Автор: Алина Саратова НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 1880 09.08.2016, 16:42
5

Symantec обнаружила кибершпионов, скрывавшихся 5 лет

Исследователи из компании Symantec сообщили о ранее неизвестной группировке Strider, занимающейся кибершпионажем. В ходе атак хакеры из Strider используют сложное вредоносное ПО Remsec.

Новая хакерская группировка действует, по крайней мере, с октября 2011 года, и до недавнего времени о ней ничего не было известно. Как показал анализ образца вредоносного ПО, Remsec разработан специально для шпионажа. Он выполняет функции бэкдора и кейлоггера (в его коде упоминается главный антигерой саги «Властелин колец» Саурон), а также похищает хранящиеся на зараженном компьютере файлы.

Вирус Remsec состоит из ряда модулей, работающих вместе как фреймворк, позволяющий злоумышленнику получить полный контроль над инфицированным компьютером. Избежать обнаружения опасному ПО удается несколькими способами. К примеру, некоторые компоненты Remsec представляют собой исполняемые BLOB-объекты (Binary Large Objects), которые весьма сложно обнаружить с помощью традиционных антивирусных решений. К тому же, большая часть функционала Remsec развертывается по сети, а значит, он сохраняется не на диске, а только в памяти компьютера.

Так как хакеры из Strider способны создавать собственные вредоносные инструменты и оставались необнаруженными в течение как минимум пяти лет, по мнению исследователей, они могут работать на правительство какого-нибудь государства. Всего пока обнаружены следы Remsec на 36 компьютерах в 7 не связанных между собой организациях (в том числе на системах нескольких российских пользователей и организаций, китайской авиакомпании, шведской организации и посольства в Бельгии).

Автор: Алина Саратова © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 1880 09.08.2016, 16:42
5

эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта