Перевертун Д.Р. Кибератаки и их виды: от DDOS до фишинга // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 10(36) с. 59–62

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

КИБЕРАТАКИ И ИХ ВИДЫ: ОТ DDOS ДО ФИШИНГА

Перевертун Д.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: danilaperevertun@gmail.com

Статья рассматривает разнообразные виды кибератак, представляющие серьезную угрозу информационной безопасности. От распространенных атак на отказ обслуживания (DDoS) до хитрых фишинговых кампаний, мы изучим их характеристики, методы действия и способы защиты от них. Эта статья поможет читателям лучше понять мир киберугроз и укрепить свою цифровую безопасность.

Ключевые слова: Кибератаки, информационная безопасность, DDoS, вредоносные программы, фишинг.

CYBERATTACKS AND THEIR TYPES: FROM DDOS TO PHISHING

Perevertun D.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: danilaperevertun@gmail.com

The article examines various types of cyber attacks that pose a serious threat to information security. From common denial of service attacks (DDoS) to cunning phishing campaigns, we will study their characteristics, methods of action and ways to protect against them. This article will help readers better understand the world of cyber threats and strengthen their digital security.

Keywords: Cyberattacks, information security, DDoS, malware, phishing.

С развитием технологий и увеличением зависимости от цифровых ресурсов кибератаки стали неотъемлемой частью нашей жизни. Они угрожают как частным лицам, так и организациям, взламывая компьютеры, сети и системы для различных целей. В этой статье мы рассмотрим разнообразные виды кибератак, начиная от распространенных DDoS-атак и заканчивая хитрыми фишинговыми схемами. Мы предоставим информацию о характеристиках каждого типа атаки и дадим советы по их предотвращению и обнаружению.

1. DDoS-атаки (Атаки на отказ обслуживания)

DDoS-атаки, или атаки на отказ обслуживания, являются одними из самых распространенных и разрушительных видов кибератак. [1-2] Злоумышленники используют ботнеты, состоящие из компьютеров, зараженных вредоносным ПО, для перегрузки целевого сервера трафиком. Это приводит к временной недоступности веб-сайтов и онлайн-сервисов.

Советы по защите от DDoS-атак: [3-4]

- Использование специализированных средств мониторинга и защиты от DDoS.
- Регулярное обновление программного обеспечения и применение патчей для предотвращения уязвимостей.
- Настройка правил фильтрации для блокировки подозрительного трафика.

2. Вредоносные программы (Малварь)

Вредоносные программы, такие как вирусы, троянские кони и руткиты, представляют собой зловредное ПО, которое может навредить вашему компьютеру и украсть личные данные. Атаки начинаются с заражения системы через фишинговые электронные письма, вредоносные веб-сайты или неактуальное программное обеспечение.

Советы по защите от вредоносных программ:

- Установка надежного антивирусного программного обеспечения и его регулярное обновление.
- Осторожность при открытии вложений в электронных письмах и при скачивании файлов с ненадежных источников.
- Регулярное обновление операционной системы и всех установленных приложений.

3. Фишинг

Фишинг - это атаки, направленные на обман пользователей с целью получения их личных данных, таких как пароли и номера кредитных карт. Атаки фишинга могут использовать маскировку писем от банков, социальных сетей или других доверенных источников.

Советы по защите от фишинга:

- Внимательно проверяйте адрес отправителя электронных писем и ссылки в них.
- Не переходите по подозрительным ссылкам и не предоставляйте личные данные на ненадежных веб-сайтах.[5-6]
- Проводите обучение сотрудников о распознавании фишинговых атак в корпоративных средах.

4. SQL-инъекции

SQL-инъекции - это атаки, направленные на внедрение зловредного SQL-кода в веб-приложения. Злоумышленники могут получить доступ к базе данных и извлечь, изменить или уничтожить ценные данные.

Советы по защите от SQL-инъекций:

- Использование параметризованных запросов в веб-приложениях.
- Валидация и санитаризация входных данных перед их использованием в SQL-запросах.
- Регулярное обновление и аудит безопасности веб-приложений.

5. Атаки с использованием слабых паролей

Злоумышленники могут атаковать систему, пытаясь угадать или взломать слабые пароли пользователей. Это часто приводит к несанкционированному доступу к учетным записям и данным.

Советы по защите от атак с использованием слабых паролей:

- Использование длинных и сложных паролей, состоящих из букв, цифр и специальных символов.
- Внедрение политики сложных паролей в организации и их периодическое обновление.
- Внедрение двухфакторной аутентификации (2FA) для дополнительного уровня безопасности. 6. Ман-в-середине атаки (Man-in-the-Middle, MITM)

Ман-в-середине атаки позволяют злоумышленникам перехватывать и манипулировать коммуникацией между двумя сторонами, будучи незаметными для них. Это может привести к утечке конфиденциальных данных, включая пароли и чувствительную информацию.

Советы по защите от MITM-атак:

- Использование шифрования трафика с помощью протокола HTTPS.[7]
- Бдительность при подключении к открытым Wi-Fi сетям и использование виртуальных частных сетей (VPN).
- Периодическая проверка сертификатов безопасности в браузере.

7. Атаки на службы облачных вычислений

Облачные вычисления становятся все более популярными, и злоумышленники нацеливаются на службы облачных провайдеров. Они могут использовать слабости в настройках безопасности, чтобы получить доступ к данным и ресурсам хостинг-провайдера или других пользователей.

Советы по защите от атак на службы облачных вычислений:

- Тщательное настройка и мониторинг прав доступа к облачным ресурсам.
- Использование средств мониторинга безопасности в облачной среде.
- Обучение сотрудников о правилах безопасности при работе с облачными сервисами.

Кибератаки продолжают развиваться и становятся все более сложными. Понимание различных видов атак и применение соответствующих мер безопасности являются критически важными для защиты цифровой информации и обеспечения информационной безопасности. Обучение и обновление сотрудников и пользователей об актуальных угрозах и методах защиты также играют важную роль в обеспечении безопасности в онлайне.

Список литературы

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.
2. Гельфанд А. М. и др. Интернет вещей (IoT): Угрозы безопасности и конфиденциальности//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике//Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.

5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.
6. Косов Н.А., Мазепин П.С., Гришин Н.А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С. 152-156.
7. Штеренберг С.И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 51-57.

References

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
2. Gelfand A.M. et al. Internet of things (IoT): security and privacy threats//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
3. Gelfand A.M. et al. Investigation of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
4. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. – 2021. – pp. 33-37.
5. Kosov N.A., Timofeev R.S. Comparison of training methods for convolutional neural networks//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 526-530.
6. KOSOV N.A., MAZEPIN P.S., GRISHIN N.A. Application of neural networks for software testing automation //The sciencosphere. - 2020. – No. 6. – pp. 152-156.
7. Shterenberg S. I. Methods of constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology //OPHTHALMOSURGERY. – 2022. – No. 4s. – pp. 51-57.