АССОЦИАЦИЯ ДОКУМЕНТАЛЬНОЙ ЭЛЕКТРОСВЯЗИ

НОРСИ-ТРАНС

Закрытое Акционерное Общество

“КРОЗ: Аппаратно-программный комплекс для автоматического определения и блокировки DDoS атак”.

Докладчик: Хохлов Р.В.

Дата: 4 октября 2017 года

НОРСИ-ТРАНС
Закрытое Акционерное Общество

ЗАО «НОРСИ-ТРАНС» - одна из лидирующих компаний России на рынке разработки и внедрения информационно-аналитических систем.

Направления деятельности Компании:

- Полный спектр решений СОРМ (СОРМ 1, СОРМ 2, СОРМ 3);
- Системы корпоративной информационной безопасности;
- Решения по защите сетей связи от DDoS-атак;
- Решения контентной фильтрации для ограничения доступа к доменным именам, указателям страниц сайтов и сетевым адресам сети Интернет;
- Аналитические системы и платформы;
- Решения для бизнес-аналитики;
- Аппаратно-программные комплексы высокоскоростного хранения и аналитической обработки данных;
- Аппаратные решения для мониторинга и управления сетью;
- Комплексные решения для защиты и анализа состояния сети;
- Комплексные системы защиты от сетевых атак для Дата-центров.

Определение DoS / DDoS атак.

DoS (от англ. Denial of Service — отказ в обслуживании) — это хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам, либо этот доступ затруднён.

Новости DoS / DDoS атак.

- 3DNews: В 2015 году было зафиксировано почти 200 тыс. попыток кибератак на столичные информсистемы;
- 3DNews: DDoS-вымогательство становится популярным среди злоумышленников;
- Cnews: Крупнейшая в истории DDoS-атака была направлена на сеть доставки контента CloudFlare. Представители компании сообщили, что мощность трафика превысила 400 Гбит/с. Для проведения атаки был использован набирающий популярность в последнее время метод с задействованием серверов синхронизации времени;
- RBC:Сбербанк не исключает повторения крупных атак, подобных произошедшей в декабре 2014 года, которая спровоцировала повышенный спрос на наличные. Об этом «РИА Новости» сообщил зампред правления Сбербанка Станислав Кузнецов.

Совместная командно-штабная тренировка "Кибер-Антитеррор-2016" (14 апреля 2016 г, Минск, Республика Беларусь)

Целью тренинга стала подготовка сотрудников оперативных подразделений органов безопасности и специальных служб стран Содружества к выполнению совместных практических задач первого этапа антитеррористического учения «Кибер-Антитеррор-2016» по предупреждению, выявлению и пресечению террористических актов, совершаемых с применением информационно-коммуникационных технологий.

До участников были доведены: методика взаимодействия при выявлении и пресечении кибератак, совершаемых с применением информационно-коммуникационных технологий и вредоносных программ; способы и порядок работы с информационными системами коллективного пользования при проведении мероприятий; особенности и порядок работы оперативно-следственных подразделений при расследовании компьютерных инцидентов в телекоммуникационных сетях.

В совместной командно-штабной тренировке приняли участие представители компетентных органов Азербайджана, Армении, Беларуси, Казахстана, Кыргызстана, Молдовы, России и Узбекистана.

http://www.cisatc.org/133/162/816.html

Примеры DDoS атак

- Атака на HTTP-сервис;
- Атака на DNS-сервис;
- Атака на NTP-сервис.

При атаке на HTTP-сервис определяется самая долго открывающаяся страница сайта, например, страница, осуществляющая SQL-запрос к базе данных сайта, и данная страница запрашивается со всех атакующих сторон, насколько позволяет производительность атакующего оборудования. Обработать такое количество HTTP-запросов к данной странице объект не может, и HTTP-сервис становится не доступен на время атаки.

При атаке на DNS-сервис злоумышленник подменят собственный Source IP на SourceIP объекта и обращается к публичным DNS-серверам (GoogleDNS, YandexDNS, FREEDNS и т.д.) так часто, насколько позволяет атакующее оборудование.

Публичные DNS-сервера начинают отвечать DNS-серверу объекта и создают шквал трафика, с которым DNS-сервер объекта не справляется и становится не доступен на время атаки.

Атака на NTP-сервис осуществляется по аналогичному предыдущему алгоритму с подменой Source IP, но теперь шквал трафика создают публичные NTP-сервера (ntp1.stratum2.ru, ntp2.stratum2.ru и т. д.) с которым NTP-сервер объекта не справляется и становится недоступен на время атаки.

Основные существующие проблемы и возможные векторы DDoS атак в сети Интернет

- Заполнения пропускной способности uplink – клиент/провайдер не может ничего сделать с такой атакой своими силами;
- Spoofing (TCP, UDP) – таблицы пиров переполняются (миллиарды записей);
- Атаки на уровень приложения – расходование всех доступных ресурсов сервиса;
- Постоянное совершенствование алгоритмов атак с помощью бот-сетей – имитация наплыва обычных пользователей, сложность/невозможность поведенческого выявления ботов;
- Массированные атаки на критические интернет сервисы (например DNS и т.п.) – сложности использования существующих протоколов/сервисов в инфраструктуре IoT;

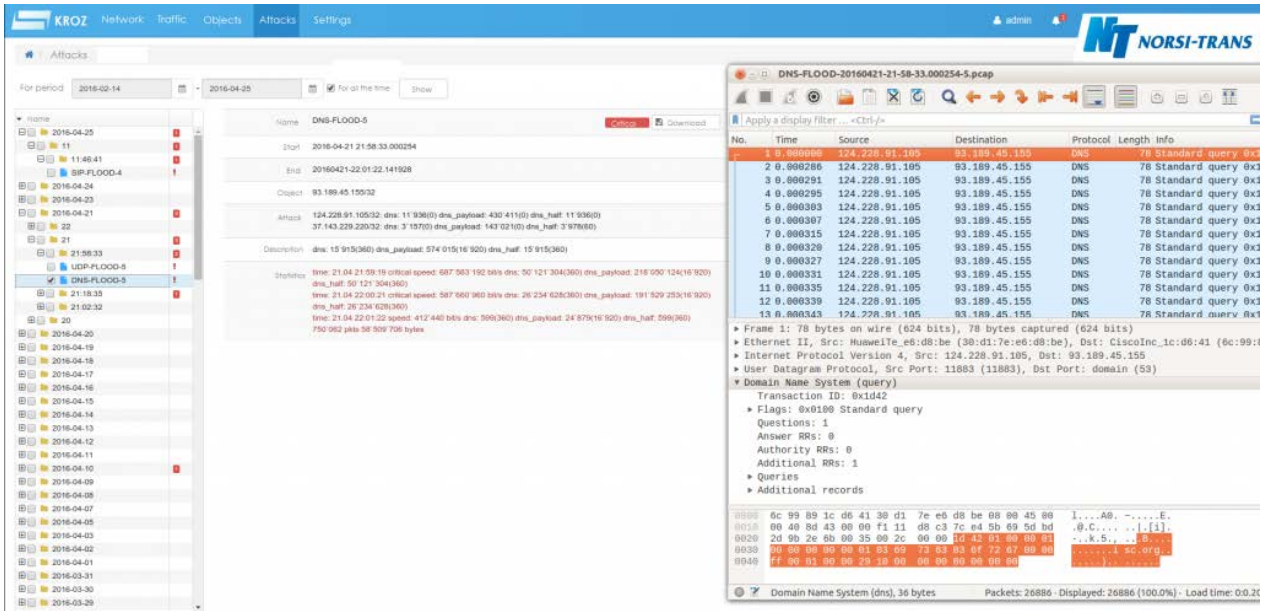
Постоянный рост числа пользователей (мобильные устройства, IoT и т.д.) Интернета – ведет к многократной актуализации проблем, описанных выше.

НОРСИ-ТРАНС
Закрытое Акционерное Общество

"КРОЗ" – комплексное решение для обеспечения законности в сетях операторов связи. Анализатор DDoS и аномалий сети.

КРОЗ - это аппаратно-программный комплекс, предназначенный для мониторинга и наблюдения за состоянием сети оператора связи, отслеживания сбоев и анализа трафика в режиме реального времени.

КРОЗ - это Аппаратно-программный комплекс автоматического обнаружения и блокирования DDOS-атак.



АССОЦИАЦИЯ ДОКУМЕНТАЛЬНОЙ ЭЛЕКТРОСВЯЗИ

Собственное решение ЗАО «НОРСИ-ТРАНС» в области защиты – КРОЗ antiDDoS

- Имеем эффективные подходы к решению самых сложных проблем защиты от DDoS;
- Работаем в каналах 10-100-1000 Гбит/с: подключение inline либо outline(BGP);
- Возможности разнесения физического размещения серверов центров очистки и анализа;
- Имеем аналитическую систему для выявления причин и закономерностей DDoS, ретроспективный анализ;
- Собираем отчеты и трафик по каждой атаке;
- Участвуем в защите собственного оператора связи и следим за изменениями профиля/вектора атак.

"КРОЗ“: Функционал

- Фоновый статистический контроль метрик сети с целью обнаружения профиля злоумышленника;
- Автоматическое блокирование трафика злоумышленника во всей контролируемой сети;
- Настраиваемые уровни и режимы контроля для выделенных подсетей, личный кабинет для клиентов оператора;
- Блокирование атак, исходящих от клиентов;
- Специальные функции защиты от широко распределенных атак;
- Возможность ручного анализа и задания правил;
- Возможность распределения сети зондов;
- Возможность активной защиты WEB-сервисов на уровне прикладных сессий;
- Детектирование широкого спектра DDoS-атак;
- Отчеты в режиме реальном времени;
- Автоматическая запись дампов трафика атак, ретроспективный анализ.

"КРОЗ“: Базовый список отражаемых атак

- Сканирование информационно-телекоммуникационных ресурсов;
- Нелегитимный трафик на невостребованный протокол и/или порт (UDP Flood, ICMP Flood);
- Атака фрагментами IP-пакетов с некорректным содержимым;
- Инициация соединения на транспортном уровне стека TCP/IP (TCP Syn Flood);
- Установка полноценного TCP-соединения с его дальнейшим сбрасыванием без обмена данными внутри socket (TCP Connection Flood);
- Атака с использованием протокола DNS и генерацией легитимных запросов/ответов, в том числе DNS Amplification;
- Атака с использованием протокола NTP и генерацией легитимных запросов/ответов, включая NTP-Amplification;
- Отправка данных по протоколу HTTP/1.0 или HTTP/1.1 вне спецификации протокола;
- Атака на SIP-сервис;
- Атака на SMTP-сервис;
- Атака на FTP-сервис;
- Spoofing атаки любого уровня сложности, такие как TCP и UDP;
- Широко распределенные атаки TCP, UDP (в том числе HTTP Flood);
- Распределенная атака на специфический сервис Заказчика.

"КРОЗ“: Технические характеристики

Зонд 1RU с возможностью обработки до 10 Гбит/с транзитного трафика, включая различные варианты floods;
Возможность безопасного включения в разрыв канала либо в схему BGP маршрутизации;
Аппаратные средства включения с функцией отказоустойчивости;
Возможность аппаратной балансировки нагрузки с каналов 40 Гбит/с и 100 Гбит/с.

Опыт ETSI в области стандартизации и изучении вопросов безопасности IT

- Создан технический комитет для изучения вопросов безопасности в IT: CYBER;
- Совместно с 3GPP создан документ, позволяющий оценить влияние атак на узел Интернет: http://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/04.02.03_60/ts_10216501v040203p.pdf (будет импортирован в CYBER);
- На данный момент разрабатывается новая версия документа, в котором будут описаны современные механизмы борьбы с атаками;
- В ETSI также занимаются изучением уязвимостей Интернет: http://www.etsi.org/deliver/etsi_gs/NGP/001_099/001/01.01.01_60/gs_NGP001v010101p.pdf

"КРОЗ" – комплексное решение для обеспечения законности в сетях операторов связи и Интернет-провайдеров. Фильтрация запрещенных URLs.

В соответствии с законом от 28 июля 2012 г. №139-ФЗ "О внесении изменений в ФЗ “О защите детей от информации, причиняющей вред их и здоровью и развитию” и отдельными законодательными актами РФ" об ограничении доступа к ресурсам сети Интернет, содержащим информацию, распространение которой в РФ запрещено, оператор обязан блокировать доступ в соответствии с реестром запрещенных URL, доменов и сайтов.

Решение "КРОЗ" разработано в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации", Приказом Роскомнадзора от 17.07.2014 №103 "Об утверждении Порядка предоставления операторами связи технических средств контроля за соблюдением операторами связи требований Федерального закона от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации"".

- Автоматизированное обновление из реестра (в том числе Реестр РосКомНадзора, ресурсы из списка МинЮста) и блокировка URL;
- Подробная статистика по блокированным URL (по каждой попытке доступа), возможность экспорта;
- Корректная проверка URL, включая все альтернативные формы записи;
- Возможности HTTP-перенаправления или отправка информационной HTML-страницы о блокировании URL.

НОРСИ-ТРАНС
Закрытое Акционерное Общество

Спасибо за внимание !

Роман Хохлов,

ЗАО «Норси-Транс»

email: r.khokhlov@norsi-trans.ru

тел: +7 916 794 81 02; +7 495 748-74-83

АССОЦИАЦИЯ ДОКУМЕНТАЛЬНОЙ ЭЛЕКТРОСВЯЗИ