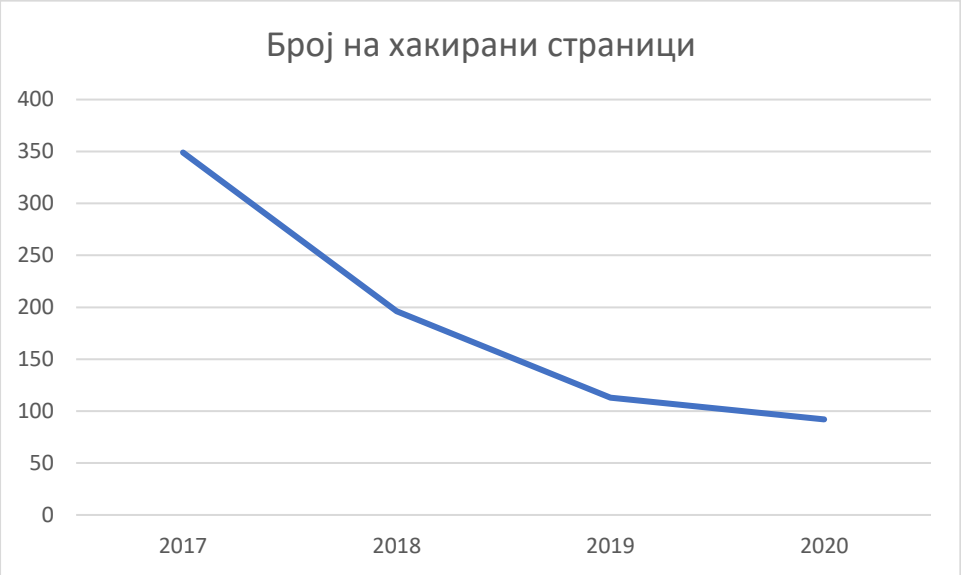
Статистика за работењето на MKD-CIRT во 2020 година

Јавни веб-страници во Република Северна Македонија

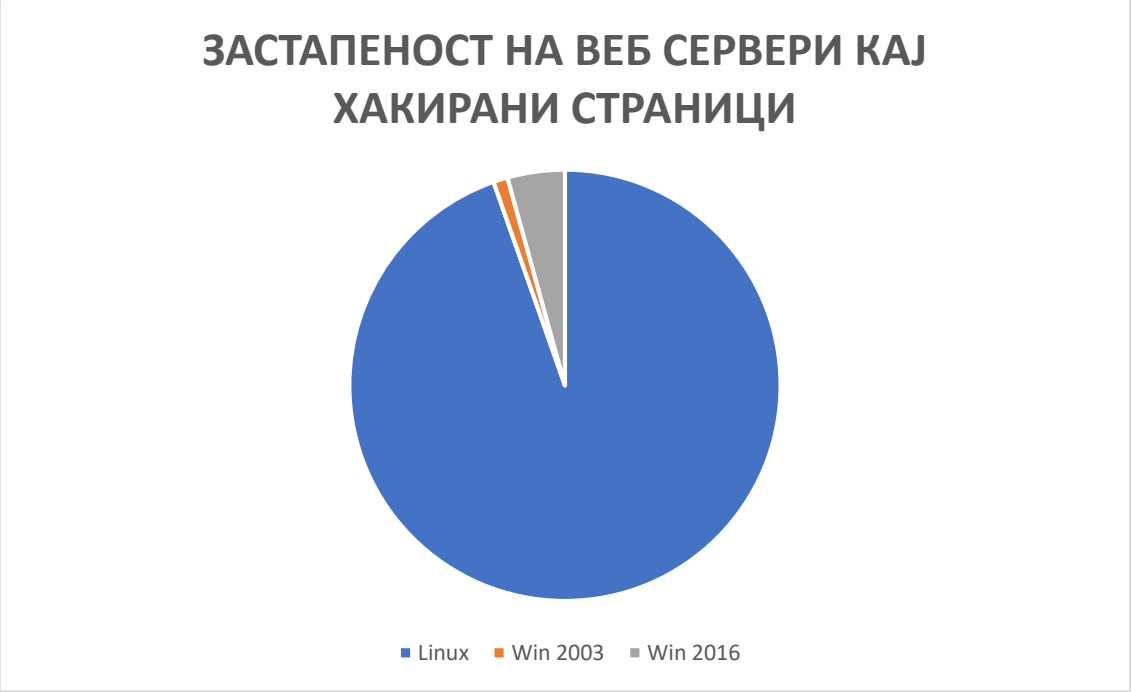
Вкупен број на регистрирани домени во .mk TLD (домен од највисоко ниво) е 29938 домени (состојба на 08.03.2021).

Во 2020 година, хакирани се вкупно 92 јавни веб-страници, споредено со 113 во 2019, 196 во 2018 и 349 во 2017 година.



Од нив, 6 се официјални страници на организации од владин сектор под .gov.mk доменот. Примарна цел при хакирањето е да се промени содржината на веб страницата и хактивизам. Информациите се од јавно достапен извор http://www.zone-h.org/archive.

Датум	Веб-страница	OS
14/08/2020	dzs.gov.mk/shiraoka.htm	Linux
15/072020	https://www.sec.mk/	Linux
21/01/2020	sovet.kicevo.gov.mk/z__r9l3l33...	Linux
21/01/2020	sovet1.kicevo.gov.mk/z__vZOQS8...	Linux
21/01/2020	hemikalii.gov.mk/images/jdownl...	Linux
05/01/2020	kicevo.gov.mk/z__hUuPR30814.htm	Linux



Дополнителната анализа на успешно хакирани веб-страници, врз основа на оперативниот систем кој се користи за веб серверот кој ги хостира овие страници, покажува дека најдоминантни оперативни системи се од фамилијата на Linux оперативните системи. Различните верзии на Linux вообичаено асоцирани со Apache и nginx, обично се дел од таканаречениот LAMP пакет, кој се користи за хостирање на некои од најпопуларните софтверски платформи со отворен код за системи кои управувуваат со веб содржини (Web Content Management Systems - Web CMSs), како што се WordPress, Joomla или Drupal. Иако Линукс е еден од по сигурните оперативни системи, главната причина за успешно хакирање на овие веб-страници е да се има администраторски привилегии на овие пакети со отворен код, а настанува како резултат на ненавремено откриени и ажурирани ранливости на CMS.

Пријави за инциденти во 2020 година

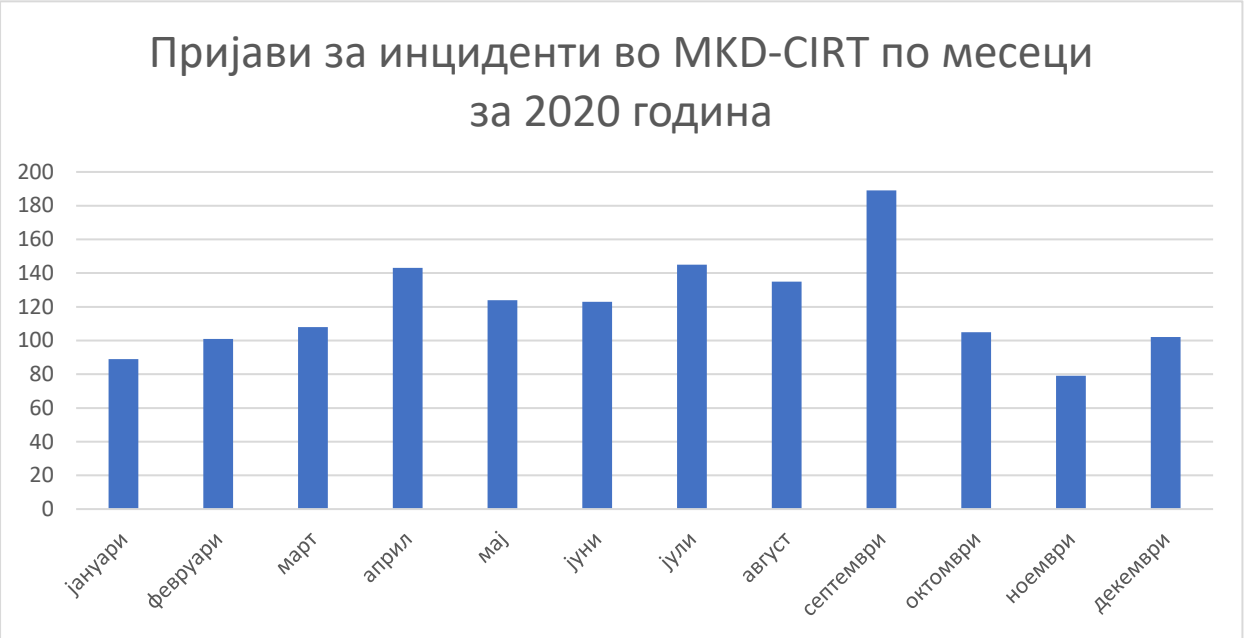
Во 2020 година, MKD-CIRT овозможи неколку начини за пријавување инциденти:

- Анонимно известување преку веб-страница на MKD-CIRT со пополнување на онлајн образецот
- Пријави за инциденти од конституентите преку нашиот систем за пријавување и управување со инциденти
- Пријави на инциденти од други организации со кои имаме воспоставено соработка и имаме доверба во точноста на доставените информации

Во 2020 година, вкупниот број на Пријави за инциденти евидентирани преку системот за прием на пријави на MKD-CIRT изнесува 1443.

Најголем дел од пријавите се автоматизирани дневни пријави за малициозни активности кои се детектирани надвор од државата, а во кои се идентификувани македонски IP адреси како извор на штетните активности. Категориите на пријавени инциденти варираат и се однесуваат за уреди

кои хостираат некој малициозен софтвер, пријави на напади за дистрибуирано одбивање на услуга (DDoS) и закани.



Видови на пријавени инциденти

Поголемиот дел од пријавите за инциденти се автоматизирани дневни пријави што доаѓаат од странство и се однесуваат за откриен штетен софтвер и fast-flux како DNS техника што се користи од страна на ботнет мрежи за да се прикријат веб-страници за фишинг и малвер со постојано менување на мрежата со компромитирани компјутери кои делуваат како прокси / посредници. И двата случаи можат да бидат знаци за постоење на комбинација од peer-to-peer мрежа, дистрибуирана команда и контрола, веб-базирано балансирање на оптоварување и пренасочување на прокси-сервери кои се користат за создавање на малициозни мрежи кои е тешко да се откријат и да се преземат мерки за заштита.

Во текот на 2020 година, MKD-CIRT доби пријави за инциденти и барања за поддршка од македонски компании при:

- онлајн измами,
- man-in-the-middle и
- фишинг напади.
- Забележан е инцидент со компромитација на сервер и клиенти за е-пошта на владина организација за што најитно е известена организацијата. и пратени се препораки до Советот за сајбер-безбедност.
- Забележан е инцидент на јавна веб страница на државна комисија. Побарани се дополните информации за настанот но не е добиен одговор.

-

Малициозен софтвер присутен во Република Северна Македонија во 2020 година

MKD-CIRT преку воспоставените канали за комуникација прима пријави за инциденти од трети лица за македонските IP адреси кои се извор на напади и штетни активности, и кои се пријавени кај нашите меѓународни соработници.

MKD-CIRT периодично ги известува операторите кои обезбедуваат услуга за широкопојасен интернет и работи со нив за да ги информира крајните корисници да ги исчистат нивните уреди од идентификуваниот малициозен софтвер, како и за заштита на безбедноста и интегритетот на мрежата на операторите кои обезбедуваат услуга за интернет. ВО моментов не постои легислатива во државата за задолжително пријавување на инциденти како и обврска за задолжително постапување по препораките од MKD-CIRT.

Според податоците од сервисот на Shadowserver, трендот за 2020 година е дневно да има до 600 - 700 македонски јавни IP v4 адреси кои во една или повеќе наврати се извор на штетни активности и најмалку ист број на уреди во државата што на дневна основа се инфицирани.