# Ransomver kao model pružanja usluga

(Ransomware-as-a-Service)

СРБ-ЦЕРТ

Ransomver predstavlja jednu od najzastupljenijih internet pretnji. Statistički podaci Evropske agencije za mrežnu i informacionu bezbednost *(ENISA)** ukazuju da je tokom 2022. godine zabeležen pad broja iznuđenih plaćanja žrtava ransomver napada, dok se u 2023. godini ponovo beleži njihov porast, baš kao i porast broja naplaćenih iznuda. Uzrok porasta je uvođenje tzv. "Duple iznude" kao dodatnog oblika iznuđivanja. Ukoliko uzmemo u obzir i činjenicu prisustva veštačke inteligencije i mogućnosti njene zloupotrebe, to nam jasno može ukazati da će ransomver napad i dalje biti u samom vrhu liste najzastupljenijih sajber napada i da je primena preventivnih mera jedna od najboljih metoda zaštite od ransomver napada

Ransomver (eng. *Ransomware*), je tip malvera (maliciozni programski kod) koji je usmeren na neovlašćeno pristupanje informacionim sistemima ili uređaju, sa zadatkom da korisniku limitira pristup, ili da zaključa određene fajlove i datoteke i na taj način u potpunosti onemogući pristup napadnutom informacionom sistemu ili uređaju. Krajnji cilj napadača je protivpravno sticanje imovinske koristi, ali može biti zloupotrebljen i za ostvarivanje političkih, odnosno haktivističkih ciljeva. Nakon neovlašćenog pristupa i zaključavanja fajlova ili datoteka, napadači šalju poruku koja se pojavljuje na monitoru žrtve koja sadrži instrukcije za otkup dekripcionih ključeva (programski kod za otključavanje), koji bi žrtvi trebalo da omogući ponovni pristup inficiranim fajlovima ili datotekama.

Tokom svog razvoja, ransomver je predstavljao tip sajber napada koji je, pre svega, bio usmeren na fizička lica, odnosno pojedince. Razlog tome je bio nizak nivo sajber kulture pojedinca, koja se najpre ogledala u kreiranju samo jedne i često jednostavne lozinke za pristup internet nalozima, kao i neadekvatna zaštita uređaja u vidu odsustva licenciranih antivirusnih softvera. Maliciozni programski kod za otključavanje enkriptovanih fajlova i datoteka je često bio lošeg kvaliteta i nije otključavao sve inficirane datoteke. Sa druge strane čest problem je predstavljala i nemogućnost brze realizacije iznude zahtevane sume novca. To su bila dva osnovna  izazova sa kojima su se suočavale žrtve, ali i napadači prilikom korišćenja ransomvera.

Sa unapređenjem malicioznog programskog koda, rastao je i nivo sofisticiranosti napada, što je hakerima omogućilo da usmere svoje napade na mala i srednja preduzeća, a zatim i na veće i bolje zaštićene sisteme. Onemogućavanje rada velikih sistema predstavlja veliki izazov kako za konkretno pravno lice, tako i za sve one koji koriste usluge ili proizvode napadnute organizacije. .

Organizovanje sajber napada na pravna lica je napadačima omogućilo i veću zaradu, što je kasnije vodilo ka organizovanju većeg broja hakera u „korporativni model poslovanja", kao i razvoja RaaS (*Ransomware-as-a-Service*) usluga.

*RaaS* usluge zapravo predstavljaju novi biznis model dizajniran od strane većih i ozbiljnijih hakerskih grupa koje kreiraju određeni tip ransomvera i nude ga na prodaju zainteresovanim kupcima, bilo da je reč o drugim hakerskim grupama, bilo da govorimo o potencijalnim kupcima koji nemaju tehnička znanja, ali iz određenih interesa žele da pokrenu ransomver napad na neki informacioni sistem.

* https://www.enisa.europa.eu/publications/enisa-threat-landscape-²0²³

Hakerske grupe svoje *RaaS* usluge najčešće nude zainteresovanim kupcima putem reklama na *Dark Web*-u. Kupac se može odlučiti za različiti „paket usluga" koje su dostupne u odgovarajućem cenovnom rangu - od jednokratne usluge, pa sve do mesečnih ili drugih odgovarajućih modela „pretplate".

U produžetku se nalazi kratak opis osnovnih deset koraka za izvršavanje Ransomver napada:

1. analiza i odabir potencijalne žrtve,
2. analiza odbrambenih kapaciteta informacionog sistema žrtve,
3. ukoliko žrtva ima kvalitetnu zaštitu sistema, pristupa se analizi odbrambenih kapaciteta informacionog sistema povezanih kompanija sa kojima žrtva ima ostvarenu poslovnu saradnju, kako bi se upalo preko tih sistema koji imaju slabiju odbranu,
4. upad u sistem žrtve (najčešće to može biti pomoću fišinga, kompromitacije poslovne korespondencije – *BEC*, iskorišćavanja ranjivosti sistema koji nije ažuriran, ili RDP pristupa) koji napadačima omogućava pristup informacionom sistemu žrtve,
5. kopiranje podataka iz sistema žrtve na sistem napadača za potrebe „Duple iznude",
6. analiza poslovnih procesa i podataka na osnovu preuzetih informacija iz sistema žrtve,
7. aktiviranje odgovarajućeg ransomver programskog koda koji zaključava datoteke na informacionom sistemu žrtve,
8. zahtevanje otkupa dekripcionih ključeva u kripto valuti,
9. pretnja javnim objavljivanjem prekopiranih poslovnih i ličnih podataka putem medija („Dupla iznuda"),
10. dostavljanje dekripcionih ključeva (u slučajevima kada žrtva plati iznuđenu sumu novca).

Vođeni „korporativnim modelom poslovanja" hakerske grupe se danas uglavnom organizuju i rade u timovima. Jedna grupa radi analizu finansijskih i poslovnih podataka prilikom odabira žrtve, dok drugi timovi mogu raditi na analizi povezanih kompanija u nameri da zloupotrebom resursa povezane kompanije omoguće napadačima lakši pristup sistemu krajnje žrtve ransomver napada.

Za potrebe napada, hakeri se najčešće odlučuju za finišg napad, kao ulazni vektor, ali to može biti i iskorišćavanje neke od ranjivosti informacionog sistema žrtve, kao i zloupotreba RDP (*Remote Desktop Protocol*) pristupa sistemu.

Nakon upada u sistem žrtve, hakeri rade detaljnu analizu poslovnih procesa i podataka, kako bi na osnovu te analize mogli da organizuju napad i definišu koji je realni iznos otkupa koji mogu zahtevati od žrtve. U ovom koraku hakeri takođe preuzimaju određenu količinu podataka iz informacionog sistema žrtve i kopiraju ih na svoje sisteme. Tako prikupljeni podaci im služe za kasniju pretnju kojom žele dodatno da prisile žrtvu da plati iznos otkupa. Ukoliko bi žrtva odbila plaćanje otkupa, napadači bi zapretili objavljivanjem prikupljenih poslovnih i ličnih podataka celokupnoj javnosti, putem medija, što predstavlja tzv. „Duplu iznudu".

Preporuka Nacionalnog CERT-a Republike Srbije je da se otkupni iznos ne plaća, jer se na taj način finansira kriminalno delovanje hakerskih grupa, pri čemu nema nikakvih garancija da će žrtva dobiti

dekripcione ključeve, ili da će dobijeni ključevi u potpunosti omogućiti pristup i korišćenje podataka koji su bili zaključani ransomverom tokom napada. Sa druge strane, ukoliko se plati otkupni iznos, hakerske grupe se često opredeljuju da i u budućnosti ponove napad na istu organizaciju ili kompaniju, bez obzira na poruku da će, ukoliko im se prvi put uplati traženi iznos, zauvek nestati iz sistema te žrtve i neće se više vraćati.

Posledice ransomver napada mogu imati veoma negativan uticaj na poslovanje, profit, ali i reputaciju organizacije ili kompanije, zbog čega je značaj primene preventivnih mera zaštite u interesu svih zaposlenih u jednoj organizaciji ili kompaniji, kao i povezanih poslovnih partnera sa kojima je ostvarena dobra saradnja. Takođe, značaj primene preventivnih mera se može odnositi i na sve korisnike kojima se nude usluge određene organizacije ili kompanije.

Preventivne mere, koje se mogu preduzeti u cilju zaštite od ransomver napada, su:

1. redovno ažuriranje operativnih i aplikativnih softvera, kako bi bile primenjene sve dostupne zakrpe za otkrivene ranjivosti,
2. segmentiranje mreže kojim se jedna velika mreža pretvori u skup manjih delova mreže, čime se onemogućava brzo potencijalno širenje malvera po celokupnoj mreži,
3. instalacija licenciranog programa za zaštitu računara od virusa i malvera,
4. redovno kreiranje rezervnih kopija svih važnih datoteka i fajlova,
5. redovno testiranje rezervnih kopija,
6. uvođenje i primena multifaktorske autentifikacije kao dodatnog sloja zaštite,
7. kontrola pristupa informacionom sistemu sa udaljenih lokacija,
8. kontinuiran rad na podizanju svesti zaposlenih o bezbednosnim pretnjama, koji se najpre ogleda u:
    - kreiranju kompleksnih lozinki,
    - primena principa: jedan nalog – jedna lozinka
    - korišćenju službenih imejl naloga isključivo u korporativne svrhe,
    - izbegavanju klika na link ili otvaranje priloga u imejlu koji stigne od nepoznatog pošiljaoca, jer se fišing često koristi kao ulazni vektor za ransomver napade,
    - čuvanju ličnih ili finansijskih podataka, odnosno da ih ne treba deliti putem: imejla, SMS ili čet poruka, telefonskog poziva ili u direktnom razgovoru sa nepoznatim osobama,
    - proveri domena internet stranica koje se posećuju, imajući u vidu da se na internetu nalazi veliki broj kompromitovanih internet stranica putem kojih se šire maliciozni sadržaji.

Ostale mere prevencije, prevashodno usmerene na poslovne korisnike, možete pogledati u našoj publikaciji „Preporuke za zaštitu od ransomver napada”.