Включение фильтрации URL-адресов ESA и оптимальные методы

Содержание

Введение

Этот документ описывает, как включить Фильтрацию URL-адресов на Cisco Email Security Appliance (ESA) и оптимальные методы для его использования.

Общие сведения

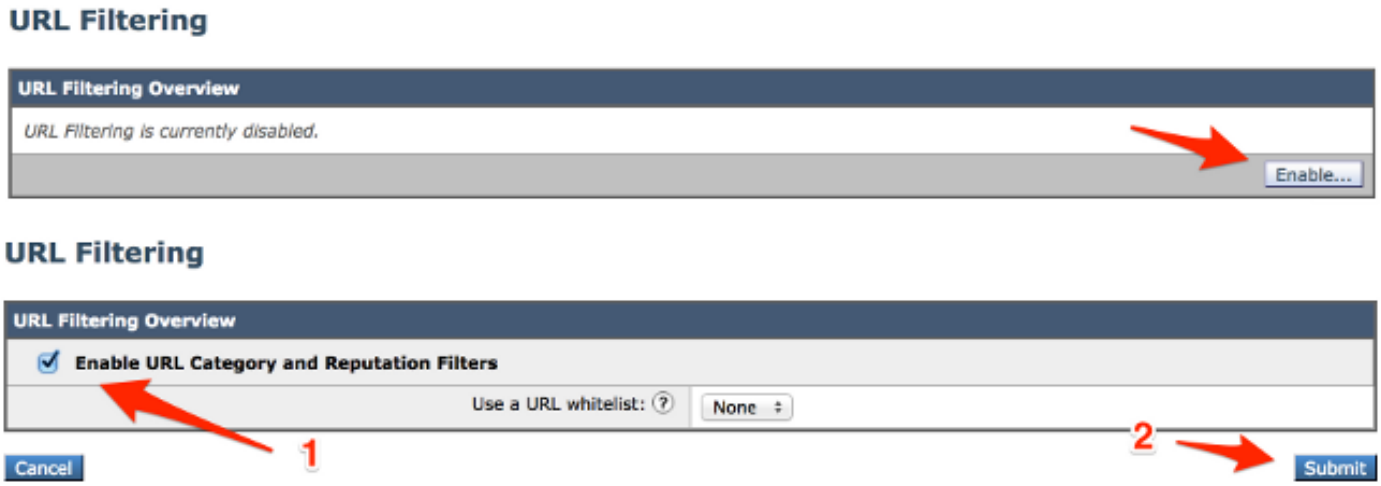
При включении Фильтрации URL-адресов на ESA необходимо также активировать другие опции, зависящие от желаемой функциональности. Вот некоторые типичные опции, которые активированы вместе с Фильтрацией URL-адресов:

- Для улучшенной защиты против спама опция Сканирования Защиты от спама должна быть активирована глобально в соответствии с применимой почтовой политикой. Это может быть или Защитой от спама Cisco IronPort (IPBы) или функцией Интеллектуального мультипросмотра (IMS) Cisco.
- Для улучшенной защиты против вредоносного ПО Фильтры Вспышки или функция Фильтров вспышки вируса (VOF) должны быть включены глобально в соответствии с применимой почтовой политикой.
- Для действий на основе репутации URL, или для осуществления политики допустимого использования с использованием сообщения и фильтров контента, необходимо включить VOF глобально.

Включение фильтрации URL-адресов

Для реализации Фильтрации URL-адресов на ESA необходимо сначала активировать опцию. Существует два других метода, которые можно использовать для активации этой опции: С использованием или GUI или CLI.

Для включения Фильтрации URL-адресов с использованием GUI перейдите к **Сервисам безопасности>, Фильтрация URL-адресов> Включает:**



Для включения Фильтрации URL-адресов с использованием CLI введите **websecurityconfig** команду:

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

Следует отметить, что необходимо также включить Регистрацию URL из VOF. Это - опция только для CLI, которая должна быть активирована как показано здесь:

```
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.

> **Примечание:** Гарантируйте **передачу** *любого* и *всех* изменений к конфигурации перед переходом или из GUI или из CLI на ESA.

Создайте действия фильтрации URL-адресов

При включении одной только фильтрации URL-адресов она не принимает меры против сообщений, которые могли бы содержать оперативные и допустимые URL.

URL, включенные во входящие и исходящие сообщения (с исключением прикреплений), оценены. Любая допустимая строка для URL оценена, для включения строк с этими компонентами:

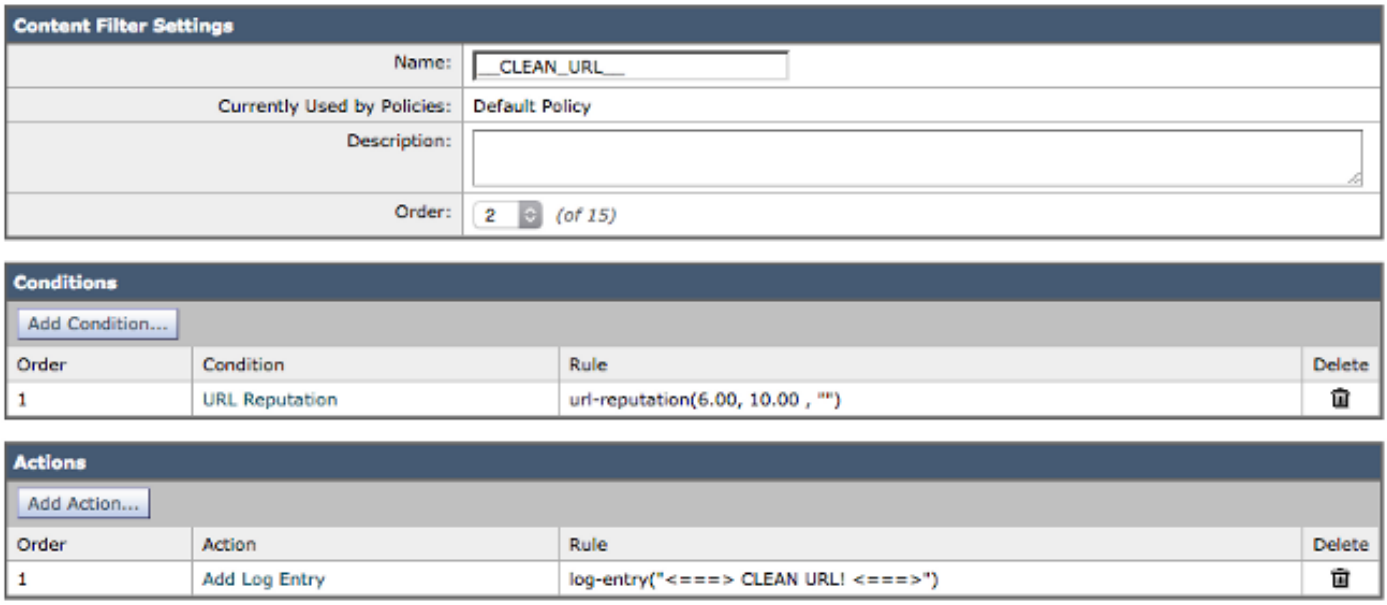
- HTTP, HTTPS или WWW
- Домен или IP-адреса
- Номера портов, которым предшествует двоеточие (:)
- Буквы в верхнем регистре или символы в нижнем регистре

Когда система оценивает URL, чтобы определить, является ли сообщение спамом, при необходимости для управления загрузки, это располагает по приоритетам и экранирует входящие сообщения по исходящим сообщениям.

Чтобы быстро просмотреть URL и принять меры, можно создать фильтр контента так, чтобы, *если* сообщение имеет допустимый URL, *то* действие применено. От GUI перейдите для **Отправки по почте Политики> Поступающий, Фильтры контента> Добавляют Фильтр**.

Фильтры контента для чистых URL

Данный пример показывает просмотр для чистых URL с реализацией этого входящего фильтра контента:



С этим фильтром на месте, система ищет URL с *чистой* репутацией (6.00 к 10.00) и просто добавляет запись журнала к почтовым журналам, чтобы инициировать и сделать запись Веб-счета репутации (WBRS). Эта запись журнала также помогает определять процесс,

который инициирован. Вот пример от почтовых журналов:

```
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
```

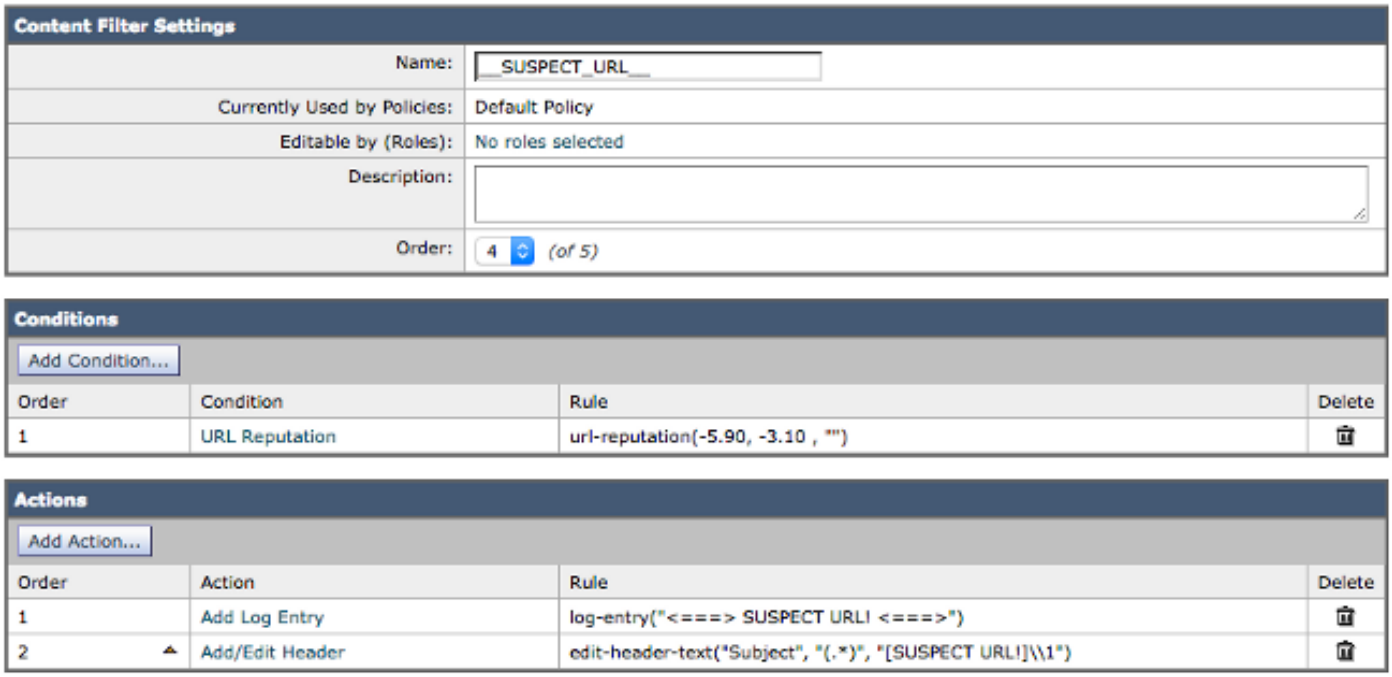
> **Примечание:** URL, который встроен в предыдущий пример, включали дополнительные пробелы в тело URL, таким образом, это не смещается никакие веб-просмотры или проксирует обнаружение.

Как показано в примере, **Yahoo.com** считают **CLEAN** и дают счет **8.39**, обращают внимание в почтовых журналах и отправляют конечному пользователю.

Фильтры контента для нейтрального или подозрительных URL

> **Примечание:** В AsyncOS 9.7 для Безопасности электронной почты и позже, URL, которые были раньше маркированы “Подозрительными”, теперь маркированы “Нейтральными” . Только маркировка изменилась; базовая логика и обработка не изменились.

Данный пример показывает просмотр для нейтральных URL / подозрительных URL с реализацией этого входящего фильтра контента:



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")	

С этим фильтром на месте, система ищет URL с *Нейтральным*, или *Подозреваемый*, репутация (-5.90 к-3.1) и добавляет запись журнала к почтовым журналам. Данный пример показывает модифицированный предмет для подготовки**" [URL SUSPECT!]"**. Вот пример от почтовых журналов:

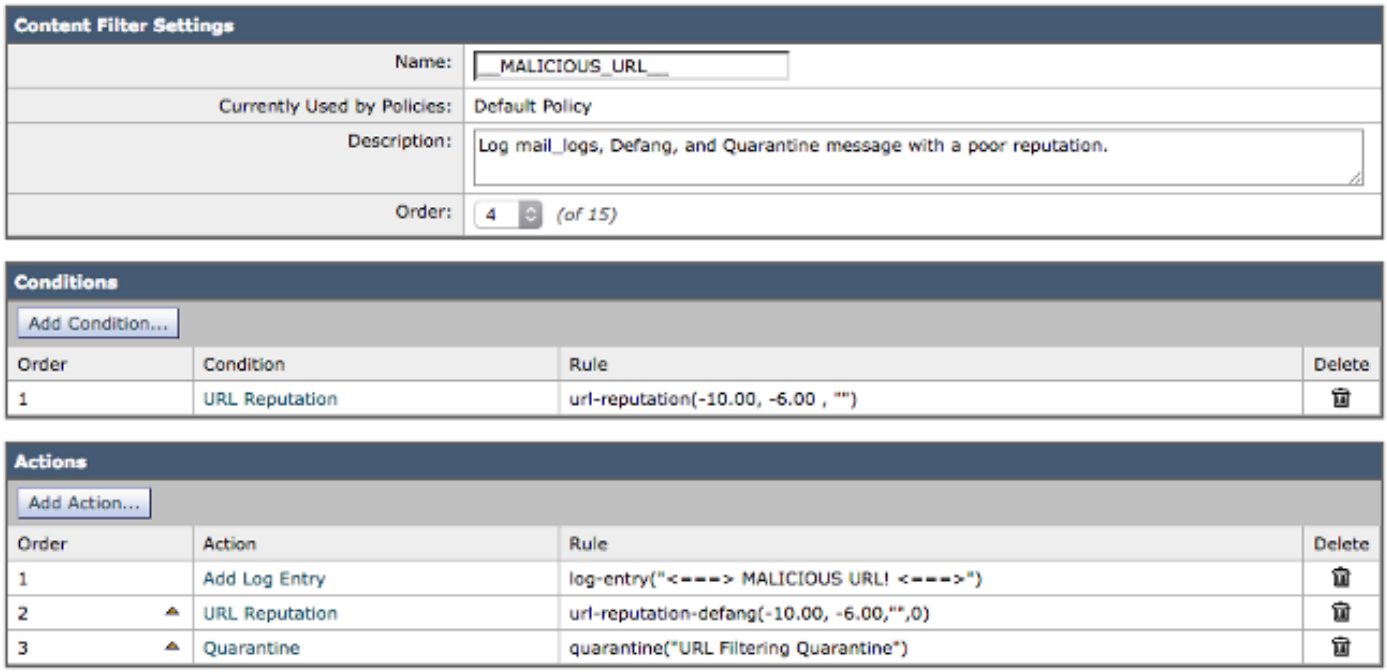
```
Wed Nov 5 21:22:23 2014 Info: Start MID 185 ICID 605
Wed Nov 5 21:22:23 2014 Info: MID 185 ICID 605 From: <bad_user@that.domain.net>
Wed Nov 5 21:22:23 2014 Info: MID 185 ICID 605 RID 0 To: <joe.user@goodmailguys.com>
Wed Nov 5 21:22:23 2014 Info: MID 185 Message-ID
'<D0804586.24BAE%bad_user@that.domain.net>'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

Примечание: URL, который встроен в предыдущий пример, включали дополнительные пробелы в тело URL, таким образом, это не смещается никакие веб-просмотры или проксирует обнаружение.

Ссылка Udemy в предыдущем примере не кажется чистой, и это - выигранный SUSPECT в-5.08. Как показано в почтовой записи журналов, этому сообщению позволяют быть переданным конечному пользователю.

Фильтры контента для злонамеренных URL

Данный пример показывает просмотр для злонамеренных URL с реализацией этого входящего фильтра контента:



Content Filter Settings

Name:	__MALICIOUS_URL__
Currently Used by Policies:	Default Policy
Description:	Log mail_logs, Defang, and Quarantine message with a poor reputation.
Order:	4 (of 15)

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-10.00, -6.00 , "")	

Actions

Add Action...

Order	Action	Rule	Delete
1	Add Log Entry	log-entry("<===> MALICIOUS URL! <===>")	
2	URL Reputation	url-reputation-defang(-10.00, -6.00,"",0)	
3	Quarantine	quarantine("URL Filtering Quarantine")	

С этим фильтром на месте, системными просмотрами для URL со *Злонамеренной* репутацией (-10.00 к-6.00), добавляет запись журнала к почтовым журналам, использует *defang* действие, чтобы сделать ссылку неактивируемой по щелчку, и размещает это в карантин Фильтрации URL-адресов. Вот пример от почтовых журналов:

```
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
```

> **Примечание:** URL, который встроен в предыдущий пример, включали дополнительные пробелы в тело URL, таким образом, это не смещается никакие веб-просмотры или проксирует обнаружение.

Этим URL для **peekquick.com** является **MALICIOUS** и выигранный в**-6.77**. Запись сделана в почтовых журналах, где вы видите все процессы в действии. Фильтр URL обнаружил злонамеренный URL, defanged, и изолировал его. VOF также выиграл его положительный на основе его набора правила и предоставил подробную информацию, что это был связанный Фиш.

Если VOF не включен, то же сообщение обработано через, но на просмотры URL не реагируют без добавленной способности VOF вести просмотры и действие. Однако в данном примере тело сообщения просматривает Механизм защиты от спама Cisco (CASE) и считают как положительное спаму:

```
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
```

Это обнаружение через один только CASE не всегда происходит. Существуют времена, когда CASE и правила IPBop могли бы содержать то соответствие против определенного отправителя, домена или содержаний сообщения для обнаружения одной только этой угрозы.

Сообщите о некатегоризированных и неправильно классифицированных URL

Время от времени URL еще не мог бы быть классифицирован, или это мог бы быть miscategorized. Для создания отчетов о URL, которые были miscategorized, и URL, которые не категоризированы, но должны быть, посетить классификацию URL Cisco, запрашивают страницу.

Вы могли бы также желать проверить статус отправленных URL. Чтобы сделать это, нажмите **Status** на вкладке Submitted URLs этой страницы.

Злонамеренные URL и торгующие сообщения не пойманы фильтрами защиты от спама или вспышки

Это может произойти, потому что репутация веб-сайта и категория являются только двумя критериями среди многих, что защита от спама и вспышка фильтруют использование для определения их вердиктов. Для увеличения чувствительности этих фильтров понизьте пороги, которые обязаны принимать меры, такие как перезапись или замена URL с текстом, или изоляции или отбрасывания сообщений.

Также можно создать содержание или передать фильтры на основе счета репутации URL.

Дополнительные сведения

- Устройство безопасности электронной почты Cisco - руководства пользователя
- Cisco Systems – техническая поддержка и документация