MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Máj 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 máj riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytli sa tiež prípady kompromitácie e-mailového konta, z ktorého útočníci rozposielali phishingové e-maily. V jednom prípade bolo zaznamenané rozposielanie phishingových e-mailov cez mailserver, pričom útočníci zneužili konfiguračnú chybu v mailing liste.

Jednotka CSIRT.SK vykonávala forenznú analýzu zaistených digitálnych stôp z ransomvérového útoku, ktorý jej bol nahlásený v apríli. Ransomvér zasiahol dva fyzické servery v infraštruktúre zasiahnutej organizácie. Zariadenia obsahovali intranet vrátane registratúry, Active Directory a mailserver organizácie.

Vládna jednotka riešila incident, kedy útočník zaregistroval na údaje vedenia organizácie účet na e-shope. Tieto získal z voľne dostupných zdrojov. Následne vytvoril objednávku, ktorej potvrdzujúci e-mail prišiel do legitímnej mailovej schránky vedenia danej organizácie. Z analýzy stôp vyplynulo, že útočník pristupoval k e-shopu cez VPN.

V rámci svojej proaktívnej činnosti CSIRT.SK varovala svoju konštituenciu pred phishingovou kampaňou šíriacou malvér Emotet, ktorý začal po odstavení svojej infraštruktúry po medzinárodnom policajnom zásahu začiatkom roka 2021 opäť naberať na sile. 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 Máj 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 tohtomesačné závažné zraniteľnosti
    - F5 BIG-IP
    - Microsoft Office - Follina

https://www.csirt.gov.sk/posts/2898.html?csrt=859628186241602558