Ссылка на код программы Mirai была опубликована на сайте Hackforumпользователем Anna-sempai. В ее задачи входит поиск и заражение приборов интернета вещей, не сменивших свои заводские пароли и логины — частое явление среди покупателей веб-камер, умных холодильников и другой подключенной техники.

Причины обнародования программы не ясны, ведь ботнеты могут дорого стоить на черном рынке. Однако, распространение кода вредоносного ПО — это способ помешать установлению авторства после того, как атака на Кребса привлекла повышенное внимание.

«Негодяи, разработавшие вредоносное ПО, часто выбрасывают свои исходные коды в свободный доступ, когда правоохранительные органы и фирмы, обеспечивающие безопасность, подбираются слишком близко к ним, — пишет журналист Брайн Кребс, жертва атаки. — Публикация кода в сети для общего обозрения и скачивания гарантирует, что автор будет не единственным, кто владеет ей, когда к нему придут с ордером на обыск».
Хакеры использовали две сети ботнет, состоящие из примерно 980 000 и 500 000 взломанных устройств, в основном подключенных к интернету камер с заводским паролем. С их помощью они обрушили сайт KrebsOnSecurity.com, принадлежащий Кребсу, автору статей, разоблачающих DDoS-хакеров.

Сила атаки превзошла 660 Гбит/с и стала одной из крупнейших в истории. Но есть подозрения, что хакеры использовали не полную мощь двух ботнетов. По мнению Дейла Дрю, главы отдела безопасности в Level 3 Communications, защищавшей сайт Кребса, злоумышленники использовали примерно 1,2 млн узлов из ботнетов с максимальным объемом 1,5 млн.

Также на прошлой неделе от серии крупных DDoS-атак пострадал французский провайдер интернет-услуг OVH. Здесь была зарегистрирована рекордная мощность в 900 Гбит/с и 1 Тбит/с. Пока нет данных о связи атак на Кребса и OVH, пишет Motherboard.

«Мы видим первые последствия плохой защиты устройств и вреда, который они могут нанести при взломе, — говорит Мэттью Принс, основатель Cloudflare, компании, обеспечивающей защиту от DDoS-атак. — Любой в интернете может стать жертвой такого рода атаки».

По мнению эксперта по вопросам кибербезопасности Брюса Шнейера, из-за изменившегося характера DDoS-атак, которые происходят в последнее время, появился риск глобального обесточивания, которое может произойти в любой момент. Эксперт обнаружил, что неизвестные хакеры целенаправленно пытаются определить предел защитных возможностей крупнейших компаний, обеспечивающих работу интернета и его инфраструктуры. Для этого они настойчиво и массировано пробивают защиту, постепенно наращивая число запросов на сервера.