Содержание

Введение

Этот документ описывает и отвечает на некоторые из большего количества часто задаваемых вопросов относительно Фильтров Вспышки или Фильтров Вспышки Вируса, на Email Security Appliance (ESA).

Что такое Фильтры Вспышки или Фильтры вспышки вируса (VOF)?

Фильтры вспышки защищают вашу сеть от крупномасштабных вспышек вируса и меньших, невирусных атак, таких как жульничества фишинга и вредоносное распределение, как они происходят. В отличие от большей части защитного программного обеспечения антивируса, которое не может обнаружить новые вспышки, пока не собраны данные, и обновление ПО публиковано, Cisco собирает материал о вспышках, поскольку они распространяются, и передает обновленные данные к вашему ESA в режиме реального времени, чтобы препятствовать тому, чтобы эти сообщения достигли ваших пользователей.

Cisco использует образцы глобального трафика для разработки правил, которые определяют, безопасно ли входящее сообщение или часть вспышки. Сообщения, которые могут быть частью вспышки, изолированы, пока они не полны решимости быть безопасными на основе обновленной информации о вспышке от Cisco, или новые антивирусные определения публикованы Sophos и McAfee.

Сообщения, используемые в небольших, невирусных атаках, используют легитимно выглядящий дизайн, информацию получателя и пользовательские URL, которые указывают к фишингу и вредоносным веб-сайтам, которые были онлайн только для короткого периода времени и неизвестны веб-сервисам безопасности. Фильтры вспышки анализируют содержание сообщения и ищут ссылки URL для обнаружения этого типа невирусной атаки. Фильтры вспышки могут переписать URL для перенаправления трафика к потенциально вредным веб-сайтам через веб-прокси безопасности, который или предупреждает

пользователей, что веб-сайт, к которому они пытаются обратиться, может быть злонамеренным или блокирует веб-сайт полностью.

Даже если я не выполняю Sophos или McAfee Anti-Virus на моем ESA, я могу использовать Фильтры Вспышки?

Cisco рекомендует позволить Sophos или McAfee Anti-Virus в дополнение к Фильтрам Вспышки Вируса увеличить защиту против вирусов. Однако VOF может работать независимо, не требуя, чтобы были включены Sophos или McAfee Anti-Virus.

Когда Фильтры Вспышки изолируют сообщения?

Сообщение изолировано, когда оно содержит вложенный файл (файлы), которые встречают или превышают текущие Правила Вспышки и пороги, установленные почтовыми администраторами. Cisco публикует текущие Правила Вспышки в каждом ESA , который имеет допустимую характерную черту, и на нашем Портале поддержки.

Информация о текущих вспышках вируса может быть найдена на SenderBase

Cisco Security Разведывательные операции (SIO) веб-сайт предоставляет список текущих невирусных угроз, включая спам, фишинг и вредоносные попытки распределения.

Когда карантин Вспышки заполняется, что происходит?

Когда карантин превышает максимальное место, выделенное к нему, или если сообщение превышает значение максимального времени, сообщения автоматически сокращены от карантина для хранения его в определенных рамках. Сообщения удалены на первым прибыл, первым обслужен (FIFO) основание. Другими словами, самые старые сообщения удалены сначала. Можно настроить карантин к любому выпуску (т.е. поставить), или удалите сообщение, которое должно быть сокращено от карантина. Если вы выбираете к сообщениям RELEASE, можно выбрать помечать строку темы с текстом, который вы задаете, который предупредит получателя, что сообщение было вызвано из карантина.

Следующий выпуск от карантина Вспышки, сообщения повторно просмотрены антивирусным модулем, и меры приняты согласно антивирусной политике. В зависимости от этой политики сообщение может быть передано, удалено или отправлено с вирусными разделенными прикреплениями. Ожидается, что вирусы будут часто находиться во время перепросмотра после выпуска от карантина Вспышки. С ESA mail_logs или отслеживание сообщений можно консультироваться, чтобы определить, как ли отдельное сообщение, на которое обратили внимание в карантине, находили, было вирусным, и если и как это было отправлено.

Прежде чем системный карантин заполняется, предупреждение передается, когда карантин достигает полных 75%, и другое предупреждение передается, когда это достигает полных

95%. Карантин Вспышки имеет дополнительную функцию управления, которая позволяет вам удалять или освобождать все сообщения, которые совпадают с определенным уровнем угрозы вируса (VTL). Это обеспечивает легкую очистку карантина после того, как обновление антивируса получено, который обращается к определенной угрозе вируса.

Каково значение уровня угрозы для Правила Вспышки?

Фильтры вспышки действуют под уровнями угрозы между 0 и 5. Уровень угрозы оценивает вероятность вирусной вспышки. На основе риска вирусной вспышки уровень угрозы влияет на изоляцию подозрительных файлов. Уровень угрозы основывается на многих факторах, включая, но не ограничиваясь, сетевым трафиком, подозрительным действием файла, вводом от антивирусных поставщиков и анализом Центром Операции Угрозы Cisco. Кроме того, Фильтры Вспышки позволяет почтовым администраторам увеличивать или уменьшать влияние уровней угрозы для их сетей.

Уровень	Риск	Значение
0	Нет	Нет никакого риска, что сообщение является
1	Низкий	Риск, что сообщение является
2	Низкая - средняя	Риск, что сообщение является
3	Средний	Или сообщение является частью подтвержденной вспышки или существует средний и крупный риск ее содержания, являющегося
4	Высокий	Или сообщение подтверждено, чтобы быть частью широкомасштабной вспышки или ее содержания, очень опасно.
5	Экстремальное значение	Сообщение? s содержание подтвержден к части вспышки, которая является или чрезвычайно крупным масштабом или широкомасштабный и чрезвычайно опасный.

Когда вспышка вируса происходит, как я могу быть предупрежден?

Когда сеть SenderBase поднимает VTL для определенного типа профиля сообщения, вы можете быть предупреждены с помощью сообщения электронной почты, передаваемого вашему настроенному аварийному адресу электронной почты. Когда VTL падает ниже вашего настроенного порога, другое предупреждение передается. Можно таким образом контролировать выполнение вируса. Для обеспечения вы получите эти предупреждения, проверите адрес электронной почты, которому передаются предупреждения в CLI с помощью **alertconfig** команды.

Настраивать, или reivew confirugation

- GUI: Сервисы безопасности> Фильтры Вспышки и анализ конфигурация при **Глобальных параметрах Редактирования...**
- CLI: **outbreakconfig> настройка**

Напр.

Новая вспышка вируса будет сначала обнаружена SenderBase, и VTL будет поднят. Если

VTL встретит или превысит ваш настроенный порог VTL, вы получите предупреждение. Предупреждения Sophos придержатся, поскольку вирус определен и перехвачен, и когда новые подписи определения вируса становятся доступными.

Дополнительные сведения

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