Научная статья
Original article
УДК 004.424

ТИПЫ КИБЕРАТАК

TYPES OF CYBER ATTACKS

Гнутова Ольга Викторовна студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), ol.gnutova@mail.ru

Мотуз Николай Сергеевич студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), motuz0nik@yandex.ru

Gnutova Olga Viktorovna bachelor's student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), ol.gnutova@mail.ru

Motuz Nikolay Sergeevich bachelor's student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), motuz0nik@yandex.ru

Аннотация. существуют тысячи известных вариантов кибератак, в статье указаны несколько из наиболее распространенных атак, с которыми организации сталкиваются каждый день. Программы-вымогатели - один из наиболее распространенных типов атак, при этом некоторые атаки используют методы вымогательства, такие как угроза раскрыть конфиденциальные данные, если цель не заплатит выкуп. Во многих случаях выплата выкупа неэффективна и не восстанавливает данные пользователя.

Annotation. There are thousands of known cyberattack variants, this article lists some of the most common attacks that organizations face every day. Ransomware is one of the most common types of attacks, with some attacks using ransomware techniques such as threatening to reveal sensitive data unless the target pays a ransom. In many cases, paying the ransom is ineffective and does not restore the user's data.

Ключевые слова: программы-сценарии, кибератаки, программное обеспечение.

Keywords: cyberattack, cybercriminals, threats

Существует следующий список программ для кибератак.

Программы-вымогатели

Программы-вымогатели - это вредоносные программы, которые используют шифрование для отказа в доступе к ресурсам (например, к файлам пользователя), обычно в попытке заставить жертву заплатить выкуп. После заражения системы файлы необратимо зашифровываются, и жертва должна либо заплатить выкуп, чтобы разблокировать зашифрованные ресурсы, либо использовать резервные копии для их восстановления.

Вредоносное ПО

Существует множество типов вредоносных программ , из которых вымогатели - лишь один из вариантов. Вредоносное ПО может использоваться для ряда целей: от кражи информации до порчи или изменения веб-контента и постоянного повреждения компьютерной системы.

Пейзаж вредоносных программ развивается очень быстро, но наиболее распространенными формами вредоносного ПО являются:

- **Вредоносное** ПО для ботнета - добавляет зараженные системы в ботнет, позволяя злоумышленникам использовать их для преступной деятельности.
- **Криптомайнеры -** добывают криптовалюту с помощью компьютера цели.

– **Инфостилеры - собирают** конфиденциальную информацию на компьютере цели.

– **Банковские трояны -** крадут финансовую и учетную информацию для банковских сайтов.

– **Вредоносное ПО для** мобильных устройств: атакует устройства с помощью приложений или SMS.

– **Руткит** -Дает злоумышленник полный контроль над операционной системой устройства

DoS- и DDoS-атаки

Атаки типа « отказ в обслуживании» (DoS) перегружают целевую систему, поэтому она не может отвечать на законные запросы. Распределенные атаки типа «отказ в обслуживании» (DDoS) похожи, но задействуют несколько хост-компьютеров. Целевой сайт наводнен незаконными запросами на обслуживание и вынужден отказывать в обслуживании законным пользователям. Это связано с тем, что серверы используют все доступные ресурсы для ответа на перегрузку запроса.

Эти атаки не предоставляют злоумышленнику доступа к целевой системе или какой-либо прямой выгоды. Они используются исключительно в целях саботажа или для отвлечения внимания служб безопасности, пока злоумышленники проводят другие атаки.

Брандмауэры и решения сетевой безопасности могут помочь защитить от мелкомасштабных DoS-атак. Для защиты от крупномасштабных DDoS-атак организации используют облачную защиту от DDoS-атак, которая может масштабироваться по запросу для ответа на огромное количество злонамеренных запросов.

Атаки фишинга и социальной инженерии

Социальная инженерия - это вектор атаки, который в значительной степени зависит от взаимодействия с человеком, он используется в более чем 90% кибератак. Он включает выдачу себя за доверенное лицо или организацию и обманным путем заставляет людей предоставлять

злоумышленнику конфиденциальную информацию, переводить средства или предоставлять доступ к системам или сетям.

Фишинговые атаки происходят, когда злоумышленник получает конфиденциальную информацию от цели и отправляет сообщение, которое выглядит как надежный и законный источник. Название «фишинг» отсылает к тому факту, что злоумышленники «выуживают» доступ к конфиденциальной информации, травмируя ничего не подозревающего пользователя эмоциональной ловушкой и надежной идентификацией.

В рамках фишингового сообщения злоумышленники обычно отправляют ссылки на вредоносные веб-сайты, предлагают пользователю загрузить вредоносное программное обеспечение или запрашивают конфиденциальную информацию напрямую через электронную почту, системы обмена текстовыми сообщениями или платформы социальных сетей. Разновидностью фишинга является «целевой фишинг», когда злоумышленники отправляют тщательно составленные сообщения лицам с особыми привилегиями, таким как сетевые администраторы, руководители или служащие, занимающие финансовые должности .

Атаки MitM

Атаки Man-in-the-Middle (MitM) - это взломы, которые позволяют злоумышленникам перехватывать данные, передаваемые между сетями, компьютерами или пользователями. Злоумышленник находится «посередине» между двумя сторонами и может шпионить за их коммуникациями, часто не будучи обнаруженным. Злоумышленник также может изменять сообщения перед отправкой их предполагаемому получателю.

Вы можете использовать VPN или применить надежное шифрование к точкам доступа, чтобы защитить себя от атак MitM.

Бесфайловые атаки

Бесфайловые атаки - это новый тип вредоносных атак, которые используют приложения, уже установленные на устройстве пользователя. В отличие от традиционных вредоносных программ, которые должны

развертываться на целевой машине, бесфайловые атаки используют уже установленные приложения, которые считаются безопасными и поэтому не обнаруживаются устаревшими антивирусными инструментами.

Атаки с использованием бесфайловых вредоносных программ могут быть инициированы действиями, инициированными пользователем, или могут быть инициированы без каких-либо действий пользователя, используя уязвимости операционной системы. Бесфайловые вредоносные программы находятся в оперативной памяти устройства и обычно обращаются к собственным инструментам операционной системы, таким как PowerShell и Windows Management Instrumentation (WMI), для внедрения вредоносного кода.

Доверенное приложение в привилегированной системе может выполнять системные операции на нескольких конечных точках, что делает их идеальными целями для бесфайловых атак вредоносных программ.

Предотвращение кибератак: общие решения для кибербезопасности

Ниже приведены несколько инструментов безопасности, обычно используемых организациями для предотвращения кибератак. Конечно, инструментов недостаточно для предотвращения атак - каждой организации нужен обученный ИТ-персонал и специалисты по безопасности или сторонние службы безопасности, чтобы управлять инструментами и эффективно использовать их для смягчения угроз.

Брандмауэр веб-приложений (WAF)

WAF защищает веб-приложения, анализируя HTTP-запросы и обнаруживая подозрительный вредоносный трафик. Это может быть входящий трафик, как в случае попытки злоумышленника атаковать путем внедрения кода, или исходящий трафик, как в случае вредоносного ПО, развернутого на локальном сервере, обменивающемся данными с центром управления и контроля (C&C).

WAF могут блокировать вредоносный трафик до того, как он достигнет веб-приложения, и могут предотвратить использование злоумышленниками

многих распространенных уязвимостей, даже если уязвимости не были устранены в базовом приложении. Он дополняет традиционные межсетевые экраны и системы обнаружения вторжений (IDS), защищая атаки злоумышленников на уровне приложений (уровень 7 сетевой модели OSI).

Защита от DDoS-атак

Решение для защиты от DDoS-атак может защитить сеть или сервер от атак типа «отказ в обслуживании». Это делается с помощью выделенного сетевого оборудования, развернутого организацией локально или в виде облачной службы. Только облачные сервисы способны отражать крупномасштабные DDoS-атаки, в которых задействованы миллионы ботов, поскольку они могут масштабироваться по запросу.

Система или служба защиты от DDoS-атак отслеживает трафик, чтобы обнаружить схему DDoS-атаки и отличить законный трафик от вредоносного. При обнаружении атаки он выполняет «очистку», проверяя пакеты трафика и отбрасывая те, которые считаются вредоносными, предотвращая их попадание на целевой сервер или сеть. В то же время он направляет законный трафик в целевую систему, чтобы гарантировать отсутствие сбоев в обслуживании.

Защита от ботов

Боты составляют значительную часть интернет-трафика. Боты сильно нагружают веб-сайты, занимая системные ресурсы. Хотя некоторые боты полезны (например, боты, которые индексируют веб-сайты для поисковых систем), другие могут выполнять вредоносные действия. Ботов можно использовать для DDoS-атак, очистки контента с веб-сайтов, автоматического выполнения атак на веб-приложения, распространения спама и вредоносных программ и т. Д.

Система защиты от ботов обнаруживает и блокирует плохих ботов, позволяя легитимным ботам выполнять такие действия, как поисковое индексирование, тестирование и мониторинг производительности. Это достигается за счет поддержки большой базы данных известных источников

ботов и выявления моделей поведения, которые могут указывать на то, что бот является вредоносным.

Облачная безопасность

Сегодня почти все организации управляют инфраструктурой, приложениями и данными в облаке. Облачные системы особенно уязвимы для киберугроз, потому что они обычно открыты для общедоступных сетей и часто страдают от низкого уровня видимости, поскольку они очень динамичны и работают за пределами корпоративной сети.

Поставщики облачных услуг берут на себя ответственность за безопасность своей инфраструктуры и предлагают встроенные инструменты безопасности, которые могут помочь пользователям облака защитить свои данные и рабочие нагрузки. Однако собственные инструменты облачной безопасности ограничены, и нет гарантии, что они используются должным образом и все облачные ресурсы действительно защищены. Многие организации используют специализированные облачные решения для обеспечения безопасности, чтобы гарантировать, что все важные активы, развернутые в облаке, должным образом защищены.

Безопасность базы данных

Базы данных обычно содержат конфиденциальную критически важную информацию и являются основной целью для злоумышленников. Защита баз данных включает усиление защиты серверов баз данных, правильную настройку баз данных для обеспечения контроля доступа и шифрования, а также мониторинг злонамеренных действий.

Решения для обеспечения безопасности баз данных могут помочь обеспечить постоянный уровень безопасности баз данных в масштабах всей организации. Они могут помочь предотвратить такие проблемы, как чрезмерные привилегии, незащищенные уязвимости в ядрах баз данных, незащищенные конфиденциальные данные и внедрение базы данных.

Безопасность API

Современные приложения используют интерфейсы прикладного программирования (API) для связи с другими приложениями, для получения данных или услуг. API-интерфейсы используются для интеграции систем внутри организации и все чаще используются для связи и получения данных от систем, управляемых третьими сторонами.

Все API-интерфейсы, особенно общедоступные API-интерфейсы, доступ к которым осуществляется через Интернет, чувствительны к атакам. Поскольку API-интерфейсы хорошо структурированы и документированы, злоумышленникам легко изучить их и использовать. Многие API-интерфейсы не защищены должным образом, могут быть слабо аутентифицированы или подвержены уязвимостям, таким как межсайтовый скриптинг (XSS), SQL-инъекция и атаки «человек посередине» (MitM).

Для обеспечения безопасности API-интерфейсов требуется ряд мер, включая строгую многофакторную аутентификацию (MFA), безопасное использование токенов аутентификации, шифрование данных при передаче и дезинфекцию вводимых пользователем данных для предотвращения атак путем внедрения. Решения API могут помочь обеспечить эти меры безопасности для API централизованно.

Аналитика угроз

Анализ угроз работает в фоновом режиме и поддерживает многие современные инструменты безопасности. Он также используется непосредственно службами безопасности при расследовании инцидентов. Базы данных аналитики угроз содержат структурированную информацию, собранную из различных источников, об участниках угроз, тактике атак, методах и процедурах, а также известных уязвимостях в вычислительных системах.

Решения для анализа угроз собирают данные из большого количества каналов и источников информации и позволяют организации быстро определять индикаторы компрометации (IOC), использовать их для выявления

атак, понимать мотивацию и режим работы злоумышленника, а также разрабатывать соответствующий отклик.

Список литературы

1. Толковый словарь по вычислительной технике. – М.: Издательский отдел "Русская редакция" ТОО "Channel trading Ltd", 2005.
2. Материалы сайта "Сервер информационных технологий". WEB: www.citforum.ru.
3. Хомоненко А. Базы данных: Учеб. Для вузов. – 2-е изд. – СПб., 2000.
4. Фёдорова А., Елманова Н. Базы данных для всех. –М.: Компьютер пресс , 2001.
5. Глушаков С.В., Ломотько. Базы данных (2001 год издания). – М.: АСТ, 2001.
6. Карпова Т. Базы данных: модели, разработка, реализация, 2001.
7. Когаловский М.Р. Энциклопедия технологий баз данных. –М.: Финансы и статистика, 2002.
8. Конноли Т., Бегг Л., Страчан А. Базы данных. Проектирование, реализация и сопровождение. Теория и практика. – 2-е изд. – Вильямс, 2000.
9. Ханенко В.Н. Информационные системы. – СПб.: Питер, 2001
10. Корнеев В.В., Гареев А.Ф. и др. Базы данных. Интеллектуальная обработка информации. М.: Изд. С.В. Молгачева, 2001.
11. Ребекка М. Райордан Основы реляционных баз данных, 2001.

References

1. Explanatory Dictionary of Computer Science. - M .: Publishing department " Russian edition " LLP " Channel trading Ltd ", 2005.
2. Materials of the site "Server of information technologies". WEB: www.citforum.ru.
3. Khomonenko A. Databases: Textbook. For universities. - 2nd ed. - SPb., 2000.
4. Fedorova A., Elmanova N. Databases for everyone. –M .: Computer press, 2001.

5. Glushakov S.V., Lomotko. Databases (2001 edition). - M .: AST, 2001.
6. Karpova T. Databases: models, development, implementation, 2001.
7. Kogalovsky M.R. Encyclopedia of Database Technologies. –M .: Finance and statistics, 2002.
8. Connolly T., Begg L., Strachan A. Databases. Design, implementation and maintenance. Theory and practice. - 2nd ed. - Williams, 2000.
9. Khanenko V.N. Information Systems. - SPb .: Peter, 2001
10. Korneev V.V., Gareev A.F. and other databases. Intelligent information processing. Moscow: Ed. S.V. Molgachev, 2001.
11. Rebecca M. Ryordan, Foundations of Relational Databases, 2001.

© Гнутова О.В., Мотуз Н.С., 20221 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.

Для цитирования: Гнутова О.В., Мотуз Н.С. ТИПЫ КИБЕРАТАК // Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.