Índice

Introdução

Este documento descreve como permitir a Filtragem URL na ferramenta de segurança do email de Cisco (ESA) e os melhores prática para seu uso.

Informações de Apoio

Quando você permite a Filtragem URL no ESA, você deve igualmente permitir os outros recursos, dependentes de sua funcionalidade desejada. Estão aqui algumas características típicas que são permitidas ao lado da Filtragem URL:

- Para a proteção aprimorada contra o Spam, a característica da exploração do Anti-Spam deve ser permitida globalmente de acordo com a política aplicável do correio. Esta pode ser o Anti-Spam de Cisco IronPort (IPA) ou a característica inteligente da Multi-varredura de Cisco (IMS).
- Para a proteção aprimorada contra o malware, a característica dos filtros da manifestação ou dos filtros da manifestação do vírus (VOF) deve ser permitida globalmente de acordo com a política aplicável do correio.
- Para as ações baseadas na reputação URL, ou a fim reforçar políticas de uso aceitável com o uso de filtros da mensagem e do índice, você deve permitir VOF globalmente.

Permita a Filtragem URL

A fim executar a Filtragem URL no ESA, você deve primeiramente permitir a característica. Há dois métodos diferentes que você pode usar a fim permitir esta característica: Com o uso do GUI ou do CLI.

A fim permitir a Filtragem URL com o uso do GUI, navegue aos **Serviços de segurança > à Filtragem URL > permitem:**

A fim permitir a Filtragem URL com o uso do CLI, incorpore o comando do **websecurityconfig**:

```
Enable URL Filtering? [N]> y
```

Éimportante notar que você deve igualmente permitir a URL que registra de dentro do VOF. Esta é uma característica CLI-somente que deva ser permitida como mostrado aqui:

```
myesa.local> outbreakconfig

Outbreak Filters: Enabled

Choose the operation you want to perform:
- SETUP - Change Outbreak Filters settings.
- CLUSTERSET - Set how the Outbreak Filters are configured in a cluster.
- CLUSTERSHOW - Display how the Outbreak Filters are configured in a cluster.
[]> setup

Outbreak Filters: Enabled
Would you like to use Outbreak Filters? [Y]>

Outbreak Filters enabled.

Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above or
back down below), meaning that new messages of certain types could be quarantined
or will no longer be quarantined, respectively.

Would you like to receive Outbreak Filter alerts? [N]>

What is the largest size message Outbreak Filters should scan?
[2097152]>

Do you want to use adaptive rules to compute the threat level of messages? [Y]>

Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N]> y

Logging of URLs has been enabled.

The Outbreak Filters feature is now globally enabled on the system. You must use the
'policyconfig' command in the CLI or the Email Security Manager in the GUI to enable
Outbreak Filters for the desired Incoming and Outgoing Mail Policies.
```

> Nota: Assegure-se de que você **comprometa** *alguns* e *todas as* mudanças a sua configuração antes que você continue do GUI ou do CLI em seu ESA.

Crie ações da Filtragem URL

Quando você permite a Filtragem URL apenas, não toma a ação contra as mensagens que puderam conter URL vivas e válidas.

As URL incluídas no mensagem de entrada e saída (com a exclusão dos acessórios) são avaliadas. Toda a série válida para uma URL é avaliada, para incluir cordas com estes componentes:

- HTTP, HTTPS, ou WWW
- Domínio ou endereços IP de Um ou Mais Servidores Cisco ICM NT
- Números de porta precedidos por uns dois pontos (:)
- Uppercase ou letras minúsculas

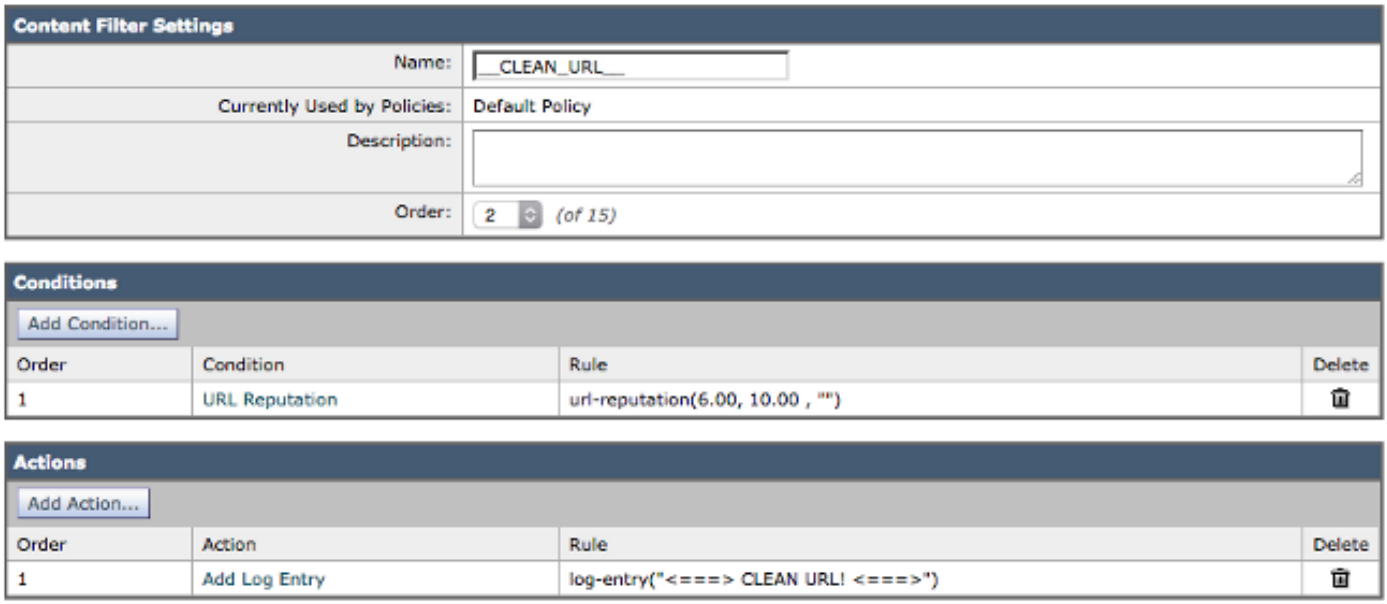
Quando o sistema avalia URL a fim determinar se uma mensagem é Spam, caso necessário para

o Gerenciamento da carga, dá a prioridade e seleciona a mensagens de entrada sobre mensagens externa.

A fim fazer a varredura rapidamente de URL e tomar a ação, você pode criar um filtro satisfeito de modo que *se a* mensagem tem uma URL válida, *a seguir a* ação é aplicada. Do GUI, navegue **para enviar políticas > filtro entrante do > Add dos filtros do índice**.

Satisfaça filtros para URL limpas

Este exemplo mostra uma varredura para URL limpas com a aplicação deste filtro satisfeito de entrada:



Com este filtro no lugar, o sistema procura por uma URL com uma reputação *limpa* (6.00 10.00) e adiciona simplesmente uma entrada de registro ao correio entra a ordem para provocar e gravar a contagem baseada Web da reputação (WBRS). Esta entrada de registro igualmente ajuda a identificar o processo que é provocado. Está aqui um exemplo dos logs do correio:

```
Wed Nov 5 21:11:10 2014 Info: Start MID 182 ICID 602
Wed Nov 5 21:11:10 2014 Info: MID 182 ICID 602 From: <bad_user@that.domain.net>
Wed Nov 5 21:11:10 2014 Info: MID 182 ICID 602 RID 0 To: <joe.user@goodmailguys.com>
Wed Nov 5 21:11:10 2014 Info: MID 182 Message-ID
'<D08042EA.24BA4%bad_user@that.domain.net>'
Wed Nov 5 21:11:10 2014 Info: MID 182 Subject 'Starting at the start!'
Wed Nov 5 21:11:10 2014 Info: MID 182 ready 2798 bytes from
<bad_user@that.domain.net>
Wed Nov 5 21:11:10 2014 Info: MID 182 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Wed Nov 5 21:11:11 2014 Info: MID 182 interim AV verdict using Sophos CLEAN
Wed Nov 5 21:11:11 2014 Info: MID 182 antivirus negative
Wed Nov 5 21:11:11 2014 Info: MID 182 URL http:// www .yahoo.com has reputation 8.39
matched url-reputation-rule
Wed Nov 5 21:11:11 2014 Info: MID 182 Custom Log Entry: <===> CLEAN URL! <===>
Wed Nov 5 21:11:11 2014 Info: MID 182 Outbreak Filters: verdict negative
Wed Nov 5 21:11:11 2014 Info: MID 182 queued for delivery
Wed Nov 5 21:11:11 2014 Info: New SMTP DCID 23 interface 192.168.0.199 address
192.168.0.200 port 25
Wed Nov 5 21:11:11 2014 Info: Delivery start DCID 23 MID 182 to RID [0]
Wed Nov 5 21:11:11 2014 Info: Message done DCID 23 MID 182 to RID [0] [('X-IronPort-AV',
```

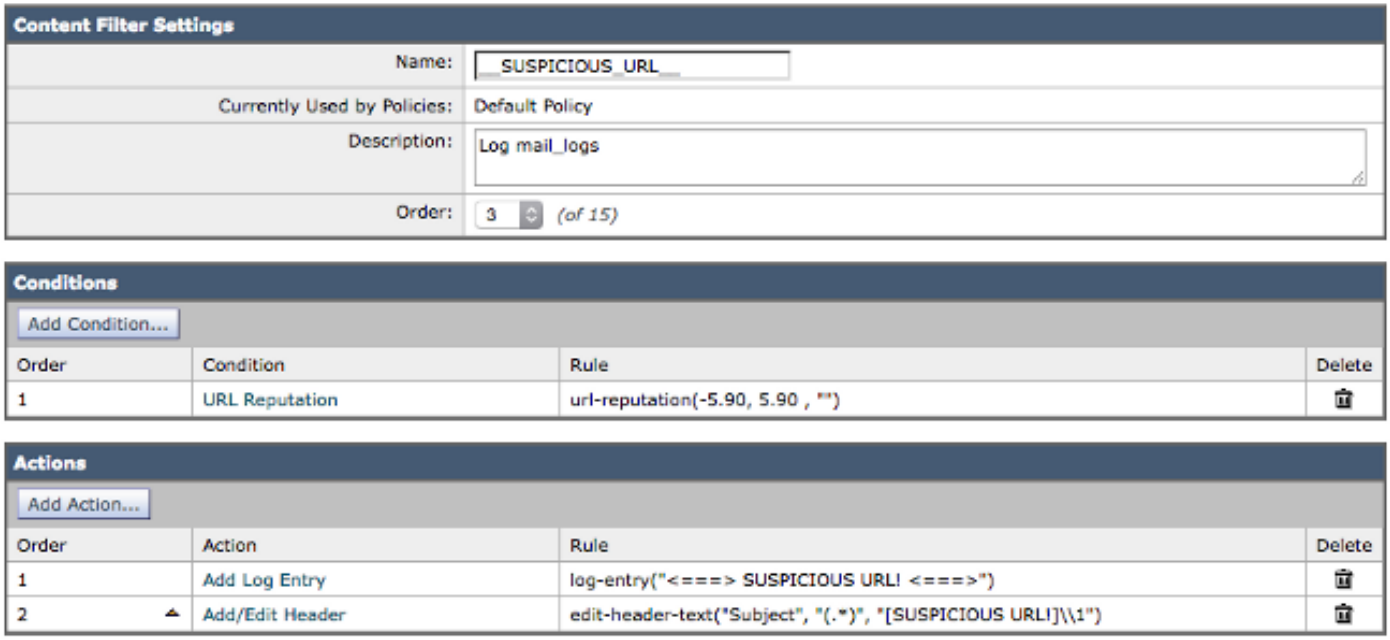
```
'E=Sophos;i="5.07,323,1413259200"; \r\n d="scan\'208,217";a="182"'), ('x-ironport-av',
'E=Sophos;i="5.07,323,1413244800"; \r\n d="scan\'208,217";a="93839309"')]
Wed Nov 5 21:11:11 2014 Info: MID 182 RID [0] Response '2.0.0 Ok: queued as 7BAF5801C2'
Wed Nov 5 21:11:11 2014 Info: Message finished MID 182 done
Wed Nov 5 21:11:16 2014 Info: ICID 602 close
Wed Nov 5 21:11:16 2014 Info: DCID 23 close
```

> Nota: A URL que é encaixada no exemplo anterior tem-no os espaços extras incluídos no corpo URL, assim que não tropeça nenhuma varreduras da Web ou detecção do proxy.

Segundo as indicações do exemplo, **Yahoo.com** é julgado **LIMPO** e dado uma contagem de **8.39**, é notado nos logs do correio, e entregado ao utilizador final.

Filtros satisfeitos para as URL suspeitas

Este exemplo mostra uma varredura para as URL suspeitas com a aplicação deste filtro satisfeito de entrada:



Com este filtro no lugar, o sistema procura por uma URL com uma reputação *suspeita* (-5.90 -3.1) e adiciona uma entrada de registro aos logs do correio. Este exemplo mostra um assunto alterado a fim prepend o **"[SUSPECT URL!]"**. Está aqui um exemplo dos logs do correio:

```
Wed Nov 5 21:22:23 2014 Info: Start MID 185 ICID 605
Wed Nov 5 21:22:23 2014 Info: MID 185 ICID 605 From: <bad_user@that.domain.net>
Wed Nov 5 21:22:23 2014 Info: MID 185 ICID 605 RID 0 To: <joe.user@goodmailguys.com>
Wed Nov 5 21:22:23 2014 Info: MID 185 Message-ID
'<D0804586.24BAE%bad_user@that.domain.net>'
Wed Nov 5 21:22:23 2014 Info: MID 185 Subject 'Middle of the road?'
Wed Nov 5 21:22:23 2014 Info: MID 185 ready 4598 bytes from
<bad_user@that.domain.net>
Wed Nov 5 21:22:23 2014 Info: MID 185 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Wed Nov 5 21:22:24 2014 Info: MID 185 interim AV verdict using Sophos CLEAN
Wed Nov 5 21:22:24 2014 Info: MID 185 antivirus negative
Wed Nov 5 21:22:24 2014 Info: MID 185 URL https:// www.udemy.com/official-udemy-
instructor-course/?refcode=slfgiacoitvbfgl7tawqoxwqrdqcerbhub1flhsmfilcfku1te5x
ofictyrmwfcfxcvfgdkobgbcjv4bxcqbfmzcrymamwauxcuydtksayhpovebpvmdllxgxsu5vx8wzkj
hiwazhg5m&utm_campaign=email&utm_source=sendgrid.com&utm_medium=email has
```

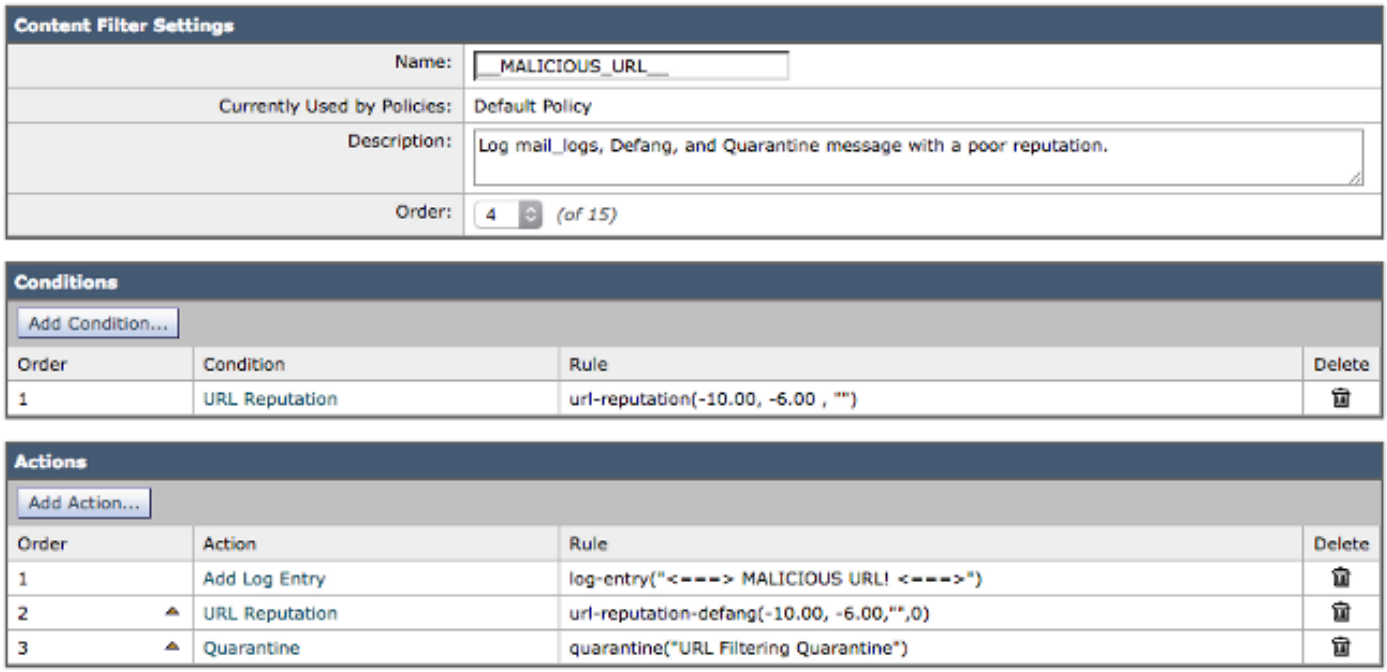
```
reputation -5.08 matched url-reputation-rule
Wed Nov 5 21:22:24 2014 Info: MID 185 Custom Log Entry: <===> SUSPECT URL! <===>
Wed Nov 5 21:22:24 2014 Info: MID 185 Outbreak Filters: verdict negative
Wed Nov 5 21:22:24 2014 Info: MID 185 queued for delivery
Wed Nov 5 21:22:24 2014 Info: New SMTP DCID 26 interface 192.168.0.199 address
192.168.0.200 port 25
Wed Nov 5 21:22:24 2014 Info: Delivery start DCID 26 MID 185 to RID [0]
Wed Nov 5 21:22:24 2014 Info: Message done DCID 26 MID 185 to RID [0]
[('X-IronPort-AV', 'E=Sophos;i="5.07,323,1413259200"; \r\n d="scan\'208,217";a="185"'),
('x-ironport-av', 'E=Sophos;i="5.07,323,1413244800"; \r\n d="scan\
'208,217";a="93843786"')]
Wed Nov 5 21:22:24 2014 Info: MID 185 RID [0] Response '2.0.0 Ok: queued as 0F8F9801C2'
Wed Nov 5 21:22:24 2014 Info: Message finished MID 185 done
```

> Nota: A URL que é encaixada no exemplo anterior tem-no os espaços extras incluídos no corpo URL, assim que não tropeça nenhuma varreduras da Web ou detecção do proxy.

O link de Udemy no exemplo anterior não parece limpo, e é **SUSPEITO** marcado - em **5.08**. Segundo as indicações da entrada de logs do correio, esta mensagem é permitida ser entregada ao utilizador final.

Filtros satisfeitos para URL maliciosas

Este exemplo mostra uma varredura para URL maliciosas com a aplicação deste filtro satisfeito de entrada:



Com este filtro no lugar, as varreduras do sistema para uma URL com uma reputação *maliciosa* (-10.00 -6.00), adicionam uma entrada de registro aos logs do correio, usam a ação do *defang* a fim fazer o link unclickable, e colocam esta em uma quarentena da Filtragem URL. Está aqui um exemplo dos logs do correio:

```
Wed Nov 5 21:27:18 2014 Info: Start MID 186 ICID 606
Wed Nov 5 21:27:18 2014 Info: MID 186 ICID 606 From: <bad_user@that.domain.net>
Wed Nov 5 21:27:18 2014 Info: MID 186 ICID 606 RID 0 To: <joe.user@goodmailguys.com>
Wed Nov 5 21:27:18 2014 Info: MID 186 Message-ID
'<COL128-W95DE5520A96FD9D69FAC2D9D840@phx.gbl>'
```

```
Wed Nov 5 21:27:18 2014 Info: MID 186 Subject 'URL Filter test malicious'
Wed Nov 5 21:27:18 2014 Info: MID 186 ready 2230 bytes from
<bad_user@that.domain.net>
Wed Nov 5 21:27:18 2014 Info: MID 186 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Wed Nov 5 21:27:18 2014 Info: ICID 606 close
Wed Nov 5 21:27:19 2014 Info: MID 186 interim verdict using engine: CASE spam positive
Wed Nov 5 21:27:19 2014 Info: MID 186 using engine: CASE spam positive
Wed Nov 5 21:27:19 2014 Info: ISQ: Tagging MID 186 for quarantine
Wed Nov 5 21:27:19 2014 Info: MID 186 interim AV verdict using Sophos CLEAN
Wed Nov 5 21:27:19 2014 Info: MID 186 antivirus negative
Wed Nov 5 21:27:19 2014 Info: MID 186 URL http:// peekquick .com /sdeu/cr.sedin/sdac/
denc.php has reputation -6.77 matched url-reputation-rule
Wed Nov 5 21:27:19 2014 Info: MID 186 Custom Log Entry: <===> MALICIOUS URL! <===>
Wed Nov 5 21:27:19 2014 Info: MID 186 URL http:// peekquick .com/sdeu/cr.sedin/sdac/
denc.php has reputation -6.77 matched url-reputation-defang-action
Wed Nov 5 21:27:19 2014 Info: MID 186 URL http:// peekquick .com /sdeu/cr.sedin/sdac/
denc.php has reputation -6.77 matched url-reputation-defang-action
Wed Nov 5 21:27:19 2014 Info: MID 186 rewritten to MID 187 by
url-reputation-defang-action filter '__MALICIOUS_URL__'
Wed Nov 5 21:27:19 2014 Info: Message finished MID 186 done
Wed Nov 5 21:27:19 2014 Info: MID 187 Outbreak Filters: verdict positive
Wed Nov 5 21:27:19 2014 Info: MID 187 Threat Level=5 Category=Phish Type=Phish
Wed Nov 5 21:27:19 2014 Info: MID 187 rewritten URL u'http:// peekquick .com
/sdeu/cr.sedin/sdac/denc.php-Robert'
Wed Nov 5 21:27:19 2014 Info: MID 187 rewritten to MID 188 by url-threat-protection
filter 'Threat Protection'
Wed Nov 5 21:27:19 2014 Info: Message finished MID 187 done
Wed Nov 5 21:27:19 2014 Info: MID 188 Virus Threat Level=5
Wed Nov 5 21:27:19 2014 Info: MID 188 quarantined to "Outbreak"
(Outbreak rule:Phish: Phish)
Wed Nov 5 21:27:19 2014 Info: MID 188 quarantined to "URL Filtering Quarantine"
(content filter:__MALICIOUS_URL__)
Wed Nov 5 21:28:20 2014 Info: SDS_CLIENT: Generated URL scanner configuration
Wed Nov 5 21:28:21 2014 Info: SDS_CLIENT: URL scanner enabled=1
Wed Nov 5 21:28:21 2014 Info: SDS_CLIENT: Generated URL scanner configuration
Wed Nov 5 21:28:21 2014 Info: SDS_CLIENT: URL scanner enabled=1
```

> Nota: A URL que é encaixada no exemplo anterior tem-no os espaços extras incluídos no corpo URL, assim que não tropeça nenhuma varreduras da Web ou detecção do proxy.

Esta URL para peekquick.com é MALICIOSA e marcada em uns -6.77. Uma entrada é feita nos logs do correio, onde você pode ver todos os processos na ação. O filtro URL detectou a URL maliciosa, defanged, e quarantined a. O VOF igualmente marcar-lo positivo baseado em seu grupo da regra, e desde que detalhes que este era um Phish relacionado.

Se VOF não é permitido, a mesma mensagem está processada completamente, mas as varreduras URL não são atuadas em cima sem da capacidade adicionada de VOF para conduzir varreduras e ação. Contudo, neste exemplo o corpo da mensagem é feito a varredura pelo motor do Anti-Spam de Cisco (CASO) e julgado como Spam-positivo:

```
Wed Nov 5 21:40:49 2014 Info: Start MID 194 ICID 612
Wed Nov 5 21:40:49 2014 Info: MID 194 ICID 612 From: <bad_user@that.domain.net>
Wed Nov 5 21:40:49 2014 Info: MID 194 ICID 612 RID 0 To: <joe.user@goodmailguys.com>
Wed Nov 5 21:40:49 2014 Info: MID 194 Message-ID
'<COL128-W145FD8B772C824CEF33F859D840@phx.gbl>'
Wed Nov 5 21:40:49 2014 Info: MID 194 Subject 'URL Filter test malicious'
Wed Nov 5 21:40:49 2014 Info: MID 194 ready 2230 bytes from <bad_user@that.domain.net>
Wed Nov 5 21:40:49 2014 Info: MID 194 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Wed Nov 5 21:40:50 2014 Info: ICID 612 close
```

```
Wed Nov 5 21:40:50 2014 Info: MID 194 interim verdict using engine: CASE spam positive
Wed Nov 5 21:40:50 2014 Info: MID 194 using engine: CASE spam positive
Wed Nov 5 21:40:50 2014 Info: ISQ: Tagging MID 194 for quarantine
Wed Nov 5 21:40:50 2014 Info: MID 194 interim AV verdict using Sophos CLEAN
Wed Nov 5 21:40:50 2014 Info: MID 194 antivirus negative
Wed Nov 5 21:40:50 2014 Info: MID 194 queued for delivery
Wed Nov 5 21:40:52 2014 Info: RPC Delivery start RCID 20 MID 194 to local IronPort
Spam Quarantine
Wed Nov 5 21:40:52 2014 Info: ISQ: Quarantined MID 194
Wed Nov 5 21:40:52 2014 Info: RPC Message done RCID 20 MID 194
Wed Nov 5 21:40:52 2014 Info: Message finished MID 194 done
```

Esta detecção através do CASO apenas não ocorre sempre. Há as épocas em que as regras do CASO e IPA puderam conter esse fósforo contra um determinados remetente, domínio, ou conteúdos de mensagem a fim detectar esta ameaça apenas.

Relate URL Uncategorized e Misclassified

Às vezes, uma URL não pôde ser classificada ainda, ou pôde ser miscategorized. A fim relatar as URL que miscategorized, e as URL que não são categorizadas mas devem ser, visite a página dos pedidos da categorização de Cisco URL.

Você pôde igualmente desejar verificar o estado de URL submetidas. A fim fazer isto, clique o **estado na** aba submetida URL desta página.

As URL maliciosas e as mensagens do mercado não são travadas por filtros do Anti-Spam ou da manifestação

Isto pode ocorrer porque a reputação e a categoria do site são somente dois critérios entre muitos que os filtros do anti-Spam e da manifestação usam a fim determinar suas sentenças. A fim aumentar a sensibilidade destes filtros, abaixe os pontos iniciais que são exigidos para tomar a ação, tal como a reescrita ou URL da substituição com texto, ou mensagens quarantining ou deixando cair.

Alternativamente, você pode criar o índice ou os filtros da mensagem baseados na reputação URL marcam.

Informações Relacionadas

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