

# BULETINI JAVOR

## 25-29 DHJETOR 2023



Shprehja

"Ajo që hakerët bëjnë është të hulumtojnë teknologjinë dhe të eksperimentojnë me të në mënyra që shumë njerëz nuk e imagjinojnë kurrë."

Emmanuel Goldstein

e javës

Përmbajtja:

- Një malware i ri synon pajisjet Android
- Mint mobile - data breach
- GitHub paralajmëron përdoruesit që të aktivizojnë 2FA përpara afatit të caktuar
- Sulmuesit spyware anashkalojnë mbrojtjen e kujtesës së iPhone



### Një malware i ri synon pajisjet Android

Ekspertët e sigurisë kibernetike në McAfee kanë zbuluar një lloj të ri malware të identifikuar si Xamalicious, i cili synon pajisjet Android.

McAfee njofton se ky malware u gjet në 25 aplikacione dhe vlerësoi se aplikacionet ishin instaluar në të paktën 327,000 raste.

Shumica e rasteve janë raportuar në Brazil, Argjentinë, SHBA, MB, Australi, Meksikë dhe pjesë të Evropës.

[Lexo më shumë](#)



### Mint mobile - data breach

Mint Mobile, një operator i rrjetit virtual celular (MVNO), ka njoftuar klientët për një incident sigurie në të cilin një sulmues mori informacionin e tyre personal.

Të dhënat e klientëve përfshijnë emrat, numrat e telefonit, numrin serial të SIM dhe një përshkrim të shkurtër të planit të shërbimit të blerë.

[Lexo më shumë](#)



### GitHub paralajmëron përdoruesit që të aktivizojnë 2FA përpara afatit të caktuar

GitHub po paralajmëron përdoruesit se së shpejti do të kenë funksionalitet të kufizuar në faqe nëse nuk aktivizojnë autentifikimin me dy faktorë (2FA) në llogaritë e tyre deri në datën 19 Janar.

Kompania e ka marrë këtë vendim për të mbrojtur llogaritë e përdoruesve nga shkelja e të dhënave dhe ndryshimi i kodit në sulmet e zinxhirit të furnizimit. Nëse përdoruesit nuk e kanë konfiguruar 2FA deri në afatin e caktuar, do kenë akses të kufizuar në llogarinë e tyre.

[Lexo më shumë](#)



### Sulmuesit spyware anashkalojnë mbrojtjen e kujtesës së iPhone

Sulmet e Operacionit "Triangulation" po abuzojnë me funksionet e padokumentuara në Apple për të anashkaluar masat e sigurisë.

Një veçori e hardware-it të padokumentuar më parë brenda sistemit iPhone të Apple lejon shfrytëzimin e vulnerabiliteteve të shumta, duke i lënë përfundimisht sulmuesit të anashkalojnë mbrojtjen e kujtesës të bazuar në hardware.

[Lexo më shumë](#)