Новый вредонос Nodersok заразил тысячи компьютеров на базе Windows

Тысячи компьютеров на базе Windows по всему миру за последние несколько недель были заражены новым видом вредоносного ПО. Вредонос под названием Nodersok загружает и устанавливает копию инфраструктуры Node.js для преобразования зараженных систем в прокси-серверы и проведения мошеннических операций.

Вредоносная программа впервые была обнаружена летом нынешнего года и распространялась с помощью вредоносной рекламы, которая принудительно загружала файлы HTA (HTML Application) на компьютеры пользователей. Запуск HTA-файлов начинал многоэтапный процесс заражения с использованием скриптов Excel, JavaScript и PowerShell, которые в конечном итоге загружали и устанавливали вредоносное ПО Nodersok.

Исследователи из компании Microsoft утверждают, что вредоносная программа превращает зараженные хосты в прокси-серверы для передачи вредоносного трафика. По словам специалистов из Cisco Talos, с другой стороны, прокси используются для мошеннических операций.

Подробнее: https://www.securitylab.ru/news/501410.php