

Содержание

- Поиск DDoS атак, BotNet и перехода на конкретный ресурс с использованием триггеров в QoE 3
 - Пример настройки триггера на поиск источника DDOS-атаки типа Flood* 3
 - Пример настройки триггера на поиск цели DDOS-атаки типа Flood* 9
- Анализ BotNet 11
- Фиксация перехода абонента на ресурс конкурента 12

Поиск DDoS атак, BotNet и перехода на конкретный ресурс с использованием триггеров в QoE

Триггеры используются для поиска данных в QoE Stor по заданным параметрам. После срабатывания триггера возможно одно из действий:

- уведомление в GUI
- HTTP действие
- отправка email

Необходимые опции SKAT DPI:

- Сбор и анализ статистики по протоколам и направлениям
- Уведомление абонентов

Необходимые дополнительные модули:

- DPIUI2 (GUI - Графический интерфейс управления)
- Внедрение и администрирование

Пример настройки триггера на поиск источника DDOS-атаки типа Flood

Общая информация триггера

Общее			
Название триггера *	Важность	Триггер	☐ Выключен
DDoS поиск источника	Информация	▼	
Дни недели *	Частота проверки *	Количество срабатываний	
Пн, Вт, Ср, Чт, Пт, Сб, Вс	▼ 1 час	▼ 1	
Дата начала	Дата окончания	Время начала	Время окончания

Название триггера «DDoS поиск источника», дни недели – все, частота проверки – 1 час, частота срабатываний триггера – 1 раз, даты и время начала/окончания не установлены.



Каждый день периодичностью в 1 час будет происходить проверка по условиям описанным ниже.

Запросы

Запросы						
+						
	Название	Отчет		Период с	Период по	
☒ Вкл.	A	Maxi		сейчас - 15 минут	сейчас	

- Добавить поле
- Название A
- Выбрать таблицу для сканирования: Сырой полный нетфлоу → Таблицы → Обнаружение атак → Топ IP-адресов хостов → Maxi
- Выбрать период с: «сейчас - 15 минут», период по: «сейчас»



В этом случае будет происходить анализ трафика по выбранной странице в период — последние 15 минут.

Условия

Условия							
+							
	Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение
☒ Вкл.	И	A	avg		Время жизни	<=	20
☒ Вкл.	И	A	avg		Сессии	>=	1500

- Добавить "+" 2 поля
- Связка - И
- Функция - avg
- Серия в 1 поле - Время жизни сессии, мс <= 20
- Серия во 2 поле - Сессии >= 1500



Мы задали условие — для срабатывания триггера необходимо, чтобы были детектированы: И сессии с жизнью меньше или равно 20мс, И с одного IP-хоста было более 1500 сессий.

Обработка ошибок

Обработка ошибок

Если нет данных *	Если ошибка выполнения или тайм-аут *
Нет данных	Сохранить последнее состояние

- В поле "Если нет данных" — нет данных
- В поле "Если есть ошибка или тайм-аут" — сохранить последнее состояние



в этой конфигурации — при отсутствии ошибок никаких данных сохраняться не будет, при их наличии — сохранится информация в виде таблицы о подозрительных сессиях.

Действия

E-mail действие

Действия

E-mail

Кому
your@email.com

Тема
Trigger fired: {trigger.name}

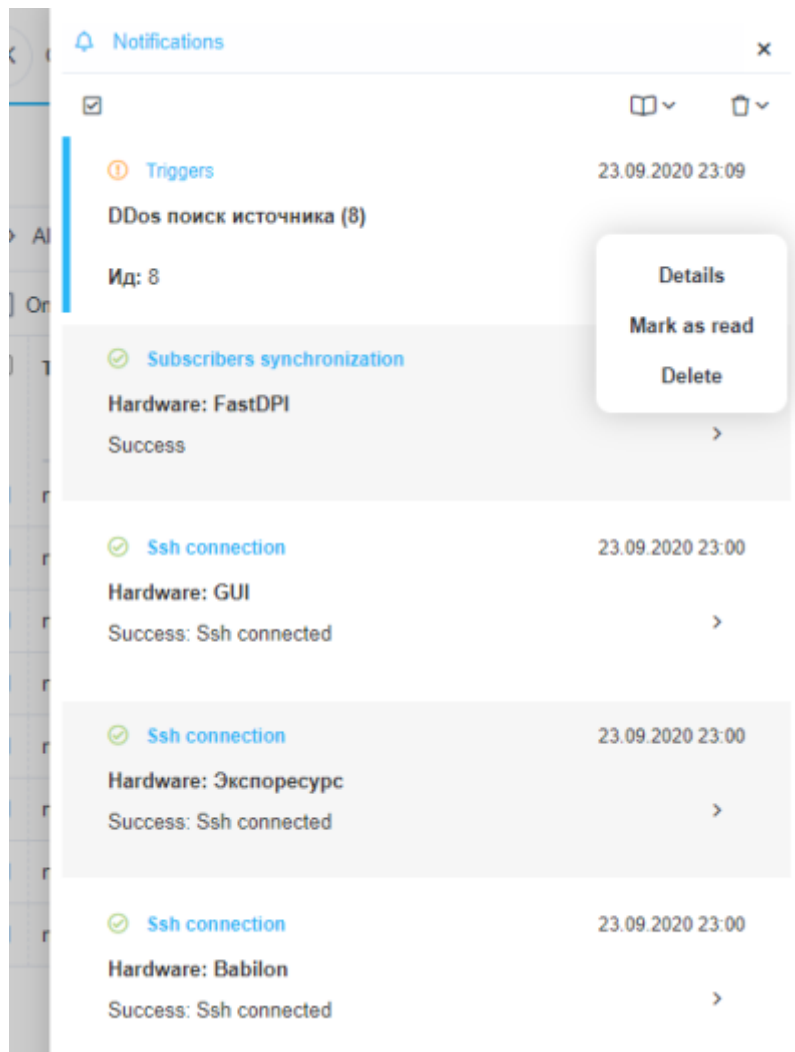
Сообщение

Id: {trigger.id}
Trigger: {trigger.name}
Status: {trigger.state}
Severity: {trigger.severity}

Queries:
{trigger.queries}

- Для автоматического заполнения — кликнуть по иконке (автоматическое заполнение формы)
- В поле "Кому" — указать адрес электронной почты
- При этой настройке, при срабатывании триггера на указанный адрес электронной почты будет отправлена вся информация о нотификации: ИД, название триггера, статус, ссылка на отчет (сохраненное состояние)

Нотификация



Выбрать нотификацию Выбрать — "Детали"

Notifications

←

Triggers

Status

Read

Notification date

23.09.2020 23:09

Notify type

Warning

Notification content

DDos поиск источника (8)

Ид: 8

Триггер: DDos поиск источника

Статус: firing

Важность: information

Запросы:

A: QoETableFullflowRawTopHostsIpsWidget

Причины возникновения нотификации:

avg(avg_ses_lifetime) <= 200000 is true in query A

avg(sessions_uniq) >= 1 is true in query A

Ссылки на отчеты:

A: https://192.168.88.11/#QoEAnyReport/report_id=rMeFuKSp316vU1b

Перейти по ссылке на отчет — отчет откроется в новом окне браузера.

HTTP действие

Действия

E-mail x Нотификация x Http x

Метод: POST Урл: Вкл.

Заголовки		Тело
+		
Имя	Значение	<pre><?xml version="1.0"?> <issue> <project_id>1</project_id> <subject>Trigger fired: {trigger.name}</subject> <priority_id>1</priority_id> <description>Id: {trigger.id}\nTrigger: {trigger.name}\nStatus: {trigger.state}\nSeverity: {trigger.severity}\nQueries: {trigger.queries}\nReasons for the occurrence of notification: {trigger.notification.notes}\nLinks to reports:\n{trigger.report.link}\n\nLinks to files:\n{trigger.report.csv}\n\n{trigger.report.tsv}\n\n{trigger.report .xlsx}\n\n{trigger.report.xlsx}</description> </issue></pre>
Content-Type	application/xml	

json Шаблон по умолчанию
xml Шаблон по умолчанию

Для автоматического заполнения — кликнуть  (автоматическое заполнение формы)
 Выбрать метод наиболее приемлемый для вашей ticket-системы и ввести URL адрес



Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.

Пример настройки триггера на поиск цели DDOS-атаки типа Flood

От предыдущего примера отличается настройкой 2 и 3 этапов (Запросы и Условия).

Запросы

Запросы

+

	Название	Отчет	Период с	Период по	
☒	Вкл.	A	Maxi	сейчас - 15 минут	сейчас

Условия

+

	Связь	
☒	Вкл.	И
☒	Вкл.	И

Обработка ошибок

Если нет данных *

Нет данных

Действия

Нотификация x

Кому

Поиск

Сырой полный нетфлоу

Таблицы

Сырой лог

Обнаружение атак

Топ прикладных протоколов

Топ групп прикладных протоколов

Топ абонентов

По трафику

По флоу

По времени жизни сессии

По абонентам и хостам

Maxi

Оператор	Значение
<=	20
>=	1500

полнения или тайм-аут *

днее состояние

Вкл.

в поле отчет выбрать Raw full netflow → Tables → Attacks detection → Top subscribers → Maxi

Условия

Условия

+

	Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение
☒	Вкл.	И	A	avg	Флоу к абоне	>=	10000

Серия — "Объем Flow к абонентам, Пак", >= 10000



Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.

Анализ BotNet

От предыдущего примера отличается настройкой 2 и 3 этапов (Запросы и Условия).

Запросы

Запросы						
+						
	Название	Отчет		Период с	Период по	
☒ Вкл.	A	Maxi	▼	сейчас - 15 минут	сейчас	🗑
☒ Вкл.	B	Полный сырой лог	▼	сейчас - 15 минут	сейчас	🗑

- Выбрать Raw full netflow → Tables → Attacks detection → Top application protocols → Maxi для значения "A"
- Raw full network → Tables → Raw log → Full raw log для значения "B"

Условия

Условия							
+							
	Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение
☒ Вкл.	ИЛИ	B	avg		Порт получат	=	6667
☒ Вкл.	ИЛИ	B	avg		Порт источн	=	6667
☒ Вкл.	ИЛИ	B	avg		Порт получат	=	1080
☒ Вкл.	ИЛИ	B	avg		Порт источн	=	1080
☒ Вкл.	И	A	avg		Флоу	>=	2000

Т.к. BotNet чаще всего использует порты 6667 и 1080 — добавить каждый порт назначения/источника выбрав запрос "B" со значением "ИЛИ", и Flow Pcts/s больше или равно 2000.



При этой конфигурации в случае если: хоть на одном из портов (6667/1080) количество проходящих пакетов будет более 2000 в секунду — сработает триггер.



Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.

Фиксация перехода абонента на ресурс конкурента

Общая информация триггера

Общее

Название триггера *

Интерес к конкурентам

Важность

Информация

Триггер

Выключен

Дни недели *

Пн, Вт, Ср, Чт, Пт, Сб, Вс

Частота проверки *

1 час

Количество срабатываний

1

Дата начала

Дата окончания

Время начала

Время окончания

Название триггера «Интерес к конкурентам», дни недели – все, частота проверки – 1 час, частота срабатываний триггера – 1 раз, даты и время начала/окончания не установлены.



Каждый день периодичностью в 1 час будет происходить проверка по условиям описанным ниже.

Запросы

Запросы						
+						
	Название	Отчет		Период с	Период по	
☒ Вкл.	A	Сырой кликстрим	☐	сейчас - 1 час	сейчас	☐
☒ Вкл.	B	Maxi	☐	сейчас - 1 час	сейчас	☐

- Добавить "+" поле
- Название A
Выбрать таблицу для сканирования: Raw clickstream → Tables → Raw clickstream
- Название B
Выбрать таблицу для сканирования: Raw full netflow → Tables → Attacks detection → Top hosts IPs → Maxi
- Выбрать период с: «now – 1 hour», период по : «now»
- В этом случае будет происходить анализ трафика каждый час по выбранным таблицам.

Условия

Условия								
+								
	Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение	
☒ Вкл.	ИЛИ	A	avg		Хост	=	*megafon.ru	
☒ Вкл.	И	B	avg		Объем флоу	>=	800	
☒ Вкл.	ИЛИ	A	avg		Хост	=	*mts.ru	

- Добавить "+" поле 3 поля
- Первое поле — выбрать таблицу "А"; Связка - "Или"; Функция - "avg";Серия Host = *megafon.ru(или ваш любимый конкурент)
- Второе поле — выбрать таблицу "Б"; связка "И"; Функция - "avg";Серия Flow volume from subscriber, Pct/s >= 800



мы задали условие — для срабатывания триггера необходимо, чтобы было детектировано: не менее 800 пакетов (не случайный а осмысленный переход) от абонента к сайту конкурента.

Обработка ошибок

Обработка ошибок	
Если нет данных *	Если ошибка выполнения или тайм-аут *
Нет данных	Сохранить последнее состояние

- В поле "Если нет ошибок" — нет данных
- В поле "Если есть ошибка или таймаут" — сохранить последнее состояние.



В этой конфигурации — при отсутствии ошибок никаких данных сохраняться не будет, при их наличии — сохранится информация в виде таблицы о подозрительных сессиях.

Действия

Е-mail действие

Действия

E-mail x

Кому
your@email.com

Тема
Trigger fired: {trigger.name}

Сообщение

Id: {trigger.id}
Trigger: {trigger.name}
Status: {trigger.state}
Severity: {trigger.severity}

Queries:
{trigger.queries}

- Для автоматического заполнения — кликнуть (автоматическое заполнение формы)
- В поле "Кому" — указать адрес электронной почты



При этой настройке, при срабатывании триггера на указанный адрес электронной почты будет отправлена вся информация о нотификации: ИД, название триггера, статус, ссылка на отчет (сохраненное состояние).

Нотификация

Действия

E-mail x Нотификация x

Заголовок нотификации
{trigger.name}

Подзаголовок нотификации
{trigger.id}

Тип нотификации
Предупреждение

Сообщение

Ид: {trigger.id}
Триггер: {trigger.name}
Статус: {trigger.state}
Важность: {trigger.severity}

Запросы:
{trigger.queries}

- Для автоматического заполнения — кликнуть  (автоматическое заполнение формы)
- Выбрать тип нотификации — "Предупреждение"
- При этой настройке будет создана нотификация в СКАТ

Alerts					Alerts actions			
☐ Only selected triggers					☐ Only selected notifications			
☐	Trigger name	Type	Date	Note	☐	Type	Date	State
	Filter	Filter	Filter	Filter		Filter	Filter	Filter
☐	Ddos	 Alerting	14.08.2020 13:58	avg(flow_vol_to_s	☐	notification	14.08.2020 13:59:03	Complete
☐	DDos поиск исто	 Alerting	14.08.2020 13:58	avg(avg_ses_lifet	☐	notification	14.08.2020 13:58:23	Complete
☐	Ddos	 Alerting	14.08.2020 13:56	avg(flow_vol_to_s	☐	notification	14.08.2020 13:56:43	Complete
☐	DDos поиск исто	 Alerting	14.08.2020 13:55	avg(avg_ses_lifet	☐	notification	14.08.2020 13:56:05	Complete
☐	Ddos	 Alerting	14.08.2020 13:54	avg(flow_vol_to_s	☐	notification	14.08.2020 13:54:23	Complete
☐	Ddos	 Alerting	14.08.2020 13:52	avg(flow_vol_to_s	☐	notification	14.08.2020 13:52:22	Complete
☐	DDos поиск исто	 OK	14.08.2020 13:51	avg(avg_ses_lifet	☐	notification	14.08.2020 13:50:25	Complete
☐	Ddos	 Alerting	14.08.2020 13:50	avg(flow_vol_to_s				

Получить ссылку на отчет можно через меню нотификаций


Notifications

☒


Triggers

DDos поиск источника (8)

Ид: 8


Subscribers synchronization

Hardware: FastDPI

Success


Ssh connection

Hardware: GUI

Success: Ssh connected


Ssh connection

Hardware: Экспоресурс

Success: Ssh connected


Ssh connection

Hardware: Babilon

Success: Ssh connected

23.09.2020 23:09

Details

Mark as read

Delete

23.09.2020 23:00

23.09.2020 23:00

23.09.2020 23:00

Выбрать нотификацию Выбрать — "Детали"

Notifications

×

← Triggers

Status	Read
Notification date	23.09.2020 23:09
Notify type	Warning

Notification content

DDos поиск источника (8)

Ид: 8

Триггер: DDos поиск источника

Статус: firing

Важность: information

Запросы:

A: QoETableFullflowRawTopHostsIpsWidget

Причины возникновения нотификации:

avg(avg_ses_lifetime) <= 200000 is true in query A
avg(sessions_uniq) >= 1 is true in query A

Ссылки на отчеты:

A: https://192.168.88.11/#QoEAnyReport/report_id=rMeFuKSp316vU1b

Перейти по ссылке на отчет — отчет откроется в новом окне браузера.

HTTP действие

Действия

E-mail x Нотификация x Http x

Метод: POST Урл: https://your_redmine_host/issues.xml?key=your_redmine_api_key Вкл.

Заголовки		Тело
+		<pre><?xml version="1.0"?> <issue> <project_id>1</project_id> <subject>Trigger fired: {trigger.name}</subject> <priority_id>1</priority_id> <description>Id: {trigger.id}\nTrigger: {trigger.name}\nStatus: {trigger.state}\nSeverity: {trigger.severity}\nQueries: {trigger.queries}\nReasons for the occurrence of notification: {trigger.notification.notes}\nLinks to reports:\n{trigger.report.link}\n\nLinks to files:\n{trigger.report.csv}\n\n{trigger.report.tsv}\n\n{trigger.report .xlsx}\n\n{trigger.report.xlsx}</description> </issue></pre>
Имя	Значение	
Content-Type	application/xml	

json Шаблон по умолчанию
 xml Шаблон по умолчанию

- Для автоматического заполнения — кликнуть  (автоматическое заполнение формы)
- Выбрать метод наиболее приемлемый для вашей ticket-системы и ввести URL адрес



Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.