Смотри, что исполняешь!

Николай Петров, *заместитель генерального директора АО "ДиалогНаука", CISSP*

Современные банки становятся все более информационными, они предлагают своим клиентам все больше удобных сервисов, позволяющих управлять своими деньгами с помощью компьютеров, планшетов или даже мобильных телефонов. В результате финансовое состояние пользователей этих сервисов оказалось зависимым от безопасности их клиентских устройств.

Часто именно клиентские устройства оказываются тем самым слабым звеном, которое приводит к финансовым потерям. Причем банки этот риск стараются по максимуму переложить на плечи клиентов: дескать, те сами должны заботиться о безопасности своих денег.

К сожалению, антивирусы не всегда могут обнаружить современные вредоносные программы. Дело в том, что антивирусы защищают только от наиболее массовых нападений, которые они знают по уже случившимся инцидентам. Однако первые жертвы всегда страдают, хотя и обеспечивают остальных сигнатурами вредоносных файлов. Кроме того, разработчики вредоносного ПО для банков делают его с учетом установленных антивирусных продуктов и стараются защитить свои приложения от обнаружения, например выключая сканирующий модуль антивируса или постоянно видоизменяя собственные программы. В результате клиенты обнаруживают троянца, когда становится слишком поздно – деньги уже утекли.

Белые списки

Сейчас активно развиваются технологии анализа не файлов (именно так поступает антивирус), а поведения программ. Можно, например, воспользоваться принципом защиты, который формулируется как "запрещено все, что явно не разрешено", он называется белым списком. Сама защита будет работать так: на устройствах, где работает банк-клиент, могут быть запущены только разрешенные приложения из белого списка. Все посторонние программы будут заблокированы и удалены с компьютера. Например, такой продукт под названием Lumension Application Control предлагает компания Lumension.

Пользоваться технологией белых списков очень неудобно – ее сложно администрировать и она часто мешает выполнять, казалось бы, простые задачи, что и приводит в конце концов к ее отключению. Но даже если белые списки удалось настроить и они никому не мешают исполнять служебные обязанности, они практически не модернизируются со временем, и в результате злоумышленники придумывают, как их можно обойти, например став модулем уже установленного и доверенного приложения. Так случилось с вирусом-шифровальщиком Petya, который был загружен на корпоративные компьютеры с очередным обновлением продукта компании M.E.Doc – приложение явно значилось в белых списках. Тем не менее белый список решает достаточно много проблем защиты от вредоносных программ, но он должен сочетаться с другими, более гибкими средствами анализа поведения.

Аномалия и блокировка

Есть второе направление развития защиты – выявление аномального поведения программ и его блокировка. Такие технологии, например, используются в продукте Fireeye HX, который как раз и позволяет выявить опасное поведение установленных на компьютере программ или библиотек, чтобы обнаружить и предотвратить исполнение вредоносных файлов. Блокировка подозрительной активности приложений позволяет защититься от неизвестных программ и даже модулей к известным приложениям. Например, если модуль операционной системы, отвечающий за обработку SMB-запросов, вдруг начинает шифровать диск, то это вызовет сильные подозрения у данного средства защиты и оно заблокирует такие действия.

К преимуществу таких технологий можно отнести то, что они могут обнаруживать и даже блокировать неизвестные угрозы. Однако проблемой таких решений являются ложные срабатывания, когда вполне легитимные программы вдруг вызывают ответную реакцию защиты. Естественно, у администраторов возникает желание ее немедленно отключить. Минимизация ложных срабатываний организуется в таких системах за счет дополнительного применения технологий сигнатурного поиска вредоносного кода. Так, например, в FireEye HX дополнительно применяется поиск по так называемым индикаторам компрометации IoC (Indicator of Compromise), описывающим набор признаков, по которым можно обнаружить атаку злоумышленника. Так что именно сочетание различных методов контроля приложений дает лучший эффект, чем их отдельное использование.

В заключение хотелось бы напомнить, что безопасность денег клиентов на банковских картах действительно находится в их руках. Лучше использовать несколько средств защиты, сочетающихся между собой, и следовать жестким правилам их эксплуатации, чем потерять деньги из-за действий вредоносной программы. Конечно, стопроцентной защиты нет, но защищаться нужно. ●

NM ●
АДРЕСА И ТЕЛЕФОНЫ АО "ДИАЛОГНАУКА"
см. стр. 56