CIRT.ME

2024

SAJBER BILTEN

05/24

Top vijesti

Dječije igrice kao mamac

Google briše neaktivne Gmail naloge

Kritične ranjivosti pronađene u Photoshopu, Premiere Pro i više drugih Adobe proizvoda

Australija zabranjuje djeci korišćenje društvenih mreža

Australija planira da uvede starosno ograničenje za djecu koja koriste društvene mreža, zbog zabrinutosti za njihovo mentalno i fizičko zdravlje.

Usvajanje zakona učiniće Australiju jednom od prvih zemlja na svijetu koje će uvesti starosno ograničenje za korišćenje društvenih mreža.

Fejsbuk i Instagram, koji su samoinicijativno uveli minimalno starosno ograničenje na 13 godina, saopštili su da žele da osnaže mlade ljude da imaju koristi od njihovih platformi umjesto da im potpuno onemoguće pristup.

Prema podacima IT industrije Australija je jedna od država sa najvećom onlajn populacijom, sa četiri petine od 26 miliona stanovnika koristi društvene mreže.

Dječje igrice kao mamac

Kompanija Kaspersky je otkrila više od 6,6 miliona pokušaja napada koje se skrivaju iza popularnih video igara. Većina napada se odnosila na video igre Minecraft, Roblox i Among Us.

Sajber kriminalci su vjerovatno izabrali ovaj metod napada na osnovu popularnosti igara, kao i sposobnosti gejmera da koriste lozinke i modove. Jedna od najčešćih prevara u igrama je ponuda za nove skinove, tj. odjeću ili oklop za heroja koji mu poboljšavaju vještine.

Kompanija Kaspersky roditeljima preporučuje da prate ove smjernice, kako bi zaštitili svoju djecu od prevara:

- Njegujte otvorenu komunikaciju sa djecom o potencijalnim rizicima na mreži.
- Pomozite djetetu da odabere jedinstvenu lozinku i trudite se da je periodično mijenjate.
- Postavite jasna pravila o tome šta mogu, a šta ne mogu da rade na mreži.
- Da biste zaštitili djecu od preuzimanja zlonamjernih datoteka, instalirajte im pouzdano bezbjednosno rješenje, koje neometano radi sa Steam-om i drugim uslugama za igre.

Nove Chrome funkcije povećavaju sigurnost i kontrolu nad ličnim podacima

Nova opcija "Safety Check" automatski će obavještavati korisnike o prekomjernim dozvolama za sajtove koje više ne posjećuju, označavati neželjena obavještenja i upozoravati na sigurnosne probleme. Na desktop verziji Chrome-a, Safety Check će takođe upozoriti ako instalirane ekstenzije predstavljaju sigurnosni rizik i pomoći u njihovom uklanjanju.
Na Pixel uređajima, novo dugme „Unsubscribe" olakšaće odjavu od neželjenih obavještenja, dok će na Android uređajima biti dostupna opcija za privremeno davanje dozvola sajtovima, koje će se automatski opozvati nakon napuštanja sajta.

Google briše neaktivne Gmail naloge

Prema saopštenju tehnološkog giganta, od 20. septembra svi nalozi koji nisu aktivni mogli bi biti obrisani, a njihovi vlasnici mogu izgubiti pristup važnim podacima kao što su mejlovi, fotografije i dokumenti (uključujući sadržaje na Gmail-u, Google Docs-u i Google Photos-u).

Ako imate više Google naloga, potrebno je da na svakom uradite jednu od sledećih stvari: pročitate ili pošaljete mejl, podijelite fotografiju, gledate YouTube dok ste prijavljeni, ili koristite Google Drive ili Google Search.

Ako obavite bilo koju od ovih aktivnosti, vaš nalog će se smatrati aktivnim i neće biti obrisan. Dovoljno je da to učinite jednom godišnje.

Novi malver „Voldemort" koristi Google Sheets za sajber špijunažu

Napadači koji se predstavljaju kao poreski organi iz Evrope, Azije i SAD-a, su napali preko 70 organizacija koristeći malver Voldemort, koji prikuplja informacije i isporučuje druge malvere.

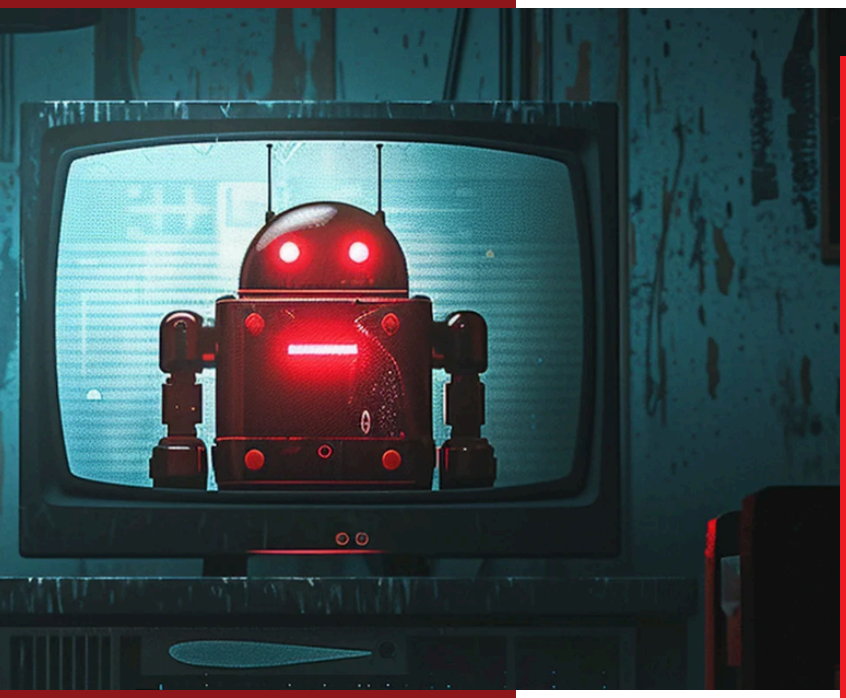
Ciljani sektori uključuju osiguranje, vazduhoplovstvo, transport, finansije, tehnologiju i zdravstvo. U napadu je poslato 20.000 emailova koji upozoravaju na promjene u poreskim prijavama i preusmeravaju žrtve na lažne stranice. Voldemort se koristi za prikupljanje informacija i učitavanje dodatnih malvera, uz korišćenje Google tabela za C2, eksfiltraciju podataka i izvršavanje komandi.

Kritične ranjivosti pronađene u Photoshopu, Premiere Pro i više drugih Adobe proizvoda

Osam Adobe proizvoda – Photoshop, Illustrator, Premiere Pro, After Effects, ColdFusion, Acrobat Reader, Audition i Media Encoder – nedavno je dobilo zakrpe za kritične, važne i umjerene bezbjednosne ranjivosti.

Američka agencija za sajber bezbjednost i sigurnost infrastrukture (CISA) upozorava da bi akteri sajber prijetnji mogli iskoristiti neke od ranjivosti kako bi preuzeli kontrolu nad pogođenim sistemima i poziva korisnike da primijene neophodna ažuriranja.

- **Photoshop:** Kritična ranjivost (7.8/10) i *out-of-bounds read* ranjivost mogu dovesti do pokretanja proizvoljnog koda i curenja memorije. Pogođene verzije su 2023 i 2024.
- **ColdFusion:** Kritična ranjivost (9.8/10) omogućava pokretanje proizvoljnog koda. Pogođene verzije su 2023 i 2021.
- **Acrobat i Reader:** Dvije kritične ranjivosti (7.8 i 8.6/10) omogućavaju daljinsko izvršavanje koda.
- **Illustrator:** Šest ranjivosti, četiri kritične (7.8/10), uključuju proizvoljno izvršavanje koda i curenje memorije. Pogođene verzije su 2023 i 2024.
- **Premiere Pro:** Kritična ranjivost (7.8/10) i umjerena ranjivost uzrokuju proizvoljno izvršenje koda i curenje memorije.
- **After Effects:** Pet ranjivosti, tri kritične (7.8/10), omogućavaju proizvoljno izvršenje koda.
- **Audition i Media Encoder:** Ranjivosti dovode do curenja memorije i proizvoljnog izvršavanja koda.



1,3 Miliona Android TV Kutija zaraženo Vo1d Malverom

Novi Android malver pod nazivom Vo1d inficirao je oko 1,3 miliona TV kutija koje koriste starije verzije operativnog sistema, upozorava Doctor Web.

Vo1d je sofisticirani backdoor malver koji može preuzeti i instalirati dodatni softver na osnovu komandi sa svog C&C servera.
Ovaj malver se skriva u sistemskoj memoriji kao legitimni dio operativnog sistema i koristi različite tehnike kako bi osigurao automatsko pokretanje prilikom restartovanja uređaja. Zaraženi uređaji su prisutni u 197 zemalja, pri čemu je Brazil najviše pogođen.
Vo1d se fokusira na starije verzije Androida zbog njihovih nepopravljenih ranjivosti. Mogući izvori infekcije uključuju ranjivosti u operativnom sistemu i korišćenje neovlašćenih verzija firmvera.

Kompromitovani podaci u Fortinetu

Fortinet je potvrdio da je došlo do narušavanja podataka nakon što je napadač pod nadimkom „Fortibitch“ objavio da je ukrao 440 GB podataka sa SharePoint instance na Azure platformi. Napadač je zatražio otkup, ali nakon što Fortinet nije pristao, omogućio je pristup ukradenim podacima putem AWS S3 bucket-a.

Kompanija je saopštila da je kompromitovan samo mali broj datoteka, što se odnosi na manje od 0,3% njihovih klijenata. Fortinet je naglasio da ovaj incident nije uticao na njihove operacije, proizvode ili usluge, te da nema dokaza o neovlašćenom pristupu drugim resursima.

Postoji li i dalje digitalna privatnost?

Dani kada je bilo dovoljno imati antivirus i izbjegavati sumnjive internet stranice su prošlost. Hakerske grupe danas napadaju ne samo pojedince, već i cijele mreže. Prije mjesec dana, podaci preko 100 miliona korisnika „AT&T"-a procurili su na „Dark web". Hakeri su došli do mobilnih brojeva i poruka, a vjeruje se i do podataka o lokaciji tokom poziva.

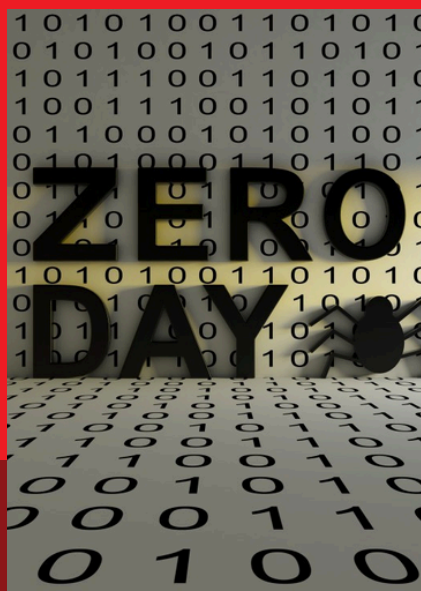
U februaru je napadnut veliki mobilni i internet operater „Verizon", pri čemu su ukradeni podaci 63 hiljade zaposlenih. Međutim, najnoviji napad na statističku ustanovu National Public Data ugrozio je podatke oko 1,5 miliona Amerikanaca, uključujući brojeve socijalnog osiguranja, adrese i e-mailove.

Hakerski napadi su svakodnevnica

FBI je nedavno upozorio na sve češće korišćenje AI alata u sajber napadima. Ovi alati su daleko napredniji od dosadašnjih, jer koriste vještačku inteligenciju za ubrzavanje i automatizaciju napada. Jedan od tih alata je GPT-J, koji može u realnom vremenu dopunjavati kompjuterski kod, omogućavajući hakerima pristup „zadnjim vratima" (backdoor). FreedomGPT je još jedan Ai model koji koriste ruske hakerske grupe, a koji je dizajniran da radi lokalno, bez povezivanja na Internet, čineći svoje aktivnosti skoro nemogućim za detekciju. Glavna osobina mu je da može samostalno da analizira kompjuterski kod bilo kog softvera, te da koristi tzv. DAN (Do Anything Now) komande za modifikaciju softvera ili iskorištavanje bezbjednosnih propusta.

Pronalaženje 'propusta nultog dana'

Međunarodna koalicija obavještajnih agencija iz nekoliko zemalja upozorila je na aktivnosti kineske hakerske grupe „Kryptonite Panda" (APT-40), specijalizovane za pronalaženje „zero day" propusta u softverima i prikupljanje podataka sa društvenih mreža.
Poslednjih par godina su naročito fokusirani i na pronalaženju propusta u popularnom setu softverskih rešenja Microsoft Exchange. Nacionalni centar za sajber bezbjednost agencije FBI navodi da je ova grupa posljednjih godina fokusirana na propuste u Microsoft Exchange softveru i Log4J, koji se koristi na serverima velikih kompanija kao što su Netflix, IBM i NASA.



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.