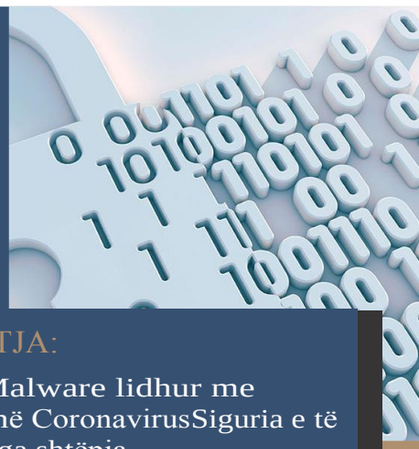
AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

BULETINI I LAJMEVE TË SIGURISË KIBERNETIKE

Prill 2020



PËRMBAJTJA:

Harta e shpërndarjes së Coronavirus është përdorur për përhapjen e malware.

Kohët e fundit, hakerat kanë filluar shpërndarjen e informacioneve në kohë reale në lidhje me normat globale të infeksionit të lidhura me pandeminë Coronavirus / COVID-19, me qëllimin për të infektuar sisteme kompjuterike me software të dëmshëm.

https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/

Këshilla mbi sigurinë e të punuarit nga shtëpia.

Nëse jeni një nga miliona punonjësit që po punoni nga shtëpia, mund t'ju vijnë në ndihmë rekomandimet e hartuara nga AKCESK mbi "Sigurinë në Internet kur punoni nga shtëpia", si dhe "Rekomandime për sigurinë në Internet për Blerje dhe shitje online". Të tjera rekomandime i gjeni në menunë Publikime të faqes zyrtare të AKCESK

https://cesk.gov.al/Publikime/publikime.html

Fushata masive spiunazhi përmes Coronavirus Phishing.

Një haker i vendosur në Pakistan dhe aktualisht i gjurmuar nën emra të shumtë, duke përfshirë APT36 dhe Tribran Fis, po zhvillon aktivitete spiunazhi përmes një fushate phishing, duke përdorur një dokument Excel me tematikë Coronavirus, i maskuar me këshilla shëndetësore.

https://www.bleepingcomputer.com/news/security/nation-backed-hackers-spread-crimson-rat-via-coronavirus-phishing/

Europol shpërbën grupet kriminale të ndërrimit të kartave SIM që vodhën miliona dollarë.

Europol së bashku me agjensitë e ligj zbatuese nga Spanja, Austria dhe Rumania arrestuan anëtarët e dy grupeve kriminale që përdornin kartat SIM. Hakerat ishin në gjendje të merrnin kontrollin mbi numrin e telefonit të objektivit dhe të merrnin të gjitha mesazhet dhe thirrjet dërguar viktimave në telefonin e tyre, duke anashkaluar faktorët e autentifikimit bazuar në SMS (MFA). Në këtë mënyrë, ata fitonin akses në përdorimin e kodeve (OTP) duke vjedhur kështu kredencialet e viktimave për t'u regjistruar në llogaritë e tyre bankare, email ose llogaritë e rrjeteve sociale, si dhe ndryshonin fjalëkalimet e llogarive të viktimave.

https://www.bleepingcomputer.com/news/security/europol-dismantles-sim-swap-criminal-groups-that-stole-millions/

Si të mbrohemi nga sulmet gjatë video-konferencave në Zoom.

Ata që përdorin platformën e konferencës me video në internet të Zoom, këshillohen nga FBI të ndërmarrin një numër masash për të parandaluar sulmet e mundshme:

- Mos i bëni mbledhjet publike: kërkoni një fjalëkalim takimi ose përdorni funksionin e "dhomës së pritjes" dhe kontrolloni pranimin e "mysafirëve".
- Mos e shpërndani link-un e konferencës Zoom në mediat sociale. Siguroni lidhjen drejtpërdrejt për njerëz specifikë.
- Menaxhoni opsionet e ndarjes në ekran: Në Zoom, ndryshoni ndarjen e ekranit në 'HostOnly'.
- Sigurohuni që bashkëbiseduesit i mbajnë të update-uar platformat e tyre Zoom.

AKCESK ka publikuar gjithashtu udhëzime të tjera specifike mbi përdorimin e ZOOM, të cilat i aksesoni në menunë Publikime të faqes zyrtare.

https://www.bleepingcomputer.com/news/security/fbi-warns-of-ongoing-zoom-bombing-attacks-on-video-meetings/

Hakerat kinezë shfrytëzojnë dobësitë e Cisco e Citrix për fushata masive spiunazhi.

APT41, një grup famëkeq i ardhur nga Kina, ka targetuar më shumë se 75 organizata në të gjithë botën në një nga fushatat më të mëdha të spiunazhit kibernetik të viteve të fundit.

https://threatpost.com/chinese-hackers-exploit-cisco-citrix-espionage/154133/

Doppel Payment Ransomware vjedh të dhëna nga kompani si SpaceX &Tesla.

Një kompani që ofron pjesë me porosi të gjigandëve të hapësirës ajrore Lockheed Martin, SpaceX dhe Boeing, ka qenë shënjestra e një sulmi nga një lloj ransomware që mund enkriptojë të dhënat. Visser Precision me bazë në Kolorado tha se ishte në shënjestër e një " sulmi kibernetik" që bëri të mundur që hakeri të hynte dhe të vidhte të dhënat e kompanisë. Një ekspert i sigurisë kibernetike gjeti disa nga dosjet e vjedhura të kompanisë që tashmë ishin publikuar në internet.

https://threatpost.com/doppelpaymer-ransomware-used-to-steal-data-from-supplier-to-spacex-tesla/153393/

Sulmi trojan "Zeus Sphinx" riaktivizohet në mes të pandemisë Coronavirus.

Sipas studiuesve Amir Gandler dhe Limor Kessem në IBM X-Force, Sphinx (a.k.a. Zloader ose Terdot) filloi të rishfaqet në dhjetor. Sidoqoftë, studiuesit vëzhguan një rritje të konsiderueshme të vëllimit në mars, pasi operatorët e Sphinx u përpoqën të përfitonin nga interesi dhe lajmet rreth pagesave të ndihmës qeveritare

https://securityintelligence.com/posts/zeus-sphinx-trojan-awakens-amidst-coronavirus-spam-frenzy/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+SecurityIntelligence+%28Security+Intelligence%29

Përditësimi i termave të Teknologjisë së Informacionit

- **Menaxhimi i të dhënave të aplikacionit (ADM)** - një disiplinë biznesi e mbështetur në teknologji, në të cilën biznesi dhe IT punojnë së bashku për të siguruar uniformitetin, saktësinë, administrimin, qeverisjen, konsistencën semantike dhe përgjegjshmërinë për të dhënat në një aplikim biznesi, si ERP.

- **Platforma e Shërbimeve të Përmbajtjes (CSP)** - një tërësi shërbimesh të paraqitura si një set i integruar i produkteve dhe aplikacioneve që ndajnë të njëjtat API dhe memorje. Një CSP shfrytëzon lloje të ndryshme përmbajtjesh dhe ka zbatim të gjerë në të gjithë organizatën.

- **Menaxhimi i të dhënave (DM)** - konsiston në praktikat, teknikat arkitekturore dhe mjetet për të arritur qasje të vazhdueshme në shpërndarjen e të dhënave në të gjithë spektrin e zonave të subjekteve të të dhënave dhe llojet e strukturës së të dhënave në organizatë, për të përmbushur kërkesat e aksesimit të të dhënave për të gjitha aplikacionet dhe proceset e biznesit.

- **Platforma e Përvojës Digjitale (DXP)** - një grup i integruar i teknologjive që mbështesin përbërjen, menaxhimin, shpërndarjen dhe optimizimin e përvojave digjitale.

- **Ofruesi i Shërbimeve të Menaxhuara (MSP)** - ofron shërbime, të tilla si rrjeti, aplikacioni, infrastruktura dhe siguria, përmes mbështetjes së vazhdueshme dhe të rregullt dhe administrimit aktiv në ambientet e klientëve, në qendrën e të dhënave të tyre të MSP-së ose në një qendër të dhënash të palëve të treta.

- **Shërbimi i rrjetave (Mesh)** - një ndërmjetës që optimizon komunikimin midis shërbimeve të aplikimit.

- **Techquilibrium** - pika e ekuilibrit kur ndërmarrja ka përbërjen e duhur të aftësive dhe pasurive tradicionale dhe digjitale, për të fuqizuar modelin e biznesit të nevojshëm për të garuar në mënyrë më efektive, në një industri që po revolucionohet teknologjikisht.

- **Çrregullimi i drejtuar nga infrastruktura** - përfshin ndërprerjen e drejtimit dhe pranimin e rrezikut për të ofruar risi të vazhdueshme në biznes, duke përdorur teknologji input&output , procese, njerëz, aftësi dhe kapacitete. Kjo do të thotë që drejtuesit e inputeve dhe outputeve duhet të jenë përparimtarë, të guximshëm dhe pohues. Ata duhet të përqëndrohen në vlerën e biznesit dhe jo vetëm të reagojnë ndaj kërkesave të biznesit.

https://www.gartner.com/en/information-technology/glossary