Proactive Detection of Interrelated Malicious Resources

TLDCON 2018

Pavel Shepetina
Lead Specialist of CERT-GIB
Group-IB

Company

Group-IB — one of the global leaders in providing high-fidelity Threat Intelligence and anti-fraud solutions

EUROPOL INTERPOL

Official EUROPOL and INTERPOL partner

OSCE

Recommended by the Organization for Security and Co-operation in Europe (OSCE)

WORLD ECONOMIC FORUM

Member of the World Economic Forum

1000+

successful investigations worldwide, 150 of which were of special complexity

$300 million

was returned to our clients due to Group-IB's efforts

Forrester Gartner

According to Forrester and Gartner, Group-IB Threat Intelligence is among the best services in the world

BUSINESS INSIDER

One of the top 7 most influential cyber security companies according to Business Insider UK

IDC

Leader of the Russian Threat Intelligence Market

Media coverage:

theguardian Bloomberg Forbes REUTERS

Esquire CNN The Register Biting the hand that feeds IT InformationWeek DARKReading SC MAGAZINE

CERT-GIB (Computer Emergency Response Team) — a round-the-clock computer security incident response team

- Incident monitoring, including distribution of malicious software, phishing, brand abuse, counterfeiting & piracy
- Full legal support on every stage of incident response and investigation
- Professional assistance from specialists with vast experience in response to cyber crime
- Prompt blockage of dangerous websites in the .RU, .РФ domains and more than 1000 other domain zones
- Close cooperation with CERT teams, domain registrars and hosting providers from all over the world
- Collection, analysis and preservation of digital evidences

Recognized as a competent organization of the Coordination Center for TLD RU (administrator of national top level domains .RU and .РФ)

Accredited member of FIRST and Trusted Introducer international associations

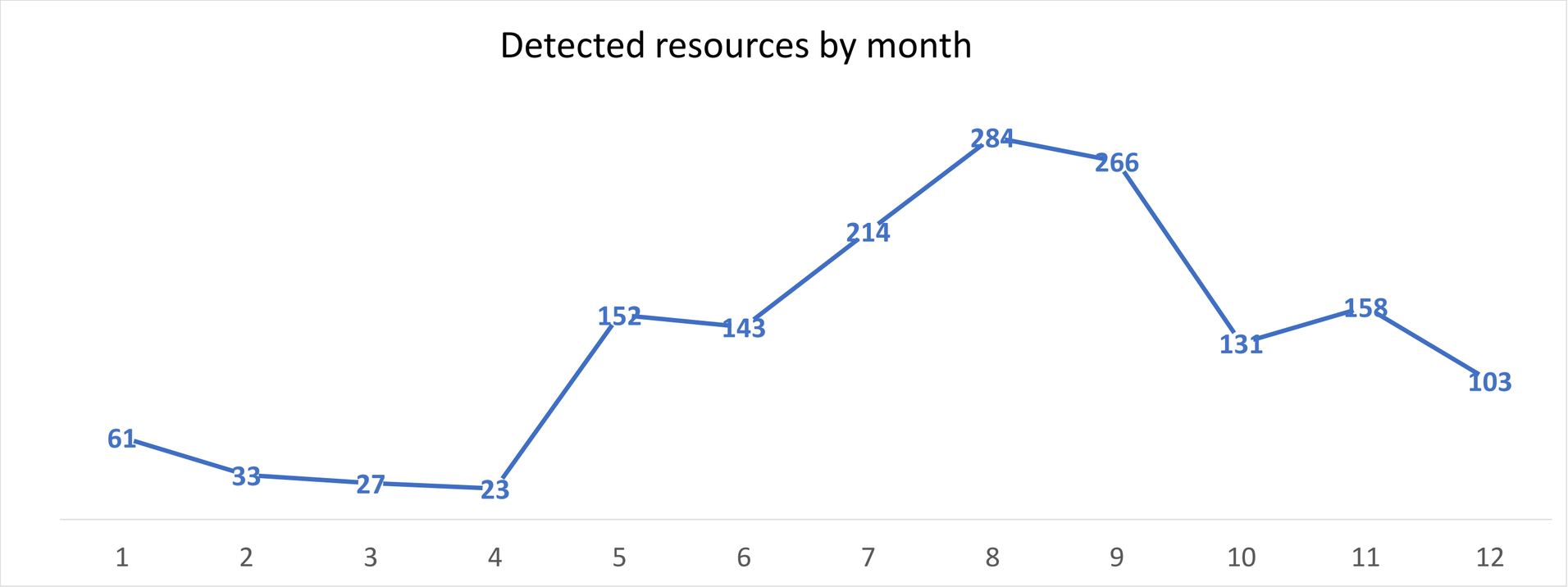
Partner of IMPACT — International Multilateral Partnership Against Cyber Threats

Officially authorized by Carnegie Mellon University and licensed to use the “CERT” trademark in its name

Malicious resources

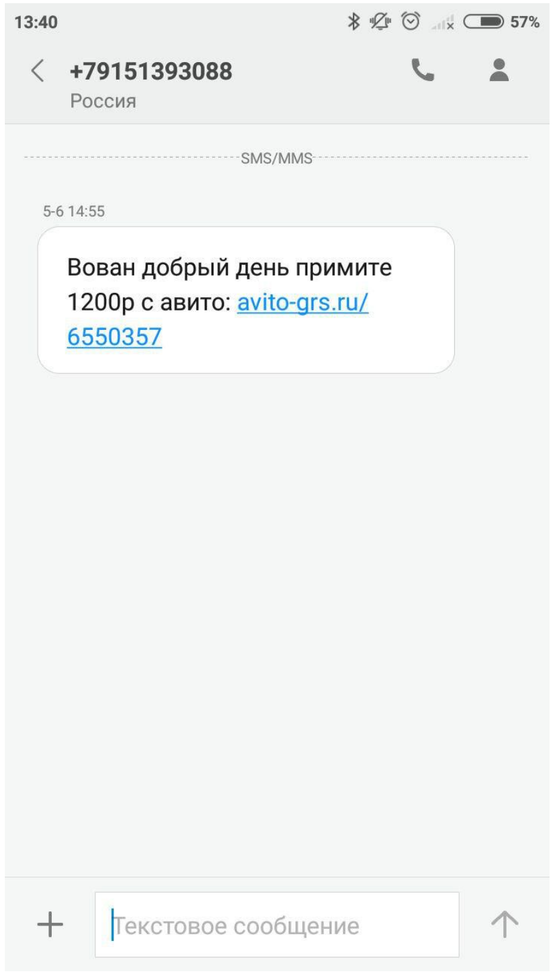
1 595

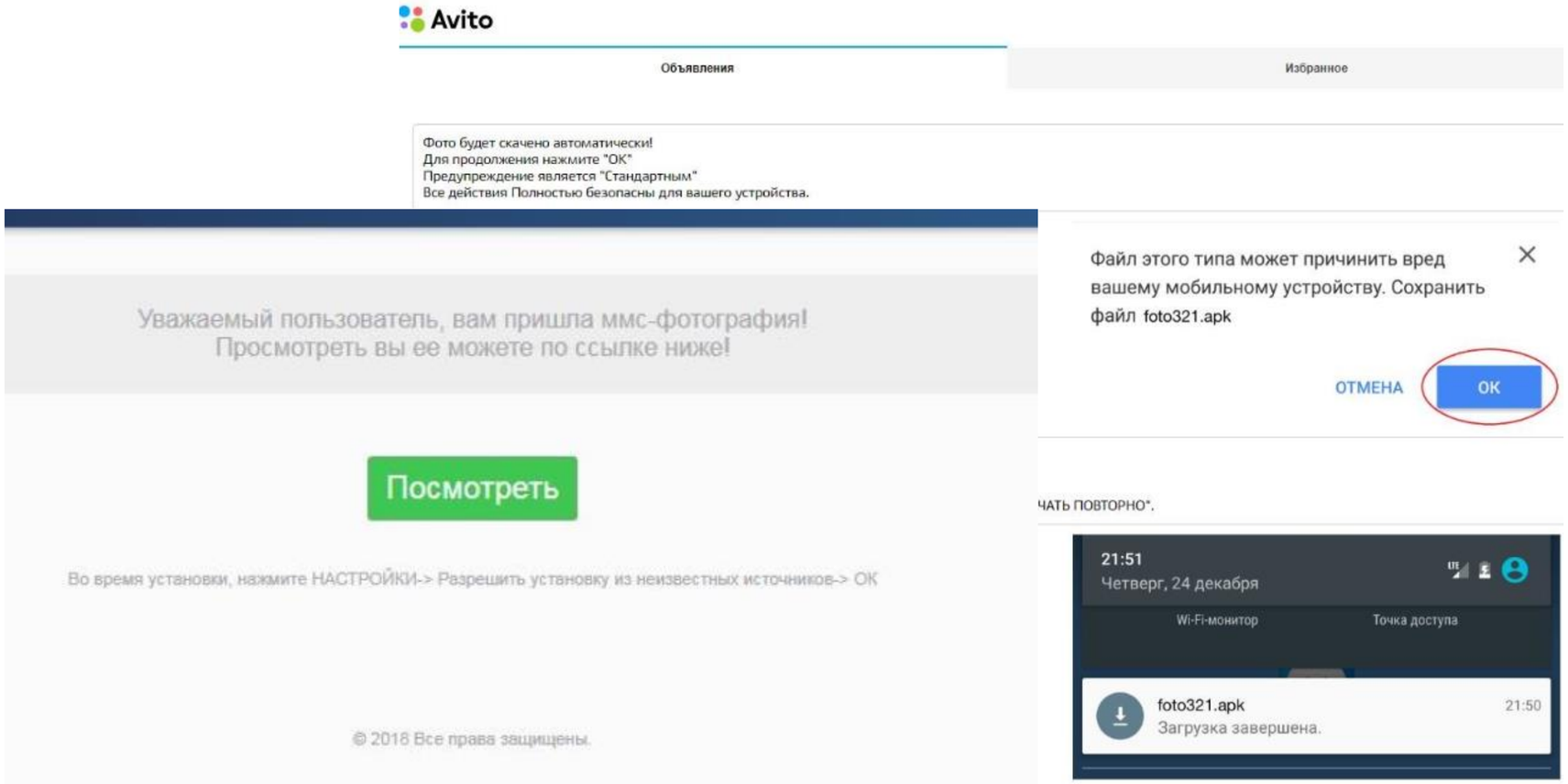
malware resources aimed at Android users in Russia was detected and blocked by CERT-GIB in last 12months. Most of them distributed APK-files that actually are banking trojans



Malicious resources

Most popular method of spreading malware is SMS spam.





How we can detect these resources before SMS send?

- By analyzing the structure of new domain names
- By monitoring IPs or SSL that already been associated with malware activity
- Check new domains from already known account of registrar that already been associated with malware activity (By Netoscope.ru in .ru/.pф)
- By similar Whois data

Proactive Detection of Interrelated Malicious Resources – structure of domain name

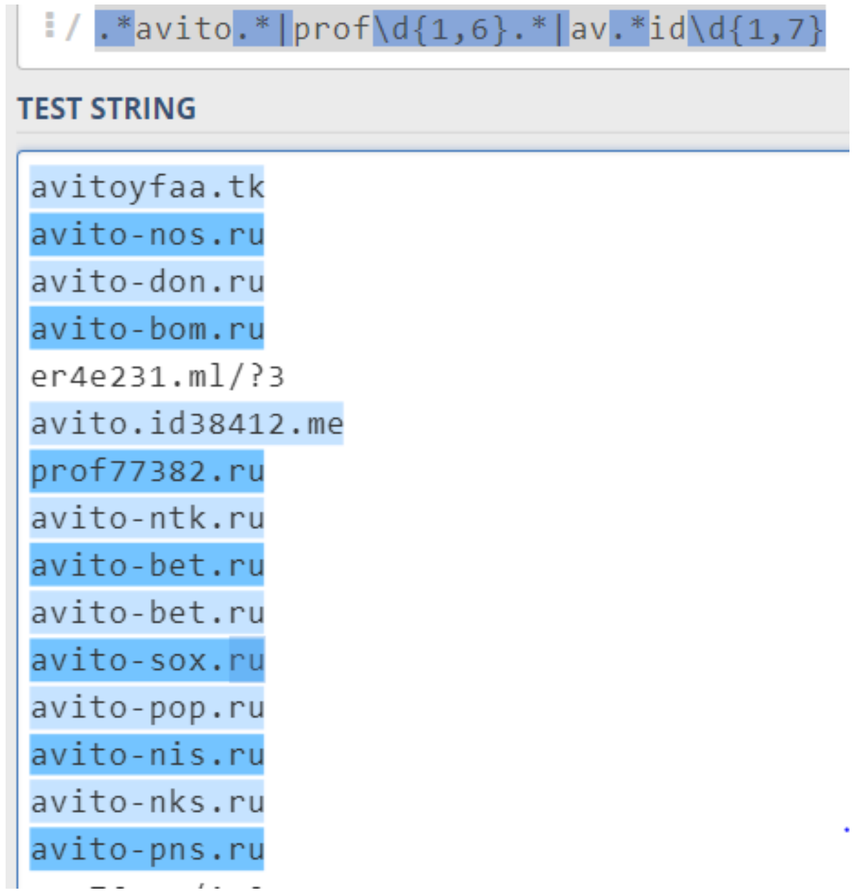
Many of these can be detected by similar regular expressions. For example we can use this for the mentioned case with android malware

.*prof\d{1,6}.*|.* avito.*|av.*id\d{1,7}

For better detect we can use different symbols of ASCII that can help us detect domains like a “**á**vito”. Best preferable to use it automatically. Finished regular expressions for “avito” will look like this:

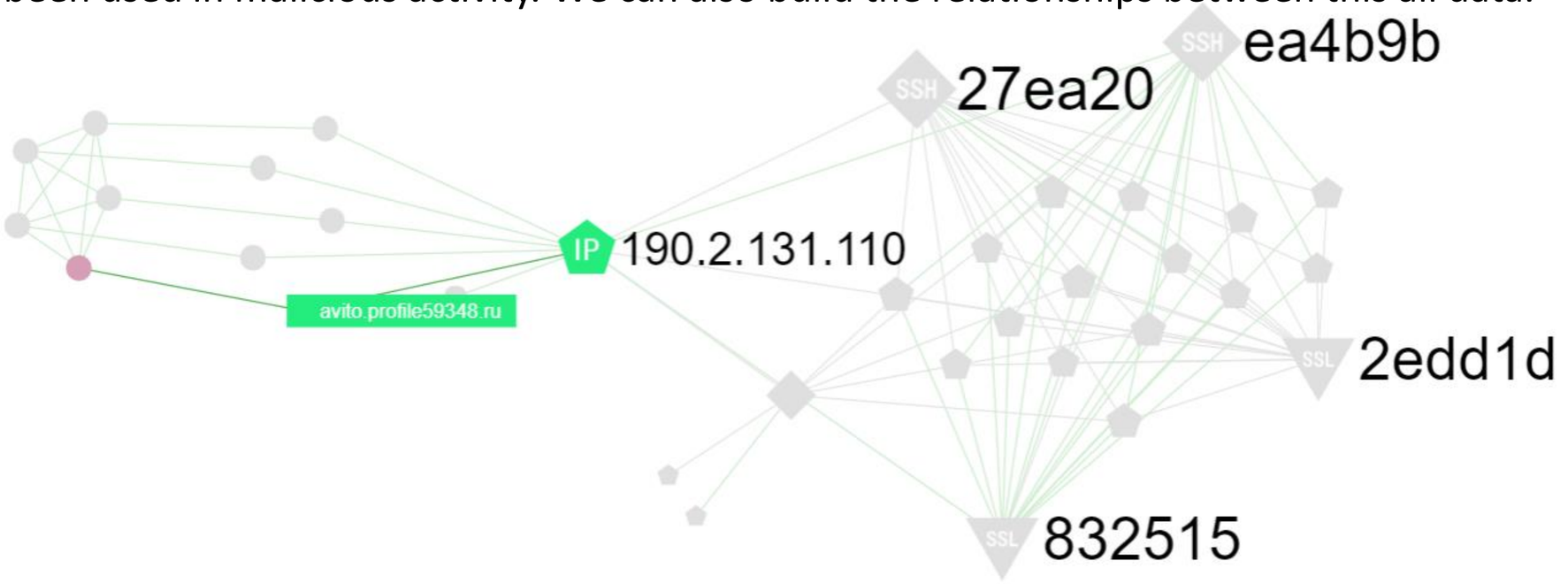
àáâãäåæāąăǎǟǡǣåǽ|vvṽṿ|iìíîïḭḯỉǐȉȋị|tţťŧṭṯṱṫṭ|ðòóôõöø

After finding suspicious domains we should check them for malicious activity from different proxies (especially from mobile network) and user agents (especially mobile devices).



Proactive Detection of Interrelated Malicious Resources – IP and SSL

New domains can use already known IPs, that was previously detected. Also some of domains can change IP and that can help to detect more potential maliciousness resources that related with the new IP. The same thing with known SSL, that already been used in malicious activity. We can also build the relationships between this all data.



Domain name	Registrar	Reg date	Exp date	Email	Phone	Organization	Name	IP-address
avito.profile59344.ru								190.2.131.110
avito.profile59349.ru								190.2.131.110
avito.profile59348.ru								190.2.131.110

Proactive Detection of Interrelated Malicious Resources – whois data

Cybercriminals also can use already known emails when they register the domain names. It also can help to detect new malicious domains, but only if whois data is open. In most cases this data is actually fake.

Domain name	Registrar	Reg date	Exp date	Email	Phone	Organization	Name	IP-address
serv1-down.pro	Tucows Domains Inc.	2018-02-06	2019-02-06	millano.sun@nm.ru	+7.9184758472	Private Person	Viktor Bereza	212.86.109.249
serv54-down.info	Limited Liability Comp…	2018-03-16	2019-03-16	millano.sun@nm.ru	+7.9134857462	Private Person	Fedor Emelninko	212.86.109.249
serv59-down.info	Registrar of domain n…	2018-03-18	2019-03-18	millano.sun@nm.ru	+7.9134857462	Private Person	Fedor Emelninko	212.86.109.249
avito-pays.info	Registrar of domain n…	2018-04-19	2019-04-19	millano.sun@nm.ru	+7.9134857462	Private Person	Fedor Emelninko	185.209.22.67
serv38-down.info	Registrar of domain n…	2018-03-09	2019-03-09	millano.sun@nm.ru	+7.9134857462	Private Person	Fedor Emelninko	212.86.109.249

Proactive Detection of Interrelated Malicious Resources – data from Netoscope

One of services for members of Netoscope.ru can provide associated domains for account but any personal data of account is not disclosed.

If we have at least 1 malicious domain it can help us to find more similar malicious domains with the same registrant. Only for .ru/.pф zones.

Personal Data

- Name
- Phone
- Email

→ MD5

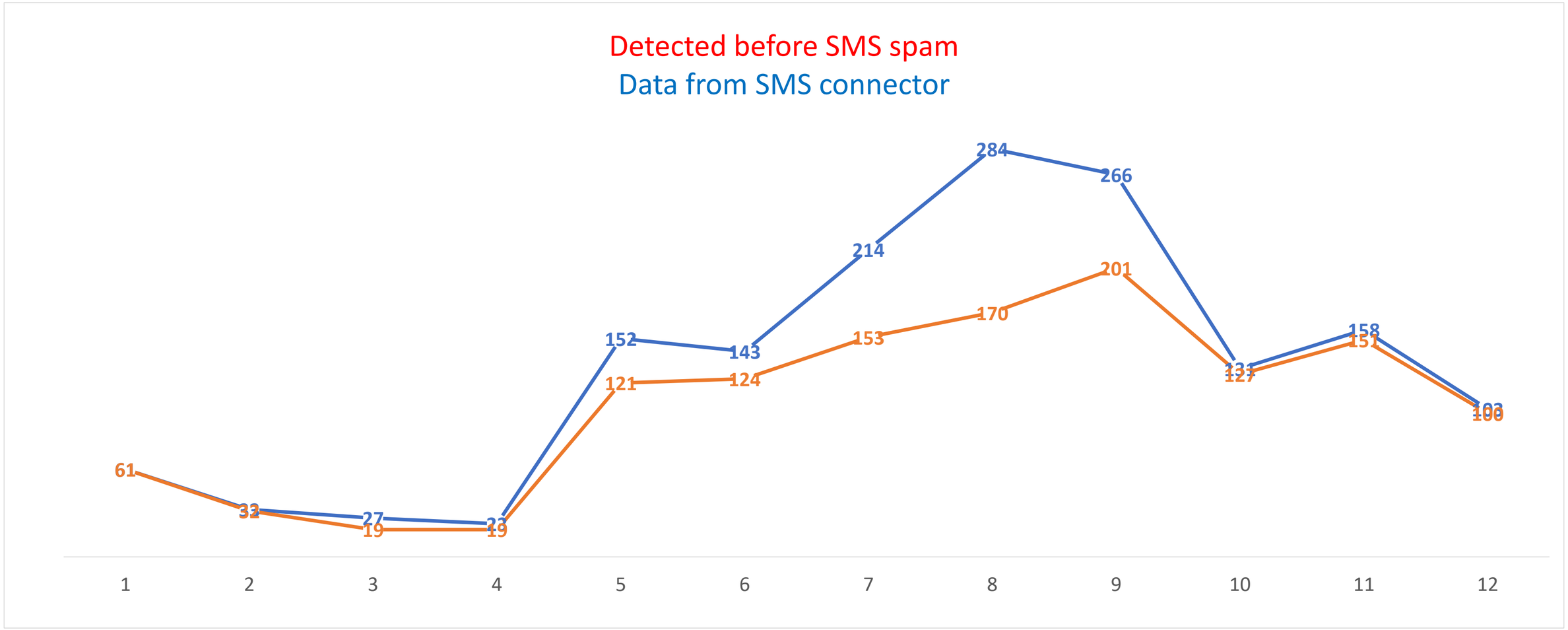
Файл запроса 201808281650.csv

```
mmsdr.ru
```

Файл ответа 201808281650_exst_ans.txt

```
Archive:  201808281650.zip
  inflating: 201808281650_exst_ans.txt
8cb3a1757f1199b53ad39da2f419b531        smsfv.ru
8cb3a1757f1199b53ad39da2f419b531        mmskp.ru
8cb3a1757f1199b53ad39da2f419b531        smsvj.ru
8cb3a1757f1199b53ad39da2f419b531        mmsdr.ru
8cb3a1757f1199b53ad39da2f419b531        smszb.ru
8cb3a1757f1199b53ad39da2f419b531        fotozg.ru
8cb3a1757f1199b53ad39da2f419b531        mmshq.ru
8cb3a1757f1199b53ad39da2f419b531        smsbw.ru
8cb3a1757f1199b53ad39da2f419b531        smsoz.ru
8cb3a1757f1199b53ad39da2f419b531        fotouc.ru
8cb3a1757f1199b53ad39da2f419b531        fotoni.ru
8cb3a1757f1199b53ad39da2f419b531        mmsyb.ru
8cb3a1757f1199b53ad39da2f419b531        mmsgx.ru
8cb3a1757f1199b53ad39da2f419b531        fotohp.ru
8cb3a1757f1199b53ad39da2f419b531        fotoca.ru
8cb3a1757f1199b53ad39da2f419b531        smsxu.ru
8cb3a1757f1199b53ad39da2f419b531        fotoad.ru
8cb3a1757f1199b53ad39da2f419b531        fotopd.ru
8cb3a1757f1199b53ad39da2f419b531        mmsqf.ru
8cb3a1757f1199b53ad39da2f419b531        smsda.ru
8cb3a1757f1199b53ad39da2f419b531        smscn.ru
```

Proactive Detection VS Data from mobile devices



80% malicious domains was detected before cybercriminals send SMS spam with them

Cooperate with Coordination Center

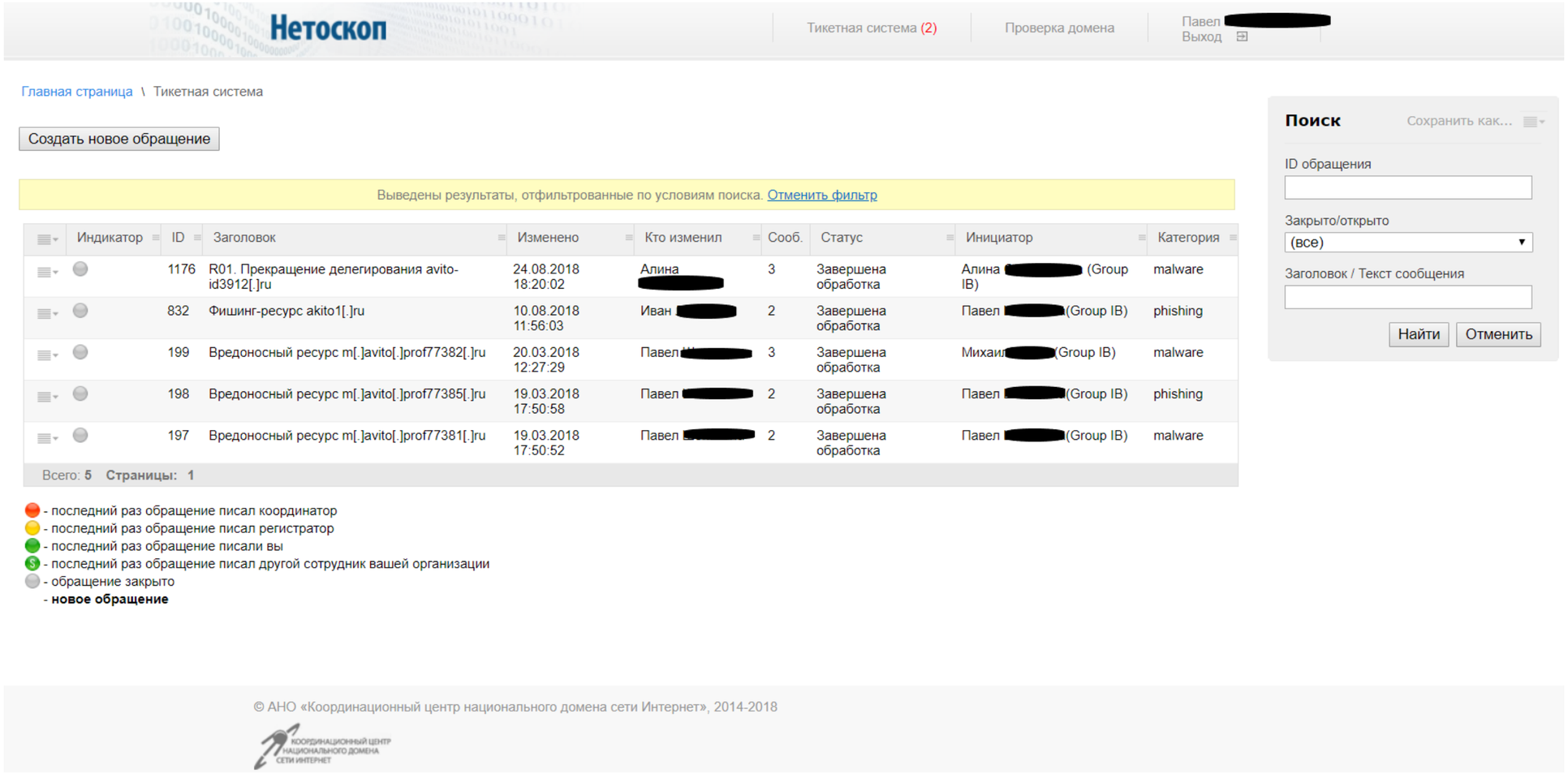
CERT-GIB (Group-IB) Recognized as a competent organization of the Coordination Center for TLD RU. It help us to cooperate with registrars in .ru/.pф zones to suspend malicious domain names, include that uses for the purposes of phishing, unauthorized access to third-party information systems, malware distribution, and controlling botnets.

3 020

domains that used for phishing, malware distribution and CNC was suspended by CERT-GIB in 2017 by using using competencies in .ru/.pф zones

Cooperate with Coordination Center

Coordination Center provide a platform that can help cooperate with registrars – ticket system between registrars and competent organizations like us.



Group-IB — one of the global leaders in providing high-fidelity Threat Intelligence and anti-fraud solutions

www.group-ib.com
info@group-ib.com
twitter.com/groupib_gib
group-ib.com/blog
+7 495 984 33 64
linkedin.com/organization/1382013