ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

упаковки и разрабатывают индивидуальные решения, программное обеспечение для обеспечения безопасности и исследователи также должны расширять свои возможности для обнаружения, анализа и нейтрализации этих угроз.

Список использованных источников

1. Galloro N. et al. A Systematical and longitudinal study of evasive behaviors in windows malware //Computers & Security. – 2022. – Т. 113. – С. 102550.
2. Obaidat I. et al. Jadeite: A novel image-behavior-based approach for java malware detection using deep learning //Computers & Security. – 2022. – Т. 113. – С. 102547.
3. Afianian A. et al. Malware dynamic analysis evasion techniques: A survey //ACM Computing Surveys (CSUR). – 2019. – Т. 52. – №. 6. – С. 1-28.
4. Sgandurra D. et al. Automated dynamic analysis of ransomware: Benefits, limitations and use for detection //arXiv preprint arXiv:1609.03020. – 2016.
5. Raff E. et al. An investigation of byte n-gram features for malware classification //Journal of Computer Virology and Hacking Techniques. – 2018. – Т. 14. – С. 1-20.
6. Lee J., Lee B., Cho S. A Study on the Analysis Method to API Wrapping that Difficult to Normalize in the Latest Version of Themida //Journal of the Korea Institute of Information Security & Cryptology. – 2019. – Т. 29. – №. 6. – С. 1375-1382.
7. Oberhumer M. F. X. J. UPX the Ultimate Packer for eXecutables //http://upx. sourceforge. net/. – 2004.
8. Chevet S. Inside VMProtect.(2015). – 2015.

УДК 681.3

ИССЛЕДОВАНИЯ ЦИФРОВОЙ ФОРЕНЗИКИ В ИНЦИДЕНТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Жақсығали Фараби Болатұлы
farabi.jax@gmail.com
Студент-магистрант ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – А. М. Нурушева

Компьютерная форензика играет важную роль в расследовании и решении инцидентов информационной безопасности (*далее* – ИБ), таких как утечки конфиденциальных данных и атаки вредоносного ПО. Использование инструментов и техник компьютерной форензики значительно увеличилось в последние годы, поскольку организации стремятся защитить свои чувствительные данные и предотвратить угрозы ИБ. Эта исследовательская работа представляет собой комплексный анализ компьютерной форензики в инцидентах ИБ, включая реальные примеры, инструменты и их использование, гипотетический пример с детальным анализом, проведенным экспертами по форензике, и рекомендации по предотвращению.

Определения и терминология компьютерной форензики:

Компьютерная форензика - это процесс сбора, анализа и интерпретации электронных данных в целях выявления, документирования и сбора доказательств, связанных с преступлениями, нарушениями безопасности или другими инцидентами, связанными с использованием компьютеров, сетей и электронных устройств.

Ниже представлены некоторые из основных терминов и определений, используемых в компьютерной форензике:

1. Диск-образ: точная копия содержимого жесткого диска или другого носителя информации, которая может быть использована для анализа и восстановления данных.
2. Хеш-сумма: уникальный числовой идентификатор, созданный из содержимого файла или другого набора данных. Хеш-сумма используется для проверки целостности данных и определения, были ли они изменены.

3. Метаданные: данные, которые описывают другие данные, например, информация о создании, изменении или доступе к файлу.

4. Slack Space: неиспользуемое пространство на диске или другом носителе, которое может содержать информацию, которая не видна обычным образом.

5. Интернет-журнал: записи о том, какие веб-страницы были посещены с компьютера или другого устройства, включая даты и время посещения.

6. Восстановление данных: процесс восстановления удаленных или поврежденных данных на компьютере или другом устройстве.

7. Эксперт по компьютерной форензике: специалист, который использует методы и инструменты компьютерной форензики для сбора и анализа цифровых доказательств.

8. Цепочка владения: документированный путь, который показывает, кто и когда имел доступ к цифровым доказательствам, чтобы обеспечить их целостность и достоверность.

9. Вредоносное ПО: программное обеспечение, созданное для нанесения вреда компьютеру или другому устройству, включая вирусы, черви, троянские программы и шпионское ПО.

10. Система мониторинга и обнаружения инцидентов: программное обеспечение, которое обнаруживает и предотвращает угрозы безопасности, используя методы мониторинга и анализа сетевого трафика и активности пользователей.

Инструменты:

Для проведения анализа команда судебно-медицинских экспертов использует ряд инструментов, в том числе:

- EnCase: EnCase — это мощный криминалистический инструмент, который позволяет экспертам-криминалистам собирать и анализировать цифровые улики. Его можно использовать для создания криминалистических образов устройств, восстановления удаленных файлов и анализа файловых систем.
- FTK Imager: FTK Imager — это бесплатный криминалистический инструмент, который позволяет экспертам-криминалистам создавать криминалистические образы устройств. Его также можно использовать для анализа образов дисков и восстановления удаленных файлов.
- Wireshark: Wireshark — это анализатор сетевых протоколов, который позволяет экспертам-криминалистам захватывать и анализировать сетевой трафик. Его можно использовать для определения источника атаки и методов, используемых злоумышленником
- Metasploit: Metasploit — это инструмент для тестирования на проникновение, который можно использовать для проверки безопасности сетей и систем. Его также можно использовать для выявления уязвимостей в сторонних программных пакетах

Примеры и гипотетический пример с анализом работы экспертов по компьютерной форензике

Пример: Утечка конфиденциальных данных в Capital One

В 2019 году Capital One объявил о нарушении безопасности данных, в результате которого злоумышленники получили доступ к более чем 100 миллионам записей клиентов, включая имена, адреса электронной почты, номера телефонов, номера социального страхования и другую чувствительную информацию. Компьютерная форензика была использована для расследования инцидента.

1. Шаг 1: Сбор данных

Эксперты по компьютерной форензике собрали данные с серверов Capital One, а также с личных устройств злоумышленников, которые были задержаны правоохранительными органами.

2. Шаг 2: Анализ данных

Эксперты использовали инструменты компьютерной форензики, такие как FTK и EnCase, чтобы анализировать собранные данные. Они искали следы взлома, попытки изменения файлов и другие аномалии в данных.

3. Шаг 3: Идентификация данных

Эксперты искали информацию, которая могла быть скомпрометирована, такую как имена клиентов, номера социального страхования, даты рождения и другую личную информацию. Они также искали информацию о кредитных картах и счетах клиентов.

4. Шаг 4: Определение причины

Эксперты выяснили, что нарушение безопасности произошло из-за конфигурационной ошибки в ***фаерволе****, который был настроен неправильно. Злоумышленники использовали уязвимость для получения доступа к серверам Capital One.

5. Шаг 5: Решение

Компьютерные эксперты разработали план восстановления и обеспечения безопасности, который включал изменение настроек фаервола, а также пересмотр процедур безопасности для предотвращения подобных инцидентов в будущем.

Гипотетический пример:

Сценарий:

В крупном финансовом учреждении произошла утечка данных, и конфиденциальные данные клиентов были украдены. Учреждение наняло экспертов по компьютерной форензике для расследования инцидента и установления источника взлома.

Анализ:

Криминалистическая группа начинает со сбора доказательств с серверов и сетевых устройств учреждения. Они используют специализированные инструменты, такие как EnCase и FTK Imager, для создания криминалистических образов серверов и устройств. Затем команда анализирует криминалистические изображения, чтобы выявить любые признаки подозрительной активности.

Криминалистическая группа обнаруживает, что злоумышленники получили доступ к сети учреждения, воспользовавшись уязвимостью в стороннем программном пакете. Они использовали этот доступ для кражи конфиденциальных данных клиентов, включая номера социального страхования и информацию о кредитных картах. Криминалистическая группа также обнаруживает, что злоумышленники использовали троян удаленного доступа (RAT) для сохранения доступа к сети учреждения даже после первоначального взлома.

Шаг 1: Сбор доказательств

Команда экспертов использовала комбинацию EnCase и FTK Imager для сбора доказательств с серверов и сетевых устройств учреждения. Они создали форензические образы устройств и собрали данные из журналов, электронной почты и системных файлов.

Команда начала с идентификации устройств, которые, вероятнее всего, содержали доказательства, связанные с атакой. Затем они использовали EnCase и FTK Imager для создания криминалистических образов этих устройств, путём использования инструментов блокировки записи, чтобы гарантировать, что оригинальные данные не будут изменены или уничтожены в процессе сбора.

Команда собрала данные из журналов, чтобы идентифицировать любую подозрительную активность в сети. Они также собрали электронную почту и другие системные файлы, чтобы идентифицировать любые связи или действия, связанные с атакой.

Шаг 2: Сохранение

После того, как доказательства были собраны, команда экспертов сохранила их, чтобы убедиться, что они не были изменены или уничтожены. Они хранили доказательства в безопасном месте и гарантировали, что они не были изменены или модифицированы каким-либо образом.

Команда использовала строгие процедуры цепочки хранения, чтобы гарантировать безопасность доказательств и сохранить их целостность на протяжении всего процесса анализа. Доказательства были помечены и отслеживались на каждом этапе анализа, и только уполномоченные сотрудники имели к ним доступ.

Шаг 3: Анализ

Команда экспертов проанализировала доказательства, чтобы идентифицировать любые признаки подозрительной активности. Они исследовали журналы, сетевой трафик и другие

данные, чтобы определить, как злоумышленники получили доступ к сети и какие данные они украли.

Команда использовала специализированные инструменты, такие как Wireshark, для захвата и анализа сетевого трафика. Они идентифицировали IP-адреса использованные злоумышленниками и проследили сетевой трафик до его источника. Команда также использовала инструменты восстановления файлов и поиска по ключевым словам для анализа файловых систем и идентификации любых подозрительных файлов или действий. Они идентифицировали используемое злоумышленниками вредоносное ПО и определили, как оно было установлено в сети.

Шаг 4: Восстановление

На основе своего анализа, команда экспертов восстановила события, которые привели к утечке данных. Они определили время атаки и методы, использованные злоумышленниками. Команда использовала свой анализ доказательств, чтобы идентифицировать уязвимости, которые были использованы злоумышленниками. Они определили, как злоумышленники получили доступ к сети и какие данные они украли. Команда также идентифицировала методы, которые использовали злоумышленники, чтобы сохранить доступ к сети даже после начального взлома. Они проследили боковое перемещение злоумышленников по сети и идентифицировали данные, которые были выведены из сети.

Шаг 5: Отчетность

Команда экспертов подготовила подробный отчет, излагающий их результаты. Отчет содержал информацию о том, как злоумышленники получили доступ к сети, какие методы они использовали для кражи данных и какие шаги учреждение может предпринять, чтобы предотвратить подобные инциденты в будущем.

Отчет также содержал рекомендации по улучшению ИБ учреждения, такие как реализация программы управления исправлениями и проведение регулярных анализов уязвимостей. Отчет был представлен руководству учреждения, которое использовало его результаты для улучшения превентивных мер и предотвращения подобных инцидентов в будущем.

Рекомендации по предотвращению инцидентов ИБ

Существует несколько методов и инструментов, которые могут быть использованы для предотвращения инцидентов и нарушений безопасности. Некоторые из рекомендаций включают следующие:

1. Установите эффективную систему мониторинга и обнаружения инцидентов, которая будет проактивно определять и предотвращать атаки на сеть и данные. Система должна быть настроена для обнаружения не только известных угроз, но и новых и неизвестных.
2. Разработайте и регулярно обновляйте политику безопасности, которая будет устанавливать правила и процедуры для защиты сети и данных. Это может включать в себя установку сильных паролей, ограничение доступа к чувствительным данным и частую смену паролей.
3. Обеспечьте регулярные обновления программного обеспечения и операционной системы, чтобы устранить известные уязвимости и предотвратить атаки на необновленные системы.
4. Установите и поддерживайте современные антивирусные программы и брандмауэры для защиты от вредоносных программ и несанкционированного доступа к сети и данным.
5. Проводите регулярные обучающие программы для сотрудников, чтобы они знали, как обнаружить и предотвратить атаки на сеть и данные. Обучение должно включать в себя основы безопасности, такие как использование сильных паролей, осмотр прикрепленных файлов и уведомление об аномалиях в работе сети.
6. Регулярно проводите тестирование на проникновение, чтобы определить уязвимости сети и данных и разработать план действий по их исправлению.

7. Создайте план реагирования на инциденты, который будет устанавливать процедуры и ответственности для быстрого и эффективного реагирования на атаки и восстановления сети и данных.

8. Регулярно резервируйте данные и храните резервные копии в безопасном месте, чтобы восстановить данные в случае утери или атаки.

9. Обеспечьте физическую безопасность серверов и других устройств, где хранятся чувствительные данные, чтобы предотвратить доступ к ним несанкционированных лиц.

Список использованных источников

1. Casey, E. (2018). Digital evidence and computer crime: forensic science, computers and the internet. Academic Press.

2. Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. Digital investigation, 7, S64-S73.

3. Choo, K. K. R. (2019). The evolution and development of digital forensics. Journal of Forensic Sciences, 64(4), 1021-1031.

4. Maimon, D., & Slay, J. (2018). Advanced persistent threat: understanding the danger and how to protect your organization. CRC Press.

5. Agarwal, A., & Zhang, H. (2019). A blockchain-based solution for internet of things security. Journal of Network and Computer Applications, 125, 82-94.

6. Gharibi, W., & Abouhossein, A. (2019). A new approach for intrusion detection based on combining data mining and forensic techniques. Journal of Ambient Intelligence and Humanized Computing, 10(3), 1003-1013.

ӘОЖ 004.021

ДИНАМИКАЛЫҚ ОРТАЛАРДА ШЕШІМ ҚАБЫЛДАУ СИПАТТАМАСЫ

Жеткиншеков Ринат Карпатович[1], Диас Маратұлы[2]
[1]zhrk2407@gmail.com
[1]магистрант, Ақпараттық жүйелер кафедрасы, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан
[2]магистрант, Ақпараттық жүйелер және технологиялар кафедрасы, Esil University, Астана, Қазақстан
Ғылыми жетекшілері – PhD, аға оқытушы У. Махажанова

Қарқынды өзгеретін қоршаған орта мен қоғамның жаһандануы жағдайында жаңа сипаттамадағы міндеттер пайда болуда. Оларды шешу үшін «сыртқы» білім қажет, бұл білімнің тікелей тасымалдаушысы–сарапшылар. Әдетте, білім бөлшекті болып келеді, еркін құрылымға ие, әртүрлі форматта және ауқымды ортаға жайылған.

Мәліметтерді талдау тұрғысынан алғанда динамикалық жүйелер нақты объектілер мен үрдістердің әрекеттерін теоретикалық зерттеу үшін қажет. Мысалы, кәсіпорын немесе бизнес – әрдайым уақыт аралығында өзгермелі және өзін зерттеуге математикалық моделді қажет ететін динамикалық жүйе.

Динамикалық орталарда шешім қабылдаудың негізгі сипаттамасы динамика, күрделілік, айқын еместік, және белгісіздік. Орта динамикасы жүйе күйінің оның алдынғы күйіне тәуеділігіне жатады. Жүйедегі динамика оң-кері байланыс немесе теріс-кері байланыста болуы мүмкін.

Күрделілік, белгісіздік жүйедегі өзара әсер етуші немесе өзара байланыстағы элементтерге айтарлықтай дәрежеде жатады, яғни жүйенің әрекетін болжауды күрделендіреді.

Күрделілікті анықтаудағы тағы бір мәселелер жүйе компоненттері жүйеде неше компонент бар екендігі жағынан, олардың арасында неше байланыс бар және осы байланыстар сипаттамасы қалай өзгеруі мүмкін.

Белгісіздік динамикалық жүйелердің кейбір аспектілерінің физикалық көрінбеуіне жатады, сонымен қатар шешім қабылдаушының жүйе компоненттері туралы білім алу қабілеттілігіне тәуелді.