Муниципальное бюджетное общеобразовательное учреждение средняя общеобразовательная школа №3.

Конференция на тему:

«Распространение вирусного ПО через «сайты»

Выполнила:

Ученица 11А класса

Ильина Ольга

Учитель:

Казанина М.В

г.Павлово 2015

План:

Киберпреступность: тенденции и развитие.

За последние несколько лет интернет стал опасным местом. Изначально созданный для сравнительно небольшого количества пользователей, он значительно превзошел ожидания своих создателей. Сегодня в мире насчитывается более 1,5 миллиардов интернет-пользователей и их число постоянно растет по мере того, как технология становится все более доступной.

Преступники тоже заметили эту тенденцию и очень быстро поняли, что совершение преступлений с помощью интернета (теперь это получило название киберпреступления) имеет ряд существенных преимуществ.

Во-первых, киберпреступность не связана с большим риском: поскольку она не имеет геополитических барьеров, правоохранительным органам трудно ловить преступников. Более того, проведение международных расследований и ведение судебных дел стоит больших денег, поэтому такие действия, как правило, предпринимаются только в особых случаях. Во-вторых, киберпреступность – это просто: в интернете предлагается огромное количество «инструкций» по взлому компьютеров и написанию вирусов, при этом каких-либо специальных знаний и опыта не требуется. Вот два основных фактора, превратившие киберпреступность в индустрию, обороты которой исчисляются многими миллиардами долларов и которая представляет собой действительно замкнутую экосистему.

И компании, занимающиеся защитой информации, и производители программного обеспечения ведут постоянную борьбу с киберпреступностью. Их цель – обеспечить интернет-пользователям надежную защиту и создать безопасное программное обеспечение. Злоумышленники в свою очередь постоянно меняют тактику для того, чтобы противодействовать принимаемым контрмерам, что в результате привело к появлению двух выраженных тенденций.

Во-первых, размещение вредоносных программ происходит с использованием zero-day уязвимостей, т.е. уязвимостей, для которых еще не созданы патчи. С помощью таких уязвимостей могут быть заражены даже такие компьютерные системы, на которых установлены все последние обновления, но при этом нет специальных защитных решений. Zero-day уязвимости – ценный товар (их использование потенциально может привести к серьезным последствиям), он продается на черном рынке за десятки тысяч долларов.

Во-вторых, мы наблюдаем резкое увеличение количества вредоносных программ, созданных специально для кражи конфиденциальной информации с целью ее дальнейшей продажи на черном рынке: номеров кредитных карт, банковских реквизитов, паролей доступа на такие сайты, как eBay или PayPal, и даже паролей к онлайн-играм, например, к WORLD OF WARCRAFT.

Одной из очевидных причин такого размаха киберпреступности является ее прибыльность, которая всегда будет являться двигателем в создании новых киберпреступных технологий.

Помимо разработок, которые проводятся для нужд киберпреступников, отметим еще одну тенденцию – распространение вредоносных программ через Всемирную Паутину.

После эпидемий начала нынешнего десятилетия, вызванных такими почтовыми червями, как Melissa, многие компании – производители систем информационной защиты сосредоточили свои усилия на разработке решений, которые могли бы нейтрализовать вредоносные вложения. Иногда это приводило к тому, что в сообщениях удалялись все исполняемые вложения.

Однако последнее время основным источником распространения вредоносных программ стала Сеть. Вредоносные программы размещают на веб-сайтах, а затем либо пользователей обманным путем заставляют вручную запускать их, либо эти программы с помощью эксплойтов автоматически исполняются на зараженных компьютерах.

Мы в «Лаборатории Касперского» с растущей тревогой наблюдаем за происходящим.

Способы заражения и методы распространения.

В настоящее время существует три основных способа заражения сайтов вредоносными программами.

Первый популярный метод – использование уязвимостей самого веб-сайта. Например, внедрение SQL-кода, что позволяет добавить на страницы сайта вредоносный код. Инструменты атаки, такие как троянец ASPXor, наглядно демонстрируют механизм работы этого метода: их можно использовать для массового сканирования и внедрения вредоносного кода по тысячам IP-адресов одновременно. Следы таких атак часто можно видеть в журналах доступа веб-серверов.

Второй метод предполагает заражение компьютера разработчика веб-сайтов вредоносной программой, которая отслеживает создание и загрузку HTML-файлов, а затем внедряет в эти файлы вредоносный код.

Наконец, еще один метод – это заражение троянцем, ворующим пароли (таким как Ransom.Win32.Agent.ey) компьютера разработчика веб-сайтов или другого человека с доступом к учетной записи хостинга. Такой троянец обычно обращается к серверу по HTTP, чтобы передать пароли к учетным записям FTP, которые он собирает из популярных ftp-клиентов, таких как FileZilla и CuteFtp. Компонент вредоносной программы, находящийся на сервере, записывает полученную информацию в базу данных SQL. Затем специальная программа, также находящаяся на сервере, выполняет процедуру входа во все учетные записи FTP, извлекает индексную страницу, добавляет туда код, зараженный троянцем, и загружает страницу обратно.

Поскольку в последнем случае данные учетной записи у хостинг-провайдера становятся известны злоумышленникам, то часто происходят повторные заражения сайтов: разработчики веб-страниц замечают заражение сами или узнают о нем от посетителей сайта, очищают страницу от вредоносного кода, а на следующий день страница вновь оказывается зараженной.

Ниже приводится последовательность действий, которые необходимо совершить в случае, если веб-сайт заражен вредоносным кодом:

- Установить, кто имеет доступ на хостинг-сервер. Запустить проверку их компьютеров программой интернет-безопасности с актуальной базой данных. Удалить все обнаруженные вредоносные программы
- Установить новый надежный хостинг-пароль. Надежный пароль должен состоять из символов, цифр и спецсимволов, чтобы усложнить его подбор
- Заменить все зараженные файлы чистыми копиями
- Найти все резервные копии, которые могут содержать зараженные файлы, и вылечить их

Наш опыт показывает, что зараженные веб-сайты после лечения нередко подвергаются повторному заражению. С другой стороны, обычно это происходит лишь один раз: если после первого заражения веб-мастер может ограничиться относительно поверхностными действиями, в случае повторного заражения он обычно принимает более серьезные меры по обеспечению безопасности сайта.

Эволюция: размещение вредоносных программ на «чистых» веб-сайтах

Пару лет назад, когда киберпреступники стали активно использовать web для размещения вредоносных программ, они как правило действовали через так называемый абузоустойчивый хостинг или через хостинг, где они расплачивались краденными кредитными картами. Заметив эту тенденцию, компании, работающие в области интернет-безопасности, объединили свои усилия в борьбе против недобросовестных хостинг-провайдеров, допускающих размещение вредоносных ресурсов (таких, как американский хостинг-провайдер **McColo** и эстонский провайдер **EstDomains**. И хотя сегодня еще встречаются случаи, когда вредоносные программы размещаются именно на вредоносных сайтах, расположенных, например, в Китае, где закрыть сайт по-прежнему сложно, произошел важный поворот в сторону размещения вредоносных программ на «чистых» и вполне заслуживающих доверия доменах.

Действие и противодействие

Как мы уже говорили, одним из важнейших аспектов постоянной борьбы между киберпреступниками и производителями антивирусных решений является умение быстро реагировать на то, что делает противник. Обе стороны постоянно меняют тактику борьбы и вводят в строй новые технологии, стараясь противодействовать противнику.

Большинство веб-браузеров (Firefox 3.5, Chrome 2.0 и Internet Explorer 8.0) теперь имеют встроенную защиту в виде URL-фильтра. Этот фильтр не позволяет пользователю заходить на вредоносные сайты, содержащие эксплойты для известных или неизвестных уязвимостей, а также использующие методы социальной инженерии для кражи личных данных.

Например, Firefox и Chrome используют Google Safe Browsing API, бесплатный сервис от Google для фильтрации URL-адресов. В момент написания список Google Safe Browsing API содержал около 300 000 адресов известных вредоносных веб-сайтов и более 20 000 адресов веб-сайтов, занимающихся фишингом.

Google Safe Browsing API придерживается рационального подхода к фильтрации URL-адресов: вместо того чтобы отсылать каждый URL-адрес на внешний ресурс для проверки,

как это делает фишинг-фильтр в Internet Explorer 8, Google Safe Browsing проверяет URL-адреса по их контрольным суммам, вычисленным по алгоритму MD5. Чтобы такой метод фильтрации был эффективным, список контрольных сумм вредоносных адресов должен регулярно обновляться; обновления рекомендуется выполнять каждые 30 минут. Недостаток этого метода заключается в следующем: количество вредоносных веб-сайтов больше, чем количество входов в списке. Для оптимизации размера списка (сейчас он составляет около 12 МБ), туда попадают только наиболее часто встречающиеся вредоносные сайты. Это означает, что даже если вы используете приложения, поддерживающие подобные технологии, ваш компьютер по-прежнему подвергается риску заражения при посещении вредоносных сайтов, не попавших в список. В общем и целом широкое применение технологий для безопасной навигации показывает, что разработчики веб-браузеров обратили внимание на новую тенденцию распространения зловредных программ через веб-сайты и предпринимают ответные действия. По сути, веб-браузеры со встроенной защитой уже становятся нормой.

Заключение.

За последние три года резко увеличилось число легитимных веб-сайтов, зараженных вредоносными программами. Сегодня количество зараженных сайтов в интернете в сто раз больше, чем три года назад. Часто посещаемые сайты привлекательны для киберпреступников, поскольку с их помощью за короткое время можно заразить большое количество компьютеров.

Веб-мастерам можно предложить несколько простых советов по поводу того, как обезопасить веб-сайты:

- Защищайте учетные записи хостинга надежными паролями
- Для загрузки файлов на серверы используйте протоколы SCP/SSH/SFTP вместо FTP – таким образом вы защититесь от пересылки паролей по интернету открытым текстом
- Установите антивирусный продукт и запустите проверку компьютера
- Имейте в запасе несколько резервных копий сайта, чтобы иметь возможность восстановить его в случае заражения.

При навигации в интернете есть несколько факторов, увеличивающих риск заражения вредоносным кодом с веб-сайта: использование пиратского ПО, игнорирование обновлений, закрывающих уязвимости в используемом ПО, отсутствие на компьютере антивирусного решения и общее незнание или неполное понимание угроз в интернете.

Пиратские программы играют значительную роль в распространении вредоносных программ. Пиратские копии Microsoft Windows, как правило, не поддерживают автоматические обновления, выпускаемые компанией Microsoft,что дает киберпреступникам возможность эксплуатировать незакрытые уязвимости в этих продуктах.

Кроме того, старые версии Internet Explorer, по-прежнему самого популярного браузера, имеют большое количество уязвимостей. В большинстве случаев Internet Explorer 6.0 без установленных обновлений незащищен от вредоносного воздействия любого

вредоносного веб-сайта. В силу этого, крайне важно избегать использования пиратского ПО, особенно пиратских копий Windows.

Еще один фактор риска – работа на компьютере без установленной антивирусной программы. Даже если в самой системе установлены последние обновления, в нее может проникнуть вредоносный код через zero-day уязвимости в стороннем ПО. Обновления антивирусных программ обычно выпускаются гораздо чаще, чем патчи к программным продуктам, и обеспечивают безопасность системы в период, когда к уязвимостям в стороннем ПО еще не выпущены исправления.

И хотя для поддержания необходимого уровня безопасности важна установка обновлений для программ, немаловажную роль играет и человеческий фактор. Например, пользователь может захотеть посмотреть «интересный видеоролик», загруженный из Сети, не подозревая, что вместо ролика ему подкинули вредоносную программу. Такая уловка нередко используется на вредоносных сайтах в случае, если эксплойтам не удается проникнуть в операционную систему. Этот пример показывает, почему пользователи должны знать, какую опасность представляют интернет-угрозы, особенно те, которые связаны с социальными сетями (Web 2.0), последнее время активно атакуемыми киберпреступниками.

Итак, вот краткие рекомендации по безопасности в интернете:

- Не загружайте пиратские программы
- Вовремя обновляйте все ПО: операционную систему, веб-браузеры, программы для просмотра PDF-файлов, плееры и т.д.
- Установите и всегда используйте антивирусный продукт, такой как Kaspersky Internet SECURITY 2010
- Возьмите за правило, чтобы ваши сотрудники каждый месяц уделяли несколько часов изучению веб-сайтов, посвященных безопасности, таких как www.viruslist.com, где они смогут узнать об интернет-угрозах и методах защиты.

Наконец, помните: предупредить заражение легче, чем вылечить. Принимайте меры безопасности!

Список литературы:

1. http://all-fantivirus.narod.ru/articles/05/virus_expansion.html