MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

August 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 august riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytli sa tiež prípady kompromitácie e-mailového konta, z ktorého útočníci rozposielali phishingové e-maily. Opakovane bolo od júla hlásených viacero kompromitovaných e-mailových kont jednej organizácie. Modus operandi kampane naznačuje úspešnú phishingovú kampaň na jej zamestnancov. Organizácii ponúkol CSIRT.SK školenie zamestnancov na hrozby spojené so sociálnym inžinierstvom.

Po dlhšom čase sa opäť začala prebúdzať spear-phishingová kampaň, v ktorej sa útočníci vydávajú za vedúceho zamestnanca organizácie, v ktorej si vytipovali svoje obete. Zamestnancov žiadajú o finančný prevod vo výške rádovo desiatok tisíc Eur na účty v cudzích krajinách. CSIRT.SK prijal iba hlásenia pokusov o podvod a nemá vedomosť o žiadnom úspešnom útoku. Vládna jednotka CSIRT pri podobných prípadoch informuje aj banky, v ktorých sú zneužité účty vedené.

Ďalšou phishingovou kampaňou, s ktorou sa jednotka viacnásobne stretla v priebehu augusta, bol podvod na inzerčných portáloch (typicky bazos.sk) s cieľom získať údaje z platobných kariet obetí. Útočníci sa väčšinou pokúšajú obeť presvedčiť, že si vybavili vyzdvihnutie tovaru, ktorý inzeruje, kuriérom spoločnosti Packeta. Tvrdia, že platbu uskutočnili súčasne s tým a obeti stačí pre získanie finančných prostriedkov vyplniť údaje o svojej platobnej karte na podvrhutej webstránke, ktorá zneužíva falošnú identitu spoločnosti Packeta. Alternatívou sú falošné stránky kuriérskych spoločností, či Slovenskej pošty. Spoločnosti Bazoš a Packeta o tejto forme podvodu informujú svojich zákazníkov. Rovnako o kampani informujú ďalšie zdroje vrátane Polície SR a niektorých médií.

CSIRT.SK riešil tento mesiac aj obzvlášť rozsiahly ransomvérový incident vo svojej konštituencii. Ransomvér zasiahol veľký počet serverov a pracovných staníc. Jednotka vykonáva forenznú analýzu zaistených digitálnych stôp a analýzu možností obnovy infraštruktúry.

Jednotka CSIRT.SK vykonávala tiež analýzy malvéru prítomného v prílohách škodlivých e-mailových správ a komunikovala s niekoľkými organizáciami v jej konštituencii ohľadom odstraňovania zraniteľností odhalených v ich IT infraštruktúre.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK 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 August 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 závažné zraniteľnosti
    - Cisco Small Business routre
    - Cisco ASA, Firepower a ASDM
    - Zimbra
    - miskonfigurácie VNC, RDP, FTP, SMB, ...

https://www.csirt.gov.sk/posts/3010.html?csrt=17474479626125847421