Итоги 2014: угрозы и эксплуатация Windows

В прошлой версии нашего отчета мы указывали, что появляющиеся в киберпространстве вредоносные программы можно условно разделить на два вида. Первые разрабатываются злоумышленниками для проведения т. н. state-sponsored кибератак и могут представлять из себя технически очень сложное вредоносное ПО. К другому виду принадлежат вредоносные программы, разрабатываемые обычным злоумышленниками. Последние также могут иметь технически сложный программный код.

В том же отчете мы упоминали о значительном росте вредоносного ПО для всех распространенных на сегодняшний день ОС. То же самое мы наблюдали и в прошлом году. Это касается не только Windows или Linux, но также OS X и Android. Несколько вредоносных программ было обнаружено и для iOS, но они затрагиваются устройства с jailbreak. Такие мобильные ОС как Windows RT 8.1 (Windows ARM) & Windows Phone 8.1 по сути все еще остаются без внимания злоумышленников.

Актуальные векторы распространения

Одним из актуальных вопросов, решаемых злоумышленниками, остается метод доставки вредоносного ПО предполагаемой жертве. Фактически, злоумышленники пользуются двумя такими методами.

- Доставка вредоносного ПО с помощью фишинговых сообщений. Этот метод широко известен и о нем было написано много раз. Злоумышленники используют различные подходы для маскировки своей деятельности: домен электронной почты адреса отправителя похож на легитимный, сообщение содержит убедительный текст, сообщение содержит «важное» вложение, и т. д. Само сообщение содержит ссылку на скачивание вредоносного исполняемого файла или такой файл находится в самом вложении.
- Автоматическая доставка вредоносного ПО с использованием одного или нескольких (набор) эксплойтов. Эксплойт может содержаться в сообщении электронной почты и автоматически установит вредоносное ПО после его открытия пользователем. Посещаемая пользователем веб-страница является вредоносной или легитимной, которая скомпрометирована вредоносным содержимым. Эксплойт автоматически установит вредоносное ПО, когда пользователь посетит такую веб-страницу.

Оба метода являются довольно эффективными и имеют свои достоинства и недостатки. Очевидное преимущество второго заключается в том, что сам процесс установки вредоносного ПО скрыт от глаз пользователя. В случае с почтовым сообщением достаточно открыть специальным образом сформированный документ Microsoft Office, в котором расположен эксплойт. После этого вредоносная программа будет установлена скрытно от пользователя. Главный его недостаток заключается в том, что злоумышленники опираются на конкретную уязвимость, например, в Office или веб-браузере MS Internet Explorer. Как правило, такие Remote Code Execution актуальны только для некоторых версий (не для всех поддерживаемых Microsoft) Office или IE. Таким образом, если пользователь использует up-to-date (новейшее) ПО, эксплойт не будет эффективен и заражения не произойдет.

Главный недостаток первого метода заключается в том, что пользователю нужно вручную скачать исполняемый файл на компьютер, а затем исполнить его. Либо такой файл в явном виде будет вложен в почтовое сообщение. Современные версии Windows, Office и веб-браузеров несколько раз предупредят пользователя об опасности скачивания подозрительных исполняемых файлов, а механизм SmartScreen в Windows 8.1 заблокирует исполнение такого файла в системе. Но механизм использования фишинговых сообщений лишен недостатка упоминавшегося выше «автоматического метода» и по сути может работать во всех случаях, т. е. не распространяется на конкретные версии ПО или ОС.

Злоумышленники могут применять и комбинированный метод, т. е. использовать оба метода одновременно. Фишинговое сообщение будет содержать документ с эксплойтом, а также ссылку на загрузку исполняемого файла. Такой подход полезен, поскольку значительно увеличивает эффективность вектора распространения вредоносного ПО.

Для iOS & Android наиболее актуальным методом распространения является фишинговое текстовое или SMS-сообщение, которое содержит ссылку на загрузку файла вредоносной программы. В случае с iOS ситуация намного сложнее, поскольку злоумышленники должны использовать специальный механизм, известный как «enterprise provisioning». Он представляет из себя единственный на сегодняшний день метод установки нежелательного или вредоносного ПО (в формате IPA) на iOS без jailbreak.

Угрозы для Windows

Общая картина угроз для Windows изменилась не существенно, т. е. нельзя сказать, что появилось что-либо принципиально новое из вредоносных программ для этой платформы. Мы фиксировали появление большого количества новых семейств вредоносных программ, а также появление новых модификаций уже существующих семейств. Они используются злоумышленниками для уже хорошо известных целей: кража аутентификационных данных онлайн-банкинга (банковские трояны), кража различных конфиденциальных данных на компьютере пользователя (стилеры), организация удаленного доступа к компьютеру жертвы (бэкдор), включение компьютера в ботнет (боты). Еще большее распространение получили вымогатели (ransomware), которые блокируют рабочий стол пользователя или шифруют файлы на компьютере с требованием выкупа. Ниже на диаграмме указана динамика активности двух представителей файловых вирусов в мире за 2014 г., это **Win32/Sality** и **Win32/Ramnit**.

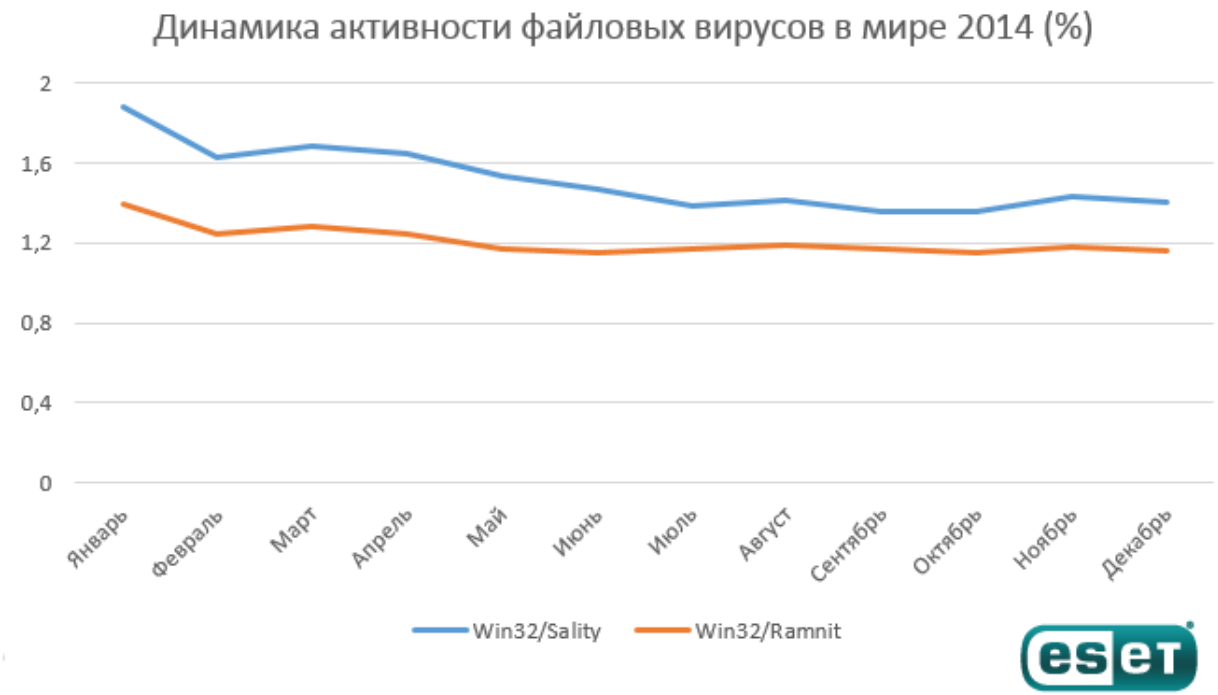


Рис. 1. Динамика активности файловых вирусов в мире.

Для России ключевым изменением за год было существенное падение активности троянской программы **Win32/Qhost**, которую злоумышленники использовали для перенаправления пользователей на вредоносные ресурсы. Qhost является очень простой вредоносной программой и специализируется на модификации hosts файла на компьютере жертвы. Про нее мы писали в нашем отчете в прошлом году, но тогда уровень его активности был существенно выше. Простота этой вредоносной программы делает ее очень популярной среди злоумышленников.

Рис. 2. Динамика активности Win32/Qhost в России.

Ниже на диаграмме показана статистика распространения других вредоносных программ в России. Все эти данные, как по России, так и по миру, были собраны с использованием нашей облачной технологии ESET Live Grid. Ниже показана статистика преобладания угроз в России, которые ежемесячно входили в рейтинг десяти самых распространенных угроз за каждый месяц в ушедшем году. Речь идет о вредоносных программах **Win32/Spy.Ursnif**, **HTML/SrcInject** и **Win32/Hoax.ArchSMS**.

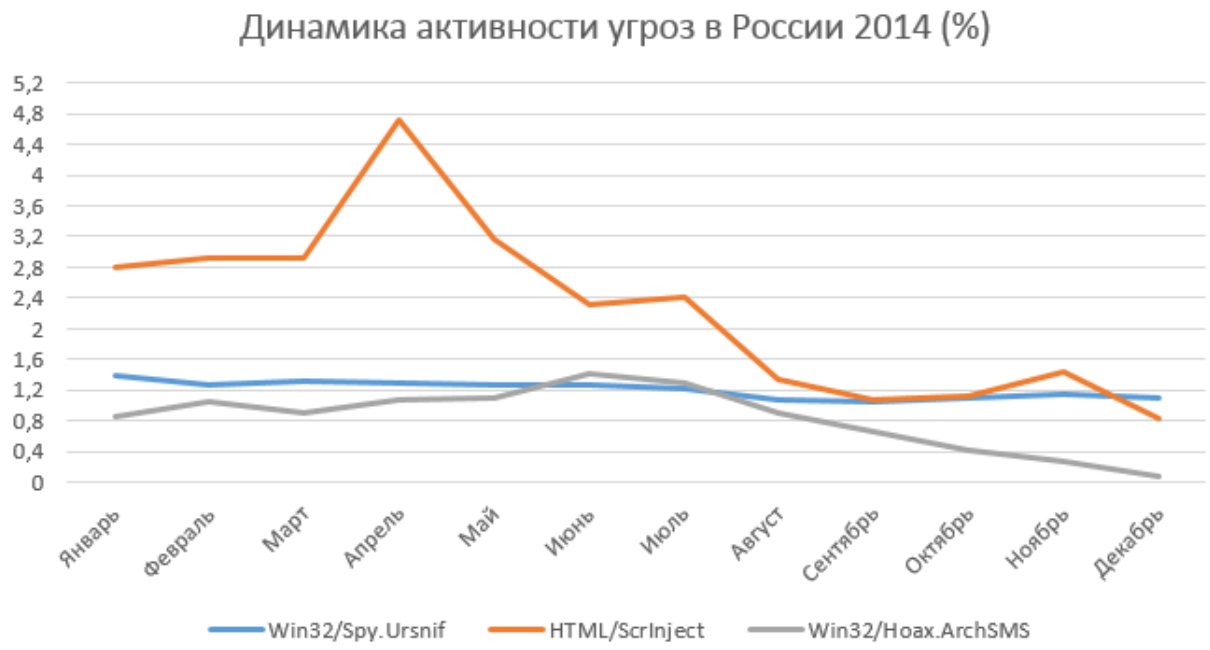


Рис. 3. Динамика активности угроз в России.

Семейство вредоносного ПО **Win32/Spy.Ursnif** относится к типу «стилер» или «похититель», который мы уже обозначили выше. Сам Ursnif специализируется на краже различных конфиденциальных данных аккаунтов пользователя от интернет-сервисов. Под «generic» обнаружением **HTML/SrcInject** мы фиксируем различные вредоносные элементы веб-страниц. В свою очередь, обнаружение **Win32/Hoax.ArchSMS** относится к платным SMS-архивам. Такой вид мошенничества стал очень популярным у злоумышленников. Они берут бесплатно распространяемые приложения и упаковывают их в архив с требованием выкупа. Подобные архивы обнаруживаются как **Win32/Hoax.ArchSMS**.

Ниже представлена география распространения сложного банковского трояна **Win32/Corkow**, исследование которого мы опубликовали в прошлом году. Эта вредоносная программа имеет российские корни и ориентирована на компрометацию систем онлайн-банкинга России и Украины. Corkow имеет в своем составе модуль, который ориентирован на компрометацию приложения Сбербанка. Такое приложение используется клиентами банка для проведения операций через интернет.

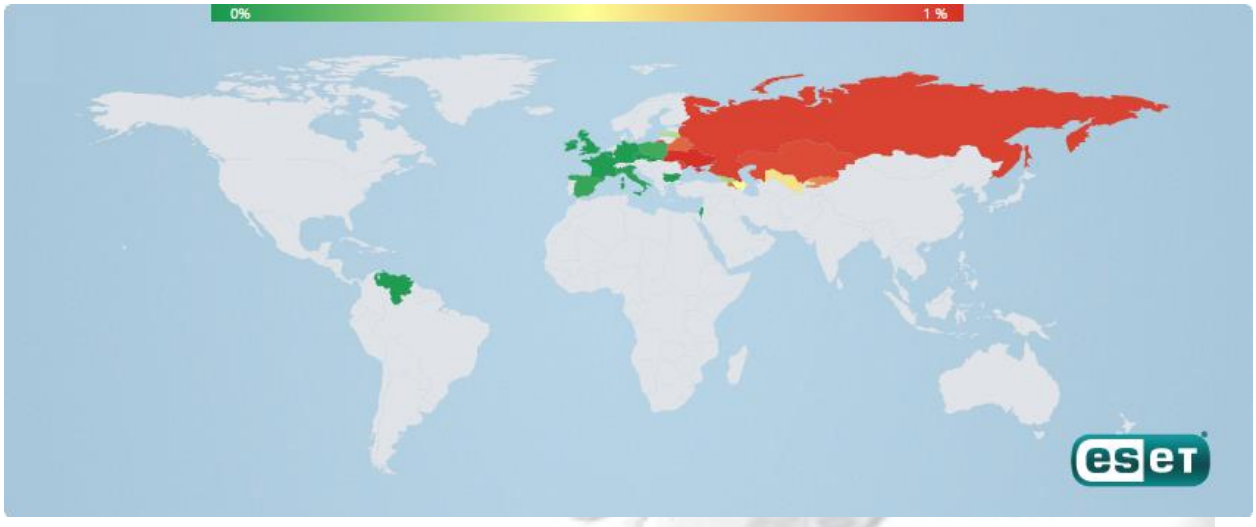


Рис. 4. География распространения банковского трояна **Win32/Corkow**.

Тренды для Windows

- Вредоносные программы вымогатели (ransomware) получили свое дальнейшее распространение. Злоумышленники используют этот тип вредоносного ПО для блокирования доступа к компьютеру или шифрования файлов пользователя. Для восстановления доступа злоумышленники требуют определенную сумму выкупа, как правило, в биткоинах. Речь идет о вымогателях не только для Windows, как, например, Win32/Virlock, TorrentLocker, но также и для Android, Android/Simplocker.
- Банковские трояны останутся очень актуальным вредоносным ПО. В прошлом году мы наблюдали появление как минимум двух сложных банковских троянов, которые способны принести злоумышленникам серьезный доход. Речь идет о многокомпонентных вредоносных программах Win32/Aibatook и Win32/Corkow. Corkow имеет в своем составе специальный модуль по компрометации мобильного приложения Сбербанка.
- Использование злоумышленниками 0day эксплойтов для доставки вредоносного ПО останется одним из основных векторов. В прошлом году мы зафиксировали использование злоумышленниками нескольких уязвимостей для Windows, в т. ч. и 0day, для доставки дропперов BlackEnergy. Одной из таких уязвимостей была CVE-2014-4114 и позволяла злоумышленникам автоматически устанавливать вредоносное ПО через специальным образом сформированный документ PowerPoint.

iOS

Эта мобильная ОС на сегодняшний день остается одной из самых безопасных. Жесткие правила безопасности, которые Apple накладывает на дистрибуцию приложений для iOS и их жестко регламентированное исполнение в sandbox среде делают ее сложной мишенью для злоумышленников. Как мы упоминали в начале, абсолютное большинство так называемого вредоносного ПО для iOS рассчитано на устройства с jailbreak. Эта операция позволяет нарушить целостность системы безопасности этой мобильной ОС.

Одной из немногих вредоносных программ, которая может компрометировать устройства как с jailbreak, так и без него является **iOS/WireLurker.A**. Она была обнаружена в 2014 году и устанавливалась на устройства посредством другой вредоносной программы для OS X под названием **OSX/WireLurker.A**. Последняя распространялась через сторонний магазин приложений OS X под названием «*Maiyadi App Store*».

Заражение iOS происходит при подключении устройства через USB-интерфейс к скомпрометированному компьютеру под управлением OS X. Для этого вредоносная программа использует специальную библиотеку libimobiledevice, которая предоставляет возможность удаленной работы с iOS через USB. Нужно отметить, что для запуска модуля вредоносной программы, который установит в систему сервис libimobiledevice, он должен получить максимальные права root, что исключено в случае использования пользователем стандартной системы безопасности OS X.

Ключевой возможностью OSX/WireLurker.A является способность заражать iOS без jailbreak. Используя вышеупомянутую библиотеку и механизм известный как «enterprise provisioning», он осуществляет установку в систему приложений в формате IPA. В таком формате для iOS поставляются приложения, которые можно установить в систему в обход App Store. Но для этого оно должно быть подписано цифровым сертификатом, выданным Apple, что и было сделано злоумышленниками (но даже при таком сценарии развития событий, пользователь должен подтвердить установку программы в iOS). На данный момент сертификат уже был отозван компанией.

В случае присутствия в системе jailbreak, OSX/WireLurker.A производит установку в файловую систему iOS вредоносной библиотеки sfbase.dylib (iOS/WireLurker.A). Доступ к файловой системе iOS при этом осуществляется с использованием сервиса AFC2, который функционирует на устройстве с jailbreak и имеет права root в системе, что позволяет получить ему прямой доступ к файловой системе.

```
<key>ExpirationDate</key>
<date>2015-02-26T07:16:16Z</date>
<key>Name</key>
<string>PPAppInstaller</string>
<key>ProvisionsAllDevices</key>
<true/>
<key>TeamIdentifier</key>
<array>
    <string>GG5L65FC6D</string>
</array>
<key>TeamName</key>
<string>Xinyi Zhongwu Network Technology Co., Ltd.</string>
<key>TimeToLive</key>
<integer>365</integer>
<key>UUID</key>
<string>ED33641B-4C7A-43B1-9F0A-9296877D5B0C</string>
<key>Version</key>
```

Рис. 5. Информация об отозванном цифровом сертификате iOS/WireLurker.A (\Payload\PPAppInstall_qudaobao.app\embedded.mobileprovision).

Другой обнаруженной для iOS вредоносной программой является **iOS/Cloudatlas**. Она распространялась через сторонний магазин приложений и могла быть установлена в систему с помощью известного ПО Cydia. Нижеприведенный значок Skype используется для обмана пользователя и находится в контейнере приложения. Файл iOS/Cloudatlas.A попал к нам в виде контейнера (дистрибутива) формата Debian. С помощью таких пакетных .deb файлов приложения распространяются через Cydia.

Рис. 6. Значок SkypeUp на скомпрометированном устройстве принадлежит iOS/Cloudatlas.A.

Вредоносная программа может получать команды на удаленную загрузку других нежелательных или вредоносных программ и затем устанавливать их в системе. Удаленно получаемые нежелательные программы устанавливаются в систему именно с помощью Cydia. Cloudatlas использует возможность директории /var/root/Media/Cydia/AutoInstall для автоматической установки скачиваемых Debian packages (deb-файлов). Эта директория задокументирована в справочной информации к Cydia и используется для ручной установки программ в iOS с jailbreak. Также он использует возможности команды Cydia «dpkg -i» для установки в систему deb-дистрибутива.

iOS/Cloudatlas.A специализируется на идентификации модели устройства и собирает о нем детальную информацию, которая включает в себя:

- Модель устройства, включая, все модели iPhone, iPad, iPod Touch, Apple TV.
- Информация о системе: имя устройства, версия, информация о процессоре, объем памяти, объем свободного места, часовой пояс, MAC-адрес.
- Информация о мобильной связи: номер телефона, ICCID код SIM-карты, InternationalRoamingEDGE.
- Информация, связанная с аккаунтом iTunes, включая, Apple ID и пользовательские настройки, связанные с iTunes Store и сервисом резервных копий (backup).
- Вся доступная информация о контактах пользователя (имя, номер телефона, адрес электронной почты, дата рождения и т. д.), для чего используется специальный SQL-запрос.
- История посещений пользователя в браузере Safari.

Эксплуатация Windows

В прошлом году Microsoft закрыла большое количество уязвимостей для своих продуктов. В нашем прошлом отчете мы упоминали, что кибератаки с использованием 0day эксплойтов являются

ключевым трендом, который получит дальнейшее развитие и в следующем году. Эти ожидания действительно оправдались.

Основная информация

В таблице ниже дано наглядное представление общей картины закрытых для браузера Internet Explorer (6-11) уязвимостей. Красным шрифтом помечены уязвимости, которые эксплуатировались атакующими еще до выхода исправления (0day). Более подробно вопросы эксплуатации IE рассмотрены ниже в разделе Internet Explorer.

Компонент	Обновление	Тип	Уязвимость
Internet Explorer	MS14-010, MS14-012, MS14-018, MS14-021, MS14-029, MS14-035, MS14-037, MS14-051, MS14-052, MS14-056, MS14-065, MS14-080	Remote Code Execution(12)	CVE-2014-0267, CVE-2014-0268, CVE-2014-0269, CVE-2014-0270, CVE-2014-0271, CVE-2014-0272, CVE-2014-0273, CVE-2014-0274, CVE-2014-0275, CVE-2014-0276, CVE-2014-0277, CVE-2014-0278, CVE-2014-0279, CVE-2014-0280, CVE-2014-0281, CVE-2014-0283, CVE-2014-0284, CVE-2014-0285, CVE-2014-0286, CVE-2014-0287, CVE-2014-0288, CVE-2014-0289, CVE-2014-0290, CVE-2014-0293, CVE-2014-0297, CVE-2014-0298, CVE-2014-0299, CVE-2014-0302, CVE-2014-0303, CVE-2014-0304, CVE-2014-0305, CVE-2014-0306, CVE-2014-0307, CVE-2014-0308, CVE-2014-0309, CVE-2014-0311, CVE-2014-0312, CVE-2014-0313, CVE-2014-0314, CVE-2014-0321, **CVE-2014-0322**, **CVE-2014-0324**, CVE-2014-0235, CVE-2014-1751, CVE-2014-1752, CVE-2014-1753, CVE-2014-1755, CVE-2014-1760, **CVE-2014-1776**, CVE-2014-0310, **CVE-2014-1815**, CVE-2014-0282, CVE-2014-1762, CVE-2014-1764, CVE-2014-1766, CVE-2014-1769, CVE-2014-1770, CVE-2014-1771, CVE-2014-1772, CVE-2014-1773, CVE-2014-1774, CVE-2014-1775, CVE-2014-1777, CVE-2014-1778, CVE-2014-1779, CVE-2014-1780, CVE-2014-1781, CVE-2014-1782, CVE-2014-1783, CVE-2014-1784, CVE-2014-1785, CVE-2014-1786, CVE-2014-1788, CVE-2014-1789, CVE-2014-1790, CVE-2014-1791, CVE-2014-1792, CVE-2014-1794, CVE-2014-1795, CVE-2014-1796, CVE-2014-1797, CVE-2014-1799, CVE-2014-1800, CVE-2014-1802, CVE-2014-1803, CVE-2014-1804, CVE-2014-1805, CVE-2014-2753, CVE-2014-2754, CVE-2014-2755, CVE-2014-2756, CVE-2014-2757, CVE-2014-2758, CVE-2014-2759, CVE-2014-2760, CVE-2014-2761, CVE-2014-2763, CVE-2014-2764, CVE-2014-2765, CVE-2014-2766, CVE-2014-2767, CVE-2014-2768, CVE-2014-2769, CVE-2014-2770, CVE-2014-2771, CVE-2014-2772, CVE-2014-2773, CVE-2014-2775, CVE-2014-2776, CVE-2014-2777, CVE-2014-1763, CVE-2014-1765, CVE-2014-2785, CVE-2014-2786, CVE-2014-2787, CVE-2014-2788, CVE-2014-2789, CVE-2014-2790, CVE-2014-2791, CVE-2014-2792, CVE-2014-2794, CVE-2014-2795, CVE-2014-2797, CVE-2014-2798, CVE-2014-2800, CVE-2014-2801, CVE-2014-2802, CVE-2014-2803, CVE-2014-2804, CVE-2014-2806, CVE-2014-2807, CVE-2014-2809, CVE-2014-2813, CVE-2014-2783, CVE-2014-2774, CVE-2014-2784, CVE-2014-2796, CVE-2014-2808, CVE-2014-2810, CVE-2014-2811, **CVE-2014-2817**, CVE-2014-2818, CVE-2014-2819, CVE-2014-2820, CVE-2014-2821, CVE-2014-2822, CVE-2014-2823, CVE-2014-2824, CVE-2014-2825, CVE-2014-2826, CVE-2014-2827, CVE-2014-4050, CVE-2014-4051, CVE-2014-4052, CVE-2014-4055, CVE-2014-4056, CVE-2014-4057, CVE-2014-4058, CVE-2014-4063, CVE-2014-4067, CVE-2014-4145, **CVE-2013-7331**, CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4080, CVE-2014-4081, CVE-2014-4082, CVE-2014-4083, CVE-2014-4084, CVE-2014-4085, CVE-2014-4086, CVE-2014-4087, CVE-2014-4088, CVE-2014-4089, CVE-2014-4090, CVE-2014-4091, CVE-2014-4092, CVE-2014-4093, CVE-2014-4094, CVE-2014-4095, CVE-2014-4096, CVE-2014-4097, CVE-2014-4098, CVE-2014-4099, CVE-2014-4100, CVE-2014-4101, CVE-2014-4102, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, CVE-2014-4111, **CVE-2014-4123**, CVE-2014-4124, CVE-2014-4126, CVE-2014-4127, CVE-2014-4128, CVE-2014-4129, CVE-2014-4130, CVE-2014-4132, CVE-2014-4133, CVE-2014-4134, CVE-2014-4137, CVE-2014-4138, CVE-2014-4140 (ASLR Bypass), CVE-2014-4141, CVE-2014-4143, CVE-2014-6323, CVE-2014-6337, CVE-2014-6339 (ASLR Bypass), CVE-2014-6340, CVE-2014-6341, CVE-2014-6342, CVE-2014-6343, CVE-2014-6344, CVE-2014-6345, CVE-2014-6346, CVE-2014-6347, CVE-2014-6348, CVE-2014-6349, CVE-2014-6350, CVE-2014-6351, CVE-2014-6353, CVE-2014-6327, CVE-2014-6328, CVE-2014-6329, CVE-2014-6330, CVE-2014-6366, CVE-2014-6368 (ASLR Bypass), CVE-2014-6369, CVE-2014-6373, CVE-2014-6374, CVE-2014-6375, CVE-2014-6376, CVE-2014-8966

Таблица 1. Исправленные уязвимости для веб-браузера Internet Explorer.

Эта таблица показывает нам, что в 2014 году Microsoft исправила приблизительно в два раза больше уязвимостей, по сравнению с 2013 годом. Ниже на диаграмме представлено более наглядное представление этой статистики. Microsoft все еще поддерживает древнюю и крайне небезопасную версию своего браузера Internet Explorer 6. Эта версия поставляется в составе Windows Server 2003 и ее поддержка завершится в конце 2015 года.

Таблица ниже предоставляет информацию об уязвимостях, которые были исправлены в различных компонентах Windows. В разделе «Windows UMC» представлены компоненты пользовательского режима этой ОС. К ним также относятся различные сервисы, работающие в ОС. Подобные сервисы запускаются в каждой сессии Windows и уязвимости в них могут использоваться атакующими для быстрого проникновения в систему. Красным шрифтом также помечены уязвимости, которые эксплуатировались атакующими в статусе 0day.

Компонент	Обновление	Тип	Уязвимость
Windows UMC (VBScript, Direct2D, MSXML, DirectShow, SAMR, File Handling/kernel32.dll, Shell handler/shell32.dll, Remote Desktop, Journal, On-Screen Keyboard, Media center/mcplayer.dll, Installer, Task Scheduler, OLE, Message Queuing, Schannel, Kerberos, Audio Service, IIS, IME (Japanese), GDI+/gdi32.dll, RPC/rpcrt4.dll, Graphics/ windowscodecs.dll	MS14-011, MS14-007, MS14-005, MS14-013, MS14-016, MS14-027, MS14-030, MS14-033, MS14-038, MS14-039, MS14-041, MS14-043, MS14-049, MS14-054, MS14-060, MS14-062, MS14-064, MS14-066, MS14-067, MS14-068, MS14-071, MS14-074, MS14-076, MS14-078, MS14-036, MS14-047, MS14-084, MS14-085	Remote Code Execution(11), Information Disclosure(3), Security Feature Bypass(4), Elevation of Privilege(9), Tampering(1)	CVE-2014-0271, CVE-2014-0263, **CVE-2014-0266**, CVE-2014-0301, CVE-2014-0317, CVE-2014-0315, **CVE-2014-1807**, CVE-2014-1816, CVE-2014-0296, CVE-2014-1824, CVE-2014-2781, CVE-2014-2780, CVE-2014-4060, CVE-2014-1814, CVE-2014-4074, **CVE-2014-4114**, CVE-2014-4971, CVE-2014-6332, **CVE-2014-6352**, CVE-2014-6321, CVE-2014-4118, **CVE-2014-6324**, CVE-2014-6322, CVE-2014-6318, CVE-2014-4078, CVE-2014-4077, CVE-2014-1818, CVE-2014-0316, CVE-2014-6363, CVE-2014-6355
Win32k	MS14-003, MS14-015, MS14-045, MS14-058, MS14-079	Elevation of Privilege(4), Denial of Service(1)	CVE-2014-0262, CVE-2014-0300, CVE-2014-0323, CVE-2014-0318, CVE-2014-1819, **CVE-2014-4113**, **CVE-2014-4148**, CVE-2014-6317
KM drivers (ndproxy.sys, tcpip.sys, afd.sys, fastfat.sys)	MS14-002, MS14-006, MS14-031, MS14-040, MS14-045, MS14-063, MS14-070	Elevation of Privilege(5), Denial of Service(2)	**CVE-2013-5065**, CVE-2014-0254, CVE-2014-1811, CVE-2014-1767, CVE-2014-4064, CVE-2014-4115, CVE-2014-4076
.NET Framework	MS14-009, MS14-026, MS14-046, MS14-053, MS14-057, MS14-072	Elevation of Privilege(3), Security Feature Bypass(1), Denial of Service(1), Remote Code Execution(1)	CVE-2014-0253, CVE-2014-0257, **CVE-2014-0295** (ASLR Bypass), CVE-2014-1806, CVE-2014-4062 (ASLR Bypass), CVE-2014-4072, CVE-2014-4073, CVE-2014-4121, CVE-2014-4122 (ASLR Bypass), CVE-2014-4149

Таблица 2. Исправленные уязвимости для различных компонентов Windows.

Диаграмма ниже представляет из себя наглядное представление статистики закрытых за год уязвимостей для различных компонентов Windows и продукта Office.

Рис. 7. Рейтинг исправленных компонентов Windows и Office.

Можно увидеть, что для Internet Explorer было закрыто наибольшее количество уязвимостей. Почти все эти уязвимости имеют тип Remote Code Execution (RCE). Это означает, что атакующие могут использовать их для удаленного исполнения кода с использованием специальным образом сформированной веб-страницы. Такие веб-страницы содержат в себе специальные вредоносные объекты, называемые эксплойтами. Обычно атакующие используют эксплойты для скрытной установки вредоносного ПО на уязвимой версии Windows. Подобные атаки получили название drive-by downloads и являются ключевым трендом эксплуатации веб-браузера Internet Explorer, как это показано на диаграмме ниже.

Рис. 8. Тренд эксплуатации различных компонентов Windows и Office.

Как упоминалось выше, термин «drive-by» представляет механизм автоматической установки вредоносного ПО с использованием RCE-эксплойтов. Отличие drive-by от RCE заключается в том, что первая представляет из себя механизм доставки вредоносного ПО именно через браузер, а в случае RCE для этого могут быть использованы и документы Office. LPE означает *Local Privilege Escalation* или, по терминологии Microsoft, Elevation of Privilege (EoP). Атакующие используют уязвимости такого типа для получения максимальных привилегий в ОС, т. е. функционирование под учетной записью SYSTEM, которая позволяет атакующим исполнять код режима ядра на 32-битных версиях Windows.

На диаграмме выше также можно увидеть, что драйвер GUI-подсистемы Windows win32k.sys и прочие драйверы Windows (KM drivers) являются теми компонентами ОС, которые чаще всего используются атакующими для повышения своих прав в работающей системе. Эксплойты для этих уязвимостей могут использоваться авторами вредоносных программ для обхода security-ограничений Windows, которые та накладывает на исполнение кода в режиме ядра (т. н. *user-mode restrictions escape*). В другой ситуации, атакующий может использовать подобные эксплойты совместно с RCE-эксплойтами для полного обхода защитных механизмов современных браузеров (т. н. *sandbox restrictions escape*).

Ниже представлено соотношение закрытых Microsoft уязвимостей в 2014 и 2013 гг.

Рис. 9. Сравнение количества уязвимостей, которые были исправлены для Windows и Office.

Как видно на диаграмме, Internet Explorer является единственным продуктом, для которого в 2014 году было закрыто больше уязвимостей, более того их количество больше в два раза. Уязвимости в продукте Office также часто используются атакующими для установки вредоносного ПО. Наши аналитики были первыми, кто обнаружил нашумевшую 0day уязвимость CVE-2014-4114. Она присутствовала в компоненте OLE package manager (packager.dll) и позволяет атакующим автоматически устанавливать вредоносное ПО на компьютер жертвы с использованием вредоносного документа PowerPoint. Исследователи ESET Роберт Липовский и Антон Черепанов выполнили анализ вредоносной кампании, которая использовалась злоумышленниками для доставки трояна BlackEnergy с использованием эксплойта для этой уязвимости.

Эксплуатация

В прошлом году мы наблюдали множество уязвимостей, которые эксплуатировались атакующими. Такие уязвимости были помечены красным шрифтом в таблицах выше. Аналитики ESET внимательно отслеживали вновь появляющиеся 0day эксплойты и оперативно добавляли их в антивирусные базы. В таблице ниже представлена дополнительная информация об уязвимостях (0day), которые использовались злоумышленники для кибератак на пользователей.

CVE	Тип	Компонент	Уязвимость	Исправлен	Обход DEP&ASLR, иное
CVE-2014-0322	Remote Code Execution	Internet Explorer 10	use-after-free	MS14-012	ActionScript-heap-spray/ROP/EMET check
CVE-2014-0502	Remote Code Execution	Flash Player	double-free	APSB14-07	ActionScript- non-ASLR-hxds.dll/ROP non-ASLR-msvcrt.dll/ROP non-ASLR-msvcr71.dll/ROP
CVE-2014-1761	Remote Code Execution	Word 2003-2013	memory-corruption	MS14-017	non-ASLR-mscomctl.dll/ROP (<=Word 2010)
CVE-2014-1776	Remote Code Execution	Internet Explorer 6-11	use-after-free	MS14-021	ActionScript-heap-spray/ROP
CVE-2014-0515	Remote Code Execution	Flash Player	buffer-overflow	APSB14-13	-
CVE-2014-0160	Information Disclosure	Windows 8.1 & RT 8.1 In-Box Junos Pulse Client (Juniper Networks)	Heartbleed	KB2962140	-
CVE-2014-4114	Remote Code Execution	Windows 2003 Server+ OLE package manager (Packager.dll)	by design (bug)	MS14-060	Удаленная установка вредоносного ПО через .INF-файл
CVE-2014-4113	Elevation of Privileges	Win32k	integer-overflow	MS14-058	Разыменование нулевого указателя в x32 Разыменование «wild» указателя в x64
CVE-2014-6352	Remote Code Execution	Windows Vista+ OLE package manager (Packager.dll)	MS14-060 fail	MS14-064	Установка вредоносного ПО через вредоносный OLE-объект
CVE-2014-6332	Remote Code Execution	Windows 2003 Server+ Windows OLE (OleAut32.dll)	by design (bug)	MS14-064	Обход DEP&ASLR по умолчанию

Таблица 3. Уязвимости in-the-wild.

В таблице мы можем наблюдать уязвимости таких приложений как веб-браузер MS Internet Explorer, проигрыватель Adobe Flash Player, приложения Office, различные компоненты Windows. Ниже в таблице даны обнаружения ESET для соответствующих уязвимостей.

Уязвимость in-the-wild	Обнаружение ESET	Месяц	Направленная атака
CVE-2014-0322	Win32/Exploit.CVE-2014-0332	Февраль	Да
CVE-2014-0502	SWF/Exploit.CVE-2014-0502	Февраль	Да
CVE-2014-1761	Win32/Exploit.CVE-2014-1761	Март	Да
CVE-2014-1776	Win32/Exploit.CVE-2014-1776 SWF/Exploit.CVE-2014-1776 JS/Exploit.Agent.NGS	Апрель	Да
CVE-2014-0515	SWF/Exploit.CVE-2014-0515	Апрель	Да
CVE-2014-4114	Win32/Exploit.CVE-2014-4114	Октябрь	Да
CVE-2014-4113	Win64/Dianti.A Win32/Dianti.A	Октябрь	Да
CVE-2014-6352	Win32/Exploit.CVE-2014-6352.A	Октябрь	Да
CVE-2014-6332	Win32/Exploit.CVE-2014-6332.A	Ноябрь	Нет

Таблица 4. Обнаружение уязвимостей ESET.

Колонка под названием «Направленная атака» демонстрирует то, что уже было сказано в самом начале: атакующие разрабатывают 0day эксплойты для их последующего использования в направленных атаках. Обнаружение для уязвимости CVE-2014-6332 было добавлено уже после того как соответствующее обновление было выпущено компанией Microsoft.

Как мы уже неоднократно наблюдали, Microsoft добавляла вспомогательные функции безопасности (*security features*) в каждом новом выпуске Windows. Наиболее важные из них, это DEP (Data Execution Prevention) & ASLR (Address Space Layout Randomization). Для обхода DEP

атакующие прибегают к использованию различных типов гаджетов ROP (Return Oriented Programming), инструкции для которых могут быть найдены в динамических библиотеках, скомпилированных без поддержки ASLR. Эти ROP гаджеты представляют из себя фрагменты исполняемого кода и могут помочь атакующим модифицировать атрибуты защиты страниц памяти с шелл-кодом. Мы наблюдали использование механизма ROP для обхода DEP в эксплойте для Adobe Flash Player. Более подробную информацию о нем можно получить в нашем исследовании.

Другая хорошо известная функция безопасности Windows под названием ASLR также значительно снижает эффективность эксплуатации той или иной уязвимости. Она позволяет системным компонентам Windows выделять регионы виртуальной памяти, а также загружать образы исполняемых файлов в память по произвольным адресам, что значительно усложняет разработку эксплойта, поскольку злоумышленникам невозможно опереться на тот или иной постоянный адрес системной функции в памяти. Таким образом, ASLR помогает защитить пользователя от целого спектра уязвимостей и создает дополнительные проблемы для атакующих, увеличивая общую стоимость разработки эксплойта.

К сожалению, некоторые версии Windows содержат компоненты, скомпилированные без поддержки ASLR. Например, ПО .NET Framework или продукт Office могут содержать такие исполняемые файлы. Они очень полезны для атакующих, поскольку размещаются в памяти по предсказуемым адресам. В таблице ниже перечислены закрытые уязвимости в различных компонентах, большинство из них относится к отсутствующей поддержке ASLR в исполняемых файлах.

Уязвимость (обход ASLR)	Продукт/Компонент	Детали
CVE-2014-0295 (MS14-009)	.NET Framework 2.0 SP2, .NET Framework 3.5.1	Уязвимость в vsavb7rt.dll Эксплуатируется ITW
CVE-2014-4062 (MS14-046)	.NET Framework 2.0 SP2 – 3.5.1	-
CVE-2014-4122 (MS14-057)	.NET Framework 2.0 SP2 – 3.5.1	-
CVE-2014-0319 (MS14-014)	Silverlight 5	-
CVE-2014-1809 (MS14-024)	Windows Common Control MS Office 2007 - 2013	Уязвимость в mscomctl.ocx Эксплуатируется ITW
CVE-2014-0316 (MS14-047)	Windows 7 – 8.1 / RT 8.1 Local RPC (LRPC)	Неявный обход ASLR череза *out-of-process memory-spray*
CVE-2014-4140 (MS14-056)	Internet Explorer 9 - 11	-
CVE-2014-6339 (MS14-065)	Internet Explorer 8-9	-
CVE-2014-6368 (MS14-080)	Internet Explorer 11	-

Таблица 5. Закрытые уязвимости обхода ASLR (ASLR bypass).

Уязвимость CVE-2014-0316 представляет особый интерес, поскольку может использоваться атакующими для обхода ASLR «удаленно» (*out-of-process*), т. е. из контекста другого процесса. Это осуществляется через отправку специальным образом подготовленного LRPC (Local Remote Procedure Call) запроса. Атакующие могут использовать эту уязвимость совместно с другой RCE уязвимостью, чтобы облегчить себе процесс проникновения в систему через процесс веб-браузера.

Атаки типа Drive-By Download и Local Privilege Escalation

На сегодняшний день атаки типа drive-by download представляют из себя типичный вид кибератак, который злоумышленники используют для удаленного исполнения кода через веб-браузер. Не секрет, что при таком сценарии злоумышленники прибегают к помощи наборов эксплойтов для перенаправления пользователей на установку вредоносного ПО. Вредоносным содержимым

может быть скомпрометирован легитимный веб-сайт, который будет перенаправлять посетителей на «веб-страницу посадки» (*landing page*). На такой веб-странице и размещаются эксплойты.

Хорошим примером случая реализации drive-by download атак является вредоносная кампания под названием «Операция Windigo». Злоумышленники использовали похищенные данные аккаунтов от серверов под управлением Linux для их компрометации вредоносным ПО. Они также распространяли подобные вредоносные программы как вспомогательные модули для известного ПО Apache. После того как сервер подвергся компрометации, вредоносная программа получает полный контроль над посетителями веб-сайта, который обслуживается этим сервером. Это означает, что пользователь будет получать вместе с легитимной веб-страницей от веб-сервера еще и вредоносное содержимое в виде фрагментов HTML-кода.

В прошлом году мы несколько раз писали о различных группах киберпреступников, которые используют атаки drive-by download в качестве основного вектора для распространения вредоносного ПО. Например, хакерская группа Sednit использовала подобные атаки для доставки троянов корпоративным пользователям Восточной Европы с применением специального набора эксплойтов. Набор эксплойтов включал в себя различные эксплойты для браузера Internet Explorer.

Атакующие используют атаки типа Local Privilege Escalation (LPE) в двух случаях. Первый случай предполагает эксплуатацию LPE уязвимости совместно с другой RCE уязвимостью для получения полного контроля над системой через веб-браузер (*sandbox bypass*). Из-за того, что механизм песочницы браузера не позволяет шелл-коду выполнять системные операции, атакующим нужна LPE уязвимость, которая позволит выполнить такую операцию и обойти ограничения песочницы.

Во втором случае, авторы вредоносного ПО могут использовать LPE уязвимости для обхода ограничений Windows, которая та накладывает на исполнение кода в режиме ядра (*user mode restriction bypass*). Эксплойт позволяет исполнить код режима ядра минуя эти ограничения ОС. Дропперы буткитов представляют из себя такой тип вредоносного ПО, который использует LPE эксплойты для загрузки своего драйвера в память. Аналитики ESET Eugene Rodionov, Aleks Matrosov и David Harley подробно останавливались на исследовании буткитов в презентации под названием Bootkits: past, present & future.

В 2014 г. мы наблюдали один из LPE эксплойтов (CVE-2014-4113), который использует уже ставшей популярной технику исполнения произвольного кода в режиме ядра через разыменование нулевого указателя (эксплойт обнаруживается как Win32/Dianti.A и Win64/Dianti.A). Эксплойт использует баг в функции *win32k!xxxHandleMenuMessages* драйвера win32k.sys. Также он может нормально функционировать в 64-битных версиях Windows при разыменовании т. н. «wild pointer».

```
signed int __usercall fnPrepareExploitation@<eax>(int Addr@<esi>)
{
  int pWin32ThreadInfoStruct; // ebx@1
  HANDLE v2; // eax@7
  int v4; // [sp+4h] [bp-4h]@7

  pWin32ThreadInfoStruct = fnCallPtiCurrentAndGetTebWin32ThreadInfo();
  if ( !pWin32ThreadInfoStruct )
  {
    GetLastError();
    fnLogMessage("[%d] Failed, %08X\n", 25);
  }
  if ( !ZwAllocateVirtualMemory )
  {
    GetLastError();
    fnLogMessage("[%d] Failed, %08X\n", 31);
  }
  v4 = 0x2000;
  *(_DWORD *)Addr = 1;
  v2 = GetCurrentProcess();
  if ( ZwAllocateVirtualMemory(v2, Addr, 0, &v4, 1060864, 64) )
  {
    GetLastError();
    fnLogMessage("[%d] Failed, %08X\n", 46);
  }
  fnFillMaliciousstagWnd(pWin32ThreadInfoStruct);
  return 1;
}
```

Рис. 10. Функция эксплойта Win32/Dianti.A, которая используется для подготовки операции эксплуатации.

На скриншоте выше можно увидеть тело функции в коде эксплойта, которая выполняет необходимые подготовительные действия для проведения эксплуатации уязвимости CVE-2014-4113 (Win32/Dianti.A). Эксплойт представляет из себя типичный пример использования операции выделения страницы памяти по нулевому указателю (NULL page) на 32-битных версиях Windows. После выделения там памяти, на этой странице будет размещена специальным образом сформированная структура драйвера win32k.sys под названием *win32k!tagwnd*. Структура содержит указатель на функцию обратного вызова (callback), которая вызывается легитимным кодом режима ядра в процессе эксплуатации. На скриншоте выше виден вызов функции под названием *fnCallPtiCurrentAndGetTebWin32ThreadInfo*, она используется для получения недокументированного указателя, который далее используется для инициализации вредоносной *win32k!tagwnd*. Формат этой структуры показан ниже на скриншоте (Windows 7 x64).

```
kd> dt win32k!tagwnd
   +0x000 head             : _THRDESKHEAD
   +0x028 state            : Uint4B
   +0x028 bHasMeun         : Pos 0, 1 Bit
.........................................
   +0x048 spwndNext        : Ptr64 tagWND
   +0x050 spwndPrev        : Ptr64 tagWND
   +0x058 spwndParent      : Ptr64 tagWND
   +0x060 spwndChild       : Ptr64 tagWND
   +0x068 spwndOwner       : Ptr64 tagWND
   +0x070 rcWindow         : tagRECT
   +0x080 rcClient         : tagRECT
   +0x090 lpfnWndProc      : Ptr64     int64
   +0x098 pcls             : Ptr64 tagCLS
   +0x0a0 hrgnUpdate       : Ptr64 HRGN__
   +0x0a8 ppropList        : Ptr64 tagPROPLIST
   +0x0b0 pSBInfo          : Ptr64 tagSBINFO
   +0x0b8 spmenuSys        : Ptr64 tagMENU
   +0x0c0 spmenu           : Ptr64 tagMENU
```

Рис. 11. Формат недокументированной структуры *win32k!tagwnd* на Windows 7 x64.

Как мы уже упоминали в нашем прошлом отчете за год под названием «Итоги 2013: угрозы и эксплуатация Windows», Microsoft добавила новую security-настройку, которая запрещает выделение памяти по нулевому адресу. Для пользователей Windows 7 эта настройка стала доступна с обновлением MS13-031. Кроме этого, 64-битные версии Windows 8 также содержат настройку безопасности под названием Supervisor Mode Execution Prevention (SMEP). SMEP запрещает исполнять в режиме ядра программный код, который расположен на страницах виртуальной памяти пользовательского режима.

Как мы можем увидеть из таблицы в разделе «Основная информация», Microsoft закрыла очень мало уязвимостей для драйвера win32k.sys, но этот драйвер содержал много уязвимостей, которые были закрыты за прошлые несколько лет. Одна из причин, по которой в этом драйвере постоянно обнаруживаются множественные уязвимости заключается в том, что его код изначально размещался в библиотеках пользовательского режима. Это касается тех версий Windows NT, которые выходили до версии 4.0. В Windows NT 4.0 GUI подсистема перекочевала из библиотек пользовательского режима в драйвер win32k.sys. Не исключено, что многие фрагменты исходного кода библиотек пользовательского режима были напрямую скопированы в код драйвера без дополнительных проверок. Именно такая ситуация могла повлечь за собой присутствие столь большого количества уязвимостей в этом драйвере.

Internet Explorer

В 2014 г. Microsoft закрыла большое количество уязвимостей в веб-браузере Internet Explorer. Уязвимости относились к типу Remote Code Execution и могли использоваться атакующими для скрытной установки вредоносного ПО на компьютеры пользователя. Кроме этого, семь из этих закрытых уязвимостей эксплуатировались in-the-wild как 0day. Новейшие версии браузера включают в себя специальные security настройки, которые помогают защитить пользователя от подобных атак.

Во-первых, речь идет о режиме Enhanced Protected Mode (EPM) работы браузера Internet Explorer. Он также называется «Расширенный защищенный режим» и появился в IE 10. Режим EPM также можно назвать режимом «полной песочницы» (*full sandbox*), так как он полностью изолирует процессы работающих вкладок веб-браузера от ресурсов Windows. Такая песочница похожа на

аналогичный механизм, используемый во всех современных ОС, включая, Apple OS X, Apple iOS, а также Google Android. На самом деле, EPM поддерживается только на Windows 8+, поскольку он опирается на специальный механизм ядра Windows, который называется *AppContainer*. Этот механизм является расширением другой известной функции ядра под названием Integrity Level (IL) или частичная песочница (*partial sandbox*). В терминологии IE он называется «Защищенный режим» работы браузера (Protected Mode) и появился в IE 7, который был выпущен в 2006 г.

Нужно отметить, что для реализации режима EPM, IE10+ опирается на те возможности ядра Windows, которые появились в Windows 8. Исключение составляет только Windows 7 x64, для которой EPM включает 64-битные вкладки для браузера.

Как мы наблюдали в последние два года, атакующие используют преимущество библиотек, скомпилированных без поддержки ASLR, для того, чтобы сделать свои эксплойты более устойчивыми или «обойти ASLR по умолчанию». В IE10 Microsoft добавила специальную опцию под названием *ForceASLR*. Как и EPM, ForceASLR опирается на нововведения ядра Windows, которые присутствуют в Windows 8 по умолчанию и в Windows 7 с обновлением KB2639308. Эта настройка IE применяет ASLR по умолчанию для всех библиотек, которые загружаются в контекст процессов вкладок браузера, в том числе для библиотек, которые скомпилированы без поддержки ASLR (отсутствует флаг /DYNAMICBASE). Сама ForceASLR похожа на настройку EMET под названием *Mandatory ASLR*. На самом деле, на Windows 8+, настройку ForceASLR можно использовать для принудительного включения ASLR в выбранном пользователем процессе.

К сожалению, по умолчанию Internet Explorer (включая новейшую версию IE11) работает как 32-битный браузер в 64-битной системе. Для того, чтобы заставить вкладки IE функционировать как 64-битные в 64-битной системе, нужно вручную задать настройку под названием *Enable 64-bit processes for Enhanced Protection Mode* (Включить 64-битные процессы для расширенного защищенного режима). Таким образом, использование IE в режиме по умолчанию значительно снижает его устойчивость к эксплуатации, поскольку в 32-битном виртуальном адресном пространстве обойти ASLR с использованием heap-spray значительно проще. Больше об этой настройке можно узнать из наших предыдущих исследований Итоги 2013: угрозы и эксплуатация Windows и Защита от эксплойтов для пользователей Windows.

Как можно увидеть из таблицы выше, посвященной типам закрытых уязвимостей, а также из нашего предыдущего отчета, уязвимости типа use-after-free (UAF) представляют из себя довольно распространенный тип уязвимостей не только для IE, но также и для других компонентов Windows.

Обычно логика работы с памятью кучи выглядит следующим образом:

1) браузер выделяет блок памяти в куче;
2) использует его;
3) высвобождает.

В случае бага в коде, работа с памятью может иметь вид:

1) браузер выделяет блок памяти в куче;
2) использует его;
3) высвобождает;
4) повторно обращается к этому блоку по сохраненному в переменной указателю (напр., через vtable).

Самый общий макет эксплуатации может выглядеть следующим образом:

1) браузер выделяет блок памяти в куче;
2) использует его;

3) высвобождает;
4) пользователь посещает веб-страницу с эксплойтом;
5) эксплойт выполняет spray кучи (для обхода ASLR) и заполняет блоки необходимым кодом (например, шелл-код) или адресами памяти (для срабатывания уязвимости);
6) эксплойт создает условия для ситуации обращения кода браузера по недействительному указателю, который уже действителен, так как пункт 4;
7) браузер повторно обращается по указателю и передает управление на блок памяти с несанкционированным кодом (перед этим выполнив гаджеты эксплойта, которые отключают DEP для блоков кучи через *ntdll!NtProtectVirtualMemory*).

Для защиты потенциально уязвимого кода браузера от эксплуатации уязвимостей такого типа, Microsoft добавила в него специальный защитный механизм под названием *anti-UAF*, который включает в себя реализацию изолированной кучи и отложенных механизмов высвобождения блоков памяти. Последняя функция является очень интересной, поскольку с точки зрения самой Windows, освобожденный кодом браузера блок памяти все еще находится в использовании менеджера кучи самого IE, поэтому атакующий не сможет получить над ним контроль. Ниже в таблице представлены обновления, в рамках которых Microsoft добавила механизм anti-UAF.

Опция	Начиная с	Описание
Расширенный защищенный режим	IE10	На Windows 7 x64 включает 64-битное виртуальное адресное пространство для процессов вкладок браузера. На Windows 8+ x32/x64 включает полную изоляцию *AppContainer* для процессов вкладок.
ForceASLR (принудительный ASLR)	IE10 (Windows 8+ или Windows 7 с KB2639308)	Указывает загрузчику применять ASLR для библиотек, скомпилированных без его поддержки.
64-битные вкладки	IE11	На Windows 7+ x64 включает 64-битное виртуальное адресное пространство для процессов вкладок.
Protected Heap & Delay Free (Anti-UAF)	IE11 (MS14-035, MS14-037)	Добавляет специальные механизмы для защиты от эксплуатации уязвимостей типа use-after-free.
Out-of-date ActiveX control blocking	IE 8-11 on Windows 7 SP1+ Oracle Java & MS Silverlight Plugins (KB2991000)	Блокирует загрузку устаревших плагинов Oracle Java и MS Silverlight в контекст процесса браузера.

Таблица 6. Ключевые механизмы безопасности веб-браузера Internet Explorer.

Другая полезная опция безопасности IE, которая была добавлена в 2014 г., называется *Out-of-date ActiveX control blocking*. Как видно из названия, она позволяет веб-браузеру блокировать загрузку устаревших версий плагинов IE. Пока настройка специализируется на блокировании out-of-date плагинов Oracle Java и Microsoft Silverlight. На самом деле *Out-of-date ActiveX control blocking* является очень полезной настройкой безопасности браузера, поскольку позволяет блокировать большое количество эксплойтов, специализирующихся на эксплуатации уязвимостей в устаревших версиях этих плагинов.

К сожалению, упоминаемая функция безопасности *full sandbox* (EPM) в IE11 может быть обойдена с использованием специальных трюков или уязвимостей в ней. Исследователи из группы Google Zero Team уже неоднократно демонстрировали слабые места в реализации EPM. В частности, одна из уязвимостей, CVE-2014-6350 (MS14-065) может быть использована атакующими для обхода этого механизма и запуска кода из браузера с привилегированными правами. Песочница IE использует специальный процесс-брокер, на который делегируется исполнение привилегированных

операций. На этот процесс может быть получен дескриптор с правами на чтение его виртуального адресного пространства, таким образом вредоносный код может использовать такую возможность как потенциальную *information disclosure* уязвимость для получения системных структур данных самой песочницы. Другой метод обхода режима песочницы основан на доступе к объекту-разделу (section object), который используется всеми процессами вкладок браузера для обеспечения единого доступа к необходимым настройкам браузера в памяти.

Предотвращение эксплуатации

Мы уже упоминали выше некоторые функции безопасности Windows, которые Microsoft добавляла в новых выпусках ОС, для защиты пользователя от эксплойтов. В 2014 г. компанией была выпущена новая версия инструмента EMET (текущая версия 5.1). Более подробно с ним можно ознакомиться на сайте компании, по этой ссылке.

В новую версию EMET Microsoft добавила некоторые полезные функции безопасности. Они называются ASR (Attack Surface Reduction) и EAF+ (Export Address Table Filtering Plus). ASR похожа на опцию IE под названием *Out-of-date ActiveX control blocking*, но покрывает больший спектр эксплойтов. Если упоминаемая опция IE может блокировать загрузку только устаревших *out-of-date* плагинов в контекст процессов вкладок IE, то ASR может блокировать загрузку *всех* модулей определенного типа. Эта настройка может работать для следующих процессов: Internet Explorer, Excel, Word, PowerPoint.

По умолчанию ASR блокирует загрузку в виртуальную память тех модулей, которые часто используются атакующими для проведения drive-by download атак. К этим модулям относятся библиотеки плагинов Oracle Java (npjpi*.dll, jp2iexp.dll), Vector Markup Language DLL (vgx.dll) (SA 2963983), Flash Player (flash*.ocx). Таким образом, при использовании этой настройки (включена в EMET по умолчанию), соответствующее содержимое нельзя будет воспроизвести в браузере или другой программе. Набор блокируемых модулей зависит от определенного приложения. Нужно отметить, что в случае с IE, настройка работает для «небезопасных» зон, так что в безопасной корпоративной зоне «интранет» пользователь сможет просматривать необходимое ему содержимое. Ниже в таблице перечислены блокируемые опцией ASR модули.

Процесс	Опция ASR (блокируемые модули)
Internet Explorer (iexplore.exe)	npjpi*.dll;jp2iexp.dll;vgx.dll; msxml4*.dll; wshom.ocx;scrrun.dll
PowerPoint (powerpnt.exe)	flash*.ocx
Word (winword.exe)	flash*.ocx
Excel (excel.exe)	flash*.ocx

Таблица 7. Настройки EMET ASR.

Еще одна новая функция EMET называется EAF+. Она улучшает уже существующую опцию под названием EAF и может работать независимо от нее. Как мы знаем, шелл-код в составе эксплойтов пытается получить адреса различных экспортируемых функций системных модулей, например, системной библиотеки ntdll.dll путем анализа виртуальных страниц памяти, на которых расположена таблица экспорта конкретного модуля (EAT). Обычная настройка EAF блокирует попытки чтения страниц памяти с EAT, если такие попытки исходят от шелл-кода, т. е. вредоносного кода. EAF контролирует страницы с таблицами экспортов таких библиотек как kernel32.dll и ntdll.dll. EAF+ расширяет действие EAF еще и на kernelbase.dll. Кроме этого, EAF+ может также блокировать

иные механизмы вредоносного ПО, которое пытается эксплуатировать уязвимости. Речь идет о ROP гаджетах из библиотек, которые используются шелл-кодом для обхода оригинальной настройки EAF. Для EAF это означает тот факт, что доступ к странице с таблицей экспорта исходит от известного EMET кода системной библиотеки, таким образом этот код никак не может быть идентифицирован как вредоносный. EAF+ может контролировать такую ситуацию, помогая EMET блокировать подобные попытки шелл-кода или его гаджетов получить доступ к EAT. С точки зрения реализации, EAF+ формирует список уже известных библиотек, коду которых запрещено обращаться к EAT. По умолчанию, EAF+ включена для процессов браузера Internet Explorer и Adobe Reader. Ниже в таблице перечислены такие библиотеки, для кода которых EMET заблокирует доступ к страницам с EAT.

Процесс	Опция EAF+
Internet Explorer (iexplore.exe)	mshtml.dll; flash*.ocx; jscript*.dll; vbscript.dll; vgx.dll
Adobe Acrobat (acrobat.exe, acrord32.exe)	AcroRd32.dll; Acrofx32.dll; AcroForm.api

Таблица 8. Настройки EMET EAF+.

На самом деле, вышеупомянутые механизмы предотвращения эксплуатации работают только в определенной конфигурации Windows и ее компонентов. В таблице ниже можно увидеть, что для эффективного противодействия эксплойтам настройки должны работать в соответствующем окружении. В качестве примера взят эксплойт для уязвимости CVE-2014-1776.

Опция	Эффективна	Детали
Расширенный защищенный режим IE10 & IE11 (EPM) на Windows 7 x32	Нет	Бесполезен (ничего не реализует)
Расширенный защищенный режим IE10 & IE11 (EPM) на Windows 8+ x32	Нет	Изоляции AppContainer недостаточно (только в связке с 64-битными процессами вкладок на x64)
Расширенный защищенный режим IE10 (EPM) на Windows 8+ x64	Нет	IE10 не содержит опцию 64-битных процессов для вкладок
Расширенный защищенный режим IE10 (EPM) на Windows 7 x64	Да	Вместо AppContainer включает 64-битное адресное пространство для процессов вкладок (на Windows 7 EPM работает только для x64)
Расширенный защищенный режим IE11 (EPM) на Windows 7+ x64 & 64-битные вкладки	Да	Используемый ActionScript-heap-spray из объекта Flash Player неэффективен в 64-битном адресном пространстве
EMET 5.0 ASR	Да	Блокирует загрузку в процесс браузера VGX.DLL и Flash (.ocx) на зоне «Интернет»
EMET 5.0 EAF+	Да	Не позволяет шелл-коду получить доступ к странице с экспортами ntdll.dll
EMET 5.0, 4.x Heap Spray	Да	Блокирует используемый эксплойтом ActionScript-heap-spray (ASLR bypass).
EMET 4.x ROP (StackPivot, Caller, MemProt)	Да	Только с установленным Deep Hooks (по умолчанию выключен, включен по умолчанию в EMET 5.0 TP).

Таблица 9. Различие поведения механизмов предотвращения эксплуатации на примере CVE-2014-1776.

Еще одна интересная опция EMET 5.1, которая активирована по умолчанию, называется *Deep Hooks*. Она была полезна для блокирования 0day эксплойта к уязвимости CVE-2014-1776. Больше подробностей можно узнать из следующего поста More Details about Security Advisory 2963983 IE 0day. Настройка Deep Hooks позволяет EMET отслеживать различные операции в Windows более глубоко за счет дополнительных перехватов API вызовов на уровне ntdll.dll (Internal API). Список таких перехватов представлен ниже в таблице. В качестве примера взяты функции работы с памятью.

	Deep Hooks OFF	Deep Hooks ON
Memory functions	*kernel32!VirtualAlloc*	*ntdll!NtAllocateVirtualMemory*
		kernelbase!VirtualAlloc
	kernel32!VirtualAllocEx	*ntdll!NtAllocateVirtualMemory*
		kernelbase!VirtualAllocEx
	kernel32!VirtualProtect	*ntdll!NtProtectVirtualMemory*
		kernelbase!VirtualProtect
	kernel32!VirtualProtectEx	*ntdll!NtProtectVirtualMemory*
		kernelbase!VirtualProtectEx

Таблица 10. Список перехватываемых API функций EMET.

Как можно увидеть из этой таблицы, настройка Deep Hooks включает перехваты API функций Windows, которые вызываются по пути исполнения потока при выполнении им функций из kernel32.dll. Например, если эта настройка включена, то EMET будет контролировать вызов не только *kernel32!VirtualAlloc* API, но также функции *ntdll!NtAllocateVirtualMemory* и *kernelbase!VirtualAlloc*. На скриншоте ниже показаны упоминаемые выше настройки EMET.

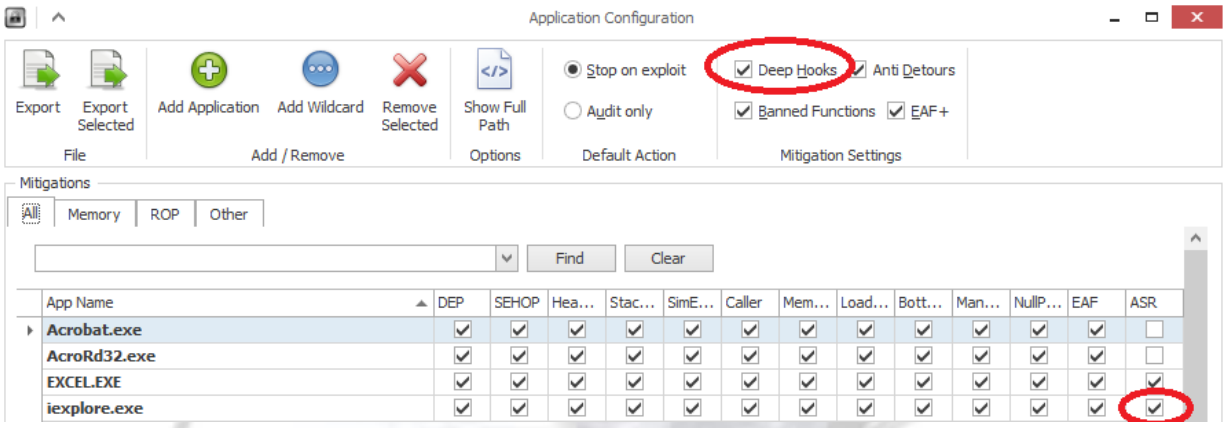
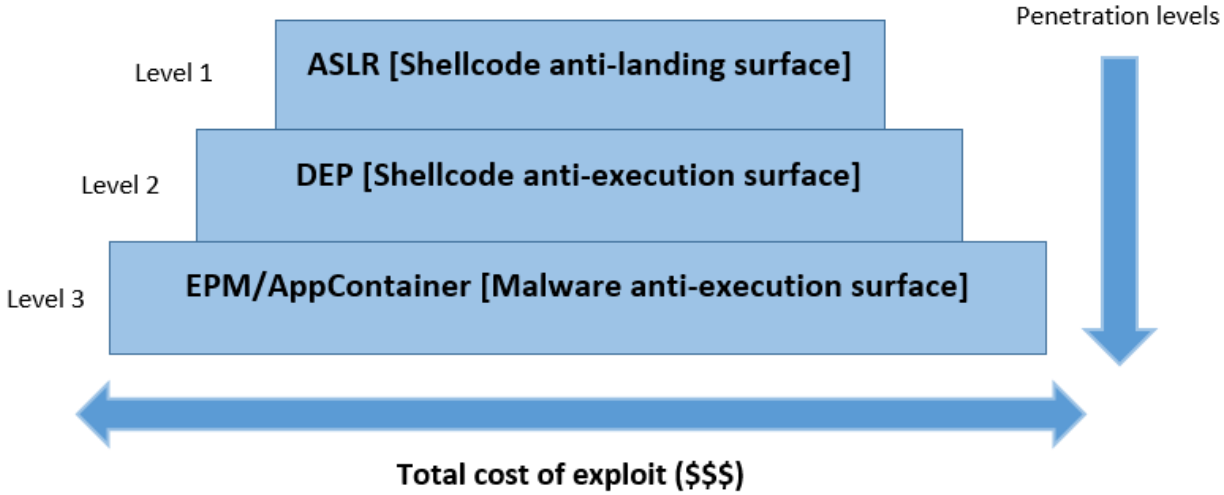


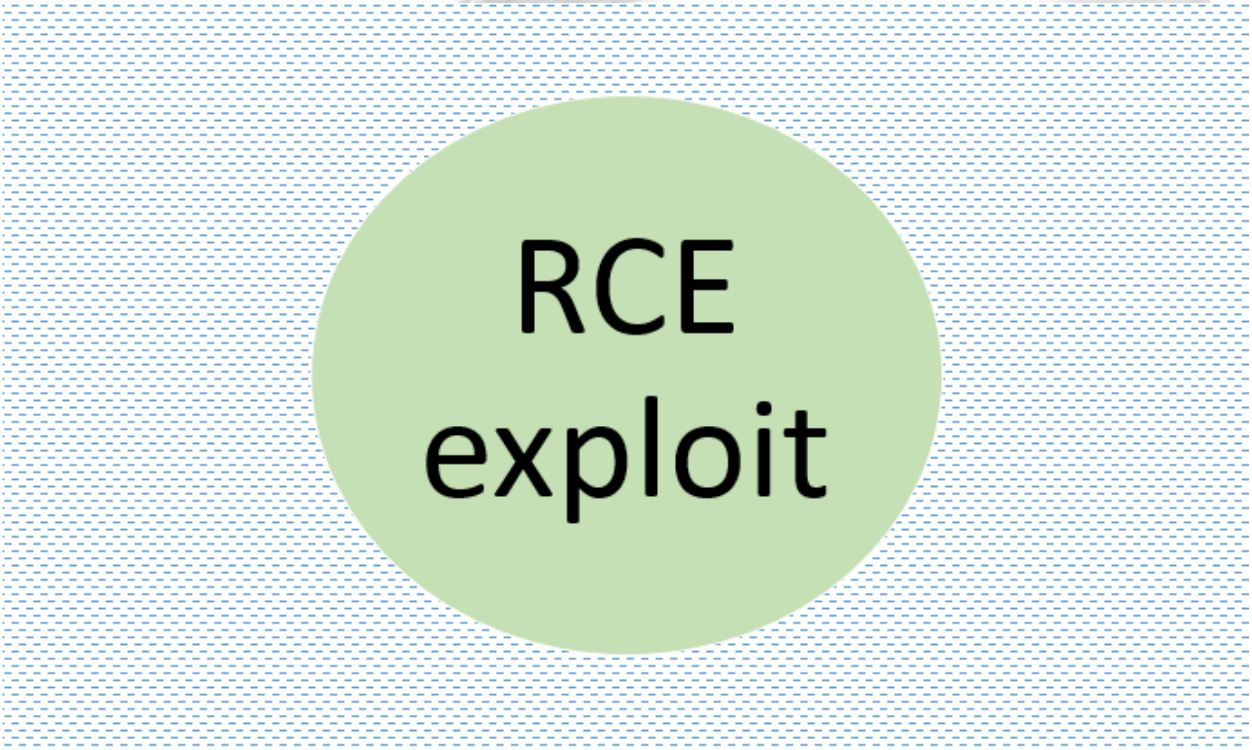
Рис 12. Настройки EMET.

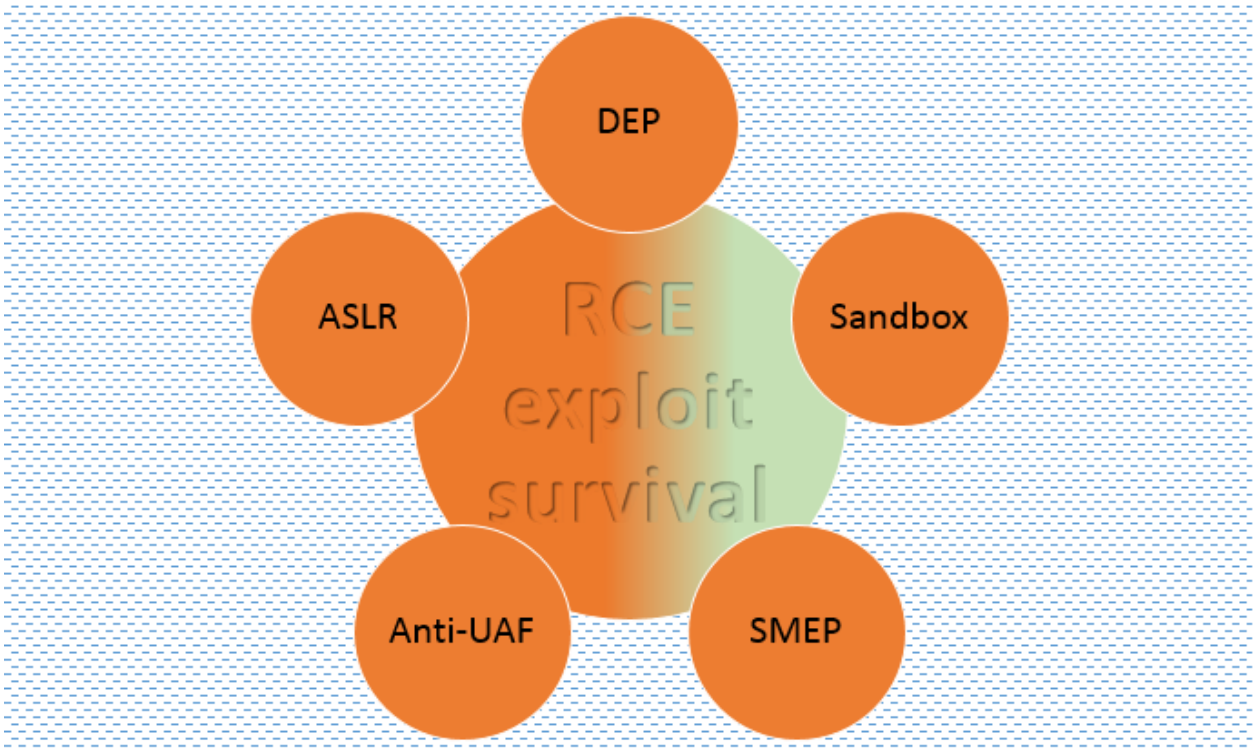
Вместо заключения

В конечном счете, улучшенные механизмы противодействия эксплуатации RCE уязвимостей приведут к значительному увеличению стоимости разработки самого эксплойта. Более наглядно это показано на схеме ниже. Атакующим нужно инвестировать значительно больше средств и выделять больше времени на исследование новых уязвимостей, которые помогут обойти улучшенные механизмы защиты Windows. Как мы показали в нашем отчете, атакующим необходим набор из двух и более эксплойтов для проникновения в систему и получение полного контроля над ней.



К сожалению, многие пользователи до сих пор используют небезопасные версии Windows, например, Windows XP. Эти версии Windows не содержат современных технологий противодействия эксплуатации уязвимостей, которые были описаны в нашем отчете. Пользователю следует понимать, что он подвергает себя существенному риску при использовании таких версий Windows. Ниже на схеме представлено наглядное различие технологическим особенностей Windows XP и Windows 8.1.





Наш прогноз на следующий год останется тем же, атаки типа drive-by download останутся главным трендом у киберпреступников для установки вредоносных программ пользователям. В связи со значительными накладными расходами на разработку 0day эксплойтов для таких атак, можно сказать, что они будут применяться, в первую очередь, для направленных атак.