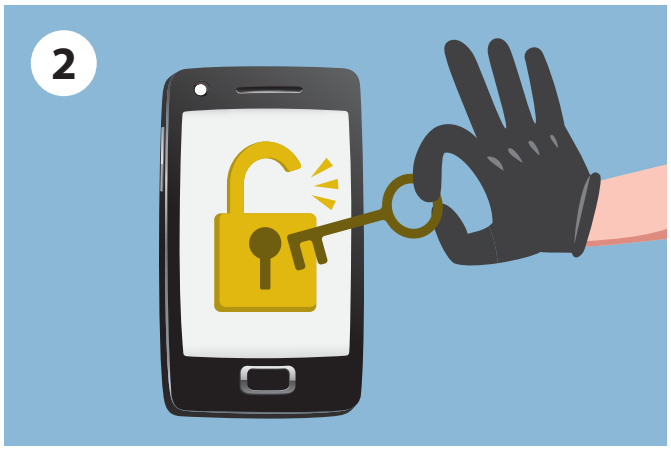
G DATA.
A BIZTONSÁG
NÉMETÜL.

G DATA AZ INTERNETES BANKOLÁS ÉS VÁSÁRLÁS VESZÉLYEI

A pénzügyi haszonszerzés régóta a magas mérnöki tudással rendelkező kiberbűnözők és az internetes szervezett bűnözés első számú motivációja. Ezért nem meglepő, hogy a banki ügyeiket az interneten keresztül intéző felhasználók folyamatosan növekvő csoportja az első számú célpontja a támadásoknak. Hiszen mi más kecsegtetne nagyobb haszonnal, mint az interneten keresztül mozgó pénzfolyam közvetlen megcsapolása?

A BITKOM szakmai szervezet adatai szerint Németországban 27 millióról 37 millióra nőtt az interneten bankolók száma 2011 és 2014 között. A 14 és 74 év közötti internetezők 47 százaléka már online intézi pénzügyeit. Ugyanebben az időszakban Magyarországon is jelentős növekedés volt, és mára az internetezők többsége online intézi pénzügyeit. Az online vásárlásról szóló felmérések pedig rendre azt támasztják alá, hogy egyre többen és többen használják kreditkártyájukat internetes vásárlásra.



A károk pedig nagyok. A Német Szövetségi Rendőrség (Bundeskriminalamt – BKA) adatai szerint 2013-ban 16,4 millió euró közvetlen kárt okozott a banki tranzakciók megcsapolása, ugyanakkor a hatóság a teljes összeget 180 millió euróra becsüli, mivel jellemzően a támadásoknak csak 10 százaléka kerül bejelentésre a rendőrséghez. A bűnözők átlagosan 4 ezer euró kárt okoznak egy felhasználónak.
Egy felmérés szerint az internetezők 2 százaléka vált már online csalás áldozatává, 17 százalék pedig azoknak az aránya, akiknek a közvetlen ismerősei vagy családtagjai sérelmére követtek el ilyen cselekményt. Összességében kimondható tehát, hogy relatív könnyű online átverés áldozatává válni.

A támadás módjai ugyanakkor alapvetően megváltoztak az elmúlt évek során. Eredetileg az egyszerű átverés (adathalászat a hiszékenységre épülő becsapással, szakkifejezéssel social engineering) volt az uralkodó módszer. Ebben az esetben jellemzően egy hamis e-mailt küldtek a bank nevében a bűnözők, melyben elkérték a felhasználó belépési azonosítóját, jelszavát és esetleges titkos kódjait (PIN vagy tranzakció-azonosító).

Mára azonban a bankok kétlépcsős azonosítási rendszereket vezettek be (például jelszó és SMS üzenetben érkező tranzakció-azonosító szám), így a támadások módja is komplexebbé vált.
Szinte kivétel nélkül rendkívül fejlett kártevőt (banki trójait) alkalmaznak, a kártékony kódot akár évekig fejlesztik. Emellett már nem csak a számítógépeket, hanem a mobiltelefonokat is megtámadják.

AZ AZONOSÍTÁS MÓDJA

A bankok ma jellemzően egy internetes banki felületen (webportálon) keresztül szolgálják ki az ügyfeleiket, akik a böngészőjüket használják az ügyintézésre. Az azonosítási folyamat alapja, hogy a weben keresztül végzett banki műveletek kezdeményezéséhez egy felhasználónévre és jelszóra vagy PIN kódra van szükség, majd a műveletek jóváhagyáshoz egy tranzakció-azonosítóra (transaction authentication number, azaz TAN) van szükség.

Mivel a tranzakció-azonosító rendkívül fontos szerepet játszik ebben a folyamatban, a bankok mindent megtesznek annak érdekében, hogy ezt a kódot a lehető legmegbízhatóbb módon generálják le és juttassák el a felhasználókhoz. Így ma már nem jellemző, hogy a tranzakció-azonosítót e-mailben küldjék ki, a legáltalánosabb mód az SMS-TAN alkalmazása. Általános, hogy a TAN manipulációjának megakadályozása érdekében a bankok már csak az adott tranzakcióhoz érvényes, az összeghez és a felhasználó számlaszámához is kötött azonosítót küldjenek a felhasználó mobilszámára. Ez rendkívül megnehezíti, hogy az azonosítót harmadik fél kikövetkeztesse.

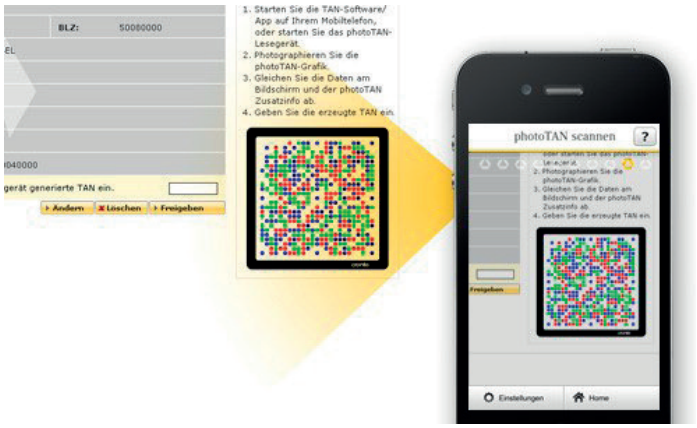
Mindazonáltal fennáll a veszélye annak, hogy az SMS üzenetet a mobiltelefonra telepített kémprogram elfogja és a bűnözők telefonszámára továbbítsa.

A FOTÓ-TAN esetében a banki művelet elvégzése után a számítógép képernyőjén egy színes kép jelenik meg, melyet a mobiltelefonnal kell lefotózni. A képet ezután a mobiltelefonra telepített banki alkalmazás konvertálja tranzakció-azonosítóvá. Opcionálisan egy olvasó is értelmezni tudja a grafikát. Ez növeli a biztonságot, mivel a mobiltelefonnal ellentétben az ilyen célhardvert nehezebb manipulálni.

A PUSH-TAN módszer esetében a tranzakció adatait internetkapcsolaton keresztül a mobiltelefonra telepített banki alkalmazásba küldik, ahol ellenőrzésre kerülnek, majd az alkalmazás TAN azonosítót generál az adatokból. Mind a FOTÓ-TAN, mind a PUSH-TAN módszer segítségével megakadályozható, hogy a TAN azonosítókat tartalmazó SMS üzeneteket egy kémprogram elfogja a telefonon. Ezzel együtt a telefonra telepített banki alkalmazás szintén támadható és adott esetben feltörhető.

A CHIP-TAN (E-TAN vagy a SMART-TAN) alkalmazása tovább növeli a tranzakciók biztonságát. A CHIP-TAN módszer egy elektronikus eszközt használ az érvényes tranzakció-azonosítók generálásához. A SMART-TAN esetében egy ügyfélkártya tartozik a számlához, melyet be kell helyezni a TAN generátorba, amely gombnyomásra érvényes azonosítót generál. Az egyik probléma ezekben az esetekben, hogy az eszköz betöréssel vagy rablással megszerezhető, és annak letiltásáig felhasználható.

Végül több bank egy úgynevezett villogó (flickering) kódot használ a tranzakciók azonosítására. Ez 5 fehér és fekete blokkból áll, és a számítógép képernyőjén jelenik meg. A kód egy optikai szenzorral rendelkező TAN generátor segítségével olvasható. Mivel a kedvezményezett számlaszáma és az átutalni kívánt összeg is ezen a módon került továbbításra, a felhasználó ellenőrizheti ezeket, mielőtt legenerálja az eszközön a TAN azonosítót. Jelenleg ez a legbiztonságosabbnak elfogadott azonosítási módszer.



KIHÍVÁS A BŰNÖZŐK SZÁMÁRA

A tranzakció-adatok és a TAN összekapcsolása, illetve a számítógépen túli hardvereszköz bevonása az érvényes tranzakció-azonosítók generálására jelentősen megnehezítette a bűnözők számára, hogy az átutalások elvégzéséhez szükséges adatokat megszerezzék.

Ezért a támadások ma általánosan azon alapulnak, hogy a tranzakciós adatokat még azelőtt manipulálják, hogy a TAN legenerálásra kerül. Ennek érdekében a kiberbűnözők rendkívül fejlett trójai kártevőket használnak, melyek a világ legösszetettebb kártékony kódjai közé tartoznak.

Általánosságban ezek a trójaiak hozzá vannak igazítva az ismert nemzetközi bankok online portáljaihoz. A böngészőkbe (Internet Explorer, Chrome, Firefox, Opera stb.) történő beépülés után a számítógép és a bank közötti kommunikáció eltérítésre kerül. A titkosított kommunikáció így megkerülhető, és hiába épül fel a számítógép és a bank portálja között egy titkosított adatkapcsolat, a trójai már minden adatot manipulál, mielőtt az még a böngészőben titkosításra kerülne. A „man-in-the-middle" (közbeékelődéses) így lesz „man-in-the-browser" támadássá, mely elegánsan megkerüli a titkosított kommunikáció által támasztott akadályokat.

A támadás módja változatos

A legegyszerűbb esetben a trójai úgy tesz, mintha a felhasználó nevében cselekedne, és a legenerált TAN segítségével a bűnöző számlájára történő utalást hagyja jóvá. Az ilyen támadás előnye, hogy a tranzakció teljesen jogszerűnek tűnik, és így jó eséllyel átmegy a biztonsági ellenőrzéseken. A hátránya viszont, hogy egy tudatos felhasználó azonnal felismeri a hamis utalást.

A mobiltelefonok megfertőzésének általános módja, hogy a felhasználót a bank hamisított weboldalára irányítják, majd azon elhelyeznek egy figyelmeztetést. A figyelmeztetés informálja a felhasználót, hogy az internetbankoláshoz egy plusz biztonsági alkalmazást kell a telefonjára töltenie, és bekérik a felhasználó telefonszámát is.
A letöltésre kerülő szoftver megfertőzi a mobiltelefont, aminek köszönhetően a bűnözők már elfoghatják az SMS üzenetekben kiküldött TAN azonosítókat. Mindez lehetővé teszi számukra, hogy tranzakciókat indítsanak és hajtsanak végre.

Megtörténhet, hogy a kártevő a tranzakciós adatokat a háttérben, a felhasználó tudta nélkül manipulálja, majd a manipulált adat alapján generálódik érvényes TAN. Az ilyen hamis átutalást csak akkor fedezi fel a felhasználó, ha a TAN megadása előtt még egyszer ellenőrzi a tranzakció adatait.

Nemzetközi szintén példa van arra is, hogy a bank meghamisított weboldalán a bűnözők a valódi telefonos ügyfélszolgálat telefonszámát is lecserélték, és a gyanakvó felhasználók hívásait a saját call-centerükbe irányították át. Itt a „bank munkatársa" elmagyarázta az áldozatnak, hogy a kártevő által kijelzett információk megbízhatóak, és arra biztatta, hogy végezze el az átutalást.

HOGYAN VÉD A G DATA BANKGUARD A TÁMADÁSOK ELLEN?

A banki trójaiak elleni védelem első vonala a vírusvédelem telepítésével kerül a számítógépre. Ha a kártevő már ismert, a szignatúra alapú védelem azonnal azonosítja és ártalmatlanítja, amint a gépre kerülne.
Amennyiben a hagyományos vírusvédelem nem képes felismerni a banki trójai legújabb változatát, a G Data a BankGuard technológia segítségével újabb, szabadalmaztatott védelmi vonalat kínál. A BankGuard technológia minden böngészőt védelmez a manipuláció ellen. Az internetes bankolás és az online fizetések során a banki portállal való kapcsolat titkosított, de a kódolásra és dekódolásra a számítógép memóriájában kerül sor. A G Data BankGuard folyamatosan összehasonlítja a memóriában lévő adatokat egy megbízható másolattal, melyet ő maga generált. Ha bármilyen manipulációt észlel, a BankGuard azonnal figyelmeztetést jelenít meg, majd lezárja a böngészőfolyamatot és megtisztítja azt a trójaitól.

ANDROIDOS VÉDELEM

Az androidos okostelefonokra és tabletekre telepíthető G Data InternetSecurity For Android hatékonyan növeli a védelmet olyankor, ha a bank a mobiltelefonhoz kötött módszert használ a tranzakciók azonosítására. A védelmi szoftver minden telepített alkalmazás engedélyeit átvizsgálja, és felismeri az adathalász alkalmazásokat. A vírusvédelmi komponens megkeresi és eltávolítja a kártevőket a letöltések és az alkalmazások között. Ez megakadályozza, hogy az SMS üzeneteket és TAN azonosítókat valamilyen kártevő elfogja.

FELHASZNÁLT IRODALOM

1. BITKOM: Eurostat eBanking Usage Statistics (German)
http://www.bitkom.org/de/markt_statistik/64034_65226.aspx

2. BITKOM: 37 million Germans use online banking (German)
http://www.bitkom.org/de/markt_statistik/64034_80365.aspx

3. Uli Ries: Bankraub Digital, c't edition 25/2014, page 76 (German)
http://www.heise.de/ct/ausgabe/2014-25-Millionenschaeden-durch-Angriffe-aufs-Online-Banking-2450695.html

4. Kurt Sagatz: Attacks on digital wallets increase (German)
http://www.tagesspiegel.de/medien/digitale-welt/online-banking-angriffe-auf-den-digitalen-geldbeutelnehmen-zu/10034102.html

5. Initiative 21 study: "Online Banking – Security pays" (German)
http://www.initiatived21.de/wp-content/uploads/2014/07/d21_fiducia_studie_onlinebanking_2014.pdf

6. Sara Zinnecker: Caution when Online Banking (German)
http://www.handelsblatt.com/finanzen/steuern-recht/recht/ratgeber-hintergrund/sicherheitsluecken-vorsicht-beimonline-banking/9434420.html

7. BITKOM: Online Banking Guidelines (German)
http://www.bitkom.org/de/publikationen/38337_81169.aspx