

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **99** ze dne **25.2.2025**

ČR nadále mezi méně bezpečnými evropskými zeměmi, rekordní nárůst kybernetických rizik na Slovensku

Výzkumný tým společnosti Check Point zveřejnil Celosvětový index dopadu hrozeb. Zpráva upozorňuje na rostoucí sofistikovanost a agresivitu kyberzločinců. Nejrozšířenějším malwarem byl v prosinci FakeUpdates, který zasáhl pět procent organizací po celém světě, těsně následovaly malwary AgentTesla a AndroXh0st.

FakeUpdates je všestranným downloaderem, zatímco AgentTesla se zaměřuje na krádeže přihlašovacích údajů a citlivých dat.

Vydán byl i žebříček zemí, které jsou nejčastěji terčem kyberútoků. Česká republika obsadila i v prosinci méně bezpečnou 43. pozici a nadále patří mezi země, které v Evropě čelí největšímu množství kyberútoků. Slovensko po mnoha měsících, kdy patřilo mezi bezpečnější země, zažilo v prosinci šok a vůbec největší nárůst kybernetických rizik ze všech zemí, což vyústilo v posun z 81. na 51. příčku. První, tedy nejnebezpečnější, pozici obsadila znovu Etiopie.

Výzkumný tým zároveň upozorňuje, že největšímu množství kyberútoků čelí nadále vzdělávací a výzkumné instituce. Následují komunikační společnosti a vládní a vojenské subjekty.

Top 3 - malware:

- FakeUpdates - FakeUpdates (nebo také SocGh0lish) je downloader, který šíří i další malware, včetně GootLoader, Dridex, NetSupport, DoppelPaymer a AZORult.
- AgentTesla - Pokročilý RAT, který krade hesla a funguje jako keylogger.
- AndroXh0st – AndroXh0st je botnet zaměřený na platformy Windows, Mac a Linux.

Top 3 - mobilní malware:

- Anubis - Bankovní trojan určený pro mobilní telefony se systémem Android. Byl odhalen už ve stovkách různých aplikací, dostupných v obchodě Google.
- Necro - Necro je trojan dropper pro Android, který dokáže stahovat další malware, zobrazovat nevyžádanou reklamu a krást peníze přihlašováním k placeným službám.
- Hydra - Bankovní trojan určený ke krádeži bankovních přihlašovacích údajů, který po obětech požaduje povolení nebezpečných oprávnění a přístupů při každém vstupu do jakékoli bankovní aplikace.

Top 3 - ransomwarové skupiny:

- Nejrozšířenější ransomwarovou skupinou byl v prosinci Funksec, který byl zodpovědný za 14 % zveřejněných útoků.
- Funksec - Skupina využívající umělou inteligenci a taktiku dvojího vydírání.
- RansomHub - RansomHub je ransomware jako služba (RaaS), který vznikl jako rebrandovaná verze

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **99** ze dne **25.2.2025**

dříve známého ransomwaru Knight. Známý je také kvůli použití sofistikovaných šifrovacích metod.

- LeakeData - Nová skupina, která kombinuje ransomware a šifrování s komplexními vyděračskými taktikami.

"Analyzovali jsme i malware útočící na podnikové sítě v České republice. V uplynulých měsících dominantní AndroXgh0st tentokrát ztratil na síle, čehož využil k dalšímu růstu zlodějský malware FormBook, který se tak stal nejrozšířenějším malwarem v Česku. Na druhé příčce je celosvětová jednička, downloader FakeUpdates. Přitom v listopadu byl až na konci českého Top 10. Podobný trend zaznamenal i zlodějský a špionážní malware AgentTesla. Nově mezi nejvýraznější škodlivé kódy pronikl trojan Flawedgrace, který se používá při cílených útocích a krade systémové informace," uvedl Tomáš Růžička, SE Team Leader z kyberbezpečnostní společnosti Check Point Software Technologies.

Zdroj: AVcentrum ČR