Funzionalità di rilevamento ransomware Cisco WSA e verifica dell'integrazione AMP

Sommario

Problema

È stata effettuata una richiesta di informazioni per stabilire se Cisco Secure Web Appliance (WSA) fornisce funzionalità specifiche di firma o rilevamento per Triple X Ransomware. La domanda comprendeva anche una richiesta di chiarimenti su come verificare se un'integrazione tra Advanced Malware Protection (AMP) e Cisco Talos Threat Intelligence funzionasse correttamente sulla piattaforma WSA.

Ambiente

- Cisco Secure Web Appliance (WSA)
- Integrazione con Advanced Malware Protection
- Integrazione con Cisco Talos Threat Intelligence
- Reputazione Web e filtro URL (WBRS)
- Motori di scansione antimalware (Webroot, McAfee, Sophos)
- Visibilità e controllo delle applicazioni (AVC)

Risoluzione

Cisco Secure Web Appliance non si basa su una singola firma dedicata specificamente nominata per Triple X Ransomware. WSA utilizza invece un'architettura di sicurezza completa a più livelli che utilizza varie tecniche di rilevamento per identificare e bloccare le minacce ransomware, incluse le varianti Triple X Ransomware.

Metodi di rilevamento WSA

La piattaforma WSA utilizza le seguenti tecniche di rilevamento per la protezione ransomware:

- Algoritmi di corrispondenza pattern
- Analisi euristica
- Tecniche di emulazione
- Advanced Malware Protection (AMP) integrato con Cisco Talos Threat Intelligence
- Reputazione Web e filtro URL (WBRS)
- Più motori di scansione antimalware, tra cui Webroot, McAfee e Sophos
- Visibilità e controllo delle applicazioni (AVC)

Queste funzionalità di rilevamento vengono continuamente aggiornate con nuove regole implementate a intervalli di pochi minuti per garantire la protezione contro le minacce emergenti.

Verifica dell'integrazione di AMP e Talos

Per verificare il corretto funzionamento dell'integrazione tra Advanced Malware Protection (AMP) e Cisco Talos Threat Intelligence su WSA, gli amministratori possono esaminare i seguenti registri:

Passaggio 1: Verifica log accessi WSA

Esaminare i log degli accessi sull'appliance WSA per verificare che i verdetti AMP vengano applicati ai file scaricati e alle richieste Web.

Passaggio 2: Verifica registri AMP

Esaminare i registri AMP per verificare che i risultati dell'analisi del malware e i dati di intelligence delle minacce siano stati elaborati.

Passaggio 3: Verifica punteggi WBRS

Verificare che i punteggi WBRS (Web Reputation) vengano popolati e siano associati a richieste

Web nei registri.

Se i verdetti AMP e i punteggi WBRS vengono inseriti e applicati nei registri, ciò indica che l'integrazione AMP e Talos funziona come previsto e fornisce decisioni basate sull'intelligence delle minacce in tempo reale.

Causa

Si tratta di una richiesta informativa relativa alle funzionalità di rilevamento ransomware WSA anziché di un problema tecnico che richiede la risoluzione dei problemi. L'indagine è nata dalla necessità di capire come WSA protegge da specifiche varianti ransomware e di verificare che le integrazioni di intelligence di minaccia funzionano correttamente.

Contenuto correlato

- Funzionalità e vantaggi di Cisco Secure Web Appliance
- Cisco Talos Threat Intelligence Services
- Cisco Secure Web Appliance - Scheda informativa
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).