CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Conficker

NCERT-PUBDOC-2010-03-294

Nacionalni CERT

u suradnji s

LSS

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

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

Nacionalni 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

Računalni crvi (*eng. worms*) su zlonamjerni programi koji se bez sudjelovanja korisnika šire putem računalnih mreža na druga računala. Za razliku od virusa, crvi na ciljanom računalu ne inficiraju datoteke te imaju sposobnost samostalnog širenja i umnožavanja samih sebe. Najčešće iskorištavaju propuste u operacijskim sustavima i programima, a svojim djelovanjem uzrokuju probleme s performansama i stabilnošću računala te računalnih mreža. Prema nekim istraživanjima, crvi danas predstavljaju najveću prijetnju računalnoj sigurnosti. Među njima najrašireniji je crv *Conficker* kojim je trenutno zaraženo više od 5 milijuna računala. Crv je otkriven u studenom 2008. godine, a širi se iskorištavanjem sigurnosnih ranjivosti u operacijskim sustavima Microsoft Windows, putem zaraženih prijenosnih medija te razbijanjem slabih lozinki. *Conficker* spada u jedan od tehnički najsloženijih poznatih računalnih crva koji zapanjuje sigurnosne stručnjake brzinom kojom se širi. Osim brzine poznat je i po metodama (iskorištavanjem sigurnosnih ranjivosti te putem zaraženih prijenosnih medija) kojima se koristi kako bi antivirusnim proizvođačima otežao otkrivanje i uklanjanje s zaraženih računala. Do danas je otkriveno pet inačica ovog crva *(Conficker.A*, *Conficker.B*, *Conficker.C*, *Conficker.D te Conficker.E*) pri čemu starije inačice imaju mogućnost nadogradnje na novije. Iako je *Conficker* trenutno u fazi mirovanja (posljednja izdana inačica se pojavila u travnju 2009. god.), sigurnosni stručnjaci i dalje upozoravaju na njega čekajući vrijeme njegove ponovne aktivacije.

U ovom dokumentu bit će riječi općenito o računalnim crvima, načinima na koji se šire te će biti dan opis najraširenijih i najopasnijih crva koji su otkriveni u posljednjih dvadeset godina. Zatim slijedi detaljan opis i analiza računalnog crva *Conficker*, koji uključuje pregled svih inačica, načine širenja, simptome infekcije te geografsku rasprostranjenost. Na kraju će biti opisani načini zaštite od računalnih crva s naglaskom na *Conficker*.

2. Računalni crvi

Računalni crvi (*eng. worms*) su zlonamjerni programi koji se šire računalnim mrežama i računalima. Za razliku od virusa koji se umeću u određene programe te aktiviraju korisničkim pokretanjem inficirane izvršne datoteke, crvi su samostalni programi koje nije potrebno aktivirati već se oni šire i djeluju koristeći isključivo vlastite mehanizme.

Postoje dvije osnovne vrste crva:

- **Crvi na računalu domaćinu (*eng. host computer worms*)**

  Crvi na računalu domaćinu nalaze se u potpunosti na računalu na kojem su pokrenuti i upotrebljavaju mrežnu komunikaciju samo za širenje na druga računala. Posebnu potkategoriju ovih crva predstavljaju oni koji prestaju s radom nakon što su se uspješno pokrenuli na drugom računalu (u jednom trenutku postoji samo jedna kopija crva na pojedinom računalu u mreži). Ovi crvi se ponekad nazivaju i zečevi (*eng. rabbits*).

- **Mrežni crvi (*eng. network worms*)**
  Mrežni crvi sastoje se od nekoliko modula, od kojih je svaki pokrenut na posebnom računalu (obično svaki dio provodi različitu aktivnost). Ovakvi crvi upotrebljavaju računalnu mrežu za međusobnu komunikaciju između modula. Šire se kopiranjem samo pojedinih dijelova na druga računala, a glavni dio koji upravlja svim ostalima naziva se hobotnica (*eng. octopus*). Glavni dio nalazi se također na jednom od zaraženih računala. Zbog znatno složenije izvedbe susreće ih se jako rijetko.

2.1. Načini širenja računalnih crva

Najvažnija osobina crva je njihovo izrazito brzo širenje. Internet, javno dostupna globalna podatkovna mreža koja povezuje računala i računalne mreže, postala je idealni medij za širenje crva. Kada govorimo o načinima širenja računalnih crva, opće prihvaćena klasifikacija je ona prema transportnom mehanizmu te prema načinu djelovanja.

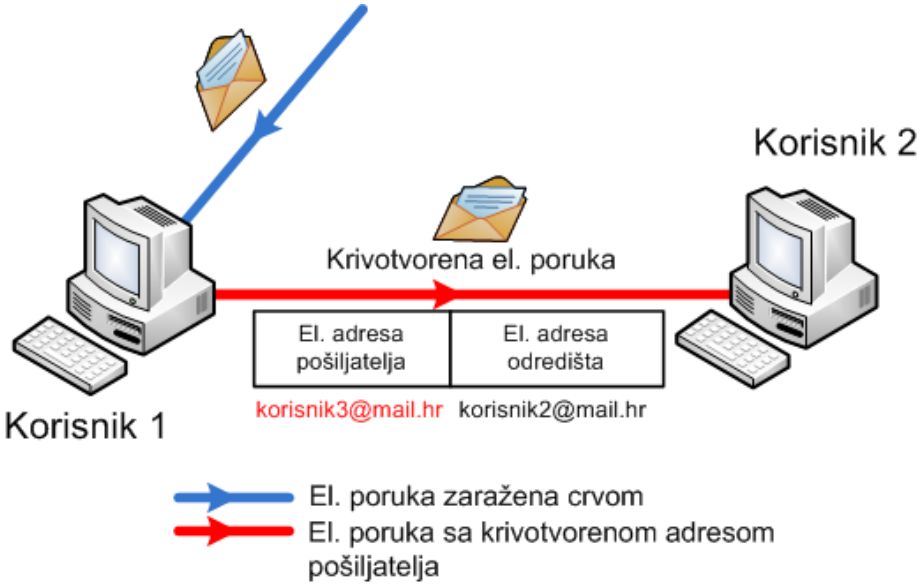
2.1.1. Podjela prema transportnom mehanizmu

1) Crvi koji se šire elektroničkom poštom

Najčešći način zaraze računala crvom je putem elektroničke pošte. Većina računalnih crva nalazi se u privitku poruke elektroničke pošte čije otvaranje uzrokuje zarazu računala. Crv u korisničkom računalu traži datoteke koje sadrže adrese elektroničke pošte (npr. Outlook adresar). Na pronađene adrese crv šalje poruke elektroničke pošte koje sadrže datoteke crva. Ovaj postupak ponavlja se na svakom računalu koje se zarazilo. Osim pretraživanja adresara elektroničke pošte, postoje i naprednije metode za pronalaženje potencijalnih adresa elektroničke pošte. Najčešće korištene tehnike su:

- pretraživanje adresara MS Outlook / Outlook Express programa,
- pretraživanje „.wab“ datoteka (koriste se za pohranu adresara MS Outlook Expressa),
- pretraživanje raznih podatkovnih datoteka u potrazi za adresama elektroničke pošte,
- slanje svoje kopije u obliku odgovora na sve pronađene poruke u pretincu za poštu i
- generiranje novih adresa elektroničke pošte konstruiranih iz nasumce odabranih imena i često korištenih domena.

Jedan od najpoznatijih crva koji se šire elektroničkom poštom je crv *Hybris* koji je u stanju promijeniti podatke u zaglavlju elektroničke pošte što primatelju poruke koja sadrži crva znatno otežava pronalazak pravog pošiljatelja. Cilj otežavanja identifikacije izvora ima za posljedicu nemogućnost obavještavanja korisnika o zaraženosti njegovog računala. Na slici 1. prikazan je način zaraze računala crvom putem elektroničke pošte.



Slika 1. Način zaraze računala crvom putem elektroničke pošte
Izvor: CERT

Slijedi opis procedure prikazane na slici:

1. Korisniku 1 je poslana poruka e-poštom koja je zaražena crvom. Otvaranje te poruke rezultira zarazom računala.
2. Crv pronalazi adrese e-pošte Korisnika 2 i Korisnika 3 u adresaru Korisnika 1.
3. S računala Korisnika 1, crv šalje zaraženu poruku e-pošte Korisniku 2, pri čemu se čini da je poruka poslana s adrese Korisnika 3.

2) Crvi koji se šire korištenjem raznih drugih mehanizama

Drugi najčešće upotrebljavani način širenja crva računalnom mrežom jest korištenje sigurnosnih propusta u određenim programima. Sigurnosni problemi operacijskih sustava i servisa su, nažalost, vrlo prisutni, a jedini način borbe protiv crva koji na taj način napadaju je redovito instaliranje sigurnosnih zakrpi. Najčešći mehanizmi kojima se računalni crvi šire su:

- **Instant messaging**

  Crvi se šire putem programa za slanje poruka u realnom vremenu (MSN, ICQ i sl.). Način je vrlo jednostavan – svim kontaktima u adresaru šalju se poruke s URL adresama koje vode na inficirane *web* stranice. Dakle, jedina razlika u odnosu na računalne crve koji se šire putem elektroničke pošte je medij kojim se crv prenosi.
- **IRC**

  IRC (*eng. Internet Relay Chat*) je još jedan način komunikacije u stvarnom vremenu, ali s naglaskom na grupne diskusije koje se odvijaju u tzv. IRC kanalima. IRC crvi šire se putem IRC kanala za chat slanjem zaraženih datoteka ili URL adresa koje vode na inficirane *web* stranice
- **File sharing**

  Širenje crva događa se putem P2P (*eng. Peer-To-Peer*) programa za razmjenu sadržaja preko Interneta. Crvi se nalaze pod bezazlenim imenima u mapama korisnika koje služe za dijeljenje te na taj način postaju dostupne svim korisnicima P2P programa. Napredniji crvi ove vrste sposobni su imitirati cjelokupne protokole mreža za razmjenu sadržaja, potvrdno odgovarati na sve zahtjeve te se širiti na sve sudionike pojedine mreže.

3) Internet crvi

Internet crvima nazivamo brojne crve koji se služe alternativnim metodama širenja koje do sad nisu spomenute. Slijedi nekoliko takvih primjera:

- Crv se kopira u razne dostupne mrežne resurse (dijeljene i nezaštićene direktorije) u lokalnoj mreži nakon čega pokušava u potpunosti ovladati računalom.

- Crv iskorištava ranjivosti operacijskih sustava (posebice onih računala koja nemaju ažurirane sigurnosne postavke) kako bi se probio i kopirao u računala ili računalne mreže.
- Crv iskorištava ranjivosti javnih mreža, inficirajući datoteke na poslužitelju (*web* stranice). Prilikom korisnikova spajanja na navedeni poslužitelj dolazi do inficiranja računala.
- Crv koristi zlonamjerne programe (*eng. Backdoor*) koji omogućavaju zlonamjernim korisnicima nesmetan i neovlašten pristup računalu. *Backdoor* programi koriste slabosti operacijskih sustava te antivirusnih programa. Ovakve vrste napada danas su sve češće i opasnije.

2.1.2. Podjela prema načinu djelovanja

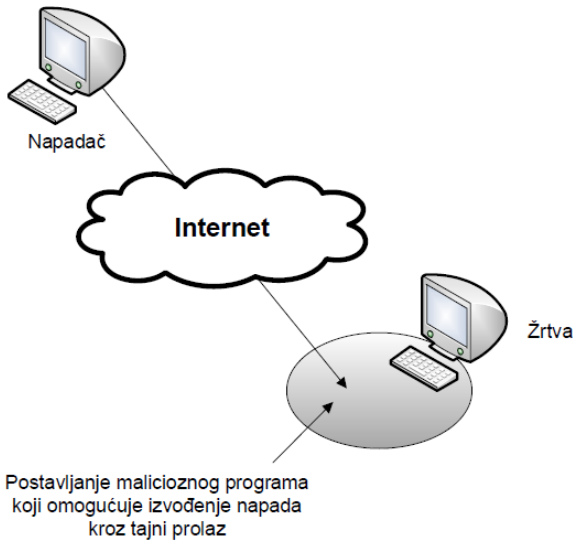
Crvi se sastoje od dijela koda za repliciranje koji omogućava razmnožavanje i širenje crva te tereta *(eng. payload)* koji može imati razne učinke. Ovisno o teretu, crvi se dijele na:

1) **Nepostojeći/nefunkcionalan**

   Najčešći slučaj, crv se sastoji samo od koda za širenje ili u dijelu koda koji određuje teret crva postoji neka pogreška tako da se taj dio ne izvodi. Cilj ove skupine crva je opterećenje mreže.

2) **Daljinski nadzor**

   Većina poznatih crva dolazi s nekom vrstom programa koji stvaraju stražnje ulaze (*eng. Backdoor*) koji neovlaštenom korisniku omogućuju nadzor nad inficiranim sustavom. Ti programi predstavljaju teret crva. *Backdoor* programi nakon instalacije na zaraženom računala otvaraju jedan ili više komunikacijskih kanala preko kojih računalo komunicira s vanjskim svijetom (*eng. port*). Preko tih kanala zlonamjernom korisniku je omogućen udaljeni pristup računalu . Slika 2. prikazuje kako zlonamjerni korisnici putem *backdoor* programa ostvaruju nadzor nad zaraženim računalom.



Slika 2. Daljinski nadzor zaraženog računala omogućen backdoor programom
Izvor: Google

3) **DOS**

   Vrlo često teret čini programski kod kojim se izvode DOS (*eng. Denial of Service*) napadi na zaraženo računalo. Napad uskraćivanjem usluge je vrsta napada na računalne resurse kojim se ti resursi mogu učiniti nedostupnim. Posljedice DOS napada mogu biti vrlo ozbiljne.

4) **Skupljači podataka**

   Većina ljudi na računalu na kojem rade imaju osjetljive podatke poput poslovnih tajni, nacrta novih uređaja, financijskih izvješća i sl. Crv može pretražiti disk računala u potrazi za tim podacima i zatim ih poslati na unaprijed određeno mjesto.

5) **Brisači podataka**

Crvi čiji teret sadrži kod za brisanje podataka. Podaci se mogu početi brisati odmah nakon infekcije računala crvom ili nakon određenog vremena.

6) **Fizička šteta**

Crvi posjeduju teret koji na zaraženim računalima radi fizičku štetu. Primjerice, većina današnjih računala podržava nadogradnju pokretačkih programa. Računala imaju BIOS čip koji je moguće nadograditi izravno iz Windowsa. Ukoliko se u BIOS čip upišu pogrešni podaci računalo se više neće moći pokrenuti.

3. Računalni crvi kroz povijest

Prvi crv koji je nametnuo pitanje sigurnosti komunikacije na Internetu se pojavio 1988. godine. Morrisov crv (*eng. Morris Worm*) je dobio ime po svom autoru Robertu T. Morrisu. Crv je napadao računala s operacijskim sustavom UNIX, iskorištavajući poznate sigurnosne probleme u servisima. Zapamćen je kao prvi automatizirani mrežni napad. Broj inficiranih računala kretao se oko 6 000 (što je u to vrijeme s obzirom na ukupan broj računala bilo jako puno), a nastala šteta je procijenjena na 96 milijuna dolara. Prvi čovjek koji je bio osuđen zbog računalnih aktivnosti u SAD-u bio je upravo R. Morris. Dobio je 3. godine zatvora, 400 sati društvenih aktivnosti te novčanu kaznu od 10 500 dolara. Kao posljedica ovog napada osnovan je prvi CERT (*eng. Computer Emergency Response Team*) čija je zadaća bila intervenirati u ovakvim slučajevima. Slijedi pregled nekih od najraširenijih i najopasnijih crva koji su se pojavili u posljednjih dvadeset godina.

3.1. Crv Code Red

2001. godine otkriven je računalni crv *Code Red* koji iskorištava ranjivost u Microsoftovom *web* poslužitelju IIS (*eng. Internet Information Services*). Crv se širi spajanjem na nasumce odabrane IP adrese. *Code Red* pokreće DOS (*eng.Denial of Service*) napad te briše ili mijenja *web* stranice na zaraženom računalu. Dvije godine kasnije (2003.) pojavila se nova inačica, nazvana *Code Red II* koja na zaraženim računalima postavlja trojanskog konja. Crv je inficirao veliki broj računala iako je zakrpa (MS01-033) za navedenu ranjivost izdana mjesec dana prije njegova otkrivanja. Na svom vrhuncu, broj računala koje je crv zarazio dosegao je 760 tisuća. Troškovi uklanjanja crva *Code Red* procjenjuju se na 2,6 milijardi dolara.

3.2. Crv Nimda

Računalni crv *Nimda* (anagram od riječi „admin“) pojavio se 2001. godine. Crv se širi elektroničkom poštom koja ima prazno polje „subject“, s privitkom koji sadrži datoteku imena „readme.exe". Ukoliko se datoteka pokrene na računalu, crv će se poslati svim kontaktima u adresaru. Osim elektroničkom poštom, širi se dijeljenim datotekama, posjetima zaraženim *web* stranicama te iskorištavanjem sigurnosnih rupa koje je ostavio *Code Red*. Sigurnosni propust na Microsoftovom *web* poslužitelju IIS omogućuje crvu dolazak na javno objavljene *web* stranice kako bi postavio link na zaraženu datoteku. Preuzimanje i pokretanje datoteke uzrokuje zarazu računala crvom. Kombinacija nekoliko vektora infekcije omogućila mu je da se u vrlo kratkom roku proširi svijetom. Već prvi dan crv je napao poslužitelje u Japanu, Hong Kongu, Kini, Koreji, Singapuru te SAD-u. Šteta koju je napravio ovaj crv procjenjuje se na oko 635 milijuna dolara.

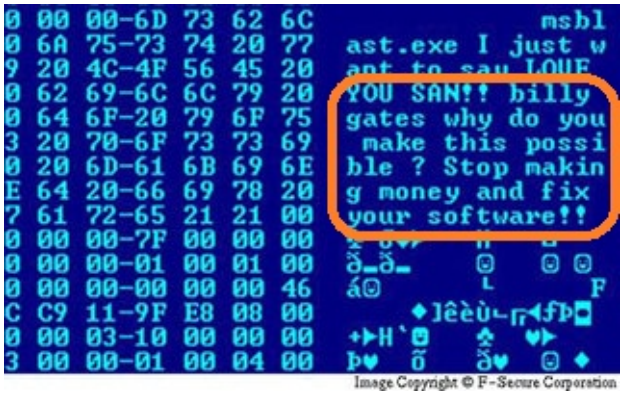
3.3. SQL Slammer crv

Crv po imenu *SQL Slammer*, poznat i kao *Saphire*, javio se 2003. godine. On koristi ranjivost u Microsoftovom SQL Server 2000 servisu. Generiranjem velikog broja malih paketa podataka koji preplavljuju DNS *(eng. Domain Name System)* poslužitelje odgovorne za preusmjeravanje prometa prema željenim adresama, crv otežava ili onemogućuje normalno korištenje mrežnih resursa. U cijeloj Južnoj Koreji, zemlji u kojoj je preko 70% domaćinstava priključeno na Internet, korisnicima je na nekoliko sati bilo onemogućen pristup zbog pada njihovog davatelja Internet usluga (*eng. Internet service provider ISP*). Prema izvještajima *Bank of America*, preko 13 tisuća njihovih bankomata širom Sjeverne Amerike je jednostavno odbijalo izdati novac tijekom vikenda. Korisnici širom Amerike i Europe imali su probleme s učitavanje *web* stranica. Rezultati istraživanja *Cooperative Association for Internet Data Analysis* (CAIDA), grupe specijalizirane za računalnu sigurnost, *SQL Slammer* crvu je trebalo samo deset minuta da se proširi širom svijeta napadajući osobna računala, korporacije te Internet poslužitelje. Naime, crv je udvostručavao broj zaraženih računala svakih 8,5 sekundi u prvoj minuti nakon pojave, dok je, primjerice, crv *Code Red*, koji se pojavio 18 mjeseci ranije, udvostručivao broj zaraza svakih 37 minuta. Sigurnosni

stručnjaci se slažu kako je brzina širenja ovog crva zapanjujuća. Koliko je ozbiljna prijetnja bila govori i činjenica da su je neke države proglasile napadom na nacionalnu sigurnost.

3.4. Crv Blaster

Crv *Blaster* pojavio se 2003. godine, nedugo nakon otkrivanja sigurnosnog propusta (MS03-026) u primjeni RPC *(eng. Remote procedure call)* sučelja na operacijskim sustavima Windows 2000 i Windows XP. RPC protokol omogućuje Windows platformama izvođenje programskog koda na udaljenom sustavu. Pogreška u jednom dijelu RPC-a utječe na DCOM (*eng. Distributed Component Object Model*) sučelje koje obrađuje zahtjeve za aktivacijom DCOM objekata, koje je klijent poslao poslužitelju. Udaljeni napadač može iskoristiti ovu ranjivost za izvođenje proizvoljnog programskog koda. Crv je u kratkom vremenskom razdoblju zarazio veliki broj računala, uzrokujući svojim širenjem napad uskraćivanjem računalnih resursa (DoS napad) na zaraženim računalima. Ostao je zapamćen po skrivenoj poruci *„Bill Gates, zašto dopuštaš ovo? Prestani zgrtati novac i popravi svoj software!"* Na slici 3. je prikazana prethodno navedena poruka pronađena u kodu crva *Blaster*.



Slika 3. Poruka koja se nalazi u kodu crva Blaster
Izvor: Google

3.5. Crv Sasser

Crv pod imenom *Sasser* otkriven je 2004. godine. Za razliku od većine crva koji se šire putem e-pošte, ovaj crv iskorištava sigurnosni nedostatak (MS04-011) u LSASS MS-RPC komponenti na operacijskim sustavima Windows 2000 te Windows XP. LSASS (*eng. Local Security Authority Subsystem Service*) je proces zadužen za sigurnost sustava, koji se među ostalim koristi i za provjeru identiteta i lozinke korisnika pri njegovom spajanju na sustav. Propust je uzrokovan pogrešnom obradom LPC (*eng. Local Procedure Call)* zahtjeva, a napadač ga može iskoristiti za pokretanje proizvoljnog programskog koda na ranjivom računalu. Uspješnim iskorištavanjem ovog propusta napadač dobiva administratorske ovlasti na računalu. *Sasser* je nanio štetu mnogim kompanijama počevši od Britanske obalne straže pa do Delta Airlinesa koji su zbog njega morali otkazati neke letove. Šteta koja je prouzročena ovim crvom procjenjuje se na 500 milijuna dolara.

3.6. Crv Storm

Glavobolje sigurnosnih stručnjaka i antivirusnih proizvođača, 2007. god. stvarao je crv *Storm*. Crv se širio slanjem poruke e-pošte koja sadrži lažirane elektroničke razglednice koje korisnika vode na zlonamjerne *web* stranice. Crv na zaraženim računalima onemogućuje rad antivirusnih i sigurnosnih alata te se povezuje na P2P (*eng. Peer-to-peer*) mrežu napadača. Zlonamjerni korisnici su prilikom projektiranja crva vodili računa kako što više otežati sigurnosnim stručnjacima analizu koda. Tako *Storm* može prepoznati izvodi li se na virtualnom računalu. Naime, sigurnosni stručnjaci često koriste virtualne strojeve kako bi sigurno izvodili i analizirali zlonamjerni kod. Ukoliko *Storm* prepozna izvođenje na virtualnom stroju, prekinut će sve svoje zlonamjerne aktivnosti i ponovno pokrenuti operacijski sustav.

4. Conficker

Računalni crv *Conficker*, također poznat kao *Downup, Downadup* ili *Kido* napada operacijski sustav Windows. Prvi put je otkriven u studenom 2008. godine. Širi se iskorištavanjem sigurnosnih ranjivosti, putem zaraženih prijenosnih medija te razbijanjem slabih lozinki. Smatra se kako je primarna zadaća crva *Confickera* u ovom trenutku stvaranje mreže kompromitiranih računala kojima upravlja jedan ili skupina zlonamjernih korisnika (*eng. botnet*), odnosno da se inficira što veći broj računala koja će kasnije omogućiti kontrolirano provođenje složenijih i vjerojatno destruktivnijih napada. *Conficker* je jedan od tehnički najsloženijih do sad napisanih računalnih crva koji koristi napredne tehnike zlouporabe ugroženih računala. Do danas je otkriveno nekoliko inačica ovog crva pri čemu starije inačice posjeduju mogućnost aktualizacije i nadogradnje. *Conficker* se trenutno smatra najraširenijom prijetnjom kojom je zaraženo više od 5 milijuna računala.

4.1. Nastanak imena

Iako postoje brojna nagađanja o nastanku imena *Conficker*, Microsoftov analitičar Joshua Phillips smatra kako je naziv nastao zbog povezanosti prve inačice crva s domenom *trafficconverter.biz*. Uzimanjem pojedinih slogova iz naziva te domene dobiva se naziv računalnog crva na sljedeći način.

Trafficconverter.biz = Traf+FIC + CON+Vert+ER = Con+Fic+"K"+Er = CONFICKER

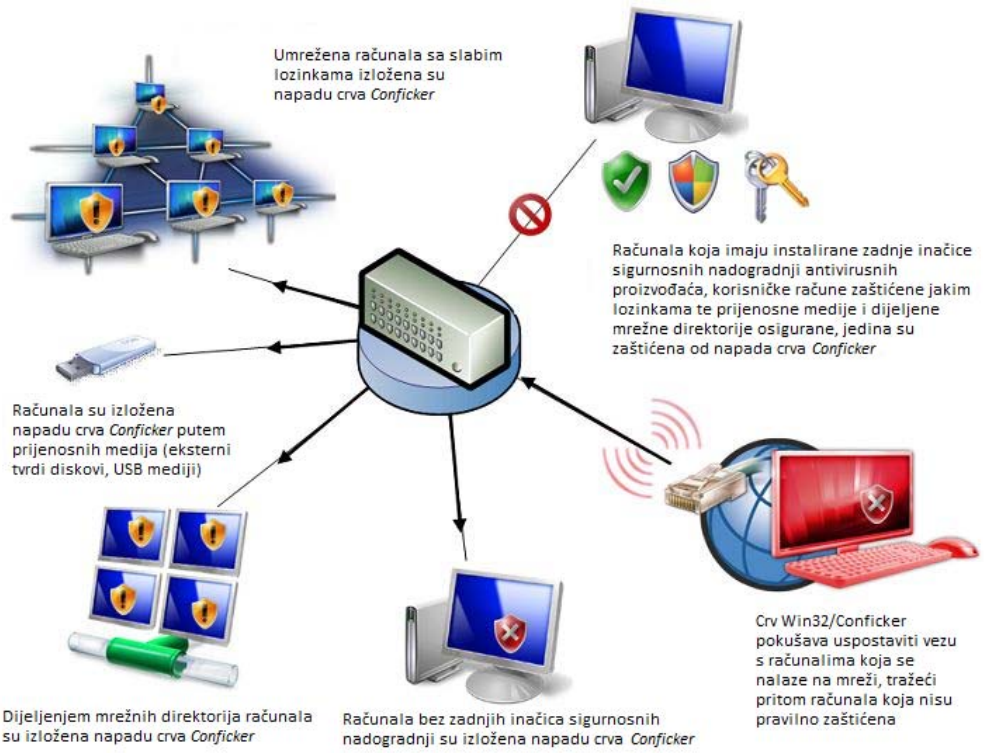
4.2. Kronološki popis inačica

4.2.1. Conficker.A

Prva inačica crva, *Conficker.A* otkrivena je 21. studenog 2008. godine kada su sigurnosni stručnjaci primijetili računalnog crva koji iskorištava kritičnu ranjivost u Server servisu (SVCHOST.EXE). Navedena ranjivost može omogućiti udaljeno izvođenje koda ako ranjivi sustav primi posebno oblikovani RPC (*eng. Remote Procedure Call*) zahtjev. Taj zahtjev omogućava napadaču pokretanje proizvoljnog koda bez autentikacije na sustavima Microsoft Windows 2000, Windows XP te Windows Server 2003. Iako je Microsoft za navedenu ranjivost objavio zakrpu (MS08-067) već 23. listopada 2008. godine, procjenjuje se kako više od 30% korisnika ne instalira redovito objavljene zakrpe. Upravo računala tih korisnika ostala su nezaštićena i izložena napadu *Confickera*. Prva inačica, *Conficker.A,* ima sposobnost povezivanja na domene te preuzimanja i pokretanja datoteka s tih domena. Prije pristupanja domenama, crv provjerava datum postavljena na zaraženom računalu. Između 1. i 25. studenog crv se trebao povezati na domenu *trafficconverter.biz* s koje bi preuzeo datoteku *loadadv.exe*. No kako je ta poveznica prije navedenog datuma otkrivena, domena je zatvorena te se preuzimanje datoteke nije nikad dogodilo. Nakon 25. studenog crv je programiran da se dnevno povezuje i preuzima sadržaje s 250 naoko nasumično stvorenih domena koje služe za nadogradnju i aktualizaciju. Preuzete datoteke su kriptirane, ali i zaštićene ključem koji posjeduju najvjerojatnije samo autori ovog crva. Preuzete datoteke mogu sadržavati daljnje naredbe autora kao i zlonamjerne programe (trojanske konje).

4.2.2. Conficker.B

Nova inačica, *Conficker.B*, pojavila se 29. prosinca 2008. godine. Riječ je o unaprijeđenoj inačici crva u koju su dodane višestruke funkcionalnosti koje su omogućile znatno učinkovitije širenje crva u odnosu na prvu inačicu. U svega nekoliko dana *Conficker.B* je inficirao milijune računala diljem svijeta. Crv koristi čitav niz vektora infekcije uključujući korištenje sigurnosne ranjivosti (MS08-067) u servisu Server, zaražene prijenosne USB medije te dijeljene mrežne direktorije pa sve do širenja kroz korisničke račune sa slabim zaporkama u Windows domenama. Slika 4. prikazuje načine širenja crva *Conficker*.



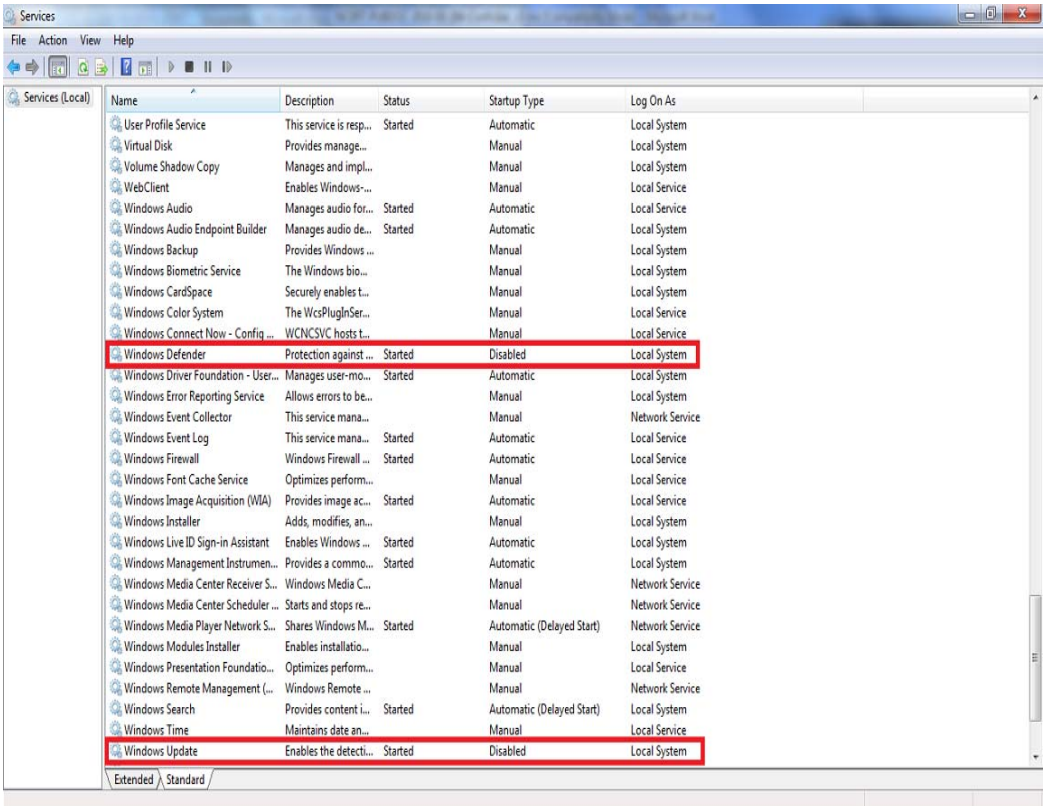
Slika 4. Prikazuje načine širenja crva Conficker
Izvor: Google

Crv isključuje sigurnosne sustave, blokira pristup URL stranicama koje su povezane sa sigurnošću te na inficiranim računalima stvara sigurnosne rupe koje je moguće kasnije iskoristiti za napade. Naime, nakon kompromitiranja sustava, zlonamjerni korisnici često ostavljaju stražnji ulaz (*eng. Backdoor*), koji će im omogućiti kasniji pristup sustavu. Čak i ukoliko se ukloni sigurnosni propust pomoću kojeg je izvorno ostvaren pristup sustavu.

Za razliku od prve inačice *Conficker.A*, inačica *Conficker.B* posjeduje dva mehanizma obrane:

1) Crv *Conficker.B* isključuje ključne servise za zaštitu računala te onemogućuje njihovo automatsko učitavanje prilikom pokretanja računala. Stanje servisa moguće je ustvrditi pomoću programa *Services* koji se nalazi u kontrolnom panelu (*Windows -> Control Panel -> System and Maintenance -> Administrative Tools -> Services)*. Ukoliko je računalo inficirano, sljedeći servisi biti će onemogućeni, odnosno postavljeni u stanje *Disabled*:
   - **Automatic Updates** (Vista – Windows Update) – servis zadužen za automatsko dohvaćanje i instalaciju zakrpi za operacijski sustav Windows i druge Microsoftove proizvode.
   - **Background Intelligent Transfer Service** (BITS) – servis zadužen za 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 antivirusni program instaliran, pokrenut, redovito osvježavan, stanje vatrozida te postavke za automatsko dohvaćanje zakrpi).
   - **Windows Defender** – Microsoftov alat za uklanjanje zlonamjernih programa koji dolazi s Windows operacijskim sustavima.

Slika 5. prikazuje stanje servisa na inficiranom računalu.



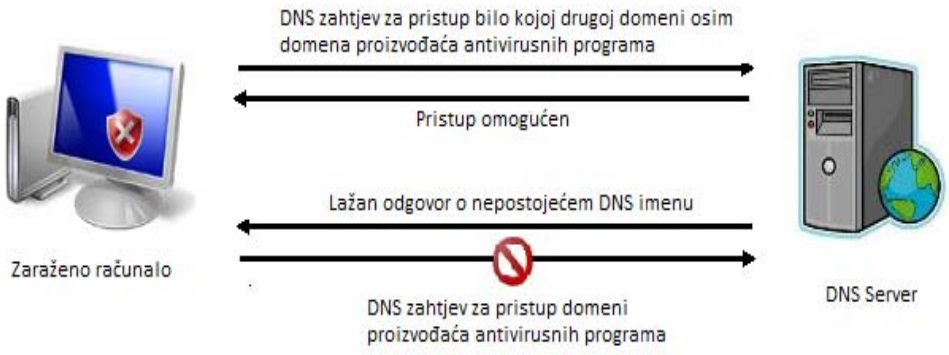
Slika 5. Prikazuje stanje servisa na inficiranom računalu

2) Na inficiranom računalu crv blokira pristup *web* stranicama proizvođača antivirusnih programa. Pristup URL adresama koje sadrže jednu od sljedećih riječi bit će onemogućen. Slika 6. prikazuje riječi koje URL adresa ne smije sadržavati.

```
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
```

Slika 6. Riječi koje URL adresa ne smije sadržavati
Izvor: Net Technology

Crv onemogućava pristup navedenim *web* stranicama tehnikom presretanja DNS (*eng. Domain Name System*) zahtjeva koji sadrže informacije vezane uz povezanost IP adresa sa stvarnim imenima domena. Ukoliko se pošalje zahtjev za pristup nekoj od domena proizvođača antivirusnih programa, vraća se lažni odgovor o nepostojećem DNS imenu. Na taj način se korisnicima onemogućuje aktualizacija svojih antivirusnih programa. Slika 7. prikazuje tehniku presretanja DNS zahtjeva kojom crv onemogućuje pristup određenim *web* stranicama.



Slika 7. Tehnika presretanja DNS zahtjeva

4.2.3. Conficker.C

Conficker.C je inačica koja je otkrivena 20. veljače 2009. godine. U odnosu na prethodne razlikuje se samo u sposobnosti stvaranja imenovanog cjevovoda (*eng. Named Pipe*). Imenovani cjevovod, posebna datoteka u datotečnom sustavu, predstavlja komunikacijski kanal između dva procesa. Način prijenosa je jednosmjeran, odnosno jedan kraj šalje podatke koji drugi kraj prima. *Conficker* preuzima datoteke s domena na koje se povezuje te primljene datoteke provjerava tražeći u njima poseban isječak koda. Samo datoteke koje imaju traženi isječak koda će se pokrenuti. S tim URL adresama, *Conficker* će stvoriti imenovani cjevovod koji mu omogućuje neprestano preuzimanje podataka s navedene adrese. S obzirom na tako malu razliku u odnosu na prethodne, mišljenja stručnjaka se jako razilaze u tome treba li se ovu inačicu smatrati novom ili samo nadogradnjom na prethodnu. Pa tako uz ime *Conficker.C* vrlo često nalazimo i naziv *Conficker.B++*. Danas je jako teško imenovati i jasno kategorizirati zlonamjerne programe jer svaki proizvođač antivirusnih programa, sam imenuje programe kako ih otkriva. Najčešće se dogodi da više proizvođača otkrije isti zlonamjerni program u isto vrijeme pa tako nastane više imena za jedan program. Isto tako pojedini proizvođači promjenu svakog binarnog koda vide kao novu inačicu (što rezultira s više od 30 različitih inačica pojedinog crva) dok drugi ne prave nikakvu razliku te imaju jedno ime za sve inačice.

4.2.4. Conficker.D

Inačica *Conficker.D* se pojavila 4. ožujka 2009. Za razliku od prethodnih, ova inačica se ne širi putem USB prijenosnih medija ili dijeljenih mrežnih diskova. Umjesto da nastave s pokušajima daljnjeg širenja crva, cilj autora je postao otežavanje uklanjanja crva sa zaraženih računala. Inačica *Conficker.D* se nadograđuje na zaraženim računalima s inačice *Conficker.C* kako bi još više otežali praćenje domena s kojih crv preuzima datoteke. Ova inačica dnevno stvori 50 000 naoko nasumično odabranih domena. Također, novost je i razmjena datoteka između zaraženih računala P2P (*eng. Peer-to-Peer*) mrežom koja omogućuje slobodnu razmjenu podataka i informacija između umreženih računala bez potrebe za poslužiteljima *(eng. Server*) ili domaćinima (*eng. Host*). Uz ovu inačicu vežu se dva nova mehanizma obrane:

- Napredniji mehanizam blokiranja DNS zahtjeva s domenama antivirusnih proizvođača izmjenom funkcija iz *„dnsapi.dll“* biblioteke. Crv mijenja funkcije *DnsQuery_A* (zadužena za ASCII znakove), *DnsQuery_W* (Unicode znakovi*), DnsQuery_UTF8* (UTF8 znakovi) te *DnsQuery_Main* koje se nalaze u biblioteci „dnsapi.dll“ kako bi što učinkovitije mogao filtrirati DNS zahtjeve.
- Sprječavanjem rada računala u *Safe mode* načinu rada, crv si osigurava pokretanje prilikom svakog paljenja sustava. Naime Windowsi pokrenuti u *Safe mode* načinu rada koriste samo osnovne dijelove operacijskog sustava, neophodne za njegovo funkcioniranje.

4.2.5. Conficker.E

Zadnja poznata inačica, *Conficker.E* pojavila se 7. travnja 2009. godine. Širenje ove inačice je ograničeno samo na iskorištavanje ranjivosti u Windows Server servisu. Inačice *Conficker.C* i *Conficker.D* se na zaraženim računalima nadograđuju na inačicu *Conficker.E*. Kao i prethodna inačica, *Conficker.E* je orijentiran na onemogućavanje alata antivirusnih proizvođača pri čemu traži i zaustavlja sve procese koji nose imena antivirusnih proizvođača. Između zaraženih računala datoteke se prenose P2P mrežom. Na zaraženim računalima crv instalira zlonamjerni program nazvan *Waladec* koji šalje neželjenu poštu (*eng. Spam*) bez znanja korisnika te lažni antivirusni program *SpyProtect 2009*. *Conficker.E* se automatski deaktivirao 3. svibnja 2009. godine.

Tablica 1. prikazuje kronološki popis svih inačica te kratki opis noviteta koji su se pojavili u pojedinoj inačici.

Inačica	Vektori infekcije	Mogućnosti aktualizacije	Mehanizmi obrane	Prestanak djelovanja
Conficker.A 21.11.2008.	- Ranjivost u Server servisu (MS08-067)	- Povezuje se s domenom trafficconverter.biz - Dnevno se povezuje te preuzima sadržaje s 250 naoko nasumično stvorenih domena	- Nema	- Nakon nadogradnje na inačicu Conficker.B/C/D
Conficker.B 29.12.2008.	- Ranjivost u Server servisu (MS08-067) - USB mediji - Dijeljeni mrežni direktoriji - Korisnički računi sa slabim lozinkama	- Dnevno se povezuje te preuzima sadržaje s 250 naoko nasumično stvorenih domena - Popravlja sigurnosni propust (MS08-067) ostavljajući sigurnosne rupe (*eng. Backdoor*) za moguće napade	- Blokira DNS upite - Isključuje Automatsku nadogradnju	- Nakon nadogradnje na inačicu Conficker.C ili Conficker.D
Conficker.C 20.2.2009.	- Ranjivost u Server servisu (MS08-067) - USB mediji - Dijeljeni mrežni direktoriji - Korisnički računi sa slabim lozinkama	- Dnevno se povezuje te preuzima sadržaje s 250 naoko nasumično stvorenih domena - Popravlja sigurnosni propust (MS08-067) ostavljajući sigurnosne rupe (*eng. Backdoor*) za moguće napade - Stvaranje imenovanih cjevovoda (*eng. Named Pipe*) za preuzimanje datoteka s točno određenih stranica	- Blokira DNS upite - Isključuje Automatsku nadogradnju	- Nakon nadogradnje na inačicu Conficker.D
Conficker.D 4.3.2009.	- Nema	- Dnevno se povezuje te preuzima sadržaje s 50 000 naoko nasumično stvorenih domena - Između zaraženih računala datoteke se prenose P2P mrežom	- Blokira DNS upite izmjenom funkcija iz dnsapi.dll biblioteke - Omogućuje rad računala u Safe mode načinu rada	- Nakon nadogradnje na inačicu Conficker.E
Conficker.E 7.4.2009.	- Ranjivost u Server servisu (MS08-067)	- Popravlja sigurnosni propust (MS08-067) ostavljajući sigurnosne rupe (*eng. Backdoor*) za moguće napade - Između zaraženih računala datoteke se prenose P2P mrežom	- Blokira DNS upite - Isključuje Automatsku nadogradnju - Zaustavlja procese antivirusnih proizvođača	- Preuzima i instalira zlonamjerni program Waledac te lažni antivirusni program SpyProtect 2009.

4.3. Opis crva Conficker

Računalni crv *Conficker* širi se putem Interneta te inficira računala korištenjem ranjivosti u Windows Server servisu. U izvornom obliku *Conficker* je na datotečnom sustavu pohranjen kao dinamička DLL (*eng. Dynamically Linked Library)* biblioteka. Većina inačica ovog crva upakirana je UPX (*eng. Ultimate Packer for eXecutables*) tehnikom koja služi za komprimiranje i dekomprimiranje izvršnih datoteka kako bi se otežala izravna analiza programskog koda. Nakon inficiranja računala crv pretražuje aktivne procese tražeći programe *svchost.exe* ili *explorer.exe*. Navedene procese crv inficira. Pokretanjem procesa, crv se aktivira te stvara datoteku u koju se kopira na sljedećim mjestima:

- *%Program Files%\Movie Maker\<random filename>.dll*
- *%Program Files%\Internet Explorer\<random filename>.dll*
- *%System%\<random filename>.dll*
- *%Documents and Settings%\<username>\Application Data\<random filename>.dll*
- *%Temp%\<random filename>.dll*

Datoteka dobiva ime slučajnom kombinacijom znakova, a obično je duljine između 5-8 znakova. Korištenjem nekoliko trikova, crv si osigurava postojanost na računalu te znatno otežava antivirusnim proizvođačima njegovo otkrivanje i otklanjanje. Slijedi popis nekih trikova kojima se *Conficker* služi:

- Kako bi osigurao svoje ponovno pokretanje, crv stvara zapis u registru (*eng. Registry*) kojim dodaje biblioteku *netsvcs* servisa:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netsvcs\Parameters\“ServiceDll“ = “[Putanja do dll. datoteke]“
- Izmjena ključa dozvoljava se samo u SYSTEM korisničkom računu te se na taj način uklanja mogućnost izmjene ili uklanjanja ključa s Administratorskim ovlastima.
- Crv isključuje prikazivanje skrivenih datoteka u Windows Explorer programu postavljanjem sljedeće vrijednost u registru:

  HKEY_LOCAL_MACHINE\SOFTWARW\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL = 0
- Brisanjem sistemskih kontrolnih točaka Windows operacijskog sustava (*eng. System restore point*) onemogućava se povratak u stanje prije zaraze.
- Onemogućuje ulaz u

  HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot

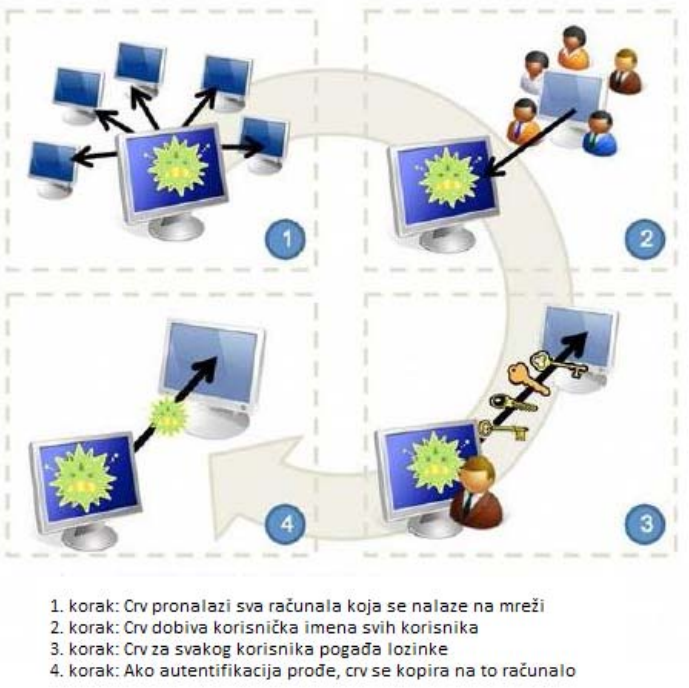
  registar kako bi spriječio rad računala u Safe mode načinu rada
- Kako bi se otežalo uklanjanje zlonamjernih datoteka s računala, crv će izmijeniti funkcije DnsQuery_A,DnsQuery_W,DnsQuery_UTF8, Query_main iz dnsapi.dll biblioteke u svrhu filtriranja DNS zahtjeva domenama antivirusnih proizvođača.

Osim iskorištavanjem ranjivosti u sustavima Microsoft Windows, *Conficker* inficira USB medije zloćudnom datotekom Autorun.inf. Umetanjem USB medija u računalo dolazi do pokretanja AutoPlay programa. Slika 8. prikazuje dijaloški prozor AutoPlay programa.

Slika 8. Dijaloški prozor AutoPlay programa
Izvor: Net Technology

Brzim pogledom na otvoreni prozor, korisnik će sigurno odabrati funkciju za otvaranje foldera kako bi vidio datoteke koje se u njemu nalaze (*eng. Open folder to view files*). No čitanjem teksta iznad te funkcije, vidljivo je da Windows zapravo ne nudi funkciju za otvaranje tog foldera, već za instaliranje i pokretanje programa s USB uređaja. Autori zlonamjernih programa iskorištavaju ovdje činjenicu da početnici te srednje iskusni korisnici neće razumjeti što se od njih traži, a da napredni korisnici samo letimično čitaju poznate stvari. Pisanjem i umetanjem vlastitih *Autorun.inf* datoteka, autori varaju korisnike koji odabirom funkcije za otvaranje foldera nisu svjesni da zapravo instaliraju i pokreću zlonamjerne programe.

Conficker se može širiti i preko djeljenih mrežnih diskova, što predstavlja veliku opasnost posebno u poduzećima. Crv se pokušava kopirati na ostala računala lokalne mreže korištenjem mrežnog diska koji se koristi za administratorske potrebe (ADMIN$). Kopiranje na mrežni disk zahtjeva autentikaciju, stoga *Conficker* prvo prebrojava sve poslužitelje na mreži korištenjem zahtjeva *NetServerEnum*, koji vraća broj svih računala vidljivih na mreži. Crv se pokušava spojiti na svako od tih računala pogađajući parove korisničkih imena i lozinki. U tom procesu koristi preko 250 uobičajenih lozinki kao što su „*password*“, „*123*“ ili „*admin*“. Neželjeni efekt pogađanja lozinki je povećan broj korisnika koji se ne mogu prijaviti na sustav zbog zaključavanja korisničkih računa nakon određenog broja neuspješnih autentikacija. No ukoliko *Conficker* uspješno obavi proces autentikacije (odnosno pogodi lozinku), kopira se sa zaraženog računala u direktorij „System 32“ udaljenog računala. Pri tome je ime datoteke slučajno stvoreno, a ekstenzija je „*dll*“. Kada se datoteka nađe na računalu, potrebno ju pokrenuti ju da bi izvršila svoju zlonamjernu ulogu. U tu svrhu *Conficker* zakazuje posao (*eng. Scheduled job)* koji će pokrenuti datoteku u sljedećem satu prema lokalnom vremenu na računalu. Na primjer, ukoliko je vrijeme inficiranja bilo 14:36, računalo će kroz zakazani posao pokrenuti datoteku u 15:00. Pokretanje datoteke izvodi se naredbom rundll32.exe jer je kopirana datoteka s *dll* ekstenzijom. Slika 9. prikazuje način širenja *Confickera* putem dijeljenih mrežnih diskova.

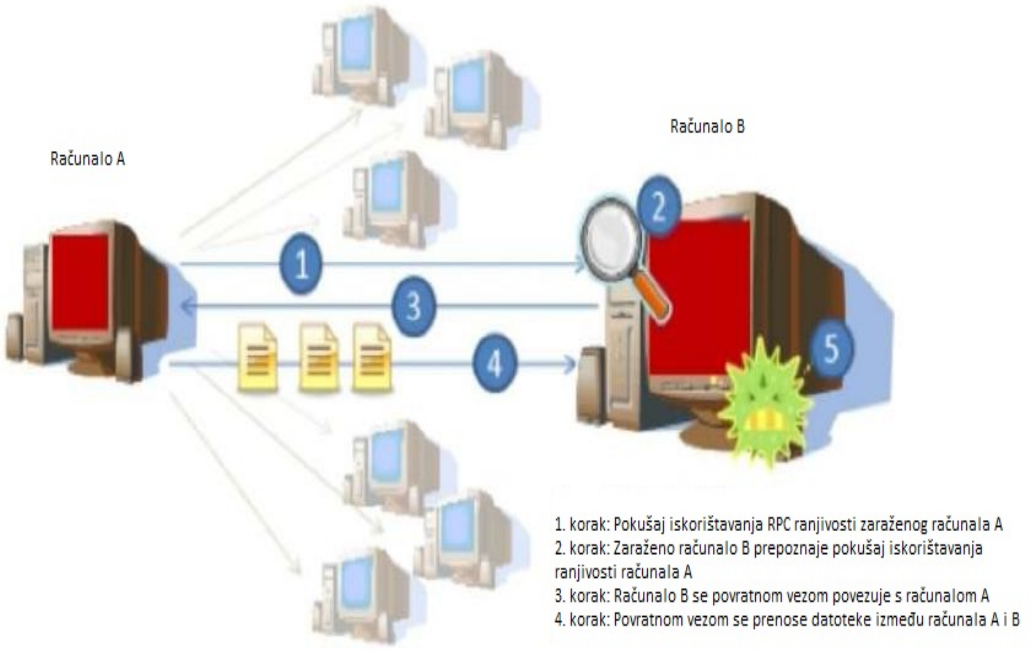


Slika 9. Prikazuje način širenja Confickera putem dijeljenih mrežnih diskova
Izvor: Net Technology

Širenje crva *Conficker* preko djeljenih mrežnih diskova predstavlja veliku opasnost posebno u poduzećima. Iako se *Conficker* 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 infekciju crvom *Conficker* moguće je primijetiti zaključavanjem velikog broja korisničkih računa. Prilikom pokušaja širenja, crv koristi *brute force* napade za pogađanje parova korisničkih imena i lozinki zbog kojih nakon 3 neuspjela pokušaja u kratkom vremenu dolazi do zaključavanja 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).

Crv ima dva mehanizma za preuzimanje tereta (*eng. Payload*).

- Dnevnim stvaranjem liste domena koje se kontaktiraju radi aktualizacije. Crv s navedenih domena preuzima datoteke koje izvodi. Iako crv preuzima sadržaje s tisuća domena, datoteke za nadogradnju zlonamjernog programa crva bit će preuzete samo s jedne od njih. To je lošiji način preuzimanja tereta, jer se te domene neprestano prate te zatvaraju ukoliko postanu kandidati za preuzimanje zlonamjernih kodova.
- P2P mreža je drugi mehanizam za distribuciju dodatnih datoteka koji je puno teže pratiti i teže zaustaviti. Crv koristi P2P (*eng. Peer-to-peer*) mrežu koja mu dozvoljava dijeljenje datoteka između zaraženih računala. Na slici 10. je prikazan navedeni mehanizam dijeljenja datoteka između zaraženih računala.



Slika 10. Mehanizam dijeljenja datoteka između zaraženih računala P2P mrežom
Izvor: Net Technology

Tijekom navedenog procesa *Conficker* ne samo da iskorištava ranjivost u RPC servisu, već može pomoću te ranjivosti prepoznati zaražena računala. Crv se sa zaraženog računala A pokuša širiti na ostala računala iskorištavanjem ranjivosti u Server servisu. Zaraženo računalo B prepoznaje pokušaj iskorištavanja te ranjivosti analiziranjem paketa koje je poslalo računalo A. Računalo B se može povratnom vezom (*eng. Back Connect*) povezati s računalom A. Za povratnu vezu se koristi HTTP protokol sa slučajno odabranim priključkom *(eng. Port)*. Na ovaj način se istovremeno može prenositi više datoteka. Sve datoteke imaju zaglavlje koje sadrži identifikator datoteke i datum. Identifikator služi kako bi crv mogao provjeriti posjeduje li već tu datoteku, a datum se koristi kako bi se slale samo najnovije datoteke. Svaka datoteka ima datum isteka i koristi se za odbacivanje zaprimljenih datoteka ukoliko je datum prošao. Primljene datoteke se kopiraju u registar te se mogu slati drugim zaraženim računalima preko P2P mreže.

4.4. Simptomi infekcije

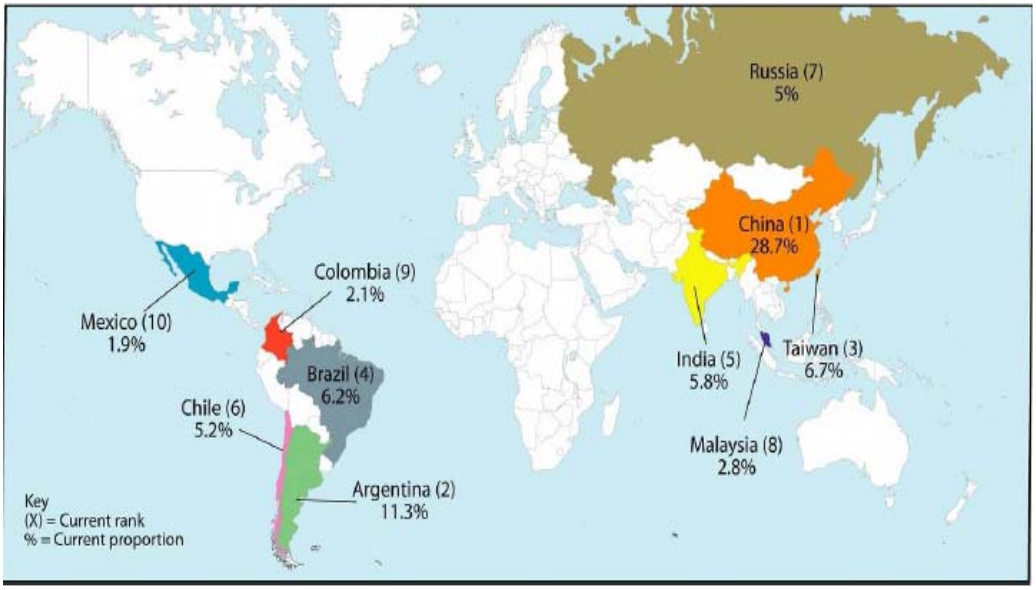
Simptomi zaraze crvom *Conficker* uključuju:

- izostanak aktivnosti Windows Security centra, servisa Windows update, Windows Defendera, Background Inteligent Transfer (BITS) te Error Reporting servisa,
- nedostupnost *web* stranica čiji je sadržaj vezan uz proizvođače antivirusnih programa Eset, Microsoft, Avast te Norton,
- spor odgovor glavnog upravljačkog servisa domene (*eng. Domain controllers*) na zahtjeve klijenata zbog filtriranja i blokiranja određenih zahtjeva,
- zagušenje lokalnih računalnih mreža LAN (*eng. Local Area Network*) i
- zaključavanje korisničkih računa.

4.5. Raširenost i materijalni gubici

Na temelju podataka kojim danas raspolažu antivirusni proizvođači te sigurnosni stručnjaci može se zaključiti kako je *Conficker* najraširenija crv u povijesti. Iako stvarni podaci ne postoje, smatra se kako je *Confickerom* do kraja siječnja 2009. godine bilo zaraženo više od 9.8 milijuna računala. Upravo taj period smatra se vrhuncem zaraze. Nakon toga pojavile su se inačice kojima autori nisu poticali daljnje širenje nego su pokušali što više otežati uklanjanje crva sa zaraženih računala. Slika 11. prikazuje grafičku ilustraciju rasprostranjenosti crva u deset zemalja koje broje najviše zaraženih računala. Slika je napravljena na temelju podataka *Symantec Intelligence Analysis Teama*, a objavljena je 19. siječnja 2009.

godine. Sa slike se vidi kako se najveći broj zaraženih računala nalazi u Kini (28%) i Argentini (11.3%), a sve ostale zemlje broje manje od 10%.

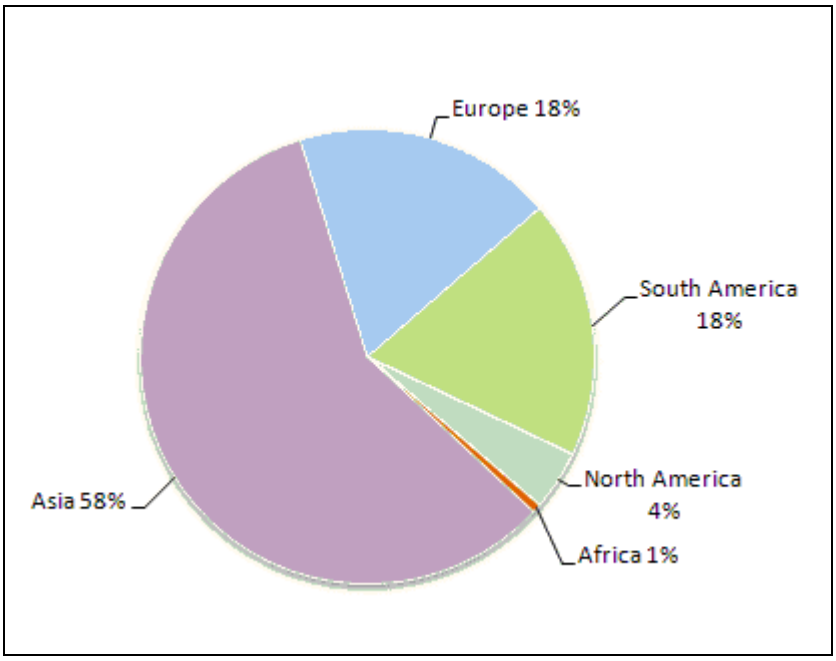


Slika 11. Grafička ilustracija rasprostranjenosti crva
Izvor: Net Technology

Prema riječima sigurnosnih stručnjaka, *Conficker* se danas nalazi u stanju mirovanja. Zadnja poznata inačica pojavila se u travnju 2009. godine, a automatski se deaktivirala mjesec dana kasnije. Na temelju podataka antivirusnih proizvođača, *Conficker* još uvijek spada u najopasnije i najčešće oblike zaraze. Procjene o broju zaraženih računala, rađene krajem 2009. godine, kreću se oko 6.5 milijuna što je još uvijek zabrinjavajuća brojka. Pozitivna stvar je što se taj broj ipak svakodnevno smanjuje.

Na udaru *Confickera*, našle su se brojne računalne mreže. U siječnju 2009. crv je zarazio računalnu mrežu Francuske mornarice *Intramar* te neke od glavnih sustava Ministarstva obrane Ujedinjenog Kraljevstva. Crv se širio putem administrativnih ureda do računala u ratnim brodovima i podmornicama te bolnicama grada Sheffild. U veljači 2009. crv je napao računala oružanih snaga Republike Njemačke. U svibnju 2009. crv se proširio Windows poslužiteljima sveučilišta Southampton i onemogućio rad računalima na kampusu, kao i pristup Internetu.

Procjenu o materijalnoj šteti koju je *Conficker* prouzročio jako je teško donijeti. Na temelju podataka koje je objavio *Cyber Secure Institute* procjenjuje se kako bi vlade, tvrtke te individualni korisnici mogli snositi troškove u iznosu od vrtoglavih 9.1 bilijuna dolara (odnosno 6.2 bilijuna eura). Materijalni troškovi se odnose na preinstalaciju računala, kupovanje boljih i skupljih antivirusnih programa, obučavanje ljudi koji rade u sigurnosnim sektorima velikih korporacija, informiranje korisnika, zapošljavanje sigurnosnih stručnjaka sposobnih za otkrivanje autora zlonamjernog programa. Slika 12. prikazuje raspodjelu troškova po kontinentima. Najveće troškove će snositi Azija (58 %), a zatim slijede sjeverna Amerika i Europa s 18%. Troškovi preostalih kontinenata su ispod 5%.



Slika 12. Prikaz raspodjele troškova po kontinentima
Izvor: Cyber Secure Institute

4.6. Conficker u medijima

Računalni crv *Conficker* digao je veliku prašinu te je shvaćen kao ozbiljna prijetnja. Pokret u njegovom zaustavljanju predvodi Microsoft, koji od 13. veljače 2009. godine nudi 250 tisuća američkih dolara onom tko pomogne u privođenju kriminalaca pravdi. Nagrada će se isplatiti za „Informaciju koja će rezultirati uhićenjem i osudom odgovornih za ilegalno lansiranje *Confickerovog* zlonamjernog koda na internetu". U istoj izjavi Microsoft je dodao kako se udružuje s Internet registrima i pružateljima DNS usluga (ICANN, ORG, NeuStar), kao i sa sigurnosnim tvrtkama (Symanteca i Arbor Networksa) u zaustavljanju ovog crva. Iako su autori ovog računalnog crva još uvijek nepoznati, postoje indikacije kako je riječ o skupini profesionalnih programera podrijetlom iz Ukrajine.

5. Zaštita od računalnih crva

Najbolja zaštita od računalnih crva je antivirusni program. Taj program može spriječiti instaliranje crva, a može i otkriti, izolirati te ukloniti crve koji su se provukli kroz obrambene mehanizme (vatrozid, Windows *Defender*). Problem antivirusnih programa je što oni štite korisnika od poznatih crva, ali ne i od novih i nepoznatih. Ostale metode zaštite su:

1. Instalacija najnovije inačice *Web* preglednika.
2. Redovita instalacija sigurnosnih zakrpi koje objavljuju proizvođači kako bi ispravili pronađene sigurnosne propuste u svojim programima.
3. Ukoliko korisnik dobije elektroničku poštu s neobičnim privitkom, datotekama imena *Iloveyou.exe ili Readme.exe,* najbolje je prije otvaranja privitka kontaktirati pošiljatelja.
4. Instalacija/konfiguracija vatrozida. Zlonamjerni korisnici česte koriste zlonamjerne programe poput virusa, crva i trojanskih konja kojima napadaju nezaštićena računala. Vatrozid je sigurnosni mehanizam kojim se provjeravaju podaci pristigli putem Interneta ili mreže, a zatim, ovisno o postavkama, odbacuju ili propuštaju do računala. Vatrozid može pomoći u obrani računala od napada zlonamjernih korisnika te povećati sigurnost računala.
5. Stalni oprez i edukacija korisnika

Danas računalni crvi spadaju u najveće prijetnje na Internetu. Na temelju podataka koje je objavila tvrtka ESET, proizvođač poznatih rješenja za borbu protiv zlonamjernih programa, Conficker zauzima prvo mjesto na tržištu zlonamjernih programa s udjelom od 8.56%. To je najbolji dokaz o još uvijek velikoj prijetnji ovog računalnog crva, i stoga je nužno znati pravilno se zaštiti od njega. Slijedi nekoliko savjeta vezanih uz zaštitu od crva Confickera:

1) 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, crv Conficker koristi ranjivost (MS08-067) u Server servisu. Prilikom instalacije sigurnosnih zakrpi posebnu pažnju treba obratiti na aplikacije čije osvježavanje nije moguće putem Windows Update servisa. Ukoliko osvježavanje nije moguće putem Windows Update servisa potrebno je samostalno provjeravati te, ako je to moguće, namjestiti sustav ili aplikaciju da nas obavijesti o novim zakrpama.
2) Instalirati i redovito osvježavati antivirusne programe. Iako antivirusni programi ne mogu u potpunosti zaštititi korisnika, oni znatno mogu podići razinu sigurnosti računala. Konkretno, u ovom slučaju antivirusni programi su bili neučinkoviti budući da niti jedan antivirusni program nije bio u mogućnosti otkriti Confickera u trenutku početka širenja. Kako su antivirusni proizvođači s vremenom dodavali definicije bilo je moguće otkriti i spriječiti inficiranje računala ovim crvom.
3) Koristiti osobne vatrozide i na taj način maksimalno ograničiti izloženost računala.
4) Potrebno je iskoristiti dostupne sigurnosne mehanizme poput definiranja potrebe za snažnim zaporkama korisnika putem *Group policy* postavki u Windows domenama.
5) Konačno, potrebno je neprestano provoditi edukaciju u svrhu podizanja sigurnosne osviještenosti.

6. Zaključak

Prema posljednjem istraživanju koje je proveo Microsoft, crvi predstavljaju najveću prijetnju računalnoj sigurnosti. Među njima je najrašireniji crv Conficker, kojim je trenutno zaraženo više od 6.8 milijuna računala. Crv se širi korištenjem sigurnosne ranjivosti u Server servisu operacijskih sustava Windows, putem zaraženih prijenosnih USB medija, dijeljenih mrežnih direktorija te kroz korisničke račune sa slabim zaporkama u Windows domenama. Postoji 5 poznatih inačica crva, od kojih se posljednja pojavila 7. travnja 2009. godine. Crv se danas nalazi u fazi mirovanja, a stručnjaci očekuju novu inačicu. S obzirom na trenutni broj zaraženih računala te još uvijek neotkriveni razlog nastajanja ovog zlonamjernog programa, postoji jako velika vjerojatnost da će se ona pojaviti.

Predviđanja za budućnost vezana u računalne crve nisu nikako svijetla. Mnogi sigurnosni stručnjaci se slažu kako će se crvi koji dolaze širiti još brže, koristiti nove vektore infekcije (vezane uz nove sigurnosne propuste), teže će ih se otkrivati, zaustavljati i otklanjati, a materijalna šteta koju će prouzročiti bit će još veća i značajnija. Računalni crv budućnosti su sigurno hibridni crvi koji kombiniraju svojstva crva, virusa i trojanskih konja. Savršen primjer hibridnog crva je Eyeveg koji se širi kao crv, ali nakon što zarazi računalo djeluje slično trojanskom konju. Crv se širi slanjem poruka elektroničke pošte s privitkom koji sadrži izvršnu datoteku. Pokretanjem izvršne datoteke dolazi do inficiranja računala. Nakon uspješnog inficiranja računala Eyeveg crv se počinje ponašati kao trojanski konj. Kontaktiranjem točno određenih URL adresa, dobiva naredbe koje odmah i izvodi. Naredbe mogu neovlaštenom korisniku omogućiti bilježenje aktivnosti na tipkovnici (*eng. Keylogging*), praćenje mrežnog prometa usmjerenog prema *web* poslužiteljima, prikupljanje korisničkih zaporki i sl. Pojava ovakvih hibrida danas je sve češća te je rezultat nastojanja tvoraca zlonamjernih kodova da svoje proizvode učine što moćnijim i prilagodljivijim.

7. Reference

[1] Tomislav Kranjec: Crvi
http://*web*.zpr.fer.hr/ergonomija/2005/kranjec/crvi.pdf

[2] Bojan Miljković, Conficker
http://www.extreme.rs/files/CONFICKER_Analiza_Pravi.pdf

[3] Net++ Technology: Downadup Codex
http://www.netpp.rs/download/downadup_codex.pdf

[4] Wikipedija: Računalni crvi
http://hr.wikipedia.org/wiki/Ra%C4%8Dunalni_crvi

[5] Microsoft: Worm:Win32/Conficker.A
http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fConficker.A, listopad 2009.

[6] Microsoft: Worm:Win32/Conficker.B
http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fConficker.B, listopad 2009.

[7] Microsoft: Worm:Win32/Conficker.C
http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fConficker.C, listopad 2009.

[8] Microsoft: Worm:Win32/Conficker.D
http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fConficker.D, listopad 2009.

[9] Microsoft: Worm:Win32/Conficker.E
http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fConficker.E, listopad 2009.