Nabídka společnosti DNS a.s.

Služba „CTI Password Hunter“

Nabídka společnosti DNS a.s. a služeb Cyber Threat Intelligence

Popis služby

CTI Password Hunter je služba, která nabízí jednorázovou analýzu a podrobný report o tom, zda se na darknetu nebo v databázích z InfoStealers nevyskytují uniklá data vztahující se ke konkrétním doménám, systémovým přístupům, uživatelským účtům, počítačům či celým sítím.

Jedná se o ověření uniknutých informací spjatých s konkrétní doménou, které byly zveřejněny na internetu anebo darknetu. Služba se zaměřuje na uniklá hesla, účty spojené s doménou, IP adresy nebo prolomené počítače a přístupy do infrastruktury či aplikací. Je možné například vyhledávat i uniklé firemní kreditní karty, vyhledávané pojmy a/nebo vyplněné formuláře uživatelem, kde součástí reportu jsou i odcizená surová data. Služba spočívá v tom, že za Vás provedeme kompletní hledání úniku dat. Hledání probíhá v prostředí internetu a darknetu, a to v masivních databázích hesel, v telegramových skupinách, na ransomwarových tržištích a v dalších zdrojích typických pro kybernetickou trestnou činnost. Služba je poskytovaná využitím databází a platformy Alerts Bar Inc., ve spolupráci se zastupující firmou AARTKOM s.r.o..

Služba se zaměřuje na kontrolu následujících typů úniku a uniklých dat:

- Přihlašovací údaje (dle domény a/nebo emailu).
- Únik firemních platebních prostředků (kreditní karty a/nebo kryptopeněženky).
- Detaily k prolomenému počítači a zařízení (HW a ID zařízení, uživatel, verze OS, SW, atd.).
- Přístupy do vzdálených ploch (IP sítě a subnety, domény a subdomény).
- Prověření zneužitelnosti zachycených Cookies (pro obcházení více faktorového ověření).
- Shrnutí citlivých souborů a informací, které unikly v rámci plochy nebo prohlížeče.

Poskytnuté výstupy

Výsledkem analýzy je přehledný report, který shrnuje seznam a typ zjištěného úniku, včetně všech odcizených údajů. Nalezené informace, ať už se jedná o prolomený počítač zaměstnance nebo uniklé přihlášení zákazníka, budou po předchozím souhlasu manuálně ověřovány. Předaný report a seznam obsahuje klíčové detaily o uživatelském jménu, heslu, datu záchytu úniku a přesném typu úniku, včetně informací k infikovanému PC, souhrnu zneužitelnosti spojení, nebo detailů k infikovanému zaměstnanci či zákazníkovi.

Potřebná součinnost: manažer kybernetické bezpečnosti nebo ICT administrátor.

Doba realizace: 1-4 týdny od objednání

Obchodní podmínky

- Kontaktujte nás pro vypracování individuální nabídky, která zohlední velikost vaší organizace, popularitu vašich domén a požadovanou úroveň detailu reportu
- Služba je hrazena zhotoviteli fakturou se splatnostní 30 dní po objednání služby.

- Objednatel informuje zhotovitele minimálně 10 pracovních dní dopředu o termínech vykonání služby a zpracování detailního reportu rizik o uniklých datech na darknetu.
- Služba je podmíněna podpisem smlouvy o dílo. Tato nabídka se stává nedílnou součástí smluvní dokumentace.
- Objednáním služby dle této nabídky akceptujete Obchodní podmínky zhotovitele dostupné na adrese: https://www.dns.cz/obchodni-podminky.
- Nabídka je platná jako celek bez úprav.
- Nabídka je platná 30 dní.