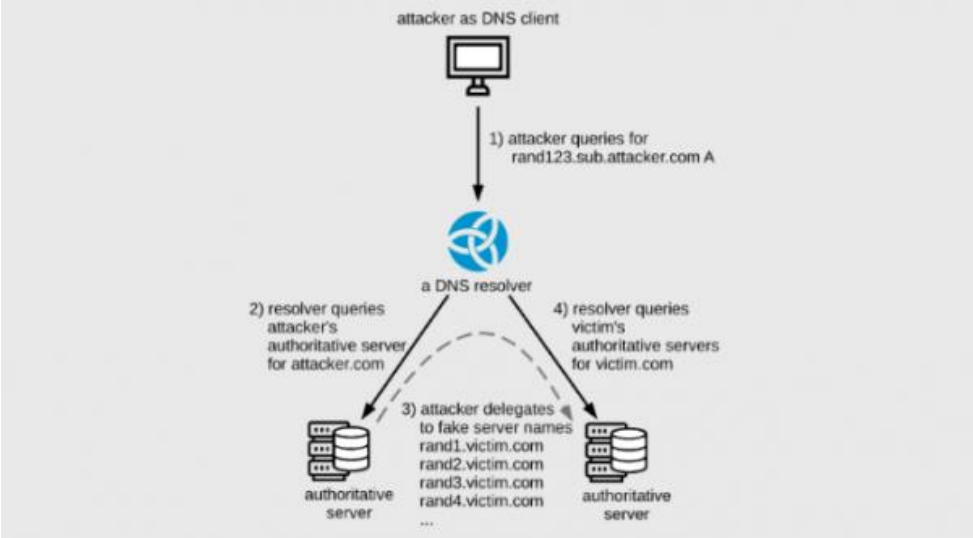
Уязвимость в DNS-серверах позволяет в тысячу раз усилить мощность DDoS-атаки



Группа исследователей из Тель-Авивского университета и Междисциплинарного центра в Герцлии (Израиль) обнаружила в DNS-серверах уязвимость, позволяющую осуществлять DDoS-атаки с фактором усиления 1620x. По словам специалистов, уязвимость, получившая название NXNSAttack, затрагивает рекурсивные DNS-серверы и процесс делегирования.

Рекурсивные DNS-серверы представляют собой системы DNS, передающие DNS-запросы в восходящем направлении, чтобы их можно было разрешить и преобразовать из доменного имени в IP-адрес. Эти операции происходят на авторитетных DNS-серверах, где хранится копия записи DNS. Однако, как часть механизма безопасности протокола DNS, авторитетные DNS-серверы также могут делегировать операцию альтернативным DNS-серверам.

В течение нескольких последних месяцев исследователи вместе с производителями ПО для DNS-серверов, сетями доставки контента и провайдерами управляемых DNS работали над исправлением проблемы по всему миру. В список затронутого уязвимостью ПО входят: ISC BIND (CVE-2020-8616), NLnet labs Unbound (CVE-2020-12662), PowerDNS (CVE-2020-10995), CZ.NIC Knot Resolver (CVE-2020-12667), а также коммерческие сервисы DNS от Cloudflare, Google, Amazon, Microsoft, Oracle (DYN), Verisign, IBM Quad9 и ICANN. Администраторам собственных DNS-серверов рекомендуется установить последние версии ПО.

Источник: https://www.securitylab.ru/news/508472.php