Сценарии смягчения последствий DDoS-атак

Область DDoS-атак: инфраструктура DNS ccTLD

Семинар TLD-OPS

Редакция 1.0 - 25 апреля 2018 года

Обзор семинара

Целью данного семинара было изучить, каким образом члены TLD-OPS могут взаимодействовать, чтобы разработать правила смягчения последствий атак типа «отказ в обслуживании» (DDOS-атак). В центре внимания были DDoS-атаки, нацеленные на официальную инфраструктуру DNS со схемой Unicast и Anycast под управлением ccTLD и партнеров, поставляющих DNS.

Повод

Данный семинар проведен в ответ на семинар TLD-OPS по смягчению последствий DDoS-атак, проведенный в ходе конференции ICANN58 в Копенгагене 12 марта 2017 года. Поскольку DDoS-атаки могут оказывать серьезное воздействие на цель (и наносить сопутствующий ущерб), Постоянный комитет TLD-OPS считает важным задействовать коллективный опыт сообщества TLD-OPS для разработки и документального оформления концепции, чтобы обеспечить оптимальную подготовку ccTLD к реагированию на DDoS-атаки.

Данный семинар способствовал ведению диалога благодаря обмену опытом, обсуждению и генерации идей.

Семинар TLD-OPS по смягчению последствий DDoS-атак №2 – ICANN61, 29-10-2017, общие замечания

На этом семинаре мы собрали меньше человек: 22. Это позволило развить неплохую динамику и степень взаимодействия. Мы собрались перед одним флипчартом, ознакомились с результатами предыдущего семинара и расширили каждую тему, чтобы сосредоточиться на тех элементах, которые вошли бы в состав руководства, для каждого этапа жизненного цикла. Результаты, записанные на флипчарте, приведены в настоящем документе.

Жизненный цикл «эффективного» смягчения последствий DDoS-атак:

- определить,
- защитить,
- обнаружить,
- ответить,
- восстановить.

Объем и содержание настоящего документа не предусматривают разработку комплексной концепции безопасности для смягчения последствий DDoS-атак. Его задача – подчеркнуть важные компоненты каждого этапа жизненного цикла для ccTLD, чтобы добиться эффективного смягчения последствий DDoS-атак (по мере реализации).

На семинаре было сказано, что всегда хорошо реализовывать лучшие практики, например, производственных операций обслуживания и управления информационной безопасности (кибербезопасности) библиотеки передового ИТ-опыта (ITIL).

ОПРЕДЕЛИТЬ.

Определить – значит задокументировать и понять инфраструктуру DNS своего ccTLD до возникновения атаки, чтобы знать: кому звонить, на кого положиться, кого уведомить (и каналы передачи разрешения проблем на более высокий уровень). Наладьте прочные отношения со своими ISP, поставщиками, правительством, средствами массовой информации, владельцами доменов и интернет-пользователями вашего ccTLD. Эту работу необходимо выполнять на регулярной основе, прежде чем придется отражать атаку.

КОНТАКТЫ	
Руководство ccTLD	Должность, Ф. И. О., телефон, домашний телефон, домашний адрес электронной почты (Председатель - Правление)
Номер экстренного вызова IANA	+1 (310) 306-6308 (будет обновляться)
Поставщики Anycast	Адреса электронной почты и номера телефонов SOC/NOC, контактные номера телефонов
Интернет-провайдер транзитных услуг	Адреса электронной почты и номера телефонов SOC/NOC, контактные номера телефонов
Местный интернет-провайдер	Адреса электронной почты и номера телефонов SOC/NOC
Группа CERT	Адреса электронной почты и номера телефонов SOC/NOC Ф. И. О. контактного лица, номер телефона, адрес электронной почты
Основные операторы преобразователей (рекурсивные)	IP-адреса Оператор, адрес электронной почты и номера телефонов
Список контактов TLD-OPS	Доступ к списку контактов TLD-OPS
СМИ	Ф. И. О. контактного лица, номер телефона, адрес электронной почты
Регулирующий орган	Ф. И. О. контактного лица, номер телефона, адрес электронной почты
Поставщики ПО	Ф. И. О. контактного лица, номер телефона, адрес электронной почты
Консультант по криминалистике	Ф. И. О. контактного лица, номер телефона, адрес электронной почты
Владельцы доменов	Эффективный способ связи с владельцами доменов

Другие контактные лица	

Четкое документирование инфраструктуры DNS вашего ccTLD:

Крайне важно четко документировать инфраструктуру DNS вашего ccTLD: какие DNS-серверы у вас в работе, их физическое местоположение, сетевые подключения, провайдеры транзитных услуг, подключения к IXP, провайдеры Anycast, потенциал каждого канала передачи транзитного трафика и IXP.

Этот актив вам нужно защищать.

DNS-сервер ccTLD, адреса IPv4 и IPv6.

- Example…
- ;; AUTHORITY SECTION:
- dk. 172800 IN NS a.nic.dk.
- dk. 172800 IN NS b.nic.dk.
- …
- ;; ADDITIONAL SECTION:
- a.nic.dk. 172800 IN A 212.88.78.122
- b.nic.dk. 172800 IN A 193.163.102.222
- b.nic.dk. 172800 IN AAAA 2a01:630:0:80::53
- …

Точная топология DNS, сети и сервера:

Задокументируйте архитектуру сети, сервера и ПО для инфраструктуры DNS вашего ccTLD и регулярно ее обновляйте.

<Вставьте сюда схемы сети>

- Оставьте ссылки на схемы сети и топологии

IP-адреса скрытого мастер-сервера

Скрытый мастер-сервер	
IP-адрес	Получите доступ к сведениям о списке (если нужно добавить нового провайдера)
Как добавить	Быстрые действия для добавления новых DNS-серверов…

Инфраструктура подписи DNSSEC

Добавьте сюда сведения об инфраструктуре DNSSEC и хранении/защите ключа.

Важные рекурсивные DNS-серверы, использующие ваш ccTLD (например, крупные рекурсивные DNS-серверы ISP в вашей стране, обслуживающие большое население)

Рекурсивный	
Название интернет-провайдера	IP-адреса

Как внести в белый список	Быстрые действия для добавления в белый список рекурсивных DNS-серверов?

Поддержание актуальности информации:

Доступ к важной информации	
Сейф с паролями	Местоположение (для входа в систему маршрутизаторов и серверов)
Склад оборудования	Местоположение (укажите IP-адрес, наименование)
Коммуникационный план	Местоположение (как связаться, сообщить)
Роли и обязанности	Местоположение (кто, что и когда делает)
Планы аварийного восстановления, копирования данных	Местоположение

Процесс управления рисками:

Определить риски и сопутствующее воздействие, а также вероятность их возникновения, и указать их в анализе последствий для деятельности для служб разрешения проблем ccTLD. Создать процедуру для регулярного анализа и обновления данного документа.

Изменение процесса управления:

Крайне важно, чтобы эта информация не устаревала; внедрите процессы, которые будут обеспечивать актуальность этой информации. Создайте ежеквартальный процесс для анализа и обновления настоящего документа.

ЗАЩИТИТЬ.

ЗАЩИТИТЬ – значит разработать и внедрить соответствующие меры защиты, которые обеспечат предоставление официальных служб DNS вашего ccTLD и позволят сдержать или ограничить воздействие DDoS-атаки.

Особенно что касается защиты от DDoS-атак, результатом этапа ЗАЩИТЫ является разработка и внедрение лучших практик по защите, например, средств управления доступом, защитных технологий, разнообразия и архитектуры DNS. Данный раздел посвящен определению лучших практик (процессов) по защите технологий, людей и партнеров.

Технология:

Внедрить меры защиты для обеспечения надежной и стабильной работы.

Списки доступа:

- список управления доступом где необходимо, разрешать трафик только на порт-адресат 53 (TCP/UDP),
- список управления доступом для управления по дополнительному каналу.

Anycast:

- внедрить глобальную топологию DNS со схемой Anycast, чтобы повысить отказоустойчивость при предоставлении услуг,
- развернуть локальные узлы Anycast, чтобы повысить отказоустойчивость при предоставлении услуг (узлы DNS без глобального транзитного трафика), по возможности, прибегнув к следующим способам:
    - расширение глобальной DNS со схемой Anycast с помощью локальных узлов Anycast, которые обслуживают конкретное «важное» сообщество преобразователей (крупный внутренний ISP, правительство, региональные сети),
    - добавление локальных узлов Anycast на ключевых IXP.

Прочие меры защиты:

- разнообразие ПО DNS-сервера (Bind, NSD, Knot и т. д.),
- сортировка дистанционно управляемых «черных дыр» (RTBH),
- аппаратное оборудование для смягчения последствий DDoS-атак,
- реализация РРЛ (обязательно),
- защита интерфейса административного управления (отдельный физический порт/кабель,транзитный трафик, VPN-туннель и т. д.),
- достаточные системные ресурсы (с точки зрения пропускной способности),
- достаточная сетевая связность и диверсификация в выборе провайдера услуг (ISP, IXP и т. д.).

Люди/процесс:

Обучить ИТ-отдел

- тренинги по знанию и пониманию мер безопасности,
- ежегодное упражнение <- поделиться сценарием в листе рассылке TLD-OPS и моделирование DDoS-атаки,
- усиление защитных свойств конфигурации (лучшая практика и т. д.) и испытание на проникновение,

- как использовать внешние средства мониторинга DNS (например, DNSMON, DNS-OARC, BGPMon или аналогичные),
- отсутствие ручных изменений, используйте конфигурацию и изменяйте процесс управления,

заблаговременная работа с ISP (провайдеры транзитных услуг),

- выяснить, как они могут помочь смягчить последствия будущих DDOS-атак,
- убедиться, что они осознают важность вашего ccTLD.

Партнеры.

Работа с партнерами там, где могут пригодиться услуги смягчения последствий DDoS-атак:

- добавить сторонних постоянных провайдеров Anycast,
- обеспечить защиту аварийных сторонних провайдеров Anycast,
- исследовать службы устранения DDoS-атак.

ОБНАРУЖИТЬ.

ОБНАРУЖИТЬ – значит разработать и внедрить соответствующие мероприятия для обнаружения – своевременного – DDoS-атаки и определения объема и степени воздействия DDoS-атак. Чем лучше работает механизм обнаружения, тем эффективнее будут техники смягчения последствий.

Результатом этапа ОБНАРУЖЕНИЯ являются внутренние и внешние процессы мониторинга DNS и обнаружения.

Мониторинг:

Внутренние средства мониторинга

- трафик мониторинга SNMP (маршрутизатор, серверы, каналы передачи),
- отказоустойчивость уведомления о пороговом аварийном сигнале (смс, электронная почта),
- понимание нормальной работы каждого узла.
- Средства анализа DNS
- перехват PCAP (демонстрирует полную картину при возникновении инцидента, но при DDoS-атаке объемы трафика могут вызвать внутренний DoS, см. примечание ниже).

Внешние средства мониторинга

- внешний RIPE Atlas DNSMON (время отклика на запрос DNS, потеря запроса и тенденции),
- статистика канала передачи ISP транзитных услуг (реальное использование исходящего трафика на вашем узле DNS),
- мониторинг соблюдения SLA ICANN (API системы мониторинга ICANN (MoSAPI)) (все еще на начальной стадии внедрения для ccTLD),
- Netlabs 360 - https://ddosmon.net/.

Масштабируемые средства (функционал в условиях DDoS-атаки)

- PCAP, DDoS-атака может вывести из строя некоторые средства или отрицательно повлиять на их работу
    - процедура для временного отключения сбора данных при неблагоприятных условиях,
    - дистанционная передача журналов в режиме реального времени, чтобы не допустить потерю данных.

Определение типа атаки:

распознавание атаки,

- тип атаки,
- список классических атак, профилей и инструментов, а также мероприятий по смягчению последствий,
- источник (откуда исходит?),
- какие узлы (что затронуто?),
- каково реальное воздействие на интернет-пользователей?

ОТВЕТИТЬ.

ОТВЕТИТЬ – значит разработать и внедрить соответствующие мероприятия, чтобы принять меры в отношении обнаруженной DDoS-атаки. Функция ответа помогает смягчить последствия воздействия потенциальной DDoS-атаки.

Этап ОТВЕТА включает планирование ответа, установление связи, анализ и смягчение последствий.

Планы ответа:

НЕ ПАНИКОВАТЬ! Скорее всего, сообщество обнаружит DDoS-атаку на вашем ccTLD одновременно с вами и захочет помочь смягчить последствия.

- Установить связь.
- Продолжить анализ.
- Решить проблему.
- Сосредоточиться на корне проблемы.
- Задокументировать {что вы меняете и наблюдения}.

Коммуникационный план:

Коммуникация – главный элемент для смягчения последствий атаки.

Механизмы коммуникации	
Местная группа CERT	Свяжитесь с местной группой CERT, даже если атака полностью не определена
TLD-OPS	Отправьте электронное письмо по адресу tld-ops@dns-oarc.net Попросите помощи в дальнейшем определении атаки
Коммутатор телеконференции	Попросите TLD-OPS/ICANN активировать коммутатор телеконференции для совместной работы над смягчением последствий
Информирование	Попросите предоставить членам TLD-OPS доступ к альтернативному листу рассылке/группе, чтобы помочь смягчить последствия атаки
прочее	

ВОССТАНОВИТЬ.

ВОССТАНОВИТЬ – значит разработать и внедрить соответствующие мероприятия, содержащие планы по обеспечению отказоустойчивости и восстановлению любых возможностей или услуг, затронутых DDoS-атакой. Функция восстановления поддерживает своевременное возвращение к нормальной работе, чтобы уменьшить воздействие DDoS-атаки.

Этап ВОССТАНОВЛЕНИЯ включает планирование, усовершенствования, выводы и обмен информацией.

Восстановление:

- нейтрализация временных мер,
- возврат инфраструктуры DNS в исходное состояние,
- постоянные изменения документа,
- сбор примечаний.

Выводы:

- провести собрание, посвященное подведению итогов, с соответствующими (внутренними) заинтересованными сторонами,
- задокументировать:
    - что сработало,
    - что не сработало,
    - определить усовершенствования.

Усовершенствования:

- определить,
- оценить,
- поделиться,
- внедрить усовершенствования.

Обмен информацией:

- Донести до сведения партнеров, клиентов, сотрудников, владельцев доменов.