

## Dodatna zaštita od Cryptolockera



Možda se sjećate članka na ovom portalu koji je upozoravao na zloćudni program <u>Cryptolocker</u> [1]. Ova je napast u međuvremenu je doživjela bezbroj novih inačica ("mutacija"), a predstavlja veliku opasnost za korisnike jer njegov način rada je da enkriptira sve korisničke dokumente na računalu. Za dekripciju morate u određenom vremenskom periodu uplatiti novčani iznos ili "zaboravite" na sve dokumente na kojima ste radili možda i dugi niz godina.

Velik je broj tipova datoteka koje Cryptolocker zaključava. Napomenut ću samo neke: doc, docx, cdr, crt, crw, wpd, wps, xls, xlsx, ppt, pdf, pst, raw, mdb, jpg, ods, odb itd. Popis je zaista podugačak.

Cryptolocker se prepoznaje po tome što obično u nazivu, točnije u ekstenziji, ima .pdf.exe, a najčešće dolazi putem elektroničke pošte.

Prva linija obrane je zabranja slanja i primanja Windows izvršnih datoteka (\*.exe) putem maila. Ovo je već podešeno ukoliko koristite standardni Debianov paket postfix i amavisd-new. Datoteka u kojoj je ovo podešeno je /etc/amavis/conf.d/20-debian\_defaults. Podsjetnik: nemojte u conf.d direktorijima mijenjati datoteke iz samog paketa, nego svoja podešenja stavite u datoteku 99-local (ili neki drugi naziv po kojem ćete prepoznati da je riječ o lokalnim podešenjima).

Što dalje? Osim redovitog kreiranja rezervnih kopija, udaljenog pohranjivanja dokumenata na "oblačne" usluge (primjerice Dropbox, Google Drive ili domaća usluga SRC-a <u>http://mojoblak.srce.hr</u> [2]), te redovitog ažuriranja antvirusnog programa, što možemo učiniti?

Zbog mogućnosti da mutirani Cryptolocker "pobjegne" antivirusnom programu, iskoristimo mogućnost onemogućavanja pokretanja izvršnih datoteka u mapama AppData, odnosno u Local AppData, mjesta gdje se maliciozni programi vole zavući.

Objasnit ćemo kako u nekoliko koraka blokirati izvršne programe i one koji dolaze u komprimiranom privitku (rar, zip). Procedura je identična za Windows XP, Windows 7 i 8, razlika je jedino u nazivima tj. putanjama mapa.

Zaštitu radimo sa Group Policy editorom (gpedit.msc), kojeg pokrećemo s administratorskim ovlastima. Iako je procedura identična za Windows XP, te Windows 7 i 8, postoji razlika u putanjama mapa, pa ću prikazati dvije tablice.

Za windows XP putanje koje treba postaviti su sljedeće:

```
%AppData%\*.exe (zabranjeno izvršavanje exe datoteka u mapi AppData)
%AppData%\*\*.exe (zabranjeno izvršavanje exe datotek u podmapama AppData)
%UserProfile%\LocalSettings\Temp\Rar*\*.exe (zabrana pokretanja exe datoteka u WinRa
r privitku koje se nalazi u korisnikovom okruženju)
%UserProfile%\LocalSettings\Temp\7z*\*.exe (zabrana pokretanja exe datoteka u 7-Zip p
rivitku koje se nalazi u korisnikovom okruženju)
%UserProfile%\LocalSettings\Temp\wz*\*.exe (zabrana pokretanja exe datoteka u WinZip
privitku koje se nalazi u korisnikovom okruženju)
%UserProfile%\LocalSettings\Temp\wz*\*.exe (zabrana pokretanja exe datoteka u zip p
rivitku koje se nalazi u korisnikovom okruženju)
%UserProfile%\LocalSettings\Temp\*.zip\*.exe (zabrana pokretanja exe datoteka u zip p
rivitku koje se nalazi u korisnikovom okruženju)
```



Za windows 7, 8 putanje koje treba postaviti su sljedeće:

```
%AppData%\*.exe (putanja do C:\Users\korisnik\AppData\Roaming)
%AppData%\*\*.exe
%LocalAppData%\Temp\Rar*\*.exe
%LocalAppData%\Temp\wz*\*.exe
%LocalAppData%\Temp\wz*\*.exe
%LocalAppData%\Temp\*.zip\*.exe
```

Pokrenimo Group Policy editor (gpedit.msc) kao administrator:

Programs (1)					
🗐 gpedit me	ie				
Documer	Open				
Documen	Author				
Mow 👰	Run as administrator				
gpedit.msc ×					
	ş 🔒 🖸	ß			

Odabiremo "Software Restriciton Polices" (Computer Configuration --> Windows Settings --> Security Settings --> Software Restriciton Policies)





Desnom tipkom miša kliknemo na "Software Restricion Policies" ili preko izbornika Action potvrdimo "New Software Restriction Policy"

📔 Network List N	lanager Policies		
D 📔 Public Key Pol	icies		
Software	New Software Restriction Policies		
🔈 📔 Applicati 📖	New Software Restriction Foncies		
> 🛃 IP Securi	All Tasks		
Advance			
Policy-based	View		
Administrative 1	Help		
er Configuration		🧾 Local 🤇	Group Policy Editor
		File Ac	tion View Help
		<b>(=</b>	New Software Restriction Policies
		🗐 Lo	All Tasks
		▲ 100	Help

Nakon potvrde "New Software Restriction Policy" dobijemo novo stablo za kreiranje pravila. Desnom tipkom miša potvrdit ćemo "Additional Rules" te odabrati "New Path Rule":

-----

e ....

Software Restriction Policies				
🧮 Security Levels				
🧮 Additional Rules				
Application Cor	New Certificate Rule			
IP Security Polic	New Hash Rule			
Advanced Audi	New Network Zone Rule			
Policy-based QoS	New Path Rule			
Administrative Templa				
User Configuration	All Tasks			
Software Settings				
	Refresh			
new path rule.				
	Help			

U novom prozoru, tekstualnom polju "Path" definiramo pravila (zavisno od operativnog sustava (XP, 7 ili 8), iz gornjih tablica kopirajte pravila u "Path" tekstualno polje, za svako pravilo treba ponoviti "New Path Rule")



-			· ·
	10000	Fa	It or
		EU	ILUI

1 2	
View Help	
🗊 🗐 🔍 🔜 👔	New Path Rule
aputer Policy	General
iputer Policy	
uter Configuration	
ftware Settings	Use rules to override the default security level.
ndows Settings	
Name Resolution Policy	Path:
Scripts (Startup/Shutdow	
Deployed Printers	
Security Settings	Browse
Account Policies	
Local Policies	Security level:
📋 Windows Firewall with	Disallowed
Network List Manager	
Public Key Policies	
Software Restriction P	Description:
Security Levels	
Additional Rules	
Application Control P	
IP Security Policies on	
Advanced Audit Polic	
Policy-based QoS	Learn more about software restriction policies
ministrative Templates	
onfiguration	OK Cancel
ftware Settings	

U tekstualno polje upisujemo pravilo: **%AppData%\\*.exe,** dok za "Security Level" odabiremo **Disallowed**, dok polje **Description** možete ostaviti prazno ili upisati što kreirano pravilo radi.



-			
D LLO	1.000.0	60	litt on a
			ILUI
- · -		_	

View Help	
🔲 📋 🗖 🗟 🔽	New Path Rule
anutar Deligu	General
nputer Policy	
uter Configuration	
Itware Settings	Use rules to overnde the default security level.
ndows Settings	
Name Resolution Policy	Path:
Scripts (Startup/Shutdow	%AnnData%\* exe
Deployed Printers	
Security Settings	Browse
済 Account Policies	
📴 Local Policies	Security level:
📔 Windows Firewall with	Disallowed 🗸
📔 Network List Manager	
Public Key Policies	
Software Restriction P	Description:
Security Levels	
Additional Rules	
Application Control P	
IP Security Policies on	
Advanced Audit Polic	
Policy-based QoS	Learn more about software restriction policies
ministrative Templates	
onfiguration	OK Cancel
ftware Settings	

Nakon što ste kreirali pravila zatvorite GP editor i napravimo jednostavan test: pokušajmo iz AppData pokrenuti neki izvršni program. Ako dobijemo poruku:

C:\Documents and Settings\\Application Data\test.exe Windows cannot open this program because it has been prevented by a software restriction policy. For more information, open Event Viewer or contact your system adm	inistrator.

pravila su dobro postavljena, a ako ne onda treba provjeriti da li su putanje dobro upisane u tekstualna polja.

sri, 201	5-02-11	14:03 - Z	dravko	Rašić <b>Kı</b>	harice:	<u>Windows</u> [3]
Katego	orije: <mark>O</mark>	peracijski	<u>sustavi</u>	[4]		
Vote:	0					



No votes yet

Source URL: https://sysportal.carnet.hr./node/1510

## Links

- [1] https://sysportal.carnet.hr./node/1415
- [2] http://mojoblak.srce.hr/
- [3] https://sysportal.carnet.hr./taxonomy/term/18
- [4] https://sysportal.carnet.hr./taxonomy/term/26