CIRT.ME

2024

# SAJBER BILTEN

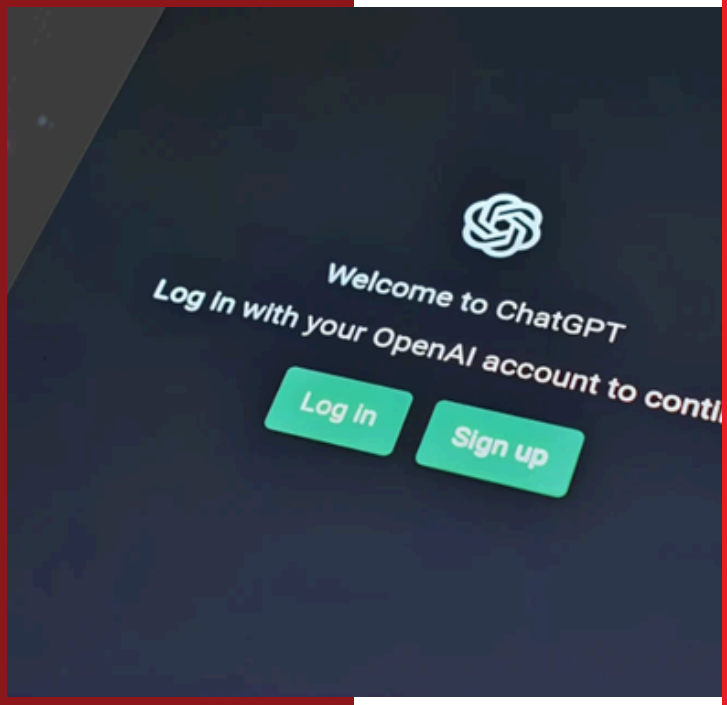
06/24

## Top vijesti

**Krađa lozinki i novca putem lažne captcha verifikacije**

**Hakeri ukrali korisničke podatke u napadu MoneyGram-a**

**Oprez! Pojavila se lažna „Temu“ aplikacija**




## ChatGPT postaje alat sajber kriminalaca

OpenAI kompanija je uspješno prekinula više od 20 sajber operacija širom svijeta od početka 2024. godine. Ove operacije uključuju ciljanje mreža hakera povezanih sa Iranom i Kinom. Ovaj trend ukazuje na rastuću povezanost između vještačke inteligencije i sajber bezbjednosti.

Iako su ove grupe pokušale da iskoriste ChatGPT za zlonamjerne svrhe, OpenAI naglašava da vještačka inteligencija nije donijela značajne mogućnosti za razvoj malvera.

Kako vještačka inteligencija nastavlja da igra ključnu ulogu u prijetnjama sajber bezbjednosti, OpenAI ostaje posvećen implementaciji čvrstih mjera za identifikaciju i sprečavanje ovih zlonamjernih aktivnosti. Kontinuirana evolucija AI-a u domenu sajber bezbjednosti naglašava važnost budnosti i inovacija u strategijama zaštite od sajber prijetnji.

## Hakeri ukrali korisničke podatke u napadu MoneyGram-a

MoneyGram je potvrdio ozbiljan sajber napad koji se dogodio u septembru, tokom kojeg su hakeri ukrali lične podatke korisnika, uključujući informacije o transakcijama.

Incident, otkriven 27. septembra, doveo je do petodnevnog prekida rada sistema, što je onemogućilo korisnicima pristup internet stranici i aplikaciji.

Prema informacijama iz kompanije, napadači su imali pristup mreži između 20. i 22. septembra, tokom čega su ukrali osjetljive podatke, kao što su imena, kontakt informacije (brojevi telefona, adrese elektronske pošte), datumi rođenja, brojevi socijalnog osiguranja kao i kopije identifikacionih dokumenata. Pored toga, ukradeni su i brojevi bankovnih računa, informacije o MoneyGram Plus Rewards programu i podaci o transakcijama.

Kompanija je pokrenula istragu uz pomoć vodećih stručnjaka za sajber bezbjednost i saradnju sa relevantnim vlastima kako bi utvrdila razmjere štete i broj pogođenih korisnika.

## Novi zakon EU nameće stroge zahtjeve za sajber bezbjednost povezanih i IoT uređaja

Savjet EU je usvojio Zakon o sajber otpornosti, koji zahtijeva da proizvođači primijene sigurnosne mjere za povezane uređaje prije nego što stignu do potrošača. Cilj je unaprijediti sajber bezbjednost proizvoda poput pametnih televizora, kućnih aparata, kamera, zvona i termostata, prije nego što se nađu na tržištu. Novi propisi će se primjenjivati na sve IoT uređaje kroz cijeli njihov razvojni ciklus – od dizajna do distribucije, uključujući hardver i softver. Trenutno, proizvodi proizvedeni i distribuirani unutar Evropskog ekonomskog prostora (EEA) nose oznaku "CE" (Conformité Européenne), koja potvrđuje da ispunjavaju visoke standarde sigurnosti, zdravlja i ekološke zaštite EU.

Po stupanju na snagu, što će se dogoditi 20 dana nakon potpisivanja zakona, očekuje se da će biti potrebno do tri godine za njegovu punu primjenu i sprovođenje.

Ovaj zakon nadopunjuje postojeći sajber bezbjednosni okvir EU, koji uključuje niz zakona, kao što su NIS direktive 1 i 2 i Zakon o sajber bezbjednosti EU.

## Troškovi ransomware napada naglo rastu u 2024. godini

Ransomware napadi su porasli za 68% u prvoj polovini 2024. u poređenju sa prethodnih šest mjeseci, prema izvještaju Osiguravajućeg društva za sajber rizike Coalition.

U SAD-u su napadi ostali stabilni, dok je Kanada zabilježila rast od 34%. Posebno su se izdvojili ransomware varijanti Play i BlackSuit, sa otkupninama od 4,3 miliona i 2,5 miliona dolara.

Ransomware je sezonski napad, s padom tokom ljeta i rastom tokom zimskih praznika, jer napadači ciljaju vrijeme kada preduzeća sporije reaguju.

Napadači sve češće ciljaju izložene login panele, što je utrostručilo vjerovatnoću sajber incidenata. Coalition preporučuje primjenu multifaktorske autentifikacije i redovno ažuriranje firmware-a kako bi se preduzeća zaštitila.


# OPREZ! Pojavila se lažna „Temu“ aplikacija

**Kako funkcioniše prevara?**

– Aplikacija izgleda identično kao originalna „Temu“ aplikacija, sa istim logotipom i sličnim korisničkim interfejsom.

– Lažna aplikacija upućuje korisnike na lažne sajtove i traži ažuriranje podataka, uključujući informacije o platnim karticama (broj kartice, CVV kod).

– Uneseni podaci se prenose prevarantima i mogu se zloupotrebljavati za neovlašćene transakcije i krađu identiteta.

**Kako da se zaštitite?**

– Preuzimajte aplikacije isključivo sa zvaničnih izvora (App Store i Google Play), a posebno provjerite ime izdavača. Originalnu „Temu“ aplikaciju izdaje „Temu International LLC“.

– Na originalnoj „Temu“ aplikaciji nalazi se obavještenje da aplikacija nikada neće tražiti dodatne podatke putem SMS-a.

– Pročitajte komentare i ocjene korisnika prije instalacije. Ne unosite podatke o kartici u aplikacije koje nisu provjerene. Redovno pratite stanje na računu i prijavite svaku sumnjivu transakciju svojoj banci.

– Koristite antivirusne aplikacije koje mogu detektovati sumnjive softvere.

**Šta učiniti ako ste već preuzeli lažnu aplikaciju?**

– Odmah uklonite aplikaciju sa uređaja. Blokirajte svoju karticu i obavijestite banku o mogućoj zloupotrebi.

– Promijenite lozinke za sve relevantne naloge koje ste koristili u aplikaciji.

– Budite oprezni i informisani – prevaranti svakodnevno traže nove načine za krađu podataka i zloupotrebu vašeg povjerenja.


## Hakerski napad na LEGO internet stranicu: pokušaj prevare s kriptovalutama

Kripto prevaranti su 5. oktobra 2024. godine nakratko hakovali zvaničnu stranicu LEGO kompanije, zamijenivši glavni baner reklamom za lažni LEGO token. Link „Kupi odmah“ je vodio posjetioce na platformu Uniswap gdje su prevareni korisnici mogli da kupe lažne LEGO tokene koristeći Ethereum.

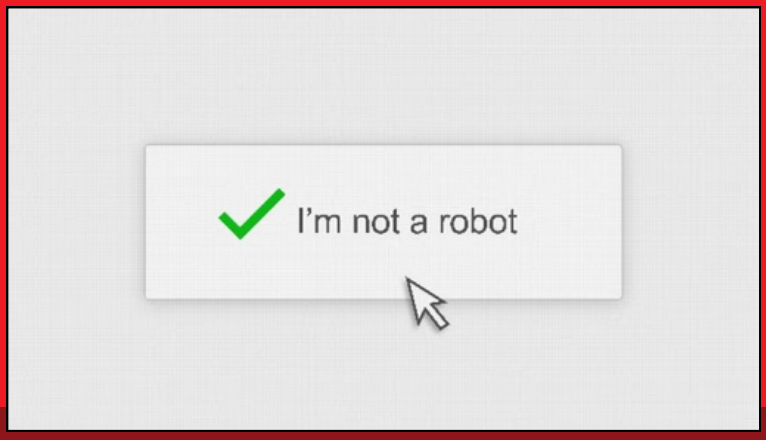
LEGO je brzo reagovao i uklonio lažni baner, ističući da nijedan korisnički nalog nije bio ugrožen i da su preduzeli mjere kako bi spriječili buduće slične napade.

## Krađa lozinki i novca putem lažne captcha verifikacije

Napadači su osmislili inovativnu strategiju za prevaru, koristeći lažne stranice za captcha verifikaciju koje izgledaju kao legitimne internet stranice. Ova taktika posebno ugrožava korisnike Windows operativnog sistema, koji mogu biti prevareni da aktiviraju malicioznu PowerShell skriptu. Kada je uređaj zaražen, napadači stiču pristup osjetljivim informacijama, uključujući lozinke, podatke iz kripto novčanika i druge lične podatke.

Captcha verifikacija, koja služi za razlikovanje ljudi od botova, obično zahtijeva da korisnici riješe jednostavne matematičke probleme ili izaberu određene fotografije. Ubjeđujući žrtve da pokrenu ovu skriptu, napadači preuzimaju kontrolu nad uređajem i instaliraju malver poznat kao Lumma Stealer.

Lumma Stealer funkcioniše kao „malver kao usluga“ (MaaS) od avgusta 2022. godine, fokusirajući se na krađu informacija iz web pregledača, uključujući lozinke, kolačiće i druge osjetljive podatke.




## Kada hakeri najčešće napadaju?

Većina ransomware napada dešava se između 1 i 5 sati ujutru, kako bi timovi za sajber bezbjednost bili zatečeni nespremni. Ove informacije dolaze iz Izvještaja o ransomware-u za 2024. godinu kompanije Malwarebytes, zasnovanog na podacima prikupljenim kroz aktivnosti na otkrivanju prijetnji i reagovanju na incidente.

Malwarebytes navodi da se ransomware napadi sada odvijaju mnogo brže – često su završeni u roku od nekoliko sati, dok su ranije trajali nedjeljama.

Najviše napada zabilježeno je u SAD (63%) i Velikoj Britaniji (67%), sa značajnim porastom. Takođe, udio manjih kriminalnih grupa porastao je sa 25% na 31%, što ukazuje na rastuću dostupnost ransomware alata.

## Ako je vaš PIN na ovom spisku kombinacija, bolje je da ga što prije promijenite

Autor istraživanja, Nik Beri iz kompanije Data Genetics, otkriva da je najčešći PIN na svijetu i dalje „1234“. Međutim, postoje i druge kombinacije koje su laka meta.

Sajber kriminalci imaju težak zadatak kada žele da opljačkaju nekoga i otkriju njegov PIN ali osobe koji koriste ove uobičajene kombinacije olakšavaju im posao.

Kako Beri ističe, dobro je poznato da nije pametno koristiti datume rođenja ili iste četiri cifre kao PIN kombinacije.

### Najčešće kombinacije PIN-a

Za istraživanje je korišćeno 3,4 miliona PIN kombinacija pronađenih na različitim forumima nakon hakerskih napada. “1234“ je najčešći PIN, koji se pojavljuje u 11% svih kombinacija. Zatim „1111“, „0000“ i „1212“. Prvih 10 takođe popunjavaju sledeće kombinacije – „7777“, „1004“, „2000“, „4444“, „2222“ i „6969“.

### Najrjeđe kombinacije PIN-a

Prema spisku najrjeđe korišćenih kombinacija „8068“ je korišćena samo u 25 od 3,4 miliona analiziranih slučajeva. Ostale rijetke kombinacije uključuju: „8093“, „8398“, „7638“, „8428“ i „8285“.

Stručnjaci za sajber bezbjednost savjetuju da periodično mijenjate PIN kako biste smanjili mogućnost zloupotrebe.

CIRT (eng. Computer Incident Response Team) je u skladu sa Zakonom o tajnosti podataka i Zakonom o informacionoj bezbjednosti zadužen za odgovor na računarsko bezbjednosne incidente u sajber prostoru Crne Gore.

Osnovan je 2012. godine kao dio zajedničkog projekta Vlade Crne Gore i Međunarodne telekomunikacione unije (ITU).

Od svog početka do danas uspješno je riješio ili pomogao rješavanju velikog broja računarskih incidenata koji su imali nacionalni ili međunarodni karakter.