Автор: Артур Скальский © РИА-Новости ИНТЕРНЕТ И ИТ, МИР 2671 03.07.2011, 10:44 388

"Лаборатория Касперского" нашла вирус, умеющий "устранять конкурентов"

Новый компьютерный вирус, который обучен уничтожать конкурирующие зловредные программы на зараженных компьютерах и позволяет хакерам создавать практически "непотопляемые" бот-сети для рассылки спама, обнаружили специалисты российской антивирусной компании "Лаборатория Касперского", сообщила компания в среду.

Обычно для прекращения деятельности бот-сети специалисты по информационной безопасности находят и отключают серверы управления, через которые владельцы бот-сети отдают команды зараженным компьютерам. По данным исследователей "Лаборатории", вредоносная программа TDSS позволяет использовать кроме командных серверов публичную файлообменную сеть KAD, что теоретически обеспечивают доступ к зараженным машинам даже при закрытии всех командных центров.

"Злоумышленники "расшаривают" в файлообменной сети зашифрованный файл, расшифровать который могут только зараженные компьютеры. После загрузки и расшифровки данного файла бот исполняет указанные там команды. Учитывая, что KAD-сеть является децентрализованной (в отличие, например, от той же BitTorrent, где есть трекеры), закрыть её на текущий момент практически невозможно", - объяснил РИА Новости один из авторов исследования, эксперт "Лаборатории Касперского" Сергей Голованов.

Работа через файлообменные сети - только одна из функций новой программы. TDSS сама отчасти заменяет антивирус и умеет удалять с зараженного компьютера более 20 популярных конкурентных вредоносных программ, среди которых такие известные приложения, как Gbot, ZeuS, Optima (включают зараженный компьютер в одноименные ботнеты) и другие.

А сам TDSS устанавливает на ПК около 30 дополнительных утилит, включая фальшивые антивирусы, системы накрутки рекламного трафика и рассылки спама. Еще одной функцией TDL-4 стала возможность открытия прокси-сервера. Злоумышленники предлагают сервис анонимного доступа к сети через зараженные компьютеры, запрашивая за такую услугу около 100 долларов в месяц.

> Исследователи отмечают, что авторы новой программы не занимаются расширением сети зараженных компьютеров самостоятельно, вместо этого оплачивая ее третьим лицам. В зависимости от ряда условий, партнерам выплачивается от 20 до 200 долларов США за тысячу установок вредоносного ПО.

Экспертам "Лаборатории Касперского" также удалось получить общую статистику по количеству зараженных компьютеров. Анализ полученных данных показал, что только за первые три месяца 2011 года с помощью TDL-4 (другое название TDSS) было заражено более 4,5 миллиона компьютеров по всему миру, большая их часть (28%) расположена в США. Учитывая упомянутые ранее "расценки" на распространение вредоносного ПО, можно оценить примерный уровень затрат киберпреступников на создание ботнета из компьютеров американских пользователей: он составляет около 250 тысяч долларов.

Размеры ботнета указывают на то, что сейчас он является одним из крупнейших в мире. Для сравнения, ботнет Rustock, который был отключен в марте этого года, насчитывал более 800 тысяч компьютеров и считался одним из крупнеших в мире генераторов спама. Его отключение уменьшило на треть объем мирового спама, правда, лишь кратковременно.

По мнению авторов исследования, экспертов "Лаборатории Касперского" Сергея Голованова и Игоря Суменкова, киберпреступники продолжат развитие TDSS. Использование инструментов атаки из арсенала Stuxnet, использование технологий p2p, собственный "антивирус" и многое другое ставят вредоносную программу TDSS в разряд самых технологически развитых и наиболее сложных для анализа. "Вредоносная программа и ботнет, объединяющий зараженные компьютеры, доставят еще много неприятностей и

пользователям, и специалистам по IT-безопасности", - констатировали эксперты "ЛК".

Автор: Артур Скальский © РИА-Новости ИНТЕРНЕТ И ИТ, МИР 2671 03.07.2011, 10:44 388