MKD-CIRT

REPUBLIC OF MACEDONIA
AGENCY FOR ELECTRONIC COMMUNICATIONS

NATIONAL CENTRE FOR
COMPUTER INCIDENT RESPONSE

“CSIRT Services, Information exchange and Cooperation”

International Regulatory Conference

16 May 2018, Ohrid, Republic of Macedonia

Инфо за MKD-CIRT / About us

Закон за електронските комуникации, член 26-а:

(1) Во состав на Агенцијата како посебна организациона единица се формира национален центар за одговор на компјутерски инциденти (MKD-CIRT) како официјална национална точка за контакт и координација во справувањето со безбедносните инциденти кај мрежите и информациските системи кој идентификува и обезбедува одговор на безбедносни инциденти и ризици.

Law on electronic communications, article 26-a

- Official national point for contact and coordination in handling security incidents on networks and information systems, that will identify and ensure response to security incidents and risks.

CERT, CIRT, CSIRT …

MKD-CIRT Constituency (1/2)

All ministries, public administration and the services of the Government of the Republic of Macedonia

Operators of Critical Infrastructure in the Republic of Macedonia, and

Large organizations in the banking, transport, communication, health, energy and other strategic sectors in the country

MKD-CIRT is open for cooperation with all stakeholders. More information on starting the cooperation can be found on the following link: https://mkd-cirt.mk/registracija/

MKD-CIRT constituency (2/2)

Sectors of critical infrastructure

- Water supply
- Transport
- Financial services
- Research and education
- Energy
- Information and communication technologies
- Health

MKD-CIRT services

Reactive	Proactive	Security Quality Management services
Alerts & Warnings Incident handling Vulnerability handling Incident coordination and response Analysis of threats and vulnerabilities	Announcements Tech watch Security audits/Pentests Tools development Intrusion detection Threat intelligence sharing	Risk Analysis BC & DR planning Security awareness Training Evaluation and certification of products and services

MKD-CIRT services

MKD-CIRT

РЕПУБЛИКА МАКЕДОНИЈА
АГЕНЦИЈА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ

НАЦИОНАЛЕН ЦЕНТАР ЗА
ОДГОВОР НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ

Coordinating an incident response

coordination point at national or regional level among the countries affected by the security incident

Alerts and warnings

for disclosing details of current threats and steps that can be undertaken to protect against these threats

Incident response and handling

provide technical assistance to address the security incidents when they occur, in order to mitigate the damage and recover from the incident.

Vulnerability response

Assess the adequate measures necessary to respond to newly discovered vulnerabilities; assess their seriousness and impact, decide whether to issue warnings thereof or verify or further investigate their weight/impact

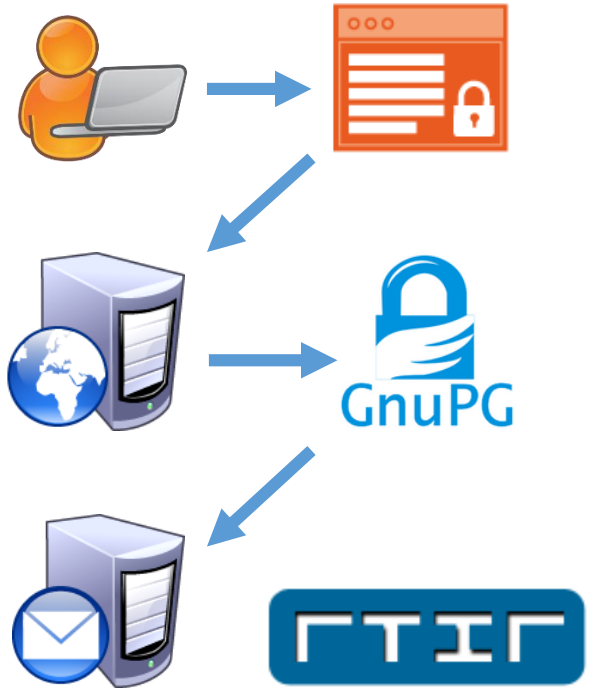
Basic awareness, education&training

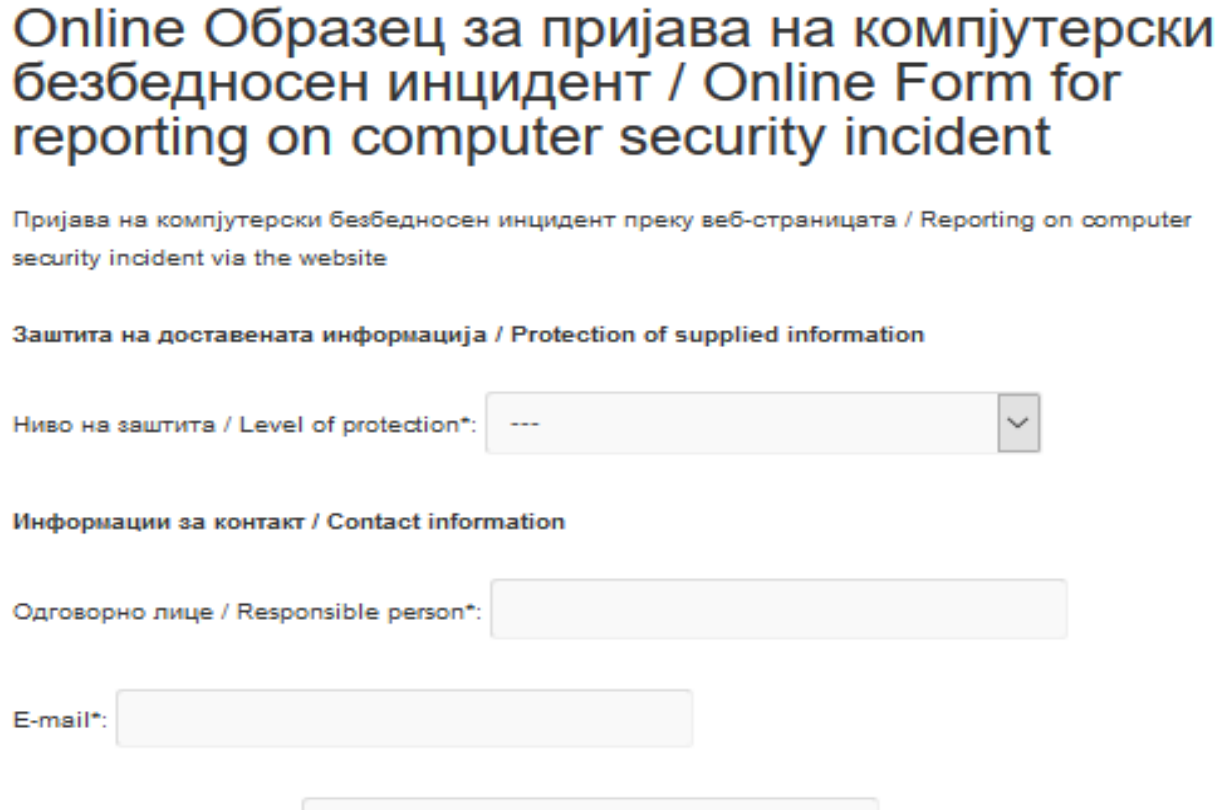
Implement small-scale programmes for raising public awareness. Conduct basic training on computer incident response and main cybersecurity best practices

Reporting incidents and response

Citizens: web form for anonymous reporting on incidients:

https://mkd-cirt.mk/prijava-na-incident/obrazec-za-prijava-na-incident/





Online Образец за пријава на компјутерски безбедносен инцидент / Online Form for reporting on computer security incident

Пријава на компјутерски безбедносен инцидент преку веб-страницата / Reporting on computer security incident via the website

Заштита на доставената информација / Protection of supplied information

Ниво на заштита / Level of protection*: ---

Информации за контакт / Contact information

Одговорно лице / Responsible person*:

E-mail*:

Reporting on incidents by constituents https://mkd-cirt.mk/prijava-na-incident/

- Fill in Word form with all the required information
  - Encryption with MKD-CIRT public key
  - Key ID: 0x333C00DB
  - Key Type: RSA 4096
  - Key Fingerprint: 0FB9 3DA3 E008 FA8B FC6A 9C71 0741 17A1 333C 00DB
- Send by e-mail to info@mkd-cirt.mk

MKD-CIRT, Guidelines for incident reporting

The Incident Report should include a description of the incident or event

- Protection level of submitted information (Strictly Confidential, Confidential or Public)
- Contact Information (Name and surname, e-mail address, phone number)
- Details of the incident
  - Date, time / timestamp of detection and time zone
  - Level of impact on the organization (Critical, High, Low, No Impact, or Unknown)
  - Incident category (one of ten categories)
  - Current status of the incident(On-going, Incident is under control (localized), Incident has occurred previously, and Unknown)
  - Number of affected systems (estimate)
  - Features (description) of the incident
- System details
  - Name and address (Host / IP)
  - System function (e.g.: DNS system, Web server, E-mail server, etc.)
  - Tracking the incident report (Initial Report to MKD-CIRT, Continuation of a previous report)

MKD-CIRT, Incident categorisation

1. Compromised information
2. Compromised asset
3. Unauthorized access
4. Malicious code
5. (Distributed) Denial of Service
6. Theft or loss
7. Phishing
8. Unlawful activities
9. Scans / probes / Access attempts
10. Policy violations

Incident response coordination 1/2

- Network for information exchange and coordination
- 49 organization at this time
  - Administrative contacts
  - Technical expertise contacts
  - Public-facing resources (CIDR, domains ...)
- Next steps: Experts registry for mutual assistance
- MISP – malware information exchange platform

Incident response coordination 2/2

- First National exercise on incident response coordination
- Organized together with OSCE mission to Skopje
- 45 participants
- 35 organizations
  - Government
  - Public sector
  - Private operators of critical infrastructure
- Highly positive feedback and requests for further trainings

Notifications on threats and vulnerabilities

- Publishing announcements, advice and guidelines on our web site at https://mkd-cirt.mk
- Announcing information on Twitter https://twitter.com/mkdcirt
- Continuous campaign Stop. Think. Connect.
- Using the MISP Platform for Informing Constituents

ЗАСТАНИ | РАЗМИСЛИ | ПОВРЗИ СЕ™

STOP | THINK | CONNECT™

International cooperation

- MoUs and agreements:
  - Governemnt CSIRT of Moldova
  - National CERT of Slovenia
  - National CERT from Kosovo
  - National CERT from Albania
  - ICCIN – International Cyber Counter Intelligence Network
  - Stop.Think.Connect – International initiative
  - Trusted Introducer TF-CSIRT – MKD-CIRT, member since 2016
  - Accredite member of TF-CSIRT since December 2017
- Frequent communication and information exchange with CSIRTs from other countries: Italy, Spain, Czech Republic, Netherlands, Bulgaria

CERT nazionale Italia

NCSC-NL

CERT.BG

certsi_

TF-CSIRT
Trusted Introducer

S2 GRUPO

NUCLEON

TR-CERT

CSIRT.CZ

ICCIN International Cyber Counter Intelligence Network

The following list contains all "Listed" teams. "Accredited" and "Certified" teams are - by definition - also "listed" teams, and are therefore contained in this list for your convenience.

Search

Clear all filters

Toggle team details

Filter by State

Clear Filter

- [ ] Certified (0)
- [ ] Accredited (1)
- [ ] Listed (0)
- [ ] Candidate (0)

Filter by Const. Type

Clear Filter

- [ ] Research & Education (0)
- [ ] ISP Customer Base (0)
- [ ] Vendor Customer Base (0)
- [ ] Financial Sector (1)
- [ ] Commercial Organisation (0)
- [ ] Service Provider Customer Base (0)

Filter by Country

MKD-CIRT

Accredited
since 08 Dec 2017

Macedonia, Former Yugoslav Republic | Last updated on 11 Apr 2018

General Information

Established	Host Organisation	Constituency Types
2016	Agencija za elektronski komunikacii Skopje (Agency for Electronic Communications)	Financial Sector, Government, National

Contact Details

Team Email	Main Phone	Emergency Phone
info@mkd-cirt.mk	+389 2 3091 232	+389 70 338 155
Encrypted Mail Support	**Public URLs**	**Timezone**
PGP	https://mkd-cirt.mk	GMT+01 / GMT+02
Business Hours		
08:30 to 16:30 Monday to Friday		

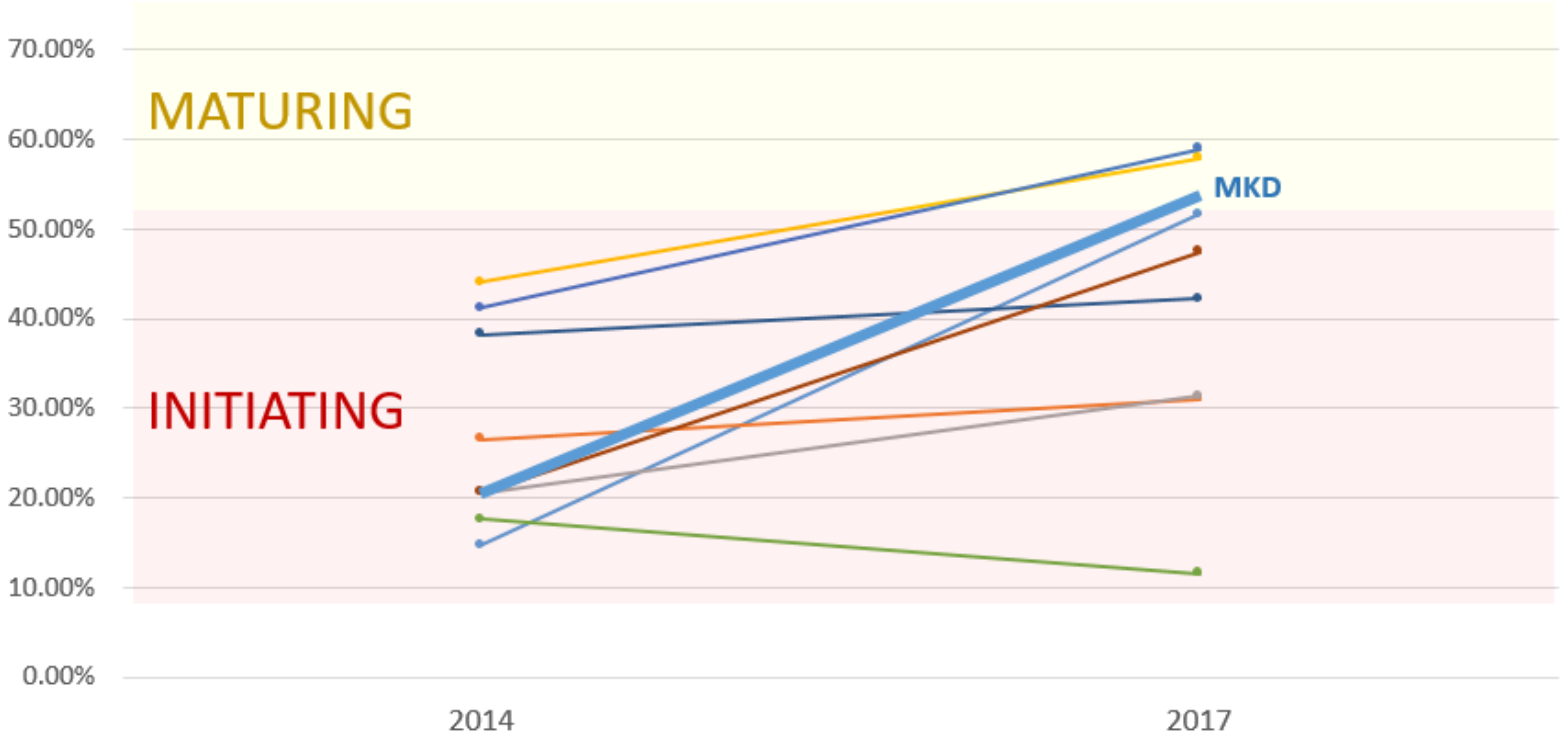
ITU Global Cybersecurity Index

GCIv1 – 2014, GCIv2 – 2017, GCIv3 - 2018

Main objectives of the GCI is to measure the cybersecurity commitment of countries, thus helping them identify areas for improvement in the field of cybersecurity, as well as motivate them to take action to improve their ranking, thus helping raise the overall level of cybersecurity worldwide.

Download the report from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx

ITU Global Cybersecurity Index



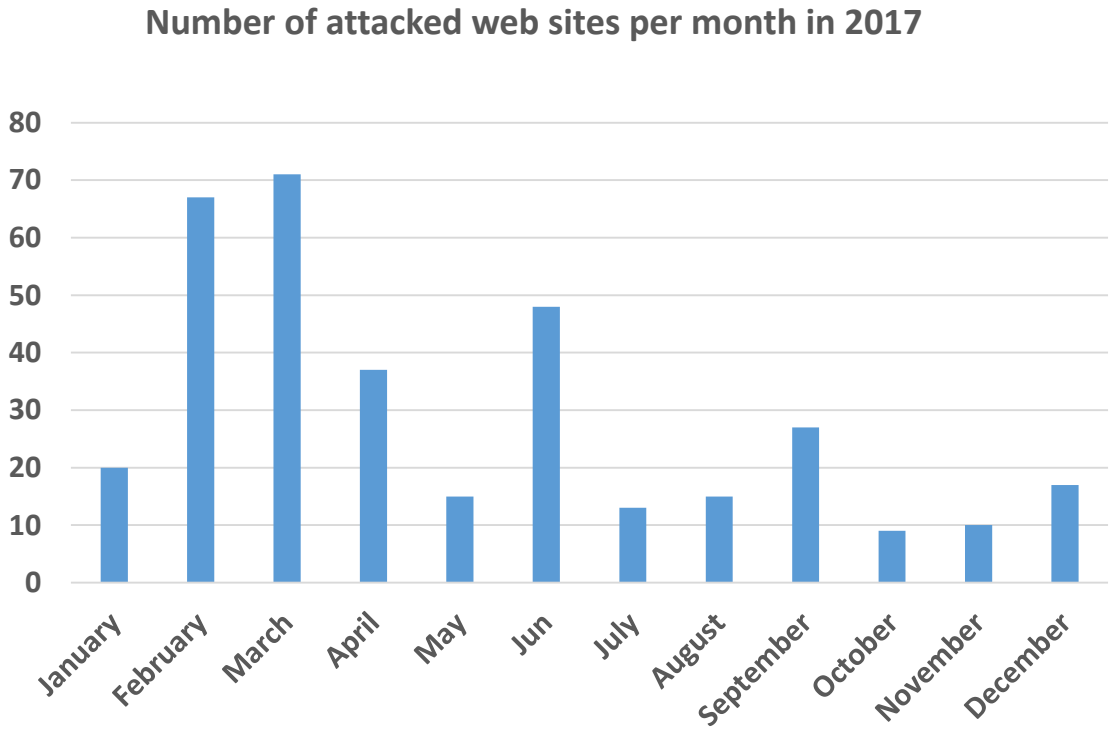
Work statistics for MKD-CIRT

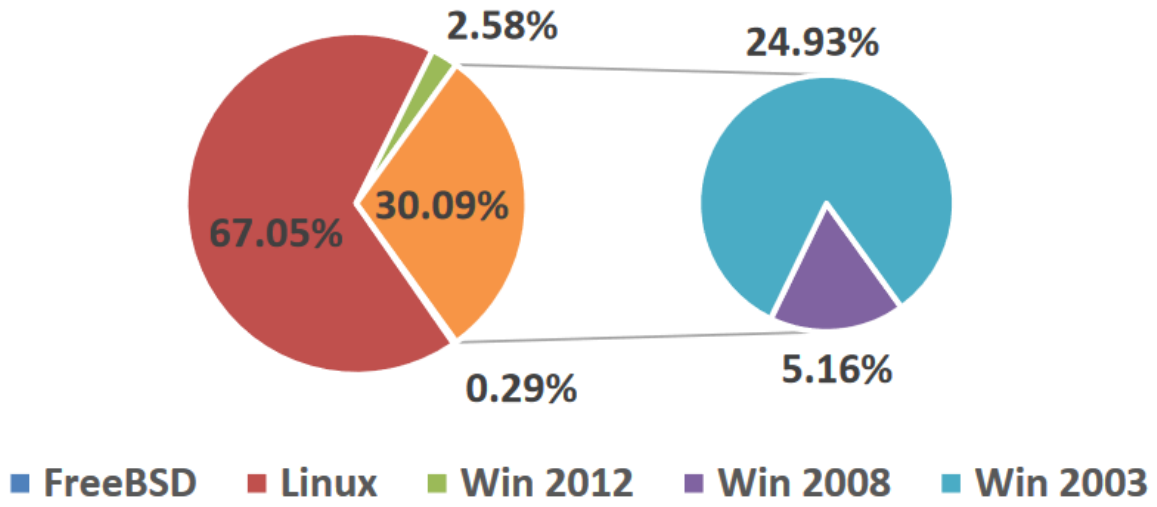
Annual work report for 2017, published at https://mkd-cirt.mk/dokumenti/

Public web in Macedonia

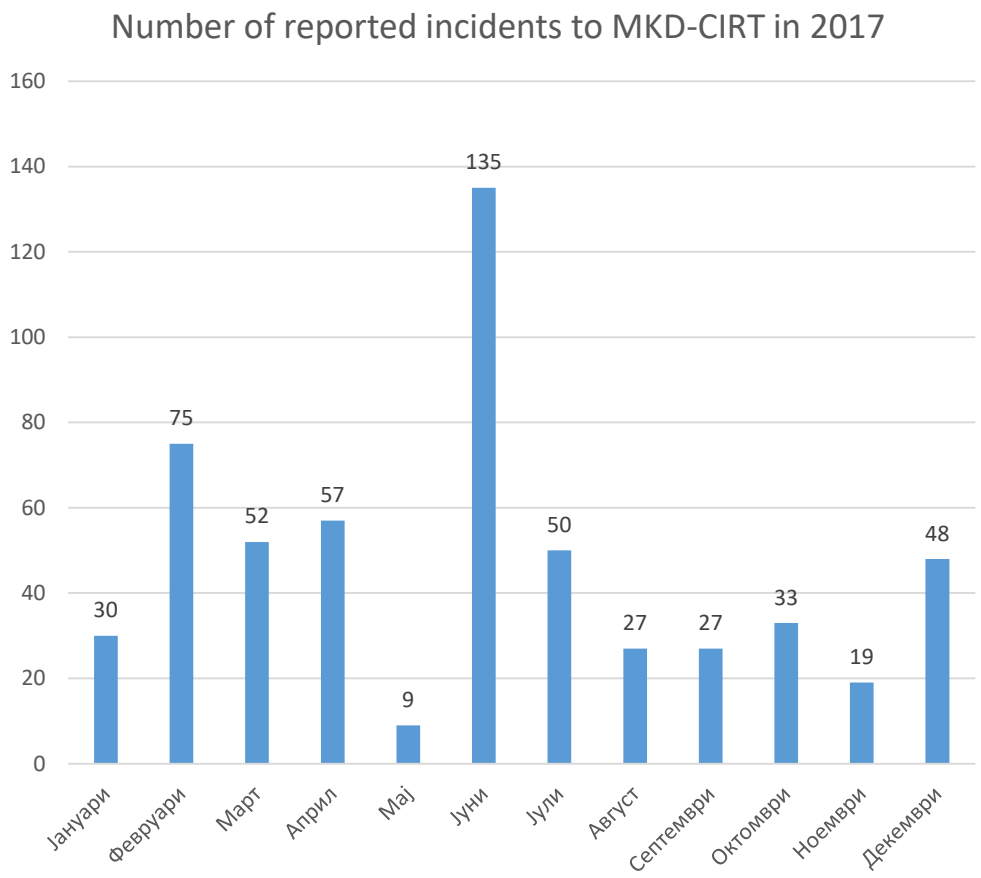
Number of registered .mk domains во 2017 TLD (Top Level Domain): 25168

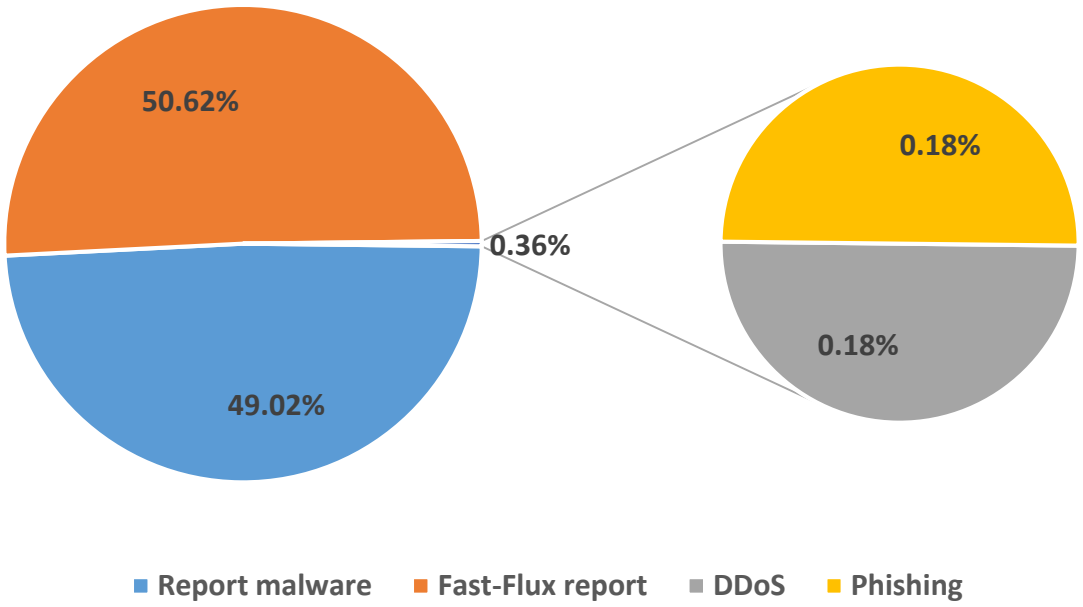
- In 2017 we had 349 public web pages that were hacked, 23 official government web sites, .gov.mk
- Defacement & hacktivism



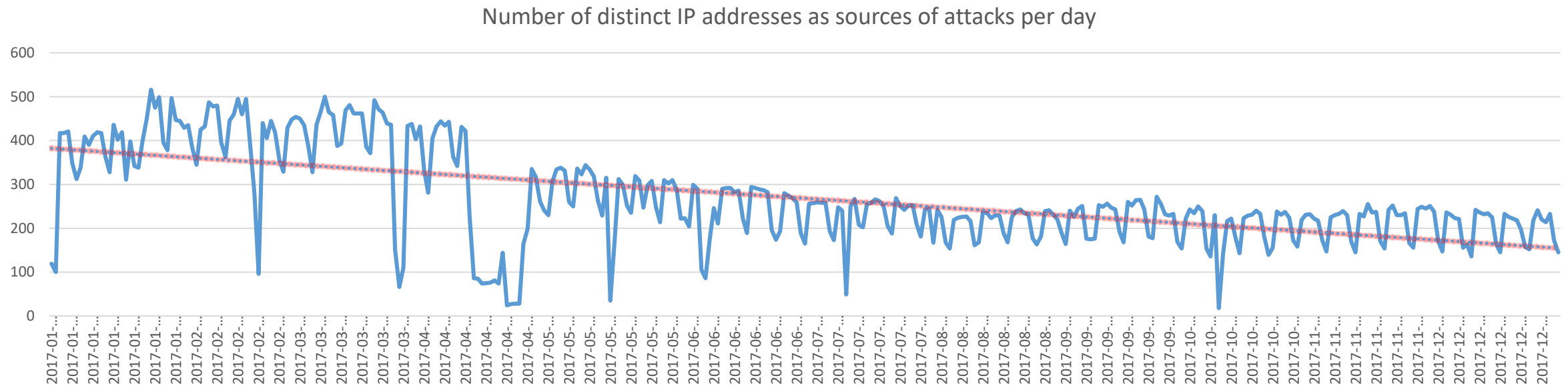


Incidents reported to MKD-CIRT

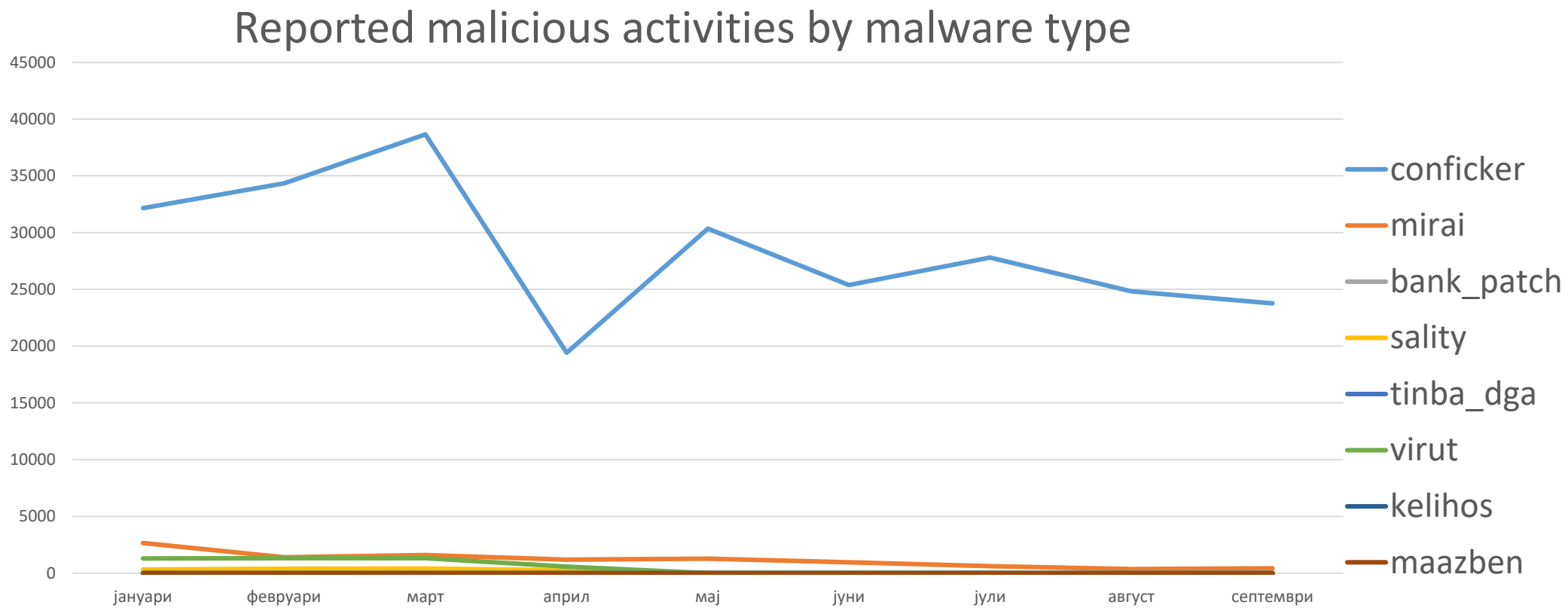




Situation with malware in Macedonia for 2017 1/2



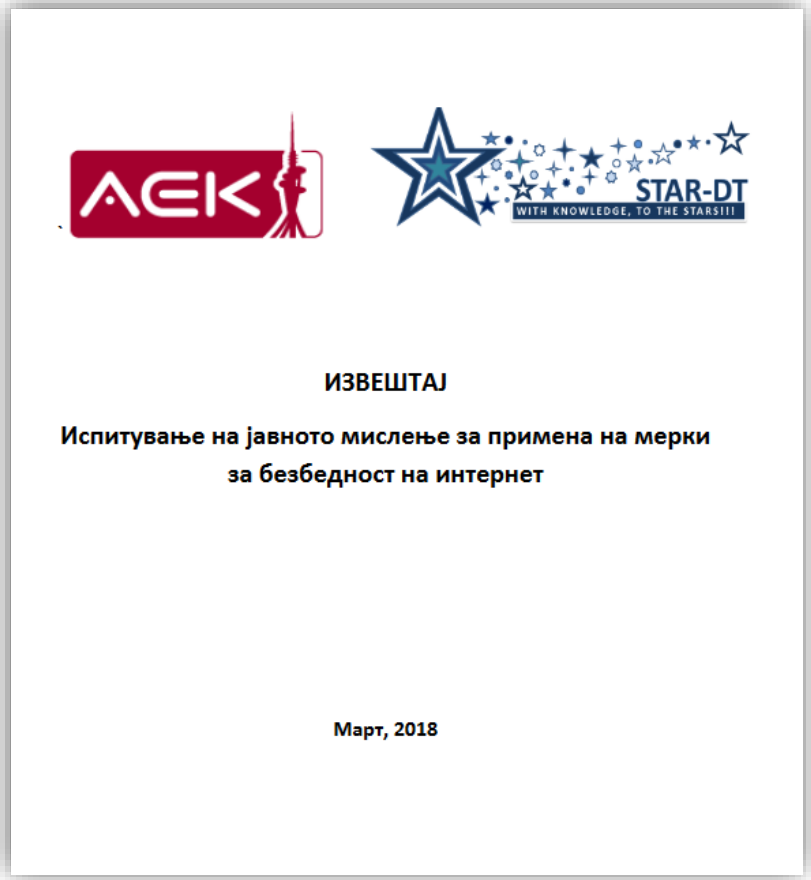
Situation with malware in Macedonia for 2017 2/2



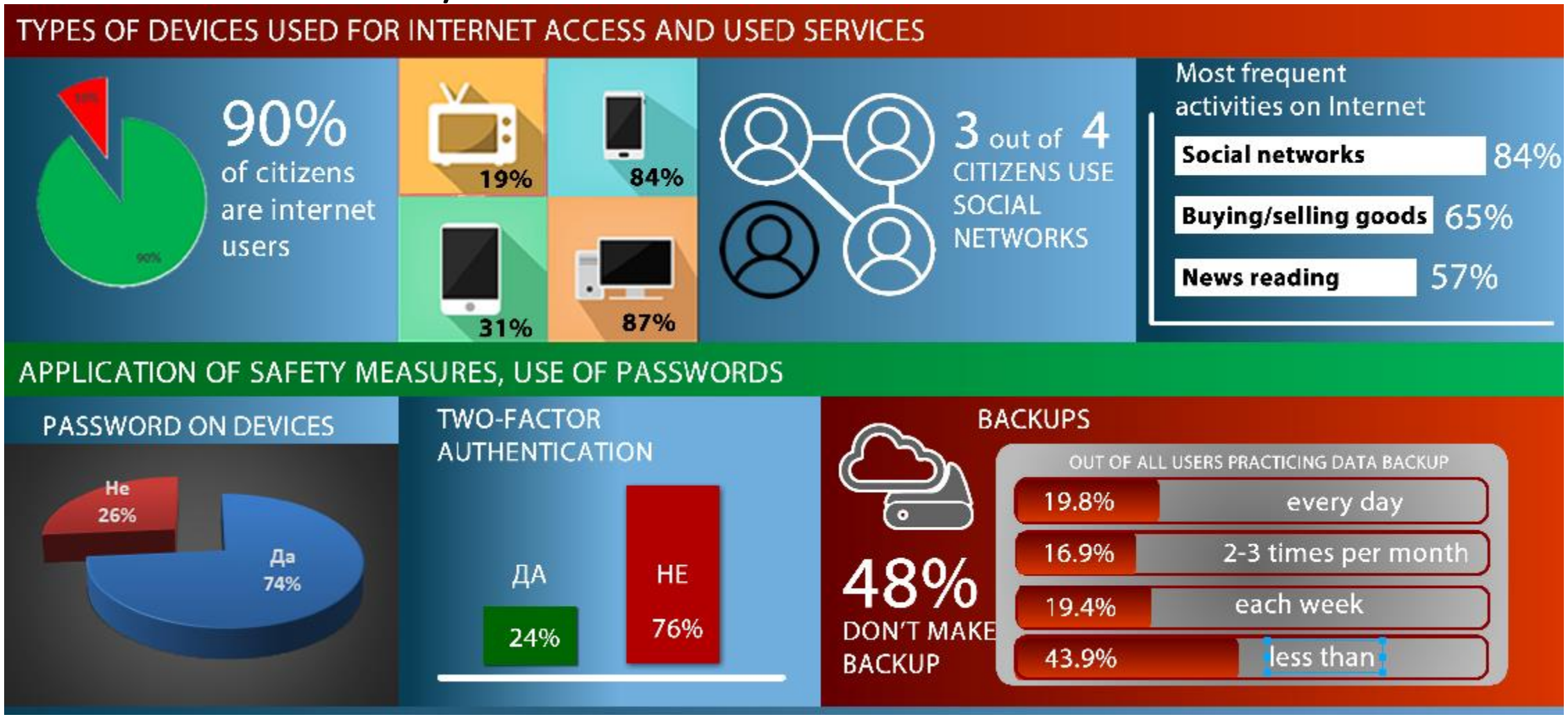
Report on the Public survey for attitude towards cyber security, March 2018

Published at https://mkd-cirt.mk/dokumenti/

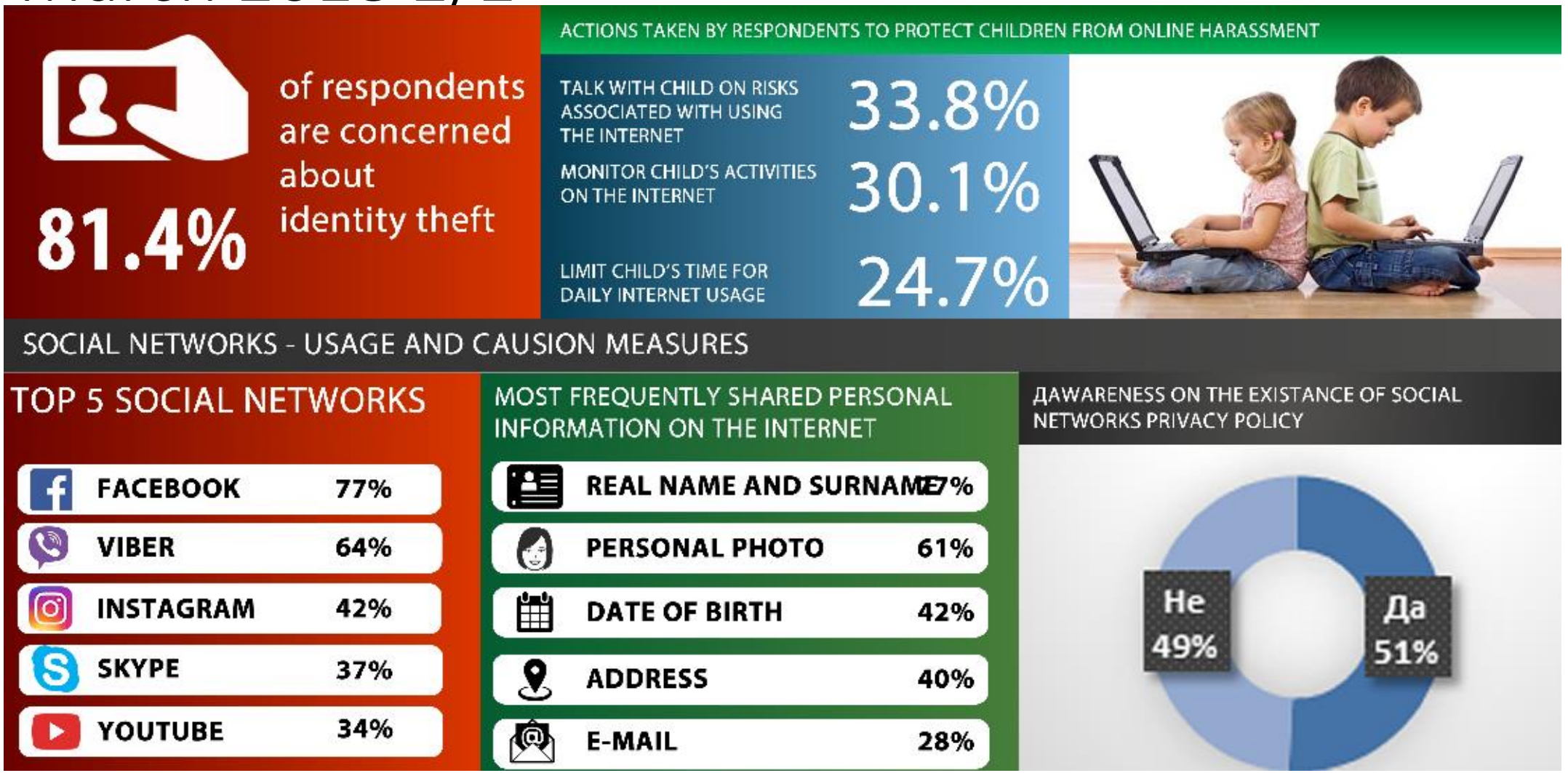
- Cybersecurity measures used when working on the internet
- Level of usage of online services and e-banking
- How well are citizens informed about protection of personal data on the internet
- Cybersecurity measures used by citizens when accessing social networks
- Types of devices used for accessing internet and online services



Public survey for attitude towards cyber security, March 2018 1/2

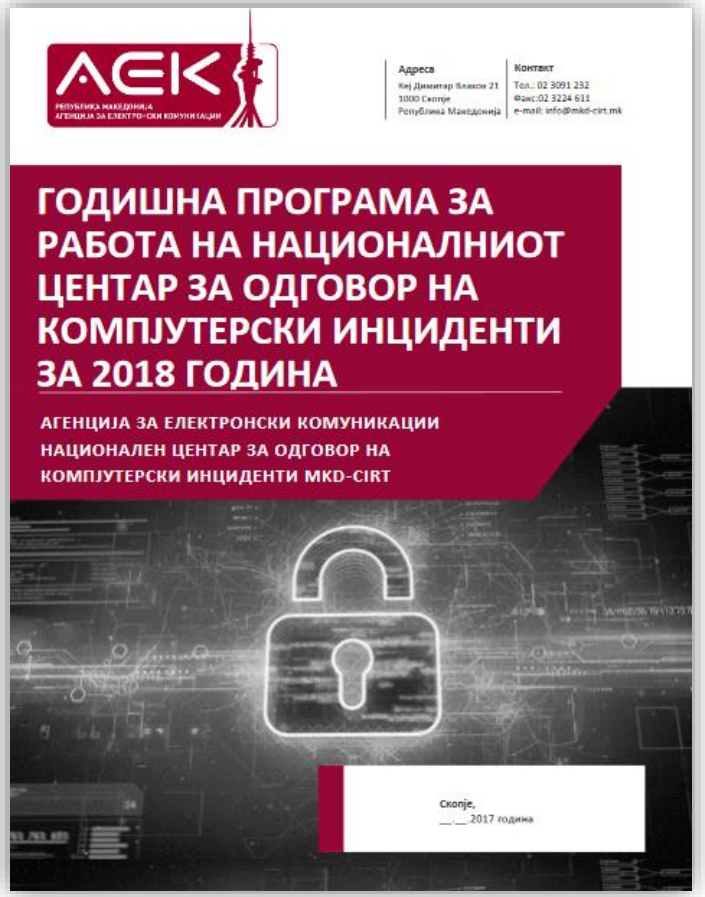


Public survey for attitude towards cyber security, March 2018 2/2



MKD-CIRT activities for 2018

Annual work program for 2018 is published at https://mkd-cirt.mk/dokumenti/



MKD-CIRT Activities in 2018

New systems for:

- Threats intelligence
- Vulnerability assessment

Vulnerability assessment of the public web in Macedonia

Publishing guides for safe internet usage

Capacity building trainings for our constituents:

- Using the malware information sharing platform for information exchange
- Web applications Vulnerability assessment
- Pentesting with Kali Linux

Cybersecurity conference, October 2018

Thank you!

You can report incidents to us by:

https://mkd-cirt.mk/prijava-na-incident/obrazec-za-prijava-na-incident/

info@mkd-cirt.mk

02/3091-232