Trendy na dark webu: jaký byl minulý rok a prognózy na 2024

19.1.2024 - | PROTEXT

V nejnovějším zpravodaji Kaspersky Security Bulletin (KSB) sestavili odborníci z oddělení Global Research and Analysis Team a Kaspersky Digital Footprint Intelligence komplexní přehled událostí uplynulého roku a naznačili nové trendy na stínovém trhu dark webu, který je centrem ilegálních služeb kyberzločinecké komunity.

Nejdůležitější události roku 2023:

Aktéři v oblasti ransomwaru obvykle vytvářejí blogy týkající se vydírání firem, popisu nových úspěšných hackerských útoků nebo zveřejňování ukradených dat. V roce 2022 bylo na veřejných platformách a dark webu měsíčně publikováno v průměru 386 blogových příspěvků. V roce 2023 tento počet vzrostl na 476 příspěvků, přičemž maximum činí 634 příspěvků za listopadu.

Na dark webovém trhu se zvýšil počet příspěvků týkajících se malwaru typu stealer, který slouží k odcizení citlivých informací, jako jsou přihlašovací, finanční a osobní údaje. Kyberzločinci tyto údaje prodávají dalším záškodníkům za účelem krádeže identity, finančních podvodů nebo jiných nezákonných činností.

Pozoruhodné je, že počet příspěvků nabízejících záznamy získané pomocí známé malwarové rodiny RedLine Stealer se z průměrných 370 měsíčně v roce 2022 zhruba ztrojnásobil na 1 200 v roce 2023. Množství různých souborů záznamů, které obsahují kompromitované údaje uživatelů a jsou volně zveřejňovány na dark webu, v roce 2023 v porovnání s předchozím rokem celkově vzrostlo o téměř 30 %.

Společnost Kaspersky ve výhledu na rok 2024 předpokládá, že trh dark webu bude ovlivňovat několik trendů:

Kyberzločinci dříve spoléhali na podvodné e-maily, nyní využívají reklamy na Googlu a Bingu, aby zajistili, že se jejich cílové stránky s malwarem dostanou na přední pozice ve výsledcích vyhledávání. Fiktivní prodejci pravděpodobně své prodejní aktivity na nelegálním trhu zintenzivní a společnost Kaspersky proto očekává další nárůst těchto podvodných praktik.

Mezi podvodníky v oblasti kryptoměn se stále větší oblibě těší tzv. crypto drainery, což je kategorie škodlivého softwaru, který slouží k rychlému a automatizovanému převodu peněz z legitimních kryptopeněženek do peněženek kyberzločinců. Společnost Kaspersky předpovídá nárůst poptávky po tomto druhu malwaru pro krádeže kryptoměn, což povede ke zvýšenému výskytu inzerátů propagujících jeho vývoj a prodej na nelegálním trhu. Očekává se, že trvalý zájem o kryptoměny, NFT objekty a podobná digitální aktiva podpoří také šíření těchto drainerů.

Kromě toho odborníci očekávají následující tendence:

„Kybernetická bezpečnost vyžaduje proaktivní přístup. Monitorování aktivit a trendů na dark webovém trhu se podobá práci špiónů v týlu nepřítele – umožňuje včasné odhalení hrozeb, pochopení taktiky protivníka a zajišťuje, že jste v oblasti kybernetické obrany o několik kroků napřed. Nejde jen o ochranu proti aktuálním hrozbám, ale i o zvládnutí vyvíjejícího se prostředí hrozeb, aby bylo možné posílit preventivní opatření i proti budoucím rizikům a zajistit odolnost firemního zabezpečení,“ říká **Sergej Lozhkin**, hlavní bezpečnostní výzkumník globálního

výzkumného a analytického týmu (GReAT) společnosti Kaspersky.

Přehled a prognózy vývoje na trhu dark webu jsou součástí zpravodaje Kaspersky Security Bulletin (KSB) – každoroční série předpovědí a analytických zpráv o klíčových změnách ve světě kybernetické bezpečnosti. Další informace najdete zde.

https://www.ceskenoviny.cz/tiskove/zpravy/trendy-na-dark-webu-jaky-byl-minuly-rok-a-prognozy-na-2024/2467933