

7. Тенденции и перспективы

Тенденции

Для чего специалисту нужно иметь представление о текущих тенденциях отрасли ИТ в целом и высокотехнологичной преступности в частности? Для того чтобы не пойти по ложному пути, впервые столкнувшись с чем-то принципиально новым, до того не известным. А новое в нашей отрасли возникает значительно чаще, чем в какой-либо другой. Возьмем, например, кроссплатформенные вирусы. До сего момента известен лишь один образец такого вируса (Sxover), к тому же не получивший распространения. Но появление следующих образцов — лишь вопрос времени. Столкнувшись с труднообъяснимым фактом, специалист или эксперт-криминалист должен вспомнить о такой тенденции и сделать предположение, что появился кроссплатформенный вирус. То есть для раскрытия и расследования компьютерных преступлений наряду с опытом (своим и чужим) специалистам должна помогать также экстраполяция текущих тенденций.

Развитие форензики в 2005–2006 годы характеризовалось следующими тенденциями:

- Выделение технических систем для сбора и хранения цифровых доказательств из систем защиты информации. Всевозможные логи, архивные копии, копии переписки и иных сообщений собираются и хранятся именно с целью расследования будущих возможных инцидентов, а не с целью восстановления на случай утраты (копии для случаев утраты делаются отдельно). Например, в политике безопасности некоторых компаний предусмотрено, что после увольнения любого сотрудника делается полная копия НЖМД его служебного компьютера, которая хранится в течение достаточного времени на случай возможных расследований.

- Дальнейшее совершенствование систем для снятия информации с цифровых каналов связи (CORM), их повсеместное внедрение. Ведущие производители коммуникационного оборудования объявили о внедрении функций «lawful interception» непосредственно в аппаратную часть своего оборудования и во встроенное ПО, чтобы операторы связи, с которых государственные органы требуют наличия таких возможностей, не тратились на отдельное оборудование для перехвата [78].

Пример конфигурации маршрутизатора (Cisco IOS 12.2) для включения доступа к функции перехвата трафика:

```
Router(config)# snmp-server view tapV ciscoTap2MIB included
Router(config)# snmp-server view tapV ciscoIpTapMIB included
```

```
Router(config)# snmp-server view tapV ciscoTap802MIB included
Router(config)# snmp-server view tapV ciscoTapConnectionMIB included
Router(config)# snmp-server group tapGrp v3 noauth read tapV write tapV
notify tapV
Router(config)# snmp-server user ss8user tapGrp v3 auth md5 ss8passwd
Router(config)# snmp-server engineID local 1234
```

- Возникновение компьютерно-криминалистических (или аналогичных) подразделений как в правоохранительных органах, так и в корпоративных службах информационной безопасности. Речь идет не о создании «компьютерной полиции», которая появилась еще в 1990-е, а именно о выделении криминалистических подразделений из состава этой полиции или корпоративных департаментов информационной безопасности. Об отделении задач сбора цифровых следов и задач расследования. Об отделении задач защиты информационных систем и задач по расследованию инцидентов.
- Появление кафедр и иных научных подразделений, специализирующихся на компьютерной криминалистике. То есть эта наука выделилась не только методически, но и организационно.

Теперь разберем долговременные тенденции, относящиеся к рассматриваемой науке.

Понимание и просвещение

Как уже отмечалось выше, для следователей, прокуроров и судей описания преступных действий подозреваемого (обвиняемого) в компьютерном преступлении могут оказаться просто непонятными. Невозможно объяснить, каким именно способом злоумышленник получил несанкционированный доступ к серверу через сеть, не объяснив предварительно, что такое сервер, удаленный доступ и как работает сеть. А объяснить все это невозможно без других знаний из области ИТ. Автор неоднократно сталкивался с ситуацией, когда показания и объяснения эксперта в суде из всех присутствующих понимает только один человек — подсудимый.

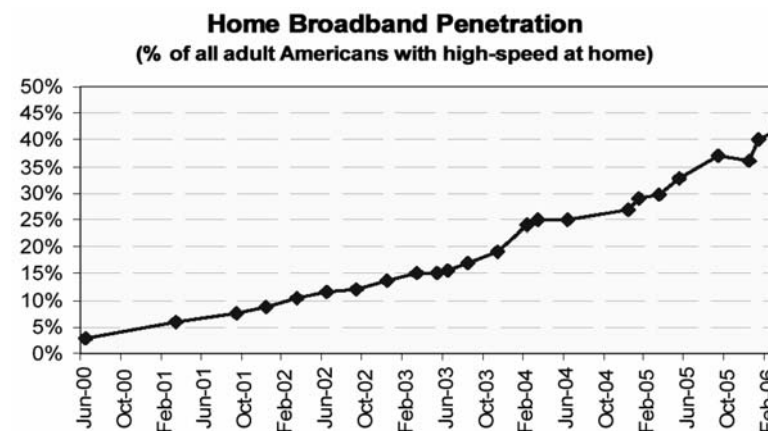
С другой стороны, пользователи и технические специалисты в массе своей остаются непродвинутыми относительно правовых вопросов. В их среде часто бытуют довольно странные представления о законе и законности, которые, похоже, основаны на просмотре голливудских боевиков. Например, системные администраторы часто на полном серьезе утверждают, что «правила использования информационного ресурса определяются владельцем этого ресурса и никем иным».

Таким образом, существует пропасть непонимания между юристами и техническими специалистами. Преодолеть ее при помощи просвещения вряд ли удастся. Повышение так называемой «компьютерной грамотнос-

ти» юристов и объяснение технарям основ законодательства — это, безусловно, дело полезное. Но обе упомянутые области настолько сложны и обширны, что нет никакой надежды совместить профессиональные юридические и профессиональные компьютерные знания для сколь-нибудь значительной группы людей. Специалистов, способных переводить с «технического» на «юридический» и обратно, свободно владеющих обоими языками, довольно мало. Поэтому проблемы с пониманием и с правовой оценкой действий в киберпространстве — останутся.

Широкополосный доступ

Дешевый широкополосный доступ в Интернет для частных (домашних) пользователей начал предоставляться в массовых масштабах в развитых странах в 2000-2001 годах. Чуть позже такой доступ появился в других странах. В России широкополосный доступ для домашних пользователей стал обычным делом в Москве в 2005 году, а в областных центрах он будет введен в 2008-2009 годах. То есть можно сказать, что домашний пользователь на широком канале — это массовое явление, в том числе и в нашей стране.



Процент граждан США, имеющих дома широкополосный доступ в Интернет.
Источник — [79]

Широкополосный доступ выглядит крайне привлекательно, с точки зрения киберпреступников. Домашние пользователи не в состоянии защитить свои компьютеры от внедрения вредоносных программ. В отличие от корпоративных компьютеров, здесь отсутствуют какие-либо дополнительные средства защиты информации — сервера доступа с трансляцией адресов, межсетевые экраны, системы обнаружения атак. Можно быть уверенным, что из нескольких миллионов таких компьютеров нес-

колько десятков тысяч наверняка обладают определенной уязвимостью. Именно на них основываются зомби-сети. Компьютеры с медленным, коммутируемым соединением для зомбирования малополезны.

Распространение широкополосного доступа дало новый толчок технологиям рассылки спама. Если в 2002 году большая часть спама рассылалась через плохо защищенные сервера электронной почты и собственные сервера спамеров, то уже с 2004 года статистика однозначно свидетельствует, что большая часть спама рассылается через затронутые компьютеры на быстрых каналах связи.

Персональные компьютеры, обслуживаемые неквалифицированными пользователями и подключенные к широкополосным линиям связи, будут в дальнейшем только множиться. Значит, на этом ресурсе будут основаны многие технологии злоумышленников — рассылка спама, DoS-атаки, хостинг нелегальных материалов, методы анонимизации, кража персональных данных и т.п.

Поскольку услуги связи постоянно дешевеют, внедряются новые, более производительные технологии и протоколы (например, Wi-Max), а тарифы используются преимущественно безлимитные, то пользователи не очень заинтересованы заботиться о защищенности своих компьютеров. Современные троянские программы не загружают ресурсы компьютера, используют имеющуюся полосу линии связи аккуратно, чтобы как можно дольше не обнаруживать своего присутствия. То есть пользователь зараженного компьютера не испытывает никаких явных неудобств от присутствия троянской программы. Неудобства от этого испытывает весь остальной мир. В аналогичной ситуации находится интернет-провайдер зараженного пользователя: он не несет прямых убытков, когда вредоносные программы функционируют в его сети, однако заинтересован, чтобы в сетях иных провайдеров вредоносных программ не было. Это создает основу для заключения многосторонних соглашений между операторами связи или объединения их под эгидой государства для совместной борьбы, взаимодействия и оказания взаимной помощи.

Подобные альянсы появляются постоянно. Из событий последних двух лет стоит отметить появление объединения операторов «Networks Fingerprint Sharing Alliance» для борьбы с DoS-атаками на основе продукта «Arbor Peakflow» [W26].

Интеллектуальная собственность

Повышение роли интеллектуальной собственности выражается в увеличении доли нематериальных вложений в стоимости почти всех видов продукции. Следовательно, и доходы производителя все больше и больше зависят от стоимости прав интеллектуальной собственности, которые он использует в производстве или которые продает. От величины этой стои-

мости существенным образом зависит стабильность экономики государств, где расположены крупнейшие правообладатели и производители «творческой» продукции. Размер стоимости авторских и патентных прав в товарообороте развитых стран таков, что сильные колебания этой стоимости могут привести к краху экономики. А стоимость интеллектуальной собственности поддерживается соответствующим законодательством и практическими мерами по его исполнению — то есть не рыночным, а административным механизмом. Понятно, что государство придает большое значение поддержанию стоимости нематериальных активов. Установление выгодных правил в области торговли интеллектуальной собственностью — одна из приоритетных задач внешней политики развитых стран.

Тенденция прослеживается достаточно четкая: постепенное увеличение объема полномочий правообладателя, расширение круга ценностей, на которые распространяются права интеллектуальной собственности, удлинение сроков охраны.

В то же время компьютерные технологии сделали необычайно легким отчуждение произведения от его носителя. Копирование и передача объектов интеллектуальной собственности в цифровой форме имеют ничтожную себестоимость и доступны практически всем. Это способствует легкости нарушения прав и затрудняет борьбу с такими нарушениями.

Ожидается продолжение данной тенденции в ближайшие годы.

То есть специалистам в области компьютерных преступлений следует ожидать усиления борьбы с нарушениями авторских прав, патентных прав, прав на товарные знаки и иных прав интеллектуальной собственности на цифровой контент. Наказания за соответствующие нарушения будут ужесточаться. Круг преступных деяний, скорее всего, расширится, поскольку, когда затруднительно пресекать сами нарушения (воспроизведение, например), пытаются запрещать то, что способствует таким нарушениям (например, файлообменные сети). На борьбу именно с правонарушениями в области интеллектуальной собственности надо ожидать наибольших ассигнований со стороны правообладателей и правительств заинтересованных стран.

С другой стороны, неизбежно и усиление реакции на подобные действия со стороны оппозиции, либералов, правозащитников, а также со стороны тех стран, которые являются потребителями и не являются производителями продуктов интеллектуальной собственности. Следует ожидать дальнейшей политизации борьбы с нарушениями авторских прав.

Конвергенция

Важной тенденцией развития отрасли связи является конвергенция различных сервисов и служб. По сетям с коммутацией пакетов (прежде всего — IP-сетям) ныне передаются не только данные, но и голос, видео-

изображение, управляющие сигналы для разнообразного оборудования, другие виды информации. По одному и тому же кабелю, по одному и тому же протоколу сетевого уровня в дом к потребителю подаются различные сервисы: телефонная связь, сигнал телевидения, видео по требованию, управление внешними устройствами и доступ в Интернет. Такая конвергенция упрощает и удешевляет все сервисы, хотя и делает их менее надежными, создавая единую «точку отказа». Впрочем, дублирование каналов эту проблему решает.

Эта тенденция порождает новые угрозы. Захват злоумышленником контроля над каналом передачи данных будет угрожать не только перехватом интернет-трафика, но и голосовой информации потребителя, а также сигналов управления бытовой техникой, охранными системами. То есть расширяется круг компьютерных преступлений.

Перспективы

Направления дальнейшего развития форензики на ближайшие годы видятся автору такими.

Законодательство

На взгляд автора, не стоит ожидать в ближайшие годы внесения таких изменений в законодательство, которые бы установили применение некоторых методов снятия и закрепления цифровых доказательств. С одной стороны, существующих методов, в принципе, достаточно. С другой стороны, степень компьютеризации нашего общества еще слишком незначительна; для существенных изменений нужно подождать смены одного поколения. Кроме того, следует учитывать скорость развития информационных технологий. Никакое законодательство не способно изменяться столь же быстро.

Криминалистическая техника

Что касается программ и аппаратных устройств для снятия информации с разнообразных носителей и ее исследования, то в этой области прорывов ожидать не стоит. Почти все, что можно было автоматизировать, уже автоматизировали. Развитие пойдет лишь по пути учета новых видов носителей и новых форматов данных.

Слежка

Многие считают, что в ближайшие годы будет падать эффективность систем перехвата коммуникаций (COPM, «Carnivore», «Echelon» и др.) вследствие все большей распространенности дешевых систем и протоколов шифрования, встраивания таких систем в различное ПО. Для многих

протоколов появляются их шифрованные версии (модификации, расширения). Широко доступны как описания, так и готовые реализации стойких алгоритмов шифрования, в том числе под свободными лицензиями. Мощность современных компьютеров такова, что шифрование в реальном времени любого разумного объема трафика занимает весьма незначительную часть ресурсов.

Национальное законодательство во многих случаях ограничивает применение шифрования или требует депонировать ключи, но любой пользователь без особого труда приобретает услуги зарубежного провайдера, где ограничения национального законодательства не действуют. Перечисленные факторы подтверждают, что среднему пользователю становится все легче защитить свои коммуникации от перехвата. Следовательно, желающих сделать это становится все больше.

Новые отношения

Как отмечалось в первом разделе книги, технический прогресс способствует возникновению новых видов преступлений двумя основными путями. Во-первых, непосредственно. Вновь появившиеся технические средства и технологии используются злоумышленниками для более эффективного совершения преступлений традиционных видов. Во-вторых, опосредованно. Технический прогресс вызывает прогресс социальный, то есть возникновение принципиально новых видов общественных отношений. Новые отношения означают новые права, которые могут быть нарушены. Таким образом, возникают принципиально новые виды преступлений, которые были раньше не то чтобы неосуществимы, но попросту немислимы.

Среди принципиально новых общественных отношений, которые только что возникли или возникнут в ближайшие годы, следует отметить следующие:

- отношения по поводу прав на доменные имена и, возможно, некоторые другие средства индивидуализации в глобальных сетях;
- отношения по поводу виртуальных предметов, персонажей, недвижимости и иных активов, существующих в виртуальных мирах;
- отношения по поводу рекламных возможностей и иного влияния на людей различных сетевых ресурсов — веб-сайтов, блогов, сетевых сервисов, поисковых систем и т.п.;
- отношения по поводу прав интеллектуальной собственности на результаты работы отдельных программ и комплексов программ, в том числе комплексов независимых друг от друга программ;
- отношения по поводу технических стандартов, форматов и протоколов, которые формально являются добровольными, но фактически обязательны для всех и вследствие этого служат механизмом недобросовестной конкуренции;

- отношения по поводу новых видов использования интеллектуальной собственности.

При возникновении новых общественных отношений первое время они законом не защищаются. Но достаточно быстро общество осознает необходимость защиты новых прав, особенно в тех случаях, когда эти права начинают стоить существенных денег. До принятия новых законов, охраняющих новые права, многие юристы пытаются «натянуть» на них прежние нормативные акты. Иногда это удается, а порой возникают забавные или трагические казусы. Новейшая история показывает, что от момента возникновения нового общественного отношения до момента, когда возникнет более-менее единообразная юридическая практика его защиты, проходит от 5 до 8 лет.

Неолиберализм и неоконсерватизм

В постиндустриальных странах классический либерализм XIX-XX веков почти повсеместно сменен на новую политико-экономическую доктрину, именуемую неолиберализмом [76, 77]. Неолиберализм характеризуется следующими тенденциями:

- сокращение реального влияния государства на общество;
- расширение роли так называемого гражданского общества;
- увеличение числа социальных иерархий;
- дерегуляция рынков, снятие ограничений на концентрацию капитала;
- транснациональное движение капитала, увеличение международного разделения труда;
- размывание понятия государственной и национальной принадлежности (космополитизм), кризис идентичности.

Как видно, Интернет воплощает в себе основные тенденции неолиберализма. Он принципиально трансграничен. Он трудно контролируем со стороны государства. Он почти не нуждается в централизованном управлении. Интернет пришелся как нельзя кстати неолиберальному обществу. И, напротив, для тех государств, которые не успели еще перейти к неолиберализму и задержались на предыдущей стадии развития (так называемые тоталитарные или просто патерналистские государства), наличие Интернета создает проблемы в идеологической сфере.

Неоконсерватизм уравнивает недостатки неолиберализма и компенсирует кризис идентичности, позволяя сохранить единство государства при новом типе общества. Для неоконсерватизма характерны профессионально-культурное объединение, насаждение толерантности, избрание общенационального врага (внешнего и внутреннего), который бы смог идеологически объединить такое космополитичное и мультикультурное общество.

Чем же уравниваются неолиберальные тенденции в Сети? Что является воплощением неоконсерватизма в Интернете?

Во-первых, борьба со «всемирным», то есть общецивилизационным врагом. На замену исчезнувшему социализму были подобраны другие враги — мировой терроризм (внешний), экстремисты (внутренний) и педофилы (внутренний). Для людей, крепко связанных с Интернетом, имеется и еще один объединяющий враг — спамеры.

Ведение борьбы с общими врагами позволяет найти платформу для национального и государственного единения, сублимировать недовольство, загрузить работой многочисленные государственные и общественные учреждения. То есть уравновесить негативные следствия неолиберальной политики.

Противодействие в Сети перечисленным врагам не будет уделом профессионалов, как для других компьютерных преступлений. Террористы, экстремисты, педофилы и спамеры, а также им сочувствующие будут (и уже сейчас являются) общим противником для самых широких кругов общества. Правоохранительные органы, ведя борьбу с соответствующими правонарушениями, будут иметь дело с самой широкой «инициативой снизу», игнорировать которую — себе дороже.

Возрастание роли Интернета

Тенденция, описанная в главе «Конвергенция», обещает нам расширение роли сетей с коммутацией пакетов, прежде всего — сетей на протоколе IP. Как все сервисы переводятся на IP, так и все связанные с ними злоупотребления становятся компьютерными.

В ближайшие годы мы можем, например, столкнуться с квартирной кражей как компьютерным преступлением. Значительная доля систем охранной сигнализации и видеонаблюдения работает на протоколе IP и

осуществляет передачу информации по публичной IP-сети. Соответственно, отключить такую систему или навязать ей ложные данные можно дистанционно, через Интернет, осуществив к ней несанкционированный доступ при помощи компьютера. В случае успешного доступа взломанная система сама сообщит вору, когда хозяев нет дома, в нужный момент разблокирует замки и прекратит видеозапись.



Камера наблюдения «D-Link Securicam Network DCS-G900». Использует беспроводную связь по протоколу Wi-Fi (IEEE 802.11g) как для передачи видеосигнала, так и для управления камерой. Из-за этого злоумышленник получает потенциальную возможность захватить управление камерой, не проникая на охраняемый объект