Кто-то пытается сломать весь интернет

Специалист по безопасности Брюс Шнайер рассказывает о DDoS-атаках на ключевую инфраструктуру сети

Lawfare

18:43, 14 сентября 2016 Источник: https://meduza.io/feature/2016/09/14/kto-to-pytaetsya-slomat-ves-internet

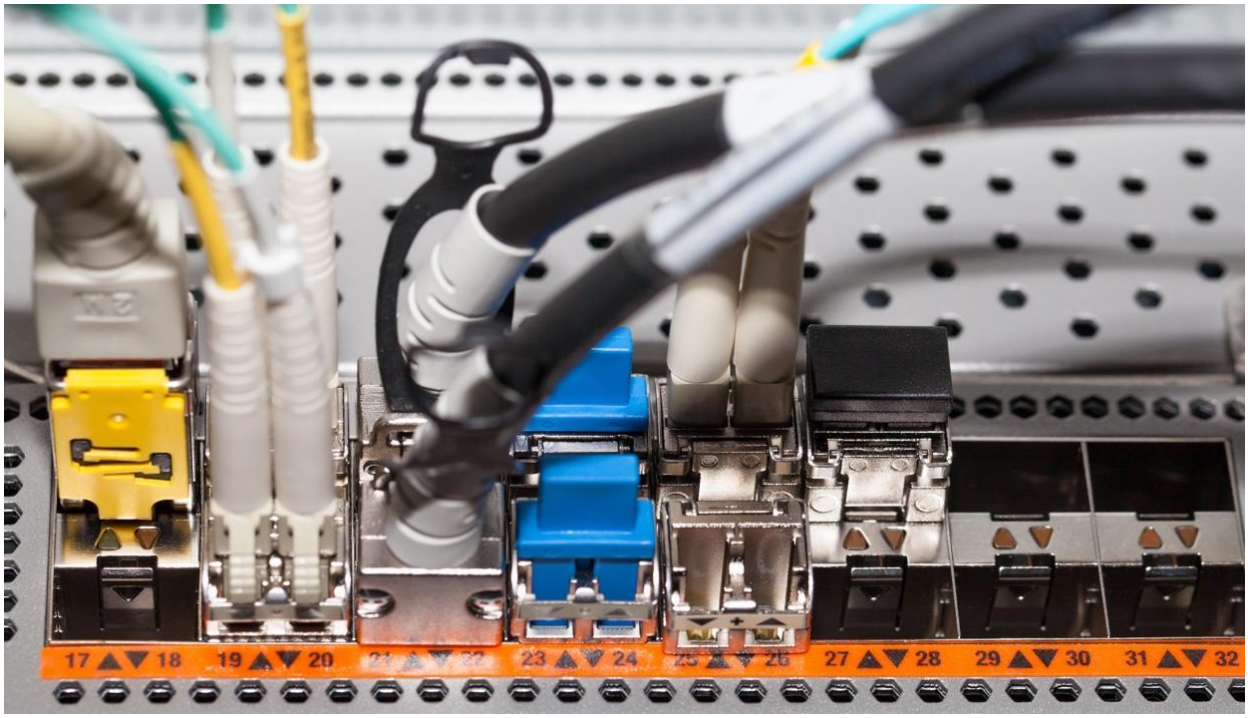

Фото: Zoonar GmbH / Alamy / Vida Press

В течение двух последних лет неизвестные проверяют на прочность основные узлы интернета, пишет специалист по безопасности Брюс Шнайер в своей колонке на сайте Lawfare. Его источники в крупных компаниях, обеспечивающих работу сети, рассказывают, что уже пару лет они сталкиваются с усиливающимися DDoS-атаками. Предположительно, атаками управляют Китай или Россия. «Медуза» пересказывает колонку Брюса Шнайера, которая называется «Кто-то изучает, как сломать интернет».

Брюс Шнайер — признанный специалист по криптографии и компьютерной безопасности. Он написал несколько книг по этим темам, в том числе один из главных трудов «Прикладная криптография», и разработал несколько новых шифров. Раньше он работал на министерство обороны США.

В своей колонке Брюс Шнайер рассказывает об атаках, которым подвергаются компании, обслуживающие ключевую инфраструктуру интернета. Он не указывает, о каких именно организациях идет речь, поскольку получил информацию от них на условиях анонимности.

Вероятно, имеются в виду компании, поддерживающие серверы DNS с информацией о доменах верхнего уровня (например,.com или.ru). Если их обрушить, при заходе на любой сайт в этой зоне компьютер не сможет понять, к какому IP-адресу он должен обращаться. Кроме того, Шнайер может говорить о точках обмена трафиком или магистральных провайдерах. Либо обо всех этих структурах вместе.

В последние пару лет эти организации испытывают DDoS-атаки, которые, во-первых, мощнее прежних, а во-вторых, — продолжительнее. Брюс Шнайер описывает паттерн атаки. Злоумышленники начинают атаку на определенном уровне, а потом медленно его повышают. Затем она прекращается, но через неделю возобновляется с того уровня, на котором закончилась.

Как пишет Брюс Шнайер, эти атаки ведутся так, чтобы исследовать, как защищены компании. Хакеры используют разные типы атак, чтобы заставить жертву показать весь свой арсенал защиты.

В своей колонке автор также указывает, что его информация соотносится с последним докладом о DDoS-атаках компании Verisign, которая поддерживает два из 13 корневых серверов DNS, а также отвечает за реестр доменов в зонах.com и.net. В нем говорится, что во втором квартале 2016 года атаки продолжаются и становятся все более частыми, настойчивыми и сложными.

Кто стоит за этими атаками, неизвестно. По словам Брюса Шнайера, размах и настойчивость указывает на то, что с этим может быть связано какое-то государство. Данные, которые изучал специалист, намекают на то, что это Китай — но злоумышленники способны подставить любую страну. «Мое первое предположение — Китай и Россия», — заключает Брюс Шнайер.

«Агентство национальной безопасности, которое следит за ключевой инфраструктурой интернета больше, чем кто-либо, вероятно, лучше знает, [кто может стоять за атаками]. Но пока США не решат раздуть из этого международный скандал, мы не увидим никаких обвинений. Но атаки идут. И люди должны об этом знать», — пишет Брюс Шнайер.

→ LAWFARE