HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

W32/Navidad crv

CCERT-PUBDOC-2000-10-07

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

U ovom dokumentu dana je analiza Navidad crva. Analiza virusa napravljena je zbog velike rasprostranjenosti na područjima CARNet-a. W32/Navidad@M je Internet crv koji se rasprostranjuje koristeći program za čitanje elektroničke pošte pod Windows operacijskim sustavima, Outlook. 11.10.2000. ovaj je crv označen da je široko rasprostranjen.

2. Analiza rada crva

Navidad je Internet crv koji koristi MAPI Outlook za rasprostiranje. Elektronička pošta koju korisnik dobije obično dolazi sa njemu poznate adrese. U privitku tih poruka nalazi se uvijek NAVIDAD.EXE datoteka koja sadrži sam crv. Ukoliko korisnik pokrene ovu datoteku dobiti će poruku u vidu okvira dijaloga naslovljenog Error u kojoj piše samo "UI". U tray dijelu pojaviti će se plava ikona oka kao što je prikazano na slici i kopija crva biti će zapisana u "winsvrc.vxd" datoteci u \Windows\System direktoriju. U slučaju da se crv uspješno postavio na sustav poslati će dalje e-mail poruke u kojoj će kao privitak biti opet NAVIDAD.EXE datoteka.
Analizom je ustanovljeno da crv stvara slijedeće postavke u registry-u sustava:

```
HKCU\SOFTWARE\Navidad
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
Win32BaseServiceMOD=C:\WINDOWS\SYSTEM\winsvrc.exe
HKCR\exefile\shell\open\command\
(default)=C:\WINDOWS\SYSTEM\winsvrc.exe "%1" %*
HKLM\Software\CLASSES\exefile\shell\open\command\
(default)=C:\WINDOWS\SYSTEM\winsvrc.exe "%1" %*
```

Kako ovi registry zapisi koriste nepravilni nastavak datoteka, rezultat postavljanja ovih zapisa biti će u tome da će onemogućiti pokretanje bili koje .exe izvršne datoteke.
Ovaj problem moguće je riješiti otvaranjem MS-DOS prompta, nakon čega je potrebno otići u Windows direktorij i kopirati REGEDIT.EXE u REGEDIT.COM datoteku. Nakon ovoga je moguće pokrenuti REGEDIT iz Start menija i otići do zapisa u registry-u te ukloniti krive zapise koji su navedeni.
Ukoliko je crv pokrenut na sustavu moguće ga je zaustaviti. Ako se klikne na ikonu oka koja je prikazana u trayu nakon što je crv pokrenut biti će prikazan prozor u kojem će stajati tekst da se ne klika. Ako se ovaj prozor zatvori na normalan način, crv će prikazati još jedan prozor sa tekstom nakon čega će biti prekinut njegov rad. Prozor je prikazan u dodatku.

2.1. Indikacije infekcije

- Prisutnost ikone oka u donjem desnom dijelu ekrana (u trayu sustava).
- Kada se pokazivač postavi na ikonu oka pokazat će se tekst "Lo estamos mirando ...", što u prijevodu znači "Gledamo vas".
- Kada se klikne na ikonu sa okom pojaviti će se prozor koji ima samo jedan button na kojem će pisati "Nunca presionar este boton", što u prijevodu znači "Ne pritišćite ovaj gumb."
- Ako se button na tom prozoru ipak pritisne pojavit će se novi prozor sa porukom "Lamentablemente cayo en la tentacion y perdio su computadora", što u prijevodu znači "Sretan Božić, nažalost niste izdržali i uništili ste računalo".

2.2. Metode infekcije

W32/Navidad@M se širi usprkos činjenici da postoji pogreška u programu. Ovaj crv dolazi na ciljno računalo kao privitak u e-mail poruci sa imenom Navidad.exe. Pokretanje ovog privitka automatski zaražuje ciljno računalo na kojem je pokrenut.
Ukoliko je crv pokrenut na sustavu moguće ga je zaustaviti. Ako se klikne na ikonu oka koja je prikazana u trayu nakon što je crv pokrenut biti će prikazan prozor u kojem će stajati tekst da se ne klika. Ako se ovaj prozor zatvori na normalan način, crv će prikazati još jedan prozor sa tekstom nakon čega će biti prekinut njegov rad.

2.3. Uklanjanje crva sa zaraženog računala

Postoje dvije mogućnosti ručnog uklanjanja crva sa zaraženog računala, obje metode su opisane u ovom dokumentu i isprobane na računalima inficiranim Navidad crvom.

1. Identificirati i označiti datoteke koje su asocirane sa crvom.
2. Napraviti UNDO.REG datoteku za čišćenje registry-a računala koja je priložena u dodatku ovog dokumenta i otvoriti je.
3. Pokrenuti Regedit.
4. Ukloniti sve ključeve koje je crv napravio ispod hijerarhije:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersionRun\`
5. Izaći iz Regedita.
6. Restartati sustav.
7. Obrisati sve datoteke koje su asocirane sa crvom.

2.4. Alternativna metoda uklanjanja crva sa zaraženog računala

1. Identificirati i označiti datoteke koje su asocirane sa crvom.
2. Pokrenuti Start -> Run i upisati
   `COMMAND /C COPY %WINDIR%\REGEDIT.EXE %WINDIR%\REGEDIT.COM`
3. Pokrenuti Regedit.com.
4. Ukloniti slijedeće reference na crva iz ovih ključeva registry-a:
   `HKEY_CLASSES_ROOT\exefile\shell\open\command\`
   `HKEY_LOCAL MACHINE\Software\CLASSES\exefile\shell\open\command`
   Ovi ključevi trebali bi imati samo vrijednosti koje ne uključuju ["%1" %*].
5. Ukloniti bilo koji ključ koji pokreće crva iz hijerarhije:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\`
6. Izaći iz Registry editora.
7. Restartati sustav.
8. Obrisati sve datoteke koje su asocirane sa crvom. Ukoliko se u ovom koraku pojavi greška da se neka datoteka ne može obrisati jer se koristi znači da procedura uklanjanja crva nije provedena uspješno i potrebno ju je ponoviti.

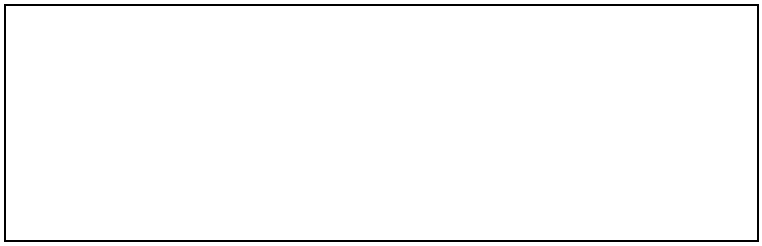
2.5. Informacije o crvu

Datum pronalaženja:	03.11.2000.
Izvor:	Južna Amerika
Veličina:	32.768 okteta
Vrsta:	Virus
Pod-vrsta:	Internet-crv
Nivo ugrožavanja:	Srednji

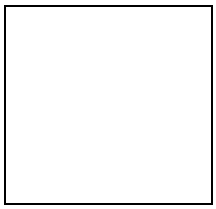
Inačica crva:
Emanuel
Emanuel dolazi također u e-mail porukama kao privitak pod imenom Emanuel.exe. Umjesto datoteke winsvrc.exe koristi se ime datoteke Wintask.exe. U ovoj inačici popravljena je pogreška sa imenima datoteka što rezultira u dodatnim instancama crva prilikom pokretanja bilo koje .exe datoteke. Umjesto ikone oka prikazuje ikonu cvijeta koja je identična ikoni ICQ programa za mrežnu komunikaciju korisnika.

Aliasi:
TROJ_NAVIDAD.B, TROJ_NAVIDAD.C, TROJ_NAVIDAD.D, TROJ_NAVIDAD.E, Emanuel, Emmanuel, I-Worm.Navidad, Navidad, TROJ_EMMANUEL, TROJ_NAVIDAD.A, W32.Navidad, W32.Navidad.16896, W32/Navidad-B, W32/Navidad.e@M, W32/Navidad.f@M, W32/Navidad.gen@M, Win32/Navidad.Worm

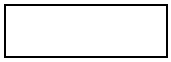
3. Prilog A: Slike rada crva



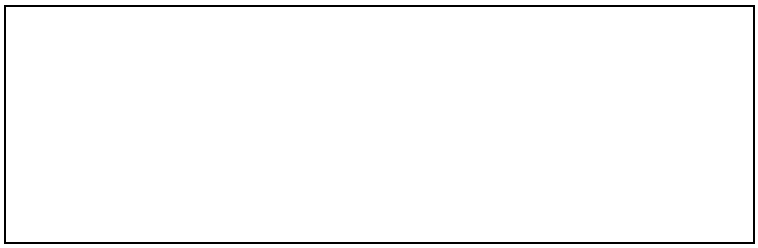
Poruka: "Sretan Božić, nažalost niste izdržali i uništili ste računalo".



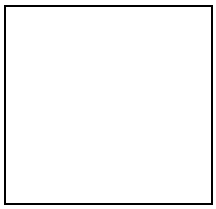
Prozor sa pogreškom kod Emanuel inačice.



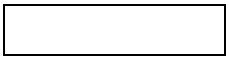
Ikona Emanuel inačice u trayu sustava.



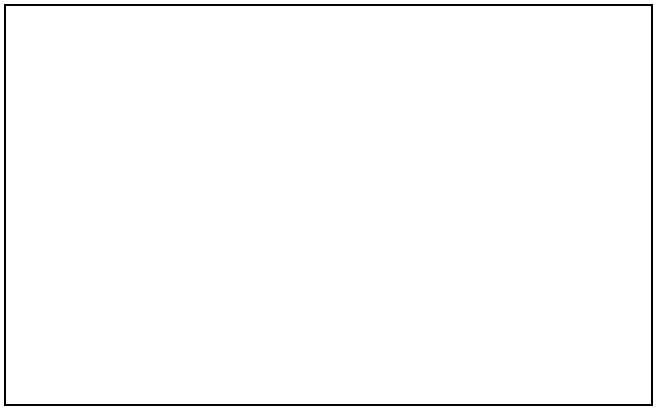
Poruka Emanuel inačice Navidad crva.



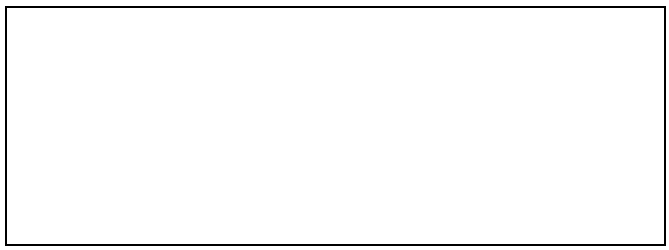
Prozor sa pogreškom.



Ikona Navidad inačice u trayu sustava.



Pogreška koja se pojavljuje prilikom postavljanja krivog imena datoteke (kod Navidada, ova je pogreška ispravljena u Emanuel-u).



Poruka: "Ne pritišćite ovaj gumb."

4. Prilog B: Undo.reg registry zapis

```
REGEDIT4

[HKEY_CLASSES_ROOT\exefile\shell\open\command]
@="\"%1\" %*"

[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command]
@="\"%1\" %*"
```