REPUBLIKA SRBIJA
RATEL
REGULATORNO TELO ZA
ELEKTRONSKE KOMUNIKACIJE
I POŠTANSKE USLUGE

PREGLED TRŽIŠTA

ELEKTRONSKIH KOMUNIKACIJA I POŠTANSKIH USLUGA

U REPUBLICI SRBIJI U 2024. GODINI

Napomena:
Podaci na osnovu kojih se analizira i priprema pregled stanja na tržištu elektronskih komunikacija u Republici Srbiji dobijaju se na osnovu upitnika koje učesnici na navedenom tržištu dostavljaju Regulatornom telu za elektronske komunikacije i poštanske usluge do 30.6.2025. godine, te će određeni podaci biti objavljeni naknadno, nakon prikupljanja i obrade, u okviru publikacije „Pregled tržišta elektronskih komunikacija i poštanskih usluga u 2024. godini“.

Beograd, jun 2025. godine

16. BEZBEDNOSNI RIZICI U INFORMACIONO-KOMUNIKACIONIM SISTEMIMA

Stanje informacione bezbednosti u svetu

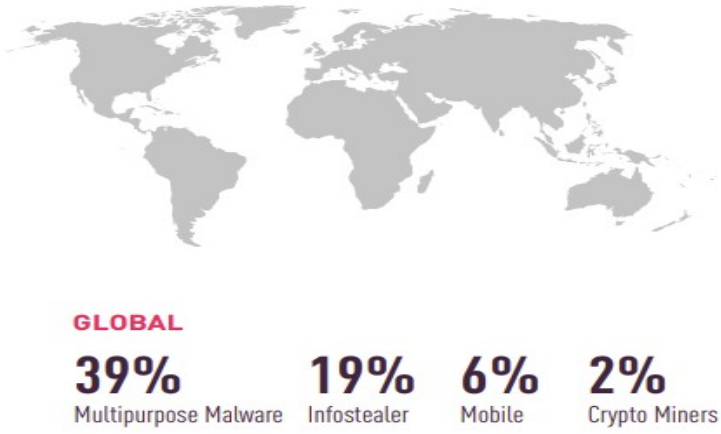
1. Statistika napada po različitim tipovima malvera

Na slici 16.1. prikazani su različiti tipovi malvera (malicioznog softvera) na globalnom nivou po procentu zastupljenosti u 2024. godini (prikaz je preuzet iz izveštaja kompanije *Check Point*), na osnovu koje se može primetiti da je došlo do značajnog porasta pokušaja napada pomoću tzv. *Infostealer* malvera i malvera koji se mogu koristiti u više namena (*multipurpose malware)* u odnosu na 2023. godinu. *Multipurpose* malveri (kao što su RAT-ovi, botneti i bankarski trojanci) često se koriste u ranim fazama napada za instalaciju dodatnih alata i omogućavanje veće kontrole napadača nad sistemima. Ova vrsta malvera je bila najzastupljenija tokom 2024. godine, sa zabeleženih 39% pogođenih organizacija, što je porast od 25% u odnosu na 2023. godinu.

Pokušaji zaražavanja *Infostealer* malverima povećani su za 58%, odnosno sa 12%, koliko je bilo pogođeno organizacija tokom 2023. godini, na 19% koliko ih je pogođeno u 2024. godini. Ovi napadi se često sprovode masovno, a ne ciljano, i ukazuju na rastuću potražnju za ukradenim podacima (nalozi, kolačići sesije, lični podaci). *Infostealer*-i se koriste za krađu finansijskih podataka i neovlašćeni pristup mreži kompanija.

Broj napada koji „preuzimaju“ resurse sa uređaja žrtve kako bi „rudarili“ kriptovalute (*Cryptominers*) je tokom 2024. godine znatno opao – sa 9% zabeleženih napada tokom 2023. godine, na 2%. Većina pomenutih malvera cilja *Monero* kriptovalutu, čija je težina rudarenja skoro udvostručena tokom godine, što znatno smanjuje isplativost takvih napada.

Slika 16.1. Procenat zastupljenosti različitih tipova malvera na globalnom nivou



2. Načini distribucije malvera

Kao inicijalni vektor napada, napadači su tokom 2024. godine u 68% slučajeva koristili elektronsku poštu kao metod za širenje malicioznih softvera, a u 32% slučajeva za distribuciju malvera korišćene su internet stranice.

Na slici 16.2. vidimo da je širenje malvera putem elektronske pošte bio trend koji se održao tokom prethodnih godina sa procentualnim porastom iz godine u godinu, međutim tokom prošle godine taj procenat je počeo drastično da opada, dok su malveri distribuirani putem internet stranica u porastu u odnosu na 2023. i to za 21%.

Slika 16.2. Uporedni prikaz broja napada koji za distribuciju koriste elektronsku poštu i internet stranice (za period 2021 - 2024. godina)

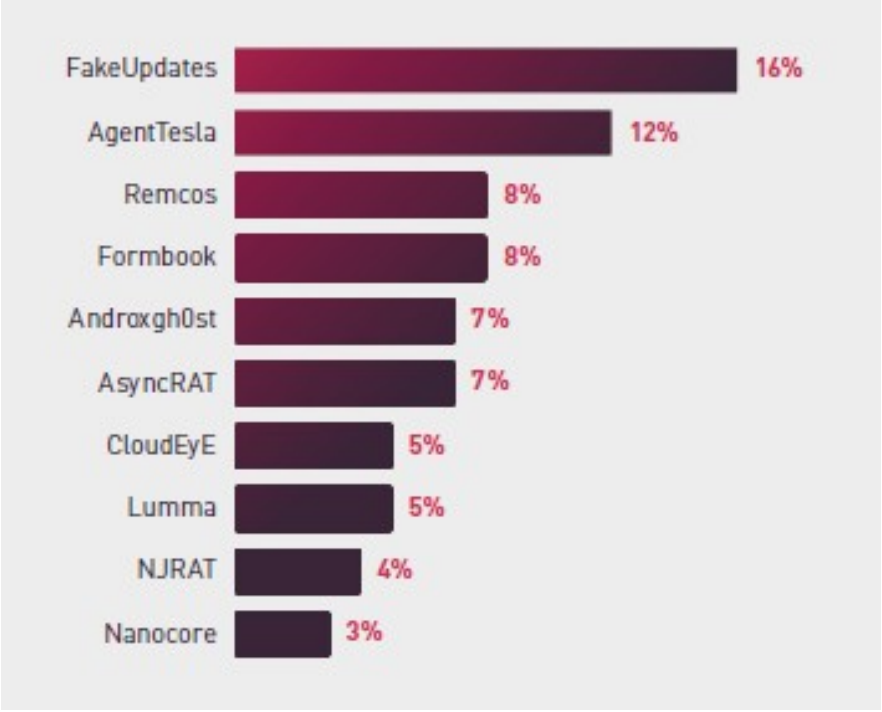
3. Statistika napada po različitim familijama malvera

Na slici 16.3. prikazane su familije malvera koje su najrasprostranjenije na globalnom nivou tokom 2024. godine.

Malver *FakeUpdates* je zadržao svoju poziciju na prvom mestu i tokom prethodne godine, sa čak 16% od ukupnog broja napada. Oslanja se na mrežu kompromitovanih internet stranica koje izgledaju kao stranice za preuzimanje ažuriranja pregledača ili nekog softvera. Lažni iskačući prozor navodi žrtvu da preuzme i pokrene program utemeljen na JavaScript-u, za navodno ažuriranje, dok žrtva zapravo preuzima zlonamerni softver odnosno malver.

AgentTesla sada već regularno od 2020. godine drži poziciju na samom vrhu liste najzastupljenijih familija malvera. Ovaj malver (*Infostealer*) ima za cilj krađu osetljivih podataka sa inficiranih sistema, poput kredencijala za logovanje sa internet pregledača (*browser*), kredencijala sa email klijenata i dr.

Slika 16.3. Zastupljenost malvera na globalnom nivou

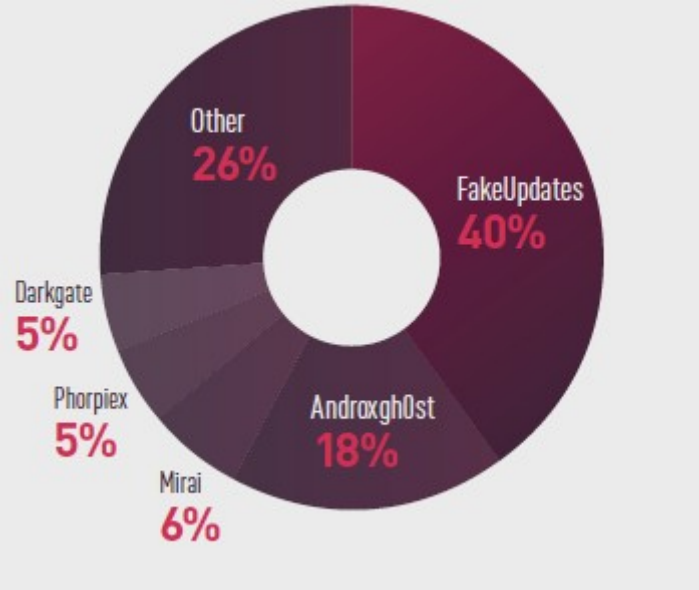


4. **Statistika napada po različitim familijama višenamenskih malvera (*multipurpose malware*)**

Najzastupljeniji napadi u 2024. godini su oni napadi koji koriste višenamenske malvere kao inicijalni vektor za dobijanje pristupa sistemu. Kod ovih napada (slika 16.4) najčešće su korišćeni malveri *FakeUpdates* (40%), *AndroxghOst* (18%), *Mirai* (6%), *Phorpiex* (5%), *Darkgate* (5%), i drugi malveri (26%).

Botnets odnosno botneti (mreža zaraženih uređaja) već tradicionalno igraju centralnu ulogu kod načina distribucije malvera. Njihovo razbijanje dovelo je do značajnih promena u vidu povećane upotrebe *Infostealer-a* (programa za krađu podataka), koji su često decentralizovani i korišćeni među sajber napadačima.

Slika 16.4. Procenat zastupljenosti različitih familija višenamenskih malvera (*multipurpose malware*) na globalnom nivou

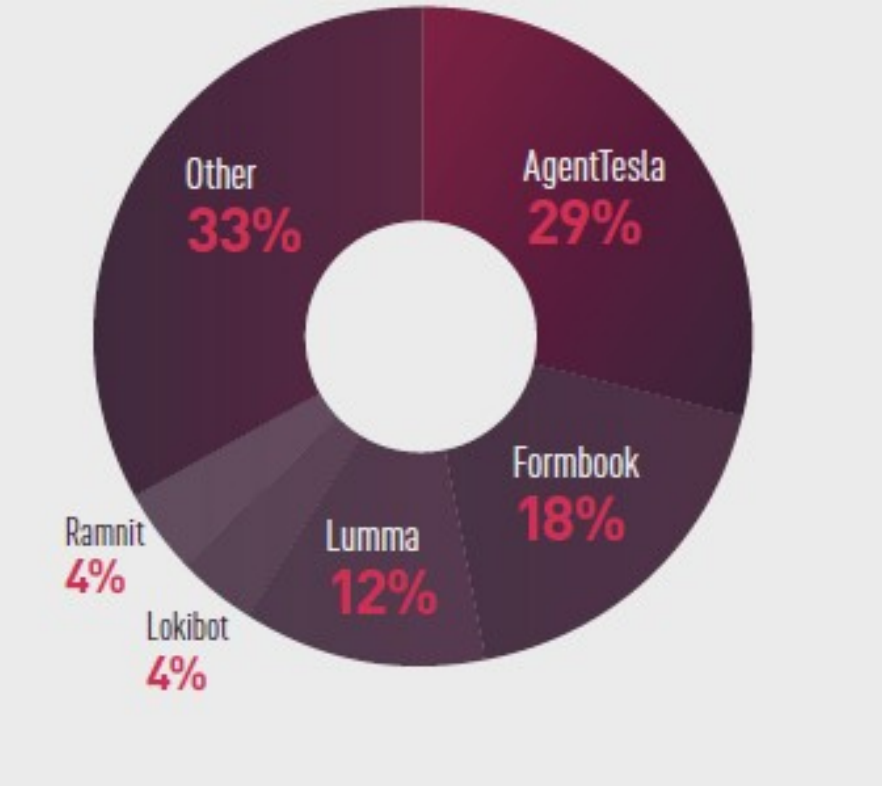


5. **Statistika napada po različitim familijama malvera za krađu korisničkih podataka**

Familijom malvera za krađu korisničkih podataka dominira nekoliko tipova, kao što je prikazano na slici 16.5, od kojih najviša mesta zauzimaju *AgentTesla* (29%), *Formbook* (18%) i *Lumma* (12%). Uprkos odsustvu značajnih novih pretnji, zabeležen je porast od 58% u pokušajima zaražavanja malverima za krađu korisničkih podataka, u odnosu na prethodnu godinu, iz čega se zaključuje da *infostealer* malveri igraju sve ključniju ulogu u sajber prostoru.

Styx Stealer, je novi malver za krađu korisničkih podataka, koji je kreiran da prikupi osetljive informacije poput lozinki, kolačića, *autofill* podataka sa različitih pregledača, podatke o sesijama sa platformi za razmenu poruka i drugo. Pored ovih podataka, prikuplja i sistemske podatke kao što su hardverske specifikacije i spoljašnje IP adrese, i može snimati ekran u cilju procene okruženja za dalje napade.

Slika 16.5. Statistika napada po različitim familijama malvera za krađu korisničkih podataka

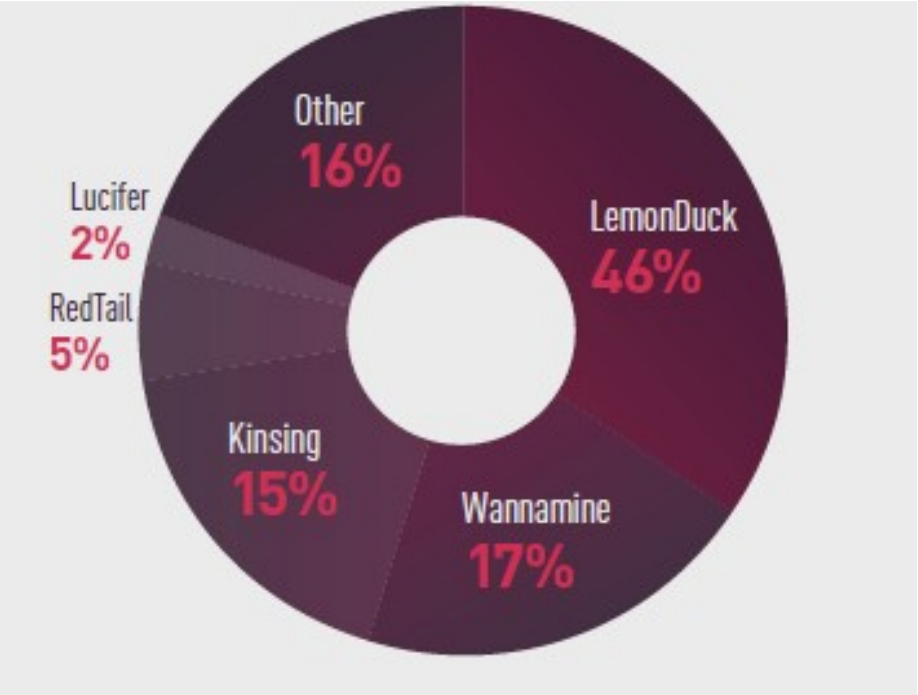


6. Statistika napada po različitim familijama malvera za krađu kriptovaluta

Pad rudarenja kriptovalutama se nastavlja i tokom 2024. godine, i to na samo 2% pogođenih globalnih korporacija malverima za krađu kriptovalutama, dok je taj procenat bio znatno veći, i to 9% u 2023. godini i 16% tokom 2022. godine.

U 2024. godini, *LemonDuck* je ostao jedan od najrasprostranjenijih malvera za kripto rudarenje i korišćen je u 46% slučajeva od ukupnog broja pokušaja ovakvih vidova napada (slika 16.6). Ovu familiju malvera korišćenu za kripto rudarenje, prvobitno otkrivenu 2018. godine, je veoma teško detektovati, imajući u vidu svoju sofisticiranost. Za *LemonDuck* kampanje upotrebljavaju se različiti ulazni vektori napada, uključujući fišing poruke sa malicioznim prilozima, *brute-force* napadima usmerenim na *RDP* i *SSH*, zaražene *USB* uređaje i druge tehnike infiltracije.

Slika 16.6. Statistika napada po različitim familijama malvera za krađu kriptovaluta



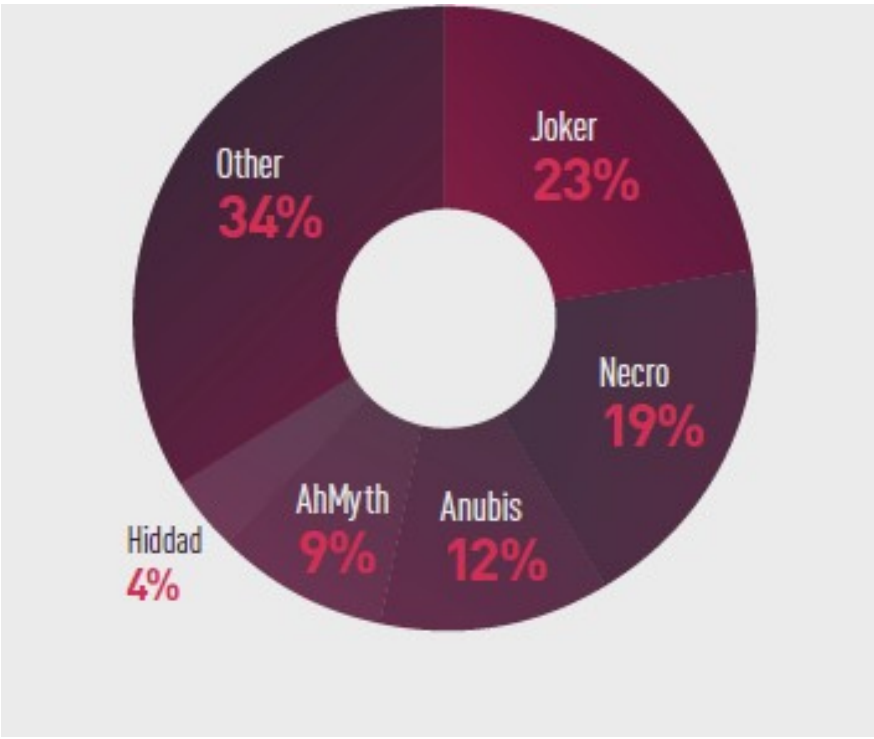
7. Statistika napada na mobilne uređaje po različitim familijama malvera

Čak 60% internet saobraćaja poticalo je sa mobilnih uređaja tokom 2024. godine, zbog čega su često na meti upravo ovi tipovi uređaja na kojima se nalaze osetljivi podaci, a putem kojih sajber napadači mogu ostvariti finansijsku dobit, kao i strane države putem špijunaže i prikupljanja obaveštajnih podataka.

Najzastupljeniji tip malvera na mobilnim uređajima tokom 2024. godine, bio je *Joker* sa 23% od ukupnog broja napada na ove tipove uređaja (slika 16.7), što ga je popelo sa petog mesta u odnosu na 2023. godinu. Primarni cilj *Joker* malvera je da neprimetno pretplati korisnike na premijum usluge simuliranjem klikova korisnika i presretanjem SMS poruka i notifikacija.

Malver *Necro* je tokom prethodne godine dospeo među tri najzastupljenija mobilna malvera (19%), a kreiran je da preuzima i izvršava dodatne zlonamerne radnje u aplikacijama. Nedavno je ovaj malver distrubuiran putem dve zaražene aplikacije na *GooglePlay* prodavnici, a koje su preuzete preko 11 miliona puta. Osim u prodavnici, *Necro* je identifikovan i u popularnim aplikacijama poput *WhatsApp, Minecraft* i drugih.

Slika 16.7. Statistika napada na mobilne uređaje po različitim familijama malvera



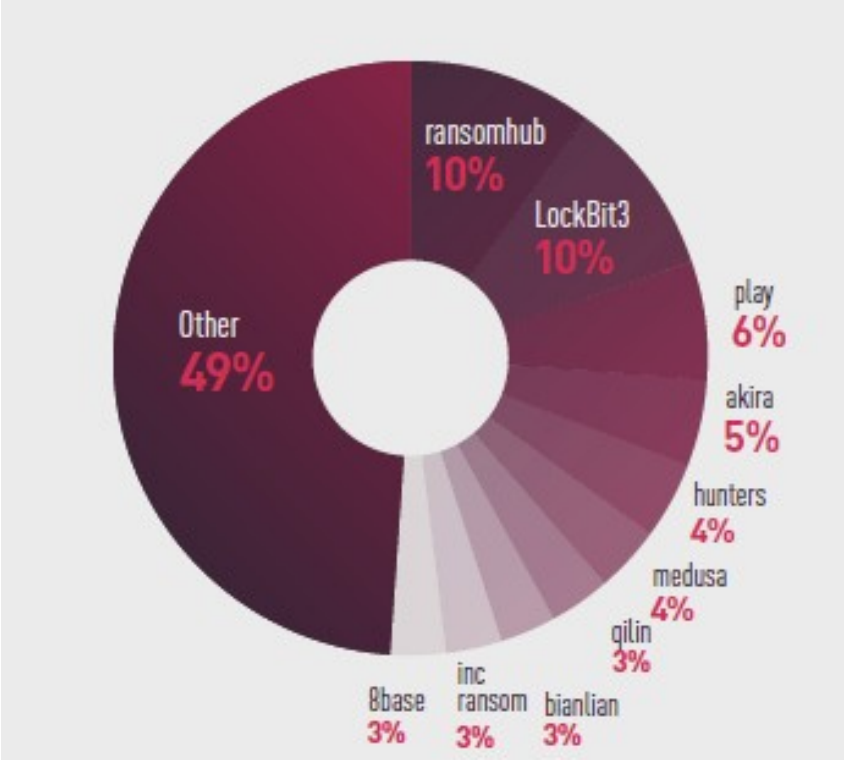
8. Statistika napada iznuđivačkim softverima – ransomver

Dve najdominantnije ransomver grupe u 2023. godini su postale neaktivne tokom prošle godine – *LockBit* koji je bio odgovoran za 21% žrtava i *ALPHV* koji je imao 9% su ili prestale sa aktivnostima ili su značajno smanjile broj žrtava. Pad ovih ransomver grupa tokom 2024. godine pripisuje se, većinom, operacijama od strane zakonodavnih vlasti. Iako *LockBit* deluje kao drugi najproduktivniji ransomver akter (slika 16.8), većina njegovih napada se desila u prvoj polovini 2024. godine, dok je poslednjih meseci bilo veoma malo prijavljenih žrtava.

Tokom prošle godine došlo je do veće podele među ransomver grupama, s obzirom da sada brojne manje grupe čine veći udeo u ukupnom broju žrtava na godišnjem nivou. To je dovelo do toga da su deset najaktivnijih grupa odgovornih za više od 66% svih objavljenih žrtava u 2023. godini, opale na samo 51% u 2024. godini.

Na osnovu globalne analize napada po sektorima, rezultati pokazuju da su najčešće ciljani sektori obrazovanja, državnih organa i zdravstva. Međutim, kada se posmatra posebno iznuda novca, proizvodnja se izdvaja kao sektor koji je najčešće pogođen ovim tipom malvera. Ova razlika se verovatno odražava u pogledu spremnosti da se otkupnina plati, s obzirom da državni i sektori obrazovanja obično u manjem procentu ispune zahteve za otkupninom, što ih onda i čini manje privlačnim sektorima za ransomver napade.

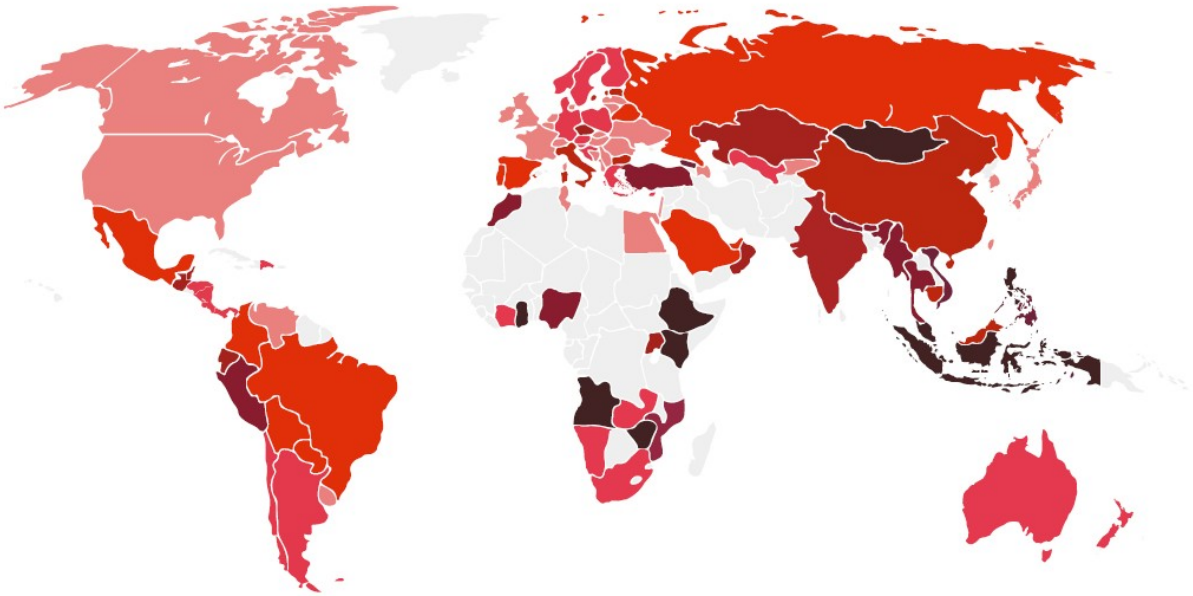
Slika 16.8. Statistika napada softverima sa dvostrukom iznudom po različitim familijama



9. Check Point Global Threat indeks

Na Slici 16.9. je dat grafički prikaz vrednosti *Check Point Global Threat* indeksa po državama u 2024. 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 16.9. Grafički prikaz *Check Point Threat* indeksa po državama

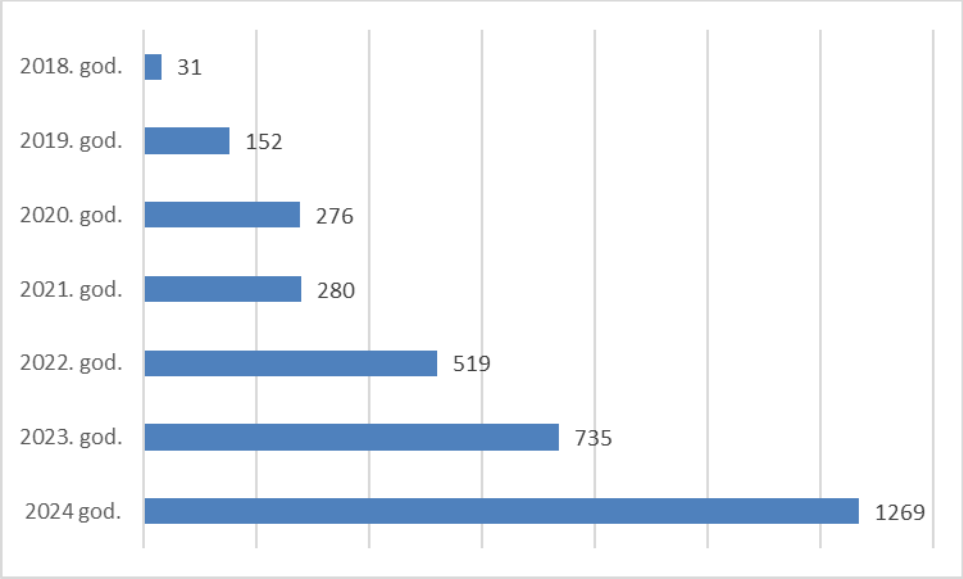


Stanje informacione bezbednosti u Srbiji

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.

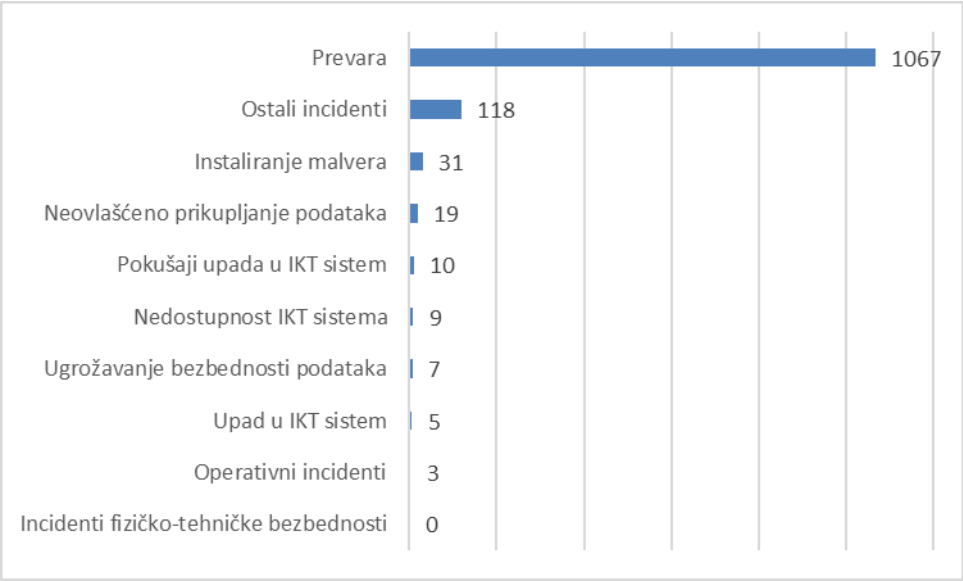
Iz godine u godinu beleži se kontinuirani rast prijava incidenata Nacionalnom CERT-u, a taj trend je posebno izražen poslednjih godina (Slika 16.10). Ovo povećanje ne samo da odražava sve veću učestalost pretnji, već i snažan razvoj svesti o značaju deljenja informacija i oslanjanja na stručne preporuke Nacionalnog CERT-a.

Slika 16.10. Broj prijava Nacionalnom CERT-u od 2018. godine do 2024. godine



U 2024. godini, Nacionalnom CERT-u je prijavljeno 1269 incidenta, što predstavlja značajno povećanje u odnosu na prethodne godine.

Slika 16.11. Prijavljeni incidenti u 2024. godini prema grupi incidenata



Na slici 16.11. 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.

U 2024. godini nastavile su se fišing kampanje usmerene na korisnike poštanskih usluga. Građanima su stizale lažne poruke u kojima su se napadači predstavljali kao Pošta Srbije, tražeći da ažuriraju određene podatke kako bi im paket bio isporučen. Ove poruke su sadržale linkove ka lažnim veb-stranicama, a unošenjem traženih podataka građani su bili izloženi riziku krađe ličnih informacija i finansijskog gubitka. Nacionalni CERT je upozoravao građane da budu oprezni, da ne otvaraju sumnjive linkove i ne dele svoje podatke nepoznatim licima, ističući da Pošta Srbije ne traži takve informacije putem SMS poruka.

Pored fišing napada, zabeležen je i porast investicionih prevara, u kojima se građanima obećavala brza i laka zarada ulaganjem u akcije ili kriptovalute. Koristeći sofisticirane metode manipulacije, napadači su nastojali da navedu ljude na nepromišljene finansijske odluke, što je prevarene građane dovelo do značajnih gubitaka.

Slika 16.12. Trend i promene u rangiranju prijavljenih sajber incidenata u 2024. godini u odnosu na 2023.

Grupe	Trend u 2024. u odnosu na 2023. godinu	Promene u rangiranju u odnosu na 2023. godinu
1. Prevara	↑	→
2. Ostali incidenti	↑	→
3. Instaliranje malvera	↓	→
4. Neovlašćeno prikupljanje podataka	↑	↑
5. Pokušaji upada u IKT sistem	↓	↑
6. Nedostupnost IKT sistema	↓	↑
7. Ugrožavanje bezbednosti podataka	↑	↑
8. Upad u IKT sistem	↓	↓
9. Operativni incidenti	↓	↓
10. Incidenti fizičko-tehničke bezbednosti	↓	→

TREND: ↓ Broj prijava u opadanju, → Broj prijava bez promene, ↑ Broj prijava u porastu

Na slici 16.12. prikazani su trendovi i promene u rangiranju prijavljenih sajber incidenata u 2024. godini u odnosu na 2023.

Broj prijavljenih prevara značajno je porastao, gotovo dvostruko u odnosu na prethodnu godinu, ali se njihova pozicija u rangiranju nije promenila, te i dalje zauzimaju prvo mesto.

Ostali incidenti takođe beleže rast broja prijava i zadržavaju drugu poziciju.

Iako je broj prijava instalacije malvera gotovo prepolovljen u odnosu na prošlu godinu, ova grupa incidenata se i dalje nalazi na trećem mestu.

Porast broja prijava neovlašćenog prikupljanja podataka doveo je do promene u rangiranju, pa se ova kategorija sada nalazi na četvrtoj poziciji.

Pokušaji upada u IKT sistem, kao i prijave nedostupnosti IKT sistema, uprkos opadajućem trendu, pomerili su se na peto i šesto mesto.

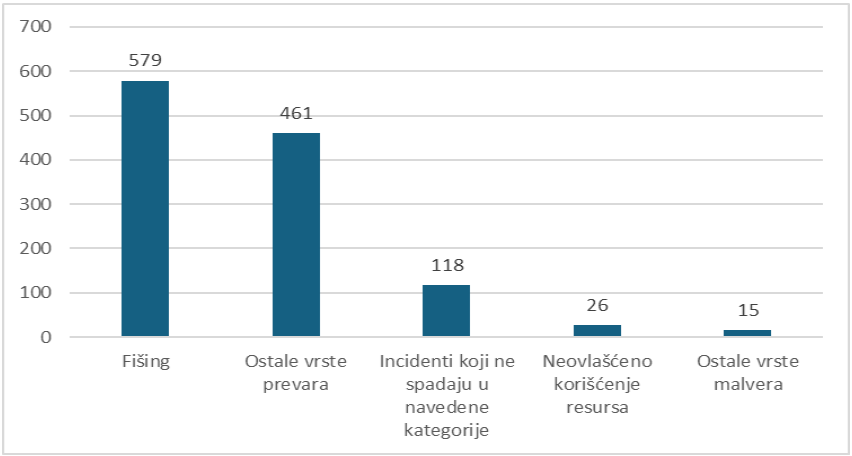
Zabeležen je porast incidenata koji se odnose na ugrožavanje bezbednosti podataka, što ih u ovoj godini svrstava na sedmu poziciju.

Upad u IKT sistem i operativni incidenti su prijavljeni u manjem broju nego prethodne godine, a njihov rang se takođe smanjio.

Konačno, broj prijava u vezi sa incidentima fizičko-tehničke bezbednosti ostao je na istom nivou, pa ova kategorija i dalje zauzima deseto mesto.

Najčešće prijavljivani incidenti, prema vrsti incidenta, bili su: fišing (46%), ostale vrste prevara (36%), incidenti koji ne spadaju u gore navedene kategorije (9%), neovlašćeno korišćenje resursa (2%) i ostale vrste malvera (1%).

Slika 16.13. Pet najčešće prijavljivanih incidenata u 2024. godini



Fišing napadi su tokom 2024. godine bili među najčešće prijavljivanim incidentima u oblasti informacione bezbednosti. Ove prevare se sprovode putem e-pošte, društvenih mreža, telefonskih poziva ili SMS poruka, u kojima napadači traže od korisnika da posete određeni link ili preuzmu prilog. Korišćenjem tehnika socijalnog inženjeringa, napadači se predstavljaju kao poznate osobe ili ugledne institucije, kako bi žrtve obmanuli i naveli ih da otkriju poverljive podatke ili instaliraju zlonamerni softver.

Fišing često vodi do ozbiljnih posledica poput krađe identiteta, neovlašćenog pristupa finansijskim sredstvima, instalacije malicioznih programa, kreiranja bot mreža i sajber špijunaže. Tokom 2024. godine, Nacionalni CERT je primio 579 prijava fišing napada, a najveći broj ovih kampanja bio je usmeren ka korisnicima poštanskih usluga i platformi za elektronsku trgovinu.

Nacionalni CERT je tokom prošle godine evidentirao 461 prijavu o ostalim vrstama prevara, pri čemu veliki deo ovih slučajeva uključuje neovlašćeno preuzimanje novčanih sredstava sa računa građana. Ovaj broj ukazuje na značajan problem, s obzirom na učestalost ovakvih incidenata, te su oštećena lica upućena da ove incidente prijave i institucijama nadležnim za pitanja visokotehnološkog kriminala.

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 ili pogrešne ispruke robe kupljene preko interneta, a takvih prijava je bilo 118.

Neovlašćeno korišćenje resursa je vrsta incidenta koja se javlja u grupi prevara, a broj prijava u 2024. godini bio je 26.

Malver (engl. malware, skraćeno od malicious software) označava svaki softver razvijen s ciljem da nanese štetu računarskim sistemima ili mrežama. Ova kategorija obuhvata različite vrste zlonamernih programa, uključujući računarske viruse, crve, ransomver, trojanske programe, špijunski softver i rutkit. Nacionalnom CERT-u je prijavljeno 15 slučajeva koji su se odnosili na maliciozne programe, ali zbog nedostatka informacija nije bilo moguće precizno ih klasifikovati u neku od pomenutih kategorija.

Krivična dela protiv bezbednosti računarskih podataka

Tokom 2024. godine u Posebnom tužilaštvu za visokotehnološki kriminal formirano je ukupno 7.198 predmeta i to:

- 529 predmeta protiv poznatih punoletnih učinilaca,

- 3.888 predmeta protiv nepoznatih učinilaca i

- 2.781 predmeta u vezi sa raznim krivičnim događajima.

Broj formiranih predmeta povećan je za 10,31% u odnosu na 2023. godinu, kada je bilo formirano 6.456 predmeta.

Sledeći podaci se odnose isključivo na krivične prijave podnete protiv poznatih punoletnih učinilaca krivičnih dela tokom 2024. godine i preduzete radnje Posebnog javnog tužilaštva za visokotehnološki kriminal u tom periodu. Podaci se odnose na broj lica, a ne na broj predmeta ili procesnih radnji.

- Broj prijavljenih lica – 682
- Broj lica protiv kojih su podneti zahtevi za prikupljanje potrebnih obaveštenja – 118
- Broj lica protiv kojih je doneta naredba o sprovođenju istrage - 10
- Broj lica protiv kojih su sprovedene dokazne radnje – 214
- Broj lica protiv kojih su podneti optužni predlozi – 93
- Broj lica protiv kojih su podignute optužnice - 8
- Broj zaključenih sporazuma o priznanju krivičnog dela – 39