Vanja Korać
Matematički insitut SANU, Beograd,
vanja@mi.sanu.ac.rs

UDK 004.056.57
Izvorni naučni članak

PREVENCIJA ŠIRENJA VIRUSA KROZ AUTORUN FUNKCIJU OPERATIVNOG SISTEMA

U ovom tekstu govori se o širenju virusa sa sistema na usb flash uređaj i sa usb flash uređaja na sistem, korišćenjem sigurnosnog propusta tj. nebezbedne Autorun funkcije operativnog sistema Microsoft Windows XP, i načinu prevencije tog širenja. To je ujedno i najrasprostranjeniji način širenja virusa. U radu je predstavljena tehnika kojom se eliminiše ovaj vid Autorun.inf pretnje.

KLJUČNE REČI : AUTORUN.INF, AUTORUN ZAŠTITA, AUTORUN VIRUS, USB VIRUS, USB ZAŠTITA, AUTORUN ZLONAMERNI KOD

UVOD

USB prenosni drajvovi su mali i lagani prenosni uređaji za transfer i pouzdano prenošenje podataka sa jedne lokacije-radne stanice na drugu. U ovom tekstu se pod USB prenosnim drajvovima (u daljem tekstu prenosni uređaj) podrazumevaju svi oni koji postaju eksterni uređaj za sistem (nrp. USB eksterni hard diskovi, Usb flash drajvovi), osim eksternih optičikih uređaja (nrp. Cd, DVD, Blueray, HD…). S obzirom da su to i najčešće korišćeni uređaji za prenos podataka, raste i mogućnost zaraze sistema i prenosa virusa na uređaj i sa njega. Pitanje koje se postavlja je kako se može uticati na prevenciju i smanjenje rizika zaraze sistema i samih prenosnih uređaja, dok se podaci prenose između sistema i prenosnog uređaja.

S obzirom da ne postoji nijedan program koji sto posto sprečava virusne napade (jer antivirusne kompanije, nažalost, objavljuju zaštitu od određenog virusa tek kad on dostigne neku kritičnu masu), ipak možemo da utičemo na smanjenje njihovog širenja. Širenje virusa se dešava na dva načina: snimanjem fajla koji sadrži zlonamerni kod, zajedno sa virusom, čime se sistem zaražava, i ako se ubaci prenosni uređaj u virusom zaraženi računar, čime se prenosni uređaj zaražava i time utiče na dalje širenje virusa na drugim računarima.

NAČIN ŠIRENJA ZARAZE

Šta se zapravo desi kada se ubaci prenosni uređaj u računar? Ukoliko je u sistemu uključena opcija Autorun i dvoklikne se na taj prenosni uređaj (koji na sebi ima zlonamerni kod zajedno sa virusnim fajlom koga poziva), sistem će se zaraziti, tako što će automatski biti izvršen zlonamerni kod (povezan sa virusom) koji se nalazi na prenosnom uređaju, kopirajući se na lokalne drajvove

računara kreirajući skrivene fajlove koji se zovu autorun.inf (koji pozivaju neki virusne fajlove) zajedno sa još nekim fajlovima tipa .exe ili dll (virusnim fajlovima). Time se osigurava da kopija virusa bude napravljena pri otvaranju lokalnog drajva tj. nekog drajva omogućujući dalje širenje virusa. Naravno ova pretnja nema uticaj samo na lokalne drajvove nego i na ostale prenosne uređaje i deljene uređaje na mreži.[1] Problem leži u činjenici da zlonamerni kod predstavlja zapravo modifikovan autorun.inf fajl koga Windows automatski izvršava. Smisao automatskog izvršenja je u tome da se automatski pokrene instalaciona skripta, ako je u pitanju instalacioni "setup" (npr. nakon ubacivanja instalacionog diska), ali nažalost modifikacijom autorun.inf koda omogućeno je i pokretanje nekog virusa. Na ovaj način se virusi lako i brzo šire i na taj način može doći do komprimitacije svih računara na mreži, ugrožavajući informacioni sistem organizacije.

Da bi se to sprečilo potrebno je pronaći neku slabost ovog načina širenja virusa i sprečiti širenje kao i eliminisati sigurnosne pretnje. U daljem tekstu biće prikazani neki od načina prevencije i prepoznavanja ovog tipa virusa. U svakom slučaju prevencija je svakako bolja od lečenja.

PREVENTIVNI METODI ZAŠTITE

Kako bi se obezbedilo preventivno sprečavanje navedenog način širenja virusa neophodno je pratiti korake koji slede.

Prvo što se primenjuje je onemogućavanje (eng. "Disable") Autorun funkcije (kao i Autoplay) u operativnom sistemu. Ovaj postupak se izvodi izmenom parametara u "Registry bazi" čime se omogućuje najjednostavniji i najefikasniji način sigurnog isključenja autorun funkcije,[2] a to se postiže sa sledećim kodom:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\
Microsoft\Windows NT\CurrentVersion\IniFile-
Mapping\Autorun.inf]
@="@SYS:DoesNotExistAnyProblem"
```

Nick Brown je otkrio pomenuti kod koji je potrebno implementirati u Registry bazu.[3] Postupak se izvodi na sledeći način: u fajl koga nazovemo autorun_disable.reg unesemo navedeni kod. Onaj ko izvršava fajl mora biti administrator sistema. Izvršimo desnim klikom nad fajlom autorun_disable.reg i odaberemo opciju "Merge". Prilikom izvršenja fajla potrebno je odgovoriti potvrdno na pitanje da li se želi dodati nova informacija u Registry bazu. Drugi način je ubacivanje koda iz Command prompta na sledeći način:

```
C:\reg add "HKEY_LOCAL_MACHINE\
SOFTWARE\Microsoft\Windows NT\Curren-
tVersion\IniFileMapping\Autorun.inf" /ve /d @
SYS:DoesNotExistAnyProblem
```

Bilo koji od ova dva načina da smo odabrali za onemogućavanja Autorun funkcije, mora se restartovati računar. Ovim izmenama u Registry bazi postiže se cilj - a to je neprihvatanje ni jednog Autorun zahteva. Postupak onemogućavanja Autorun funkcije prikazan u ovom tekstu se odnosti na operativne sisteme Windows XP (Home i PRO verzije) kao i za Windows Vistu (sve verzije).[4] Naravno, posledica onemogućavanja Autorun funkcije je sledeća: na primer, kada se ubaci neki instalacioni disk u CD drajv ili DVD drajv, neće biti moguće automatsko pokretanje postupka instalacije, već se mora ručno kroz Windows explorer pokrenuti odgovarajući setup fajl.

Ova metoda je preporučena od strane CCIRC (Canadian Cyber Incident Response Centre), naročito za poslovna okruženja. Postoje i drugi način da se onemogući Autorun funkcija u operativnom sistemu ali jedini način koji se pokazao najefikasnijim je navedeni. Drugi načini onemogućavanja Autorun funkcije kao i njihove slabosti dati su u prilogu ovog rada.

Dodatana mera opreza sastoji se u kreiranju foldera autorun.inf na svim drajvovima na računaru, a posebno na prenosnim uređajima. Naravno, ni ovaj metod nije savršen, jer virus može da izbriše postojeći folder zamenivši ga sa zlonamernim kodom, ukoliko se to kreiranje ne izvrši na pravilan način. Time bi se takva zaštita onesposobila. Međutim kreirajući autorun.inf folder sa odgovarajućim dozvolama i pravima, dobi-

1 National Cyber Alert System 2009

2 Cert blogs, The Dangers of Windows AutoRun 2008

3 Brown 2007

4 Landesman 2008

jamo efikasniju zaštitu, istovremeno sprečavajući sposobnost virusa da obriše adekvatno zaštićen folder.

Da bi se ovaj postupak sproveo drajvovi u računaru kao i prenosni uređaji moraju biti NTFS formatirani jer se koriste specifične funkcije NTFS fajl sistema. Ukoliko uređaj poseduje fajl sistem FAT ili FAT32, preporuka je da se prvo sačuvaju ("backup") svi podaci sa prenosnog uređaja i da se zatim taj uređaj formatira kao NTFS.

Nakon te pripreme uraditi sledeće korake:

Kreirati novi folder u root direktorijuma prenosnog uređaja sa imenom "AUTORUN.INF"

Opciono: Preporuka je da se na prenosnom uređaju kreiraju još 4 foldera sa sledećim imenima: "SETUP" "RECYCLER" "RECYCLED" "RECYCLE". Razlog kreiranja ovih foldera leži u činjenici da se u zlonamernom kodu često koriste ova imena i nazivi u cilju maskiranja zlonamernog programa (virusa). Ova 4 foldera nije preporučljivo kreirati na sistemskom disku jer ih Windows OS takođe koristi u svrhu backup-a obrisanih fajlova.

Otvoriti command prompt (Start-Run-cmd) i otići u root direktorijum prenosnog uređaja.

Podesiti atribute za folder koji smo kreirali "AUTORUN.INF" sa sledećim komandama:

j:\>**attrib autorun.inf /s /d –a +s +r +h**

Sledeći korak je podešavanje privilegija nad folderom i to na osnovu sledećih komandi:

j:\>**cacls autorun.inf /c /d administrators**

Na pitanje "Are you sure (Y/N)?" odgovoriti potvrdno sa "Y"

Na kraju je potrebno istestirati folder na brisanje, izmene, kopiranje otvaranja i kreiranje foldera. Ukoliko bilo koja od ovih funkcija ne može da se izvrši, realizacija ove dodatne zaštitne mere je uspešno implementirana.

Ova tehnika praktično sprečava izvršenje zlonamernog koda prouzrokovano virusom, čime se sprečava širenje virusa putem prenosnog uređaja, koristećenjem poznavanja načina umnožavanja samog virusa. Preporuka bi bila da se folder Autorun.inf kreira i na sve lokalne drajvove u sistemu na opisani način. Time bismo sprečili i potencijalne viruse da se "umnožavaju" na druge particije (sa i na), čak i ako pridružimo sistemu neki zaraženi prenosni urađaj. Naime, na njima je kreiran folder autorun.inf, pa zlonamerni program ne može da upiše novi autorun.inf fajl (odnosi se na viruse Autorun tipa). Time smo sistem zaštitili i sprečili dalje širenje ovog tipa virusa.

Postoje i besplatni programi koji mogu da obezbede zaštitu od širenja ovakvih tipova virusa. Neki od takvih programa su besplatni kao npr. program Autorun protector (zahteva prethodnu instalaciju minimum dotnetfx 2.0) ili Usb firewall.

Usb firewall sprečava automatsko izvršenje programa koji se poziva iz autorun.inf fajla prenosnog uređaja, obaveštavajući preko iskačućeg (eng. Pop-up) prozora o potencijalnoj autorun pretnji. U programu Autorun protector-u postoji mogućnost automatskog kreiranja autorun.inf folder-a za sve postojeće drajvove na računaru kao i indikator postojanja autorun.inf fajla koji može da predstavlja zlonamerni kod. Ovi programi su odlični, jer se mogu koristiti u zaštiti drugih prenosnih uređaja koji se priključuju na računar. Na taj način sprečavamo širenje zaraze.

Njihovo podešavanje, za razliku od command-nog, je veoma jednostavno kroz GUI interfejs. Krajnji rezultat je isti kao i kod prethodno navedenog postupka.

PRETPOSTAVKA ZARAZE

Ukoliko se desi da je USB prenosni drajv ubačen u računar i posumnja se da je zaražen, u daljem tekstu sledi procedura uklanjanja pretnje-virusa i bez formatiranja prenosnog drajva. Veoma je bitno, da se brisanju autorun.inf fajla i virusnog fajla koga on poziva, pristupa iz command prompta. Takođe bitno je i napomenuti da bilo koje otvaranje Windows explorer-a, njegovo osvežavanje (Refresh), utiče na ponovno kreiranje autorun.inf fajla kao i pokretanje samog virusa. Razlog tome je što je virusni fajl sa zlonamernim kodom povezan sa mnogo instanci (events) windows explorera uključujući i npr.: OPEN, REFRESH… Potrebno je, u tom slučaju, prvo zatvoriti sve otvorene Windows explorer prozore, zatim pokrenuti skeniranje sa antivirusnim programom, pa onda manuelno eliminisati virus i sigurnosnu pretnju.

Naime, postoje dva načina eliminacije. U prvom slučaju zaražen je i sisem i prenosni uređaj. Drugi slučaj je kada sistem nije zaražen, ali se na prenosnom uređaju zlonamerni kod koji predstavlja potencijalnu pretnju.

Ukoliko je sistem zaražen učiniti sledeće:

1. Start - Run - ukucajte cmd

2. Ulogujte se na sumnjivi drajv (npr c: ili d: ili slovo koje je dobio usb prenosni uređaj)

3. Npr: c:\> dir /w /o /a /p (lista sve fajlove i foldere)

4. Ako se primeti autorun.inf fajl, u tom slučaju, potrebno je učiniti sledeće korake kada je u pitanju sistemska particija hard diska :

c:\>attrib -h -r -s –a c:\autorun.inf

C:\>del c:\autorun.inf

C:\>md c:\autorun.inf

c:\>attrib autorun.inf /s /d –a +s +r +h

c:\>**cacls autorun.inf /c /d administrators**

Postupak ponoviti za sve drajvove koje postoje na sistemu. Na taj način sprečavamo dalje širenje virusa.

Ukoliko je u pitanju zaražen USB prenosni drajv (nrp. F:\>) :

F:\>attrib -h -r -s -a *.* (briše sve atribute fajlova koji se nalaze na zaraženom prenosnom drajvu, tako da se mogu videti svi skriveni i sistemske fajlove koje je virus sakrio).

Ukoliko postoji autorun.inf fajl, njega je potrebno obrisati takođe, kao i u prethodnom postupku.

Nakon brisanja, potrebno je i kreiranje bezbednog autorun.inf foldera, čime se sprečava širenje virusa kroz sistem, na sledeći način

F:\>del c:\autorun.inf

F:\>md c:\autorun.inf

F:\>attrib autorun.inf /s /d –a +s +r +h

F:\>**cacls autorun.inf /c /d administrators**

Nakon ovog postupka potrebno je izbrisati sve virusne fajlove koji su se pozivali iz autorun.inf fajla. Oni su se uglavnom nalazili u folderima Recycle, Recycler, Restore.[5] To su fajlovi uglavnom sa .exe ili .bat ili .com ekstenzijom. Takođe, preporuka je da se sav sadržaj navedenih foldera izbriše.

Kada je virus onesposobljen brisanjem zlonamernog autorun.inf koda, ostaci virusa se mogu mogu obrisati i iz Windows explorera (“Folder Options“ u Tools meniju Windows explorera), tako što se omogući prikazivanje skrivenih i sistemskih fajlova i foldera.

ZAKLJUČAK

Ono što sledi iz svega do sada navedenog, a postavlja se kao krajnji cilj, odnosi se na primenu navedene tehnike kojom se eliminiše autorun.inf pretnja. Druge tehnike koje su prikazane u prilogu ovog rada mogu donekle da spreče izvršenje autorun.inf fajla na manje efikasniji način od predložene u radu. Efikasnost svakog rešenja se uglavom oslanja na svest kranjeg korisnika. Poslovne mreže mogu imati onemogućenu autorun funkciju , ali to ne znači da kranji korisnik ne može da klikne izvršnu datoteku koja u sebi sadrži zlonamerni kod ili virus. Preporuka je da se obezbede i preventivne mere bezbednosti kao npr. :ograničavajući prava izvršenja, redovno ažuriranje Antivirusnog programa, podešavanja Firewal-a, kao i podizanje svesti o sigurnosnim pretnjama kod samih korisnika.

PRILOG 1

Ostali postupci Disable-ovanja Autorun funkcije.[6]

BRISANJE MOUNTPOINT2 REGISTRY KLJUČA

Jedan od načina da se spreči izvršenje autorun.inf fajla je brisanje „MountPoint2“ ključa iz Registry baze. Kada računar detektuje prenosni uređaj, on pristupa njegovom skeniranju tražeći autorun.inf fajlove. Pronađene vrednosti upisuje u “MountPoint2“ ključ Registry baze. Ovaj ključ sadrži sačuvane informacije o svakom uređaju koji je ikada bio priključen na računar.

Promena dozvole nad “MountPoint2“ ključu Registry baze, ima za cilj sprečavanje izvršenja autorun.inf fajla, čak i ako računar nije video prenosni uređaj ranije. Da bi se promenile dozvole za MountPoint2 ključ Registry baze, potrebno je izvršiti sledeće korake:

1. Pokrenuti “Regedit“ (Start- Run-regedit)

2. Pronađe se: “

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2;

3. Desni klik nad ključem “MountPoints2“ i izabere se “permission“;

5 PreciseSecurity 2008

6 The Canadian Cyber Incident Response Centre 2008

4. Zatim se klikne na “Advance“ i isključi se “ Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here “;

5. Klikne se na “Remove“, pa “YES“ i na kraj u“OK“ .

Iako je ovo rešenje efikasno, CCIRC (Canadian Cyber Incident Response Centre) ga ne preporučuje zbog nedovoljno raspoloživih informacija o tome šta MountPoint2 ključ Registry baze radi i koje to druge efekte može imati na operativni system.[7] Pošto je u pitanju rad sa Registry bazom obavezna je procedura backup-ovanja Registry baze pre bilo kakve promene u njoj.

KORIŠĆENJE SHIFT KEY NA TASTATURI

Najjednostavniji način da se spreči izvršenje datoteke autorun.inf je dražanje **“**Shift**“** tastera na tastaturi, prilikom priključivanja prenosnog uređaja na sistem. Nedostatak ovog pristupa je što bi korisnici zaboravili da slede ovu proceduru svaki put prilikom priključivanja prenosnog uređaja. Ova procedura pogodna je ukoliko priključujete svoj prenosni uređaj na neki bezbedan sistem, a niste u prilici da primenite neki od pomenutih metoda zaštite.

CCIRC ne preporučuje ovo rešenje zato što se oslanja isključivo na pamćenje krajnjeg korisnika. Ne predstavlja pouzdanu meru bezbednosti, posebno u poslovnom okruženju.

LITERATURA

PreciseSecurity 2008

PreciseSecurity - *How to Enable Show Hidden Files and Folders, May 2008,* http://www.precisesecurity.com/tools-resources/troubleshooting/how-to-enable-show-hidden-files-and-folders/

Landesman 2008

Mary Landesman, How to disable autorun, December 2008, http://antivirus.about.com/od/securitytips/ht/autorun.htm

National Cyber Alert System 2009

National Cyber Alert System, *Technical Cyber Security Alert TA09-020A*, *Microsoft Windows Does Not Disable AutoRun Properly***,** *January* 20, 2009,

http://www.us-cert.gov/cas/techalerts/TA09-020A.html

Cert blogs, The Dangers of Windows AutoRun 2008

Cert blogs, The Dangers of Windows AutoRun, http://www.cert.org/blogs/vuls/2008/04/the_dangers_of_windows_autorun.html

The Canadian Cyber Incident Response Centre 2008

The Canadian Cyber Incident Response Centre, *Disabling Autorun*,

http://www.publicsafety.gc.ca/prg/em/ccirc/2008/tr08-004-eng.aspx**, Number: TR08-004, December 2008**

Brown 2007

Nick Brown, *Memory stick worms*, http://nickbrown-france.blogspot.com//2007/10/memory-stick-worms.html

PREVENTING THE SPREAD OF THE VIRUS THROUGH THE AUTORUN FEATURE OF THE OPERATING SYSTEM

This paper discusses about the of the spread of the virus from system to the usb flash drive and from usb flash drive to the system, by using the security flaws of unsafe Autorun feature of Microsoft Windows XP and how to prevent the spread. This is the most common way of spreading the virus. In this paper is also presented the technique for eliminating this kind of threat type Autorun.inf.

KEYWORDS: AUTORUN.INF, AUTORUN PROTECTION, AUTORUN VIRUS, USB VIRUS, USB PROTECTION, AUTORUN MALWARE

7 The Canadian Cyber Incident Response Centre 2008