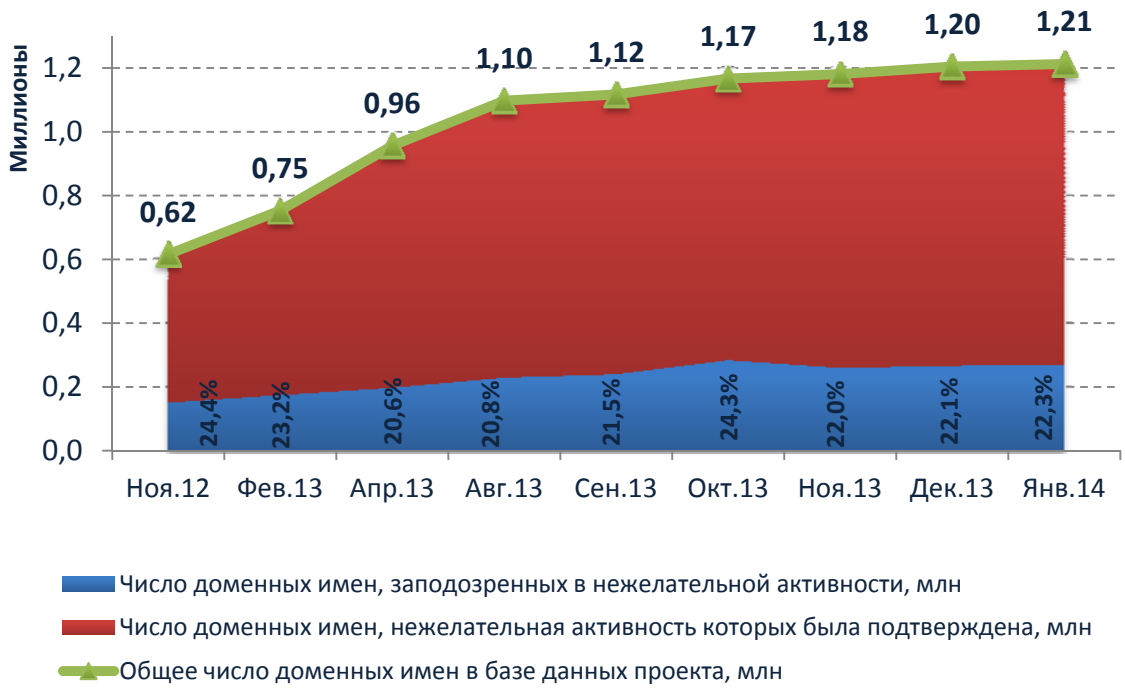
Аналитический отчет
«НЕТОСКОП. Январь 2014»

Информационно-аналитический проект
Координационного центра национального домена сети Интернет
(Статистика по полученным данным)

По данным на 31.01.2014

Сбор данных начался в ноябре 2012 года одновременно с началом работы исследовательской платформы для агрегации информации о вредоносных ресурсах. По итогам января 2014 года зафиксировано 1 212 478 доменных имен, хотя бы раз за этот период (ноябрь 2012-январь 2014) 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 вдвое и продолжает стабильно расти. Домены, попавшие в поле зрения экспертов проекта, не удаляются и учитываются в дальнейших исследованиях. В настоящее время 22% базы 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 7 896 вредоносных доменах.

Динамика расширения базы данных проекта "Нетоскоп"



Практически половина (50,5%) 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 70,8% 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.

Качественный анализ доменов 2-го уровня в базе проекта (по состоянию на конец января 2014 года)

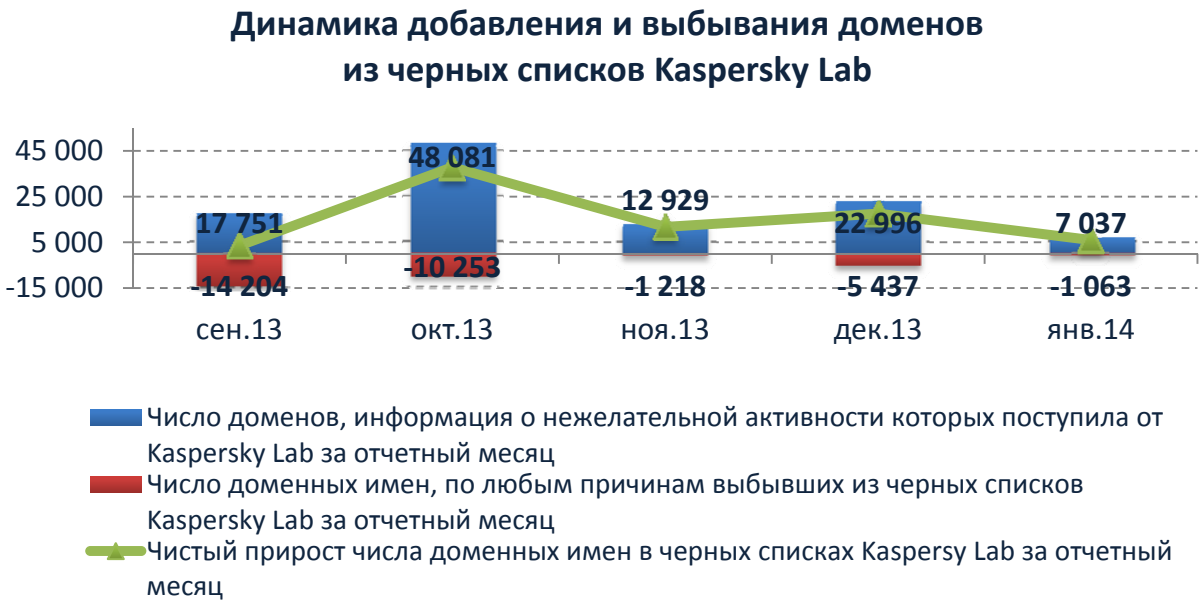
Распределение долей между существующими и несуществующими* доменными именами второго уровня продолжает изменяться в сторону последних. В начале 2014 года доля удаленных из реестра доменов составила 29,2%, в то время как в конце 2013 года она составляла 27,5%, а в сентябре – 21,5%. Такой рост свидетельствует, 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.*

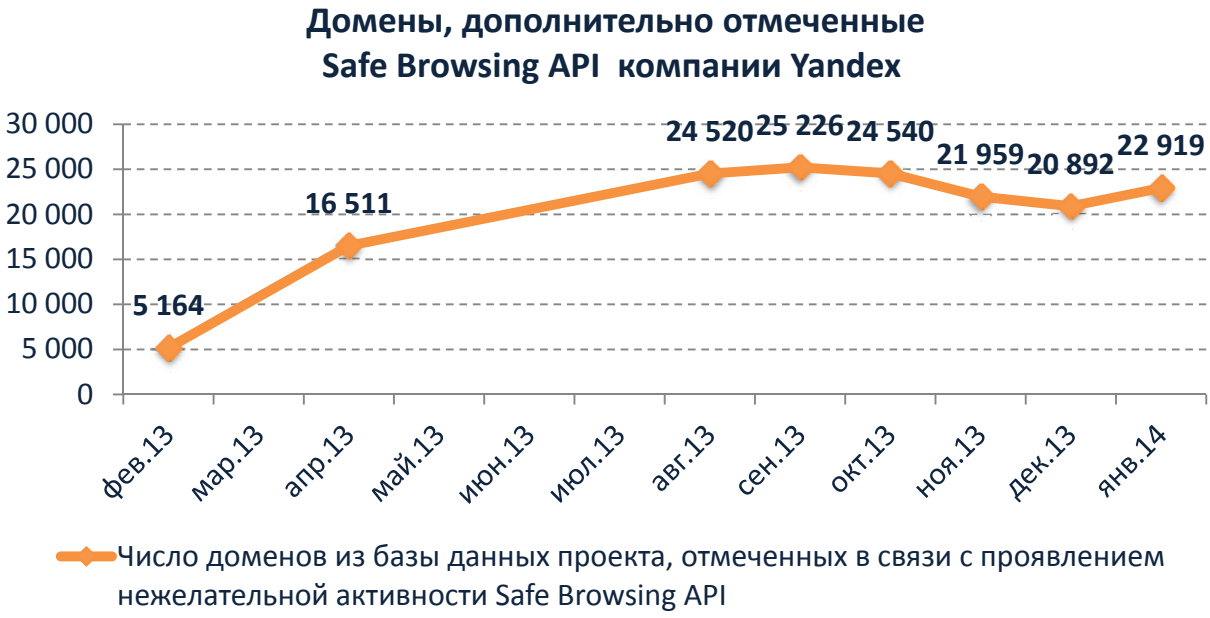
Источники информации проекта «Нетоскоп»

Основными источниками поступления информации о доменах с нежелательной активностью продолжают оставаться Лаборатория Касперского (7 037 новых доменных имен за январь) и RU-CERT (1206 новых доменных имени). Кроме того, на отдельном графике ниже продемонстрирована работа в этой области, проводимая компанией Yandex. Все эти компании являются сегодня крупнейшими исследователями безопасности киберпространства и основными борцами со зловредными доменными именами в Рунете. 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.

Общее количество доменов (8 243), информация о которых поступила из разных источников, выше показателя прироста базы проекта за текущий месяц, который составил 7 896 домена. Возникновение разницы обусловлено тем фактом, что информация об одном домене может поступать (и поступает) из разных источников. В январе 2014 года 347 доменных имен были замечены в нежелательной активности как компанией Kaspersky Lab, так и организацией RU-CERT.



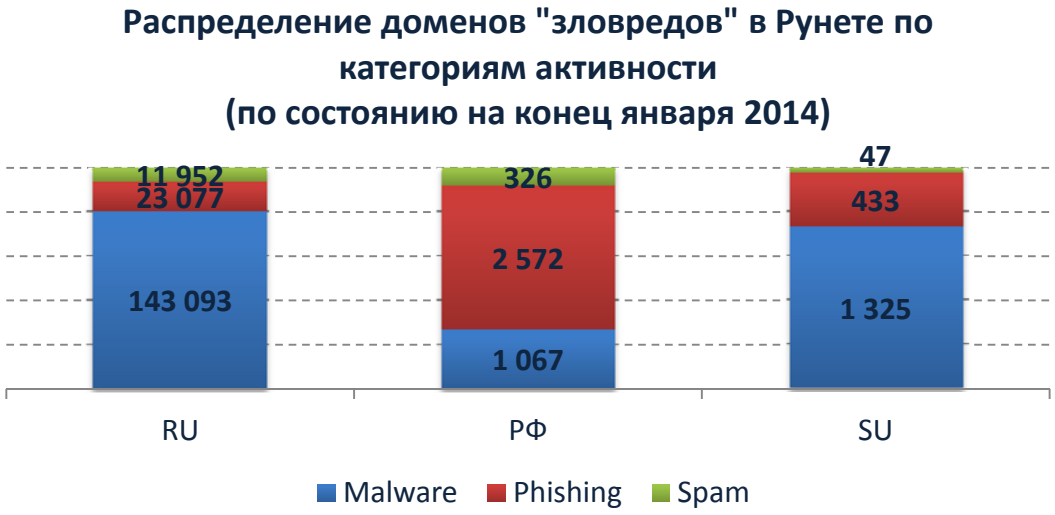
За январь 2014 года из «черных списков» Лаборатории Касперского выбыло 1 063 вредоносных домена. Речь идет как о тех доменных именах, делегирование которых было прекращено, так и о доменах, администраторы которых устранили причины попадания домена в базу данных «Нетоскопа». Всего с ноября 2012 года из черных списков компании была удалена информация о нежелательной активности 245 980 доменов.

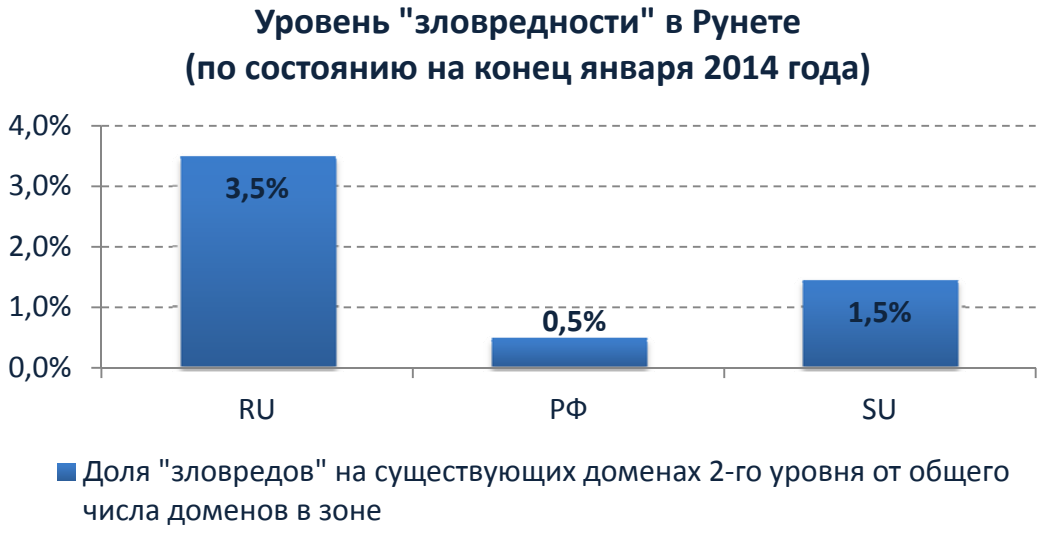


Safe Browsing API — программный интерфейс, позволяющий проверять URL на наличие в списках документов, представляющих угрозу. Списки созданы и поддерживаются Яндексом. Документы, представляющие угрозу, могут быть разделены на две группы: «malware» (приводят к исполнению вредоносного кода) и «phishing» (запрос конфиденциальных данных пользователя для дальнейшего несанкционированного использования). Важно отметить, что после начала сотрудничества количество доменных имен, отмеченных сервисом Яндекса, выросло более чем в 4 раза.

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

Среди доменных имен второго уровня доля «зловредов»* в домене .RU составляет 3,5%, в .РФ – 0,5% и в .SU – 1,5%. 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, связанных с распространением фишинга.





**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.*

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