Научная статья
Original article
УДК 004.424

АТАКИ НА ФАЙЛОВЫЕ СИСТЕМЫ

ATTACKS ON FILE SYSTEMS

Куренная Валерия Олеговна, студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), kurinaaa@rambler.ru

Kurennaya Valeria Olegovna, bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), kurinaaa@rambler.ru

Аннотация. Появление искусственного интеллекта во всех сферах жизни человека, дает возможность на более глубинный анализ данных. Так Cisco прогнозирует, что количество устройств с применением искусственного интеллекта в мире достигнет от 15 до 50 миллиардов в 2022 году. Искусственный интеллект дает возможность упростить работу пользователей.

Abstract. The emergence of artificial intelligence in all spheres of human life makes it possible for a deeper analysis of data. So Cisco predicts that the number of devices using artificial intelligence in the world will reach from 15 to 50 billion in 2022. Artificial intelligence makes it possible to simplify the work of users.

Ключевые слова: информационная безопасность, искусственный интеллект, атаки на информационные системы.

Keywords: information security, artificial intelligence, attacks on information systems.

Атаки на основе файлов по-прежнему являются одним из наиболее важных векторов кибератак, доступных сегодня, таких как недавняя программа-вымогатель которая может обойти механизм белого списка системы. Большое количество вредоносных программ, замаскированных под исполняемые файлы (.exe), PDF-документы и документы Microsoft Office, являются наиболее распространенными каналами атаки для фишинговых атак и ботнетов. В настоящее время технологии безопасности AI на основе файлов включают Cylance, Deep Instinct и Invincea.4.3. Одной из самых больших проблем, с которыми сталкиваются сегодня группы безопасности предприятий, является усталость, вызванная большим количеством предупреждений безопасности. Североамериканские компании получают до 1000 предупреждений о безопасности в день.

Большое количество вредоносных атак было перегружено в предупреждении и не воспринималось всерьез. Последней тенденцией является интеграция и анализ нескольких источников информации, включая корпоративную операционную регистрируйте данные и внешние службы разведки угроз, что очень ценно для крупных предприятий с независимыми операционными центрами безопасности.

Количественная оценка рисков безопасности предприятий - очень сложная задача. Основными проблемами являются отсутствие исторических данных и большое количество переменных, которые необходимо учитывать. Но сегодня многие компании, заинтересованные в количественной оценке рисков (включая страховщиков, предлагающих услуги кибербезопасности), должны пройти через болезненные и длительные процессы оценки кибербезопасности, основанные на систематической оценке соответствия политики и стандартов, управления безопасностью и культуры риска.

Анкета является традиционным подходом к оценке рисков, но неэффективна и с трудом отражает реальные риски корпоративной безопасности. Технология искусственного интеллекта может быстро обрабатывать и обрабатывать миллионы точек данных и генерировать прогнозные отчеты, что помогает предприятиям и страховщикам сетевой

безопасности получать точные отчеты об оценке рисков безопасности. В настоящее время многие стартапы по безопасности искусственного интеллекта начинают разрабатывать методы оценки рисков безопасности искусственного интеллекта.

На сегодняшний день искусственный интеллект является актуальной информацией в Интернете и в категориях информационных навыков. Информационная безопасность, несомненно, является основой любых данных. Информационная безопасность требует соблюдения конфиденциальности, целостности и доступности информации, предотвращения несанкционированного раскрытия и использования информации, предотвращения фальсификации и уничтожения информации, а также обеспечения того, чтобы авторизованные пользователи и программы могли использовать информацию своевременно. Искусственный интеллект в информационной безопасности в приложении не имеет существенных изменений, но применение искусственного интеллекта приведет к скачку генерации и передачи информации и изменению характеристик, а также к новым возможностям информационной безопасности. Например, растущее число вирусов, таких как вирус WannaCry, вирус Petya и вирус CopyCat, привлекло к информационной безопасности беспрецедентное внимание. Искусственный интеллект играет все более важную роль в информационной безопасности, особенно в защите и нападении. Как правильно использовать и улучшить защиту за счет улучшения информационной безопасности стали горячей темой в отрасли.

Несколько стратегий искусственного интеллекта в мире коснулись информационной безопасности. Хотя подробные описания различны, общая логика в основном одинакова, включая следующие аспекты:

1) надежность, это основной показатель безопасности и контроля искусственного интеллекта. То есть работа видимым для пользователя способом; доверенный, то есть вывод системы, приемлемый для пользователя;

2) проверяемость и допустимость являются логически естественными расширениями двусмысленности и достоверности.

3) вопросы морали и конфиденциальности в первую очередь связаны с чувствительностью данных -слепой искусственный интеллектуальные алгоритмы для ошибок и неправильного использования, а также опасения по поводу возможных последствий пола, возраста, расы или экономической информации.

4) ответственность означает ответственность планировщиков и организаторов системы искусственного интеллекта в отношении результатов поведения системы искусственного интеллекта.

Сравнивая вышеперечисленные аспекты, проблема режима ответственности является более целенаправленной, и теперь она в основном отражается в разделении ответственности за несчастные случаи, например, во время вождения автомобиля.

Искусственный интеллект разрушает существующую индустрию информационной безопасности

Например, выявление утечек паролей и неправильное использование является хорошим примером. Этот тип атаки становится все более распространенным, поскольку электронные письма и пароли людей попадают в темные сети после утечки данных. Например, уязвимость Equifax привела к раскрытию миллионов действительных писем; в Yahoo! нарушение данных злоумышленники получили информацию об учетной записи на 500 миллионов 7-я ежегодная международная конференция по геопространственным знаниям и интеллекту.

Поскольку люди склонны повторно использовать пароли, преступники будут случайным образом пробовать разные электронные письма и пароли на разных машинах в надежде на успех. Чтобы идентифицировать этот тип атаки, искусственный интеллект устанавливает базовый уровень для пользователей, которые подключаются и входят в систему на нескольких устройствах каждый день. Для человека принято пробовать сотни логинов на сервере, но трудно найти человека, пытающегося подключиться на 100 разных машинах и войти только один раз. Искусственный интеллект также может использоваться для автоматической оценки потенциальных ошибок в открытом исходном коде.

Однако другим приложением с точки зрения уязвимости является обзор и прогнозирование. Если объявлена новая уязвимость, можно использовать данные журнала, чтобы узнать, использовалась ли она в прошлом. Или, если это действительно новая атака, искусственный интеллект может оценить, достаточно ли доказательств, чтобы определить, каков следующий шаг злоумышленника. Искусственный интеллект также хорошо справляется с утомительными, повторяющимися задачами, такими как поиск определенного шаблона. Его реализация может облегчить ограничения ресурсов, с которыми сталкиваются большинство центров управления безопасностью.

Литература

1. Ван Хайтао Исследование системы осведомленности об информационной безопасности на основе технологий больших данных и искусственного интеллекта, Технологии и приложения сетевой безопасности, 2018 (3): 60-63.
2. Чжэн Яньфан Исследования и практика применения искусственного интеллекта и технологий анализа в системе ситуационной осведомленности информационной безопасности Мир цифровых коммуникаций, 2018, № 160 (4): 229.
3. Чжэн Фан Информационная безопасность в эпоху искусственного интеллекта, Исследования в области информационной безопасности, 2017, 3 (11): 966-967.
4. Дэн Вэньбинь Проблемы и меры противодействия надзору за информационной безопасностью в эпоху искусственного интеллекта Информационная безопасность Китая, 2018 г., 106 (10): 106-108.

References

1. Wang Haitao Research on Information Security Situation Awareness System Based on Big Data and Artificial Intelligence Technology, Network Security Technology and Application, 2018 (3): 60-63.
2. Zheng Yanfang Research and Practice of Artificial Intelligence Application and Analysis Technology in Information Security Situational Awareness System Digital Communication World, 2018, No.160 (4):229.

3. Zheng Fang Information Security in the Age of Artificial Intelligence, Information Security Research, 2017, 3 (11): 966-967.
4. Deng Wenbing Challenges and Countermeasures for Information Security Supervision in the Age of Artificial Intelligence China Information Security, 2018, 106 (10): 106-108.

© Куренная В.О., 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №6/2022.

Для цитирования: Куренная В.О. АТАКИ НА ФАЙЛОВЫЕ СИСТЕМЫ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №6/2022.