

Шпионское программное обеспечение - защита шлюзов и оконечных устройств от кражи данных

Бурное распространение шпионского ПО вынудило корпорации решать проблемы в области информационной безопасности - от кражи данных и повреждения сетей до потери репутации и возможных судебных исков. В этом докладе рассматривается, как шпионское ПО проникает в организации и воздействует на них, а также описываются меры защиты против такого ПО.

Шпионское программное обеспечение - защита шлюзов и оконечных устройств от кражи данных

Определение шпионского ПО

Шпионское программное обеспечение представляет значительную угрозу для безопасности организаций, так как оно может привести к краже или повреждению конфиденциальной корпоративной информации, а также снижению уровня защиты сетей для последующих вредоносных атак. Такое ПО устанавливается на компьютере пользователя путем тайного проникновения, различных уловок или социального инжиниринга, после чего передает информацию третьей стороне без ведома или разрешения пользователя.

Шпионское ПО существует в различных видах, и хотя в 2006 году количество программ-загрузчиков превысило число других видов шпионского ПО, Sophos предполагает, что это приведет к тому, что еще большее количество шпионского ПО будет установлено на компьютерах ничего не подозревающих пользователей.

Организациям также необходимо решить сопутствующую проблему рекламного ПО, которое доставляет адресную рекламу, например, всплывающие сообщения на компьютеры пользователей, и вызывает их раздражение. Однако, несмотря на то, что рекламное ПО и иные потенциально нежелательные приложения (PUA) могут негативно влиять на продуктивность и эффективность системы, они всё же востребованы некоторыми пользователями. В качестве примера можно привести программы удаленного администрирования, такие как Azrael. Таким образом, несмотря на то, что грань различия между шпионским ПО и рекламным ПО является зачастую размытой, этот доклад отражает угрозы, представленные шпионским ПО.

Растущая угроза

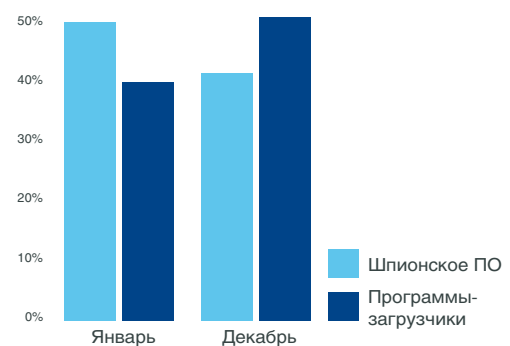


Рис 1. Шпионское ПО и трояны-загрузчики в 2006 году

Проблема шпионского ПО постоянно эволюционирует и сейчас представляет вторую по значимости угрозу для безопасности организаций¹. Хотя темп роста мгновенно опознаваемого шпионского ПО замедлился, возрастающее использование троянских программ-загрузчиков приведет к появлению многосторонних и сложных способов доставки шпионского ПО на компьютеры неискушенных пользователей. На рисунке 1 показано процентное соотношение электронных сообщений, содержащих шпионское ПО, и процентное соотношение электронных сообщений, содержащих ссылки на веб-сайты, с которых загружается шпионское ПО, на начало и конец 2006 года. Рост использования систем мгновенного обмена сообщениями Instant Messaging (IM) и приложений для совместного доступа к файлам Peer-to-Peer (P2P) также добавил потенциальные механизмы доставки для пользователей и распространителей шпионского ПО. Однако, исследование, проведенное Sophos, показывает, что организации уже демонстрируют высокую степень осознания проблемы шпионского ПО.

Подавляющее большинство респондентов интернет-опроса Sophos - 95% - указали, что рассматривают свое антивирусное программное обеспечение как средство защиты также и от шпионского ПО.² Однако по мере роста объема шпионского ПО также растет и его многообразие, причем постоянно появляются новые технологии.

В начале 2006 года супруги Хефрати (Haephraati) – менеджеры фирмы Target-Eya – разработали и продавали троянскую программу, специально предназначенную для частных детективов в целях коммерческого шпионажа.³

Угрозы шпионского ПО включают:

- Программы для кражи паролей и информации - похищают пароли и иную засекреченную личную информацию.
- Клавиатурные шпионы - программы, записывающие нажатия пользователем клавиш с целью кражи информации, например, паролей.
- Банковские троянские программы – отслеживают информацию, вводимую в банковские приложения и в банковские веб-формы.
- Трояны класса «черный ход»- могут выполнять любые из перечисленных функций, включая предоставление хакерам неограниченного доступа к компьютеру, если он работает в онлайн-режиме.
- Черви бот-сетей - создают сеть зараженных компьютеров, которые удаленно конфигурируются для совместной работы с целью выполнения каких-либо из перечисленных функций.
- "Захватчики" браузера - снижают уровень настроек безопасности браузера и/или меняют установки браузера с целью перенаправления пользователя на сайты автоматической загрузки троянских программ.

Угроза шпионского ПО усугубляется свободным доступом к готовым пакетам такого ПО в интернете, предоставляемым всего за 15 долларов США. В 2006 году SophosLabs™ обнаружила российский сайт, на котором потенциальные хакеры могли за небольшую плату приобрести скрипты, упрощающие задачу заражения компьютеров. Такие пакеты ПО являются также привлекательными для тех, у кого не хватает навыков, но имеются злоумышленные намерения.⁴

Как шпионское ПО атакует организации

Шпионское ПО представляет реальную угрозу, которая наносит ущерб деятельности различными способами.

Кража данных

Шпионское ПО может осуществить кражу важной или конфиденциальной информации, например, Troj/BankAsh-A – троян для кражи паролей и одновременно клавиатурный шпион. После установки он начинает передавать информацию при работе компьютера в онлайн-режиме. Этот тип шпионского ПО может также похищать финансовые данные, электронные таблицы, персональные данные, номера банковских счетов, пароли и любую иную информацию, набираемую на клавиатуре компьютера. Более 33% всех угроз, проанализированных SophosLabs, ориентированы на кражу информации, при этом 16% обладает функцией клавиатурного шпиона. Кража данных может привести к ухудшению репутации, потере денежных средств или снижению конкурентоспособности, а также к повышенному риску судебного преследования.

Взлом

Наряду с кражей данных, шпионское ПО может сделать компьютеры компании уязвимыми к шпионажу со стороны хакеров - более 40% всех угроз, выявленных компанией Sophos, предоставляют посторонним лицам доступ к зараженной системе. Троянцы типа «черный ход», такие как Troj/Feutel-L, позволяют хакерам получить контроль над компьютером и похитить любую хранящуюся в нем информацию. Для администратора информационных систем такой тип нападения потенциально более опасен, чем вирус, так как предугадать поведение хакера, получившего доступ к системе, невозможно.

Атака зомби

Шпионское ПО, такое как черви бот-сетей, может быть эффективным инструментом спамера. Если использовать червя или троянскую программу, такую как Mytob, являющуюся семейством наиболее распространенных угроз 2006 года из выявленных компанией Sophos, спамеры могут захватить управление уязвимым компьютером или веб-сервером и заставить его высылать письма по их указанию. Таким образом спам-письма будут высылаться как бы от легального источника. Захваченный компьютер может использоваться и для других преступных целей, таких как участие в атаке типа "отказ в обслуживании" (DoS). В ходе такой атаки тысячи компьютеров одновременно запрашивают доступ к веб-сайту, что приводит к его отказу. Захваченные компьютеры, связанные с другими такими же зараженными ПК, называются бот-сетью или сетью "зомби".

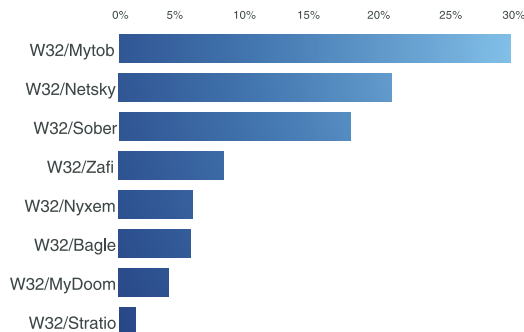


Рисунок 2. Семейство Mytob, создающее зомби-сети, возглавляет список наиболее распространенных угроз 2006 г.

По оценкам компании Sophos, свыше 60% спама рассылается с компьютеров-зомби. Хотя чаще всего риску подвергаются частные лица, эта проблема касается и корпоративных сетей. В начале 2006 г. житель Калифорнии был оштрафован за запуск атаки зомби, в результате которой были заражены 150 компьютеров Northwest Hospital и медицинского центра в Сиэтле, США.⁵

В мае 2006 г. в Южной Корее, которая занимает третье место в мире по объему рассылаемого спама (информация SophosLabs⁶), власти арестовали лицо, подозреваемое в организации работы сети из 16000 компьютеров-зомби, посылавших 18 миллионов спамерских писем в 133 страны ежедневно.⁷

Ущерб сети

В результате атак шпионского ПО может снижаться производительность сети, поскольку такое программное обеспечение создает дополнительную нагрузку. Для предприятия это может означать перерывы в работе и снижение производительности в течение срока, когда вредоносное ПО не было обнаружено, а также расход дополнительных ресурсов на поиск и решение проблемы.

Как устанавливается шпионское программное обеспечение

Шпионское ПО может быть установлено с помощью вируса или при нажатии пользователем веб-ссылки, или при открытии им приложения к сообщению электронной почты. Как упоминалось выше, расширенное использование технологий Web 2.0, таких как IM, предоставило авторам шпионского ПО дополнительные средства для переноса вложений с вредоносным содержанием. Для установки шпионской программы на компьютер в большинстве случаев требуется действие пользователя, например, загрузка полезной и желательной программы (например, P2P-программы обмена файлами между компьютерами), которая может содержать шпионское ПО. Пользователи также могут быть введены в заблуждение всплывающими сообщениями, которые настойчиво побуждают их загрузить "необходимую" программную утилиту. Для установки шпионского кода могут также использоваться уязвимости в ПО, например, в некоторых веб-браузерах. Иногда пользователю достаточно посетить определенный веб-сайт или просмотреть электронное сообщение в формате HTML, чтобы шпионское ПО установилось на его компьютер. Этот тип скрытой установки называется "Drive-by Download" (заставить загрузить).

Защита от шпионского ПО

Основные меры

Аналогично действиям при отражении любых других угроз безопасности, организация должна предпринимать меры для защиты от шпионского ПО как эффективную комбинацию следующего:

- Обучение - обеспечение понимания всеми пользователями необходимости быть осторожными при открытии вложений в электронные письма, загрузке и установке программного обеспечения.
- Политика - реализация жесткой единой политики компании в области использования интернета, позволяющей исключить несанкционированную загрузку ПО, и использование системы паролей, исключая несанкционированный доступ к рабочим станциям.
- Безопасность - установка новейших исправлений браузеров и операционных систем, обеспечение правильной настройки параметров безопасности, а также использование современных систем защиты от угроз на уровне шлюза и на уровне оконечных устройств.
- Контроль - обеспечение интеграции средств контроля за такими приложениями, как IM, VoIP (интернет-протокол голосовой связи) и P2P-обмен данными между компьютерами в существующую инфраструктуру управления и обнаружения вредоносного ПО.

Безопасность и управление

Кроме этих основных мер, предприятия должны использовать единое решение для обеспечения безопасности, защищающее как оконечные устройства, так и шлюзы. Так же, как и в отношении мер защиты от вирусов, троянских программ, фишинговых атак, атак зомби и спама организациям необходимо исключить нарушение политик, использование несанкционированных приложений и несанкционированный доступ к сети, и управлять всё более сложными угрозами в целом, а не как отдельными проблемами.

Резюмируя, компании должны использовать упреждающий (проактивный) подход к защите от шпионского ПО; для этого необходимо сочетать меры по обучению пользователей, реализацию политик и технологических решений. Решение от надежного изготовителя, обеспечивающее одновременно безопасность и средства контроля, - это ключевой элемент победы над угрозами, исходящими от шпионского ПО и связанными с ним приложениями. ◆

Решение Sophos

Sophos обеспечивает эффективную защиту от шпионского ПО на всех уровнях – от шлюза до оконечных устройств.

Sophos Web Security Appliance блокирует шпионское, вредоносное и нежелательное ПО на шлюзе и обеспечивает полный контроль доступа к интернету для безопасного и эффективного просмотра веб-ресурсов.

Решение **Sophos Email Security Appliances** защищает шлюз электронной почты от внутренних и внешних угроз, являясь мощным и доступным средством защиты от шпионского ПО, вирусов, спама и фишинга.

Sophos PureMessage® уникальным образом интегрирует средства защиты от шпионского ПО, вирусов, спама и соблюдения правил политик с целью защиты шлюза электронной почты.

Sophos Endpoint Security обеспечивает целостную защиту от шпионского и рекламного ПО, вирусов, нежелательных приложений и действий хакеров, а также от использования несанкционированных приложений.

Sophos NAC блокирует несанкционированных пользователей, контролирует доступ гостей пользователей и обеспечивает соблюдение требований политик легальными пользователями так, что администраторам известно, кто и что подключается к сети.

Sophos ZombieAlert™ - эта служба немедленно предупреждает организации о спаме, отправляемом из их сетей в результате заражения их компьютеров шпионским ПО.

Больше информации о продукции Sophos содержится на сайте www.DialogNauka.ru компании «ДиалогНаука», которая является платиновым партнером Sophos в России.

Источники

- 1 Обновленный прогноз развития глобального безопасного управления информационным контентом на 2005-2009 гг. и доли вендоров в 2004 г.: шпионское ПО, спам и вредоносный код продолжают свое разрушающее действие. Отчет IDC. Сентябрь 2005 г.
- 2 95% пользователей считают, что антивирусные пакеты программ должны также защищать от шпионского ПО, Sophos.
<http://www.dialognauka.ru/main.phtml?/press-center/security&newser=0000001123490442.txt&arh=1&start=261>
- 3 Супружеской паре предъявлено формальное обвинение в распространении шпионского ПО - троянской программы – для целей промышленного шпионажа, Sophos.
<http://www.dialognauka.ru/main.phtml?/press-center/security&newser=0000001142586475.txt&arh=1&start=131>
- 4 В сети Интернет за 15 долларов продается комплект шпионского ПО, Sophos.
<http://www.dialognauka.ru/main.phtml?/press-center/security&newser=0000001143725848.txt&arh=1&start=131>
- 5 Мужчину обвинили в зомби-атаке на компьютеры больницы, после чего её компьютеры отключились, Sophos. <http://www.dialognauka.ru/main.phtml?/press-center/security&newser=0000001140020939.txt&arh=1&start=151>
- 6 Отчет об угрозах безопасности 2007 г., Sophos.
<http://www.dialognauka.ru/main.phtml?/press-center/security&newser=0000001174051938.txt>
- 7 Подозреваемый «король зомби», возможно, рассылал 18 миллионов писем спама в день, Sophos.
<http://www.dialognauka.ru/main.phtml?/press-center/security&newser=0000001149000603.txt&arh=1&start=101>



Продукты Sophos:
100% обнаружение
шпионского ПО

О компании Sophos

Sophos является мировым лидером по безопасности и контролю в области информационных технологий. Предлагает предприятиям, учреждениям образования и органам государственного управления средства для полной защиты и контроля. Эти средства обеспечивают защиту от известных и неизвестных видов вредоносного и шпионского ПО, несанкционированного доступа, нежелательных приложений, спама, нарушения требований политик и обеспечивает комплексный контроль за сетевым доступом. Надежно спроектированные и легкие в эксплуатации продукты Sophos защищают свыше 150 миллионов пользователей в более чем 150 странах. Компания имеет 20-летний опыт работы и глобальную сеть центров анализа угроз, что обеспечивает быстрое реагирование на новые угрозы и высший в отрасли уровень удовлетворенности клиентов. Sophos работает во всем мире; головные офисы компании расположены в г. Бостон, США, и г. Оксфорд, Великобритания.

Бостон, США • Майнц, Германия • Милан, Италия • Оксфорд, Великобритания • Париж, Франция
Сингапур • Сидней, Австралия • Ванкувер, Канада • Йокогама, Япония

© Copyright 2007. Sophos Plc.

Компания Sophos признает и принимает все зарегистрированные торговые марки и авторские права.

Запрещается воспроизводить, хранить в системе поиска информации или передавать любую часть этого документа любым способом или на любом носителе без предварительного письменного разрешения издателей.

SOPHOS
WWW.SOPHOS.COM