Автор: Administrator
20.02.2016 12:07 -

Эксперты компании Sucuri сообщили, что сайты под управлением **WordPress вновь подвергаются массовым кибератакам**
. На этот раз против ресурсов на базе популярной CMS проводятся
Layer 7 DDoS-атаки
, которые к тому же эксплуатируют функцию pingback и генерируются ботнетом из… WordPress-сайтов.

В отличие от обыкновенных DDoS-атак на заказ , атаки Layer 7 осуществляются на уровень приложений. То есть злоумышленники занимаются не ковровой бомбардировкой, а действуют прицельно и не задействуют при этом больших мощностей. Так, пакеты, созданные специальным образом, приводят к повышению нагрузки на CPU сервера до таких значений, что сайт жертвы эффективно выходит из строя.

Проблема с функцией pingback в WordPress и вовсе не нова. Давно известно, что ее можно использовать для осуществления DDoS-атак. Несколько лет назад разработчики CMS даже попытались исправить проблему, представив в версии 3.9 инструмент, позволяющий вести логи pingback-запросов. Теоретически, это должно помочь администраторам сайтов быстро определить IP-адреса атакующих и добавить в их черный список. На деле этим мало кто пользуется.

Теперь эксперты компании Sucuri зафиксировали кампанию, сочетающую в себе обе вышеописанные техники. Более 26 000 сайтов на базе WordPress объединились в ботнет и атакуют другие ресурсы, функционирующие под управлением данной CMS. Ботнет генерирует порядка 10000-20000 HTTPS-запросов в секунду, направляя свои усилия против сервиса WordPress XML-RP. В итоге сайт жертвы задыхается под валом pingback-запросов. Сервер, на котором располагается сайт, вынужден выделять атакуемому сайту все больше ресурсов CPU и памяти, так как поддержание такого количества зашифрованных соединений – дело нелегкое. Заказать ддос атаку можно по ссылке .