ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

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 имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

БАҚ арқылы IoT-ның Қазақстандағы дамуы туралы және оның қоғамға әсері туралы мәлімет тарату.

Университеттер мен зерттеу орталықтарында IoT технологияларын зерттеуге арналған арнайы лабораторияларды құру. Мұндай орындар жаңа идеяларды сынап көруге және тәжірибе жинақтауға мүмкіндік береді.

Жаңа технологияларды көрсету және олардың практикалық пайдасын түсіндіру үшін арнайы орталықтар ашу.

Қазақстандағы IoT-ны оқыту және хабардар ету бағдарламалары технологиялық инновацияларды ынталандыруға және қоғамның қауіпсіздікке деген сезімталдығын арттыруға көмектеседі, бұл болашақта технологиялық өзгерістерге бейімділікті және тұрақтылықты қамтамасыз етеді.

IoT құрылғыларының кең таралуы мен олардың әртүрлі қолданылуы қауіпсіздік аудитінің маңызын арттырады. Қауіпсіздік аудиті арқылы ұйымдар өздерінің желілері мен құрылғыларындағы мүмкін қауіптерді азайта алады және оларды тиімді басқара алады. Бұл процесс барлық құрылғылар мен желілерді қауіпсіз, сенімді және тұрақты етіп сақтауға көмектеседі.

Пайдаланған әдебиеттер тізімі

1. «Introduction to the Internet of Things» - Cisco Networking Academy.
2. Rajkumar Buyya, Amir Vahid. Internet of Things: Principles and Paradigms. 2016. 378 p.
3. Shancang Li, Li Da Xu. Securing the Internet of Things. 2017. 154 p.
4. Bruce Sinclair. IoT Inc: How Your Company Can Use the Internet of Things to Win in the Outcome Economy. 2017. 304 p.

УДК 004.056.5

КРИМИНАЛИСТИЧЕСКИЕ МЕТОДЫ АНАЛИЗА РЕЕСТРА WINDOWS ДЛЯ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ, СВЯЗАННЫХ С УТЕЧКАМИ ДАННЫХ

Жакиева Асел Нартаевна
aselzakieva0@gmail.com,
студент III курса образовательной программы 6B06306 «Системы информационной безопасности», Евразийский национальный университет им. Л.Н. Гумилева
Алимбетова Аида Арманқызы
aidalimbetova18@gmail.com
студент III курса образовательной программы 6B06306 «Системы информационной безопасности», Евразийский национальный университет им. Л.Н. Гумилева
Научный руководитель Аймичева Гаухар Ислямовна

В современном мире, с увеличением числа цифровых технологий и расширением присутствия в интернете, обеспечение безопасности данных становится приоритетом не только для отдельных лиц, но и для организаций и компаний. Несмотря на принятие самых строгих мер безопасности, не исключены случаи утечек информации. Проведение тщательного расследования подобных инцидентов играет важную роль в выявлении причин и предотвращении подобных ситуаций в будущем.

Исследование, проведенное IBM и Ponemon Institute, показало (рис.1), что средняя стоимость утечки данных в мире в 2022 году составит 4,4 миллиона долларов США по сравнению с 4,2 миллиона долларов США в 2021 году и 3,9 миллиона долларов США в 2020 году [1]. Эта цифра является тревожным сигналом о серьезности последствий таких инцидентов и подчеркивает важность расследования каждого случая утечки данных. Каждая утечка данных не только влечет финансовые потери, но и подрывает доверие клиентов и репутацию организации. Таким образом, расследование утечек данных становится

критическим шагом для обеспечения безопасности данных и защиты интересов как частных лиц, так и компаний.

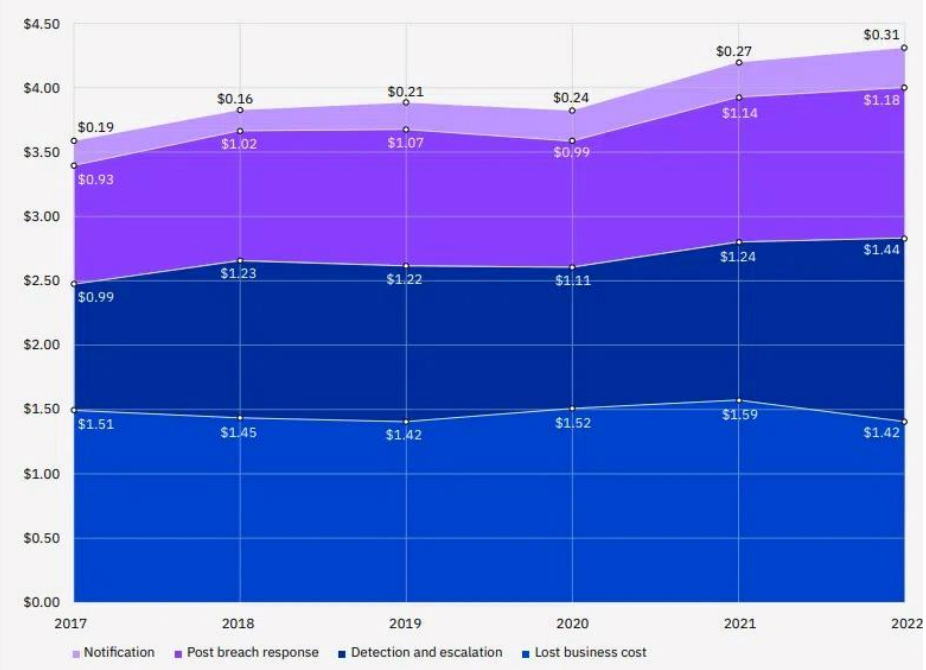

Рисунок 1. Средняя стоимость утечки данных за 2022 год. IBM (источник Allinsurance, 2017-2022гг.).

В свете этого, криминалистический анализ реестра Windows (рис. 2) выделяется как эффективный инструмент для расследования инцидентов утечек данных. Ведь, как показывает экспертная практика, системный реестр часто используется для решения таких задач, как определение факта использования зарегистрированным пользователем какой-либо программы, устройства внешней памяти и его содержимого, средств сетевой связи, времени инициализации и длительности этих событий [2]. Без исследования реестра, исследование информационной среды компьютера нельзя считать полным и объективным, поскольку значительная часть других областей следообразования имеет достаточно простую структуру и могут подвергаться корректировке со стороны злоумышленника. Настоящая статья связывает статистические данные о утечках данных с криминалистическими методами анализа реестра Windows, чтобы показать эффективность такого подхода.

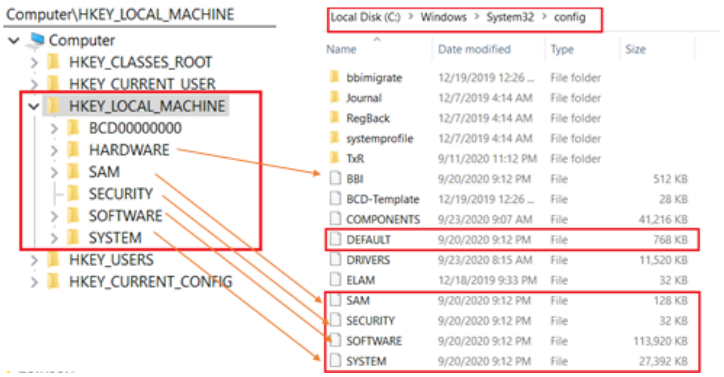

Рисунок 2. Системный реестр ОС Windows [3].

Рассмотрим процедуру расследования, связанную с реестром Windows. В процессе проведения всех подобных расследований необходимо наличие установленного RegRipper 3.0 и предполагается, что файлы, которые будут извлечены, содержат информацию реестра ПК.

1-шаг. Извлечение информации о компьютере и часовом поясе.

Отклик на команду *rip.pl -l* приводит к запуску RegRipper с параметром *-l*, который отображает список всех доступных плагинов. Вслед за этим *grep -i* name используется для фильтрации списка плагинов, чтобы найти тот из них, который имеет отношение к названию компьютера (рис. 3).

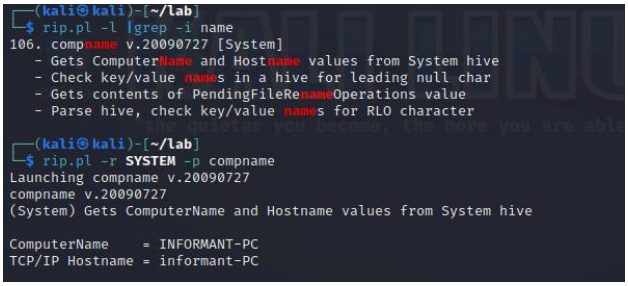

Рисунок 3. Извлечение информации о компьютере и часовом поясе.

2-шаг. Определение последнего пользователя, вошедшего в систему.

Ключ команды *rip.pl -r SOFTWARE -p lastloggedon* предназначен для выполнения анализа реестра операционной системы, в частности реестра SOFTWARE, с целью получения данных о последнем пользователе, который покинул систему (рис. 4).

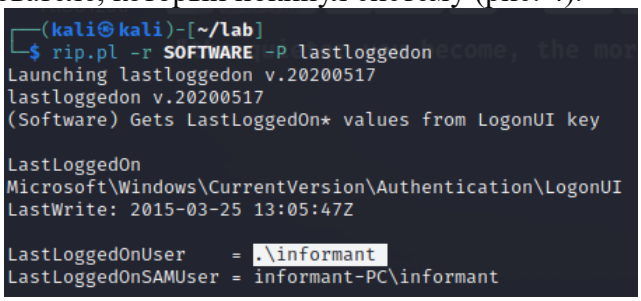

Рисунок 4. Определение последнего пользователя, вошедшего в систему.

3-шаг. Определение последней записанной даты/времени выключения.

Команда *rip.pl -r SYSTEM -p shutdown* используется для проведения анализа реестра операционной системы, конкретно реестра SYSTEM, с целью извлечения информации о последней дате и времени выключения компьютера. Вывод анализа указывает на то, что информатор последний раз вошел в систему в 13:05, а затем выключил компьютер в 15:31 (рис. 5).

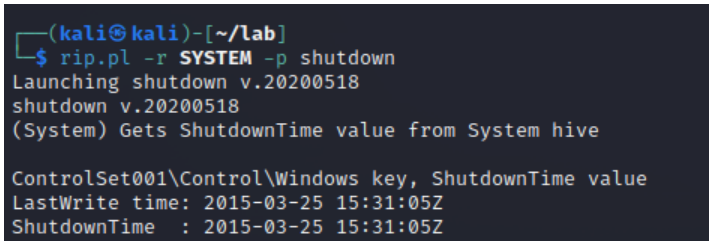

Рисунок 5. Определение последней записанной даты/времени выключения.

4-шаг. Определение установленных приложений после установки операционной системы.

Команда *rip.pl -r SOFTWARE -p installer | grep -E 2015 | head* используется для проведения анализа реестра программного обеспечения операционной системы с помощью инструмента RegRipper. Данная команда фильтрует результаты, чтобы показать приложения, установленные в определенный период времени (в данном случае, в 2015 году). Это помогает выявить приложения, установленные подозреваемым после установки операционной системы (рис. 6).

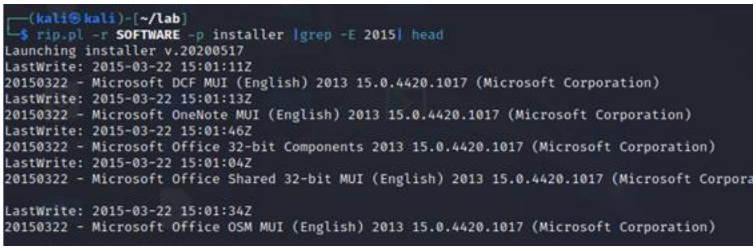

Рисунок 6. Определение установленных приложений после установки операционной системы.

5-шаг. Определение приложений, которые может удалить подозреваемый после установки операционной системы.

Команда *rip.pl -r SOFTWARE -p installer | head -n 12* используется для анализа реестра программного обеспечения операционной системы при помощи инструмента RegRipper. Эта команда выводит первые 12 записей об установленных приложениях, что позволяет выявить потенциальные программы, которые могут быть удалены подозреваемым после установки операционной системы (рис. 7).

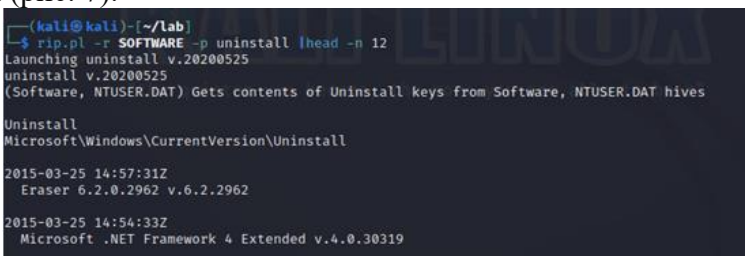

Рисунок 7. Определение приложений, которые может удалить подозреваемый после установки операционной системы.

В завершении стоит отметить, что процесс анализа реестра Windows с использованием инструмента RegRipper 3.0 является важным этапом в расследовании инцидентов компьютерной безопасности. Для того чтобы получить информацию о деятельности на системе, нам пришлось пройти ряд последовательных шагов. В результате мы получили сведения о том как работает система: начиная от определения информации о компьютере и часовом поясе, выявления последнего входа пользователя в систему и определения даты и времени последнего выключения компьютера. Дополнительно, мы проанализировали установленные и потенциально удаленные приложения после установки операционной системы. Этот многоступенчатый процесс анализа позволяет специалистам по информационной безопасности выявлять уязвимости и предотвращать потенциальные атаки. Полученные результаты обеспечивают основу для дальнейших расследований и эффективного реагирования на угрозы безопасности в компьютерных системах.

Список использованных источников

1. Казахстанский портал о страховании. «Средняя стоимость убытков от утечки данных в 2022 году выросла» [Электронный ресурс]. Режим доступа: https://allinsurance.kz/articles/analytical/19894-srednyaya-stoimost-ubytkov-ot-utechki-dannykh-v-2022-godu-vyrosla (дата обращения: 03.03.2024).

2. Gortinsky Alexey Vladimirovich «Some aspects of forensic analysis of the windows registry» [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/nekotorye-osobennosti-sudebno-ekspertnogo-issledovaniya-reestra-windows (дата обращения: 03.03.2024).

3. W. Xu, L. Deng, and D. Xu, "Towards Designing Shared Digital Forensics Instructional Materials," in Proceeding of the 46st Annual International Computer Software and Applications Conference (COMPSAC 2022), pp. 117-122, July 2022.