## Троянец и стабильность

Эксперты по безопасности обнаружили, что новая версия известного банковского троянца **TrickBot**, появившегося в 2016 г., стала собирать несколько неожиданный тип данных: информацию о функционировании и сбоях операционной системы Microsoft Windows.

В Windows присутствует специализированная функция *Reliability Analysis Component* («Средство анализа стабильности»), которая снабжает монитор стабильности Windows сведениями об установке ПО, обновлениях, ошибках в ОС и приложениях, а также об аппаратных сбоях.

Средство анализа стабильности запускают своего агента RACAgent, который каждый час собирает все эти данные и сохраняет их в локальной папке C:\ProgramData\Microsoft\RAC\. Данную опцию можно отключать через «Планировщик заданий» (Task Scheduler), однако это скажется на функционировании монитора стабильности.

Эксперты *My Online Security* обнаружили, что троянец **TrickBot** стал проявлять нездоровый интерес к этим данным. Что именно злоумышленники собираются с ними делать, пока не понятно.

## Фишинг и новые атаки

Эксперт по информационной безопасности компании *SEC Consult Services* Михаил Зайцевпридерживается мнения о том, что эти сведения могут использоваться для фишинга, но это не единственный вариант. «Данные о сбоях в функционировании в операционной системе и приложениях вполне можно использовать для определения слабых мест в системе, — говорит эксперт. — Такой информацией, естественно, вполне заинтересуются всевозможные злоумышленники, занимающиеся распространением вредоносного ПО».

Эксперты гадают о причинах проснувшегося интереса известного трояна к Windows

TrickBot в последнее время активно распространяется в виде фальшивых сообщений от банка *Lloyds Bank*. Письма якобы исходят с адреса *donotreply@lloydsbankdocs.com*, а вредоносный код содержится в макросе во вложенном файле Microsoft Word.

Документ также содержит логотип антивирусной компании *Symantec*, чтобы убедить пользователя, что он прошёл проверку на вредоносное ПО, однако как минимум 30 антивирусных разработок корректно идентифицируют этот вредонос.