Activation et pratiques recommandées de Filtrage URL ESA

Contenu

Introduction

Ce document décrit comment activer le Filtrage URL sur l'appliance de sécurité du courrier électronique de Cisco (ESA) et les pratiques recommandées pour son usage.

Informations générales

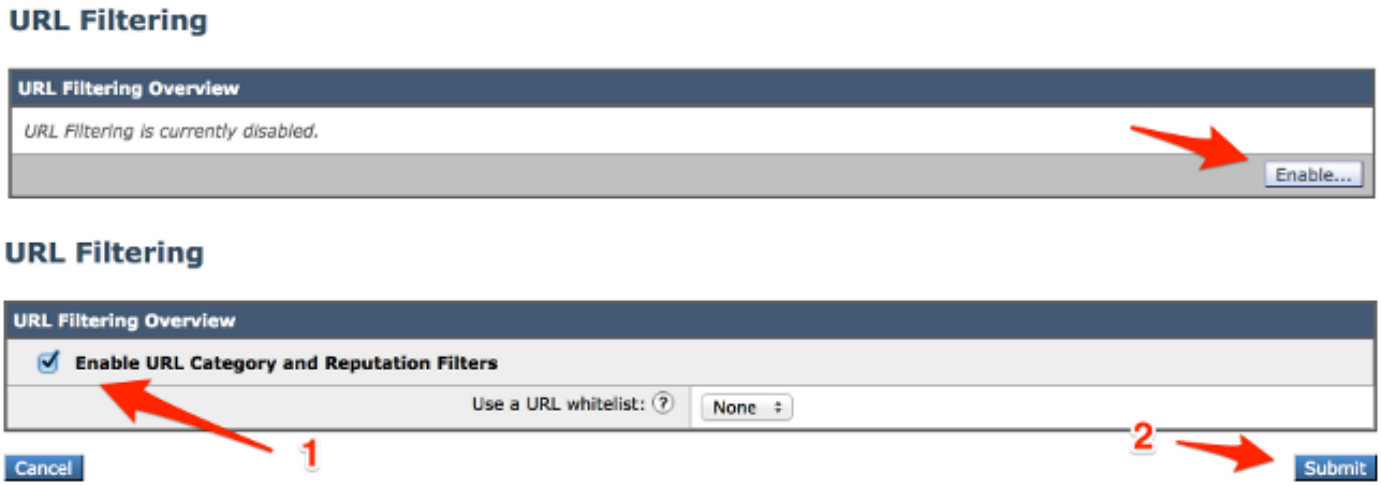
Quand vous activez le Filtrage URL sur l'ESA, vous devez également activer d'autres caractéristiques, dépendantes sur votre fonctionnalité désirée. Voici quelques caractéristiques typiques qui sont activées à côté du Filtrage URL :

- Pour la protection améliorée contre le Spam, la caractéristique de lecture d'anti-Spam doit être activée globalement selon la stratégie applicable de messagerie. Ceci peut être l'anti-Spam d'IronPort Cisco (IPAS) ou la caractéristique intelligente du Multi-balayage de Cisco (IMS).
- Pour la protection améliorée contre le malware, la caractéristique de filtres d'épidémie ou de filtres d'attaque de virus (VOF) doit être activée globalement selon la stratégie applicable de messagerie.
- Pour des actions basées sur la réputation URL, ou afin d'imposer des politiques d'utilisation acceptable avec l'utilisation des filtres de message et de contenu, vous devez activer VOF globalement.

Activer le filtrage URL

Afin d'implémenter le Filtrage URL sur l'ESA, vous devez d'abord activer la caractéristique. Il y a deux différentes méthodes que vous pouvez employer afin d'activer cette caractéristique : Avec l'utilisation du GUI ou du CLI.

Afin d'activer le Filtrage URL avec l'utilisation du GUI, naviguez vers des **Services de sécurité > le Filtrage URL > l'enable :**



Afin d'activer le Filtrage URL avec l'utilisation du CLI, sélectionnez la commande de **websecurityconfig** :

```
myesa.local> websecurityconfig
Enable URL Filtering? [N]> y
```

Il est important de noter que vous devez également activer l'URL se connectant du VOF. C'est à caractéristique CLI réservée qui doit être activée comme affiché ici :

```
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.`

> Remarque: Assurez-vous que vous **commettez** *l'intégralité de* modifications à votre configuration avant que vous procédiez à partir du GUI ou du CLI sur votre ESA.

Créez les actions de Filtrage URL

Quand vous activez seul le Filtrage URL, il n'agit pas contre les messages qui pourraient contenir vivant et des URL valides.

L'URLs inclus dans les messages d'arrivée et sortants (avec l'exclusion des connexions) sont évalués. N'importe quelle chaîne valide pour un URL est évaluée, pour inclure des chaînes avec ces composants :

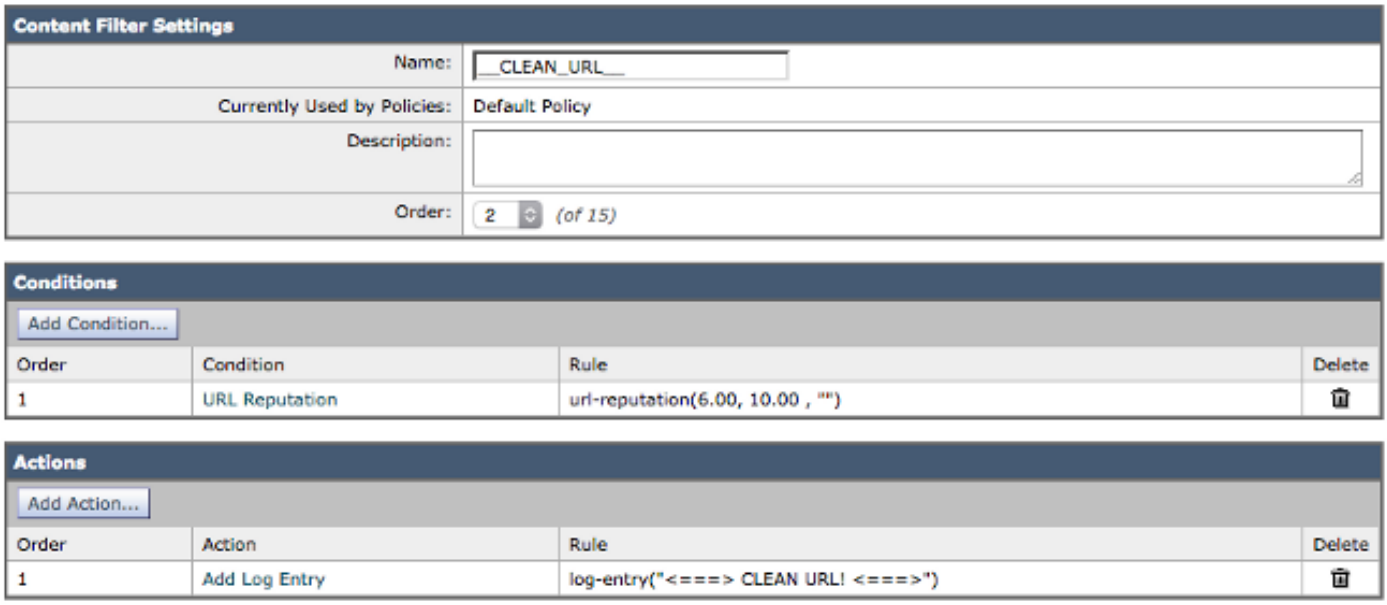
- HTTP, HTTPS, ou WWW
- Domaine ou adresses IP
- Numéros de port précédés par des deux points (:)
- Lettres majuscules ou minuscules

Quand le système évalue l'URLs afin de déterminer si un message est Spam, s'il y a lieu pour la Gestion de chargement, il donne la priorité et examine aux messages d'arrivée au-dessus des messages sortants.

Afin de balayer rapidement l'URLs et agir, vous pouvez créer un filtre satisfait de sorte que *si le* message a un URL valide, *alors l'*action est appliquée. Du GUI, naviguez **pour envoyer par mail des stratégies > les filtres satisfaits entrants > ajoutent le filtre**.

Filtres satisfaits pour l'URLs propre

Cet exemple affiche un balayage pour l'URLs propre avec l'implémentation de ce filtre satisfait d'arrivée :



Avec ce filtre en place, le système recherche un URL avec une réputation *propre* (6.00 10.00) et ajoute simplement une entrée de journal à la commande de logins de messagerie pour déclencher et enregistrer le score basé sur le WEB de réputation (WBRS). Cette entrée de journal aide

également à identifier le processus qui est déclenché. Voici un exemple des logs de messagerie :

```
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
```

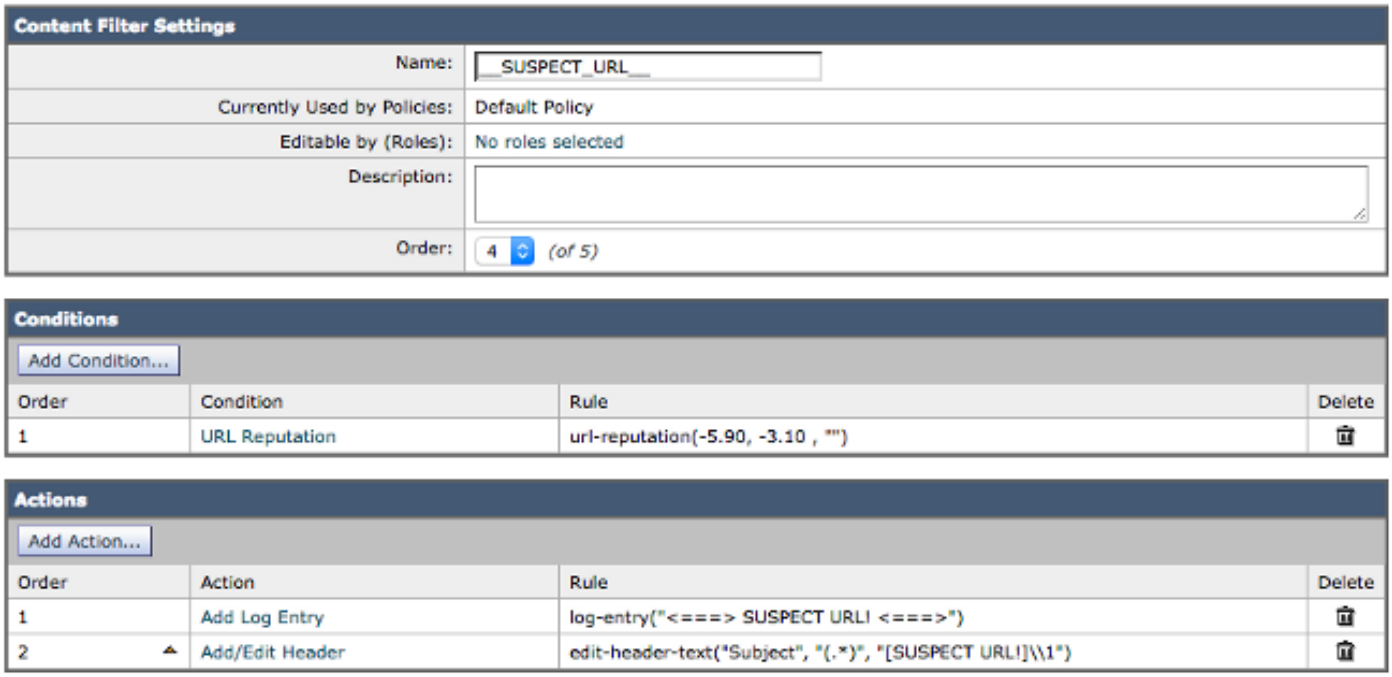
> Remarque: L'URL qui est encastré dans l'exemple précédent a les espaces supplémentaires inclus dans le corps URL, ainsi lui ne se déclenche pas n'importe quels balayages de Web ou détection de proxy.

Suivant les indications de l'exemple, **Yahoo.com** est considéré **PROPRE** et donné une vingtaine de **8.39**, est noté dans les logs de messagerie, et est livré à l'utilisateur final.

Filtres satisfaits pour l'URLs neutre ou suspect

> Remarque: Dans AsyncOS 9.7 pour la sécurité du courrier électronique et plus tard, l'URLs qui ont été autrefois étiquetés « méfiants » sont maintenant étiquetés « point mort. » Seulement l'écriture de labels a changé ; la logique sous-jacente et le traitement n'ont pas changé.

Cet exemple affiche un balayage pour neutre/suspect URLs avec l'implémentation de ce filtre satisfait d'arrivée :



Content Filter Settings

Name:	__SUSPECT_URL__
Currently Used by Policies:	Default Policy
Editable by (Roles):	No roles selected
Description:	
Order:	4 (of 5)

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-5.90, -3.10 , "")	

Actions

Add Action...

Order	Action	Rule	Delete
1	Add Log Entry	log-entry("<===> SUSPECT URL! <===>")	
2	Add/Edit Header	edit-header-text("Subject", "(.*)", "[SUSPECT URL!]\\1")	

Avec ce filtre en place, le système recherche un URL avec un *point mort*, ou le *suspect*, la réputation (-5.90 -3.1) et ajoute une entrée de journal aux logs de messagerie. Cet exemple affiche qu'un sujet modifié ajoutait au début **« [l'URL SUSPECT !] »**. Voici un exemple des logs de messagerie :

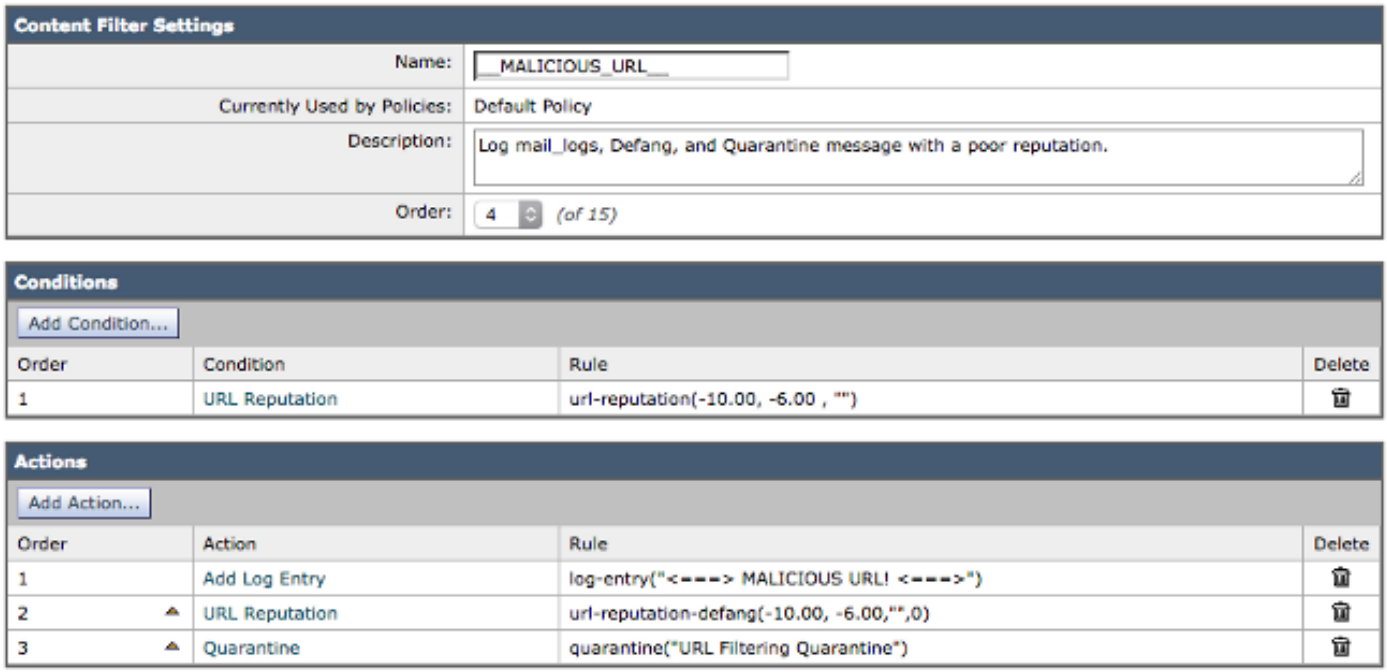
```
Wed Nov 5 21:22:23 2014 Info: Start MID 185 ICID 605
Wed Nov 5 21:22:23 2014 Info: MID 185 ICID 605 From: <bad_user@that.domain.net>
Wed Nov 5 21:22:23 2014 Info: MID 185 ICID 605 RID 0 To: <joe.user@goodmailguys.com>
Wed Nov 5 21:22:23 2014 Info: MID 185 Message-ID
'<D0804586.24BAE%bad_user@that.domain.net>'
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
```

> Remarque: L'URL qui est encastré dans l'exemple précédent a les espaces supplémentaires inclus dans le corps URL, ainsi lui ne se déclenche pas n'importe quels balayages de Web ou détection de proxy.

Le lien d'Udemy dans l'exemple précédent ne semble pas propre, et c'est **SUSPECT** marqué - à **5.08**. Suivant les indications de l'entrée de logs de messagerie, on permet à ce message pour être fourni à l'utilisateur final.

Filtres satisfaits pour l'URLs malveillant

Cet exemple affiche un balayage pour l'URLs malveillant avec l'implémentation de ce filtre satisfait d'arrivée :



Avec ce filtre en place, les balayages de système pour un URL avec une réputation *malveillante* (-10.00 -6.00), ajoute une entrée de journal aux logs de messagerie, emploie l'action de *defang* afin de rendre le lien unclickable, et place ceci dans une quarantaine de Filtrage URL. Voici un exemple des logs de messagerie :

```
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
```

> Remarque: L'URL qui est encastré dans l'exemple précédent a les espaces supplémentaires inclus dans le corps URL, ainsi lui ne se déclenche pas n'importe quels balayages de Web ou détection de proxy.

Cet URL pour peekquick.com est MALVEILLANT et marqué à des -6.77. Une entrée est faite dans les logs de messagerie, où vous pouvez voir tous les processus dans l'action. Le filtre URL a détecté l'URL malveillant, defanged, et l'a mis en quarantaine. Le VOF l'a également marqué positif basé sur son ensemble de règles, et si des détails que c'était un Phish relatif.

Si VOF n'est pas activé, le même message est traité, mais des balayages URL ne sont pas agis au moment sans capacité ajoutée de VOF de piloter des balayages et l'action. Cependant, dans cet exemple le corps du message est balayé par l'engine d'anti-Spam de Cisco (CAS) et considéré en tant que Spam-positif :

```
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
```

Cette détection par l'intermédiaire seul de CAS ne se produit pas toujours. Il y a des périodes où les règles de CAS et IPAS pourraient contenir cette correspondance contre un certains expéditeur, domaine, ou contenus du message afin de détecter cette seule menace.

URLs Uncategorized et mauvais d'état

Parfois, un URL ne pourrait pas être classifié encore, ou il pourrait miscategorized. Afin de signaler l'URLs qui miscategorized, et l'URLs qui ne sont pas classés mais devraient par catégorie être, visitez la page de demandes de catégorisation URL de Cisco.

Vous pourriez également désirer vérifier l'état de l'URLs soumis. Afin de faire ceci, cliquez sur l'**état** sur l'onglet soumis URLs de cette page.

L'URLs malveillant et les messages commerciaux ne sont pas attrapés par des filtres d'anti-Spam ou d'épidémie

Ceci peut se produire parce que la réputation et la catégorie de site Web sont seulement deux critères parmi beaucoup que les filtres d'anti-Spam et d'épidémie emploient afin de déterminer leurs verdicts. Afin d'augmenter la sensibilité de ces filtres, diminuez les seuils qui sont exigés pour agir, tel que la réécriture ou remplacer l'URLs par le texte, ou mettre en quarantaine ou les messages de baisse.

Alternativement, vous pouvez créer des filtres de contenu ou de message basés sur le score de réputation URL.

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems