СКРЫТЫЕ ИНФОРМАЦИОННЫЕ УГРОЗЫ

© 2014 г. В.В. ШЕПЕЛЕВ

Московский государственный технический университет радиотехники,
электроники и автоматики

Введение

Большинство современных систем безопасности, по сути, занимаются поиском сигнатур и моделей поведений уже знакомых угроз. И в случае новых атак они окажутся бессильны до тех пор, пока не появятся сигнатуры или патчи от производителя. Чаще всего новые атаки предназначены для скрытного проникновения, и как правило не приносят заметного ущерба.

Алгоритм проникновения

Распространенный случай, когда в крупной организации сотруднику может прийти электронное письмо, содержащее направленную угрозу (фишинг), в виде прикрепленного файла или архива. Чаще всего используют наиболее уязвимое корпоративное приложение и файлы его форматов, например Adobe Reader (pdf)[1]. Как только пользователь открывает или просматривает файл, то запускается процесс. Происходит переполнение буфера приложения открывшего файл, после чего получает права локального администратора, после запуска соответствующей команды. Затем код производит связь с управляющим сервером. Благодаря этому злоумышленник получает информацию об используемой операционной системе и о установленном программном обеспечении. Получив эту информацию, происходит загрузка кода с удаленного сервера, обычно в зашифрованном виде и замаскированным под файл с расширением jpg, чтобы избежать удаления (во многих компаниях корпоративная политика запрещает загрузку.exe файлов). Попав в систему, происходит запуск файла, после чего он начинает сбор данных: логины, пароли, личные данные и.т.д. после чего отправляет по определенному адресу. В завершение происходит дальнейшее распространение кода по другим системам с помощью уже полученных данных. Чаще всего происходит повторная рассылка от имени жертвы по всем адресам.

Защита

Обнаружить такие угрозы не просто, но возможно чаще всего требуется сторонние средства. Например, статистический и динамический анализ всех вложений и документов.

Статистический анализ заключается в проверке специальным ПО на наличие сигнатур.

В случае, если среди объектов не было обнаружено угроз, то происходит дополнительная проверка при помощи:

- эвристического анализа;
- проверке YARA и SNORT(инструменты позволяющие определить и классифицировать угрозу)[2,3] правилам;
- проверка на наличие цифровой подписи документа.

Если после проверки возникло подозрение, то производится динамический анализ–происходит эмуляция пользовательской среды, который моделирует наличие вир-

туальной машины с предустановленными приложениями. После чего происходит мониторинг за поведением исследуемого объекта. По завершению принимается решение, является ли объект вредоносным, если да, то ПО блокирует его, если нет – предоставляет для пользования.

Заключение

Несмотря на то, что производители ПО стараются повышать безопасность своей продукции, нельзя забывать о существующих угрозах. Для снижения риска нежелательных атак требуется специализированное ПО, которое может выявлять скрытые угрозы. Порой простая внимательность при проверке электронной почты или переходе по вложенным ссылкам поможет избежать риска проникновения и получения доступа к конфиденциальной информации.

СПИСОК ЛИТЕРАТУРЫ

1. Secureview Magazine 2010-2014 Kaspersky Lab ZAO // http://secureviewmag.com
2. http://plusvic.github.io/yara/
3. http://www.snort.org/
4. Engineering and Technology Magazine vol 8. Issue 8 // http://eandt.theiet.org/magazine/ /2013/08/bodies-of-evidence.cfm