базой данных контрольных сумм порнографических материалов с изображением несовершеннолетних, получить их классификацию, сделанную другими сотрудниками и при необходимости добавить свою собственную. Предусмотрена также возможность сохранения файлов и их организации по контрольным суммам, что дает быстрый доступ к ним в процессе проведения оперативных мероприятий.

Факт обнаружения в P2P-сети информации, представляющей оперативный интерес, может послужить основанием для возбуждения уголовного дела и производства расследования. В процессуальной же форме программное обеспечение может найти применение при проведении таких следственных действий, как осмотр (все его виды), выемка предметов, документов, а также следственный эксперимент, выполняемый с целью опытной проверки показаний.

Следует отметить, что доступ к Child Protection System разрешен исключительно пользователям, имеющим персональную лицензию, которую могут получить только действующие сотрудники правоохранительных органов, активно занимающиеся борьбой с распространением детской порнографии. Лицензии предоставляются бесплатно и действуют исключительно на территории государства национальной принадлежности сотрудника. Однако обязательным условием получения лицензии является прохождение сотрудниками правоохранительных органов соответствующего обучения. Такое обучение с 2013 г. проводится в Международном учебном центре подготовки, повышения квалификации и переподготовки кадров в сфере миграции и противодействия торговле людьми Академии МВД Республики Беларусь.

Вышеизложенное позволяет сформулировать следующие выводы.

1. Актуальным направлением деятельности оперативных подразделений по изучению материалов и расследованию дел об обороте детской порнографии является получение информации из P2P-сетей, используемых в преступных целях, а также перехват имеющих уголовно-релевантное значение изображений и сообщений, циркулирующих в них. Факт обнаружения объектов или информации в сети, представляющей оперативный интерес, может послужить основанием для возбуждения уголовного дела и производства расследования.

2. Использование специальных поисковых программных средств значительно упрощает процедуру блокирования ресурсов с запрещенным контентом и привлечения их владельцев к предусмотренной законодательством ответственности. Испытанная на практике методика использования Child Protection System в совокупности с уже имеющимися приемами поисковой деятельности в сети Интернет предоставляет широкие возможности для выявления фактов распространения запрещенного контента в P2P-сетях.



Учитывая, что в настоящее время информационный поиск в P2P-сетях выступает для субъектов оперативно-розыскной деятельности в качестве относительно нового направления деятельности, специфика применения поисковых мероприятий данного вида в сетевом информационном пространстве является актуальной темой отдельного исследования.

УДК 343.985.7:343.542.1

***К.Ю. Гутер***

## DOS-АТАКИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ: СУЩНОСТЬ И КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМАЯ КЛАССИФИКАЦИЯ

В современном мире все большее значение приобретают автоматизированные системы, которые управляют различными критически важными процессами. Отказ в обслуживании в таких системах может привести к непредсказуемым последствиям. Именно поэтому возрастает актуальность вопросов защиты от DoS-атак (от англ. Denial of Service – отказ в обслуживании), обычно определяемых как умышленные атаки на вычислительную систему с целью доведения ее до отказа в обслуживании, т. е. создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам) либо этот доступ будет затруднен.

Для установления истинной картины содеянного и уяснения, в чем конкретно выразилось общественно опасное деяние рассматриваемого вида, имеет смысл подвергнуть криминалистически значимой классификации способы совершения DoS-атак в отношении автоматизированных систем управления (АСУ). Это позволит, с одной стороны, установить в первоначальных следственных ситуациях характерный способ совершения расследуемого преступления (даже по отдельным признакам) и выдвинуть типовую версию о расследуемом событии, а с другой – создать необходимую основу для разработки, внедрения и эффективного применения средств и методов противодействия преступлениям против информационной безопасности.

Анализ практики раскрытия и расследования преступлений, предусмотренных ст. 349–355 Уголовного кодекса Республики Беларусь (преступления против информационной безопасности), показывает, что способы совершения DoS-атак не всегда исследуются в полном объеме. Это вызвано прежде всего неразработанностью научно обоснован-

ной криминалистически значимой классификации способов совершения DoS-атак, что подтверждает преобладающее большинство опрошенных нами респондентов из числа оперативных работников и следователей, специализирующихся на раскрытии и расследовании рассматриваемых преступлений.

Обобщение теории и практики совершения преступлений против информационной безопасности позволяет выделить следующие типы и виды DoS-атак в зависимости от причин, из-за которых может возникнуть DoS-условие.

I. Насыщение полосы пропускания. Этот тип основан на «классической» атаке flood (англ. flood – наводнение, переполнение), которая предполагает критически большое количество бессмысленных или сформированных в неправильном формате запросов к компьютерной системе или сетевому оборудованию АСУ, приводящих к отказу в работе из-за исчерпания системных ресурсов – процессора, памяти или каналов связи.

1. HTTP-флуд (ping-флуд). Механизм этой DoS-атаки состоит в следующем: атакующий посылает незначительный по объему HTTP-пакет, в результате чего сервер АСУ отвечает на него пакетом, размер которого в сотни раз больше. Для предотвращения отказа в обслуживании из-за получения ответных HTTP-пакетов злоумышленник каждый раз подменяет свой IP-адрес IP-адресами узлов в сети. Указанный вид атак можно осуществить только в том случае, если канал атакующего намного шире канала атакуемой АСУ.

2. Smurf-атака (ICMP-флуд). Для реализации этой вида DoS-атаки злоумышленник использует широковещательную рассылку для проверки работающих в системе узлов, отправляя ping-запросы. Затем по широковещательному адресу злоумышленник отправляет поддельный ICMP-пакет, после чего адрес атакующего меняется на адрес АСУ, на который все узлы начинают отправлять ответы на ping-запросы. Соответственно, чем больше объем сети, тем быстрее наступает отказ в обслуживании.

3. Атака Fraggle (UDP-флуд). Атака Fraggle является аналогом Smurf-атаки, однако вместо ICMP-пакетов используются пакеты UDP. Принцип действия заключается в отправке на седьмой порт сервера АСУ echo-команд по широковещательному запросу, а затем – в подмене IP-адреса злоумышленника на IP-адрес сервера АСУ, который начинает получать множество ответных сообщений. Данная атака приводит к насыщению полосы пропускания и полному отказу в обслуживании.

4. Атака переполнения пакетами SYN (SYN-флуд). Принцип атаки заключается в отправке большого количества SYN-запросов (запросов на подключение по протоколу TCP) в достаточно короткий срок с целью переполнять на сервере очередь на подключения. При этом злоумышленник игнорирует SYN+ACK-пакеты цели, не высылая ответных пакетов, либо подделывает заголовок пакета, чтобы ответный SYN+ACK отправлялся на несуществующий адрес. В очереди подключений появляются так называемые полуоткрытые соединения, ожидающие подтверждения от клиента. По истечении определенного таймаута эти подключения отбрасываются. Задача злоумышленника заключается в том, чтобы поддерживать очередь заполненной таким образом, чтобы не допустить новых подключений. Из-за этого клиенты, не являющиеся злоумышленниками, не могут установить связь либо устанавливают ее с существенными задержками.



II. Недостаток ресурсов. Злоумышленники прибегают к данному типу DoS-атак для захвата системных ресурсов АСУ, таких как оперативная и физическая память, процессорное время и др. Обычно такие атаки проводятся с учетом того, что хакер уже обладает некоторым количеством ресурсов системы. Целью атаки является захват дополнительных ресурсов. Для этого не обязательно насыщать полосу пропускания, а достаточно просто перегрузить процессор сервера атакуемой АСУ, то есть занять все допустимое процессорное время.

1. Отправка «тяжелых» пакетов. Атакующий посылает серверу пакеты, которые не насыщают полосу пропускания (канал обычно довольно широкий), но тратят все его процессорное время. Процессор сервера, когда будет их обрабатывать, может не справиться со сложными вычислениями. Из-за этого произойдет сбой, и пользователи не смогут получить доступ к необходимым ресурсам.

2. Переполнение сервера лог-файлами. Лог-файлы сервера – это файлы, в которых записываются действия пользователей сети или программы. Неквалифицированный администратор может неправильно настроить систему на своем сервере, не установив определенный лимит. Хакер воспользуется этой ошибкой и будет отправлять большие по объему пакеты, которые вскоре займут все свободное место на жестком диске сервера. Эта атака сработает только в случае с неопытным администратором, который не хранит лог-файлы на отдельном системном диске.

3. Плохая система квотирования. На некоторых серверах АСУ имеется так называемая CGI-программа, которая связывает внешнюю программу с Web-сервером. Если хакер получит доступ к CGI, он сможет создать скрипт, который задействует значительное количество ресурсов сервера, таких как оперативная память и процессорное время. Так, например, скрипт CGI может содержать в себе циклическое создание больших массивов или вычисление сложных математических формул.

При этом центральный процессор может обращаться к такому скрипту несколько тысяч раз. Следовательно, если система квотирования настроена неправильно, то такой скрипт за малое время отнимет все системные ресурсы у сервера. Конечно, выход из этой ситуации очевиден – установить определенный лимит на доступ к памяти, но и в этом случае процесс скрипта, достигнув этого лимита, будет находиться в ожидании до тех пор, пока не выгрузит из памяти все старые данные. Поэтому пользователи АСУ будут испытывать существенный недостаток в системных ресурсах.

4. Недостаточная проверка данных пользователя. Этот вид атак также приводит к бесконечному либо длительному циклу или повышенному длительному потреблению процессорных ресурсов АСУ (вплоть до исчерпания процессорных ресурсов) либо выделению большого объема оперативной памяти (вплоть до исчерпания доступной памяти).

5. Провокация. Это атака, которая стремится вызвать ложное срабатывание системы защиты и таким образом привести к недоступности ресурса.

III. Ошибки программирования. Данный тип атак основан на использовании специальных программ (эксплойтов), которые помогают атаковать сложные вычислительные ресурсы АСУ чаще всего из-за ошибок в программном коде, приводящих к обращению к неиспользуемому фрагменту адресного пространства, выполнению недопустимой инструкции или другой необрабатываемой исключительной ситуации, когда происходит аварийное завершение программы-сервера – серверной программы.

1. Недостатки в программном коде. Суть атаки данного вида заключается в том, что злоумышленники ищут ошибки в программном коде какой-либо программы либо операционной системы АСУ, заставляя ее обрабатывать такие исключительные ситуации, которые она обрабатывать не умеет, в результате чего возникают ошибки. Простым примером такой атаки может служить частая передача пакетов, в которой не учитываются спецификации и стандарты RFC-документов. Злоумышленники наблюдают, справляется ли сетевой стек с обработкой исключительных ситуаций. Если не справляется, то передача таких пакетов приводит к панике ядра (kernel panic) или даже к краху всей системы в целом.

К этому виду относится ошибка Ping of death, распространенная еще в 1990-е гг. Длина пакета IPv4 по стандарту RFC 791 IPv4 не может превышать 65 535 байт. При этом на атакуемый сервер АСУ посылается ICMP-пакет большей длины, предварительно разбитый на части, в результате чего на сервере от такого пакета переполняется буфер.



2. Переполнение буфера. Переполнение буфера возникает и в том случае, если программа из-за ошибки программиста записывает данные за пределами буфера. Например, программист написал приложение для обмена данными по сети, которое работает по какому-либо протоколу. В этом протоколе строго указано, что определенное поле пакета максимум может содержать 65 536 байт данных. Однако после тестирования приложения оказалось, что в ее клиентской части сети в это поле нет необходимости помещать данные, размер которых больше 255 байт. Поэтому и серверная часть примет не более 255 байт. Далее злоумышленник изменяет код приложения так, что клиентская часть отправляет все допустимые по протоколу 65 536 байт, но сервер к их приему не готов. Из-за этого возникает переполнение буфера, и пользователи АСУ не могут получить доступ к приложению.

3. DoS-атака на уязвимости в программном обеспечении на DNS-серверах. В процессе этой атаки злоумышленник осуществляет подмену IP-адреса DNS-сервера домена АСУ. После чего атакуемый при запросе HTML-страницы попадает либо в «черную дыру» (если IP-адрес был заменен на несуществующий), либо прямиком на сервер злоумышленника. Второй случай чреват более серьезными последствиями, поскольку злоумышленник легко может получить доступ к информационным ресурсам АСУ.

Из вышеизложенного можно определить существование различных видов DoS-атак. К основным их разновидностям относятся насыщение полосы пропускания, недостаток ресурсов, ошибки программирования. Каждый тип угроз характеризуется специфическим способом осуществления и причинами возникновения DoS-условий.

УДК 004 + 351.74/76 + 623.71

***А.В. Железняков***

## ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ РАЗРАБОТКЕ ПЛАНА КОМПЛЕКСНОГО ИСПОЛЬЗОВАНИЯ СИЛ И СРЕДСТВ

В процессе управления подразделениями внутренних войск МВД Республики Беларусь возникает необходимость в выполнении ряда расчетных задач, обеспечивающих подготовку и планирование действий приданных сил. Принимаемые решения определяются опытом ответственного лица и реальным знанием местности района ответственности. В то же время при организации управления подчиненными си-