АТАКИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

SOCIAL ENGINEERING ATTACKS

УДК 004.424

Камбулов Данил Александрович, магистрант, Донской государственный технический университет, г. Ростов-на-Дону

Kambulov D. A. kambulovdan@yandex.ru

Аннотация

Социальная инженерия - это термин, используемый для широкого спектра вредоносных действий, совершаемых посредством человеческих взаимодействий. Он использует психологические манипуляции, чтобы обманом заставить пользователей совершать ошибки безопасности или выдавать конфиденциальную информацию.

Атаки социальной инженерии происходят в один или несколько этапов. Преступник сначала исследует предполагаемую жертву, чтобы собрать необходимую справочную информацию, такую как потенциальные точки входа и слабые протоколы безопасности, необходимые для продолжения атаки. Затем злоумышленник пытается завоевать доверие жертвы и создать стимулы для последующих действий, нарушающих правила безопасности, таких как раскрытие конфиденциальной информации или предоставление доступа к критически важным ресурсам.

Annotation

Social engineering is a term used for a wide variety of harmful acts performed through human interactions. It uses psychological manipulation to trick users into making security errors or giving away confidential information.

Social engineering attacks occur in one or more stages. The attacker first examines the alleged victim in order to gather the necessary background information, such as potential entry points and weak security protocols required to continue the attack. The attacker then tries to gain the victim's trust and create incentives for follow-up actions that violate security rules, such as disclosing confidential information or providing access to critical resources.

Ключевые слова: социальная инженерия, фишинг, злоумышленник, атака, информационная безопасность, жертва, вредоносное программное обеспечение.

Keywords: social engineering, phishing, intruder, attack, information security, victim, malicious software.

Социальная инженерия заключается в том, чтобы обманом заставить пользователей предоставить точку входа для вредоносных программ. Жертва предоставляет конфиденциальную информацию или невольно устанавливает вредоносное ПО на свое устройство, потому что злоумышленник выдает себя за законного участника [1].

Вот некоторые из основных типов атак социальной инженерии:

Приманка - злоумышленник заманивает пользователя в ловушку социальной инженерии, обычно обещая что-то привлекательное, например бесплатную подарочную карту. Жертва предоставляет злоумышленнику конфиденциальную информацию, такую как учетные данные.

Претекст - **аналогично** травле, злоумышленник **вынуждает цель передать** информацию под ложным предлогом. Обычно это подразумевает выдачу себя за кого-то, наделенного властью, например сотрудника IRS или полиции, чья позиция заставит жертву подчиниться.

Фишинг - злоумышленник рассылает электронные письма якобы из надежного источника. Фишинг часто связан с отправкой мошеннических писем как можно большему количеству пользователей, но он также может быть более целенаправленным. Например, «целевой фишинг» персонализирует

электронную почту для нацеливания на конкретного пользователя, в то время как «китобойный промысел» делает еще один шаг вперед, ориентируясь на ценных людей, таких как генеральные директора.

Вишинг (голосовой фишинг) - самозванец использует телефон, чтобы обманом заставить цель раскрыть конфиденциальные данные или предоставить доступ целевой системе. Вишинг обычно нацелен на пожилых людей, но может быть использован против кого угодно.

Smishing (SMS-фишинг) - злоумышленник использует текстовые сообщения как средство обмана жертвы.

Совмещение - авторизованный пользователь предоставляет физический доступ другому человеку, который «совмещает» учетные данные пользователя. Например, сотрудник может предоставить доступ кому-то, выдающему себя за нового сотрудника, который потерял свою учетную карту.

Захват - неавторизованное лицо следует за авторизованным пользователем в определенное место, например, быстро проскользнув через защищенную дверь после того, как авторизованный пользователь ее открыл. Этот метод похож на совмещение, за исключением того, что человек, которого преследуют, не подозревает, что его использует другой человек [2,3].

Атаки на цепочку поставок

Атаки на цепочки поставок представляют собой новый тип угроз для разработчиков и поставщиков программного обеспечения. Его цель - заражать легитимные приложения и распространять вредоносное ПО через исходный код, процессы сборки или механизмы обновления программного обеспечения.

Злоумышленники ищут незащищенные сетевые протоколы, серверную инфраструктуру и методы кодирования и используют их для компрометации процесса сборки и обновления, изменения исходного кода и скрытия вредоносного содержимого [4].

Атаки на цепочку поставок особенно серьезны, потому что приложения, скомпрометированные злоумышленниками , подписаны и сертифицированы надежными поставщиками. При атаке на цепочку поставок программного

обеспечения поставщик программного обеспечения не знает, что его приложения или обновления заражены вредоносным ПО. Вредоносный код работает с теми же доверием и привилегиями, что и скомпрометированное приложение [5].

Типы атак на цепочку поставок включают:

Компрометация инструментов сборки или конвейеров разработки

Компрометация процедур подписи кода или учетных записей разработчиков

Вредоносный код, отправляемый в виде автоматических обновлений оборудования или компонентов прошивки

Вредоносный код, предустановленный на физических устройствах

Атака человека посередине

Человек-в-середине (MitM) атаки включает в себя перехват связи между двумя конечными точками, например, пользователем и приложением. Злоумышленник может подслушивать общение, украсть конфиденциальные данные и выдать себя за каждую сторону, участвующую в общении.

Примеры атак MitM включают:

Подслушивание Wi-Fi - злоумышленник устанавливает соединение Wi-Fi, выдавая себя за законного субъекта, такого как бизнес, к которому могут подключаться пользователи. Мошеннический Wi-Fi позволяет злоумышленнику отслеживать активность подключенных пользователей и перехватывать такие данные, как данные платежной карты и учетные данные для входа.

Email угон - Атакующий подменяет адрес электронной почты легитимной организации, такой как банк, и использует его , чтобы заставить пользователей отказаться от конфиденциальной информации или перевода денег на злоумышленника. Пользователь следует инструкциям, которые, по его мнению, исходят из банка, но на самом деле исходят от злоумышленника.

Подмена DNS. Сервер доменных имен (DNS) подделывается, направляя пользователя на вредоносный веб-сайт, выдающий себя за законный.

Злоумышленник может перенаправить трафик с легального сайта или украсть учетные данные пользователя.

IP-спуфинг - адрес интернет-протокола (IP) соединяет пользователей с определенным веб-сайтом. Злоумышленник может подделать IP-адрес, выдавая себя за веб-сайт, и заставить пользователей думать, что они взаимодействуют с этим веб-сайтом.

Подмена HTTPS. HTTPS обычно считается более безопасной версией HTTP, но также может использоваться, чтобы заставить браузер думать, что вредоносный веб-сайт безопасен. Злоумышленник использует HTTPS в URL-адресе, чтобы скрыть вредоносный характер веб-сайта [6].

Следующие советы могут помочь повысить бдительность в отношении социальных инженерных взломов.

Не открывайте электронные письма и вложения из подозрительных источников – если вы не знаете отправителя, вам не нужно отвечать на электронное письмо. Даже если вы знаете их и подозреваете их сообщение, перепроверьте и подтвердите новости из других источников, таких как по телефону или непосредственно с сайта поставщика услуг. Помните, что адреса электронной почты все время подделываются; даже сообщение электронной почты, предположительно поступающее из надежного источника, может быть на самом деле инициировано злоумышленником.

Используйте многофакторную аутентификацию. Одной из самых ценных частей информации, которую ищут злоумышленники, являются учетные данные пользователя. Использование многофакторной аутентификации помогает обеспечить защиту вашей учетной записи в случае компрометации системы.

Будьте осторожны с заманчивыми предложениями. Если предложение звучит слишком заманчиво, подумайте дважды, прежде чем принять его как факт. Поиск в системах этой темы поможет вам быстро определить, имеете ли вы дело с законным предложением или ловушкой.

Обновляйте свое антивирусное/антивирусное программное обеспечение – убедитесь, что включены автоматические обновления, или возьмите за привычку

первым делом каждый день скачивать последние сигнатуры. Периодически проверяйте, были ли применены обновления, и сканируйте вашу систему на предмет возможных инфекций.

Литература

1. Кевин Митник, Вильям Саймон «Искусство обмана»: Компания АйТи; 2004
2. Крис Касперски «Секретное оружие социальной инженерии»: Компания АйТи; 2005
3. Домарев В. В. Безопасность информационных технологий. Системный подход — К.: ООО ТИД Диа Софт, 2004. — 992 с.
4. Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009.
5. Гришина Н.В. – Организация комплексной защиты информации. – М: Гелиос АРВ, 2007. – 256.
6. Козиол Дж., Личфилд Д., Эйтэл Д., Энли К. и др. Искусство взлома и защиты систем. — СПб/ Питер, 2006. — 416 с: ил.

Literature

1. Kevin Mitnick, William Simon "The Art of Deception": IT Co.; 2004
2. Chris Kaspersky "The Secret Weapon of Social Engineering": IT Co.; 2005
3. Domarev V.V. Security of information technologies. Systematic approach - Kiev: OOO TID Dia Soft, 2004 .-- 992 p.
4. Information security (2nd book of the socio-political project "Actual problems of social security"). M .: "Arms and Technologies", 2009.
5. Grishina N.V. - Organization of comprehensive information protection. - M: Helios ARV, 2007 .-- 256.
6. Coziol J., Lichfield D., Eitel D., Enley K. et al. The art of hacking and protecting systems. - SPb / Peter, 2006 .-- 416 p: ill.