MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Máj 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 máj 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.

Vládna jednotka CSIRT zachytila viacero spear-phishingových útokov na organizáciu štátnej správy, pričom jeden iba zneužíval meno inštitúcie v kampani na zahraničné ciele.

V rámci podvodov prijala jednotka v máji hlásenie podvodného online obchodu na doménach gaborslovakia.sk a gaborslovensko.sk. Útočník zneužil totožnosť slovenskej značky Gabor.

Vládna kyberbezpečnostná jednotka riešila v máji prípady infekcie zariadení v infraštruktúre dvoch organizácie, čo bolo odhalené komunikáciou na škodlivé domény smerom zvnútra zasiahnutých inštitúcií. Riešila tiež prípad kompromitovaného perimetrového firewallu, kam sa útočník dostal cez odcudzené prístupy do účtov VPN a odkiaľ začal skenovanie internej infraštruktúry organizácie.

CSIRT.SK prijal v máji informáciu o útoku typu DDoS na webové stránky Magistrátu hlavného mesta Bratislavy (bratislava.sk) a aplikáciu mestskej parkovacej politiky Paas. K útoku sa prihlásila skupina CyberTriad, ktorá ako dôvod uviedla organizovanie bezpečnostnej konferencie GlobSec v Bratislave.

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 máji zároveň vydala odporúčania pre organizácie, ako pracovať s čoraz obľúbenejšou aplikáciou ChatGPT.

Mesačník zraniteľností máj 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
    - Cisco Small Business Series Switches
    - Apple
    - Protokol SLP
    - VMware Workstation a Fusion
    - APC Easy UPS Online Monitoring

https://www.csirt.gov.sk/posts/3418.html?csrt=1989870140478149912