



# Buletini i Lajmeve të Sigurisë Kibernetike

Mars 2022

## GJURMIMI I AKTIVITETIT KIBERNETIK NË EVROPËN LINDORE



Në fillim të marsit, Google's Threat Analysis Group (TAG) publikoi një përditësim mbi aktivitetin kibernetik që po gjurmonte në lidhje me luftën në Ukrainë. Që nga përditësimi i fundit, TAG ka vëzhguar një numër vazhdimisht në rritje të aktorëve të kërcënimit që përdorin luftën si një mënyrë për phishing dhe malware. Aktorë të mbështetur nga qeveria e Kinës, Iranit, Koresë së Veriut dhe Rusisë, si dhe grupe të ndryshme të paatribuar, kanë përdorur tema të lidhura me luftën në Ukrainë me objektiv për t'i detyruar viktimat të klikojnë në malicious email ose malicious link.

Aktorët e motivuar financiarisht dhe kriminelë po përdorin gjithashtu ngjarjet aktuale si një mjet për të synuar përdoruesit. Për shembull, një aktor po imiton personelin ushtarak për të kërkuar para për të shpëtuar të afërmit në Ukrainë.

<https://www.cybersecurity-review.com/news-march-2022/tracking-cyber-activity-in-eastern-europe/>

## MICROSOFT KONFIRMON THYERJEN E SIGURISË NGA GRUPI LAPSUS\$

Microsoft ka konfirmuar se ishte prekur nga grupi i hakerëve Lapsus\$, duke iu shtuar listës në rritje të viktimave të këtij grupi.

Në një postim në blog, Microsoft u shpreh se:

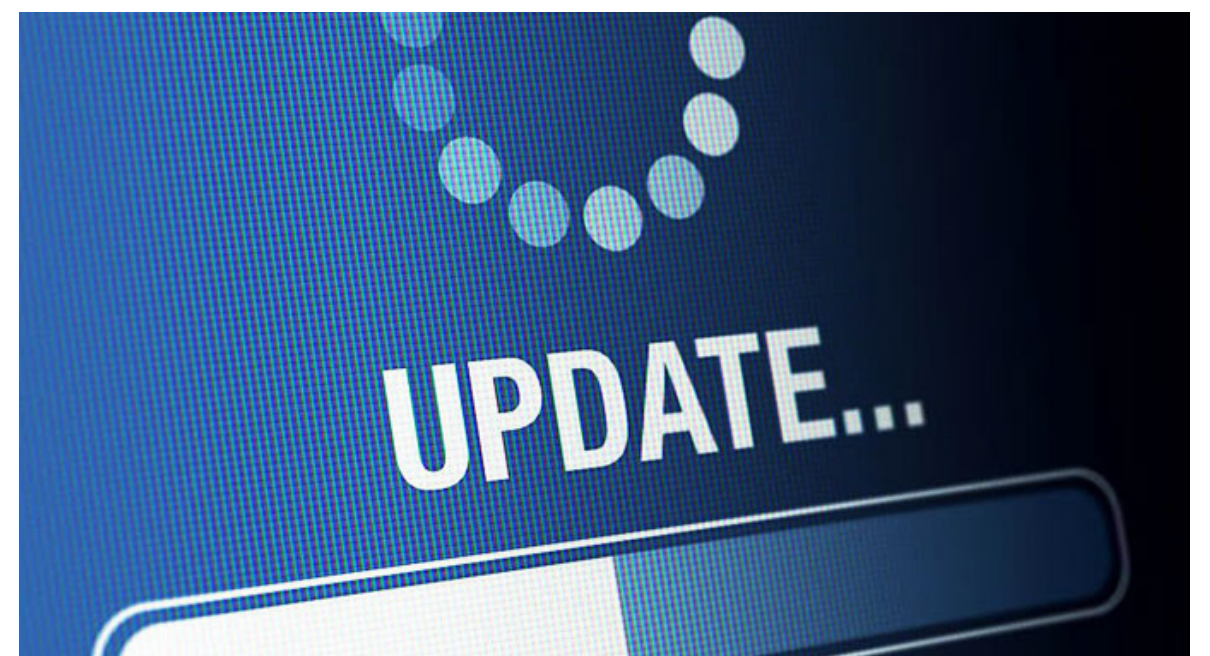
"Lapsus\$ kishte komprometuar një nga llogaritë e tij, duke rezultuar në "akses të kufizuar" në sistemet e kompanisë, por jo në të dhënat e ndonjë klienti të Microsoft.

Ekipe të reagimit të sigurisë kibernetike u angazhuan për të rikthyer llogarinë e komprometuar dhe për të parandaluar aktivitetin e mëtejshëm".

<https://www.cybersecurity-review.com/news-march-2022/microsoft-confirms-it-was-breached-by-hacker-group/>



## PËRDITËSIMI I "PATCH TUESDAY" I MICROSOFT-IT



Përditësimi i "Patch Tuesday" i Microsoft-it për muajin mars është bërë zyrtarisht i disponueshëm me 71 rregullime që përfshijnë produktet e tij softuerike si Windows, Office, Exchange dhe Defender, ndër të tjera.

Nga gjithsej 71, tre janë vlerësuar si Kritike dhe 68 janë vlerësuar të Rëndësishme për nga ashpërsia. Asnjë nga dobësitë nuk është renditur si e shfrytëzuar në mënyrë aktive, tre prej tyre janë të njohura publikisht në kohën e publikimit.

Vlen të theksohet se Microsoft trajtoi veçmas 21 defekte në manualin Microsoft Edge të bazuar në Chromium në fillim të këtij muaji.

<https://thehackernews.com/2022/03/critical-security-patches-issued-by.html>

## PESË TENDENCAT KRYESORE TË SIGURISË KIBERNETIKE PËR 2022

Mashtime të panumërta, shkelje të sigurisë, vjedhje dhe rrjedhje të të dhënave ndodhën vitin e kaluar dhe tendencat tregojnë se ato do të vazhdojnë të ndodhin në vitin 2022. Në fakt, rezultatet e një studimi tregojnë shqetësimin në rritje të kompanive në lidhje me sigurinë e informacionit dhe se 69% e organizatave parashikojnë se do të rrisin investimet e tyre në sigurinë kibernetike në vitin 2022.

Këtu janë pesë tendencat në sigurinë kibernetike që u sugjerojmë kompanive t'i vëzhgojnë në këtë vit.

1. Ransomware Cyberattacks.
2. 5G Vulnerabilities
3. Remote Environments And The Decentralization Of Access
4. Synthetic Identities
5. Offline Fraud