ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. А.Н.Тихонова

Домашнее задание №1, вариант 1. Основы цифровой форензики.
По направлению 10.04.01 – «Информационная безопасность»

Проверил:

преп. Сорокин А. В.

Подпись _____

Выполнил:

Новиков В. С. МКБ 241

Подпись _____

Москва 2025

Задание

Вариант 1.

Конфиденциальная переписка руководителя компании N, связанная с заключением новых контрактов с поставщиками и их обсуждением с рядом сотрудников оказалась размещенной в открытых источниках в сети Интернет.

Исходя из состава и текстов опубликованной переписки, можно заключить, что скомпрометирована именно учетная запись электронной почты руководителя. В качестве основного подозреваемого рассматривается системный администратор организации, ранее привлекавшийся для установки корпоративных программ на личный ноутбук руководителя. Помимо ноутбука руководить пользуется смартфоном, планшетом и домашним настольным компьютером. Для подключения к сети Интернет этих устройств – за исключением домашнего компьютера – он использует подключение через свой смартфон. У системного администратора имеются ноутбук и смартфон, для подключения к сети Интернет он использует мобильный интернет или общедоступные Wi-Fi-сети,

включая сеть компании N.

Требуется подтвердить или опровергнуть факт компрометации ноутбука руководителя и его почтового ящика, подтвердить или опровергнуть причастность системного администратора, выявить иные возможные каналы утечки электронных писем руководителя.

Решение

1. Что мы можем отдать экспертам для анализа

Для расследования инцидента необходимо предоставить экспертам следующие устройства и данные:

- **ноутбук руководителя** – возможный источник утечки, который мог быть скомпрометирован.
- **смартфон руководителя** – используется для подключения к интернету и может содержать следы компрометации.
- **планшет руководителя** – аналогично смартфону, мог использоваться для работы с почтой.
- **домашний настольный компьютер руководителя** – потенциальный источник утечки информации.
- **ноутбук системного администратора** – возможно использовался для организации атаки.
- **смартфон системного администратора** – может содержать следы компрометации или организации атаки.
- **журналы событий корпоративной почтовой системы** – помогут установить, откуда и когда осуществлялся доступ к учетной записи руководителя.
- **журналы сетевого трафика** – позволят выявить аномальные подключения и возможные утечки данных.
- **логи VPN-подключений (если использовались)** – помогут определить, был ли удаленный доступ к учетной записи руководителя.

2. Обоснование для передачи на экспертизу

Каждое из этих устройств или данных может содержать следы компрометации учетной записи электронной почты руководителя. Анализ оборудования и логов поможет:

- выявить вредоносное ПО, кейлоггеры или иные следы несанкционированного доступа.
- определить маршруты возможной утечки данных (локально или через интернет).
- проверить наличие сохраненных паролей и автозаполнения учетных данных.
- установить, были ли манипуляции с почтовым клиентом или веб-интерфейсом электронной почты.
- определить, осуществлял ли системный администратор или кто-то еще несанкционированный доступ.

3. Конкретные вопросы к экспертам

Экспертиза должна ответить на следующие ключевые вопросы:

1. Была ли учетная запись электронной почты руководителя скомпрометирована (да/нет)?
2. Был ли доступ к почтовому ящику получен с ноутбука руководителя (да/нет)?
3. Обнаружены ли на ноутбуке руководителя следы вредоносного ПО или кейлоггеров (да/нет)?

4. Происходила ли передача учетных данных почты через ноутбук или смартфон руководителя (да/нет)?
5. Был ли системный администратор причастен к компрометации почтового ящика (да/нет)?
6. Какие IP-адреса использовались для несанкционированного доступа?
7. Обнаружены ли на устройствах руководителя следы удаленного управления?
8. Могла ли утечка произойти через взлом домашней сети руководителя?
9. Есть ли признаки утечки данных через общественные Wi-Fi сети?

Эти вопросы позволят получить четкие выводы о характере инцидента и причастности конкретных лиц.

4. Выводы по расследованию инцидента

1. **Факт компрометации** – если будет подтвержден несанкционированный доступ к учетной записи почты руководителя, это укажет на взлом или утечку учетных данных.
2. **Источник компрометации** – анализ устройств позволит установить, откуда произошло вмешательство: с ноутбука, смартфона, планшета или стороннего источника.
3. **Метод атаки** – если найдены следы вредоносного ПО, кейлоггеров или фишинга, это поможет определить механизм утечки и позволят построить схему атаки в соответствии с MITRE ATT&CK и Cyber Kill Chain.
4. **Причастность системного администратора** – если на его устройствах найдены следы компрометации или взаимодействия с учетной записью руководителя, это станет основанием для дальнейших действий.
5. **Возможные альтернативные каналы утечки** – если компрометация не связана с системным администратором, стоит рассмотреть другие варианты: перехват трафика, взлом домашней сети или использование уязвимостей почтовой системы.
6. **Последствия инцидента** – оценка масштаба компрометации поможет понять, насколько критична утечка данных и нужно ли уведомлять партнеров, поставщиков и сотрудников.
7. **Рекомендации по устранению уязвимостей** – исходя из результатов экспертизы, необходимо принять меры по усилению защиты учетных записей, корпоративной сети и личных устройств руководителя.

Эти выводы помогут не только разобраться в конкретном инциденте, но и предотвратить подобные случаи в будущем.