Protect against fileless malware with Cisco AMP for Endpoints

Exploit Prevention

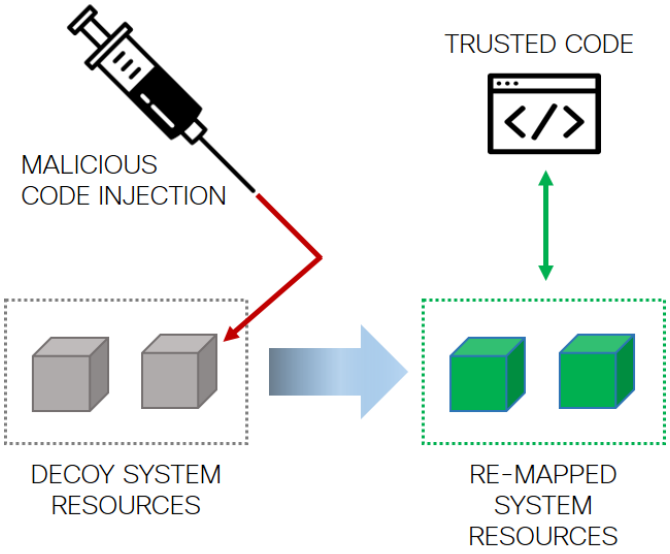
Malware can infiltrate endpoints by exploiting vulnerabilities in software and operating system processes, and thereby load themselves into memory. These include Web-based attacks that use shellcode to execute their payload, and ransomware that uses in-memory techniques. The Exploit Prevention engine on Cisco AMP for Endpoints defends your endpoints from malware and zero-day attacks that use memory injection on unpatched software vulnerabilities.

This capability will protect you from fileless and memory injection attacks, including:

- web-borne attacks, such as Java exploits that use shellcode to run payload
- malicious Adobe and Office document files
- malicious sites containing Flash, Silverlight and Javascript attacks
- vulnerabilities exploited by fileless and non-persistent malware
- zero-day attacks on software vulnerabilities yet to be patched
- ransomware, Trojans, or macros using in-memory techniques

How it works

The Exploit Prevention feature identifies common business applications running on your endpoints, remaps the libraries, and DLL entry and exit points, and then moves them to a randomized location upon every execution of the application. It then presents a decoy of these resources to any other processes, such as malware, trying to access or exploit them. The malware, unable to locate the real application, will then target the decoy instead, and AMP will log and block the attempt. Meanwhile, the real application is kept safe, and the attack is prevented.



Secure Networkers

Daron Walker - DIR Account Manager
Direct (832) 334-3625
CiscoDIR@SecureNetworkers.com
SecureNetworkers.com/dir
323 Sawdust Road, Spring, TX 77380

PROTECTED PROCESSES

- Microsoft Excel Application
- Microsoft Word Application
- Microsoft PowerPoint Application
- Microsoft Outlook Application
- Internet Explorer Browser
- Mozilla Firefox Browser
- Google Chrome Browser
- Microsoft Skype Application
- TeamViewer Application
- VLC Media player Application
- Microsoft Windows Script Host
- Microsoft Powershell Application
- Adobe Acrobat Reader Application
- Microsoft Register Server
- Microsoft Task Scheduler Engine

"In testing, AMP detected 100 percent of exploits, demonstrating its leadership in identifying the malicious software used to breach and compromise systems."

Senior Manager - IT Services, HCL Technologies

Learn More:

Cisco AMP for Endpoints Webpage
Cisco AMP for Endpoints Customer Testimonials
Cisco AMP for Endpoints Competitive Comparison