УДК 004.056.5

Д. А. Шергин[1], Ю. О. Якович[1], А. Н. Поликанин[1]*

Использование инструментов OSINT для осуществления таргетированных атак

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[*] e-mail: shergindanil717@gmail.com

Аннотация. В мире, где цифровизация охватывает все аспекты нашей жизнедеятельности становиться все сложнее скрыть какую-либо информацию о себе в интернете, чем могут воспользоваться злоумышленники, совершив таргетированную атаку на организацию или частное лицо с целью кражи конфиденциальной информации или компрометации данных. Актуальность темы обусловлена простотой и доступностью в использовании такой технологии как OSINT, а также высокой тенденцией совершения таргетированных атак на организации и частные лица за последнее время. В статье описаны основные инструменты, которые может использовать злоумышленник для пассивного сбора информации о цели для совершения третированных атак, а также приведен реальный пример возможных действий злоумышленника и их последствий для организации. Для проведения практической части исследовательской работы были использованы такие инструменты, как Spiderfoot и Gophish. В статье также рассмотрены все необходимые меры для минимизации совершения успешных атак данного вида.

Ключевые слова: информационная безопасность, кибер-атака, разведка по открытым источникам, таргетированная атака

D. A. Shergin[1], Yu. O. Yakovich[1], A. N. Polikanin[1]*

Using OSINT tools to perform targeted attacks

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
[*] e-mail: shergindanil717@gmail.com

Abstract. In a world where digitalization covers all aspects of our lives, it is becoming increasingly difficult to hide any information about ourselves on the Internet, which can be used by attackers to launch a targeted attack on an organization or individual to steal confidential information or compromise data. The relevance of the topic is due to the simplicity and availability of such technology as OSINT, as well as the high trend of targeted attacks on organizations and individuals in recent times. This article describes the main tools that can be used by an attacker to passively collect information about the target to commit tertiary attacks, as well as a real example of possible actions of an attacker and their consequences for the organization. Tools such as Spiderfoot and Gophish were used to conduct the practical part of the research work. The article also discusses all the necessary measures to minimize the occurrence of successful attacks of this type.

Keywords: information security, cyber-attack, open-source intelligence, targeted attack

Введение

В современном мире цифровизация происходит в каждой сфере нашей жизнедеятельности. Люди ежедневно пользуются сервисами доставки и оплаты, гос-

ударственными услугами, социальными сетями и т.п. Вся информация, которая проходит от клиента к серверу и обратно, так или иначе, может оказаться в сети. Многие пользователи даже не задумываются о том, что оставляют о себе огромное количество информации в интернете, отсюда у злоумышленника появляется все больше возможностей собрать информацию о ком-либо для осуществления атаки [1].

Актуальность

На сегодняшний момент одним из самых популярных видов атак являются таргетированные атаки. Как показывает статистика компании Positive Technologies, число успешных таргетированных атак на организации к четвертому кварталу достигла своего максимума за 2023 год и стала трендом года (рис. 1).

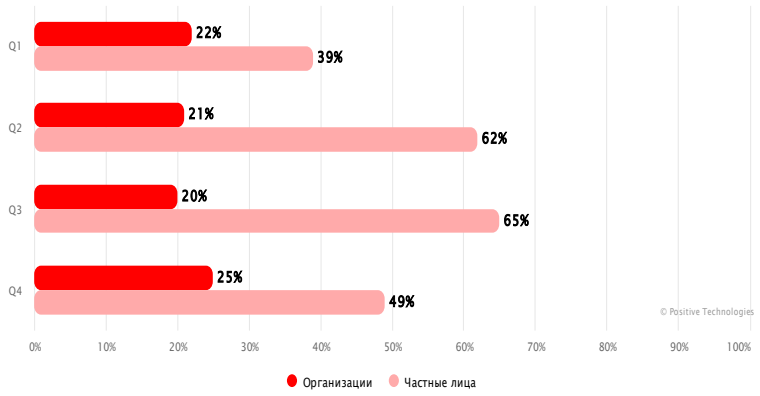

Рис. 1. Доля таргетированных атак от общего количества за каждый квартал 2023 год

Статистика показывает, что таргетированные атаки занимают большую часть киберугроз от всего объема. Основная проблема заключается в простоте реализации и огромном объеме информации об организациях, а также частных лицах, который злоумышленник может получить в интернете [2,3].

Технология пассивной разведки – OSINT

Для сбора информации о цели злоумышленник может прибегнуть к такой технологии, как OSINT. Open Source INTelligence – так звучит полная версия аббревиатуры на английском. Дословно это можно перевести как «разведка по открытым источникам». Основная суть этой технологии – поиск, сбор и анализ полученных данных, собранных из открытых источников в интернете, а также «слитых» баз данных и утечек информации [4, 5]. Собирая информацию о конкретной цели из общедоступных источников, злоумышленник может составить профиль потенциальной жертвы, чтобы лучше понять ее характеристики и сузить область поиска возможных уязвимостей [6, 7]. Без активного взаимодействия с целью злоумышленник может использовать полученные данные для по-

строения модели угрозы и разработки плана атаки. Таргетированные кибератаки, как и военные атаки, начинаются с разведки, и первый этап цифровой разведки – это пассивный сбор разведданных без оповещения цели [8]. Данные, которые собирает злоумышленник, могут содержать следующую информацию о цели:

– персональные данные;
– почтовые адреса;
– поддомены;
– IP-адреса и автономные системы компании;
– открытые порты и сервисы, находящиеся на них;
– подбор уязвимостей и эксплойтов для обнаруженных сервисов;
– конфиденциальные документы [4].

Ниже представлено несколько популярных сервисов по сбору информации о инфраструктуре сети, позволяющих собирать информацию об IP-адресах, поддоменах, MX-записях, адресах электронных почт, а также открытых портах, используемых протоколах:

– Dnsdumpster;
– Shodan;
– theHarvester;
– Spiderfoot.

Все ранее перечисленные ресурсы помогают собрать большой пласт информации о цели, зная которые злоумышленник способен развивать вектор своей атаки, переключаясь на физические лица, используя ресурсы для сбора таких данных, как номера телефонов, адреса, местоположение, паспортные данные и возможные пароли пользователей, утекшие в сеть [9–13].

Используя технологию OSINT, ход действий злоумышленника может быть примерно следующим: он может проанализировать домены и поддомены, в результате чего получить почтовые адреса из MX-записей домена, а также узнать возможные скрытые поддомены с секретным функционалом. Далее возможен более углубленный сбор данных о сетевой инфраструктуре, открытых портах и версиях сервисов на них. После чего происходит анализ полученных данных на предмет уязвимости. На этапе пассивной разведки взаимодействие с сетевой инфраструктурой можно закончить и использовать технологии OSINT для обширного сбора информации о сотрудниках по данным, которые были найдены на первых этапах, после чего возможна разработка таргетированных фишинговых атак. Стоит помнить и про то, что OSINT – это технология, применяемая для пассивной разведки, что означает отсутствие прямого контакта с целью во время сбора информации, тем самым позволяет остаться злоумышленнику незамеченным [14–16].

Практическая часть исследования

Для демонстрации описанного ранее материала был проведен эксперимент в рамках профессиональной деятельности. К компании обратился заказчик с целью проведения аудита осведомленности и действий сотрудников при получении подозрительной рассылки на корпоративную почту. В связи с соглашением

о неразглашении данные, раскрывающие личность заказчика, не приводятся. Заказчик предоставил 146 корпоративных электронных почт сотрудников. В рамках эксперимента был проведен поиск корпоративных почт по домену компании с применением такого инструмента, как Spiderfoot [10]. Данный инструмент позволил найти 83 корпоративных электронных почт сотрудников компании (рис. 2).

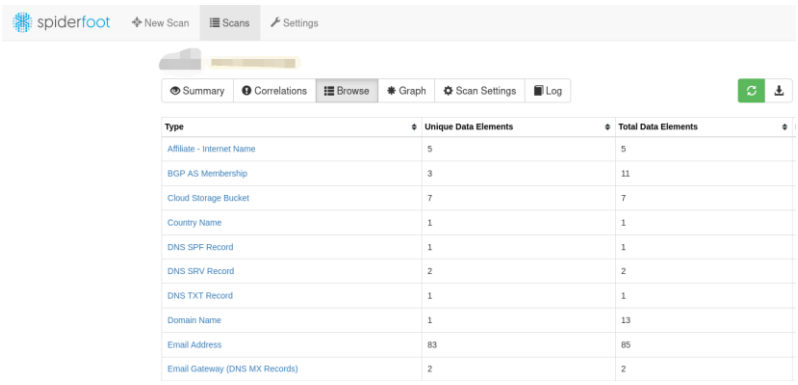

Рис. 2. Результат работы Spiderfoot

Сверив данные полученные от заказчика и данные полученные при помощи технологий OSINT, можно сказать, что 79 корпоративных адресов действующих сотрудников компании может найти потенциальный злоумышленник. Отсюда следует, что таргетированная атака на данную организацию весьма вероятна и может быть реализована злоумышленником для кражи конфиденциальных данных, распространения вредоносного ПО и проникновения внутрь системы организации, что может привести к ее полной компрометации. Далее была произведена фишинговая рассылка по шаблону, согласованному с заказчиком с помощью специального инструмента Gophish (рис. 3) [17].

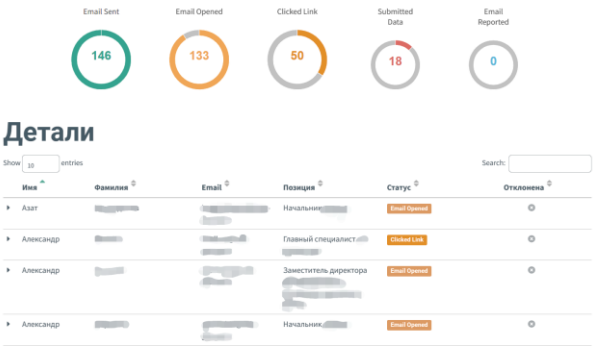

Рис. 3. Результаты рассылки на организацию

В результате данной рассылки были получены следующие данные:
– количество доставленных писем, равно 146;

– количество сотрудников, которые открыли электронное письмо – 133 сотрудника;

– количество сотрудников, которые перешли по ссылке, указанной в электронном письме – 50 человек;

– количество сотрудников, которые ввели свои учетные данные от корпоративного аккаунта и потенциально раскрыли свои данные злоумышленнику – 18 сотрудников.

Результат данной рассылки показал, что сотрудники компании заказчика являются достаточно грамотными с точки зрения информационной безопасности, а часть сотрудников, которые ввели свои данные, составила всего 12,32 % от всех сотрудников компании. Несмотря на достаточно неплохой результат, общий процент сотрудников, перешедших по ссылке в электронном письме, составил 34,25 %, что является достаточно высоким результатом, ведь злоумышленник мог внедрить атаку непосредственно в ссылку, находящуюся в письме [18, 19]. По завершению анализа полученных результатов была проведена встреча с Заказчиком и был составлен перечень мер, которые необходимо реализовать для повышения уровня информационной безопасности в организации среди сотрудников, а также был заключен договор на повторный аудит по истечению обговоренного времени и выполнения всех мер, обговоренных с заказчиком [20, 21].

Заключение

Данное исследование несет исключительно информативный характер и было выполнено с целью освещения такой темы, как технология OSINT, и того, что может достичь злоумышленник с ее помощью. В работе был представлен наглядный практический пример, основанный на реальных событиях, по результатам исследования была получена подробная статистика, которая подкрепляет актуальность проделанной работы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Балашов А.М. Использование ИТ-технологий в различных сферах деятельности и формирование новой информационно-цифровой реальности // Теоретическая экономика. 2022. №9. С.35-41.

2. Актуальные киберугрозы для организаций: итоги 2023 года. – Текст: электронный // Positive Technologies – 2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-dlya-organizacij-itogi-2023-goda/ – (дата обращения: 22.04.2024).

3. Актуальные киберугрозы: IV квартал 2023 года. – Текст: электронный // Positive Technologies – 2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q4/ – (дата обращения: 20.04.2024).

4. OSINT: инструменты. – Текст: электронный // Хабр – 2023. – URL: https://habr.com/ru/articles/769690/ – (дата обращения: 24.04.2024).

5. Open-Source Intelligence (OSINT) . – Текст: электронный // Imperva : [сайт]. – URL: https://www.imperva.com/learn/application-security/open-source-intelligence-osint/ – (дата обращения: 24.04.2024).

6. What Is Open Source Intelligence and How Is it Used? – Текст: электронный // Recorded Future – 2022. – URL: https://www.recordedfuture.com/blog/open-source-intelligence-definition – (дата обращения: 22.04.2024).

7. OSINT: в чем опасность и как защититься. – Текст: электронный // Kaspersky daily – 2023. – URL: https://www.kaspersky.ru/blog/osint-open-source-intelligence/35955/ – (дата обращения: 22.04.2024).

8. Хлестова Д., Попов К. Общий цикл развития таргетированных атак // Символ науки. 2016. №7. С.43-47.

9. OSINT Framework. Текст: электронный // OSINT Framework : [сайт]. – URL: https://osintframework.com/ – (дата обращения: 27.04.2024).

10. Spiderfoot. Текст: электронный // KALI : [сайт]. – URL: https://www.kali.org/tools/spiderfoot/ – (дата обращения: 26.04.2024)

11. Shodan Search Engine. Текст: электронный // Shodan : [сайт]. – URL: https://www.shodan.io/ – (дата обращения: 27.04.2024).

12. Theharvester. Текст: электронный // KALI : [сайт]. – URL: https://www.kali.org/tools/theharvester/ – (дата обращения: 27.04.2024)

13. DNSDumpster. Текст: электронный // DNSDumpster : [сайт]. – URL: https://dnsdumpster.com/ – (дата обращения: 22.04.2024).

14. Cik Feresa Mohd Foozy, Rabiah Ahmad, Mohd Faizal Abdollah. A framework for SMS spam and phishing detection in Malay language: A case study. United States (US): International Review on Computers and Software (IRECOS). 2014: p.1248-1255.

15. Ahmed Aleroud, Lina Zhou. Phishing environments, techniques, and countermeasures: A survey. Indiana: Computers & Security. 2017: p.160-196.

16. Спам и фишинг в 2022 году. – Текст: электронный // SecureList by Kaspersky – 2022. – URL: https://securelist.ru/spam-phishing-scam-report-2022/106719/ – (дата обращения: 22.04.2023).

17. Open-Source Phishing Framework. Текст: электронный // Gophish : [сайт]. – URL: https://getgophish.com/ – (дата обращения: 27.04.2024).

18. Шеер Е.Е. Актуальность вопроса подготовки квалифицированных специалистов в области информационной безопасности // Скиф. Вопросы студенческой науки. 2021. №1. С.7-12.

19. Методика оценки угроз безопасности информации. – Текст : электронный // Федеральная служба по техническому и экспортному контролю : [сайт]. – URL: https://fstec.ru/component/attachments/download/2919 (дата обращения: 20.12.2023).

20. Вилкова А.В, Литвишков В.М, Швырев Б.А. Проблемы непрерывного обучения персонала информационной безопасности // Мир науки, культуры, образования. 2019. №1. С.29-31.

21. J. Neumeier, A.L. Zelezinskii, O.V. Arhipova. Management of security of information in companies // Экономический вектор. 2023. №2. С.38-41.