BULETIN JAVOR
9-13 TETOR 2023

Shprehja e javës

"Teknologjia ashtu si arti është një trajnim i imagjinatës njerëzore."

Daniel Bell

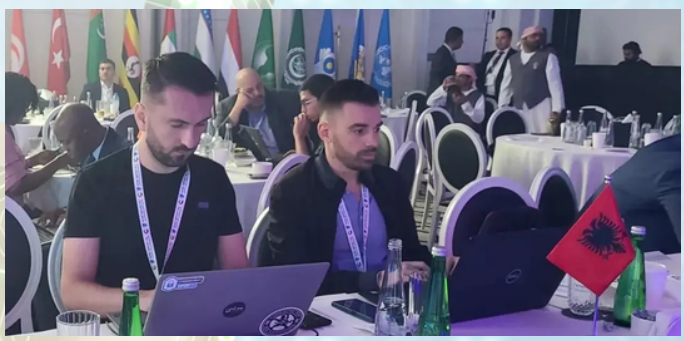
Përmbajtja:

- **Politikat e Sigurisë dhe Menaxhimi i Krizës për Sektorin e Shëndetësisë.**
- **AKCESK pjesmarrës në trajnimin Cyber Week Regional**

Politikat e Sigurisë dhe Menaxhimi i Krizës për Sektorin e Shëndetësisë.

Në kuadër të trajnimeve që do të organizohen nga AKCESK për periudhën Tetor-Dhjetor 2023, në datat 11-12 Tetor, u zhvillua trajnimi me temë *"Politikat e Sigurisë Kibernetike dhe Menaxhimi i Krizës "* për Sektorët e Shëndetësisë.

Gjatë këtij trajnimi dy ditor u bënë prezantime lidhur me Legjislacionin, Strategjinë, Politikat dhe nevojat mbi Qeverisjen Kibernetike, si dhe u zhvilluan 3 Table Top Exercises për menaxhimin e incidenteve dhe krizës Kibernetike, Simulimi i sulmit "Phishing" si dhe një rast skenari infektimi nga Malware (programe keqdashëse), gjithashtu u organizua një Cyber Drill ku kishte ushtrime konkrete mbi menaxhimin e incidenteve. Gjatë diskutimeve u theksua rëndësia e përmirësimit të koordinimit, bashkëpunimit dhe shkëmbimit të informacionit mbi kapacitetet analizuese dhe reaguese të subjekteve të sektorit shëndetësor lidhur me incidentet e sigurisë kibernetike.



AKCESK pjesmarrës në trajnimin Cyber Week Regional

AKCESK mori pjesë në Cyber Week Regional me ftesë nga Këshilli I Sigurisë Kibernetike të Emirateve të Bashkuara Arabe. Në dy ditët e para u organizua Cyber Drill (Stërvitje Kibernetike) ku kishte përfaqësues nga 70 kombe.

Përfaqësuesit e AKCESK përfaqësuan denjësisht Shqipërinë dhe u klasifikuan si vijon:

Skenari 1 – Log Analysis Web Apps hacked and Crypto mining : Vendi i parë nga 70 vende pjesmarrëse

Skenari 2 – Taktikat e Mbrojtjes për Sigurinë Kibernetike (Vendi I 12);
Skenari 3 – DFIR (Vendi I 9) ;
Skenari 4 – Cyber threat Intelligence (nuk kishte klasifikime) ;
Skenari 5 – CPX Ransomware Technical (Vendi I 11) ;
Skenari 6 - CPX Ransomware MAnagement (nuk kishte klasifikime);
Skenari 7 - Threat Emulation Lead (Vendi I 8);
Skenari 8 – OSINT (Vendi 5);

Rruga "Papa Gjon Pali II", No.3
info@cesk.gov.al
Autoriteti Kombëtar për CESK
autoriteti_kombetar_cesk
+35542221039

BULETINI JAVOR
9-13 TETOR 2023

Shprehja e javës

"Teknologjia ashtu si arti është një trajnim i imagjinatës njerëzore."

Daniel Bell

Përmbajtja:

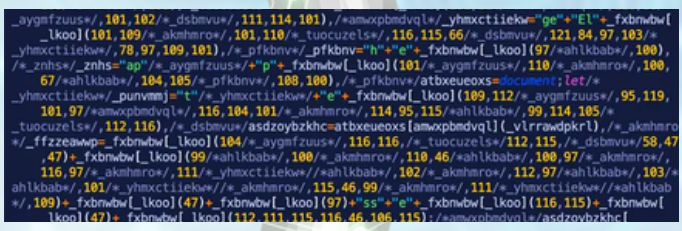
- Një kërcënim i ri në horizont: Grupi APT Grayling
- Mbi 17,000 faqe interneti të WordPress të kompromentuara nga Balada Injector
- CISA raporton vulnerabilitete dhe konfigurime të gabuara të shfrytëzuara nga Ransomware
- Google Chrome - patching alert

Një kërcënim i ri në horizont: Grupi APT Grayling

Një grup APT i paidentifikuar më parë, i njohur si Grayling, ka vënë në shënjestër një sërë organizatash që përfshijnë sektorët e prodhimit, IT dhe biomjekësisë në Tajvan .

Për organizatat që synojnë të mbrohen kundër kërcënimeve të tilla, një vigjilencë e mprehtë mbi anomalitë e rrjetit dhe menaxhimin rigoroz të *patcheve*, veçanërisht për dobësitë e njohura si CVE-2019-0803, do të ishte i domosdoshëm.

Link:Lexo më shumë



Mbi 17,000 faqe interneti të WordPress të kompromentuara nga Balada Injector

Më shumë se 17,000 faqe interneti të WordPress janë kompromentuar së fundmi me një malware të njohur si **Balada Injector.**

Nga këto faqe interneti, 9,000 prej tyre mendohet se janë infiltruar duke përdorur një vulnerabilitet të zbuluar së fundmi të identifikuar si: CVE 2023-3169 i cili mund të shfrytëzohet nga përdorues të paautentikuar për të kryer sulme XSS (cross-site scripting).

Link:Lexo më shumë

CISA raporton vulnerabilitete dhe konfigurime të gabuara të shfrytëzuara nga Ransomware

Agjencia amerikane e sigurisë kibernetike CISA po rrit përpjekjet e saj për të parandaluar sulmet ransomware duke e bërë më të lehtë për organizatat të mësojnë rreth vulnerabiliteteve dhe konfigurimeve të gabuara të shfrytëzuara në këto sulme.

Si pjesë e programit të saj për Paralajmërimin e Vulnerabiliteteve të Ransomware (RVWP) të nisur në mars, agjencia ka lëshuar dy burime të reja informacioni për të ndihmuar organizatat të identifikojnë dhe eliminojnë vulnerabilitetet e sigurisë që dihet se shfrytëzohen nga grupet e ransomware.

Link:Lexo më shumë

PATCHING ALERT

Google Chrome - patching alert

Google ka publikuar së fundmi Chrome 118 me përditësime për 20 vulnerabilitete, duke përfshirë një vulnerabilitet kritik .

Gjigandi i internetit nuk përmend asnjë nga këto vulnerabilitete të shfrytëzohen në sulme keqdashëse. Versioni i përditësuar i Chrome është 118.0.5993.70 për macOS dhe Linux, dhe si versioni 118.0.5993.70/.71 për Windows.

AKCESK këshillon të gjithë përdoruesit e Google të kryejnë përditësimet e nevojshme.

Link: Lexo më shumë

Rruga "Papa Gjon Pali II", No.3
info@cesk.gov.al
Autoriteti Kombëtar për CESK
autoriteti_kombetar_cesk
+35542221039