Д. Н. Макрушин

ИНФРАСТРУКТУРА SAAS КАК СРЕДСТВО УСИЛЕНИЯ РАСПРЕДЕЛЕННЫХ АТАК

Введение

Любой веб-проект, вне зависимости от своего назначения, имеет такую важную характеристику своей работоспособности, как предельная нагрузка. Значение данного показателя становится первостепенным, когда веб-приложение частично или полностью отказывается выполнять возложенные на него функции по обработке запросов от пользователей. Для кого-то из владельцев веб-приложения отказ в обслуживании может нести прямые финансовые и репутационные риски.

У каждого веб-ресурса есть предельное значение количества одновременно обрабатываемых запросов пользователей. Поэтому разработчики и владельцы веб-приложений уделяют особое внимание процедурам нагрузочного и стрессового тестирований. Современные сервисы нагрузочного тестирования удобны и полезны, однако некоторые их особенности оставляют лазейку для использования этих сервисов злоумышленниками.

Нагрузочное и стрессовое тестирование

Нагрузочное тестирование информационной системы — процедура оценки характеристик работоспособности тестируемой системы в рамках значений нагрузки, не превышающих предельное. Стрессовое тестирование представляет собой аналогичную процедуру, но проводимую за рамками предельного значения нагрузки. Стресс-тесты в большинстве случаев ведут к аномальному поведению тестируемой системы или ее отказу в обслуживании — аналогично атакам distributed denial of service (DDoS). Распределение множеств тестовых сценариев по мощности нагрузки на информационную систему изображено на рис. 1.

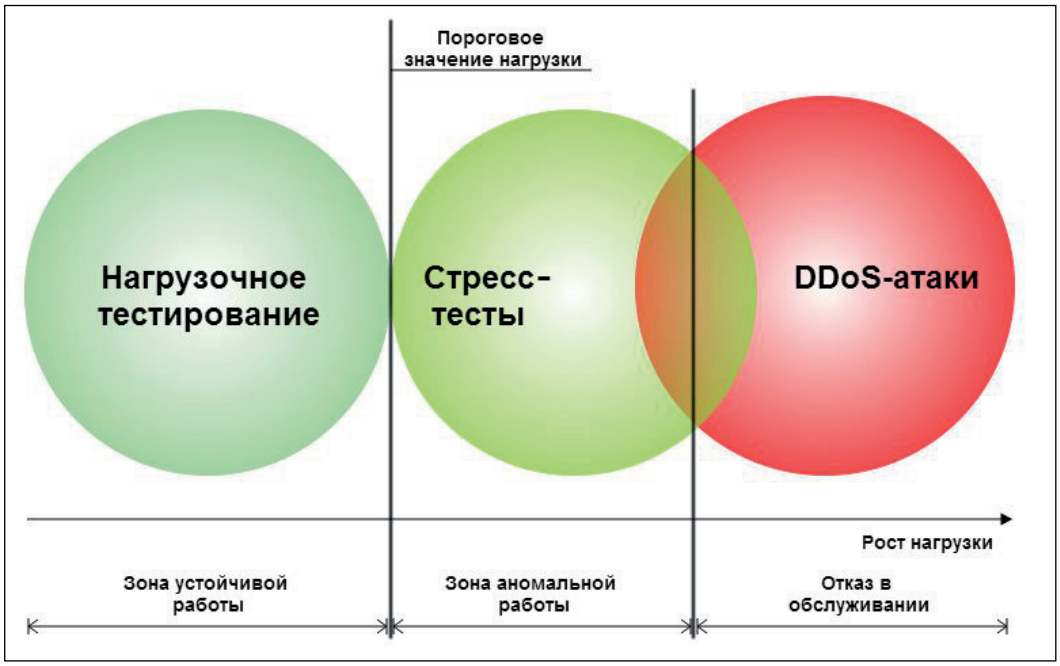

Рис. 1. Распределение множеств тестовых сценариев по мощности нагрузки на информационную систему

Как видно на рис. 1, нагрузочные тесты выполняются в рамках предельного значения нагрузки, а стресс-тесты, как и сценарии DDoS-атак, реализуются за пределами данного значения.

Однако цели у стрессового тестирования и DDoS-атаки совершенно разные. Задача стрессового тестирования — получить показатели предельной нагрузки тестируемой системы, в то время как DDoS-атака имеет цель «положить» атакуемый объект любыми эффективными методами и тем самым нарушить работоспособность целевой инфраструктуры.

Стрессовое тестирование оказывается необходимой процедурой, когда владельцу информационной системы нужно узнать, как она будет вести себя при аномальных нагрузках. Иногда есть необходимость выяснить, как будут справляться с нагрузкой имеющиеся средства защиты от DDoS-атак — для этого также используются процедуры стрессового тестирования.

Сбор информации

Стрессовое тестирование является частью процесса повышения уровня защищенности внешних ИТ-ресурсов целевой инфраструктуры и позволяет получить следующие результаты:
- определить текущие предельные значения нагрузки на внешние сервисы. Если мы знаем точку отказа нашей информационной системы, то для повышения отказоустойчивости мы можем оптимизировать имеющиеся процессы или внедрить новые. Другими словами, кто предупрежден, тот вооружен;
- проверить устойчивость внешних сервисов к некоторым сценариям распределенных атак, направленных на отказ в обслуживании. Взглянув на свой проект глазами злоумышленника, мы можем сделать какие-то выводы, например, о необходимости установки средств защиты от DDoS-атак или эффективности уже существующих решений.

В отличие от других этапов разработки веб-проекта, будь то отладка приложения или его функциональное тестирование (проверка работоспособности его функционала), нагрузочные тесты имеют важную особенность, которая делает нетривиальной задачей процедуру их реализации: тестирование проводится на реальной информационной системе, которая может находиться в процессе функционирования. Тестирование действующего проекта может стать причиной временного прекращения какого-либо бизнес-процесса.

Именно для решения задачи тестирования работающего веб-приложения или внешних информационных ресурсов, доступных из Интернета (почтовый сервер, FTP-сервер и т. п.), созданы специальные онлайн-сервисы нагрузочного тестирования.

Стресс-тест

Концепция «All as a Service» (ПО как сервис) позволяет владельцам веб-приложений избежать процедуры настройки сложных систем нагрузочного тестирования и подготовки облачной инфраструктуры и тому подобных действий. Все это уже сделано в фоновом режиме и предоставляется пользователю как онлайн-сервис: ввел пару «логин — пароль», задал параметры нагрузки, оплатил вычислительные мощности и знай себе фиксируй поведение своего веб-проекта.

Конфигурация нагрузочного тестирования в одном из рассмотренных проектов: задаем сценарий нагрузки, выбираем мощность нагрузки, оплачиваем используемые вычислительные ресурсы и получаем отчет.

Теперь владельцу какого-либо веб-ресурса, чтобы выяснить, как его веб-проект ведет себя при аномальных нагрузках, достаточно зарегистрироваться в одном из подобных сервисов. Особо ленивым некоторые сервисы нагрузочного тестирования предлагают моментальную проверку (без регистрации), возможности которой не слишком впечатляют, но позволяют быстро познакомиться с интерфейсом сервиса. Пример отчетности о процедуре нагрузочного тестирования изображен на рис. 2 и 3.

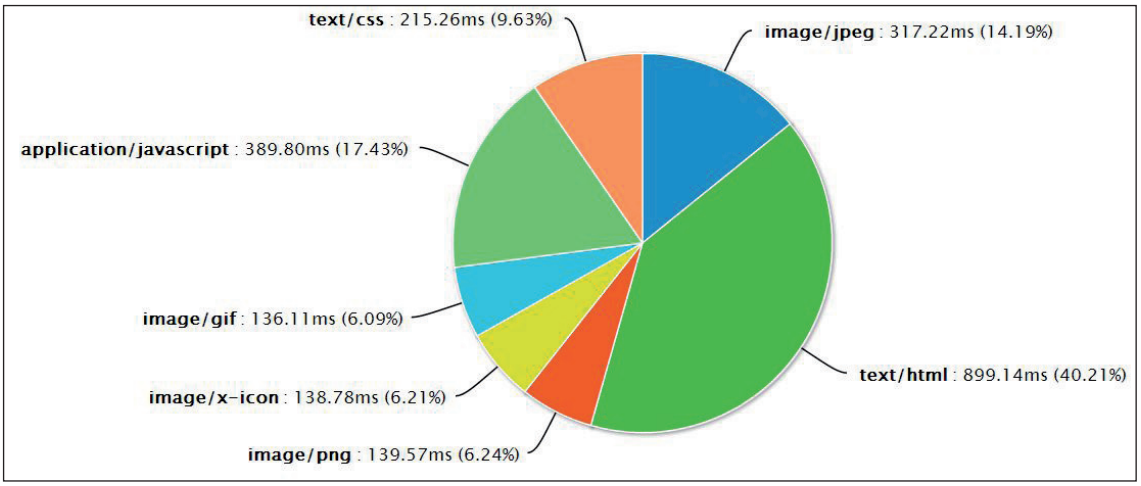

Рис. 2. Статистическая информация о процедуре нагрузочного тестирования

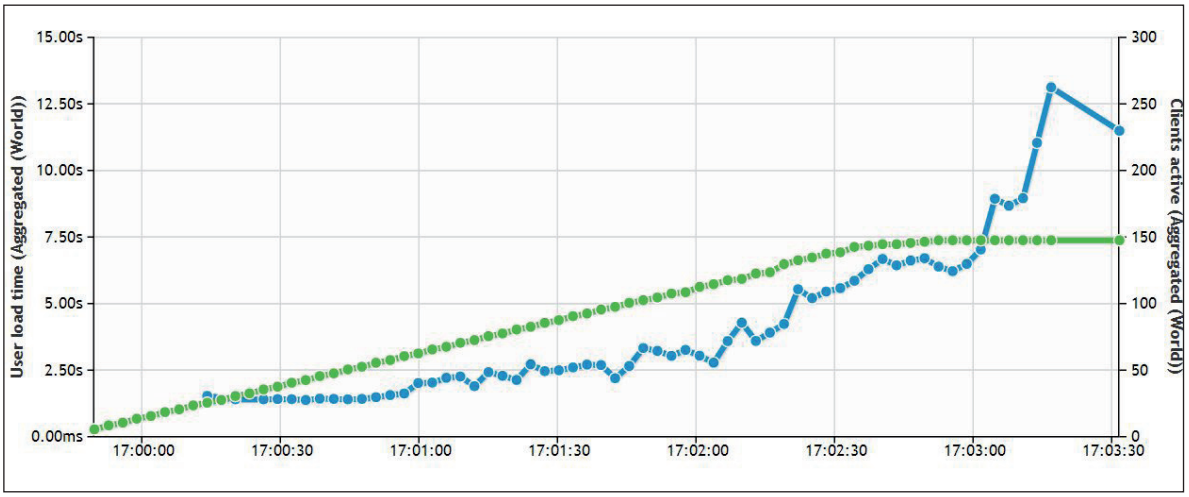

Рис. 3. Результат нагрузочного тестировании веб-приложения с помощью веб-сервиса

Нагрузочное тестирование как веб-сервис, несомненно, очень полезная и удобная процедура. Однако данная реализация процедуры тестирования не так безобидна, как может показаться на первый взгляд.

Тестирование или DDoS?

Ряд особенностей онлайн-сервисов нагрузочного тестирования позволяют взглянуть на них с позиции злоумышленника.

Для эксперимента выберем несколько популярных сервисов тестирования и в качестве объекта для тестов используем веб-приложение, которое «дрейфует» по не самым слабым виртуальным машинам (инстансам) облака Amazon EC2. Результат: даже в бесплатном тестовом режиме, когда пользователю предоставляется очень небольшое количество вычислительных ресурсов сервисов, нагрузки оказалось достаточно, чтобы заметно увеличить время отклика нашего блога.

Тестовый режим онлайн-систем нагрузочного тестирования позволяет имитировать посещаемость в 10000 пользователей в месяц, что может оказаться фатальным для многих небольших веб-проектов. Даже нагрузка в 50 пользователей за трехминутный интервал времени может внести аномалии в поведение какого-нибудь несложного веб-проекта.

При этом многие сервисы нагрузочного тестирования не требуют подтверждения того, что веб-ресурс тестирует его владелец, а не злоумышленник, нет никаких дополнительных привязок к телефонному номеру или кредитной карте.

Так, из шести рассмотренных нами сервисов тестирования только на одном просят разместить на тестируемом ресурсе специальный файл, получив доступ к которому сервис убедится, что администратор тестируемого ресурса уведомлен о процедуре. Более того, два из рассмотренных веб-сервисов позволяют осуществить нагрузочное тестирование вообще без регистрации, пользователю достаточно ввести URL тестируемого ресурса.

Простота использования данных инструментов дает возможность анонимно «протестировать» чужой веб-проект без регистрации и согласия на тест со стороны владельца тестируемого ресурса. Тот факт, что тестирование без регистрации является еще и бесплатным, может сделать эти сервисы очень заманчивым инструментом для DDoS-атак.

Новые возможности для злоумышленников

На наш взгляд, онлайн-сервисы нагрузочного тестирования могут являться инструментом для анонимного осуществления некоторых сценариев DDoS-атак. Быстрое создание сценариев нагрузки, простота и понятность в сочетании с пулом вычислительных ресурсов — вот особенности такой «бот-сети». Злоумышленник легко может использовать несколько независимых учетных записей в онлайн-сервисах нагрузочного тестирования, назначить им одно и то же время нагрузки на атакуемый сайт.

Известно, что наиболее эффективными являются такие DDoS-атаки, при которых отличить легитимный трафик от нелегитимного (генерируемого ботами) практически невозможно. Достаточно представить, что количество читателей блога возросло со ста человек в день до ста тысяч и при этом все ведут себя так, как положено рядовому пользователю, — тратят время на «ознакомление» с содержимым страницы, пытаются писать комментарии, просматривают картинки и являются географически независимыми друг от друга.

Некоторые сервисы предоставляют демонстрационную нагрузку вообще без регистрации, а это может означать, что владелец какого-нибудь «ущербного» ботнета из 50—100 зомби с помощью таких сервисов может в сотни раз увеличить эффективность DDoS-атаки. Один бот генерирует 10 независимых запросов на нагрузочное тестирование в различные веб-сервисы. Те, в свою очередь, независимо друг от друга инициируют сотни запросов. Результат: целевой ресурс задыхается от объемов вполне «легитимного» трафика.

Заключение

Как же можно избежать нелегитимного использования ресурсов сервиса нагрузочного тестирования? Для начала отметим, что владельцы подобных сервисов снимают с себя ответственность за нелегитимное использование своих разработок в пользовательском соглашении. Возможный вариант формулировки:

«Сервис нагрузочного тестирования позволяет получить актуальную информацию о состоянии целевой информационной среды. При этом разработчики Сервиса не несут ответственность за неправомерное использование вычислительных ресурсов, которые предоставляет Сервис».

Однако избежать неправомерного использования данных сервисов все же можно. Для этого каждый сервис нагрузочного тестирования должен запрашивать согласие на тест от владельца тестируемой системы. Например, можно просить его разместить какой-нибудь уникальный код или специальный баннер на тестируемом веб-ресурсе, только после чтения которого будет произведена нагрузка. В дополнение к этому можно использовать CAPTCHA (технология аутентификации действий) при работе с сервисом. Подобные процедуры верификации заметно усложнят процесс отправки автоматизированных запросов для генерации нагрузки, которые могут осуществлять роботы.

СПИСОК ЛИТЕРАТУРЫ:

1. *Гольцев Ю., Гордейчик С.* Abuse their clouds. Облачные вычисления глазами пентестера. ЗАО «Позитив Текнолоджис». 2011 [Электронный ресурс]. URL: http://www.ptsecurity.ru/download/clouds_полный_ED.pdf (дата обращения: 08.10.2013).
2. *Amazon*. Amazon Elastic Compute Cloud (Amazon EC2). Amazon. 2012 [Электронный ресурс]. URL: http://aws.amazon.com/ec2 (дата обращения: 08.10.2013).
3. *Лозовюк А.* Заоблачные вычисления: Cloud Computing на пальцах. Медиакомпания «Gameland». 2009 [Электронный ресурс]. URL: http://www.xakep.ru/post/49024 (дата обращения: 20.09.2013).

REFERENCES:

1. *Goltsev Y., Gordeychik S*. Abuse their clouds. Positive Technologies. 2011 [Web Source]. URL: http://www.ptsecurity.ru/download/clouds_полный_ED.pdf.
2. *Amazon*. Amazon Elastic Compute Cloud (Amazon EC2). Amazon. 2012 [Web Source]. URL: http://aws.amazon.com/ec2.
3. *Lozovyuk A.* Zaoblachniye Vichisleniya: Cloud Computing na paltsah. Gameland. 2009 [Web Source]. URL: http://www.xakep.ru/post/49024.