# Cisco WSA Ransomware Detection Capabilities and AMP Integration Verification

## Contents

## Issue

An inquiry was made regarding whether Cisco Secure Web Appliance (WSA) provides specific signature or detection capabilities for Triple X Ransomware. This question also included a request for clarification on how to verify whether an integration between Advanced Malware Protection (AMP) and Cisco Talos Threat Intelligence was functioning correctly on the WSA platform.

## Environment

- Cisco Secure Web Appliance (WSA)
- Advanced Malware Protection (AMP) Integration
- Cisco Talos Threat Intelligence Integration
- Web Reputation and URL Filtering (WBRS)
- Anti-Malware Scanning Engines (Webroot, McAfee, Sophos)
- Application Visibility and Control (AVC)

## Resolution

Cisco Secure Web Appliance does not rely on a single, dedicated signature specifically named for Triple X Ransomware. Instead, WSA employs a comprehensive multi-layered security architecture that utilizes various detection techniques to identify and block ransomware threats, including Triple X Ransomware variants.

### WSA Detection Methods

The WSA platform uses these detection techniques for ransomware protection:

- Pattern matching algorithms
- Heuristic analysis
- Emulation techniques
- Advanced Malware Protection (AMP) integrated with Cisco Talos Threat Intelligence
- Web Reputation and URL Filtering (WBRS)
- Multiple anti-malware scanning engines including Webroot, McAfee, and Sophos
- Application Visibility and Control (AVC)

These detection capabilities are continuously updated with new rules deployed every few minutes to ensure protection against emerging threats.

## Verifying AMP and Talos Integration

To confirm the integration between Advanced Malware Protection (AMP) and Cisco Talos Threat Intelligence is functioning correctly on WSA, administrators can review these logs:

**Step 1: Review WSA Access Logs**

Examine the Access Logs on the WSA appliance to verify AMP verdicts are being applied to downloaded files and web requests.

**Step 2: Check AMP Logs**

Review the AMP Logs to confirm that malware analysis results and threat intelligence data being processed.

**Step 3: Verify WBRS Scores**

Ensure the Web Reputation (WBRS) scores are being populated and they are associated with web requests in the logs.

If AMP verdicts and WBRS scores are being populated and enforced in the logs, this indicates the AMP and Talos integration is working as expected and providing real-time threat intelligence-based decisions.

## Cause

This was an informational request regarding WSAs ransomware detection capabilities rather than a technical issue requiring troubleshooting. The inquiry arose from a need to understand how WSA protects against specific ransomware variants and to verify that threat intelligence integrations are functioning properly.

## Related Content

- Cisco Secure Web Appliance Features and Benefits
- Cisco Talos Threat Intelligence Services
- Cisco Secure Web Appliance Datasheet
- Cisco Technical Support & Downloads