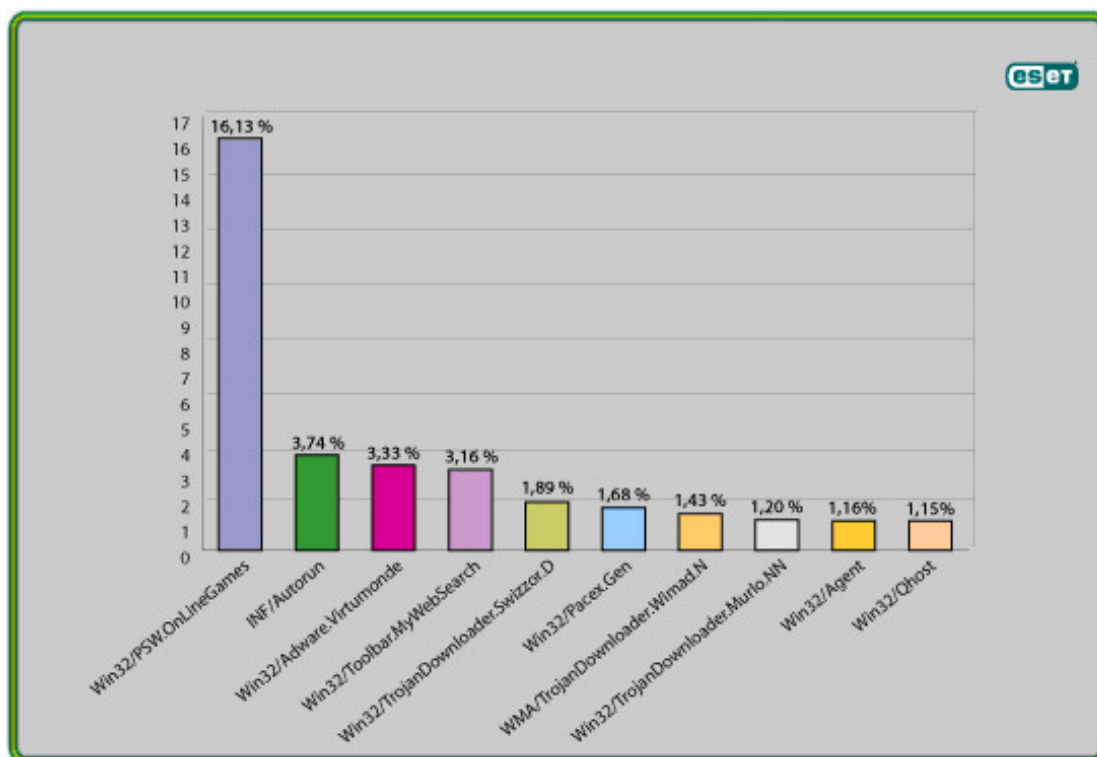




Trendi globalnih groženj – avgust 2008

Graf 1: deset najaktualnejših groženj v avgustu 2008



Napreden sistem zaznavanja in zasledovanja zlonamerne kode – ESET ThreatSense.Net® je tudi ta mesec najpogosteje zaznal škodljivo kodo iz družine Win32/PSW.OnLineGames, tokrat z najvišjim številom zaznav - 16.13 %.

Dodatne podrobnosti o zgoraj navedenih grožnjah, vključujoč njihovo prejšnje mesto na lestvici »Top Ten« in njihovo pogostost zaznavanja, so navedene spodaj.

1. Win32/PSW.OnLineGames

Prejšnje mesto na lestvici: 1

Odstotek zaznave: 16.13 %

V mesecu juliju 2008 je bilo 12.72 % vseh groženj označenih kot Win32/PSW.OnLineGames. To je družina trojancev, ki uporablja beleženje gesel in 'rootkit' za zbiranje podatkov o spletnih igrah in z njimi povezanimi osebnimi podatki. Ta škodna koda lahko pošilja te podatke tudi oddaljenemu računalniku. Statistika prikazuje upad v zaznavanju te zlonamerne kode v nasprotju s prejšnjim mesecem, vendar pa to ne pomeni, da se je zmanjšalo tudi število okužb.

Kaj to pomeni za uporabnika?

Pomembno je, da se igralci spletnih iger (MMORPG - Massively Multi-player Online Role Playing Games) kot so Lineage, World of Warcraft in celo Second Life, zavedajo števila groženj, ki so uperjene proti njim – ne samo nadlegovanja s strani drugih igralcev in nesmiselnih napadov 'grey goo' (podvajanje objektov v igri), ampak tudi 'phishing' in ostale prevare, ki lahko povzročijo finančne izgube v resničnem svetu. V takih primerih je cilj napadalcev kraja informacij o vašem bančnem računu ali kraja objektov v igri, ki jih kasneje preprodajo na črnem trgu ali na eBay-u.

2. INF/Autorun

Prejšnje mesto na lestvici: 3

Odstotek zaznave: 3.74 %

Ta zaznana oznaka se uporablja za opisovanje zlonamerne kode, ki uporablja datoteko autorun.inf za ogrožanje računalnika. V tej datoteki se nahajajo podatki o programih, ki naj bi se samodejno zagnali iz izmenljivih medijev (ponavadi so to USB ključi in podobne naprave). ESET NOD32 hevrstično identificira zlonamerno kodo, katera namesti ali spremeni autorun.inf datoteke v INF/Autorun, kadar niso prepoznane kot člani bolj specifičnih zlokodnih družin. Izmenljivi mediji so dandanes zelo razširjeni, česar se zavedajo tudi avtorji škodljivih kod. Večina zlokodnih datotek se samodejno širi na izmenljive medije, kar povzroči njihovo hitro razširjenost.

Kaj to pomeni za uporabnika?

Izmenljive naprave so zelo popularne, česar se zavedajo tudi pisci škodljive kode. Privzete nastavitve operacijskega sistema Windows samodejno zaženejo program, ki je vpisan v datoteki autorun.inf, ko želite dostopati do več vrst izmenljivih naprav. Obstaja več vrst škodljive kode, ki se samodejno kopira na izmenljive naprave čeprav to ni njihov glavni mehanizem za širjenje.

3. Win32/Adware.Virtumonde

Prejšnje mesto na lestvici: 3

Odstotek zaznave: 3.33 %

Ta zaznava predstavlja družino »potencialno nezaželenih« programov, ki se uporabljajo za oglaševanje na uporabnikovem računalniku. Kadar so ti programi zagnani, lahko poleg drugih dejanj odpirajo tudi več nezaželenih oglaševalnih oken, poleg tega jih je zelo težko v celoti odstraniti. Nezaželeni oglasi prinašajo velik dobiček razvijalcem nezaželenih kod, kar dokazuje prisotnost Virtumonde, Toolbar.MyWebSearch in Adware.SearchAid na lestvici »Top Ten«.

Kaj to pomeni za uporabnika?

Virtumonde predstavlja težavo tako za proizvajalce antivirusnih programov kot za uporabnike le-teh. Več o tej grožnji si lahko preberete v poročilu o trendu globalnih groženj iz julija.

4. Win32/Toolbar.MywebSearch

Prejšnje mesto na lestvici: 5

Odstotek zaznave: 3.16 %

To je potencialno nezaželen program. V tem primeru gre za orodno vrstico, katera vsebuje možnost iskanja, ki preusmerja iskana gesla na MyWebSearch.com.

Kaj to pomeni za uporabnika?

Ta nadloga se nahaja na naši lestvici že nekaj mesecev. Podjetja, ki se ukvarjajo z zaščito pred nezaželeno kodo imajo pogosto težave, saj to grožnjo pogosto označijo kot neškodljivo, pri nameščanju podobnih programih pa se vedno izplača prebrati drobn tisk, saj je v njem opisano obnašanje programa zaradi česar je tudi nezaželen.

5. Win32/TrojanDownloader.Swizzor.D

Prejšnje mesto na lestvici: neuvrščen

Odstotek zaznave: 1.89 %

Trojanec Downloader.Swizzor.D napadalcu omogoča prenos dodatnih komponent škodljive kode na okužen računalnik.

V večini primerov Swizzor.D prenaša in namešča adware, trojanec pa se izdaja za orodje, ki optimizira vaše omrežje enak z enakim (peer-to-peer).

Kaj to pomeni za uporabnika?

Ni nujno, da je na okuženem računalniku Swizzor edina okužba, saj ta trojanec prenaša še ostale komponente, ponavadi iz domene lops.com. V nekaj dneh se je na internetu pojavilo nekaj deset tisoč različnih namestitvenih paketov te grožnje.

6. Win32/Pacex.Gen

Prejšnje mesto na lestvici: 4

Odstotek zaznave: 1.68 %

Oznaka Pacex.gen označuje širok krog škodljivih datotek, ki uporabljajo specifične zavajajoče oznake. Te zavajajoče oznake se najpogosteje uporabljajo pri trojancih, k se uporabljajo za tatvine gesel. Končnica .gen predstavlja »generic« datoteke, kar pomeni, da ta oznaka pokriva veliko število znanih različic in omogoča zaznavanje tudi nepoznane različice z podobnimi lastnostmi.

Kaj to pomeni za uporabnika?

Trojanci iz te družine največkrat kradejo gesla, nekateri kradejo gesla tudi iz spletnih iger, zato so zaznani kot trojanci iz družine Pacex in ne iz družine PSW.OnLineGames, saj med njima obstajajo nekatere razlike. To nam pove, da bi bila zaznava groženj iz družine PSW.OnLineGames še veliko večja.

7. WMA/TrojanDownloader.Wimad.N

Prejšnje mesto na lestvici: 6

Odstotek zaznave: 1.43 %

Ta grožnja je datoteka Windows Media, ki preusmerja uporabnikov multimedijски iskalnik na škodljive URL naslove s katerih se prenesejo dodatne škodljive komponente, tudi nezaželeno oglaševalska okna. Prenos takih datotek se je zelo razširil tudi na račun omrežij enak z enakim (peer-to-peer ali P2P) v obliki mp3 datotek.

Kaj to pomeni za uporabnika?

Izmenjava datotek mp3, Flash animacij, video kodekov ipd. je zelo pogosta, zato to avtorji škodljivih kod s pridom izkoriščajo. Navidez neškodljiva datoteka se lahko samodejno zažene in vsiljivcem omogoči dostop do vašega računalnika. Pomembno je, da se zavedamo, da lahko tudi neizvršljive datoteke vsebujejo škodljivo kodo, zato bodite pazljivi, ko se naslednjič na vašem zaslonu odpre okno za program, ki ga 'imate imeti'.

8. Win32/TrojanDownloader.Murlo.NN

Prejšnje mesto na lestvici: 8

Odstotek zaznave: 1.55 %

Oznaka je uporabljena za identifikacijo trojanskega konja, ki ko je enkrat nameščen na računalnik, prenaša dodatne škodljive komponente na zahtevo napadalca.

Ta grožnja ustvari datoteko imenovano IEXPLORE.exe v direktoriju %windows% in vnese kodo v procese spletnega brskalnika (trenutno Firefox, Opera in Internet Explorer). Vnesena koda se uporablja za prenos dodatnih datotek z interneta.

Kaj to pomeni za uporabnika?

Veliko zaznanih groženj je v prvi fazi procesa okuževanja. Velikokrat škodljiva koda ne počne nič drugega kot to, da s spleta prenaša druge datoteke, ki potem prenašajo še ostale komponente, posodobitve itn. Podoben mehanizem uporabljajo tudi programi, ki jih nameščamo sami, zato morajo hevristični algoritmi določiti, ali gre morebiti za zlonamerni namen. Pisci te zlonamerne kode svoje programe neprestano spreminjajo, da bi se zavarovali pred zaznavo antivirskih programov kot že znano grožnjo.

9. Win32/Agent

Prejšnje mesto na lestvici: 21

Odstotek zaznave: 1.16%

ESET NOD32 Antivirus to škodljivo kodo obravnava kot generično, saj vsebuje vse člane družine, ki so sposobni iz okuženega računalnika pridobiti informacije o uporabniku.

Kaj to pomeni za uporabnika?

Ta škodljiva koda se ponavadi kopira v začasne mape in v register vpiše ključ, ki jih potrebuje za svoje delovanje. To pomeni, da se bo proces tega trojanca zagnal skupaj z zagonom operacijskega sistema Windows, vse dokler bo sistem okužen. Ker gre za generično grožnjo, je odstranjevanje na vsakem okuženem računalniku različno.

10. Win32/Qhost

Prejšnje mesto na lestvici: 10

Odstotek zaznave: 1.31 %

Člani te skupine trojancev se namnožijo v mapo Windows %system32% preden začnejo komunicirati prek DNS-ja s svojim ukaznim in kontrolnim strežnikom. Win32/Qhost se lahko širi preko e-pošte in tako omogoči napadalcu nadzor nad okuženim računalnikom.

Kaj to pomeni za uporabnika?

Ta trojanec spremeni DNS nastavitve na okuženem računalniku tako, da spremeni način po katerem so domenska imena dodeljena določenemu IP naslovu. To je pomembno zato, da se uporabnik okuženega računalnika ne more povezovati na spletne strani ponudnikov računalniške zaščite, kjer bi si lahko prenesel posodobitve, ali zato, da preusmeri povezavo z željene spletne strani na drugo.

Zadnji dogodki

Ta mesec se je odvijalo kar nekaj zanimivih konferenc na temo računalniške varnosti. Od 6. – 10. avgusta je na konferenci The Black Hat in DefCon sodelovalo tudi 10 ESET-ovih strokovnjakov. Dan Kaminsky je predstavil varnostno luknjo, ki jo je našel v DNS (Domain Name Server) strukturi. Ta omogoča napadalcu preprosto okužbo DNS strežnikov in preusmeritev uporabnikov na spletne strani, ki vsebujejo škodljivo kodo.

V avgustu smo bili priča tudi nenavadno velikemu številu poslanih sporočil, ki so škodljivo kodo vsebovali v priponki. Najbolj opazen je bil Spy.Agent.NES, ki se uporabniku predstavi kot poziv za nakup letalske vozovnice ali kot eden največjih podjetij za pošiljanje sporočil. Datoteka v priponki je imela ikono programa Excel ali Word, čeprav je šlo za izvršilno datoteko. V preteklosti smo videli tudi podobne priponke, ki so imele ikono programa ZIP. Uporabnika to pogosto zavede, saj misli, da gre za neškodljivo podatkovno datoteko. Naslednja stvar, ki jo Spy.Agent.NES stori, je namestitev lažnega antivirusnega programa, ki uporabnika napeljuje k nakupu navidezne zaščite proti grožnjam, ki sploh ne obstajajo.

Svojo pozornost smo posvetili tudi črvu, ki se v španščini širi med uporabniki programa Windows Live Messenger, okuži pa lahko tudi uporabnike programov MSN, AIM in Triton. Uporabniki, ki nasedejo lažnemu sporočilu, si prenesejo in namestijo okuženo datoteko. ESET-ovi programi to grožnjo zaznajo pod imenom Win32/Inject.NBL, obnaša pa se precej podobno kot standarden IRC bot, ki se prijavlja na različne IRC kanale in čaka navodila.

Globalna pokritost z ESET's ThreatSense.Net®

Zlonamerna koda, ki se trenutno širi 'In the Wild' ima široko paleto različnih zmožnosti in sposobnosti, pogosto pa obstajajo tudi različice vsake grožnje, ki so kategorizirane v veliko število družin škodljivih kod. Poleg rednega posodabljanja vašega protivirusnega programa je pomembno tudi, da ima tak program proaktivno sposobnost zaznave, kot jo imata na primer ESET-ova NOD32 in Smart Security. Tako boste zaščiteni pred znanimi in neznanimi grožnjami, ki se na spletu pojavljajo dnevno.

Čeprav je v tem poročilu nismo omenili posebej, je hevristična zaznava zaslužna za zelo visok odstotek vseh zaznav pri ThreatSense.Net. Gre za napredno zaznavo groženj, ki beleži statistiko milijonov računalnikov iz celega sveta. Verjetno gre tudi za najnaprednejše beleženje škodljive kode na svetu.

ThreatSense.Net® se je razvila na pobudo ESET-a, kot del storitve spletne strani VIRUS RADAR® (<http://www.virusradar.com>). Sistem sporočanja se je pri kakovosti zbranih statističnih podatkov s časom dodobra izpopolnil.

Medtem ko VIRUS RADAR zaznava nove grožnje, ki se pojavljajo pri e-pošti, ThreatSense.Net vključuje vse vrste grožnje, ki ogrožajo uporabnike. Statistični podatki se zbirajo na anonimen način, podatke pa pošiljajo uporabniki ESET-ovih programov, ki imajo omogočen 'reporting service'. To nam omogoča boljši pogled na obnašanje in širjenje škodljive kode v resničnem svetu. Podatki se trenutno zbirajo iz več kot deset milijonov računalnikov, sistem pa je v tem kratkem času do sedaj zabeležil več kot 10.000 različnih družin škodljive kode.