ватели решат задачу получения доступа к необходимым гидрометеорологическим данным, их хранению и обработке.

Список литературы

1. Код для оперативной передачи данных приземных метеорологических наблюдений с сети станций Росгидромета. Режим доступа: http://meteork.ru/doc/serv/synop.pdf (дата обращения 15.03.2015).
2. Ботыгин И.А., Попов В.Н. Архитектура распределенной файловой системы // Интернет-журнал «НАУКОВЕДЕНИЕ» 2014. № 6 http://naukovedenie.ru/PDF/137TVN614.pdf (доступ свободный). Загл. с экрана. яз. рус., англ. DOI: 10.15862/137TVN614.
3. Botygin I.A., Popov V.N., Tartakovsky V.A., Sherstnev V.S. Architecture of scalability file system for meteorological observation data storing // Proc. of SPIE, 21st International Symposium Atmospheric and Ocean Optics: Atmospheric Physics. – 2015. – Vol. 9680. – pp. 96800J-1– 96800J-4. – doi: 10.1117/12.2205749.

УДК 004

КЛАССИФИКАЦИЯ DDOS-АТАК И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

Фролов С.Г., Демин А.Ю.
Научный руководитель: Демин А.Ю.

Национальный Исследовательский Томский политехнический университет,
634050, Россия, г. Томск, пр. Ленина, 30
E-mail: sgf2@tpu.ru

DDoS is the most popular type of attack on the company for disabling its service. This article presents classification of the most popular types of DDoS and methods of defending and preventing from it.

***Key words**: DoS attack, DDoS attack, defending methods, methods of prevention of DDoS.*

***Ключевые слова**: DoS attack, DDoS attack, методы защиты, методы профилактики DDoS-атак.*

DoS-атака или атака типа «отказ в обслуживании» направлена на вычислительную систему с целью создать такие условия, при которых пользователи системы не могут получить данные к определенным ресурсам или сервисам. Одновременная атака с большого числа компьютеров свидетельствует о *DDoS*-атаке – распределенной атаке типа «отказ в обслуживании». Атаки выполняются с помощью зараженных специальными программами компьютеров, которые часто называют «компьютерами-зомби» [1].

Классификация *DDoS*-атак и защита от них

Существует очень много видов *DDoS*-атак, у каждой свой характер и способы борьбы. Наиболее часто встречающиеся виды представлены ниже.

***UDP* флуд.** Тип *DDoS*-атаки, при которой атакующий перегружает случайный порт на хост-машине, используя *UDP*-пакеты. Атакуемое оборудование проверяет, использует ли этот порт какое-либо из запущенных приложений или процессов, и если не находит, то отправляет ответ «*Destination Unreachable*». Так как система получает все больше и больше

UDP-пакетов и отвечает на них, то в скором времени она становится недоступной для пользователей. Простейшая защита – блокировка *UDP*-трафика.

***ICMP* флуд.** Затопление атакуемого компьютера пакетами *ICMP*. Система должна ответить на такой пакет, тем самым создаётся большое количество пакетов, которые снижают производительность (пропускную способность) канала. Защита – блокировка *ICMP*-трафика. Пропинговать сервер будет невозможно, зато он будет доступен и одной лазейкой будет меньше [2].

***SYN* флуд.** Тип *DDoS*-атаки, которая использует часть нормального «тройного рукопожатия», присущего *TCP*-соединению, чтобы задействовать все ресурсы атакуемой машины и сделать ее недоступной для окружающих. В большинстве случаев, при *SYN* флуде атакующая сторона посылает запросы на TCP-соединение быстрее, чем атакуемая сторона может их обработать, что забивает сетевой канал и делает недоступным конечное оборудование.

***MAC* флуд.** Тип сетевой атаки, при которой атакующая сторона, подключенная к какому-либо порту маршрутизатора, засыпает интерфейс маршрутизатора большим количеством *Ethernet*-пакетов с разными поддельными *MAC*-адресами источников.

Атака нулевого дня. Атака, основанная на использовании уязвимости нулевого дня, то есть применяемая в период, когда данная уязвимость остается неизвестной и против которой пока не разработаны защитные механизмы.

Деградация сервиса. Основная суть данного типа – множественная симуляция действий реальных людей. Самый простой вариант – частые запросы одной и той же страницы сайта. Защита – временная блокировка страницы с выдачей сообщения об ошибке.

Общий принцип защиты – анализ поведения и отсеивание подозрительных *IP*-адресов на уровне брандмауэра. Чем более сложный алгоритм используется атакующей программой, тем сложнее выявить паразитный трафик и тем больше ложных срабатываний, блокирующих доступ к ресурсу реальным пользователям.

Методы профилактики

До мелочей изучите свою сетевую конфигурацию. У каждого сервиса есть характерные черты использования сети: объём и типы используемого трафика и т. п. Изучите стандартные характеристики и регулярно отслеживайте текущую картину. Вы сможете заранее принять необходимые меры, если будете знать, что атака начинается.

Держите под рукой необходимые контакты. Вы должны точно знать, к кому обратиться в случае, если Вы уже находитесь под атакой или ощущаете её приближение. Искать того, кто смог бы помочь – это последнее, что необходимо, когда беда уже пришла.

Имейте четкий план действия при атаке. Необходимо иметь краткую инструкцию, что делать в случае атаки, по аналогии с планом эвакуации. Она должна быть прописана на бумаге и висеть на видном месте. В момент атаки на смене может оказаться сотрудник без практического опыта решения текущей проблемы, и чрезвычайно важно, чтобы у него не возникало необходимости долго думать и искать решение.

Тренируйтесь на учебных тревогах. *DDoS* – такая же чрезвычайная ситуация, как и пожар. Поэтому необходимо устраивать периодические проверки навыков оперативной обработки незапланированных ситуаций. Это поможет усвоить и закрепить навыки и обнаружить слабые места в процедурах.

Заранее блокируйте неиспользуемые порты. Заблаговременно заблокируйте на брандмауэре всё лишнее, что таким образом уменьшит поле для атаки. Если Вы имеете узкий круг проверенных, важных клиентов, добавьте их адреса в белый список, чтобы в случае атаки не отсеивать их запросы.

Знайте, где блокировать. Блокировать трафик на брандмауэре или на роутере? Подключать аппаратный или внешний сервис фильтрации трафика? Решите эти важные вопросы заранее. Исключите метод проб и ошибок тогда, когда на него определенно нет времени.

Список литературы

1. DDoS-атаки. Причины возникновения, классификация и защита от DDoS-атак [Электронный ресурс]. URL: http://efsol.ru/articles/ddos-attacks.html
2. Флёнов М. Linux глазами хакера. – СПб.: БХВ-Петербург, 2010. – 480 с.

УДК 004

РАСПОЗНАВАНИЕ ИЗОБРАЖЕНИЙ ЛИЦ НА ОСНОВЕ КЛАСТЕРИЗАЦИИ

Горемыкина Д.С.
Научный руководитель: Немировский В.Б., доцент каф. ИПС ИК ТПУ

Национальный Исследовательский Томский политехнический университет,
634050, Россия, г. Томск, пр. Ленина, 30
E-mail: goremykina2008@mail.ru

This article describes the use of clustering for face recognition image. Clustering was performed using a recurrent neural network used at two stages of the recognition process. The algorithm includes the recognition process itself perform clustering pixel brightness image, calculating image information close proximity and clustering measures to in order to obtain the cluster containing the original similar images.

Ключевые слова: *изображение, рекуррентная нейронная сеть, кластеризация, распознавание изображений.*

Key words: *image, recurrent neural network, clustering, recognition of images.*

Задача распознавания изображений лиц является ключевой для процесса распознавания лиц по предъявленному образцу в криминалистике, службах и системах контроля, и других подобных системах. Значительная часть современных технологий распознавания изображений основана на количественной оценке близости изображений по значениям некоторой функции, называемой расстоянием. При таком подходе необходимо определить, какую характеристику изображения выбрать для оценки близости изображений, и какую функцию использовать в качестве расстояния. Применение кластеризации яркостей пикселей изображения позволяет получить распределение относительных мощностей кластеров яркости. В настоящей работе такое распределение использовалось в качестве характеристики изображения. Вопрос о выборе функции для количественной оценки близости изображений рассмотрен далее.

Кластеризация яркостей изображения

В работе [1] предложена и рассмотрена процедура сегментации изображений, основанная на кластеризации значений яркости пикселей изображения рекуррентной нейронной сетью.

В [1] указано, что нейронную сеть с локальной обратной связью нейронов входного слоя можно использовать для кластеризации данных. Обратная связь приводит к одномерно-