Probleemoplossing voor misdaadpreventie in beveiligde endpoints

Inhoud

Inleiding

In dit document wordt beschreven hoe de engine voor explosiepreventie in de Secure Endpoint-console is geconfigureerd en hoe u een basisanalyse kunt uitvoeren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan.

- Admin-toegang tot Secure Endpoint-console
- Secure Endpoint-connector
- Functie Exploit Prevention ingeschakeld

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies.

- Connector, versie 7.3.15 of hoger
- Windows 10 versie 1709 en hoger voor Windows Server 2016 versie 1709 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De procedure die in dit document wordt beschreven, is handig voor het uitvoeren van een basisanalyse op basis van de gebeurtenissen, getriggerd in de console en stelt u voor Exploit Prevention-uitsluitingen uit te voeren voor het geval u het proces kent en het in uw omgeving gebruikt.

De Exploit Prevention Engine biedt de mogelijkheid om uw endpoints te verdedigen tegen geheugeninjecties die vaak worden gebruikt door malware en andere zero-day aanvallen op ongepatched software kwetsbaarheden. Wanneer het een aanval tegen een beschermd proces ontdekt wordt het geblokkeerd en genereert het een gebeurtenis maar het wordt niet in quarantaine geplaatst.

Beschermde processen

De Exploit Prevention Engine beschermt deze 32-bits en 64-bits (Secure Endpoint Windows-connector versie 6.2.1 en hoger) processen en hun onderliggende processen:

- Microsoft Excel-toepassing
- Microsoft Word-toepassing
- Microsoft PowerPoint-toepassing
- Microsoft Outlook-toepassing
- Internet Explorer-browser
- Mozilla Firefox-browser
- Google Chrome-browser
- Microsoft Skype-toepassing
- TeamViewer-toepassing
- VLC Media Player-toepassing
- Microsoft Windows Script-host
- Microsoft PowerShell-toepassing
- Adobe Acrobat Reader-toepassing
- Microsoft-registratieserver
- Microsoft Task Scheduler Engine
- Microsoft Run DLL-opdracht
- Microsoft HTML-toepassingshost
- Windows Script-host
- Microsoft Assembly Registration Tool
- Zoomen
- gleuf
- Cisco Webex Teams
- Microsoft Teams

Uitgesloten processen

Deze processen worden uitgesloten (niet bewaakt) van de Exploit Prevention motor vanwege compatibiliteitsproblemen:

- McAfee DLP-service

- McAfee Endpoint Security Utility

Exploit Prevention versie 5 (Connector, versie 7.5.1 en hoger)

Secure Endpoint Windows-connector 7.5.1 bevat een belangrijke update om Exploit Prevention uit te voeren. De nieuwe eigenschappen in deze versie omvatten:

- Bescherm netwerkdrives: Beschermt automatisch processen die lopen van netwerkdrives tegen bedreigingen zoals ransomware
- Bescherm externe processen: Beschermt automatisch processen die op afstand worden uitgevoerd op beschermde computers die een domein authenticated user (admin) gebruiken
- AppControl bypass via rundll32: Stopt speciaal ontworpen rundll32 commando lijnen die geinterpreteerde opdrachten kunnen uitvoeren
- UAC-omleiding: Vergrendelt de escalatie van de voorrechten door kwaadwillige processen, het verhindert de omzeilen van het mechanisme van de Controle van de Rekening van de Gebruiker van Windows
- Browser/Mimikatz vaults referenties: Indien ingeschakeld, beschermt Exploit Prevention tegen inbraak van referenties in Microsoft Internet Explorer en Edge-browsers
- Schaduwkopie wissen: Traceert het wissen van schaduwkopieën en onderschept de COM API in de Microsoft Volume Shadow Copy Service (vsvc.exe)
- SAM hashes: Beschermt tegen SAM hash credential diefstal door Mimikatz, onderschept pogingen om alle SAM hashes op te sommen en te decoderen in de register hive **Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users**

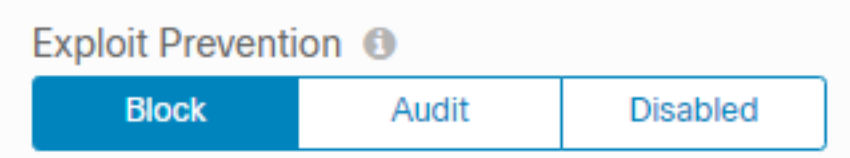
- Bescherm uitgevoerde processen: Injecteer in processen die lopen, als die zijn begonnen vóór de Exploit Prevention instantie (explorer.exe, lsass.exe, spoolsv.exe, winlogon.exe)

Deze functies zijn standaard ingeschakeld wanneer Exploit Prevention is ingeschakeld in het beleid.

Configuratie

Om de Exploit Prevention engine in te schakelen, navigeer naar de **modi en motoren** in uw beleid en selecteer Audit Mode, Block Mode, of Uitgeschakeld modus, zoals in de afbeelding.

> **Opmerking:** De Auditmodus is alleen beschikbaar in Secure Endpoint Windows-connector 7.3.1 en hoger. Eerdere versies van de connector behandelen de auditmodus hetzelfde als de blokmodus.

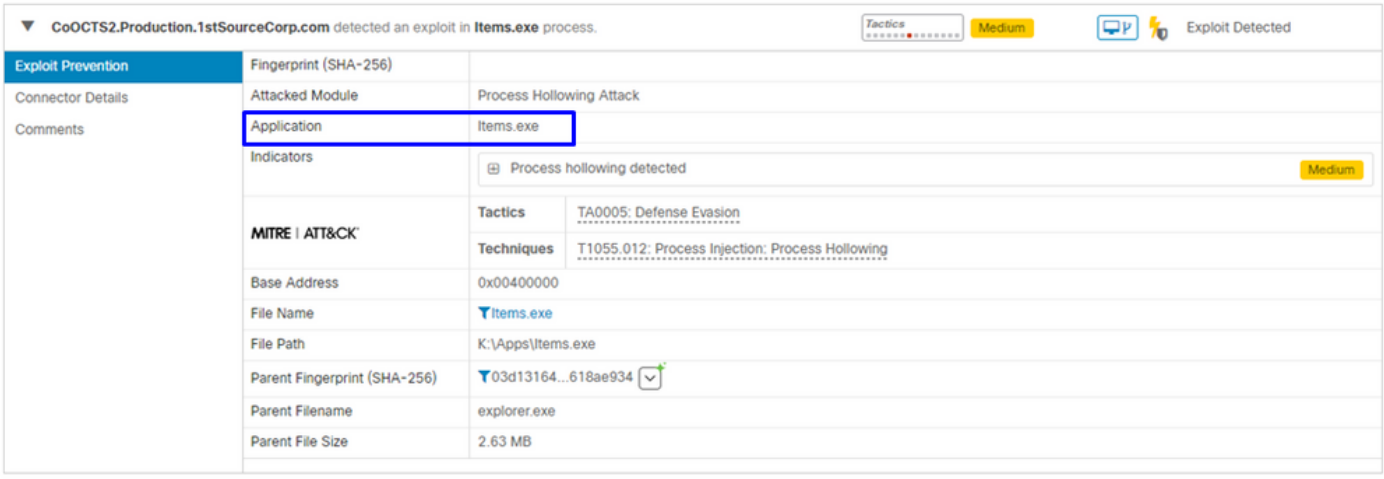


> **Opmerking:** Op Windows 7 en Windows Server 2008 R2 moet u de patch voor Microsoft Security Advisory 303929 toepassen voordat u de connector installeert.

Detectie

Zodra de detectie is geactiveerd, wordt een pop-upmelding weergegeven op het eindpunt, zoals in het beeld wordt weergegeven.

De console geeft een Exploit Prevention-gebeurtenis weer, zoals in de afbeelding.

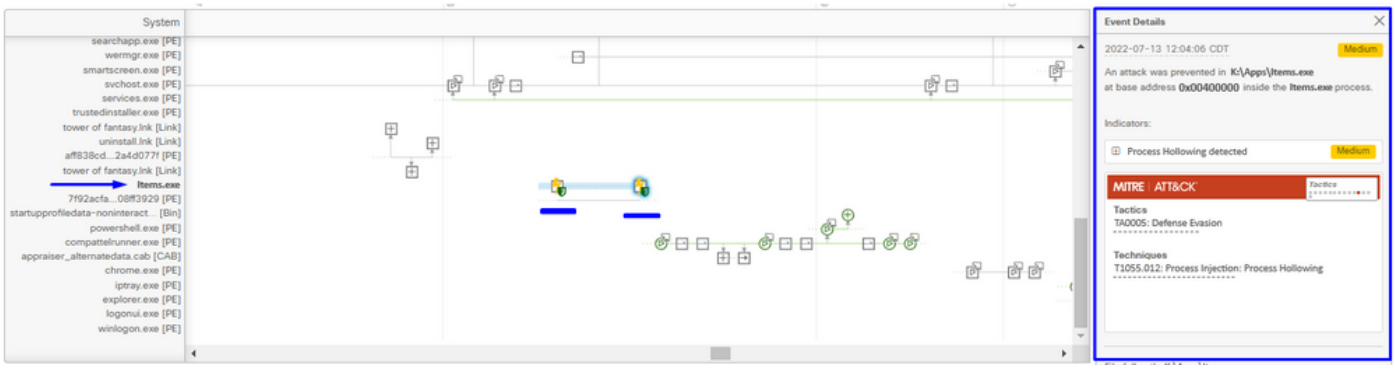


Problemen oplossen

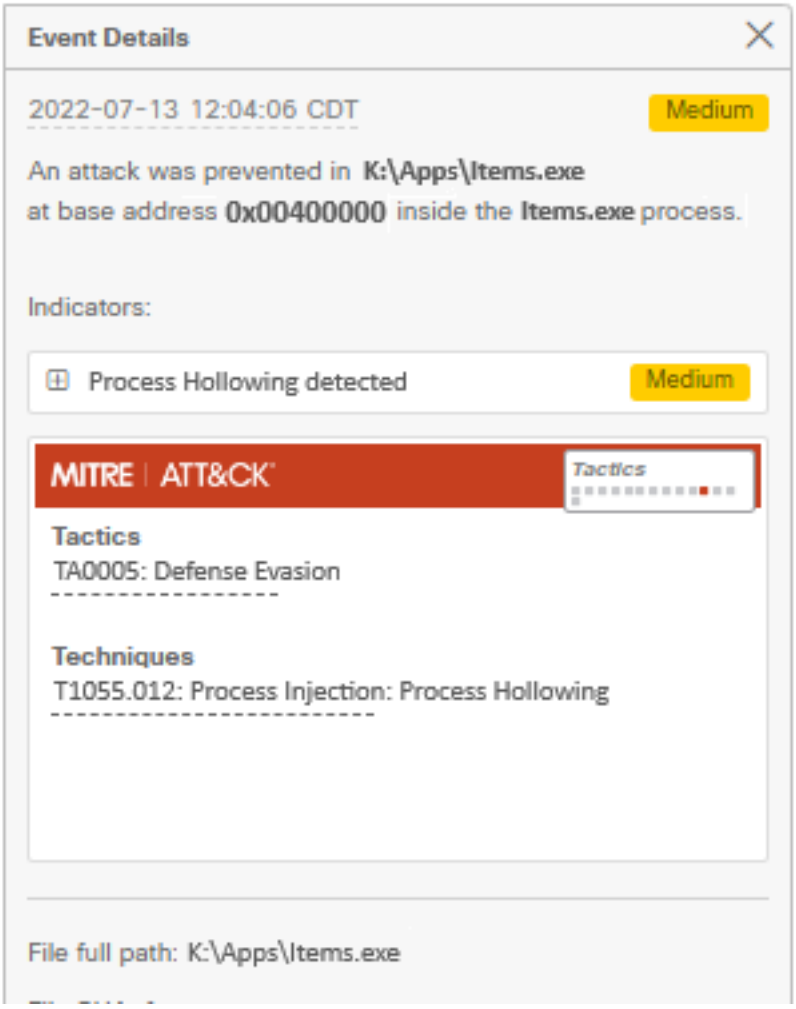
Wanneer een Exploit Prevention-gebeurtenis in de console wordt geactiveerd, is een manier om het gedetecteerde proces te identificeren gebaseerd op de details om u inzicht te geven in de gebeurtenissen die plaatsvonden terwijl de toepassing of het proces liep, kunt u naar het **Apparaattraject** navigeren.

Stap 1. Klik op het pictogram **Apparaattraject** dat wordt weergegeven in de gebeurtenis Exploit Prevention, zoals in de afbeelding.

Stap 2. Vind het pictogram Exploit Prevention in de tijdlijn van het apparaattraject om de sectie **Event Details** te zien, zoals in de afbeelding.



Stap 3. Identificeer de details van de gebeurtenis en evalueer of het proces of de toepassing in uw omgeving vertrouwd/bekend is.



Fout-positieve detectie

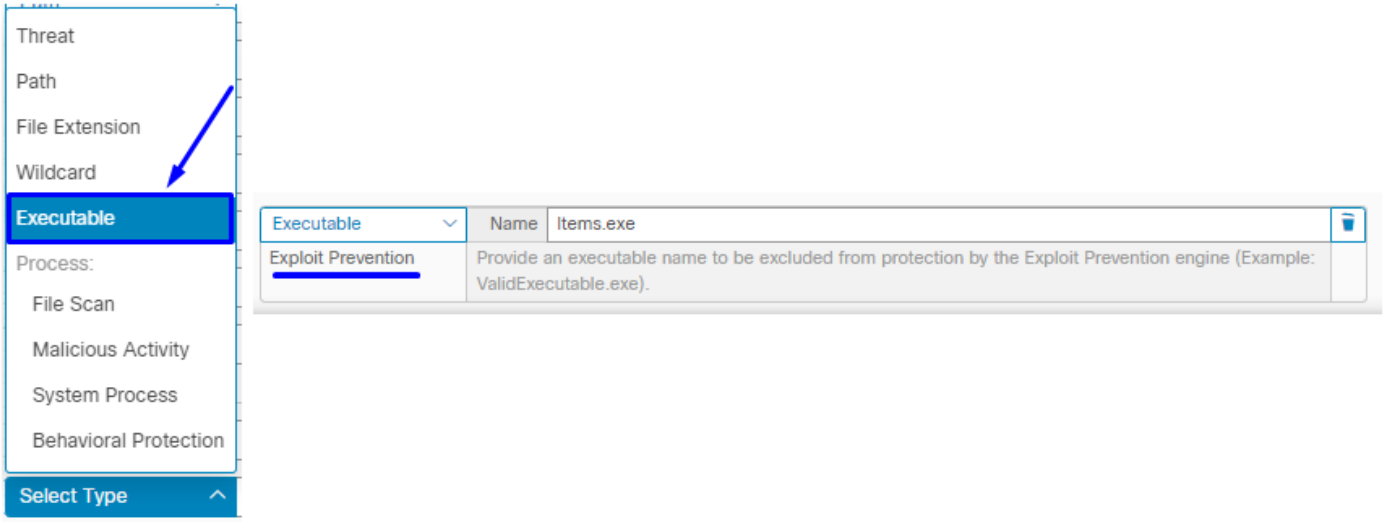
Zodra de detectie is geïdentificeerd en als het proces/uitvoerbaar wordt vertrouwd op en bekend is bij uw omgeving, kan het als een uitsluiting worden toegevoegd. Om te voorkomen dat de connector scant.

Uitsluitbare uitsluitingen zijn alleen van toepassing op connectors die geschikt zijn voor Exploit Prevention (Connector, versie 6.0.5 en hoger). Een uitvoerbare uitsluiting wordt gebruikt om bepaalde uitvoerbare goederen uit te sluiten van de Exploit Prevention engine.

> **Let op**: jokerteken en extensies anders dan exe worden niet ondersteund.

U kunt de lijst met beschermde processen controleren en alle processen uitsluiten van de Exploit Prevention engine, u moet de uitvoerbare naam opgeven in het veld Application Exclusion. U kunt ook alle toepassingen uitsluiten van de engine. De uitvoerbare uitsluitingen moeten de uitvoerbare naam precies in het formaat **name.exe** aanpassen, zoals in het beeld wordt getoond.

> **Opmerking:** Alle uitvoerbare bestanden die u uitsluit van Exploit Prevention moeten opnieuw worden gestart nadat de uitsluiting is toegepast op de connector. En als u Exploit Prevention uitschakelt, moet u een van de beschermde processen die actief waren opnieuw opstarten.



> **Opmerking:** Zorg ervoor dat de uitsluitingsset is toegevoegd aan het beleid dat is toegepast op de betreffende connector.

Tot slot kunt u het gedrag controleren.

Neem contact op met TAC ondersteuning als de detectie van exploitepreventie blijft voortduren om een diepere analyse uit te voeren. Hier vindt u de vereiste informatie:

- Schermafbeelding van het evenement Exploit Prevention
- Schermafbeelding van het apparaattraject en gebeurtenisgegevens
- SHA256 van de betrokken toepassing/procedure
- Komt het probleem voor met Uitbuitingspreventie uitgeschakeld?
- Komt het probleem voor wanneer de Secure Endpoint connector service is uitgeschakeld?
- Heeft het eindpunt andere Security of Antivirus software?
- Wat is de betreffende toepassing? Beschrijf de functie ervan
- Diagnostische bestand (Debug bundel logbestanden) met Debug modus ingeschakeld wanneer de kwestie voorkomt (in dit artikel kunt u vinden hoe het diagnostische bestand te verzamelen)

Gerelateerde informatie

- Gebruikershandleiding Secure Endpoint
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.