UA Linux
http://ualinux.com
Аналитика, обзоры, рекомендации.

user And LINUX
{ Secure Shell }

Читайте в этом номере:

- От мошенничества с платежными карточками в прошлом году пострадала половина украинских банков.

- В Одессе разоблачили финансовую интернет-пирамиду.

- Поддельные магазины Android-приложений воруют личные данные пользователей.

- Kaspersky Security Bulletin 2012. Развитие угроз в 2012 году.

- Kaspersky Security Bulletin 2012. Основная статистика за 2012 год.

- Топ самых популярных видов кибер-мошенничества на День святого Валентина.

И многое другое.

От мошенничества с платежными карточками в прошлом году пострадала половина украинских банков

Почти каждый второй украинский банк в прошлом году понес убытки от мошеннических операций с использованием платежных карточек, однако их реальный объем оценить очень трудно из-за опасений банков утратить доверие клиентов.

Об этом на пресс-конференции в УКРИНФОРМе, посвященной старту кампании "Противодействие киберпреступности", заявила директор генерального департамента информационных технологий и платежных систем Национального банка Украины Наталия Синявская.

"Рост количества безналичных операций приводит к увеличению случаев мошеннических операций с использованием платежных карточек и несанкционированного перевода средств со счетов клиентов. В соответствии с полученными отчетами, в 2012 году количество банков-членов платежных систем, которые понесли убытки, по сравнению с 2011 годом увеличилась на 6 банков и составляла 57, или 40% от общего количества банков-членов карточно-платежных систем", - сказала Синявская.

Она проинформировала, что, по официальным данным, предоставленным банками НБУ, общее количество мошеннических операций в 2012 году по сравнению с предыдущим увеличились на 47%, а сумма убытков по этим операциям возросла на 20%. Почти все убытки (99,7% от общей суммы), нанесенные банкам по операциям с платежными карточками, были совершены с карточками международных платежных систем.

По словам Синявской, основными типами мошеннических действий с использованием платежных карточек является их подделка, потом идут операции с потерянными карточками и довольно большой пласт представляют операции без предъявления карточки, то есть в сети интернет или через телефонные или факс-заказы.

Директор департамента отметила, что после перехода в течение последних лет большинства европейских стран на чиповые карточки основная тенденция на европейском рынке - переток мошеннических операций в виртуальную среду, то есть без предъявления карточки. Не является исключением в этом пласте и Украина: по сравнению с 2011 годом этот показатель по количеству и суммам операций возрос более чем в 3 раза, констатировала Синявская.

Источник: http://www.creditdeposit.com.ua

В Одессе разоблачили финансовую интернет-пирамиду

Управлением по борьбе с киберпреступностью ГУМВД Украины в Одесской области в результате мониторинга сети Интернет была получена информация о групповой преступной деятельности, связанной с привлечением денег граждан. Во время проверки указанной информации в поле зрения правоохранителей попал предприимчивый двадцативосьмилетний уроженец удаленного от областного центра района, который в сети Интернет разработал, организовал и администрировал On-line ресурс, на котором под видом агентства по привлечению инвестиций организовал деятельность «финансовой пирамиды».

Будучи неплохо осведомленным в области компьютерных технологий и финансов предприимчивый парень не торопился реализовывать их на законном поле. Хотя высшее юридическое образование позволяло осознавать последствия выбранного им уголовного пути. Своих потенциальных жертв, под видом инвестиций в финансовый проект, он выбирал среди друзей, приятелей, знакомых и друзей из социальных сетей. Как рассказал начальник управления Юрий Выходец, схема указанной преступной деятельности предусматривала привлечение денег граждан под видом финансовых инвестиций с возможностью получения сверхприбылей в виде дивидендов. По мере увеличения количества инвесторов и при наличии достаточного объема инвестиций осуществлялись лишь единичные выплаты «дивидендов» отдельным участникам пирамиды.

Как пример, один из товарищей «криминального гения», который первым поддержал его в незаконной деятельности, в качестве одноразовых «дивидендов» получил 2000 долларов США.

- Однако, при достижении критического предела, когда количество необходимых выплат равна или превышает количество привлеченных денежных средств, деятельность финансовой пирамиды прекращается и большое количество средств, привлеченных гражданами, остается на счетах организаторов-мошенников, - резюмировал чиновник.

С целью документирования деятельности структуры, которая носила все признаки финансовой пирамиды, были проведены мероприятия, направленные на установление потерпевших лиц, которые перечисляли банковскими переводами на счет организаторов преступного замысла деньги в иностранной валюте. По факту организации финансовой структуры, которая носит признаки финансовой пирамиды, организованной в сети Интернет, было начато уголовное производство по признакам преступления. предусмотренного ч.3 ст. 190 УК Украины.

В рамка досудебного расследования был проведен обыск в офисе учреждения, в результате которого изъята компьютерная техника и документацию о деятельности структуры. В настоящее время устанавливаются личности всех пострадавших и размер нанесенного им ущерба.

Сообщает:
ОСО ГУМВД по материалам Управления по борьбе с киберпреступностью
Источник: http://vchaspik.ua

Парольная защита для закладок Chrome

У каждого пользователя среди закладок в браузере есть такие, которые н

е хотелось бы показывать жене и детям. Или спрятать от взгляда сослуживцев, если вы пользуетесь браузером на рабочем компьютере, к которому имеют доступ посторонние лица. К сожалению, штатные средства браузера Chrome не позволяют выделить эти закладки в отдельную категорию и скрыть их. В таких ситуациях можно воспользоваться расширением Secure Bookmarks. Оно сразу решает именно эту проблему: создаёт отдельную категорию закладок, которые надёжно зашифрованы и отображаются только после ввода пароля.

Для быстрого доступа к защищённым закладкам расширение помещает кнопку на панели инструментов. Расширение очень удобное и простое в использование. Единственное, чего не хватает, на первый взгляд, это возможности переноса в защищённое хранилище старых закладок.

Источник: http://www.xakep.ru

Поддельные магазины Android-приложений воруют личные данные пользователей

Компания Symantec объявила об открытии новой угрозы - Android.Exprespam. Преступники создают поддельные магазины приложений и воруют с их помощью персональную информацию пользователей, сообщает oborot.ru

Android.Exprespam был обнаружен в начале этого года, но за время своего недолгого, но очень бурного существования программа смогла собрать много информации. Так лишь с 13 по 20 января Android Express's Play, одно из поддельных магазинов прилажений, насчитывает более 3000 посещений – и это лишь часть общей картины.

По оценкам Symantec, за все время нарушители могли похитить от 75 до 450 тысяч записей личных данных.

Учитывая тот факт, данная схема нарушений является новой, специалисты прогнозируют, что количество подобных ситуаций в ближайшее время будет лишь расти. Так создатели Exprespam уже зарегистрировали новый домен, где находится еще одна версия их "магазина". Никаких контактных данных "магазин" не содержит, как нет у него и названия. Эксперты считают, что это может говорить о том, что проект только готовится к запуску.

Обезопасить себя от мошенников пользователи Android могут достаточно просто. Во-первых, не нужно переходить по подозрительным ссылкам от незнакомых людей. Во-вторых, скачивать приложения нужно лишь с надежных ресурсов.

Источник: http://itexpert.org.ua

UA Linux
http://ualinux.com
Эксперт в области безопасности.

Kaspersky Security Bulletin 2012. Развитие угроз в 2012 году.

Данный отчет является продолжением серии ежегодных аналитических отчетов «Лаборатории Касперского». В нем рассматриваются основные проблемы, затрагивающие персональных и корпоративных пользователей и связанные с использованием вредоносных, потенциально нежелательных и мошеннических программ, а также спама, фишинга и различных видов хакерской активности.

Отчет подготовлен экспертами Global Research&Analisys Team (GReAT) в сотрудничестве с подразделениями Content&Cloud Technology Research и Anti-Malware Research «Лаборатории Касперского».

10 важнейших инцидентов IT-безопасности 2012 года

В начале этого года мы опубликовали обзор вирусной активности в 2011 году в котором охарактеризовали год одним словом — «взрывоопасный». Тогда самой большой проблемой было поместить всего в десять сюжетов — главные сюжеты года - все многочисленные инциденты, темы, факты, новые тенденции и загадочных игроков.

События и игроки, определившие десятку главных сюжетов безопасности 2011 года, позволили нам сделать ряд прогнозов на 2012 год:

- Продолжение роста активности хактивистских групп.
- Рост числа инцидентов, связанных с атаками класса APT (Advanced Persistent Threat)
- Первые свидетельства применения кибероружия. Борьба самых могущественных государств за доминирующее положение с применением кибершпионажа.
- Атаки на разработчиков ПО и игр, таких как Adobe, Microsoft, Oracle и Sony.
- Более активные действия правоохранительных органов по отношению к злоумышленникам, совершающим традиционные компьютерные преступления.
- Взрывной рост угроз, нацеленных на Android.
- Атаки на платформу Apple Mac OS X.

Насколько точными оказались наши прогнозы? Давайте посмотрим, какими в 2012 году были десять наиболее значительных инцидентов, связанных с информационной безопасностью.

1. Flashback: атака на Mac OS X

Несмотря на то что предназначенная для заражения Mac OS X троянская программа Flashback/Flashfake появилась в конце 2011 года, по-настоящему широкое распространение она получила только в апреле 2012 года. Говоря «по-настоящему широкое распространение», мы имеем в виду именно то, что программа распространилась действительно очень широко. Собранные нами статистические данные говорят о том, что троянец Flashback поразил более 700 000 компьютеров Mac. Это, по-видимому, самая крупная на сегодняшний день эпидемия вредоносных программ для MacOS X. Как же она стала возможна? Здесь сыграли свою роль два основных фактора: уязвимость в Java (CVE-2012-0507) и практически полное безразличие поклонников компьютеров Mac к проблемам безопасности.

С появлением Flashback возникла проблема, которая по-прежнему актуальна, потому что миф о неуязвимости всего, что связано с компьютерами Mac оказался разрушен и стало ясно: массовые эпидемии возможны не только в среде Windows. В 2011 году мы предсказали новые вредоносные атаки на компьютеры Mac. Однако мы не ожидали, что они приобретут такой масштаб.

2. Flame и Gauss: кибершпионаж на государственном уровне

В середине апреля 2012 года в результате серии кибератак были выведены из строя компьютерные системы нескольких нефтяных платформ на Ближнем Востоке. Ответственное за атаки вредоносное ПО, получившее название «Wiper», так и не было найдено, хотя по некоторым признакам оно имело много общего с Duqu и Stuxnet. Однако в ходе расследования мы наткнулись на масштабную кампанию по кибер-шпионажу, которая теперь известна как Flame.

Как нам представляется, Flame — одна из наиболее сложных угроз за всю историю вредоносного ПО. После полного развертывания ее на компьютере суммарный размер входящих в ее состав модулей составлял более 20 МБ. Эти модули выполняли широкий набор вредоносных функций, таких как перехват аудиоданных, сканирование устройств, подключенных по протоколу Bluetooth, кража документов и создание снимков экрана на зараженной машине. Наиболее впечатляющей возможностью программы было использование поддельного сертификата Microsoft для проведения атаки типа Man-in-the-Middle, нацеленной на службу Windows Update. Это позволяло вредоносной программе моментально заражать компьютеры, работающие под управлением Windows 7 со всеми необходимыми патчами. Сложность этого механизма не оставляла никаких сомнений в том, что программа была создана при государственной поддержке. Кроме того, специалисты «Лаборатории Касперского» обнаружили тесную связь между Flame и Stuxnet. Это позволило прийти к выводу, что разработчики Flame действовали в сотрудничестве с разработчиками Stuxnet, возможно в рамках одного проекта.

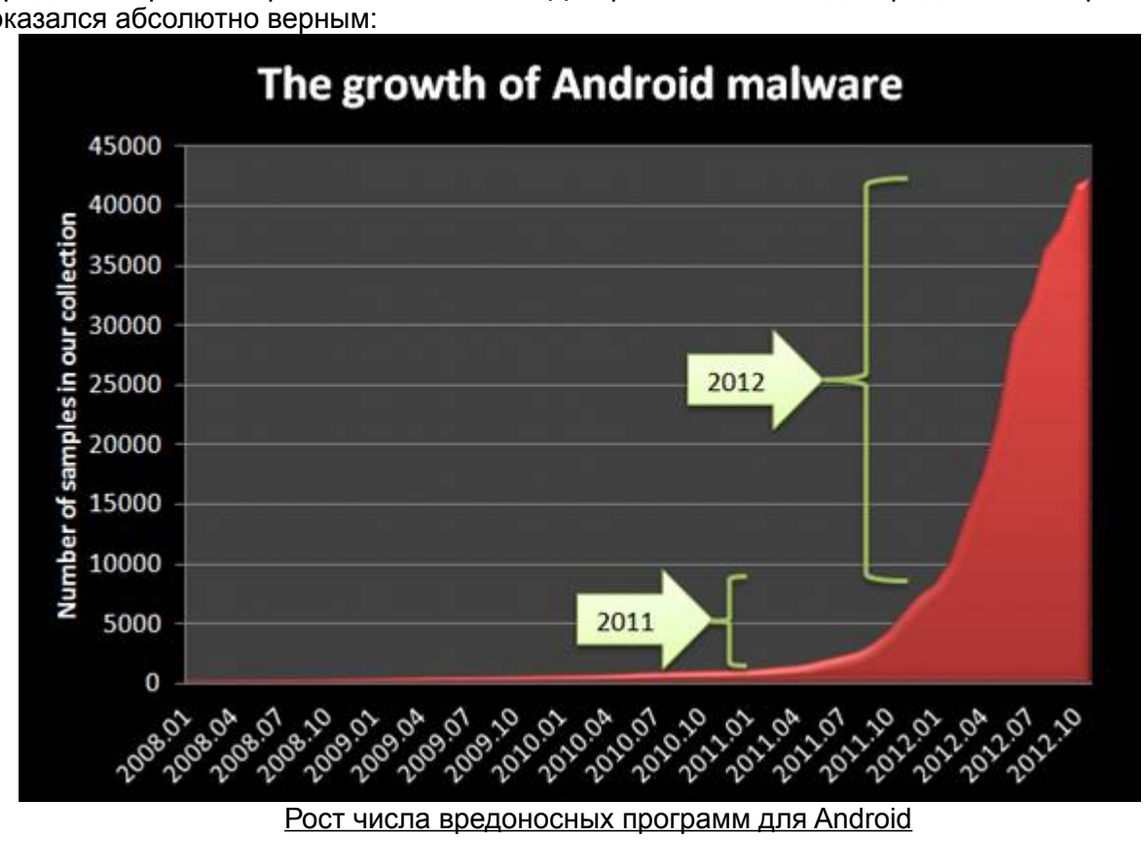
Программа Flame имеет большое значение, поскольку она продемонстрировала, что сложное вредоносное ПО способно оставаться необнаруженным в течение многих лет. По нашим оценкам, проекту Flame не меньше пяти лет. Вдобавок, Flame заставил специалистов по-новому взглянуть на угрозы «нулевого дня» из-за используемого им метода распространения, основанного на атаке man-in-the-middle, подобной чит-коду в компьютерной игре, включающему «режим бога».

Конечно же, после обнаружения Flame возник вопрос о том, много ли проводится других подобных кампаний. Вскорости другие кампании были обнаружены. В частности, Gauss — еще один сложный троянец, широко распространенный на Ближнем Востоке, давший новое измерение киберкампаниям, проводимым на государственном уровне. Gauss интересен по нескольким причинам, причем ответы на некоторые вопросы отсутствуют по сей день. Среди множества загадок — для чего нужен нестандартный шрифт Palida Narrow и каково назначение зашифрованного вредоносного функционала, рассчитанного на компьютеры, отключенные от интернета. Кроме того, это первый созданный при государственном участии троянец, способный к краже у жертв логинов и паролей к системам онлайн-банкинга, преимущественно принадлежащим ливанским банкам.

Flame и Gauss усложнили и без того непростую ситуацию на Ближнем Востоке, сделав кибероружие важным фактором ее развития. Похоже, что нынешняя геополитическая напряженность имеет мощную кибернетическую составляющую — возможно, даже более мощную, чем можно было ожидать.

3. Взрывной рост числа Android-угроз

В течение 2011 года мы были свидетелями взрывного роста числа мобильных угроз, нацеленных на платформу Android. Мы предсказали, что число угроз для Android продолжит расти огромными темпами. Диаграмма ниже подтверждает, что прогноз оказался абсолютно верным:



Рост числа вредоносных программ для Android

Число получаемых нами образцов продолжало расти, достигнув максимума в июне 2012 года, когда мы выявили почти 7000 вредоносных программ для Android. Всего в 2012 году мы идентифицировали почти 35 000 вредоносных программ для Android — это примерно в шесть раз больше, чем в 2011 году. Вдобавок, это примерно в пять раз больше, чем суммарное число образцов вредоносных программ для Android, полученных нами с 2005 года!

Такой невероятный рост числа вредоносных программ для Android можно объяснить двумя факторами: экономическим и связанным с самой платформой. Прежде всего, сама платформа Android стала невероятно популярной. На ее основе выпускается самое большое число телефонных аппаратов, а завоеванная ею доля рынка превысила 70%. В дополнение к этому открытый характер операционной системы, легкость создания приложений и разнообразные (неофициальные) магазины приложений вместе оказывают негативное влияние на уровень безопасности, заложенный в платформу Android.

Заглядывая в будущее, можно констатировать, что эта тенденция, несомненно, сохранится — ситуация в данном случае такая же, как с вредоносным ПО для операционной системы Windows много лет назад. Поэтому мы ожидаем, что 2013 год станет годом целевых атак против пользователей Android, угроз «нулевого дня» и утечек данных.

4. Утечка паролей из сервисов LinkedIn, Last.fm, Dropbox и Gamigo

5 июня 2012 года сайт LinkedIn, одной из крупнейших в мире социальных сетей, специализирующейся на поиске и установлении деловых контактов, был взломан неизвестными злоумышленниками. В результате взлома произошла утечка в интернет хешей более 6,4 миллионов паролей к пользовательским учетным записям. С помощью высокоскоростных графических процессоров специалистам по безопасности удалось восстановить 85% оригиналов паролей — поразительный результат. Это стало возможным по нескольким причинам. Во-первых, сервис LinkedIn хранил пароли в форме хешей, созданных по алгоритму SHA1. Несмотря на то что такие хеши обеспечивают более высокий уровень безопасности, чем созданные по чрезвычайно популярному алгоритму MD5, современные графические процессоры способны взламывать хеши SHA1 с поразительной скоростью. Например, процессор Radeon 7970 стоимостью 400 долларов способен проверять почти 2 миллиарда вариантов пароль/хеш в с секунду. Злоумышленники использовали также современные криптографические атаки, такие как применение цепей Маркова для оптимизации подбора паролей или сокрытия атак. Все это преподало веб-разработчикам урок того, как не следует хранить зашифрованные пароли.

Когда DropBox объявил о произошедшем взломе и утечке данных пользовательских учетных записей, это стало очередным подтверждением того, что хакеры охотятся за ценными данными (особенно логинами и паролями пользователей) на популярных веб-сервисах. В 2012 году были осуществлены похожие атаки на сервисы Last.fm и Gamigo. В результате последнего инцидента на общедоступные ресурсы попали более 8 миллионов пользовательских паролей.

Чтобы проиллюстрировать масштаб проблемы, на конференции InfoSecSouthwest 2012 компания Korelogic распространила архив, содержащий около 146 миллионов хешей паролей, собранных в результате нескольких инцидентов со взломом сайтов, причем 122 миллиона паролей из этого числа уже были взломаны.

Эти атаки показывают, что в эпоху облачных вычислений, когда данные миллионов учетных записей хранятся на одном сервере, а доступ в интернет осуществляется по высокоскоростным каналам, угроза утечки данных приобретает новый масштаб. В прошлом году мы анализировали эту проблему применительно к взлому Sony Playstation Network. Наверное, нет ничего удивительного в том, что столь же масштабные взломы и утечки данных продолжились и в 2012 году.

5. Кража сертификатов Adobe и вездесущая APT-атака

В 2011 году мы были свидетелями нескольких громких атак на центры сертификации. Произошедший в июне взлом серверов голландской компании DigiNotar привел к уходу этой компании с рынка. Филиал компании Comodo выпустил в марте сертификаты по поддельным учетным данным. Обнаружение в сентябре 2011 года вредоносной программы Duqu также было связано со взломами центров сертификации.

27 сентября 2012 года компания Adobe объявила об обнаружении двух вредоносных программ, подписанных действительным сертификатом Adobe, предназначенным для подписывания кода компании. Сертификаты Adobe хранились с соблюдением правил обеспечения безопасности в особом защищенном хранилище — аппаратном модуле безопасности (HSM, hardware security module). Это специальное криптографическое

устройство, значительно затрудняющее проведение атак. Тем не менее, злоумышленникам удалось взломать сервер, выполнявший запросы о подписывании кода.

Это была одна из чрезвычайно узконаправленных целевых атак, осуществляемых высококвалифицированными злоумышленниками, использующими полный арсенал вредоносных средств. Подобные инциденты часто называют APT-атаками. APT — Advanced Persistent Threat.

Тот факт, что серверы такой крупной и известной компании, как Adobe, были взломаны подобным образом, говорит о необходимости пересмотреть общепринятые представления о границах возможного для злоумышленников столь высокого уровня.

6. Отключение серверов DNSChanger

После того как киберпреступники, стоящие за вредоносной программой DNSChanger, были арестованы в ноябре 2011 года в ходе операции Ghost Click, управление инфраструктурой, которую они использовали для кражи личных данных пользователей, взяло на себя ФБР.

ФБР согласилось поддерживать серверы до 9 июля 2012 года, чтобы дать жертвам время удалить вредоносную программу со своих машин. Вопреки предполагаемым сценариям вселенской катастрофы, указанный день прошел достаточно спокойно. Это стало возможным благодаря тому, что свои ресурсы и время в проект вложили ФБР, другие правоохранительные органы, частные компании и государственные организации по всему миру. Это был крупномасштабный проект, который продемонстрировал, что успехов в борьбе с киберпреступностью можно добиться, развивая открытое сотрудничество и обмен информацией.

7. Инцидент с Ma(h)di

В конце 2011 и первой половине 2012 года злоумышленниками проводилась кампания по проникновению в компьютерные системы, нацеленная на пользователей в Иране, Израиле, Афганистане и других странах мира. В партнерстве с компанией Seculert мы провели подробное расследование этой операции, дав ей название «Madi» исходя из того, какие строки и идентификаторы использовали киберпреступники.

Несмотря на то что вредоносная программа Madi была относительно несложной, ей удалось заразить множество компьютеров по всему миру благодаря применению приемов социальной инженерии и технологии Right-To-Left-Override (RTLO). Кампания Madi продемонстрировала еще один чрезвычайно важный аспект операций по кибершпионажу в ближневосточном регионе: наравне с вредоносными программами, создаваемыми на государственном уровне с неограниченным бюджетом, малозатратные операции могут быть весьма успешны.

8. Уязвимости нулевого дня в Java

После описанного выше инцидента с Flashback корпорация Apple сделала решительный шаг и приняла решение отключить поддержку Java на компьютерах миллионов пользователей Mac OS X. Стоит отметить, что, хотя патч, закрывающий уязвимость, которую использовал Flashback, появился в феврале, владельцы компьютеров Apple оставались под ударом еще несколько месяцев после этого из-за медлительности компании Apple в отправке патча пользователям операционной системы Mac OS X: в отличие от других операционных системам, пользователи которых получали патчи напрямую от Oracle, патчи для Mac OS X доставляла на компьютеры пользователей сама корпорация Apple.

Кроме того, в августе 2012 в Java была обнаружена уязвимость нулевого дня (CVE-2012-4681), которая на тот момент уже активно использовалась в «дикой среде». Эксплойт для этой уязвимости был включен в чрезвычайно популярный набор BlackHole и быстро оказался наиболее эффективным из всех эксплойтов, входящих в этот набор, обеспечив заражение миллионов компьютеров по всему миру.

Во втором квартале 2012 года мы проанализировали, какое уязвимое ПО установлено на компьютерах пользователей, и обнаружили, что более 30% машин содержат старые уязвимые версии Java. Это, по-видимому, было самое распространенное уязвимое ПО на компьютерах пользователей.

9. Shamoon

В середине августа появилась подробная информация о крайне разрушительном вредоносном ПО, которое было использовано для атаки на Saudi Aramco — один из крупнейших в мире нефтяных конгломератов. По сообщениям, эта вредоносная программа полностью вывела из строя более 30 000 компьютеров.

Мы выполнили анализ Shamoon и обнаружили, что в эту вредоносную программу встроен переключатель, активирующий деструктивный процесс 15 августа в 8:08 по Гринвичу. Позднее появились сообщения еще об одной атаке той же вредоносной программы, нацеленной на другую ближневосточную нефтяную компанию.

Shamoon имеет большое значение, поскольку реализует идею, заложенную во вредоносную программу Wiper — разрушительный вредоносный функционал, который применяется для того, чтобы поставить под удар функционирование компании. Как и в случае с Wiper, многие детали остаются неизвестными, в частности каким образом происходило заражение компьютеров вредоносной программой и кто за ней стоял.

10. DSL-модемы, проблемы с продукцией Huawei и взломы аппаратных средств

В октябре 2012 года эксперт «Лаборатории Касперского» Фабио Ассолини (Fabio Assolini) опубликовал подробную информацию об атаке, осуществляемой киберпреступниками в Бразилии с 2011 года и использующей одну уязвимость в микропрограмме устройств, два вредоносных скрипта и 40 вредоносных DNS-серверов. Для атаки уязвима продукция шести производителей аппаратных средств. Речь идет об осуществляемой непрерывно в течение длительного времени скрытой массовой атаке на DSL-модемы, жертвой которой стали миллионы пользователей интернета в Бразилии.

В марте 2012 года специалисты бразильского центра CERT подтвердили, что в результате атаки злоумышленниками взято под контроль более 4,5 миллионов модемов, которые используются киберпреступниками для осуществления разнообразной мошеннической деятельности.

На конференции T2 в Финляндии эксперт в области безопасности Феликс Линднер (Felix ‘FX’ Lindner) из компании Recurity Labs GmbH сделал доклад об уровне безопасности и уязвимостях, обнаруженных в линейке маршрутизаторов Huawei. Этот доклад появился вскорости после того, как администрация США приняла решение провести в отношении компании Huawei расследование с целью определить уровень риска, связанного с потенциальной угрозой шпионажа со стороны этой компании.

Истории с Huawei и бразильскими DSL-маршрутизаторами нельзя считать случайными инцидентами. Они наглядно показали, что аппаратные маршрутизаторы могут быть источником такого же, если не большего риска IT-безопасности, как и устаревшее или полученное из неизвестных источников и не обновляемое ПО. Они продемонстрировали также, что задача обеспечения защиты стала более комплексной и сложной, чем когда-либо ранее, — в некоторых случаях, даже нереализуемой.

Заключение: от взрывоопасного к удивительному и сенсационному

Накануне нового 2013 года мы все задаем себе вопрос: «Что же будет дальше?» Подтверждением точности наших прогнозов можно считать представленную выше десятку наиболее значительных сюжетов уходящего года.

Несмотря на арест Ксавьера Монсегура (Xavier Monsegur) из хакерской группы LulzSec и многих маститых хакеров из группы Anonymous, хактивисты продолжали свою деятельность. Военные действия в киберпространстве и кибершпионаж получили новое измерение с обнаружением вредоносных программ Flame и Gauss. APT-атаки по-прежнему занимали видные места в новостных лентах: угрозы нулевого дня и сложные методы проведения атак использовались для взлома компьютерных систем, которые принадлежат занимающим высокое положение людям. На пользователей Mac OS X обрушилась эпидемия Flashfake — самая масштабная атака на компьютеры под управлением Mac OS X на сегодняшний день. А крупные компании пытались бороться с разрушительным вредоносным ПО, которое вывело из строя тысячи компьютеров.

Наиболее значительные игроки 2011 года остались прежними: это группы хактивистов, компании, работающие в области IT-безопасности, государства, сводящие счеты друг с другом с помощью кибершпионажа, крупнейшие разработчики ПО и компьютерных игр, такие как Adobe, Microsoft, Oracle и Sony, правоохранительные органы и киберпреступники, использующие традиционные методы, Google как производитель операционной системы Android, а также корпорация Apple — благодаря своей платформе Mac OS X.

2011 год мы охарактеризовали как «взрывоопасный». Инциденты 2012 года, на наш взгляд, также удивили и поразили многих наблюдателей. Но пока мы осознавали масштабы существующих угроз, шел процесс формирования новых…

Прогноз на 2013 год

В конце года мы, по традиции, оглядываемся назад и оцениваем то, как прожили это время, а также строим планы на будущее. Предлагаем вашему вниманию прогноз, в котором мы рассмотрим основные угрозы безопасности киберпространства в 2013 году. Но поскольку будущее — это всегда продолжение настоящего, начать можно с нашей статьи, посвященной основным тенденциям 2012 года.

1. Целевые атаки и кибершпионаж

В то время как в киберпространстве по-прежнему доминируют бессистемные атаки, направленные на кражу личной информации у случайных пользователей, целевые атаки стали в последние два года заметным явлением. Такие атаки проводятся с целью проникнуть в корпоративную сеть конкретной организации и зачастую связаны со сбором конфиденциальных данных, на которые имеется спрос на чёрном рынке. Зачастую целевые атаки являются весьма изощрёнными, однако в большинстве случаев все начинается с «человеческого фактора» — сотрудников организации обманом заставляют раскрыть информацию, чтобы затем с ее помощью получить доступ к корпоративным ресурсам.

Росту числа таких атак способствует огромный объём информации, публикуемой онлайн, и все более активное использование социальных медиа в бизнес-целях. Особенно уязвимыми оказываются сотрудники, занятые на «публичных» должностях — например, в сфере продаж или маркетинга. Можно ожидать, что в 2013 году (и далее) кибершпионаж будет становиться все более распространенным явлением. Если верить компьютерной прессе, может сложиться впечатление, что целевые атаки являются проблемой лишь для крупных организаций, особенно для тех, что обеспечивают работу критически важных объектов инфраструктуры своих стран. Однако мишенью злоумышленников может оказаться любая организация. Абсолютно все предприятия имеют дело с информацией, способной заинтересовать киберпреступников; при этом похищенные данные зачастую используются для того, чтобы подобраться к другим компаниям.

2. «Хактивисты» наступают

Кража средств с банковских счетов или похищение конфиденциальных данных с целью наживы — не единственные мотивы для проведения атак. Иногда целью служит привлечение внимания общественности к политической или социальной проблеме. В 2012 году в подобных атаках недостатка не было — достаточно вспомнить DDoS-атаки группы Anonymous на веб-сайты правительства Польши, сообщившего о своем намерении поддержать Международное соглашение по борьбе с контрафактной продукцией; взлом официального сайта Формулы-1 после разгона массовых антиправительственных протестов в Бахрейне; взлом сайтов нефтяных компаний в знак протеста против бурения в Арктике; атака на веб-сайт Saudi Aramco; взлом французского веб-сайта лотереи Euromillions в знак протеста против азартных игр.

Растущая зависимость общества от интернета делает любые организации потенциальными жертвами атак такого рода, так что «хактивизм», по всей вероятности, продолжится в 2013 году и далее.

3. Кибератаки, финансируемые государствами

Stuxnet стал первым случаем, когда весьма сложное вредоносное ПО использовалось для проведения целевых атак на ключевые производственные объекты. Хотя такие атаки и не являются широко распространенными, сейчас уже совершенно ясно, что инцидент со Stuxnet был далеко не единственным. Мы вступаем в эпоху «холодной кибервойны», когда страны могут воевать друг с другом, не будучи связанными существующими ограничениями на применение обычного, традиционного оружия.

Можно ожидать, что в дальнейшем кибероружие появится у большего числа стран и будет применяться как для кражи информации, так и для проведения диверсий. Немаловажным фактором здесь служит значительно бóльшая доступность разработки такого оружия по сравнению с обычным.

Также вероятно, что довольно скоро к подобным кибератакам будут прибегать страны, не имеющие статуса национальных государств. При этом косвенный ущерб может быть нанесен объектам, на которые атака не была направлена изначально. Жертвами таких атак могут стать центры управления энергетическими и транспортными системами, финансовые и телекоммуникационные системы, а также другие критически важные объекты инфраструктуры.

4. Использование средств слежения правоохранительными органами

В последние годы атаки киберпреступников становятся все более изощренными. Это бросает вызов не только специалистам по борьбе с киберугрозами, но и правоохранительным органам разных стран. В своем стремлении угнаться за технологическим развитием киберпреступности защитники правопорядка вторгаются в сферы, где отсутствует устоявшаяся правоприменительная практика.

Например, как поступить с заражёнными компьютерами после ликвидации ботнета? Этот вопрос пришлось решать ФБР после завершения операции GhostClick, о чем мы писали ранее.

Сюда же можно отнести использование современных технологий для слежки за лицами, подозреваемыми в преступной деятельности. Эта проблема отнюдь не нова — достаточно вспомнить полемику вокруг кейлоггера Magic Lantern, разработанного ФБР, и «федерального троянца» (BundesTrojan). Более свежий пример — горячая дискуссия, развернувшаяся после появления сообщений о том, что британская компания пыталась продать режиму Хосни Мубарака (Египет) программу для мониторинга под названием Finfisher, а также о том, что индийское правительство обратилось к ведущим производителям (в т.ч. Apple, Nokia и Research in Motion) с просьбой предоставить тайный доступ к мобильным устройствам пользователей.

Совершенно очевидно, что использование средств слежения правоохранительными органами поднимает вопросы, связанные с соблюдением гражданских прав и неприкосновенностью тайны частной жизни. Поскольку правоохранительные органы и правительства стран стараются быть на шаг впереди киберпреступников, можно ожидать, что применение подобных инструментов, а также полемика по этому поводу, в будущем будут продолжаться.

5. Облачно, вероятны вредоносные атаки

Очевидно, что использование облачных сервисов в ближайшие годы будет расширяться. Их развитию способствуют два фактора. Первый из них — значительная экономия средств для любого бизнеса за счёт эффекта масштаба при хранении данных или хостинге приложений в облаке. Второй фактор — гибкость: данные доступны в

любое время, из любой точки мира, с любого устройства (в т.ч. с ноутбука, планшета или смартфона). В то же время, по мере расширения использования облачных сервисов будет расти и количество нацеленных на них угроз.

Во-первых, облачные центры обработки данных — привлекательная мишень для киберпреступников. Слово «облако» ассоциируется у нас с чем-то белым и пушистым, но не следует забывать, что за ним стоят реальные физические серверы, на которых хранятся данные. С точки зрения киберпреступников они представляют собой потенциальную единую точку отказа. На таких серверах размещены большие объемы личных данных, которые, в случае успешной кибератаки на провайдера, могут целиком попасть в руки киберпреступников.

Во-вторых, велика вероятность того, что в будущем киберпреступники будут чаще использовать облачные сервисы для размещения и распространения вредоносных программ — как правило, с использованием «угнанных» аккаунтов.

В-третьих, обращение к данным, хранимым в «облаке», происходит с устройств, находящихся в реальном физическом мире. Получив доступ к такому устройству, киберпреступники получают доступ и к данным — где бы они ни хранились.

Широкое использование мобильных устройств представляет значительные преимущества для бизнеса, но при этом повышает уровень риска — доступ к данным, хранящимся в «облаке», возможен с мобильных устройств, которые зачастую не так надежно защищены, как обычные узлы сети. Риск ещё выше в том случае, когда одно и то же мобильное устройство используется как в личных целях, так и для решения бизнес-задач.

6. Кто украл мою частную жизнь?!

Утрата неприкосновенности тайны частной жизни — предмет горячих дебатов в IT-индустрии. Интернет проник во все сферы нашей жизни; многие ежедневно используют всемирную паутину для совершения банковских операций и покупок, а также для общения. Каждый раз, когда мы заводим новую учётную запись, мы вынуждены сообщить о себе определенную информацию. Этим пользуется множество компаний, активно собирающих данные о своих клиентах.

Угроза для тайны частной жизни может принимать две формы. Во-первых, личные данные подвергаются опасности в том случае, когда злоумышленники получают доступ к компьютерным системам компаний-поставщиков товаров и услуг. Сейчас практически каждую неделю мы слышим в новостях об очередном взломе сайта компании и утечке личных данных ее клиентов. Дальнейшее развитие облачных сервисов, несомненно, лишь усугубит эту проблему.

Во-вторых, компании собирают информацию о клиентах, причем зачастую без ведома последних. Эти данные затем используются для рекламы и продвижения товаров и услуг, и не всегда понятно, как отказаться от участия в этом процессе. В будущем ценность личных данных как для легального бизнеса, так и для киберпреступников будет лишь возрастать, а вместе с этим будет расти потенциальная угроза для тайны частной жизни.

7. Кому верить?

Представьте, что к вам в дверь позвонил незнакомый человек, представился сотрудником коммунальных служб и попросил его впустить. Вы, скорее всего, потребуете, чтобы он предъявил документы. Но что если он покажет вам подлинное служебное удостоверение, а затем окажется мошенником? Это ставит под вопрос основные принципы доверия, на которые мы опираемся, чтобы не стать жертвой злоумышленников.

Аналогичные принципы действуют и в киберпространстве. Мы склонны доверять веб-сайтам, имеющим сертификат безопасности, выданный известным центром сертификации, а также приложениям, подписанным с помощью действительного цифрового сертификата. К сожалению, киберпреступники теперь не только фабрикуют фальшивые сертификаты для вредоносного ПО (так называемые самозаверенные сертификаты), но и успешно взламывают серверы центров сертификации, чтобы затем заверять краденными сертификатами свой код. Использование поддельных и краденых сертификатов неизбежно будет продолжаться и далее.

Проблема может даже усугубиться: в последние годы к набору технологий для обеспечения IT-безопасности добавились так называемые «белые списки». Теперь дело не ограничивается сканированием программ на наличие вредоносного кода — они также проверяются по базам известного легитимного ПО. Поэтому, если вредоносные программы каким-то образом проникнут в «белые списки», защитные решения перестанут их детектировать.

Существует несколько путей попадания вредоносных программ в «белые списки». Вредоносная программа может быть заверена краденым сертификатом; если в «белые списки» автоматически добавляется ПО, подписанное данным центром сертификации, то вредоносная программа может быть включена в категорию доверенных. При другом сценарии киберпреступники (или кто-то внутри компании) могут получить доступ к директории или базе данных, содержащей «белые списки», и добавить туда вредоносное ПО. Инсайдер всегда представляет серьезную угрозу безопасности данных — как в физическом, так и в цифровом мире.

8. Кибервымогательство

В 2012 году выросло количество троянцев-вымогателей, которые шифруют данные на жёстком диске или блокируют доступ к системе на компьютерах жертв, а затем требуют заплатить выкуп. До недавних пор этот вид киберпреступности в основном ограничивался территорией России и других постсоветских государств. Однако теперь кибершантаж стал общемировым явлением, хотя его форма при этом несколько изменилась. Например, в России троянцы, блокирующие доступ к системе, часто сообщают, что они якобы обнаружили на компьютере жертвы нелицензионное ПО, и требуют заплатить за нарушение авторских прав.

В Европе, где пиратское ПО менее распространено, такой подход недостаточно эффективен, поэтому здесь троянцы-вымогатели выводят на экран всплывающее окно с сообщением (якобы от правоохранительных органов), что на компьютере жертвы обнаружена детская порнография или другой незаконный контент. За этим следует требование выплатить штраф. Подобные атаки легко проводить, и, как и в случае с фишинговыми атаками, недостатка в потенциальных жертвах не наблюдается. Соответственно, в будущем следует ожидать роста числа вредоносных программ такого типа.

9. Зловреды для Mac OS

Вопреки расхожим представлениям, компьютеры Mac не обладают абсолютным иммунитетом к вредоносным программам. Конечно, по сравнению с объемом вредоносного ПО, нацеленного на Windows, количество зловредов для Mac OS незначительно. С другой стороны, в последние 2 года оно неуклонно растёт; со стороны пользователей Mac было бы наивно полагать, что они защищены от атак киберпреступников на все 100%.

Речь идет не только о массовых угрозах (таких как ботнет Flashfake, состоявший из 700 000 заражённых компьютеров Mac); нам приходилось сталкиваться и с целевыми атаками на конкретных пользователей или группы пользователей Mac. Таким образом, угрозы для Mac вполне реальны, и в дальнейшем их число, скорее всего, будет только расти.

10. Мобильные зловреды

Последние полтора года количество мобильных зловредов резко возросло. При этом более 90% из них нацелены на устройства на базе Android. ОС Android отвечает всем «требованиям» киберпреступников: она популярна и для нее легко писать программы, которые пользователи могут с легкостью загружать из любых источников. Поэтому разработка вредоносных приложений для Android, скорее всего, будет продолжаться с той же интенсивностью.

На сегодняшний день большинство мобильных зловредов создаются с целью получить доступ к устройствам. В ближайшем будущем ожидается появление вредоносных программ, эксплуатирующих уязвимости в операционной системе, и, соответственно, использование drive-by загрузок. Велика вероятность разработки первого массового червя для Android, распространяющегося через текстовые сообщения со ссылками на копию зловреда, размещенную в каком-нибудь онлайн-магазине приложений. Скорее всего, мы также столкнемся с новыми мобильными ботнетами — аналогами созданного в первом квартале 2012 г. при помощи бэкдора RootSmart.

Напротив, iOS — это закрытая система с жесткими ограничениями, допускающая загрузку и использование приложений из единственного источника — AppStore. Это позволяет значительно повысить уровень безопасности: чтобы заразить вредоносным кодом устройства на базе iOS, вирусописателям приходится искать способы «протащить» свой код в AppStore. Появление в этом году приложения Find and Call доказывает, что шансы на успех у них есть. Однако в ближайшем будущем Android, скорее всего, продолжит быть основной мишенью киберпреступников. (Приложение Find and Call ставило под удар тайну частной жизни пользователей, а также их личные данные и репутацию: оно загружало из мобильного устройства на удаленный сервер базу контактов, адреса из которой затем использовались для рассылки SMS-спама.)

11. Уязвимости и эксплойты

Одним из ключевых способов, который используют киберпреступники для установки вредоносного ПО на компьютеры пользователей, является эксплуатация незакрытых уязвимостей в приложениях. Уязвимости в приложениях есть, а домашние пользователи или организации не устанавливают вовремя патчи. В данный момент более 50% атак направлены на Java-уязвимости, а 25% — на уязвимости в Adobe Reader.

Это неудивительно, поскольку большинство киберпреступников интересуются уязвимостями в популярных приложениях, редко обновляемых пользователями. Это даёт злоумышленникам время, необходимое для достижения своих целей. Java-приложения не только установлены на большом числе компьютеров (по данным Oracle, на 1,1 млрд машин), но и обновления для них устанавливаются по требованию, а не автоматически.

В связи с этим в будущем году киберпреступники продолжат эксплуатировать уязвимости в Java. По всей вероятности, Adobe Reader также будет «популярен» среди киберпреступников, однако в меньшей степени, поскольку в последних версиях этой программы реализована автоматическая установка обновлений.

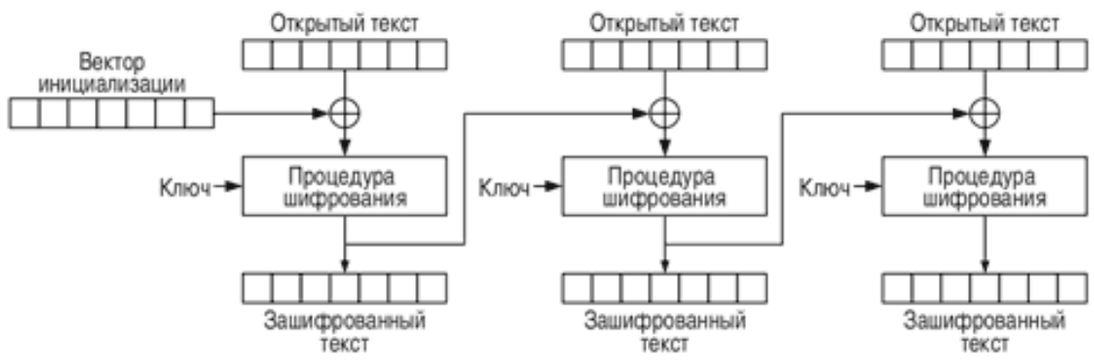
Источник: http://www.securelist.com

Lucky 13: новый метод атаки на TSL и DTLS

Разработчики многих библиотек SSL, в том числе OpenSSL, NSS, GnuTLS, yaSSL, PolarSSL, Opera и BouncyCastle выпустили или готовятся выпустить патчи, чтобы устранить уязвимость, которая потенциально позволяет извлечь конфиденциальную информацию из зашифрованного канала связи, в том числе пароли и аутентификационные cookies.

Выпуску патчей предшествовала публикация отчёта с описанием нового метода атакина реализации SSL, TLS и DTLS, использующие режим сцепления блоков шифротекста (CBC). Уязвимость связана именно с недоработкой в спецификациях TLS, а не с конкретными реализациями, поэтому баг присутствует во всех библиотеках.

Режим сцепления блоков шифротекста (Cipher Block Chaining) — один из режимов шифрования для симметричного блочного шифра с использованием механизма обратной связи. Каждый блок открытого текста (кроме первого) побитово складывается по модулю 2 (операция XOR) с предыдущим результатом шифрования.



Новый метод атаки разработали криптологи из Royal Holloway College при Лондонском университете. Заблаговременно уведомив всех ведущих разработчиков SSL/TLS-библиотек и оказав им помощь в выпуске патчей, исследователи опубликовали в открытом доступе подробное описание атаки, которую они назвали “Lucky 13”.

Новый метод использует хорошо известную атаку типа padding oracle, подменяя шифротекст и анализируя задержку при ответе. Атака мало применима на практике, потому что требует весьма специфических условий от клиента и сервера. Например, злоумышленник должен находиться в одной локальной сети с сервером.

Источник: http://www.xakep.ru

Kaspersky Security Bulletin 2012. Основная статистика за 2012 году.

Эксперт в области безопасности.

Эта часть отчета является частью Kaspersky Security Bulletin 2012 и сформирована на основе данных, полученных и обработанных при помощи Kaspersky Security Network. KSN использует «облачную» архитектуру в персональных и корпоративных продуктах и является одной из важнейших технологий «Лаборатории Касперского».

Kaspersky Security Network позволяет нашим экспертам оперативно, в режиме реального времени обнаруживать новые вредоносные программы, для которых еще не существует сигнатурного или эвристического детектирования. KSN помогает выявлять источники распространения вредоносных программ в интернете и блокировать доступ пользователей к ним.

Одновременно KSN позволяет реализовать значительно большую скорость реакции на новые угрозы — в настоящее время мы можем блокировать запуск новой вредоносной программы на компьютерах пользователей через несколько десятков секунд с момента принятия решения о ее вредоносности, и это осуществляется без обычного обновления антивирусных баз.

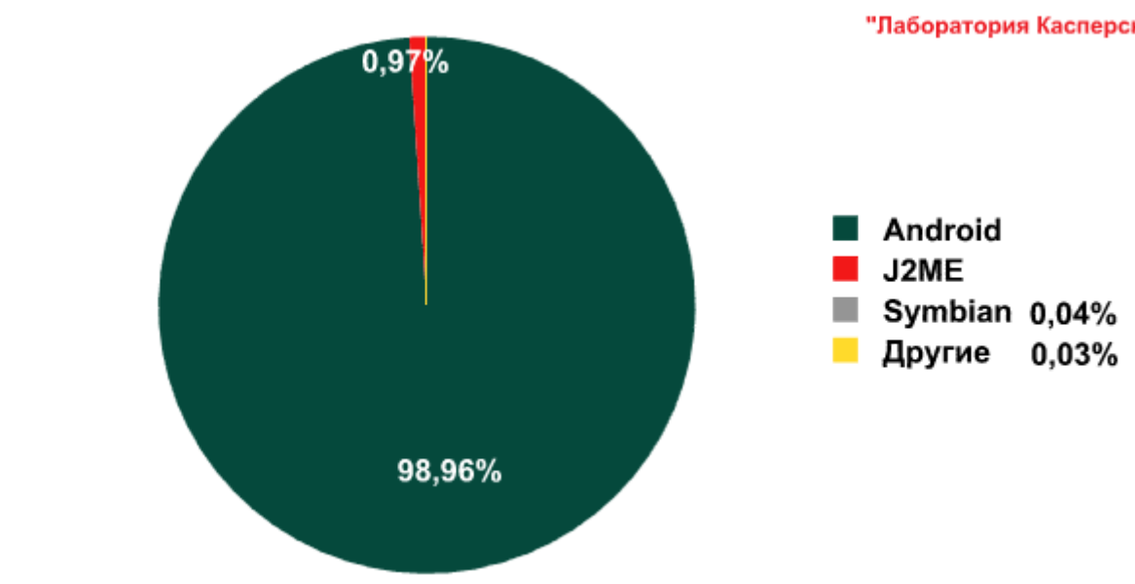
Статистика в отчете основана на данных, полученных от продуктов «Лаборатории Касперского», пользователи которых подтвердили свое согласие на передачу статистических данных.

Мобильные угрозы

Развитие мобильных угроз в 2012 году прошло под девизом «Все внимание — на Android». Вирусописатели, в основном, сконцентрировались на «зеленом роботе». Оправдались и наши прогнозы по развитию мобильных угроз в 2012 году, касающиеся создания мобильных ботнетов, целевых атак с использованием мобильных зловредов и «мобильного» шпионажа.

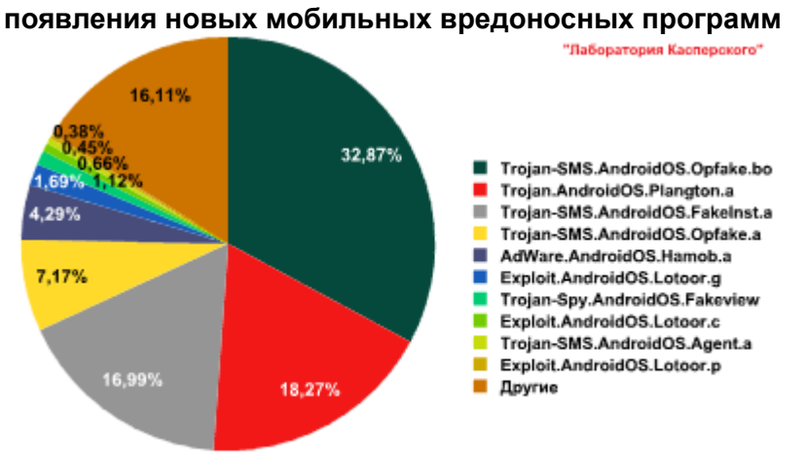
Вредоносные программы для Android

В 2012 году усилия вирусописателей были направлены в основном на создание вредоносных программ для Android. Это привело как к качественному, так и количественному росту мобильных зловредов под эту платформу. 99% обнаруживаемых нами ежемесячно зловредов для мобильных платформ были нацелены на Android.



Распределение мобильных зловредов по платформам

Динамика появления новых мобильных вредоносных программ по месяцам



TOP 10 зловредов для Android

Наиболее распространенные детектируемые объекты на Android-смартфонах можно разделить на 3 основные группы: SMS-троянцы, рекламные модули и эксплойты для получения прав root на смартфоне.

Самыми распространенными из них оказались SMS-троянцы, которые нацелены, в основном, на пользователей из России. В этом нет ничего удивительного, учитывая давнюю популярность подобных вредоносных программ среди российских вирусописателей. Дорогостоящие SMS-сообщения остаются способом заработка №1 среди "мобильных" киберпреступников.

Вторую группу мобильных угроз из TOP 10 составляют рекламные модули Plangton и Hamob. Первое семейство не зря детектируется как Trojan. Plangton встречается в бесплатных приложениях и действительно показывает рекламу, однако в нем имеется еще и функционал смены стартовой страницы браузера. Стартовая страница при этом меняется без предупреждения и согласия пользователя, что считается вредоносным поведением. Что же касается Hamob, то как AdWare.AndroidOS.Hamob детектируются приложения, которые выдают себя за какие-либо полезные программы, а на самом деле лишь показывают рекламу пользователю.

И, наконец, третья группа. К ней относятся различные модификации эксплойтов для получения прав root на смартфонах с ОС Android различных версий.

Такая популярность эксплойтов обусловлена, в частности, тем, что разнообразные модификации бэкдоров из разных семейств, число которых за последний год выросло, используют одни и те же модификации эксплойтов для повышения привилегий (прав root на устройстве).

Рост числа инцидентов с вредоносными программами в официальных магазинах приложений

Несмотря на то, что Google внедрил антивирусный модуль Google Bouncer, осуществляющий автоматическую проверку всех новых приложений на Google Play (бывший Android Market), существенных изменений в среднем количестве инцидентов и их масштабах не произошло. Внимание общественности обычно привлекают случаи с наибольшим количеством заражений, как, например, инцидент с вредоносной программой Dougalek, копии которой загрузили десятки тысяч пользователей (в основном, из Японии). Это привело к одной из наиболее масштабных утечек персональной информации пользователей в результате заражения мобильных устройств. Однако не стоит забывать и о сотнях инцидентов с меньшим количеством пострадавших.

Отметим также первый случай обнаружения вредоносного ПО в App Store для iOS. В самом начале июля было обнаружено подозрительное приложение под именем «Find and Call», копии которого были найдены как в App Store, так и на Android Market. Загрузив и запустив данную программу, пользователь сталкивался с запросом на регистрацию в программе, для чего было необходимо ввести e-mail и телефонный номер. После регистрации введенные данные и телефонная книга жертвы скрытно отправлялись на удаленный сервер.

```
_text:000146E8 __RootViewController_sendPhoneBook__
_text:000146E8
_text:000146E8 var_C           = -0xC
_text:000146E8
_text:000146E8                 PUSH            {R4,R5,R7,LR}
_text:000146EA                 ADD             R7, SP, #8
_text:000146EC                 SUB             SP, SP, #4
_text:000146EE                 LDR             R1, =(mainBundle - 0x146F8)
_text:000146F0                 MOV             R4, R0
_text:000146F2                 LDR             R0, =(_NSBundle - 0x146FC)
_text:000146F4                 ADD             R1, PC
_text:000146F6                 SXTB            R5, R2
_text:000146F8                 ADD             R0, PC
_text:000146FA                 LDR             R1, [R1]
_text:000146FC                 LDR             R0, [R0]
_text:000146FE                 BLX             _objc_msgSend
_text:00014702                 LDR             R1, =(localizedStringForKey_value_table - 0x1470C)
_text:00014704                 LDR             R2, =(cfstr_Findfriends_se - 0x1470E)
_text:00014706                 LDR             R3, =(stru_8B740 - 0x14710)
_text:00014708                 ADD             R1, PC
_text:0001470A                 ADD             R2, PC  ; "findfriends_send_phonebook_message"
_text:0001470C                 ADD             R3, PC
_text:0001470E                 LDR             R1, [R1]
_text:00014710                 MOV.W           R12, #0
_text:00014714                 STR.W           R12, [SP,#0xC+var_C]
_text:00014718                 BLX             _objc_msgSend
_text:0001471C                 LDR             R1, =(off_A18AC - 0x14724)
_text:0001471E                 MOVS            R2, #1
_text:00014720                 ADD             R1, PC
```

Часть процедуры загрузки телефонной книги на удаленный сервер

На каждый украденный номер из телефонной книги через какое-то время придет SMS-спам сообщение с предложением перейти по ссылке и загрузить приложение «Find and Call».

Первые мобильные ботнеты

Первым «звоночком» стало обнаружение в самом начале года IRC-бота для Android с именем Foncy, который работал в связке с SMS-троянцем с таким же именем. Именно IRC-бот мог управлять смартфоном после заражения. Ведь помимо SMS-троянца в APK-дроппере содержался также и root-эксплойт, использовавшийся для повышения привилегий в зараженной системе. А после соединения с командным сервером бот был способен получать и исполнять shell-команды. Фактически, все зараженные IRC-ботом Foncy смартфоны составляли полноценный ботнет и были готовы осуществлять практически любые действия по команде «хозяина».

Китайским вирусописателям удалось создать ботнет, число активных устройств которого варьировало от 10 000 до 30 000, при этом общее число зараженных смартфонов исчислялось сотнями тысяч. Основой этого ботнета стал бэкдор RootSmart, который имеет разнообразный функционал для удаленного управления мобильным устройством с ОС Android. Для распространения RootSmart киберпреступники положились на известный и действенный прием: перепаковали легальную программу и выложили ее на сайт одного из неофициальных, но очень популярных в Китае магазинов приложений для Android. В результате пользователи, скачавшие программу якобы для настройки телефона, получили вместе с ней бэкдор, включавший их устройство в ботнет.

Масштабы заражения RootSmart позволили злоумышленникам эффективно монетизировать созданную сеть из зараженных телефонов. Для этого они выбрали самый популярный у мобильных киберпреступников способ — отправку платных

SMS-сообщений на короткие номера. Злоумышленники использовали самые дешевые номера для того, чтобы жертвы как можно дольше не замечали потери средств. Полный контроль над мобильными устройствами, который получили злоумышленники, давал им возможность длительное время скрывать присутствие вредоносной программы на телефоне и дольше выкачивать деньги со счетов.

Точечные атаки с использованием мобильных зловредов

В 2012 году некоторые новые зловреды для ОС, отличных от Android, использовались для точечных атак.

Ярким примером таких атак являются атаки с помощью ZitMo и SpitMo (Zeus- и SpyEye-in-the-Mobile). Новые версии ZitMo и SpitMo появлялись регулярно, как для Android, так и для других операционных систем. Вирусописатели по-прежнему используют те же способы маскировки зловредов, что и два года назад. Это либо маскировка под «сертификаты безопасности», либо под программное обеспечение для защиты смартфонов.

Традиционные способы маскировки ZitMo/SpitMo

Несмотря на то, что операционные системы, отличные от Android, не настолько популярны, это вовсе не значит, что ими уже никто не пользуется. Вирусописателям, например, нет никакого дела до слухов о возможной скорой смерти платформы Blackberry. В 2012 году новые версии ZitMo появлялись и для этой платформы, причем в одной волне атак злоумышленники использовали как зловреды для Blackberry, так и для Android. По крайней мере, C&C номера в них были одними и теми же.

Шпионаж с использованием мобильных вредоносных программ

В прошлом году мы предположили, что кража данных с мобильных телефонов и слежка за объектом при помощи его телефона и геолокационных сервисов станет распространенным явлением и выйдет за пределы обычного применения этих технологий правоохранительными органами и отдельными компаниями, которые занимаются детективной деятельностью.

К сожалению, так и произошло. Количество вредоносных программ, которые по своему поведению являются либо троянцами-шпионами, либо бэкдорами, выросло в сотни раз. Стоит отметить также возросшее количество коммерческих приложений для мониторинга, которые иногда сложно отличить от вредоносных программ.

Наиболее ярким примером шпионажа с использованием мобильных вредоносных программ служит инцидент с программным модулем FinSpy. Данный модуль был разработан британской компанией Gamma International, которая специализируется на создании программных средств мониторинга для правительственных организаций. Фактически, эта программа обладает функционалом троянца-шпиона. Обнаружить мобильные версии FinSpy удалось компании The Citizen Lab в августе 2012 года. Были найдены модификации троянца под платформы Android, iOS, Windows Mobile и Symbian. Различия между ними, безусловно, есть, но все они способны логировать практически любую активность пользователей на зараженном устройстве, отслеживать его координаты, осуществлять скрытные звонки, загружать информацию на удаленные серверы.

Ответов на вопросы о заказчиках атак FinSpy и конкретных жертвах на данный момент нет, и вряд ли ответы появятся в будущем. Однако даже без этой информации появление FinSpy означает начало новой главы в истории мобильного вредоносного ПО: мобильные устройства становятся такими же мишенями целевых и шпионских атак, как и обычные компьютеры.

Мас-зловреды

В 2012 году все мифы о безопасности Mac были разрушены. Этот год показал, что Mac-зловреды являются действительно серьёзной угрозой безопасности.

В начале года был обнаружен 700-тысячный ботнет Flashfake, состоявший исключительно из Mac-компьютеров. (Полный разбор этого троянца-загрузчика был опубликован на securelist.com.

Новых волн эпидемий после FlashFake не последовало, но зато злоумышленники в течение всего года активно использовали Mac-зловреды для проведения целевых атак. Это в первую очередь связано с тем, что продукты компании Apple пользуются популярностью у многих влиятельных политических деятелей и крупных бизнесменов, и информация, хранящаяся на устройствах этих людей, представляет интерес для определенной категории киберзлоумышленников.

В 2012-м году нашими антивирусными экспертами было добавлено на 30% больше сигнатур для детектирования различных Mac-троянцев, чем в 2011; если же сравнивать с 2010 годом, то количество сигнатур, добавленных за год, увеличилось в 6 раз.

Самым распространенным Mac-зловредом года, безусловно, можно считать FlashFake, первые версии которого были обнаружены еще в 2011 году. По итогам первого полугодия 2012 FlashFake стал абсолютным лидером. Давайте посмотрим, какие OSX-зловреды были распространены во втором полугодии 2012 года.

Количество новых антивирусных записей, добавляемых ежегодно для детектирования зловредов под Mac OS X

TOP 10 зловредов для Mac OS X, H2 2012

Место	Название	% от всех атак
1	Trojan.OSX.FakeCo.a	52%
2	Trojan-Downloader.OSX.Jahlav.d	8%
3	Trojan-Downloader.OSX.Flashfake.ai	7%
4	Trojan-Downloader.OSX.FavDonw.c	5%
5	Trojan-Downloader.OSX.FavDonw.a	2%
6	Trojan-Downloader.OSX.Flashfake.ab	2%
7	Trojan-FakeAV.OSX.Defma.gen	2%
8	Trojan-FakeAV.OSX.Defma.f	1%
9	Exploit.OSX.Smid.b	1%
10	Trojan-Downloader.OSX.Flashfake.af	1%

На первом месте Trojan.OSX.FakeCo.a (52%). Эта вредоносная программа маскируется под установочный файл видеокодека. После инсталляции никаких кодеков в системе не появляется, а установленная программа ведет себя как программа категории AdWare, собирая интересную для маркетинга информацию о пользователе и отсылая ее злоумышленникам.

Второе место в списке занял известный уже четыре года троянец Jahlav (8%). Вредоносная программа также маскируется под установочный файл видеокодека. Вместо кодека на компьютер устанавливается зловред, который незаметно для пользователя подключается к серверу злоумышленников и может с него загружать на зараженную машину другие файлы. Как правило, эта вредоносная программа пытается загрузить троянца, который меняет адреса в настройках DNS на адреса серверов злоумышленников (детектируется «Лабораторией Касперского» как Trojan.OSX.Dnscha).

На четвертом и пятом местах расположились программы семейства Trojan-Downloader.OSX.FavDonw, на которые в сумме пришлось 7% инцидентов. Программы служат лишь одной цели: после установки на Mac они скачивают лжеантивирусы.

На 7-м и 8-м местах в TOP 10 расположились фальшивые антивирусы семейства Trojan-FakeAV.OSX.Defma, которые вымогают у пользователей деньги за лечение якобы обнаруженных вредоносных программ.

На 9-м месте расположился эксплойт Exploit.OSX.Smid.b, нацеленный на уязвимость в Java и позволяющий злоумышленнику запустить произвольных код на машине с необновлённой Java.

После обнаружения ботнета FlashFake компания Apple активнее занялась вопросами безопасности своей операционной системы. Примерами могут служить и выпуски критических патчей для Oracle Java одновременно с их Windows-версиями, и новые защитные функции в Mac OS X Mountain Lion: по умолчанию возможность установки программ только из официального магазина, использование песочницы для программ, загруженных из магазина, автоматическая установка обновлений и т.д.

Вредоносные программы в интернете (атаки через Web)

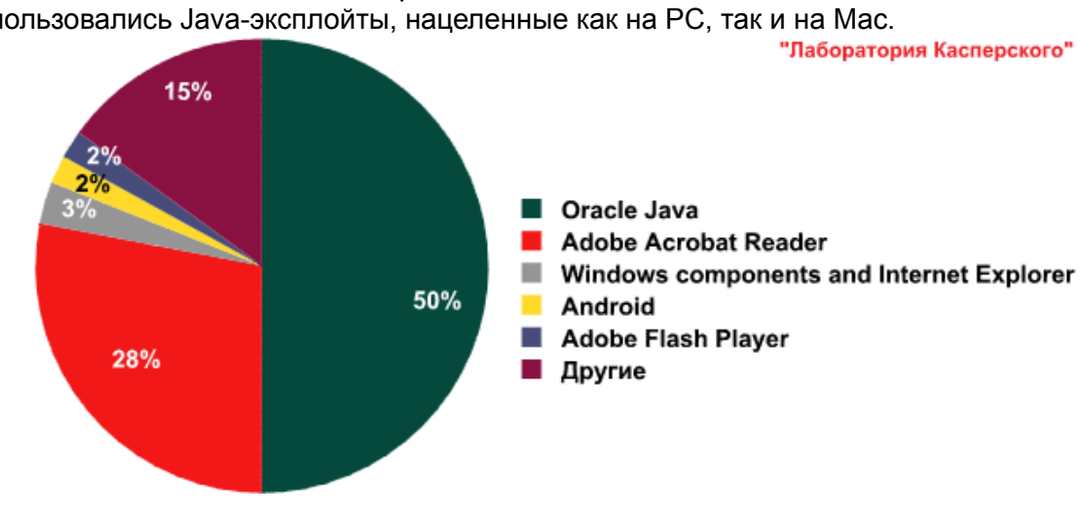
Количество атак через веб-браузер за год увеличилось с 946 393 693 до 1 595 587 670. Таким образом, наши продукты защищали пользователей при серфинге в интернете в среднем 4 371 473 раз в день.

По сравнению с прошлым годом темпы роста числа атак через браузер практически не изменились. Число отраженных в 2012 году интернет-атак превышает аналогичный показатель 2011 года в 1,7 раза, а в 2011 году мы зафиксировали рост в 1,6 раз. Основной способ атаки — через эксплойт-паки — дает злоумышленникам практически гарантированную возможность заражения компьютеров, если на них не установлена защита и имеется хотя бы одно популярное и уязвимое (не обновленное) приложение.

Уязвимые приложения, используемые злоумышленниками

Если 2011 год мы назвали годом уязвимостей, то 2012 можно смело назвать годом Java-уязвимостей: в этом году половина всех зафиксированных атак с использованием эксплойтов была нацелена на уязвимости в Oracle Java.

Сегодня Java установлена более чем на 3 миллиардах устройств, использующих различные ОС. Следовательно, для некоторых ошибок в Java можно создать кроссплатформенные эксплойты. В течение года мы регистрировали как массовые атаки с использованием наборов эксплойтов, так и целевые атаки, в которых использовались Java-эксплойты, нацеленные как на PC, так и на Mac.



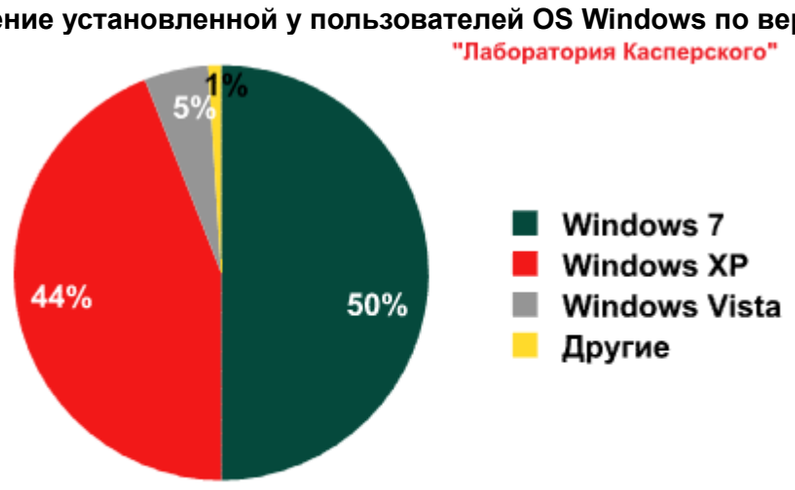
Приложения, уязвимости в которых использовали веб-эксплойты

В 2012 году снизилась популярность эксплойтов к Adobe Reader — с ними было связано 28% всех инцидентов. В итоге Adobe Reader заняла второе место в рейтинге. Заметим, что в последних версиях Adobe Reader было уделено много внимания проблеме уязвимостей, в частности, были реализованы механизмы, защищающие приложение от срабатывания эксплойта. Подобные меры значительно усложняют создание эффективных эксплойтов.

На третьем месте расположились программы, использующие уязвимости в компонентах Windows и Internet Explorer. В течение года активно использовались эксплойты к уязвимостям, обнаруженным еще в 2010 году: MS10-042 в Windows Help and Support Center и MS04-028, связанной с неправильной обработкой jpeg-файлов.

На 4-м месте с 2% расположились эксплойты для мобильной платформы Android OS. Эти эксплойты злоумышленники используют, чтобы получить root-привилегии, которые дают практически неограниченные возможности для манипуляций над системой.

Распределение установленной у пользователей OS Windows по версиям, 2011



Распределение установленной у пользователей OS Windows по версиям, 2012

За год доля Windows 7 среди используемых пользователями Windows версий OS выросла с 30% до 50%. Хотя Windows 7 регулярно автоматически обновляется, атаки на компьютеры пользователей Windows продолжаются: как мы писали выше, проникновения в систему, происходят в основном не через компоненты Windows, а через установленные приложения других производителей.

Вредоносные программы в интернете: TOP 20

Из всех вредоносных программ, участвовавших в интернет-атаках на компьютеры пользователей, мы выделили 20 наиболее активных. На них пришлось 96% всех атак в интернете.

Место	Название*	Количество атак	% от всех атак**
1	Malicious URL	1 393 829 795	87,36%
2	Trojan.Script.Iframer	58 279 262	3,65%
3	Trojan.Script.Generic	38 948 140	2,44%
4	Trojan.Win32.Generic	5 670 627	0,36%
5	Trojan-Downloader.Script.Generic	4 695 210	0,29%
6	Exploit.Script.Blocker	4 557 284	0,29%
7	Trojan.JS.Popupper.aw	3 355 605	0,21%
8	Exploit.Script.Generic	2 943 410	0,18%
9	Trojan-Downloader.SWF.Voleydaytor.h	2 573 072	0,16%
10	AdWare.Win32.IBryte.x	1 623 246	0,10%
11	Trojan-Downloader.Win32.Generic	1 611 565	0,10%
12	AdWare.Win32.ScreenSaver.e	1 381 242	0,09%
13	Trojan-Downloader.JS.Iframe.cxk	1 376 898	0,09%
14	Trojan-Downloader.JS.Iframe.cyq	1 079 163	0,07%
15	Trojan-Downloader.JS.Expack.sn	1 071 626	0,07%
16	AdWare.Win32.ScreenSaver.i	1 069 954	0,07%
17	Trojan-Downloader.JS.JScript.ag	1 044 147	0,07%
18	Trojan-Downloader.JS.Agent.gmf	1 040 738	0,07%
19	Trojan-Downloader.JS.Agent.gqu	983 899	0,06%
20	Trojan-Downloader.Win32.Agent.gyai	982 626	0,06%

** Детектирующие вердикты модуля веб-антивируса. Информация предоставлена пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.*

*** Процент от всех веб-атак, которые были зафиксированы на компьютерах уникальных пользователей.*

Вредоносные сайты, обнаруженные с помощью облачных эвристических методов детектирования без обновления классических антивирусных баз, занимают первую строчку рейтинга. Развитие новых технологий детектирования, опирающихся на возможности KSN, позволило за год увеличить долю угроз, обнаруживаемых такими методами, с 75% до 87%. Значительная часть детектов Malicious URL приходится на сайты с эксплойтами.

На втором месте — вредоносные скрипты, внедряемые злоумышленниками в код взломанных легитимных сайтов с помощью специальных программ. Это говорит о том, что на многих легитимных сайтах присутствуют инъекции вредоносного кода в виде неотображаемых тегов «iframe». Такие скрипты незаметно для пользователя перенаправляют его на вредоносные веб-ресурсы в ходе drive-by атак. Аналогичные вредоносные скрипты разместились на 13-м и 14-м местах.

Позиции с 3-й по 5-ю занимают различные эвристические вердикты, детектирующие вредоносные скрипты и исполняемых PE-файлы, которые можно разделить на два категории. Зловреды первой категории осуществляют загрузку и исполнение других вредоносных программ. Вредоносные объекты второй категории несут саму «полезную» нагрузку — воруют данные интернет-банкинка, аккаунты к социальным сетям, сервисам и тому подобное.

На 9-м месте Trojan-Downloader.SWF.Voleydaytor.h, который обнаруживается на различных сайтах категории «18+». Под видом обновления программы просмотра видео на компьютеры пользователей доставляются различные вредоносные программы.

В рейтинге присутствуют два представителя эксплойтов — Exploit.Script.Generic, загрузка которого была заблокирована почти в 3 миллионах случаев, и Exploit.Script.Bloker — 4,5 миллиона заблокированных попыток загрузки. В абсолютном большинстве случаев пользователи сталкиваются с работой не отдельно взятых эксплойтов, а наборов эксплойтов. Они являются на сегодняшний день неотъемлемой частью drive-by атак. Что важно, эксплойт-паки оперативно модифицируются и обновляются, чтобы включать эксплойты для свежих уязвимостей и эффективно противодействовать средствам защиты.

Три позиции из TOP 20 заняли рекламные программы семейств iBryte и ScreenSaver. Рекламная программа AdWare.Win32.IBryte.x распространяется как загрузчик популярных бесплатных программ. После запуска она загружает нужную пользователю бесплатную программу и заодно устанавливает рекламный модуль. С тем же успехом установленную IBryte.x программу пользователь может скачать с официального сайта и избежать установки рекламного модуля. В прошлом году представителей AdWare было в два раза больше. Сокращение доли таких программ связано с постепенным вытеснением их различными более эффективными и, что самое главное, легальными методами показа рекламы, такими как контекстная реклама в поисковых системах и социальных сетях.

В отличие от 2011 года в рейтинге нет программ, используемых в мошенничестве с короткими номерами, — Hoax.Win32.ArchSMS. Это программы, требующие отправить SMS на короткий номер для получения кода расшифровки содержимого архива, скаченного пользователем. В 2011 году мошенники создавали сайты, похожие на обычные файловые хранилища, однако в предлагаемых архивах не было указанного содержимого. В 2012 году мошенники стали активно создавать сайты, которые дают возможность реализовать аналогичную схему мошенничества без загрузки каких-либо файлов на диск. Такие сайты автоматически заносятся продуктами «Лаборатории Касперского» в черный список.

Страны, на веб-ресурсах которых размещены вредоносные программы: TOP 20

Для проведения **1 595 587 670** атак через интернет злоумышленники воспользовались 6 537 320 уникальными хостами, что на два с половиной миллиона больше, чем в 2011 году. Серверы, на которых был размещен вредоносный код, были обнаружены в **202** странах и территориях мира.**96,1%** всех зафиксированных нами в Сети атак были произведены с вредоносных хостингов расположенных в интернет-пространстве двадцати стран.

Место	Страна*	Количество атак**	% от всех атак
1	США	413 622 459	25,5%
2	Россия	317 697 806	19,6%
3	Нидерланды	271 583 924	16,8%
4	Германия	184 661 326	11,4%
5	Великобритания	90 127 327	5,6%
6	Украина	71 012 583	4,4%
7	Франция	56 808 749	3,5%
8	Китай	31 637 561	2,0%
9	Британские Виргинские острова	26 593 331	1,6%
10	Канада	19 316 279	1,2%
11	Чешская Республика	13 311 441	0,8%
12	Израиль	9 953 064	0,6%
13	Швеция	9 093 053	0,6%
14	Румыния	6 881 404	0,4%
15	Вьетнам	6 624 570	0,4%
16	Испания	6 543 135	0,4%
17	Польша	6 325 848	0,4%
18	Люксембург	5 669 370	0,3%
19	Ирландия	4 854 163	0,3%
20	Латвия	4 685 861	0,3%

Настоящая статистика основана на детектирующих вердиктах модуля веб-антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.

** Для определения географического источника атаки используется методика сопоставления доменного имени к реальному IP-адресу, на котором размещен данный домен, и установление географического местоположения данного IP-адреса (GEOIP).*

*** Суммарное число зафиксированных веб-антивирусом уникальных атак с веб-ресурсов, размещенных в стране.*

Первые две позиции в рейтинге занимают США (25,5%) и Россия(19,6%). Нидерланды (16,8%) и Германия(11,4%) стабильно находятся в пятерке стран-лидеров и третий год подряд занимают в рейтинге 3-ю и 4-ю позиции соответственно. Если показатель США за год увеличился всего на 0,1%, то в России (+5%), Голландии (+7%) и Германии (+2,7%) доля вредоносных хостингов значительно увеличилась.

До 2010 года первое место в рейтинге занимал Китай, на серверы которого приходилось более 50% всех вредоносных хостингов мира. В 2010 году властям Китая удалось убрать из локального киберпространства множество вредоносных хостингов, в то же время были ужесточены правила регистрации доменов в зоне .cn. После этого доля вредоносных хостингов в Китае резко сократилась, и мы наблюдаем постепенную консолидацию хостингов в США, России, Нидерландах и Германии.

Стабильный рост показателя России имеет две причины. Во-первых, взломы легитимных сайтов, в том числе крупнейших порталов зоны .ru, с целью заражения компьютеров пользователей через эксплойты, увы, не редкость. Второй причиной является тот факт, что российские киберпреступники чувствуют себя в российском киберпространстве достаточно вольготно и создают множество вредоносных сайтов. По российским законам наказания за киберпреступления достаточно мягкие (в основном, преступникам дают условные строки), а случаи отключения командных серверов ботнетов в России достаточно редки. Если темпы роста доли вредоносных хостингов, приходящихся на российские серверы, сохранятся на текущем уровне, Россия может выйти на первое место по количеству вредоносных хостингов уже в следующем году.

В Голландии и Германии киберпреступники действуют куда аккуратнее — регистрируют или взламывают огромное количество сайтов, а когда адреса вредоносных сайтов попадают в черные списки провайдеров, оперативно переносят вредоносный контент с одних серверов на другие.

Локальные угрозы

Исключительно важным показателем является статистика локальных заражений пользовательских компьютеров. В эти данные попадают объекты, которые проникли на компьютеры не через Web, почту или сетевые порты.

Наши антивирусные решения успешно обнаружили почти 3 миллиарда вирусных инцидентов на пользовательских компьютерах, участвующих в Kaspersky Security Network.

Всего в данных инцидентах было зафиксировано **2,7 миллиона** разных вредоносных и потенциально нежелательных программ.

Вредоносные объекты, обнаруженные на компьютерах пользователей: TOP 20

Вредоносные программы, попавшие в первую двадцатку, являются самыми распространенными угрозами 2012 года.

Место	Детектируемый объект	Кол-во уникальных пользователей*	%%
1	Trojan.Win32.Generic	9 761 684	22,1%
2	DangerousObject.Multi.Generic	9 640 618	21,9%
3	Trojan.Win32.AutoRun.gen	5 969 543	13,5%
4	Trojan.Win32.Starter.yy	3 860 982	8,8%
5	Virus.Win32.Virut.ce	3 017 527	6,8%
6	Net-Worm.Win32.Kido.ih	2 752 409	6,2%
7	Net-Worm.Win32.Kido.ir	2 181 181	4,9%
8	Virus.Win32.Sality.aa	2 166 907	4,9%
9	Hoax.Win32.ArchSMS.gen	2 030 664	4,6%
10	Virus.Win32.Generic	2 017 478	4,6%
11	Virus.Win32.Nimnul.a	1 793 115	4,1%
12	HiddenObject.Multi.Generic	1 508 877	3,4%
13	Trojan.WinLNK.Runner.bl	1 344 989	3,1%
14	Worm.Win32.AutoRun.hxw	948 436	2,2%
15	Virus.Win32.Sality.ag	841 994	1,9%
16	Virus.Win32.Suspic.gen	408 201	0,9%
17	Trojan.Win32.Patched.dj	367 371	0,8%
18	Email-Worm.Win32.Runouce.b	295 887	0,7%
19	Trojan-Dropper.Script.Generic	232 007	0,5%
20	AdWare.Win32.GoonSearch.b	196 281	0,4%

Настоящая статистика представляет собой детектирующие вердикты модуля антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.
** Число уникальных пользователей, на компьютерах которых антивирус детектировал данный объект.*

На 13,5 миллионах компьютеров были заблокированы попытки заражения, обнаруженные с помощью различных эвристических методов: Trojan.Win32.Generic (1-е место), Virus.Win32.Generic (8-е место), HiddenObject.Multi.Generic (12-е место), Trojan-Dropper.Script.Generic (19-е место).

Второе место в рейтинге занимают различные вредоносные программы, обнаруженные с помощью облачных технологий и детектируемые как DangerousObject.Multi.Generic. Эти технологии работают, когда в антивирусных базах еще нет ни сигнатуры, ни эвристики для детектирования вредоносной программы, но в облаке антивирусной компании уже есть информация об объекте. По сути, так детектируются самые новые вредоносные программы. При помощи системы мгновенного обнаружения угроз UDS, работающей в составе Kaspersky Security Network, более 9,6 млн. компьютеров пользователей были защищены в режиме реального времени.

8 программ из TOP 20 либо имеют механизм самораспространения, либо используются как одна из составляющих в схеме распространения червей: Trojan.Win32.Starter.yy (4-е место), Net-Worm.Win32.Kido.ih (6-е место), Net-Worm.Win32.Kido.ir (7-е место), Virus.Win32.Sality.aa (8-е место), Virus.Win32.Nimnul.a (11 место), Virus.Win32.Sality.ag (15-е место) и Virus.Win32.Suspic.gen (16-место).

В 2012 году более 2 миллионов пользователей столкнулись с мошенничеством с использованием коротких SMS-номеров (Hoax.Win32.ArchSMS.gen, 9-е место). Под различными предлогами, в основном обещая доступ к содержимому архива или инсталлятора с игрой, программой, книгой или чем-то подобным, злоумышленники пытаются вынудить пользователей отправить SMS на короткий премиум-номер. В большинстве случаев после отправки сообщения пользователь ничего не получает взамен.

Trojan.WinLNK.Runner.bl (13 место) и Worm.Win32.AutoRun.hxw (14 место) являются детектами вредоносных lnk-файлов (ярлыков). В lnk-файлах данных семейств производится выполнение cmd.exe с параметром запуска вредоносного exe-файла. Они активно используются червями для распространения через usb-накопители.

Интересным представителем является Trojan.Win32.Patched.dj (17 место). Это детект зараженных exe и dll файлов. Вредоносный функционал сводится к отсылке по почте вирусописателю информации о заражении, после чего программа открывает порт на компьютере и ожидает команды хакера, который может загружать файлы, запускать их, останавливать запущенные на компьютере программы и т.д. В конечном итоге зловред используется для построения ботнета.

Методы заражения активно эволюционируют и сегодня мы видим, что в топ не попало ни одно новое семейство вирусов и червей: правят бал Sality, Virut, прошлогодний Nimnul и Kido. Киберпреступники массово переключились на создание ботнетов через интернет-заражения с использованием эксплойтов. Техники заражения исполняемых файлов не пользуются популярностью у коммерчески-ориентированных вирусописателей в силу того, что процесс самораспространения вирусов и червей контролировать очень сложно, а большие ботнеты быстро привлекают внимание правоохранительных органов.

«Картина мира»

Чтобы оценить, в каких странах пользователи чаще всего сталкиваются с киберугрозами, для каждой из стран мы подсчитали, насколько часто в течение года пользователи в ней сталкивались со срабатыванием антивирусной программы. Полученные данные характеризуют степень риска заражения, которому подвергаются компьютеры в разных странах мира, и являются показателем агрессивности среды, в которой работают компьютеры в разных странах.

Веб-угрозы

Наибольший интерес представляет риск заражения через интернет, который является основным источником вредоносных объектов для пользователей большинства стран мира.

Место	Страна	% уникальных пользователей*
1	Россия	58,6%
2	Таджикистан	58,5%
3	Азербайджан	57,1%
4	Армения	55,7%
5	Казахстан	55,5%
6	Белоруссия	51,8%
7	Бангладеш	51,7%
8	Шри-Ланка	51,5%
9	Индия	51,1%
10	Судан	51,0%
11	Туркменистан	51,0%
12	Оман	48,0%
13	Узбекистан	47,5%
14	Малайзия	47,3%
15	Молдавия	47,2%
16	Мальдивы	46,8%
17	Украина	46,8%
18	Италия	45,6%
19	США	45,1%
20	Испания	44,7%

Настоящая статистика основана на детектирующих вердиктах модуля веб-антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных. При расчетах мы исключили страны, в которых число пользователей ЛК относительно мало (меньше 10 тысяч).
**Процент уникальных пользователей, подвергшихся веб-атакам, от всех уникальных пользователей продуктов ЛК в стране.*

Второй год подряд в этом рейтинге лидирует Россия. Для российских пользователей за год уровень риска при веб-серфинге увеличился с 55,9% до 58,6%. К сожалению, в Рунете реализуется большое количество киберпреступных схем. Поскольку в стране у частных пользователей и предпринимателей растет популярность интернет-банкинга, в 2012 году киберпреступники активно распространяли соответствующие зловреды. Еще один достаточно часто встречающийся в Рунете вид мошенничества — монетизация с использованием платных SMS: мошенники предлагают пользователю оплатить товар/услугу с помощью SMS, но обещанного покупатель так и не получает.

С 17-го на 2-е место в рейтинге поднялся Таджикистан с показателем 58,5. На третьем месте Азербайджан, поднявшийся с шестого места с 57,1% атакованных пользователей.

В двадцатке стран 2012 года Италия, США и Испания заняли последние три места.

США, которые по итогам 2011 года занимали 3-е место, в 2012 сместились сразу на 19-е: доля атакованных пользователей в этой стране сократилась с 50,1% до 45,1%. Это обусловлено успешной борьбой с киберпреступностью и закрытием нескольких больших ботнетов, в том числе DNSChanger, Hlux и нескольких ZeuS (Zbot) ботнетов.

Италия и Испания впервые попали в TOP 20 стран по доле атакованных пользователей при серфинге в интернете. В этих странах количество инцидентов, приходящихся на одного пользователя, было достаточно большим в течение всего года, что, в первую очередь, связано с атаками банковских троянцев.

Все страны мира можно распределить по степени риска заражения при серфинге в интернете.

1. **Группа повышенного риска** В эту группу с результатом 41-60% вошла 31 страна. Помимо стран из TOP 20 в нее также попали Австралия (44,4%), Индонезия(44,2%), Канада(42,8%), Грузия (42,3%) и Великобритания (41,1%).
2. **Группа риска** В эту группу с показателями 21-40% попали 110 стран, в том числе Турция (39,9%), Франция (39,8%), Чили (39.4%), Китай (38,4%), Польша (37,1%), Литва (35,3%), Швеция (34,1%), Австрия (34%), Эквадор (33,3%), Германия (31,8%) Финляндия (27,9%), Норвегия (27,3%), Япония (22,8), Дания (21,6%).
3. **Группа самых безопасных при серфинге в интернете стран** (0-20%) В 2012 году в эту группу попали 10 стран: Габон (20,6%), Того (20,5%), Реюньон (20,2%), Нигер (19,6%), Маврикий (18%), Гваделупа (17,8%), Мартиника (17,7%), Бенин (17,2%), Бурунди (16,9%) и Конго (16,7%).

Первая группа увеличилась на 8 стран. БОльшая часть группы — это страны постсоветского пространства и страны Азии. Огорчает тот факт, что и европейских стран за год в этой группе стало больше.

Из группы безопасных при серфинге в интернете стран вышли все европейские страны, и теперь она полностью состоит из стран Африки. Отметим, что страны, пополнившие группу безопасных при веб-серфинге, по уровню локальных угроз попали в группы с высоким и максимальным уровнем заражения. Их попадание в группу стран, безопасных для серфинга в интернете, объясняется характером распространения файлов в этих странах: интернет там пока еще не очень хорошо развит, поэтому для обмена файлами пользователи активно используют различные съемные носители информации. В итоге в этих странах на наши радары практически не попадают веб-угрозы, а вот с вирусами и червями, расползающимися по флешкам и заражающими файлы, сталкивается огромное количество пользователей.

В среднем по миру уровень опасности интернета второй год подряд увеличивается и по итогам 2012 года составил 34,7% — на 2,4% больше, чем в прошлом году. Каждый третий пользователь интернета в мире хотя бы раз в год подвергается компьютерной атаке.

Локальные угрозы

Помимо заражений через веб интерес представляют данные о детектировании вредоносных программ, обнаруженных непосредственно на компьютерах пользователей или же на съемных носителях, подключенных к компьютерам — флешках, картах памяти фотоаппаратов, телефонов, внешних жестких дисках. По сути, эта статистика отражает уровень зараженности персональных компьютеров в различных странах мира.

Место	Страна	%*
1	Бангладеш	99,7%
2	Судан	88,2%
3	Малави	78,0%
4	Танзания	77,4%
5	Руанда	76,5%
6	Афганистан	75,6%
7	Индия	75,2%
8	Лаос	73,3%
9	Непал	72,9%
10	Ангола	72,0%
11	Вьетнам	70,4%
12	Мавритания	69,8%
13	Ирак	69,6%
14	Мальдивы	69,2%
15	Уганда	69,0%
16	Шри-Ланка	68,5%
17	Монголия	68,0%
18	Джибути	67,4%
19	Мали	67,3%
20	Кот-д'Ивуар	67,0%

Настоящая статистика основана на детектирующих вердиктах модуля антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных. При расчетах мы исключили страны, в которых число пользователей ЛК относительно мало (меньше 10 тысяч).
** Процент уникальных пользователей, на компьютерах которых были заблокированы локальные угрозы, от всех уникальных пользователей продуктов ЛК в стране.*

Двадцатка 2012 года состоит из стран Африки и Азии. За год ситуация в странах-лидерах рейтинга не изменилась в лучшую сторону. Как и год назад, в Судане и Бангладеш на 9 из 10 компьютеров пользователи в течение года хотя бы раз сталкивались с заражением вредоносной программой. Еще неразвитая культура использования антивирусов и поверхностные знания пользователей о возможных компьютерных угрозах делают компьютеры в этих странах уязвимыми для вредоносных программ.

В случае локальных угроз мы также можем разделить все страны мира на несколько категорий.

1. **Максимальный уровень заражения** (более 75%): 7 стран из Азии и Африки, в том числе Индия (75,2%) и Бангладеш (99,7%), которые попали и в группу повышенного риска при серфинге в интернете.
2. **Высокий уровень заражения** (56-75%): 41 стран мира, в том числе Индонезия (64,7%), Эфиопия (58,2%) и Кения (58%).
3. **Средний уровень заражения** (35-55%): 67 стран, в том числе Китай (52,7%), Казахстан (52,6%), Россия (48,7%), Турция (48,67%), Бразилия (43,5%), Южная Корея (39,8%), Испания (39,8%), Португалия (35,8%) и Литва (35,7%).
4. **Наименьший уровень заражения** (0-35%): 38 стран мира. В том числе США (33,3%), Франция(32,8%), Великобритания (30,9%), Латвия (31,4%) и Бельгия (27,2%). Количество стран в этой группе по сравнению с 2011 годом выросло в 2,7 раз, в прошлом году в нее попало всего 14 стран. В первую очередь изменения связаны с постепенным отмиранием классических вирусов и авторан-червей.

Топ 10 стран с минимальным процентом зараженных компьютеров:

Место	Страна*	%
1	Дания	15,0%
2	Япония	19,5%
3	Финляндия	19,8%
4	Швеция	22,9%
5	Чехия	23,5%
6	Нидерланды	23,9%
7	Норвегия	24,0%
8	Люксембург	24,2%
9	Германия	24,3%
10	Швейцария	24,4%

В среднем в группе самых безопасных стран мира было атаковано25,4% компьютеров пользователей. По сравнению с прошлым годом этот показатель уменьшился на 4 пункта.

Заключение

2012 год — это год, когда киберпреступники стали активно интересоваться новыми платформами, прежде всего Mac OS X и Android OS. Кибепреступников всегда привлекала возможность легко заразить большое количество компьютеров и устройств пользователей, и число атак на пользователей Mac и Android растет.

В начале года был обнаружен огромный 700-тысячный ботнет из Mac-компьютеров, созданный программой Flashfake. Злоумышленники могли устанавливать на зараженные машины любые дополнительные вредоносные модули. Известно, что один из модулей занимался подменой трафика в браузере. Массовыми атаками история с Mac-зловредами не ограничивается. В течение всего года мы детектировали целевые атаки с использованием бэкдоров, нацеленных на пользователей Mac OS X. Тенденция отразилась и в наших цифрах — количество созданных антивирусных записей под Mac OS X увеличилось на **30%** по сравнению с 2011 годом.

Эпидемия Mac-троянца и бесконечная череда Android-зловредов сделала тему защиты новых платформ очень острой. Необходимость такой защиты стала очевидной для большинства интеренет-населения планеты. Мифы о неуязвимости Mac для вирусов были разрушены. Производители стали больше внимания уделять защите платформ: в новой версии Mac OS X было реализовано несколько функций, улучшающих безопасность; Google со свой стороны реализовала скан приложений, добавляемых в магазин приложений. Более высокий уровень защиты предложила и антивирусная индустрия, которая готова к такому повороту событий и уже некоторое время предлагает решения, подобные Kaspersky One, направленные на защиту всего спектра устройств — от PC и Mac до телефона и планшетного компьютера.

К сожалению, несмотря на успехи в борьбе с киберпреступностью, в 2012 году процент атакованных пользователей в интернете продолжил расти и составил 34%. Ни одна европейская страна не попала в группу стран, в которых процент атакованных в процессе веб-серфинга пользователей меньше 20%.

Если 2011 год мы назвали годом уязвимостей, то 2012 год можно назвать годом Java-уязвимостей. По нашей статистике половина атак с использованием эксплойтов в 2012 году проходила с использованием уязвимостей именно в Java. Что немаловажно, уязвимости использовались киберпреступниками как в массовых атаках, так и в целевых, а эксплойты работали как под PC, так и под Mac.

Источник: http://www.securelist.com

Twitter сообщил о масштабных хакерских атаках на американские компании

Отдел информационной безопасности Twitter сообщил о направленных на сервис кибер-атаках, поставив их в одном ряду с аналогичными нападениями на другие американские IT- и медиакомпании. Об этом сообщается на официальной странице крупнейшего в мире сервиса микроблогов.

По словам руководителя отдела информационной безопасности Twitter Боба Лорда, на прошедшей неделе в компании обнаружили новые механизмы доступа к данным, которыми могли пользоваться хакеры. Специалисты выявили одну кибер-атаку, которую удалось отразить, но при этом признали, что хакеры могли получить доступ к информации 250 тысяч пользователей сервиса. Речь идет, в частности, об именах пользователей, их электронных адресах и паролях, сообщает lenta.ru.

В Twitter заявили, что не считают эту атаку единичным случаем, подчеркнув, что осуществившие ее хакеры были профессионалами.

Всем клиентам, чьи данные могли быть доступны хакерам, было направлено письмо с уведомлением. В качестве меры предосторожности представители Twitter предложили этим пользователям сменить пароли, а остальным проверить, являются ли их пароли достаточно безопасными. Эти рекомендации распространяются не только на сервис микроблогов, но и на любые другие сайты.

При этом, по мнению Twitter, другие компании и организации недавно подверглись аналогичным атакам. В отделе информационной безопасности напомнили о череде крупных хакерских атак, направленных на американские медиакомпании, в том числе на издания New York Times и Wall Street Journal. «Именно поэтому мы решили сообщить об этой атаке, хотя пока только собираем информацию», — заявил Боб Лорд. В настоящий момент Twitter сотрудничает с правительством и правоохранительным органами США с целью найти и привлечь к ответственности хакеров, причастных к нападению, и в результате сделать интернет безопаснее для всех пользователей.

30 января газета New York Times сообщили об атаках на сайт издания и взломе почты десятков ее сотрудников. Газета написала, что нападения продолжались в течение четырех месяцев, начиная с октября 2012 года, и осуществлялись из Китая. На следующий день о постоянных атаках китайских хакеров заявило американское издание The Wall Street Journal. В посольстве Китая в США причастность Китая к нападениям на американские СМИ не признали.

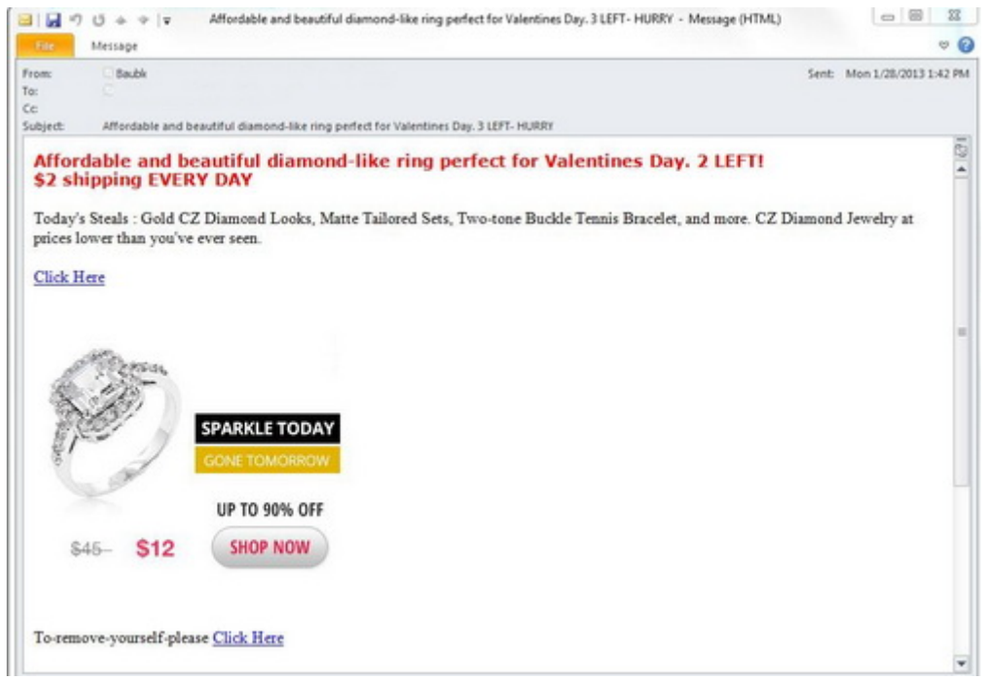
Источник: http://www.anti-malware.ru

UA Linux
http://ualinux.com
Эксперт в области безопасности.

10 самых популярных видов кибер-мошенничества на День святого Валентина.

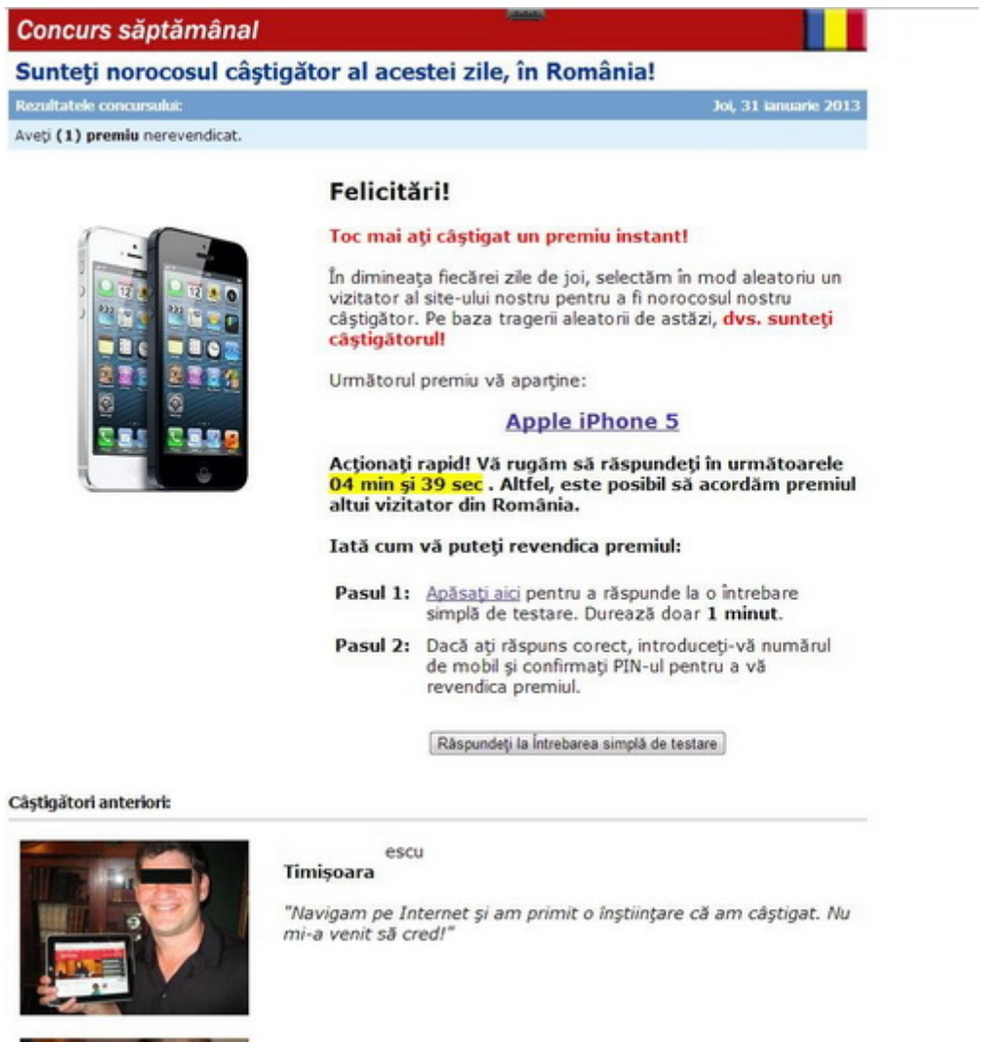
Компания Bitdefender решила предупредить влюбленных по всему миру о сетевых видах мошенничества, которые могут их подстерегать в сети в День святого Валентина. По словам специалистов, они заметили целую волну самых разных обманных схем.

Bitdefender советует клиентам держаться как можно дальше от фальшивых предложений снять лимузин или онлайн-экспертов, которые предлагают наладить ваши отношения с любимой. Подобные предложения, как правило, распространяются по электронной почте. Ссылка в таком письме перенаправит на страницы сайтов, напичканных вредоносным программным обеспечением и троянами.



Спам, связанный с подарками для женщин.

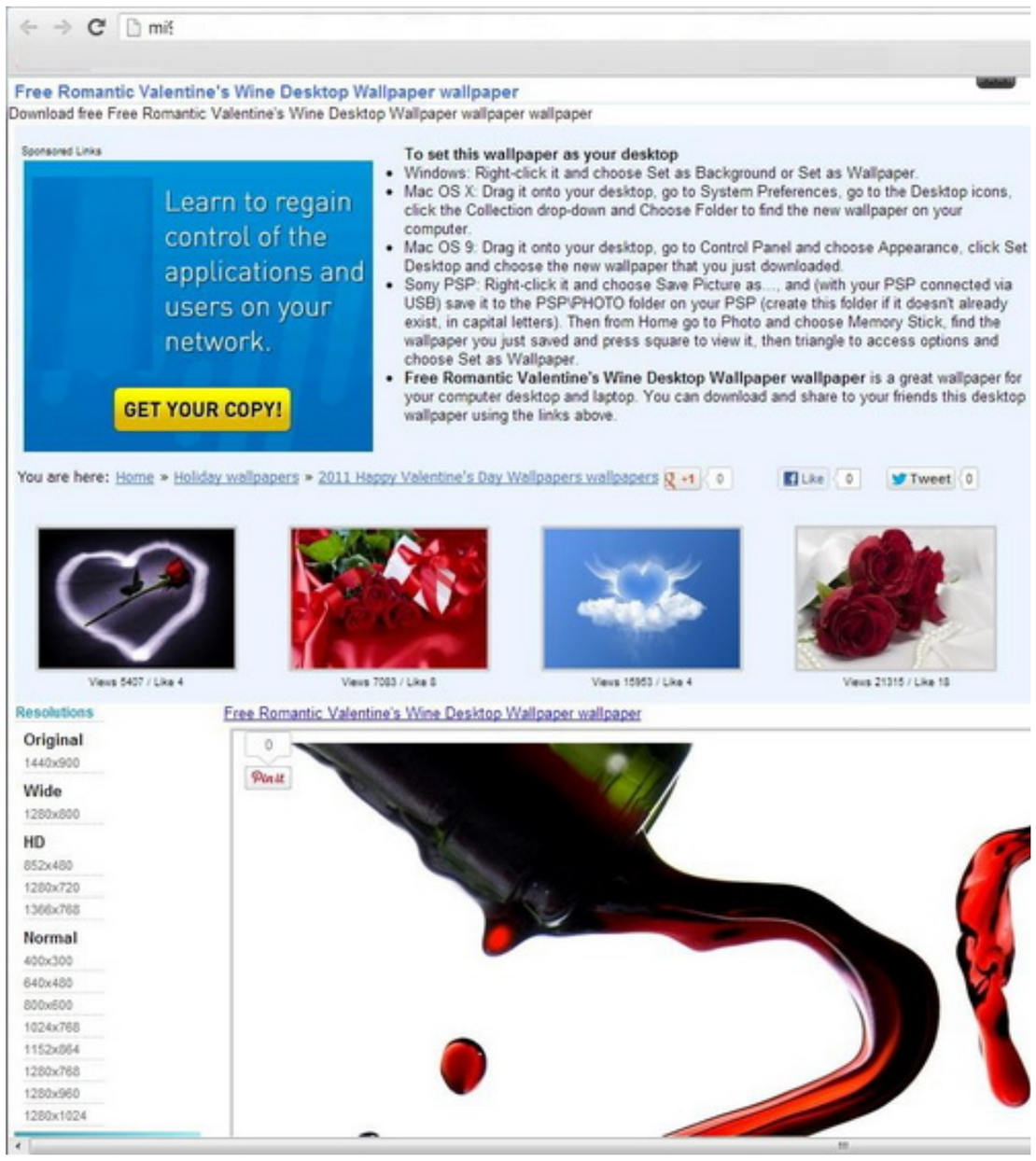
Мужчины собираются потратить на праздник Святого Валентина на 75% больше, чем женщины (поданным CreditDonkey.com). Поэтому мошенники специально ориентируют свои предложения на представителей сильного пола, предлагая им «уникальные» идеи для подарков. Как правило, чтобы заманить мужчину достаточно привлечь его внимание сообщениями о шоколаде, колечках, духах, бижутерии и фальшивых часах.



Спам, связанный с розыгрышом iPhone 5.

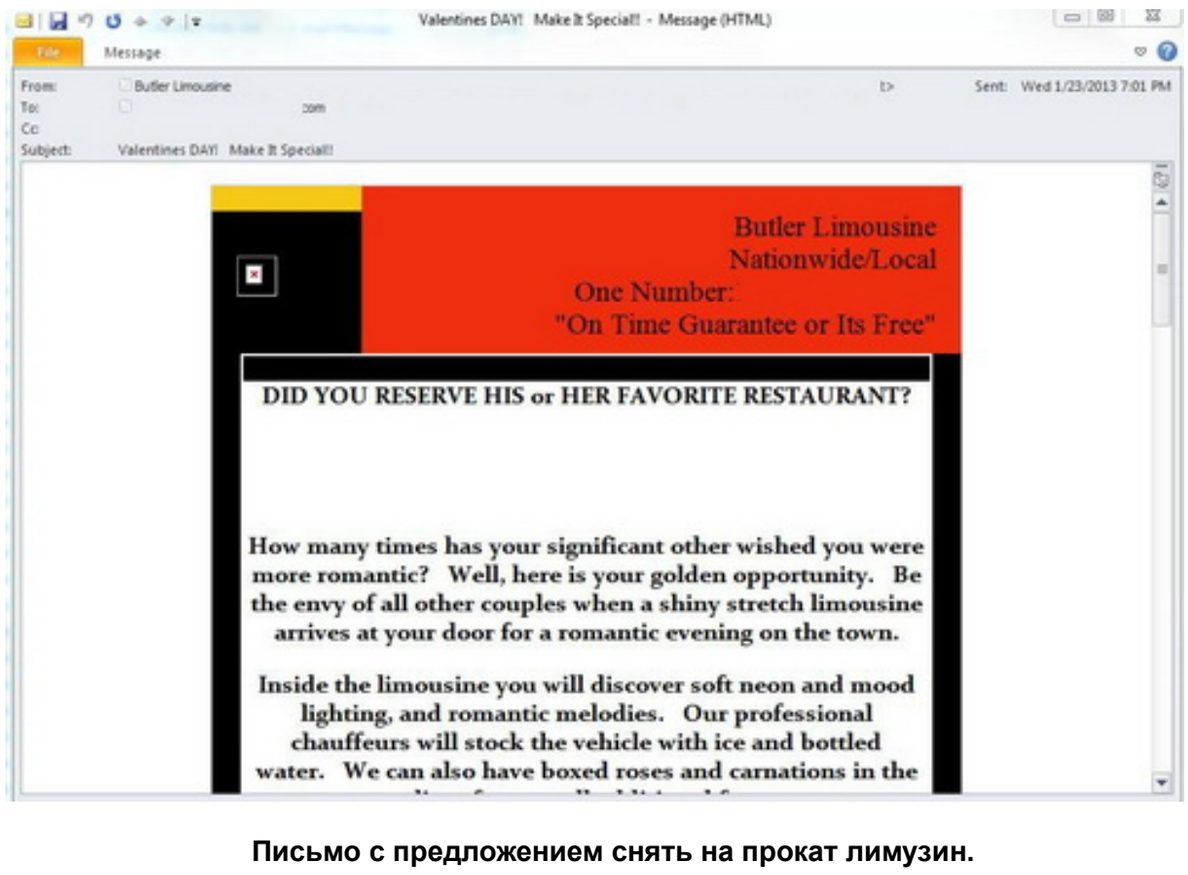
«*Мошенники стреляют во влюбленных в упор, если позволите такое сравнение. Спам, связанный со свиданиями, составляет около 7% от общего количества спама рассылаемого по миру в это время*», – говорит старший стратег по вопросам безопасности Bitdefender Кэтэлин Косои. «*С приближением Дня Святого Валентина растет количество мошеннических писем, связанных с романтическими отношениями, так что людям стоит обходить стороной сомнительные сайты знакомств или непонятные странички в социальных сетях. Все эти ресурсы будут просто собирать вашу личную информацию, используя ее для вымогания денег*».

Еще одной популярной аферой, которая пользуется особенной популярностью с приближением дня всех влюбленных, стало скачивание обоев для рабочего стола, которые просто направляют вас на различные вредоносные сайты. Или, например, пользователям может прийти письмо, оповещающее их о выигранном iPhone 5. Разумеется, чтобы получить заветный смартфон, нужно ввести личные данные. Подобные же аферы проводятся и через Facebook.



Сайт с обоями, посвященными Дню святого Валентина.

Стоит также опасаться различных игр и программ, связанных с Днем Святого Валентина. Если вы скачиваете их из неофициальных источников, то они могут содержать различное вредоносное программное обеспечение, способное навредить вашему компьютеру.



Письмо с предложением снять на прокат лимузин.

Жителям Великобритании эксперты советуют быть особенно осторожными с заказом цветов. День Святого Валентина не только самый напряженный день для флористов в Англии, но и самый урожайный для аферистов. Например, одна афера в Великобритании завлекает граждан романтическими красными розами, а другая заставляет пользователей покупать духи с ненадежного сайта, маскируясь доменом «co.uk».

Преступники также пользуются немецкой любовью к рассылкам разных поздравительных открыток. Посредством различных сомнительных алгоритмов, доверчивых клиентов направляют на сайты, которые могут включать трояны.

В целом Bitdefender советует быть осторожнее и помнить, что для любимых важен не столько сам подарок, сколько внимание.

Источник: http://www.securelist.com

UA Linux
http://ualinux.com

Аналитика, обзоры, рекомендации.

user And LINUX

{ Secure Shell }

Нам можно доверять!

И про Вас узнают Все...

{

Адрес журнала в интернете:
http://ualinux.com/index.php/journal

Обсуждение журнала на форуме:
http://ualinux.com/index.php/forum

}

{

Адрес редакции:

Украина, 03040, г.Киев, а/я 56
email: journal@ualinux.com

}

Тип издания: электронный/печатный
Тираж: *более 15 000 копий.

*указано суммарное количество прошлого выпуска журнала с первичных источников, а также загрузок с других известных ftp, http и torrent серверов.