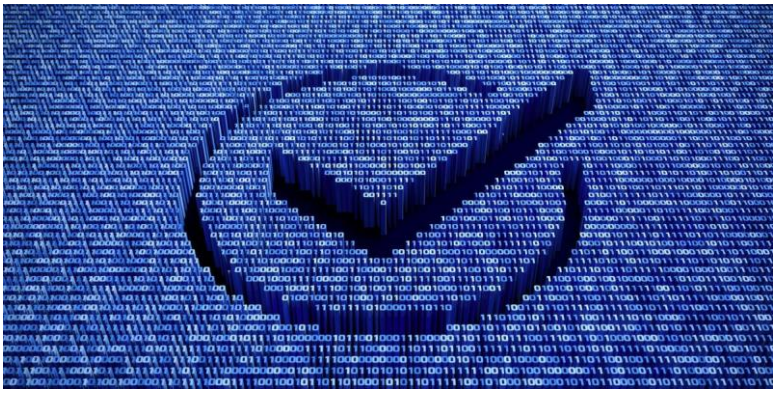
LAJME

RRITJA E AKTIVITETEVE NGA APT IRANIANE KËRKON VIGJILENCË TË SHTUAR!



Kohët e fundit është vënë re një rritje e aktivitetit nga APT Iraniane.

Pas sulmeve kibernetike të zbuluara në 17 Korrik 2022, Shqipëria u bë shteti i parë në botë që ndërpret marrëdhëniet diplomatike për shkak të një sulmi kibernetik! Në atë kohë, agjencitë e specializuara brenda vendit dhe partnerët strategjikë ndërkombëtarë adresuan dhe asistuan trajtimin e sulmit të sofistikuar, të orkestruar nga aktorë të sposorizuar nga Republika Islamike e Iranit.

Në shkurt 2022, CISA, Byroja Federale e Hetimit (FBI), U.S. Cyber Command Cyber National Mission Force' (CNMF) , Qendra Kombëtare e Sigurisë Kibernetike e Mbretërisë së Bashkuar (NCSC-UK) dhe Agjencia Kombëtare e Sigurisë (NSA) publikuan një deklaratë e përbashkët në lidhje me monitorimin ndaj APT MuddyWater të sponsorizuar nga qeveria iraniane - një APT iranian, i cili targetonte industrinë e mbrojtjes, naftës dhe gazit natyror, qeverinë lokale dhe industrinë e telekomunikacionit.

Taktikat dhe teknikat e aktivitetit APT analizohen nga artikulli: https://www.avertium.com/resources/threat-reports/iranian-cyber-threats-apt42-and-homeland

Sulmi që kishte synim shmangien e zbulimit dhe shkaktimin e dëmeve maksimale, analizohet gjithashtu në artikullin e mëposhtëm, duke konkluduar me këshilla për monitorimin e programeve të aksesimit remote, si dhe monitorimin e certifikatave të skaduara që mund të përdoren për ekzekutimin e malware-ve.

https://securelist.com/ransomware-and-wiper-signed-with-stolen-certificates/108350/

AKCESK, në cilësinë e Autoritetit përgjegjës për sigurinë kibernetike, rikujton operatorët e infrastrukturave kritike për rëndësinë e aplikimit të masave të sigurisë kibernetike dhe rritjen e vigjilencës ndaj këtyre sulmeve globale.

KONTAKT
Rr. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Albania 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al