# Drámaian megnőtt a COVID-19-hez kapcsolódó kibertámadások száma

Sajtóközlemény – 2020. 08. 12./PResston PR

**A világjárványhoz kapcsolódó adathalász és kártékony programokon alapuló támadások száma ugrásszerűen megnövekedett február óta. Március végéig meghaladta a 42.000-et azon weboldalak száma, *amelyek domainneve tartalmazza a „corona" vagy „covid" szavakat*, és sokat ezek közül haszonszerzési céllal hoztak létre. Ez a rendkívüli időszak ugyanis számos előnyt nyújtott a hackerek számára, akik a krízishelyzet kiaknázása érdekében felgyorsították működésüket. A Google áprilisi jelentése szerint a kiberbűnözők egy hét leforgása alatt több mint 18 millió malware-t és adathalász e-mailt küldtek a COVID-19-hez kapcsolódóan.**

## Célkeresztben a félelem

A hackerek egyik legfőbb taktikája a bizonytalanság és a feszültség kihasználása, hiszen a fokozott stressz hatására csökken a racionális gondolkodás képessége. Amikor nyugodtak vagyunk, könnyebben észreveszünk egy hamis e-mailt vagy gyanús weboldalt, ami bár szemlátomást nagyon hitelesnek tűnik, ám nyelvhasználatában és a megfogalmazás módjában is eltér a valóditól. A világjárvány megkönnyítette a csalók dolgát, ugyanis a vírustól való félelem és a korlátozások okozta bizonytalanság nehezítették a racionális gondolkodást.

Jó példa erre a koronavirus.gov.hu nevével szemérmetlenül visszaélő csalási kísérlet, amelyben a magyar kormány nevében próbáltak meg személyes adatokat begyűjteni az áldozatoktól. A levél írói azt ígérték a címzetteknek, hogy egy regisztrációs lap kitöltése után pénzügyi segítséget kapnak a kormánytól.

*„A spam látszólag a noreply KUKAC koronavirus PONT hu címről érkezett, és ebben arról tájékoztatnak, hogy a magyar kormány az Egészségügyi Világszervezettel együttműködve állítólag úgy döntött, hogy pénzügyi támogatást nyújt az új koronavírus elleni küzdelemben."*- mondta **Csizmazia-Darab István**, az ESET termékeket forgalmazó **Sicontact Kft.** biztonsági szakértője.

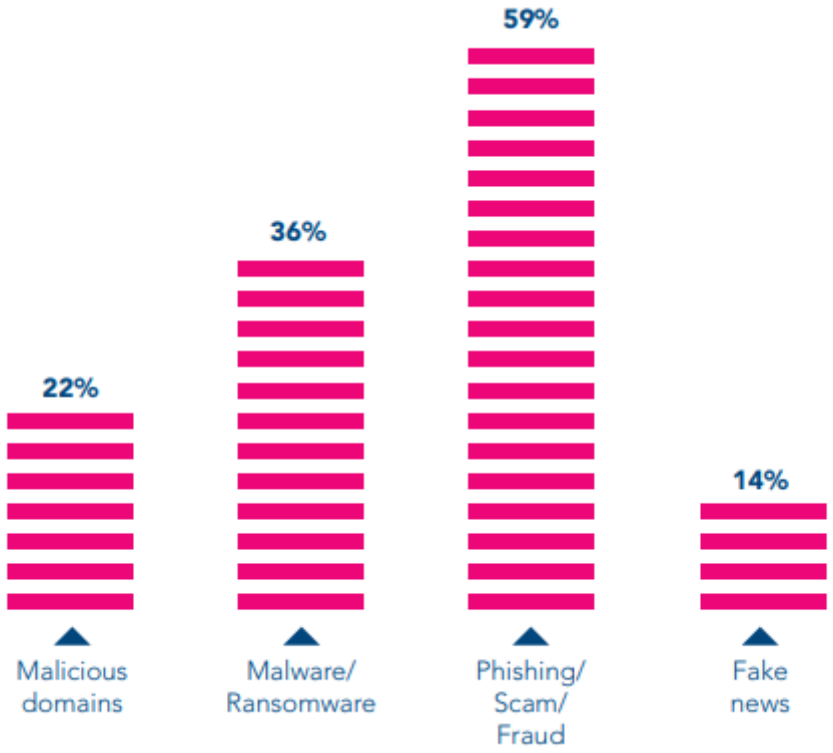
Természetesen kártérítésről szó sem volt, a hackerek célja a kitöltött regisztrációs lapon lévő személyes adatok ellopásában merült ki, melyeket aztán csalásokra, megszemélyesítéses támadásokra, sőt akár banki SIM Swap csalásokra is felhasználhatnak. Ez egy egyre inkább terjedő csalási forma, ahol a célszemélyről begyűjtött, kiszivárgott, ellopott személyes adatokkal visszaélve a nevében SIM kártya cserét kezdeményeznek a mobilszolgáltatónál, és így már ők kapják a banki kétfaktoros jóváhagyó és tájékoztató SMS üzeneteket.

**Megváltozott életviszonyok**

Egy másik nagy előny, amelyet a számítógépes bűnözők kaptak a világjárványtól, a normál, megszokott élet felborulása volt. Átlagos körülmények között a hivatalos szervezetektől érkező, az adatainkat bekérő üzenetek szokatlannak tűnnek, azonban a feje tetejére állt hétköznapokban nehezebbé vált kiszűrni a furcsaságokat.

A megváltozott életviszonyokra a kibertámadók is hamar reagáltak, kihasználva a felhasználók frusztrációját és bizonytalanságát.

Ezt bizonyítja az Interpol legfrissebb, 2020. augusztusi jelentése is, mely szerint a járvánnyal kapcsolatos leggyakoribb online fenyegetések az adathalászat és átverések, a kártevők és zsarolóprogramok, a rosszindulatú domainek, illetve az álhírek.




*A leggyakoribb online fenyegetések balról jobbra haladva: rosszindulatú domainek, kártevők és zsarolóprogramok, adathalászat/átverés/csalás, hamis hírkeltés*

*Forrás és fotókredit:* https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

**Magyarországot sem kímélték a hackerek**

Hazánkban például az elmúlt hónapokban többször próbáltak a Nemzeti Adó- és Vámhivatal nevében érzékeny adatokat lopni a támadók. Levelük szerint a felhasználó adóvisszatérítésre

jogosult, azonban ha az e-mailben található linkre kattintott, az egy adathalász weboldalra irányította.

*„Hogy csak néhány jelentősebb akciót emeljünk ki a tavaszi bevallási szezon időszakából, márciusban már kaphattunk a nav KUKAC info PONT com címről olyan értesítést, ami visszatérítés helyett adathalász oldalra vitt. Áprilisban arról olvashattunk, hogy több változatban is felbukkant már a százezres összegről szóló NAV nevével visszaélő üzenet, amely szintén a személyes és banki adatok lehalászására törekedett."*- mondta Csizmazia-Darab István.

Sokszor valóban nehéz felismerni a rosszindulatú e-maileket, hiszen hivatalos szervezetek nevében, azok arculatát felhasználva szólítják meg az áldozatokat. A védekezés érdekében a biztonságtudatos, óvatos online jelenlét mellett érdemes olyan vírusvédelmi programokat is használni, amelyek rendelkeznek adathalászat elleni funkcióval, mint például az ESET Internet Security.

További információ: https://www.eset.com/hu/otthoni/internet-security/

**Otthoni munkavégzés**

A koronavírus terjedése miatt egyre nagyobb mértékben kell digitális megoldásokra támaszkodnunk a mindennapi életünk során. Ezt a hackerek is jól tudják, és a felhasználók tapasztalatlanságát próbálják kihasználni -a járvánnyal kapcsolatos információkeresés mellett- az otthoni munkavégzés területén is.

Az egyik napról a másikra történő home office átállás következtében az emberek kiszolgáltatottabbá váltak a számítógépes támadásokkal szemben, mivel nehezebb megvédeni az otthoni hálózatokat a rájuk leselkedő veszélyektől. A statisztikák azt mutatják, hogy a vírusok, kártékony kódok 38%-a álcázza magát valamilyen Microsoft Office dokumentumnak, vagy használja fel ezt a formátumot a támadásokhoz.

*Az adathalászat és a kártevők számának növekedése mellett a visszaélések azokat a videókonferencia alkalmazásokat sem kímélték, amelyek az online munkavégzés alapvető feltételeivé váltak.* A legismertebb példa erre az úgynevezett *zoom-bombing* jelenség, amikor a nyilvános Zoom hívásokhoz illetéktelenek is csatlakoztak, és nem odaillő tartalmakat jelenítettek meg a gyanútlan résztvevők számára.

**Hogyan ne váljunk áldozattá?**

A fenti példák jól mutatják, hogy mennyire fontos tisztában lenni a digitális veszélyekkel, és azzal, hogyan óvhatjuk meg magunkat a számítógépes fenyegetésekkel szemben. *A digitális tudatosság szerepe napjainkban egyre inkább felértékelődik, hiszen ez egy olyan készség, amely segít megvédeni az érzékeny személyes és pénzügyi adatainkat az online térben.*

Az alábbiakban bemutatunk néhány kulcsfontosságú tippet, amelyek betartásával elkerülhetjük azt, hogy csalók áldozatává váljunk:

● Fő a nyugalom - a támadók igyekeznek időbeli nyomást gyakorolni az áldozatokra, hogy ösztönözzék őket a stresszhelyzetben történő döntéshozatalra, ezért ha sürgető e-mailt vagy üzenetet kapunk, vegyünk egy mély levegőt és **nyugodtan gondoljuk át** az abban leírtakat.

● Ellenőrizzük a feladót - ha olyan üzenetet kapunk, amely arra szólít fel, hogy kattintsunk egy linkre, vagy adjuk meg az érzékeny adatainkat, különösen fontos, hogy **ellenőrizzük a feladó hitelességét**. Ha kétségeink támadnak, **töröljük az üzenetet**, és vegyük fel a kapcsolatot a szervezettel, amelynek a nevében érkezett.

● Ellenőrizzük a feladó hivatalos weboldalát – minden esetben ajánlott a hivatalos weboldalakon tájékozódni, ezért ha e-mailt kapunk egy szervezet nevében, akkor **ne az üzenetben elhelyezett linket használjuk**, inkább keressünk rá a böngészőnkben.

● Végezzünk rendszeres frissítéseket - ha az alkalmazásokban sérülékenységeket fedeznek fel, a vállalatok frissítést küldenek a probléma megoldásához. Ezért elengedhetetlen a szoftver **folyamatos frissítése** - ha lehetséges, válasszuk az „automatikus frissítés" lehetőséget, hogy ne felejtsük el telepíteni a frissítéseket.

● Használjunk megbízható vírusvédelmi szoftvert- a rosszindulatú programok, az adathalászat és az egyéb online fenyegetések elleni küzdelmet jelentősen megkönnyíti, ha rendelkezünk **naprakész és megbízható vírusvédelmi programmal**.

**A Sicontact Kft.-ről röviden:**

A Sicontact Kft. hazánkban az egyik legjelentősebb **IT biztonsággal foglalkozó** cég, az ESET termékek kizárólagos magyarországi forgalmazója. Mottója és küldetése, ami köré termékportfolióját kialakította: „**biztonság a digitális világban**". A Sicontact Kft. Magyarországon az **ESET NOD32** technológiára épülő termékeivel mind a lakossági, mind a vállalati szegmensben meghatározó piaci szereplő. A cég 2007-ben megszerezte az ESET ausztriai képviseletét, így azóta regionális piaci szereplőként tevékenykedik. A Sicontact Kft. több ízben elnyerte a kitüntető **Business Superbrands** díjat. Az ESET Smart Security programcsomagot többször is **az év antivírus megoldásának** választották.

A független tesztelő szervezet több díjjal is elismerte az otthoni ESET termékeket a 2019-es eredményeket összefoglaló riportjában:

- Arany díjat nyert a fejlett, célzott és fájlnélküli kártevő támadások kivédésében, amely új kategóriaként jelent meg 2019-ben. Az ESET volt azon két gyártó egyike, akik mind a 15 célzott támadást sikeresen blokkolták a tesztelés során.

- 2018-ban ezüst, majd 2019-ben arany díjat szerzett a rendszer gyorsaságára és teljesítményére gyakorolt hatást vizsgáló kategóriában, az ESET szoftverek alacsony erőforrásigényének köszönhetően.

- Bronz díjat nyertek el a téves riasztások kategóriájában, amelyek ugyanúgy gondot okozhatnak, mint egy valós fertőzés, ezért az elkerülésük kulcsfontosságú a biztonsági szoftvereknél.

A Sicontact Kft. az ESET szoftvereit a lehető legrugalmasabb konstrukciókban, magyar nyelvű terméktámogatással kínálja. Az ESET már több mint 25 éve biztosít védelmet a digitális világ fenyegetéseivel szemben. Egy kicsi és dinamikus vállalatból mára egy több mint 100 millió felhasználót számláló és 202 országot és területet lefedő globális márkává nőtte ki magát. Rengeteg minden változott, de az alapvető törekvéseik és a hozzáállásuk változatlan maradt, továbbra is céljuk egy biztonságosabb digitális világ felépítése, amelyben mindenki élvezheti a biztonságos technológia előnyeit.

**További információ és interjúegyeztetés:**

**Terdik Adrienne** | **Ügyvezető igazgató** | **PResston PR** | **Rózsadomb Center** | **1025 Budapest** | **Törökvész u. 87-91.** | **T + 36 1 325 94 88** | **F +36 1 325 94 89** | **M +36 30 257 60 08** | **adrienne.terdik@presstonpr.hu** | **www.presstonpr.hu**

**Szekeres Nikoletta** | **PR vezető** | **PResston PR** | **Rózsadomb Center** | **1025 Budapest** | **Törökvész u. 87-91.** | **T + 36 1 325 94 88** | **F +36 1 325 94 89** | **M +36 30 831 64 56** | **nikoletta.szekeres@presstonpr.hu** | **www.presstonpr.hu**