MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Október 2022

(skrátená verzia)

Vypracoval: CSIRT.SK

TLP: White

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci október riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytli sa tiež prípady kompromitácie e-mailového konta, z ktorého útočníci rozposielali phishingové e-maily. Vládna kyberbezpečnostná jednotka zaznamenala tento mesiac pokračujúcu phishingovú kampaň predstierajúcu doručenie predvolania na súdne pojednávanie od Europolu kvôli prechovávaniu detskej pornografie a obdobným sexuálnym deliktom. Objavili sa tiež prípady spear-phishingových e-mailov v niekoľkých organizáciách podpísaný menom vedúceho zamestnanca, pokúšajúcich sa presvedčiť obeť, aby vykonala finančný prevod na zahraničný účet.

6. októbra sa udial významný kybernetický útok typu DDoS, ktorý zasiahol webové sídla viacerých subjektov v Slovenskej republike vrátane niekoľkých organizácií v konštituencii CSIRT.SK. Vládna jednotka CSIRT počas riešenia incidentu koordinovala svoju činnosť a zdieľala informácie so svojimi partnermi. Kontaktovala tiež zasiahnuté subjekty vo svojej konštituencii, a zároveň varovala ďalších svojich konštituentov o hroziacich útokoch DDoS. Podľa informácií známych VJ CSIRT dňa 06.10.2022 po 23:00 už neprebiehali DDoS útoky na kybernetický priestor Slovenska, aktér hrozby pokračoval útokmi na ukrajinské banky. Stopy, s ktorými bola jednotka oboznámená, nasvedčovali využitiu konkrétneho, známeho botnetu Anonymus.ru (s vysokou pravdepodobnosťou nedávno obnovený Killnet) riadeného z Ruskej federácie. Ohľadom koncových, viditeľných IP adries sa jednalo o adresy z Číny, Japonska, Malajzie, Fínska, Holandska, Tajvanu, USA a Ruska.

CSIRT.SK prijal v októbri kuriózne hlásenie o prístupe na darkwebovú doménu z jednej organizácie v jeho konštituencii. Jednalo sa o presmerovanie na online knižnicu. Ďalšími riešenými prípadmi boli útok typu Man-in-the-middle na komunikačné linky organizácie v konštituencii CSIRT.SK, či únik údajov z webovej služby.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK poskytla organizáciám vo svojej konštituencii indikátory kompromitácie kampane šíriacej inštalačné balíky známych softvérových nástrojov, infikované nešpecifikovaným malvérom, ktoré získala od partnera. Jednotka ďalej vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií v jej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje.

Mesačník zraniteľností október 2022

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
    - Microsoft Exchange
    - BIOS Lenovo
    - FortiOS, FortiProxy

https://www.csirt.gov.sk/posts/3103.html?csrt=14026195921514260495