Университет ИТМО, факультет программной инженерии и компьютерной техники

Двухнедельная отчётная работа по «Информатике»: аннотация к статье

Дата лекции: 29.10.20 Дата сдачи: 12.11.20

Выполнил(а) Романов А.М , № группы *P3110* , оценка

Фамилия И.О. студента не заполнять

|  |  |  |
| --- | --- | --- |
| 1. Как хакеры используют Microsoft Excel против него самого | | |
| **ФИО автора статьи (или e-mail)**  *janna-maslova* | **Дата публикации**  "30" Сентября 2020 г. | **Размер статьи**  **655** |
| **Прямая полная ссылка на источник и сокращённая ссылка**  [*https://habr.com/ru/post/458278/*](https://habr.com/ru/post/458278/)  http://bit.do/fKV6g | | |
| **Теги, ключевые слова или словосочетания**  Информационная безопасность, Excel | | |
| **Перечень фактов, упомянутых в статье**   1. Для большинства Excel – скучная программа, однако для хакеров это видится иначе 2. Специалисты Mimecast рассказали, как встроенная функция Power Query может быть использована для атаки. Она позволяет автоматически собирать данные из указанных источников. Это потенциальная возможность кражи данных, если сайт, указанный в качестве источника, содержит вредоносный файл 3. Такой способ атаки является универсальным, потому что использует стандартные функции Excel, а также работает на всех его версиях вплоть до самых последних версий и является кроссплатформенным, поскольку использует функции программы, а не баг 4. Как только Power Query устанавливает связь с вредоносным сайтом, появляется возможность задействовать Dynamic Data Exchange – протокол обмена данных между приложениями в Windows. За злоумышленником остаётся только выгрузить DDE-совместимую инструкцию для атаки 5. Перед установлением DDE соединения пользователь должен дать на это своё согласие, однако большинство пользователей соглашаются со всеми запросами, не вдаваясь в суть 6. Как возможное решение данной уязвимости Microsoft предложили отключать DDE для конкретных приложений, однако описанный вид атаки используется на устройствах, на которых отсутствует возможность отключать DDE | | |
| **Позитивные следствия и/или достоинства описанной в статье технологии (минимум три пункта)**   * Простота атаки невнимательных пользователей (позитивное следствие для атакующей стороны) * Нежелание Microsoft предпринимать меры по исправлению уязвимости по причине глубокой интегрированности DDE (позитивное следствие для атакующей стороны) * Проявление благоразумия со стороны Microsoft, отказываясь жертвовать важной функцией ради небольшого улучшения безопасности.   «на языках программирования пишут вирусы, почему их не запретят?» | | |
| **Негативные следствия и/или недостатки описанной в статье технологии (минимум три пункта)**   * Простота атаки невнимательных пользователей * Нежелание Microsoft предпринимать меры по исправлению уязвимости по причине глубокой интегрированности DDE * Снижение вероятности добавления новых функций со стороны Microsoft, ввиду опаски создать новые уязвимости | | |