COFENSE

2022
Q1, Q2
Adathalász trendek

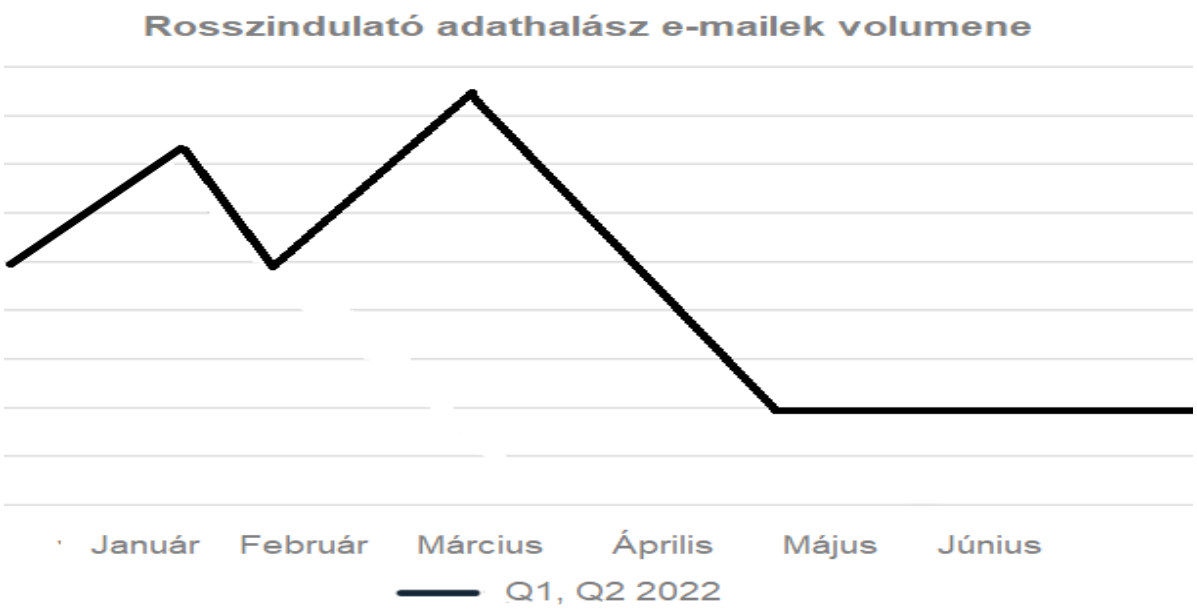
Nem kérdés, hogy 2021 a zsarolóvírusok és a nulladik napi sérülékenységek, na meg a COVID-19 éve volt. A káros kódok és vírusok ellen ádáz küzdelmet folytattak a kiberbiztonsági és az egészségügyi szakemberek is.

Adódhat a kérdés, hogy a pandémia miként és miért is került ide, az adathalász trendeket és azok statisztikáit bemutató összefoglalóba? Úgy, hogy a kiberbűnözők borzasztóan jól alkalmazkodnak minden szituációhoz, így nem kellett sokat várni arra, hogy a koronavírushoz kapcsolódó adathalász e-mailek elterjedjenek a világban, és még 2021-ben, sőt 2022-ben is aktívan keringjenek a kibertérben. Alapvetően ez a trend 2022 első felében sem változott meg, bár az adathalász e-mailek tekintetében sok minden másra is érdemes figyelni.

Összességében elmondható, hogy a megfigyelt adathalász tevékenység 2022 első félévében - az előző évhez képest - növekvő tendenciát mutatott, kiemelten pedig 2022 első negyedve volt erősebb az adathalász kampányok tekintetében, a második negyedévben kisebb csökkenés mutatkozott, főként az Emotet mérséklődésének köszönhetően. Viszont ha Emotet nélkül nézzük a big picture-t, akkor az egyéb rosszindulatú programcsaládokat kézbesítő adathalász e-mailek mennyisége Q2-ben is növekedett. A márciusi nagymértékű kiugrás után, a második negyedév végig stabil maradt, és nem volt tapasztalható kiugró érték.

Az adatok elemzése során megállapítást nyert, hogy az Emotet és a QakBot üzemeltetői új kézbesítési mechanizmusokat vezettek be adathalász kampányaik során, valószínűleg a Microsoft által az Office makrók alapértelmezett beállításainak módosítása miatt. A fél év során nagy hangsúlyt kapott a Business Email Compromise (BEC) nevű adathalászat, ami egyébiránt a legköltségesebb e-mail fenyegetési forma.

A jelentésben szereplő adatok legnagyobb része a Cofense Phishing Defense Center (PDC) kutatólaborjának és a Cofense egyéb e-mail biztonsági szolgáltatásai során keletkeztek. A Cofense PDC több millió adatot elemez évente, így a fenyegetettségi szereplők taktikáival és technikáival kapcsolatos meglátásai első kézből származó, friss információk.



A rosszindulatú adathalász e-mailek volumene 2022 első fél évében

A fenti diagramon jól látható, hogy a rosszindulatú adathalász e-mailek száma az első negyedévben volt meghatározóbb, míg ez a tendencia áprilistól kezdődően csökkenésnek indult. Májusban és júniusban pedig egy átlag alatti szinten stagnáltak a számok, de azért így is jelentős volumenről lehet beszélni.

Az év első felében a felhasználók olyan meghatározó csalásokkal találhatták magukat szemben, mint például az orosz-ukrán konfliktushoz kapcsolódó adathalász tevékenység, vagy éppen az EMOTET kártevővel végrehajtott támadások. Az általános adathalász tevékenységet az EMOTET botnet teljes működőképességének visszatérése nagyban befolyásolta, hiszen 2021 utolsó negyedévében visszatért a kártevő, de az ezt követő időszakban a volumen nem érte el a teljes potenciált. Bár kifejezetten jelentős volt ez az aktivitás és a teljes volumen is stabil maradt, de a korábbi csúcsokat meg sem közelítette.

TOP FIVE MALWARE TYPES	TOP FAMILY IN TYPE
Loader	Emotet/Geodo
Information Stealer	FormGrabber
Keylogger	Agent Tesla
Banker	QakBot
Remote Access Trojan	Remcos RAT

Top 5 malware típus és a hozzájuk köthető legjelentősebb malwere-családok

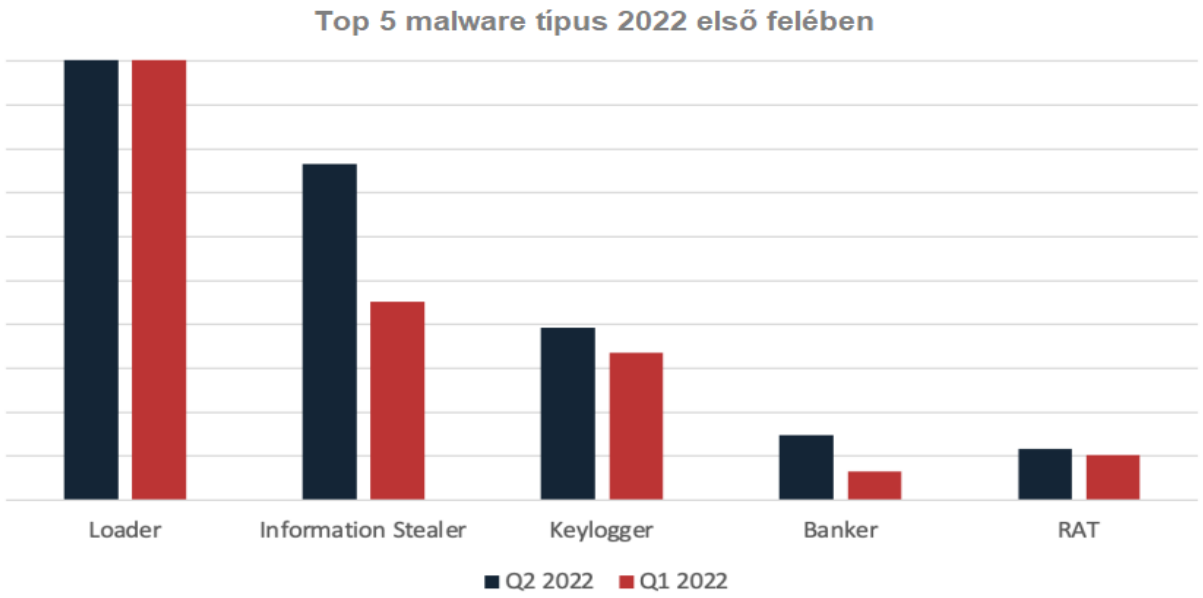
Az idei első fél évben a Loader-ek mennyisége továbbra is minden más rosszindulatú programtípust háttérbe szorított, köszönhetően az EMOTET-nek.

Az információlopók esetében a legnagyobb növekedést az olyan rosszindulatú szoftvercsaládok érték el, mint a FormBook és a Loki Bot.

Az Agent Tesla és a Snake keyloggerek a keyloggerek mennyiségének nagy százalékához járultak hozzá.

A banki kártevők – köszönhetően főleg a QakBot nevű káros kódnak – és a távoli hozzáférésű trójaik (a Remcos RAT és a NanoCore RAT jóvoltából) szintén tagjai az „exkluzív társaságnak”.

Az EMOTET mellett mi a QakBot nevű káros kódra hívnánk fel a figyelmet, ami az idei első fél évben a vállalati felhasználókat elérő legjelentősebb kártevőcsaládnak bizonyult. A QakBot-ot 2008ban fedezték fel, és gyakran Gold Lagoon néven is találkozhatunk ezzel a banki trójaival, ami – többek között - pénzügyi adatokat, böngészőinformációkat, billentyűleütéseket és hitelesítő adatokat képes ellopni.



A leggyakoribb malware típusok 2022 első fél évében

Ami az adathalászat során használt fájlkiterjesztéseket illeti: a .pdf csatolmányok a számítanak a legnépszerűbb kiterjesztés formátumnak a kiberbűnözők körében. 2022 második negyedévében még a korábbiakhoz képest is nagymértékű növekedést tapasztalhattunk ezzel a kiterjesztéssel kapcsolatosan, hiszen aránya több mint 40%-kal nőtt. Ez több mint a .html és .htm fájlok együttes 35%-os növekedési aránya.

Az olyan office fájlok, mint a .docx, .xlsx, .xls és .doc továbbra is megtalálhatóak az adathalász e-mail mellékletek top 10 fájlkiterjesztése között. Ezeket a fájlokat különböző célokra használják a bűnözők: például hitelesítő adatokat célzó adathalászathoz, rosszindulatú Office makrókhoz, és akár sebezhetőségek kihasználására is.

Top 10 leggyakrabban használt fájlkiterjesztés adathalász e-mailek esetében

Az elemzés következő szakasza olyan URL-címekre tér ki, melyeket hitelesítő adatokat célzó adathalász e-mailekben használtak, és amelyek védett környezetben lévő felhasználókhoz jutottak el. Az elemzett URL-címek a következők két kategóriába sorolhatóak: 1. és 2. szakaszba. Az 1. fázisú URL-ek az adathalász e-mailekbe ágyazódnak be, és a fertőzési lánc első lépéseként értelmezhetőek, míg a 2. fázisú URL-ek csak akkor érhetők el, ha a felhasználó a beágyazott URL-ek segítségével lépéseket tesz, tehát ha a felhasználó rákattint az URL-re.

Az alábbi képen a 10 leggyakoribb TLD (top-level domain, azaz legfelső szintű tartomány) látható, melyeket hitelesítő adatokat célzó adathalász e-mailekben használtak, és amelyek védett környezetben lévő felhasználókhoz jutottak el. Jól látható, hogy a .com TLD-t használó domainek az összes többi domaint az esetek kb. 50%-ában fordult elő adathalászat során, bár Q2-ben számuk kissé csökkent az első negyedévhez képest. A .net TLD 6.5% -os arányt ért el, és mellettük még az alábbi TLD-k kerültek be 2022 első fél évének top 10-es listájára: .co, .me, .org, .io, .br, .xyz és .in. Az egyetlen új belépő ebben a fél évben az .app TLD volt.

Ami az év hátralévő részét érinti: a Cofense szerint az év végéhez közeledve ismét növekvő tendenciát fog mutatni az adathalász támadások száma.

Továbbra is számolni kell az orosz-ukrán konfliktushoz köthető kampányokra, amelyek az idei év első negyedévében jelentek meg a kibertérben. A kiberbűnözők jelentős számú, főleg a kriptovaluta tulajdonosokat célzó adományozási csalási e-mail kampányt használtak a pénzügyi haszonszerzéshez, melynek folytatása a jövőben is prognosztizálható, hisze semmi jel nem utal arra, hogy a háború, illetve a konfliktus adathalászra gyakorolt hatása befejeződne.

A Qakbot nevű malware továbbra is aktív szereplője marad a kibertámadásoknak, hiszen – többek között - a Cofense Phishing Defense-nek bejelentett adathalász e-mailekben jelenleg is ez a legelterjettebb rosszindulatú szoftvercsalád. 2022 harmadik negyedében különösen figyelni kell rá, hiszen egy sikeres Qakbot fertőzés könnyen zsarolóvírus támadásba csaphat át.

A BEC (Business Email Compromise) típusú adathalász tevékenység volumene továbbra is emelkedő fázisban marad, hiszen a csalás végrehajtásához nincs szükség rosszindulatú programra, vagy egy-egy káros linkre, weboldalra. Ebben esetben a kiberbűnözők kizárólag az emberi interakciókra támaszkodnak, és így követik el támadásaikat. Röviden: a bűnözők a kiszemelt áldozat egyik felettesének álcája mögé bújva arra veszik rá a leendő áldozatot, hogy nagyobb összeget utaljon át a céges bankszámláról egy olyan számlára, amely mögött a hackerek állnak.

A világszerte tapasztalható gazdasági bizonytalanság önmagában komoly befolyásoló tényező lehet idén az adathalászat kapcsán, hiszen az adathalászfenyegetések általános volumene a legtöbb esetben a gazdasági változásokhoz igazodik. Így volt ez a COVID-19 elterjedése során is, amely időszak során számtalan olyan adathalász kampányt lehetett látni világszerte, melynek rengeteg felhasználó esett áldozatul.

A **Cofense** az adathalász támadások gyors megállítása érdekében 32 millió felhasználóból álló bázisából származó támadási információit vegyíti a fejlett automatizálással ellátott, és mesterséges intelligencia alapú technológiájával. A Cofense víziója szerint a jövőben az adathalász támadásokat már azelőtt megállítják, mielőtt a címzettnek esélye lenne az interakcióra. Szolgáltatásaik a vállalati felhasználók folyamatos és friss támadási információkkal ellátott biztonságtudatos oktatásra, és ennek a tudásnak, valamint a felhasználók viselkedésének rendszeres tesztelésére épülnek.

A biztributor vezető IT-biztonsági, hálózati és üzemeltetés-támogató disztribútor cég. Az általa képviselt gyártók közé tartozik többek között az APT-támadások elleni védelem szakértője, a **Trellix**, a kiberhírszerzés etalonja, a **Mandiant**, a vezetékes és Wi-Fi hálózatokban jeleskedő **Ruckus**, a sokszoros végpontvédelmi tesztgyőztes **Bitdefender**, valamint a kis- és középvállalati biztonságban stabil pontnak tekintett **GFI.**