Kyberhrozby dosáhly tříletého maxima; Podvody v Česku za 2. čtvrtletí narostly o 81 %, na Slovensku o 57 %

10.8.2023 - | Avast Software

PRAHA, Česko & TEMPE, Arizona, 10. srpna 2023

Podle Avastu, přední značky v oblasti digitální bezpečnosti a ochrany soukromí společnosti Gen™ (NASDAQ: GEN), v současnosti bezpečnost na internetu nejvíce ohrožuje sociální inženýrství, tedy psychologické manipulování s lidmi, aby sdíleli své osobní údaje. Nejnovější zpráva Avastu o hrozbách za 2. čtvrtletí uvádí, že více než 75 % všech detekovaných hrozeb na počítačích mají na svědomí podvody, phishing a malvertising. Data za čtvrtletí od dubna do června 2023 také ukázala výrazný celkový nárůst kybernetických rizik, přičemž počet zablokovaných unikátních útoků se oproti předchozímu období zvýšil globálně o 24 %, což je nejvyšší zaznamenané riziko za poslední tři roky.

„Zaznamenali jsme výrazný posun ve sféře kyberbezpečnosti," říká ředitel výzkumu malwaru v Avastu Jakub Křoustek. „Nejenže množství hrozeb patří k nejvyšším v historii, ale kyberzločinci se také častěji uchylují k psychologickým manipulacím než k tradičním technikám malwarových útoků. Z toho vyplývá nejen potřeba přizpůsobit zabezpečení, ale také aby lidé lépe porozuměli podvodům a vzdělávali se, což poslouží jako další vrstva obrany."

Podvodů všech typů stále přibývá a nyní tvoří více než tři čtvrtiny všech detekcí. Jen v období od dubna do června odhalili výzkumníci Avastu celou řadu účinných podvodů, od podvodných seznamek (zde došlo ke zvýšení o 39 % oproti předchozímu kvartálu) přes podvodné dárcovské stránky a klamavou reklamu až po tisíce nových phishingových e-mailů. Metody se mohou lišit, ale konečný cíl zůstává stejný: přesvědčit nic netušící osoby, aby prozradily citlivé informace nebo se rozloučily se svými těžce vydělanými penězi.

Phishing – žádosti o informace zdánlivě od známého a důvěryhodného subjektu, jako je banka nebo úřad – představoval ve 2. čtvrtletí 25 % všech hrozeb. Využívá přirozené lidské důvěry a navozuje pocit naléhavosti, čímž nutí oběti, aby prozradily důvěrné informace nebo se zapojily do finančních transakcí pod falešnou záminkou. Kromě toho se rozšířil tzv. smishing – phishing prostřednictvím SMS –, který využívá vysoké míry otevírání textových zpráv a přirozené důvěry, již k nim lidé mají.

Ukazují se i budoucí mobilní trendy, například to, že kyberzločinci využívají umělou inteligenci k vytváření téměř dokonalých napodobenin legitimní komunikace, takže pro jednotlivce je stále obtížnější rozlišit, co je skutečné a co ne.

K zemím, v nichž došlo k největšímu nárůstu v podvodech, patří i Česko, kde se míra podvodů zvedla o 81 %. Na Slovensku to bylo o 57 %. Počet podvodů se nejvíce zvýšil ve Vietnamu (více než třikrát), dále i v Argentině (o 117 %), Španělsku (o 112 %), Francii (o 97 %), Brazílii (o 95 %), Mexiku (o 87 %) a Velké Británii (o 78 %).

Ačkoli se ve druhém čtvrtletí ve srovnání s předchozím kvartálem snížil výskyt adwaru, stále přetrvává na desktopu, mobilních zařízeních a v prohlížečích. Pozoruhodným příkladem je kampaň HiddenAds, adware napojený na známé herní aplikace, která během svého kralování v obchodě s aplikacemi zaznamenala desítky milionů stažení.

Prostředí těžby kryptoměn se neustále vyvíjí, tzv. coinminery se tak potýkají s poklesem aktivit. V prvním čtvrtletí 2023 klesla míra rizika o 4 %. Podíl na tom měly i potíže autorů malwaru v důsledku přechodu z algoritmu proof-of-work na proof-of-stake u řady kryptoměn.

Výzkumníci Avastu objevili nové trojské koně pro vzdálený přístup, jako je HotRat či AsyncRat reimplementovaný pro .NET, který obsahuje řadu nových příkazů a funkcí.

Dalším úspěšným objevem byla zranitelnost CVE-2023-29336, lokální zvýšení oprávnění ovladače win32k v jádře systému Windows. Díky rychlé reakci byla chyba opravena v květnové aktualizaci zabezpečení a uživatelé upozorněni.

Ransomware zůstával i ve 2. čtvrtletí roku 2023 stále velkým problémem. I přes mírný pokles v šíření se autoři ransomwaru nadále zaměřují na konkrétní oběti a při průniku do firemních sítí stále více spoléhají na cílené útoky a exploity. Kromě toho častěji experimentují s novými taktikami, jako jsou techniky vydírání obětí, aniž by jejich data skutečně zašifrovali, nebo doxing. To dokazují zejména úspěšné útoky na široce používaný software, jako je PaperCut.

Výzkumníci Avastu vyvinuli bezplatný dešifrovací nástroj pro ransomware Akira, aby pomohli napadeným lidem a firmám. Tento nástroj již pomohl mnoha vydíraným obětem i podnikům při obnově souborů, což ještě zdůrazňuje závazek poskytovat softwarová řešení a pomoc těm, kteří je potřebují.

Špičkovou ochranu proti phishingovým útokům poskytují produkty Avast Free Antivirus, všechny prémiové verze Avastu i prohlížeč Avast Secure Browser, což potvrzují i čtvrtletní testy nezávislé testovací organizace AV-Comparatives.

Celou zprávu Avastu o hrozbách za 2. čtvrtletí 2023 naleznete na:
https://decoded.avast.io/threatresearch/avast-q2-2023-threat-report/

http://press.avast.com/cs-cz/avast-kyberhrozby-dosahly-trileteho-maxima-podvody-v-cesku-za-2-ctvrtleti-narostly-o-81-na-slovensku-o-57-