

Analiza crva Conficker / Downadup

INFIGO-TD-2009-03

2009-02-16

Ovaj dokument namijenjen je javnoj objavi, a vlasništvo je INFIGO IS. Svatko ga smije koristiti pozivati se na njega ili ga citirati, ali isključivo u izvornom obliku i uz obvezno navođenje izvora.

Korištenje dokumenata na bilo koji drugi način od gore navedenog, bez dozvole INFIGO IS predstavlja povredu vlasništva i kao takvo podložno je zakonskoj odgovornosti koja je regulirana zakonima Republike Hrvatske ili drugom primjenjivom regulativom.

Infigo IS d.o.o.
Horvatovac 20
10000 Zagreb

tel. +385 1 4662 700
fax. +385 1 4662 701
info@infigo.hr
www.infigo.hr



SADRŽAJ

1. SAŽETAK	4
2. DETEKCIJA I UKLANJANJE CRVA	5
2.1. DETEKCIJA CRVA	5
2.2. UKLANJANJE CRVA	7
2.2.1. UKLANJANJE S OSOBNIH RAČUNALA	7
2.2.2. UKLANJANJE U KORPORATIVNOM OKRUŽENJU	8
3. TEHNIČKA ANALIZA CONFICKER CRVA	9
3.1. VEKTORI INFEKCIJE	9
3.2. INFEKCIJA SUSTAVA	9
3.3. IDENTIFIKACIJA VIRTUALNIH OKRUŽENJA	11
4. ZAŠTITA	13

1. SAŽETAK

U studenom 2008. godine detektirane su prve inačice crva Conficker. Prva inačica crva, pod nazivom Conficker.A, bila je karakteristična po tome što je kao vektor infekcije koristila sigurnosnu ranjivost u Windows operacijskom sustavu (MS08-067), objavljenu u listopadu iste godine. Conficker.A nije bio značajno raširen te se pretpostavlja da je broj računala u Hrvatskoj pogođenih ovim crvom izuzetno malen.

Nova inačica crva, Conficker.B, pojavila se 29. prosinca 2008. godine. Riječ je o unaprjeđenoj inačici crva u koju su dodane višestruke funkcionalnosti koje su omogućile znatno učinkovitije širenje crva u odnosu na njegovu prvu inačicu. Stručnjaci tvrtke INFIGO IS među prvima su u svijetu detektirali i analizirali novu inačicu crva, koja se vrlo brzo rasprostranila i po Hrvatskoj.

U svega nekoliko dana, Conficker.B inficirao je milijune računala po cijelom svijetu. Crv koristi čitav niz vektora infekcije; počevši od infekcije preko računalne mreže korištenjem MS08-067 sigurnosne ranjivosti, preko USB medija pa do širenja kroz korisničke račune s slabim zaporkama u Windows domenama, što mu i dalje omogućava uspješno širenje, iako je većina anti-virusnih proizvođača izdala definiciju za detekciju.

Iako se Conficker.B crv širi iznimno agresivno, trenutna inačica ne posjeduje nikakve destruktivne mogućnosti, tako da korisnik inficiranog računala u većini slučajeva niti ne primjećuje da je njegovo računalo inficirano. U korporativnim okruženjima pojavu infekcije moguće je indirektno uočiti prilikom pokušaja širenja crva kroz Windows domenu što može dovesti do zaključavanja legitimnih korisničkih računa. Posebnu opasnost predstavlja činjenica da je crv u stanju uspješno inficirati sve Microsoft Windows operacijske sustave (Microsoft Windows 2000, XP, Vista te Server 2003 i 2008).

U ovom dokumentu dane su preporuke za uklanjanje crva s računala te tehnička analiza crva koju su proveli stručnjaci tvrtke INFIGO IS.

2. DETEKCIJA I UKLANJANJE CRVA

2.1. DETEKCIJA CRVA

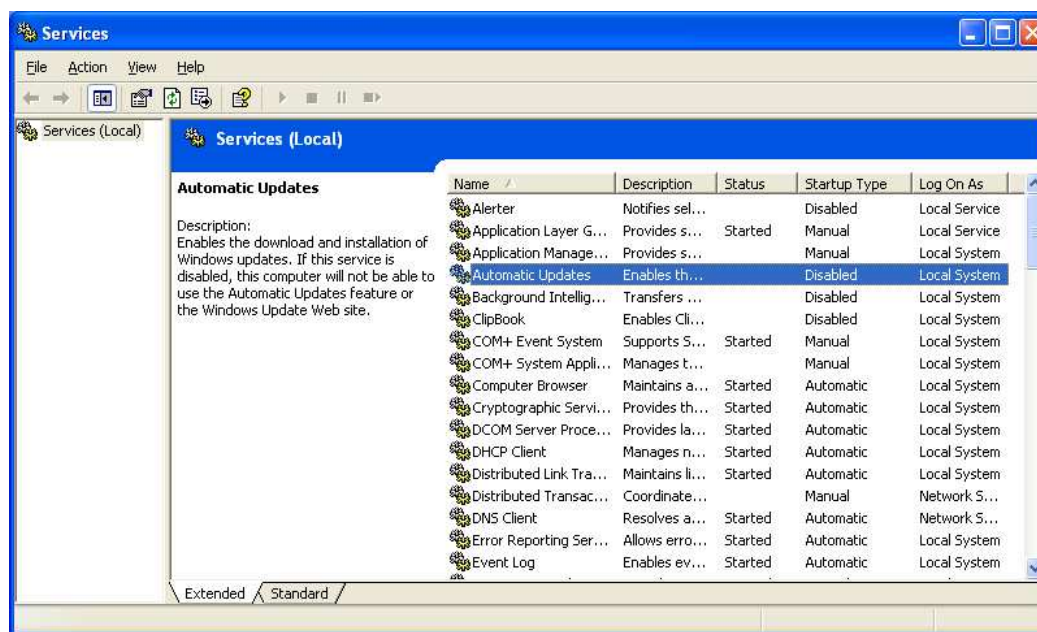
Prisutnost Conficker crva često nije očita, budući da crv u trenutnoj inačici ne provodi aktivnosti koje bi rezultirale izravnim nanošenjem veće štete za osobna računala, odnosno informacijske sustave. Na temelju provedenih analiza moguće je pretpostaviti da je jedan od glavnih ciljeva Conficker crva u ovom trenutku kreiranje tzv. *botnet* mreže računala, odnosno da se inficira što veći broj računala koja će kasnije omogućiti kontrolirano provođenje složenijih i vjerojatno znatno destruktivnijih napada. Računalo zaraženo Conficker crvom moguće je prepoznati na temelju određenih pokazatelja koji su opisani u nastavku:

- Crv Conficker.B isključuje ključne servise za zaštitu računala te onemogućuje njihovo automatsko pokretanje prilikom ponovnog pokretanja računala. Stanje servisa moguće je utvrditi pomoću **Services** programa koji se nalazi u kontrolnom panelu (na Windows XP računalima: *Start -> Control Panel -> Administrative Tools -> Services*, na Vista računalima: *Windows -> Control Panel -> System and Maintenance -> Administrative Tools -> Services*).

Ukoliko je računalo inficirano, slijedeći servisi biti će onemogućeni, odnosno postavljeni u stanje **Disabled**:

- **Automatic Updates** (na Vista računalima **Windows Update**) – servis zadužen za automatsko dohvaćanje i instalaciju zakrpi za operacijski sustav i Microsoftove proizvode,
- **Background Intelligent Transfer Service (BITS)** – servis zadužen za sam postupak dohvaćanja datoteka,
- **Error Reporting Service** – servis zadužen za prijavu grešaka o aplikacijama,
- **Security Center** – servis zadužen za nadgledanje sigurnosnih postavki sustava (da li je anti-virusni program instaliran, pokrenut i redovito osvježavan, stanje vatrozida te postavke za automatsko dohvaćanje zakrpi),
- **Windows Defender** - Microsoftov alat za uklanjanje malicioznih programa koji dolazi s Windows operacijskim sustavima.

Na sljedećoj slici prikazano je sučelje **Services** programa zaraženog računala, unutar kojega je moguće primijetiti da su servisi Automatic Updates i BITS onemogućeni, odnosno postavljeni u stanje **Disabled**.



Slika 1: Stanje servisa na inficiranom računalu

- Kao što je opisano u tehničkoj analizi crva (poglavlje 3 Tehnička analiza Conficker crva), ukoliko je crv aktivan na inficiranom računalu biti će onemogućen pristup web stranicama koje u URL adresi sadrže jednu od slijedećih riječi:

cert.	norman	f-prot
sans.	k7computing	jotti
bit9.	ikarus	kaspersky
vet.	hauri	f-secure
avg.	hacksoft	computerassociates
avp.	gdata	networkassociates
nai.	fortinet	etrust
windowsupdate	ewido	panda
wilderssecurity	clamav	sophos
threatexpert	comodo	trendmicro
castlecops	quickheal	mcafee
spamhaus	avira	norton
cpsecure	avast	symantec
arcabit	esafe	microsoft
emsisoft	ahnlab	defender
sunbelt	centralcommand	rootkit
securecomputing	drweb	malware
rising	grisoft	spyware
prevx	eset	virus

Budući da crv onemogućava pristup navedenim web stranicama tehnikom presretanja DNS upita i vraćanjem lažnih odgovora o nepostojećem DNS imenu, postojanje aktivnog crva na sustavu moguće je jednostavno provjeriti pokušajem otvaranja bilo koje web stranice koja sadrži navedene riječi u web pregledniku. Alternativno, razlučivanje DNS imena moguće je jednostavno provjeriti korištenjem PING naredbe.

Slijedeći primjer prikazuje korištenje PING naredbe prema adresi www.microsoft.com, u slučaju inficiranog računala:

```
C:\>ping www.microsoft.com

Ping request could not find host www.microsoft.com. Please
check the name and try again.
```

U slučaju ispravnog računala PING naredba trebala bi uspješno razlučiti www.microsoft.com DNS zapis (adrese se mogu razlikovati od onih prikazanih u nastavku):

```
C:\>ping www.microsoft.com
Pinging 1b1.www.ms.akadns.net [207.46.192.254] with 32 bytes
of data:
Request timed out.
```

Nemogućnost slanja PING paketa (*Request timed out* poruka o grešci) ne ovisi o crvu već o postavkama lokalne mreže te ju se može ignorirati. Ispravnost razlučivanja vidi se u pronađenoj IP adresi (označenoj žuto).

Prisutnost navedenih znakova ne garantira da je računalo inficirano s Conficker.B crvom, ali ukazuje na sigurnosne probleme u radu računala.

2.2. UKLANJANJE CRVA

Zbog korištenja naprednih tehnika prikrivanja, crv Conficker.B nije jednostavno ukloniti s računala. U tu svrhu anti-virusni proizvođači izdali su specijalizirane programe koji olakšavaju i automatiziraju postupak uklanjanja crva sa inficiranog računala. Više o metodama uklanjanja dano je u nastavku poglavlja.

2.2.1. UKLANJANJE S OSOBNIH RAČUNALA

S ciljem uklanjanja crva s osobnih računala preporučuje se dohvaćanje i pokretanje specijaliziranih alata navedenih u nastavku. Ovdje je potrebno napomenuti da je dohvaćanje navedenih alata s inficiranih računala otežano budući da crv Conficker.B, ukoliko je aktivan, onemogućava razlučivanje DNS imena web stranica anti-virusnih proizvođača.

Zbog toga se preporučuje dohvaćanje programa za čišćenje s drugog (neinficiranog) računala te prijenos na inficirano računalo putem CD (*read only*) medija. Ukoliko se za prijenos programa na inficirano računalo koristi USB medij posebnu je pozornost potrebno obratiti na način rukovanja istim, budući da će USB medij automatski biti inficiran nakon priključivanja na računalo inficirano Conficker.B crvom.

Specijalizirani alati za uklanjanje crva navedeni su u nastavku (abecednim redom, bez preferencija):

- AhnLab - http://global.ahnlab.com/global/file_removeal_down.jsp?filename=12339039520971&down_filename=v3conficker.exe
- BitDefender - <http://www.bitdefender.com/site/Downloads/downloadFile/1584/FreeRemovalTool>
- ESET - <http://download.eset.com/special/EConfickerRemover.exe>
- F-Secure - <ftp://ftp.f-secure.com/anti-virus/tools/beta/f-downadup.zip>
- Kaspersky - http://data2.kaspersky-labs.com:8080/special/KidoKiller_v3.1.zip
- McAfee - <http://vil.nai.com/vil/stinger/>
- Microsoft MSRT - <http://www.microsoft.com/security/malwareremove/default.aspx>
- Sophos - https://secure.sophos.com/support/updates/dp/full/scct_10_sfx.exe
- TrendMicro - http://www.trendmicro.com/ftp/products/pattern/spyware/fixtool/SysClean-WORM_DOWNAD.zip

Nakon provedenog čišćenja specijaliziranim alatima preporučuje se provjera stanja servisa navedenih u poglavlju 2.1, budući da u većini slučajeva anti-virusni programi neće vratiti

ispravno stanje ovih servisa već će korisnik to morati napraviti sam. Također, u nekim slučajevima programi neće ispravno očistiti *Registry* računala te će ovaj postupak također trebati provesti ručno.

2.2.2. UKLANJANJE U KORPORATIVNOM OKRUŽENJU

Uklanjanje crva u korporativnom okruženju otežano je zbog višestrukih vektora infekcije i kompleksnosti korporativnih informacijskih sustava. S ciljem uspješnog uklanjanja potrebno je identificirati kritične poslovne resurse i pažljivo planirati sve korake uklanjanja koji se mogu razlikovati u ovisnosti o pojedinom okruženju.

Ispravan redoslijed postupaka prilikom uklanjanja crva iznimno je važan kako bi se informacijski sustav u što kraćem vremenu u potpunosti očistio te zaštitio od ponovne infekcije.

3. TEHNIČKA ANALIZA CONFICKER CRVA

S ciljem detaljnijeg upoznavanja s načinom rada Conficker crva i sprječavanja njegovog širenja, u nastavku poglavlja navedene su tehničke informacije vezanu uz analizu crva koju su proveli sigurnosni stručnjaci INFIGO IS.

3.1. VEKTORI INFEKCIJE

Kao što je već ranije spomenuto, kao jedan od vektora infekcije Conficker crv koristi sigurnosni propust opisan u sigurnosnoj preporuci pod oznakom MS08-067 (<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>). Navedeni sigurnosni propust moguće je iskoristiti slanjem posebno oblikovanog RPC zahtjeva koji dalje omogućuje pokretanje proizvoljnog programskog koda na ranjivom sustavu.

U izvornom obliku Conficker je na datotečnom sustavu pohranjen kao dinamička biblioteka (eng. *DLL - Dynamically Linked Library*). Većina varijanti ovog crva pakirana je UPX tehnikom (eng. Ultimate Packer for eXecutables - <http://upx.sourceforge.net/>), kako bi se otežala izravna analiza programskog koda.

Iako kao osnovni vektor infekcije crv koristi MS08-067 ranjivost, autori ovog malicioznog programa osmislili su i dodatne tehnike kojima je cilj unaprijediti mogućnosti njegovog širenja. Spomenute tehnike najvećim dijelom oslanjaju se na korisničke navike u smislu korištenja prijenosnih medija kao što su USB stickovi i sl., te relativno nisku razinu sigurnosti lokalnih računalnih mreža.

Osnovni vektori infekcije koje crv Conficker koristi navedene su u nastavku:

- Iskorištavanje MS08-067 sigurnosnog propusta,
- Inficiranje USB uređaja i mrežnih dijeljenih diskova `Autorun.inf` datotekom,
- Iskorištavanjem slabih korisničkih zaporki.

Ovisno o vektoru širenja crv će poduzeti različite korake kako bi inficirao sustav i osigurao svoju postojanost. Prvi korak je pretraživanje aktivnih procesa za jednim od slijedećih programa:

- `svchost.exe -k netsvcs`
- `explorer.exe`

Nakon što je identificiran aktivni proces spomenutog imena Conficker će otvoriti njegov adresni prostor, alocirati memoriju potrebnu za smještaj programskog koda crva, te pozvati `CreateRemoteThread()` funkciju. Funkcija će kreirati dretvu (eng. *thread*) u adresnom prostoru ciljanog procesa kako bi se pokrenuo programski kod crva. Crv to radi na način da kreira dretvu funkcije `LoadLibrary()` i kao argument joj prosljeđuje DLL biblioteku samoga sebe. Ovakav poziv rezultirati će izvršavanjem programskog koda biblioteke tj. programski kod crva koji će nastaviti inficirati sustav.

Nakon što je umetnut u proces i nakon što je završio s učitavanjem biblioteke, crv kreira još jednu dretvu u kojoj će započeti s djelovanjem usmjerenim na daljnje širenje i sprječavanje uklanjanja.

3.2. INFEKCIJA SUSTAVA

Nakon što je pokrenut, crv će generirati slučajno ime te kreirati datoteku tog imena u jednoj od slijedećih lokacija:

- `%Program Files%\Internet Explorer\[slučajno ime].dll`
- `%Program Files%\Movie Maker\[slučajno ime].dll`
- `%Documents and Settings%\All Users\Application Data\[slučajno ime].dll`
- `%Temp%\[slučajno ime].dll`

- %System32%\[slučajno ime].dll

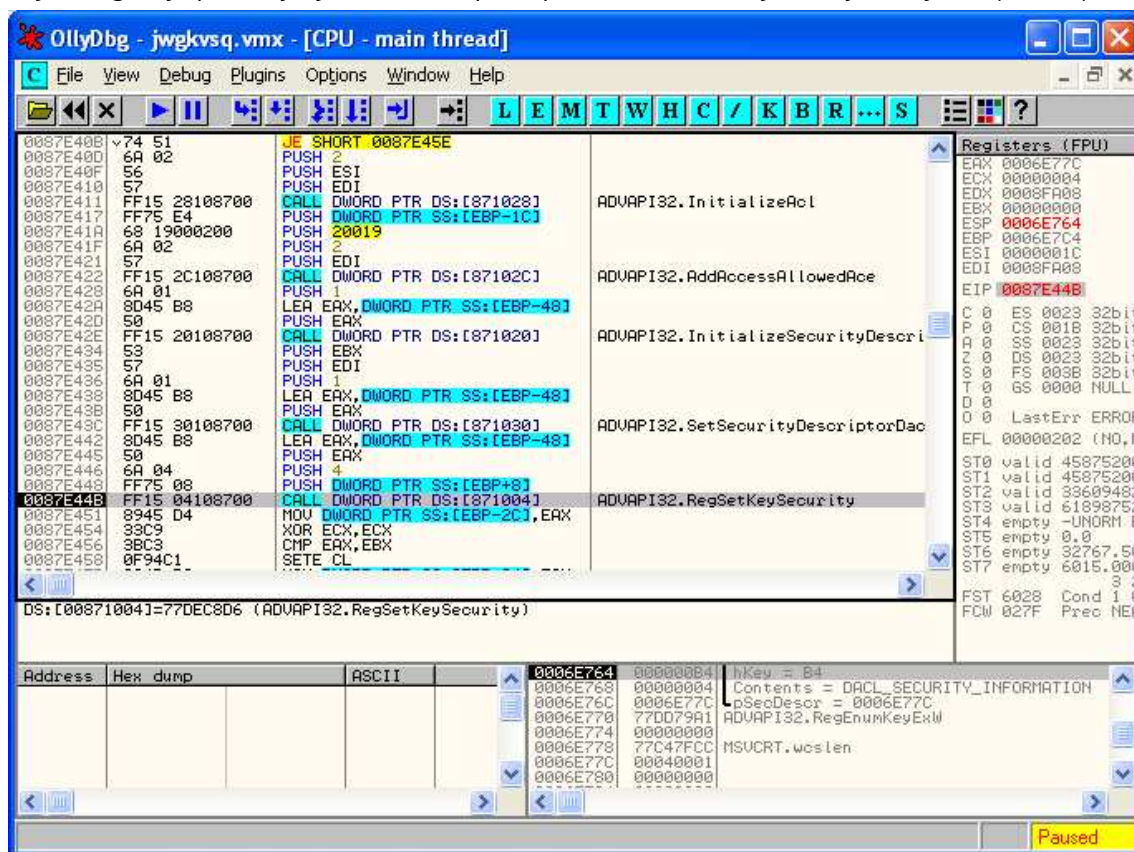
Kako bi osigurao svoju postojanost na sustavu crv će zakrpati, odnosno ukloniti MS08-067 sigurnosni propust tako što će dodati programski kod provjere argumenta ranjive `NetpPathCanonicalize()` funkcije.

Potrebno je napomenuti kako je u ovom slučaju propust ispravljen samo u memoriji i za vrijeme aktivnosti crva. Ukoliko crv bude uklonjen s računala, a korisnik samostalno ne instalira zakrpu, računalo će i dalje biti ranjivo i izloženo novim infekcijama.

Ponovno pokretanje malicioznog koda crv ostvaruje kreiranjem zapisa u *Registry*-u koji dodaje biblioteku `netsvcs` servisu:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netvcs\Parameters\ "ServiceDll" = "[Putanja do dll datoteke]"

Dozvoljavanjem izmjene ključa samo SYSTEM korisničkom računu uklanja se mogućnost da se sa ovlastima Administrator korisničkog računa ključ izmijeni ili ukloni. Dio programskog koda koji omogućuje postavljanje navedenih pristupnih lista označen je na sljedećoj slici (Slika 2).



Slika 2: Postavljanje pristupnih lista na *Registry* ključ

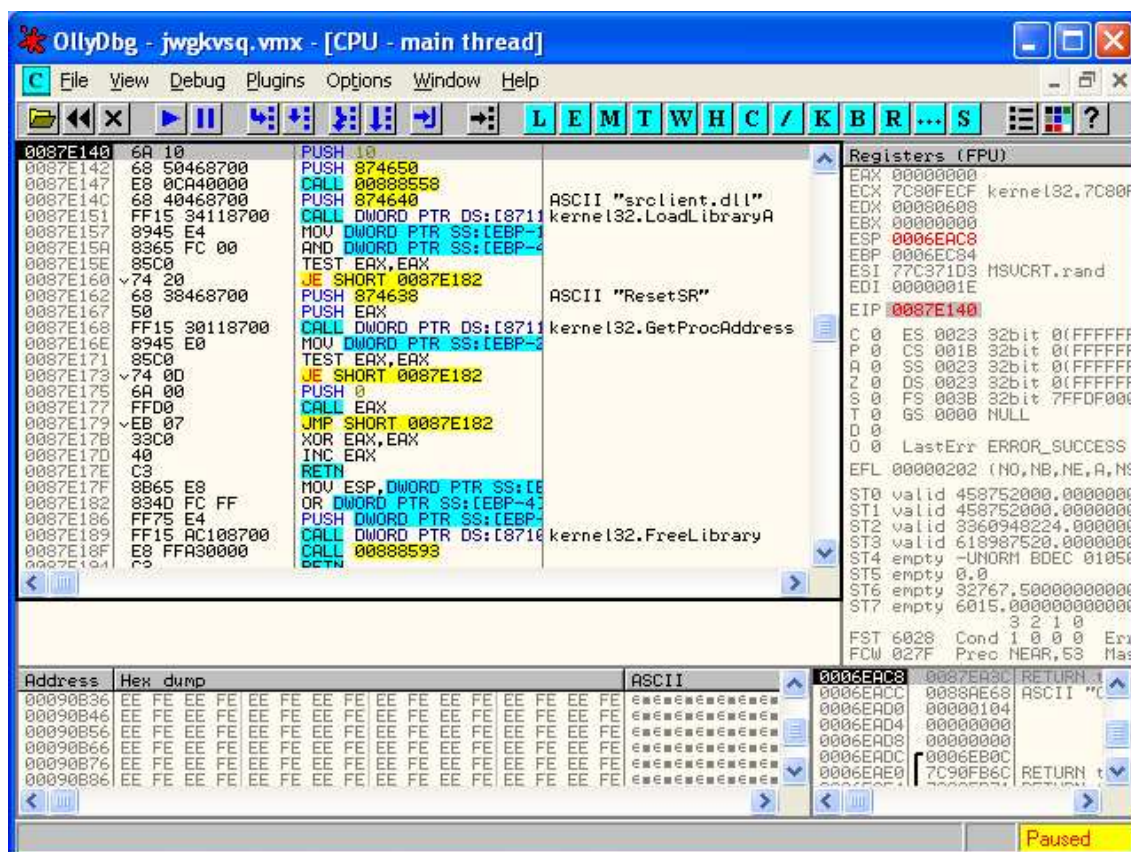
Crv također isključuje prikazivanje skrivenih datoteka u Windows Explorer programu postavljanjem slijedeće *Registry* vrijednosti:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL = 0

Kako bi se otežalo uklanjanje malicioznih datoteka s računala, crv će izmijeniti funkcije `DnsQuery_A`, `DnsQuery_W`, `DnsQuery_UTF8`, `Query_Main` iz `dnsapi.dll` biblioteke u svrhu filtriranja DNS zahtjeva prema domenama koje sadrže neki od navedenih znakovnih nizova. Znakovni nizovi koje program detektira i na temelju kojih blokira određene zahtjeve navedeni su u poglavlju 2.1 Detekcija crva.

Dodatni način na koji crv otežava svoje uklanjanje je brisanje sistemskih kontrolnih točaka Windows operacijskog sustava (eng. *System restore point*), te na taj način onemogućava povratak sustava u stanje prije zaraze.

Na sljedećoj slici (Slika 3) prikazan je dio asemblerskog programskog koda koji implementira navedenu funkcionalnost.



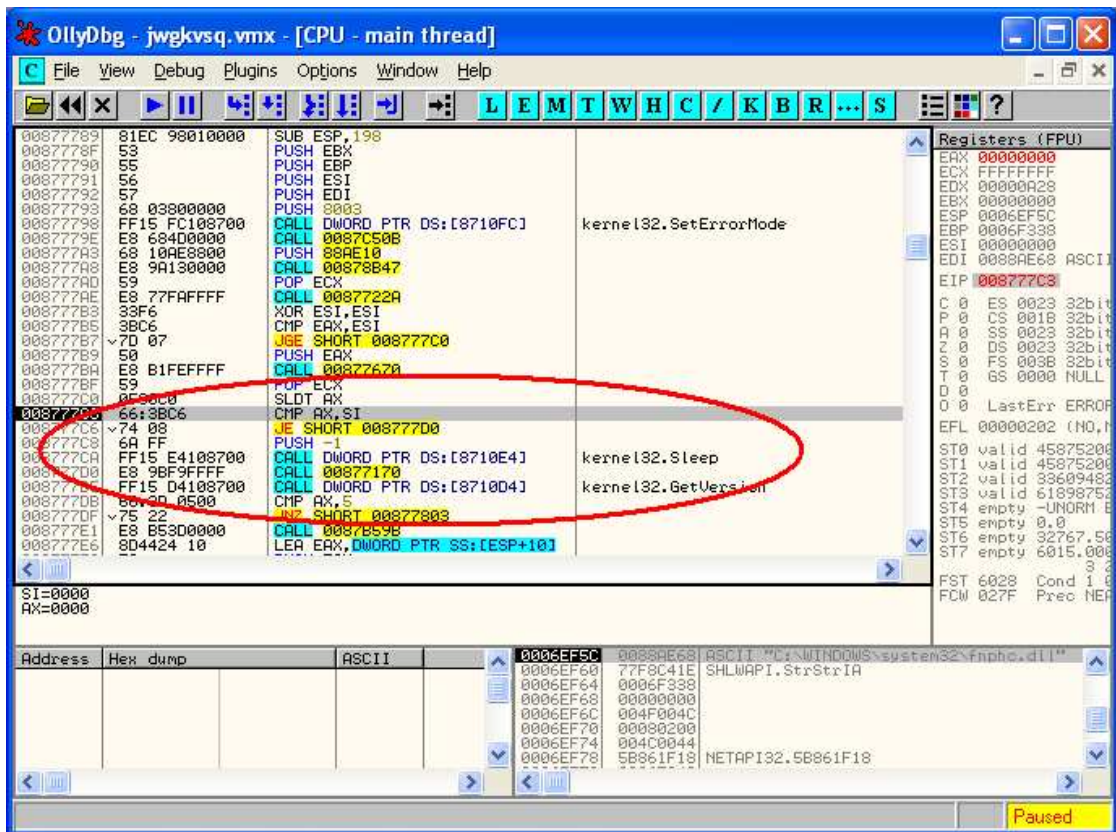
Slika 3: Brisanje sistemskih kontrolnih točaka

3.3. IDENTIFIKACIJA VIRTUALNIH OKRUŽENJA

Kako bi se otežala analiza samog crva, autori programa ugradili su funkcionalnost koja onemogućava njegovo pokretanje u kontroliranom, odnosno virtualnom okruženju, što je česta praksa koju sigurnosni stručnjaci primjenjuju prilikom analize malicioznih programa.

Detekcija virtualnog okruženja izvodi se korištenjem SLDT (eng. *Store Local Descriptor Table*) asemblerske instrukcije. Spomenuta instrukcija daje različite rezultate prilikom izvođenja u virtualnom i izvornom operacijskom sustavu, što je iskorišteno kao podloga za identifikaciju okruženja u kojem je program pokrenut.

U slučaju virtualnog sustava instrukcija vraća vrijednost različitu od 0 u ax registru, što omogućava jednostavnu detekciju virtualnog okruženja. Dio programskog koda koji omogućuje detekciju virtualnih okruženja prikazan je na sljedećoj slici (Slika 4). Kao što je moguće primijetiti na slici, u slučaju da je identificirano virtualno okruženje crv poziva Sleep() funkciju koja će zaustaviti daljnje izvršavanje programa.



Slika 4: Detekcija virtualnog okruženja SLDT instrukcijom

4. ZAŠTITA

Kao i kod većine malicioznih programa, ne postoji jedinstveno rješenje zaštite korisnika, već ju je potrebno provesti na svim razinama. U cilju zaštite preporuča se sljedeće:

- Redovito instalirati sigurnosne zakrpe za operacijske sustave i aplikacije. Zakrpe moraju biti redovito instalirane na sva računala kako bi se izbjegla mogućnost iskorištavanja poznatih sigurnosnih ranjivosti. Konkretno u ovom slučaju, Conficker crv kao jedan od vektora infekcije koristi ranije spomenutu MS08-067 ranjivost u Windows operacijskim sustavima. Prilikom instalacije sigurnosnih zakrpi posebnu pozornost valja obratiti na aplikacije čije osvježavanje nije moguće putem Windows Update servisa.
- Instalirati i redovito osvježavati anti-virusne programe. Iako anti-virusni programi ne mogu u potpunosti zaštititi korisnika, oni znatno mogu podići razinu sigurnosti računala. Konkretno, u slučaju Conficker.B crva, anti-virusni su programi bili neučinkoviti budući da ga niti jedan anti-virusni proizvođač nije bio u mogućnosti detektirati u trenutku početka širenja. Kako su anti-virusni proizvođači s vremenom dodavali definicije bilo je moguće daljnje sprječavanje širenja infekcije.
- Koristiti osobne vatrozide i na taj način maksimalno ograničiti izloženost računala.

U korporativnom okruženju prije svega je potrebno uspostaviti efikasne procese za upravljanje promjenama i upravljanje incidentima. Također, potrebno je iskoristiti dostupne sigurnosne mehanizme poput definiranja potrebe za snažnim zaporkama korisnika putem Group policy postavki u Windows domenama i sl. Konačno, potrebno je kontinuirano provoditi edukaciju zaposlenika u svrhu podizanja razine sigurnosne osviještenosti.