

BULETIN I LAJMEVE TË SIGURISË KIBERNETIKE



Gusht 2023

Përmbajtja:

- Takimi zyrtarë i Ambasadores së Izraelit me Autoritetin Kombëtarë për Certifikimin Elektronik dhe Sigurinë Kibernetike
- Google Workspace kërkon identifikimin e dy administratorëve gjatë ndryshimeve kritike.
- Zbulohet një malware i ri i identifikuar si WikiLoader
- Microsoft - patching alert



Takimi zyrtarë i Ambasadores së Izraelit me Autoritetin Kombëtarë për Certifikimin Elektronik dhe Sigurinë Kibernetike

Në datën 15 Gusht, Ambasadorja e Izraelit, znj. Galit Peleg, në kuadër të miqësisë dhe bashkëpunimit midis vendeve tona, zhvilloi një takim zyrtarë pranë Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike, ku u prit nga Drejtori i Përgjithshëm z. Iglj Tafa dhe stafi i Autoritetit. Në këtë takim u diskutua mbi mundësi bashkëpunimi midis institucioneve të dy vendeve, përfshirë edhe institucionet në fushën e sigurisë Kibernetike.

Znj. Ambasadore, shprehu vlerësimin dhe konsideratën për një zhvillim të madh që ka marrë Shqipëria në një kohë të shkurtër në sektorë të ndryshëm, përfshirë edhe fushën e Sigurisë Kibernetike. Drejtori i Autoritetit Z. Tafa, i shprehu Ambasadores falenderimet për mbështetjen e dhënë si dhe parashtrori sfidat dhe strategjinë institucionale e drejtuar për të mundur një rritje të nivelit të Sigurisë Kibernetike në vend.



Zbulohet një malware i ri i identifikuar si WikiLoader

Studiuesit e Proofpoint kanë identifikuar një malware të ri, të quajtur WikiLoaderi cili është zbuluar në të paktën tetë fushata që synojnë organizatat italiane që nga dhjetori 2022.

Këto fushata përdorën emailë që përmbajnë bashkëngjitjet e Microsoft Excel, bashkëngjitjet e Microsoft OneNote ose bashkëngjitjet PDF, duke shkaktuar shkarkimin e Trojanit *Ursnif* si një ngarkesë shtesë.

[Link: Lexo më shumë](#)

PATCHING ALERT



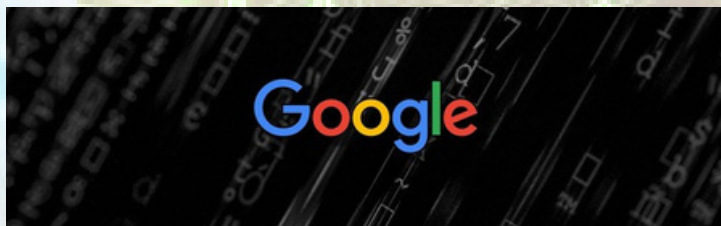
Microsoft lançon patche për 74 vulnerabilitete të reja në përditësimin e muajt Gusht.

Microsoft ka korrigjuar gjithsej 74 vulnerabilitete në softuerin e tij si pjesë e përditësimeve të kompanisë për muajin gusht 2023.

Kjo përfshin gjashtë vulnerabilitete kritike, 67 të rëndësishme dhe një vulnerabilitet me ashpërsi të moderuar. Lëshuar së bashku me përmirësimet e sigurisë janë edhe dy raporte me përditësime të thella (ADV230003) dhe (ADV230004).

Microsoft njoftoi se instalimi i përditësimit më të fundit "ndalon zinxhirin e sulmit" që çon në gabimin e ekzekutimit të kodit remote.

[Link: Lexo më shumë](#)



Google Workspace kërkon identifikimin e dy administratorëve gjatë ndryshimeve kritike.

Google njoftoi së fundmi kontrollë të reja të mbrojtjes së sigurisë kibernetike që do të lejojnë ekipet e sigurisë të pengojnë sulmet e inxhinierisë sociale të cilat synojnë përdoruesit e Workspace.

Google shpjegoi gjithashtu se si një malware Androidi mund të infektojë Google Play Store me ndihmën e një taktike të njohur si versionimi që u mundëson aktorëve keqdashës të shmangin kontrollet e sigurisë.

[Lexo më shumë](#)

BULETIN I LAJMEVE TË SIGURISË KIBERNETIKE



Përmbajtja:

- Siguria Kibernetike për bizneset.
- Këshilla sigurie për bizneset:

Siguria Kibernetike për bizneset.

"Një nga gabimet më të mëdha në bizneset e vogla është se punëdhënësit ose punonjësit nuk krijojnë dhe menaxhojnë fjalëkalimet siç duhet."

Scott Schober

Siguria kibernetike është bërë një domosdoshmëri për bizneset e të gjitha madhësive pasi sistemet dhe rrjetet e tyre që përmbajnë të dhëna të ndjeshme dhe të vlefshme, janë vënë nën kthetrat e aktorëve keqdashës.

Pa një strategji të sigurisë kibernetike, biznesi juaj nuk mund të mbrohet nga kërcënimet duke e lënë atë të pambrojtur ndaj aktorëve keqdashës, të cilët do ta identifikojnë biznesin tuaj si një objektiv të lehtë. Së bashku me mënyrën se si teknologjia ka evoluar gjatë viteve, ka pasur gjithashtu një rritje të qëndrueshme të rreziqeve ndaj bizneseve.



Këshilla sigurie për bizneset:

1. Sigurohuni t'i mbani fjalëkalime tuaja private



2. Mbroni të gjitha pajisjet tuaja me një program antivirusi

3. Mos hapni bashkëngjitjet në emaille të dyshimta . Tregohuni vigjilentë ndaj bashkëngjitjeve Word, Excel, PowerPoint ose PDF.



4. Aplikoni siguri shtesë në procesin tuaj të identifikimit, duke konfiguruar vërtetimin me shumë faktorë (MFA).