HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza MyDoom.a
i
MyDoom.B crva

CCERT-PUBDOC-2004-01-57

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

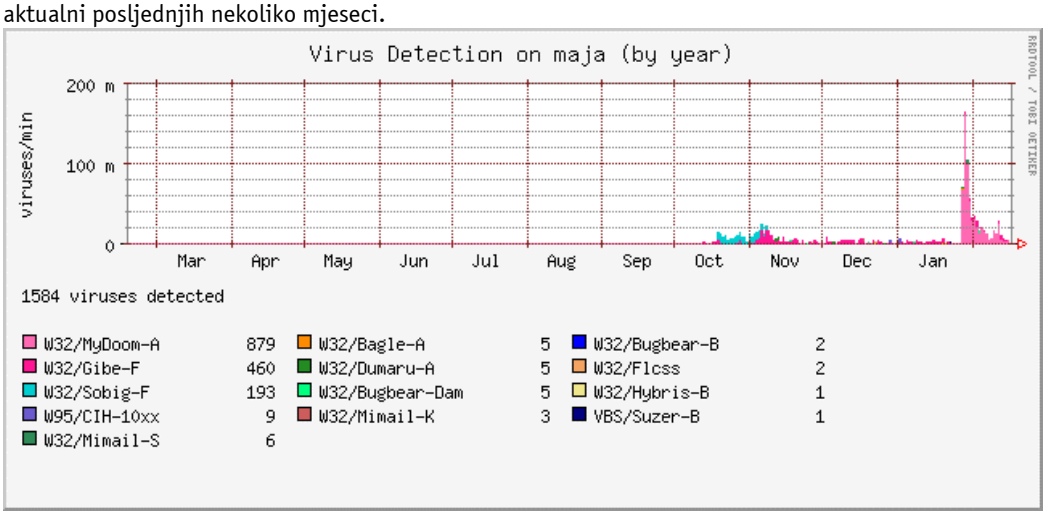
CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

MyDoom.A (poznatiji i pod imenima Novarg, Shimgapi i Worm_Mimail.R) i Mydoom.B dvije su varijante mrežnog crva koji napada računala s instaliranim Microsoft Windows operacijskim sustavima. Osnovni način širenja Mydoom-a je distribucija putem poruka elektroničke pošte i KaZaA mreže za dijeljenje datoteka. Pri tome se koristi tehnika krivotvorenja *From* polja zaraženih poruka elektroničke pošte, što otežava identifikaciju zaraženog računala i izaziva pomutnju među korisnicima.
Mehanizam širenja ovog mrežnog crva vrlo je agresivan i rezultira velikim brojem zaraženih poruka, što opterećuje i usporava poslužitelje za distribuciju elektroničke pošte. Na **Slici 1** prikazan je broj zaraženih poruka zaustavljenih na mrežnom poslužitelju jedne prosječne računalne mreže sa oko 60-ak korisnika. Iz grafičkog prikaza vidljivo je da broj poruka zaraženih Mydoom-om (označen ružičastom bojom) višestruko nadmašuje broj poruka zaraženih ostalim crvima i virusima koji su bili aktualni posljednjih nekoliko mjeseci.



Slika 1: Grafički prikaz broja zaraženih poruka koje su zaustavljene na e-mail poslužitelju

Stvarno opterećenje poslužitelja još je i veće, ako se uzme u obzir vrlo velik broj zaraženih poruka koji se zbog nepostojećeg *From* polja vraćaju poslužiteljima zaduženima za te domene kao neisporučena pošta.
Unutar ovog dokumenta detaljno će se analizirati način i posljedice širenja ovog mrežnog crva, kao i osnovne metode i alati za njegovo uspješno prepoznavanje i uklanjanje.

2. Analiza

2.1. Mydoom.A

Kao što je spomenuto u uvodu, MyDoom mrežni crv se širi putem poruka elektroničke pošte i KaZaA mreže za dijeljenje datoteka.
Zaražene poruke elektroničke pošte moguće je prepoznati po "Subject" polju koje sadrži neke od sljedećih riječi:

```
test
hi
hello
Mail Delivery System
Mail Transaction Failed
Server Report
Status
Error
```

Tijelo poruke sadrži neki od sljedećih tekstova:

- `test`
- `The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.`
- `The message contains Unicode characters and has been sent as a binary attachment.`
- `Mail transaction failed. Partial message is available.`

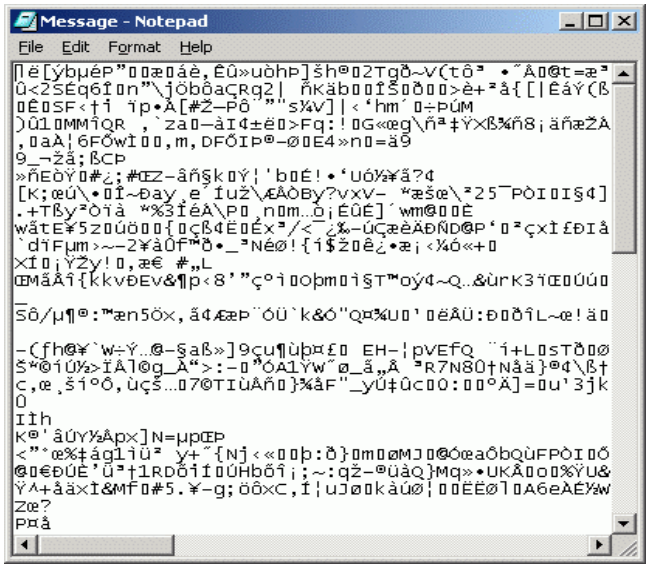
Privitak uz poruku, unutar kojega je sadržan crv, nosi neko od sljedećih imena u kombinaciji sa nastavcima `.pif`, `.scr`, `.exe`, `.cmd`, `.bat`, `.zip`.

```
document
readme
doc
text
file
data
test
message
body
```

Pri tome je potrebno naglasiti kako otvaranjem datoteka sa nastavkom `.zip` sustav neće biti ugrožen, budući da se crv aktivira tek kada se pokuša pokrenuti izvršna datoteka sadržana unutar `.zip` arhive.
U slučaju širenja MyDoom-a putem KaZaA mreže, crv će kopirati svoju izvršnu datoteku u direktorij sa dijeljenim datotekama pod nekim od sljedećih imena,

```
winamp5
icq2004-final
activation_crack
strip-girl-2.0bdcom_patches
rootkitXP
office_crack
nuke2004
```

kombiniranih s nastavcima `.bat`, `.exe`, `.pif`, `.scr`. Korisnici koji sa inficiranih računala dohvate i pokrenu ovakve datoteke, inficirati će vlastito računalo.
Prilikom svog širenja, crv izbjegava slanje zaraženih poruka na određeni skup predefiniranih domena, kao i slanje poruka određenim korisničkim računima kao što su na primjer `root`, `info`, `nobody`, i sl., ali istovremeno pokušava poslati poruke na adrese sastavljene od računalnih domena pronađenih u datotekama na sustavu i popisa korisničkih računa koji je skriven u kodu crva. Budući da su ovako sastavljene adrese u većini slučajeva nepostojeće, slanje poruka koje ih sadrže kao odredište na izvornim SMTP poslužiteljima prouzročiti će velik broj upozorenja o neisporučenoj elekroničkoj pošti.
Kada se crv pokrene, bilo iz *e-mail* klijenta, bilo putem KaZaA mreže za dijeljenje datoteka, na ekranu će se pojaviti prozor 'Notepad' uređivača teksta, unutar kojega će biti ispisana gomila slučajnih znakova (**Slika 2**), koji su pohranjeni u datoteci `Message` u `temp` direktoriju.



Slika 2: Prozor koji se otvara prilikom pokretanja MyDoom crva

Izvršna datoteka MyDoom-a pri tome će se kopirati u glavni direktorij sustava (`%System%`), koji se uobičajeno nalazi na lokaciji `c:\Windows\System` ili `c:\Winnt\System32` na Windows 2000/XP/NT sustavima, pod imenom `taskmon.exe`.

Kako bi se osiguralo pokretanje izvršne datoteke crva pri svakom ponovnom pokretanju računala, u *Registry* sustava upisuje se sljedeći ključ `[HKLM\Software\Microsoft\Windows\CurrentVersion\Run] "TaskMon" = %System%\taskmon.exe` ili (u slučaju neuspjeha) `[HKCU\Software\Microsoft\Windows\CurrentVersion\Run] "TaskMon" = %sysdir%\taskmon.exe`.

Uz izvršnu datoteku, u `%System%` direktorij pohranjuje se i datoteka `shimgapi.dll`, čiji je cilj osluškivanje dolaznih konekcija na mrežnim portovima 3127 do 3198. U Registry sustava dodaje se linija `[HKCR\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InprocServer32]`, koja osigurava da se datoteka `shimgapi.dll` u memoriju učita kao dodatak Windows Explorer programu i na taj način *backdoor* proces čini nevidljivim u Task Manager programu za nadzor sustava.

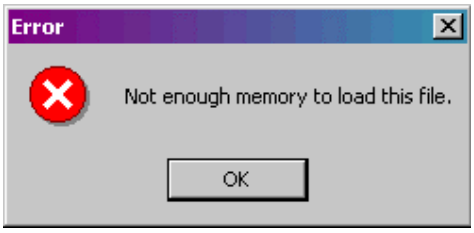
Pomoću ovako otvorenog ulaza u sustav, neovlašteni korisnik je u mogućnosti ubaciti dodatne izvršne datoteke na sustav i pokrenuti ih, ili inficirani sustav jednostavno upotrijebiti kao TCP *proxy* poslužitelj.

Osim širenja porukama elektroničke pošte i ostavljanjem ulaza u sustav, MyDoom.A je programiran i da 1. veljače u 16:09 sati (prema satu na sustavu) pokrene DDoS napad na Web stranicu www.sco.com. Sva inficirana računala u zadano će vrijeme uputiti 64 simultana zahtjeva za glavnom stranicom ovog Web poslužitelja, pokušavajući ga na taj način preopteretiti. Aktivnost crva prestati će 12. veljače, ali potrebno je imati na umu da navedeni ulaz u sustav ostaje otvoren i nakon tog datuma.

2.2. Mydoom.B

MyDoom.B druga je inačica MyDoom crva, sličnog načina širenja i sa vrlo sličnim djelovanjem. Osim DDoS napada na www.sco.com, ova inačica crva izvedena je tako da isti napad ponovi i na Web stranicu www.microsoft.com, kao i da inficiranom računalu spriječi pristup stranicama sa antivirusnim alatima.

Prilikom pokretanja crva na ekranu će se pojaviti lažna poruka o pogrešci (**Slika 3**), koja bi trebala zavarati korisnika kako se odabrana datoteka nije otvorila. Uz lažnu poruku, otvara se i prozor Notepad uređivača teksta identičan onome kao i kod MyDoom.A crva (**Slika 2**).



Slika 3: Lažna poruka o pogrešci koja se javlja prilikom pokretanja MyDoom.B crva

Kako bi se osiguralo da samo jedna inačica crva bude pokrenuta na sustavu, MyDoom.B će zaustaviti proces koji predstavlja staru inačicu crva i obrisati datoteku `shimgapi.dll`. Izvršna datoteka crva kopira se u glavni direktorij sustava (`%sysDir%`) pod imenom `explorer.exe`. Potrebno je primijetiti da na sustavu postoji i legalna `explorer.exe` datoteka koje se nalazi unutar `%windir%` direktorija.

U *Registry* sustava upisuju se ključevi `[HKLM\Software\Microsoft\Windows\CurrentVersion\Run] "Explorer" = %sysdir%\explorer.exe` ili (u slučaju neuspjeha) `[HKCU\Software\Microsoft\Windows\CurrentVersion\Run] "Explorer" = %sysdir%\explorer.exe`.

Kao i njegov prethodnik, i ovaj crv sadrži komponentu koja omogućava ulaz u sustav (*backdoor*), a nalazi se u `%sysdir%` direktoriju pod imenom `ctfmon.dll`. Za pokretanje backdoor komponente, kod podizanja sustava, koristi se *Registry* ključ `[HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32]`.

Navedeni ulaz u sustav otvoriti će se na mrežnim portovima 80, 1080, 3128, 8080 i 10080, a kao i kod prethodne inačice crva, pomoću njega je moguće pokretanje proizvoljnog koda na zaraženom sustavu ili njegova upotreba kao *proxy* poslužitelja, što se može iskoristiti za distribuciju neželjenih poruka elektroničke pošte (spam).

U svrhu onemogućavanja pristupa Web stranicama antivirusnih tvrtki, MyDoom.B na zaraženom sustavu kreira `hosts` datoteku sljedećeg sadržaja:

```
0.0.0.0     engine.awaps.net awaps.net www.awaps.net ad.doubleclick.net
0.0.0.0     spd.atdmt.com atdmt.com click.atdmt.com clicks.atdmt.com
0.0.0.0     media.fastclick.net fastclick.net www.fastclick.net ad.fastclick.net
0.0.0.0     ads.fastclick.net banner.fastclick.net banners.fastclick.net
0.0.0.0     www.sophos.com sophos.com ftp.sophos.com f-secure.com www.f-secure.com
0.0.0.0     ftp.f-secure.com securityresponse.symantec.com
0.0.0.0     www.symantec.com symantec.com service1.symantec.com
0.0.0.0     liveupdate.symantec.com update.symantec.com updates.symantec.com
0.0.0.0     support.microsoft.com downloads.microsoft.com
0.0.0.0     download.microsoft.com windowsupdate.microsoft.com
0.0.0.0     office.microsoft.com msdn.microsoft.com go.microsoft.com
0.0.0.0     nai.com www.nai.com vil.nai.com secure.nai.com www.networkassociates.com
0.0.0.0     networkassociates.com avp.ru www.avp.ru www.kaspersky.ru
0.0.0.0     www.viruslist.ru viruslist.ru avp.ch www.avp.ch www.avp.com
0.0.0.0     avp.com us.mcafee.com mcafee.com www.mcafee.com dispatch.mcafee.com
0.0.0.0     download.mcafee.com mast.mcafee.com www.trendmicro.com
0.0.0.0     www3.ca.com ca.com www.ca.com www.my-etrust.com
0.0.0.0     my-etrust.com ar.atwola.com phx.corporate-ir.net
```

Datoteka ovakvog sadržaja rezultirati će pridjeljivanjem IP adrese 0.0.0.0 imenima navedenih Web poslužitelja, tj. učiniti će ih nedostupnima.

Za svoju daljnju distribuciju, crv koristi vlastiti SMTP poslužitelj koji šalje zaražene poruke elektroničke pošte na adrese prikupljene iz raznih datoteka sa sustava. *From* polje kreirane poruke krivotvoriti će se adresom elektroničke pošte dobivenom na identičan način kao i ciljna adresa, dok će polje Subject sadržavati neke od sljedećih riječi:

```
Status
hi
Delivery Error
Mail Delivery System
hello
Error
Server Report
Returned mail
```

Tijelo poruke sadrži neki od sljedećih tekstova, koji upućuju korisnika da otvori attachement koji je poslan uz poruku:

- `The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.`
- `sendmail daemon reported: Error #804 occured during SMTP session. Partial message has been received.`
- `The message contains Unicode characters and has been sent as a binary attachment.`
- `The message contains MIME-encoded graphics and has been sent as a binary attachment.`
- `Mail transaction failed. Partial message is available.`

Ime privitka slučajno je odbrano između riječi:

```
document
readme
doc
text
file
data
message
body
```

i kombinirano s nekim od nastavaka `.pif`, `.scr`, `.exe`, `.cmd` i `.bat`.

U slučaju širenja MyDoom-a putem KaZaA mreže, crv će kopirati svoju izvršnu datoteku u direktorij sa dijeljenim datotekama pod nekim od sljedećih imena:

```
NessusScan_pro
attackXP-1.26
winamp5
MS04-01_hotfix
zapSetup_40_148
BlackIce_Firewall_Enterpriseactivation_crack
xsharez_scanner
icq2004-final
```

Slično kao i njegov prethodnik, MyDoom.B izbjegava slanje inficiranih poruka na određene domene i koristi vlastiti popis korisničkih imena za generiranje ciljanih adresa elektroničke pošte.

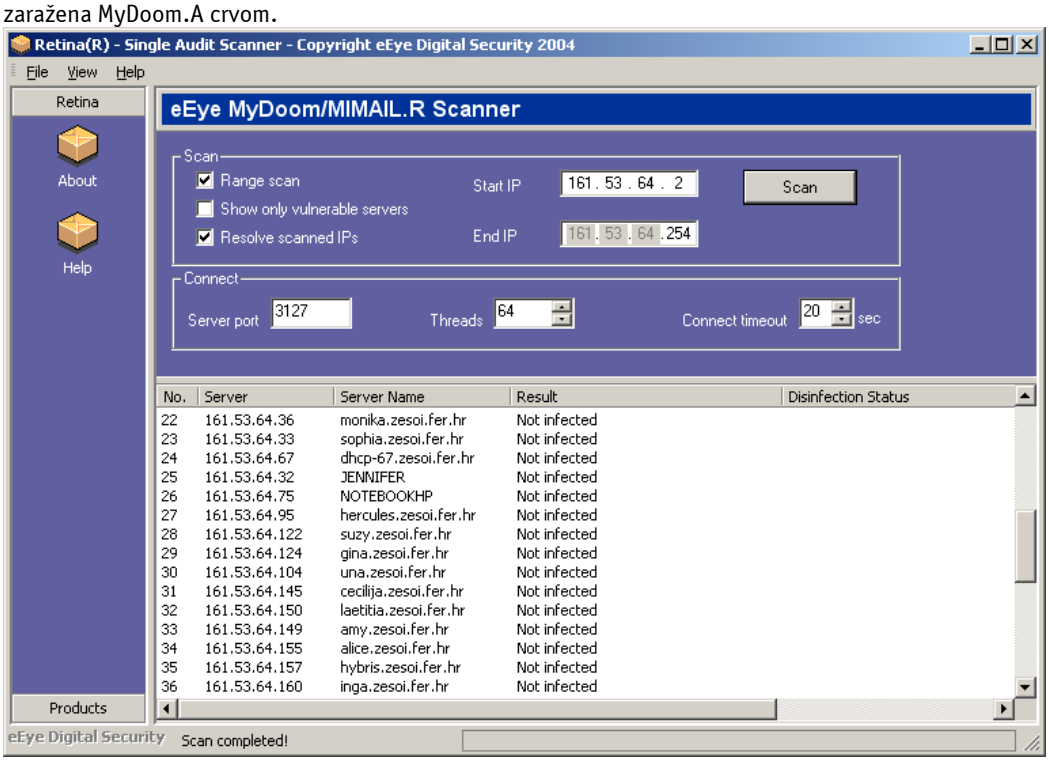
Dok je pokrenut, MyDoom.B će slati probne pakete na port 3127 slučajno odabranih računala na mreži. Cilj slanja probnih paketa je pronalaženje računala koja su zaražena MyDoom.A crvom. Ukoliko naiđe na zaraženi sustav, Mydoom.B će na njega prebaciti svoju izvršnu datoteku i pokrenuti se, uklanjajući na taj način staru inačicu crva zamjenjujući je novom.

1. veljače i 3. veljače MyDoom.B pokušati će izvesti DDoS napade na Web stranice www.sco.com, odnosno www.microsoft.com, a njegovo širenje automatski će se prekinuti 1. ožujka 2004. godine. Nakon tog datuma i dalje će ostati otvoreni portovi koji predstavljaju ulaz u sustav, kao i zapisi u `hosts` datoteci koji onemogućuju pristup određenim Web stranicma.

3. Detekcija i uklanjanje

Na mrežama sa manjim brojem osobnih računala moguće je, u svrhu detektiranja Mydoom-a, ručno pregledati svako računalo i uočiti eventualne znakove koji bi ukazivali na postojanje crva. Budući da ovakav postupak troši dragocjeno vrijeme mrežnog administratora i samih korisnika osobnih računala, na većim računalnim mrežama preporučuje se korištenje alata koji bi automatiziranim postupkom provjere utvrdili postojanje Mydoom crva na pojedinim računalima.

Kao primjer takvih alata, u ovom dokumentu će se opisati "MyDoom/MIMAIL.R scanner" (**Slika 4**) tvrtke eEye koji se može pronaći na Internet adresi http://www.eeye.com/html/Research/Tools/MyDoom.html. Korištenjem ovog alata trenutno je moguće prepoznati isključivo računala zaražena MyDoom.A crvom.



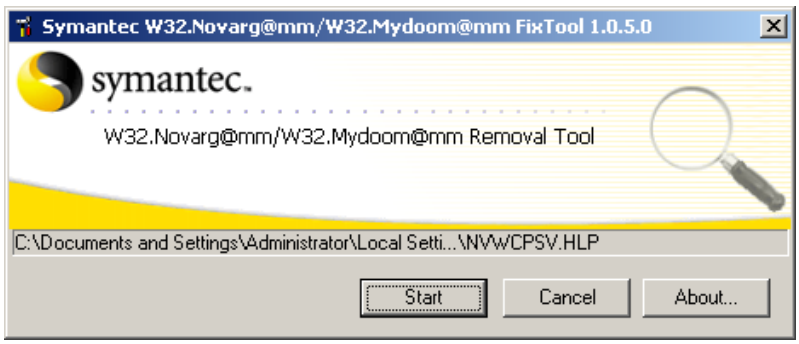
Slika 4: MyDoom pretraživač tvrtke eEye

Unutar sučelja ovog alata potrebno je unijeti raspon IP adresa koje se provjeravaju (besplatna inačica ovog programa ograničena je na raspon od 255 adresa) i kliknuti mišem na tipku *Scan*. Po završenom pregledavanju, unutar glavnog prozora grafičkog sučelja ispisati će se adrese računala za koje se sumnja da su inficirane MyDoom.A crvom.

Program radi na principu pregledavanja mrežnih portova računala na zadanoj mreži. Pregledava se pet uzastopnih portova, počevši od porta 3127 čije je postojanje uobičajeno za ovu inačicu crva. Ukoliko su ciljani portovi zatvoreni, smatra se da računalo nije inficirano i pokreće se pregledavanje portova sljedećeg računala na listi. U slučaju otvorenih portova 3127 do 3132, alat pokušava uspostaviti komunikaciju sa servisom koji osluškuje na spomenutim portovima i ukoliko dobije odgovor specifičan za MyDoom crv, proglasiti će računalo inficiranim.

Alat će označiti i potencijalno inficirana računala, tj. ona računala kod kojih sumnju u infekciju nije moguće u potpunosti potvrditi. Kod ovakvih računala potrebno je ručno obaviti provjeru nekim od automatiziranih alata ili ručnim pretraživanjem *Registry-a* računala i pregledom pokrenutih procesa.

Za automatsko uklanjanje crva sa zaraženih računala moguće je koristiti neki od posebnih alata za uklanjanje koje razvijaju kompanije koje se bave izradom antivirusnog softvera. Na **Slici 5** prikazan je jedan takav alat tvrtke Symantec, koji se može dohvatiti sa adrese http://securityresponse.symantec.com/avcenter/FxMydoom.exe.



Slika 5: Alat za uklanjanje MyDoom crva sa inficiranih računala

Ovaj alat sposoban je prepoznati i ukloniti MyDoom.A i MyDoom.B crve sa inficiranih računala. Pregledavanje računala pokreće se pritiskom na tipku Start, a cjelokupan tijek pregledavanja zapisuje se u log datoteku koja se kreira u direktoriju u kojem se nalazi alat.

U nedostatku alata za automatizirano uklanjanje Mydoom-a, moguće je obaviti i ručnu dezinfekciju računala.

Na računalima inficiranim crvom Mydoom –a potrebno je napraviti sljedeće korake:

1. Iz Windows *Registry-a* potrebno je ukloniti vrijednosti `[HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Taskmon]` i `[HKLM\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\lnprocServer32];`
2. Resetirati računalo;
3. Iz glavnog (`%System%`) direktorija sustava potrebno je obrisati datoteke `taskmon.exe` i `shimgapi.dll`. `%System%` direktorij uobičajeno je `C:\Windows\System` na Windows 95/98/Me operacijskim sustavima, dok je isti direktorij na Windows NT/2000/XP sustavima na lokaciji `C:\Windows\System32`.

Posebnu pozornost potrebno je obratiti prilikom uklanjanja datoteke `Taskmon.exe` sa Windows 95/98/Me sustava, budući da isto ime nosi i legalna datoteka na sustavu koja se nalazi u `C:\Windows` tj. `%Windir%` direktoriju.

Postupak za uklanjanje Mydoom.B crva gotovo je identičan i sastoji se od sljedećih koraka:

1. Iz Windows *Registry-a* potrebno je ukloniti vrijednosti `[HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Explorer]` i `[HKCR\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32];`
2. Resetirati računalo;
3. Iz glavnog (`%System%`) direktorija sustava potrebno je obrisati datoteke `explorer.exe` i `ctfmon.dll`;
4. Kako bi se omogućio ponovni pristup Web stranicama koje je crv blokirao, iz `hosts` datoteke potrebno je obrisati naknadno dodane retke.

Kao i kod MyDoom.A crva potrebno je obratiti pozornost prilikom uklanjanja datoteke `explorer.exe`, koja također postoji i kao legalna datoteka na sustavu i nalazi se u `%Windir%` direktoriju.

Prilikom postupka uklanjanja crva sa sustava, korisnicima Windows XP i Windows Me operacijskih sustava preporučuje se privremeno onemogućavanje System Restore opcije. System Restore opcija inicijalno je uključena na spomenutim sustavima, a upotrebljava se za povratak oštećenih ili nehotice obrisanih datoteka sustava. Korištenjem ove opcije postoji mogućnost da se postupkom restauracije inficirane datoteke vrate ne sustav.

4. Zaključak

Iako im je djelovanje vremenski ograničeno, obje inačice ovog crva predstavljaju veliku prijetnju po integritet inficiranog sustava. Prijetnju predstavljaju trajno otvoreni mrežni portovi pomoći kojih neovlašteni korisnik može, sa udaljenog računala, na sustav ubaciti proizvoljni programski kod i izvesti ga na inficiranom računalu. Veliku opasnost predstavljaju i neki mrežni crvi koji za svoje širenje koriste upravo ovaj propust.
Zbog spomenutih sigurnosnih prijetnji, osim uklanjanja Mydooma sa inficiranih računala preporučuje se i detaljna analiza operacijskog sustava koja bi otkrila eventualne maliciozne promjene nastale naknadnim djelovanjem neovlaštenih korisnika. Ukoliko je to moguće, svakako se preporučuje reinstalacija operacijskog sustava.

5. Reference

1. Symantec,
MyDoom.A, http://securityresponse.symantec.com/avcenter/venc/data/w32.novarg.a@mm.html,
MyDoom.B, http://securityresponse.symantec.com/avcenter/venc/data/w32.mydoom.b@mm.html.

2. Sophos,
MyDoom.A, http://www.sophos.com/virusinfo/analyses/w32mydooma.html,
MyDoom.B, http://www.sophos.com/virusinfo/analyses/w32mydoomb.html.

3. F-Secure,
MyDoom.A, http://www.f-secure.com/v-descs/novarg.shtml,
MyDoom.B, http://www.f-secure.com/v-descs/mydoom_b.shtml.