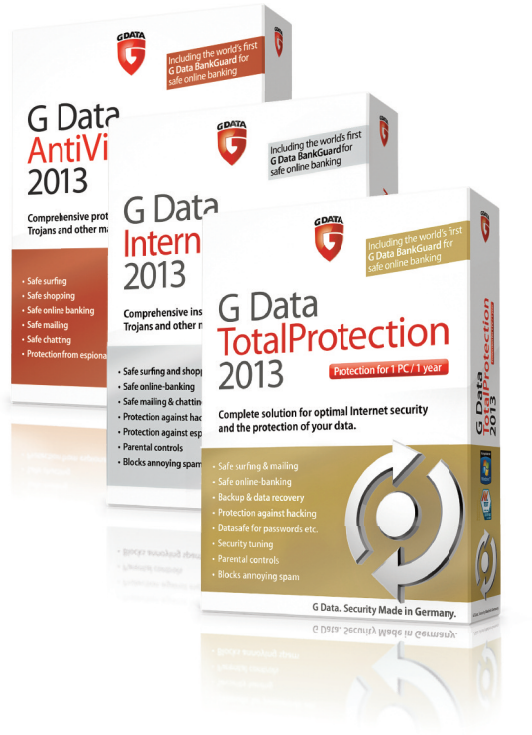
G Data
BankGuard Technológia



A hitelkártyaszámokat és banki adatokat eltulajdonító kártevők évente több száz millió euró kárt okoznak.
A G Data BankGuard Technológia csaknem 100%-os védelmet nyújt még a legújabb trójaiak ellen is.

A G Data BankGuard Technológia minden G Data vállalati és lakossági termék részét képezi, és együttműködik minden böngészővel.

VERIFIED by VISA MasterCard Maestro PayPal

G Data. A biztonság németül.

Vezetői összefoglaló

A banki adatokat eltulajdonító kártevők egyre komolyabb fenyegetést jelentenek. Használatukhoz már szinte számítógépes tudás sem szükséges. Üzemeltetésük hagyományos szervezett bűnözői csoportok kezében van, akik a technológiát csupán licencelik annak fejlesztőitől.

Az elektronikus bűnözés éves szinten több száz millió euró kárt okoz közvetlenül a bankoknak, és még többet a felhasználóknak.

Az adatlopásra ott kerül sor, ahol a leggyengébb a védelem: a felhasználók számítógépein.
A hagyományos antivírusszoftverek nem nyújtanak megfelelő védelmet az adatlopást végző trójaiak ellen, melyek a böngészők hálózati könyvtárait támadják meg, ahol az adatok kódolatlanul rendelkezésre állnak.

A Man-in-the-Browser (ügynök a böngészőben) típusú támadások képesek ellopni az űrlapok adatait, vagy akár hamis átutalásokat elvégezni a felhasználók nevében.

A G Data vírusvédelmi szoftvereibe épített G Data BankGuard Technológia újfajta védelmet kínál a trójaiak ellen.

A szoftver a böngészőkbe épülve azok integritását védi, felismeri és megakadályozza az adatlopást.

A G Data BankGuard Technológia önállóan is licencelhető technológia, melyet a bankok az ügyfeleik rendelkezésére tudnak bocsátani.

A G Data BankGuard Technológia OEM szerződés keretében márkázható megoldást kínál a bankok számára az ügyfeleik védelmére és a szolgáltatásaik iránti bizalom növelésére.

G Data. A biztonság németül.

A G Data már több mint 27 éve megbízható partner a vírusvédelemben. 1985-ben a cég mutatta be a világ első vírusirtó koncepcióját.

A Ruhr-vidékről induló vállalkozás szoftverei hamarosan több millió német számítógépen futottak, és a G Data azóta is őrzi pozícióját az anyaországban.

Referenciái között számos bank, vezető nagyvállalat, kormányzati szervezet és több százezer kis- és közepes vállalkozás található.

A G Data ma több mint 300 saját alkalmazottal rendelkezik, és 9 európai országban önálló képviseletet tart fenn.

A vállalatot emellett elkötelezett disztribútorok több ezer minősített szakértő munkatársa képviseli az Egyesült Államoktól Ausztráliáig, több mint 90 országban.

Internetes bankolás Magyarországon

A verseny a pénzügyi piac minden szereplőjét rákényszeríti a költségek lefaragására. A kiadások csökkentésére több módszer is kínálkozik, melyek közül az egyik legkézenfekvőbb az online ügyintézés elterjesztése. Az egyik fő kérdés, hogy miközben folyamatosan növekszik a pénzügyi adatokat eltulajdonító kártevők száma, hogyan tudják fenntartani a bankok az ügyfelek bizalmát.

2009-ben még csupán a 18–69 éves internetezők 46%-a vett igénybe netbank szolgáltatást, ez az arány 2011-re azonban már 57%-ra növekedett. (Forrás: Az NRC piackutató kutatása az internetes bankolásról, 2011. Minta: 1000 fő, 18–69 éves, lakossági folyószámlával rendelkező internetező.)

Az NRC piackutató 2012 augusztusi felmérése szerint 100-ból 6 magyar lakos tapasztalta már azt, hogy visszaéltek bankkártyájával.

Az adatok ugyanakkor azt mutatják, hogy a felhasználók körülbelül 10%-a a netbankok használatakor nem figyel kellőképpen a biztonságra: ezen ügyfelek gyakran jelszóval nem védett wifi hálózatokról, nem otthoni, illetve mások által is használt számítógépekről netbankolnak.

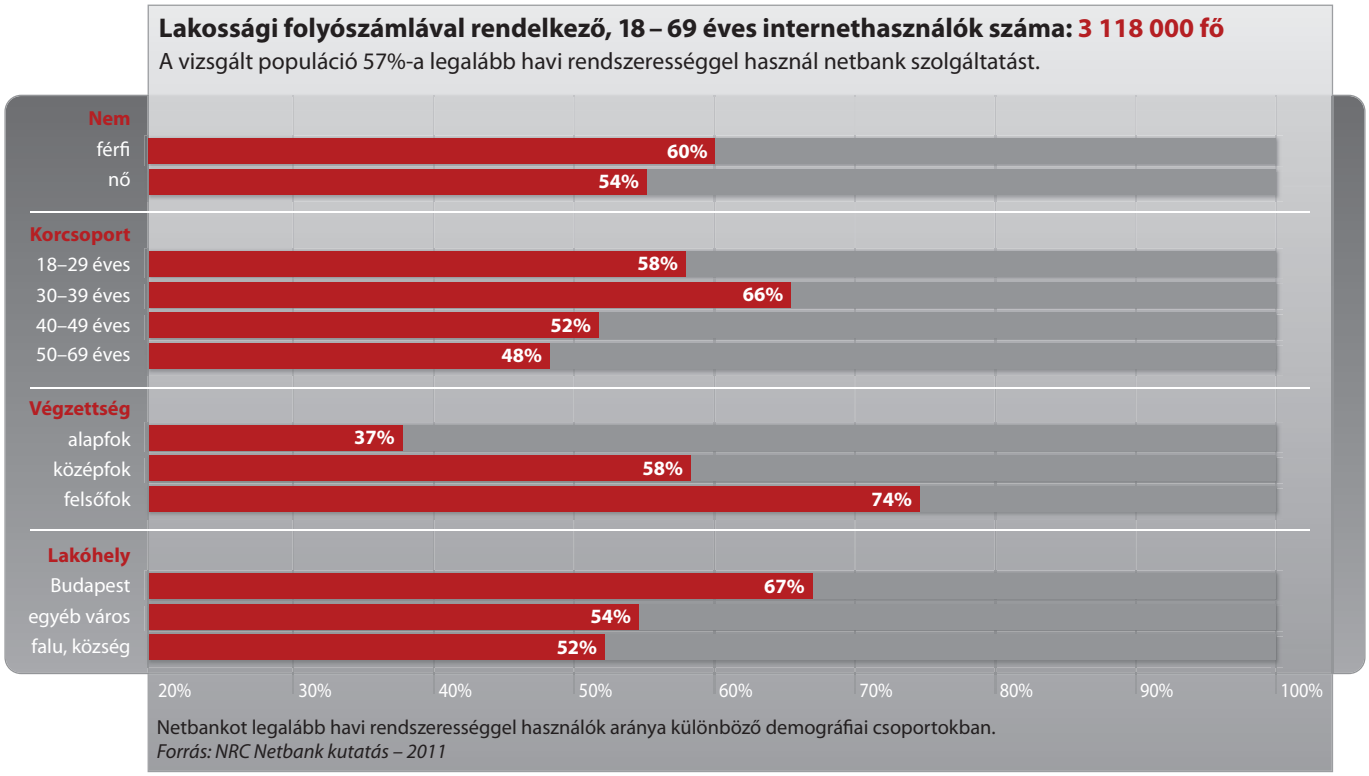
A biztonságban a felhasználók nem partnerei a pénzügyi szolgáltatóknak – nem óvják tudatosan adataikat.

Minden jel arra mutat, hogy az internetes bankolás aránya a jövőben még tovább fog emelkedni. A növekedés elsősorban a kommunikáció hatékonyságától függ, vagyis attól, hogy a bankok eredményesen tudják-e bemutatni a netbankrendszerük használatával elérhető előnyöket, illetve, hogy sikerül-e érdemben válaszolni a rendszerekkel kapcsolatos negatív kritikákra.

Milyen veszélyek állnak fenn?

Ahogy egyre több felhasználó használja bankkártyáját az interneten, ez a bűnözők számára egyre csábítóbb vadászterületet jelent. A hitelkártyaadatokat, banki belépési adatokat és jelszavakat ellopó, úgynevezett trójai programok 2011-ben Németországban körülbelül 100 millió euró kárt okoztak. A Magyarországon terjedő vírusok havi 10-es toplistáján rendszeresen 4-5 trójai program szerepel.

A bűnözők megszerzik a bankkártyaadatokat, de a legújabb trójaiak már ennél jóval többre képesek. Utalásokat hajtanak végre a felhasználók nevében, sőt a cselekmény felderítésének megnehezítése érdekében még az egyenlegét is meghamisítják.



Netbankot legalább havi rendszerességgel használók aránya különböző demográfiai csoportokban.
Forrás: NRC Netbank kutatás – 2011

Trójai programok

Számítógépes értelemben a trójai faló (röviden trójai) egy olyan program, ami mást tesz a háttérben, mint amit a felhasználónak mutat. Az elnevezés a görög mitológiában szereplő trójai falóból származik, utalva Odüsszeusz cselvetésére, hogy a görögök megnyerjék a trójai háborút. A legtöbb trójait a felhasználók maguk telepítik a számítógépükre, annak reményében, hogy ingyenes csengőhangokat, játékokat vagy más szoftvereket kapnak. A trójaiak nem feltétlenül tartalmaznak közvetlen rosszindulatú programkódokat, azonban a többségük úgynevezett hátsó kaput telepít a számítógépre, ami a bűnözők számára lehetővé teszi a számítógép irányításának megszerzését.

A magyar bankszámlák is veszélyben vannak

2012 áprilisában, a húsvéti ünnepek alatt számos magyar számlatulajdonos ébredt arra, hogy számlaegyenlege több tízezer forinttal csökkent. A HVG.hu információi szerint két pénzintézet, az Erste Bank és a Citibank ügyfelei voltak érintve a csalásban, melynek során a bűnözők az Egyesült Államokban, Chicagóban vettek fel pénzt a magyar számlákról.

Az egyik citibankos ügyfelet szombat hajnali fél háromkor a pénzintézet ügyfélszolgálatáról hívták fel, és megkérdezték tőle, hogy az országban tartózkodik-e, mivel a rendszerük külföldi tranzakciót jelzett. Az adatazonosítás után letiltották a kártyáját, de már későn. A nem sokkal később érkező banki SMS-ből kiderült, hogy több részletben szinte az összes elérhető pénzét – több mint 200 ezer forintot – leemelték a számlájáról. A pénzlopás időzítése is rendkívül kellemetlenre sikerült, a háromnapos húsvéti ünnep miatt ugyanis korlátozott volt az azonnali ügyintézés lehetősége.

ZeuS – egy trójai élete

A banki adatok, hitelkártyaszámok és online belépési adatok eltulajdonítása több milliárd dolláros feketepiaci üzlet világszerte. Az új kártevők fejlesztését és terjesztését olyan szervezett bűnözői csoportok végzik, melyek felépítése a maffiáéhoz hasonló. A megkárosított bankok nem szívesen hozzák nyilvánosságra a valódi számokat, a hagyományos vírusvédelmi módszerek pedig egyre kevésbé nyújtanak védelmet az újabb és újabb variánsok ellen.

Az egyik leghírhedtebb trójai program a ZeuS. Az áldozatokat világszerte több száz millió dollártól megszabadító kártevő a billentyűzetleütések elfogásával és az online űrlapok tartalmának ellopásával szerezte meg az online pénzügyi tranzakciókhoz kapcsolódó adatokat. A trójai a legtöbb számítógépet egyszerű böngészés közben fertőzte meg, de adathalász e-mailekben is terjesztették készítői.

Először 2007-ben azonosították, amikor az Egyesült Államok Szállítási Hivatalából lopott el adatokat. Ezt követően 2009-ben a Prevex biztonsági vállalat fedezte fel, hogy a ZeuS több mint 74 ezer ftp belépési adatot lopott el olyan vállalatoktól, mint a Bank of America, a NASA, a Monster.com, az Oracle, a Cisco, az Amazon vagy a BusinessWeek.

Ebben az időben a ZeuS készítői több millió számítógép irányítását vették át világszerte. Csupán az Egyesült Államokban 3,6 millióra becsülik a megfertőzött gépek számát. 2009. október 28-án a bűnözők 1,5 millió adathalász levelet küldtek a Facebook felhasználóinak annak érdekében, hogy azok tovább terjesszék a kártevőt. 2009. november 3-án egy brit párt letartóztattak, mivel a ZeuS-t használták, hogy személyes adatokat lopjanak. 2009. november 14–15-én a ZeuS készítői 9 millió adathalász e-mailt küldtek ki, látszólag a Verizon Wireless nevében.

2010-ben a Trusteer biztonsági vállalat egy újabb esetet fedett fel, melynek keretében 15 meg nem nevezett amerikai bank hitelkártyaadatait lopták el a ZeuS készítői. 2010. október 1-jén az FBI bejelentette, hogy egy nemzetközi bűnszövetség nyomára bukkant, melynek tagjai a ZeuS-t használták arra, hogy egyesült államokbeli számítógépekre törjenek be, és mintegy 70 millió dollárt lopjanak el.

A hálózat több mint 90 tagját tartóztatták le az Egyesült Államokban, de az Egyesült Királyságban és Ukrajnában is akadtak horogra bűnözők.

Végül 2011 májusában a ZeuS forráskódja nyilvánosságra került, de októberben a www.abuse.ch biztonsági blog szakértői már egy új trójairól számoltak be, mely még kifinomultabb p2p tulajdonságokkal rendelkezik.

Szervezett bűnözők kezében

A ZeuS összesen 196 országban irányított számítógépeket. A legfertőzöttebb területek közé Egyiptom, az Egyesült Államok, Mexikó, Szaúd-Arábia és Törökország tartozott. Összesen 2411 szervezet számolt be arról, hogy a trójai üzemeltetői valamilyen támadást indítottak hálózatuk ellen.

A ZeuS annyira finomhangolható kártevő volt, hogy az egyes bűnözők beállíthatták, hogy milyen adatokat lopjon el a megfertőzött gépekről, beleértve a közösségi hálózatok és az e-mail fiókok belépési adatait, vagy a bankoláshoz és más pénzügyi szolgáltatásokhoz (például PayPal) kapcsolódó adatokat. A leggyakrabban a Facebook, a Yahoo, a HI5, a Metroflog, a Sonico és a Netlog belépési adatait tulajdonították el.

A feketepiacon a trójai kiforrott példányait 700 dollár körüli összegért árulták a dílerek, míg a legfrissebb, teljes funkcionalitással rendelkező verzióért 15 ezer dollárt kértek. A csomag tartalmazta a botnet létrehozásához szükséges végrehajtható fájlokat előállító fájlgenerátort, a szerverekre telepítendő PHP állományokat és SQL sablonokat. Miközben a ZeuS elsősorban pénzügyi információk megszerzésére hivatott, készítői olyan képességekkel is felruházták, melyek segítségével a bűnözők teljes mértékben át tudták venni az irányítást a megfertőzött számítógépek felett.

Az internetes elkövetésre szakosodott szervezett bűnözői csoportok meglehetősen összetettek. A ZeuS készítői csak a technológiát gyártják, majd alvilági csatornákon értékesítik a terméket különböző bűnözőcsoportok számára.

A technológiát megvásárló szervezett csoportok hackereket bíznak meg azzal, hogy hozzanak létre minél nagyobb zombihálózatokat, és kövessenek el támadásokat az eszköz segítségével.

A hackerek a megtámadott bankszámlákról a pénzt olyan szállítókhoz – közvetítőkhöz – utalják el, akik nincsenek tudatában, hogy az honnan jön. A közvetítőket a szervezett bűnözői csoportok a világ minden részéről toborozzák. A szerepük sokszor az, hogy hamis dokumentumokkal nyissanak olyan bankszámlákat, melyeket nehéz visszanyomozni. A közvetítők feladata, hogy a számlájukra érkező pénzt egy másik országba utalják, vagy készpénzben felvegyék és kicsempésszék az országból, majd egy kis százalék levonása után átadják közvetítőjüknek.

A történetet még érdekesebbé teszi, hogy a feketepiac szereplői hasonló védelmet alkalmaznak szellemi tulajdonuk megóvására, mint a legális szoftverek készítői. Így a ZeuS példányai klasszikus másolásvédelmi mechanizmust tartalmaztak, mely a Windows operációs rendszeréhez hasonlóan egy ujjlenyomatot hozott létre arról a hardverkonfigurációról, melyen a kártevő licencét aktiválta a felhasználó. A SecureWorks biztonsági vállalat beszámolója szerint a ZeuS gyártója az aktiválás után névre szóló licenckulccsal látta el az egyes bűnözőket.

A trónörökös

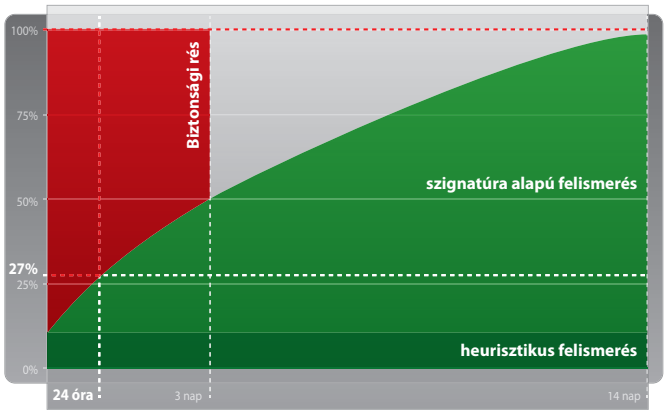
2010 végén több biztonsági vállalat jelentette, hogy a ZeuS készítői visszavonultak, és kártevőjük forráskódját eladták legnagyobb versenytársuknak, a SpyEye trójait készítő csoportnak. Ugyanakkor hangsúlyozták azt is, nem zárható ki, hogy az eredeti készítők egy új, még fejlettebb kártevő létrehozásán dolgoznak.

A SpyEye trójaival kapcsolatos utolsó, 2012. januári hírek szerint ez a kártevő már nem csupán arra képes, hogy ellopja a pénzügyi tranzakciók végrehajtásához szükséges adatokat, majd az áldozat számlájáról leemelje a pénzt, de arra is, hogy mindezek után hamis egyenleget közöljön a felhasználóval, és így lelassítsa a bűncselekmények felfedezését. A trójaiak fejlesztése tehát folytatódik.

Versenyfutás a védők és a támadók között

A ZeuS-hoz hasonló kártevőket egyre nehezebb felfedezni hagyományos vírusvédelmi módszerekkel. Több tanulmány bizonyítja, hogy az egyes kártevők élettartama csupán néhány nap, és a legtöbb fertőzésre az első órákban kerül sor.

A Springer Lecture Notes in Computer Science 2011. szeptemberi számában megjelent adatok szerint a hagyományos vírusvédelmi megoldások csupán a trójaiak 27%-át képesek felismerni már az első napon.



Emellett a mai trójaiak annak ellenére képesek eltulajdonítani a személyes adatokat, hogy az egyes tranzakciók titkosított https kapcsolaton keresztül zajlanak. Ennek oka, hogy titkosításra a böngészőben kerül sor, miközben a trójai még azelőtt lopja el az adatokat, hogy azok a böngészőkbe kerülnének.

A hagyományos antivírusszoftverek nem nyújtanak megfelelő védelmet az ilyen kártevők ellen, mivel:

- a vírusszignatúrákon alapuló felismerés egyszerű eszközökkel kiiktatható,
- a heurisztikus védelmi módszerekkel csak a fertőzések töredéke ismerhető fel,
- a tűzfalak nem képesek megakadályozni a böngészők manipulálását.

A problémát az jelenti, hogy az olyan trójaiak, mint a SpyEye, a ZeuS vagy a Sinowal/Torping szilárdan kapcsolódnak a számítógéphez, és beépülnek azokba a böngészőkbe, melyeken keresztül a felhasználók megadják hitelkártya-számaikat és jelszavaikat.

A legfőbb célpontjuk a hálózati könyvtárak elérése (például a wininet.dll a Microsoft Internet Explorerben), mivel ezekben még nem kerül titkosításra az adatforgalom. A trójaiak a kulcsfontosságú funkciókhoz kapcsolódnak, így észrevétlenül tudják ellopni és manipulálni a fájlokat és adatokat. Az ilyen támadást „Man-in-the-Browser", röviden MitB támadásnak nevezik, amit magyarul „Ügynök a böngészőben" típusú támadásnak lehet fordítani.

Tranzakcióazonosítók megszerzése

A ZeuS trójai készítői emellett olyan eljárást fejlesztettek ki, melynek segítségével még az SMS-ben küldött azonosítókat is megszerezhették. Az SMS azonosítók segítségével a bankok jó ideig meggátolták az illetéktelen tranzakciókat, a bűnözők gyakorlatilag csak az ügyfelek telefonjának megszerzésével vagy feltörésével voltak képesek azokat végrehajtani. A ZeuS készítői azonban olyan weboldalakat hoztak létre, melyek látszólag biztonsági frissítést ígértek a felhasználók telefonjaihoz. A megtévesztett felhasználók SMS-t küldtek a megadott számra, majd egy linket kaptak vissza, melyről a hamis biztonsági frissítést tölthették le.

A telefonra azonban a ZeuS mobilverziója érkezett meg, mely ezután minden SMS-t analizált, majd a megfelelőket továbbította a bűnözők számára, miközben a felhasználók elől elrejtette azokat. A mobil trójaiból Symbian (.sis) és BlackBerry (.jad) telefonokon futó verzió is készült. A bűnözők ezután a megfertőzött személyi számítógépről származó adatokat összekapcsolták a telefonokról érkező azonosítókkal, így teljes hozzáférést kaptak az ügyfelek bankszámlájához.

A tranzakciós azonosítók megszerzése azonban a számítógépen keresztül is lehetséges – a trójaiak készítői a böngészőn keresztül is hozzájuthatnak a tranzakciós adatokhoz és a PIN kódokhoz, beleértve azokat is, melyeket nem a billentyűzet, hanem az egér segítségével visznek be a felhasználók.

Versenyfutás

A trójai programok képesek meghamisítani a számlaegyenleget és a tranzakciók listáját, de arra is, hogy kitöltsék az átutalási űrlapot. Néhány trójai a tranzakciókat is manipulálja, miközben a felhasználónak az eredeti átutalásról küld visszaigazolást. A megadott tranzakcióazonosítóval a felhasználó maga legitimálja a hamis átutalást.

Független tesztek szerint a vírusirtók csupán az új trójaiak 25-35%-át ismerik fel már az első napon, és ugyan a felismerési arány nagymértékben és gyorsan növekszik az első példányok észlelését követően, a vírusvédelmi cégek és a bűnözők továbbra is macska-egér játékot folytatnak.

Védelem új alapokon

G Data BankGuard Technológia

A hitelkártya- és banki adatokat megszerző trójaiak ellen olyan új védelmi módszerre van szükség, mely a böngészőket teszi biztonságosabbá. A 2012 áprilisában bemutatott G Data BankGuard Technológia a világon jelenleg egyedülálló, teljesen új alapelvek mentén kialakított védelmet kínál a trójaiak adatlopása ellen.

A G Data BankGuard Technológia folyamatosan ellenőrzi a hálózati könyvtárak integritását, és amennyiben valamilyen illetéktelen változást tapasztal, megakadályozza az adatok továbbítását.

Leegyszerűsítetten megfogalmazva a technológia nem csupán kártevőket keres, hanem megtanulja a Windows fontos mappáinak tartalmát, és felügyeli azokat. Ezzel a technológiával a BankGuard Technológia az új, még ismeretlen trójaiak 99%-a ellen is azonnali védelmet biztosít.

Védelem a böngészőben

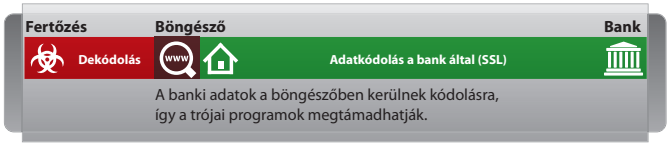
A G Data BankGuard Technológia beépítésre került a több mint 27 éve élenjáró vírusvédelmi megoldásokat fejlesztő német G Data összes vállalati és lakossági termékébe.

A G Data BankGuard Technológia új és egyedülálló módon észleli a kártevőket és óvja meg a böngészők integritását.

A G Data BankGuard Technológia védelmet nyújt a Man-in-the-Browser (MitB) támadásokkal szemben. Egy trójai nem tudja lehallgatni a titkosított SSL kapcsolatokon zajló adatforgalmat, de a hagyományos vírusvédelem mellett megtámadhatja a böngészők hálózati könyvtárait, mivel az itt tárolt adatok még nem kódoltak. A G Data BankGuard Technológia pontosan ezeket a támadásokat ismeri fel és fordítja vissza.

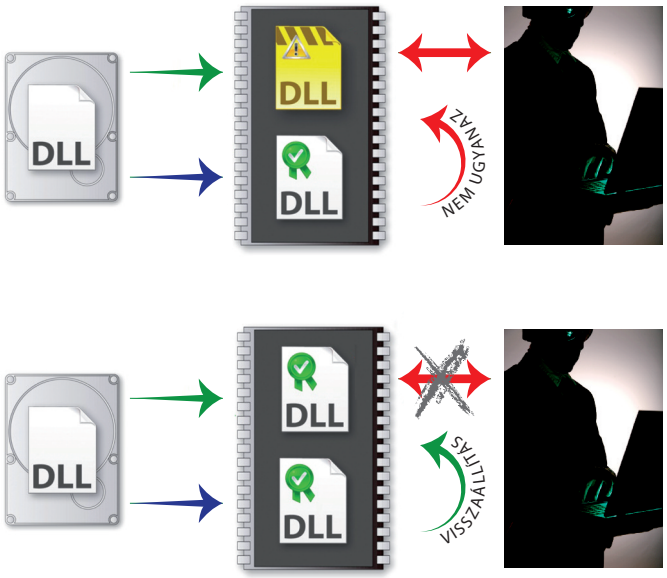
Működési elv

A pénzügyi tranzakciók végrehajtása és a bankolás során a szolgáltatók weboldalai titkosított https kapcsolaton keresztül kommunikálnak a felhasználók böngészőivel.
Az adatok azonban csak a böngészőben kerülnek titkosításra, akkor, amikor elhagyják a felhasználó számítógépét.
Ezt megelőzően a böngészők hálózati könyvtáraiban érhetőek el, és a trójai kártevők ezen a ponton hajtják végre támadásukat. A trójaiak lehallgatják és manipulálják az adatokat, mielőtt azok titkosításra kerülnének, így a felhasználó számítógépét már nem az eredeti adatok hagyják el.
Az eljárást a bűnözők arra használják, hogy megváltoztassák a banki űrlapok egyes mezőit, és hamis utalásokat hajtsanak végre.



A G Data BankGuard Technológia proaktív védelmi eljárása felismeri a jelenlegi és jövőbeli trójaiak manipulációit, így védelmet nyújt a SpyEye, a ZeuS és többi hasonló kártevő – mint például a Sinoway, a Kheagol és a Gozi – ellen.

A G Data BankGuard Technológia felügyeli, hogy a böngésző adatai ne kerüljenek meghamisításra. Ehhez először leképezi, hogy milyen képet mutatnak a böngészők hálózati könyvtárai, majd ezután a könyvtárak tényleges állapotát folyamatosan összehasonlítja az eltárolt képpel. Ha a két kép nem egyezik meg, a böngésző sérült.



Ha manipulációt fedez fel, a G Data BankGuard Technológia visszaállítja a böngésző memóriájának tartalmát, aminek köszönhetően a böngésző visszakerül biztonságos állapotába.

Miután a böngészőt megtisztította, a G Data BankGuard Technológia egy elkülönített folyamaton belül megpróbálja azonosítani a fertőzésért felelős kártevőt. A fertőzés forrását azokon a fájlokon és regisztrált bejegyzéseken keresztül keresi, melyek a trójaihoz tartoztak. Ezenkívül felderíti azokat a funkciókat, melyeket a kártevő arra használt, hogy elrejtse magát. A G Data BankGuard Technológia ezután törli, illetve letiltja a trójaihoz tartozó fájlokat és bejegyzéseket.
A G Data BankGuard Technológia sikeresen eltávolítja az ismert trójai kártevőket, a még ismeretlen, új fertőzések ellen pedig teljes körű proaktív védelmet nyújt.

A védelmi szoftver folyamatosan frissíti magát az interneten keresztül.