УДК 004

Жуков С.В.
студент магистратуры
2 курс, факультет «Информационная безопасность»
ИМИТ СКФУ, Россия, г. Ставрополь
Леджиев Д.Ю.
студент магистратуры
2 курс, факультет «Информационная безопасность»,
ИМИТ СКФУ, Россия, г. Ставрополь
Научный руководитель: Минкина Т.В.
кандидат технических наук, доцент кафедры «ОТЗИ»
Zhukov S.V.
graduate student
2st year, Faculty of "Information Security"
IMIT NCFU, Russia, Stavropol
Ledzhiev D.Yu.
graduate student
2st year, Faculty of "Information Security",
IMIT NCFU, Russia, Stavropol
Scientific adviser: Minkina T.V.
Candidate of Technical Sciences, Associate Professor of the
Department "OTZI"

ТАКТИКА ЗАЩИТЫ ОТ ПЕРЕПОЛНЕНИЯ УЧЕТНЫХ ДАННЫХ

В статье говорится о проблеме переполнения учетных данных и тактике построения защиты от такого рода атак. Проблема, связанная с авторизацией пользователей, появилась из-за огромного роста количества веб-сервисов, где пользователь авторизуется, используя одинаковые данные для входа в систему. Это приводит к проблеме обеспечения конфиденциальности данных не скомпрометированных веб-сервисов. Для противодействия такому роду атак рекомендуется использование MFA и системы анализа трафика.

Ключевые слова: аутентификация, учетные данные, атака, защита данных.

TACTICS FOR DEFENDING AGAINST CREDENTIAL STUFFING

The article deals with the problem of credential overflow and tactics for building protection against such attacks. The problem with user authorization has arisen due to the huge growth in the number of web services where a user logs in using the same login information. This leads to the problem of ensuring the confidentiality of the data of non-compromised web services. To counter this type of attack, the use of MFA and a traffic analysis system is recommended.

Keywords: authentication, credentials, attack, data protection.

Введение

Атаки с заполнением учетных данных на данный момент являются огромной отраслевой проблемой и обычно реализуются с помощью однофакторной аутентификации, взломанных списков учетных данных, повторного использования паролей и инструментов для реализации атаки.

На многих веб-сайтах и в приложениях обычно предлагают только выбор пароля для аутентификации, чтобы получить доступ. Для сокращения такого рода атак требуется некоторые усовершенствования, одним из которых является многофакторная аутентификация (MFA), реализация такой системы позволит сократить риски потери конфиденциальной информации.

Скомпрометированный список учетной информации может содержать множество учетных данных, которые могут быть не актуальными, но помимо бесплатных списков бывают и платные в которых с большей долей вероятности получится обнаружить необходимую информацию. Такие сервисы собирают свои базы данных несколькими способами, например, с помощью фишинговых атак или через небезопасные базы данных, в то время как повторное использование паролей слишком распространено, когда средний пользователь имеет 26 учетных записей и пять паролей.

Целями этих атак обычно являются услуги по подписке, так как входе атаки злоумышленники получают доступ к учетным записям они обычно продаются по более низкой цене на теневых форумах.

Что касается воздействия на компании, репутация таких компании может быть подорвана, а «негативная ассоциация может длиться годами», что приведет к освещению в СМИ, а также к потере доверия со стороны пользователей. Финансовые последствия выражаются в затратах на расследование, остановку обслуживания и на устранение последствий атаки.

Чтобы снизить риски реализации подобных атак рекомендуется проводить анализ вашего трафика, а также сравнить его с эталонным, чтобы могли обнаружить всплески и неудачных попыток входа в систему. Также рекомендуется отслеживать неудачные попытки входа в систему с IP-адресов, чтобы понять, откуда исходит атака.

«Основной способ защиты — это увеличение систем проверки подлинности пользователя», можно выделить три основных системы: многофакторная аутентификация, обнаружение взломанного пароля и обнаружение ботов. Создание таких систем в веб сервисах позволяет в реальном времени отслеживать потенциальные атаки и своевременно предотвращать их.

При обнаружении ботов рекомендуется добавить Captcha, так как она позволяют блокировать нежелательный трафик, создаваемый попытками авторизации ботов.

Что касается обнаружения взломанных паролей, сервис Auth0 хранит базу данных общих паролей и предупреждает пользователя, если он использует слабый и часто используемый пароль. Систему многофакторной аутентификации (MFA) можно добавить в качестве дополнительного способа защиты данных для пользователя.

Выводы

В заключение можно отметить, что совокупность управления паролями, обнаружения ботов и анализ трафика может помочь в обнаружении и отражении атак с заполнением учетных данных. Так же при внедрении многофакторной аутентификации (MFA) можно сократить риски потери конфиденциальной информации пользователей систем.

Использованные источники:

1. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.

2. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018. - 88 с.

3. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. - М.: Гелиос АРВ, 2010. - 336 с.

4. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: Форум, 2018. - 256 с.4. Лобанков И.Д. Современные концепции виртуальной реальности. / Вестник ПАГС. – 2015. – С. 98-103.