Речь идёт о банкере — банковском Windows-трояне Grandoreiro, который ранее распространялся только в Латинской Америке, были случаи его использования в Испании и Португалии, а хакеры, создавшие вредонос, — из Бразилии. На некоторе время разработчики Grandoreiro выпали из инфополя, но только для того, чтобы «допилить» свой продукт.

Как оказалось, на днях Grandoreiro снова объявился, но уже с более серьёзной системой защиты от расшифровки кода, с переработанным DGA-генератором доменов, который используется для связи с сервером C2, и с возможностью дальнейшего распространения вируса через сервис Outlook.

Причём теперь троян нацелен на 1500 банковских приложений от организаций, работающих в 60 странах. И первые жертвы уж есть.

Атаки трояна начинаются с фишингового электронного письма с вредоносной ссылкой. Как правило, злоумышленники маскируются под местные госорганы, в основном налоговую службу. Загружаемый по URL вредоносный файл в письме замаскирован под требование платежа либо какой-либо другой неоплаченный счёт.