RANSOMWARE
2023

Šta je ransomware, njegov uspon i povecanje ransomware-a kroz godine, različiti tipovi i svest o ransomware-u

Šta je ransomware

Ransomware je vrsta zlonamernog softvera koji šifruje i zaključava fajlove na računaru ili mreži žrtve i zahteva plaćanje u zamenu za ključ za dešifrovanje. To je poslednjih godina postala značajna i rastuća pretnja.

> **Ransomware je više o manipulisanju ranjivostima u ljudskoj psihologiji nego o tehnološkoj sofisticiranosti protivnika**
> – ***Džejms Skot, Institut za tehnologiju kritične infrastrukture***

Rast ransomware napada kroz godine[1]

2018	2019	2020	2021	2022
75% 206,4 miliona prijavljenih ransomware napada	41% 187,9 miliona prijavljenih ransomware napada	150% 304,2 miliona prijavljenih ransomware napada	78% 623,2% miliona prijavljenih ransomware napada	71% 493,33 miliona prijavljenih ransomware napada

---

[1] AAG IT Services

Različiti tipovi ransomware-a

Napad **WannaCry** ransomwarea 2017. godine pogodio je preko 300.000 računara i naneo značajnu finansijsku štetu.

Procenjuje se da je napad **Petya/NotPetya** u istoj godini prouzrokovao štetu od 10 milijardi dolara.

Locky ransomware je zabeležio porast od 141% u 2016. godini, dok je **CryptoLocker** prouzrokovao tri miliona dolara plaćenih iznuda u 2013.

Noviji tipovi ransomwarea kao što su **Ryuk (700% 2018. godine)**, **Maze (700% 2019. godine)** i **Sodinokibi (820% 2020. godine)** zabeležili su značajan porast u poslednjih nekoliko godina.

Najveći deo ransomeware napada u 2021. i 2022. realizovan je putem tri tipa napada - **Kontijem (19%)**, **Avadonom (16%)** i **Doppelpaymer (14%)**

Zanimljivost

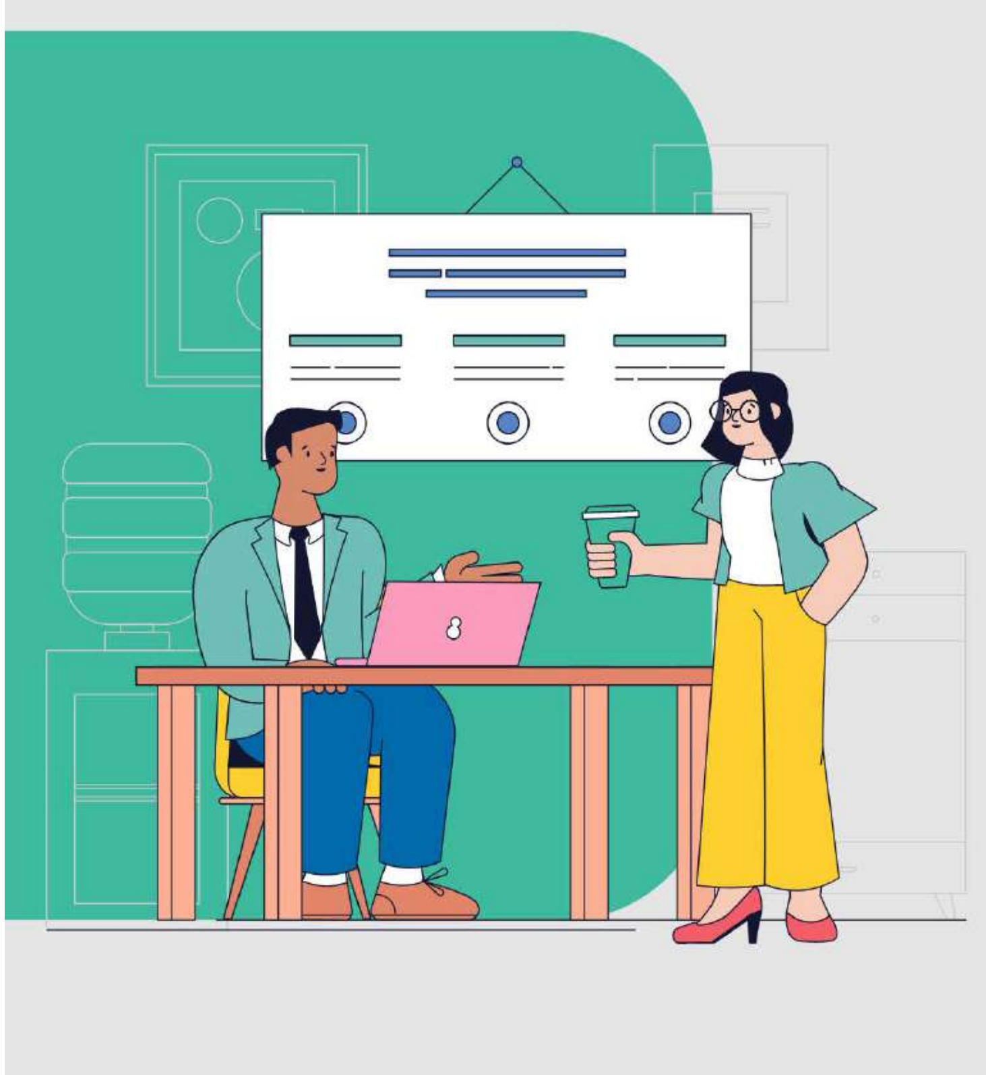
FBI preporučuje žrtvama ransomware napada da ne plaćaju otkupninu, jer ne postoji garancija da će napadač zaista obezbediti ključ za dešifrovanje i plaćanje otkupnine samo podstiče više napada.

Svest o ransomware-u

Saznanja

Svest o ransomwareu je nivo znanja i razumevanja koje pojedinac ili organizacija ima o rizicima i uticaju ransomware napada. To uključuje saznanja o tome kako dolazi do ransomware napada, o različitim tipovima ransomware-a i kako sprečiti i odgovoriti na ove napade.Ovo takođe podrazumeva da se shvati značaj redovnog pravljenja rezervnih kopija važnih datoteka, ali i identifikacija najčešćih taktika koje koriste napadači

- Ako dođe do napada ransomware-a, važno je imati plan reagovanja, uključujući korake za prijavljivanje incidenta, sanaciju štete i vraćanje sistema i podataka.
- Prevencija je ključna za izbegavanje ransomware napada i podrazumeva mere kao što su držanje softvera i bezbednosnih sistema ažurnim, korišćenje jakih lozinki i edukacija korisnika.
- Ransomware napadi mogu da se realizuju na različite načine - putem e maila, ranjivosti softvera ili preuzimanja zaraženih fajlova.
- Ransomware napadači često koriste taktiku socijalnog inženjeringa kako bi prevarili žrtve da preuzmu ili otvore zaražene fajlove.
- Postoje različiti tipovi ransomware-a, uključujući screen lockers, enkripcioni ransomware i doxware.



Trendovi i dešavanja

Svest o trendu rasta i razvoju, usavršavanju ransomware napada je važan aspekat odbrane od istih. To uključuje praćenje novih pretnji, kao i razumevanje taktika, tehnika i procedura koje koriste napadači da izvršavaju ransomware napade. Ostajući svesni trenutnih trendova i razvoja, pojedinci i organizacije mogu bolje da se pripreme da spreče i ublaže uticaj napada ransomvera.

Svest menadžmenta

Svest menadžmenta o ransomware napadima je izuzetno važna jer ukoliko donosioci odluka razumeju kakav uticaj takav napad ima na poslovanje, biće spremniji da ulažu u mere zaštite, da se takvi napadi spreče i ublaže.

Ovo uključuje:

1. Razumevanje rizika
2. Ulaganje u sajber bezbednost
3. Izradu planova reagovanja na incidente
4. Redovno testiranje i ažuriranje mera bezbednosti

Davanjem prioriteta **menadžmentu** svesti o ransomware-u, organizacije mogu bolje da se zaštite od napada ransomvera i minimiziraju uticaj od bilo kojih napada.

Zaključak

Napadi ransomvera su u porastu i postali su značajna pretnja pojedincima i organizacijama širom sveta.

Napadi ransomvera mogu imati ozbiljne posledice, uključujući finansijske gubitke, krađu podataka i narušenu reputaciju organizacije.

Od suštinske je važnosti da ostanete oprezni i proaktivni u suočavanju sa sve većim okruženjem pretnji ransomvera.

Vojin Ninčić
386/22
EMAIL
vojin.nincich@gmail.com

Katarina Štetić
192/22
EMAIL
katarina.stetic6@gmail.com

Zašt!tise