

мощности проводимых DDoS-атак постоянно возрастают (до 500 Гбит/с в 2015 г.), а стоимость организации таких атак постоянно падает (1 час — \$5, неделя — \$260, месяц — \$900).

2. Проведение DDoS-атак возможно на всех семи уровнях модели OSI. Наибольший интерес для злоумышленников представляют удаленные DDoS-атаки на сетевом (3), транспортном (4) и прикладном уровнях (7).

3. Особенную опасность представляют DDoS-атаки с использованием метода усиления (амплификатора).

ИССЛЕДОВАНИЕ СЕТЕВЫХ СЕРВИСОВ/РЕСУРСОВ КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ НА ПРЕДМЕТ ПРОВЕДЕНИЯ DOS / DDOS-АТАК

В.В. Маликов, М.А. Бабич, Г.В. Обрядин

Главной предпосылкой для успешного проведения DoS-атак являются ошибки программного кода в реализации соответствующих сетевых сервисов/ресурсов, которые позволяют выполнить недопустимую инструкцию или исключительную ситуацию, которая может привести к аварийному завершению процесса/службы.

Авторами исследован уровень информационной безопасности сервисов/ресурсов в сети интернет на примере кредитно-финансовых организаций (КФО) Республики Беларусь. Для проведения исследования были выбраны 20 белорусских КФО из реестра Национального банка Республики Беларусь, имеющие специальные разрешения (лицензии) на осуществление банковской деятельности.

По результатам проведенного исследования, можно сделать следующие выводы:

1. В настоящее время существуют предпосылки для проведения DoS / DDoS-атак на сервисы / ресурсы КФО в сети интернет за счет наличия множества ошибок в программном коде, а также критических уязвимостей в алгоритмах реализации программного обеспечения (ПО).

2. Тестирование программного кода (тест ПО «CSE HTML Validator Professional») сервисов/ресурсов КФО показало, что все 100% КФО имеют ошибки в коде, а в коде одной из КФО имеются 2 грубые ошибки. Данная ситуация существенно увеличивает риск проведения DoS / DDoS-атак.

3. Особую опасность представляют уязвимости в реализации алгоритмов / протоколов шифрования (например: CVE-2016-0800), так как указанное ПО обеспечивает в том числе удаленное проведение финансовых операций:

– результаты проведенного тестирования (тест ПО «DROWN-attack») сервисов/ресурсов КФО на предмет реализации уязвимости CVE-2016-0800 показали, что в 20% КФО возможно проведение DROWN-атаки;

– тестовая эксплуатация уязвимости CVE-2016-0800 (DROWN) на уязвимом поддомене одной из КФО с использованием ресурсов ПО «Censys» позволила выделить секретный ключ, используемый для шифрования информации.

СОКРЫТИЕ ИНФОРМАЦИИ В СЕТИ С ЦЕЛЬЮ ЗАЩИТЫ

А.Л. Мاستыкин

В настоящее время возможности предоставляемые пространством не индексируемой части интернета («темного интернета» или «darknet») по сокрытию информации серьезно недооценены. Ими просто пренебрегают. Тяжело даже предположить соотношение «видимой» (легко доступной) его части и «невидимой» (той, которая требует для доступа к себе специального подхода). Проблему представляет не столько наличие динамики в строении этих составляющих, сколько размытость границ между ними. По большей части «темный интернет» представляет собой «свалку» того, что когда-то являлось ресурсом открытого интернета или никогда не использовалось вовсе, того что популярные поисковые системы, по какой-либо причине, оставили без внимания. Ежедневно в «сеть» загружаются и выкачивается огромное количество информации. К концу 2016 года трафик достигнет зеттабайта, а к 2019 двух зеттабайт в год [1]. Ежегодный прирост общего объема информации составляет 24% [2]. И это говорит о том, что количество информации в отмирающих ресурсах также колоссально. Хаотичность условий нахождения в сети «забытых» ресурсов дает возможность скрытого размещения нужной информации, предназначенной для узкого круга лиц. Эта информация может быть анонимно, как размещена, так и принята.