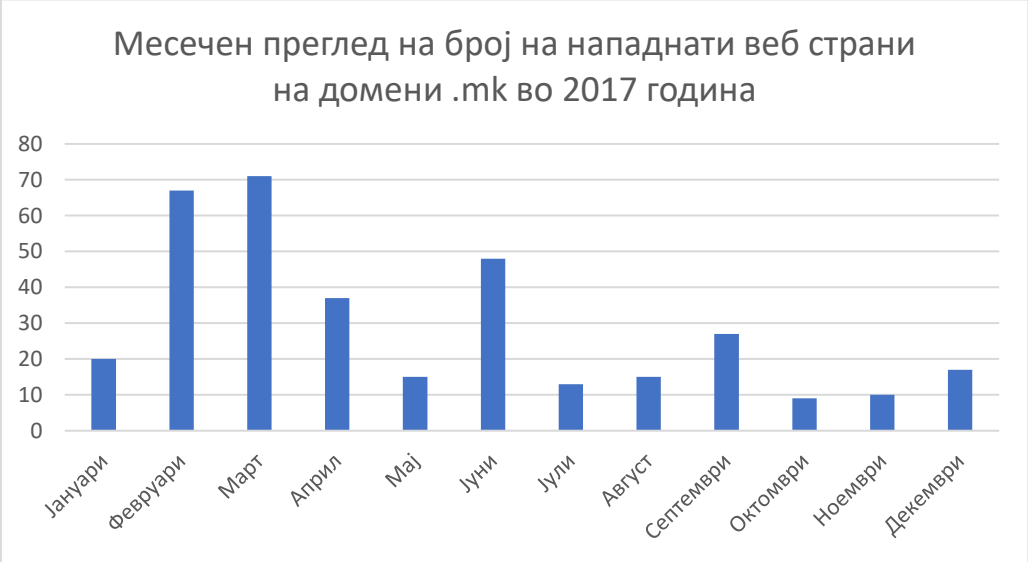
2017

Јавни веб-страници во Република Македонија

Вкупен број на регистрирани домени во .mk TLD (домен од највисоко ниво) на крај на 2017 година е 25168 домени.

Во 2017 година, хакирани се вкупно 349 јавни .mk веб-страници, од кои 23 се веб страници на .gov.mk домен. Примарна цел при хакирањето е да се промени содржината на веб страницата и хактивизам.



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 два најдоминантни оперативни системи се Linux (верзии како Debian, Suse, ...), застапен со две третини или 67% и Microsoft Windows 2003 застапен со скоро една четвртина или 25%.

Пријави за инциденти во 2017 година

Во 2017 година, вкупниот број на Пријави за инциденти изнесува 561.

Дел од пријавите се добиваат на дневна основа и се однесуваат на детектирани штетни активности на македонски IP адреси во странство. 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 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.

Во текот на 2017 година, MKD-CIRT доби пријави за инциденти и барања за поддршка од македонски компании при онлајн измами, man-in-the-middle и фишинг напади. Поради криминалната природа на овие инциденти, MKD-CIRT, го извести Министерството за внатрешни работи за овие пријавени инциденти.

Малициозен софтвер присутен **во Република Македонија** во **2017** година

Секој ден се детектирани во просек 270 македонски јавни IP v4 адреси како извори на напади или штетни активности, кои таргетираат системи надвор од земјата, при што во Република Македонија има 610.000 јавни IP адреси v4 кои ги користат македонските оператори кои нудат услуги за пренос на податоци - интернет провајдери.

Откриените видови на штетен софтвер укажуваат на користење на застарени оперативни системи, како и користење на нелиценциран или пиратски софтвер.

Најголемиот дел од пријавените јавни IP адреси се во сопственост на 19 од вкупно 101 регистрирани оператори кои обезбедуваат услуга за широкопојасен интернет за крајните корисници. Овие адреси најчесто се динамички доделени на крајните корисници - граѓаните во

Република Македонија.

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.

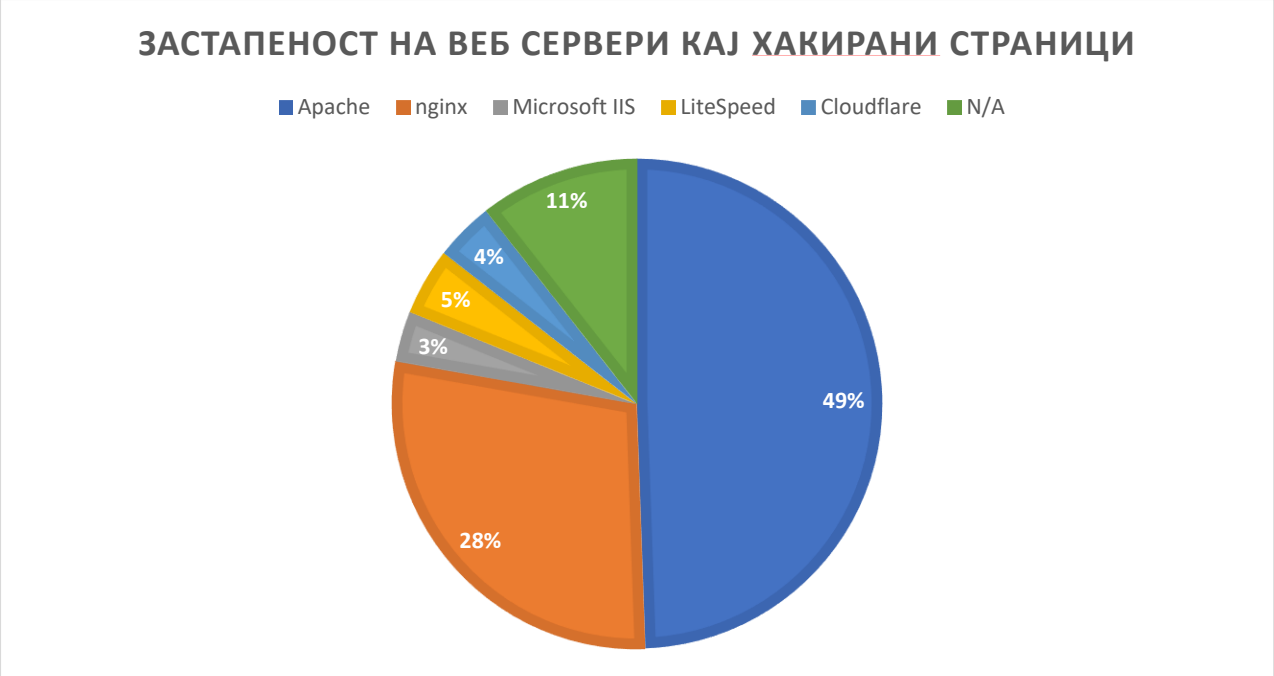
Доминантен вид на малициозен софтвер во Република Македонија во 2017 година беше Conficker, 99% од пријавените активности. Овој тип на малициозен софтвер ги експлоатира слабостите на Microsoft Windows XP и најчесто е знак за користење на застарена и пиратска верзија на оперативниот систем. Последната појава на малициозниот софтвер Mirai беше во септември 2017 година. Мираи е најпознатиот ботнет кој се користи за масовни DDoS напади кои користат IoT (Internet-of-things) уреди, како што се мрежни насочувачи и веб-камери. Заканата од идни DDoS напади од различни варијанти на Mirai се уште е присутна, бидејќи нејзиниот изворен код беше јавно објавен и може да се користи од хакерски групи.

2018

Јавни веб-страници во Република Македонија

Вкупен број на регистрирани домени во .mk TLD (домен од највисоко ниво) е 27413 домени (состојба на 05.03.2019).

Во 2018 година, хакирани се вкупно 196 јавни .mk веб-страници, споредено со 349 во 2017 година. Од нив, 24 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.

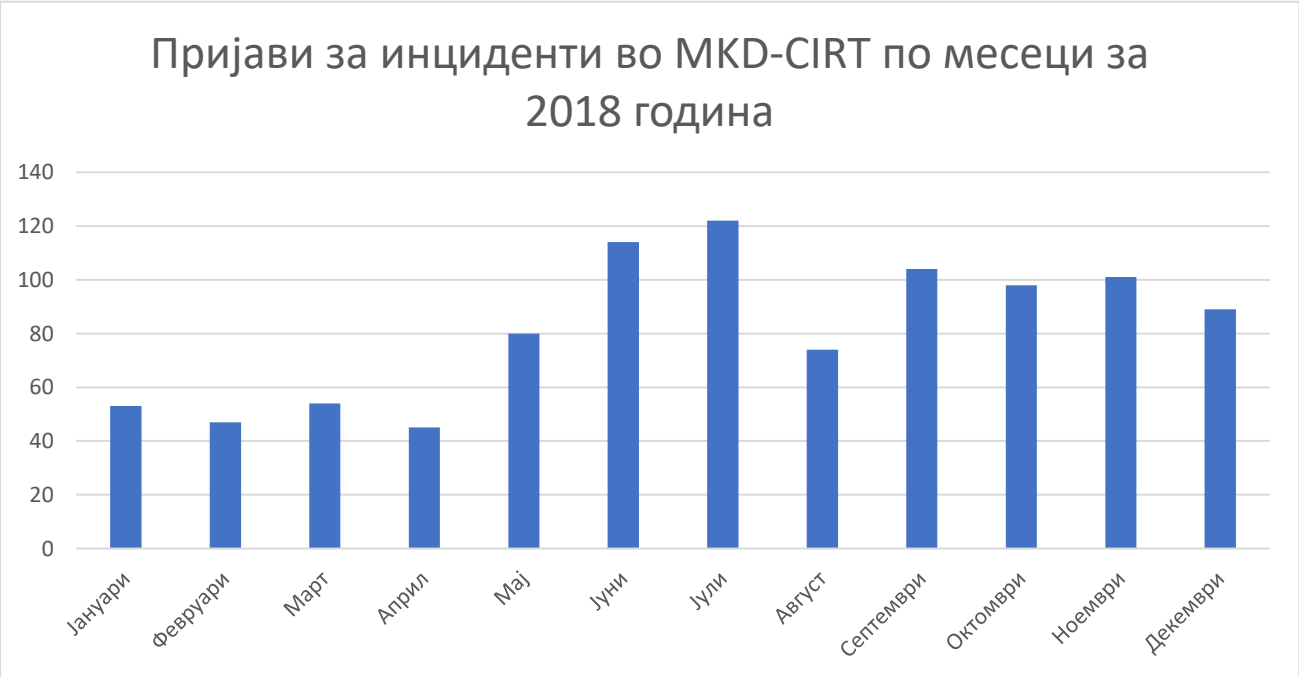


Дополнителната анализа на успешно хакирани веб-страници, врз основа на оперативниот систем кој се користи за веб серверот кој ги хостира овие страници, покажува дека два најдоминантни оперативни системи се Apache и nginx .

Пријави за инциденти во 2018 година

Во 2018 година, вкупниот број на Пријави за инциденти изнесува 981.

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 2018 година, MKD-CIRT доби пријави за инциденти и барања за поддршка од македонски компании при онлајн измами, man-in-the-middle и фишинг напади.

Малициозен софтвер присутен во Република Македонија во 2018 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.

Најголемиот дел од пријавените македонски јавни IP адреси како извор на штетни активности се во сопственост на 10 од вкупно 101 регистрирани оператори кои обезбедуваат услуга за широкопојасен интернет за крајните корисници. Овие адреси најчесто се динамички доделени на крајните корисници - граѓаните во Република Македонија. На следниот график е прикажана распределба на процентуално учество во МК јавни IP адреси по оператор на дневна основа

Од септември 2018 се забележува зголемено присуство на wannacrypt. Ransom.WannaCrypt е име за ransomware апликација која ќе ги криптира датотеките на машината на жртвата и ќе бара исплата на откупнина за жртвата да ги добие дешифрирани информациите.

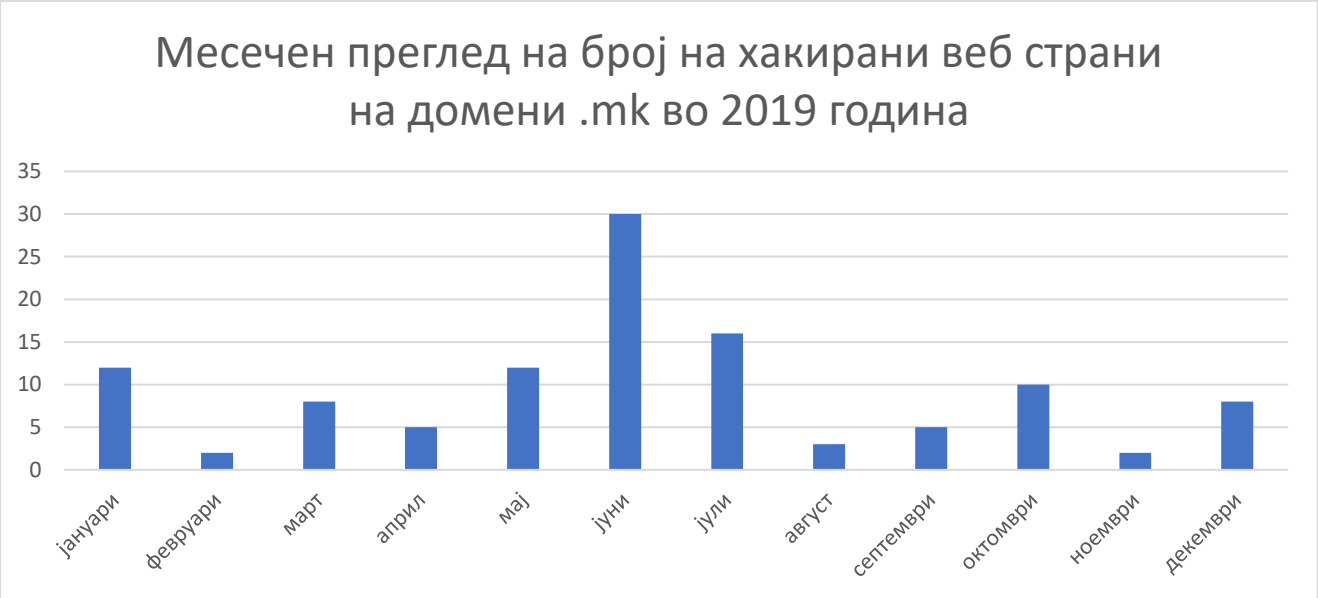
2019

Јавни веб-страници во Република Северна Македонија

Вкупен број на регистрирани домени во .mk TLD (домен од највисоко ниво) е 29938 домени (состојба на 15.03.2019).

Во 2019 година, хакирани се вкупно 113 јавни веб страници, споредено со 196 во 2018 и 349 во 2017 година. Од нив, 24 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.



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 два најдоминантни оперативни системи се Linux и Windows Server 2003 .

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 2019 година

Во 2019 година, вкупниот број на Пријави за инциденти евидентирани преку системот за прием на пријави на MKD-CIRT изнесува 1060.

Поголем 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.

Во текот на 2019 година, MKD-CIRT доби пријави за инциденти и барања за поддршка од македонски организации при онлајн измами, man-in-the-middle и фишинг напади. Забележан е инцидент со компромитација на сервер и клиенти за е-пошта на организација од јавен/владин сектор за што најитно е известен и пратени се препораки до Советот за сајбер-безбедност.

Малициозен софтвер присутен во Република Северна Македонија во 2019 година

Најприсутни типови на малвер во 2019 година се Conficker, Ransom.WannaCrypt и варијантите на Mirai. Ова укажува на понатамошно користење на застарена ИТ опрема и користење на сомнителни извори за преземање на апликации и софтвер.

2020

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 со комбинација на DDoS напади и искористување на ранливости 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 просечно секој ден да има 600 - 700 македонски јавни IP v4 адреси кои се извор на штетни активности и најмалку ист број на уреди во државата што на дневна основа се инфицирани.

2021

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 2021 година, хакирани се вкупно 122 јавни веб-страници, споредено со 92 во 2020, 113 во 2019, 196 во 2018 и 349 во 2017 година. Од нив, 8 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.

Хакирани страници на доменот .gov.mk

jpmrd.gov.mk/er.php
kicevo.gov.mk/ks.html
investnorthmacedonia.gov.mk/az...
invest.gov.mk/az.txt
tc.sep.gov.mk/noname.html
plasnica.gov.mk/shell.txt
mavrovoirostuse.gov.mk/rn.php
www.vlada.gov.mk

Хакирани страници на доменот .edu.mk

www.kimkuceviste.edu.mk/robots...
sandomasev.edu.mk/kaizer.htm
nubsk.edu.mk/images/xx.txt
shmtkgostivar.edu.mk/by_Panata...
js.ugd.edu.mk/public/site/imag...

ktk.gf.ukim.edu.mk/vuln.gif

Најчесто компромитиран серверски софтвер за поставување на веб-страници:

Пријави за инциденти во 2021 година

Во 2021 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 2021 година, вкупниот број на Пријави за инциденти евидентирани преку системот за прием на пријави на MKD-CIRT изнесува 1880, но најголем дел од пријавите се автоматизирани дневни пријави и извештаи 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

Од поединечните пријави и случаи по кои постапуваме би ги издвоиле следните:

- Повеќе случаи на хакирани македонски веб сајтови на кои се поставени фишинг содржини со кои криминалците се обидуваат да измамат корисници на услуги од компании во

странство. Често сопствениците на овие македонски веб сајтови не знаат дека хакерите поставиле штетна содржина. Често овие веб сајтови немаат редовно ажурирање и техничка поддршка.

- Случаи кога МК јавни IPv4 адреси се идентификувани во странство како извори на напади и обиди за кражба на податоци од сервери во странство:

- Случај на компромитација на сметки за е-пошта на македонски сервер за е-пошта од организација од владин/јавен сектор. Извршена е злоупотреба на меил сервер за испраќање на фишинг пораки на адреси од адресар на компромитирани сметки за е-пошта;

- Случаи на компромитација или ранливости на сервери за е-пошта што ги користат македонски организации. Кај некои од нив, бидејќи не се отстранети ранливостите, хакерите реализирале успешни рансомвер напади;

- Просечно по 2 фишинг кампањи по месец што ги таргетираат македонските граѓани. Од пријавите и примероците на овие фишинг пораки, ги идентификуваме вистинските испраќачи и бараме нивно блокирање. Вообичаено станува збор за компромитирани меил сервери во странство. Ако во пораката има линк/врска кон фишинг веб-сајт, бараме од сопственият и хостинг-компанијата да ја избришат штетната содржина; Секој граѓанин може да пријави сомнителна или фишинг порака на prijavi@mkd-cirt.mk;

- Пријави за DDoS напади. ВО овие случаи на организациите им праѓаме совети идобра пракса за заштита од вој тип напади и насоки за подобра соработка меѓу организацијата и нејзините интернет-провајдери кои имаат важна улога во спречувањето на DDoS нападите

- Случај за лажно претставување како образовна организација, со цел кражба на кориснички сметки и обиди за неавторизиран пристап во компјутерски системи;

- Ексфилтрација, т.е. кражба на податоци од македонски организации од јавен/владин сектор. Најчесто се злоупотребуваат ранливости на веб-страниците на организациите за да се добие пристап до податоци запишани на веб-серверот и да се добие пристап до другите мрежни ресурси на организацијата, како што се пораките за е-пошта и други документи на организацијата. Чести цели на овие напади/инциденти се уцена на организацијата и продажба на украдените информации и податоци.

- Периодично испраќање извештаи за идентификувани малициозни активности до интернет провајдери. Во најголем дел тоа се динамички доделени јавни IP адреси на крајни корисници/граѓани;

-

Малициозен софтвер присутен во Република Северна Македонија во 2021 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.

Во државата најзастапени типови на малвер се следните 5:

МАЛВЕР
Gamarue
Unidentified
Powmet
HiddenAds
Necurs