Автор:
14.02.14 10:40 -

Свое видение направлений развития мобильных угроз и возможных путей защиты от них предлагает ведущий технический специалист ESET в Украине Вячеслав Зарицкий

Автор:
14.02.14 10:40 -

1.Специалисты по информационной безопасности утверждают, что с каждым годом увеличивается количество угроз для мобильных устройств. Наблюдаете ли Вы данную тенденцию? Есть ли конкретные примеры роста угроз?

Современные телефоны и смартфоны являются удобным средством для хранения личных данных и конфиденциальной информации пользователей, представляя тем самым огромный интерес для киберпреступников.Таким образом, появление большого количества вредоносных программ под мобильные платформы было неудивительным, и,начиная с 2011 года, стала прослеживаться тенденцияэкспоненциального увеличения **количества данного вида угроз** .Например, в 2010 году, по данным ESET, было выявлено 3 семейства(группы вредоносных кодов, имеющих уникальную классификацию) вредоносных программ под Android, в то время как в конце 2013 года это число возросло до 79. При этом ежегодно растёт не только количество семейств, но и количество разновидностей угроз в каждом из них. В последнее время наблюдается значительный рост числа сигнатур, модификаций и, следовательно, количества вредоносных программ под мобильные платформы (таким же образом как это было с ОС Windows).Так, если в 2011 году широко известное семейство TrojanSMS.Agentобъединяло около 30 видов вредоносных программ, то уже в 2013 количество данных угроз выросло дооколо 350 видов. Отметим, что под разновидностью подразумевается модифицированная версия определенных и известных угроз.

2.Наблюдался ли рост мобильныхботнетов? Была ли зафиксирована работа мобильных банковских троянцев?

В 2013 году специалисты ESET сообщали о выявлении новой троянской программы, которая направлена на пользователей Интернет-банкинга в Европе и Азии. Целью вредоносной программы является получение учетных данных для доступа к банковским счетам, а также заражение мобильных ОС Symbian, Blackberry или Android.

Угроза распространяется под видом корреспонденции от известных компаний, что вводит пользователя в заблуждение и подталкивает к запуску вредоносного ПО. Жертвами данной угрозы уже стало большое количество Интернет-пользователей, которые понесли значительные финансовые потери. Выявленное вредоносное ПОявляется опасным банковским трояном, который распространяется с помощью фишинга. Более того данная вредоносная программа пытается заразить как персональные компьютеры, так и мобильные устройства под управлением ОС Android, Symbian и Blackberry.

По словам специалистов исследовательской лаборатории ESET, данная угроза имеет функции кейлоггера и способна делать скриншоты рабочего стола, записывать видео, перенаправлять информацию на удаленный прокси-сервер. Также угрозаобладает несколькими дополнительными функциями, такими как создание скрытого удаленного подключения к инфицированной системе.

3. Какие мобильные платформы подвергаются атакам больше и чаще других?

Согласно данным аналитического агентстваGartner, на протяжении последних трех лет Android является наиболее популярной операционной системой — так, во второй половине 2011 года ее доля на рынке составляла 43.4%, в 2012 выросла до 64.3%, а в 2013 достигла 79%. При этом из года в год данный рост сопровождаетсяпрямо пропорциональным увеличением количества вредоносных кодов, разработанных подAndroid. Кроме того,постоянное увеличение количества и развитие угроз для данной мобильной платформы, расширение спектра их вредоносных действий, а также открытие уязвимостей говорят о высоком уровне интереса киберпреступников к операционной системе Android.

Специалисты ESET зафиксировали, что количество вредоносных программ под Android в 2013 году возросло больше чем на 60% по сравнению с 2012 годом, и прогнозируют продолжение данной тенденции в 2014 году.

Основными видами вредоносной деятельности угроз под Android остается кража информации (шпионское ПО), отправка дорогостоящих SMS-сообщений и превращение мобильных устройств в «зомби» (ботнеты). В последнем случае киберпреступники получают возможность удаленного управления зараженным устройством, а именно — выполнять различные действия, устанавливать другие вредоносные программы, осуществлять кражу конфиденциальной информации, изменять конфигурации параметров и многое другое.

4. Какие решения предлагает Ваша компания для защиты мобильных платформ? Когда запланирован выпуск новых версий данного программного обеспечения?

В 2011 году был отмечен значительный рост популярности мобильной платформы

Автор:
14.02.14 10:40 -

Android как среди конечных потребителей, так и среди вирусописателей. В связи с этим специалисты ESET приступили к разработке комплексного решения, способного обеспечить надежную защиту смартфонов и планшетов на базе Android. Таким образом, в конце года пользователям был представлен продукт ESET MobileSecurity для Android , в котором были реализованы передовые технологии и современные инструменты защиты.Наряду с защитой от вредоносных программ, спама, блокировкой вызовов с нежелательных номеров и многими другими функциями, в данном продукте ESET была реализована «новинка» на рынке антивирусного программного обеспечения под мобильные устройства — Антивор модуль, позволяющий сохранять полный контроль над данными, хранящимися в телефоне, в случае его потери или кражи.

Но, как известно, технологии вирусописания не стоят на месте, в связи с этим специалисты ESET регулярно обновляют продукт, что позволяет использовать передовые технологии обнаружения угроз, новые методы и инструменты защиты, а также расширять возможности решения ESETMobileSecurityдляAndroid . Так, сегодня на стадии бета-тестирования находится третья версия продукта, доступна по загрузки пользователям на
странице официального сообществе Google+
.

5. Каким будет дальнейшее, по Вашему мнению, развитие мобильных угроз?

Пользователи продолжают отдавать предпочтение устройствам на базе Android, что в свою очередь стимулирует киберпреступников к разработке новых видов угроз под данную операционную систему. При этом специалисты ESET прогнозируют увеличение не только количества угроз, но также появление новых семейств вредоносных программ и типов атак. Основными видами вредоносной деятельности угроз под Android будет оставаться кража информации (шпионское ПО), отправка дорогостоящих SMS-сообщений и превращение мобильных устройств в «зомби» (ботнеты). Также широко распространенными станут программы-вымогатели, блокирующие операционную систему с требованием выкупа. Кроме этого, увеличится количество жертв высокотехнологичных угроз и вредоносных кодов, основной целью которых является кража электронных денег.

Дополнительно

Read more http://www.chip.ua/novosti/eset-chem-populyarnee-mobilnaya-platforma-tem-bolshe-pod-nee-vredonosnyih-programm/