CIRT.ME

03/2024

SAJBER BILTEN

TOP VIJESTI

Otkriven novi malver za bankomate u Evropi

Ransomver napad na bolnice u Londonu

Lažne AI alatke kradu lozinke

Google Password Manager sada dozvoljava korisnicima da bezbjedno dijele lozinke sa članovima porodice

Nova funkcija dijeljenja lozinki primjenjuje se na lozinke koje se čuvaju u Google Password Manager-u koji čuva lozinke i pristupne ključeve u Chrome-u i Android-u i povezan je sa Google nalogom.
Funkcija dijeljenja lozinke radi na mobilnim uređajima ali trenutno ne i u Chrome-u na računarima. Kada podijelite lozinku sa nekim od članova porodice, njena kopija će biti sačuvana u Google menadžeru lozinki tog člana.
Ovu funkciju ne možete da koristite sa ljudima koji nisu u vašoj porodičnoj grupi koju je odobrio Google a koja može da ima najviše šest ljudi.

Hakovani TikTok nalozi

Nedavno su napadači iskoristili ranjivosti nultog dana kako bi kompromitovali više naloga na TikTok-u, uključujući i naloge poznatih ličnosti i kompanija poput Sony, CNN-a i Paris Hilton. Napadači su hakovali naloge preko DM-a, a potrebno je bilo samo da korisnik otvori poruku.

Nalozi su na kraju morali biti uklonjeni da bi se spriječila zloupotreba, a TikTok je ispravio bezbjednosne greške koje su omogućavale napadačima da zaobiđu zaštitu privatnosti platforme i iskoriste ranjivost nultog dana.

EU traži načine rješavanja zavisnosti od društvenih mreža

Evropske institucije proteklih godinu dana su se bavile pitanjem zavisnosti od društvenih mreža, pri čemu su regulatori EU prošloga mjeseca otvorili istragu protiv Mete.

Za „velike platforme“ predviđena je kazna do šest odsto globalnih prihoda u slučaju nepoštovanja odredbi Zakona o digitalnim uslugama. Meta je odbacila optužbe, istaknuvši da kompanija već „deset godina razvija više od 50 alata i politika“ za zaštitu maloljetnih korisnika.

Ransomver napad na bolnice u Londonu

Britanski zdravstveni sistem je ponovo pogođen ransomver napadom, ovaj put usmjeren na dijagnostički centar Synnovis koji pruža laboratorijske usluge patologije za nekoliko bolnica koje vodi Nacionalna zdravstvena služba (NHS).

Incident je označen kao „kritični" i imao je veliki uticaj na usluge, posebno na transfuziju krvi i operacije. Napad je doveo do znatnih prekida u zdravstvenim uslugama kod više NHS bolnica pa su sve procedure i operacije otkazane ili preusmjerene na drugo mjesto.

Britanski zdravstveni sistem je pogođen i ranije napadom ransomvera 2017. godine, kada je zamrznuo računare u bolnicama širom zemlje.

Otkriven novi malver za bankomate u Evropi

Sajber kriminalci su razvili novi malver za bankomate u Evropi, koji se prodaje na jednom hakerskom forumu pod nazivom „EU ATM Malware". Ovaj malver navodno može kompromitovati bankomate u Evropi, odnosno 60% bankomata širom svijeta.

Napadi se vrše tako što napadači instaliraju malver na računaru bankomata, često preko USB porta.

Iako tvrdnje o novom malveru još nisu potvrđene, ukoliko su istinite, mogle bi predstavljati značajnu prijetnju za globalnu bankarsku industriju. Slična situacija se dogodila 2017. godine, kada je malver „Cutlet Maker" doveo do niza napada u Njemačkoj, koji su kradljivcima sa minimalnim tehničkim vještinama donijeli više od milion i po eura.

Otkriveni podaci miliona korisnika Alibaba platforme

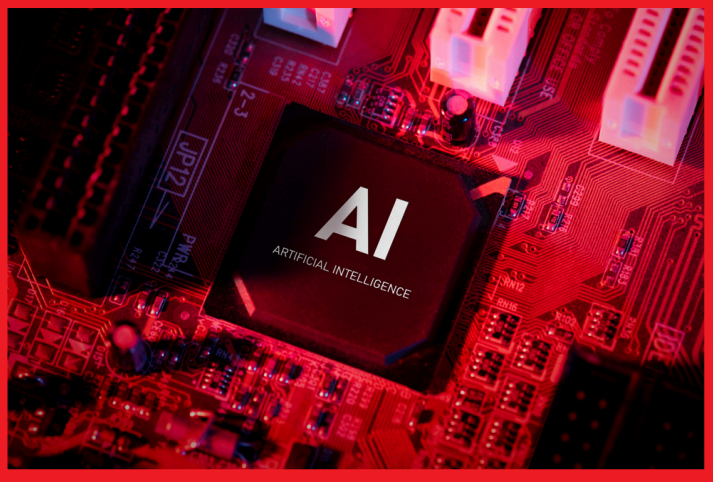
Brojevi telefona, kućne adrese i druge lične informacije miliona korisnika otkriveni su na Taobao-u, platformi koja je u vlasništvu tehnološkog giganta Alibaba. Podaci miliona korisnika su vjerovatno bili izloženi nakon što su istraživači otkrili nezaštićeni Elasticsearch klaster sa javno dostupnim podacima korisnika. Prema Taobao-u, analiza kompanije nije ukazala na bilo kakve curenja podataka.

Lažne AI alatke kradu lozinke

Otkriven je zlonamjerni softver koji koristi rastuću popularnost AI alata pod maskom AI generatora glasa.

Preuzimanje aplikacije koja oponaša popularne AI generatore glasa omogućava sajber kriminalcima da kradu različite vrste podataka, rudare kriptovalute i preuzimaju dodatni zlonamjerni softver. ž

Nakon što korisnik klikne na "Instaliraj", počinje instalacija legitimnih aplikacija, ali u pozadini skripta izvršava zlonamjerne aktivnosti. Tokom instalacije, Gipy preuzima i pokreće zlonamjerni softver treće strane sa GitHub-a upakovanog u ZIP arhivu zaštićenu lozinkom.



Još 2020. godine, detalji 1,1 milijarde korisnika platforme ilegalno su pribavljeni od strane marketing konsultanta koji je koristio softver za web scraping.
Prevaranti bi mogli iskoristiti izložene informacije za krađu identiteta, fišing napade ili druge prevare dok se lične informacije kao što su imena, brojevi telefona i adrese mogu iskoristiti za zlonamjerne svrhe uključujući prevaru sa identitetom i slanje neželjene pošte.
Taobao je među najvećim e-trgovinskim platformama sa 895 miliona aktivnih korisnika. Kancelarija trgovinskog predstavnika Sjedinjenih Američkih Država je 2022.godine dodala Taobao na listu Ozloglašenih tržišta za falsifikovanje i pirateriju.

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.