или знака обслуживания. Избегание созвучности имени с чужими брендами. Создание собственных методик.

Литература

1. Журнал «Компьютерные вести» № 17, 16.11.2011, стр. 3-5
2. Журнал «Главная Книга.by» №2, январь 2012, стр. 30-36
3. Википедия, ru.wikipedia.org/wiki/Киберсквоттинг
4. Газета «Хартия», 05.03.2012
5. Газета «Советская Белоруссия», 03.11.2010

Гринько Е.Ю.
БГЭУ, ФМБК, ДЯК-3, 1 курс

ЗАЩИТА ОС ANDRIOD ОТ МОБИЛЬНОГО БОТНЕТА

В 2008г. эксперты в области информационной безопасности считали, что уже в течение года злоумышленники могут попытаться сформировать мобильные ботнеты с целью проведения различного рода атак при помощи портативных устройств. Как сообщал CNET News, ожидать появления первых мобильных ботнетов стоило уже в 2009 году. Такие ботнеты злоумышленники теоретически могли использовать для рассылки спама абонентам сотовых операторов или для организации атак на беспроводные сервисы.

В феврале 2012г компанией Symantec было обнаружено вредоносное приложение для мобильных телефонов на платформе ОС Android - RootSmart, которое распространяется в альтернативных китайских каталогах программного обеспечения. В официальном Android Market такого пока не обнаружено. Программа RootSmart устанавливается вместе с обычными программами из каталога, но при этом передаёт на удалённый сервер информацию о заражённом устройстве: номер IMEI, номер IMSI, ID соты, location area code и код мобильной сети.

RootSmart является второй программой после GingerMaster, которая применила на практике известный рут-эксплоит GingerBreak (для Android OS

младше 2.3.3 и для 3.0), утилиту, которая обеспечивает root доступ на Android 2.3 Gingerbread. Когда вирус скачивается (как часть выглядящего вполне невинным приложения) с неофициального магазина программ для Android, он обращается к удаленному серверу для закачки GingerBreak, повышает свои привилегии и собирает всю доступную информацию с телефона. После рутования телефона программа подгружает с удалённого сервера программу DroidLive, которая играет роль средства удалённого администрирования и выполняет команды с сервера C&C. Таким образом, телефон становится частью ботнета. На рутованном телефоне хозяин ботнета может инициировать любые действия. По словам китайских исследователей, они уже видели, что программа для удалённого управления посылает SMS, блокирует входящие SMS, записывает информацию об исходящих вызовах (включая номер телефона и продолжительность звонка), инициирует собственные телефонные вызовы. Программа также способна менять адрес командного сервера, самостоятельно подключаться к интернету и передавать данные. По словам исследователей, самое опасное то, что она передаёт большие объёмы данных в сторону C&C, так что есть риск утечки приватных данных немалого количества пользователей.

В связи с появлением подобной технологии и массовым распространением вируса на маркете возникает вопрос: как защитить свой мобильный телефон от атаки вредоносным приложением?

Основной проблемой индикации вируса RootSmart является то, что непосредственно вредоносного элемента в загружаемом приложении нет. Он загружается после установки приложения с удаленного сервера, что и делает многие мобильные антивирусные программы практически беспомощными. Т.к. вирус RootSmart – новый, существующие на момент его появления антивирусные программы не были приспособлены к обнаружению вредоносного приложения. Первым антивирусным продуктом, решившим эту проблему, стал AegisLab Antivirus Free/Elite, сделав об этом заявление 6 февраля 2012 года, и в результате активных разработок за февраль и март 2012

года на данный момент уже 20 из 43 существующих мобильных антивирусов могут обеспечить клиентам возможность идентифицирования и блокирования вредоносных приложений, среди которых известные всем Avast, DrWeb, Ikarus, NOD32, Kaspersky и др. Но самый действенный способ избежать вируса RootSmart - воздержаться от рутования мобильных телефонов и ограничиться скачиванием проверенных приложений с официального Android маркета. Хотя вредоносное приложение распространено пока только в китайских альтернативных каталогах ПО, угроза всемирного распространения мобильных ботнетов велика, поэтому пользователи должны предпринять все возможные меры для защиты своих гаджетов.

Данишевская В.А.

БГЭУ, ИСГО, группа ДИМ, 1 курс

ТЕХНОЛОГИЯ «25-ГО КАДРА»

1957 год, Нью-Джерси, США. Учёный Джеймс Вайкери провёл в кинотеатрах города уникальный эксперимент - во время демонстрации фильмов с помощью дополнительного проектора в моменты смены кадров проецировались кадры рекламы. В кино кадры меняются 24 раза в секунду, поэтому дополнительное проецирование получило название «25-го кадра». Эффект от рекламы был потрясающим, эксперимент получил широкую огласку и был запрещён законом штата. Но с тех пор желающие воздействовать на подсознание человека получили ещё одно оружие, а многие исследователи начали усовершенствовать данный метод. Так начиналась история 25-го кадра.

За прошедшие десятилетия эффект «25-го кадра» изучался различными структурами и институтами. Возможность напрямую воздействовать на подсознание человека рисовала громадные перспективы: можно лечить вредные привычки, можно стимулировать покупательский спрос, а можно проводить обучение языкам и наукам. И всё это без непосредственного участия сознания человека.

□□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□□ □□□□□□□□□□□□. □□□□□□□□□□.
□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□ □□□□□□□□□□□□□ □□□□□□□□□□□□. □□□□□□□□□□.
БДЭУ Беларускі дзяржаўны эканамічны ўніверсітэт. Бібліятэка.
БГЭУ Белорусский государственный экономический университет. Библиотека.
BSEU Belarus State Economic University. Library.
http://www.bseu.by elib@bseu.by