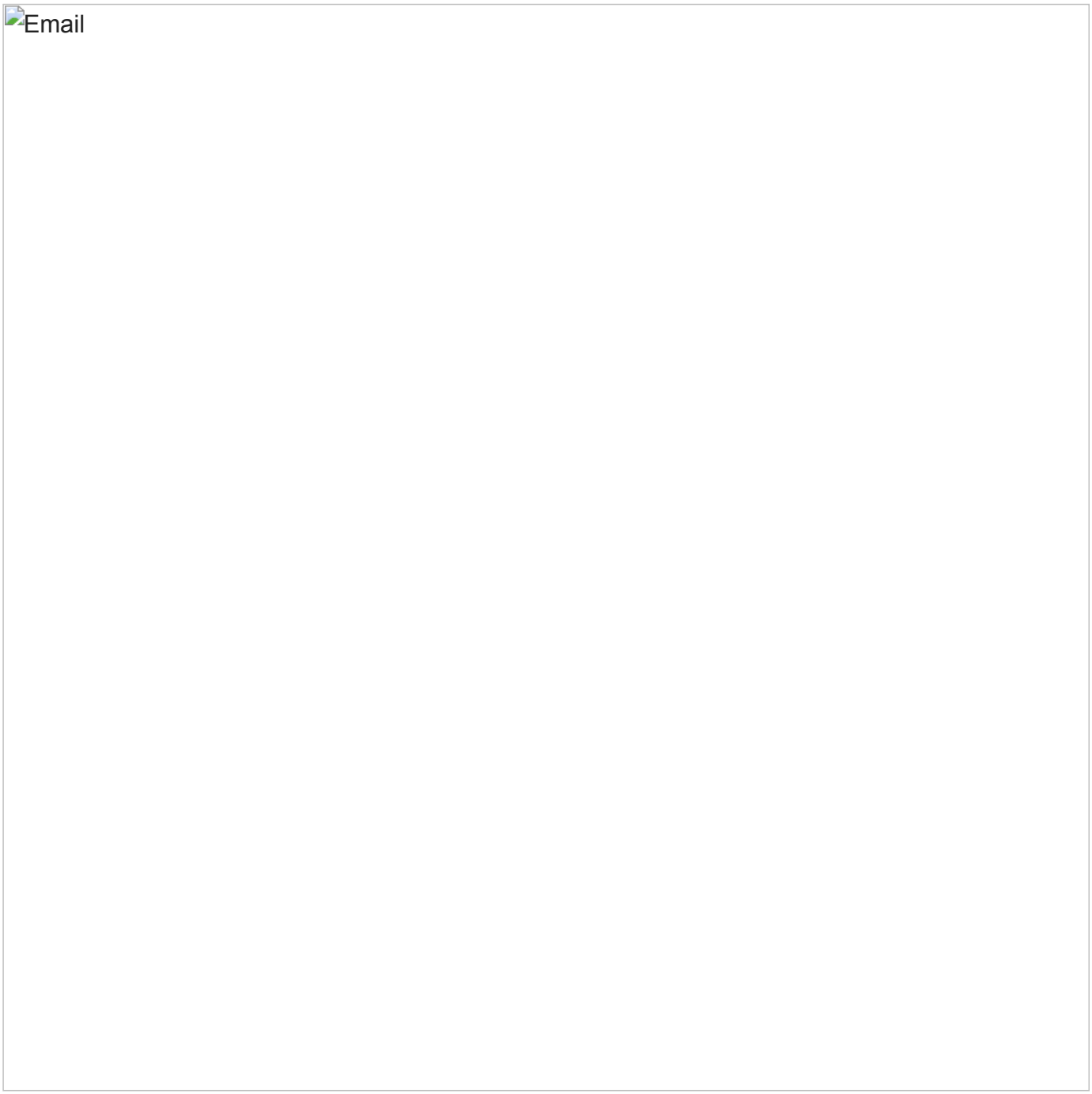
Upozornění na phishingovou kampaň cílící na Českou republiku

portal.neweb.govcert.cz/informacni-servis/informace/upozorneni-a-hrozby/upozorneni-na-phishingovou-kampan-cilici-na-ceskou-republiku

Od října 2023 probíhá phishingová kampaň, která mimo jiné cílí i na Českou republiku. Cílem kampaně je zisk informací ze sítí vládních institucí.

Kampaň se podobá kampani evidované v září tohoto roku ukrajinským CERT (CERT-UA). [1] CERT-UA připisuje danou kampaň skupině APT28 (též označované jako Fancy Bear či, Forest Blizzard), která je spojována s ruským vojenským zpravodajstvím GRU.

Prvotním vektorem útoku je phishingový e-mail, který vyzývá uživatele ke stažení archivu přes odkaz a následně k jeho otevření. Tématem e-mailu není nic konkrétního, přičemž se snaží zneužít zvědavosti uživatele.



Archiv po extrakci viditelně obsahuje LNK soubor s názvem `SEDE-PV-2023-09-1_EN`, který dle ikonky vypadá jako dokument z aplikace Word. Po spuštění uživatelem dojde na pozadí ke spuštění binárky `WINWORD.EXE`, která je legitimní aplikací. Pomocí techniky DLL-sideloading importuje škodlivou knihovnu `WindowsCodecs.dll`. Knihovna otevře `SEDE-PV-2023-09-1_EN.docx`. Jde zdánlivě o legitimní a veřejně dostupný dokument návrhu agendy jednání podvýboru pro bezpečnost a obranu Evropského parlamentu. Útočník se touto akcí snaží uživateli navodit dojem, že otevřel dokument Word. Současně dojde ke spuštění souboru

`command.cmd`, který vytvoří další dokumenty (typu VBS a BAT) pro komunikaci s C2 a odstraní škodlivé soubory, co jsou součástí archivu. Ke komunikaci na C2 server dojde v případě, že veřejná IP adresa stroje má jako geolokaci Českou republiku a dotaz byl proveden prohlížečem Microsoft Edge.

K distribuci archivu, komunikaci C2 i exfiltraci dat je použita infrastruktura třetích stran. Jedná se konkrétně o domény `mockbin[.]org`, `mocky[.]io` a `infinityfreeapp[.]com`, které jsou součástí nabízených služeb jako tvorba API nebo webhosting. Nález komunikace na tyto služby nemusí tedy ihned znamenat kompromitaci organizace. Může se jednat o legitimní provoz. Pro správné vyhodnocení tohoto typu nálezu je třeba danou komunikaci zasadit do širšího kontextu.

Pro ověření, zda vaše organizace byla cílem této kampaně, využijte námi publikovanou událost v platformě MISP [2]. Doporučujeme dané indikátory vyhledat v datech za uplynulé dva měsíce.

V MISP události je i hash SHA256 archivu, který má přidaný komentář „clean“. Jedná se o archiv, který je součástí distribuovaného archivu, ale obsahuje pouze kopii výše zmíněného dokumentu Word. Tento archiv je využit souborem command.cmd k mazání stop.

Pokud dané IoCs naleznete ve vašich systémech a usoudíte, že se jedná o útok v rámci této kampaně, informujte o této události cert@nukib.cz.

Zdroje

- [1] https://cert.gov.ua/article/5702579
- [2] https://misp.neweb.govcert.cz/events/view/182

Klasifikace

TLP:AMBER

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

02. 11. 2023

Obsah

Reakce

11