MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Jún 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 jún 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. Jednotka zachytila pokračujúcu spearphishingovú 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 ruskou skupinou APT29, známou tiež pod názvom Sandworm.

CSIRT.SK riešil s júni tiež prípad malvérovej infekcie zamestnaneckého zariadenia v infraštruktúre organizácie v jeho správe. Na základe indikátorov kompromitácie, ktoré jednotka poskytla monitoringu NASES, boli odhalené ďalšie infikované organizácie a hrozba bola odstránená.

Jednotka ďalej riešila presahy ransomvérového útoku na Univerzitu Mateja Bela v Banskej Bystrici, pretože univerzita využíva IT služby niektorých štátnych organizácií. Cieľom bolo zabrániť šíreniu infekcie na tieto externé inštitúcie. Okrem toho, prijala hlásenie o neúspešných útokoch hrubou silou na VPN pripojenie do siete jednej inštitúcie.

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. V júni navyše informovala organizácie štátnej a verejnej správy o doménach spojených s malvérom, ktorý zneužíva zero-click zraniteľnosť v iOS iMessages.

Mesačník zraniteľností jún 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
    - FortiNAC
    - FortiGate SSL VPN
    - Microsoft Azure AD
    - Splunk Enterprise
    - KeePass

https://www.csirt.gov.sk/posts/3470.html?csrt=11328508017543543280