Столыпинский вестник

Научная статья
Original article
УДК 004.424

DDOS-АТАКИ И ЗАЩИТЫ ОТ НИХ

DDOS ATTACKS AND PROTECTION FROM THEM

Крыгин Никита Дмитриевич, студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), krigginnn@rambler.ru

Krygin Nikita Dmitrievich, bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), krigginnn@rambler.ru

Аннотация: Распределенный отказ в обслуживании с выкупом (RDDoS) — это DDoS-атаки с вымогательством: хакеры угрожают провести DDoS-атаки, если не будет выплачен выкуп. Хакер требует оплату, как правило, в виде криптовалюты, чтобы правоохранительные органы не могли отследить транзакцию.

Abstract: Distributed denial of service with ransom (RDDoS) is a ransomware DDoS attack: hackers threaten to carry out DDoS attacks unless a ransom is paid. The hacker demands payment, usually in the form of cryptocurrency, to prevent law enforcement from tracking the transaction.

Ключевые слова: DDoS-атака, хакеры, угрозы, информационная безопасность.

Keywords: DDoS attack, hackers, threats, information security

Как и обычная DDoS-атака, RDDoS заполняет серверы или сети поддельными запросами, которые не позволяют законным сетевым запросам достичь места назначения. Это может негативно сказаться на репутации бизнеса, нарушить работу, а в некоторых случаях привести к потере доходов. Тем не менее, рекомендуется не платить комиссию за вымогательство, так как нет гарантии, что злоумышленники остановят атаку, и впоследствии они могут потребовать более крупные платежи.

DDoS-вымогательство/RDDoS-атаки отличаются от атак программ-вымогателей. Атака программы-вымогателя происходит, когда вредоносное программное обеспечение шифрует файлы, принадлежащие организации, и блокирует доступ владельцев данных до тех пор, пока не будет выплачен выкуп. Атака RDDoS не связана с проникновением в сеть организации, а только с нарушением сетевого трафика или трафика приложений.

Вот несколько причин, по которым RDDoS становится вектором угрозы. Атаки теперь требуют меньше усилий, чем установка вредоносного ПО — установка вредоносного ПО в ИТ-инфраструктуру организации требует экспертных навыков. Также требуется время для настройки и развертывания вредоносного программного обеспечения в целях саботажа или кражи данных. Для сравнения, DDoS-атаки просты в осуществлении, а ботнеты можно арендовать по низкой цене.

Злоумышленники могут легко проводить атаки с помощью обычных веб-приложений — злоумышленники все чаще используют устройства со встроенными сетевыми протоколами для усиления DDoS-атак. Это требует минимальных ресурсов. Отключение встроенных сетевых функций, таких как CoAP, ARMS и WS-DD, не является решением, поскольку может привести к потере функциональности, производительности и возможности подключения.

Рост стоимости биткойнов делает методы вымогательства более ценными для злоумышленников — по мере роста цен на биткойны

преступники RDDoS пересматривают свои стратегии спроса и инициируют массовые кампании по вымогательству.

Атаки RDDoS появились в конце 1990-х годов, когда их влияние на бизнес-функции было минимальным (поскольку большинство из них все еще выполнялись в автономном режиме). Организации были в первую очередь обеспокоены влиянием RDDoS-атак на поведение клиентов, поскольку они могли решить переключиться на конкурента.

В 2014 году серьезность RDDoS-атак стала очевидной, когда киберпреступная организация DDoS для биткойнов (DD4BC) провела крупномасштабные атаки. Сначала они были нацелены на компании, занимающиеся онлайн-азартными играми, которые обменивают биткойны, но затем расширились до развлекательного, энергетического и финансового секторов.

Атака DD4BC обычно включает в себя мелкомасштабные DDoS-атаки, за которыми следуют сообщения с требованием выкупа в биткойнах для предотвращения крупномасштабных атак. Угрозы и выкупы усиливаются в отношении невосприимчивых жертв.

С конца 2015 года DD4BC добавил угрозы, чтобы разоблачить компании, которые не платят выкуп, чтобы нанести ущерб их репутации. К началу 2016 года, когда европейские власти арестовали двух членов DD4BC, мишенями стали более 140 организаций.

Эта тактика оказалась выгодной для DD4BC и привлекла киберпреступников -подражателей, которые могут выдавать себя за известные хакерские группы, чтобы использовать свою известность для запугивания жертв. Например, Armada Collective утверждала, что в конце 2015 года провела RDDoS-кампанию против различных организаций, включая Hushmail и ProtonMail. Однако ProtonMail подвергалась непрерывным атакам даже после выплаты выкупа.

В 2017 году тактика RDDoS вышла на новый уровень сложности с использованием ботнетов. Эти ботнеты, состоящие из зараженных IoT-

устройств, позволяли проводить крупномасштабные DDoS-атаки. Однако к концу года эта тактика потеряла популярность, так как оказалась менее эффективной, и многие злоумышленники не смогли реализовать свои угрозы.

К концу 2017 года тенденция сместилась в сторону крупномасштабных кампаний по электронной почте, угрожающих DDoS-атаками, в первую очередь со стороны Phantom Squad, которые требовали выкуп в размере около 800 долларов в биткойнах.

С начала августа 2020 года изощренная кампания RDDoS постоянно нацелена на тысячи организаций по всему миру в различных секторах. В конце августа ФБР выпустило предупреждение, утверждая, что в этом могут участвовать такие группы, как Armada Collective, Fancy Bear, Cozy Bear и Lazarus Group.

Большинству жертв удалось смягчить эти атаки, но некоторые из них столкнулись с постоянными перебоями в работе своих бизнес-процессов. Например, в августе Новозеландская фондовая биржа несколько раз приостанавливала торги, поскольку ее хостинг-провайдер Spark неоднократно подвергался нападениям. со стороны злоумышленников, что привело к перебоям в работе сети и у других клиентов Spark.

В отличие от других злоумышленников, которые обычно нацелены на общедоступные веб-сайты своих жертв, поставщик кибербезопасности Akamai сообщил, что, хотя большинство злоумышленников, как правило, нацелены на общедоступные веб-сайты, эта кампания была нацелена на конечные точки API, DNS-серверы и внутреннюю инфраструктуру. Злоумышленникам удалось запутать свое поведение при атаках, часто меняя протоколы, используемые для атак RDDoS. Это говорит о том, что киберпреступники, ответственные за эту кампанию, очень опытны и имеют доступ к обширным ресурсам.

Многие DDoS-атаки с целью выкупа инициируются с запиской о выкупе, которая угрожает целевой организации. В некоторых случаях, прежде

чем отправить записку с требованием выкупа, преступник может организовать небольшое нападение, чтобы продемонстрировать свою серьезность.

Если угроза реальна, и злоумышленник решает продолжить, атака может происходить следующим образом: преступник или группа злоумышленников начинает направлять атакующий трафик на цель. Они могут использовать собственный ботнет или арендованный DDoS-сервис. Атакующий трафик может быть нацелен на уровни сети 3 или 4 (DDoS на уровне сети) или на уровень 7 (DDoS на уровне приложения).

Атакующий трафик перегружает целевую службу или приложение, и оно либо замедляется, либо полностью аварийно завершает работу.

Атака продолжается до тех пор, пока ресурсы преступника не будут исчерпаны, цель успешно смягчит атаку или преступник не остановит атаку. Методы смягчения, такие как блокировка IP-адресов и ограничение скорости, эффективны только против мелкомасштабного отказа в обслуживании. Для крупномасштабных DDoS организации обычно используют облачные службы защиты, которые могут масштабироваться с использованием облачных ресурсов, чтобы противостоять очень крупным атакам.

Преступник может организовать новые атаки, возобновить призыв к оплате или и то, и другое. Предотвращение и смягчение последствий DDoS-атак с вымогательством.

Если вы подвержены риску атаки RDDoS, не рекомендуется платить выкуп. Поэтому основное внимание уделяется предотвращению и смягчению атак по мере их возникновения. Вот несколько мер, обычно используемых организациями для смягчения последствий DDoS и, таким образом, нейтрализации риска вымогательства.

Расширение защиты от DDoS-атак на дополнительные IP-адреса. Защита от DDoS -атак защищает серверы и сетевое оборудование организации от DDoS-атак, обнаруживая вредоносный трафик и перенаправляя его из сети или сервера, на который направлена атака. Однако злоумышленники могут

определить IP-адреса, которые не защищены службой защиты от DDoS-атак организации, и вместо этого нацелить их.

Чтобы защититься от этого, организации могут расширить защиту от DDoS, чтобы защитить как можно больше веб-сервисов, IP-адресов компаний, DNS-серверов и инфраструктуры с выходом в Интернет. Новая изощренная техника DDoS заключается в том, что злоумышленники распределяют свои атаки таким образом, чтобы пороговые значения миграции DDoS не сбрасывались. Организации могут защититься от этой тенденции, сотрудничая с поставщиками средств смягчения для настройки порогов смягчения, чтобы изолировать и остановить это поведение.

Чтобы предотвратить DDoS-атаки, компании работают со своими интернет-провайдерами (ISP), чтобы гарантировать, что они могут контролировать сетевой трафик в ходе события. И Verizon, и AT&T успешно устранили сбои в работе сетевых служб, с которыми столкнулись их клиенты. Интернет-провайдеры также могут предоставить некоторую криминалистическую информацию, необходимую правоохранительным органам.

Сетевые маршрутизаторы и брандмауэры можно настроить так, чтобы блокировать неавторизованные IP-адреса и блокировать нежелательный сетевой трафик. Это может помочь предотвратить усиление атак через собственное сетевое оборудование организации. Организации должны убедиться, что на брандмауэрах, маршрутизаторах и других сетевых устройствах установлены последние версии программного и микропрограммного обеспечения, а также установлены самые последние исправления безопасности.

Лучший способ предотвратить DDoS-атаки с целью выкупа — иметь надежную стратегию защиты от DDoS-атак. Imperva предоставляет услугу защиты от DDoS -атак , которая блокирует атакующий трафик на границе сети, чтобы обеспечить непрерывность бизнеса с гарантированным временем безотказной работы и без влияния на производительность. Защитите свои

локальные или облачные ресурсы независимо от того, размещены ли вы в AWS, Microsoft Azure или Google Public Cloud.

Помимо защиты от DDoS, Imperva обеспечивает комплексную защиту приложений, API и микросервисов:

Брандмауэр веб-приложений. Предотвращайте атаки с помощью высококлассного анализа веб-трафика ваших приложений.

Самозащита приложений во время выполнения (RASP) — обнаружение и предотвращение атак в реальном времени из среды выполнения вашего приложения, где бы ни находились ваши приложения. Остановите внешние атаки и инъекции и уменьшите количество незавершенных уязвимостей.

Безопасность API. Автоматическая защита API обеспечивает защиту ваших конечных точек API по мере их публикации, защищая ваши приложения от эксплуатации.

Расширенная защита от ботов. Предотвращайте атаки на бизнес-логику со всех точек доступа — веб-сайтов, мобильных приложений и API. Обеспечьте полную видимость и контроль над трафиком ботов, чтобы остановить онлайн-мошенничество путем захвата учетной записи или извлечения конкурентоспособных цен.

Аналитика атак — обеспечивает полную видимость с помощью машинного обучения и экспертизы предметной области в стеке безопасности приложений, чтобы выявлять закономерности в шуме и обнаруживать атаки на приложения, позволяя изолировать и предотвращать кампании атак.

Защита на стороне клиента. Получите видимость и контроль над сторонним кодом JavaScript, чтобы снизить риск мошенничества в цепочке поставок, предотвратить утечку данных и атаки на стороне клиента.

Литература

1. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.

2. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
3. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 400 с.
4. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 476 с.
5. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.
6. Баранова, Е.К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. - М.: Риор, 2008. - 400 с.
7. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.
8. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.

References

1. Babash, A.V. Information security: Laboratory workshop / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: KnoRus, 2019. - 432 p.
2. Babash, A.V. Information Security. Laboratory workshop: Textbook / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: KnoRus, 2013. - 136 p.
3. Baranova, E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2017. - 400 p.
4. Baranova, E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2017. - 476 p.
5. Baranova, E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2018. - 400 p.
6. Baranova, E.K. Information Security. History of special methods of cryptographic activity: Textbook / E.K. Baranova, A.V. Babash, D.A. Larin. - M.: Rior, 2008. - 400 p.

7. Biryukov, A.A. Information security: protection and attack / A.A. Biryukov. - M.: DMK Press, 2013. - 474 p.
8. Gafner, V.V. Information Security: Textbook / V.V. Gafner. - Rn / D: Phoenix, 2010. - 324 p.

Для цитирования: Крыгин Н.Д. DDOS-АТАКИ И ЗАЩИТЫ ОТ НИХ // Научный сетевой журнал «Столыпинский вестник», номер 4/2022.