ПРОГРАММНЫЙ МОДУЛЬ ПО ПОИСКУ ФИШИНГОВЫХ ДОМЕННЫХ ИМЕН В НАЦИОНАЛЬНОМ СЕГМЕНТЕ СЕТИ ИНТЕРНЕТ

Феденко Р.Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Игнатенко А.А.

Аннотация. Фишинг, как вид интернет-мошенничества, целью которого является получение персональных данных пользователей Интернет. Угроза данной кибератаки, способы защиты от неё. Тайпсквоттинг и киберсквоттинг, как вид фишинговой атаки, использование программного модуля для защиты от данной атаки.

Фишинг – подмножество социальной инженерии, цель которого – получить персональные данные пользователя или другую ценную информацию. Существует два вида фишинговых атак:

– массовый фишинг – это тип атаки на нескольких людей сразу,

– целевой фишинг – это атаки на конкретных пользователей.

Фишинг представляет собой сообщение в мессенджере, почтовые письма со ссылкой на веб-ресурс или рекомендациями для дальнейших действий, поддельные страницы служб поддержки компаний, создание фишинговых сайтов, идентичных с легитимными.

Опасность фишинга в том, что не увидеть угрозу может любой человек, если он недостаточно внимателен к мелким деталям. Злоумышленники имитируют действующие публичные сети Wi-Fi в общественных местах, защищают свои фишинговые сайты с помощью классического изображения HTTPS в начальной адресной строки. В случае отсутствия активности, веб-страница перезагружается на странице ввода пароля, имитирующую легитимный сайт. Используют уязвимости сайтов для встраивания скрытых ловушек, для перехвата персональных данных, ловят пользователей на неправильном вводе веб-адреса, перенаправляют трафик с безопасного веб-сайта на фишинговую страницу. В случае получения доступа к электронной почте пользователя, злоумышленник может рассылать фишинговые письма от имени пользователя, что делает атаку еще более скрытой.

Для защиты от фишинга необходимо:

– не сообщать кому-либо конфиденциальную информацию,

– не открывать вложения, содержащие в письмах от неизвестного адресата,

– не переходить по ссылкам в письмах,

– своевременно обновлять программное обеспечение и операционную систему.

Фишинг наносит большой вред легитимным компаниям, понижая репутацию того или иного продукта. Поэтому выявлять и ликвидировать фишинг, необходимо до того, как он причинит значительный ущерб.

Тайпсквоттинг – это один из видов фишинговых атак, нацеленный на пользователей интернета, допустивших опечатку при вводе веб-адреса в браузере, начальный этап такой фишинговый атаки заключается в кибersквоттинге – вид киберпреступления, представляющий собой покупку или регистрацию доменного имени, полностью схожим с существующим [1]. Злоумышленники регистрируют домены с именами, являющимися намеренно ошибочными названиями известных веб-сайтов и пользователи могут попасть на такие альтернативные веб-сайты при случайном ошибочном вводе названия популярных веб-сайтов, или в результате перенаправления на вредоносный веб-сайт в рамках широкой фишинговой атаки [2].

Один из первых и самых известных примеров атак с тайпсквоттингом, связан с Google. В 2006 году был зарегистрирован сайт Goggle.com, который функционировал, как фишинговый. За прошедшие годы были зарегистрированы различные варианты названия Google: foogle, hoogle, boogle, yoogle (все они были выбраны из-за близости их первых букв к букве g на qwerty-клавиатурах). В преддверии президентских выборов 2020 года в США сообщалось [3], что злоумышленниками были созданы тайпсквоттинговые домены на имена нескольких кандидатов с различными злонамеренными мотивами.

С целью защиты от тайпсквоттинга, был разработан модуль по поиску фишинговых доменных имен в национальном сегменте сети Интернет, который поможет сохранять репутацию популярных компаний, а также известных личностей.

Список использованных источников:

1. Kaspersky [Электронный ресурс]. – Режим доступа : https://www.kaspersky.ru/resource-center/preemptive-safety/cybersquatting

2. Kaspersky [Электронный ресурс]. – Режим доступа : https://www.kaspersky.ru/resource-center/definitions/what-is-typosquatting

3. CPOmagazine [Электронный ресурс]. – Режим доступа : https://www.cpomagazine.com/cyber-security/will-typosquatting-influence-the-2020-presidential-election/