Отчет о современных интернет-угрозах.
3 квартал 2011

entensys

commtouch®

Содержание

3 квартал 2011

93 триллиона

Писем рассылается спамерами каждый день

Стр. 6

336,000 зомби

Ежедневно активизируются

Стр. 13

Потоковое медиа/Загрузки

Наиболее популярная тема в Web 2.0

Стр. 14

Медицина и фармацевтика

Остается самой популярной темой спам-рассылок (29%)

Стр. 9

Индия

Рассылает больше всего спама (18%)

Стр. 13

Запаркованные домены

Наиболее востребованная категория сайтов у распространителей вирусов

Стр. 12

Введение

В третьем квартале 2011 года специалистами CommTouch Labs выявлена самая большая за последние два года вспышка активности распространителей вредоносных программ, использующих в качестве инструмента электронную почту. Реальный замысел злоумышленников в данном случае до сих пор не раскрыт. Как правило, после подобных крупных вспышек уровень спама начинает увеличиваться, однако в отчетном квартале показатели распространителей нежелательных сообщений продолжили снижаться. Целый ряд вирусов, предназначенных для устройств на платформе Android, внесен в расширенный Wildlist.

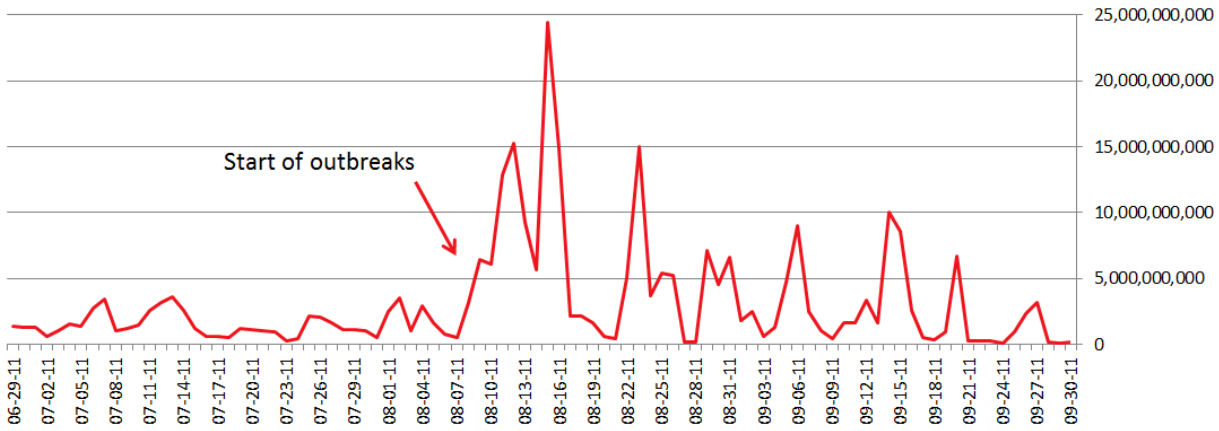
CommTouch Labs наблюдались дальнейшие рассылка спама и мошенническая деятельность посредством взломанных учетных записей. Экспертами проведено тщательное исследование с целью выявления и оценки тенденций, связанных с кражей, восстановлением и использованием данных почтовых аккаунтов.

Вирусные тренды

Возвращение зараженных писем

В 2010 году популярность использования электронной почты в качестве средства распространения вирусов неуклонно падала. Доля подобных писем составляла менее одного процента от общего числа вредоносных почтовых сообщений (спам, фишинг и т.п.). Март 2011 года положил начало изменения сложившейся тенденции. Именно тогда замечено увеличение объемов писем, содержащих вирусы во вложении. В последующие же месяцы данные показатели вновь снизились до уровня первого месяца весны.

В августе 2011 сообщения с вирусами вновь составили значительную долю всеобщего почтового трафика. Увеличение четко показано на графике, приведенном ниже. Показатели колебались от нескольких сотен миллионов до двух миллиардов писем в день. Во время пика активности злоумышленники разослали 25 миллиардов почтовых сообщений с зараженным вложением за одни сутки.



Источник: Commtouch.

Анализ сообщений на форумах конечных пользователей показал, что «вирусные» кампании были весьма успешными: значительная часть получателей подобных писем запускали прикрепленные файлы. Зависимость между показателями заражения и объемами рассылаемых сообщений, как правило, является линейной - чем больше писем, тем больше и количество пострадавших пользователей.

Список видов зараженных писем, использованных злоумышленниками в отчетном квартале, включает в себя Sasfis, SpyEye, Zeus, поддельный АнтиВирус и другие. Почти все вирусы, содержащиеся во вложении, после своей активации соединяются с внешним сервером и загружают еще несколько вредоносных файлов, которые затем автоматически запускаются на зараженном компьютере.

Каждый из вышеупомянутых типов вирусов связан с определенным видом вредоносной активности, например, Zeus является инструментом мошенничества в сфере банковских услуг.

В прошлом, крупные ботнеты использовались для отправки значительных объемов спама. Уровень нежелательных сообщений и изменение его показателей приведены на графике, содержащимся в отчете ниже. Тенденция снижения объемов рассылаемых спам-писем четко видна на нем. «Вирусная» кампания прошлого месяца на данный момент значительно не повлияла на показатели активности распространителей нежелательных писем.

Существует несколько альтернативных способов использования огромных ботнетов:

- масштабные мошеннические действия в банковской сфере;
- кража аккаунтов Facebook, Gmail, Yahoo;
- DDOS-атаки;
- иная преступная деятельность.

В данное время крупные сети не замечены и в перечисленных выше активностях.

Каждую из массированных вирусных атак отличала определенная «тема», используемая злоумышленниками для обмана пользователей. Среди них можно выделить:

- Оповещения служб доставки (UPS, Fedex, DHL) – уведомления о местонахождении пакета. Более подробная информация содержится во вложении.
- Ошибки отелей – прикрепленный файл являлся формой для корректировки ошибочно составленного счета.
- «Карта любви» - предложения популярных видов досуга.
- Проблемы с кредитными картами – некорректно проведенные кредитные операции, нуждающиеся в подтверждении.
- Отсканированные документы – получение документа, отсканированного на оборудовании внутри офиса.
- Ошибки NACHA – уведомления об отклонении межбанковской операции. Причины отказа содержатся во вложении.

Трюк «шрифт справа налево»

Во многих электронных письмах для отображения типа содержимого используется иконка PDF-документа, даже если файл является исполняемым. Данный способ обмана является достаточно эффективным в случае с пользователями, которые не особо внимательно следят за расширением запускаемых файлов.

Особую популярность приобретает использование специального шрифта (U+202E), позволяющего изменить традиционное написание букв на «справа налево».

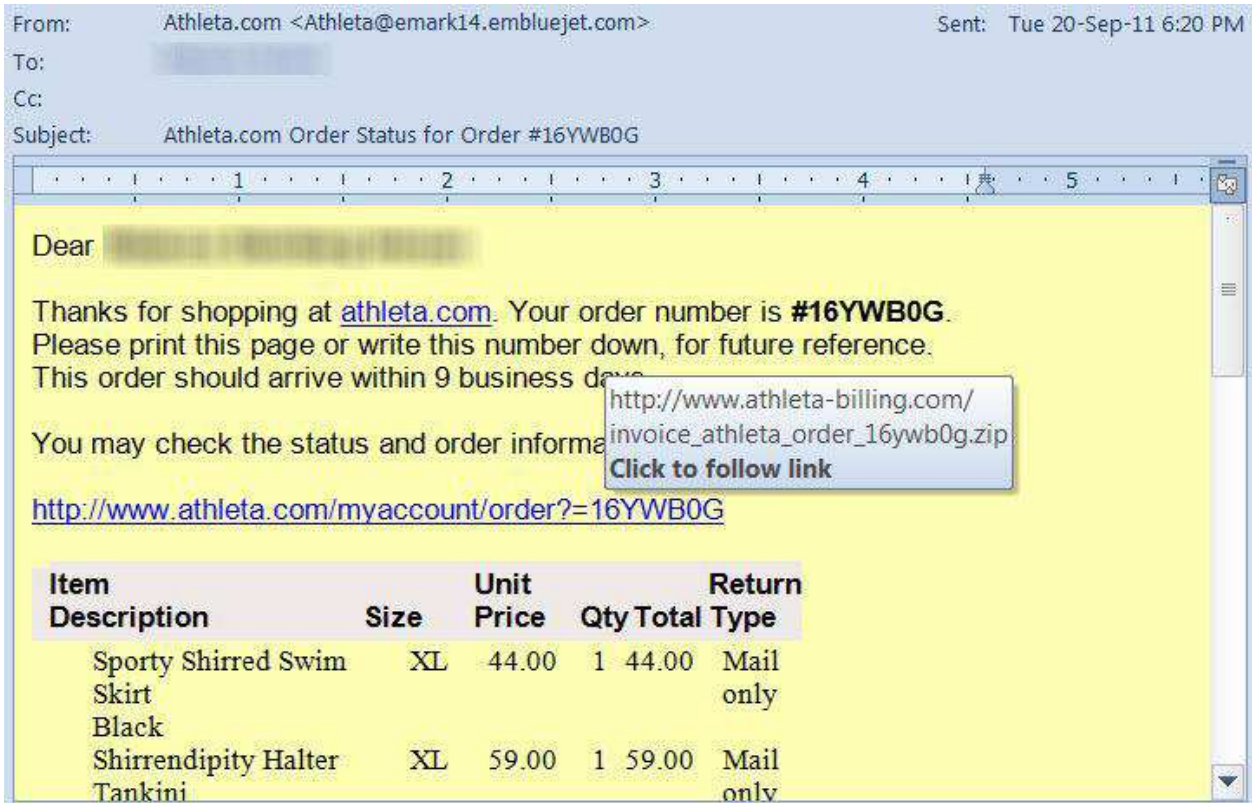
Источник: Commtouch.

Реальное имя файла из примера – **«CORP_INVOICE_08.14.2011_Pr.rhylcod.exe».** Таким образом, пользователи считают, что открывают безобидный документ, хотя на самом деле запускают исполняемый файл.

Вирусы от Athleta

В сентябрьской атаке, организованной с целью кражи паролей, злоумышленники использовали в качестве прикрытия подделки уведомлений о состоянии заказа в магазине одежды Athleta (сеть Gap). Многочисленные письма содержат достаточно ограниченное количество избранных в качестве «покупки» предметов. Данная активность отличается особой эффективностью, так как многие получатели были заинтересованы одеждой, которую они «заказали». При нажатии на «статус заказа» или другие

активные ссылки загружается Zip-архив, содержащий исполняемый файл «invoice_athleta_order-.exe». При открытии данного файла закачивается ряд других вирусов («google.exe», «googles.exe», «googletools.exe» и «SOD.exe»), а также на внешний сервер отправляются данные о географическом положении зараженной машины.



Источник: Commtouch.

«Googletools.exe» загружает конфигурационный файл со списком интернет-ресурсов. Просмотр этих сайтов несет в себе потенциальную угрозу заражения компьютера рядом другим вредоносных программ, а также потерей контроля учетных записей. Среди ресурсов, выбранных злоумышленниками, фигурируют: Amazon, AT&T, Bank of America, Best Buy, CHASE Home, Citibank, Craigslist, Facebook, Fifth Third Bank, Go Daddy, Google Checkout, IMVU, LastPass, Moneybookers, Myspace, Netflix, Newegg, PayPal, PlayStation, RapidShare, RoboForm, Target, T-Mobile, U.S. Cellular, Verizon, Walmart.com, WebMoney, Western Union, и World of Warcraft.

«Горячая десятка» вирусов

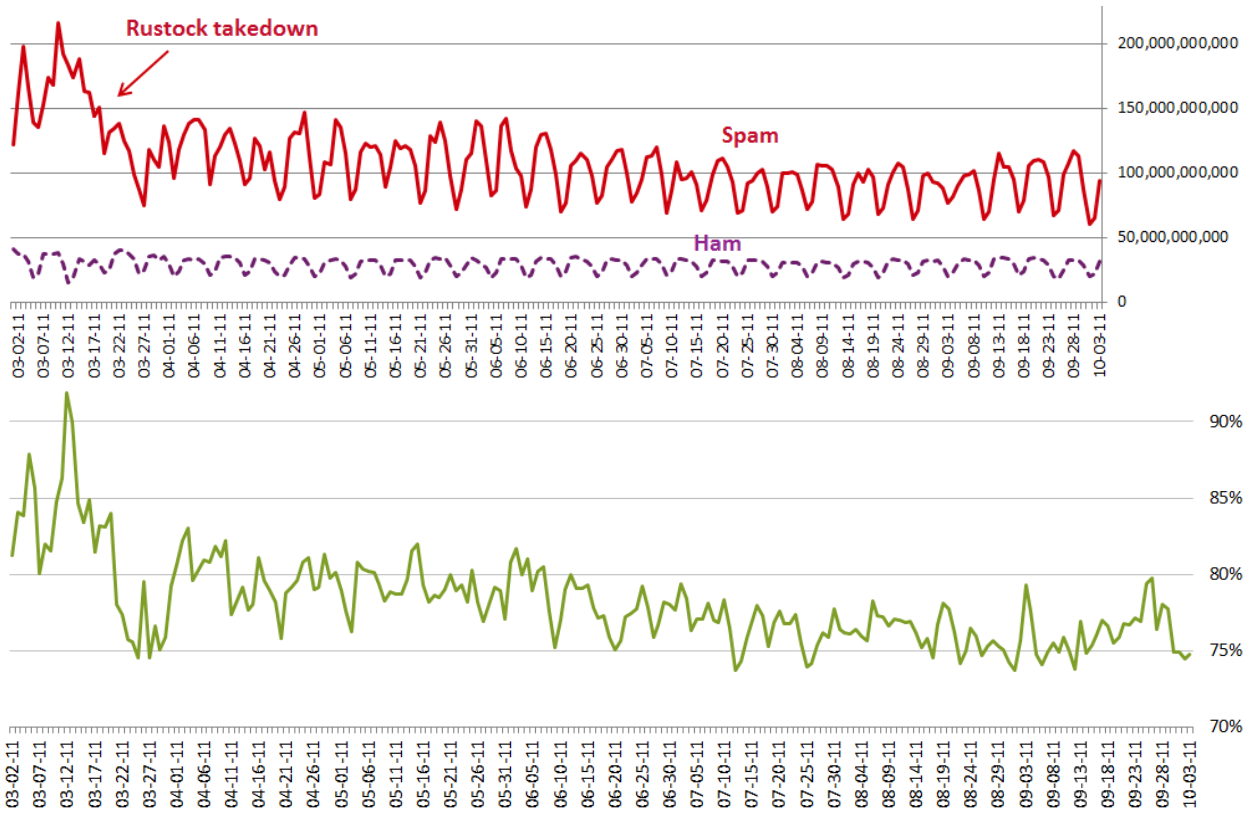
В таблице ниже приведена десятка наиболее популярных вирусов, составленная Лабораторией CommTouch по итогам третьего квартала.

Место	Название вредоносного ПО
1	W32/Oficla.FO
2	W32/RAHack.A.gen!Eldorado
3	W32/Adware.PAP
4	W32/Sality.gen2

5	JS/Pdfka.BG
6	W32/Patched.G
7	W32/Damaged_File.B.gen!Eldorado
8	W32/Bredolab.AP.gen!Eldorado
9	W32/MalwareF.AFPRH
10	W32/Heuristic-210!Eldorado

Тенденции спама

Показатели спама в мире остаются на низком уровне. Распространители нежелательных писем до сих пор не могут оправиться от демонтажа Rustock или заняты изменением тактики атак. Как уже было сказано выше, августовские и сентябрьские вирусные атаки не оказали влияния на уровень спама, который составил только 93 триллиона сообщений ежедневно (76% от всех почтовых сообщений, передаваемых в мире).

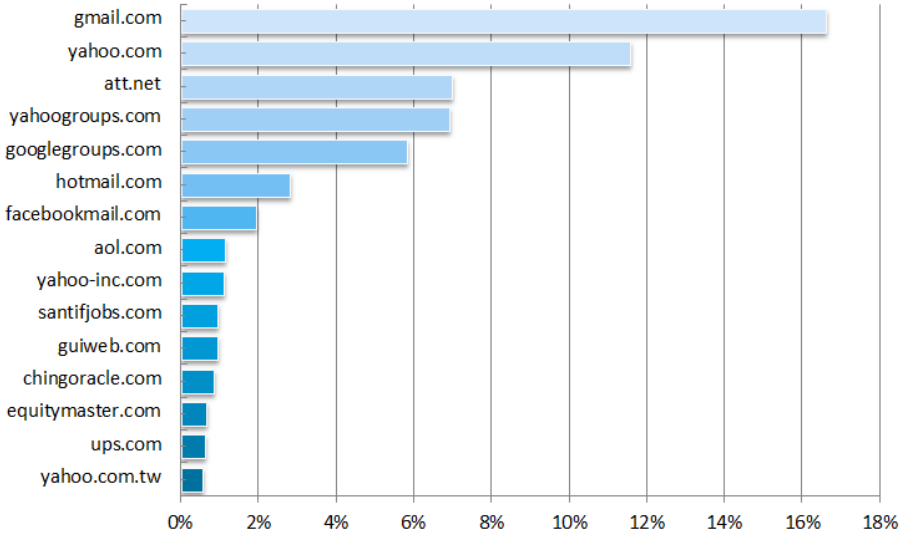


Источник: Commtouch.

Домены-отправители спама

В рамках анализа трендов в области спама Лаборатория Commtouch отслеживала почтовые домены, которые наиболее часто используются спамерами в качестве отправителей. Обычно используются фальшивые адреса с целью использования имени авторитетных и подлинных источников.

В отчетном квартале лидером рейтинга вновь является gmail.com. 14-е место осталось за ups.com из-за огромного количества поддельных уведомлений, отправленных от имени UPS.



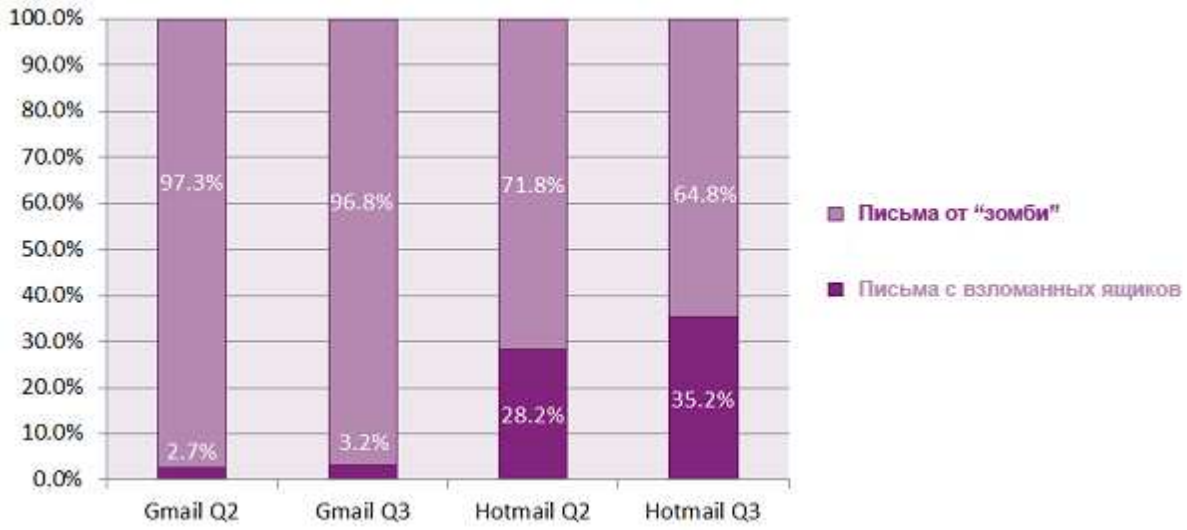
Источник: Commtouch.

Взломанные аккаунты

В дополнение к поддельным письмам необходимо отметить значительный процент почтовых сообщений, отправленных с реально существующих аккаунтов Gmail, Hotmail и Yahoo. Чаще всего данные учетные записи взломаны, реже – специально созданы распространителями спама для своих преступных целей. Использование злоумышленниками реальных аккаунтов затрудняет работу антиспам-фильтров, так как популярные почтовые домены внесены в белый список. Таким образом, нежелательное сообщение, отправленное с помощью взломанной учетной записи, имеет значительно больше шансов достичь адресата, нежели в случае использования ботнета.

Приведенный ниже график сравнивает объемы писем, отправленных от «Gmail» и «Hotmail» во втором и третьем кварталах. На основании IP-адреса можно выделить:

- Письма, отправленные с зараженного компьютера (с фальшивого адреса);
- Письма, отправленные с взломанных или созданных спамером реальных почтовых ящиков.



Источник: Commtouch.

Как видно из графика, 28-35% спама от «Hotmail» отправляется с реально существующих почтовых аккаунтов, от «Gmail» - 3%.

Полученные данные говорят о росте популярности использования злоумышленниками взломанных учетных записей. Специалисты Commtouch провели опрос среди людей, контроль над почтовыми аккаунтами которых был утерян. Более половины респондентов подтвердили, что с их личных ящиков рассылались нежелательные письма. 23 процента опрошенных не были уверены, что злоумышленники использовали их взломанные аккаунты для распространения спама, но не отрицали факт потери контроля. Помимо учетных записей на популярных почтовых доменах респонденты отмечали случаи взлома личных аккаунтов на Facebook.

Опрошенным также были заданы следующие вопросы:

1. Какая именно (Gmail, Facebook и т.д.) учетная запись была взломана?

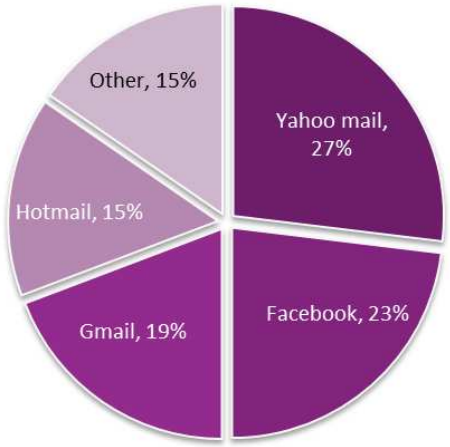
а. Yahoo;

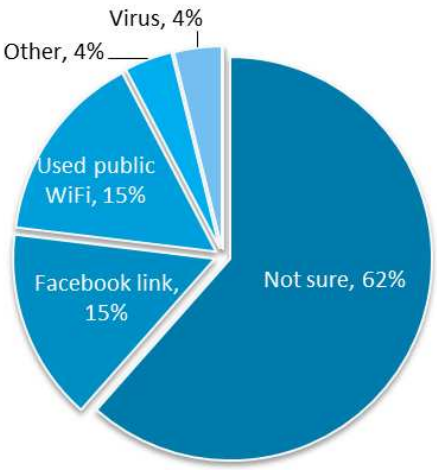
б. Hotmail;

в. Gmail;

г. Facebook;

д. Другое.





2. Каким образом был утерян контроль над аккаунтом?

а. Я использовал публично доступный Wi-Fi (например, в кафе);

б. Я запустил файл, возможно, содержащий вирус;

в. Я перешел по ссылке в письме;

г. Я указал свои данные для доступа к аккаунту на одном сайте;

д. Я прошел по ссылке, присланной мне другом в социальной сети;

е. Не знаю;

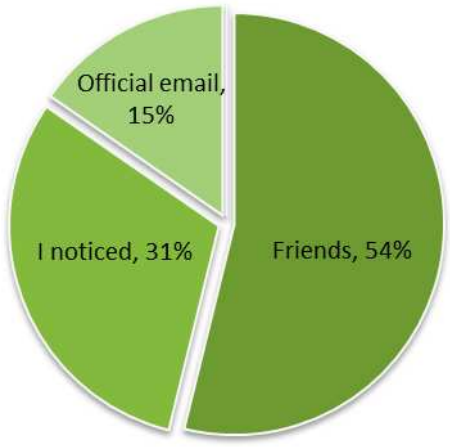
ж. Другое.

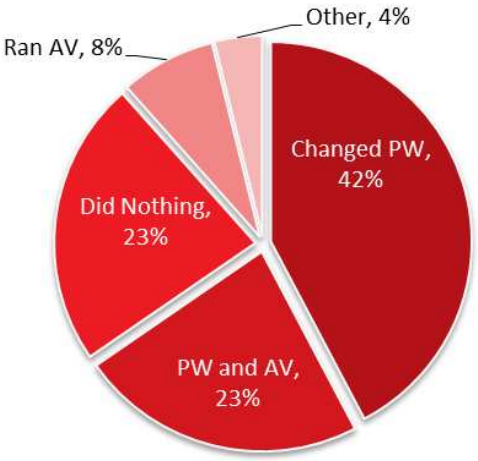
3. Как владелец учетной записи обнаружил взлом?

а. Пришло официальное оповещение;

б. Сам заметил;

в. Сообщили друзья.





4. Какие действия были предприняты для восстановления контроля над аккаунтом?

а. Изменил пароль;

б. Запустил антивирусную проверку;

в. Оба действия, приведенные выше;

г. Не сделал ничего (это случилось одни раз, но сейчас уже все хорошо);

д. Другое.

5. Как использовался взломанный аккаунт злоумышленниками?

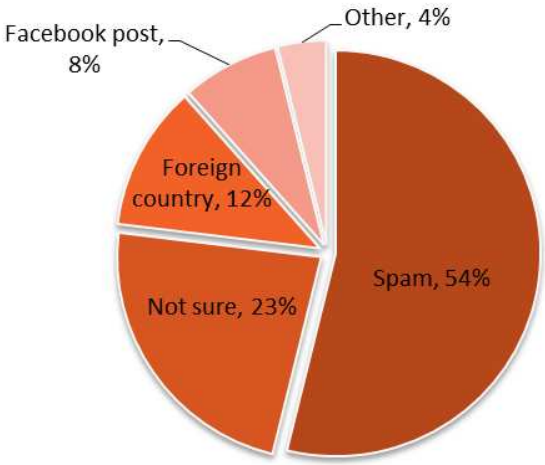
а. Для рассылки спама;

б. Моим друзьям приходили просьбы отправить мне деньги, так как я застрял в другой стране;

в. Для отправки сообщений и постов на стену в социальной сети;

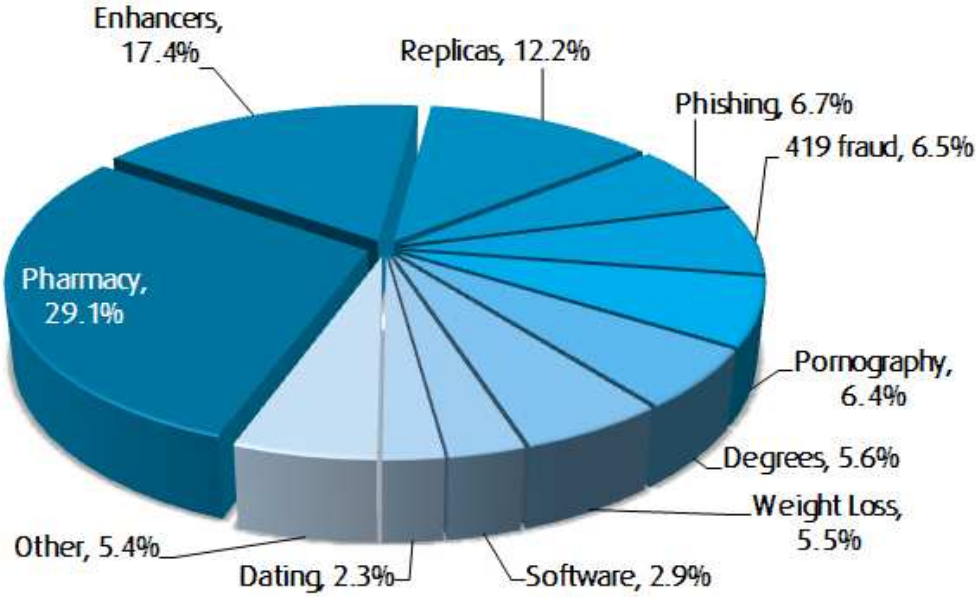
г. Я не уверен, что потерей контроля над моей учетной записью успели воспользоваться;

д. Другое.



Тематика спама

Показатели «медицинского» спама перестали ползти вниз, как это было на протяжении шести последних кварталов, и достигли 29% от общей доли всего спама (на 5% больше, чем в предыдущем квартале). «Аксессуары» также поднялись на 5 пунктов и составили 17% от всех нежелательных писем.



Источник: Commtouch.

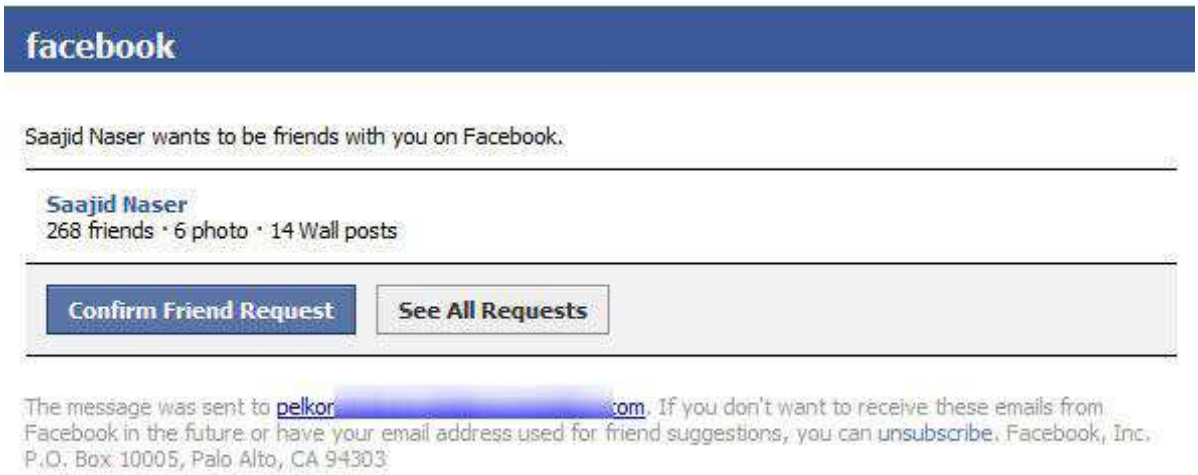
Набирает обороты деятельность спамеров в Facebook и Twitter. Злоумышленники используют уведомления, приходящие от данных социальных сетей в своих преступных целях.

Источник: Commtouch.

Веб-безопасность

Опасности Facebook

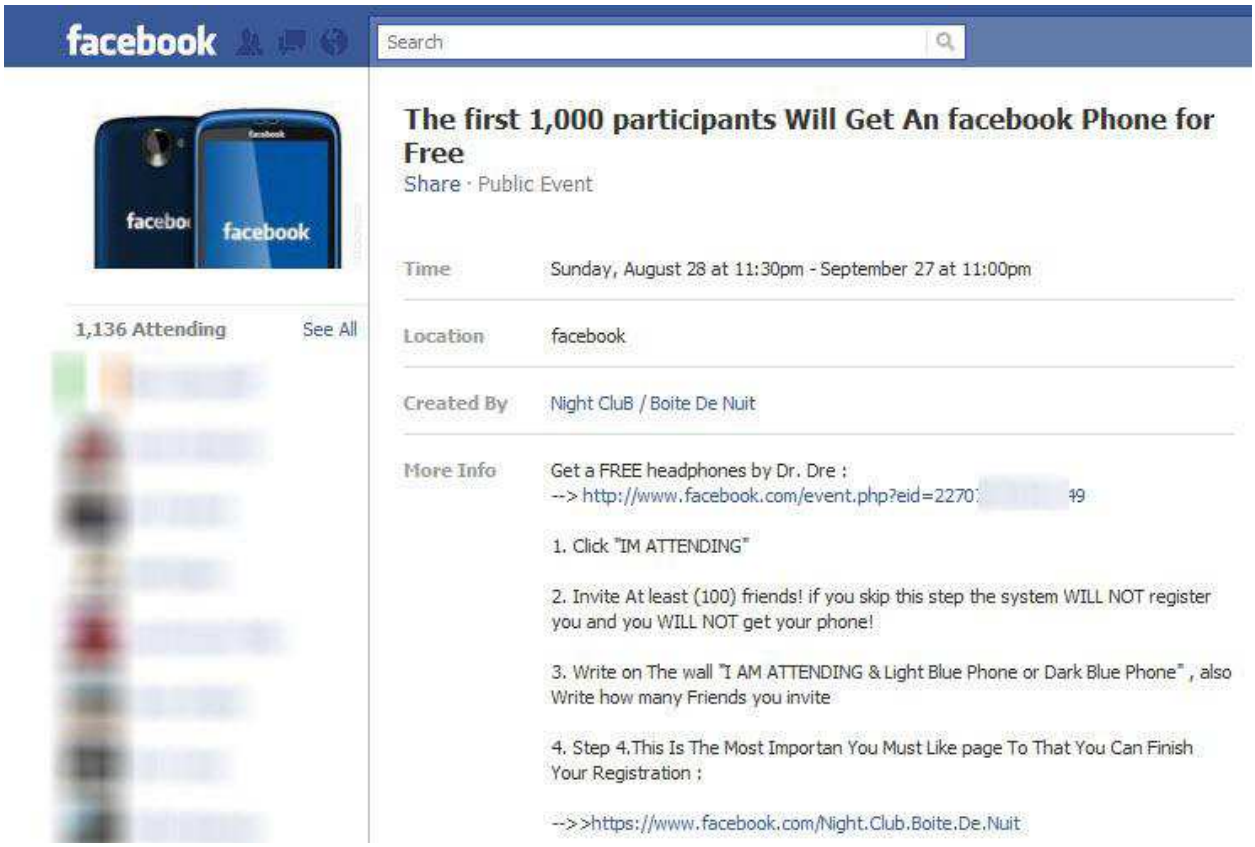
Социальная сеть Facebook продолжает привлекать внимание разработчиков вирусов. В августовской «вирусной» кампании разработка Цукерберга была использована в качестве инструмента распространения «банковского» трояна.



Источник: Commtouch.

Мошенники не ушли из Facebook и во время сентябрьского всплеска активности. Пользователи получали сообщения с заголовками такого рода, как:

- «Первые 50000 участников получат IPhone 4 бесплатно»;
- «Первым 500 участникам достанется бесплатная майка от Facebook»;
- «Получи бесплатные наушники».



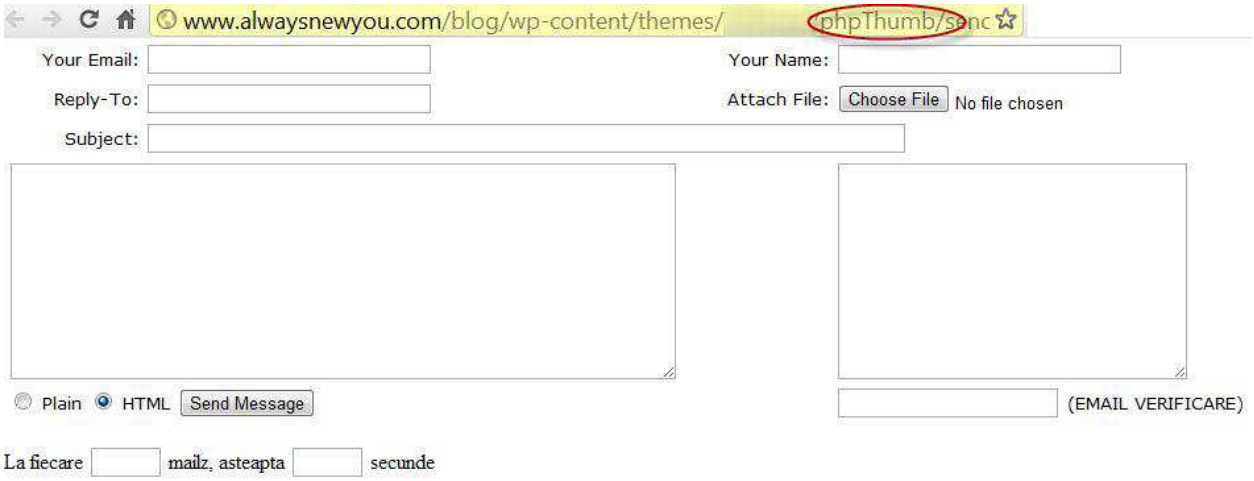
Источник: Commtouch.

Для получения призов пользователям предлагалось с помощью приглашений распространить новость по наибольшему количеству своих друзей. Также привлекательным инструментом для преступных действий является функция «Мне нравится».

PHP Thumb

Тысячи сайтов используют скрипт «php Thumb» для управления изображениями на страницах. Данный скрипт позволяет исправить размеры изображений, добавить водяные знаки и осуществлять еще целый ряд действий с графикой при создании ресурса.

Помимо всех преимуществ, которые дает использование «php Thumb», оно также предоставляет возможность злоумышленникам запустить любой код на странице. В августе огромное количество писем содержало ссылки на интернет-ресурсы взломанные благодаря уязвимостям, связанных с «php Thumb». Как правило, на данных сайтах были размещены специальные формы (фишинговые страницы), пример одной из которых приведен ниже.



Источник: Commtouch.

Данный метод представляет большую опасность для пользователей, так как письма, отправленные с веб-сервера взломанного сайта, в начале атаки не блокируются фильтрами, использующими блокировку по IP.

Категории зараженных сайтов

В течение третьего квартала 2011 года Лаборатория Commtouch анализировала категории веб-сайтов, которые наиболее часто содержат вредоносные программы. Порносайты опустились на третью строчку данного рейтинга, уступив лидирующие позиции запаркованным доменам и порталам. Стоит отметить, что зачастую размещение вирусов на сайте одобрено владельцами ресурса.

Категории сайтов, содержащих вредоносные программы			
Место	Категория	Место	Категория
1	Запаркованные домены	6	Бизнес
2	Порталы	7	Компьютеры и технологии
3	Порнография	8	Здоровье и медицина
4	Образование	9	Покупки
5	Развлечение	10	Путешествия

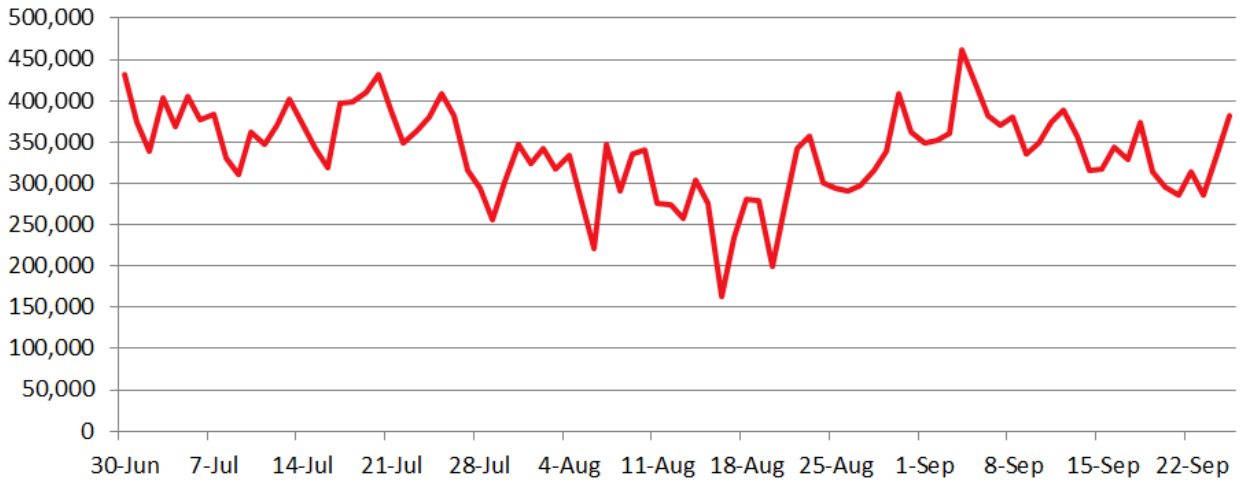
Предпочтения фишеров

Лаборатория Commtouch проводила анализ категорий веб-сайтов, наиболее часто используемых фишерами в качестве прикрытия. Интернет-ресурсы, связанные с играми, по-прежнему находятся на вершине данного рейтинга.

Категории сайтов, содержащих фишинговые страницы			
Место	Категория	Место	Категория
1	Игры	6	Спорт
2	Порталы	7	Досуг и отдых
3	Покупки	8	Бизнес
4	Мода и красота	9	Здоровье и медицина
5	Образование	10	Развлечение

Зомби

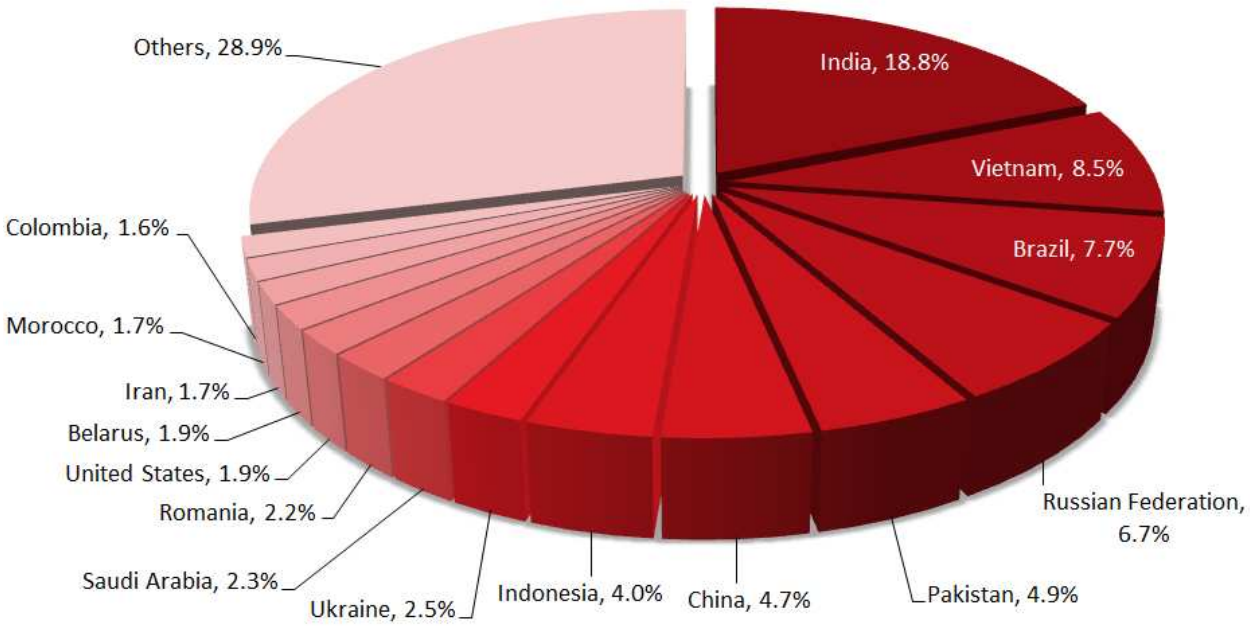
В отчетном квартале каждый день для распространения спама и вирусов активировались 336,000 зомби. Таким образом, данный показатель снизился по сравнению с 377,000 во втором квартале. Крупные вирусные атаки в августе и сентябре не повлияли на число активных зомби.



Источник: Commtouch.

Горячие точки зомби

Индия с показателем 18% от общей численности зараженных рабочих станций вновь занимает первое место среди стран-хостеров зомби. Бразилия опустилась на третье место, уменьшив свои показатели на 3%. США и Иран присоединились к ТОП-15, вытеснив Польшу и Италию. Россия осталась на четвертом месте.



Источник: Commtouch.

Тенденции Web 2.0

Commtouch's GlobalView URL Filtering service включает в себя классификацию контента Web 2.0. В дополнение к точности фильтрации, это дает представление о том, какие ресурсы, контент которых формируется пользователями, являются наиболее популярными. Категория «Потоковое мультимедиа и загрузки» вновь стала самой востребованной в среде Web 2.0, увеличив свою долю почти до четверти от всего создаваемого пользователями контента.

Место	Категория	Проценты	Место	Категория	Проценты
1	Потоковое мультимедиа и загрузки	24%	8	Искусство	5%
2	Развлечения	9%	9	Спорт	4%
3	Компьютеры и технологии	8%	10	Образование	4%
4	Порнография	6%	11	Досуг и отдых	3%
5	Мода и красота	5%	12	Здоровье и медицина	3%
6	Религия	5%	13	Игры	3%
7	Рестораны и питание	5%	14	Половое воспитание	2%

О компании Commtouch

Основанная в 1991 году компания Commtouch, специализируется на изучении возникающих спам-активностей и разработке противоспамных продуктов. Многолетний опыт компании Commtouch в создании эффективных, массовых услуг масштабной безопасности привел к смягчению угроз сети Интернет для тысяч организаций и миллионов пользователей в 190 странах мира. Штаб-квартира компании расположена в Нетании, Израиль, а филиал в Саннивейл, Калифорния.

О компании Entensys

С 2001го года компания Entensys использует многолетний опыт разработки передовых технологий на IT-рынке для разработки решений в области безопасности Интернета и корпоративных коммункаций. Entensys уделяет большое внимание борьбе со спамом и сочетает использование собственных наработок и лучших сторонних решений. Компания также считает важным регулярно проводить исследования как в области Интернет-угроз, так и в плане общих тенденций использования Интернета.