Iparszerű módszerekkel okoznak dollármilliárdos károkat az e-mail levelezésre szakosodott adathalászok

Az elmúlt négy évben 38 százalékkal növekedett az üzleti levelezést célkeresztbe állító adathalász támadások száma a Microsoft friss kiberbiztonsági jelentése, a Cyber Signals szerint. A bűnözők kifinomult, és ma már szolgáltatásként is árult módszerek bevetésével tévesztik meg a felhasználókat. A jelentés megoldásokat is kínál a támadások elhárítására és a kockázatok csökkentésére.

A Microsoft negyedik alkalommal hozta nyilvánosságra Cyber Signals című kiberbiztonsági jelentését. Ebben rámutatott: egyre erőteljesebb az az adathalász tevékenység, amelynek fókuszában az üzenetváltások, különösen az üzleti, munkahelyi email levelezés áll. A Microsoft 2019 és 2022 között a kiberbűnözés, mint szolgáltatás (CaaS) igénybevételének 38 százalékos növekedését regisztrálta, miközben ezek többsége az üzleti levelezést vette célba.

Az üzleti levelezést érintő támadások évről évre dollármilliárdokra rúgó károkat okoznak a vállalatoknak. 2022-ben az FBI kiberbűnözők által okozott károk megelőzésére szakosodott csapata, a Recovery Asset Team (RAT) Financial Fraud Kill Chain (FFKC) néven indított programot, amely eddig 2 838 üzleti levelezést érintő ügyben több mint 590 millió dollárnyi kárt hárított el.

Az üzleti levelezésekre szakosodott kiberbűnözők súlyos fenyegetést jelentenek a szervezetek számára, és komoly károkat képesek okozni. Az FBI friss jelentésében 21 832 ilyen jellegű feljelentésről számolt be 2022-ben, amelyek nyomán több mint 2,7 milliárd dollár kár keletkezett.

Az üzleti levelezést érő támadások abban térnek el más kibertámadásoktól, hogy erőteljesen építenek az emberi viselkedésmintákra, és mesterfokon űzik a megtévesztést. 2022 és 2023 áprilisa között a Microsoft Threat Intelligence 35 millió üzleti levelezést érintő esetet tárt fel és vizsgált ki, ami azt jelenti, hogy átlagosan naponta mintegy 156 000 támadási kísérlettel volt dolguk.

Milyen taktikákat vetnek be az adathalászok az üzleti levelezést célzó támadásaik közben?

A bűnözők számtalan formában igyekeznek megtéveszteni áldozataikat. Előfordul, hogy felhívják őket telefonon, SMS-t küldenek nekik, vagy a közösségi médiában írnak rájuk. Tipikus, hogy a személyazonosság megerősítését kérik valamilyen kitalált ügy miatt, és gyakran lépnek fel más személy vagy egy vállalat nevében. Ahelyett, hogy a nem megfelelő védett eszközök sérülékenységeit használnák ki, az üzleti levelezésekre szakosodott adathalászok a mindennapi e-mail-levelezésbe és az egyéb módon zajló üzenetváltásokba kapcsolódnak be azért, hogy rávegyék áldozataikat banki adataik kiadására, vagy az adataik felhasználásával, a tudtukon kívül, a nevükben végeznek bűncselekményekhez kötődő pénzátutalásokat.

A látványos zsarolóvírusos támadásoktól eltérően, amelyekhez a fenyegető hangvételű zsaroló üzenetek is hozzátartoznak, az e-mail levelezésre szakosodott adathalászok udvariasabb modorban, de annál magabiztosabban dolgoznak: kitalált határidőkkel nyomasztják az áldozataikat, akik ilyenkor megfeledkeznek az óvatosságról, vagy fel sem merül bennük a gyanú, hiszen hozzá vannak szokva az ilyen sürgetésekhez. Ezek a bűnözők nem állnak elő valamilyen soha nem látott szoftverrel. Ők inkább olyan módszerekre hagyatkoznak, amelyekkel a lehető legtöbb embert lehet megszólítani; amelyek

hitelessé és megbízhatóvá teszi őket a legtöbb ember szemében, és olyan csaló üzeneteket küldenek ki tömegével, amelyek előre megjósolható magas arányban érnek célba.

A Microsoft azt is megállapította, hogy a támadók egyre gyakrabban használnak olyan platformokat, mint például a BulletProofLink, amelyekkel ipari méretekben lehet előállítani és kampányszerűen kiküldeni csaló üzenteket. Ezek a platformok komplett szolgáltatáscsomagot kínálnak a bűnözők számára, amelyek tartalmazzák a szövegterveket, a hosztingot és az automatizált funkciókat. Akik a kiberbűnözést szolgáltatásként (CaaS) veszik igénybe, IP-címeket is kapnak, amelyek a kampányok célcsoportjainak meghatározását segítik. A decentralizált átjáróval rendelkező BulletProofLink platformot – amely gazdagépként blokkláncra csatlakoztatott internetalapú számítógépeket is kínál az adathalász és csaló üzeneteket terjesztésére – jóval nehezebb leleplezni és hatástalanítani. Ezek az oldalak az egyre komplexebb és folyamatosan fejlődő nyilvános blokklánc-technológián alapulnak, emiatt az azonosításukat és a hatástalanításukat célzó műveletek is egyre összetettebbek.

Már eddigi is nagyon sok nagyszabású támadást hajtottak végre egyéni IP-címek felhasználásával, ám a Microsoft a bűnüldöző szervekkel és más szervezetekkel együtt attól tart, hogy ezek száma a jövőben gyors ütemben még tovább emelkedhet, miközben a hagyományos riasztások és értesítések hamarosan elégtelennek bizonyulhatnak a leleplezésükre. A Microsoft Digitális Bűnözés Elleni Osztálya arra is rávilágított: azok a szervezetek, amelyek a kiberbűnözést szolgáltatásként értékesítik, új szolgáltatásokat kezdtek el kínálni, például a potenciális áldozatok kontaktadatait és IP-címeit, amelyek segítségével olyan széleskörű adathalász kampányokat lehet indítani, amelyeket nagyon nehéz felderíteni és hatástalanítani.

Annak ellenére, hogy speciális megoldásokat fejlesztettek ki az üzenetváltásokra szakosodott bűnözők számára – például adathalász szolgáltatáscsomagokat, magasrangú cégvezetők, valamilyen cégnek rendszeres kifizetéseket lebonyolító, vagy más okból sajátos pozíciót betöltő emberek e-mail címeit tartalmazó listákat –, léteznek olyan módszerek, amelyekkel a szervezetek kivédhetik ezeket a támadásokat, és mérsékelhetik a kockázataikat.

A sokasodó támadások arra is rámutatnak, hogy miért szükséges a kiberbűnözés ellen az IT, a jogi osztály, és a kibertámadások elhárításáért felelős csapat mellett a vállalatvezetés, a pénzügy, a HR és akár további szakterületek bevonásával közösen fellépni: utóbbiak kezelnek például olyan szenzitív munkavállalói adatokat, mint amilyenek a társadalombiztosítási számok, az adóbevallások, az elérhetőségi adatok és a napi időbeosztás.

Mit érdemes tenni az üzleti levelezést célzó kiberbűnözői tevékenység ellen?

- Biztonságos levelezőrendszer. Manapság a felhőalapú e-mail levelező rendszerek mesterséges intelligenciára alapuló technológiákat, például gépi tanulást használnak a védelem megerősítése érdekében. Ez az adathalász támadások ellen nyújt hatékony védelmet, miközben nyomonköveti a gyanús levéltovábbításokat is. A felhőalapú levelező és kollaborációs alkalmazásoknak megvan az az előnyük is, hogy folyamatosan és automatikusan frissülnek, és egységes kiberbiztonsági szabványoknak felelnek meg.
- A felhasználói adatok védelme a rendszerbe történő behatolás megakadályozása érdekében. Az üzleti levelezésre szakosodott bűnözőkkel szembeni küzdelem első lépése a felhasználói adatok védelme. Az alkalmazásokhoz és adatokhoz csak ellenőrzött módon, a „Zéró bizalom elv” érvényesítése és automatizált protokollok mellett lehessen hozzáférni.
- Biztonságos fizetési platform használata. Az e-mailen érkező számlák helyet érdemes lehet megfontolni egy olyan rendszer alkalmazását, amit kifejezetten a kifizetések hitelesítésére terveztek.

- Tegyük képessé a munkavállalókat a gyanús jelek felismerésére! A munkavállalókat folyamatosan képezni kell arra, hogy milyen jelekből ismerhetik fel, ha egy e-mailt csaló, vagy más ártó szándékkal küldtek nekik (pl. a domain és az e-mail cím eltérő), és hogy milyen kockázatokkal és károkkal járhat egy sikeres támadás.

Az idézett Cyber Signals jelentés negyedik kiadása ide kattintva érthető el teljes terjedelmében.

Sajtókapcsolat:

- Kovács Ágnes Veronika, PR és vállalati kommunikációs vezető
- +36 1 267 4636
- sajto@microsoft.com

Eredeti tartalom: Microsoft

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el: https://hellosajto.hu/3886/iparszeru-modszerekkel-okoznak-dollarmilliardos-karokat-az-e-mail-levelezesre-szakosodott-adathalaszok/