Две основные угрозы безопасности

Владимир Безмалый

С тех пор как написание вредоносного кода перестало быть уделом небольшого количества талантливых программистов и превратилось в средство зарабатывания денег, темпы развития угроз в отношении систем безопасности предприятий и индивидуальных пользователей значительно ускорились. По данным компании Microsoft, приведенным в докладе руководителя программы информационной безопасности Андрея Бешкова, сделанном на конференции Microsoft SWIT, 39% компьютеров в мире заражены вредоносным кодом, каждый 14-й скачиваемый из Интернета файл содержит вредоносный код, а более миллиона компьютеров взламывается каждый день, то есть один компьютер каждые 14 секунд.

Более того, сегодня написание программ для взлома — это один вид бизнеса, а непосредственное распространение и атаки — задача совершенно других людей. Вот какие сведения о стоимости зловредных программ можно почерпнуть из отчета компании Trend Micro под названием Russian Underground 101 (http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf):

- руткит для Linux стоит 500 долл., для Windows 292 долл.;
- готовый набор Winlocker — 20 долл;
- полиморфный шифровальщик — 100 долл.;
- аренда набора программ использования уязвимостей — 400 долл. в месяц;
- отказоустойчивый хостинг — 20 долл.

Как видите, можно просто заплатить, и инструменты для взлома у вас в руках. Но самое интересное в этом отчете — угрозы типа «0-day», которыми нас так любят пугать. Они составляют всего... 0,12% (!) общего числа угроз. Всего-то! Об остальных уязвимостях уже давно все известно, но тем не менее они существуют и через них идут атаки. По данным отчета Microsoft Security Intelligence Report выпуск 11 (http://www.microsoft.com/security/sir/archive/default.aspx), мы имеем распределение угроз, представленное на рисунке 1.

Большая часть вредоносного кода либо требует явного разрешения на запуск, либо использует уже давно известные изъяны в программном обеспечении. Итак, мы знаем два основных способа распространения угроз, это социальная инженерия и использование изъянов в программном обеспечении.

Социальная инженерия

Статистика атак с использованием методов социальной инженерии, или фишинговых атак, по версии Anti-Phishing World Group (http://apwg.org/apwg-news-center/crimeware-map), по данным отчета за четвертый квартал 2012 года (см. таблицу), говорит о том, что около 30% персональных компьютеров во всем мире были заражены вредоносным программным обеспечением, более 57% компьютеров в Китае были заражены, за исключением октября 2012 года, число фишинговых сайтов уменьшалось каждый месяц с апреля до декабря 2012 года.

На рисунке 2 приведен пример вида фишинговых сайтов. Обратите внимание на выделенный красным адрес домена: видно, что он на одну (!) букву отличается от настоящего.

Первое место в Top10, по данным компании G Data Security Labs, среди самых опасных сайтов занимают тематические порталы о тех-

Таблица. Отчет APWG за IV-й квартал 2012 года

	Октябрь 2012	Ноябрь 2012	Декабрь 2012
Число уникальных фишинговых отчетов, полученных по e-mail от пользователей APWG	25365	24563	28195
Количество уникальных фишинговых веб-сайтов	51232	46002	45628
Число брендов, использованных фишерами	401	430	418
Страны, в которых зарегистрировано большинство фишинговых сайтов	USA	USA	USA
Содержат некоторую часть целевого имени в URL	60,31%	54,23%	53,59%
Нет имени сайта, только IP-адрес	1,63%	1,87%	1,93%
Количество сайтов, не использующих порт 80	0,3%	0,24%	1,04%

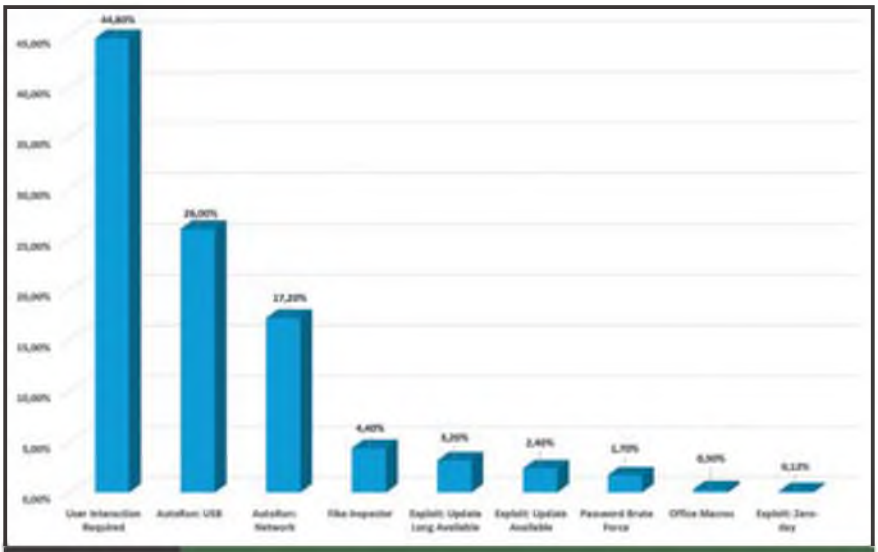

Рисунок 1 Методы распространения вредоносного кода

нологиях и телекоммуникациях (16,2%). В эту категорию входят сайты о компьютерах, технологиях связи, мобильных новинках, о сети Интернет и пр. Самое интересное, что посетители подобных порталов — зачастую люди грамотные в области информационной безопасности, но именно они принимают на себя основную волну интернет-атак. Во вторую группу входят сайты под общим названием «бизнес» (11,3%): бизнес-издания, порталы бизнес-новостей, всевозможные курсы лекций, сайты для повышения эффективности бизнеса. И только третью позицию с долей чуть больше 10% занимают сайты с порнографическим контентом, которые всегда имели дурную репутацию из-за содержания вредоносного кода. Как бы то ни было, исследование, проведенное G Data в прошлом году, выявляет отсутствие какой-либо связи между порнографическим содержимым сайта и возможностью заражения компьютера. Достаточно закономерно, что сайты, связанные с обменом файлов и одноранговым соединением (7,1%), также находятся в первой пятерке. Огромный объем вредоносных файлов распространяется вместе с нелегальным контентом среди любителей нарушать закон об авторском праве. С этой группой напрямую связана и следующая категория опасных сайтов, которая расположилась на шестом месте, — развлечения (5,2%). К ней относятся развлекательные порталы с музыкой, фильмами, видео с концертов, сайты с новостями из мира шоу-бизнеса и сплетнями о знаменитостях.

Категория с блогами (3,7%), занимающая восьмую позицию, включает любые виды журналов: от фото, аудио и киноблогов до стандартных текстовых блоговых площадок. Так как большая часть контента на подобных сайтах формируется самими пользователями, авторам блога будет несложно ввести своих читателей в заблуждение и заманить на опасные страницы. Зачастую блоговые платформы не могут похвастаться хорошим техническим оснащением, которое поможет противостоять злоумышленникам. Это позволяет хакерам внедрять вредоносный контент в явной или незаметной форме и причинять вред читателям блогов. И последние два места разделили сайты о путешествиях (3,5%) и игровые порталы (3,3%).

Но, даже учитывая составленный рейтинг, нельзя сказать, что тема сайта является главным фактором для кибермошенников в вопросе размещения ловушек. Еще больше их интересует количество наивных пользователей, которые посетят сайт, и минимальные затраты на заражение портала. Поэтому безопасность того или иного сайта или сервера напрямую зависит от того, насколько хорошо защищены все его компоненты от всевозможных атак. Например, если существует уязвимое место в системе управления контентом, в подключаемом модуле или программе, это значит, что каждый веб-сервер, оборудованный этими же компонентами, оказывается в зоне риска независимо от наполнения сайта. А как известно, обнаружив одну уязвимость, мошенники начинают осуществлять массовые атаки и рас-

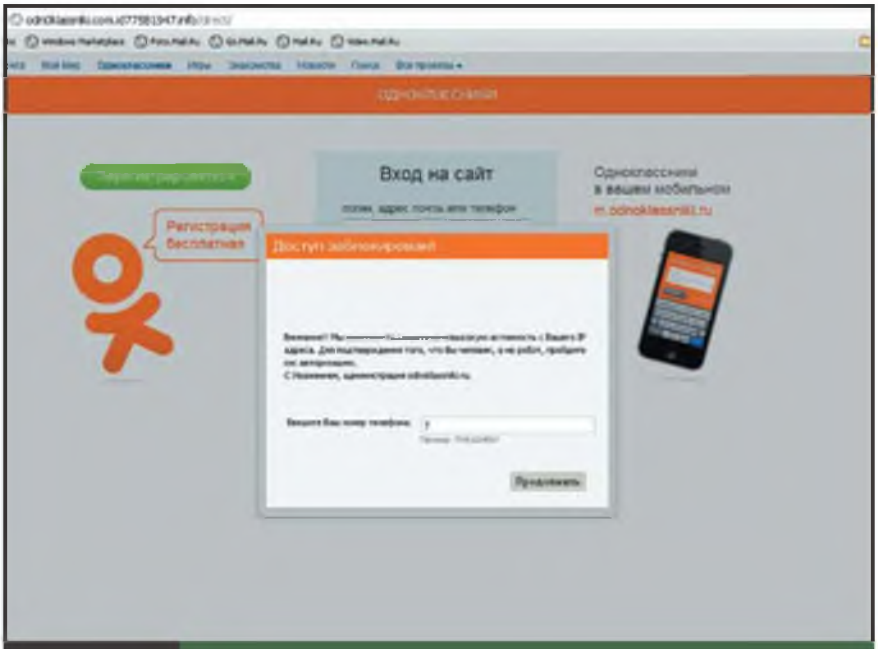

Рисунок 2 Пример фишингового адреса

пространять вредоносные программы, использующие известные слабые места в подобных системах. Соответственно, популярные сайты, привлекающие большое количество пользователей, становятся главной мишенью для злоумышленников.

Как защититься от обмана?

Защитой от данного типа атак может служить технология Smart Screen, встроенная в Internet Explorer, соответствующие фильтры в других браузерах или различные антифишинговые модули. Вот несколько примеров.

- WOT (Web of Trust) — это бесплатная надстройка к браузеру, которая предупреждает пользователя во время поиска информации или совершения покупок о потенциально небезопасных веб-страницах. WOT совместим с такими браузерами, как Internet Explorer, Mozilla Firefox, Opera (в 11-й версии при помощи расширения), Google Chrome и Safari. WOT создан на основе отзывов сообщества пользователей, и уровень доверия к тому или иному сайту зависит от оценок, выставленных предыдущими посетителями. Рейтинги постоянно обновляются миллионами пользователей WOT-сообщества, а также многочисленными проверенными ресурсами (например, списки фишинговых сайтов). Количество русскоязычных активных пользователей WOT составляет 103 тыс. человек. Ссылка на модуль для Internet Explorer http://www.viruslab.ru/download/wot/ie.php. Ссылка на модуль для Firefox http://www.viruslab.ru/download/wot/firefox.php.
- AVG LinkScanner for Windows — бесплатный модуль для Internet Explorer и Firefox. Загрузить его можно по адресу http://www.avg.com/ww-en/linkscanner.
- Panda Cloud Security — бесплатный «облачный» антивирус http://www.cloudantivirus.com/en/#!free-antivirus-download.
- G Data Cloud Security — бесплатный антивирус http://www.free-cloudsecurity.com/ru/. G Data CloudSecurity — это новый бесплатный модуль для самых распространенных браузеров Internet Explorer и Mozilla Firefox. Он эффективно блокирует доступ к известным вредоносным программам и фишинговым веб-сайтам в реальном времени. Его можно использовать вместе с другим защитным программным обеспечением сразу после установки, дополнительные настройки не требуются.

Фильтр SmartScreen в Internet Explorer 9

Начиная с Internet Explorer 8 в состав IE входит фильтр SmartScreen — набор технологий, предназначенный для защиты от возможных интернет-угроз, в том числе с использованием методов социальной инженерии. Базируется SmartScreen на технологии фишингового фильтра и предназначен для защиты пользовательских компьютеров от известных вредоносных сайтов. Кроме того, данный фильтр включает защиту от ClickJacking, технологии, применяемой для перехвата нажатий клавиш, искажения веб-страниц и т. д. По умолчанию он включен.

Фильтр SmartScreen в Internet Explorer 9 использует сразу несколько технологий. В первую очередь происходит сравнение адреса посещаемого сайта со списком известных мошеннических и вредоносных сайтов. Если сайт есть в этом списке, больше проверок не производится. В противном случае он анализируется на предмет наличия признаков, характерных для мошеннических сайтов. Также возможна отправка адреса того сайта, куда пользователь собирается зайти, онлайн-службе Microsoft, которая ищет его в списке фишинговых и вредоносных сайтов. Причем доступ к онлайн-службе производится асинхронно по SSL-соединению, так что это не сказывается на скорости загрузки страниц. Однако обращение к данной службе пользователь может запретить.

Чтобы уменьшить сетевой трафик, на клиентском компьютере хранится зашифрованный DAT-файл со списком наиболее посещаемых узлов; все включенные в этот список сайты не подвергаются проверке фильтром SmartScreen.

Для защиты от фишинга и вредоносных программ фильтр SmartScreen исследует строку URL целиком, а не подмножество адресов URL, на которые заходил пользователь, а значит, службе URL Reputation Service (URS) могут быть переданы личные сведения, поскольку иногда они находятся в самой строке URL. Вместе с тем необходимо добавить, что в состав SmartScreen входит и проверка репутации загружаемых файлов Application Reputation Service (ARS)

При загрузке программы в IE 9 идентификатор файла и издателя приложения (если оно заверено цифровой подписью) отправляются на проверку с помощью новой услуги репутации приложений в «облаке». Если программа имеет репутацию, то предупреждение отсутствует. Если же файл будет загружаться с вредоносного сайта, IE 9 блокирует загрузку, как и IE 8. Однако если файл не имеет данных о репутации, IE покажет это в строке уведомления и менеджере загрузки, что позволит принять обоснованное решение о доверии этому файлу.

Фильтр SmartScreen в Internet Explorer 9 предупреждает пользователя о подозрительных или уже известных мошеннических сайтах. При этом фильтр проводит анализ содержимого соответствующего сайта, а также использует сеть источников данных для определения степени надежности сайта. Фильтр SmartScreen сочетает анализ веб-страниц на стороне клиента на предмет обнаружения подозрительного поведения с онлайн-службой, доступ к которой пользователь разрешает или запрещает. При этом реализуется три способа защиты от мошеннических и вредоносных узлов:

1. Сравнение адреса посещаемого сайта со списком известных сайтов. Если сайт найден в этом списке, больше проверок не производится.

2. Анализ сайта на предмет наличия признаков, характерных для мошеннических сайтов.
3. Отправка адреса сайта, на который пользователь собирается зайти, онлайн-службе Microsoft, которая ищет сайт в списке фишинговых и вредоносных сайтов. При этом доступ к онлайн-службе производится асинхронно по SSL-соединению, так что это не сказывается на скорости загрузки страниц.

Во избежание задержек обращения к URS производятся асинхронно, так что на работе пользователя это не отражается. Чтобы уменьшить сетевой трафик, на клиентском компьютере хранится зашифрованный DAT-файл со списком тысяч наиболее посещаемых узлов; все включенные в этот список узлы не подвергаются проверке фильтром SmartScreen. В фильтре SmartScreen также применяется механизм локального кэширования адресов URL, позволяющий сохранять ранее полученные рейтинги узлов и избежать лишних обращений по сети. Один из способов выявления подставных узлов, применяемый службой URS, — сбор отзывов пользователей о ранее неизвестных узлах. Пользователь может решить, следует ли отправлять информацию об узле, который вызывает у него подозрения.

Для защиты от фишинга и вредоносных программ фильтр SmartScreen исследует строку URL целиком, а не подмножество адресов URL, на которые заходил пользователь. Учтите, что службе URS могут быть переданы личные сведения, поскольку иногда они находятся в самой строке URL.

Фильтр SmartScreen можно включать или отключать избирательно для каждой зоны безопасности, но только в том случае, когда эта функция включена глобально. По умолчанию фильтр SmartScreen включен для всех зон, кроме местной интрасети. Если вы захотите исключить некоторые узлы из списка проверяемых фильтром SmartScreen, но не отключать при этом фильтр полностью, необходимо включить фильтр глобально, а затем отключить фильтрацию только для зоны «Надежные узлы», после чего конкретные узлы добавить в эту зону. Для того чтобы пользователи в организации не могли отключить фильтр SmartScreen, необходимо применить групповую политику.

Угрозы в отношении мобильных устройств

Как полагают специалисты, к 2015 году будет использоваться более 2 млрд мобильных устройств. На сегодня, по данным Virustotal, существует более 5,6 млн образцов вредоносного кода под Android, из которых 1,3 млн подтверждены двумя и более поставщиками антивирусных решений. Уже существует рынок вредоносного кода для мобильных устройств, который предлагает самые разнообразные типы вредоносного программного обеспечения для мобильных устройств: шпионы, фишинговые программы, троянцы, черви, приложения для загрузки вредоносного кода, бот-сети, SMS-атаки, программы для слежения за маршрутами передвижения и привычками владельцев устройств.

Все уязвимости мобильных устройств можно разделить на:

- архитектурные;
- инфраструктурные;
- уязвимости прав доступа;
- программные;
- NFC.

Архитектура. Сегодня смартфоны объединяют в себе все больше различных функций. Это уже не только телефоны, но и средства определения координат и оптимизации маршрутов передвижения и многое другое. А пользователи при этом остались прежними. Они не желают задумываться о проблемах безопасности и легкомысленно разрешают запрашиваемые функции, не интересуясь при этом, зачем, предположим, вашей игрушке функции определения ваших координат или доступ к адресной книге. Пользователь на подобные запросы чаще всего отвечает «Да». И в результате снижает уровень своей безопасности.

Инфраструктурные уязвимости. Атакующие выбирают режим и способ осуществления атаки в зависимости от ее цели. Однако нужно понимать, что могут измениться устройства, операционные системы на них, но останется неизменным ряд функций, например доступ к Интернету по какому-то из интерфейсов — Bluetooth, Wi-Fi, GPRS и т. д.

Уязвимости программного обеспечения. Главной в этом ряду, без сомнения, является задержка в выпуске обновлений программного обеспечения для смартфонов. Сегодня существует огромное количество смартфонов под управлением Android, для которых никогда не будет выпущено обновление операционных систем. Кроме того, не стоит забывать, что очень часто пользователи даже при наличии исправлений для имеющихся версий операционной системы не торопятся устанавливать их. Это может длиться неделями, а иногда и месяцами.

Уязвимости в приложениях. Многие пользователи даже сегодня устанавливают свои приложения из сомнительных источников. Это, в свою очередь, используют злоумышленники.

Пользователи как уязвимость. И производители, и поставщики заинтересованы прежде всего в том, чтобы продать свои устройства и облегчить их использование. В результате пользователь обладает крайне поверхностными знаниями в отношении необходимых правил безопасности. Безусловно, некоторые пользователи могут беспокоиться по поводу конфиденциальности, однако лишь немногие понимают, как это связано с предоставлением разрешения на получение доступа к определенному типу информации. Да и, кроме того, советы пользователям мобильных устройств сегодня найти куда сложнее, чем советы пользователям компьютеров.

Владимир Безмалый (vladb@windowslive.com) — специалист по обеспечению безопасности, имеет звания MVP Consumer Security, Microsoft Security Trusted Advisor