УДК 623.618:355.40

С.А. СИДЧЕНКО[1], В.Л. ПЕТРОВ[2], В.В. БЕЛИМОВ[1], С.В. ЗАЛКИН[1]

[1] *Харьковский университет Воздушных Сил им. И. Кожедуба, Украина*
[2] *Объединенный научно-исследовательский институт Вооруженных Сил, Украина*

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ РАЗВЕДКИ ИНФОРМАЦИИ В КИБЕРНЕТИЧЕСКОМ ПРОСТРАНСТВЕ

В статье рассмотрены основные характеристики (дальность, точность и время) разведки информации с помощью различных видов программно-математического воздействия в кибернетическом (телекоммуникационном, виртуальном) пространстве.

киберразведка, кибернетическое пространство, дальность разведки, время разведки, точность разведки

Введение

Постановка проблемы. В связи с расширением виртуального информационного пространства (киберпространства) получило широкое распространение одно из проявлений информационной войны – кибервойна. Она дала возможность проведения агрессивных действий, минуя государственные границы, малыми силами, которые к тому же могут быть распределены (децентрализованы) и тщательно замаскированы, существенно затрудняя тем самым их обнаружение и уничтожение. Кибервойна – это новые знания, новые технологии и использование интеллекта "на полную катушку" [1].

Ведение любых боевых действий всегда связано с использованием информации, которая добывается и обрабатывается в процессе разведки. При этом важную роль приобретает киберразведка.

Анализ литературы. Общая характеристика форм и способов ведения информационной войны, направлений их развития на современном этапе рассмотрена в работах В.Б. Толубко, А.А. Рося, С.Я. Жука, И.С. Руснака, В.А. Фомина, С.Н. Гриняева и др.

Основы обработки разведывательной информации представлены в [2].

Технические системы и средства разведки, их классификация, порядок оценки дальности радиотехнической и радиолокационных разведок представлены в [3]. Анализ способов и методов интеллектуального противодействия информационному оружию рассмотрен в [4].

Вместе с тем, в печати мало рассмотрен новый вид разведки – "киберразведка".

Цель статьи. Рассмотреть основные характеристики (дальность, точность и время) разведки информации в кибернетическом (телекоммуникационном, виртуальном) пространстве с помощью различных видов программно-математического воздействия.

Изложение основного материала

Под "киберразведкой" будем понимать комплекс мероприятий по добыванию, обработке и анализу разведывательной информации в кибернетическом (телекоммуникационном, виртуальном) пространстве с помощью различных видов программно-математического воздействия. Она должна проводиться силами и средствами штатных подразделений разведки и специальных подразделений "кибервоинов".

"Кибеpразведка" представляет собой угрозу раскрытия конфиденциальности информации в телекоммуникационной сети.

В общем виде реализация стратегии применения системы разведки информации направлена на осуществление несанкционированного доступа к информации I ($I = \sum_i I_i$, где i – количество информационных ресурсов) в заданном временном интервале времени $\Delta t_{зад}$ с заданной вероятностью p_1 результата осуществления несанкционированного доступа (НСД) к информации при максимально возможном осуществлении способа разведки F_n и минимальных затратах на разведку C_p.

Формально это можно записать следующим образом:

$$\{R\} = \begin{cases} p_1 = \max\limits_{\Delta t_{зад}} p(acsess(I)); \\ p_2 = \min\limits_{\Delta t_{зад}} p(noacsess), \quad p_1 + p_2 = 1; \\ F_n = \max\limits_{\Delta t_{зад}} \sum\limits_{j=1}^{k} (b_j \cdot f_j); \\ C_p = \min\limits_{\Delta t_{зад}} \sum\limits_{j=1}^{k} (a_j \cdot r_j); \end{cases} \quad (1)$$

где $\{R\}$ – множество стратегий системы разведки;

I – множество разведываемых информационных ресурсов;

noacsess – событие, заключающееся в невозможности НСД к информации;

acsess – событие, заключающееся в возможности НСД к информации I;

p_1 – вероятность совершения НСД к информации;

p_2 – вероятность неполучения НСД к требуемой истинной информации I;

F_n – числовое значение суммы приведенных способов ведения разведки;

f_j – j-й вид разведки: $f_j = 1$, если разведка имеет место, $f_j = 0$ – в противном случае;

b_j – весовой коэффициент, отражающий существенность j-го способа разведки;

$j = 1..k$, k – количество способов ведения разведки;

C_p – числовое значение суммы приведенных затрат системы разведки;

r_j – значение затрат j-го уровня системы разведки;

a_j – весовой коэффициент, отражающий существенность j-го уровня затрат для системы разведки.

Основными средствами "кибеpразведки" выступают: поисковые системы, специальное программное обеспечение поиска информации, компьютерные вирусы, "троянские кони", логические бомбы, средства проведения удаленных атак и "социальной инженерии".

"Кибеpразведка" характеризуется дальностью, точностью и временем разведки.

Поисковые системы. Порядка 80% всей секретной информации в глобальной сети Internet можно найти в открытом виде.

Основным средством поиска открытой информации в глобальной телекоммуникационной сети являются информационные поисковые системы (например, Yahoo, Alta Vista, Rambler, UkrNet и др.).

Дальность разведки $Д_P$ ограничивается дальностью действия поисковой системы $Д_{ПС}$, т.е. областью доступных информационных ресурсов сети для данной поисковой системы (область ресурсов, на которые поисковая система имеет ссылки):

$$Д_P \le Д_{ПС}, \quad (2)$$

$$Д_{ПС} = \bigcup_{i=1}^{N} Д_i, \quad (3)$$

где $Д_i$ – дальность от компьютера-разведчика до сервера-источника информации, доступного в сети;

i – количество всех доступных серверов-источников информации (адресов источников информации), $i = \overline{1, N}$.

Время разведки t_P:

$$t_P = t_{пи} + t_{об}, \quad (4)$$

где $t_{пи}$ – время поиска информации в телекоммуникационной сети поисковой системой;

$t_{об}$ – время обработки информации.

Время поиска информации конкретной информации не превышает время поиска всей семантически однотипной информации

$$t_{пи} \le t_{рПС} + \sum_{j=1}^{M} (t_{д_j} + t_{поб_j}), \quad (5)$$

где $t_{рПС}$ – время работы поисковой системы (время поиск однотипной информации по ключевому слову или фразе);

$t_д$ – время доставки информации с сервера-источника на компьютер разведчика (характеризуется в основном параметрами канала);

$t_{поб}$ – время первичной обработки доставленной информации (заключается в определении принадлежности информации к "нужной" или к "мусору");

j – количество информационных ссылок на конкретную информацию, соответствующую ключевому слову или фразе, $j = \overline{1, M}$.

Точность разведки характеризуется нахождением истинной ("нужной") информации. Вероятность нахождения истинной информации по заданному ключевому слову или фразе равна

$$P_{ИИ} \ge \frac{I_C}{M_C}, \quad (6)$$

где I_C – количество истинных информационных ссылок на конкретную информацию, соответствующую ключевому слову или фразе;

M_C – количество всех информационных ссылок на конкретную информацию, соответствующую ключевому слову или фразе.

Существуют поисковые системы, которые объединяют в себе несколько поисковых систем (например, http://adclick.ru) и могут вести поиск в выбранных пользователем поисковых системах.

Для таких поисковых систем дальность разведки

$$Д_P \le \bigcup_{l=1}^{L} Д_{ПСl}, \quad (7)$$

где l – количество поисковых систем, задействованных в поиске, $l = \overline{1, L}$.

Дальностью действия каждой поисковой системы рассчитывается по формуле (3).

Время разведки и точность разведки рассчитывается по аналогичным формулам (4) – (6) для одной поисковой системы, но с учетом увеличения множества однотипных ключевому слову или фразе ссылок.

Специализированное программное обеспечение поиска. Специальное программное обеспечение поиска предназначено для поиска информации во всем телекоммуникационном пространстве.

Дальность, время и точность разведки рассчитываются по формулам (2) – (6).

Компьютерные вирусы. Это особый вид информационного оружия воздействия на программно-математическое обеспечение АСУ, который может содержать безвредные функции (или ничего не содержать), полезные для пользователя функции (мало вероятно и только гипотетически возможно), а также деструктивные действия – разведки и поражения.

Как правило, эти вирусы разведчики ищут нужную информацию по ключевым словам, собирают адреса (и пароли доступа) и/или необходимую информацию и отправляют по почте на заранее созданные постовые ящики.

К таким вирусам относятся вирусы-"троянские кони" семейства Trojan.PSW. Данное семейство вирусов-"троянских коней" объединяет программы, "ворующие" системные пароли (PSW – Password-Stealing-Ware). При запуске PSW-троянцы ищут системные файлы, хранящие различную конфиденциальную информацию (обычно номера телефонов и пароли доступа к Internet) и отсылают ее по указанному в коде троянца электронному адресу или адресам. Некоторые Windows-PSW-троянцы копи-

руют себя в каталог Windows, регистрируют в системном реестре и запускаются при каждой перезагрузке Windows. Такой тип троянцев является более опасным, поскольку они в состоянии отсылать конфиденциальную информацию в течение длительного промежутка времени.

Например, Trojan_PSW_Spion отсылает ключевую информацию по адресу ranger812@mail.ru. Как видно, адрес является бесплатным и установить владельца невозможно.

Все существующие на данный момент средства защиты от вирусов просто уничтожают этот класс вирусов и никак не используют выгоду, которую можно извлечь.

Но этот класс вирусов можно использовать и в собственных целях. Во-первых, самый напрашиваемый – это создание программного обеспечения (вируса), который изменяет адрес, заложенный в исходный код вируса, на собственный адрес и запуск этого вируса для дальнейшей работы и размножения в киберпространство.

Во-вторых, наиболее эффективный способ – это чтение адреса пересылки, заложенного в исходный код вируса, и удаление вируса из своей системы. Затем, подобрав пароль доступа к почтовому ящику, указанному в коде вируса, получить доступ к уже полученным базам данных паролей и информации, представляющей ценность. При этом время разведки значительно снижается.

Вирус-разведчик характеризуется следующими параметрами: дальность разведки, время разведки, скорость размножения, точность разведки.

Дальность разведки вируса $Д_{PB}$ ограничивается дальностью действия видимого участка сети $Д_C$:

$$Д_{PB} \le Д_C , \tag{8}$$

$$Д_C = \bigcup_{i=1}^{N} Д_i . \tag{9}$$

Время разведки t_P:

$$t_P \le t_{рас} + t_{пи} + t_{д} + t_{об} , \tag{10}$$

где $t_{рас}$ – время распространения вируса по сети;

$t_{пи}$ – время поиска информации в телекоммуникационной сети;

$t_{д}$ – время доставки информации;

$t_{об}$ – время обработки информации.

Скорость распространения вируса V_B:

$$V_B = \frac{P \cdot Q}{t_з} , \tag{11}$$

где P – количество зараженных программ, запущенных за время $t_з$;

Q – количество одновременно заражаемых вирусом программ;

$t_з$ – время работы вируса (в фазе заражения).

Точность разведки характеризуется нахождением истинной ("нужной") информации. Вероятность нахождения истинной информации рассчитывается по формуле

$$P_{ИИ} \ge \frac{I_B}{M_B} , \tag{12}$$

где I_B – количество истинных информационных ссылок на конкретную информацию или сама информация, полученная с помощью вируса;

M_B – количество всех информационных ссылок на конкретную информацию или сама информация, полученная с помощью вируса.

"Троянские кони" и логические бомбы. По своей сути "троянские кони" являются достаточно мощными утилитами удаленного администрирования компьютеров в сети, позволяющими контролировать компьютеры-источники информации в локальной сети или через Internet, предоставляя большие возможности на удаленном Windows-компьютере. К таким троянцам относятся Backdoor.BO (aka Back Orifice Trojan), Backdoor.DeepThroat, Backdoor.Executor, Backdoor.Netbus, Backdoor.Phase aka Phase Server, Backdoor.DeepThroat и др.

При запуске троянец устанавливает себя в сис-

теме и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянца в системе.

Более того, ссылка на троянца отсутствует в списке активных приложений. В результате пользователь этой троянской программы может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

В зависимости от команды троянец выполняет следующие:

– высылает имена компьютера, пользователя и информацию о системе: тип процессора, размер памяти, версия системы, установленные устройства и т.п.;

– дает разрешение на удаленный доступ к дискам (sahre);

– ищет файл на дисках;

– посылает/принимает файл, а также архивирует, уничтожает, копирует, переименовывает и запускает на выполнение любой файл;

– создает/уничтожает каталог;

– отключает текущего пользователя от сети;

– "завешивает" компьютер;

– высылает список активных процессов;

– выгружает указанный процесс;

– подключается к сетевым ресурсам;

– выводит сообщение;

– читает/модифицирует системный реестр;

– открывает/перенаправляет другие сокеты TCP/IP;

– поддерживает протокол HTTP и эмулирует Web-сервер (т.е. троянцем можно управлять при помощи браузера);

– перехватывает, запоминает и затем высылает строки, вводимые с клавиатуры в момент подсоединения компьютера к сети и т.д.

Троянец также позволяет расширить список своих функций при помощи подключаемых ресурсов (plug-in). Они могут быть переданы на сервер и инсталлированы там как часть троянца и в дальнейшем могут выполнять практически любые действия на пораженном компьютере.

Как правило, такой класс троянцев устанавливается на информативные серверы-источники информации. Они характеризуются следующими параметрами: дальность разведки, время разведки, точность разведки.

Дальность разведки троянца ограничивается дальностью действия видимого участка сети и определяется по формуле (8), как и для любого вируса.

Время разведки t_P:

$$t_P \le t_{под} + t_{пи} + t_д + t_{об}, \qquad (13)$$

где $t_{под}$ – время подключения к серверу-источнику информации;

$t_{пи}$ – время поиска информации на нем;

$t_д$ – время доставки информации;

$t_{об}$ – время обработки информации.

Точность разведки характеризуется нахождением истинной ("нужной") информации. Вероятность нахождения истинной информации рассчитывается по формуле

$$P_{ИИ} \ge \frac{I_P}{M_P}, \qquad (14)$$

где I_P – количество истинных информационных ресурсов на сервере-источнике;

M_P – количество всех информационных ресурсов на сервере-источнике.

Логические бомбы характеризуются аналогичными параметрами, что и программы-троянцы.

Удаленная атака. Классификация удаленных атак на распределенные вычислительные системы рассмотрена в [4, 5].

Разведывательная атака (как и любая другая атака) характеризуются следующими параметрами: дальность, время, точность (вероятность совершения атаки), стоимость.

Дальность разведки $Д_р$ определяется по следующей формуле:

$$Д_р \le \bigcup_{b=1}^{B} Д_{сер} , \qquad (15)$$

где $Д_{сер}$ – дальность до сервера атаки; b – количество серверов-источников информации, подвергающихся атаке одновременно, $b = \overline{1, B}$.

Точность, как вероятность совершения атаки (преодоления системы защиты) $P_{пр}$ определяется по формуле

$$P_{пр} = \bigcup_{s=1}^{S} P_{пу_s} \bigcup P_{обз} , \qquad (16)$$

где $P_{пу_s}$ – вероятность s-го преодоления уровня защиты; $P_{обз}$ – вероятность обхода защиты; s – количество уровней защиты, $s = \overline{1, S}$.

Время разведки t_P:

$$t_P \le t_{под} + t_{пз} + t_{пи} + t_{д} + t_{об} , \qquad (17)$$

где $t_{под}$ – время подключения к серверу-источнику информации; $t_{пз}$ – время преодоления системы защиты; $t_{пи}$ – время поиска информации на нем; $t_{д}$ – время доставки информации; $t_{об}$ – время обработки информации.

Подходы к оценке стоимости систем атаки рассмотрены в [6].

"Социальная инженерия" – одна из частей социальной психологии, направленная на манипулирование людьми или порождение в их разуме новой модели поведения. Основные характеристики разведки, с использованием методов "социальной инженерии" в кибернетическом пространстве, зависят от характеристик средств обнаружения.

Выводы

Рассмотренные основные характеристики (дальность, точность и время) разведки информации в кибернетическом (телекоммуникационном, виртуальном) пространстве являются условными и напрямую зависят от возможностей применяемых сил и средств разведки и профессионализма специальных подразделений.

Дальнейшие направления развития. В дальнейшем планируется рассмотреть возможную структуру специальных подразделений "кибервоинов" и наряд сил и средств для проведения разведывательных операций.

Литература

1. Ребров А.В. Кибервойны // Защита информации. Конфидент. – 1999. – № 3. – С. 41-45.

2. Кудрявцев А.М. Обработка разведывательной информации. – Л.: ВАС, 1989. – 332 с.

3. Основи радіоелектронної боротьби в радіотехнічних військах. Конспект лекцій // І.С. Добринін, О.М. Бовкун, В.І. Писаревський, А.В. Снігуров, В.П. Фінаєв / За ред. І.С. Добриніна. – Х.: ООО "Контур", 2006. – 108 с.

4. Гриняев С.Н. Интеллектуальное противодействие информационному оружию. – М.: СИНТЕГ, 1999. – 232 с.

5. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через INTERNET – М.: НПО "Мир и семья-95", 1997. – 224 с.

6. Петров В.Л., Сидченко С.А., Антонов Д.В. Подходы к обоснованию показателей стоимости системы защиты // Сборник научных трудов ХВУ. – Х.: ХВУ, 2001. – № 7(37). – С. 89-92.

Поступила в редакцию 1.09.2006

Рецензент: д-р воен. наук, проф. И.О. Кириченко, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.