

# Powershell'in Karanlık Yüzü

Sistemlere Sızma, Bırakılan İzler, Phant0m

# whoami

- **Halil DALABASMAZ**
- Sr. Penetration Tester & Instructor @ BGA Security
- C|EH, OSCP, OSWP, OSCE
- **artofpwn.com**
- Twitter @hlldz
- LinkedIn @hlldz
- Exploit-DB @Halil DALABASMAZ



# >\_ Powershell

- Microsoft tarafından Windows komut satırı cmd.exe ve Windows Script Host'a alternatif olarak geliştirilen yeni nesil bir komut satırı uygulamasıdır.



# >\_ Powershell

## TeslaPSModule

---

Control your Tesla vehicle from PowerShell. Watch the demo at <https://channel9.msdn.com/Events/PowerShell-Team/PowerShell-10-Year-Anniversary/PowerShell-For-My-Tesla!>

## Tesla PowerShell Module

---

This module will enable you to call Tesla commands (like those from <http://mytesla.com> and your phone app) in a PowerShell script, and automate them in Scheduled Tasks etc. just like Windows services.

- Start your climate control automatically
- Log your physical location over time
- Use your imagination!

# >\_ Karanlık Taraf

Talos team spotted a PowerShell malware that uses DNS queries to contact the C2

March 3, 2017 By [Pierluigi Paganini](#)

December 12, 2016 by [LIFARS](#)

## Microsoft's PowerShell is Being Abused by Malware Authors

Microsoft Powershell, the software giant's prominent scripting language that is now the default shell in the ever-popular Windows operating system is being used by cybercriminals to spread malware, security researchers have revealed.

## The Dark Power of Windows PowerShell

By: [Roberto Sponchioni](#)  SYMANTEC EMPLOYEE

Created 07 Apr 2014 |  0 Comments |  : [日本語](#)

Windows PowerShell, the Microsoft scripting language, has made the headlines recently due to malware authors leveraging it for malicious purposes. Symantec has identified more [PowerShell scripts](#) being used

## PowerShell threats surge: 95.4 percent of analyzed scripts were malicious

Symantec analyzed 111 threat families that use PowerShell, finding that they leverage the framework to download payloads and traverse through networks.

By: [Candid Wueest](#)  SYMANTEC EMPLOYEE  ACCREDITED

Created 08 Dec 2016 |  0 Comments |  : [简体中文](#), [日本語](#)

# >\_ Neden

- Signed, Legal
- Varsayılan Olarak Yüklü
- Şifreli Trafik İle Uzaktan Erişim İmkânı
- Anti-Forensic Friendly
- Anti-Application Whitelisting Friendly
- Script-Based Malware Bağışıklığı
- Obfuscation Kolaylığı

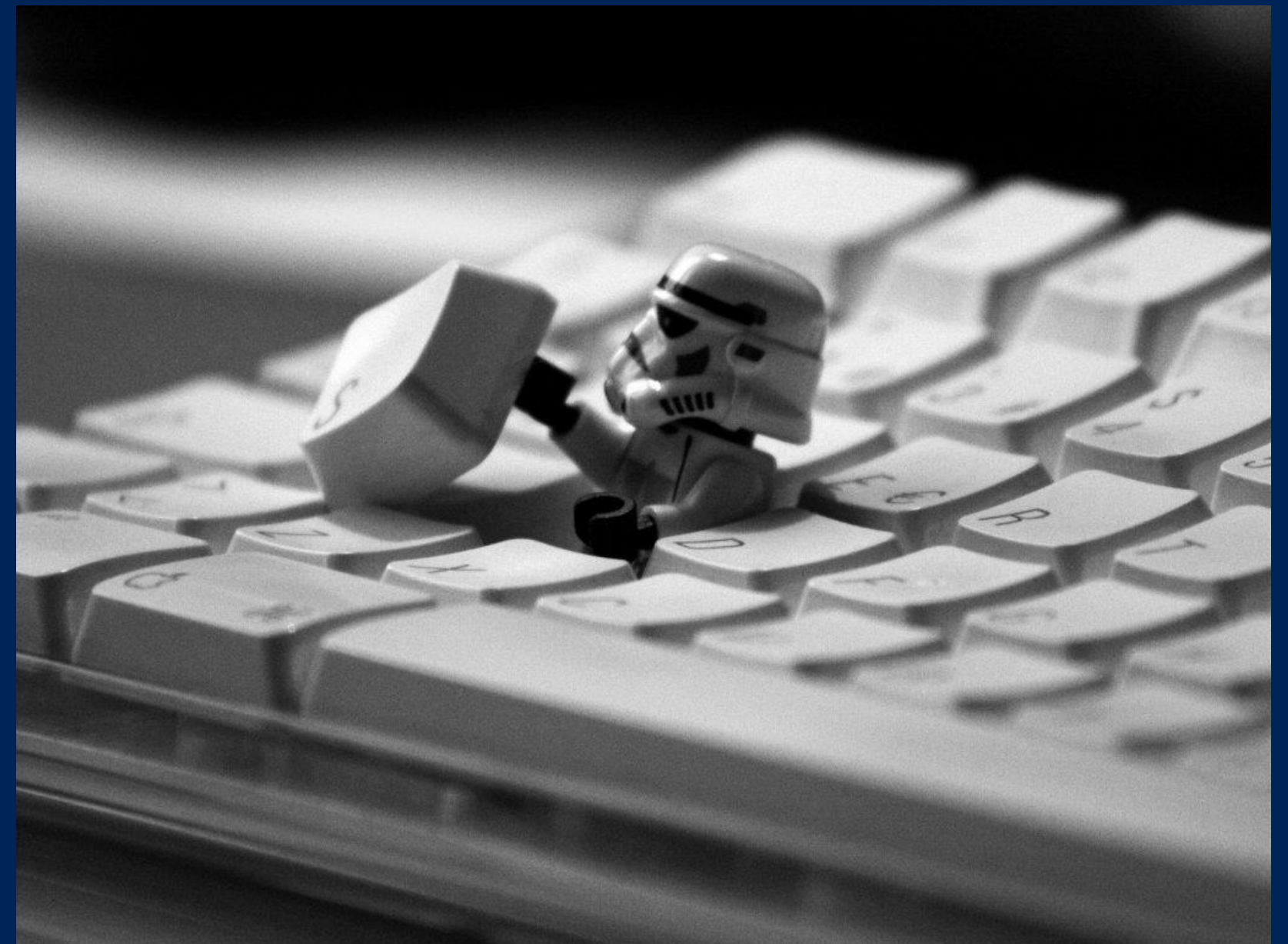


# >\_ Execution Policy

- Restricted
- RemoteSigned
- AllSigned
- Unrestricted
- Bypass

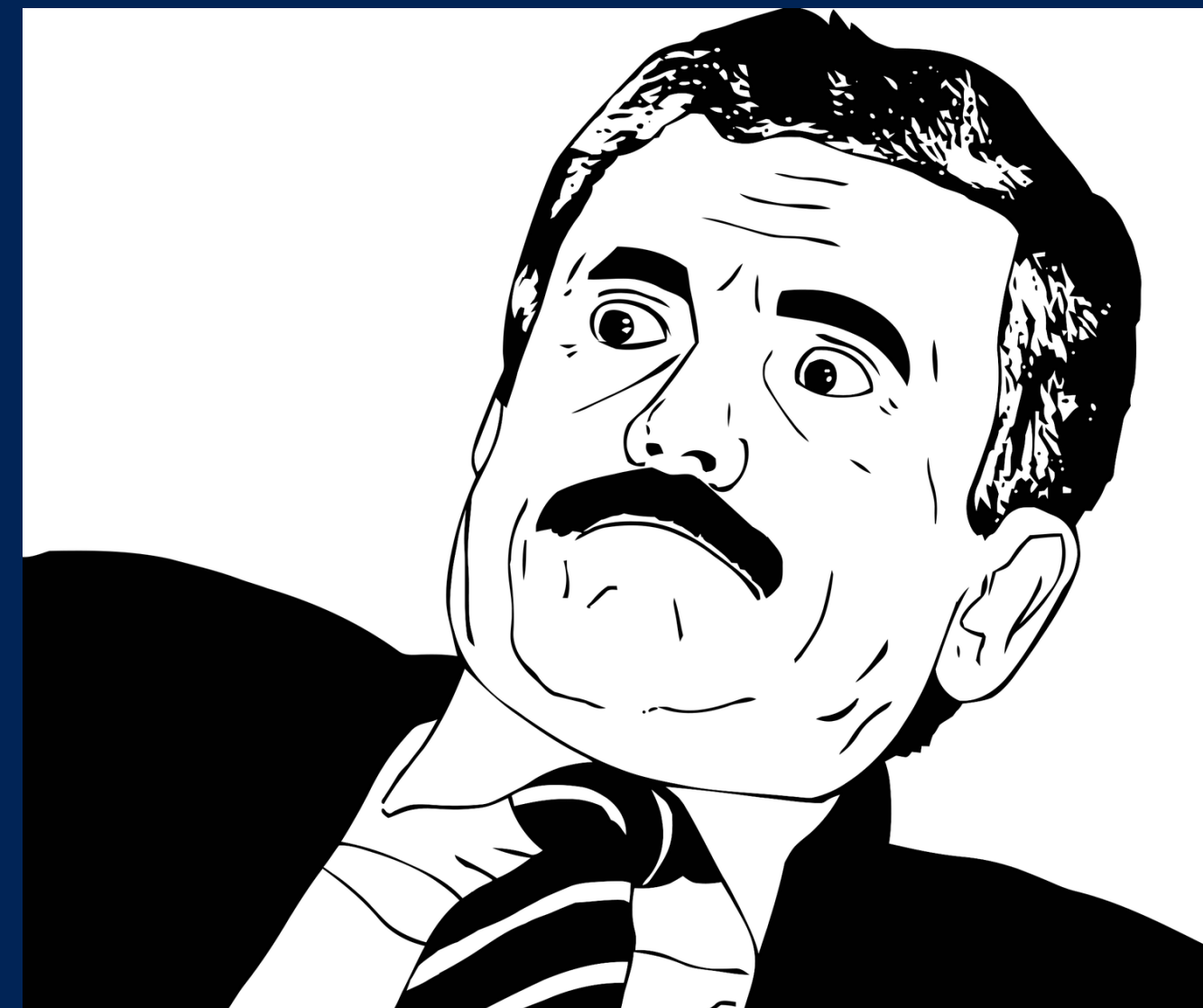
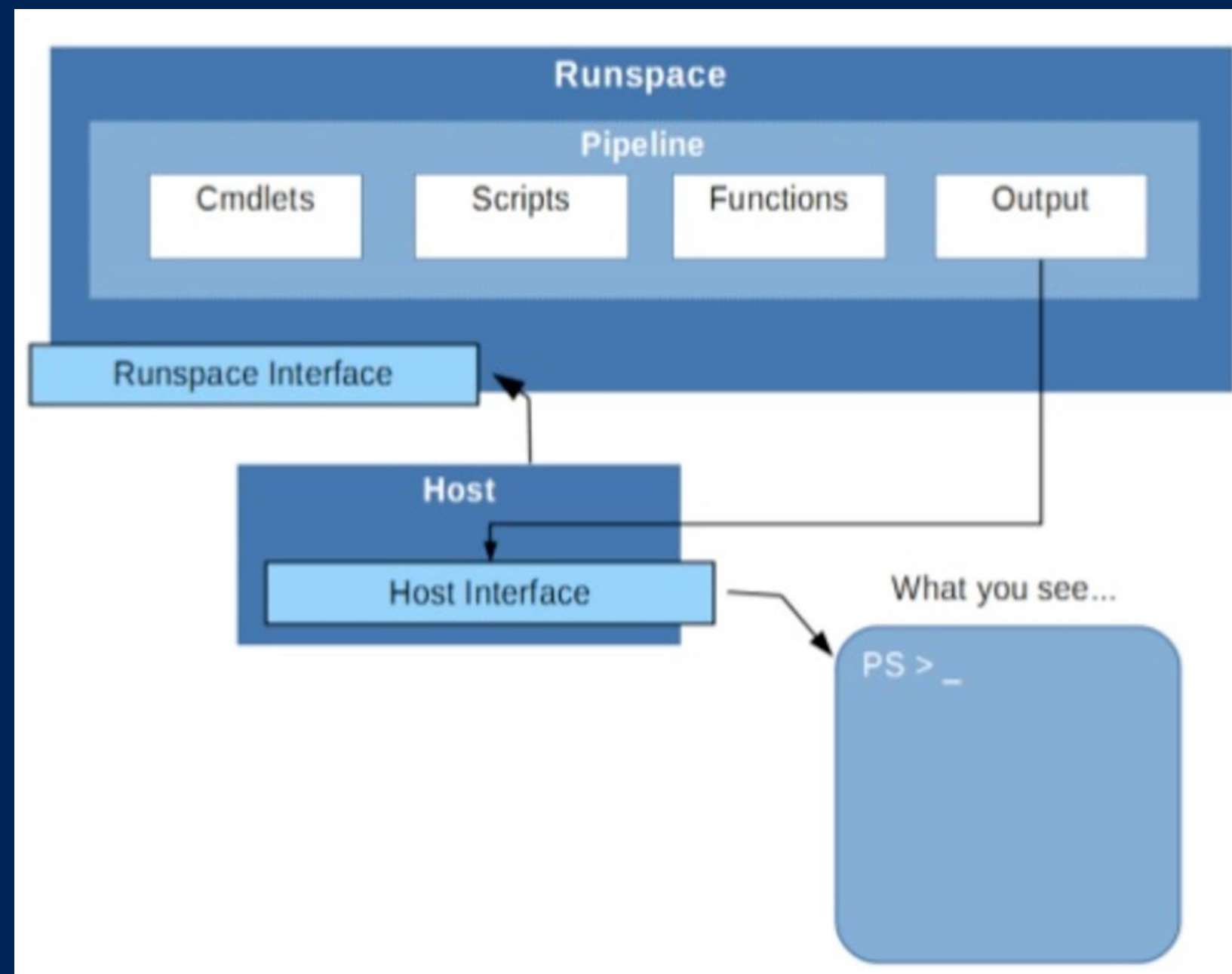
# >\_ Projeler

- Powershell Empire
- PowerSploit
- Nishang
- PowerOPS
- p0wnedShell
- Inveigh
- Unicorn





# >\_ Powershell > Powershell.exe



# >\_ Birakılan izler

- Kayıt Defteri
- Ağ Trafiği
- Memory
- Prefecth
- Event Log



# >\_ Kayıt Defteri

- Kalıcı Olmak (Persistent)



# >\_ Aă Trafiăi

- WinRM, Windows Remote Management
- Powershell Remoting
- HTTP 5985, HTTPS 5986





# >\_Memory

- Powershell Remoting?
- svchost.exe - DCOM Server Process
- DCOMLaunch
- C:\Windows\System32\wsmpromhost.exe



# >\_ Prefecth

- C:\Windows\Prefetch
- \*.pf



# >\_ Windows Event Log

- Powershell 3.0 +
- Windows PowerShell.evtx
- Microsoft-Windows-PowerShell%4Operational.evtx
- Microsoft-Windows-PowerShell%4Analytic.etl
- Microsoft-Windows-WinRM%4Operational.evtx
- • Microsoft-Windows-WinRM%4Analytic.etl



# >\_ Phant0m

- İz bırakmamak!?
- Windows Event Log





# >\_svchost.exe

## svchost.exe

---

From Wikipedia, the free encyclopedia

**svchost.exe** (**Service Host**, or **SvcHost**) is a system [process](#) that hosts multiple [Windows services](#) in the [Windows NT](#) family of [operating systems](#).<sup>[1]</sup> Svchost is essential in the implementation of so-called *shared service processes*, where a number of services can share a process in order to reduce resource consumption. Grouping multiple services into a single process conserves computing resources, and this consideration was of particular concern to NT designers because creating

# >\_ Windows Event Log

Process Hacker [DZLAB\PoC]+ (Administrator)

Hacker View Tools Users Help

Refresh Options Find handles or DLLs System information

Processes Services Network Disk

Name	PID	CPU	I/O tot...	Private ...	User name
SearchIndexer.exe	3140			14,34 MB	NT AUTHORITY\SYSTEM
SearchUI.exe	3440			34,64 MB	DZLAB\PoC
services.exe	732	0,03		2,6 MB	NT AUTHORITY\SYSTEM
ShellExperienceHost.exe	3332			15,91 MB	DZLAB\PoC
sihost.exe	3052			3,38 MB	DZLAB\PoC
smss.exe	484			336 kB	NT AUTHORITY\SYSTEM
spoolsv.exe	1444			8,03 MB	NT AUTHORITY\SYSTEM
svchost.exe	560			6,09 MB	NT AUTHORITY\LOCAL SERVICE
svchost.exe	580			4,73 MB	NT AUTHORITY\SYSTEM
svchost.exe	804	0,01		4,42 MB	NT AUTHORITY\SYSTEM
svchost.exe	836			2,97 MB	NT AUTHORITY\NETWORK SERVICE
svchost.exe	1004			14,8 MB	NT AUTHORITY\SYSTEM
svchost.exe	1048	0,03		2,73 MB	NT AUTHORITY\LOCAL SERVICE
svchost.exe	1076			13,71 MB	NT AUTHORITY\LOCAL SERVICE
svchost.exe	1300			4,07 MB	NT AUTHORITY\NETWORK SERVICE
svchost.exe					NT AUTHORITY\LOCAL SERVICE
svchost.exe					NT AUTHORITY\LOCAL SERVICE
svchost.exe					NT AUTHORITY\LOCAL SERVICE
svchost.exe					NT AUTHORITY\LOCAL SERVICE
svchost.exe					NT AUTHORITY\LOCAL SERVICE
System					
System Idle Process					
taskhostw.exe					
VGAAuthService.exe					
vmacthlp.exe					
vmtoolsd.exe					
vmtoolsd.exe					
wininit.exe	656			812 kB	NT AUTHORITY\SYSTEM
winlogon.exe	664			1,76 MB	NT AUTHORITY\SYSTEM
WmiPrvSE.exe	2372			4,78 MB	NT AUTHORITY\NETWORK SERVICE
WmiPrvSE.exe	2792			19,63 MB	NT AUTHORITY\SYSTEM
WUDFHost.exe	820	0,05		1,63 MB	NT AUTHORITY\LOCAL SERVICE

File: C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted

Host Process for Windows Services 10.0.10240.16384

Microsoft Corporation

Service group name: LocalServiceNetworkRestricted

Services:

- Audiosrv (Windows Audio)
- Dhcp (DHCP Client)
- EventLog (Windows Event Log)
- NgcCtnrSvc (Microsoft Passport Container)
- Wcmsvc (Windows Connection Manager)
- wscsvc (Security Center)

Notes:

Signer: Microsoft Windows Publisher

svchost.exe (1076) Properties

Services		GPU		Disk and Network		Comment		
General	Statistics	Performance	Threads	Token	Modules	Memory	Environment	Handles
TID	CPU	Cycles delta	Start address	Priority	Service			
1080			svchost.exe+0x3440	Normal				
1356			ntdll.dll!EtwEventRegister+0x50	Normal				
1396			ntdll.dll!EtwEventRegister+0x50	Normal				
2276			ntdll.dll!EtwEventRegister+0x50	Normal				
2348		159.331	ntdll.dll!EtwEventRegister+0x50	Normal				
2788			ntdll.dll!EtwEventRegister+0x50	Normal				
3912			ntdll.dll!EtwEventRegister+0x50	Normal				
1392			audiosrv.dll+0x40000	Normal	Audiosrv			
3256			combase.dll!CoFreeUnusedLibra...	Normal	Audiosrv			
1216			sechost.dll!RegisterServiceCtrlH...	Normal	Dhcp			
1272			dhcpcore6.dll!Dhcpv6Main	Normal	Dhcp			
1176			wevtsvc.dll+0x42bf0	Normal	EventLog			
1196			wevtsvc.dll!ServiceMain+0x66e0	Normal	EventLog			
1200			wevtsvc.dll!ServiceMain+0x66e0	Normal	EventLog			
1208			wevtsvc.dll!ServiceMain+0x66e0	Normal	EventLog			
1400			cmintegrator.dll+0x1130	Normal	Wcmsvc			
1404			wcmsvc.dll!WcmSvcMain+0x10260	Normal	Wcmsvc			
724			wscsvc.dll!ServiceMain+0x2410	Normal	wscsvc			
2716			wscsvc.dll!ServiceMain+0x1580	Normal	wscsvc			

Start module:

Started: N/A

State: N/A

Kernel time: N/A

User time: N/A

Context switches: N/A

Cycles: N/A

Priority: N/A

Base priority: N/A

I/O priority: N/A

Page priority: N/A

Ideal processor: N/A

Close

# >\_ Demo

1. .DOC (Macro)
2. MS16-032 LPE
3. Phant0m
4. Meterpreter

