



Активности Националног ЦЕРТ-а

др Марко Крстић, руководиоцац
Службе за информациону
безбедност и послове
Националног ЦЕРТ-а



Садржај

- О Националном ЦЕРТ-у
- Надлежности Националног ЦЕРТ-а
- Развој нових сервиса Националног ЦЕРТ-а
- Активности Националног ЦЕРТ-а у вези са промоцијом и едукацијом из области информационе безбедности
- Пријава инцидената
- Извештај о статистичким подацима
- Сарадња на регионалном и међународном нивоу



О Националном ЦЕРТ-у

- Основан Законом о информационој безбедности, из фебруара 2016. године;
- Национални ЦЕРТ обавља послове координације превенције и заштите од безбедносних ризика у ИКТ системима у Републици Србији на националном нивоу;
- За послове Националног ЦЕРТ-а надлежна Регулаторна агенција за електронске комуникације и поштанске услуге;
- Национални ЦЕРТ почео са радом 2017. године



Надлежности Националног ЦЕРТ-а (1)

- Прати стање о инцидентима на националном нивоу;
- Пружа рана упозорења, узбуне и најаве и информише релевантна лица о ризицима и инцидентима;
- Реагује по пријављеним или на други начин откривеним инцидентима у ИКТ системима од посебног значаја, као и по пријавама физичких и правних лица, тако што пружа савете и препоруке на основу расположивих информација о инцидентима и предузима друге потребне мере из своје надлежности на основу добијених сазнања;



Надлежности Националног ЦЕРТ-а (2)

- Континуирано израђује анализе ризика и инцидената;
- Подиже свест код грађана, привредних субјеката и органа власти о значају информационе безбедности;
- Води евиденцију Посебних ЦЕРТ-ова;
- Извештава Надлежни орган на кварталном нивоу о предузетим активностима



Развој нових сервиса Националног ЦЕРТ-а

- Развој платформе за размену података између Националног ЦЕРТ-а и ИКТ система од посебног значаја и циљу информисања о актуелним ризицима и претњама у области информационе безбедности и промовисања примера добре праксе;
- Развој система за пружање раних упозорења.



Платформа за размену података о претњама у области информационе безбедности

- Завршена тестна фаза и дефинисане основне функционалности платформе;
- Кроз платформу ће бити омогућен приступ информацијама које чланице Forum of Incident Response and Security Teams (FIRST) организације деле између себе, као и информацијама о претњама и ризицима на националном нивоу које само Национални ЦЕРТ због својих надлежности добија;
- FIRST је организација која окупља преко 600 ЦЕРТ-ова из целог света;



Услови коришћења платформе

- Доступна за ИКТ операторе од посебног значаја, ЦЕРТ-ове самосталних оператора, ЦЕРТ органа власти и посебне ЦЕРТ-ове;
- Поштовање Traffic Light Protocol (TLP) и Permissible Actions Protocol (PAP);



Traffic Light Protocol (TLP) – дефиниције

- Заједница је група која дели заједничке циљеве, праксе и неформалне односе поверења.
- Организација је група која дели заједничку припадност кроз формално чланство и везана је заједничким политикама које је утврдила та организација
- Клијенти су они особе или ентитети који добијају услуге сајбер безбедности од организације.



Traffic Light Protocol (TLP) - правила

TLP:RED = Само за очи и уши појединачних прималаца, без даљег дељења.

TLP:AMBER = Ограничено дељење, примаоци ово могу ширити само по потреби унутар своје организације и међу њеним клијентима. Треба имати у виду да ознака TLP:AMBER+STRICT ограничава дељење искључиво на организацију.

TLP:GREEN = Ограничено дељење, примаоци ово могу ширити унутар своје заједнице.

TLP:CLEAR = Примаоци ово могу раширити даље свима, нема ограничења за дељење.



Permissible Actions Protocol (PAP)

ПАП: ЦРВЕНО Само активности које се не могу детектовати.

ПАП: ЖУТО Пасивна унакрсна провера.

ПАП: ЗЕЛЕНО Активне радње су дозвољене.

ПАП: БЕЛО Нема ограничења за коришћење ових информација.








Систем за пружање раних упозорења

- Унапређење превенције безбедносних ризика у ИКТ системима на националном нивоу
- Аутоматизација и консолидација раних упозорења из различитих извора (Shadowserver фондација, Shodan ...)

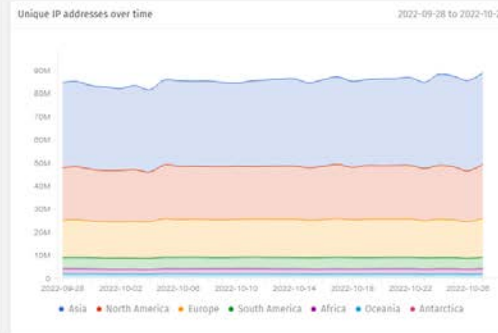
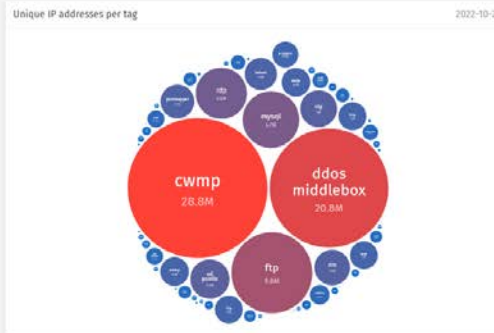
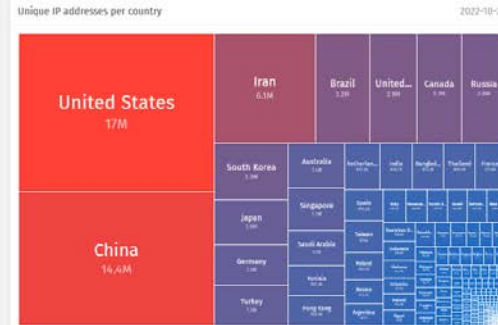


Систем за пружање раних упозорења - Shadowserver фондација -

-  Sinkholes »
-  Scans »
-  Honeypots »
-  DDoS »
-  ICS/OT »

About this data

Shadowserver scans the entire IPv4 Internet for over 100 different network protocols every day, and also performs IPv6 scans based on IPv6 hitlists for selected protocols. These are "hello" type port scans that do not exploit any vulnerability. They enable identification of misconfigured, vulnerable or abusuable devices, unnecessarily exposed attack surfaces, or simply just population enumeration. Population enumeration results can be found under the "population" source type.





Активности Националног ЦЕРТ-а у вези са промоцијом и едукацијом из области информационе безбедности

- Израда брошура и истраживања
- Сајбер азбука
- Платформа за подизање свести и знања о информационој безбедности кроз интерактивне програме – 'За безбеднији клик'
- Cyberbit платформа



Израда брошура и истраживања



21. Фебруар 2022	Како поступити уколико дође до компромитовања електронске поште и како заштитити налоге	pdf	1.18MB	Преузми	2022
9. Новембар 2021	Обавезе оператора ИКТ система од посебног значаја	pdf	2.27MB	Преузми	2021
12. Октобар 2021	Фишинг	pdf	0.97MB	Преузми	2020
4. Октобар 2021	Национални ЦЕРТ Републике Србије	pdf	2.38MB	Преузми	2019
1. Септембар 2021	Безбедно коришћење отвореног бежичног интернета (Wi-Fi)	pdf	2.68MB	Преузми	2018
2. Август 2021	Критична инфраструктура - ИКТ системи од посебног значаја	pdf	2.29MB	Преузми	2017
29. Јун 2021	Пожељно понашање и заштита приватности на друштвеним мрежама	pdf	2.12MB	Преузми	
27. Мај 2021	Врсте сајбер напада	pdf	2.08MB	Преузми	
25. Јануар 2021	Сајбер култура у Србији	pdf	6.08MB	Преузми	
1. Октобар 2020	Гласовни и СМС фишинг - Vishing и Smishing	pdf	3.66MB	Преузми	
22. Септембар 2020	Business email compromise (BEC)	pdf	949.85KB	Преузми	
21. Август 2020	Основни појмови управљања ризиком и континуитетом пословања	pdf	2.90MB	Преузми	
22. Јул 2020	Социјални инжењеринг	pdf	2.93MB	Преузми	
18. Јун 2020	Како умањити ризик од пријема фишинг мејлова (SPF, DMARC, DKIM)	pdf	485.67KB	Преузми	
28. Мај 2020	Како поступити уколико се реализује DDoS напад	pdf	326.18KB	Преузми	
26. Мај 2020	DDoS и типови DDoS напада	pdf	5.50MB	Преузми	
6. Мај 2020	Злоупотреба пандемије вируса COVID-19 у сајбер простору	pdf	1.48MB	Преузми	
30. Април 2020	VPN приступ за мала и средња предузећа	pdf	5.13MB	Преузми	
24. Април 2020	Безбедносне препоруке за рад од куће	pdf	231.29KB	Преузми	
4. Март 2020	Препоруке за опоравак од ransomware напада	pdf	149.88KB	Преузми	



Израда брошура и истраживања





Азбука термина из области сајбер безбедности

САЈБЕР АЗБУКА

А



Азбука основних сајбер препорука које могу помоћи да будемо сајбер свесни

Б



Бесплатан Wi-Fi је препоручен само за сурфовање нетом

В



Ваша лозинка је само ваша, баш као и ваша четкица за зубе

Г



Губитак података је на само један погрешан клик од нас

Д



Добра пракса је имати различите лозинке за сваки интернет налог

Ђ



Ђаци исто могу бити мете сајбер напада

Е



Електронска трговина је безбедна ако се упознамо са могућим изазовима

Ж



Живот на мрежи такође може бити пун изазова

З



Закључавајте своје уређаје, кад год их не користе

И



Интернет је веома користан, само га треба пажљиво употребљавати

Ј



Једном објављен садржај на интернету остаје заувек на интернету

К



Креирање резервних копија је једна од основних превентивних мера

Л



Лозинка увек треба да буде комплексна

Љ



Људи су најслабија карика у ланцу сајбер одбране

М



Мултифакторска аутентификација је важна додатна мера заштите

Н



Национални ЦЕРТ је увек доступан свим корисницима

Њ



Нушкала постоје свуда, па и на интернету

О



Онлајн трансакције само преко заштићене Wi-Fi конекције

П



Пријавите инцидент Националном ЦЕРТ-у

Р



Редовно ажурирање уређаја чини уређај отпорнијим на нападе

С



Сигурност је важна и на интернету

Т



Текстуалне поруке могу бити почетна тачка сајбер напада

Ђ



Ђаскање је безбедније када познајемо своје саговорнике

У



Уколико и на интернету нешто звучи сувише добро да би било истинито, вероватно није

Ф



Фишинг је најзаступљенији тип сајбер напада

Х



Хакерски напад се може догодити у било ком тренутку и било ком кориснику

Ц



Цена неплањоње корисника на интернету икада може бити веома висока

Ч



Чувајмо своју и поштујмо туђу приватност на интернету

Џ



Џак новца испод интернет дуге чувају једнораз

Ш



Што више препорука усвојимо, бићемо безбеднији на интернету



Платформа “За безбеднији клик”





Cyberbit платформа

- Донација Краљевине Норвешке
- Подржана двадесет и три (23) сценарија симулације реалистичних напада на различитим нивоима (мрежном и апликативном), као и напада на различите оперативне системе (Windows и Linux)





Пријава инцидента

Naslovna // Пријави инцидент

Пријави инцидент

PRIJAVI
INCIDENT

Molimo Vas da odaberete odgovarajuću kategoriju korisnika prijave incidenta

FIZIČKO
LICE



МАЛО I СРЕДЊЕ
ПРЕДУЗЕЋЕ



IKT SISTEM OD
POSEBNOG ZNAČAJA



Контакт телефон: 062/20-20-30

E-mail: info@cert.rs



Извештај о статистичким подацима

ИЗВЕШТАЈ О СТАТИСТИЧКИМ ПОДАЦИМА О СВИМ ИНЦИДЕНТИМА У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА У 2021. ГОДИНИ



Јун, 2022. година



Сарадња на регионалном и међународном нивоу





Хвала на пажњи!