

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **2** ze dne **14.12.2021**

FINANČNÍ HROZBY V ROCE 2022 - ÚTOKY NA PLATEBNÍ SYSTÉMY, RŮST INFOSTEALERŮ A ZNEUŽÍVÁNÍ KRYPTOMĚN.

Státem podporované hackerské skupiny, které se zaměří na zneužívání kryptoměn, a kyberzločinci, kteří se budou snažit okrádat investory vytvářením podvodných digitálních peněženek se zadními vrátky. To jsou hlavní finanční hrozby na rok 2022. Kromě toho pravděpodobně zažijeme nárůst útoků na platební systémy a více pokročilých mobilních hrozeb, shrnuje nejnovější zpráva Cyberthreats to Financial Organizations in 2022 (Kybernetické hrozby pro finanční organizace v roce 2022).

Rok 2021 přinesl mnoho výzev a změn. Vždy se ale najdou tací, co se dokáží rychle zorientovat a přizpůsobit, aby tyto změny zneužili ve svůj prospěch. Většinu těchto kyberzločinců motivují peníze, proto mezi nejvýznamnější bezpečnostní hrozby loňského roku patřily útoky na finance. Analytici předpověděli při hodnocení významných událostí a trendů v sektoru finančních hrozeb v roce 2021 několik důležitých prognóz, které očekávají v roce 2022. Zde jsou jejich klíčová zjištění:

- **Bude přibývat cílených útoků na kryptoměny.** Jde o digitální aktiva, u nichž se všechny transakce uskutečňují online a uživatelé zůstávají anonymní – to vše je velmi atraktivní záležitost pro kyberzločince. Na toto odvětví se však zaměřují nejen známé kyberzločinecké organizace, ale i státem sponzorovaní aktéři hrozeb. Už nějakou dobu pozorujeme, jak se skupiny využívající APT rozrůstají a agresivně útočí na kryptoměnový byznys, a předpokládáme, že v tom budou pokračovat.
- **Špatné zabezpečení a podvodné hardwarové peněženky jako hardwarové hrozby pro kryptoměny.** Útoky na kryptoměny jsou stále cílenější a kyberzločinci přicházejí s novými způsoby, jak ukrást finanční aktiva investorů. V případě příležitostí souvisejících s investicemi do kryptoměn výzkumníci odhadují, že kyberzločinci budou využívat výroby a prodeje podvodných zařízení se zadními vrátky, doplněné kampaněmi sociálního inženýrství a dalšími technikami k odcizení finančních aktiv obětí.
- **Rychlejší a rozsáhlejší nasazování infostealerů.** Malware pro krádež informací bude díky svojí jednoduchosti, cenové dostupnosti a účinnosti častým nástrojem při útocích na finanční aktiva, přinejmenším pro prvotní sběr dat. Aktéři hrozeb budou využívat výhody infostealerů k vytipování obětí, například k následným cíleným finančním, ransomwarovým nebo jiným útokům.
- **Konsolidace vývoje škodlivých kódů pro mobilní zařízení.** Pandemie přispěla k rozvoji mobilního bankovníctví, které získalo mnoho dalších funkcí. Experti proto očekávají více mobilních bankovních trojských koní pro Android, zejména typu RAT, které dokážou obejít bezpečnostní prostředky využívané bankami (například OTP a MFA). Lokální a regionální projekty škodlivých kódů pro Android se začnou využívat v globálním měřítku a začne export útoků do západní Evropy a dalších zemí světa.

„Letošní rok byl pro mnoho organizací velmi náročný – musely zajišťovat vzdálený přístup pro zaměstnance pracující z domu, záplatovat systémy připojené k internetu, aby vydržely nápor ransomwaru, a také se vypořádat s výrazným nárůstem mobilního bankovníctví a souvisejících malwarových implantátů. Kyberzločinci se nezdráhali využívat nabídky z tržišť na darkwebu, kde je k mání celá řada škodlivých kódů. Zaznamenali jsme, jak původně regionální kyberzločinci expandují do dalších částí světa, což ztěžuje práci lidem z oblasti kybernetické bezpečnosti. Proto je důležité určit hlavní trendy v neustále se vyvíjejícím prostředí finančních hrozeb a sdílet naše odborné znalosti, abychom pomohli firmám připravit se na ochranu před těmito hrozbami,“ říká Dmitrij Bestužev, vedoucí globálního výzkumného a analytického týmu (GReAT).

zdroj: Avcentrum ČR