Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

- **A pszichológiai manipulációról**
- **Hogyan ismerjük fel és védjük ki a pszichológiai manipulációs támadásokat?**

A pszichológiai manipuláció

Áttekintés

Az általánosan elterjedt vélekedés szerint a kiberbűnözők csak 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

James Lyne (**@jameslyne**) minősített SANS oktató és fejlesztési vezető a Sophosnál, aki a kiberbűnözők legfrissebb szerzeményeit fejti vissza. James a szerzője a SANS Metasploit (SEC580) és a Social Engineering (SEC567) kurzusainak.

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 két 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 arra kérhet

A pszichológiai manipuláció

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.

A józan ész a legerősebb védelem a pszichológiai manipulációs támadások felismerésére és kivédésére.

Másik példa az ún. vezetői átverés (CEO fraud), amely jellemezően munkahelyi környezetben történik. Ekkor, a kiberbűnöző egy online kutatást végez a szervezetünkkel kapcsolatban és beazonosítja a vezetőnket vagy munkatársunkat. A támadó ezután összeállít egy levelet a vezetőt vagy munkatársat megszemélyesítve és ezt küldi nekünk. Az email olyan sürgős cselekedetre kér minket, mint például egy banki átutalás vagy érzékeny munkahelyi adatok megküldése. Sokszor ezek az emailek a szükséghelyzetre hivatkoznak és a szokásos biztonsági szabályok megkerülését kérik, például hogy erősen érzékeny adatokat @gmail címre küldjünk. Az teszi ezeket a támadásokat különösen veszélyessé, hogy a támadók előzetes kutatást végeznek, és nincs semmilyen káros csatolmány vagy link a levélben, amit a vírusirtók kiszűrhetnének.

Fontos tudni, hogy a pszichológiai manipulációs támadások nem csak telefonon vagy emailen keresztül történnek, hanem bármilyen üzenetküldési csatornán, vagy akár személyesen is. A legjobb, ha tudjuk mivel állunk szemben,így mi magunk tudjuk a legjobb védelmet nyújtani.

Hogyan ismerjük fel és védjük 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 valaki a jelszavunk iránt érdeklődik, egyetlen hiteles szervezet sem kérdez ilyet.

A pszichológiai manipuláció

- Ha valaki nyomást akar ránk gyakorolni a szokásos munkahelyi biztonsági szabályok megkerülésére.
- Ha valami túl szép ahhoz, hogy igaz legyen. Például ha értesítést kapsz arról, hogy nyertél a lottón, pedig nem is játszottál.
- Ha levelet kapunk ismerőstől vagy kollégától, aminek a nyelvezete nem rá vall. A kiberbűnözők feltörhették valamilyen fiókjukat és rajtuk keresztül akarnak minket átverni. Ilyen megkeresésnél a legjobb, ha egy másik kommunikációs csatornán, például telefonon keresztül vagy személyesen bizonyosodunk meg a megkeresés valódiságáról.

Amikor olyan érzésünk támad, hogy valaki éppen ilyen pszichológiai manipulációs támadást követ el ellenünk, akkor ne kommunikáljunk vele többet. Ha a munkahelyen keresett minket, akkor feltétlenül értesítsük az ügyfélszolgálatot vagy a biztonsági csoportot. Ne feledjük, a józan ész a legjobb véldelem.

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a securingthehuman.sans.org/ouch/archives 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:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_hu.pdf
Vezetői átverés:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201607_hu.pdf
Zsarolóvírus:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201608_hu.pdf
OUCH archívum:	https://securingthehuman.sans.org/ouch/archives

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Fordította: Birkás Bence

