Отчет о современных интернет-угрозах.
2 квартал 2011

Содержание

1 квартал 2011

119 миллиардов

Писем рассылается спамерами каждый день

Стр. 3

377,000 зомби

Ежедневно активизируются

Стр. 15

Потоковое медиа/Загрузки

Наиболее популярная тема в блогосфере

Стр. 16

Медицина и фармацевтика

Остается самой популярной темой спам-рассылок (24%)

Стр. 6

Индия

Рассылает больше всего спама (17%)

Стр. 15

Порнография

Наиболее востребованная категория сайтов у распространителей вирусов

Стр. 12

Введение

Отчетный квартал отметился самым низким за последние три года показателем среднесуточного количества отправляемых спам-сообщений. Данный факт по-прежнему чаще связывают с последствиями закрытия ботнета Rustock. Число активизируемых каждый день зомби напротив растет – Лаборатория Commtouch отмечает, что оборот зараженных рабочих станций увеличился более чем вдвое.

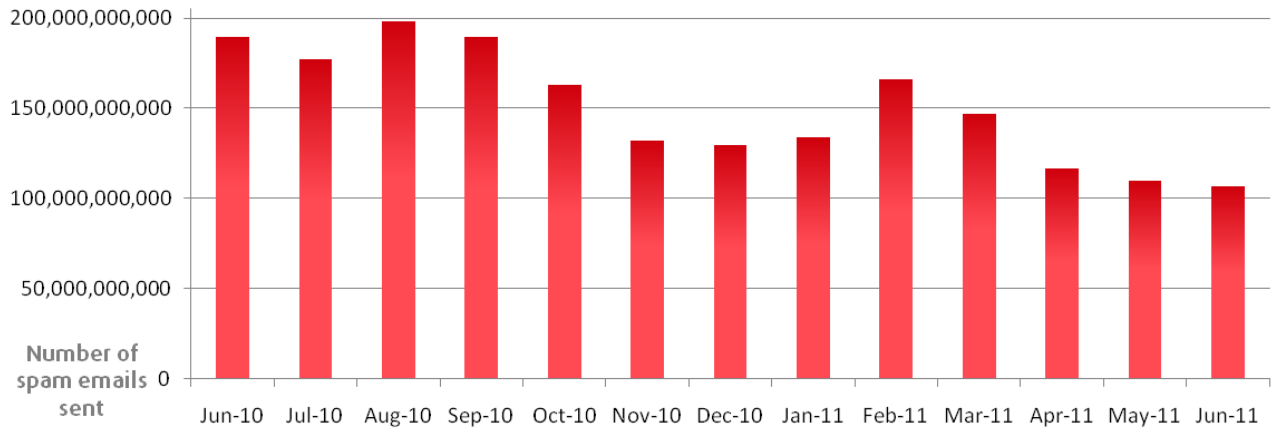
Огромные пользовательские базы Facebook остаются излюбленной мишенью для злоумышленников. На этот раз особую популярность имело сообщение со ссылками на различные видео, посвященные смерти Усама Бин Ладена.

В отчет о втором квартале включены многочисленные вспышки заражения вирусами, связанные с SEO, фальшивыми уведомлениями «Платеж отклонен» от IRS и вредоносными скриптами в PDF-вложениях. Всемирный день IPv6, празднуемый 8 июня, закрепил значимость замены IPv4, а также подчеркнул актуальность потенциальных угроз, сопровождающих внедрение новой технологии.

Тенденции в области спама

Изменения тактики спамеров

В середине марта Microsoft демонтировала ботнет Rustock. Вследствие этого уровень спама упал на 30% - среднее количество ежедневно рассылаемых сообщений составило 119 миллиардов сообщений в течение последних двух недель первого месяца весны. В прошлом, после закрытия крупных спам-сетей непременно имели место временное падение показателей, а затем стабильный рост активности вновь создаваемых ботнетов. Однако, предполагается, что этом квартале восстановление прежнего уровня спам-активности можно не ожидать. Спамеры заняты вопросом изменения тактики и подхода к своей деятельности. Среднесуточные показатели спама за год приведены ниже:



Источник: Commtouch.

Июньский уровень спама (106 млрд.) является самым низким за последние три года. На низшей точке июня, доля спама во всемирном почтовом сообщении составляла всего 75%.

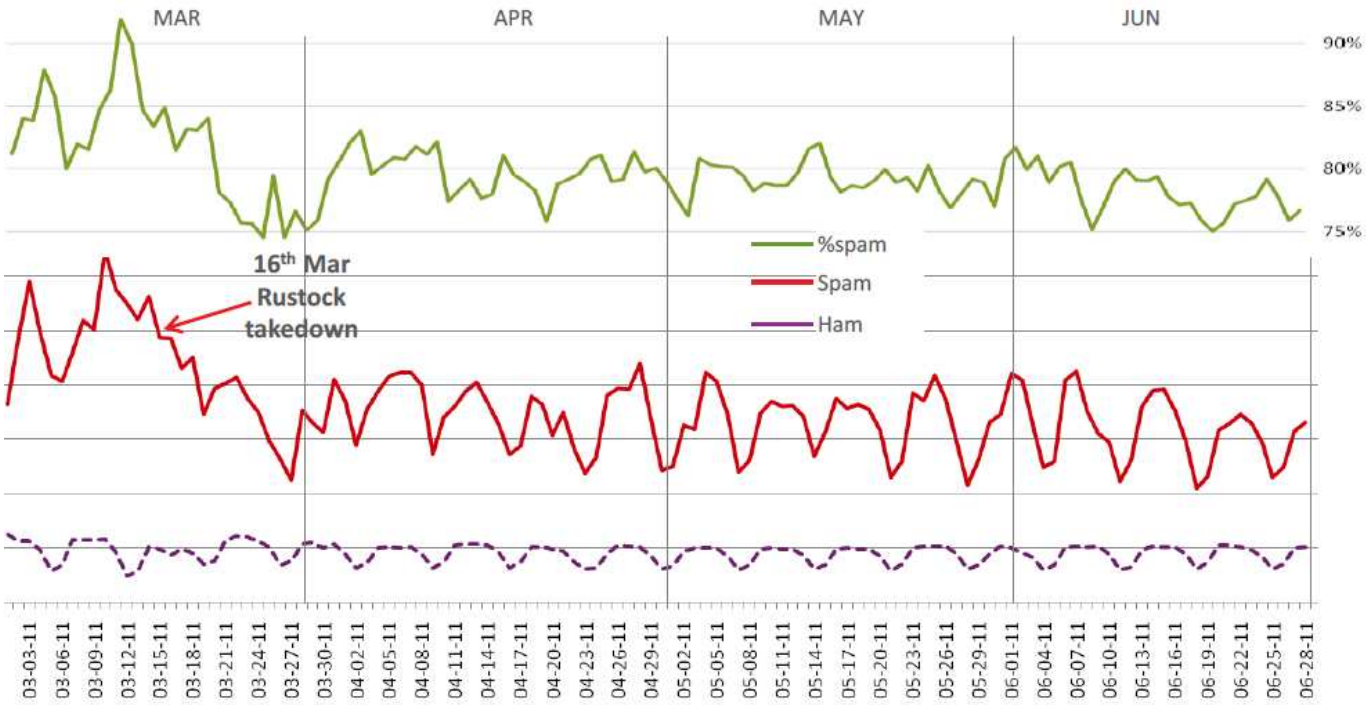
В дополнении к снижению уровня спама, следующие статистические показатели позволяют делать вывод об тактических переменах среди спамеров:

- После демонтажа Rustock последовала крупная вирусная атака через электронную почту;
- Число актизируемых ежедневно зомби удвоилось в течение нескольких недель после вирусных атак;
- Орда зомби не была использована для рассылки спама (причина снижение показателей в данной области), но замечена в вирусных атаках меньшего размера;
- Спам приходит со взломанных или спамерских учетных записей так же, как и со взломанных почтовых серверов.

Тактика использования взломанных аккаунтов для рассылки спама взамен ботнетам обусловлена наличием механизма блокировки зараженных рабочих станций, отправляющих нежелательные почтовые сообщения. Фильтрация спама от взломанных учетных записей по IP-адресу проблематична для большинства антиспам технологий, поскольку данные аккаунты включены в белый список IP-адресов, например, GMail и Hotmail.

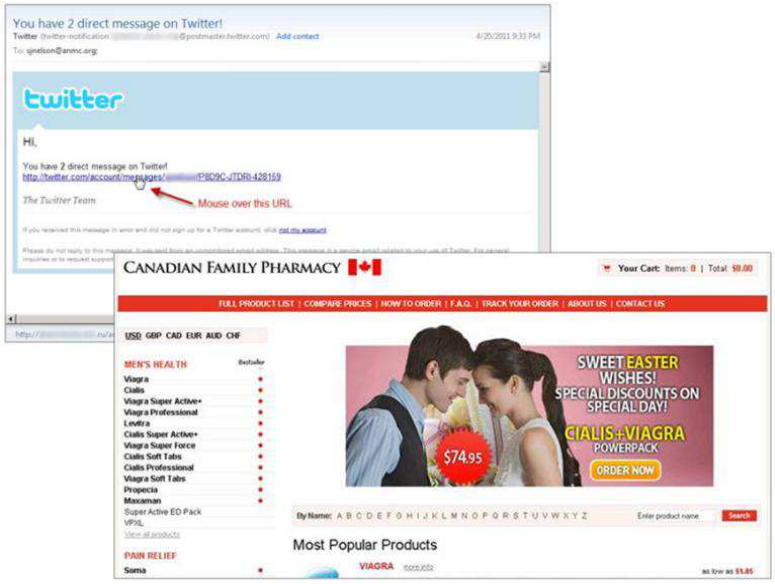
Одной из главных целей наибольших вирусных вспышек и фишинговых атак в данном квартале являлось заражение почтовых учетных записей пользователей для последующего их использования в качестве инструмента распространения спама.

Уловка для спамеров: До сих пор спам, отправленный со взломанных аккаунтов с меньшей вероятностью будет заблокирован системой репутации IP. Объем почтовых сообщений, которые можно отправить со взломанных учетных записей, ограничен лимитами, действующими для данных аккаунтов. Это частично объясняет низкие показатели спама в отчетном периоде.



Источник: Commtouch.

Несмотря на снижение уровня, спам, конечно же, не исчез из нашей жизни. В течение квартала поддельные уведомления от Twitter, содержащие ссылки на сайты с рекламой фармацевтики, заполонили почтовые ящики по всему миру. Пример почтового сообщения подобного характера взят из апрельской вспышки:

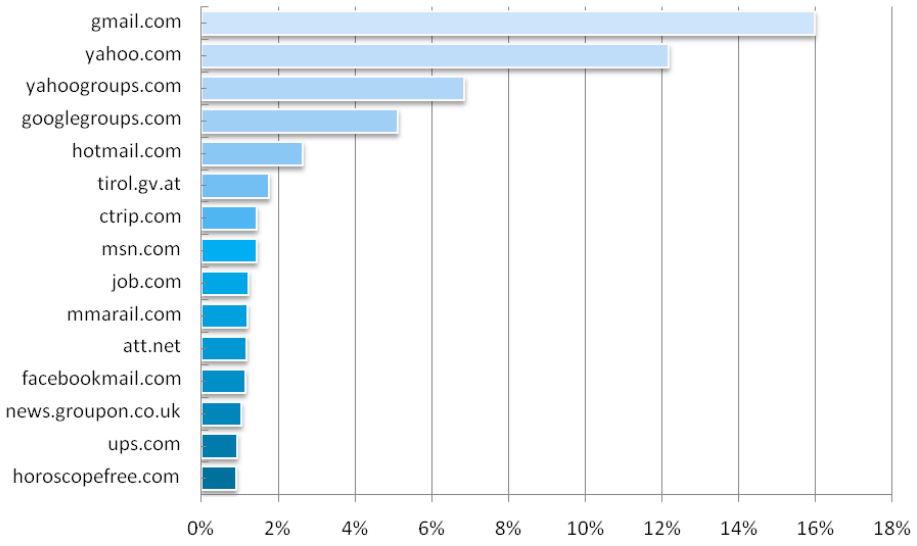


Источник: Commtouch.

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 этом квартале gmail.com вновь вернул себе лидерство. По причине многочисленности фальшивых уведомлений с UPS, отправленных в ходе вспышек спам-активности, домен ups.com занял 14-е место.

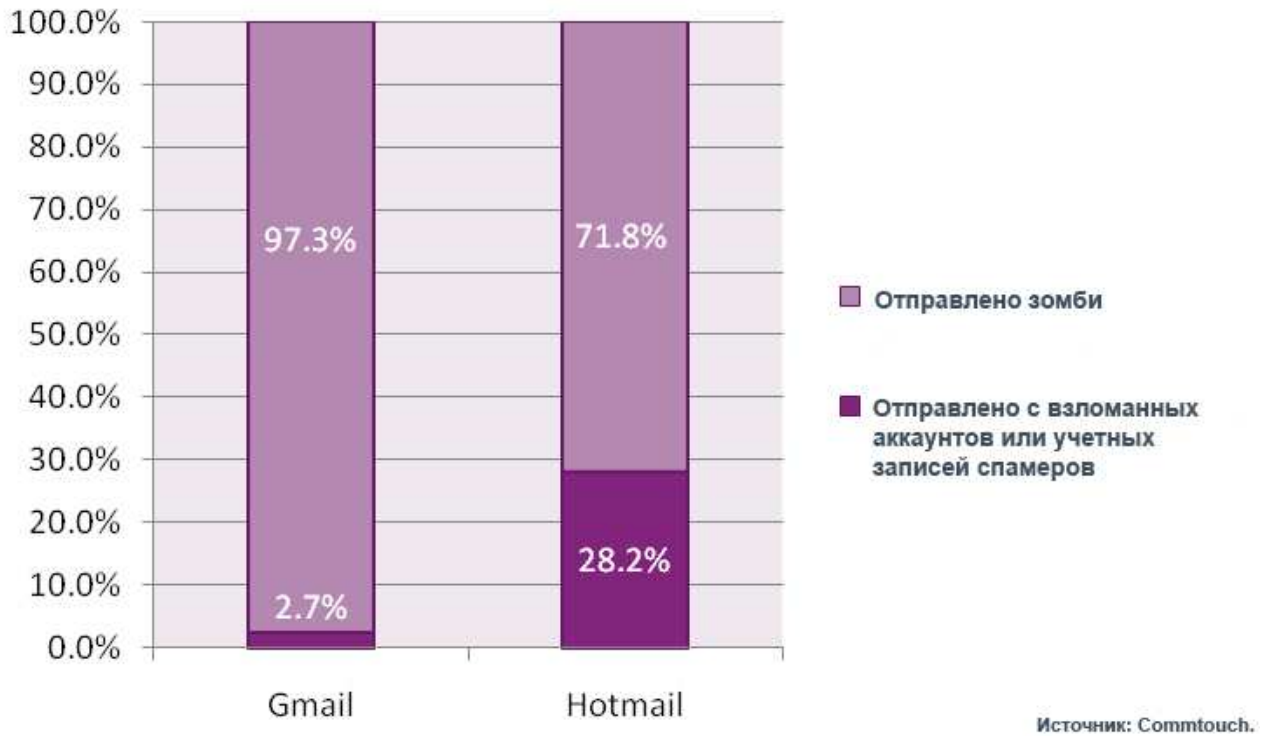


Источник: Commtouch.

Анализ взломанных аккаунтов

В дополнении к поддельным почтовым адресам, значительный процент писем от Gmail и Hotmail был отправлен с реально существующих аккаунтов. Они были взломаны или специально созданы спамерами для рассылки. График ниже наглядно показывает, какая часть всего спама была отправлена за текущий квартал с доменов gmail.com и hotmail.com.

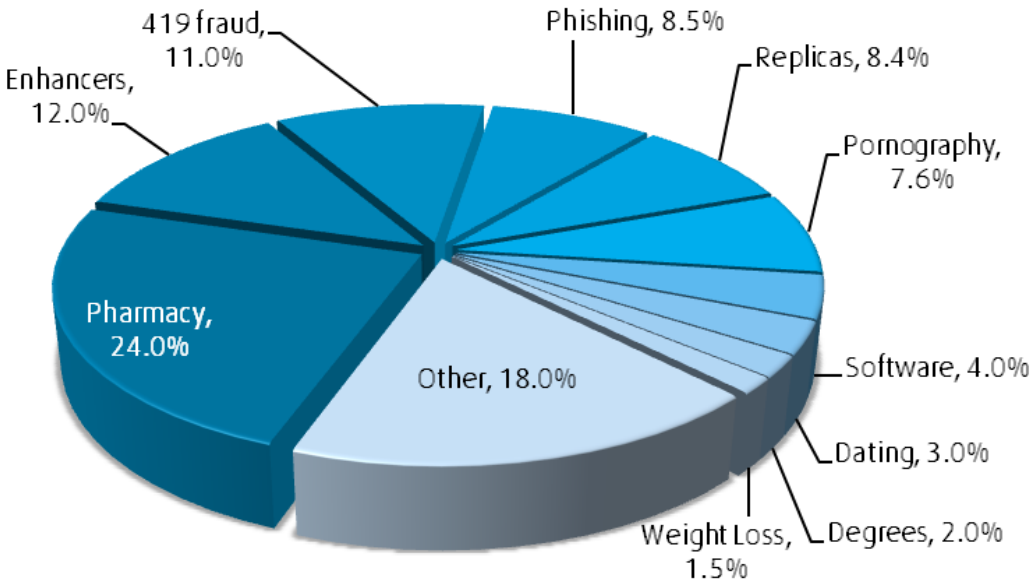
В результате анализа стало известно, что 30 процентов спама от Hotmail было направлено с реально существующих учетных записей: взломанных или специально созданных спамерами. В случае же с Gmail, чаще всего зомби просто подделывают адреса, использую «доброе имя» gmail.com.



Источник: Commtouch.

Тематика спама

Фармацевтический спам продолжает занимать первое место несмотря на снижение показателей в отчетном периоде до 24% (по сравнению с 28% в прошлом квартале).



Источник: Commtouch.

К традиционно рекламируемым посредством спама продуктам во во втором квартале 2011 года добавились электронные сигареты. На данный момент нет единого мнения о вреде данных устройств для здоровья, поэтому зачастую возникают разногласия между законодательствами стран относительно электронных сигарет. Часть стран запретили продажу подобных устройств, другая – ограничила реализацию электронных сигарет, остальные – переложили всю ответственность на местные органы самоуправления. Распространители спама не могли данную тему стороной. Они предлагают электронные сигареты каждому, кто имеет электронный адрес:

- Оптовые поставки электронных сигарет
- E-сигареты опт
- e-сигареты из Китая (опт)
- e-сигареты – из Азии (опт)

Спамеры из Франции отмечают пользу электронных сигарет для здоровья, ссылаясь на 4000 вредных веществ, содержащихся в обычной сигарете.

Источник: Commtouch.

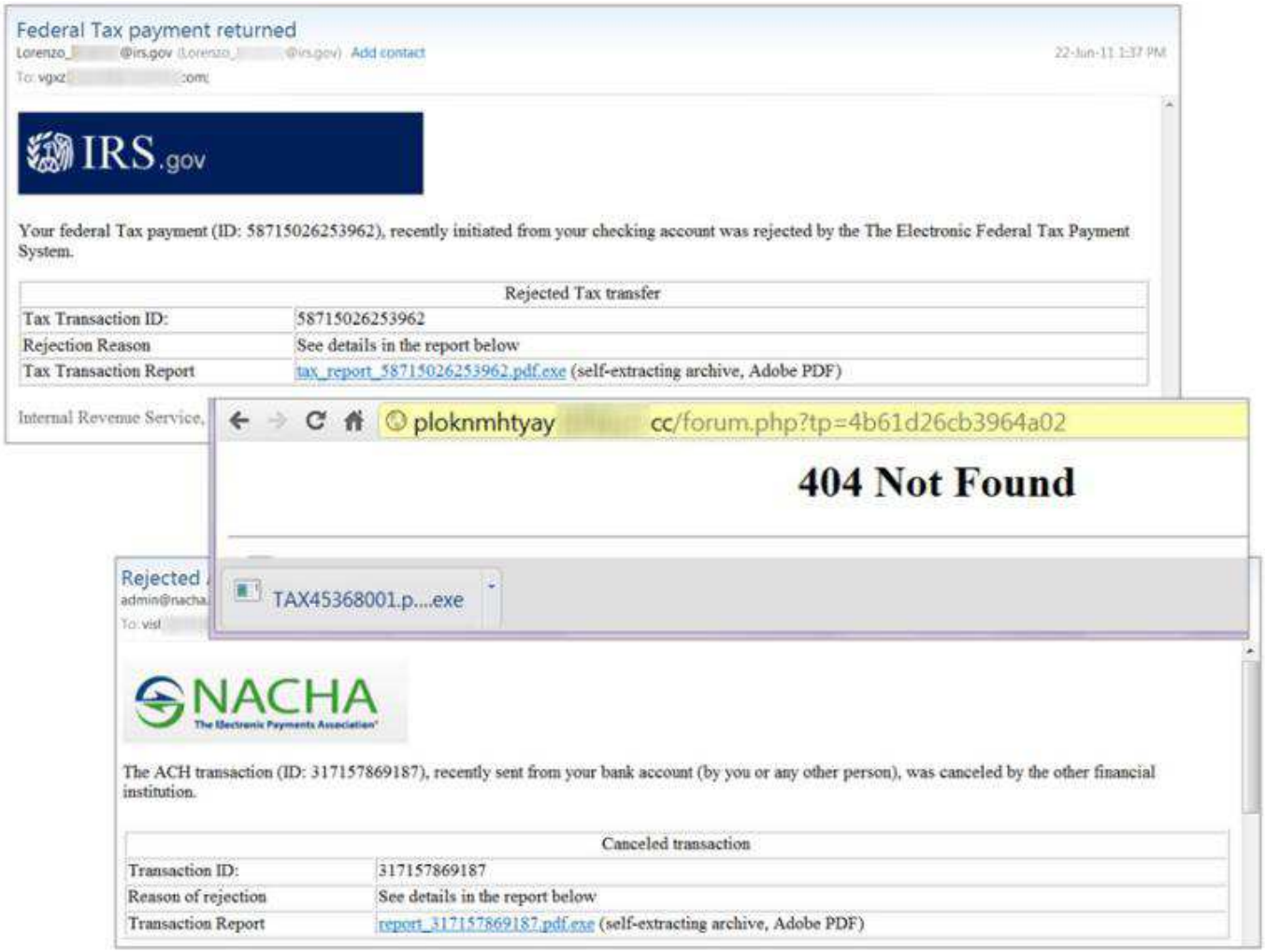
Вирусные тенденции

Первый квартал закончился большой вирусной атакой посредством электронной почты – в некоторые моменты подобные письма составляли до 30% всего почтового сообщения мира. На первом этапе вредоносные вложения содержали поддельные UPS-уведомления. Затем спамеры использовали в качестве прикрытия письма от компании DHL. В начале второго квартала атаки продолжились. На этот раз вирусы содержали уведомления от FedEx.

Источник: Commtouch.

IRS: «Ваш платеж отклонен!»

Электронные письма с поддельных адресов домена irs.gov были весьма популярным явлением в прошедшем Июне. Спамеры сообщали получателям писем об отказе по платежам через электронную систему IRS. Злоумышленники ссылались на отчет по налогам, объясняя расширение .exe тем, что файл является самораспаковывающимся архивом.



Источник: Commtouch.

Ссылки ведут на один из 2,500 доменом, зарегистрированных за 48 часов до начала атаки. Страницы содержат сообщение «404 not found», а также скрипт, запускающий параллельно скачивание PDF-файла. Загруженный файл содержит вирус, предназначение которого состоит в краже паролей.

Через неделю после данной вспышки, практически идентичный шаблон был использован для новой атаки – на этот раз злоумышленники использовали имя платежной системы NACHA.

CEO-оптимизация: фальшивые антивирусы

YeheyTV – интернет-ресурс, предлагающий для просмотра программы Филиппинского телевидения. Сайт существует с 2009 года и используется филиппинцами со всего мира. В июне распространители фальшивых антивирусов воспользовались доверчивостью интернет-пользователей, искавших сайт YeheyTV. По запросу «yeheytv pinoy», поисковые системы Google и Bing выдавали следующие результаты:

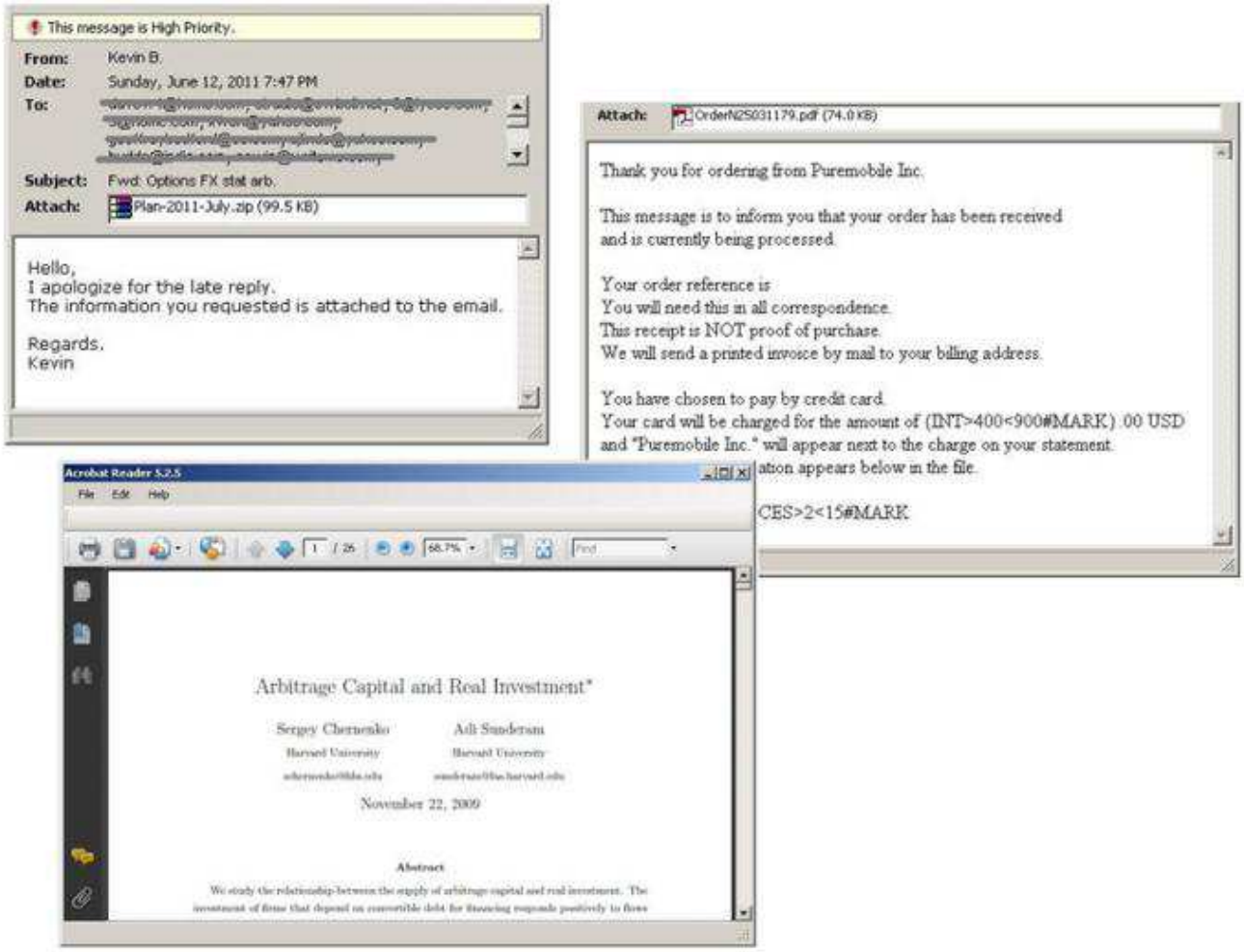
Источник: Commtouch.

Переход по обведенным красным ссылкам приводил к запуску сканирования страницы подделками антивирусных систем. Это стандартный прием, используемый злоумышленниками в качестве способа убедить пользователей загрузить вредоносные программы.

PDF-вирусы

PDF-файлы, а также скрывающиеся под маской PDF исполняемые файлы, весьма часто использовались в многочисленных атаках в течение второго квартала. Два примера представлены ниже:

Zip-архив содержит исполняемый файл, иконка для отображения которого позаимствована у файлов PDF-формата. Пользователей, отключивший возможность просмотра расширения файлов, думает, что перед ним стандартный PDF-документ. Запуск файла приводит к отображению незараженного PRF-документа в окне поддельного PDF-Reader'а.



Источник: Commtouch.

Затем вирус:

- Запоминает все действия и нажатия клавиш пользователя при работе в сети Интернет;
- Сохраняет полученные сведения на жестком диске в файле «updates2.txt»;
- Отправляет данный файл на адрес злоумышленника.

Второй пример PDF-вируса использует сложное кодирование с целью скрыть вредосный Java-скрипт. Поддельное подтверждение заказа в виде PDF-файла содержит то, что на первый взгляд может показаться обычным PNG-изображением. Обычно PNG-файл используется для кодирования изображения, но в этот раз графический файл является электронной формой. Данная форма (в формате XFA) содержит зараженный Java-скрипт.

Top-10 вирусов

В таблице ниже представлен список 10 самых популярных вирусов, составленный Commtouch's Command Antivirus Lab.

Место	Название вредоносного ПО
1	IFrame.gen
2	W32/Ramnit.E

3	W32/Worm.BAOX
4	W32/RAHack.A.gen!Eldorado
5	W32/Sality.gen2
6	W32/Worm.MWD
7	W32/VBTrojan.17E!Maximus
8	W32/Ramnit.D
9	W32/Mydoom.O@mm
10	W32/Vobfus.L.gen!Eldorado

Интернет-безопасность

Защищенный Facebook

Постоянно растущая база пользователей Facebook продолжает привлекать кибер--преступников по всему миру. Использование социальной сети в качестве платформы для распространения вирусов не только предоставляет ряд преимуществ, но и несет в себе ряд трудностей. Привлекательным для злоумышленника является доверие пользователей Facebook к приходящим от друзей сообщениям, ссылкам и приглашениям. В то же время кибер-преступники сталкиваются со сложностями в процессе своей деятельности на платформе, разработанной Цукербергом:

1. Необходимость взлома аккаунтов – сообщения и приглашения можно отправить только друзьям;

2. Атаки ограничены несколькими сотнями людей, и Facebook разработали систему отслеживания массовой рассылки одинаковых сообщений.

Таким образом, спам и вирусы, отправляемые с помощью обычной электронной почты, покрывают большую аудиторию.

Взломанные сайты

Киберпреступники часто взламывают сайты с целью размещения вредоносных программ и фишинга. Подобный подход имеет следующие преимущества:

1. Легитимные домены имеют хорошую репутацию среди URL-фильтров, следовательно, с меньшей вероятностью будут заблокированы.

2. Взломанный сайт предоставляет бесплатный хостинг для размещения фишинговых страниц и вирусов.

Вирус «IPhone 5»

В мае весьма распространенным явлением стала рассылка писем, информирующих общественность о выходе «iPhone 5G S». В сообщении описывались особенности нового устройства, например, более тонкий дисплей, высокая скорость работы и прочее. Все картинки и ссылки веди на файл «iphone5.gif», на самом деле являющимся вирусом «iphone5.gif.exe».

Источник: Commtouch.

Любое нажатие клавиши мышки при нахождении курсора в области письма приведет к загрузке вредоносных файлов. При более подробном рассмотрении ссылки, указанной в сообщении, видно, что вирус скрыт на взломанном сайте. Ниже представлен пример исходной страницы:

Категории зараженных сайтов

В течение второго квартала 2011 года Лаборатория Commtouch анализировала категории веб-сайтов, которые наиболее часто содержат вредоносные программы. Порносайты вновь занимают первую строчку в данном рейтинге. Стоит отметить, что зачастую размещение вирусов на сайте одобрено владельцами ресурса.

Категории сайтов, содержащих вредоносные программы			
Место	Категория	Место	Категория
1	Порнография	6	Бизнес
2	Предоставление доменов	7	Медицина и здоровье
3	Порталы	8	Путешествия
4	Образование	9	Компьютеры и технологии
5	Развлечение	10	Мода и красота

Тенденции в области фишинга

Продолжаются фишинг-атаки на банки, пользователей почты и Facebook, а также игровые сайты.

Взломанные аккаунты Facebook весьма ценятся среди злоумышленников. Доступ к учетной записи позволяет осуществлять взаимодействие с многочисленными «друзьями» пользователя. Фишинговая страница для Facebook представлена в примере. Владельцу аккаунта предлагают увеличить уровень защиты учетной записи. Для этого пользователь должен ввести свои реальные данные в специальную форму. Конечно же, логины и пароли становятся добычей фишера.

Источник: Commtouch.

Прогресс фишинговых сайтов

Для защиты от клавиатурных шпионов некоторые финансовые учреждения добавили на страницу входа на сайт дополнительную экранную клавиатуру. Фишеры не стоят на месте. В примере мы можем увидеть фишинговую страницу ADCB (Коммерческий банк Абу Даби), на которой успешно имитируется виртуальная клавиатура с реального сайта организации. Пароль к учетной записи можно ввести только таким способом.

Источник: Commtouch.

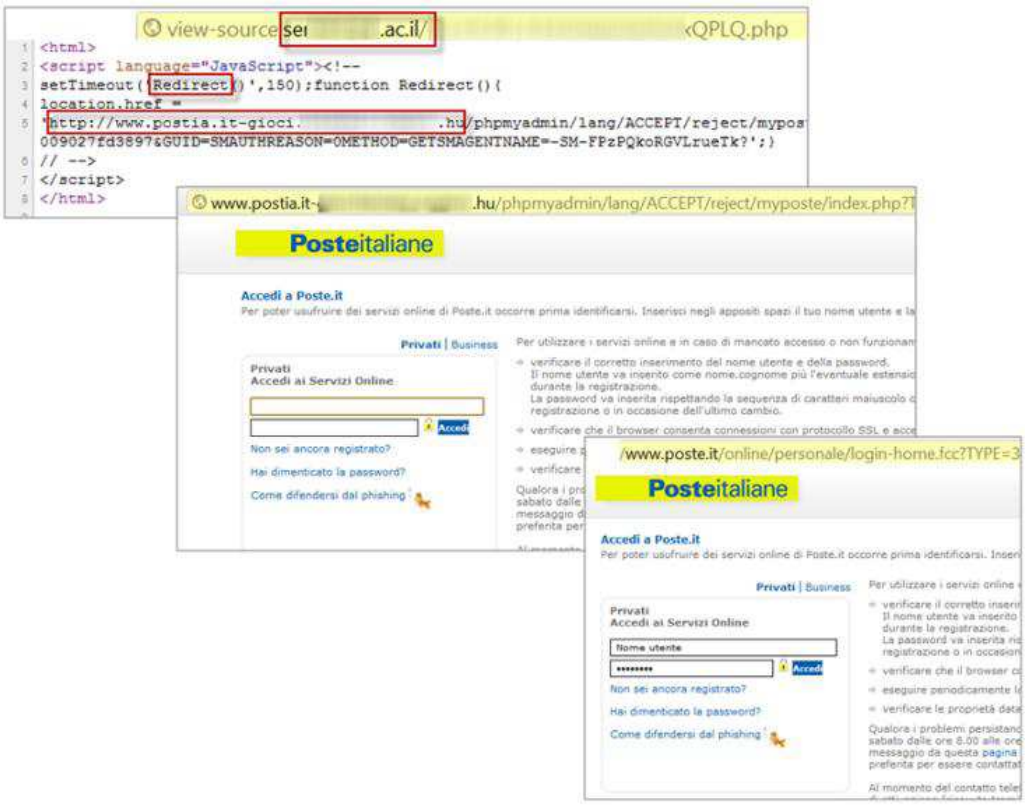
Предпочтения фишеров

В течение второй квартала 2011 года 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	Мода и красота
2	Порталы	7	Досуг и отдых
3	Покупки	8	Спорт
4	Форумы	9	Образование
5	Некоммерческие организации и партнерства	10	Бизнес

Глобальная структура фишинга

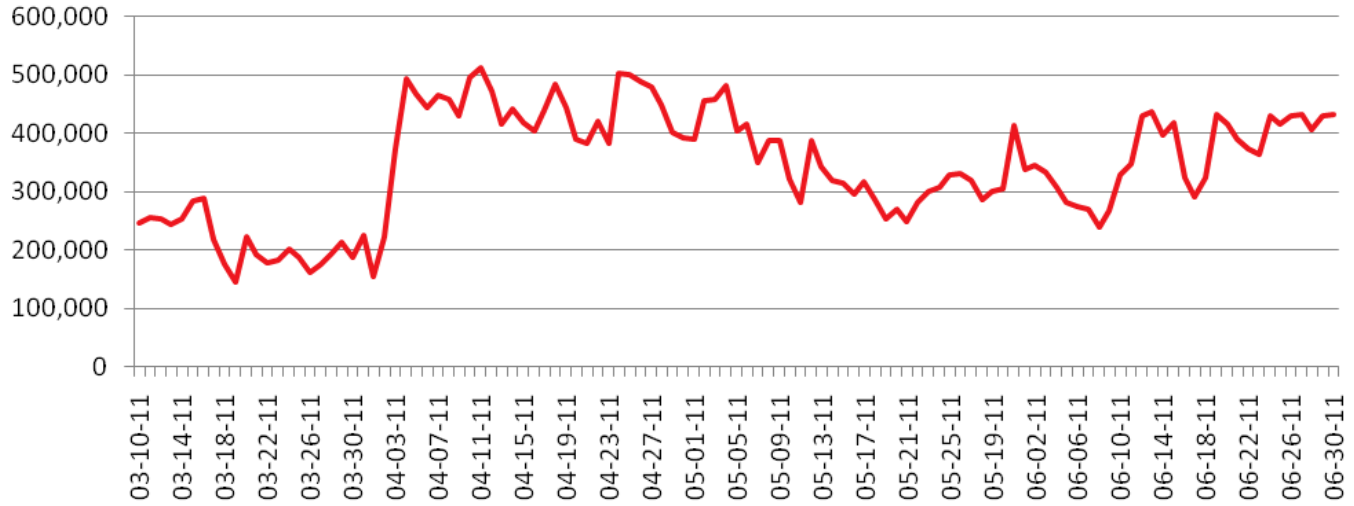
Взломанные сайты не всегда являются местом размещения фишинговых страниц, но они по-прежнему представляют опасность для пользователей. В приведенном примере ресурс израильского учебного заведения просто перенаправляет пользователя на фишинг-страницу, которая находится на одном из доменов в Венгрии. Фишер стремится украсть данные клиентов итальянской компании, предоставляющей банковские услуги Онлайн. Эта многонациональная фишинг-схема демонстрирует глобальную структуру индустрии фишинга.



Источник: Commtouch.

Зомби

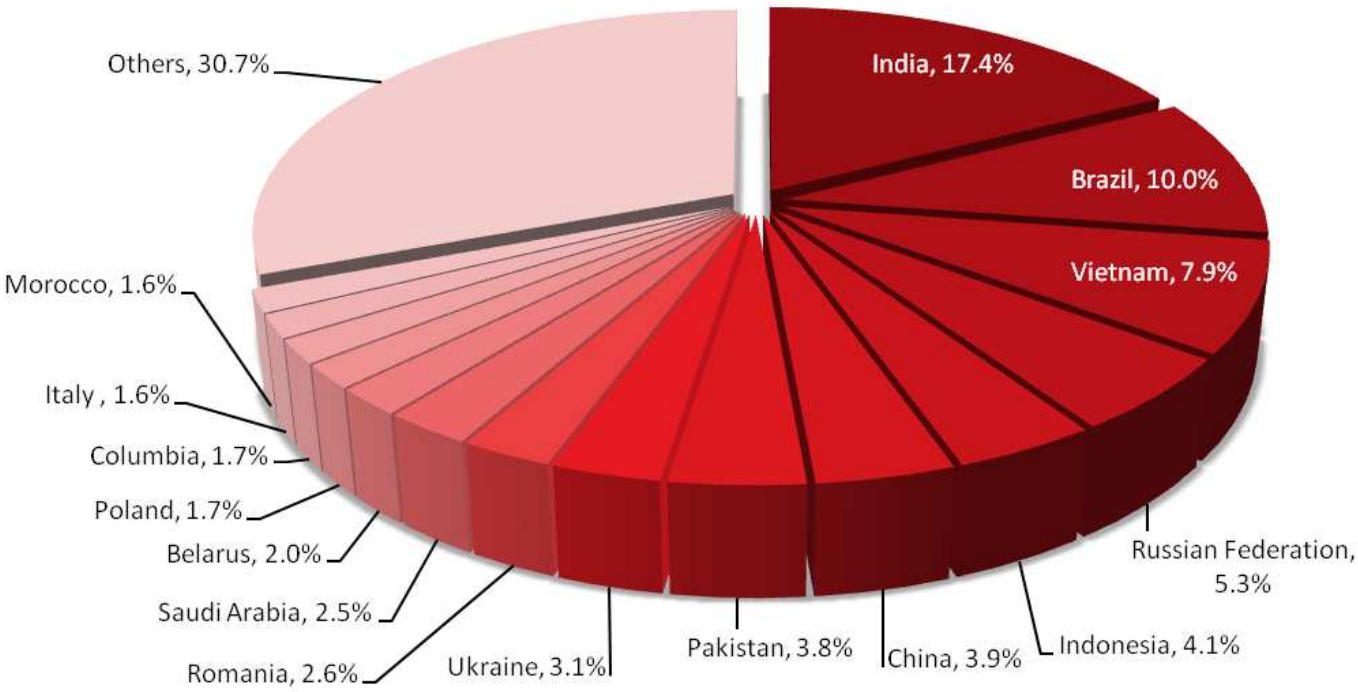
В отчетном квартале каждый день для распространения спама и вирусов активировались 377,000 зомби. Таким образом, данный показатель значительно вырос по сравнению с 258,000 в первом квартале. Крупная вирусная атака в конце марта привела к появлению большого числа новых зомби. Стоит отметить, что после данной активности количество активируемых каждый день зараженных рабочих станций выросло более чем вдвое.



Источник: Commtouch.

Горячие точки зомби

Индия с показателем 17% от общей численности зараженных рабочих станций вновь занимает первое место среди стран-хостеров зомби. Бразилия, Вьетнам и Россия также сохранили свои места. Перу и Аргентина покинули ТОП-15. Их сменили Румыния и Морокко.



Источник: Commtouch.

IPv6 – новые возможности для зомби

8 июня было днем глобального перехода на IPv6, когда ведущие веб-сайты и Интернет-провайдеры по всему миру, включая Google, Facebook, Yahoo! и Commtouch объединились с более чем 1000 других электронных ресурсов для полномасштабного испытания нового Интернет-протокола. Глобальное внедрение IPv6 помимо всего прочего таит в себе множество угроз.

В диапазоне IPv4, зомби чаще всего связаны с одним IP-адресом в силу ограниченности количества доступных адресов. Внедрение IPv6 открывает перед зараженными рабочими станциями большие возможности. После блокирования одного адреса, зомби может перейти на другой IP. Запрет доступа для диапазона адресов также не является эффективным по следующим причинам:

- Данный диапазон может использоваться пользователями, не имеющими отношения к злоумышленникам;
- На данный момент не существует стандартного распределения IP-адресов, поэтому достаточно сложно понять, какой диапазон адресов необходимо заблокировать.

Лаборатория Commtouch начала отслеживать активность зомби, функционирующих на IPv6. Следующие отчеты по Интернет-угрозам будут подготовлены уже с учетом данных, полученных в ходе анализа деятельности злоумышленников на новом протоколе.

Тенденции Web 2.0

Commtouch's GlobalView URL Filtering service включает в себя классификацию контента Веб 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» включает сайты с архивами медиа для загрузки или потоковый контент, такой как Интернет-радио, Интернет-телевидение или MP3-файлы. Развлекательные блоги, как правило, затрагивают телевидение, фильмы, музыку, а также сайты фан-клубов звезд и развлекательные новости.

Место	Категория	Проценты	Место	Категория	Проценты
1	Потоковое мультимедиа и загрузки	21%	8	Религия	4%
2	Развлечения	9%	9	Спорт	4%
3	Компьютеры и технология	8%	10	Рестораны и питание	4%
4	Покупки	5%	11	Образование	3%
5	Порнография	5%	12	Досуг и отдых	3%
6	Искусство	4%	13	Здоровье и медицина	3%
7	Красота и мода	4%	14	Игры	2%

Источник: Commtouch.

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.