Kingdom of the Netherlands

Centar za sigurnosne studije - BIH
Centre for Security Studies - BH

Procjena budućih trendova organiziranog kriminaliteta u BiH – OCASSESS BiH

Globalni trendovi kibernetičkih napada 2019 - 2024

Ovaj sažeti prikaz doprinosa sigurnosti u BiH nastao je u okviru projekta „Procjena budućih trendova organiziranog kriminaliteta u BiH – OCASSESS BiH", koji se realizuje uz podršku MATRA programa Kraljevine Nizozemske. Predmetni prikaz zasniva se na nalazima sprovedenog naučnog istraživanja o kibernetičkoj sigurnosti u BiH, upotrebom metode horizont skeniranja, te predstavlja informacije o globalnim trendovima pojavnih oblika kibernetičkih napada u razdoblju od 2019. do 2024. godine. Uvažavajući metodologiju horizont skeniranja, 2019. godina uzeta je kao polazište, odnosno referentna vrijednost, u odnosu na koju su praćeni signali razvoja stanja i eventualnih promjena u periodu 2020. - 2024. godina.

2019

Referentna vrijednost

Pojavni oblici napada:

Ransomware:
Grupa "Ryuk" odgovorna je za značajne gubitke u sektorima poput zdravstva

Phishing:
Upotreba sofisticiranih tehnika za napade na finansijske institucije

DDoS napadi:
Upotreba botneta za ometanje rada kritičnih infrastruktura

Zero-Day ranjivosti:
Zloupotreba nepoznatih sigurnosnih slabosti

Napadači i grupe:

Organizirane kriminalne grupe:
Grupe "FIN7" i "APT29" koristile su napredne taktike infiltracije

Državno sponzorirane grupe:
Uključene u industrijsku i političku špijunažu

Haktivisti:
Ciljali su korporacije i vlade, motivirani ideološkim razlozima

2020 – 2024

Pojavni oblici napada:

2020
Phishing, Ransomware, Supply Chain napadi

2021
Phishing, Ransomware, IoT napadi , Spoofing

2022
IoT napadi, Ransomware as a Service (RaaS), Deepfake Tehnologija, Business Email Compromise (BEC)

2023
AI-Driven Malware, Zero-Click Exploits, Blockchain napadi

2024
Automatizacija napada (AI), IoT napadi, Supply chain napadi, Zero-click exploits , Deepfake, Blockchain ransomware

Napadači i grupe:

2020
Grupe poput REvil, DarkSide i Maze izvodile su sofisticirane ransomware napade, s naglašenim međunarodnim djelovanjem i vezama prema Rusiji

2021
Conti dominira ransomware scenom, uz intenziviranje kineske i ruske industrijske špijunaže

2022
BlackCat podiže tehničku složenost napada, dok Iran pojačava prisutnost u globalnim kibernetičkim sukobima

2023
Clop koristi napredne metode za izbjegavanje detekcije; Sjeverna Koreja nastavlja finansiranje režima kroz kibernetički kriminal

2024
Royal postaje istaknuti akter; Aktivnost državnih aktera iz Azije

Šta znamo o kibernetičkim napadima?

Ransomware

Maliciozni softver koji kriptira podatke i uvjetuje njihov povrat isplatom otkupnine

Phishing

Kibernetička manipulacija kojom se lažnim komunikacijama pribavljaju povjerljivi podaci

DDoS napadi

Koordinirani pokušaji preopterećenja sistema radi onemogućavanja pristupa korisnicima

Zero-Day ranjivosti

Neotkriveni sigurnosni propusti koje napadači eksploatiraju prije nego što je dostupna zakrpa

Supply Chain napadi

Zloupotreba ranjivosti u dobavljačkim mrežama s ciljem kompromitiranja sistema

Spoofing

Tehnika lažiranja identiteta radi prevare korisnika, često u cilju krađe podataka

Ransomware as a Service (RaaS)

Komercijalizacija ransomwarea - ustupanje alata napadačima u zamjenu za dio otkupnine

Deepfake Tehnologija

Primjena AI-a (umjetne inteligencije) za oponašanje stvarnih osoba u audiovizualnom sadržaju

Business Email Compromise

AI-prevara putem lažnih poslovnih e-mailova radi krađe novca ili podataka

AI-Driven Malware

Maliciozni softver koji koristi AI za izbjegavanje detekcije i izvršavanje napada

Zero-Click Exploits

Zloupotreba ranjivosti bez korisničke interakcije
- napadi se pokreću uz pomoć AI-a

Blockchain Napadi

Zloupotreba ranjivosti u mrežama za krađu sredstava ili manipulaciju podacima

Automatizacija napada

Upotreba AI-a i automatiziranih alata za efikasno izvođenje kibernetičkih napada

Blockchain ransomware

Upotreba blockchain tehnologije za prijenos otkupnina, čineći praćenje i identifikaciju napadača težim

#MATRA #NLinBiH

Ovaj projekat finansira Vlada Kraljevine Nizozemske kroz MATRA program. Za sadržaj je odgovoran Centar za sigurnosne studije i on ne odražava nužno stavove Ministarstva vanjskih poslova Kraljevine Nizozemske.