Вредоносное ПО, фишинг и ботнеты в национальных доменах .RU, .SU, .РФ, .ДЕТИ, .TATAR

(проект: NETOSCOPE.RU)

Павел Храмцов
p.khramtsov@msk-ix.ru

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. Посетителям ресурса доступен онлайн-сервис по проверке доменных имен на использование в «зловредной» активности, а также формирование отчетов по типам и количеству зловредов, зафиксированных компаниями-участниками проекта.

Участники научно-технического сотрудничества совместно развивают исследовательскую платформу для агрегации информации о вредоносных ресурсах в сети Интернет, проводят анализ источников «зловредов» и обмениваются аналитическими данными. Работу над созданием исследовательской платформы для сбора и анализа данных о доменных именах в доменах .RU, .РФ и .SU, используемых для размещения «зловредов» на интернет-ресурсах, Координационный центр начал в 2012 году.

Вредоносная активность

- Malware
  - Количество зарегистрированных в БД фактов размещения malware на данном домене
  - Тип(ы) Malware если возможно определить — в случае если мы располагаем такой информацией.
    - First seen / Время начала активности (время первого зарегистрированного в БД размещения malware на данном домене)
    - Last Seen / Время последней активности (последние данные о размещении malware по данному домену)
    - Уровень доверия (0-10) — в зависимости от достоверности источников и частоты жалоб (по фактам размещения malware) на данный домен присваивается число.
- Phishing
- Botnet

Вредоносная активность

- Malware
- Phishing
  - Количество зарегестрированных в БД фактов размещения phishing на данном домене
  - Phishing Target(s) (Ebay, Paypal, Яндекс Деньги etc..) если возможно определить
  - First seen (по аналогии с malware)
  - Last Seen
  - Уровень доверия (0-10)
- Botnet

Вредоносная активность

- Malware
- Phishing
- Botnet
  - Количество зарегестрированных в БД фактов размещения элементов управления ботнетами
  - Botnet type (Zeus, Spyeye etc..) если возможно определить
  - Уровень доверия (0-10)

Участники НТС (с 2012)

Group-IB

Координационный центр национального домена сети Интернет

Лаборатория Касперского

Mail.ru

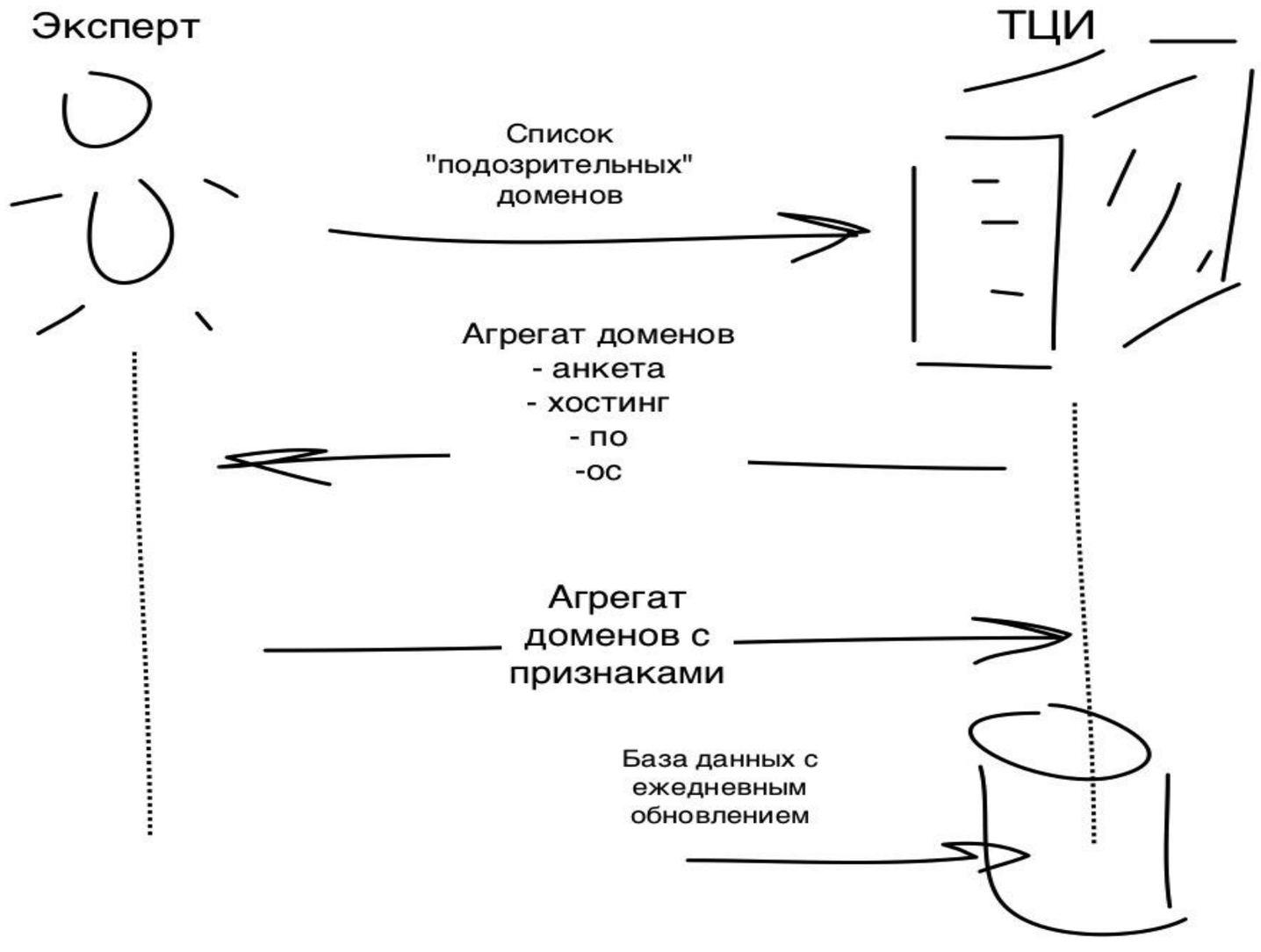
Ростелеком

RU-CERT

Технический Центр Интернет

Яндекс

Порядок накопления информации и ее использования



1. Предупреждение администратора о наличии проблем по аналогии с поисковыми системами
2. Предупреждение Хостинг-провайдеров о наличии проблем
3. Предупреждение регистраторов о наличии проблем
4. Подготовка информации для администрации КЦ и ТЦИ
5. Взаимодействие с коллегами и «братьями по оружию»

Нетоскоп

КООРДИНАЦИОННЫЙ ЦЕНТР НАЦИОНАЛЬНОГО ДОМЕНА СЕТИ ИНТЕРНЕТ

Проверить домен

Например: cctld.ru

ПРЕДУПРЕЖДЕНИЯ

New! Опасная уязвимость в библиотеке AFNetworking SSL

Злоумышленник мог организовать атаку Man-in-the-Middle, подставив любой сертификат, подписанный доверенным УЦ

Критическая уязвимость в продуктах Microsoft

Обнаружена уязвимость в библиотеке HTTP.sys - обработчике HTTP-запросов

Аудит TrueCrypt

Недавно был проведен аудит безопасности программы для шифрования дисков TrueCrypt, в ходе анализа в коде не было обнаружено признаков каких-либо критических уязвимостей или преднамеренно заложенных бэкдоров

Смотреть все предупреждения

СОВЕТЫ

Электронная почта служит одним из главных источников угроз. Снизить риски поможет соблюдение нескольких несложных правил. »»

ОТЧЕТЫ

Апрель 2015

Всего доменов:	1743742	+54584
Вредоносное ПО:	1197809	+55167
Спам:	197177	+523
Фишинг:	67395	+460

Скачать отчёт за месяц .PDF

ТЕМА ДНЯ

Они заряжают пушку

Введите домен

vkontakte.ru

Например, cctld.ru

Введите код ;

Проверить

Апрель 2015

Всего доменов:	1743742	+54584
Вредоносное ПО:	1197809	+55167
Спам:	197177	+523
Фишинг:	67395	+460

Скачать отчёт за месяц .PDF

Данные whois по vkontakte.ru:

[Querying whois.tcinet.ru]

[Terms of Use: http://tcinet.ru/whois/terms.php]

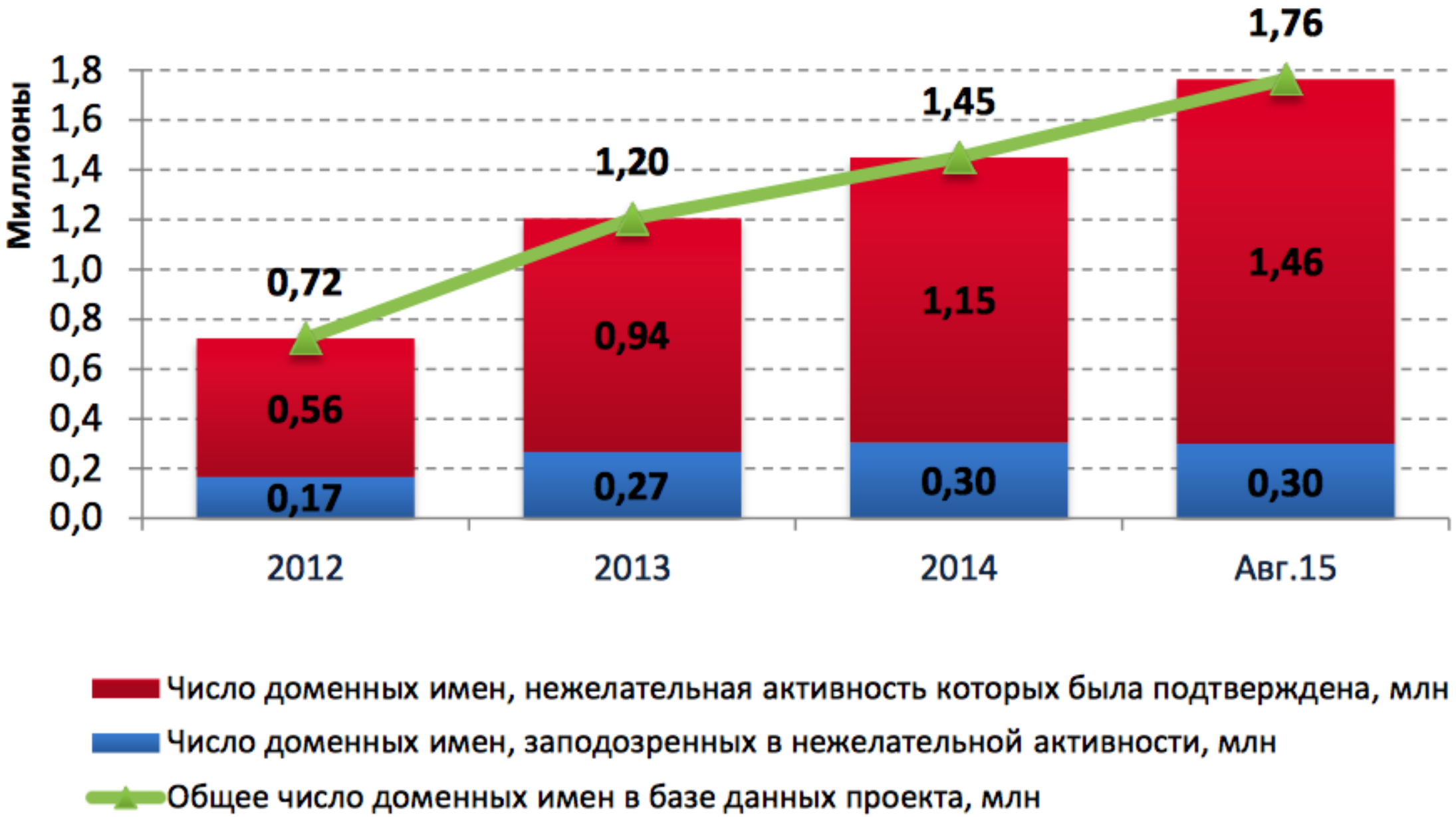
domain: VKONTAKTE.RU
nserver: ns1.vkontakte.ru. 93.186.237.2,
2a00:bdc0:ff:1::2
nserver: ns2.vkontakte.ru. 93.186.224.100,
2a00:bdc0:ff:2::2
nserver: ns3.vkontakte.ru. 93.186.238.24,
2a00:bdc0:ff:3::2
nserver: ns4.vkontakte.ru. 93.186.239.253,
2a00:bdc0:ff:4::2
state: REGISTERED, DELEGATED, VERIFIED
org: LLC "V Kontakte"
registrar: RU-CENTER-RU
admin-contact: https://www.nic.ru/whois
created: 2006.10.01
paid-till: 2015.10.01
free-date: 2015.11.01
source: TCI

В домене vkontakte.ru участниками проекта зафиксированы типы зловредов:

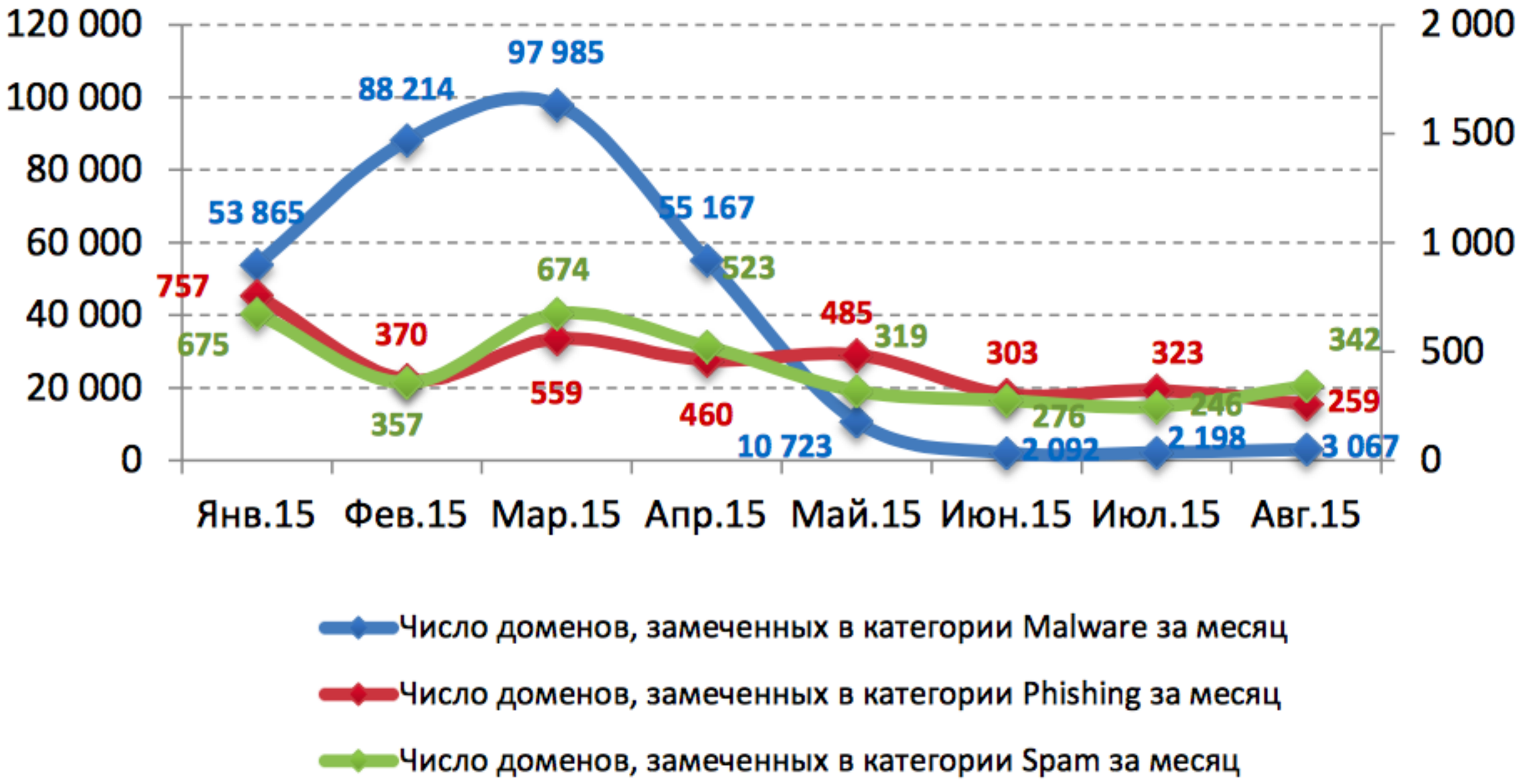
- фишинг
- вредоносное ПО
- кц ботнета
- в прошлом fast flux

Сообщить о зловреде!

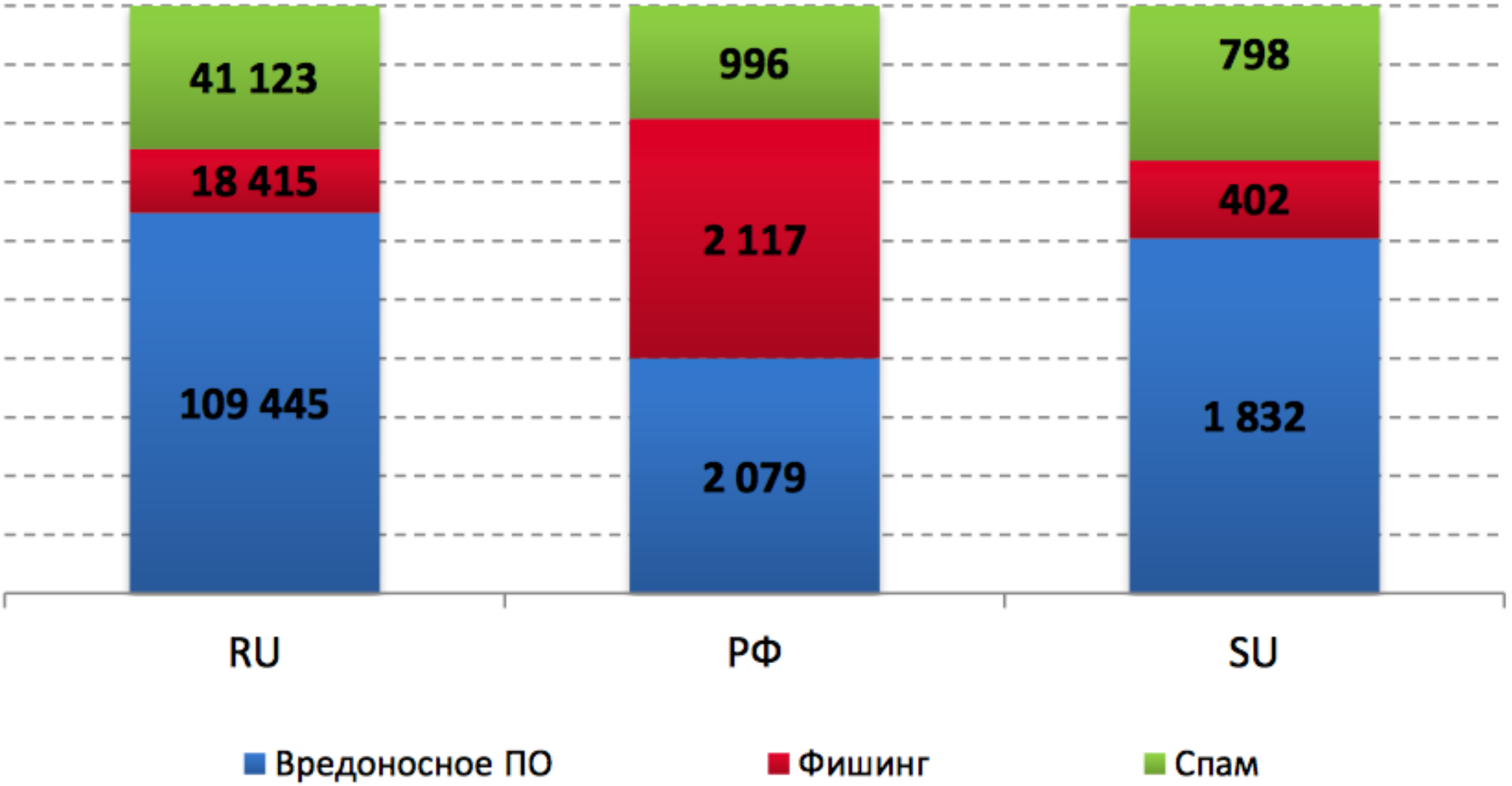
Динамика расширения базы данных проекта "Нетоскоп"



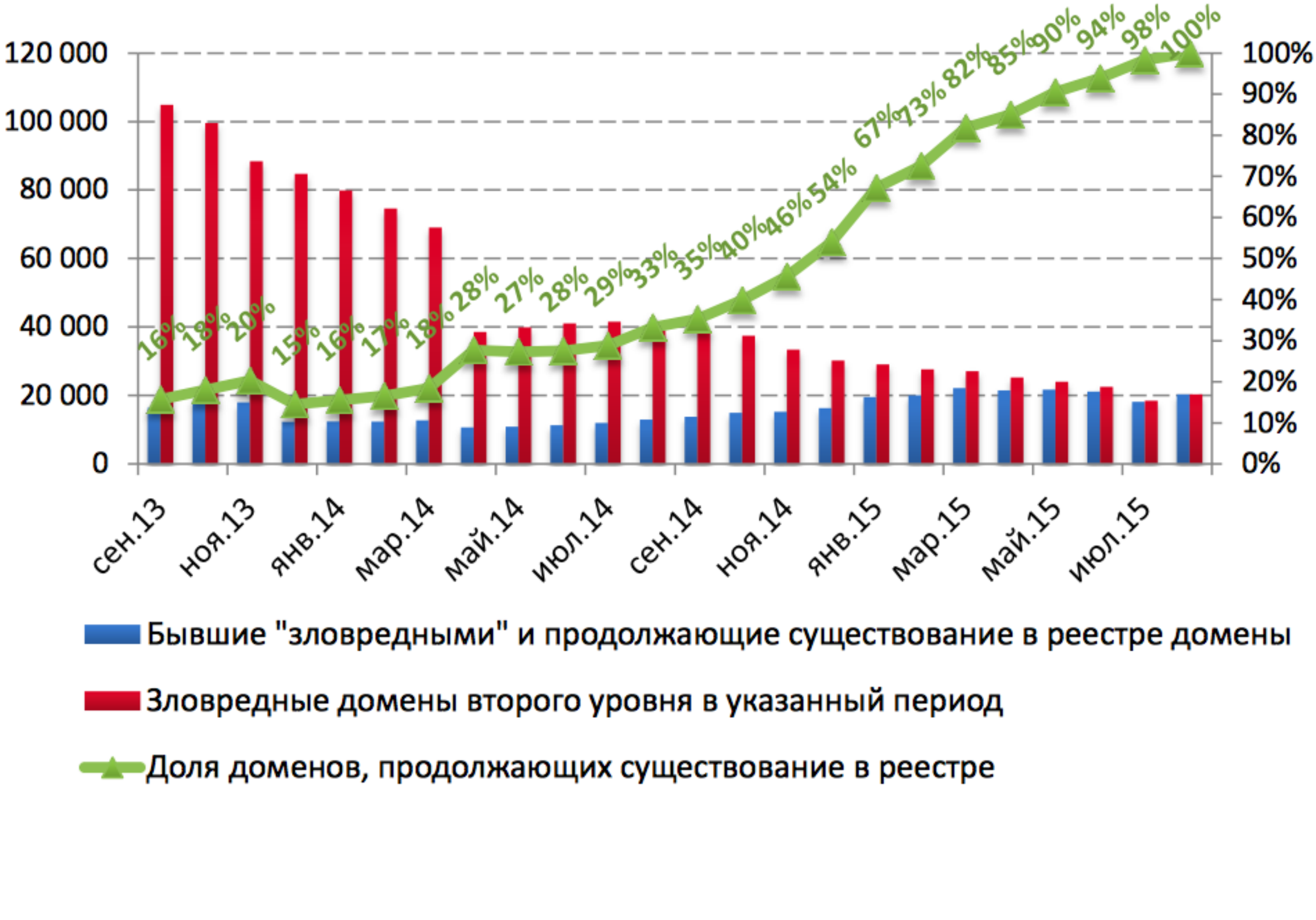
Динамика расширения базы проекта по категориям активности доменов



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



Динамика «лечения» доменов



А что еще есть в БД «Нетоскопа», но нет пока на сайте?

- Данные рубрикатора (Результаты проекта «Категоризатор»):
  - Технометрики (тип ОС, тип CMS, тип HTTP-сервера и т.п.);
  - Списки категорий (например, «Семья и дети»).
- Данные из внешних «Черных» списков (см. доклад Дмитрия Белявского)
- Личные кабинеты регистраторов и компетентных организаций

Резюме

- Борьба со «зловредами» препятствует повторному появлению в национальных доменных зонах доменов, на которых была замечена вредоносная деятельность. Домены не попадают на вторичный рынок и не регистрируются по спискам освобождающихся доменов.
- Борьба со «зловредами» «притормаживает» рост национальных доменов за счет противодействия их использования с «вредоносными» целями. До 30% доменов – это «зловредные» домены.
- Широкое сотрудничество с Интернет-индустрией позволяет существенно снизить размер «вредоносной» активности и повысить эффективность работы интернет-компаний.

Вредоносное ПО, фишинг и ботнеты в национальных доменах
.RU, .SU, .РФ, .ДЕТИ, .TATAR…

p.khramtsov@msk-ix.ru