Předpovědi vývoje na dark webu a darknet trhu pro rok 2025

20.12.2024 - | PROTEXT

Narušení ochrany dat prostřednictvím napadení dodavatelů

Při zneužívání důvěryhodných vztahů mezi firmou a jejím dodavatelem proniknou aktéři hrozeb nejprve do systémů dodavatele a přes něj získají přístup do infrastruktury cílové organizace. Takové útoky vedou někdy k významným únikům dat – jako například v případě, kdy útočníci údajně získali přístup ke cloudovému účtu Snowflake společnosti Ticketmaster prolomením systému třetí smluvní strany. Dalším významným aktérem využívajícím tuto taktiku byla skupina IntelBroker – ta a její spřízněný gang údajně pronikli prostřednictvím třetích stran do společností Nokia, Ford, řady zákazníků společnosti Cisco včetně Microsoftu a dalších.

Společnost Kaspersky tvrdí, že v roce 2025 bude počet útoků prostřednictvím dodavatelů nadále narůstat, a to povede k napadání dat u hlavních koncových cílů. Cloudové platformy a IT služby často ukládají a zpracovávají firemní data z více organizací, což znamená, že průnik do pouhé jedné organizace může otevřít dveře k mnoha dalším. Je třeba poznamenat, že narušení bezpečnosti se nemusí nutně týkat kritických aktiv, aby bylo destruktivní. Ne každý inzerát o úniku dat na temném webu je výsledkem skutečně závažného incidentu. Některé „nabídky“ mohou být prostě jen dobře marketingově zpracované materiály – například některé databáze mohou kombinovat veřejně dostupná nebo dříve uniklá data a prezentovat je jako aktuální průnik nebo jen tvrdit, že jde o narušení bezpečnosti známé značky. Vytvořením humbuku kolem starých a pravděpodobně již irelevantních dat mohou kyberzločinci vyvolat publicitu, rozruch a poškodit pověst dodavatele i jeho zákazníků.

Obecně jsme na temném webu zaznamenali celkový nárůst četnosti inzerátů týkajících se firemních databází. Například na jednom z populárních fór se v období srpen–listopad 2024 zvýšil počet souvisejících příspěvků o 40 % ve srovnání se stejným obdobím loňského roku a dosáhl několika vrcholů.

I když lze část tohoto nárůstu přičíst opětovnému zveřejnění nebo kombinaci starších úniků, kyberzločinci mají zjevně zájem o šíření uniklých dat, ať už nových nebo starých, či dokonce falešných. V roce 2025 tedy pravděpodobně budeme svědky nejen nárůstu počtu hackerských útoků a úniků firemních dat prostřednictvím napadení dodavatelů, ale také obecného nárůstu případů narušení bezpečnosti dat.

Migrace trestné činnosti z Telegramu na fóra temného webu

Navzdory nárůstu aktivity kyberzločinců na Telegramu v roce 2024 očekáváme, že se stínová komunita přesune zpět na fóra temného webu. Správci stínových kanálů Telegramu totiž upozorňují na jejich stále častější zakazování:

Očekává se, že návrat nebo příchod kyberzločinců na fóra temného webu zvýší konkurenci mezi těmito zdroji. Aby vynikli a přilákali nové publikum, začnou provozovatelé fóra pravděpodobně zavádět nové funkce a zlepšovat podmínky pro obchodování s daty. Mezi ně mohou patřit automatizované služby uzavírání smluv, zjednodušené procesy řešení sporů a zdokonalená opatření pro zajištění bezpečnosti a anonymity.

Nárůst významných operací orgánů činných v trestním řízení proti skupinám páchajícím kybernetickou trestnou činnost

Rok 2024 byl významným rokem v celosvětovém boji proti kyberkriminalitě. Po světě proběhla spousta úspěšných operací: „Cronos“ proti LockBitu, likvidace BreachForums, zatčení členů klubu WWH, úspěšných iniciativ jako „Magnus“ proti RedLine a Meta stealers a „Endgame“ proti malwaru TrickBot, IcedID a SmokeLoader, a mnoho dalších. Na úsilí orgánů činných v trestním řízení v boji proti kybernetické kriminalitě se aktivně podílela také společnost Kaspersky. Podpořili jsme například akci koordinovanou INTERPOLem s cílem narušit působení malwaru Grandoreiro, pomáhali jsme bojovat proti kybernetické kriminalitě během olympijských her 2024 a přispěli jsme k operaci Synergie II, jejímž cílem bylo omezit kybernetické hrozby, například cílený phishing, ransomware a infostealery, a pomáhali jsme i při společné operaci INTERPOLu a AFRIPOLu v boji proti kybernetické kriminalitě v Africe. Tyto a mnohé další případy ukázaly význam koordinace a spolupráce mezi orgány pro prosazování zákonů a organizacemi zabývajícími se kybernetickou bezpečností.

Předpokládáme, že v roce 2025 dojde k nárůstu zatýkání kyberzločineckých skupin a likvidaci jejich infrastruktur a fór, které získají publicitu. V reakci na úspěšné policejní operace v roce 2024 však aktéři hrozeb pravděpodobně změní svou taktiku a stáhnou se do hlubších a anonymnějších vrstev temného webu. Očekáváme také vznik uzavřených fór a nárůst modelů přístupu pouze na pozvánky.

Nárůst propagace stealerů a drainerů jako služeb na temném webu

Kryptoměny jsou již několik let jedním z hlavních cílů kyberzločinců. Lákají uživatele kryptoměn pod různými záminkami na podvodné stránky a boty na Telegramu a přidávají další funkce pro krádeže kryptoměn do infostealerů a bankovních trojanů. Kurz Bitcoinu láme rekord za rekordem, lze tedy očekávat, že popularita drainerů, navržených speciálně ke krádeži kryptoměnových tokenů z peněženek obětí, bude s největší pravděpodobností přetrvávat i v příštím roce.

Infostealery jsou dalším typem malwaru, který ze zařízení uživatelů získává citlivé informace, včetně soukromých klíčů k peněženkám s kryptoměnami, hesel, cookie souborů a dat pro automatické vyplňování položek v prohlížečích. V posledních letech jsme pozorovali dramatický nárůst úniků přístupových údajů způsobených tímto malwarem a očekáváme, že tento trend bude přetrvávat a déle se vyvíjet. S největší pravděpodobností se objeví nové rodiny stealerů a zároveň se zvýší aktivita těch stávajících.

Stealery i drainery budou na temném webu pravděpodobně stále častěji propagovány jako služby. Malware jako služba (MaaS) nebo jeho „předplatné“ je obchodní model temného webu, který zahrnuje pronájem softwaru k provádění kybernetických útoků. Klientům těchto služeb je obvykle nabízen osobní účet, prostřednictvím kterého mohou útok řídit, a také technická podpora. Tím se snižuje počáteční práh odborných znalostí, které potenciální kyberzločinci potřebují.

Kromě nabídek samotných stealerů nebo drainerů se na temném webu setkáváme také s inzeráty, které hledají traffery – osoby, které pomáhají kyberzločincům distribuovat a propagovat stealery, drainery nebo podvodné a phishingové stránky.

Eskalace hrozeb na Blízkém východě: hacktivismus a ransomware na vzestupu

Podle databáze Kaspersky Digital Footprint Intelligence (DFI) byly v první polovině roku 2024 jednou z nejzávažnějších kyberbezpečnostních hrozeb na Blízkém východě souvisejících s aktivitami na temném webu akce hacktivistů – hackerů provádějících politicky motivované kybernetické útoky. V regionu došlo k nárůstu těchto hrozeb v důsledku současné geopolitické situace, která, pokud se

napětí nesníží, bude pravděpodobně dále narůstat.

Výzkumníci shromažďující údaje pro Kaspersky DFI zaznamenali v celém regionu více než 11 hacktivistických hnutí a různých aktérů. V návaznosti na současnou geopolitickou nestabilitu se útoky hacktivistů již přesouvají od DDoS útoků a poškozování webových stránek k závažným narušením bezpečnosti, jako jsou úniky dat a kompromitace cílových organizací.

Další hrozbou, která bude v regionu pravděpodobně i nadále velmi aktivní, je ransomware. V posledních dvou letech došlo na Blízkém východě k prudkému nárůstu počtu obětí ransomwarových útoků, který výrazně vzrostl z průměrných 28 za půl roku v období 2022–2023 na 45 v první polovině roku 2024. Tento trend bude pravděpodobně přetrvávat i v roce 2025.

https://www.ceskenoviny.cz/tiskove/zpravy/predpovedi-vyvoje-na-dark-webu-a-darknet-trhu-pro-rok-2025/2611463