Автор: Administrator
21.02.2016 22:24

{jcomments on}

Специалисты IBM обнаружили модифицированную версию банковского трояна Gozi, нацеленную на пользователей ОС Windows 10. Вредонос поражает Microsoft Edge – браузер по умолчанию в новой оперативной системе, призванный заменить устаревший Internet Explorer.

Вирусописатели смогли использовать устаревший метод инъекции кода для работы с браузером Microsoft Edge. Троян поражает основной процесс обозревателя MicrosoftEfgeCP.exe.

Gozi - один из старейших функционирующих банковских троянов. Вредонос был создан в 2007 году. Злоумышленники раскрыли исходный код трояна в 2010 году. Тогда же злоумышленники начали применять вторую версию Gozi в массивной мошеннической кампании против американских банков. В 2013 году Gozi получил возможность внедряться в сектор MBR жесткого диска, а на протяжении последнего года вирусописатели добавили в троян улучшенные возможности по web-инъекции.

В версии для Windows 10 Gozi использует ряд хуков в kernel32.dll для внедрения кода в браузер. Троян также проникает в процесс RuntimeBroker.exe - родительский процесс Edge и внедряет код в explorer.exe. Обновленная версия Gozi способна работать и с другими браузерами, включая Internet Explorer, Chrome, Opera и Firefox.

Источник: www.securitylab.ru