Научная статья
Original article
УДК 004.424

АТАКИ НА РАЗЛИЧНЫЕ СФЕРЫ ДЕЯТЕЛЬНОСТИ

ATTACKS ON VARIOUS FIELDS OF ACTIVITY

Куренная Валерия Олеговна, студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), kurinaaa@rambler.ru

Kurennaya Valeria Olegovna, bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), kurinaaa@rambler.ru

Аннотация. Атаки на различные сферы деятельности человека на данном этапе развития общества стали обыденностью. В данной статье описаны методы работы злоумышленников, как например мошенник может выдать себя за финансового директора или сотрудника финансового отдела и попытаться убедить цель перевести средства на оффшорный счет, мошенничество в сфере социального обеспечения и медицинского обслуживания. Существуют сценарии анализа и избегания потери данных в данных ситуациях.

Annotation. Attacks on various spheres of human activity at this stage of the development of society have become commonplace. This article describes how attackers work, such as a fraudster who can impersonate a CFO or an employee of the finance department and try to convince the target to transfer funds to an offshore

account, fraud in the field of social security and medical care. There are scenarios for analyzing and avoiding data loss in these situations.

Ключевые слова: Атака, вишинг, информационная безопасность.

Key words: Attack, vishing, information security.

Чаще всего атаки идут на банковскую сферу. Злоумышленники пытаются украсть финансовую информацию, такую как номера банковских счетов и кредитных карт. Один из методов, который они используют, чтобы обмануть своих жертв, — это подмена идентификатора, когда они выдают себя за владельца, используя идентификатор, который выглядит подлинным. Например, мошенник может выдать себя за финансового директора или сотрудника финансового отдела и попытаться убедить цель перевести средства на оффшорный счет.

Незапрашиваемые инвестиции и кредитные предложения

Мошенники часто называют своих целей, предлагая нереально заманчивые сделки, такие как быстрые решения для погашения долгов или схемы быстрого обогащения. Эти предложения, как правило, требуют немедленных действий, сопровождаемых комиссией. Законный кредитор или инвестор не инициирует нежелательные контакты и не делает чрезмерно оптимистичных предложений.

Мошенничество в сфере социального обеспечения и медицинского обслуживания

Телефонные звонки являются предпочтительным методом для обмана старых целей. Мошенники часто выдают себя за представителей Medicare или Управления социального обеспечения. Они могут попытаться украсть личную информацию, такую как номера Medicare или Social Security, или угрожать приостановкой или прекращением льгот. Мошенники могут использовать украденную информацию для кражи денег или перенаправления выгод.

Налоговое мошенничество

Мошенники часто отправляют предварительно записанное сообщение якобы от IRS, информируя жертв о предполагаемой проблеме с их налоговыми декларациями. Поддельные идентификаторы вызывающего абонента часто создают впечатление, что звонок исходит от IRS.

Профилактика Вишинга

Осведомленность о кибербезопасности

Вы должны включить следующие пункты в свой тренинг по повышению осведомленности о кибербезопасности:

Никогда не раскрывайте личные данные — вишинг-атаки предназначены для того, чтобы заставить цель раскрыть личную информацию, которую злоумышленники могут использовать для других атак или мошенничества. Никогда не сообщайте номер многофакторной аутентификации (MFA), пароль, финансовые данные или аналогичные данные по телефону.

Всегда проверяйте номера телефонов — вам могут позвонить вишеры, выдавая себя за представителей законной организации. Прежде чем предоставлять какую-либо личную информацию или следовать инструкциям звонящего, узнайте его имя и убедитесь, что вы можете связаться с ним по официальному номеру компании. Если звонящий пытается отговорить вас от этого, скорее всего, это мошенничество.

Организации не принимают оплату с помощью предоплаченных или подарочных карт — посетители часто просят оплатить суммы, которые жертва предположительно должна в виде предоплаченных или подарочных карт. Ни одна законная организация не будет запрашивать предоплаченную кредитную или подарочную карту в качестве оплаты.

Никогда не предоставляйте удаленный доступ к компьютеру — вишеры могут запросить удаленный доступ к вашему компьютеру под предлогом удаления вредоносного ПО или решения какой-либо проблемы. Вы никогда не должны предоставлять кому-либо доступ к вашему компьютеру, если только они не являются проверенными сотрудниками ИТ-отдела.

Сообщайте о подозрительных инцидентах — вишеры обычно повторяют одну и ту же аферу по нескольким целям. Сообщайте властям или сотрудникам службы безопасности вашей организации о предполагаемых вишинг-атаках, чтобы они могли защитить другие цели.

Смягчение дополнительных векторов атак

В отличие от фишинга, вишинг трудно остановить с помощью технологий. Поскольку вишинг происходит по телефону, организация должна будет прослушивать все телефонные звонки и находить предупреждающие знаки, чтобы обнаружить атаку.

В связи с этим организациям следует построить модель угроз и сосредоточиться на целях злоумышленника при предотвращении вишинг-атак. Например, вишинг-атака, нацеленная на организацию, может иметь одну из нескольких целей:

Заражение компьютера сотрудника вредоносным ПО

Компрометация учетных данных сотрудника

Получение доступа или контроля над устройством пользователя

Изолируя каждый из этих сценариев угроз, организация может внедрять решения, которые останавливают злоумышленников на более поздних этапах атаки, даже если первоначальный вызов вишинга остается необнаружимым.

Существует различные способы для решения обеспечения безопасности электронной почты, архивирования и непрерывности работы позволяют клиентам стать более устойчивыми к целенаправленным фишинговым атакам и многим другим угрозам, с которыми сталкивается корпоративная безопасность.

Литература

1. Ван Хайтао Исследование системы осведомленности об информационной безопасности на основе технологий больших данных и искусственного интеллекта, Технологии и приложения сетевой безопасности, 2018 (3): 60-63.

2. Чжэн Яньфан Исследования и практика применения искусственного интеллекта и технологий анализа в системе ситуационной осведомленности информационной безопасности Мир цифровых коммуникаций, 2018, № 160 (4): 229.
3. Чжэн Фан Информационная безопасность в эпоху искусственного интеллекта, Исследования в области информационной безопасности, 2017, 3 (11): 966-967.
4. Дэн Вэньбинь Проблемы и меры противодействия надзору за информационной безопасностью в эпоху искусственного интеллекта Информационная безопасность Китая, 2018 г., 106 (10): 106-108.

References

1. Wang Haitao Research on Information Security Situation Awareness System Based on Big Data and Artificial Intelligence Technology, Network Security Technology and Application, 2018 (3): 60-63.
2. Zheng Yanfang Research and Practice of Artificial Intelligence Application and Analysis Technology in Information Security Situational Awareness System Digital Communication World, 2018, No.160 (4):229.
3. Zheng Fang Information Security in the Age of Artificial Intelligence, Information Security Research, 2017, 3 (11): 966-967.
4. Deng Wenbing Challenges and Countermeasures for Information Security Supervision in the Age of Artificial Intelligence China Information Security, 2018, 106 (10): 106-108.

© Куренная В.О., 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №6/2022.

Для цитирования: Куренная В.О. АТАКИ НА РАЗЛИЧНЫЕ СФЕРЫ ДЕЯТЕЛЬНОСТИ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №6/2022.