

ТЕСТИРОВАНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ ПОЧТОВЫХ СЕРВИСОВ ОТ СКАНИРОВАНИЯ ВНЕШНИХ Е-МАЙЛ ТРЕКЕРОВ

В.В. Маликов, А.В. Макатерчик

Возможности дистанционных сервисов на основе информационно-коммуникационных технологий (ИКТ) позволяют существенно снизить издержки организаций при значительном росте качества/эффективности предоставляемых услуг/продуктов. Массовый переход на использование дистанционных сервисов на основе ИКТ позволил обеспечивать потребности граждан, а также изменил фокус внимания злоумышленников.

Информация, полученная на основе технологий сканирования внешних e-mail трекеров может быть использована для проведения как легитимных, так и не легитимных операций.

Авторами проведено исследование уровня эффективности защиты 4-х почтовых сервисов (gmail.com, yandex.by, mail.ru) от технологий сканирования 3-х внешних e-mail трекеров (mailtracking.com, didtheyreadit.com, getnotify.com). Проведенное авторами исследование осуществлялось строго в научных целях, его результаты не являются и не могут признаваться руководством к совершению каких-либо противоправных действий (fair use/fair dealing).

В ходе исследования оценивалась потенциальная возможность сканирования/извлечения информации по работе почтового сервиса на основе 20 параметров/показателей, например, таких как:

- дата и время каждого открытия/прочтения/переадресации письма;
- IP-адреса/порты получателей письма, а также имя интернет-провайдера;
- физическое местонахождение (город/страна) получателя (или его интернет-провайдера);
- переходы по URL-адресам вложений в письмо (дата/время/URL-адрес);
- браузер/программное обеспечение электронного почтового сервиса, используемого получателем и т.д.

Проведенное исследование показало, что из заданных 20 параметров / показателей сканирования / извлечения информации по работе почтового сервиса возможно верифицированное извлечение от 5 до 12 параметров/показателей.