MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Február 2023

(skrátená verzia)

Vypracoval: CSIRT.SK

TLP: White

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci február riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytli sa tiež prípady kompromitovaných e-mailových účtov zamestnancov verejných inštitúcií, z ktorých útočníci rozposielali phishingové e-maily na ďalšie organizácie v konštituencii CSIRT.SK. Pokračovala niekoľkomesačná phishingová kampaň zameraná na občanov Slovenskej republiky, v ktorej útočníci predstierajúci totožnosť Europolu a vysokopostavených členov Polície SR posielajú svojim obetiam falošné predvolania kvôli prechovávaniu detskej pornografie a podobným sexuálnym deliktom. Opäť bola pozorovaná spearphishingová kampaň, v ktorej sa útočníci vydávajú za vedúceho zamestnanca obete a požadujú prevod väčšej sumy na zahraničné účty.

Vládna jednotka CSIRT riešila incident spojený so spear-phishingovou kampaňou na ministerstvá zahraničných vecí viacerých krajín, vedenou pravdepodobne čínskou APT skupinou Mustang Panda. O incidente jednotku informovali partneri. E-mail obsahujúci malvér určený pre organizáciu v konštituencii CSIRT.SK bol zachytený pred doručením.

CSIRT.SK monitoroval vo februári niekoľko útokov typu DDoS na webové sídla viacerých štátnych organizácií vrátane MV SR (www.minv.sk), MO SR (www.mosr.sk) MZVaEZ SR (foreign.gov.sk). Zasiahnuté boli aj weby energetického a bankového sektora. Útoky boli vedené proruskými skupinami NoName057(16) a Killnet v rámci jej projektu DDosia. Dané ministerstvá sa podľa vyjadrení skupín na ich telegramovom kanály stali terčom útokov napríklad kvôli tomu, že Slovensko prijalo uznesenie, ktoré označuje Rusko za štát podporujúci terorizmus alebo kvôli úvahám poskytnúť Ukrajine vyradené stíhačky MIG 29.

Zaujímavým prípadom bolo umiestnenie obsahu pre dospelých na doméne www.dobrefondy.eu, ktorú pôvodný prenajímateľ uvoľnil a prenajal si ju útočník. Odkaz na túto doménu bol uverejnený na stránke https://partnerskadohoda.gov.sk. Správca stránky, ktorým je Úrad vlády SR, zanedbal odstránenie nepoužívanej domény z kódu svojho webu, čím sa vystavil reputačnému riziku. Podobný incident sa stal v roku 2020 a informácia o ňom bola publikovaná na https://www1.pluska.sk/video/neuverite-vlastnym-ociam-toto-nemysli-urad-vlady-vazne-odkaz-porno-webovej-stranke

Jednotka CSIRT.SK prijala tiež nahlásenie kompromitácie zariadenia FortiSSL VPN. Útočník pravdepodobne zneužil známu zraniteľnosť CVE-2022-42475 na zariadení. Bočný pohyb v infraštruktúre zasiahnutej organizácie nebol potvrdený.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií vo svojej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje. Jednotka rozšírila svoj monitoring o nedostupné webové domény. Vo februári navyše informovala majiteľov zraniteľných MS Exchange serverov o vydaní opravy vysoko závažnej zraniteľnosti CVE-2023-21707, ktorá umožňuje vzdialene vykonávať kód.

Mesačník zraniteľností február 2023

CSIRT.SK vydáva a uverejňuje na svojej stránke prehľad kritických zraniteľností bežného softvérového vybavenia na mesačnej báze. Jedná sa o nasledovné produkty:

1. Operačné systémy Microsoft Windows
2. Kancelárske balíky Microsoft Office a Office Web Apps
3. Internetové prehliadače
    - Microsoft Internet Explorer
    - Microsoft Edge
    - Mozilla Firefox
    - Google Chrome
4. Adobe Acrobat a Reader
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java
6. Iné tohto mesačné závažné zraniteľnosti
    - ClamAV
    - 3x Microsoft zero-day
    - FortiNAC

https://www.csirt.gov.sk/posts/3323.html?csrt=11488975689505737584