Автор: Administrator
05.11.2013 23:00 -

Антивирусная компания ESET представила отчет о наиболее активных угрозах октября 2013 года. В прошлом месяце наблюдалось некоторое снижение активности интернет-угроз. Положительную динамику продемонстрировали только три вредоносные программы: троян Win32/Bundpil (3.79%), вредоносные элементы веб-страниц HTML/ScrInject (1.69%), а также впервые попавшая в нашу десятку программа Win32/Sirefef (1.02%). Бэкдор Sirefef (ZeroAccess) представляет собой сложное вредоносное ПО, которое используется злоумышленниками для скрытого доступа на компьютер пользователя, а также для накрутки переходов по рекламным ссылкам, благодаря чему киберпреступники извлекают материальную выгоду из специальных партнерских программ (в рамках которых рекламодатель платит злоумышленникам за каждого посетителя сайта). Различные версии Sirefef содержат в своем арсенале руткит-технологии, которые позволяют ему успешно скрываться в системе. В начале октября стало известно об успешной кибератаке на корпорацию Adobe. Злоумышленники смогли получить доступ к миллионам аккаунтов пользователей, а также к их конфиденциальной информации: логинам, паролям, customer ID, номерам кредитных карт. Разумеется, вся эта информация хранилась в зашифрованном виде. Специалисты Adobe уведомили пользователей о необходимости сменить регистрационные данные своих аккаунтов. Помимо сведений о клиентах, злоумышленникам удалось получить доступ к исходным кодам таких известных программ, как Adobe Acrobat, ColdFusion и Photoshop. Архивы с похищенной информацией уже были замечены на некоторых веб-сайтах. В прошлом месяце компания Microsoft закрыла ряд серьезных уязвимостей в своих продуктах. Обновление MS13-080 нацелено на исправление девяти критических уязвимостей в браузере Internet Explorer, которые могут использоваться для скрытной установки вредоносного кода. Причем обновлению подверглись все версии, начиная с IE6 и заканчивая новейшим IE11 для Windows 8.1 и RT 8.1. Одна из закрытых уязвимостей, CVE-2013-3893, присутствовала во всех версиях Internet Explorer; она использовалась злоумышленниками в целенаправленных атаках на пользователей. Антивирусные продукты ESET NOD32 детектируют эксплойт для этой уязвимости как Win32/Exploit.CVE-2013-3893.A. Всего компания Microsoft закрыла 27 уникальных уязвимостей в своих продуктах. Помимо Internet Explorer, обновлению подверглись программная платформа .NET Framework, драйвер подсистемы Win32k.sys, продукты Microsoft Office и Silverlight. Эксперты компании ESET в октябре сообщили об обнаружении вредоносного кода в популярном менеджере загрузок Xunlei. Некоторые версии этой программы содержали код, который в скрытом режиме мог устанавливать на компьютер или мобильное устройство пользователя сторонние приложения. Сами файлы программы были подписаны цифровым сертификатом, что отводило от них какие-либо подозрения во вредоносной деятельности. Тем не менее, они использовались для проведения различных операций на ПК и маскировались под расширения программ Microsoft Office. В российском рейтинге угроз был отмечен рост активности таких вредоносных программ, как HTML/ScrInject (2.76%), HTML/IFrame (2.26%), Win32/Dorkbot (1.85%), и Win32/Bicololo (1.32%). Активность вредоносных элементов JavaScript, которые используются злоумышленниками для перенаправления пользователей на веб-сайты с вредоносным содержимым, по сравнению с сентябрем значительно снизилась и составила 1.62%.

Доля России в мировом объеме вредоносного ПО в прошлом месяце составила 7.93%.