Аналитический отчет

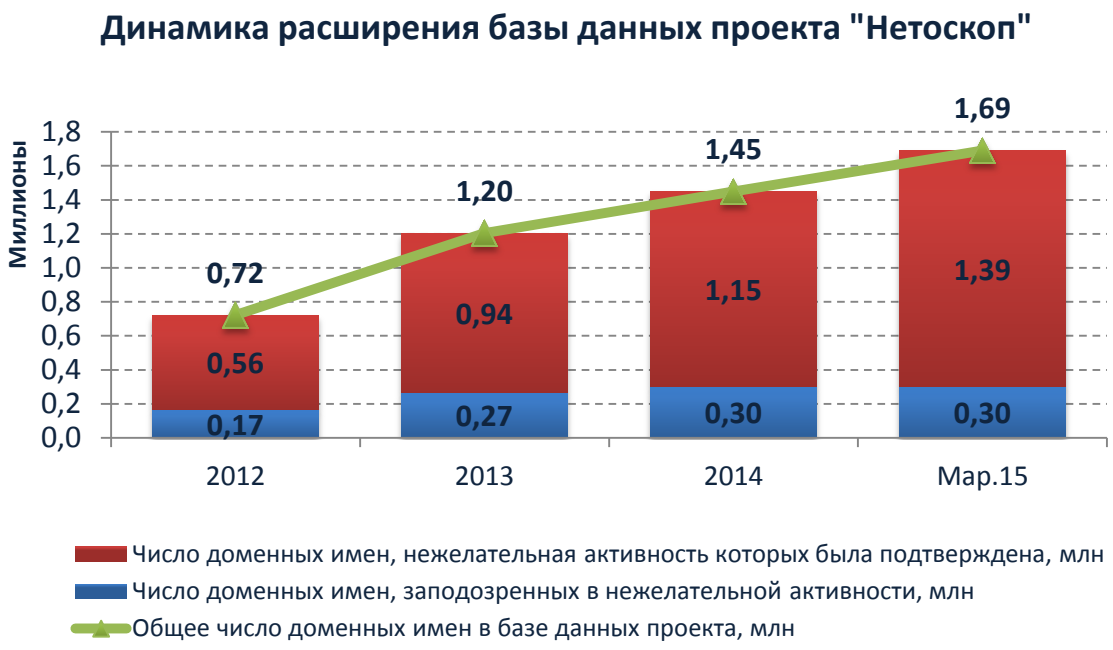
«НЕТОСКОП. Март 2015»

Информационно-аналитический проект Координационного центра национального домена сети Интернет

(Статистика по полученным данным)

По данным на 31.03.2015

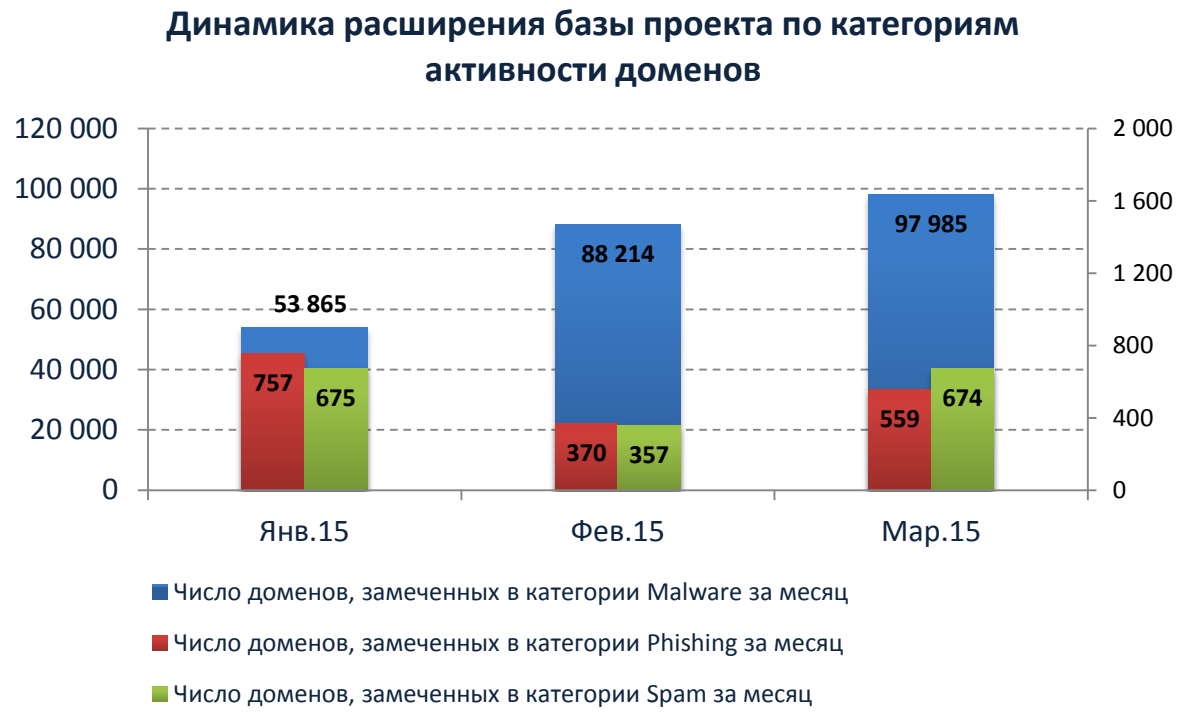
Сбор данных начался в ноябре 2012 года одновременно с началом работы исследовательской платформы для агрегации информации о вредоносных ресурсах. По итогам марта 2015 года зафиксировано 1 689 158 доменных имен, хотя бы раз за этот период (ноябрь 2012 - март 2015) замеченных или заподозренных в нежелательной активности. Все домены внесены в базу в соответствии со сведениями, предоставленными участниками проекта. За время работы проекта объем базы увеличился более чем в два раза и продолжает стабильно расти. Домены, попавшие в поле зрения экспертов проекта, не удаляются и учитываются в дальнейших исследованиях.



В настоящее время 17,8% базы (301 071 домен) составляют доменные имена, нежелательная активность которых не была подтверждена в наиболее значимых категориях: распространение вредоносного ПО, фишинг и спам. Эти доменные имена по ряду критериев составляют «группу риска», и по ним проводится дополнительный мониторинг.

За отчетный месяц база проекта пополнилась информацией о 97 495 вредоносных доменах.

Анализ динамики пополнения базы проекта в марте 2015 года свидетельствует о том, что наибольшей популярностью у нарушителей пользуется такой вид деятельности как размещение на сайтах в сети вредоносного кода. При этом прирост числа ресурсов, связанных с определенными категориями активности (99 218) превышает показатель прироста базы проекта за месяц (97 495). Данный факт объясняется тем, что вредоносный код, спам и фишинг были выявлены не только на вновь попавших в базу ресурсах, но и на доменах, которые уже числились в базе данных проекта, но были связаны с другими видами нежелательной активности.



Источники информации проекта «Нетоскоп»

Основными источниками поступления информации о доменах с нежелательной активностью в ноябре остаются Лаборатория Касперского (96 109 доменов в марте), и RU-CERT (2 167 доменов). С компаниями Yandex и Mail.Ru Group эти организации являются сегодня крупнейшими исследователями безопасности киберпространства и основными борцами со зловредными доменными именами в Рунете.

Mail.Ru Group – одна из крупнейших российских интернет-компаний, услугами которой пользуется множество российских граждан, подключилась к проекту в марте 2014 года. Сотрудничество осуществляется с подразделением «Антиспам Mail.Ru», которое занимается вопросами безопасности в рамках почтовой системы Mail.Ru.

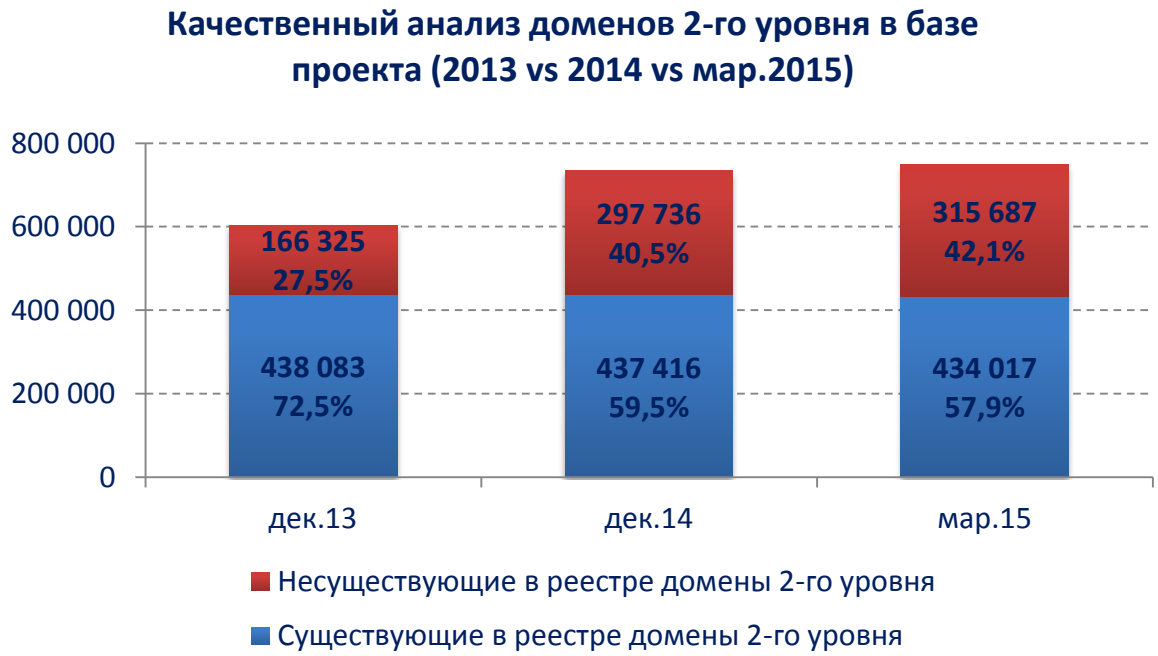
Компания Yandex поддерживает собственный продукт Safe Browsing API —интерфейс, позволяющий проверять URL на наличие в списках документов, представляющих угрозу. Списки созданы и поддерживаются Яндексом. Документы, представляющие угрозу, могут быть разделены на две группы: «malware» (приводят к исполнению вредоносного кода) и «phishing» (запрос конфиденциальных данных пользователя для дальнейшего несанкционированного использования). По итогам марта 2015 года Яндексом дополнительно отмечено 20 499 домена из базы данных «Нетоскоп».

Общее количество доменов (98 276), информация о которых поступила из разных источников, выше показателя прироста базы проекта за текущий месяц, который составил 97 495 доменов. Наличие разницы обусловлено тем фактом, что информация об одном домене может поступать (и поступает) из разных источников. 781 домен, добавленных в базу в марте 2015 года, были замечены в нежелательной активности несколькими источниками.

База данных «Нетоскопа» включает в себя исключительно доменные имена, отмеченные в нежелательной активности по технологическим признакам: вопросы анализа контента не входят в компетенцию «Нетоскопа» и не рассматриваются при сборе данных.

Распределение «зловредов» в российских доменах верхнего уровня .RU, .РФ, .SU

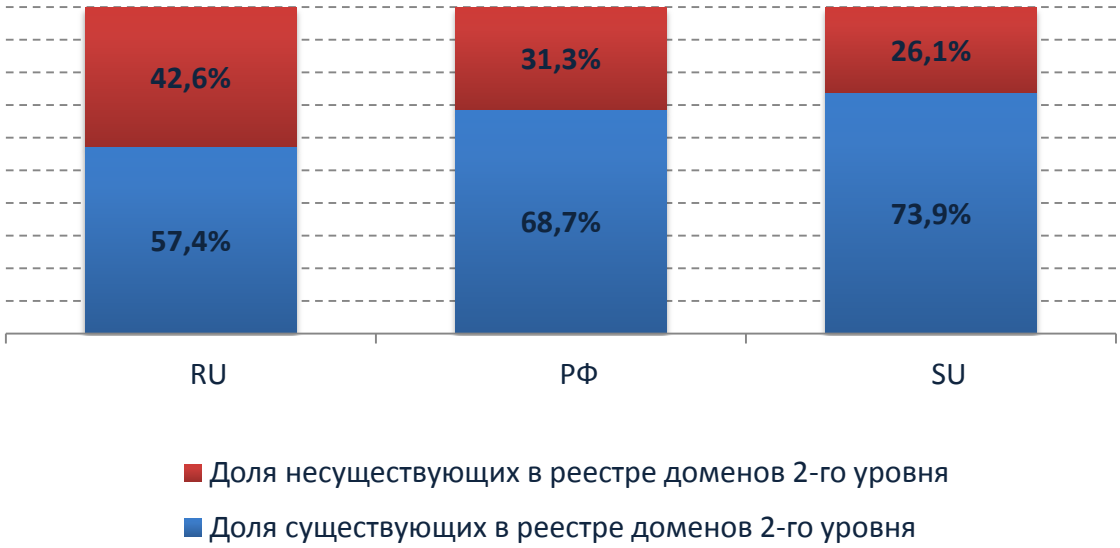
Чуть менее половины (44,4%) исследуемых доменных имен – это доменные имена второго уровня. Факт их существования в настоящее время может быть установлен путем проверки наличия информации о таких именах в реестре соответствующего домена верхнего уровня. По состоянию на конец месяца существующие в реестре доменные имена составляют 57,9% от общего числа доменных имен второго уровня в базе данных проекта. Доменные имена, администраторы которых не устраняют причины попадания домена в базу данных проекта "Нетоскоп", постепенно удаляются из реестров и переходят в категорию несуществующих.



Распределение долей между существующими и несуществующими* доменными именами второго уровня продолжает изменяться в сторону последних. В марте 2015 года доля удаленных из реестра доменов составила 42,1%, в то время как в конце 2013 года она составляла 27,5%, а в сентябре 2013 года – 21,5%. В марте 2015 года продолжается снижаться не только доля существующих в реестре доменных имен, ранее замеченных в нежелательной активности, но и их абсолютное число по сравнению с аналогичным показателем 2013-2014 года. Такие изменения свидетельствуют, что комплекс мероприятий по очистке Рунета от «зловредов» постепенно приносит плоды.

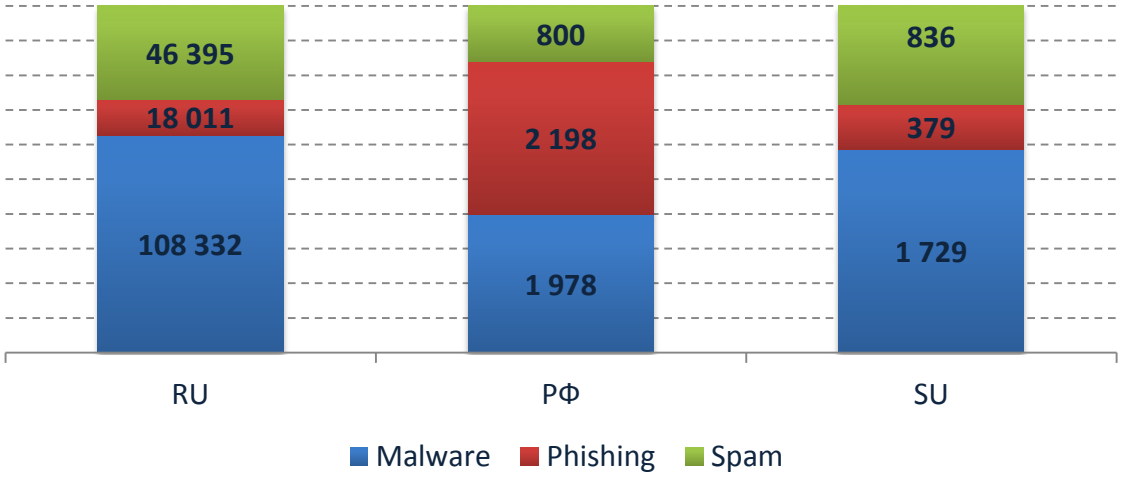
**Несуществующие доменные имена – это имена, ранее замеченные в зловредной активности, и удаленные из реестров соответствующих доменов верхних уровней.*

Качественный анализ доменов 2-го уровня по зонам Рунета (март 2015 года)



Основная масса доменов базы замечена в распространении вредоносного ПО. При этом если в доменах .RU и .SU среди “зловредов” преобладают доменные имена, распространяющие вредоносное ПО, то в .РФ преобладают имена, связанные с распространением фишинга.

Распределение доменов "зловредов" в Рунете по категориям активности (март 2015)



**Под зловредами в контексте данного исследования понимаются доменные имена 2-го уровня, нежелательная активность которых была ранее подтверждена, и которые продолжают существовать в реестре соответствующего домена верхнего уровня.*

На графике ниже представлена информация о том, как изменяется «жизненный статус» «зловредных» доменов с течением времени. Из доменов, нежелательная активность которых подтверждалась источниками проекта Нетоскоп в конце 2013 года, продолжают существование в реестре менее 20%. Чем ближе к сегодняшнему дню, тем выше доля доменов, которые продолжают существование, так как применение различных мер воздействия на «зловредов» требует времени даже в сетевом пространстве.

Важнейшим же результатом работы Нетоскопа является не только постепенное уменьшение числа «плохих» доменов, но и налаживание постоянного обмена данными о доменных именах, замеченных во вредоносной активности, между участниками проекта, а также предоставление этой информации всем, кто в ней заинтересован.

В целом, можно констатировать, что пространство Рунета становится чище. Участники проекта «Нетоскоп» приложат все усилия для сохранения такой тенденции в наступившем году.

О проекте:

Проект Координационного центра национального домена сети Интернет «Нетоскоп» – это первый в России информационно-аналитический ресурс, посвященный информационной безопасности в доменном пространстве. На сайте публикуются информационные, справочные и аналитические материалы о распространении «зловредов» в сети Интернет и ходе борьбы с вредоносными ресурсами.

http://нетоскоп.рф
http://netoscope.ru