Table of Contents

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	0
Фиксация перехода абонента на ресурс конкурента	1

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
- НТТР действие
- отправка email

Необходимые опции СКАТ DPI:

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

Необходимые дополнительные модули:

- DPIUI2 (GUI Графический интерфейс управления)
- QoE Stor (Модуль сбора статистики)

Пример настройки триггера на поиск источника DDOSатаки типа Flood

Общая информация триггера

Common										-
Trigger name * DDos поиск источника				s	everity nformation		~	Trigger	Disabled	
Days of the week * Mon, Tue, Wed, Thu, Fri, Sat, Su	n	v	Check frequency * 1 hour			~	Number (of positives		
Start date	E	nd date			Start time		(End time		(1)

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

Queries							
+							
	Query name	Report		Period from	Period to		
🗹 On	A	Maxi	7	now - 15 minute	now	0	I

- Добавить поле
- Название А
- Выбрать таблицу для сканирования: Raw full netflow \rightarrow Tables \rightarrow Attacks detection \rightarrow Top hosts IPs \rightarrow Maxi
- Выбрать период с: «now 15minute», период по : «now»



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

Условия

Conditions												
	+											
			Bind	Query name	Function	Combinator	Serie	Operator	Value			
		On	AND	A	avg		Session lifetime	<=	20	Û		
		On	AND	A	avg		Sessions	>=	1500	Û		

- Добавить "+" 2 поля
- Связка И
- Функция avg
- Серия в 1 поле время жизни сессии <= 20(мс)
- Серия во 2 поле количество сессий >= 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

No data & error handling			*
If no data *		If execution error or timeout *	
No data	۲	Keep last state	×

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



Действия

E-mail действие

Actions	
Notification × E-mail ×	+
Send to	On
Your@email.com	_
Subject	
Trigger fired: {trigger.name}	
Message	R da
	U 1
B I U E E E E Foot Size V Font Family V Foot Format V E E V S S S S S S S S S S S S S S S S	÷
Ид: {trigger.id}	
Триггер: (trigger.name)	
Craryc: {trigger.state}	
Важность: {trigger.severity}	
Запросы:	
{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

ctions				
Notification ×	E-mail	×		+
Notification title				On
{trigger.name}				
Notification subtitle			Notification type	
(trigger.id)			Warning	*
В / Ц ≣ ≣ ≣ ≣ Ид:{trigger.id}	i≣ Font Size	v Font Family v Fo	ont Format. 👻 🗊 🍺 🎼 🍕 🏟 🌒 🔐 X2 🗴	은 등 /월 로 🖬 🔺
Триггер: {trigger.name}				
Статус: (trigger.state)				
Важность: {trigger.severi	ty}			
Запросы:				
{trigger.queries}				

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

	ថ	Alerts				<	\$ Alerts actions				<
1		Only selected trigge	rs.		Û	ø	Only selected notification	s		Û	ø
		Trigger name	Туре	Date	Note		Туре	Date	State		
		Q, Filter	÷	8	Q Filter		v	ė		÷	
1		Ddos	Alerting	14.08.2020 13:58	avg(flow_vol_to_s	Ō	notification	14.08.2020 13:59:03	Complete		Û
t		DDos поиск источ	Alerting	14.08.2020 13:58	avg(avg_ses_lifet	Û	notification	14.08.2020 13:58:23	Complete		Û
		Ddos	Alerting	14.08.2020 13:56:	avg(flow_vol_to_s	Ō	notification	14.08.2020 13:56:43	Complete		Û
		DDos поиск источ	Alerting	14.08.2020 13:55:	avg(avg_ses_lifeti	Ō	notification	14.08.2020 13:56:05	Complete		Û
		Ddos	Alerting	14.08.2020 13:54:	avg(flow_vol_to_s	Û	notification	14.08.2020 13:54:23	Complete		Û
		Ddos	Alerting	14.08.2020 13:52	avg(flow_vol_to_s	Û	notification	14.08.2020 13:52:22	Complete		Û
		DDos поиск источ	Ok	14.08.2020 13:51:	avg(avg_ses_lifeti	٥	notification	14.08.2020 13:50:25	Complete		Û
		Ddos	Alerting	14.08.2020 13:50:	avg(flow_vol_to_s	Û					

Получить ссылку на отчет можно через меню нотификаций



Выбрать нотификацию Выбрать — "Детали"

```
A Notifications
                                                                    ×
              Triggers
    ←
                    Read
Status
                   23.09.2020 23:09
Notification date
                   ① Warning
Notify type
 Notification content
DDos поиск источника (8)
Ид: 8
Триггер: DDos поиск источника
Статус: firing
Важность: information
Запросы:
A: QoETableFullflowRawTopHostslpsWidget
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.

НТТР действие

Notification	× E-mail	1	Http ×	+ 1
Method	Url			0
POST	https://y	our_re	lmine_host/issues.xml?key=your_redmine_api_key	
Headers		<	Body	> ²
+				
Name Content-Type	Value application/xml	o	xml version="1.0"? <issue> <project_id>1</project_id> <subject>Cpa6oran тригтер: {trigger.name}</subject> <prionty_id>1 <description>Ид: {trigger.id} Тригтер: {trigger.name} Статус: {trigger.severity} Важность: {trigger.severity} Запросы: {trigger.queries}</description></prionty_id></issue>	REDMINE JSON REDMINE XML

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

Queries										•
+										
	Query name	Report			Period from		Period to			
🗹 On	A	Maxi		7	now - 15 minu	ites	now			Û
		C.) 🖽 Ssh brutetorce							
Conditions		⊞ [🗄 🖽 Top application proto	ocols						*
+		80	🗈 🖽 Top subscribers							
	Bind		🗅 🖽 By traffic			Ope	rator	Value		
🗹 On	AND		🗅 🖽 By flow		1	>=		100		Û
			🗅 🖽 By session lifetin	пе						
No data & e	error handling		🗅 🖽 By subscribers a	nd hos	ts					•
If no data '			🗅 🖽 Maxi			meou	it *			
No data		I Top hosts IPs							`	~
		🕀 🗅 Raw die	ckstream							
						11				

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

Условия

Conditions										
+										
		Bind	Query name	Function	Combinator	Serie	Operator	Value		
	On	AND	A	avg		Flow volume to	>=	10000	Û	

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



Анализ BotNet

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

Запросы

Queries										
+										
	Query name	Report		Period from	Period to					
🗹 On	A	Maxi	7	now - 15 minute	now		Û			
🗹 On	В	Full raw log	7	now - 15 minute	now		Û			

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

Условия

Conditions	Conditions											
+	+											
	Bind	Query name	Function	Combinator	Serie	Operator	Value					
🗹 On	OR	В	avg		Destination port	=	6667	Û				
🗹 On	OR	в	avg		Source port	=	6667	Û				
🗹 On	OR	в	avg		Destination port	=	1080	Û				
🗹 On	OR	В	avg		Source port	-	1080	Û				
🗹 On	AND	A	avg		Flow, Pkts/s	>=	2000	Û				

Т.к. BotNet чаще всего использует порты 6667 и 1080 — добавить каждый порт назначения/источника выбрав запрос "В" 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

Common								•
Trigger name * Интерес к конкурентам			Severity Information		~	Frigger	Disabled	
Days of the week * Mon, Tue, Wed, Thu, Fri, Sat, Sur	~	Check frequency * 1 hour		~	Number of 1	f positives		¢
Start date	End date		Start time		C	End time		0

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



Запросы

Queries									
+									
	Query name	Report		Period from	Period to				
🛛 On	A	Raw clickstream	∇	now - 1 hour	now	Û			
🗹 On	в	Maxi	∇	now - 1 hour	now	Û			

- Добавить "+" поле
- Название А

Выбрать таблицу для сканирования: Raw clickstream → Tables → Raw clickstream

• Название В

Выбрать таблицу для сканирования: Raw full netflow \rightarrow Tables \rightarrow Attacks detection \rightarrow Top hosts IPs \rightarrow Maxi

- Выбрать период с: «now 1 hour», период по : «now»
- В этом случае будет происходит анализ трафика каждый час по выбранным таблицам.

Условия

Conditions											
+											
	Bind	Query name	Function	Combinator	Serie	Operator	Value				
🗹 On	OR	A	avg		Host	=	*megafon.ru	Û			
🗹 On	AND	в	avg		Flow volume fro	>=	800	Û			
🗹 On	OR	A	avg		Host	=	*mts.ru	Û			

- 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

No data & error handling			*
If no data *		If execution error or timeout *	
No data	×	Keep last state	×

- 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

E-mail действие

ctions	
Notification × E-mail ×	+
Send to	On
Your@email.com	
Subject	
Trigger fired: {trigger.name}	
Message	
B I U = = = = = = Font Size v Font Family v Font Format v = = = 😰 🗟 on 🔅 🧇 🍙 X, X' S 🖧 = 🔤	
Ид: {trigger.id}	Î
Триггер: (trigger.name)	
Статус: {trigger.state}	
Важность: {trigger.severity}	
Запросы:	
{trigger.queries}	-

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



Нотификация

Actions	*
Notification × E-mail ×	+
Notification title	On
{trigger.name}	
Notification subtitle Notification type	
(trigger.id) Warning	~
Message	₽
B / U = = = = = Font Size v Font Family v Font Format v = = = 🖉 🎼 🗞 🚸 49 🔐 X_2 X^2 + 45 🌾 = 💷	
Ид: {trigger.id}	î.
Триггер: {trigger.name}	
Craryc: (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

ថ	Alerts				<	Alerts actions					<
Only selected triggers							Only selected notifications				
	Trigger name Q. Filter	Туре	Date	Note Q Filter			Туре	Date	State	v	
	Ddos	Alerting	14.08.2020 13:58	avg(flow_vol_to_s	0		notification	14.08.2020 13:59:03	Complete		Û
	DDos поиск источ	Alerting	14.08.2020 13:58	avg(avg_ses_lifet	٥		notification	14.08.2020 13:58:23	Complete		Û
	Ddos	Alerting	14.08.2020 13:56:	avg(flow_vol_to_s	Û		notification	14.08.2020 13:56:43	Complete		Û
	DDos поиск источ	Alerting	14.08.2020 13:55:	avg(avg_ses_lifet)	Ō		notification	14.08.2020 13:56:05	Complete		Ċ
	Ddos	Alerting	14.08.2020 13:54:	avg(flow_vol_to_s	٥		notification	14.08.2020 13:54:23	Complete		Û
	Ddos	Alerting	14.08.2020 13:52	avg(flow_vol_to_s	Û		notification	14.08.2020 13:52:22	Complete		Û
	DDos поиск источ	Ok	14.08.2020 13:51:	avg(avg_ses_lifet	0		notification	14.08.2020 13:50:25	Complete		Û
	Ddos	Alerting	14.08.2020 13:50	avg(flow_vol_to_s	0						

Получить ссылку на отчет можно через меню нотификаций





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

НТТР действие

Actions				-	12	no
Notification	× E-mail	×	Http ×	+		no
Method	Url			On		no
POST	https://j	your_redr	mine_host/issues.xml?key=your_redmine_api_key			not
Headers		<	Body	>		not
+				B	2	not
Name Content-Type	Value application/xml	Ċ	xml version="1.0"? <issue> <project_id>1</project_id> <subject>Cpa6oran тритер: {trigger.name}</subject> <description>Ид: {trigger.id} Тритер: {trigger.same} Статус: {trigger.state} Важность: {trigger.severity} Запросы: {trigger.queries}</description></issue>	REDMINE X	IN VIL	

- 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.