Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadványban...

- A pszichológiai manipulációról
- Hogyan ismerhetjük fel és védhetjük ki a pszichológiai manipulációs támadásokat?
- Jövőbeni támadások megelőzése

A pszichológiai manipuláció (social engineering)

Áttekintés

Az általánosan elterjedt vélekedés szerint a kiberbűncselekményeket elkövető hacker-ek mindig fejlett módszereket és eszközöket használnak arra, hogy betörjenek az áldozataik számítógépére, online fiókjaiba vagy mobil eszközeikbe. Ez azonban korántsem igaz. A bűnözők pontosan tudják, hogy a legegyszerűbben úgy lophatják el az adatokat, és törhetnek be áldozataik rendszerébe, ha beszélnek velük, és félrevezetik őket. Az OUCH! ehavi számában bemutatjuk a támadások e formáját, amit pszichológiai manipulációnak, vagy közismertebben social engineering-nek neveznek, illetve azt, hogyan védhetjük meg magunkat.

A szerzőről

Alissa Torres minősített SANS oktató, akinek a fejlett számítógépes bűncselekmények felderítése és az incidenskezelés a fő szakterülete. Szakmai tapasztalatait a kiberbűncselekmények elleni védekezés első vonalaiban szerezte egy internetes biztonsági csoport tagjaként. A Twitteren **@sibertor** néven található meg.

A pszichilógiai manipulációról

A pszichológiai manipuláció egy pszichológiai alapú támadás, amikor a támadó félrevezeti az áldozatot, így az olyan dolgokat tesz meg akarata ellenére, amire a kiberbűnöző ráveszi. Ez a támadási forma már évezredek óta létezik, a mások becsapása és befolyásolása nem új jelenség. Azonban a kiberbűnözők mára megtanulták annak a módját, hogyan lehet az Internet segítségével rendkívül hatékonyan, egyidejűleg akár több millió embert is megtéveszteni. Ha megvizsgálunk egy átlagos támadást, mi magunk is könnyedén meg fogjuk érteni, hogyan működik ez a módszer.

Érkezik egy telefonhívás, amiben a beszélgetőpartner azt állítja, hogy egy számítógépes cégtől, az internetszolgáltatótól, vagy akár a Microsoft technikai segítségnyújtó központjából (tech support) hív. Állítása szerint azt látják, hogy furcsán viselkedik a számítógépünk, az Internetet pásztázza, vagy spam-et küld, és ezért úgy gondolják, hogy káros szoftverrel fertőződött meg, őt magát pedig azzal bízták meg, hogy segítsen kinyomozni a probléma forrását, és biztonságosabbá tenni a számítógépet. Miután megnyerte a bizalmunkat, különböző szakkifejezésekkel igyekszik összezavarni minket, és elhitetni velünk, hogy a rendszerünk valóban fertőzött.

Például arra kérhet, hogy ellenőrizzük, hogy bizonyos fájlok jelen vannak-e a számítógépen, és el is magyarázza, pontosan hol találhatók ezek az állományok. Mikor megtaláltuk ezeket a fájlokat, a hívó biztosít arról, hogy ezek bizony a káros szoftver fertőzés jelei, miközben a valóság az, hogy ezek teljesen ártalmatlan állományok, amelyek minden számítógépen rajta vannak. Miután sikeresen meggyőztek arról, hogy fertőzött a számítógépünk, kérheti, hogy nyissunk meg egy weboldalt, ahonnan meg lehet vásárolni egy megfelelő biztonsági alkalmazást, esetleg

A pszichológiai manipuláció (social engineering)

arra kérhet bennünket, hogy engedélyezzük számára a távolról történő hozzáférést, hogy meg tudja oldani a problémát. Azonban az eladni kívánt alkalmazás tulajdonképpen egy káros program. Amennyiben valaki megvásárolja és telepíti ezt az alkalmazást, akkor nem csupán ő maga fertőzi meg a saját rendszerét, hanem még fizet is érte. Ha pedig távoli hozzáférést engedélyezünk a hívó számára, akkor ő maga fogja valamilyen káros szoftverrel megfertőzni.

Fontos tudni, hogy a pszichológiai manipulációs támadások nem csak telefonon keresztül történnek, hanem adathalász támadásként email-ben, SMS-ben, Facebook-on vagy Twitter-en keresztül, esetleg valamilyen online chat-et felhasználva.

A pszichológiai manipulációs támadások megelőzésével, felismerésével és kivédésével tudjuk a leghatékonyabb megvédeni saját magunkat.

Hogyan ismerhetjük fel és védhetjük ki a pszichológiai manipulációs támadásokat?

A pszichológiai manipulációs támadások elleni védekezés legegyszerűbb módja, a józan ész használata. Ha valami gyanúsnak látszik, vagy egyszerűen nem tűnik valódinak, az könnyen lehet támadás. Az összes ilyen típusú támadásnak van néhány közös jellemzője:

- Ha valaki sürgetni akar, és emiatt nyomást gyakorol ránk, hogy gyorsan hozzunk meg egy döntést, akkor legyünk óvatosak!
- Ha valaki olyan információt kér tőlünk, amelyhez semmi köze, vagy amit már eleve tudnia kellene.
- Ha valami túl szép ahhoz, hogy igaz legyen. Például ha értesítést kapsz arról, hogy nyertél a lottón, pedig nem is játszottál.

Amikor olyan érzésünk támad, hogy valaki éppen ilyen pszichológiai manipulációs támadást követ el ellenünk, akkor ne kommunikáljunk vele többet! Tegyük le, ha telefonon hívott! Lépjünk ki a társalgásból, ha online chat-en talált meg! Ha email-t küldött, akkor töröljük a számítógépünkről a levelet! Ha a munkahelyen keresett minket, akkor feltétlenül értesítsük az ügyfélszolgálatot vagy a biztonsági csoportot!

Jövőbeni támadások megelőzése

Szerencsére vannak olyan intézkedések, amelyek megelőzhetik, hogy ilyen támadás áldozatává váljunk:

- **Soha senkinek ne adjuk meg a jelszavunkat!** Nincs olyan szervezet, amely elkérné a jelszavunkat. Ha mégis ilyen történik, akkor az egyértelműen támadás.

© The SANS Institute 2014

A pszichológiai manipuláció (social engineering)

- **Ne osszuk meg túl sokat magunkról!** Minél többet tud rólunk a támadó, annál könnyebben tud megtéveszteni, és rávenni arra, hogy azt tegyük, amit akar. Még ha csak kevés információt is teszünk közzé magunkról, idővel összeáll a teljes kép. Minél kevesebbet osztunk meg magunkról a közösségi oldalakon, termékértékelő weboldalakon, nyilvános fórumokon és levelezőlistákon, annál nagyobb biztonságban vagyunk.

- **Ellenőrizzük a kapcsolatot!** Bármikor felhívhatnak a bankunktól, az internet- vagy mobilszolgáltatónktól vagy más szervezettől teljesen törvényes és valódi okkal. Ha kétségeink támadnak arról, hogy a hívó fél jogosult-e az adott információt megismerni, akkor kérjük el a nevét és valamilyen azonosítóját! Ezután pedig biztos forrásból keressük ki az adott szervezet elérhetőségét (például szerződésen lévő telefonszám vagy a cég weboldala)! Így le tudjuk ellenőrizni, hogy valóban ők hívtak-e minket. Még ha úgy is tűnik, hogy ez csak felesleges kellemetlenkedés, a személyes adataink védelme megéri ezt a lépést.

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a http://www.securingthehuman.org weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Hivatkozások

Adathalász email támadások:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_hu.pdf
Közösségi oldalak biztonságosan:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201303_hu.pdf
Átverések elkerülése:	http://biztonsagosinternet.hu/tippek/szemelyes-biztonsag-az-interneten

OUCH! a SANS Securing The Human program által közzétett hírlevél, amelyre Creative Commons BY-NC-ND 4.0 licensz feltételei vonatkoznak. A hírlevél szabadon terjeszthető vagy felhasználható tudatosító programban, addig amíg az nem kerül módosításra. A fordításért vagy további információért kérjük írjon az ouch@securingthehuman.org címre.

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Fordította: Birkás Bence, Árvai Gábor

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus