossible to evade detection with simple changes to file hashes or obfuscation with the user of packers.

See it live here.

Appendix

Frequently asked questions

Question: If the process was quarantined by mistake, can it be restored back to normal operation?

The process that was incorrectly convicted and quarantined, as a result, can be restored using the normal AMP for Endpoints restore process. It then needs to be placed into a whitelist or excluded from AMP inspection through the AMP for Endpoints console and any occurrence like that should also be reported to engineering through the Cisco Technical Assistance Center.

Question: Can MAP address a use case where malicious code was injected into a legitimate process and used it for data encryption?

Because of the guardrails built into the AMP Connector, they may protect a legitimate process from being convicted by the MAP engine (even though it may contain malicious code inside, as a result of using process hollowing or other code injection techniques). Use of code injection techniques may be prevented by exploit prevention and system process protection engines that may be enabled through AMP's policy.

Question: Would the MAP engine stop ransomware launched from a connected USB drive?

Yes, the MAP engine monitors connected USB drives and blocks/quarantines ransomware processes launched from those.

Question: Is there a guarantee that all in-the-wild ransomware samples will get blocked or quarantined by the MAP engine?

Such a guarantee can never be provided. However, AMP's research and development teams perform continuous efficacy testing and ongoing investment in development of the feature to provide greater protection levels to customers.

Summary

Ransomware attacks significantly impact many organizations around the world. Over the years, this business has grown dramatically, and the most widespread ransomware attacks of the past do a decent job of telling the story of how it has grown. As is the case with so many breaches, the fault could be in the way organizations build and maintain their IT infrastructure. There is also always a human factor—many ransomware attacks begin with a simple phishing email, not even always targeted and well prepared by attackers.

MAP introduces a different approach to malware and ransomware protection that is more focused on run-time detection for blocking and quarantine. This approach is superior in identifying variants of ransomware at execution time without dependence on signature-based approaches and does not require prior knowledge on how the threat was built. Cisco strongly recommends leveraging this capability in conjunction with an architectural approach to security and best practices of information security that would contribute to an effective solution of either preventing or seriously limiting the impact of such threats. Having a sound, layered defense-in-depth strategy in place will ensure that organizations can limit widespread system outages, and detect and respond when system compromise occurs within their environments to minimize the impact these attacks may have.

Discover AMP for endpoints

To learn more about AMP for Endpoints and how it protects you against todays threats visit us at https://cisco.com/go/endpoints

Watch a demo of AMP for Endpoints at https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html?socialshare=lightbox-hero2

C11-740980-00 07/18