HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Mimail crva

CCERT-PUBDOC-2003-08-35

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

Početkom kolovoza pojavio se novi *mass-mailing* crv pod nazivom mimail. Ovaj crv po prirodi nije destruktivan, ali je njegovo agresivno širenje uzrokovalo zagušenje poslužitelja elektroničke pošte. Mimail se širi iskorištavanjem sigurnosnih propusta u Microsoft Internet Explorer-u, koji dozvoljavaju izvršavanje malicioznog programskog koda umetnutog unutar .html dokumenta, bez dodatne interakcije korisnika. Više o navedenim ranjivostima može se pročitati u Microsoft-ovim sigurnosnim priopćenjima MS03-014 i MS02-015.
U trenutku pisanja ovog dokumenta, u Hrvatskoj još uvijek nema podataka o djelovanju Mimail crva.

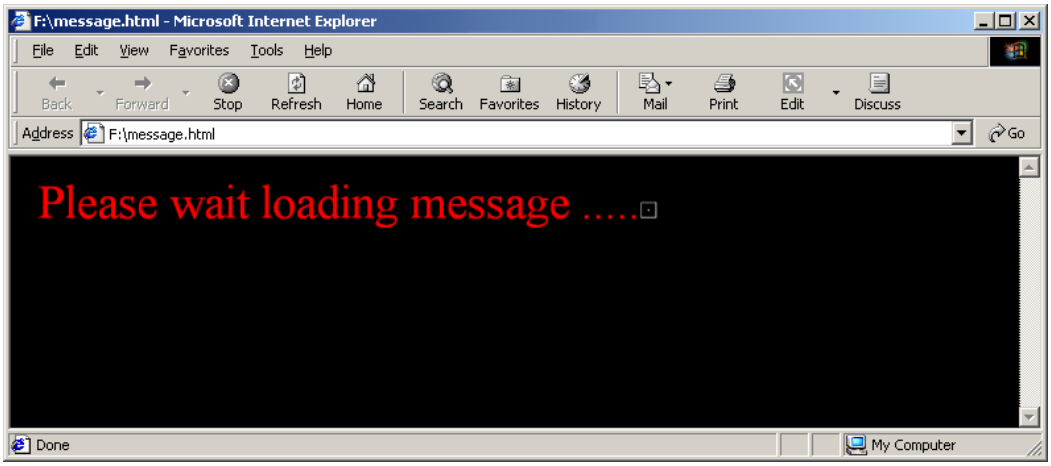
2. Analiza

Mimail se širi pomoću poruka elektronske pošte koje su sastavljene tako da korisnika navode na zaključak da je autor poruke administrator lokalne mreže i upućuju ga na otvaranje datoteke u prilogu (engl. *attachment*). Izvorišna adresa svih poruka prikazuje se kao administrator@ime_lokalne_domene. Naslov poruke sadrži riječi "*your account*" iza kojih slijedi slučajno odabrani niz znakova, dok tijelo poruke sadrži sljedeći tekst:

```
Hello there,

  I would like to inform you about important information regarding
your
  email address.  This email address will be expiring.
  Please read attachment for details
  ---
  Best regards,   Administrator
```

U prilogu se nalazi datoteka `message.zip`, unutar koje je zaražena datoteka `message.html`. Ova datoteka sadrži izvršni kod crva i JavaScript kod koji iskorištava ranjivost u Microsoft-ovom Internet Explorer-u. Njenim otvaranjem korisnik uzrokuje spremanje izvršnog koda crva u obliku datoteke `foo.exe` u direktorij `Downloaded Internet Files` i njegovo pokretanje. Za vrijeme pokretanja crva korisniku se unutar prozora Internet Explorer-a prikazuje poruka "*Please wait loading message .....*" (*Slika 1*).



Slika 1: Pokretanje crva na zaraženom računalu

Izvršni kod crva potom se kopira u datoteku `videodrv.exe` unutar sistemskog direktorija Windows sustava i u *Registry* ključ

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

upisuje se vrijednost `"VideoDriver"="%Windir%\videodrv.exe"`. Na taj način osigurano je pokretanje Mimail-a pri svakom ponovnom pokretanju operacijskog sustava.
Jednom pokrenut, Mimail provjerava da li je računalo spojeno na mrežu pokušavajući razlučiti IP adresu stranice www.google.com i, ukoliko u tome uspije, prikuplja sve adrese elektroničke pošte iz

svih datoteka na sustavu, osim onih koje nose nastavke `.bmp`, `.jpg`, `.gif`, `.exe`, `.dll`, `.avi`, `.mpg`, `.mp3`, `.vxd`, `.ocx`, `.psd`, `.tif`, `.zip`, `.rar`, `.pdf`, `.cab`, `.wav` i `.com`. Pronađene adrese spremaju se u datoteku `eml.tmp`, u isti direktorij kao i `videodrv.exe` datoteka.
Osim navedenih datoteka, u istom direktoriju, kreiraju se i datoteke `zip.tmp` i `exe.tmp` koje sadrže zaraženu html poruku, odnosno izvršni kod Mimail-a.
Za daljnje širenje Mimail koristi ugrađenu podršku za slanje poruka elektroničke pošte. Za svaku poruku koju šalje, crv će pokušati dohvatiti MX zapis za domenu na koju se šalje poruka i nakon toga izravno kontaktirati ciljani poslužitelj elektroničke pošte. Podatke o DNS poslužitelju Mimail će pokušati dobiti sa DNS poslužitelja zaraženog računala, a slučaju neuspjeha, koristiti će se DNS poslužitelj 212.5.86.163, čija je adresa upisana u izvršnom kodu virusa.
Mimail također pokušava dohvatiti određene podatke sa operacijskog sustava i poslati ih na adresu elektroničke pošte sadržanu u programskom kodu.

3. Uklanjanje

Prije uklanjanja Mimail-a sustav je potrebno nadograditi sigurnosnim zakrpama protiv ranjivosti MS02-015 i MS03-014, kako bi se izbjegla mogućnost ponovne zaraze. U *Windows Task Manager-u* potrebno je zaustaviti proces `videodrv.exe`. Korisnici Windows 95 i 98 operacijskih sustava proces mogu zaustaviti resetiranjem računala i pokretanjem u *Safe Mode* načinu rada.
Unutar Windows sistemskog direktorija (tipično `C:\windows` ili `C:\winnt`) potrebno je obrisati datoteke `videodrv.exe`, `eml.tmp`, `exe.tmp`, `zip.tmp`. Iz Windows *Registry-a* mora se ukloniti vrijednost `VideoDriver` iz ključeva
`"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"`, `"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run"`, te ključ `"{11111111-1111-1111-1111-111111111111}"` unutar `"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CodeStoreDatabase\Distribution Units"`.
Prije uklanjanja crva, korisnicima Windows XP i Windows Me operacijskih sustava preporučuje se isključivanje *System Restore* opcije, kako se prilikom restauracije sustava ne bi ponovo aktivirao virus.
Tvrtka Symantec je za potrebe automatskog uklanjanja Mimail crva izdala besplatan alat koji se može dobaviti sa adrese:
http://securityresponse.symantec.com/avcenter/venc/data/w32.mimail.a@mm.removal.tool.html.
Alat je moguće pokrenuti u grafičkom sučelju, ali i iz naredbene ljuske (engl. *command shell*). Prije pokretanja ovog alata, također je, kao i kod ručnog uklanjanja Mimail-a, poželjno nadograditi sustav sigurnosnim zakrpama i isključiti *System Restore* opciju.

4. Zaključak

Iako za sada Mimail ne uzrokuje stvarnu štetu na zaraženim računalima, smatra se kako je ovo samo početna faza razvoja ovog crva. Vrlo skoro se mogu očekivati novije inačice ovog crva koje bi mogle biti opasnije.
Zaraza Mimail crvom zaobišla je naša područje i teško je ocijeniti koliko računala još uvijek nije nadograđeno zakrpama protiv opisane ranjivosti. Korisnicima se preporučuje hitna nadogradnja zakrpama protiv ranjivosti opisane u dokumentu MS03-014, kako bi se, u slučaju pojavljivanja nove inačice Mimail crva, izbjegle eventualne štete.