Ordem da quarentena ESA/CES quando embandeirado por serviços múltiplos

Índice

Introdução

Este documento descreve o comportamento dos dispositivos da Segurança do email da ferramenta de segurança (ESA) e da nuvem do email de Cisco (CES) quando um email é embandeirado por serviços múltiplos para quarantining e o fluxo FO o email com o resto do encanamento do email.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada em Cisco ESA com versão de AsyncOS 12.1.0.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Os email que corre através Cisco ESA e dispositivos CES para filtrar seguem o encanamento da fila de trabalho do email. O encanamento é estático e se há umas ações múltiplas dos serviços múltiplos definidos para embandeirar um email para as quarentena, não segue a ordem conforme o encanamento; em lugar de, o ESA/CES quarantines o com sua própria ordem.

> Nota: Os email a que são embandeirados com as ações ajustadas (ação final) tomarão a precedência imediata e retiram o processamento da fila de trabalho.

Que acontece ao email quando embandeirado por serviços múltiplos para a quarentena?

O email é dado a prioridade na quarentena da manifestação do vírus da política (PVO) primeiramente. Não há nenhuma ordem específica em que a quarentena da política ele entra enquanto o PVO alista cada outra quarentena que o email está guardado igualmente dentro. Depois que o email é liberado fora de uma das quarentena PVO, realiza-se em todas as quarentena respectivas a ser embandeiradas dentro.

Depois que o email foi liberado (manualmente ou através do temporizador onde a ação padrão é ajustada se liberar) os email a seguir incorporam a quarentena do Spam. Quando o email é liberado da quarentena do Spam, transverses na entrega enfileira-se para a entrega final depois disso.

> Nota: Um email que seja suprimido fora de uma quarentena PVO, removerá o email de todo o subsequente quarantines o guardou dentro também.

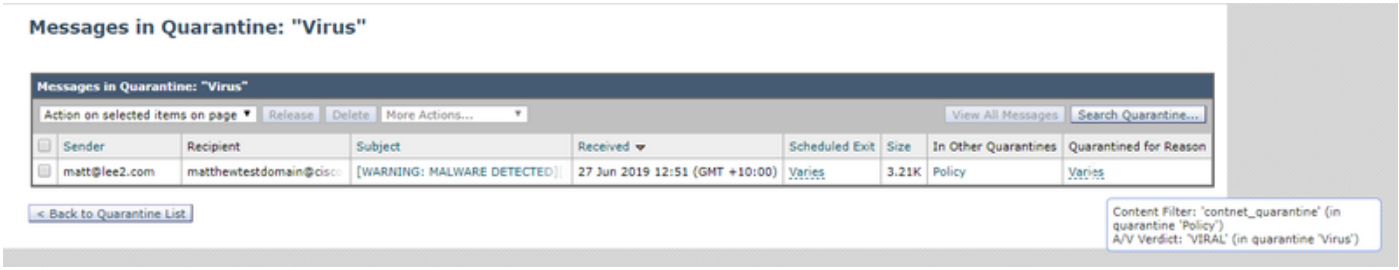
- As mensagens liberadas das quarentena da política e do vírus são tornadas a varrer pela proteção do malware, e pelos motores anti-vírus, avançados do graymail.
- As mensagens liberadas da quarentena da manifestação são tornadas a varrer pelos motores do anti-Spam, os anti-vírus, e AMP.
- As mensagens liberadas da quarentena da análise do arquivo são tornadas a varrer para ameaças.
- As mensagens com acessórios são tornadas a varrer pelo serviço da reputação do arquivo em cima da liberação das quarentena da política, do vírus, e da manifestação.

Injeção inicial do email com a filtração feita pelo ESA. Nesta saída você vê que está embandeirada pela quarentena do Spam, pela quarentena do vírus, e pela quarentena da política:

```
Thu Jun 27 12:51:03 2019 Info: Start MID 378951 ICID 391696
Thu Jun 27 12:51:03 2019 Info: MID 378951 ICID 391696 From: <matt@lee2.com>
Thu Jun 27 12:51:10 2019 Info: MID 378951 ICID 391696 RID 0 To: <matthewtestdomain@cisco.com>
Thu Jun 27 12:51:14 2019 Info: MID 378951 Subject 'Test email with AV EICAR and other triggers'
Thu Jun 27 12:51:15 2019 Info: MID 378951 ready 3292 bytes from <matt@lee2.com>
Thu Jun 27 12:51:15 2019 Info: MID 378951 matched all recipients for per-recipient policy matt
in the inbound table
Thu Jun 27 12:51:15 2019 Info: MID 378951 interim verdict using engine: CASE spam positive
Thu Jun 27 12:51:15 2019 Info: MID 378951 using engine: CASE spam positive
Thu Jun 27 12:51:15 2019 Info: ISQ: Tagging MID 378951 for quarantine
Thu Jun 27 12:51:15 2019 Info: MID 378951 interim AV verdict using Sophos VIRAL
Thu Jun 27 12:51:15 2019 Info: MID 378951 antivirus positive 'EICAR-AV-Test'
Thu Jun 27 12:51:15 2019 Info: MID 378951 AMP file reputation verdict : MALWARE
Thu Jun 27 12:51:15 2019 Info: MID 378951 attachment 'testAV.txt'
Thu Jun 27 12:51:15 2019 Info: MID 378951 URL https://ihaveabadreputation.com has reputation -
9.3 matched Condition: URL Reputation Rule
Thu Jun 27 12:51:15 2019 Info: MID 378951 Custom Log Entry:  - Match whole word filter
Thu Jun 27 12:51:15 2019 Info: ISQ: Tagging MID 378951 for quarantine (X-Ironport-Quarantine)
Thu Jun 27 12:51:15 2019 Info: MID 378951 quarantined to "Policy" (content
filter:contnet_quarantine)
Thu Jun 27 12:51:15 2019 Info: MID 378951 quarantined to "Virus" (a/v verdict:VIRAL)
Thu Jun 27 12:51:15 2019 Info: Message finished MID 378951 done
Thu Jun 27 12:51:15 2019 Info: ICID 391696 close
```

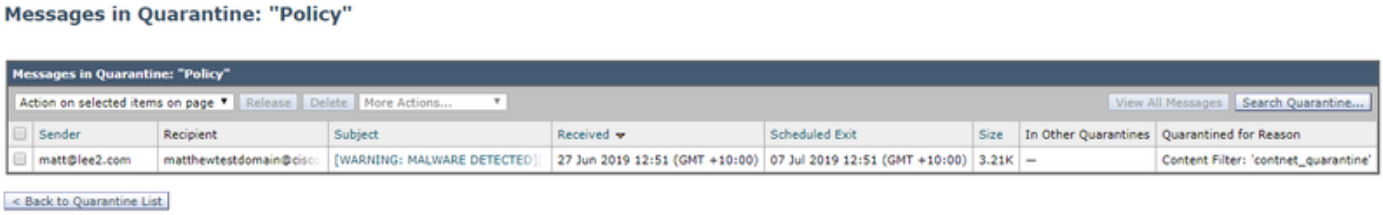
Investigado uma vez dentro da quarentena, do email realizado na quarentena que PVO você

marcou é visto, assim como das algumas outras quarentena embandeira para estar dentro.



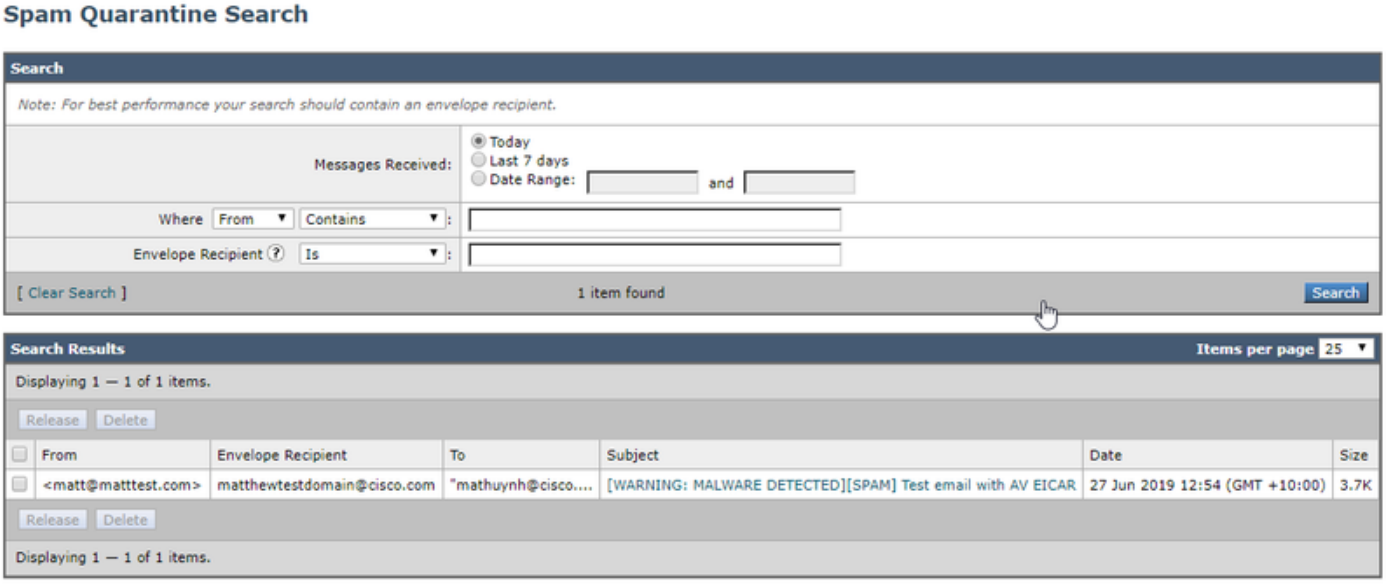
Depois que se libera desta quarentena, registra este evento em seus **mail_logs** e reflete nas outras quarentena também que está já não disponível na outra quarentena.

```
Thu Jun 27 12:52:59 2019 Info: MID 378951 released from quarantine "Virus" (manual) t=104
```



Libere-a fora da quarentena PVO que permanece permite que os email viajem à quarentena embandeirada do Spam depois disso.

```
Thu Jun 27 12:54:15 2019 Info: MID 378951 released from quarantine "Policy" (manual) t=180
Thu Jun 27 12:54:15 2019 Info: MID 378951 released from all quarantines
Thu Jun 27 12:54:15 2019 Info: MID 378951 matched all recipients for per-recipient policy matt
in the inbound table
Thu Jun 27 12:54:15 2019 Info: MID 378951 interim AV verdict using Sophos VIRAL
Thu Jun 27 12:54:15 2019 Info: MID 378951 antivirus positive 'EICAR-AV-Test'
Thu Jun 27 12:54:15 2019 Info: MID 378951 AMP file reputation verdict : MALWARE
Thu Jun 27 12:54:15 2019 Info: ISQ: Tagging MID 378951 for quarantine (X-Ironport-Quarantine)
Thu Jun 27 12:54:15 2019 Info: MID 378951 queued for delivery
Thu Jun 27 12:54:15 2019 Info: RPC Delivery start RCID 13914 MID 378951 to local IronPort Spam
Quarantine
Thu Jun 27 12:54:15 2019 Info: ISQ: Quarantined MID 378951
Thu Jun 27 12:54:15 2019 Info: RPC Message done RCID 13914 MID 378951
Thu Jun 27 12:54:15 2019 Info: Message finished MID 378951 done
```



Lá na versão final da quarentena do Spam, o email é destinado para a fila da entrega.

```
Thu Jun 27 12:55:33 2019 Info: Start MID 378952 ICID 0 (ISQ Released Message)
Thu Jun 27 12:55:33 2019 Info: ISQ: Reinjected MID 378951 as MID 378952
Thu Jun 27 12:55:33 2019 Info: MID 378952 ICID 0 From: <matt@lee2.com>
Thu Jun 27 12:55:33 2019 Info: MID 378952 ICID 0 RID 0 To: <matthewtestdomain@cisco.com>
Thu Jun 27 12:55:33 2019 Info: MID 378952 Subject '[WARNING: MALWARE DETECTED][SPAM] Test email
with AV EICAR'
Thu Jun 27 12:55:33 2019 Info: MID 378952 ready 9661 bytes from <matt@lee2.com>
Thu Jun 27 12:55:33 2019 Info: MID 378952 queued for delivery
```

Informações Relacionadas

- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final
- Suporte Técnico e Documentação - Cisco Systems