УДК 004.056.5

Слюсарев Артём Андреевич, специалист, пятый курс, факультет кибербезопасности, кафедра защищенных систем связи, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург

Усков Арсений Николаевич, специалист, пятый курс, факультет кибербезопасности, кафедра защищенных систем связи, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург

Кухтин Владимир Олегович, специалист, пятый курс, факультет кибербезопасности, кафедра защищенных систем связи, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург

ЗАЩИТА ТЕХНИЧЕСКИХ СИСТЕМ ОТ КИБЕРАТАК: РОЛЬ ЦИФРОВОЙ КРИМИНАЛИСТИКИ В РАССЛЕДОВАНИИ ИНЦИДЕНТОВ

Аннотация

В условиях повсеместной цифровизации и роста числа киберугроз обеспечение безопасности технических систем становится критически важной задачей. Традиционных превентивных мер защиты, антивирусы, межсетевые экраны, уже недостаточно. Актуальность работы обусловлена необходимостью не только предотвращать атаки, но и эффективно расследовать уже произошедшие инциденты для минимизации ущерба, атрибуции злоумышленников и предотвращения будущих атак. Цель статьи — проанализировать роль и методы цифровой криминалистики, как

ключевого инструмента в расследовании инцидентов кибербезопасности, связанных с техническими системами. Цифровая криминалистика является не просто реактивным инструментом, а неотъемлемой частью проактивной стратегии кибербезопасности, позволяющей замкнуть цикл "Защита → Обнаружение → Реакция → Расследование → Улучшение".

Annotation

In the context of widespread digitalization and the growth of cyber threats, ensuring the security of technical systems is becoming a critical task. Traditional preventative security measures, such as antivirus software and firewalls, are no longer sufficient. The relevance of this work stems from the need not only to prevent attacks but also to effectively investigate past incidents to minimize damage, attribute attackers, and prevent future attacks. The purpose of this article is to analyze the role and methods of digital forensics as a key tool in investigating cybersecurity incidents related to technical systems. Digital forensics is not just a reactive tool, but an integral part of a proactive cybersecurity strategy that closes the cycle of "Protect → Detect → Respond → Investigate → Improve."

Ключевые слова: кибербезопасность, цифровая криминалистика, расследование инцидентов, технические системы, кибератака.

Keywords: cybersecurity, digital forensics, incident investigation, technical systems, cyberattack.

Литература

1. Красов, А.В. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения / Красов А.В., Штеренберг С.И., Фахрутдинов Р.М., Рыжаков Д.В., Пестов И.Е. // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 10. С. 36-40.

2. Гельфанд, А.М. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе / Гельфанд А.М., Пестов И.Е., Катасонов А.И., Рязанцев К.С. // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2018. № 8. С. 91-97.
3. Иванов, А.В. Исследование возможностей методики скрытого вложения цифрового водяного знака в class-файлы на виртуализированных платформах с отличающейся архитектурой / Иванов А.В., Красов А.В., Шариков П.И.// Научно-аналитический журнал Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2018. № 2. С. 79-89.
4. Котенко, И.В. Общее перечисление и классификация шаблонов атак (CAPEC): описание и примеры применения / Котенко И.В., Дойникова Е.В., Чечулин А.А. // Защита информации. Инсайд. 2012. № 4 (46). С. 54-66.
5. Шемякин С.Н. Описание разнообразных ddos атак с использованием botnet / Шемякин С.Н., Гельфанд А.М., Холоденко В.Ю., Орлов Г.А., Ходжаев Ш.А.У. // Colloquium-journal. 2019. № 23-2 (47). С. 52-53.
6. Лаврова, Д.С. Предупреждение Dos-атак путем прогнозирования значений корреляционных параметров сетевого трафика / Лаврова Д.С., Попова Е.А., Штыркина А.А., Штеренберг С.И. // Проблемы информационной безопасности. Компьютерные системы. 2018. № 3. С. 70-77.
7. Костарев, С.В. Модель процесса передачи результатов аудита и контроля в автоматизированной системе менеджмента предприятия интегрированной структуры / Костарев С.В., Липатников В.А., Сахаров Д.В. // Проблемы информационной безопасности. Компьютерные системы. 2015. № 2. С. 120-125.

Literature

1. Krasov, A.V. Analysis of enterprise information security based on collecting user data from open resources and monitoring information resources using machine learning / Krasov A.V., Shterenberg S.I., Fakhrutdinov R.M., Ryzhakov D.V., Pestov I.E. // T-Comm: Telecommunications and transport. 2018. Vol. 12. No. 10. P. 36-40.
2. Gelfand, A.M. Development of a model for the distribution of self-modifying code in a protected information system / Gelfand A.M., Pestov I.E., Katasonov A.I., Ryazantsev K.S. // Modern science: current problems of theory and practice. Series: Natural and technical sciences. 2018. No. 8. P. 91-97.
3. Ivanov, A.V. Study of the capabilities of the method of hidden embedding of a digital watermark in class files on virtualized platforms with different architecture / Ivanov A.V., Krasov A.V., Sharikov P.I. // Scientific and analytical journal Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia. 2018. No. 2. pp. 79-89.
4. Kotenko, I.V. Common Enumeration and Classification of Attack Patterns (CAPEC): Description and Application Examples / Kotenko I.V., Doynikova E.V., Chechulin A.A. // Information Security. Inside. 2012. No. 4 (46). P. 54-66.
5. Shemyakin S.N. Description of various DDoS attacks using botnet / Shemyakin S.N., Gelfand A.M., Kholodenko V.Yu., Orlov G.A., Khodjaev Sh.A.U. // Colloquium-journal. 2019. No. 23-2 (47). P. 52-53.
6. Lavrova, D.S. Prevention of DoS attacks by predicting the values of correlation parameters of network traffic / Lavrova D.S., Popova E.A., Shtyrkina A.A., Shterenberg S.I. // Problems of information security. Computer systems. 2018. No. 3. P. 70-77.
7. Kostarev, S.V. Model of the process of transferring audit and control results in the automated management system of an enterprise with an integrated

structure / Kostarev S.V., Lipatnikov V.A., Sakharov D.V. // Problems of information security. Computer systems. 2015. No. 2. P. 120-125.

Введение

В современном мире технические системы, от промышленных контроллеров до устройств «Интернета вещей», все чаще становятся целями кибератак. Последствия таких атак могут быть катастрофическими, приводя не только к финансовым потерям, но и к остановке критической инфраструктуры.

Проблема заключается в том, что превентивные меры защиты не могут гарантировать 100% безопасности. Инциденты неизбежно происходят. В этот момент на первый план выходит процесс реагирования на инцидент, и его ядром является цифровая криминалистика.

Актуальность работы обусловлена необходимостью не только предотвращать атаки, но и эффективно расследовать уже произошедшие инциденты для минимизации ущерба, атрибуции злоумышленников и предотвращения будущих атак.

Цель данной статьи – определить место и значение цифровой криминалистики в общей архитектуре защиты технических систем, а также систематизировать основные этапы и методы криминалистического анализа при расследовании киберинцидентов.

Цифровая криминалистика: Понятие и задачи в контексте технических систем

Цифровая криминалистика – это прикладная наука о методах сбора, сохранения, анализа и представления цифровых данных в форме, пригодной для использования в суде или в рамках внутреннего расследования.

Применительно к техническим системам, она имеет свою специфику. В отличие от расследования атак на офисные ПК, здесь эксперты сталкиваются с следующими факторами:

- Гетерогенной средой: SCADA-системы, ПЛК (программируемые логические контроллеры), специализированные протоколы (Modbus, Profinet);
- Требованиями непрерывности: Зачастую невозможно просто выключить систему для снятия образа диска, так как это остановит производственный процесс;
- Волатильностью данных: Многие улики существуют только в оперативной памяти контроллеров.

Ключевые задачи криминалистики в данном контексте:

- Идентификация инцидента: Подтверждение факта несанкционированного доступа;
- Сбор и сохранение летучих данных;
- Анализ холодных данных (Образы дисков, логи, дампы сетевого трафика);
- Атрибуция атаки (Поиск ответа на вопросы «Кто?» и «Как?»);
- Оценка ущерба.

Этапы криминалистического расследования инцидента

Процесс расследования можно условно разделить на несколько канонических этапов, описанных во многих стандартах, например, NIST:

- Этап 1. Подготовка. Создание группы реагирования. Подготовка инструментов (ПО для снятия образов, чистые носители, блокираторы записи);
- Этап 2. Идентификация и Сбор. Это самый критический этап. Принцип Chain of Custody (Каждый шаг по работе с уликами должен быть документирован). Сбор данных по принципу, от наиболее летучих к

наименее летучим (Оперативная память, сетевые подключения и трафик, данные на жестких дисках, логи с межсетевых экранов, серверов, контроллеров).

- Этап 3. Анализ. Поиск индикаторов компрометации (IoC – IP-адреса, хэши вредоносного ПО, сигнатуры). Восстановление удаленных данных. Анализ временной шкалы (что и когда делал злоумышленник). Анализ вредоносного ПО.
- Этап 4. Формирование отчета и представление. Подготовка технического отчета для ИТ-специалистов, с рекомендациями по устранению уязвимостей. Подготовка отчета для руководства (оценка ущерба, риски). В случае необходимости — подготовка юридически значимых заключений для правоохранительных органов.

Роль криминалистики в проактивной защите

Главная ценность цифровой криминалистики не только в наказании виновных, но и в усилении защиты. Расследование — это лучший источник информации об эффективности существующих мер.

По результатам анализа инцидента компания может:

- Устранить коренную причину, не просто удалить вирус, а закрыть уязвимость, например, обновить прошивку ПЛК, через которую он проник;
- Улучшить мониторинг, настроить SIEM-систему на обнаружение техник, которые использовал злоумышленник;
- Обучить персонал, если атака прошла с использованием фишинга.

Таким образом, криминалистика замыкает цикл управления безопасностью.

Заключение

Цифровая криминалистика из узкоспециализированной дисциплины превратилась в обязательный компонент системы обеспечения кибербезопасности технических систем.

Ее роль не сводится к пост-инцидентному анализу. Она предоставляет критически важные данные для проактивного усиления защиты и предотвращения будущих атак.

Особую сложность представляет криминалистический анализ специфических технических систем, что требует от специалистов не только ИТ-знаний, но и понимания промышленных технологий.

Перспективы развития данного направления лежат в области автоматизации процессов сбора и анализа данных, а также применения технологий искусственного интеллекта для выявления сложных, скрытых аномалий в поведении систем.