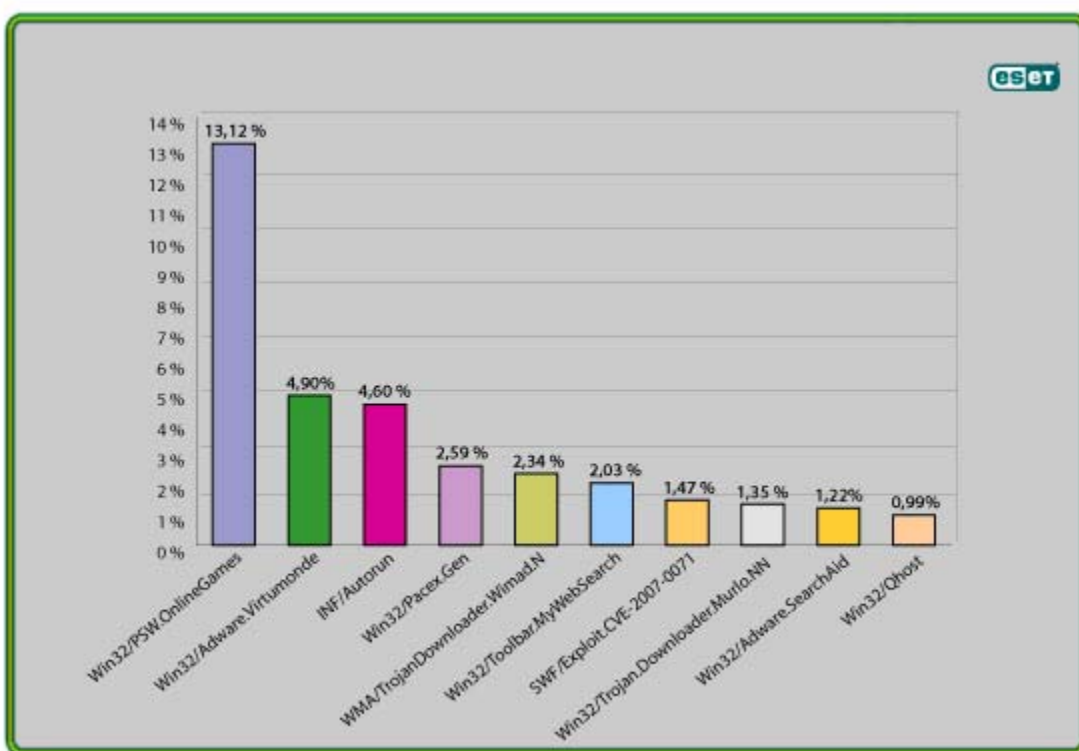




Trendi globalnih groženj – Junij 2008

Graf 1: Deset najaktualnejših groženj v juniju 2008



ESET ThreatSense.Net® analiza je napreden sistem zaznavanja in zasledovanja zlonamerne kode. Iz grafa lahko razberemo, da ESET ThreatSense.Net® ponovno najpogosteje zaznava škodljivo kodo iz družine Win32/PSW.OnLineGames, tokrat z najvišjim številom zaznav - 13.12 %.

Dodatne podrobnosti o zgoraj navedenih grožnjah, vključujoč njihovo prejšnje mesto na lestvici »Top Ten« (če je bil tja uvrščen) 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: 13.12%

V mesecu juniju 2008 je bilo skoraj 13,29% 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.

2. Win32/Adware.Virtumonde

Prejšnje mesto na lestvici: 2

Odstotek zaznave: 4.90%

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«.

3. INF/Autorun

Prejšnje mesto na lestvici: 3

Odstotek zaznave: 4.60%

Ta zaznana oznaka se uporablja za opisovanje zlonamerne kode, katera uporablja datoteko autorun.inf za ogrožanje računalnika. V tej datoteki se nahajajo podatki o programih, ki naj bi se avtomatsko 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 škodljivokodnih datotek se samodejno širi na izmenljive medije, kar povzroči njihovo hitro razširjenost.

4. Win32/Pacex.Gen

Prejšnje mesto na lestvici: 8

Odstotek zaznave : 2. 59%

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 in omogoča zaznavanje tudi nepoznane različice z podobnimi lastnostmi.

5. WMA/TrojanDownloader.Wimad.N

Prejšnje mesto na lestvici: 17

Odstotek zaznave: 2.34%

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.

6. Win32/Toolbar.MywebSearch

Prejšnje mesto na lestvici: 6

Odstotek zaznave: 2.03%

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

7. SWF/Exploit.CVE-2007-0071

Prejšnje mesto na lestvici: neuvrščen

Odstotek zaznave: 1. 47%

Ta zaznava se nanaša na poskus izkoriščanja varnostne luknje v Adobe Flash Player-ju do verzije 9.0.115.0, ki omogoča napadalcu izvajanje arbitrarne kode z uporabo prilagojene SWF datoteke. SWF (Shockwave Flash) je multimedijaska datoteka, ki se pogosto uporablja za prikaz animiranih vektorskih grafik. To varnostno luknjo je Adobe zakrpal že 8. Aprila 2008, več o tem si lahko preberete na spletni strani: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0071>.

8. Win32/TrojanDownloader.Murlo.NN

Prejšnje mesto na lestvici: neuvrščen

Odstotek zaznave: 1.35%

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 %windows% direktoriju in vnese kode v procese spletnega brskalnika (trenutno Firefox, Opera in Internet Explorer). Vnesena koda se uporablja za prenos dodatnih datotek z interneta.

9. Win32/Adware.SearchAid

Prejšnje mesto na lestvici: 5

Odstotek zaznave: 1.22%

Značilno za ta program je, da se uporablja za usmerjanje brskalnika v odpiranje nazaželenih reklamnih oken in da se namesti kot obvezen del nekega drugega licenčnega programa.

10. Win32/Qhost

Prejšnje mesto na lestvici: 8

Odstotek zaznave: 0.99%

Člani te skupine trojancev se namnožijo v Windows %system32% mapo 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. Ta trojanec spremeni DNS nastavitve na okuženem računalniku tako, da spremeni način po katerem so domenska imena dodeljana določenemu IP naslovu. To je pogosto opravljeno 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.

Od lestvice "Top Ten" do zastarelih BSI okužb

Za tiste, ki ste zamudili dobo, ko so bili na pohodu virusi boot-sector infection (BSI), naj povemo, da BSI okuži računalnik takrat, ko se ta zažene iz okužene diskete. To, da je disketa sistemska ni pogoj za okužbo. Uporabnikom smo priporočali, da v BIOS-u nastavijo zagon računalnika iz trdega diska, tako se računalnik ne okuži niti v primeru, če se okužena disketa v času zaganjanja nahaja v disketniku.

Datoteke, okužene z BSI z lahkoto odkrije večina modernih antivirusov (nekateri antivirusi so medtem zaradi zastarelosti teh virusov, iz svojih baz odstranili zaznavanje le-teh), težje pa je preprečiti okužbo. Če se računalnik zaganja iz okužene diskete do okužbe pride še preden lahko antivirusni program utegne posredovati. Odstranjevanje takšne okužbe je še posebej težavno pri operacijskih sistemih NT.

Čeprav se taka okužba v letu 2008 zdi skoraj nemogoča, se je pred nekaj tedni pojavila okužba z BSI virusom Stoned-Angelina, lani pa so okužbo z enakim virusom zaznali pri pošiljki prenosnikov podjetja Medion. Podobna neprijetnost se je lani pripetila tudi podjetju Seagate, ki je na tržišče poslalo trde diske s trojanskim konjem Autorun Trojan.

Okužbi se lahko torej izognemo z lahkoto, če nastavimo zaganjanje računalnika iz trdega diska, možnost okužbe pa se hitro poveča, če do okužbe pride že pri proizvajalcu trdih diskov ali ponudniku računalniške opreme.

VB100

Verjetno že veste, da je ESET pred kratkim osvojil že svojo petdeseto VB100 nagrado (smo prvo podjetje, ki mu je upelo osvojiti toliko nagrado). Virus Bulletin to nagrado podeli produktom, ki med njihovim testiranjem dosežejo 100 odstotno zaznavo virusov "In The Wild" in ne javijo nobenega lažnega alarma pri njihovih preverjenih datotekah iz zaupljivega vira. Po objavi VB100 rezultatov testiranj smo lahko v medijih prebrali dvome o smiselnosti takih testiranj enega izmed proizvajalcev antivirusne zaščite, ki je zagrozil, da se bo iz takih testiranj tudi umaknil.

Pri ESET-u smo na nagrade ponosni in se ne strinjamo s tistimi, ki menijo, da gre za nepomembna testiranja. Kot je v svojem blogu zapisal že Randy Abrams - <http://www.eset.com/threat-center/blog/?p=125>, se moramo zavedati omejitev teh nagrad in WildList seznama, ki se na takšnih testiranjih uporablja.

WildList ne predstavlja 100 odstotkov vse škodljive kode "in the wild", saj vključuje samo viruse. Organizacija WildList dela na tem, da bi v svoja testiranja vključila čim bolj raznoliko škodljivo kodo. Uporabljajo predvsem vzorce virusov, ki so v zbirkah strokovnjkov iz tega področja, vseeno pa gre za viruse, ki so se že pojavljali na internetu.

Obstajajo tudi veliko večje zbirke virusov, ki jih za testiranja uporabljajo priznani strokovnjaki ampak tudi take zbirke niso 100 odstotno merodajne (nobena zbirka ne more vsebovati čisto vsak škodljiv program), saj obstajajo tudi veliko večja možnost javljanja lažnih alarmov. Uporaba produkta, ki je uspešno prestal VB100 ali katerikoli podoben test, vam ne zagotavlja, da ste pred škodljivo kodo varni. VB100 je test, ki bi ga moral v večini primerov uspešno prestati vsak antivirusni program, saj imajo dostop do vzorcev virusov uporabljenih na testiranju vsi. Del testiranja se tiče tudi lažnih alarmov pri zaznavanju, ta del testiranja preprečuje, da bi antivirus kot škodljivo kodo označil večino ali kar vse datoteke. Veseli smo lahko, če antivirusni program odkrije vso zlonamerno kodo, a ne, če nam onemogoči tudi dostop do datotek in programov iz zaupljivega vira.

Testiranje je ključnega pomena tako za proizvajalce kot končne uporabnike, tega se pri ESET-u dobro zavedamo in temu posvečamo veliko pozornosti. Več o tem si lahko preberete tudi v dokumentu:

[http://www.eset.com/download/whitepapers/TestingTesting\(May2008\).pdf](http://www.eset.com/download/whitepapers/TestingTesting(May2008).pdf). Daljši članek na to temo smo prispevali tudi za knjigo "The AVIEN Malware Defense Guide", verjamemo pa, da bomo o tej temi še pisali.

Kako beležimo škodljivo kodo

Škodljivi "In The Wild" programi, ki se trenutno širijo uporabljajo več vrst načinov z različnimi zmožnostimi in sposobnostmi, obstaja veliko različic, ki jih uvrščamo v različne družine škodljive kode.

Pri večini zaznav, ki jih zabeležimo gre za generične grožnje, ki jih beležimo pod enakim imenom, zaznavajo pa se tudi nove različice. To delamo zato, ker imajo posamezne različice zelo kratko življenje preden so zamenjane s spremenjenimi in nadgrajenimi različicami, z namenom, da jih antivirusni programi ne bi zaznali.

Beleženje generičnih oz. hevrističnih zaznav škodljive kode nam omogoči boljše razumevanje obnašanja groženj. V preteklosti se je posvečanje določeni različici obrestovalo, saj so avtorji svojo kodo želeli čim hitreje in čim bolj razširiti, danes pa to nima smisla, saj avtorji svojo kodo neprestano posodajajo in nadgrajujejo.

Globalna pokritost z ESET ThreatSense.Net®

Poleg redno posodobljenega antivirusa je pomembno tudi to, da ima antivirus možnost proaktivne zaznave, kot to velja za napredno hevristično zaznavanje pri ESET NOD32 in ESET Smart Security. Tako ste zaščiteni pred novimi in neznanimi grožnjami, ki se na internetu pojavjajo vsak dan.

Čprav 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 spročanja 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.