REPUBLIKA E SHQIPËRISË

AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Tiranë, më 13.02.2024

PËRDITËSIM MBI SITUATËN PAS SULMIT KIBERNETIK NË INSTAT

Më datë 1 shkurt 2024, Instituti i Statistikave u përball me një sulm kibernetik që synonte infrastrukturën e tij teknologjike.

Në momentin e parë që AKCESK u vu në dijeni të sulmit, angazhoi menjëherë ekipin e Analizës së Sigurisë Kibernetike për të ofruar ndihmë në parandalimin dhe rimëkëmbjen e sistemeve të kësaj infrastrukture. Në bashkëpunim të ngushtë me ekspertët e INSTAT, AKCESK ka drejtuar procesin për disa ditë radhazi për të zbardhur dhe neutralizuar sulmin.

Pas ndihmës së AKCESK në parandalimin e përshkallëzimit të sulmit, ekspertet tanë bënë një skanim total të gjithë serverëve për të identifikuar kërcënime të mundshme dhe për të rivendosur të dhënat në serverët e prekur. Në të njëjtën kohë, po punojmë edhe në bashkëpunim me aleatët ndërkombëtarë, të cilët kanë ofruar ndihmë për të adresuar këtë situatë të ndërlikuar.

AKCESK ka koordinuar në kohë reale punën me të gjitha infrastrukturat e tjera kritike dhe të rëndësishme të vendit, duke monitoruar situatën dhe duke shkëmbyer detaje nga sulmi. Si rezultat i këtij bashkëpunimi të gjithanshëm, është arritur të parandalohen sulme të ngjashme në infrastruktura kritike të vendit, në këtë vazhdë sulmesh kibernetike.

Nga analiza e zhvilluar deri tani, është konfirmuar se sulmuesit përdorën skedarin *MEK-DDMC.exe* për të ekzekutuar një virus me përmbajtje keqdashëse. Ky sulm i njohur si *Wiper (Fshirës)* kishte si qëllim fshirjen e të dhënave të sektorit *Boot* dhe prekjen e pajisjeve brenda *Active Directory (AD).*

Për hyrjen në sistem mendohet se është shfrytëzuar serveri *Exchange* për shkak të një versioni të pa përditësuar. Aktoret keqdashës arritën të tejkalonin privilegjet dhe të merrnin kontrollin e sistemit *Active Directory* dhe *"Data Protection Manager"*, duke shpërndarë virusin tek pajisjet dhe serverat në rrjet. Virusi i shpërndarë ka infektuar 40 kompjuterë, nga ku ka fshirë 6 prej tyre. Më pas virusi ka bërë fshirjen e serverit në të cilin kryheshin ekzekutimet e komandave. Pas kësaj, aktorët kanë humbur komunikimin me infrastrukturën.

Bazuar në informacionin e disponueshëm, aktorët që qëndrojnë pas këtij sulmi kibernetik janë identifikuar si "Homeland Justice", një grup sulmi i sponsorizuar nga shteti iranian që ka kryer tashmë sulme të tjera në të kaluarën.

Sulmi kibernetik ndaj INSTAT-it thekson rëndësinë e një përgjigjeje proaktive dhe strategjike ndaj kërcënimeve të sofistikuara kibernetike.

Adresa: Rruga “Papa Gjon Pali II”, Nr. 3, Kati 1, Tiranë;
Faqe web: www.cesk.gov.al E-mail: info@cesk.gov.al
Tel./Fax: 04 2221 039