RANSOMWARE

Digitalna ucena

i vaše poslovanje suočeno sa ovom vrstom malvera...

www.uridium.rs

Sadržaj

DIGITALNA UCENA

Nazovimo ga onim što i jeste:

Ransomware predstavlja digitalni mehanizam iznude.

Najčešći je slučaj da ransomware pri napadu šfrira (enkriptuje) podatke žrtve i **pre nego što je poslata ucena**.

Mnoge žrtve odlučuju da plate otkupninu iz razloga velike vrednosti podataka. Međutim, nije preporučljivo plaćati otkup, iz samog razloga nepouzdanosti.

Možete platiti i na kraju ostati praznih ruku, ili Vam, što je mnogo gori scenario, mogu tražiti još veći otkup. Moderni kripto malveri koriste enkripciju koja je do sad bila nemoguća za dešifrovanje, tako da jedino što preostaje žrtvi napada moguće, jeste da bira između plaćanja iznude ili potpunog gubitka podataka.

Opet napominjemo da ni plaćanje ne donosi nikakvu garanciju, da ćete dobiti pristup podacima.

U daljem tekstu će biti reči o najčešćim **ransomware scenarijima**, kao i trendovima u ovom vidu sajberkriminala kao i preporukama i savetima koji će pomoći Vašoj firmi da ne dođe u ulogu žrtve sajberkriminala.

Gubitak pristupa značajnim podacima, bilo da su u pitanju fotografije ili poslovna dokumenta, je nešto za šta ne bi biste nikome poželeli da iskusi. Ali u slučaju da do najgoreg dođe, i vaš računar postane zaražen sa Kriptolokerom ili nekom drugom vrstom ransomware-a, šta je to što biste trebali da preduzmete?

Da li će hakeri ispoštovati dogovor i dekriptovati podatke, nakon što im uplatite određenu sumu novca?

Vaše opcije prilikom ransomware prevara

Nedavno nam se obratio klijent sa problemom napada ransomware-a na server firme. Usled napada im je zaključan pristup celokupnim podacima firme koji obuhvataju vremenski okvir od par godina. Klijent nije imao **nikakav bekap na eksternoj lokaciji ili cloud-u**, već samo na samom serveru, što predstavlja veliku nebezbednost po podatke. **Ili je potrebno server koristiti samo kao server, ili imati još jedan vid bekapa za svaki slučaj**.

Pretpostavimo situaciju da se dogodio napad ransomware-a na isti ovaj računar, ali da su imali i back up podataka u cloud-u, pored servera.

Neko od zaposlenih otvori email baš na ovom računaru, biva radoznao, klikne na prilog email-a, raspakuje ga i pokrene .exe fajl.

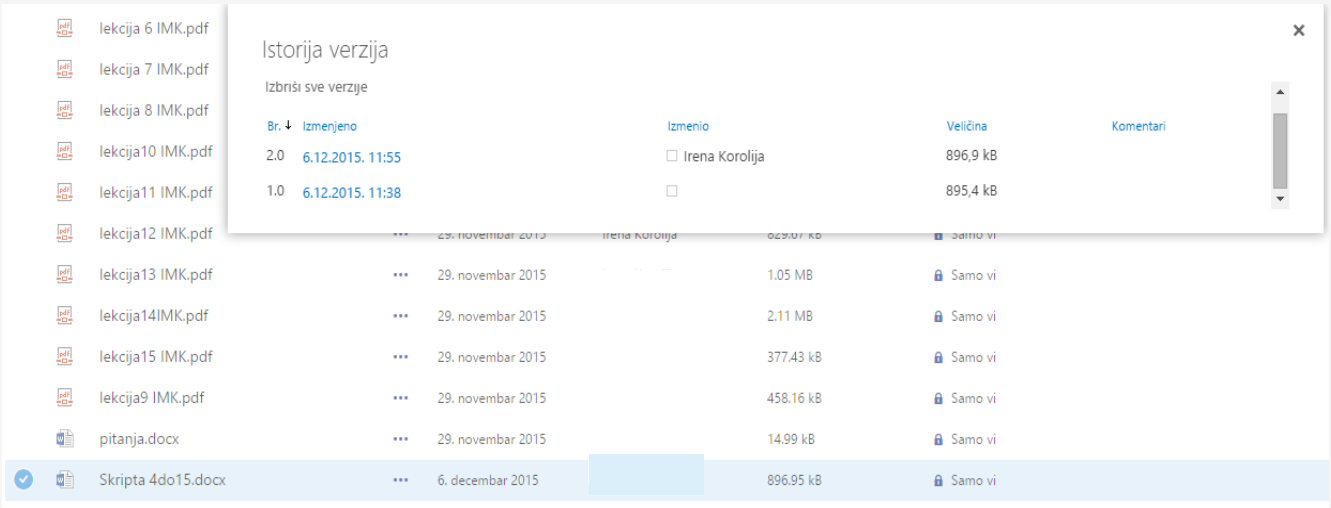
Odjednom mu se na ekranu pojavljuje nešto poput sledeće slike.

Međutim pošto je u firmi iz predostrožnosti redovno rađen bekap na dve lokacije, na serveru i na cloud-u, podacima na cloud-u ne biva ništa, ukoliko je korišćen cloud provajder koji omogućava **verziranje fajlova.** Ukoliko verziranja nije bilo, i podaci na cloud-u će biti najverovatnije izgubljeni.

Verziranje fajlova

Verziranje predstavlja, kako mu i ime kaže, čuvanje više verzija istog fajla. Npr. kod **Office-a 365** postoji verziranje, i samim tim se mogu povratiti verzije fajlova pre trenutka napada malvera.

Kako verziranje otprilike izgleda pogledajte na narednoj slici. Verzije se označavaju brojevima 1.0, 2.0,… A takođe je moguće postaviti i čuvanje podverzija (1.1, 1.2…).



Slučaj ransomware-a

Skoro se u Americi desio slučaj da je bolnica u Holivudu dospela u novine nakon što je rukovodstvo priznalo da su platili blizu **17.000 $ hakerima**, kako bi povratili važne podatke pacijenata. Prema izveštaju, kriminalci su nakon uplate ipak predali podatke bolnici, samo 10 dana nakon napada.

Međutim, **ne postoji garancija** da će se isto poneti i kriminalci koji stoje iza drugih vrsta ovog opasnog virusa. Velika je verovatnoća da Vam uplata ne donese ništa na kraju.

Kompanije obično ne pristaju na plaćanje otkupnine, iz razloga što im je pristup mreži već ugrožen. Stoga **niko nije u potpunosti siguran u verovatnoću povratka podataka** nakon uplate.

Besplatni ransomware alati za dekripciju

Otkup se obično kreće oko par desetina hiljada dinara, što je jeftinije od angažovanja firme za ***data recovery***, koja bi radila na dešifrovanju podataka. Ali pre nego što platite bilo koga, proverite da li slučajno na internetu postoji besplatan alat koji bi Vam pomogao.

Kasperski npr. poseduje ransomware decryptor koji je odličan za Coinvault i Bitcryptor (vrste ransomware-a). Takođe postoji i alat za fajlove koji su enkriptovani sa Teslacrypt-om.

Ransomware prevare: Platiti ili ne?

Prvo što je potrebno uraditi kada dođe do napada je **istraživanje koji tačno malver je u pitanju**, dok je sledeći korak pretraga mogućih besplatnih alata za dekripciju.

Nakon toga je potrebno da **proverite da li imate aktuelan bekap**, koji bi Vam značajno smanjio muke ukoliko i dođe do susreta sa ransomware-om.

Opet sa druge strane, **ukoliko nemate bekap**, najbolji savet koji daju iz FBI-a je, verovali ili ne, da platite otkup. Smatraju da je to najbrži i najjeftiniji način da se reši problem. Međutim ne slažu se svi sa tim.

Postoje dva ugla posmatranja stvari.

Prvi je da kriminalci žele da Vam učine što jednostavnijim način plaćanja i da Vam dostave ključ za dekripciju. Na kraju krajeva, oni samo žele da im ljudi plate i da se pročuje za to da tim plaćanjem zaista dobijaju pristup svojim podacima. Ne ide im u prilog priča da plaćanjem ljudi ipak ne dobijaju pravo pristupa. Tako da je veoma važno da pratite instrukcije kada Vam se na ekranu pojavi poruka sa ucenom, kako biste povratili svoje podatke.

S druge strane postoji priča da **kriminalci nemaju nameru da predaju ključ** iako do uplate dođe. Takođe, ljudi koji plate otkup i ne dobiju ništa, teško da će drugima pričati o tome: izgubili su novac i bili prevareni, i nisu ni blizu tome da im fajlovi budu dekriptovani, tako da i ne žele to baš da dele sa drugima i da se hvale na sav glas.

Dalje, čak i u slučaju da dobijete ključ ili određeni alat za dekripciju, **i dalje niste bezbedni**. Kriminalci i dalje imaju pristup Vašem računaru i ponovo mogu zahtevati otkup, samo sada mnogo veći.

Oni koji Vas savetuju da ne plaćate otkup, takođe će Vas upozoriti da ne verujete u priče poput ove sa holivudskom bolnicom, jer će se držati toga da je moguće da takve priče objavljuju i sami kriminalci, kako bi ubedili žrtve da im plaćaju za ucenjivanje.

Kako se štititi od ransomware-a?

Ukoliko čitate ovo, a već ste pogođeni ransomware-om, naredni saveti Vam neće biti korisni. Ali ukoliko razmišljate unapred i želite da zaštite svoje poslovanje i podatke od nepotrebne štete i troškova, ono što sledi će Vam biti poprilično zanimljivo.

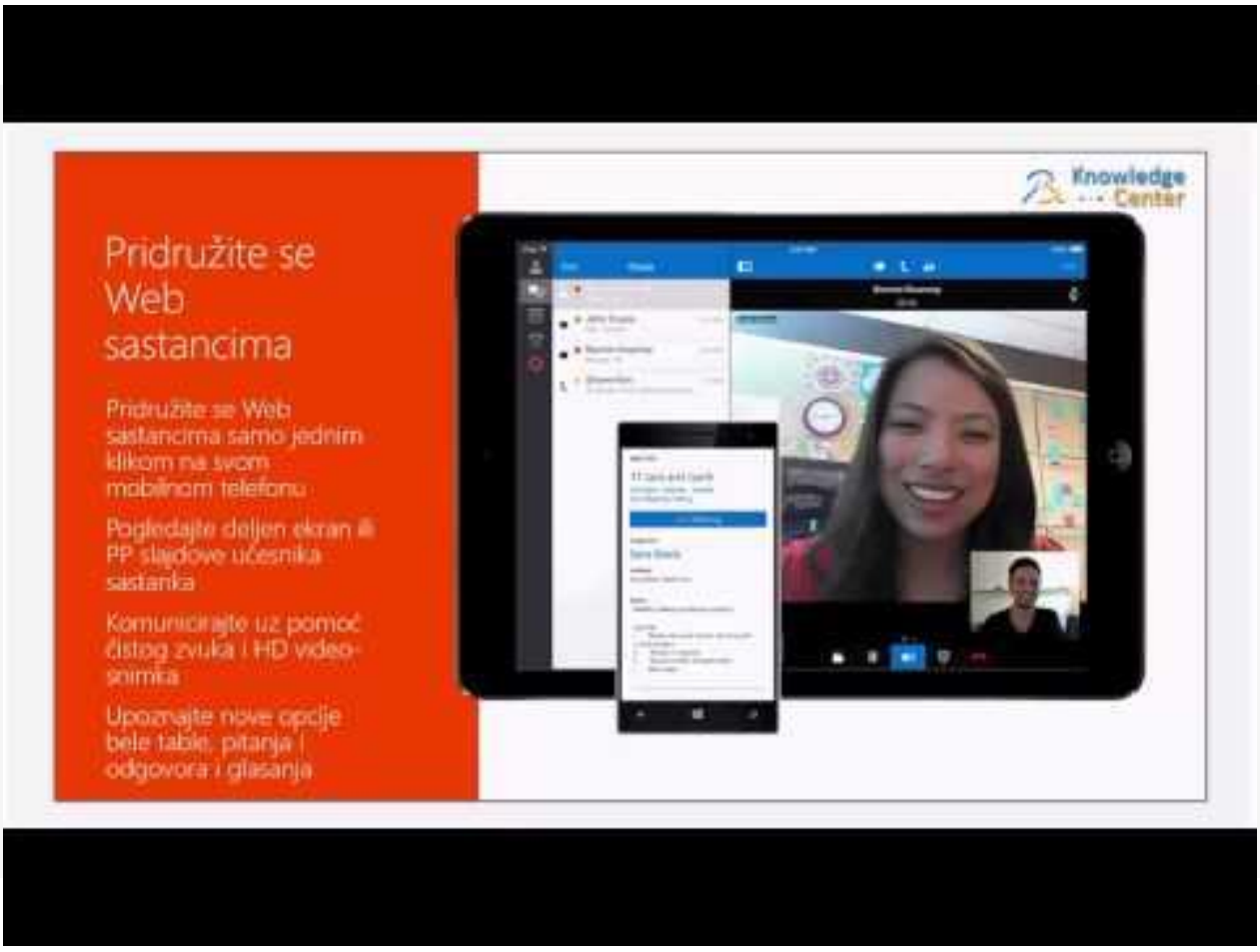
1. Pravite redovne **bekape** svih fajlova, koje nipošto ne biste želeli da izgubite.
   Najbolje rešenje bi bilo pravljenje više bekapa koji uključuju kopije na hard disku ili bilo kom drugom mediju koji je povezan na računar ili internet.
   Prenosivi USB hard disk je idealan.
   Kada je u pitanju **bekap na eksterne uređaje**, opcija koja se nudi u Windows 8 i Windows 10 operativnim sistemima koja to omogućava se zove **File history.**
   Takođe tu je i **bekap u cloud-u**. Što je takođe odlična varijanta, međutim **problem sa cloud tehnologijom** je to što novim tehnologijama **ljudi slabo veruju**.
   Što se **cloud bekapa** tiče, činjenica je da ako vam neko ošteti fajlove na računaru, biće oštećeni i na cloud prostoru (**mada neki servisi nude mogućnost bekapa fajla verziranjem**) a isto važi i u kontra smeru…ako neki haker ošteti fajlove na cloud serveru, biće oštećeni i na vašem računaru(što se do sad nije događalo u praksi, jer su fajlovi u cloud-u mnogo bolje zaštićeni od fajlova na bilo kom pojedinačnom računaru)
2. Neka Vaša **antivirus i internet zaštita uvek bude ažurna** i takođe je veoma bitno da koristite softver koji Vas može zaštititi od različitih vrsta malvera, uključujući ransomware.
3. Budite veoma **oprezni prilikom otvaranja i preuzimanja email priloga** kao i linkova koji se nalaze u okviru mejla. Ransomware obično cilja ljudske slabosti, pre nego slabosti sigurnosnog softvera. Čak i ako je email ili prilog od osobe koja Vam je poznata, ili provajdera usluga koje koristite, ponovo proverite da li je to originalni mejl. Ukoliko sumnjate, ne otvarajte ga, ne preuzimajte prilog, i ne klikćite na linkove koji Vas vode ka stranama gde biste uneli svoje bankovne podatke npr.

Za više informacija o cloud tehnologijama u okviru Office-a 365, možete pogledati neki od sledećih tekstova:

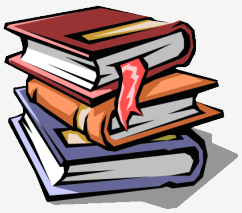
- Mitovi vezani za prelazak u cloud
- Šta tačno podrazumeva primena Office-a 365 na mobilnim uređajima?
- Infografika Office 365- Vaša kancelarija u oblaku
- OneDrive for Business u odnosu na druge cloud usluge
- 10 mitova vezanih za cloud računarstvo

Dodatno…

…pogledajte i naš webinar na temu- ***Office 365 - Cloud u službi vašeg poslovanja***



Nadamo se da će Vam ovaj e-book pomoći u bržem i produktivnijem obavljanju Vašeg posla. Za više uputstava na različite IT teme, posetite Uridium *IT biblioteku*, a ukoliko imate predlog za neko novo uputstvo, pišite nam na *kontakt@uridium.rs*.



O Uridiumu

Uridium je kompanija u privatnom vlasništvu osnovana 1994. godine sa ciljem unapređenja poslovanja upotrebom informacionih tehnologija. Od samog osnivanja Uridium postavlja nove standarde i pomera granice uspostavljene nekom vrstom inercije i neinventivnosti u poslovnim razmišljanjima.

Prvi poslovni projekti su bili projekti poslovne analitike, kao nadogradnja tada veoma aktuelnih „dbase“ poslovnih rešenja za unos podataka. Pomeranje fokusa sa unosa podataka na pregled i analizu podataka koji su uneti, otvara ujedno i dosta izazova, pošto klijenti počinju da traže i analize za koje uopšte ne unose informacije u postojećem sistemu.

Tako nastaje ideja da se napravi sopstveni proizvod, koji počinje svoj život 1995. godine. UBPro je zaživeo u preko 30 preduzeća u veoma kratkom roku. Zbog loše ekonomske situacije, kao i zbog nedovoljno brze adaptacije korisnika na Windows okruženje, Uridium prestaje sa razvojem samo 5 godina kasnije. Naš softver međutim, nastavlja svoj život i nakon toga do danas.

Sa već akumuliranim znanjima o poslovnim procesima, i velikim iskustvom u implementaciji i uvođenju poslovnih rešenja u preduzeća, kao logičan korak napred, Uridium se odlučuje za traženje većeg i sveobuhvatnijeg rešenja, koje će kao partner implementirati i time na najbolji način ugraditi već stečena znanja u nove projekte. Potraga za rešenjem nije baš kratko trajala i tek krajem 2002 godine, uspostavljamo saradnju sa slovenačkom kompanijom DataLab Tehnologije d.d. i potpisujemo ugovor kao SIS (sales, implementation and support) partner.

Od tada do danas, Uridium prodaje, uvodi i održava Pantheon kao vodeći ERP u regionu. Tokom prethodnih 10 godina, uspešno smo implementirali Pantheon u preko 100 preduzeća u Srbiji, Hrvatskoj, Makedoniji, Bosni i Hercegovini i Sloveniji.

Pored ERP projekata, možemo se pohvaliti da smo uspešno uradili i preko 180 raznih IT projekata, od IP telefonije, IT infrastrukture do implementacije specifičnih poslovnih rešenja.

Uridium d.o.o. trenutno zapošljava 12 profesionalaca, čije je radno iskustvo u implementaciji poslovnih rešenja preko 100 čovek godina.

Uridium ima najvišu bonitetnu ocenu A1, u procesu je implementacije ISO 9001:2008 standarda za usluge u informacionim tehnologijama, a u planu je, i veoma ozbiljno se pripremamo za implementaciju ITIL V3 standarda.

Uridium Valjevo
Uzun Mirkova BB
14000 Valjevo
+381 14 292 222

Uridium Beograd
Jurija Gagarina 28/13
11070 Novi Beograd
+381 22 83 081

info@uridium.rs
www.uridium.rs