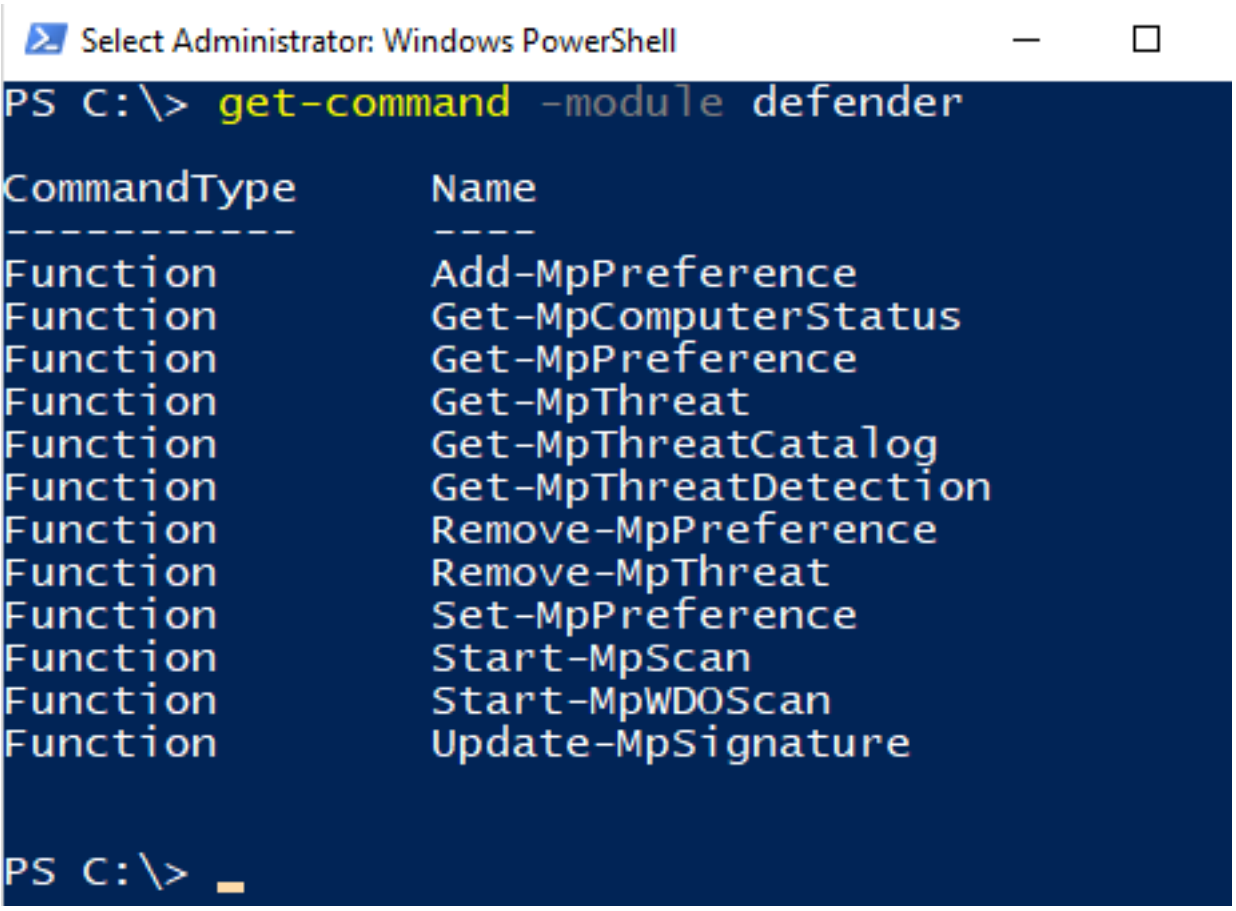
Udaljeno upravljanje Windows Defenderom

Kontinuiranim razvijanjem Windows Defendera kao univerzalnog anti-malware rješenja za novije desktop i serverske Windows OS-ove, Microsoft je uspio to svoje „ružno pače“ pretvoriti u... pa ne baš labuda, ali svakako u respektabilan namjenski softver. Stavovi upućenih u antivirusni softver uglavnom su pozitivni, ili barem nisu tako ubitačno negativni kao ranije. :o)

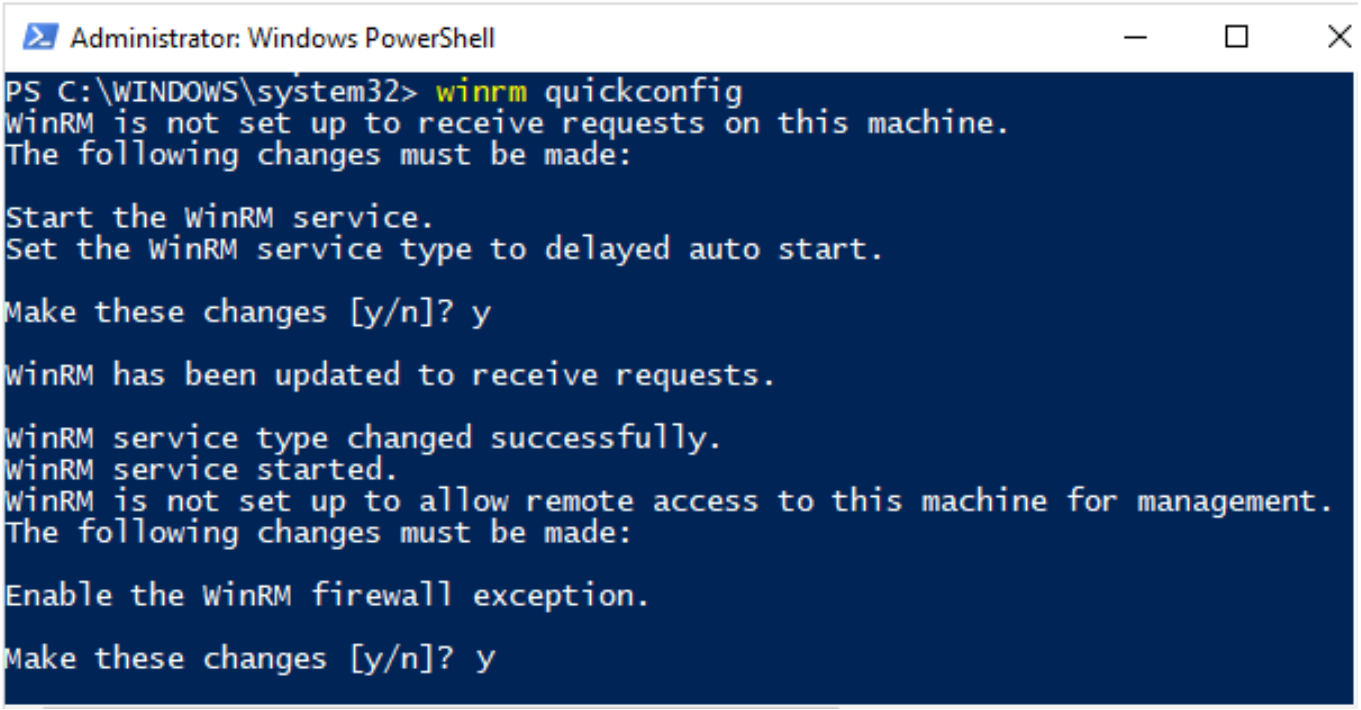
Ono što se u raznim osvrtima na Windows Defender prečesto prešućuje, a vrijedi znati, jest da nas je Microsoft odlično opremio za udaljeno upravljanje WDefenderom. Već lokalnu instalaciju tog zaštitnog softvera možemo administrirati GUI aplikacijom Windows Defender (msascui.exe), CMD naredbom mpcmdrun.exe i PowerShell modulom Defender. Za udaljeno administriranje, što nam je kao IT profićima puno zanimljivije, raspolažemo PowerShellom, domenskim grupnim politikama (Group Policies) te s komercijalnim Microsoft System Center Configuration Manager,. Spomenimo još i WSUS jer se putem njega mogu distribuirati nadogradnje i antivirusne definicije pa nije potrebno opterećivati internet link.

Microsoft System Center Configuration Manager je najbolje rješenje za centralizirano upravljanje WDefender instancama ali se mora kupiti, stoga ćemo ga ovom prilikom elegantno zaobići. Što se tiče PowerShella, integralnog dijela Windowsa, niža slika pokazuje naredbe modula Defender. Sve su one opremljene parametrom –cimsession, što je jasan znak da se mogu iskoristiti za upravljenje WDefenderom preko mreže.



Lokalni help je opširan, stoga se sa svakom naredbom modula Defender možemo zbližiti naredbom općeg oblika get-help PSnaredba –full.

Ako su nam Windows računala u domeni, što je zamalo pa neizbježno zbog raznih benefita koje takva implementacija donosi, PowerShell je vrlo lako rabiti za obrađivanje više računala odjednom. Podsjetnik: ukoliko neko računalo nije podešeno za prihvat udaljenih PowerShell konekcija, odradimo na tom računalo kako je prikazano nižom slikom i sve će biti OK. Veći broj računala podesit ćemo grupnom politikom, postoje na Webu brojni članci koji to opisuju.



Naredbom što slijedi sabiramo informacije o WDefenderu s nekoliko računala i zapisujemo ih na disk admin stanice:

```
get-mpcomputerstatus –cimsession stanica1,stanica2,stanica3,server1 > defstatus.log
```

Kako to već biva, izvještaj možemo otvoriti kao cjelinu pa gubiti vid tragajući za ciljnim podacima, a možemo se poslužiti i naredbom poput niže. Ispisati će stanje (ažurnost) signatura na svakom pojedinačnom računalu.

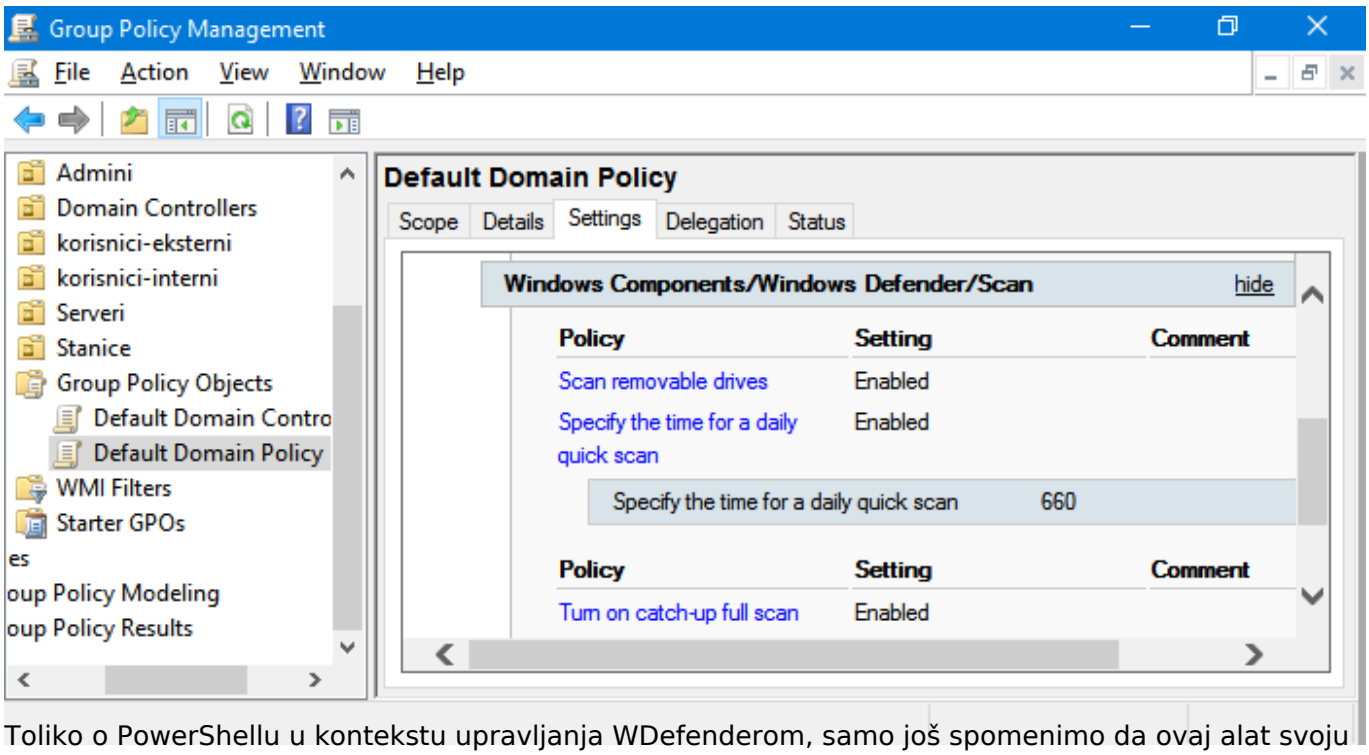
```
select-string –path defstatus.log –pattern pscomputername,signature
```

Povremeno ćemo htjeti pogledati je li WDefender otkrio kakvu prijetnju:

```
get-mpthreatdetection –cimsession stanica1,stanica2,stanica3,server1
```

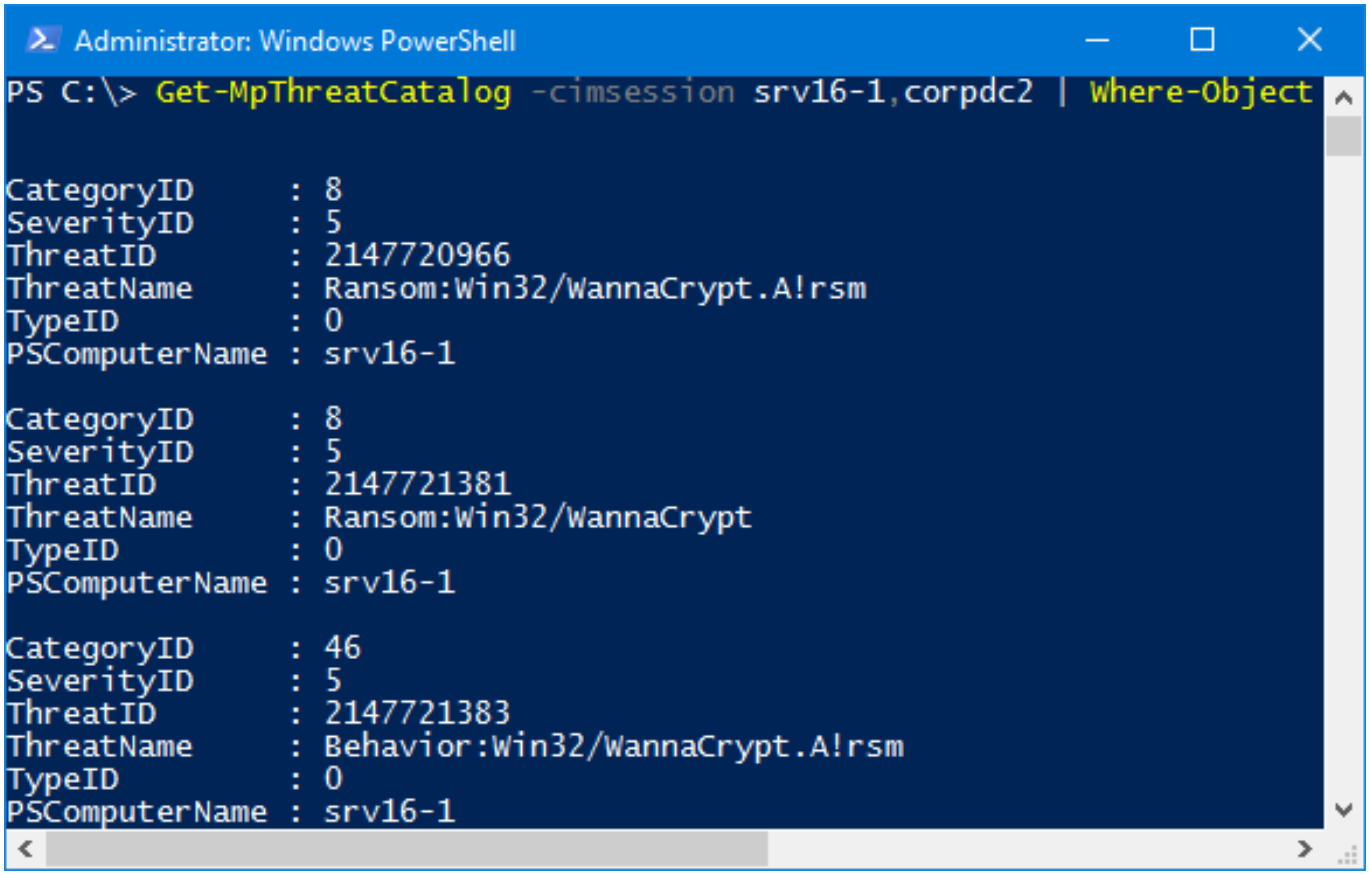
Zanima nas je li WDefender na serverima već povukao definiciju za najnoviji malware, recimo da je to WannaCry kojemu je Microsoft u svojim artikima dodijelio slično ime ali, jao, ne možemo se prisjetiti koje (službeni MS-ov naziv za predmetni ransomware je Win32\WannaCrypt)... evo kako ćemo zaviriti u baze WDefendera na serverima:

```
Get-MpThreatCatalog –cimsession server1,server2 | Where-
Object {$_.threatname -like "*wannac*"} | more
```



Toliko o PowerShellu u kontekstu upravljanja WDefenderom, samo još spomenimo da ovaj alat svoju pravu snagu pokazuje u skriptnom načinu rada. S nekoliko kvalitetno napisanih skripti možemo djelovati na grupe ili sva Windows računala odjednom u vrlo kratkim vremenskim intervalima.

Glede domenskih grupnih politika, još jednog vrijednog alata svakog sistemca zaduženog za Windows računala, brojne opcije za konfiguriranje WDefendera nalaze se pod Computer Configuration > Administrative Templates > Windows Components. Niža slika pokazuje neke postavke koje kroz Default Domain Policy namećemo svim Windows računalima domene.



Na kraju ovog kratkog pregleda i jedno osobno iskustvo: vašem je autoru već godinama upravo

Windows Defender glavni A/V softver na privatnim Windows instalacijama, s besplatnom off-line inačicom Malwarebytes kao „inspektorom inspektora“. Webom skitaram lokalno ulogiran kao običan korisnik, primjenjujem uobičajene mjere zaštite računala... i nemam nikakvih problema. Kad bih administrirao IT pogon s manjim brojem Windows desktop i serverskih instalacija (radim u firmi s tisućama Windows računala), svakako bih pokušao upogoniti besplatni Windows Defender, jasno, uz prethodni dogovor s nadređenima te uz primjenu uobičajenih filtriranja i kontrola na aktivnoj mrežnoj opremi.

Odlučite li dati šansu WDefenderu, ovaj web resurs puno će vam pomoći: https://docs.microsoft.com/en-us/windows/threat-protection/windows-defender-antivirus/windows-defender-antivirus-in-windows-10 [1].

sri, 2017-09-20 15:00 - Ratko Žižek**Kuharice:** Windows [2]
Kategorije: Operacijski sustavi [3]
Vote: 0

No votes yet

story_tag: windows defender [4]
udaljeno upravljanje [5]
remote management [6]

Source URL: https://sysportal.carnet.hr/node/1761

Links
[1] https://docs.microsoft.com/en-us/windows/threat-protection/windows-defender-antivirus/windows-defender-antivirus-in-windows-10
[2] https://sysportal.carnet.hr/taxonomy/term/18
[3] https://sysportal.carnet.hr/taxonomy/term/26
[4] https://sysportal.carnet.hr/taxonomy/term/139
[5] https://sysportal.carnet.hr/taxonomy/term/140
[6] https://sysportal.carnet.hr/taxonomy/term/141