Рекогносцировка наоборот

Индустрия получения, обработки, регистрации, передачи, распространения информации в настоящее время является одной из ведущих областей деятельности человечества, куда с каждым годом вкладывают все более значительные средства. Информация становится важнейшим стратегическим ресурсом, нехватка которого приводит к существенным потерям во всех областях жизни

Раньше считалось, что информация всего лишь обеспечивает осведомленность людей о событиях и фактах в окружающем мире. Информация воспринималась как полезный ресурс, предназначенный для расширения человеческих возможностей. Теперь же любой бизнес-процесс или процесс в обществе нуждается в обработке чрезвычайно большого количества информации, и эта обработка уже давно является невозможной без информационно-коммуникационных технологий (ИКТ)

Но ежедневно мы становимся свидетелями процессов, когда политические, общественные и бизнесовые конфликты переходят в плоскость информационного противоборства, которое без преувеличения имеет характер информационной войны. В классическом понимании информационная война — это одна из форм информационного противоборства, комплекс мероприятий по информационному влиянию на массовое сознание для изменения поведения людей и навязывания им целей, которые не соответствуют их интересам, а также защита от подобных влияний.

Системы, построенные на основе ИКТ, становятся одной из первых целей и часто — первыми жертвами информационной войны. Глубокое проникновение всемирной компьютерной сети Интернет в жизнь общества невероятно увеличивает как возможности противников, так и их уязвимости. Рассмотрим некоторые пути анализа уязвимостей собственных ИКТ-ресурсов, способы предотвращения и противодействия использованию уязвимостей ИКТ-систем в ходе так называемых «информационных операций».

Понятие «информационные операции»

Термин «информационные операции» распространился благодаря многочисленным документам и публикациям Департамента обороны США. Информационные операции определяются как «акции, направленные на влияние на информацию и информационные системы противника и защиту собственной информации и информационных систем».

В соответствии с полевым уставом военного ведомства США (FM 100-6) «Информационные операции», «ориентация в ситуации означает комбинацию ясного представления о диспозициях своих и враждебных сил с оценкой ситуации и намерений со стороны командования».

Уровень готовности к проведению информационных операций сегодня считается ключевым фактором успеха проведения любой как военной, так и социальной процедуры, кампании.

Информация является отображением вложенного у нее содержания, а информационные системы обрабатывают информацию, критичную для принятия решений. Поэтому сегодня информация превратилась из абстрактного термина в объект, цель и средство информационных операций.

Особенной целью при проведении информационных операций являются информационно-аналитические системы субъекта влияния. Осуществляя влияние на такие системы, можно добиться того, что принимающие решение лица из лагеря противника примут неадекватные выводы, и необходимый социальный процесс изменит траекторию в направлении, необходимом для стороны, которая влияет (рис. 1). В этом случае к непосредственным информационным влияниям может быть отнесено размещение в информационном пространстве документов, которые компрометируют противоположную сторону, рекламу (в том числе скрытую) своих преимуществ, перекрученные данные о внешней среде, перекрученную информацию о намерениях и тому подобное.

РЕКОГНОСЦИРОВКА (от лат. recognosco — осматриваю) — в военном деле — визуальное изучение противника и местности в районе предстоящих боевых действий лично командиром (командующим) и офицерами штабов для получения данных и принятия решения

Большой энциклопедический словарь

ТЕЛЕКОМ-ИНФО

Социальная сеть «ВКонтакте» была взломана хакерами

Самая популярная российская социальная сеть «ВКонтакте» взломана. На одном из хакерских сайтов были опубликованы данные учетных записей более 130 тысяч ее пользователей.

По предварительным данным, схема похищения логина и пароля для доступа к социальной сети была такой: сначала на компьютер пользователя устанавливалась вредоносная программа Trojan.Win32.VkHost.an — она распространялась через приложение «ВКонтакте» которое в настоящий момент заблокировано администрацией ресурса.

После установки в систему троянец подменял содержимое файла hosts на следующее: 83.133.120.252 vkontakte.ru и 83.133.120.252 odnoklassniki.ru.

Впоследствии, когда пользователь пытался открыть сайт одной из этих социальных сетей, его перенаправляли на фишинговую страницу, в которой требовалось ввести свой логин и пароль. Регистрационные данные уходили в базы на том же сайте, а пользователю сообщалось, что его аккаунт будет заблокирован, причем для разблокирования нужно отправить на некий короткий номер СМС, стоимость которого достигала $10.

«В настоящий момент база украденных паролей «Одноклассников» на фишинговом сайте пуста, поэтому говорить о компрометации данных пользователей этой социальной сети пока нет оснований», — говорит Александр Гостев, руководитель центра глобальных исследований и анализа угроз «Лаборатории Касперского».

В компании рекомендуют всем пользователям «ВКонтакте» и «Одноклассники» проверить содержимое своих файлов hosts, которые находятся в каталоге %windir%\system32\drivers\etc, и если в них обнаружены ссылки на vkontakte.ru и odnoklassniki.ru, удалить данные файлы.

«Также необходимо сменить все пароли от всех аккаунтов в социальных сетях. В случае попадания на подобные фишинговые страницы, ни в коем случае не следует вводить свои логин и пароль и не отправлять никаких SMS-сообщений», — говорится в сообщении.

http://mycityua.com/news/country/2009/08/03/145632.html

Информационное влияние

Одним из основных методов ведения информационных операций является информационное влияние, которое предоставляется с целью «непрямого» информационного управления — когда объекту управления дается определенная информационная картина, под воздействием которой он формирует линию своего поведения.

Процесс информационного влияния может быть разделен на такие этапы:

✓генерация источником влияния данных, информационных элементов и информационной совокупности;

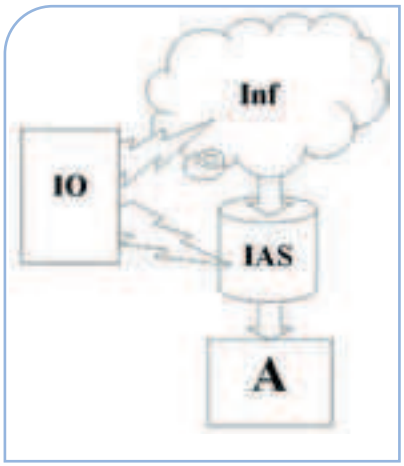


Рис. 1. Влияние на информационно-аналитическую систему противника:
Inf — информационное пространство;
IAS — информационно-аналитическая система;
A — абонент системы (лицо, принимающее решение);
IO — информационные воздействия

✓передача информации источником влияния;

✓прием информации реципиентом;

✓генерация совокупности данных, информационных элементов и новой совокупности объекта влияния;

✓соответствующие активные действия на объект влияния.

Информационные влияния на элементы систем можно классифицировать по таким признаками, как источники возникновения, длительность влияния, природа возникновения и т. п.

Для выбора конкретных способов реализации информационного управления необходимо конкретизировать задания, провести анализ процесса формирования информационных операций и определить критерии их оценки. Информационное управление рассматривают как процесс, который охватывает такие три взаимозависимых направления:

✓управление обменом данными между реальным миром и виртуальным миром субъекта влияния;

✓управление виртуальным миром субъектов влияния, механизмами принятия решений;

✓управление процессом превращения решений в действия субъектов влияния в реальном мире.

Информационное влияние может быть двух основных видов:

✓изменение в необходимую сторону данных, которые использует информационно-аналитическая система объекта влияния при принятии решений;

✓непосредственное влияние на процесс принятия решения объекта влияния, например, на процедуры принятия решения или отдельных личностей, которые принимают решение.

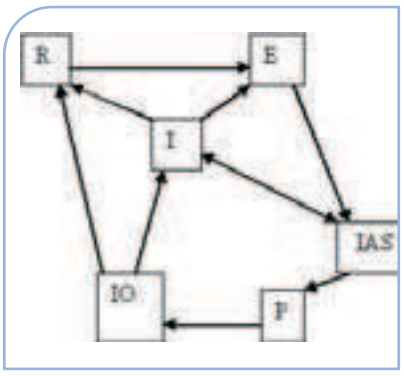


Рис. 2. Диаграмма оперативного управления с использованием информационно-аналитических систем

Рис. 3. Исследование отправлений с помощью поисковых систем

Оперативное управление информационными операциями с использованием информационно-аналитических систем можно проиллюстрировать с помощью диаграммы, представленной на рис. 2.

В соответствии с приведенной диаграммой информация из реального мира (R) поступает в информационное пространство, в частности, в средства массовой информации (I) или непосредственно экспертам (E), а также через средства массовой информации. От экспертов или непосредственно из информационного пространства (например, с помощью средств контент-мониторинга) информация поступает в информационно-аналитическую систему (IAS). Информационно-аналитическая система передает лицам, принимающим решение (P), данные, которые определяют мероприятия информацион-

ТЕЛЕКОМ-ИНФО

GMail, Yahoo!, Hotmail и AOL подверглись атаке хакеров

Крупнейшие в интернете почтовые службы -- GMail, Yahoo!, Hotmail и AOL — подверглись фишинг-атакам, в результате которых в сеть просочилась информация о паролях около 30 тысяч пользователей, пишет The Daily Telegraph.
Представители Google (владельца GMail) и Microsoft (собственника Hotmail) подтвердили, что их сервисы стали целью киберпреступников, однако, по их словам, собственно серверы и системы компаний никаких потерь не понесли.
В качестве ответной меры в массовом порядке были изменены пароли почтовых ящиков, пострадавших от фишинга, сообщает издание. По данным газеты, действия хакеров распространились и на другие популярные в США почтовые сервисы — например, Comcast и Earthlink.
Список украденных e-mail и паролей к ним был опубликован на Pastebin.com, который используют программисты для обмена данными. При этом газета уточняет, что информация об электронных почтовых ящиках впоследствии была удалена с этого сайта.
Принцип так называемого фишинга (от англ. fishing — ловля рыбы, рыбалка) заключается в том, чтобы направить пользователя на поддельный сайт, очень похожий на «настоящий» (например, сайт платежной системы, банка, почтового ящика и т. д.). «Жертве» под каким-нибудь благовидным предлогом предлагается ввести свои логин и пароль. Таким образом человек сам отдает конфиденциальную информацию в руки киберпреступников.
http://www.sostav.ua/news/2009/10/08/51/25962/

ного влияния на информационное пространство и непосредственно на объекты реального мира (людей, окружающую среду, компьютерные системы и т. п.).

Информационное влияние на ИКТ-ресурсы

В XXI веке влияние в ходе информационной операции на ИКТ-ресурсы противника может стать самым производительным орудием информационных войн. Вмешательство в технологии передачи, обработки и хранения информации в автоматизированных системах может происходить с целью:

✓несвоевременного попадания информации в информационно-аналитический центр (ИАС), а как следствие — несвоевременного анализа информации и реагирования со стороны пользователя ИАЦ;

✓задержки в обработке и распространении информации, а как следствие — несвоевременного распространения информации, которая порождена согласно решений абонента ИАЦ; это может существенно снизить эффективность социального и общественного влияния информации, которая должна была быть распространена;

✓снабжение в ИАЦ порочной информации путем несанкционированного вмешательства в доверенные каналы снабжения информации, в том числе подделки сетевых атрибутов, электронных подписей и т. п., что может повлиять на анализ настоящей информации и заставить абонента принять ошибочные решения;

✓получение конфиденциальной информации о противнике путем несанкционированного вмешательства в его автоматизированные системы или путем влияния на определенных пользователей автоматизированных систем противника, которые имеют доступ к конфиденциальной информации;

✓распространение дезинформации от имени противника путем вмешательства в его каналы распространения и (или) подделки атрибутов источника информации.

Кроме того, атака на ИКТ-ресурсы, которая достигла цели, в то же время является действенным средством собственного информационного влияния.

Поиск уязвимостей ИКТ

Процесс информационной атаки через вмешательство в ИКТ может быть условно разделен на три основных этапа: исследование ИКТ-структуры противника, анализ уязвимостей и использование уязвимостей.

Исследование ИКТ-структуры организации начинается «извне», с использованием лишь открытой информации. Приведем несколько ситуаций на примере частных доменов, принадлежащих авторам.

Исследуются поисковые системы WWW по-поводу их «знаний» об известных доменах и IP-адресов объекта исследования, участие пользователей с такими доменами и IP-адресами в различных форумах (рис. 3). Также с помощью поисковых систем можно найти «скрытые» страницы сайтов, которые когда-то были соединены с основными, но на момент исследования уже не существует ссылок на них с других ресурсов.

Результаты могут быть ошеломляющими. Так, на сайте одной организации стали публично доступными отчеты прокси-сервера относительно внутренних пользователей и перечня ресурсов, которые они посещали.

Исследуются публичные базы данных WHOIS, которые принадлежат администраторам публичных доменов, чтобы выяснить, где подключены авторитетные DNS и кто их адми-

нистрирует. На рис. 4 представлены результаты анализа домена, который предлагает сайт www.robtex.com в виде графа и таблицы.

Также исследуются публичные базы данных регионального интернет-реестра (RIR), которые управляют предоставлением IP-адресов в определенном регионе, чтобы выяснить, какие блоки IP-адресов связаны с сетью исследуемого объекта, как они взаимодействуют с другими провайдерами и кто их администрирует.

Кроме того, анализируются глобальные таблицы маршрутизации Интернета, которые являются публично доступными во многих центрах координации сети. Информация из серверов — маршруты по так называемым «Looking glass» — позволит обнаружить, к каким операторам подключена исследуемая сеть, путем изучения взаимодействия автономных систем (AS) и даже узнать, какими были эти связки в течение последнего времени (рис. 5).

Провести такой анализ тем сложнее, чем меньше такой информации позволяет увидеть организация. К сожалению, полностью скрыть структуру сети невозможно, потому что во многих случаях усиление защиты приводит к существенному или даже неприемлемому осложнению взаимодействия ИКТ с внешним миром — сетью Интернет. В первую очередь, невозможно скрыть точки входа (IP-адреса) для сообщений e-mail, DNS, адрес публичного веб-сайта.

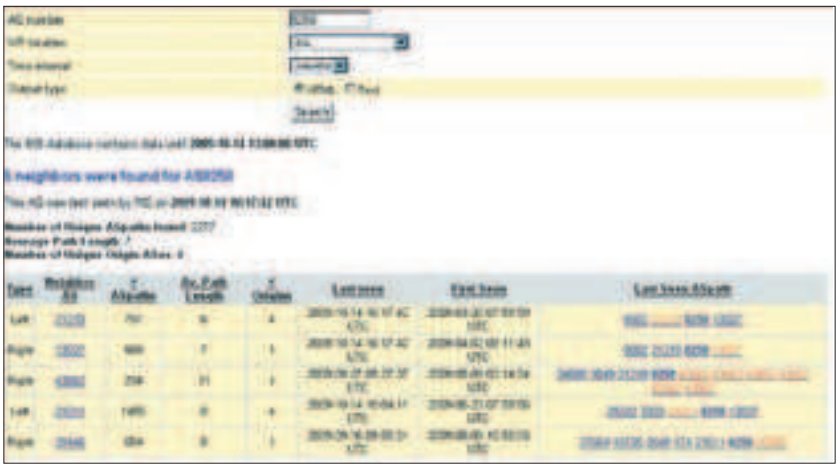


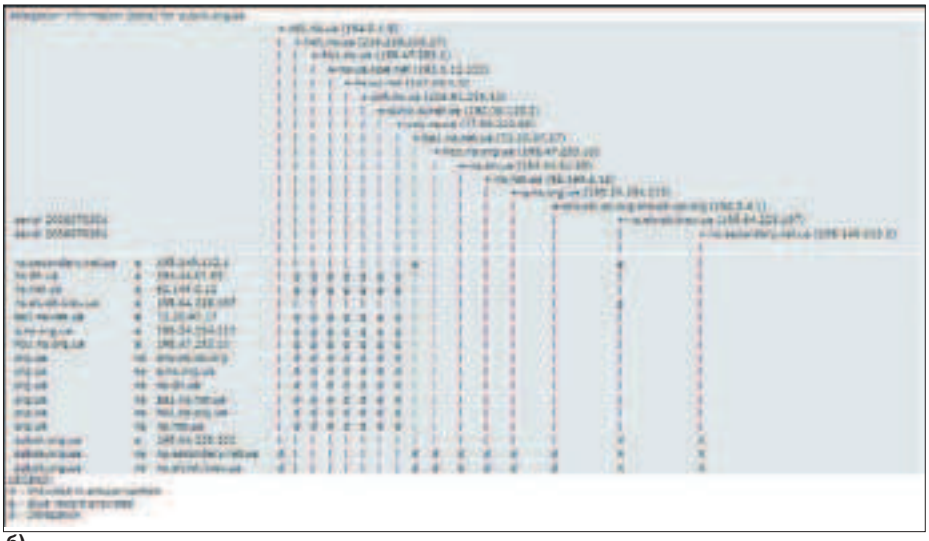
Рис. 5. Исследования «провайдерских» связей относительно требуемых IP-адресов за последнее время (с сайта www.ripe.net)

После изучения открытой информации при проведении информационных операций встречаются сугубо «хакерские» методы анализа сетевой инфраструктуры и сетевых служб на наличие известных уязвимостей. Под «хакерскими» методами подразумеваются сканирования адресов и сетей, попытки грубого подбора паролей, разнообразных атак, связанных с проблемами реализации коммуникационных протоколов в определенном программном обеспечении атакованной сети. Конечной целью атаки на ИКТ-ресурс может быть получение конфиденциальной информации, выведение из строя (то есть недосягаемость для легальных пользователей) определенного сервиса, изменение информации на официальном сайте противника (deface). Все это должно помочь в реализации цели всей информационной операции, которая была приведена раньше и в целом определяется как информационная атака.

Если выполняется тестирование сети большой организации, когда организация позволяет увидеть минимум информации, оценка безопасности такой большой сети может стать достаточно длительным циклическим процессом. Шаг за шагом, данные, полученные через источники информации, относительно доверенных доменных имен, IP-адресов, деталей учетных записей пользователей могут быть переданы другим процессам для последующего тестирования. Блок-схема на рис. 6 очерчивает эту процедуру и данные, которые передаются между процессами.

Эта блок-схема включает составление реестра (enumeration) сети, массовое сканирование сети и, в конце, тестирование специфических сервисов. В процессе тестирования аналитик может натолкнуться на неконтролируемый сервис DNS, который позволит идентифицировать предварительно неизвестные блоки IP-адресов, которые могут быть снова «скормлены» процессу enumeration, чтобы идентифицировать последующие компоненты сети. Таким же образом в публично доступных директориях аналитик может натолкнуться на несколько учетных записей, к которым может быть применен метод подбора паролей.

а)



б)

Рис. 4. Анализ DNS в виде графа (а) и таблицы иерархии DNS (б) с веб-сайта www.robtex.com

Меры против исследования ИКТ-ресурсов

Очевидно то, что при защите собственных ИКТ-ресурсов во время проведения информационных операций первым заданием является осложнение работы противника относительно исследования ИКТ-инфраструктуры.

Наиболее действенной контрмерой такому изучению есть приведение объема публично доступной информации к такому минимуму, чтобы постороннее оценивание безопасности стало буквально бесконечным циклическим процессом. Чтобы достичь этого, можно воспользоваться такими рекомендациями:

✓публично доступные серверы не должны содержать или выдавать лишнего контента:

- никаких веб-документов, кроме тех, к которым необходим доступ внешних пользователей;
- запретить листинг директорий (directory index);
- не детализировать структуру почтовой системы в заголовках e-mail;
- не детализировать, и тем более не конкретизировать информацию обратного DNS- резолвинга относительно адресов, кроме тех, которые принадлежат открытым сервисам;

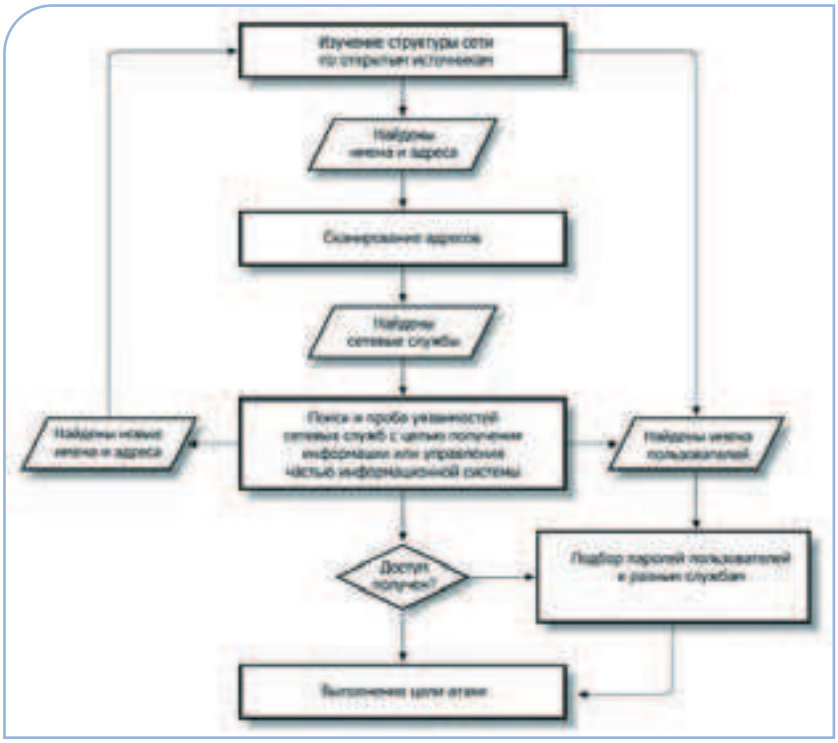


Рис. 6. Блок-схема алгоритма исследования и вмешательства в информационно-коммуникативную сеть

✓опубликованные контакты по административным и техническим вопросам должны быть не персональными, а обобщенными, для предотвращения атак отдельной личности средствами социальной инженерии.

Используя схему, приведенную на рис. 6, и специализированное программное обеспечение, можно самостоятельно проверять степень открытости собственных ИКТ-ресурсов организации к такому исследованию.

Вмешательство в ИКТ-ресурсы сегодня является одним из действенных средств проведения информационных операций, и ему свойственна такая же этапность и схема проведения, что и более традиционным операциям, которые проходят за пределами ИКТ.

Как и традиционная информационная операция, атака на ИКТ-ресурси может оказаться или удачной, или неудачной. Для своевременного выявления атаки необходимо уделить внимание изучению сетевой активности, попыток сканирования, относительного объема электронных писем с вредным контентом и т. п. Для этого уместно использовать и ретроспективный анализ, то есть нахождение аналогов, операций, которые уже состоялись, удачных или неудачных. Употребление профилактических мер пресечения, которые направлены на осложнение и замедление изучения ІКТ-инфраструктуры объекта атаки, существенно снизит ее эффективность. ●

В. Ю. Зубок, Д. В. Ландэ

ТЕЛЕКОМ-ИНФО

Около 1000 сетевых устройств уязвимы к атакам

Недавно Колумбийский университет провел крупное исследование, в рамках которого состоялось глобальное сканирование IP-адресов. Результаты удивили аналитиков: примерно 21 000 роутеров, VoIP-устройств и веб-камер совершенно не защищены от удаленных атак. Любой желающий может получить доступ к их административному интерфейсу, владельцы даже не считают нужным менять стандартные заводские пароли.

Большинство доступных роутеров в Америке от производителя Linksys. Всего в регионе было найдено 2729 аппаратов, 45 % из них были в открытом доступе со стандартным паролем доступа к административному интерфейсу. Следующую позицию по степени незащищенности заняли VoIP-устройства от Polycom: из 585 найденных аппаратов 29 % могут с легкостью подвергнуться атаке.

Последствия несанкционированного доступа к административному интерфейсу сетевого устройства могут быть весьма плачевными. Роутер может быть использован для сетевых атак на другие компьютеры, а VoIP-устройство — перепрошито так, что будет записывать все разговоры и отправлять их прямиком злоумышленнику. На базе незащищенного оборудования может быть создан ботнет, ведь совсем недавно многие роутеры и модемы подверглись серьезной вирусной атаке, и теперь производители оперативно латают дыры в системе защиты своих устройств.

Окончательные результаты исследования таковы: более 300 тысяч сетевых устройств имеют свободный доступ к административному интерфейсу. Несмотря на то, что большинство пользователей все же меняет стандартные пароли, оборудование по-прежнему остается уязвимым для хакеров.

http://itua.info/news/security/23202.html