УДК 004.736

**HIDDENEYE: ИНСТРУМЕНТ ДЛЯ ФИШИНГА**

**Бютнер С.И.**

*ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: serafimkavasaki@gmail.com*

**HiddenEye — это популярный инструмент для создания фишинговых страниц, который активно используется злоумышленниками для кражи учётных данных и другой конфиденциальной информации. Статья раскрывает технические возможности HiddenEye, типы атак, которые могут быть осуществлены с его помощью, а также методы защиты от фишинговых угроз, включая фильтрацию почты, использование многофакторной аутентификации и обучение пользователей распознаванию фишинга.**

Ключевые слова:HiddenEye, фишинг, кибербезопасность, фишинговые атаки, кража данных, защита.

**HIDDENEYE: A PHISHING TOOL**

**Buetner S.I.**

*ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: serafimkavasaki@gmail.com*

**As the popularity of containers and containerization technologies like Docker and Kubernetes grows, cybercriminals are actively seeking vulnerabilities within these environments. Container vulnerabilities pose serious security risks, potentially leading to malicious code execution and unauthorized data access. The article covers key types of container vulnerabilities, examples of real attacks, and protection methods such as updating images, configuring access controls, and regular vulnerability scanning.**

Keywords: HiddenEye, phishing, cybersecurity, phishing attacks, data theft, protection.

**Введение**

С ростом цифровизации и внедрением онлайн-сервисов, фишинг остаётся одной из самых распространённых и эффективных кибератак. Злоумышленники всё активнее используют специализированные инструменты для создания фальшивых сайтов и приложений, которые маскируются под популярные веб-сайты, с целью кражи учётных данных и личной информации. Одним из таких инструментов является HiddenEye — универсальный фишинговый инструмент с широким набором функций, позволяющий злоумышленникам создавать убедительные копии веб-сайтов, собирать данные и отправлять вредоносные ссылки.

HiddenEye изначально был создан для исследовательских целей, однако быстро завоевал популярность среди киберпреступников благодаря своей доступности и простоте использования. Этот инструмент поддерживает создание фальшивых страниц для таких популярных платформ, как Facebook, Instagram, Google, PayPal и многих других. Он предоставляет возможности не только для фишинга, но и для таких операций, как захват IP-адресов и мониторинг активности жертвы в реальном времени. В данной статье рассмотрим, как HiddenEye работает, какие риски он создаёт для пользователей, а также меры безопасности, которые помогают защититься от фишинга.

**HiddenEye**

HiddenEye позволяет злоумышленникам легко создавать фальшивые страницы, которые внешне неотличимы от настоящих веб-сайтов, и отправлять их пользователям в виде ссылок через электронную почту, социальные сети или мессенджеры. В зависимости от предпочтений злоумышленника, HiddenEye может использоваться для создания страниц логина таких сервисов, как Instagram, Google, Twitter и многих других. Когда пользователь вводит свои данные на поддельной странице, HiddenEye записывает введённые данные и отправляет их злоумышленнику, предоставляя ему доступ к учётной записи жертвы[1].

Благодаря широкому набору функций, HiddenEye позволяет настраивать страницу фишинга под любой выбранный сайт, предоставляя шаблоны, которые максимально похожи на оригинальные веб-страницы. Это усложняет распознавание поддельных страниц для пользователей, которые могут случайно передать свои конфиденциальные данные в руки злоумышленников. Помимо этого, HiddenEye предоставляет инструменты для скрытия своего присутствия, например, изменяя адреса отправки ссылок и маскируя поддельные страницы за доменными именами, которые выглядят надёжно[2].

Вдобавок, HiddenEye поддерживает множество технических функций, которые помогают усилить атаки. Например, инструмент может отслеживать местоположение жертвы с помощью IP-логирования, что особенно полезно для целевых атак. Также HiddenEye позволяет отправлять массовые сообщения и уведомления для вовлечения множества пользователей, что увеличивает вероятность успешного получения данных. Из-за этого инструмент получил популярность среди киберпреступников и стал одной из угроз в киберпространстве[3].

Использование HiddenEye представляет собой серьёзную угрозу для компаний и индивидуальных пользователей, так как успешные фишинговые атаки могут привести к краже финансовых данных, корпоративной информации и персональных данных, которые могут быть проданы или использованы для дальнейших атак. Базовая защита, такая как уникальные пароли и базовое антивирусное ПО, не всегда способна предотвратить подобные атаки, особенно если пользователь не подозревает, что взаимодействует с поддельной страницей[4].

Защита от HiddenEye и аналогичных инструментов фишинга требует комплексного подхода. Одним из наиболее эффективных методов является многофакторная аутентификация (MFA), которая добавляет дополнительный уровень защиты, затрудняя доступ к учетной записи даже при компрометации пароля. Фильтрация электронной почты также играет ключевую роль, так как многие атаки начинают с фишингового письма. Использование надёжных антивирусных решений с функцией фильтрации ссылок и веб-контента может помочь заблокировать доступ к вредоносным страницам до их открытия[5].

Обучение пользователей также играет критически важную роль. Поскольку фишинговые атаки всё чаще используют социальную инженерию, необходимо повышать осведомлённость о признаках поддельных ссылок, таких как орфографические ошибки, подозрительные домены и неожиданные запросы на ввод учётных данных. Компании могут внедрять регулярные тренировки по безопасности для сотрудников, что способствует снижению вероятности успешного фишинга.

**Заключение**

HiddenEye демонстрирует, насколько опасными могут быть современные фишинговые инструменты, доступные даже для неопытных пользователей. С помощью таких программ злоумышленники могут получить доступ к конфиденциальной информации, компрометировать финансовые и корпоративные данные и нанести значительный ущерб. Инструменты вроде HiddenEye продолжают развиваться, становясь всё более эффективными и сложными для обнаружения.

Для защиты от таких угроз пользователям важно соблюдать лучшие практики кибербезопасности, включая использование многофакторной аутентификации, регулярное обновление антивирусного ПО, фильтрацию электронной почты и обучение сотрудников. Комплексный подход к безопасности помогает минимизировать риски, связанные с фишинговыми атаками, и противостоять инструментам, подобным HiddenEye, которые угрожают информационной безопасности каждого пользователя в цифровом пространстве.

**Список литературы**

1. Цветков А. Ю., Рузманов Е. Ю. РАССМОТРЕНИЕ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ //ББК 3 П27. – 2021. – С. 55.

2. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657.

3. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.

4. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.

5. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.

**References**

1. Tsvetkov A. Yu., Rozanov E. Yu. CONSIDERATION OF PENETRATION TESTING IN INFORMATION SECURITY TASKS //PC 3 P27. – 2021. – p. 55.
2. Sinelshchikov V. S., Tsvetkov A. Yu. Protection of personal data at the enterprise //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 653-657.
3. Lesnova E. M., Pestov I. E. Development of a method for detecting and correcting errors for a distributed information network based on big data //Regional informatics and information security. - 2018. – pp. 236-240.
4. Kushnir D. V. Research and development of methods for distributing confidential data via quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch–Bruevich, 1996.
5. Krasov A.V., Sakharov D. V., Stasyuk A. A. Designing an intrusion detection system for an information network using large data //High–tech technologies in space research of the Earth. – 2020. – Vol. 12. – No. 1. - pp. 70-76.