2016. május 8. - **Hazánkban van a hatodik legtöbb botok által fertőzött komputer, főleg a tudatosság hiánya, a vírusok elleni programok hanyagolása és a kalózszoftverek miatt.**

Az otthoni számítógépek fertőzöttsége szempontjából Magyarországon rossz a helyzet. A Symantec 2015-ről szóló jelentése alapján hazánk – megelőzve Németországot és Franciaországot – a hatodik helyen áll a botware-fertőzöttségben, a világ 2,2 százalékát adja, ez több százezer számítógépet jelent.

A botok olyan programok, melyek segítségével egy távoli támadó átveheti az irányítást az áldozatok gépei felett, és annak erőforrásait kihasználva levélszemetet, spamet küldözgethet, különböző illegális szoftvereket tölthet le rájuk és tárolhat rajtuk, de akár túlterheléses támadásra is használhatja azokat, megbénítva ezzel a célpontot. Az érintett felhasználók a legtöbb esetben nem is tudják, hogy bot van a gépükön, és ezáltal akár komoly támadások részeseivé is váltak vagy válhatnak. Ezek, illetve általában a kibertámadások pedig a nap huszonnégy órájában zajlanak, vizuálisan nyomon is követhetők, valós időben látható, hogy honnan hova, milyen jellegű támadás zajlik éppen.

Bármire rákattintunk

Antal Lajos, a Deloitte kiberbiztonsági tanácsadás üzletágának vezetője szerint az otthoni számítógépek nagyarányú fertőzöttsége több dolognak köszönhető. Részben a tudatosság hiányának, tehát sokan mindenféle körültekintés nélkül böngészik az internetet, és rákattintanak mindenre, ami szembe jön. Ez nagyban összefügg a gyér ismeretekkel; egy átlagos felhasználó nem tudja, milyen veszélyei lehetnek, ha nem elég óvatos szörfözés közben. Antal Lajos elmondása szerint az is esetleges, hogy használ-e valaki vírusirtót, illetve operációs rendszere jogtiszta-e. Az illegális úton beszerzett szoftver ugyanis nem frissíthető, ahogy azok az alkalmazások sem, amelyeket futtat, ez pedig komoly problémákat okozhat.

Mint a természetben

A számítógépes vírus tulajdonképpen pont úgy viselkedik, mint egy biológiai, a szakemberek csak a tünetekből jönnek rá a létezésükre. Ha nem indul el a gép, vagy rendszeresen újraindul, esetleg kimerevedik a képernyő, abban gyaníthatóan szerepe lehet egy malware-nek.

Akár évekig lappanghat

A vírusok esetében a legnagyobb nehézséget nem az elhárítás és a javítás jelenti, hanem a kártevő detektálása – magyarázta Antal Lajos. Hozzátette, akár hónapokba telhet, míg a szakemberek tudomást szereznek egy rosszindulatú program létezéséről, de volt már rá példa, hogy egy kémprogram évekig jelen volt egy legális programkódban, és senki nem vette észre. A

detektálás után viszont órák alatt bekerül a malware rész- vagy teljes mintája az azt felfedező vírusirtó adatbázisába, onnan pedig nagyjából 48 óra alatt az összesébe.
A kártevőkkel kapcsolatban a szakértő elmondta, nem ezek számossága jelent kihívást, hanem az, hogy egyre szofisztikáltabbak, technológiai megvalósításuk egyre kifinomultabb. Többségében pedig igaznak mondható, hogy nem a merőben új típusú vírusoknak áll a zászló, hanem a régebbiek mutációinak.

Mindenki célpont
Manapság már az sem mondható el, hogy a netbankok lennének a hekkertámadások legfőbb célpontjai, tulajdonképpen minden szektor és a kormányzatok is érintettek. Igaz, utóbbiak nem az anyagi haszonszerzés miatt válnak áldozattá, a támadás főként egy bizonyos eseményre, viselkedésre – például ideológiai vagy kommunikációs változás – adott válasznak tudható be. Többnyire ilyenek például az Anonymus, valamint más hacktivista csoportok akciói, melyek ugyanakkor nem jelentenek tartós fenyegetést – magyarázta Antal Lajos.
Mindazonáltal Magyarország ebből a szempontból szinte rajta sincs a térképen, a hekkerek inkább ott támadnak, ahol nagy lehet a nyereség. A viszonylagos védettségünkben nagy szerepe van az ország méretének, valamint nyelvünk bonyolultságának is, a nyelvismeretre ugyanis szükség van, elég akár egy adathalász támadásra gondolni, ahol a megfelelő nyelvezetet fel kell építeni. Világviszonylatban százalékosan elhanyagolható azon hekkerek száma, akik beszélnek magyarul és hajlandóak részt venni adott kibertámadásban. ***Molnár Dániel***

Ransomware
Áprilisban megírtuk, egy újfajta zsarolóvírus, úgynevezett ransomware terjed a világhálón, méghozzá nem fertőzött e-mail-csatolmányokkal vagy bizonyos programok sérülékenységét kihasználva, hanem az egyik legnépszerűbb torrentkliensbe, a µTorrentbe beépülve.

Mint a természetben
A számítógépes vírus tulajdonképpen pont úgy viselkedik, mint egy biológiai, a szakemberek csak a tünetekből jönnek rá a létezésükre. Ha nem indul el a gép, vagy rendszeresen újraindul, esetleg kimerevedik a képernyő, abban gyaníthatóan szerepe lehet egy malware-nek.

Felelősségre vonás
A botnetben részt vevő számítógépek, ha nem önszántukból váltak a hálózat részévé, egy

esetleges támadásban való részvétel miatt nem vonhatók felelősségre, a jogrendszer áldozatként kezeli ezeket. Természetesen más a helyzet akkor, ha valaki önszántából „fertőződött meg”, esetleg az Anonymus vagy más hacktivista csoportok túlterheléses akcióját támogatandó.