Наши специалисты выявили новую тенденцию распространения вируса Dridex и использование PowerShell Empire перед атакой шифровальщика BitPaymer.

Dridex – это банковский троян, разработанный для кражи денег с банковских счетов. После установки вируса, злоумышленники используют PowerShell Empire (open-source фреймворк для тестирования на проникновение) для повышения привилегий и для доступа к контроллеру домена, после чего по всей сети устанавливается шифровальщик BitPaymer.

Dridex распространяется с помощью спама. Злоумышленник отправляет письмо с вложением. После загрузки и открытия зараженного документа запускается макрос, содержащий вредоносный код.

Если специалисты по защите информации или системные администраторы выявили в своих сетях заражение вирусом Dridex или использование PowerShell Empire, необходимо незамедлительно принять меры по смягчению последствий последующих атак данным шифровальщиком.

**Профилактические меры**

* Создайте план резервного копирования.
* Обновите PowerShell до последней версии и централизуйте журналы для обнаружения часто используемых команд PowerShell, связанных с вредоносным по.
* Регулярно обновляйте и исправляйте всё программное обеспечение и операционные системы для устранения известных уязвимостей, например уязвимость в протоколе SMBv1. Целые эпидемии, вызванные вредоносными программами «WannaCry» и «Petya», использовали лазейку в протоколе SMBv1.
* Обеспечьте соблюдение требований к паролям, а также соблюдение групповых политик доступа к SMB. По возможности используйте двухфакторную аутентификацию для всех аккаунтов.
* Расскажите сотрудникам о том, как идентифицировать попытки фишинга, социальной инженерии и спуфинга.
* При загрузке вложений и запуске исполняемых файлов сотрудники должны быть уверены, что данное ПО легитимное.

**Меры по смягчению последствий**

* Системные администраторы, обнаружившие заражение вирусом Dridex, Emotet, Trickbot, Ursnif, Qakbot или использование PowerShell Empire должны немедленно принять меры по созданию резервных копий и защите конфиденциальных данных, так как эти вирусы могут свидетельствовать об атаке шифровальщика BitPaymer. Системные администраторы должны принять меры по защите сетевых устройств.
* Мы настоятельно рекомендуем вам обратиться в правоохранительные органы, чтобы сообщить о вторжении и запросить помощь, при этом предоставив журналы событий.