"Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"

Решение по защите от DDoS в Лаборатории Касперского «Kaspersky DDoS Prevention» решили делать "своими руками" несколько лет назад, но только в 2008м решение из перспективного проекта перешло к реальному воплощению. Еще порядка полутора лет потребовалось на создание и доводку аппаратно-программного комплекса до "боевой версии", выбор типологии размещения: только с лета 2010 года подобную услугу, на базе этого решения, стали предлагать широкому спектру коммерческих клиентов. О специфике решения, его стоимости, эффективности и SLA, а также о специфике DDoS-атак нам рассказал менеджер проектов DdoS Prevention «Лаборатории Касперского» Михаил Савельев.

История создания

"Вербовка" пользовательских компьютеров и мощных серверов в зомби-сети тесно связана с их заражением компьютерными вирусами, поэтому неудивительно, что спецификой защиты от DDoS в "лаборатории Касперского" занимались достаточно давно. "Не всегда антивирусы могут выявить и поймать новых зловредов, особенно если речь идет о «свежих» вирусах, в т.ч. написанных для реализации определенной задачи, - отмечает Михаил Савельев. - Поэтому если уж мы не можем отловить эту гадость, надо минимизировать воздействие подобного типа угроз для наших клиентов. Кроме того, потребность в защите сейчас очень велика: DDoS-атаки представляют вполне перспективный тип информационного оружия, защита от которого требуется любой компании, зарабатывающей в Сети деньги". Так и родился проект Kaspersky DDoS Prevention - на базе знаний тех людей, которые занимались этим профессионально.

["Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"]

Пример интерфейса «Kaspersky DDoS Prevention»

«Часть из них была аналитиками, изучавшими и имевшими опыт борьбы с ботнетами, которые помогли поставить задачу по функционалу решения, часть – уже работали у провайдеров связи и имели опыт внедрения существующих типовых аппаратно-программных решений защиты от DDoS и, следовательно, могли выделить сильные и слабые стороны таких проектов, - говорит Михаил Савельев. - Кроме того, мы добавили в эту группу разработчиков несколько аналитиков, которые занимались ранее расследованием подобных инцидентов. Они могли оценить перспективы развития таких решений и определить, какой блок статистики и отчетности был бы интересен клиентам с т.з. передачи информации правоохранительным органам. Таким образом, у нас получилась интересная система противодействия широкому спектру атак, суммарный бюджет которого составил несколько десятков миллионов рублей. Достоинство Системы сосредоточено в ее гибкости и модульности. Существующие защитные механизмы и порядок их применения может настраиваться в ходе атаки, ну а по мере эволюции угрозы создаются новые защитные модули».

норма	["Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"]
аномалия	["Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"]

Визуализация DDoS-атаки – отчеты системы «Kaspersky DDoS Prevention»

Если посмотреть по времени, то разработка была достаточно стремительной. Первая версия системы «Kaspersky DDoS Prevention» начала работать в 2008 году, бета-версия была доступна в октябре 2009 года, а версия, доступная для боевого применения, в июне 2010 года. "Разработка у нас была специфической, - признается Михаил Савельев, - в идеальных условиях система просуществовала всего-то 2,5 месяца, после чего мы вывели ее в "дикие" условия Сети и обкатывали на реальных атаках, активно учились защищать информационные ресурсы. Главное было получить ценный опыт борьбы с управляемыми атаками - обычно это получалось при работе с "тяжелыми" корпоративными клиентами, против которых работают серьезно. Такого рода атаки индивидуальны. В целом, каждая атака приносит что-то новое в нашу копилку опыта. Поэтому, сложно сказать, что разработка системы завершена полностью: скорее, она постоянно эволюционирует". Общие инвестиции в Kaspersky DDoS Prevention составили к настоящему моменту порядка 40 млн. руб.

["Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"]

["Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"]

["Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"]
Визуализация атаки по параметрам (серая линия – профиль, желтая – уровень внимания, красная – уровень тревоги, синяя – реальный трафик). Момент включения системы (принятие решения заказчиком) – 11-45.

Вдобавок, как говорит Михаил Савельев: "Нам очень хотелось, чтобы система, которую мы используем, могла развиваться просто и дешево. И не была бы привязана ни к какой специализированной и, самое главное, определенной и закрытой аппаратной платформе. Она должна была базироваться на типовых серверах (в основном, производства компании IBM – Прим. ред.), которые можно собрать или арендовать достаточно просто, т.е. должна быть "всеядна"... Это позволяет свободно развивать Систему и помогает в критических ситуациях. Мы можем существенно нарастить мощность фильтрации в течение суток, арендовав любое доступное железо в каком-либо ЦОДе ".

Схема решения

Суммарная пропускная способность Kaspersky DDoS Prevention сейчас составляет 10 Гбит/с, ее типология - распределенная система. "Наши центры очистки мы стараемся располагать в центрах обмена трафиком, как за рубежом, так и в России. Выход «за рубеж» целесообразен и с той точки зрения, что мы становимся ближе к потенциальному источнику атаки: паразитный трафик со стороны, например, США или Китая мы стараемся отсекать еще на "подходах к цели", чтобы не перегружать локальные каналы провайдеров, - говорит Михаил Савельев. -.Могу отметить, что в России мы имеем «точки присутствия» на узлах М9 и М10, но о конкретной их дислокации я умолчу в целях безопасности. Сам центр очистки, на самом деле, это многокомпонентная структура. Это и мощные межсетевые экраны, и анализаторы трафика, работающие в сложно организованных кластерах для повышения надежности и живучести".

Причем, ресурсы этой распределенной системы могут работать как автономно, по своему направлению, так и в общей структуре, когда атака по какому-то направлению слишком заметна и значительна. Тот факт, что вычислительная мощность не сосредоточена в какой-то отдельной точке, дает возможность маневрировать ресурсами: многокомпонентность дает возможность, в зависимости от характера атаки, "перетасовывать" и менять ресурсы, выделять больше мощности под проверку трафика. Более подробно архитектура «Kaspersky DDoS Prevention» представлена на Схеме №1.

Схема №1. Архитектура «Kaspersky DDoS Prevention»

["Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"]

"Наличие большого числа центров фильтрации позволяет нам не иметь единой точки отказа, - говорит Михаил Савельев. - Это как ванна с несколькими затычками: трафик сливается по ним без проблем и равномерно. Но если какой-то узел в нашей системе "перегружается, то мы распределяем нагрузку по оставшимся."

Исходя из схемы решения «Kaspersky DDoS Prevention», специфической можно признать и его позиционирование. "Провайдер или ЦОД, оказывающие услуги по защите от DDoS, могут взять под защиту только своих клиентов, тех, кто закупает у него услугу хостинга или арендует каналы связи. Для нас же месторасположения клиента не имеет большого значения. Не обязательно быть клиентом того же провайдера, где мы арендуем место для размещения нашего оборудования. Мы ориентируемся на то, что у клиентов уже есть сложившаяся инфраструктура и они уже привязаны к какому-либо поставщику услуг, и не хотят ничего менять, - отмечает Михаил Савельев. - Мы же находимся как бы "над Интернетом". Мы можем "перенаправить" на систему очистки трафик любого клиента. . Перенаправление трафика, в зависимости от обстоятельств, может осуществляться, например, путем изменения DNS-записи ресурса. Разумеется, такой способ защиты удлиняет маршрут движения трафика, но задержка, уверяет г-н Савельев, все-таки незначительна.

Более подробно схема взаимодействия компонент системы «Kaspersky DDoS Prevention» представлена на Схемах №2 и №3.

Схема №2. Взаимодействие компонент системы «Kaspersky DDoS Prevention» в «мирное время»

["Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"]

Схема №3. Взаимодействие компонент системы «Kaspersky DDoS Prevention» во время атаки

["Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"]

Кстати, в качестве подготовительных мер, помимо сбора данных сенсорами системы о нормальном процессе функционирования защищаемых ресурсов, специалисты «Лаборатории Касперского» рекомендуют владельцам, защищаемых ими систем, уменьшить время жизни DNS записи о ресурсе

до 10-15 минут. Таким образом, в случае начала атаки, такое небольшое время жизни DNS-записи позволит оперативно осуществить переключение трафика на фильтрующие компоненты системы «Kaspersky DDoS Prevention». Более подробно работа системы представлена в Схеме №4.

Схема №4. Схема работы системы «Kaspersky DDoS Prevention»

1) Нормальная работа ресурса

["Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"]

2) Начало атаки

["Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"]

3) По истечению времени жизни DNS-записи начинается переключение на компоненты системы

["Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"]

4)Трафик перенаправлен на компоненты системы

["Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"]

Важно, что система Kaspersky DDoS Prevention не является замкнутым программно-аппаратным комплексом. Со стороны «Лаборатории Касперского» она постоянно управляется и сопровождается из специализированного центра безопасности. Он располагается в Москве, и в нем постоянно находится дежурная смена. "Но это не техники, а именно аналитики, которые видят атаки, которые проходят через наше оборудование, и контролируют доступность ресурсов наших клиентов. Дело в том, что борьба с DDoS-атакой – это искусство: не бывает двух похожих атак, поэтому далеко не всегда может должным образом помочь заранее определенный набор неких настроек каких либо защитных механизмов. Так что сотрудникам центра мониторинга нужен большой опыт и определенная доля основанной на этом опыте интуиции", - уверен Михаил Савельев.

Всего системой занимается порядка 15-ти человек, она работает в круглосуточном режиме. Если атака сложная, то дежурным аналитикам достаточно высокой квалификации готовы оказать помощь остальные участники команды – в режиме реального времени. "Большинство этих специалистов спит если не в обнимку, то рядом с включенным мобильным телефоном и ноутбуком, который подключен к корпоративной сети с помощью VPN-доступа", - с улыбкой замечает Михаил Савельев. Один из принципов, заложенных в систему, оказывать минимальное воздействие на трафик легитимных пользователей ресурсов. То есть система скорее пропустит на ресурс немного паразитного трафика, чем отсечет легитимных пользователей. Единственное участие в работе, которое требуется от клиента, это волеизъявление об активации защитных механизмов. "Причина тут в том, что порой существенные всплески в трафике могут быть вызваны успехом рекламной компании, т.е. фильтровать, пусть даже и в возросшем потоке данных, по сути нечего, - говорит г-н Савельев. - Ну и, кроме того, часть наших тарифных планов повременные, предполагающие тарификацию за каждый день атаки. В любом случае, клиент получает уведомление об отклонении от нормальных параметров работы, а затем он при помощи наших специалистов определяется с тем, насколько эта активность похожа на атаку".

Пока что у "Лаборатории Касперского" двадцать клиентов, которые подключили «Kaspersky DDoS Prevention». Они сосредоточены в европейской части страны, по запросам они примерно равноценно распределены по всем четырем, имеющимся в наличии, тарифным планам.

Стоимость и SLA

Стоимость защиты у "Лаборатории Касперского" зависит от объема сервиса, который предоставляется клиенту. Фактически, это третий подход, который применяется на рынке: не важна полоса пропускания или количество защищаемых объектов. Важно только время, в течение которого клиент находится под защитой. Самый простой уровень (подробнее см. Таблицу №1) - это Basic Edition, с абонентской платой 30 тыс. руб. По сути, это "страховой тариф": система клиента полностью проверена, созданы профили нормальной работы, а система «Kaspersky DDoS Prevention» готова перенаправлять трафик на свои системы фильтрации. Если атака не произойдет, то все так и останется в "горячем резерве", но если все-таки DDoS-атака случится, то клиенту это будет стоить 50 тыс. руб. в день. При этом, деньги за трафик с него брать не будут: этот объем может быть любым. По сути, такое решение может использоваться компаниями для поддержки аналогичной услуги, которую они заказывают у своего провайдера связи. Если он справится - это и не пригодится.

Самый дорогой тариф - Ultimate Edition, его стоимость в пять раз выше и составляет 150 тыс. руб. Здесь никаких ограничений нет в принципе: клиент может подключать систему к своим ресурсам время от времени, может не подключать, а может находится за ней, работающей в активном режиме, постоянно все 4 недели в месяц. Если атака проидойдет, то никаких дополнительных платежей в

адрес "Лаборатории Касперского" не последует, это предложение из серии "все включено". Остальные тарифы, Standard Edition за 70 тыс. руб. и Advanced Edition за 110 тыс. различаются, в основном, резервом полосы пропускания, а объем обеспечения защиты у них одинаковый. Все время сверх лимита в три дня надо будет оплатить дополнительно.

Таблица №1. Тарифные планы на услугу «Kaspersky DDoS Prevention»

Тарифный план	Мониторинг	Резерв полосы пропускания	Объем обеспечения защиты	Время хранения журналов	Предоставление отчетов
Basic Edition	+	-	-	-	-
Standard Edition	+	2 Гбит/с	3 дня в месяц	-	-
Advanced Edition	+	Без ограничений	3 дня в месяц	1 год	-
Ultimate Edition	+	Без ограничений	Без ограничений	3 года	+

Всего существует три основных параметра: 1) Время регистрации инциндента - период времени, который проходит от Обращения до подтверждения представителями Лицензиара факта принятия Инцидента к рассмотрению; 2) Время реакции - период времени (начиная с момента регистрации инцидента), в течение которого будет начата обработка инцидента. Естественно, продолжительность времени реакции напрямую зависит от критичности инцидента; 3) Время решения - период времени (с момента окончания времени реакции), в течение которого будет найдено постоянное или временное решение инцидента. Эти параметры можно посмотреть в Таблицах №2-№4.

Таблица №2. Время реакции на обращения

["Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"]

Таблица №3. Время реакции на инциденты

["Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"]

Таблица №4. Время разрешение инциндентов

["Лаборатория Касперского": "Каждая DDoS-атака уникальна и приносит нам что-то новое"]

Отметим, что:

- «Существенный инцидент» – инцидент, который существенно сказывается на работе Ресурса.
- «Критический инцидент» – инцидент, который делает Ресурс Лицензиата полностью неработоспособным или приводит к существенному ухудшению его работоспособности.
- «Некритичный инцидент» – все остальные инциденты, которые не оказывают существенного негативного влияния на работоспособность Ресурса.

И самое интересное – это параметры фильтрации трафика клиента. По сути, в процессе фильтрации трафика во время Атаки, Лицензиар обязуется, что:

- 1) Фильтрующее ПО будет пропускать трафик от адресатов, помещенных Лицензиатом в «белые листы»;
- 2) Защищающий его ресурс ПО будет блокировать трафик от адресатов, помещенных Лицензиатом в «черные листы»;
- 3) «Kaspersky DDoS Prevention» ПО обеспечит очистку трафика от паразитной составляющей на уровне.

№ п/п	Тип Атаки	Средний % очистки*	Средний % прохождения легитимных запросов**
1.	нелегитимный трафик на невостребованный протокол и/или порт (пример — UDP Flood, ICMP Flood)	98%	98%
2.	инициация соединения по протоколу TCP (SYN-Flood) со случайной подменой IP-адреса отправителя данных (IP-Spoof)	98%	98%
3.	установка полноценного TCP-соединения и с его дальнейшим сбрасыванием без обмена данными внутри сокета (TCP Connect Flood)	98%	98%
4.	отказ в обслуживании сервиса/ресурса атакой по протоколу HTTP/1.0 или HTTP/1.1 путем отправки данных: 1.вне спецификации протокола; 2. по спецификации протокола без дальнейшего следования инструкциям перенаправления (HTTP Redirect, JavaScript Redirect); 3. по спецификации протокола с дальнейшим следованием инструкций перенаправления против защиты на уровне теста Тьюринга (captcha).	98%	98%
5.	отказ в обслуживании сервиса/ресурса по протоколу HTTPS в случае наличия криптографического сертификата на фильтрующих ресурсах	98%	98%
6.	отказ в обслуживании сервиса/ресурса по протоколу HTTPS в случае отсутствия сертификата на фильтрующих ресурсах	80%	80%
7.	фильтрация трафика в условиях наличие большого количества легитимных пользователей ресурса с генерацией трафика разных характеристик	80%	80%

8.	атака по протоколу DNS с генерацией легитимных запросов	80%	80%
9.	Иные типы атак	75%	

* Указанный процент очистки рассчитан на основе следующего алгоритма: если IP адрес является вредоносным, то вероятность его блокировки равна указанному в таблице проценту по прошествии 10 минут после того, как IP адрес начал атаковать защищаемый Ресурс. ** Указанный процент прохождения легитимных запросов рассчитан на основе следующего алгоритма: если IP адрес является адресом легитимного пользователя ресурса, то вероятность его прохождения равна указанному в таблице проценту по прошествии 10 минут после того как IP адрес начал обращаться к защищаемому Ресурсу во время Атаки.

Специфика рынка

Современный рынок предложения DDoS-атак достаточно развит: исполнителей достаточно, между ними существует иерархия и специализация. Устоялись и цены. "Весной этого года я проводил очередной мониторинг по стоимости атак, - говорит с улыбкой Михаил Савельев, - так вот люди, которые вызывали у меня «внутреннее доверие», просили за день атаки от 100 долл в день. Можно считать это начальной стоимостью организации атак на черном рынке". Средняя цена достаточно мощной атаки, по моим оценкам, составляет около 3000 долларов в день».

Эти деньги, помимо дохода преступников, идут и на поддержание работоспособности атакующего ботнета. Во время атак ботнет достаточно быстро регрессирует - какие-то машины отсекаются антивирусами, какие-то банально выключаются по той причине, что их хозяева ложатся спать, порой сами пользователи обращают внимание на возросший трафик и непонятную загрузку компьютера, и переустанавливают ОС. По нашим данным, скорость обновление ботнета может составлять составляет до 25% в день, что, к слову, делает малоэффективной фильтрацию по заранее выявленным на других атаках IP-адресам.

Для поддержки ботнета, злоумышленники нуждаются в постоянном притоке новых членов бот-сети, для чего в Интернете постоянно проводятся массовые заражения пользовательских компьютеров. Один из типовых сценариев упрощенно можно описать так: сначала злоумышленником набирается база FTP-аккаунтов (взлом, подбор и кража паролей и т.п.), откуда потом будет проходить заражение. На эти ресурсы просто выкладывается контейнер с вирусом. Параллельно с этим осуществляется либо взлом популярных и посещаемых ресурсов, либо создаются некие странички (в том числе в социальных сетях), на которые разными способами заманиваются доверчивые пользователи. На этих страничках организуется скрытое перенаправление пользователей на те самые подготовленные контейнеры.

"Перенаправление, например, организуется путем использования тегов iframe или путем эксплуатации известных, или только что найденных злоумышленниками уязвимостей в браузерах, - говорит Михаил Савельев, - и от этого не спасут межсетевые экраны: пользователь сам инициирует это соединение, поэтому сетевой экран его пропустит совершенно спокойно. А содержимое контейнера может и не числиться в антивирусных базах, поэтому "боевую стойку" на эту систему антивирус может и не сделать".

Подобные вирусы, заразив системы пользователей, обращаются к распределенной системе командных центров, которые раздают членам ботнета команды. В том числе, это могут быть и команды на загрузку нового зловредного ПО. Сами командные центры маскируются под реально существующие сайты, что затрудняет их выявление обычными пользователями. А дальше – зараженный компьютер участвует в сети "зомби-машин" до тех пор, пока пользователь не удивится тому, что его компьютер "притормаживает" или отправляет в Сеть большее количество запросов, чем необходимо. Подсадить "заразу" на свой компьютер можно и другими путями, например, через содержимое закачек из торрент-сетей и еще десятком способов. "Лично для меня самым неприятным является то, что по сути "опасность" таит даже простой веб-серфинг по известным и знакомым для пользователя веб-ресурсам", - отмечает Михаил Савельев. Так, например, в мае этого года Веб-сайты, принадлежащие Государственному казначейству США, стали перенаправлять пользователей на сторонние ресурсы, которые, в свою очередь, пытались установить на компьютеры посетителей вредоносные программы, в июне 2010 года киберпреступники скомпрометировали веб-сайт издания Jerusalem Post, после чего тот тоже начал распространять зловред и т.д.

Кстати, во время атаки ботнет достаточно быстро регрессирует - какие-то машины отсекают сами пользователи, наиболее "засоренные" сегменты отключают провайдеры из-за увеличения трафика на каких-то машинах, после обновления, срабатывают антивирусы и т.д. В целом, обновление бота составляет до 25% в день, поэтому фильтрация по конкретным IP-адресам, в целом, имеет мало

смысла. Кроме того, Михаил Савельев категорически утверждает, что боты-миллионники существуют: "Самое большое, что видели мы, это ботнет из 1,5 млн. зомби-машин, - утверждает Михаил Савельев, - и это было совсем недавно". Можно также вспомнить и про общее количество зараженных Kido машин – это число предположительно составляет 5 или даже 10 млн. компьютеров по всему миру.

Кроме системы по отражению DDoS-атак у "Лаборатории Касперского" есть своя методика выявления и отслеживания деятельности ботнетов. Она позволяет разбираться в их системе работы, локализовать центры управления, анализировать новые образцы зловредного ПО для пополнения баз вирусов компании. "Если мы обнаруживаем командные центры, которые располагаются на территории России - мы уведомляем правоохранительные органы, - говорит Михаил Савельев, - благо подобное взаимодействие уже налажено". В базе компании около 2 тыс. записей о подобных системах. Г-н Савельев объясняет это тем, что описывать и учитывать имеет смысл только активные командные центры и "боевые" версии ботнетов. "В Сети можно найти огромное число командных центров, некоторые из них - даже с открытым интерфейсом. Каждый может зайти и дать команду на атаку любого компьютера, - говорит он. - Но это слишком слабые системы с единицами боеспособных "зомби" или уже мертвые ботнеты, вообще не имеющие в своем составе активных членов . Весь этот "мусор" мы даже не учитываем".