CARNET

# Sigurnosni rizici pohrane lozinki u preglednike

CERT.hr-PUBDOC-2023-6-409

CERT.hr

**Sadržaj**

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

# 1 Uvod

Brojni preglednici imaju funkcionalnost pohrane lozinki te sinkronizacije lozinki između različitih uređaja istog korisnika. Iako ta funkcionalnost poboljšava korisničko iskustvo, povećava i rizik od nekih napada. Osobito su opasni scenariji u kojima zaposlenik u pregledniku svog osobnog računala pohranjuje lozinke za pristup poslovnim resursima (npr. lozinku za poslovni mail).

U ovom dokumentu su opisane neke od situacija u kojima napadači mogu doći do lozinki pohranjenih u pregledniku te mjere koje organizacija i pojedinac mogu poduzeti kako bi se zaštitili od takvih napada.

**Svi pristupni podaci vidljivi na snimkama zaslona u slikama korištenim u dokumentu izrađeni su za potrebe dokumenta i ne pripadaju stvarnim korisničkim računima**.

# 2 Opasnosti

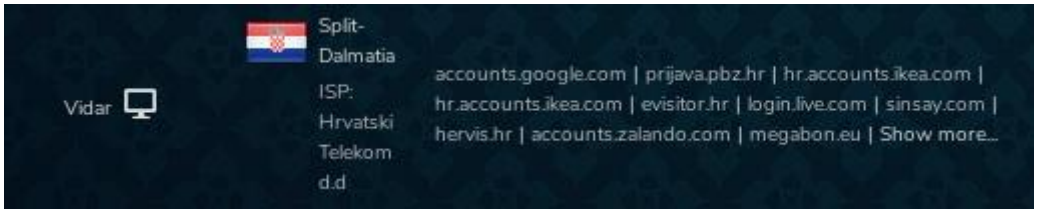
## 2.1 Zlonamjerni programi (engl. *malware*)

Većina popularnih zlonamjernih programa za krađu podataka (engl. *infostealer* [1] *malware*) ima mogućnost krađe lozinki pohranjenih u pregledniku [2]. Takav zlonamjerni program se često prodaje na kriminalnim forumima, a napadači koji koriste takav program ne moraju imati napredne tehničke vještine.

Napadači obično socijalnim inženjeringom nagovore žrtvu da instalira zlonamjerni program za krađu podataka, primjerice postavljanjem zlonamjernog oglasa u rezultate tražilice (engl. *malvertising*) [3]. Takve kampanje često ne ciljaju specifičnu žrtvu nego im je cilj prikupiti što više pristupnih podataka. U nekim slučajevima napadači ne iskoriste te pristupne podatke samostalno, nego ih prodaju drugim kriminalcima.

Baze podataka na kriminalnim tržištima obično nude mogućnost pretraživanja domena za koje se pristupni podaci nude na prodaju. Napadači koji žele kompromitirati neku organizaciju mogu pretraživati domene te organizacije i kupiti pristupne podatke (ako su dostupni) koji će im omogućiti pristup internim resursima te organizacije.

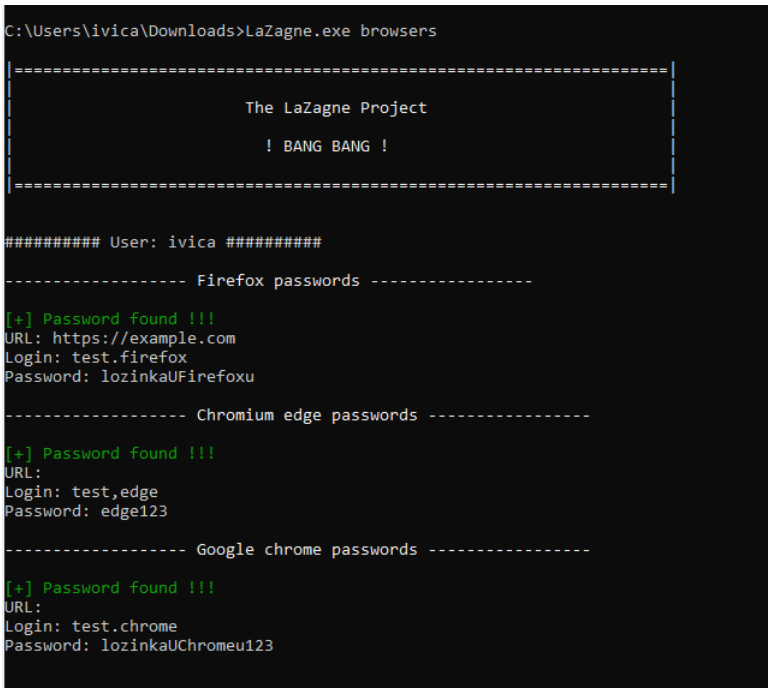
Tako je primjerice kriminalna grupa *LAPSUS$* kupovala pristupne podatke s kriminalnih tržišta kako bi dobila inicijalni pristup internoj mreži organizacije koju su htjeli kompromitirati [4].




**Slika 1. – Snimka zaslona s jednog od kriminalnih tržišta. Navedene su domene za koje se prodaju pristupni podaci. Napadač je koristio *infostealer* Vidar [5].**

Slika 1. prikazuje snimku zaslona na kojoj je vidljiv popis domena za koje se prodaju pristupni podaci s korisničkih računa žrtve dostupni na kriminalnom tržištu.

Na slici 2. vidljiva je demonstracija krađe podataka iz preglednika alatom *LaZagne*. *LaZagne* je alat otvorenog kôda koji se može koristiti za pronalazak vjerodajnica (engl. *Credentials*) na uređaju [6]. Slika prikazuje kako su pomoću alata izvučene vjerodajnice iz Chromea, Firefoxa i Edgea.




**Slika 2. – ispis vjerodajnica iz preglednika pomoću alata LaZagne**

## 2.2 Kompromitirani korisnički račun za sinkronizaciju preglednika

Neki preglednici nude mogućnost sinkronizacije lozinki pohranjenih u pregledniku između uređaja.

Napadači mogu doći do tih podataka ako kompromitiraju korisnički račun pod kojim se izvodi sinkronizacija. Na primjer, u slučaju da korisnik koristi uslugu *Chrome sync* [7] uz preglednik Google Chrome, napadači mogu doći do lozinki ako kompromitiraju korisnikov Google račun.

Tako su u svibnju 2022. napadači dobili pristup internoj mreži tvrtke Cisco. Napadači su kompromitirali osobni Google račun jednog zaposlenika Cisca koji je imao uključenu sinkronizaciju lozinki te je u pregledniku imao pohranjene poslovne pristupne podatke koje su napadači koristili za daljnji napad [8].

Sigurnost mehanizma sinkronizacije lozinki ovisi i o tome kako pružatelj usluge sinkronizacije (Google, Mozilla, Microsoft i dr.) šifrira lozinke koje se sinkroniziraju između uređaja. U slučaju da se ne koristi metoda šifriranja s kraja na kraj (engl. *end-to-end encryption*) pružatelj usluge ima mogućnost pročitati lozinke koje su pohranjene na njihovim poslužiteljima. To predstavlja opasnost u slučaju da pružatelj usluge ima zlonamjerne zaposlenike ili ako računalni sustavi pružatelja usluge budu kompromitirani.

Ako pružatelj usluge koristi šifriranje s kraja na kraj, sinkronizirane lozinke su šifrirane pomoću korisnikove lozinke ili nekog drugog autentifikacijskog faktora koji bi trebao biti dostupan samo korisniku. U tom slučaju, ako korisnik zaboravi svoju lozinku,

pružatelj usluge neće moći oporaviti spremljene lozinke (npr. ako resetira lozinku putem SMS-a za oporavak).

Tablica 1. navodi popularne preglednike i način na koji šifriraju sinkronizirane podatke.

| Preglednik | Šifriranje lozinki s kraja na kraj? |
|---|---|
| Google Chrome | Opcionalno (po zadanim postavkama ne) [9] |
| Mozilla Firefox | Da [10] |
| Microsoft Edge | Ne [1] |
| Apple Safari | Da [11] |
| Brave Browser | Da [12] |
| Opera | Da [13] |

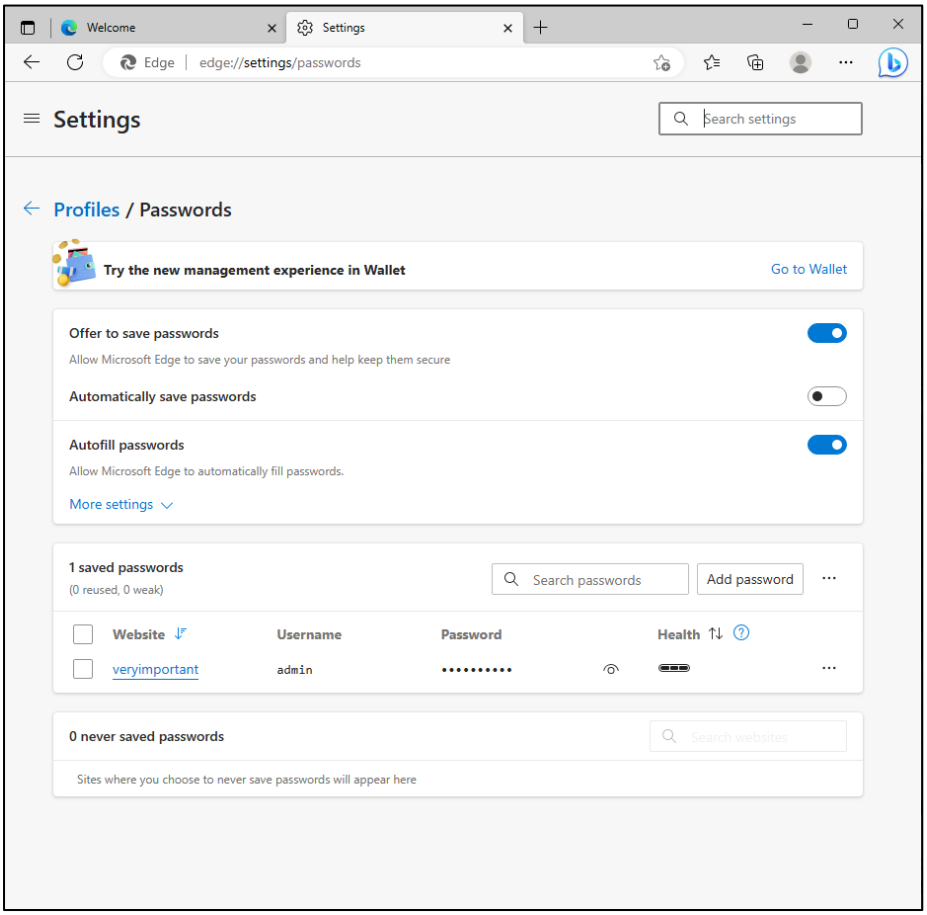
**Tablica 1.: Pregled šifriranja end-to-end po preglednicima**

Osim zlonamjernog ili kompromitiranog pružatelja usluga, nedostatak šifriranja s kraja na kraj predstavlja opasnost i u scenariju gdje napadač može resetirati lozinku putem SMS kôda za oporavak računa.

### 2.2.1 Opis mogućeg scenarija napada na korisnika koji koristi sinkronizaciju u pregledniku Microsoft Edge:

[1] Microsoft u svojoj dokumentaciji ne opisuje detaljno kakvo šifriranje koristi Edge Sync sustav, no iz demonstracije na sljedećoj stranici može se zaključiti da u trenutku pisanja ovog dokumenta ne koristi šifriranje s kraja na kraj

1) Žrtva spremi lozinku u Microsoft Edge



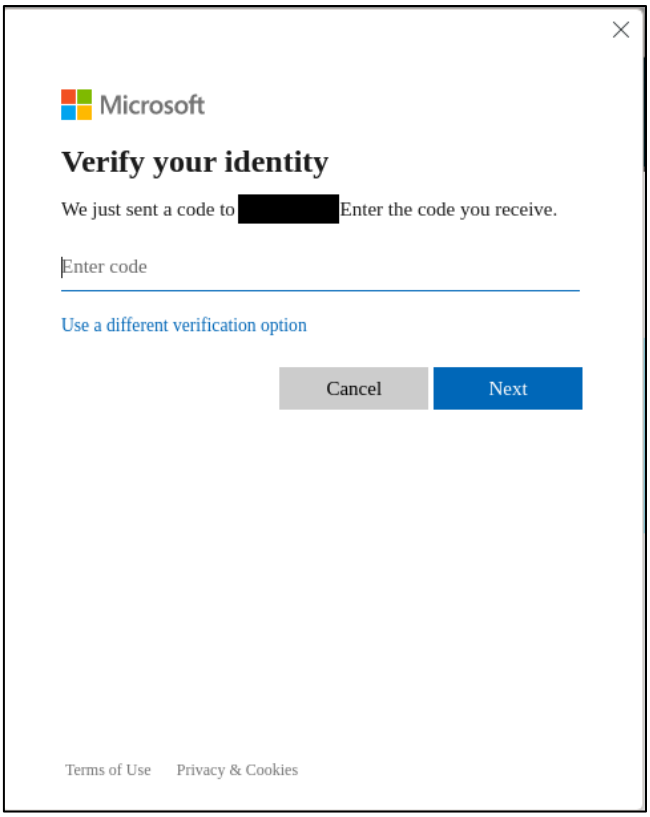

**Slika 3. - Žrtva spremi lozinku u preglednik**

2) Žrtva ima uključenu sinkronizaciju pomoću svog osobnog Outlook računa. U postavkama Outlook računa, žrtva je postavila broj mobilnog telefona za oporavak.

3) Napadač sazna žrtvin broj telefona.

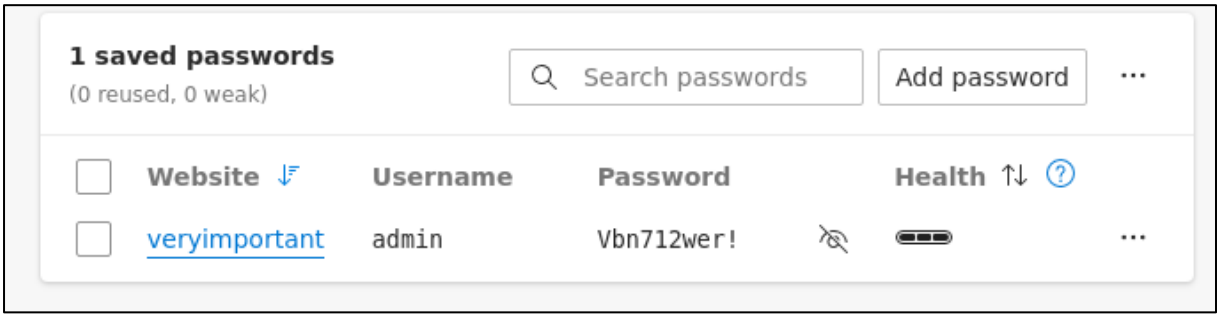
4) Napadač socijalnim inženjeringom uvjeri zaposlenika telekoma da prebaci žrtvin telefonski broj na napadačev uređaj (tzv. *SIM swapping* napad).

5) Napadač primi SMS kôd za oporavak računa i promijeni lozinku.



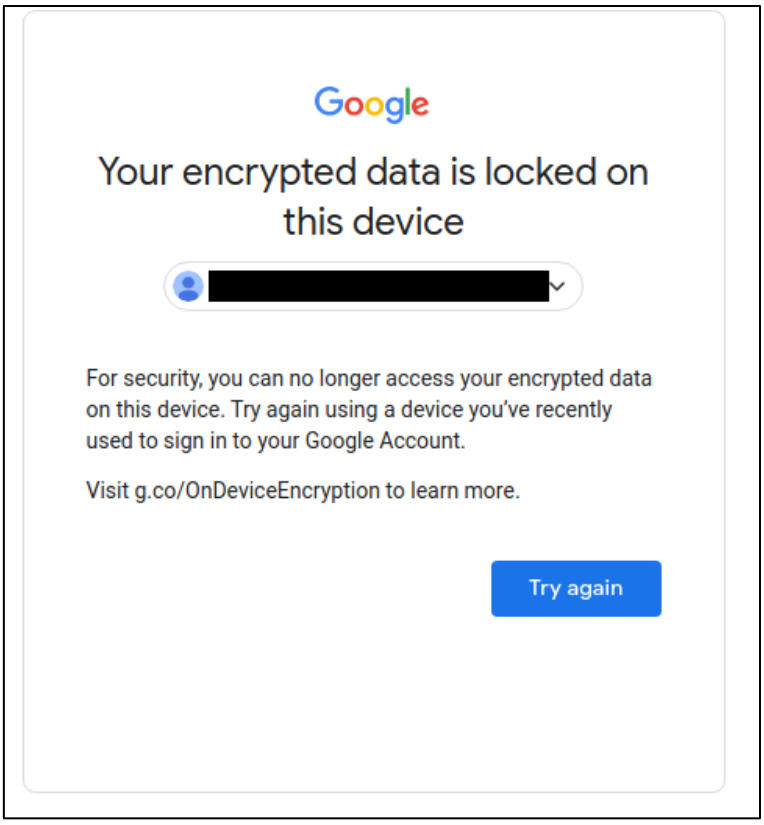

**Slika 4. -Napadač resetira lozinku SMS kôdom**

6) Napadač sad može pročitati lozinke koje je žrtva spremila.




**Slika 5. - Napadač može pročitati spremljene lozinke**

Ovakav napad nije moguć ako pružatelj usluga koristi šifriranje s kraja na kraj. Primjerice, kada bi napadač pokušao izvesti ovakav napad na Googleov račun s uključenom opcijom *on-device encryption* dobio bi sljedeću poruku:



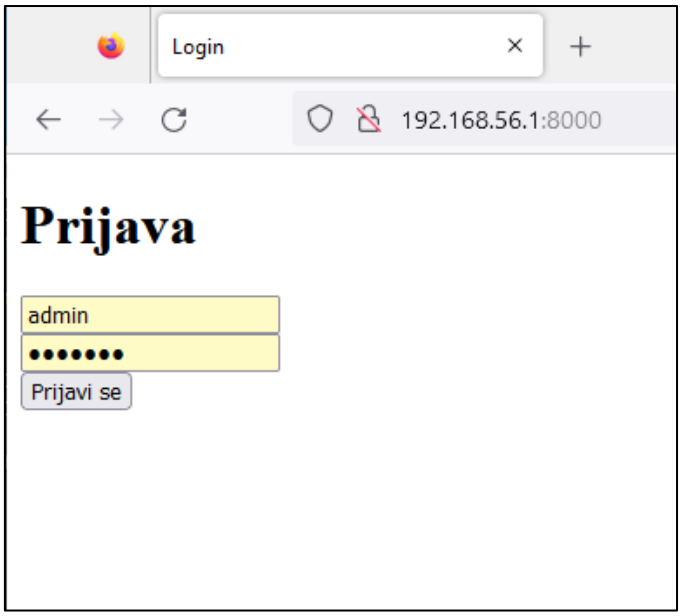

**Slika 6. - Pokušaj napada kada je uključen *on-device encryption***

## 2.3 Krađa lozinki XSS napadom

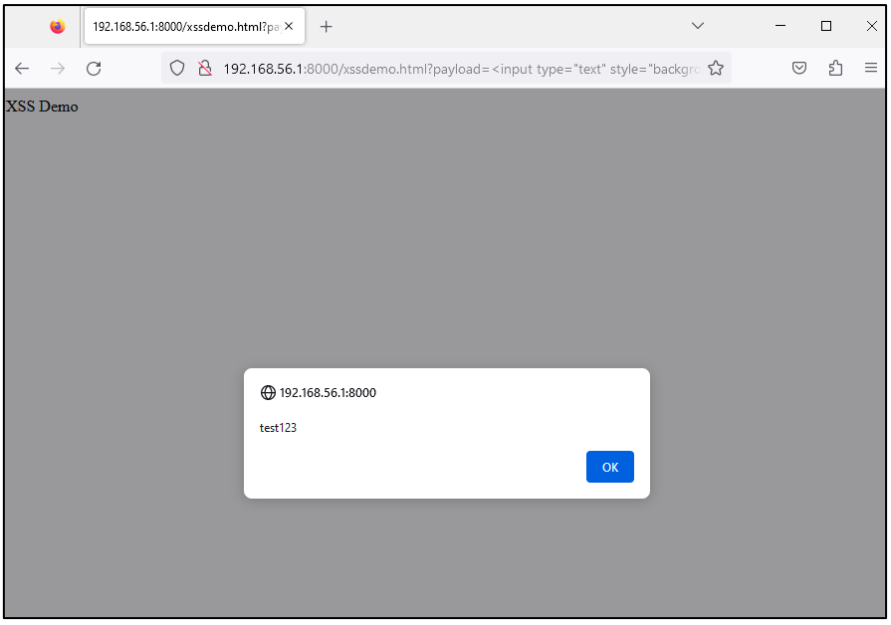
XSS (engl. *cross-site scripting*) je ranjivost kojom napadač može ubaciti zlonamjerni JavaScript kôd u neku web stranicu [14] [15].

Ako je, uz funkcionalnost pohrane, u pregledniku uključena i funkcionalnost automatskog popunjavanja formi (engl. *autofill*), to može napadaču olakšati iskorištavanje XSS ranjivosti.

U slučaju da je web sjedište ranjivo na XSS, napadač može ubaciti HTML formu koja će se automatski popuniti kao što je vidljivo na Slici 7., a zatim pomoću JavaScripta izvući spremljenu lozinku. Forma može biti učinjena nevidljivom pomoću CSS-a (*Cascading Style Sheets*), kako žrtva ne bi posumnjala na napad. To olakšava napadaču iskorištavanje XSS ranjivosti jer može kompromitirati korisnički račun i ako korisnik nije prijavljen u web aplikaciju [16].




**Slika 7. - Automatski popunjena lozinka**




**Slika 8. - Dobivanje lozinke XSS napadom - u stvarnom napadu napadač bi umjesto skočnog prozora (engl. *pop-up)* poslao lozinku na svoj poslužitelj**

Potrebno je napomenuti da je ovakvim napadom moguće napasti i korisnike koji koriste programe za upravljanje lozinkama (engl. *password managers*) koji imaju uključenu opciju automatskog popunjavanja formi s lozinkama.

S druge strane, opcija automatskog popunjavanja lozinki može pomoći u prepoznavanju *phishing* stranice. Ako je korisnik naviknut na to da mu se za neko web sjedište uvijek automatski popuni lozinka, može primijetiti da se događa nešto sumnjivo ako se lozinka ne popuni automatski. Na phishing stranicama se lozinka neće automatski popuniti zato

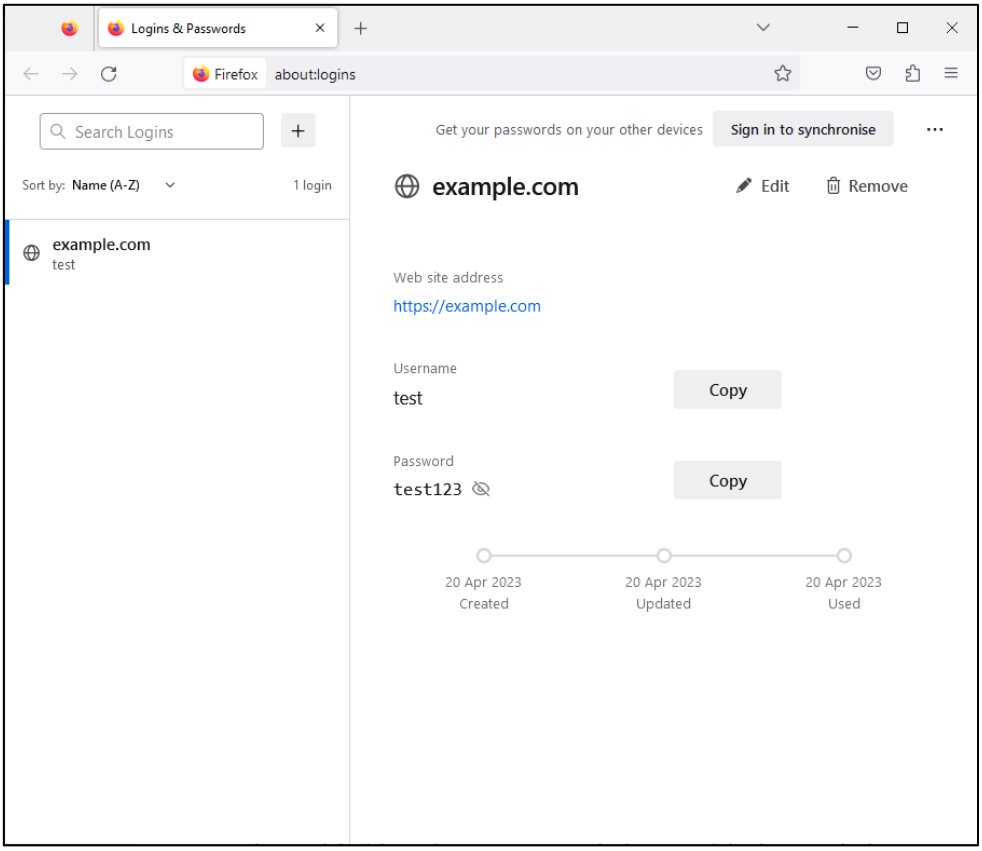
što će se nalaziti na krivoj domeni. To je važno, jer je za većinu korisnika, *phishing* napad realnija prijetnja.

## 2.4 Fizički pristup računalu

### 2.4.1 Pristup otključanom računalu

U slučaju da napadač dobije fizički pristup otključanom računalu korisnika može pristupiti svim lozinkama pohranjenim u pregledniku kroz korisničko sučelje, bez naprednijih tehničkih vještina.

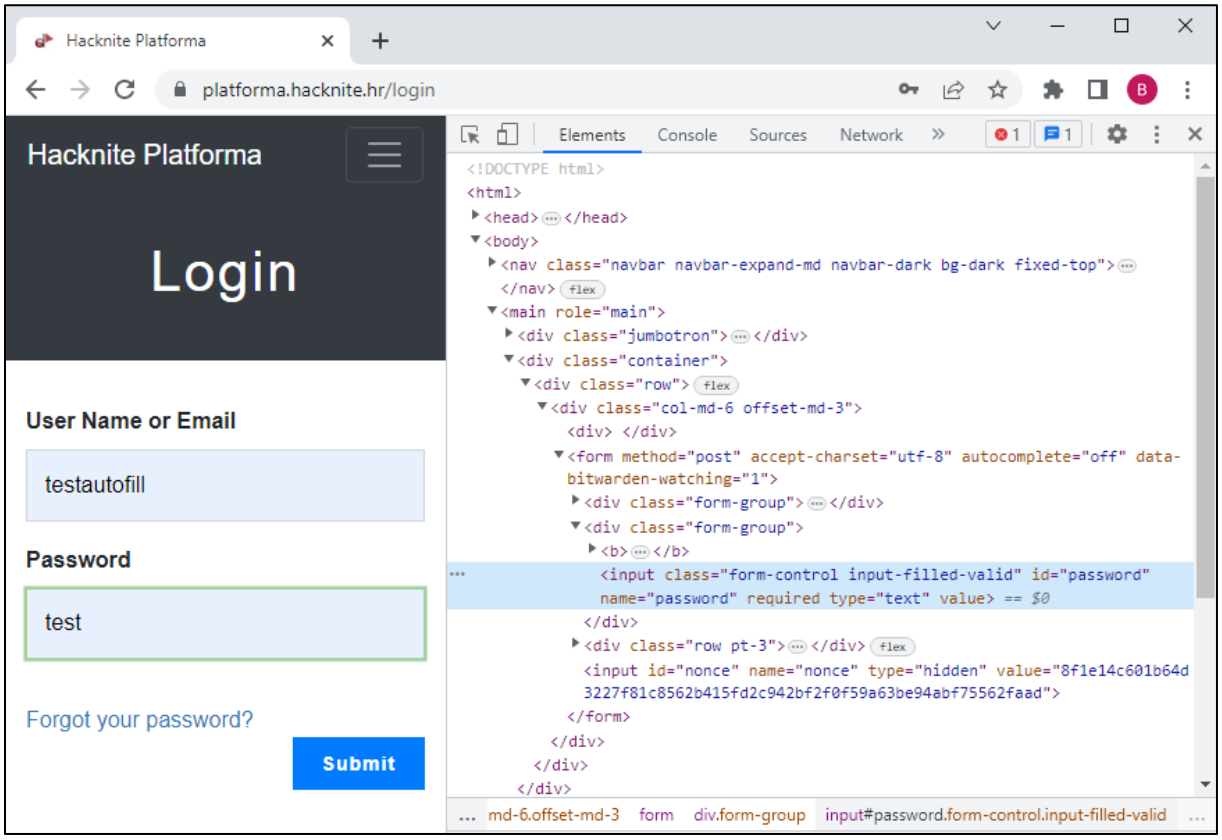
Firefox preglednik na Windows operacijskom sustavu dozvoljava pregled spremljenih lozinki[2] putem korisničkog sučelja bez potrebe za dodatnom autentifikacijom kao što je prikazano na Slici 9.




**Slika 9. - Pristup pohranjenim lozinkama na Firefoxu**

[2] Na Linuxu su lozinke tako šifrirane ako je instaliran softver Gnome-Keyring ili Kwallet, što je slučaj za većinu popularnijih desktop distribucija (npr. Ubuntu). Ako nisu instalirani Gnome-Keyring ili Kwallet, lozinke nisu šifrirane.

Prema zadanim postavkama, na Windowsu, preglednici temeljeni na Chromiumu [3] traže autentifikaciju Windows lozinkom prije nego što se lozinke mogu vidjeti. Takva mjera može samo usporiti napadača i ne pruža zaštitu od napadača koji dulje vrijeme ima fizički pristup računalu (npr. napadač koji ukrade računalo dok je ono otključano). Napadač i dalje može ukrasti pohranjene lozinke jednu po jednu tako da posjeti web sjedište za koju je lozinka spremljena, a zatim koristeći „inspect element“ promijeni atribut „password“ u „text“ kao što je prikazano na Slici 10.




**Slika 10. – Otkrivanje pohranjene lozinke pomoću „inspect element“**

Na nekim preglednicima moguće je konfigurirati dodatne mjere zaštite od ne-sofisticiranih fizičkih napada. Primjerice Microsoft Edge je moguće konfigurirati tako da se Windows autentifikacija traži i prije automatskog popunjavanja lozinke čime bi se mogao spriječiti prethodno opisani XSS napad. Međutim, uz takvu zaštitu je i dalje moguće pročitati lozinke korištenjem alata kao što je LaZagne, spomenut u poglavlju 2.1.

Edge i Firefox također nude mogućnost postavljanja druge lozinke, nevezane za Windows. Tada napadač bez poznavanja te lozinke neće moći pročitati lozinke pohranjene u pregledniku čak ni korištenjem alata kao što je *LaZagne*.

[3] Primjerice Google Chrome, Microsoft Edge, Opera, Brave, Vivaldi itd.

### 2.4.2 Analiza diska

Ako napadač dobije fizički pristup računalu dok je ono isključeno ili zaključano, može pokušati doći do pristupnih podataka pohranjenih u pregledniku forenzičkom analizom diska. Svi napadi opisani u ovom poglavlju pretpostavljaju da disk nije šifriran ili da je napadač uspio dešifrirati disk.

Na preglednicima temeljenim na Chromiumu lozinke i kolačići u pregledniku su šifrirani pomoću kriptografskog ključa izvedenog iz lozinke korisnika operacijskog sustava. Taj mehanizam se koristi na Windowsu, Mac OS-u i Linuxu. Ako je lozinka operacijskog sustava dovoljno kompleksna, napadač ne može doći do lozinki ni do autentifikacijskih kolačića pohranjenih u pregledniku.

Firefox bez korištenja primarne lozinke ne šifrira ni lozinke ni autentifikacijske kolačiće pa napadač može analizom diska otkriti vrijednost lozinki koristeći alate poput *firefox_decrypt*. [17] kao što je prikazano na Slici 11., a kolačiće je moguće vidjeti otvaranjem datoteke *cookies.sqlite*.

```
$ python3.9 firefox_decrypt.py zs87g7o5.default-release/
2023-04-21 11:03:08,633 - WARNING - profile.ini not found in zs87g7o5.default-release/
2023-04-21 11:03:08,634 - WARNING - Continuing and assuming 'zs87g7o5.default-release/' is a profile location

Website:   https://example.com
Username: 'test'
Password: 'Test123'
```

**Slika 11. - Korištenje alata *firefox_decrypt***

U slučaju da je žrtva na Firefoxu konfigurirala primarnu lozinku, napadač bez poznavanja primarne lozinke ne može otkriti vrijednost lozinki, ali i dalje može pročitati autentifikacijske kolačiće.

# 3 Zaštitne mjere

## 3.1 Korištenje poslovnih uređaja

Najsigurniji način kojim se organizacija može zaštititi od napada i kompromitacije uzrokovane propustom zaposlenika je taj da osigura i uredi pravila i politike prema kojima zaposlenici koriste isključivo poslovne uređaje za pristup poslovnim resursima.

Organizacija može osigurati da se na poslovnim uređajima primjenjuju strože sigurnosne mjere nego što je to uobičajeno za osobna računala. Primjerice, može zaposleniku dati samo ograničene ovlasti nad uređajem, ograničiti koje aplikacije zaposlenik može pokretati na uređaju (engl. *application whitelisting*) i osigurati da disk uređaja bude šifriran.

## 3.2 Višefaktorska autentifikacija i istek sesije (engl. *session*)

Višefaktorska autentifikacija može otežati napad zato što napadaču nije dovoljna samo lozinka pohranjena u pregledniku kako bi se prijavio u web aplikaciju.

Osim lozinki, napadač može ukrasti i autentifikacijske kolačiće (engl. *cookies*) ili tokene pohranjene u pregledniku. Ako autentifikacijski kolačići još vrijede tada napadaču ne treba ni lozinka ni drugi faktor autentifikacije kako bi se prijavio u web aplikaciju. Zbog toga je bitno da sesije važnih web aplikacija ne traju dugo. Pojedinac također može smanjiti vjerojatnost uspješnog napada tako da se odjavi nakon što završi s korištenjem aplikacije.

Budući da operateri zlonamjernih programa za krađu podataka često nisu ti koji iskoriste ukradene podatke nego ih prodaju drugim kriminalcima, ako je vrijeme trajanja sesije kratko sesije će vjerojatno isteći do vremena kad podaci budu kupljeni.

Napadači ponekad pokušaju zaobići dvofaktorsku autentifikaciju korištenjem socijalnog inženjeringa. Zbog toga, sigurnija opcija za organizaciju je implementacija dvofaktorske autentifikacije koja je otpornija na *phishing* napade poput korištenja fizičkih sigurnosnih tokena (npr. YubiKey, Titan Security Key, Feitian Key i sl.) [18].

## 3.3 Obavještajni podaci o prijetnjama (engl. *Threat intel)*

Organizacija može unajmiti usluge tvrtki koje se bave nadzorom kriminalnih tržišta, koje mogu obavijestiti organizaciju kada se pristupni podaci za neki njihov resurs prodaju. Neke od takvih tvrtki su *Mandiant*, *Recorded future* i *Socradar* [19] [20] [21].

## 3.4 Upravitelji lozinkama (engl. *password managers*)

Upravitelji lozinkama su programi koji pohranjuju lozinke u šifriranom obliku. Uz to, pružaju mogućnost nasumičnog generiranja lozinke. Korisnik svim svojim lozinkama pristupa korištenjem jedne glavne lozinke (engl. *master password*) koju treba zapamtiti.

Korištenjem upravitelja lozinki umjesto pohrane lozinki u preglednik moguće je spriječiti ili otežati neke napade.

Napadač koji dođe do šifrirane baze lozinki, neće ju moći otključati ako ne zna glavnu lozinku.

U slučaju zlonamjernog programa, upravitelj lozinki ne može zaštititi lozinke od svih napada. Jednom kad napadač može izvršavati kôd na žrtvinom računalu, može doći do dešifriranih lozinki snimanjem pritisnutih tipki (engl. *keylogging)* prilikom unosa glavne lozinke, nadzorom međuspremnika (engl. *clipboard*) (čime može dobiti lozinke koje se kopiraju iz upravitelja), ubacivanjem svog kôda u memoriju procesa upravitelja ili drugim metodama. Ipak, korištenje upravitelja lozinki umjesto pohrane lozinki u preglednik može otežati aktivnosti nekih napadača.

Zlonamjerni program može ukrasti lozinke samo dok je baza lozinki otključana. Brojni zlonamjerni programi za krađu podataka izbrišu sami sebe (ili ih barem napadači mogu tako konfigurirati) nakon što završe s krađom, kako ne bi ostavili tragove koje bi antivirusno rješenje kasnije moglo detektirati, što bi moglo potaknuti žrtvu da promijeni svoje lozinke [22] [23] [24] [25] [26]. Napadačima je teže ukrasti lozinke pohranjene pomoću upravitelja lozinki nego one pohranjene u pregledniku, zato što baza lozinki možda neće biti otključana tijekom pokretanja zlonamjernog programa. S druge strane, zlonamjerni program koji radi na takav način i dalje može ukrasti šifriranu bazu lozinki zbog čega je vrlo bitno da glavna lozinka bude dovoljno kompleksna kako ju napadač ne bi mogao pogoditi.

Neovisno o tome izbriše li zlonamjerni program samog sebe ili ne, većina popularnih programa za krađu podataka (npr. Redline Stealer) u vrijeme pisanja ovog dokumenta nema ugrađenu funkcionalnost za krađu lozinki iz otključanog upravitelja lozinkama. Ipak, takav zlonamjerni program postoji, primjerice - *Rhadamantys* može izvući lozinke iz memorije procesa *Keepass* programa [27].

Zbog svojih sigurnosnih značajki, upravitelji lozinkama su dobra alternativa pohrani lozinka u preglednike.

Postoje dva osnovna tipa upravitelja lozinkama, lokalni i mrežni.

Kod lokalnih upravitelja lozinkama, lozinke se u šifriranom obliku pohranjuju u datoteci na računalu korisnika. Ako korisnik želi imati pristup lozinkama s više uređaja može koristiti neki vanjski servis za dijeljenje datoteka. Korisnik je ujedno i odgovoran za izradu pričuvnih kopija. Primjer takvog upravitelja lozinkama je Keepass o kojem više možete pročitati u CERT-ovom dokumentu.

Mrežni upravitelji lozinkama pohranjuju lozinke šifrirane na poslužitelju, korisnik se spoji na upravitelj lozinki putem web sučelja, desktop ili mobilne aplikacije i dešifrira lozinke na klijentskoj strani pomoću svoje glavne lozinke. Neki od takvih upravitelja lozinki su 1Password, Bitwarden, Dashlane i Nordpass [28] [29] [30] [31].

# 4 Zaključak

Pristupni podaci pohranjeni u preglednicima su primamljiva meta za napadače.

Najbolji način na koji organizacija može spriječiti ili bar otežati napade kojima je cilj dohvatiti pristupne podatke u pregledniku je taj da zaposlenicima osigura poslovne uređaje koji se koriste isključivo u poslovne svrhe. Primjenom strožih sigurnosnih mjera na poslovnim uređajima znatno se smanjuje vjerojatnost da će poslovni pristupni podaci biti kompromitirani.

Također, implementacija dvofaktorske autentifikacije te istek sesije nakon perioda neaktivnosti može ublažiti posljedice napada kojim je uspješno dobiven pristup lozinkama pohranjenim u pregledniku.

Korištenje upravitelja lozinkama može otežati aktivnosti manje sofisticiranih napadača, pa se može koristiti kao alternativa pohrani lozinka u preglednike.

# 5 Literatura


[1] [Mrežno] https://www.trendmicro.com/vinfo/us/security/definition/Info-stealer. [Citirano 10 5 2023].

[2] [Mrežno] https://www.accenture.com/us-en/blogs/security/information-stealer-malware-on-dark-web [Citirano 14.4.2023].

[3] [Mrežno]. https://securelist.com/malvertising-through-search-engines/108996/. [Citirano 14 4 2023].

[4] [Mrežno].https://krebsonsecurity.com/2022/04/leaked-chats-show-lapsus-stole-t-mobile-source-code/. [Citirano 19 4 2023].

[5] [Mrežno].https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/what-is-vidar-malware/. [Citirano 10 5 2023].

[6] [Mrežno]. https://github.com/AlessandroZ/LaZagne. [Citirano 20 4 2023].

[7] [Mrežno]. https://support.google.com/chrome/answer/185277. [Citirano 10 5 2023].

[8] [Mrežno]. https://blog.talosintelligence.com/recent-cyber-attack/. [Citirano 14 4 2023].

[9] [Mrežno] https://support.google.com/accounts/answer/11350823?ctx=ep. [Citirano 19 4 2023].

[10] [Mrežno] https://support.mozilla.org/en-US/kb/how-firefox-sync-keeps-your-data-safe-even-if-tls-fails. [Citirano 19 4 2023].

[11] [Mrežno] https://support.apple.com/en-us/HT202303. [Citirano 19 4 2023].

[12] [Mrežno] https://support.brave.com/hc/en-us/articles/360047642371-Sync-FAQ. [Citirano 19 4 2023].

[13] [Mrežno] https://help.opera.com/en/opera36/sync-your-browser/. [Citirano 19 4 2023].

[14] [Mrežno] https://owasp.org/www-community/attacks/xss/. [Citirano 10 5 2023].

[15] [Mrežno] https://www.chromium.org/Home/. [Citirano 10 5 2023].

[16] [Mrežno] https://www.gosecure.net/blog/2022/06/29/did-you-know-your-browsers-autofill-credentials-could-be-stolen-via-cross-site-scripting-xss/. [Citirano 14 4 2023].

[17] [Mrežno] https://github.com/unode/firefox_decrypt. [Citirano 21 4 2023].

[18] [Mrežno] https://www.sans.org/blog/what-is-phishing-resistant-mfa/. [Citirano 14 4 2023].

[19] [Mrežno] https://www.mandiant.com/advantage/digital-threat-monitoring. [Citirano 10 5 2023].

[20] [Mrežno] https://socradar.io/. [Citirano 10 5 2023].

[21] [Mrežno] https://www.recordedfuture.com/threats/dark-web-monitoring. [Citirano 10 5 2023].

[22] [Mrežno] https://blog.cyble.com/2021/10/26/vidar-stealer-under-the-lens-a-deep-dive-analysis/. [Citirano 21 4 2023].

[23] [Mrežno] https://blog.sekoia.io/bluefox-information-stealer-traffer-maas/. [Citirano 21 4 2023].

[24] [Mrežno] https://outpost24.com/blog/an-in-depth-analysis-of-the-new-taurus-stealer. [Citirano 21 4 2023].

[25] [Mrežno] https://www.bleepingcomputer.com/news/security/jester-stealer-malware-adds-more-capabilities-to-entice-hackers/. [Citirano 21 4 2023].

[26] [Mrežno] https://cyware.com/news/new-oski-redesign-steals-crypto-and-2fa-codes-56b21e31. [Citirano 21 4 2023].

[27] [Mrežno] https://elis531989.medium.com/dancing-with-shellcodes-analyzing-rhadamanthys-stealer-3c4986966a88. [Citirano 14 4 2023].

[28] [Mrežno] https://1password.com/. [Citirano 10 5 2023].

[29] [Mrežno] https://bitwarden.com/. [Citirano 10 5 2023].

[30] [Mrežno].https://www.dashlane.com/. [Citirano 10 5 2023].

[31] [Mrežno] https://nordpass.com/. [Citirano 10 5 2023].

[32] [Mrežno] https://textslashplain.com/2020/09/28/local-data-encryption-in-chromium/. [Citirano 14 4 2023].

[33] [Mrežno] https://www.f-secure.com/v-descs/trojan_w32_lokibot.shtml. [Citirano 14 4 2023].

[34] [Mrežno] https://support.apple.com/en-us/HT202303. [Citirano 19 4 2023].

[35] [Mrežno] https://www.trendmicro.com/vinfo/us/security/definition/Info-stealer. [Citirano 10 5 2023].

[36] [Mrežno] https://www.chromium.org/Home/. [Citirano 10 5 2023].

[37] [Mrežno] https://www.mandiant.com/advantage/digital-threat-monitoring. [Citirano 10 5 2023].