MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Január 2024

(skrátená verzia)

Vypracoval: CSIRT.SK

TLP: White

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci január 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. Zaznamenané boli e-maily spearphishingovej kampane, v ktorej sa útočníci vydávajú za vedúceho zamestnanca obete a požadujú prevod väčšej sumy na zahraničné účty.

VJ CSIRT objavila na Telegrame výhražné správy skupiny CryptHades o plánovanom útoku typu DDoS na subjekty obranného a zbrojného priemyslu s prepojením na Ministerstvo obrany SR, patriace pod Czechoslovakia Group a.s.. Skupina proruských hacktivistov spájala svoju vyhrážku s použitím zbraňových systémov, ktoré vyrobila daná spoločnosť. Systémy boli dodané ukrajinskej armáde a použité pri protiútoku ukrajinských síl proti odpaľovačom balistických rakiet v oblasti Belgorodu, v nadväznosti na ruské útoky proti ukrajinským mestám. V dôsledku tejto akcie a reakcie ruskej protivzdušnej obrany v okolí Belgorodu došlo ku materiálnym škodám a stratám na životoch civilného obyvateľstva v Belgorode. CSIRT.SK informoval zainteresované subjekty v SR a ČR, vrátane jednotky CSIRT pod Vojenským spravodajstvom SR a českej vládnej kyberbezpečnostnej jednotky NÚKIB.

V januári požiadalo Ministerstvo kultúry SR jednotku CSIRT.SK o súčinnosť pri riešení incidentu s oficiálnym facebookovým kanálom ministerstva, kde zodpovední zástupcovia organizácie predpokladali neoprávnený prístup neznámeho útočníka a manipuláciu s obsahom. Po krátkom čase však spoluprácu ukončilo a incident si prevzalo na riešenie v rámci svojich kapacít.

Zaujímavým prípadom bol incident na strednej škole, kde došlo k vymazaniu časti súborov na spoločnom školskom úložisku. Preverením incidentu sa ukázalo, že nešlo o útok, ale nedbalosť používateľa.

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. Systém Achilles slúži tiež na monitoring dostupnosti webových domén. V januári navyše informovala svoju konštituenciu o spear-phishingovej kampani skupiny APT28 (Fancy Bear) šíriacej malvér Headlace, spolu s indikátormi kompromitácie spojenými s danou kampaňou. Pri identifikovaných slovenských cieľoch bolo účelom kampane kompromitovať dôveryhodné e-mailové kontá, ktoré by mohli útočníci zneužiť pri ďalšej fáze útoku, resp. na šírenie samotného malvéru.

Mesačník zraniteľností január 2024

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
    - Atlassian Confluence Data Center a Server
    - F5 BIG-IP
    - Ivanti
    - Microsoft Sharepoint Server
    - FortiOS a FortiProxy

https://www.csirt.gov.sk/posts/373.html?csrt=10276056912468538203