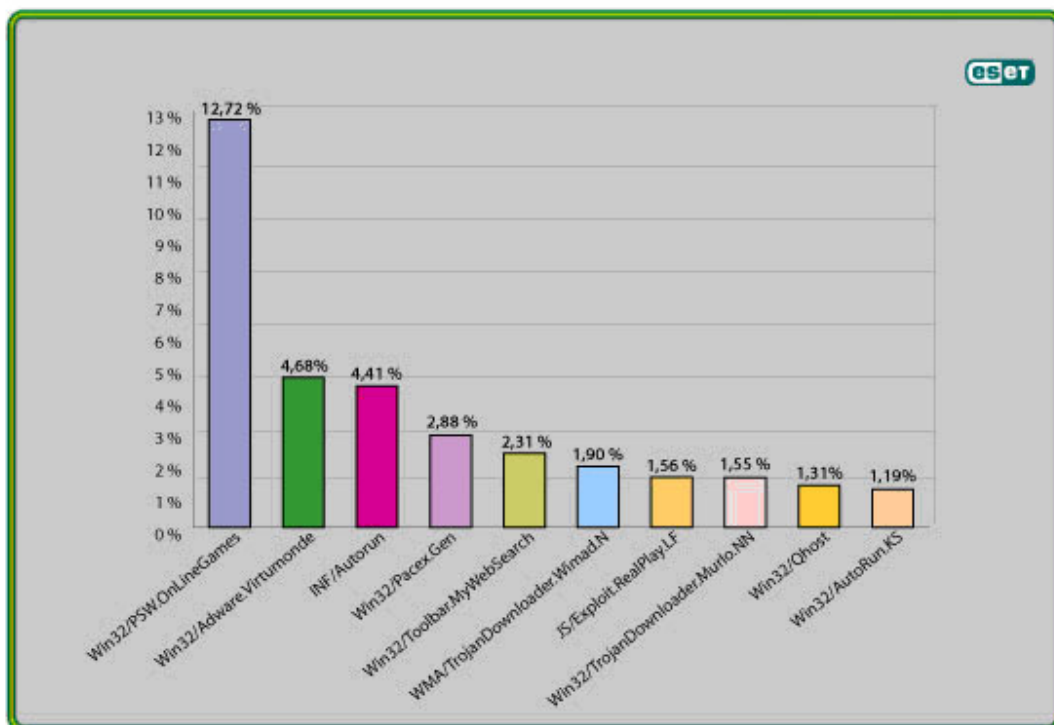




Trendi globalnih groženj – julij 2008

Graf 1: deset najaktualnejših groženj v juliju 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 - 12.72 %.

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

Več informacij kako sistem zaznavanja deluje, si lahko preberete na dnu tega poročila, v sestavku »Globalna pokritost z ESET ThreatSense.Net«.

1. Win32/PSW.OnLineGames

Prejšnje mesto na lestvici: 1

Odstotek zaznave: 12.72 %

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: 4.68 %

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: 2

Odstotek zaznave: 4.41 %

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 računalnikov. Več o tej grožnji si lahko preberete na zadnjih straneh tega dokumenta.

4. Win32/Pacex.Gen

Prejšnje mesto na lestvici: 4

Odstotek zaznave: 2.88 %

Oznaka Pacex.gen označuje širok krog škodljivih datotek, ki uporabljajo specifične zavajajoče oznake. Te zavajajoče oznake se najpogosteje uporabljajo pri trojancih, kateri 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.

5. Win32/Toolbar.MywebSearch

Prejšnje mesto na lestvici: 6

Odstotek zaznave: 2.31 %

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.

6. WMA/TrojanDownloader.Wimad.N

Prejšnje mesto na lestvici: 5

Odstotek zaznave: 1.90 %

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. Prenost 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 'morate imeti'.

7. JS/Exploit.RealPlay.LF

Prejšnje mesto na lestvici: nevrščen

Odstotek zaznave: 1.56 %

Gre za grožnjo, ki poskuša zagnati arbitrarno kodo na računalnikih z operacijskim sistemom Windows z izkoriščanjem varnostnih pomankljivosti programa RealPlayer. Napad se zgodi z različnih spletnih strani s pomočjo Javascripta-a, ki napadalcu omogoči zagon programov na napadenem računalniku. V glavnem se tak napad uporabi za namestitvev ostalih nezaželenih programov na napadenem računalniku.

Kaj to pomeni za uporabnika?

Ta ranljivost v programu RealPlayer je bila uporabljena v večjih napadih, ko so napadalci na varne spletne strani obesili svojo škodljivo kodo, ki je obiskovalce preusmerjala na strežnike, ki je okužil nezaščitene računalnike.

Več o tej grožnji si lahko preberete na strani <http://nvd.nist.gov/nvd.cfm?cvename=CVE-2007-5601>. Če žrtev odpre HTML dokument s škodljivo kodo (to je lahko spletna stran ali e-poštno sporočilo), se napad lahko sproži ne glede na to, ali program RealPlayer deluje ali ne. Možnost takega napada lahko zmanjšamo z namestitvijo varnostnih popravkov programa RealPlayer ali z onemogočanjem ActiveX ali IERPCtl ActiveX vmesnikov-

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 antivirusnih programov kot že znano grožnjo.

9. 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.

10. Win32/AutoRun.KS

Prejšnje mesto na lestvici: 19

Odstotek zaznave: 1.19 %

Grožnje označene z 'AutoRun' so znane po tem, da zlorabljuje datoteko Autorun.INF. Ta datoteka se uporablja za samodejni zagon programov ob priključitvi izmenljivih pogonov v računalnik (npr. USB ključ).

Kaj to pomeni za uporabnika?

Gre za konkreten primer škodljive kode, ki izrablja Autorun funkcijo. Tej nevarnosti se lahko izognete, če onemogočite samodejni zagon.

Prepleteni splet

Z lestvice »Top Ten« je razvidno, da so v vzponu grožnje iz spletnih strani. Za to obstaja več vzrokov, prvi pa je zagotovo ta, da so spletni brskalniki vse pogostejši. Uporabljamo jih za branje pošte, novice, igranje iger ali celo za sestavljanje dokumentov. Brskalniki so zato postali priljubljena tarča piscev škodljive kode, saj hkrati postajajo tudi vse kompleksnejši. Informacije, ki jih brskalniki vsebujejo lahko predstavljajo tudi velik vir dobička (zakonito in nezakonito). Vsebina iz spletnih strani je dandanes verjetno glavni vir informacij, ki jih dobivamo mi in naš računalnik. ESET-ovi programi pa so narejeni tako, da sproti preverjajo spletne strani, ki jih obiskujete in tako preprečijo veliko število napadov še preden se ti izvedejo.

Virtumonde: nezaželen in vztrajen gost

Škodljivo kodo iz družine Virtumonde zaznavamo že dlje časa, pogoste pa so tako okužbe s starimi kot novimi različice. Če se Virtumonde na vaš računalnik uspe namestiti, je njegova odstranitev zelo težavna, običajno je potrebno tudi 'ročno' posredovanje.

Na našo lestvico »Top Ten« se Virtumonde konstantno uvršča že nekaj mesecev kljub dejstvu, da njegovi distributerji karakteristiko in način razmnoževanja neprestano

spreminjajo. To pomeni, da smo pri zaznavi te grožnje uspešni. Kakorkoli že, priznati je treba, da imamo pri zaznavi in odstranitvi te grožnje težave vsi proizvajalci antivirusnih programov, vsaj pri nekaterih različicah. Do neke mere je to posledica uspešnosti najpogosteje uporabljenih antivirusnih programov – bolj kot je program poznan, lažje je najti način, kako napisati škodljivo kodo, ki je tak antivirusni program ne bo prepoznal. Ne preseneča dejstvo, da avtorji zlonamerne kode veliko časa posvečajo raziskovanju kako bi svoj program čimbolj skrili. ESET-ovi preiskovalniki so z njihove strani deleženi velike pozornosti.

Dejstvo je, da antivirusni programi niti s pomočjo napredne hevristike ne morejo vedno zaznati vseh znanih in neznanih groženj, še posebej ne škodljive kode, ki je napisana z namenom, da je določen antivirusni program ne more zaznati. Oni distribuirajo, mi zaznamo, oni spremenijo in redistribuirajo, mi spremenimo svojo zaznavo, oni spremenijo in redistribuirajo, mi spremenimo svojo zaznavo... neizogibno je to, da se neke vmes med distribucijo in zaznavo nekateri sistemi okužijo.

Ko pride do okužbe je čiščenje zahtevno, saj se škodljiva koda nahaja tudi v spominu. Komericalni preiskovalniki so v določenih primerih tu prikrajšani, saj si ne morejo privoščiti brisanja 'po bližnjicah' - včasih se zgodi, da se datoteke ne da varno izbrisati in takrat se pojavi obvestilo, da se določene datoteke ne da očistiti. Nekateri proizvajalci so objavili generični postopek za odstranitev, kar pa ni vedno ustrezno, saj je pri Virtumonde okužbi nujen interaktiven odstranitveni postopek. Nekateri sistemski administratorji s katerimi smo govorili, pri odstranjevanju te grožnje uporabljajo kombinacijo tehnik in orodij, ne obstaja pa preprost in enak postopek za odstranjevanje na vseh računalnikih.

To pa ne pomeni, da se moramo predati – svoje programe neprestano posodabljam in izboljšujemo, pravkar smo v program vgradili sistem, s katerim bomo nekaj časa spet korak pred pisci te kode. Zavedati pa se moramo, da gre za vojno in ne za eno samo bitko. Spreminjajo se prizorišča, enkrat smo v prednosti mi, drugič oni, končnega udarca, ki bi nasprotnika porazil pa ni.

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 naprimer 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.