Научная статья
Original article
УДК 004.424

ЗАХВАТ АККАУНТА

ACCOUNT TAKEOVER

Казарян Каторина Камоевна студент специалитета, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), kazaryan_katorina@mail.ru

Белан Виктория Вадимовна магистрант, Донской государственный технический университет, г. Ростов-на-Дону, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), viktoriyabelan2018@gmail.com

Kazaryan Katorina Kamoevna specialty student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), kazaryan_katorina@mail.ru

Belan Victoria Vadimovna Master student, Don State Technical University, Rostov-on-Don, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), viktoriyabelan2018@gmail.com

Аннотация В данной статье описана методика захвата аккаунта, процесс атаки в электронной коммерции, а также ее обнаружение на основе искусственного интеллекта. Обычно пользователи не меняют пароли регулярно и повторно используют данные для входа на разных сайтах. Злоумышленники могут использовать ботов, чтобы легко выполнять атаки с заполнением учетных данных и перебором, перебирая множество комбинаций пароля и имени пользователя для захвата учетной записи.

Abstract This article describes the account hijacking technique, the attack process in e-commerce, as well as its detection based on artificial intelligence. Typically, users do not change passwords regularly and reuse their login information across different sites. Attackers can use bots to easily perform credential stuffing and brute-force attacks, trying many combinations of password and username to take over an account.

Ключевые слова захват аккаунта, процесс атаки, электронная коммерция

Keywords account hijacking, attack process, e-commerce

Определение захвата аккаунта (ATO)

Захват учетной записи (ATO) - это атака, при которой киберпреступники становятся владельцами учетных записей в Интернете, используя украденные пароли и имена пользователей. Киберпреступники обычно покупают список учетных данных через темную сеть, обычно полученный в результате социальной инженерии , утечки данных и фишинговых атак . Они используют эти учетные данные для развертывания ботов, которые автоматически получают доступ к сайтам путешествий, розничной торговли, финансов, электронной коммерции и социальных сетей, для проверки комбинаций пароля и имени пользователя и попытки входа в систему.

В конце концов, злоумышленники получают список проверенных учетных данных и получают прибыль, продавая эти учетные данные другим людям или злоупотребляя учетной записью. Атаки, связанные с захватом учетных записей, вызывают кражу личных данных.

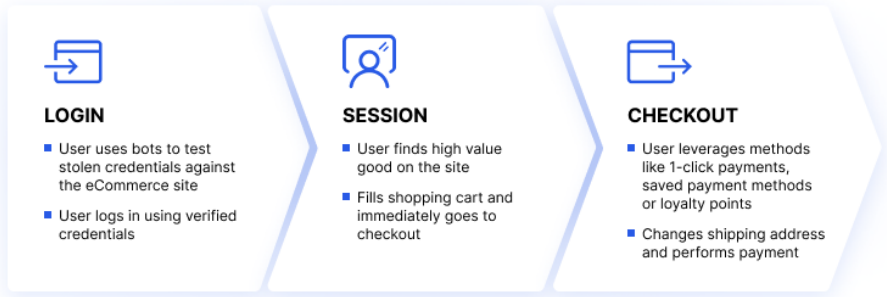
Киберпреступники также могут взломать страницы авторизации на мобильных сайтах, веб-сайтах и через собственные API-интерфейсы мобильных приложений. После того, как киберпреступники получают доступ, они могут совершать злоупотребления и мошенничество, связанные с захватом учетной записи, например, используя баллы лояльности пользователя.

Исторически финансовые учреждения больше всего беспокоились о мошенническом доступе к учетным записям пользователей. Сегодня атаки ATO могут повлиять на все организации, у которых есть доступ к пользователю. Наиболее распространенная мотивация киберпреступников - финансовая: киберпреступники обычно ищут самые быстрые и простые способы получения финансовой выгоды. Сегодня это включает в себя кражу криптовалюты, продажу личной информации или принуждение жертв к установке программ- вымогателей .

В разных ситуациях целью киберпреступника является сбор информации, позволяющей установить личность (PII). Личная информация очень востребована, потому что она может использоваться для кражи личных данных различными методами, например, путем совершения страхового мошенничества, получения данных кредитной карты и для кредитных линий.

Персональные данные могут использоваться в спам-кампаниях и фишинговых кампаниях, чтобы мошеннические сообщения выглядели более реалистичными, и чтобы помочь киберпреступникам добраться до своих жертв. Эти формы атак обычно нацелены на государственный сектор, медицинские и академические учреждения.

Атаки ATO также затрагивают сайты электронной коммерции. Киберпреступники могут завладеть существующей учетной записью и использовать ее для покупки товаров от имени пользователя. После компрометации учетной записи злоумышленники войдут в систему, быстро добавят дорогостоящие товары в корзину и произведут оплату, используя сохраненные учетные данные пользователя, изменив адрес доставки на свой собственный.



Процесс атаки ATO в электронной коммерции

Как происходит мошенничество с захватом аккаунта

Вот несколько распространенных векторов атак для захвата аккаунтов:

Кража учетных данных для входа в систему через нарушение данных

Ежегодно доступ к миллиардам документов о личных данных осуществляется через утечки данных. Утечка имен пользователей и паролей обычно требуется киберпреступникам, чтобы получить доступ к учетной записи. Учитывая, что многие люди используют идентичные данные для входа на несколько веб-сайтов или сервисов, киберпреступники будут пытаться получить доступ к разным онлайн-сервисам, используя просочившиеся имена пользователей и пароли.

Взлом учетных данных методом грубой силы

Киберпреступники могут получить доступ к вашим личным данным, пробуя различные пароли, чтобы узнать, какой из них правильный. Чтобы ускорить процесс, они используют ботов, которые могут проверять большое количество комбинаций паролей. Используя современные инструменты, доступные хакерам, 8-символьные пароли можно взломать за час или меньше.

Фишинг для получения информации для входа

Киберпреступники также могут просто попросить жертв предоставить им свои данные для входа. Это достигается с помощью фишинговых атак, во время которых жертв обманом заставляют предоставить свои данные. Попытки фишинга могут осуществляться с помощью SMS, электронной

почты, мошеннических веб-сайтов, чатов, вредоносных телефонных приложений, телефонных звонков и т. Д.

Кража данных с помощью вирусов и вредоносного ПО

Вирусы и вредоносные программы могут выполнять множество функций. Обычно они крадут информацию с устройства жертвы. Многие вирусы могут отслеживать нажатия клавиш при вводе паролей, а другие могут захватить банковские реквизиты, шпионя за вашим браузером. Вы можете остановить это с помощью антивирусного программного обеспечения.

Человек посередине (MitM) атакует

Ваш интернет-трафик проходит через множество серверов, прежде чем попасть на веб-сайт. Если человек перехватывает ваш трафик, пока он находится в пути, и он не зашифрован, он может просматривать все ваши передвижения в Интернете, включая ваши имена пользователей и пароли. Как правило, эти атаки типа "злоумышленник посередине" осуществляются через домашние интернет-маршрутизаторы или общедоступные сети Wi-Fi. Вы можете обезопасить себя с помощью надежного программного обеспечения VPN.

Выявление мошенничества с захватом счетов в финансовых учреждениях

В финансовых учреждениях АТО более серьезен, потому что он может напрямую привести к краже и компрометации финансовых счетов человека. Постоянный мониторинг дает организациям возможность увидеть признаки мошенничества, представляющие собой захват учетной записи, до того, как это произойдет.

Хорошая система обнаружения мошенничества предоставит финансовым учреждениям полную информацию о действиях пользователя на протяжении всего процесса транзакции. Самая эффективная защита - это система, которая проверяет все действия на банковском счете: прежде чем киберпреступник сможет забрать деньги, он должен сначала предпринять другие действия, в том числе создать получателя платежа.

Отслеживая каждое действие в учетной записи, вы можете выделить модели поведения, указывающие на вероятность мошенничества с захватом учетной записи. Киберпреступники должны выполнить различные действия, прежде чем переводить деньги со счета, поэтому процесс обнаружения мошенничества, который постоянно отслеживает поведение, может выявить подсказки и шаблоны, чтобы определить, подвергается ли клиент атаке.

Этот вид процесса обнаружения мошенничества также позволяет отслеживать риски на основе информации, в том числе местоположения. Например, если клиент сначала получает доступ к своей учетной записи из Южной Америки, а затем через 20 минут из Азии, это может быть подозрительным и может свидетельствовать о том, что два разных человека используют одну и ту же учетную запись.

Защита от захвата аккаунта

Вот несколько способов защитить свою организацию от ATO.

Многофакторная аутентификация

На этом этапе попросите вашего пользователя пройти аутентификацию, используя что-то помимо пароля:

- **Что-то, что они знают** - секретный вопрос, например, девичья фамилия их матери, имя первого питомца и т. Д.
- **Что-то, что у них есть** - жетон, ключ или другой физический объект.
- **Что-то такое** - идентификатор лица, скан радужной оболочки глаза, отпечаток пальца или что-то подобное.

Вам не нужно постоянно запрашивать это MFA, и вы можете создать адаптивный процесс, который варьируется в зависимости от предполагаемого риска. Например, вы можете запросить двухфакторную аутентификацию после того, как пользователь попытается получить доступ к учетной записи с другого устройства входа или из необычного места.

Система отслеживания учетной записи

Когда учетная запись взломана, у вас должен быть процесс, который остановит дальнейшие атаки. Поместив в песочницу учетную запись, которая считается подозрительной, вы можете проверить все действия, связанные с этой учетной записью, и при необходимости приостановить действие учетной записи.

Обнаружение на основе ИИ

Процессы защиты и обнаружения АТО на основе искусственного интеллекта могут обнаруживать более изощренные попытки захвата учетных записей и атаки ботов. Попытки АТО часто связаны с использованием ботов четвертого поколения, которые способны имитировать поведение людей, и поэтому их труднее изолировать. Передовая технология на основе искусственного интеллекта необходима для выявления изощренных попыток АТО и успешного мониторинга сайта на предмет подозрительного поведения.

Брандмауэр веб-приложений (WAF)

Web Firewall Application (WAF) защищает веб - приложения с помощью фильтрации HTTP - трафика. WAF могут идентифицировать вредоносный трафик и блокировать его. WAF могут помочь смягчить атаки АТО одним или несколькими из следующих методов:

- Выявление и блокировка запросов от известных злоумышленников
- Обнаружение плохих ботов, используемых злоумышленниками в рамках атак АТО
- Определите набивку учетных данных на порталах входа в систему
- Обнаружение и блокировка атак методом грубой силы путем определения сеансов, передающих необычное количество учетных данных
- Включение многофакторной аутентификации (MFA) или аутентификации через сторонних поставщиков удостоверений, таких как Google
- Сканирование трафика на предмет «отпечатков пальцев», указывающих на инструменты заполнения учетных данных

Литература

1. Mark Liberman Phishing - itre.cis.upenn.edu/~myl/languagelog/archives/001477.html (англ.) (22 сентября 2004).
2. Cave Paintings Phishing - historyofscience.com/G2I/timeline/index.php?id=1682 (англ.).
3. Usenet - groups.google.com/group/alt.online-service.america-online (англ.). — 2 января 1996 г.
4. The Phishing Guide - www.webcitation.org/5w9YT7W5q (англ.). Архивировано из первоисточника - www.technicalinfo.net/papers/Phishing.html 31 января 2011.
5. phishing - www.webcitation.org/5w9YTyC3n (англ.) (1 августа 2003). Архивировано из первоисточника - www.wordspy.com/2003/08/phishing.html 31 января 2011.
6. Michael Stutz AOL: A Cracker's Paradise? - wired-vig.wired.com/science/discoveries/news/1998/01/9932 (англ.) (29 января 1998).
7. History of AOL Warez - www.webcitation.org/5w9YV2fuL (англ.). Архивировано из первоисточника - www.rajuabju.com/warezirc/historyofaolwarez.htm 31 января 2011.

References

1. Mark Liberman Phishing - itre.cis.upenn.edu/~myl/languagelog/archives/001477.html (English) (September 22, 2004).
2. Cave Paintings Phishing - historyofscience.com/G2I/timeline/index.php?id=1682.
3. Usenet - groups.google.com/group/alt.online-service.america-online (English). - January 2, 1996

4. The Phishing Guide - www.webcitation.org/5w9YT7W5q (English). Archived from the original - www.technicalinfo.net/papers/Phishing.html January 31, 2011.
5. phishing - www.webcitation.org/5w9YTyC3n (English) (August 1, 2003). Archived from the original - www.wordspy.com/2003/08/phishing.html on January 31, 2011.
6. Michael Stutz AOL: A Cracker's Paradise? - wired-vig.wired.com/science/discoveries/news/1998/01/9932 (January 29, 1998).
7. History of AOL Warez - www.webcitation.org/5w9YV2fuL. Archived from the original - www.rajuabju.com/warezirc/historyofaolwarez.htm on January 31, 2011.

© Казарян К.К., Белан В.В., 20221 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.

Для цитирования: Казарян К.К., Белан В.В. ЗАХВАТ АККАУНТА // Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.