CIRT.ME

SAJBER BILTEN

02/2024

TOP VIJESTI

Hakovan Dropbox sign

„Zaraženi“ antivirus

U Velikoj Britaniji stupio na snagu **„Zakon o bezbjednosti proizvoda i telekomunikacionoj infrastrukturi”** koji zabranjuje korišćenje slabih lozinki na pametnim uređajima.

U Velikoj Britaniji stupio na snagu „Zakon o bezbjednosti proizvoda i telekomunikacionoj infrastrukturi”

Nacionalni centar za sajber bezbjednost Velike Britanije pozvao je proizvođače pametnih uređaja da se pridržavaju zakona koji zabranjuje korišćenje lozinki kao što su „123456” ili „admin” za uređaje povezane na internet.

Kompanije koje se ne pridržavaju odredbi mogu biti kažnjene kaznama do 10 miliona funti ili sa 4% njihovih globalnih godišnjih prihoda.

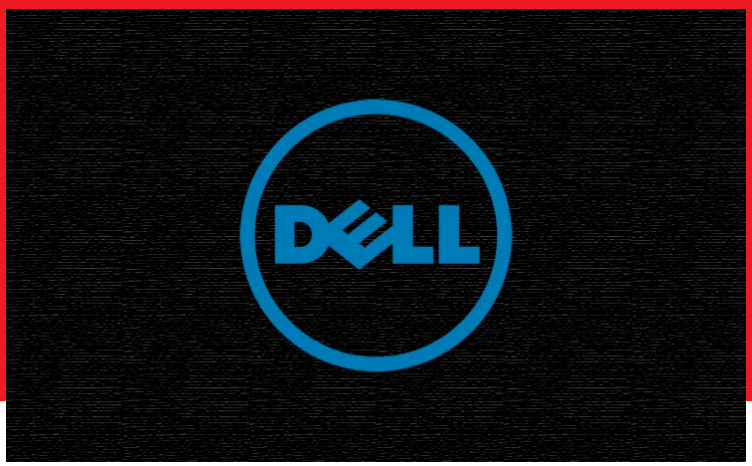
Ovim zakonom se nastoje uvesti minimalni bezbjednosni standardi kako bi se spriječilo da ranjivi uređaji budu hakovani i iskorišćeni za masovne napade.

Hakovan Dropbox Sign

Dropbox, popularna usluga za dijeljenje fajlova, objavila je da je elektronski potpisni servis Dropbox Sign hakovan i da su korisnički podaci otkriveni.

Šta treba da uradite? Dropbox je resetovao lozinke za sve naloge tako da ćete morati da generišete novu lozinku. Pošto su tokeni za dvofaktorsku autentifikaciju ukradeni, trebalo bi i njih resetovati.

Za one koji koriste SMS 2FA, resetovanje je automatsko dok oni koji koriste aplikaciju, moraće to sami da urade.



Napadači ukrali podatke o 49 miliona kupaca

IT kompanija DELL objavila je da su hakeri ukrali podatke o 49 miliona kupaca koje uključuju ime, adresu stanovanja, informacije o Dell-ovom hardveru i porudžbinama, uključujući servisnu oznaku, opis proizvoda, datum porudžbine i informacije o garanciji. Kompanija ističe da ukradene informacije ne uključuju podatke o plaćanju, adrese elektronske pošte ni brojeve telefona.

Ukoliko ste kupili bilo šta od Dell opreme budite oprezni sa elektronskom poštom u kojoj se od vas traži da instalirate softver, promijenite lozinke ili izvršite neke druge potencijalno rizične radnje.

Posljedice ruskih i kineskih upada u Microsoft

Agencije za sajber sigurnost pod nadzorom Bijele kuće uputile su niz kritika i upozorenja na račun Microsofta, kazavši da su hakeri povezani s Moskvom i Pekingom uspjeli iskoristiti propuste u sistemima te kompanije, pogotovo one vezane za elektronsku poštu, što im je omogućilo krađu dokumenata i podataka američkih zvaničnika.

Microsoft ima partnere i korisnike širom svijeta, što potencijalno predstavlja „ rupe" u sigurnosnom sistemu. Takođe, partneri s raznim privilegijama mogu biti „kapija" kojom se zlonamjerne osobe potencijalno mogu „uvući" dublje u sistem.

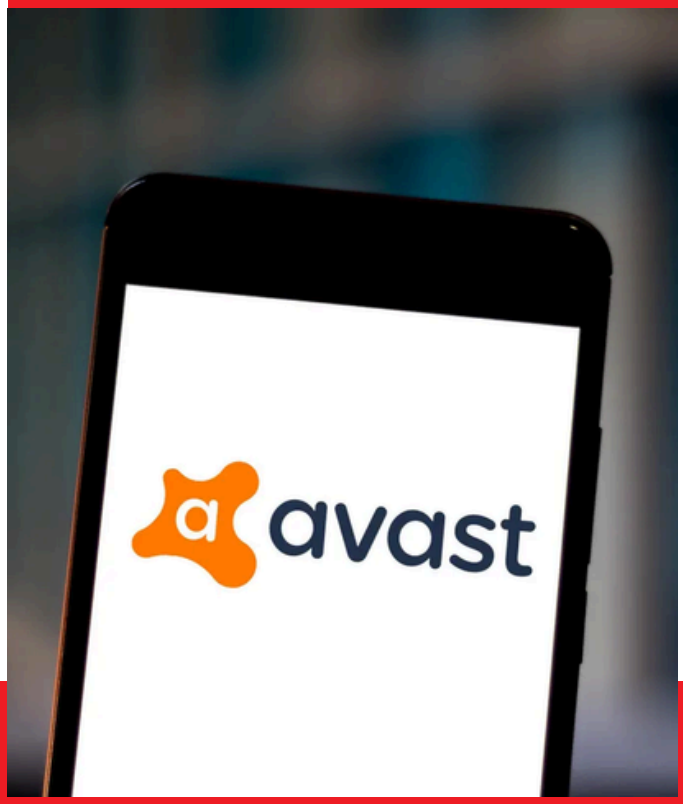
Microsoft bi mogao biti optužen za neki vid saučesništva, ako se ispostavi da su znali za upade, a da o tome nisu obavijestili relevantne agencije u zemljama u kojim nudi usluge.

„Zaraženi" antivirus

U novom izvještaju kompanije Avast stoji da su hakeri koristili ranjivosti u antivirus programu, i zatim su u njega ubacili zlonamjerni softver po imenu GuptiMiner. Nakon što su ostvarili poziciju koju su htjeli, hakeri su uspjeli da zaraze ažuriranje antivirusa, i da postave malver.

Avast je ovaj napad pripisao hakerskoj grupi iz Sjeverne Koreje pod nazivom Kimsuki, jer je GuptiMiner prilično sličan „keyloggeru" koji koristi ova grupacija. Takođe, u oba slučaja je korišćen domen mygamesonline[.]org.

Meta ovog napada su velike korporacije, a eScan je, kako je saopštio, „zakrpio" rupu kroz koju je prolazio hakerski napad, i preporučuju svim korisnicima da ažuriraju program.



Fišing napadi putem Autodesk Drive platforme

Napadači su preuzeli korišćenje kompromitovanih naloga kako bi slali fišing poruke postojećim kontaktima, prateći sofisticiranu strategiju koja im omogućava da poruke izgledaju autentično. U samom sadržaju poruka, uključuju zlonamjerni PDF dokument hostovan na platformi za dijeljenje podataka Autodesk Drive. Ova strategija dodatno povećava nivo legitimnosti jer poruke sadrže ime pošiljaoca i ime njegove kompanije.

AUTODESK

Novi bankarski malver daje hakerima potpunu kontrolu nad Android telefonima

Analitičari ThreatFabric-a otkrili su trojanca *Brokewell-a*, upozoravajući da predstavlja značajnu prijetnju za bankarsku industriju i korisnike jer omogućava napadačima da daljinski pristupe svim sredstvima dostupnim putem bankarskih aplikacija.

„Brokewell je tipičan savremeni bankarski malver opremljen kako krađom podataka tako i mogućnostima daljinskog upravljača ugrađenim u malver", navode istraživači u izvještaju.

Novi malver je prvi put primijećen kao ažuriranje pregledača - uobičajena metoda koju koriste sajber kriminalci kako bi namamili žrtve da kliknu na zlonamjerne linkove.

Trojanac putem zaraženog telefona prikuplja korisničke akreditive i druge unose. Pored toga, krade kolačiće i šalje ih na komandno-kontrolni server. Brokewell je opremljen „evidentiranjem pristupačnosti", hvatajući svaki događaj koji se dešava na uređaju: dodire, brzo prevlačenje, prikazane informacije, unos teksta i otvorene aplikacije. Brokewell je primijećen kako cilja popularne aplikacije za finansijske usluge „kupi odmah, plati kasnije" i austrijsku aplikaciju za digitalnu autentifikaciju.

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.