REPUBLIKA SRBIJA
RATEL
REGULATORNO TELO ZA ELEKTRONSKE KOMUNIKACIJE I POŠTANSKE USLUGE

PREGLED TRŽIŠTA

ELEKTRONSKIH KOMUNIKACIJA I POŠTANSKIH USLUGA

U REPUBLICI SRBIJI U 2023. GODINI

Napomena:

Imajući u vidu da je u toku obrada finansijskih podataka koje dostavljaju učesnici na tržištu elektronskih komunikacija kroz odgovarajuće upitnike, Pregled tržišta elektronskih komunikacija i poštanskih usluga za 2023. godinu će naknadno biti dopunjen ovim podacima. Takođe, naknadno će biti objavljena i poglavlja ***Osvrt na tržište telekomunikacija u Evropskoj uniji*** *i* ***Indeks digitalne ekonomije i društva (DESI),*** *a nakon pribavljanja i obrade podataka relevantnih za navedena poglavlja.*

Beograd, jun 2024. godine

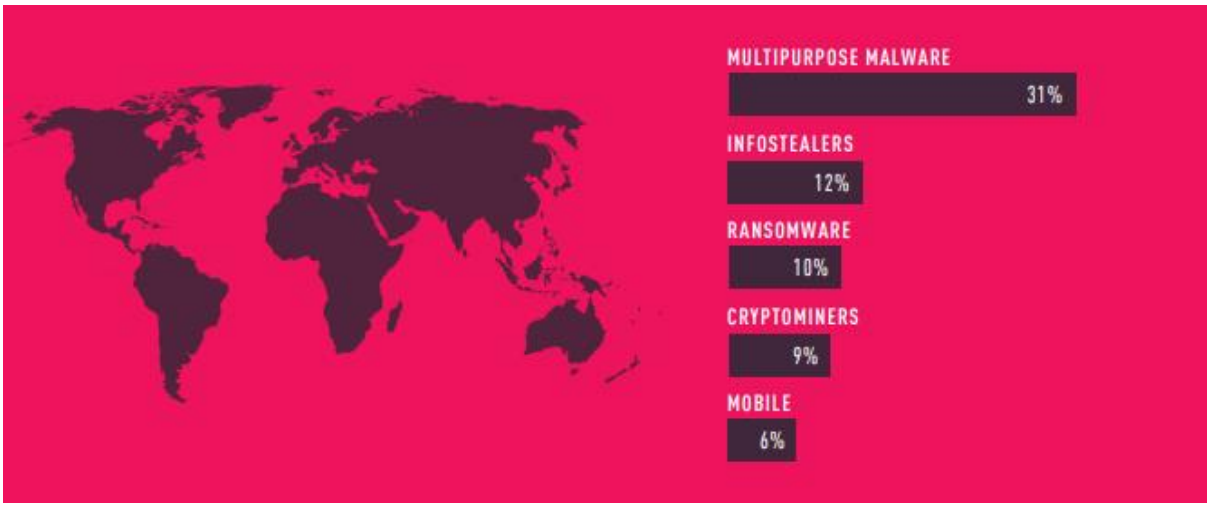
15. BEZBEDNOSNI RIZICI U INFORMACIONO-KOMUNIKACIONIM SISTEMIMA

Stanje informacione bezbednosti u svetu

1. Statistika napada po različitim tipovima malvera

Na slici 15.1. dat je prikaz procenta zastupljenosti različitih tipova malvera (malicioznog softvera) na globalnom nivou u 2023. godini (prikaz je preuzet iz izveštaja kompanije *Check Point*). Može se uočiti da su najzastupljeniji napadi malverima koji se mogu koristiti u više namena (*multipurpose malware)*. Sledeći po zastupljenosti je maliciozni softver tzv. *Infostealer* malver koji napadači mogu koristiti u ranim fazama napada kako bi prikupili informacije o meti napada. Na trećem mestu, nalazi se iznuđivački softver (*Ransomware*) koji beleži porast sa petog mesta u broju napada u odnosu na prethodnu godinu. Sledeći na listi su napadi koji „preuzimaju" resurse sa uređaja žrtve kako bi „rudarili" kriptovalute (*Cryptominers*), dok poslednje mesto na ovoj listi zauzimaju maliciozni softveri razvijeni za potrebe napada na mobilne uređaje.

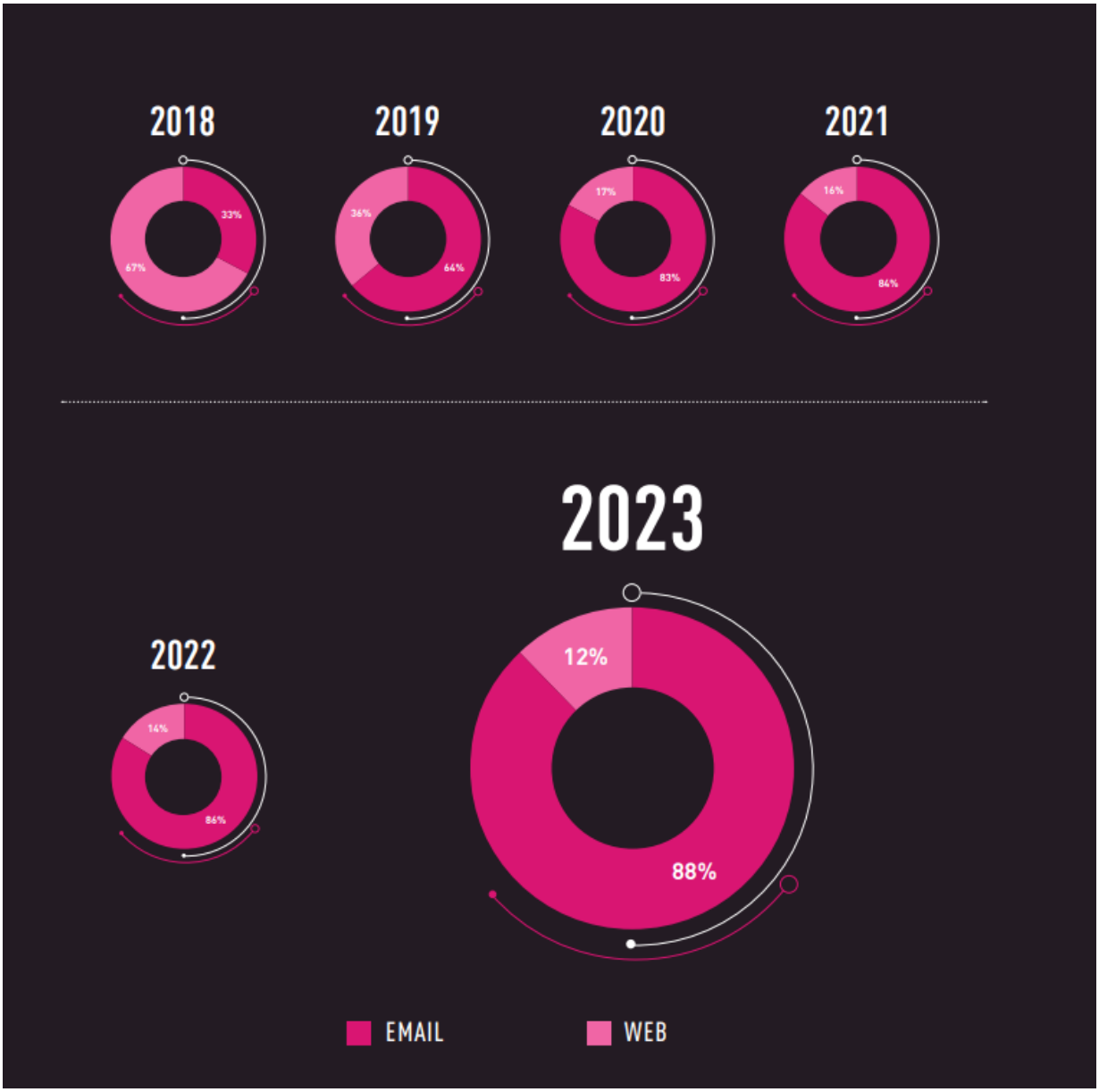
Slika 15.1. Procenat zastupljenosti različitih tipova malvera na globalnom nivou



2. Načini distribucije malvera

Kada se govori o načinima distribucije malvera, tokom 2018. godine dominantan vid bio je putem internet stranica, međutim već naredne godine situacija se promenila i načini širenja malicioznog softvera bili su putem elektronske pošte. Ovaj trend se održao i tokom narednih godina sa procentualnim porastom iz godine u godinu. U poređenju sa 2022. godinom, malveri distribuirani putem elektronske pošte su u blagom porastu u 2023. i to za 2%, kao što je prikazano na slici 5.2.

Slika 15.2. Uporedni prikaz broja napada koji za distribuciju koriste elektronsku poštu i internet stranice (za period 2018 - 2023. godina)



3. Statistika napada po različitim familijama malvera

Procenat organizacija na svetskom nivou, koje su bile zaražene posmatranom familijom malvera prikazan je na Slici 15.3.

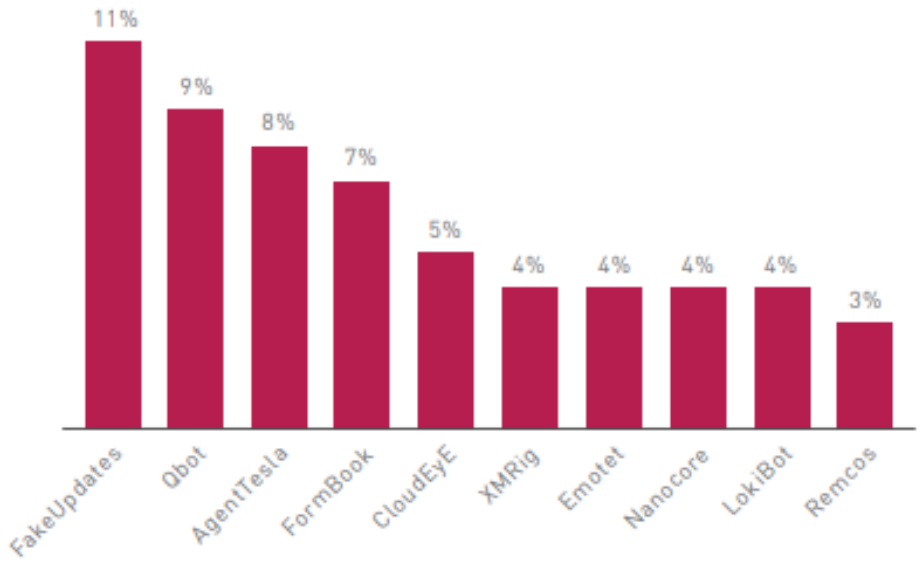
Značajnije promene u rangiranju malvera u odnosu na prethodnu godinu su pojava nove familije malvera *FakeUpdates*, koji se naziva još i *SocGholish.* Ovaj tip malvera oslanja se na mrežu kompromitovanih internet sajtova koji preusmeravaju korisnike na stranice za preuzimanje malicioznih ažuriranja za različite softvere i internet pregledače. Preuzimanjem fajlova za navodna ažuriranja, korisnici se zapravo navode na preuzimanje i pokretanje *JavaScript downloader-a,* a koji služi kao inicijalni vektor napada omogućavajući na taj način dalju kompromitaciju pomoću drugih tipova malvera kao što su *GootLoader, NetSupport and DoppelPaymer.*

Qbot, zauzima drugo mesto na ovoj listi. Ovaj tip malvera namenjen *Windows* korisnicima, prvi put je otkriven 2008. godine kao bankarski trojanac, dok je tokom decembra prošle godine ovaj malver otkriven i u mnogim fišing kampanjama.

Emotet beleži pad sa prvog mesta u odnosu na 2022. godinu i uprkos padu ipak je pogodio 4% korporativnih mreža tokom 2023. godine na globalnom nivou.

Među malverima koji se nalaze na drugom i trećem mestu, a koji su se koristili za krađu podataka (*Infostealers*) u 2023. godini, nalaze se malveri *AgentTesla* i *Formbook.*

Slika 15.3. Zastupljenost malvera na globalnom nivou

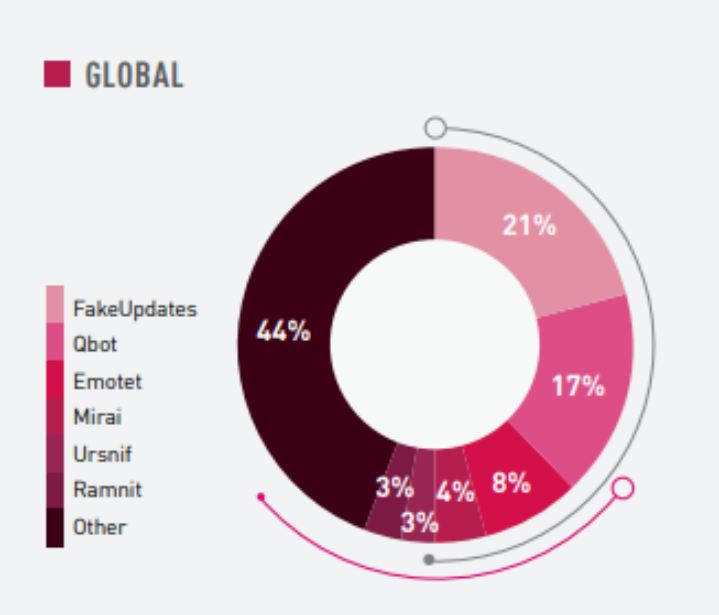


4. Statistika napada po različitim familijama višenamenskih malvera (*multipurpose malware*)

Najzastupljeniji napadi u 2023. godini su oni napadi koji koriste višenamenske malvere kao inicijalni vektor za dobijanje pristupa sistemu. Kod ovih napada najčešće su korišćeni malveri *FakeUpdates* (21%), *Qbot* (17%), *Emotet* (8%), *Mirai* (4%), *Ursnif* i *Ramnit* (po 3%), i drugi malveri (slika 15.4.).

U drugoj polovini 2023. godine *DarkGate* je stekao značajnu popularnost zbog svoje sposobnosti da izbegne detekciju sigurnosnih sistema. Za razliku od *Emotet* i *Qbot*, ovaj tip malvera koristi direktnu strategiju modela *Malware-as-a-Service (MaaS)*.

Slika 15.4. Procenat zastupljenosti različitih familija višenamenskih malvera (*multipurpose malware*) na globalnom nivou

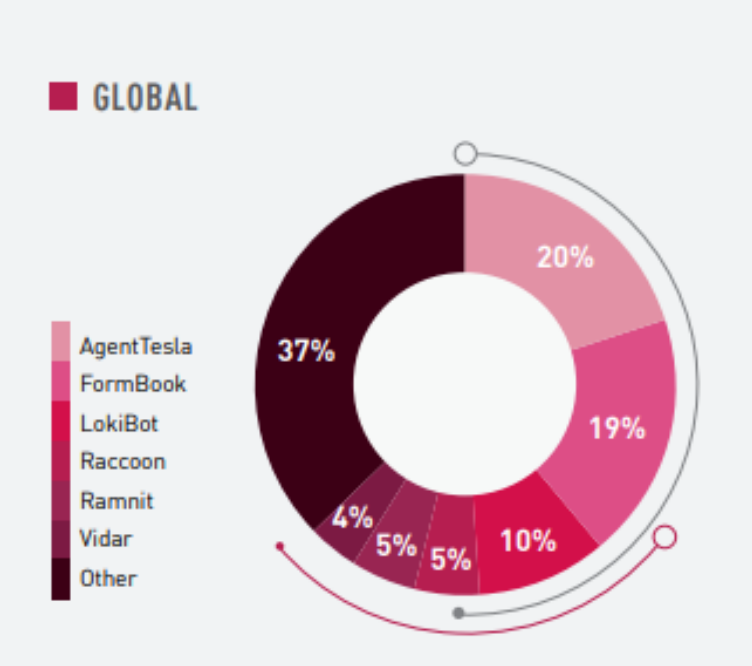


5. Statistika napada po različitim familijama malvera za krađu korisničkih podataka

Ovom familijom dominira nekoliko malvera, kao što je prikazano na slici 15.5., od kojih se mogu izdvojiti *AgentTesla* (20%), *Formbook* (19%) i *LokiBot* (10%), koji su i ove godine široko rasprostranjeni.

AgentTesla prvi put otkriven je 2014. godine, a njegova trenutna verzija je unapređena za krađu kredencijala iz različitih aplikacija, uključujući i internet pretraživače, VPN, FTP servise i imejl klijente.

Slika 15.5. Statistika napada po različitim familijama malvera za krađu korisničkih podataka

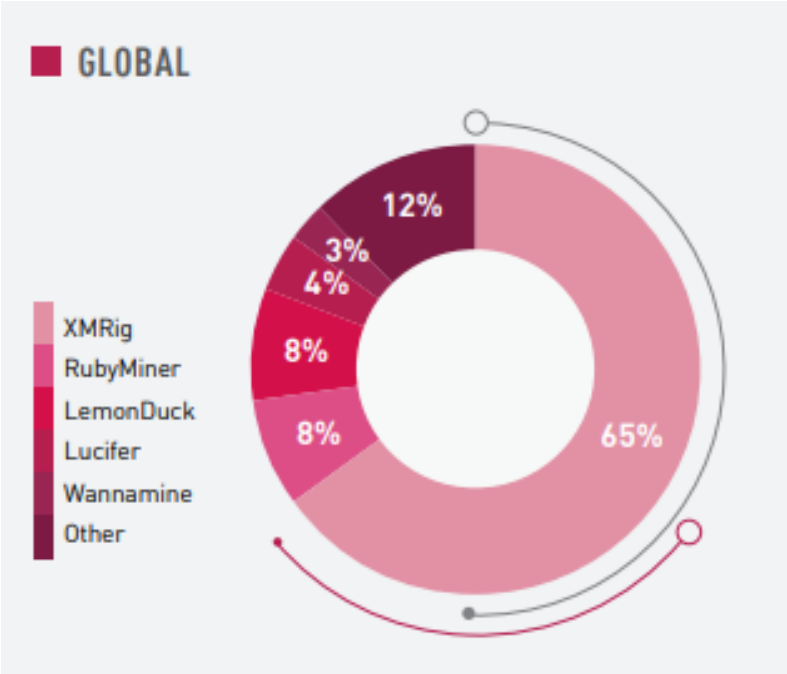


6. Statistika napada po različitim familijama malvera za krađu kriptovaluta

Ilegalno rudarenje kriptovaluta nastavlja da beleži pad i tokom 2023. godine, usled nepostizanja vrednosti *Bitcoin*-a iz 2021. godine. Samo 9% globalnih korporacija bilo je pogođeno malverima za krađu kriptovaluta u 2023. godini u poređenju sa 16% u 2022. godini.

Monero, kriptovaluta poznata po svojoj privatnosti, ostaje profitabilna za rudarenje, a njen uobičajen alat otvorenog koda za rudarenje, XMRig, korišćen je u 65% napada kritorudarenjem u 2023. godini (slika 15.6.).

Slika 15.6. Statistika napada po različitim familijama malvera za krađu kriptovaluta



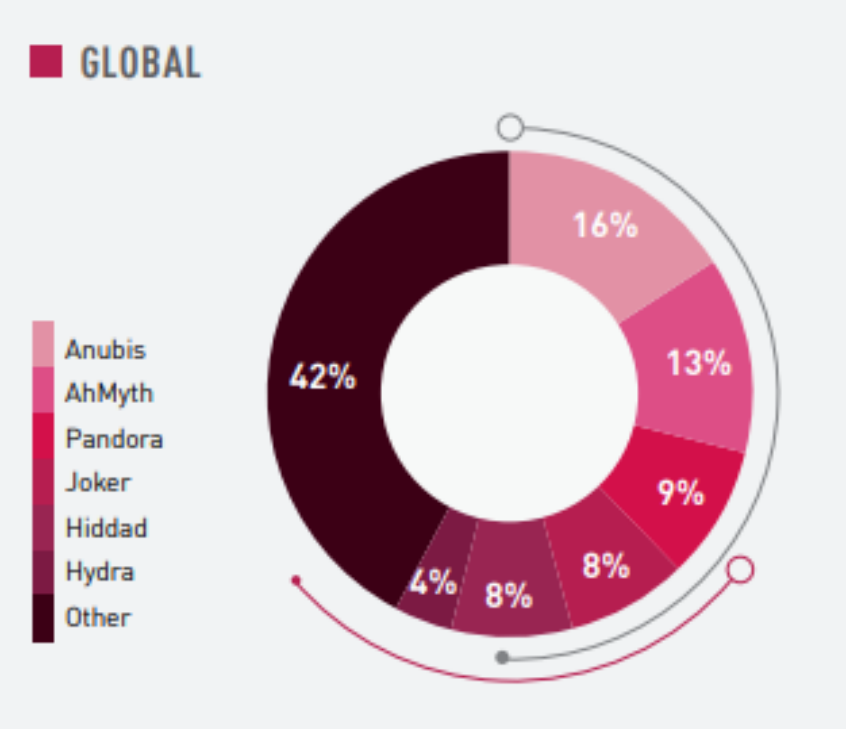
7. Statistika napada na mobilne uređaje po različitim familijama malvera

Mobilni uređaji predstavljaju glavne mete sajber napada zbog njihove centralne uloge u svakodnevnom životu korisnika i važnosti podataka koje sadrže.

Anubis, koji se i dalje nalazi u vrhu najčešćih malvera (42%), kao što je prikazano na slici 15.7. je bankarski trojanac dizajniran za *Android* mobilne uređaje, i primećen je u stotinama različitih aplikacija dostupnih na *Google Play* prodavnici.

AhMyth, Android trojanac za daljinski pristup (RAT), je zlonamerni softver otvorenog koda koji je besplatno dostupan na *GitHub*-u i često se koristi kao osnova za napade. Varijanta ovog malvera *AhRat* pronađena je u aplikaciji pod nazivom „*iRecorder-Screen Recorder*“, koja je dostupna u *Google Play* prodavnici sa preko 50.000 preuzimanja.

Slika 15.7. Statistika napada na mobilne uređaje po različitim familijama malvera

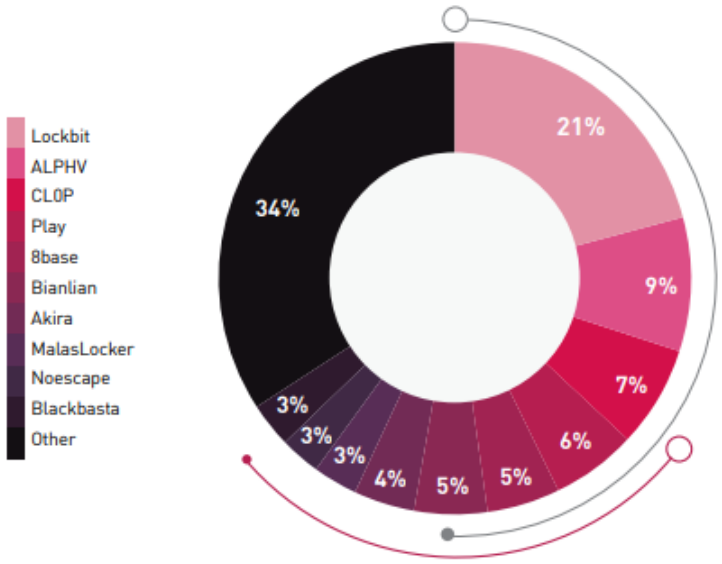


8. Statistika napada iznuđivačkim softverima – ransomver

Tokom 2023. godine ukupno 68 aktivnih ransomver grupa su objavili da su uspešno realizovali napade na kompanije i javno iznudili preko 5.000 žrtava, što predstavlja značajan porast u odnosu na prethodne godine. Sajber napadači, koriste i tehniku duple iznude, kako bi pojačali pritisak na žrtve koje ne plate odmah otkupninu.

Lockbit se našao na samom vrhu liste (slika 15.8.) i odgovoran je za 21% prijavljenih incidenata u 2023. godini, sa preko 1.050 slučajeva. Akteri pretnji obično daju žrtvama rok od jedne do dve nedelje za plaćanje otkupnine, kako kompanije ne bi bile javno izložene, što sugeriše da bi stvarni broj žrtava mogao biti znatno veći.

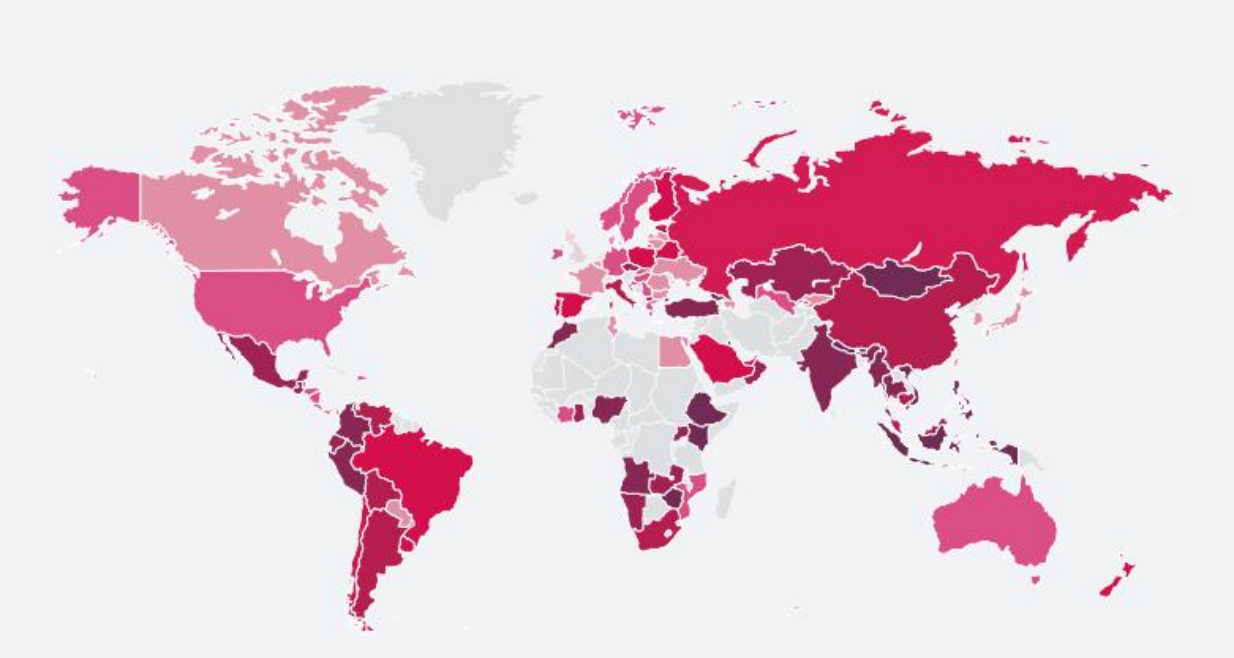
Slika 15.8. Statistika napada softverima sa dvostrukom iznudom po različitim familijama



9. Check Point Global Threat indeks

Na Slici 15.9. je dat grafički prikaz vrednosti *Check Point Global Threat* indeksa po državama u 2023. godini. Ovaj indeks se računa na osnovu informacija o napadima prikupljenim u realnom vremenu uz pomoć *Threat Cloud World Cyber Threat Map* platforme i opisuje verovatnoću da uređaj u posmatranoj zemlji bude zaražen malicioznim softverom. Primetno je da postoje razlike između zemalja u nivou opasnosti od malicioznog softvera. Što je boja određene zemlje tamnija, veća je verovatnoća da uređaj bude zaražen malicioznim softverom, dok su sivom bojom obeležene zemlje za koje nije bilo dovoljno podataka za analizu.

Slika 15.9. Grafički prikaz *Check Point Threat* indeksa po državama

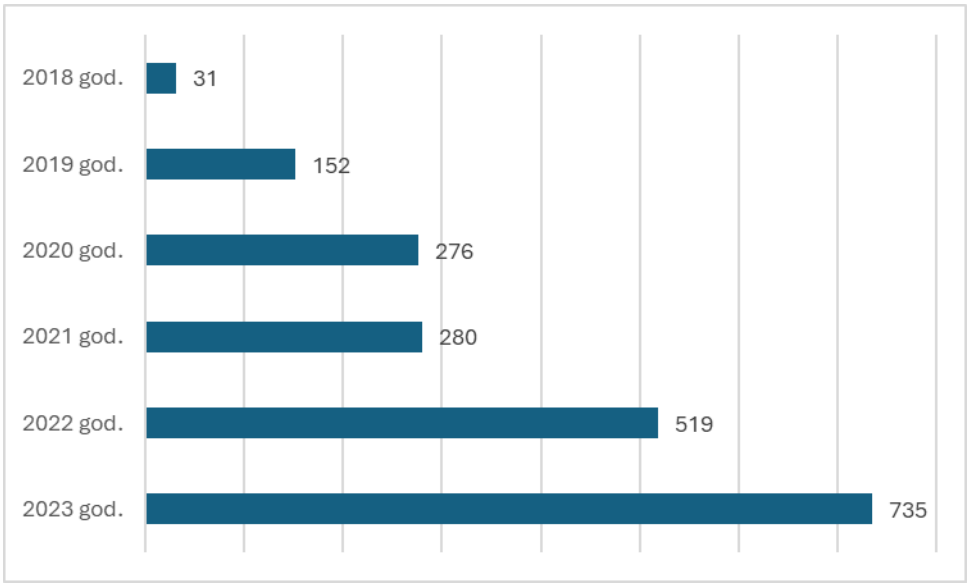


Stanje informacione bezbednosti u Srbiji

Zakonom o informacionoj bezbednosti („Službeni glasnik RS“, broj 6/16, 94/17 i 77/19) propisana je obaveza operatora IKT sistema od posebnog značaja da izveste nadležni organ o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti.

U periodu od 2018. godine do 2023. godine primećeno je značajno uvećanje broja prijava incidenata Nacionalnom CERT-u (Slika 15.10). Ovaj trend ne samo da ukazuje na rastući broj pretnji, već i na povećanje svesti građana i zaposlenih u IKT sistemima, o važnosti deljenja informacija i obaveštavanja relevantnih institucija kao i u poverenje u savete koje Nacionalni CERT pruža.

Slika 15.10: Broj prijava Nacionalnom CERT-u od 2018. godine do 2023. godine



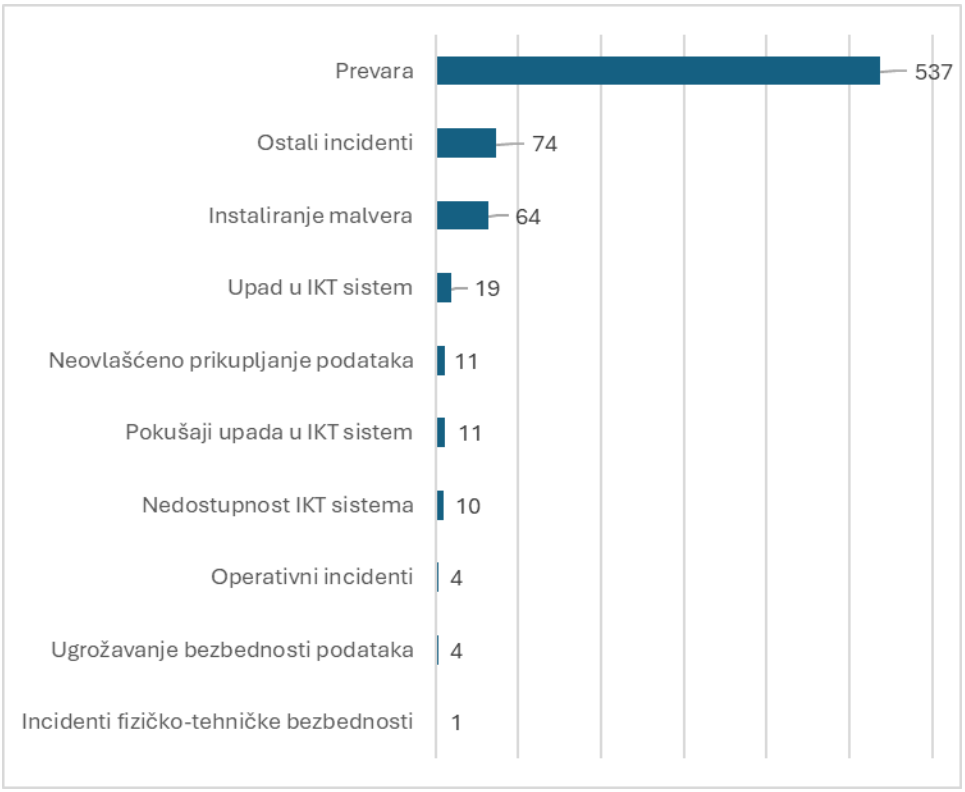
U 2023. godini, Nacionalnom CERT-u je prijavljeno 735 incidenta, što predstavlja povećanje više od 40% u odnosu na prethodnu godinu. Incidenti koji su narušili bezbednost IKT sistema, a koji su vezani za izvršenje krivičnog dela, prijavljivani su u skladu sa odredbama zakona i podzakonskih akata ili su prosleđivani Posebnom tužilaštvu za visokotehnološki kriminal. Broj takvih incidenata u 2023. godini je bio 47.

Na slici 15.11 prikazani su prijavljeni incidenti prema grupi incidenata. Najveći broj prijava se odnosi na prevaru, a pod prevarom se podrazumevaju fišing napadi, neovlašćeno korišćenje resursa i drugi oblici prevare.

Tokom 2023. godine sprovedeno je nekoliko velikih fišing kampanja čija su meta bili korisnici interneta u Srbiji. Posebno se ističu kampanje koje su bile usmerene na korisnike poštanskih usluga i platformi za e-trgovinu. E-pošta je najčešće sadržala obaveštenje da je

stigao paket za korisnika, ali da nije mogao biti isporučen jer nije uplaćen određeni iznos za carinske troškove ili se zahtevalo ažuriranje adrese primaoca. Klikom na ponuđeni link korisnik se preusmeravao na lažnu stranicu za internet plaćanje Pošte Srbije, u kojoj se zahtevao unos podataka sa platne kartice koji su omogućili napadačima pristup bankovnom računu i finansijsku dobit za napadača. Fišing kampanja usmerena na korisnike platformi za e-trgovinu se odvijala tako što je navodni kupac komunikaciju inicirao pitanjem oglašivaču o dostupnosti proizvoda i mogućnosti da se kupovina obavi elektronskim putem. Tada je napadač u svoje ime ili u ime „administratora platforme za e-trgovinu“ dostavljao žrtvi tj. oglašivaču link ka lažnoj veb stranici na kojoj je bilo prikazano da je navodni kupac već uplatio sredstva preko aplikacije i da je potrebno da oglašivač na veb formi unese podatke sa svoje bankovne kartice (broj kartice i CVV broj) kako bi mu se navodno izvršila uplata, odnosno transfer sredstava. Na taj način je napadač preuzimao sredstva sa bankovnog računa žrtve. Nacionalni CERT je povodom ovih fišing napada objavio više obaveštenja i saopštenja za javnost kako bi građanima ukazao na zastupljenost ovih prevara.

Slika 15.11: Prijavljeni incidenti u 2023. godini prema grupi incidenata



Pet najčešće prijavljivanih incidenata u 2023. godini su prikazani na Slici 15.12.

Fišing je sajber napad koji je najčešće prijavljivan u 2023. godini, a sprovodi uz pomoć elektronske pošte, društvenih mreža, telefonskog poziva ili SMS-a, kojim se zahteva da se poseti link ili otvori prilog. Napadač koristi socijalni inženjering da bi se predstavio kao

neko poznat ili renomirana institucija i tako naveo žrtvu da ostavi poverljive podatke ili preuzme zlonamerni softver. Ovaj napad je često povezan sa napadima poput krađe identiteta, preuzimanja novčanih sredstava sa računa, instalacije malvera, mreže botova i sajber špijunaže. U 2023. godini je Nacionalnom CERT-u stiglo 417 prijava, a najveći broj se odnosi na fišing kampanje čija su meta bili korisnici poštanskih usluga i platformi za e-trgovinu.

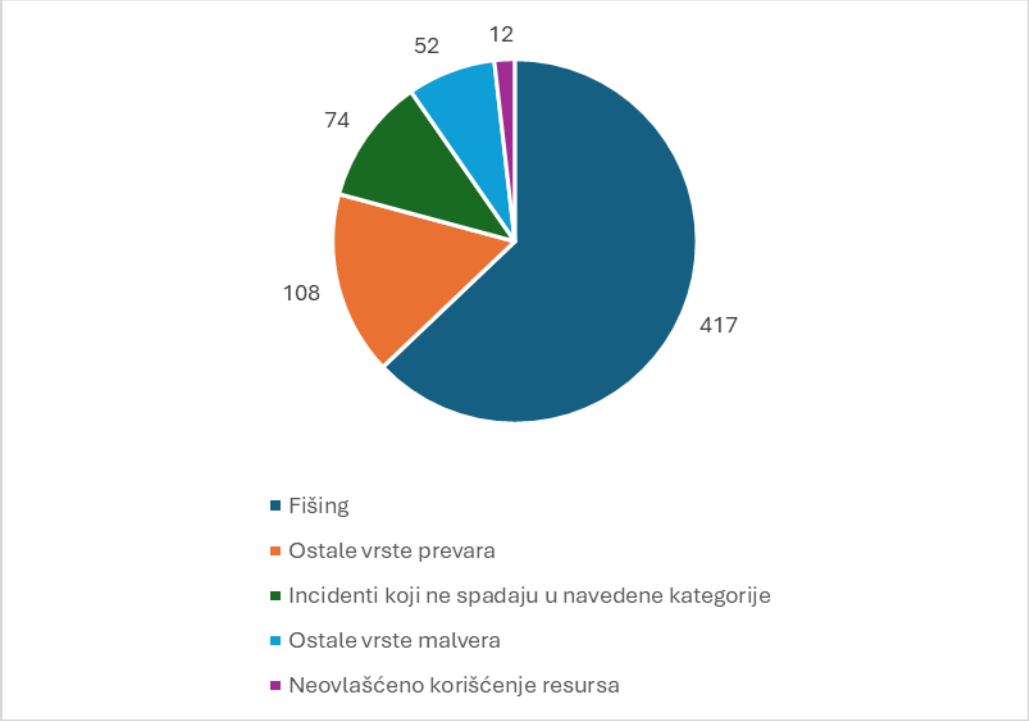
Nacionalni CERT je dobio 108 prijava o **ostalim vrstama prevara**, a ovaj broj ukazuje na broj prevara u kojima je došlo do preuzimanja novčanih sredstava sa računa građana.

Incidenti **koji ne spadaju u kategorije** navedene u Uredbi o postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja mogu biti, na primer detekcija potencijalno nebezbednih aplikacija, neodobrene platne transakcije i lažni profili na društvenim mrežama, a takvih prijava je bilo 74.

Malver (engl. *malware*, izvedeno od *malicious software*) predstavlja svaki softver koji je napisan u zlonamerne svrhe, odnosno čiji je cilj da nanese štetu računarskim sistemima ili mrežama. U ove programe spadaju: računarski virus, računarski crv, ransomver, računarski trojanac, špijunski softver i rutkit. Nacionalnom CERT-u je prijavljeno 52 incidenta koja se odnose na zlonamerne programe za koje nije postojalo dovoljno podataka da bi mogli da se svrstaju u neku od navedenih kategorija.

Neovlašćeno korišćenje resursa je vrsta incidenta koja se javlja u grupi prevara, a broj prijava u 2023. godini bio je 12.

Slika 15.12: Pet najčešće prijavljivanih incidenata u 2023. godini



Krivična dela protiv bezbednosti računarskih podataka

Tokom 2023. godine u Posebnom tužilaštvu za visokotehnološki kriminal formirano je ukupno 6.456 predmeta, i to:

- 485 predmeta protiv poznatih punoletnih učinilaca;

- 2.907 predmeta protiv nepoznatih učinilaca i;

- 3.064 predmeta u vezi sa raznim krivičnim događajima.

Broj formiranih predmeta povećan je za 14,67% u odnosnu na 2022. godinu, kada je formirano 5.630 predmeta.

Sledeći podaci se odnose isključivo na krivične prijave podnete protiv poznatih punoletnih učinilaca krivičnih dela tokom 2023. godine i preduzete radnje Posebnog javnog tužilaštva za visokotehnološki kriminal u tom periodu i predstavljaju broj lica, a ne broj predmeta ili procesnih radnji.

- Broj prijavljenih lica - 554;
- Broj lica protiv kojih su podneti zahtevi za prikupljanje potrebnih obaveštenja – 172;
- Broj lica protiv kojih je doneta naredba o sprovođenju istrage – 15;
- Broj lica protiv kojih su sprovedene dokazne radnje – 178;
- Broj lica protiv kojih su podneti optužni predlozi – 105;
- Broj lica protiv kojih su podignute optužnice – 28;
- Broj zaključenih sporazuma o priznanju krivičnog dela – 61.