**Доклад 1. Анализ угроз безопасности в компьютерных сетях.**

Для организации коммуникаций в неоднородной сетевой среде применяется набор протоколов TCP/IP, который обеспечивает совместимость между компьютерами разных типов. Совместимость – одно из основных преимуществ TCP/IP, поэтому большинство компьютерных сетей поддерживает эти протоколы. Кроме того, протоколы TCP/IP предоставляют доступ к ресурсам глобальной сети Интернет.

Благодаря своей популярности TCP/IP стал стандартом де-факто для межсетевого взаимодействия. Однако повсеместное распространение стека протоколов TCP/IP обнажило и его слабые стороны. Создавая свое детище, архитекторы стека TCP/IP не видели причин особенно беспокоиться о защите сетей, строящихся на его основе. Поэтому в спецификациях ранних версий протокола IP отсутствовали требования безопасности, что привело к изначальной уязвимости реализации этого протокола.

Рост популярности интернет-технологий сопровождается ростом серьезных угроз разглашения персональных данных, критически важных корпоративных ресурсов, государственных тайн и т.д. Каждый день хакеры и другие злоумышленники подвергают угрозам сетевые информационные ресурсы, пытаясь получить к ним доступ с помощью специальных атак. Эти атаки становятся все более изощренными по воздействию и несложными в исполнении. Этому способствуют два основных фактора.

Во-первых*,* это повсеместное проникновение Интернета. Сегодня к этой сети подключены миллионы компьютеров.

Многие миллионы компьютеров будут подключены к Интернету в ближайшем будущем, поэтому вероятность доступа хакеров к уязвимым компьютерам и компьютерным сетям постоянно возрастает.

Кроме того, широкое распространение Интернета позволяет хакерам обмениваться информацией в глобальном масштабе.

Во-вторых, это всеобщее распространение простых в использовании операционных систем и сред разработки. Данный фактор резко снижает требования к уровню знаний злоумышленника. Раньше от хакера требовались хорошие знания и навыки программирования, чтобы создавать и распространять вредоносные программы. Теперь, для того чтобы получить доступ к хакерскому средству, нужно просто знать IP-адрес нужного сайта, а для проведения атаки достаточно щелкнуть мышью.

Проблемы обеспечения информационной безопасности в корпоративных компьютерных сетях обусловлены угрозами безопасности для локальных рабочих станций, локальных сетей и из-за атак на корпоративные сети, имеющие выход в общедоступные сети передачи данных.

Сетевые атаки столь же разнообразны, как и системы, против которых они направлены. Некоторые атаки отличаются большой сложностью. Другие может осуществить обычный оператор, даже не предполагающий, какие последствия может иметь его деятельность.

Нарушитель, осуществляя атаку, обычно ставит перед собой следующие цели:

* нарушение конфиденциальности передаваемой информации;
* нарушение целостности и достоверности передаваемой информации;
* нарушение работоспособности системы в целом или отдельных ее частей.

С точки зрения безопасности распределенные системы характеризуются прежде всего наличием *удаленных атак*, поскольку компоненты распределенных систем обычно используют открытые каналы передачи данных, и нарушитель может не только проводить пассивное прослушивание передаваемой информации, но и модифицировать передаваемый трафик (активное воздействие). И если активное воздействие на трафик может быть зафиксировано, то пассивное воздействие практически не поддается обнаружению. Но поскольку в ходе функционирования распределенных систем обмен служебной информацией между компонентами системы осуществляется тоже по открытым каналам передачи данных, то служебная информация становится таким же объектом атаки, как и данные пользователя.

Трудность выявления факта проведения удаленной атаки выводит этот вид неправомерных действий на первое место по степени опасности, поскольку необнаруживаемость препятствует своевременному реагированию на осуществленную угрозу, в результате чего у нарушителя увеличиваются шансы успешной реализации атаки.

Безопасность локальной сети, по сравнению с безопасностью межсетевого взаимодействия, отличается тем, что в этом случае на первое по значимости место выходят *нарушения зарегистрированных пользователей*, поскольку в основном каналы передачи данных локальной сети находятся на контролируемой территории, защита от несанкционированного подключения к которым реализуется административными методами.

На практике IP-сети уязвимы для ряда способов несанкционированного вторжения в процесс обмена данными. По мере развития компьютерных и сетевых технологий (например, с появлением мобильных Java-приложений и элементов ActiveX) список возможных типов сетевых атак на IP-сети постоянно расширяется.

Существуют четыре основные категории сетевых атак:

* атаки доступа;
* атаки модификации;
* атаки на отказ в обслуживании;
* комбинированные атаки.

***Атаки доступа***

Атака доступа – это попытка получения злоумышленником информации, для ознакомления с которой у него нет разрешения. Атака доступа направлена на нарушение конфиденциальности информации.

***Подслушивание* (*Sniffing*).** По большей части данные передаются по компьютерным сетям в незащищенном формате (открытым текстом), что позволяет злоумышленнику, получившему доступ к линиям передачи данных в вашей сети, подслушивать или считывать трафик. Для подслушивания в компьютерных сетях используют сниффер. *Сниффер пакетов* представляет собой прикладную программу, которая перехватывает все сетевые пакеты, передаваемые через определенный домен.

В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (Telnet, FTP, SMTP, POP3 и т. д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли). Предотвратить угрозу сниффинга пакетов можно с помощью следующих мер и средств: применение для аутентификации однократных паролей; установка аппаратных или программных средств, распознающих снифферы; применение криптографической защиты каналов связи.

***Перехват* (*Hijacking*).** В отличие от подслушивания, перехват – это активная атака. Злоумышленник захватывает информацию в процессе ее передачи к месту назначения. Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют один пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме клиент/сервер, а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам.

В самом худшем случае хакер получает доступ к пользовательскому ресурсу на системном уровне и с его помощью создает атрибуты нового пользователя, которые можно в любой момент применить для доступа в сеть и к ее ресурсам.

***Перехват сеанса* (*Session Hijacking*).** По окончании начальной процедуры аутентификации соединение, установленное законным пользователем, например, с почтовым сервером, переключается злоумышленником на новый хост, а исходному серверу выдается команда разорвать соединение. В результате «собеседник» законного пользователя оказывается незаметно подмененным.

После получения доступа к сети у атакующего злоумышленника появляются большие возможности:

* он может посылать некорректные данные приложениям и сетевым службам, что приводит к их аварийному завершению или неправильному функционированию;
* он может также наводнить компьютер или всю сеть трафиком, пока не произойдет останов системы в связи с перегрузкой;
* наконец, атакующий может блокировать трафик, что приведет к потере доступа авторизованных пользователей к сетевым ресурсам.

***Атаки модификации***

Атака модификации – это попытка неправомочного изменения информации. Такая атака возможна везде, где существует или передается информация; она направлена на нарушение целостности информации.

***Изменение данных.*** Злоумышленник, получивший возможность прочитать ваши данные, сможет сделать и следующий шаг – изменить их. Данные в пакете могут быть изменены, даже если злоумышленник ничего не знает ни об отправителе, ни о получателе. Даже если вы не нуждаетесь в строгой конфиденциальности всех передаваемых данных, наверняка вы не захотите, чтобы они были изменены по пути.

***Добавление данных.*** Другой тип атаки – добавление новых данных, например, в информацию об истории прошлых периодов. Взломщик выполняет операцию в банковской системе, в результате чего средства со счета клиента перемещаются на его собственный счет.

***Удаление данных.*** Атака удаления означает перемещение существующих данных, например аннулирование записи об операции из балансового отчета банка, в результате чего снятые со счета денежные средства остаются на нем.

***Атаки отказа в обслуживании***

Атака на отказ в обслуживании (Denial-of-Service, DoS) отличается от атак других типов. Она не нацелена на получение доступа к вашей сети или на получение из этой сети какой-либо информации. Атака DoS делает сеть организации недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения. По существу, эта атака лишает обычных пользователей доступа к ресурсам или компьютерам сети организации.

Большинство атак DoS опирается на общие слабости системной архитектуры. В случае использования некоторых серверных приложений (таких как веб- или FTP-сервер) атаки DoS могут заключаться в том, чтобы занять все соединения, доступные для этих приложений, и держать их в занятом состоянии, не допуская обслуживания обычных пользователей. В ходе атак DoS могут использоваться обычные интернет-протоколы, такие как TCP и ICMP (Internet Control Message Protocol).

Атаки DoS трудно предотвратить, так как для этого требуется координация действий с провайдером. Если трафик, предназначенный для переполнения вашей сети, не остановить у провайдера, то на входе в сеть вы это сделать уже не сможете, потому что вся полоса пропускания будет занята.

Если атака этого типа проводится одновременно через множество устройств, мы говорим о *распределенной атаке отказа в обслуживании DDoS* (*Distributed DoS*)*.*

Простота реализации атак DoS и огромный вред, причиняемый ими организациям и пользователям, привлекают к этим атакам пристальное внимание администраторов сетевой безопасности.

***Отказ в доступе к информации.*** В результате DoS-атаки, направленной против информации, последняя становится непригодной для использования. Информация уничтожается, искажается или переносится в недоступное место.

***Отказ в доступе к приложениям.*** Другой тип DoS-атак направлен на приложения, обрабатывающие или отображающие информацию, или на компьютерную систему, в которой эти приложения выполняются. В случае успеха подобной атаки решение задач, выполняемых с помощью такого приложения, становится невозможным.

***Отказ в доступе к системе.*** Общий тип DoS-атак ставит своей целью вывод из строя компьютерной системы, в результате чего сама система, установленные на ней приложения и вся сохраненная информация становятся недоступными.

***Отказ в доступе к средствам связи.*** Целью атаки является коммуникационная среда. Целостность компьютерной системы и информации не нарушается, однако отсутствие средств связи лишает доступа к этим ресурсам.

***Комбинированные атаки***

Комбинированные атаки заключаются в применении злоумышленником нескольких взаимно связанных действий для достижения своей цели.

***Подмена доверенного субъекта.*** Большая часть сетей и операционных систем использует IP-адрес компьютера, для того чтобы определять, тот ли это адресат, который нужен. В некоторых случаях возможно некорректное присвоение IP-адреса (подмена IP-адреса отправителя другим адресом) – такой способ атаки называют *фальсификацией адреса*, или *IP-спуфингом* (*IP-spoofing*).

IP-спуфинг имеет место, когда злоумышленник, находящийся внутри корпорации или вне ее, выдает себя за законного пользователя. Злоумышленник может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Злоумышленник может также использовать специальные программы, формирующие IP-пакеты таким образом, чтобы они выглядели как исходящие с разрешенных внутренних адресов корпоративной сети.

Атаки IP-спуфинга часто являются отправной точкой для других атак. Классическим примером является атака типа «отказ в обслуживании» (DoS), которая начинается с чужого адреса, скрывающего истинную личность хакера. Обычно IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложениями или по каналу связи между одноранговыми устройствами.

Угрозу спуфинга можно ослабить (но не устранить) с по мощью следующих мер: правильная настройка управления доступом из внешней сети; пресечение попыток спуфинга чужих сетей пользователями своей сети.

Следует иметь в виду, что IP-спуфинг может быть осуществлен при условии, что аутентификация пользователей производится на базе IP-адресов, поэтому введение дополнительных методов аутен тификации пользователей (на основе одноразовых паролей или других методов криптографии) позволяет предотвратить атаки IPспуфинга.

***Посредничество.*** Атака типа «посредничество» подразумевает активное подслушивание, перехват и управление передаваемыми данными невидимым промежуточным узлом. Когда компьютеры взаимодействуют на низких сетевых уровнях, они не всегда могут определить, с кем именно они обмениваются данными.

***Посредничество в обмене незашифрованными ключами* (*атака Man-in-the-Middle –* «*человек в середине*»).** Для проведения атаки «человек в середине» злоумышленнику нужен доступ к пакетам, передаваемым по сети. Такой доступ ко всем пакетам, передаваемым от провайдера ISP в любую другую сеть, может, например, получить сотрудник этого провайдера. Для атак этого типа часто используются снифферы пакетов, транспортные протоколы и протоколы маршрутизации.

**Рисунок. Иллюстрация man-in-the-middle attack.**

В более общем случае атаки «человек в середине» проводятся с целью кражи информации, перехвата текущей сессии и получения доступа к частным сетевым ресурсам, для анализа трафика и получения информации о сети и ее пользователях, для проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии.

Эффективно бороться с атаками типа «человек в середине» можно только с помощью криптографии. Для противодействия атакам этого типа используется *инфраструктура управления открытыми ключами PKI* (Public Key Infrastructure).

***Атака эксплойта.*** Эксплойт (*exploit* – вредоносный код) – это компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на компьютерную систему. Целью атаки может быть, как захват контроля над системой, так и нарушение ее функционирования (DoS-атака).

В зависимости от метода получения доступа к уязвимому программному обеспечению эксплойты подразделяются на удаленные и локальные:

* удаленный эксплойт работает через сеть и использует уязвимость в защите без какого-либо предварительного доступа к уязвимой системе;
* локальный эксплойт запускается непосредственно в уязвимой системе, требуя предварительного доступа к ней. Обычно используется для получения взломщиком прав суперпользователя.

Атака эксплойта может быть нацелена на различные компоненты компьютерной системы – серверные приложения, клиентские приложения или модули операционной системы.

***Парольные атаки*.** Целью этих атак является завладение паролем и логином законного пользователя. Злоумышленники могут проводить парольные атаки, используя такие методы, как

* подмена IP-адреса (IP-спуфинг);
* подслушивание (сниффинг);
* простой перебор.

IP-спуфинг и сниффинг пакетов были рассмотрены выше. Эти методы позволяют завладеть паролем и логином пользователя, если они передаются открытым текстом по незащищенному каналу.

Часто хакеры пытаются подобрать пароль и логин, используя для этого многочисленные попытки доступа. Такой подход носит название «*атака полного перебора*»(*Brute Force Attack*). Для этой атаки используется специальная программа, которая пытается получить доступ к ресурсу общего пользования (например, к серверу). Если в результате злоумышленнику удается подобрать пароль, он получает доступ к ресурсам на правах обычного пользователя. Если этот пользователь имеет значительные привилегии доступа, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если пользователь изменит свои пароль и логин.

Средства перехвата, подбора и взлома паролей в настоящее время считаются практически легальными и официально выпускаются достаточно большим числом компаний. Они позиционируются как программы для аудита безопасности и восстановления забытых паролей, и их можно на законных основаниях приобрести у разработчиков.

Парольных атак можно избежать, если не пользоваться паролями в текстовой форме. Использование одноразовых паролей и криптографической аутентификации может практически свести на нет угрозу таких атак. К сожалению, не все приложения, хосты и устройства поддерживают указанные методы аутентификации.

При использовании обычных паролей необходимо придумать такой пароль, который было бы трудно подобрать. Минимальная длина пароля должна быть не менее восьми символов. Пароль должен включать символы верхнего регистра, цифры и специальные символы (#, $, &, % и т. д.).

***Угадывание ключа.*** Криптографический ключ представляет собой код или число, необходимое для расшифровки защищенной информации. Хотя узнать ключ доступа трудно и это требует больших затрат ресурсов, тем не менее это возможно. В частности, для определения значения ключа может быть использована специальная программа, реализующая метод полного перебора. Ключ, к которому получает доступ атакующий, называется скомпрометированным. Атакующий использует скомпрометированный ключ для получения доступа к защищенным передаваемым данным без ведома отправителя и получателя. Ключ дает возможность расшифровывать и изменять данные.

***Атаки на уровне приложений.*** Эти атаки могут проводиться несколькими способами. Самый распространенный из них состоит в использовании известных слабостей серверного программного обеспечения (FTP, HTTP, веб-сервера).

Главная проблема с атаками на уровне приложений состоит в том, что они часто пользуются портами, которым разрешен проход через межсетевой экран.

Сведения об атаках на уровне приложений широко публикуются, чтобы дать возможность администраторам устранить проблему с помощью коррекционных модулей (патчей). К сожалению, многие хакеры также имеют доступ к этим сведениям, что позволяет им учиться.

Невозможно полностью исключить атаки на уровне приложений. Хакеры постоянно открывают и публикуют на своих сайтах в Интернете все новые уязвимые места прикладных программ. Здесь важно осуществлять хорошее системное администрирование. Чтобы снизить уязвимость от атак этого типа, можно, в частности, использовать системы распознавания атак IDS (Intrusion Detection Systems).

***Анализ сетевого трафика.*** Целью атак подобного типа являются прослушивание каналов связи и анализ передаваемых данных и служебной информации с целью изучения топологии и архитектуры построения системы, получения критической пользовательской информации (например, паролей пользователей или номеров кредитных карт, передаваемых в открытом виде). Атакам данного типа подвержены такие протоколы, как FTP и Telnet, особенностью которых является то, что имя и пароль пользователя передаются в рамках этих протоколов в открытом виде.

***Сетевая разведка*** *–* это сбор информации о сети с помощью общедоступных данных и приложений. При подготовке атаки против какой-либо сети хакер, как правило, пытается получить о ней как можно больше информации.

Сетевая разведка проводится в форме запросов DNS, эхо-тестирования (Ping Sweep) и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо-тестирование адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, хакер использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. В результате добывается информация, которую можно использовать для взлома. Системы IDS на уровне сети и хостов обычно хорошо справляются с задачей уведомления администратора о ведущейся сетевой разведке, что позволяет лучше подготовиться к предстоящей атаке и оповестить провайдера, в сети которого установлена система, проявляющая чрезмерное любопытство.

***Злоупотребление доверием.*** Данный тип действий не является атакой в полном смысле этого слова. Он представляет собой злонамеренное использование отношений доверия, существующих в сети. Типичным примером такого злоупотребления является ситуация в периферийной части корпоративной сети. В этом сегменте обычно располагаются серверы DNS, SMTP и HTTP. Поскольку все они принадлежат к одному и тому же сегменту, взлом одного из них приводит к взлому и всех остальных, так как эти серверы доверяют другим системам своей сети. Риск злоупотребления доверием можно снизить за счет более жесткого контроля уровней доверия в пределах своей сети. Системы, расположенные с внешней стороны межсетевого экрана, никогда не должны пользоваться абсолютным доверием со стороны систем, защищенных межсетевым экраном.

***Псевдоантивирусы*** – это мошеннические программы, являющиеся фальшивыми антивирусами. Хотя псевдоантивирусы выводят сообщения об обнаружении вредоносных программ, на самом деле они ничего не находят и не лечат. Их задача состоит совсем в другом: убедить пользователя в наличии угрозы (на самом деле не существующей) для компьютера и спровоцировать его уплатить деньги за активацию «антивирусного продукта». Такой вид мошеннических программ, согласно классификации «Лаборатории Касперского», называется FraudTool и относится к классу RiskWare.

**Рисунок. Фальшивый антивирус Security Essentials 2011. Обратите внимание на пугающий своими масштабами список якобы обнаруженных в системе угроз.**

Для распространения фальшивых антивирусов используются способы, применяемые для распространения большинства вредоносных программ, например, скрытая загрузка при помощи Trojan-Downloader, эксплуатация уязвимостей, взломанных/зараженных сайтов. Мошенники используют также рекламу в Интернете. В настоящее время множество сайтов размещают баннеры с информацией о новом «волшебном» продукте, который избавляет от всех проблем.

Первым этапом деятельности псевдоантивируса является «сканирование» системы пользователя. По ходу «сканирования» псевдоантивирус выводит сообщения, последовательность которых хорошо продумана: например, ошибка Windows, обнаружение вредоносных программ, необходимость установить антивирус. Фальшивый антивирус предлагает исправить якобы выявленные ошибки и вылечить систему, но уже за деньги. Чем достовернее имитация действий серьезного легального ПО, тем больше у мошенников шансов получить плату за «работу» лжеантивируса.

Фальшивые антивирусы приносят очевидную выгоду мошенникам, которые получают прибыль от продажи «лицензий» на фальшивые защитные программы. Кроме того, фальшивки нередко содержат действительно вредоносные программы, которые могут использоваться для получения доступа к вашему компьютеру, кражи ваших персональных данных с целью их дальнейшей перепродажи или для превращения компьютера в зомби-машину и рассылки огромного количества спама.

***Фишинг*** является относительно новым видом интернет-мошенничества, цель которого – получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов, PIN-кодов и другой конфиденциальной информации, дающей доступ к деньгам пользователя. Фишинг использует не технические недостатки программного обеспечения, а легковерность пользователей Интернета. Сам термин phishing, созвучный с fishing (рыбная ловля), расшифровывается как password harvesting fishing – выуживание пароля. Действительно, фишинг очень похож на рыбную ловлю. Злоумышленник закидывает в Интернет приманку и «вылавливает» всех «рыбок» – пользователей Интернета, которые клюнут на эту приманку.

**Рисунок. Подделка сайта mail.ru для фишинга.**

Злоумышленником создается практически точная копия сайта выбранного банка (электронной платежной системы, аукциона и т. п.). Затем при помощи спам-технологии по электронной почте рассылается письмо, составленное таким образом, чтобы быть максимально похожим на настоящее письмо от выбранного банка. При составлении письма используются логотипы банка, имена и фамилии реальных руководителей банка. В таком письме, как правило, сообщается о том, что из-за смены программного обеспечения в системе интернет-банкинга пользователю необходимо подтвердить или изменить свои учетные данные. В качестве причины для изменения данных могут быть названы выход из строя ПО банка или же нападение хакеров. Наличие правдоподобной легенды, побуждающей пользователя к необходимым действиям, – непременная составляющая успеха мошенников-фишеров. Во всех случаях цель таких писем одна – заставить пользователя щелкнуть по приведенной ссылке, а затем ввести свои конфиденциальные данные (пароль, номер счета, PIN-код) на ложном сайте банка (электронной платежной системы, аукциона). Зайдя на ложный сайт, пользователь вводит в соответствующие строки свои конфиденциальные данные, а далее аферисты получают доступ в лучшем случае к его почтовому ящику, а в худшем – к электронному счету.

Технологии фишеров совершенствуются, применяются методы социальной инженерии. Клиента пытаются напугать, придумать критичную причину для того, чтобы он выдал свои конфиденциальные данные. Как правило, сообщения содержат угрозы, например, заблокировать счет в случае невыполнения получателем требований, изложенных в сообщении.

В настоящее время мошенники часто используют троянcкие программы. Задача фишера в этом случае сильно упрощается – достаточно заставить пользователя перебраться на фишерский сайт и «подцепить» программу, которая самостоятельно разыщет на винчестере жертвы все, что нужно. Наравне с троянскими программами стали использоваться и кейлоггеры. На подставных сайтах на компьютеры жертв загружают шпионские утилиты, отслеживающие нажатия клавиш. При использовании такого подхода необязательно находить выходы на клиентов конкретного банка или компании, а потому фишеры стали подделывать и сайты общего назначения, такие как новостные ленты и поисковые системы.

Успеху фишинг-афер способствует низкий уровень осведомленности пользователей о правилах работы компаний, от имени которых действуют преступники. В частности, около 5% пользователей не знают простого факта: банки не рассылают писем с просьбой подтвердить в онлайне номер своей кредитной карты и ее PIN-код. Основной защитой от фишинга пока остаются спам-фильтры. К сожалению, программный инструментарий для защиты от фишинга обладает ограниченной эффективностью, поскольку злоумышленники эксплуатируют в первую очередь не бреши в ПО, а человеческую

психологию.

Появилось сопряженное с фишингом понятие – фарминг.

***Фарминг*** – это еще один вид мошенничества, ставящий целью получить персональные данные пользователей, но не через почту, а прямо через официальные веб-сайты. Фармеры заменяют на серверах DNS цифровые адреса легитимных веб-сайтов на поддельные, в результате чего пользователи перенаправляются на сайты мошенников. Этот вид мошенничества еще опаснее, так как заметить подделку практически невозможно.

Для защиты от фишинга и фарминга разрабатываются технические средства безопасности, прежде всего плагины для популярных браузеров. Суть защиты заключается в блокировании сайтов, попавших в черные списки мошеннических ресурсов. Следующим шагом могут стать системы генерации одноразовых паролей для интернет-доступа к банковским счетам и аккаунтам в платежных системах.

***Применение ботнетов.*** Ботнет (зомби-сеть) – это сеть компьютеров, зараженных вредоносной программой поведения Backdoor. Backdoor’ы позволяют киберпреступникам удаленно управлять зараженными машинами (каждой в отдельности, частью компьютеров, входящих в сеть, или всей сетью целиком) без ведома пользователя. Такие программы называются ботами.

Ботнеты обладают мощными вычислительными ресурсами, являются грозным кибероружием и хорошим способом зарабатывания денег для злоумышленников. При этом зараженными машинами, входящими в сеть, хозяин ботнета может управлять откуда угодно: из другого города, страны или даже с другого континента, а организация Интернета позволяет делать это анонимно.

Управление компьютером, который заражен ботом, может быть прямым и опосредованным.

В случае прямого управления злоумышленник может установить связь с инфицированным компьютером и управлять им, используя встроенные в тело программы-бота команды.

В случае опосредованного управления бот сам соединяется с центром управления или другими машинами в сети, посылает запрос и выполняет полученную команду.

В любом случае хозяин зараженной машины, как правило, даже не подозревает о том, что она используется злоумышленниками. Именно поэтому зараженные вредоносной программой-ботом компьютеры, находящиеся под тайным контролем киберпреступников, называют еще зомби-компьютерами, а сеть, в которую они входят, – зомби-сетью. Чаще всего зомби-машинами становятся персональные компьютеры домашних пользователей.

Рисунок. Структура ботнет.

Ботнеты могут использоваться злоумышленниками для решения криминальных задач разного масштаба: от рассылки спама до атак на государственные сети.

*Рассылка спама.* Это наиболее распространенный и один из самых простых вариантов эксплуатации ботнетов. По экспертным оценкам, в настоящее время более 80% спама рассылается с зомбимашин. Спам с ботнетов не обязательно рассылается владельцами сети. За определенную плату спамеры могут взять ботнет в аренду. Среднестатистический спамер зарабатывает 50–100 тысяч долларов в год. Многотысячные ботнеты позволяют спамерам осуществлять с зараженных машин миллионные рассылки в течение короткого времени. Еще одно «преимущество» ботнетов – возможность сбора адресов электронной почты на зараженных машинах. Украденные адреса продаются спамерам либо используются при рассылке спама самими хозяевами ботнета. При этом растущий ботнет позволяет получать новые и новые адреса.

*Анонимный доступ в Сеть.* Злоумышленники могут обращаться к серверам в Сети, используя зомби-машины, и от имени зараженных машин совершать киберпреступления – например, взламывать вебсайты или переводить украденные денежные средства.

*Продажа и аренда ботнетов.* Один из вариантов незаконного заработка при помощи ботнетов основывается на сдаче ботнета в аренду или продаже готовой сети. Создание ботнетов для продажи является отдельным направлением киберпреступного бизнеса.

*Кража конфиденциальных данных.* Этот вид криминальной деятельности постоянно привлекает киберпреступников, а с помощью ботнетов улов в виде различных паролей (для доступа к e-mail, FTP-ресурсам, веб-сервисам) и прочих конфиденциальных данных пользователей увеличивается в тысячи раз! Бот, которым заражены компьютеры в зомби-сети, может скачать другую вредоносную программу – например, троянца, ворующего пароли. В таком случае инфицированными троянской программой окажутся все компьютеры, входящие в эту зомби-сеть, и злоумышленники смогут заполучить пароли со всех зараженных машин. Украденные пароли перепродаются или используются, в частности для массового заражения веб-страниц (например, пароли для всех найденных FTP-аккаунтов) с целью дальнейшего распространения вредоносной программы-бота и расширения зомби-сети.

Перечисленные атаки на IP-сети возможны в силу ряда причин:

* использование общедоступных каналов передачи данных. Важнейшие данные передаются по сети в незашифрованном виде;
* уязвимости в процедурах идентификации, реализованных в стеке ТСР/ІР. Идентифицирующая информация на уровне ІР передается в открытом виде;
* отсутствие в базовой версии стека протоколов ТСР/ІР механизмов, обеспечивающих конфиденциальность и целостность передаваемых сообщений;
* аутентификация отправителя осуществляется по его IP-адресу. Процедура аутентификации выполняется только на стадии установления соединения, а в дальнейшем подлинность принимаемых пакетов не проверяется;
* отсутствие возможности контроля за маршрутом прохождения сообщений в сети Интернет, что делает удаленные сетевые атаки практически безнаказанными.