

Így vernek át téged, ha nem hagy hidegen az ukrajnai háború



PC World

| 2022 április 8. 10:45

Nő a kiberfenyegetettség, a támadások egyre kifinomultabbá és összetettebbé válnak, a rosszindulatú kódolók folyamatosan változtatják taktikáikat, technikáikat, eljárásaikat, és pontosan tudják, hova kell célozni: a szívre.

Békeidőben sem unatkoznak a hackerek, ám a krízisek, járványok, konfliktusok, katasztrófák okozta gyorsan változó és bizonytalan helyzet szinte ajándékként hullik az ölükbe. Napról napra bukkannak fel új weboldalak, és érkeznek kéretlen e-mailek, amelyek jótékonyági célokra hivatkozva próbálnak pénzt kicsalni a jóhiszemű emberekből.

Míg a közösségi oldalak nagy szerepet játszanak abban, hogy a válságok idején tájékoztassanak a segítségnyújtás lehetőségeiről, a csalásoknak is rendkívül jó táptalajt adnak. Bárhol is találkozunk ezekkel, az éppen aktuális szívfájdító eseményeket használják ki, és erőteljesen ezekre az érzelmekre hatva intéznek hamis felhívásokat a segítő szándékú felhasználók felé.

Már a pandémia alatt nagyot ugrott az online térben elkövetett bűncselekmények száma, ráadásul a hibrid oktatás miatt pont a legkiszolgáltatottabb csoportok - például a gyerekek - kerültek az átverések célkeresztjébe, napjainkban pedig az orosz-ukrán háború kapcsán szembesülhetünk azzal, hogy milyen gátlástalan és pénzsóvár szereplői vannak a kibertérnek, akik még egy ilyen drámai krízishelyzetet is a maguk javára próbálnak fordítani.

A háború elől tömegesen menekülők - akik főként nők és gyerekek - sorsa természetes, hogy még a legköszívűbbekből is kiváltja az együttérzést és segítő szándékot, nem csoda hát, hogy azonnal fel is bukkantak azok, akik az ukrán nép támogatására felhívva a figyelmet gyűjtenek - leginkább pénzt.

A helyzet olyan súlyos, hogy már a Nemzeti Kibervédelmi Intézet is figyelmeztetést adott ki az Ukrainát névleg támogató, hamis adományozási mozgalmak tevékenysége és növekvő száma miatt.

Például a hamis "Segítse Ukrainát" mozgalom során a támadók olyan, jellemzően bitcoin és ethereum kriptovaluta-adománygyűjtést hirdetnek, amely semmilyen kapcsolatban nem áll az ukrán kormánnyal. Hogy hihetőbbé tegyék a gyűjtés valóságát, számos meggyőzésre alkalmas eszközt alkalmaznak, például a npr.org vagy az ENSZ Humanitárius Ügyeket Koordinációs Hivatala (OCHA) nevében küldenek ki e-maileket az áldozatoknak, és fórumbejegyzéseket tesznek közzé a hamis mozgalomról.



A PC World szakértőkkel igyekeznek a témát körül járni:

Erdős Márton, PC World főszerkesztő

Sok-sok évig kivételezett helyzetben voltunk mi, magyar felhasználók, no de nem azért, mert elkerültek az online zsaroló támadások, hanem azért, mert ezek magyar fordítása olyan égbekiáltóan rossz volt, hogy még azok sem kattintottak rájuk, akik egyébként gyanútlanul megtették volna. A fordítószoftverek azonban óriásit fejlődtek, emellett pedig a hackercsapatok és a csalók anyanyelvi tagokat toboroztak, hogy nehezen felismerhető átverésekkel jelentősen javítsák hatékonyságukat. Ez sajnos működni is látszik: napi rendszerességgel érkeznek e-mailek, amelyeket látszólag a Magyar Posta, a [hazai bankok](#) vagy éppen az [energiaszolgáltatók](#) küldtek, ám jobban megvizsgálva ezek átverések, és egyetlen céljuk a pénz- és haszonszerzés. Sajnos a mindenkit érintő és érdeklő globális események az ilyen átveréseknek is kiváló melegágyai, legyen szó akár a Covid-helyzetről vagy a jelenlegi háborúról.

Az elektronikus üzenet érkezhetsz bármelyik csatornán, lehet támogatásra felszólító, elmaradt befizetésre emlékeztető, fenyegető, sőt egyenesen zsaroló hangvételű is, a lényeg, hogy

sokkal elővigyázatosabbnak kell lenni, mindent gyanúsként kezelni, és csak a legvégén kattintani.

Bor Olivér, PR-vezető és szóvivő, biztributor

A jelenlegi orosz-ukrán konfliktus részeként a kibertér is aktív szereplője a viszálynak. A kiberoffenzívák és dezinformációs kampányok mellett elszaporodtak az online csalások is. A támadások célja - a destabilizáción túl - a pénz- és adatszerzés. Az adathalász támadások egy része kifejezetten az ukrán katonákat és azok családtagjait, valamint a menekülteket segítő civileket célozza. Az úgynevezett megszemélyesített adathalász kampányok is felütötték a fejüket, amikor is a csalók magukat egy ismert szervezet munkatársának adják ki. Mind közül a legaljasabbak az [adománygyűjtő csalások](#), amelyek a segíteni akaró emberek érzelmeit és jóindulatát használják ki. Számtalan ilyen átverős e-maillal, bejegyzéssel, weboldallal, fórummal lehet találkozni, amely a segíteni akaró emberek pszichológiai manipulációját veti be. A Bitdefender kutatói azt a trendet figyelték meg, hogy a támadók gyorsan reagálnak Ukrajna és más szervezetek törvényes közleményeire, és lemásolják ezeket. Jelenleg a támadók ehhez igazítják pszichológiai manipuláción alapuló módszereiket. A felhasználóknak ezekben a nehéz időkben fokozottan ébernek, gyanakvónak és biztonság tudatosnak kell lennie.



Csizmazia-Darab István, IT-biztonsági szakértő, ESET/Sicontact

A rendkívüli események hatására gyakran megjelennek az álhírek, a spamek, a kártevőterjesztők és azok a csalók is, akik a részvétet kihasználva gyűjtenek állítólagos adományokat. A 2013-as bostoni maratonversenyen történt bombamerénylet után például egy hamis Twitter-bejegyzés azt ígérte, hogy minden megosztással 1 dollárt kapnak az áldozatok - ezt 52 ezren meg is osztották. Most a háború kapcsán láthatjuk, hogy jó pár kétes szervezet felbukkant, amely az emberek jóhiszeműségét kihasználva próbál pénzhez jutni. Az ESET szakemberei számos ilyen weboldalt lepleztek le. A csalók a honlapokon kitalált vagy megszemélyesített valós segélyszervezetek nevében gyűjtenek pénzt, ám az adakozáshoz egy kriptovaluta-tárca számát adják meg, homályosan fogalmaznak a segély felhasználási módjáról, és pontos elérhetőségük sincs. E-mailben vagy közösségi oldalakon keresztül is érkezhettek

hasznos átverési kísérletek. Kéretlen levelek esetén legyünk gyanakvók, különösen, ha csatolmány vagy link is érkezik az üzenettel. Gondosan ellenőrizzük adakozás előtt, hogy pontosan milyen alapítványt vagy szervezetet támogatunk, és legyünk óvatosak a pénz átutalásra vonatkozó kérelmekkel.

Petrányi-Széll András, magyarországi kommunikációs vezető, G DATA

A kibertérben már jóval a háború kitörése előtt eszkalálódott a konfliktus. Januárban ukrán kormányzati oldalakat törtek fel, majd DDoS-támadásokat indítottak, és az oroszok zsarolóvírusokat, adattörlő kártevőket terjesztettek Ukrajnában. Mindeközben az ukrán kormányzat igyekszik adományokat gyűjteni. Az interneten viszont, ahol pénz mozog, ott a csalók is megjelennek. Egyrészt feltehetően az orosz kormányzat próbálja kisiklatni az ukránok akcióit, de az alkalomra váró bűnözői csoportok is megjelentek. A koronavírus-világjárvány alatt például több tíz millió eurót veszített a német Észak-Rajna-Vesztfália tartomány kormányzata, miután adathalász-támadás áldozatául estek. A gazdasági minisztérium járványügyi támogatást szeretett volna nyújtani, ám a csalók eltérítették az utalásokat.

A jótékonyági pénzgyűjtő kezdeményezések egy része átverés.

Ezért nem célszerű egy véletlenül feltűnő hirdetésre kattintva támogatni, inkább segítsük a jól ismert jótékonyági szervezetek - például a [Magyar Vöröskereszt](#) - munkáját, és csak akkor adományozunk, ha meg tudunk győződni arról, hogy valóban a támogatni kívánt szervezet vagy állam áll a gyűjtés mögött.