MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

November 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 november riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytli sa tiež prípady kompromitácie e-mailového konta, z ktorého útočníci rozposielali phishingové e-maily. Pokračovala phishingová resp. podvodná kampaň zameraná na občanov Slovenskej republiky, v ktorej sa útočníci snažia presvedčiť svoje obete, že ich kontaktuje slovenská pobočka Europolu kvôli prechovávaniu detskej pornografie a obdobným sexuálnym deliktom. Opäť preto pripomíname, že Slovenské úrady obdobné dokumenty nikdy neposielajú online, ale doručujú ich štandardne v papierovej forme. V novembri jednotka CSIRT.SK opäť zaznamenala hlásenia phishingových e-mailov z kampane Sextortion. Objavila sa tiež jej obdoba, v ktorej sa útočníci vyhrážajú zverejnením exfiltrovanej databázy z backendu webovej domény obete. Platbu požadujú štandardne v BTC.

Častým druhom podvodov sa stal phishing na inzerčných portáloch (najmä bazos.sk). Útočník predstiera záujem o tovar obete. Navrhne, že pošle kuriéra na jeho vyzdvihnutie a platbu pošle vopred online. Obeť má na podvodnej webstránke zadať údaje zo svojej platobnej karty, čo má umožniť previesť sumu na jej účet. V skutočnosti však po získaní týchto údajov podvodník vyberie financie z účtu obete. Podobne funguje druhá rozšírená phishingová kampaň, ktorá imituje Slovenskú poštu či inú doručovateľskú spoločnosť. V nej podvodníci predstierajú, že obeť potrebuje doplatiť malú čiastku za poštovné, aby mu bola doručená pozdržaná zásielka. Aby phishingovú doménu nezachytávali antimalvérové riešenia, útočníci niekedy používajú presmerovanie cez legitímne domény akou je napríklad služba Linkedin.

CSIRT.SK prijal v novembri informáciu o úniku veľkého množstva citlivých pracovných dokumentov jednej organizácie, ktoré boli objavené na portáli uloz.to. Zamestnanci by za žiadnych okolností nemali zdieľať pracovné dokumenty cez verejné služby. Mali by využívať na to určené systémy zamestnávateľa, prípadne ich posielať zabezpečenou formou. Vhodným riešením sú šifrované e-maily či šifrované archívy so silným heslom, ktoré odosielateľ odovzdá adresátovi iným kanálom.

Vládna jednotka CSIRT sa aj v novembri stretla s ransomvérom. Nahlásený incident však nebol veľkého rozsahu – zasiahnutý bol zdieľaný priečinok sieťového dátového úložiska, na ktoré sa pripojil zamestnanec s infikovaným zariadením. Poškodená organizácia zvládla riešenie incidentu bez vyžiadania asistencie, jednotka odovzdala iba odporúčania ako postupovať.

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.

TLP: White

Mesačník zraniteľností november 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
    - OpenSSL
    - VMware Workspace ONE
    - Citrix ADC a Gateway
    - F5 BIG-IP a BIG-IQ
    - Protokol Samba

https://www.csirt.gov.sk/posts/3138.html?csrt=5955185371473447813