УДК 004

Студ. И.С. Супрунович, П.Д. Петручук
Науч. рук. ст. преп. И.А. Лепесий
(военная кафедра, БГТУ)

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ВОЕННОЕ ВРЕМЯ

С самых древних времен важной частью любых конфликтах была информационная война.

Пропаганда и шпионаж являюсь основополагающими этого вида войны. Однако с внедрением в нашу жизнь информационных технологий принципиально изменила вектор действий. Теперь один человек обладая специальными знаниями, не только в области информационной безопасности, но и социальной инженерии, способен влиять или проводить диверсионные действия везде, где есть интернет или локальная сеть.

Важнейшим инструментом в арсенале «хакера» является Dos и DDos-атака (Атака отказа в обслуживание и распределённая атака отказа в обслуживание). Ее смысл в создание сбое в работе или выведение из работы способности устройства жертвы. Важно понимать принцип ее работы заключается в «потопление» устройства жертвы за счет не прекращающегося потока данных от других устройств [1].

Вся опасность этого метода атак заключается в простоте его применение. Самым простым примером можно показать так называемые «кибер ополчения» и «народные кибер армии» и им подобные. В которых происходит координация Dos атак, а поток таких атак и создает DDos атаку.

В таких группировках иерархия выстраивается на подобие террористических группировок, которые существуют и ведут свою деятельность только за счет неофитов, которых на почве патриотизма или иных мотиваций рекрутируют в свои ряды. Такой рекрут за частую не обладает какими-либо знаниями в области ИБ. Им предоставляет софт, который выполняет все действия. Важен только вычислительный ресурс и трафик, которые предоставляет неофит [1].

Следующие по опасности виды атак – это атаки троянскими программами, винлокерами, черви.

Троянские программы или Трояны – это разновидность вредоносных программ, которые наносят вред системе, маскируясь под другие программы. Принцип действия заключается в вредительстве системе и данным, находящимся в ней. Искажения или уничтожение данных, уничтожение физических частей устройства, кража данных и

получения удаленного доступа к устройству жертвы, например, для использования в DoS-атаках.

Винлокер – это программа принцип действий которой заключается в блокировке устройства и вымогательстве денег у жертвы под предлогом уничтожения данных или устройства.

Червь – это автономная вирусная программа способная самостоятельно распространяться по сети. Это программа практически безобидна в начале своего пути и его поведение напоминает поведение паразита в организме жертвы. Попадая в устройство, он начинает размножаться и потреблять все больше и больше ресурсов устройства жертвы. Пока в конечном итоге не истощит его полностью. В процессе размножения распространяясь по локальной сети как по наиболее простому и уязвимому пути.

Все эти вредоносные программы способны работать в месте для провидения массированных атак.

В любое время подобные атаки проводиться постоянно и повсеместно. Но в военное время или в бою предпочтения в первую очередь хакеры будут отдавать предпочтение наиболее эффективным с точки психологического давления.

Спам – это атака путем злоупотребления приемам жертвы информации.

Получив адрес электронной почты, страницы в социальных сетях или номеру телефона военнослужащего, злоумышленник моет начать «спамить» как другими вредоносными программами, так и шокирующим контентом или угрозам, шантажом, предложениями сдаться или перейти на сторону противника.

ЛИТЕРАТУРА

1. Олифер, В. Компьютерные сети: Принципы, технологии, протоколы / В. Олифер. – В. 829-845 с.