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

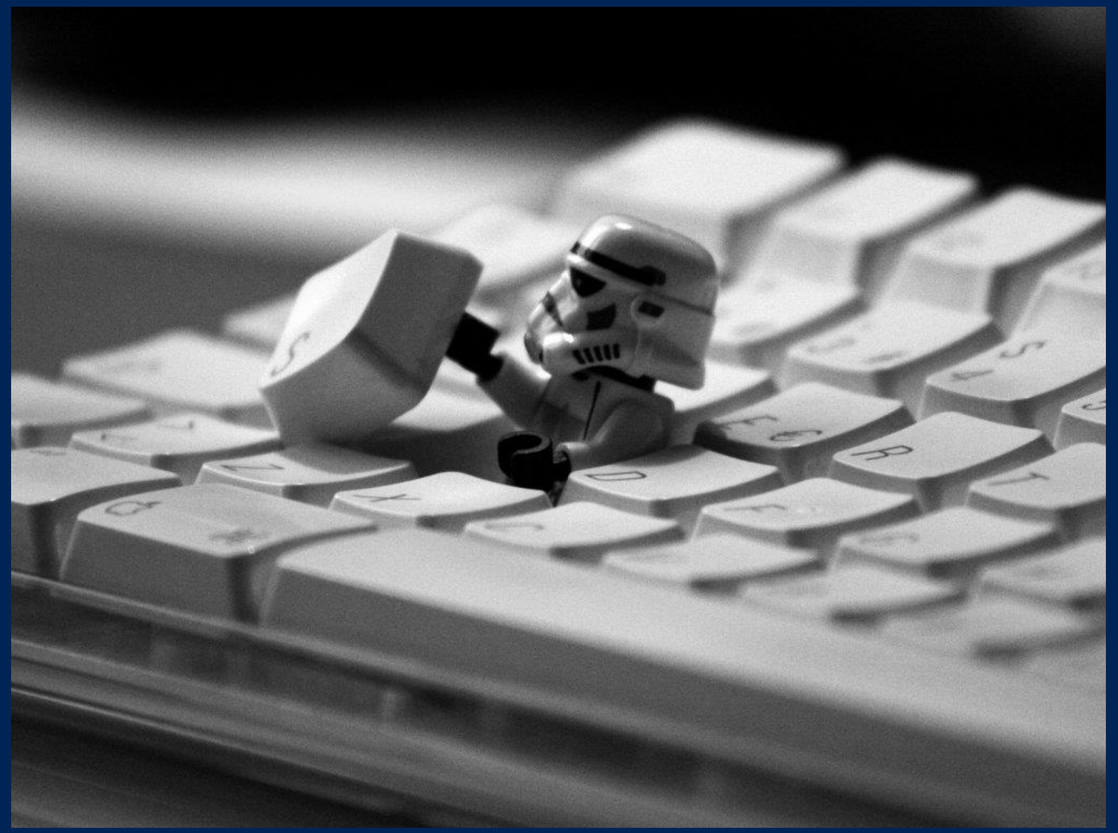
- Signed, Legal
- Varsayılan Olarak Yüklü
- Şifreli Trafik İle Uzaktan Erişim İmkanı
- Anti-Forensic Friendly
- Anti-Application Whitelisting Friendly
- Script-Based Malware Bağışıklığı
- Obfuscation Kolaylığı

>_ Execution Policy

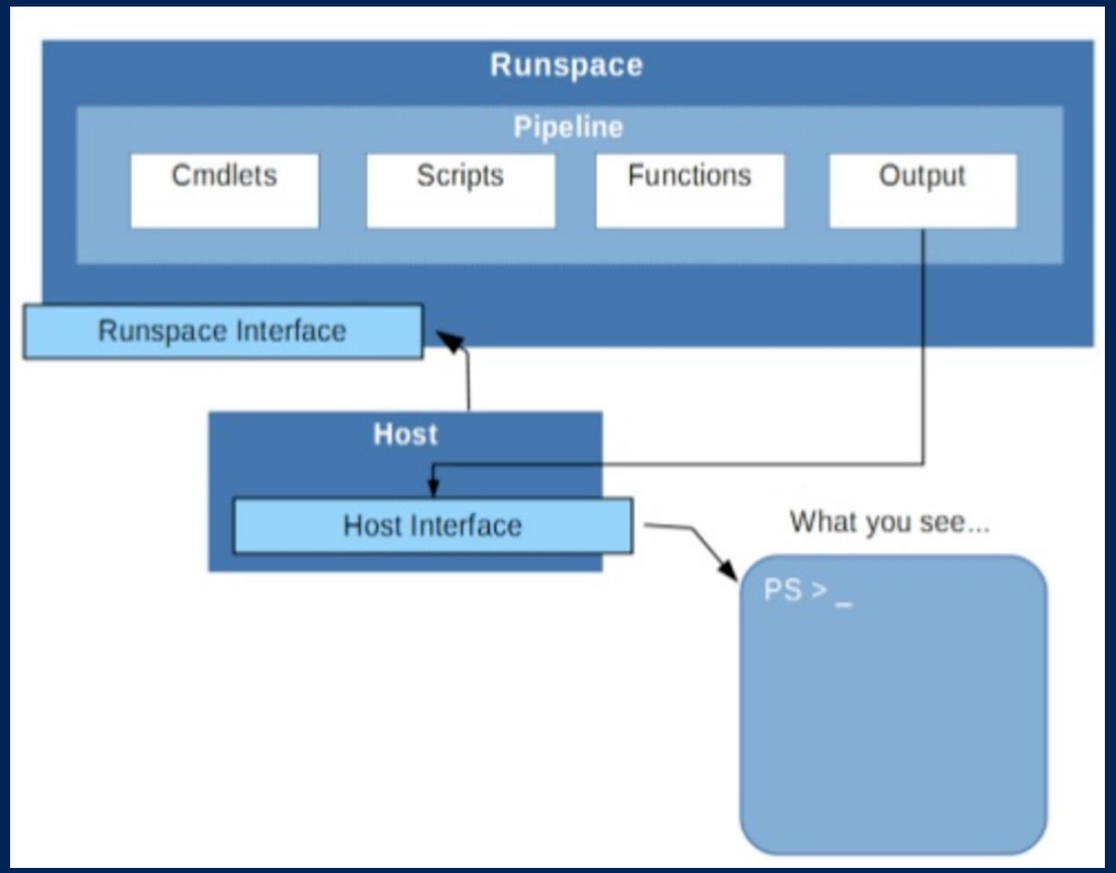
- Restricted
- RemoteSigned
- AllSigned
- Unrestricted
- Bypass

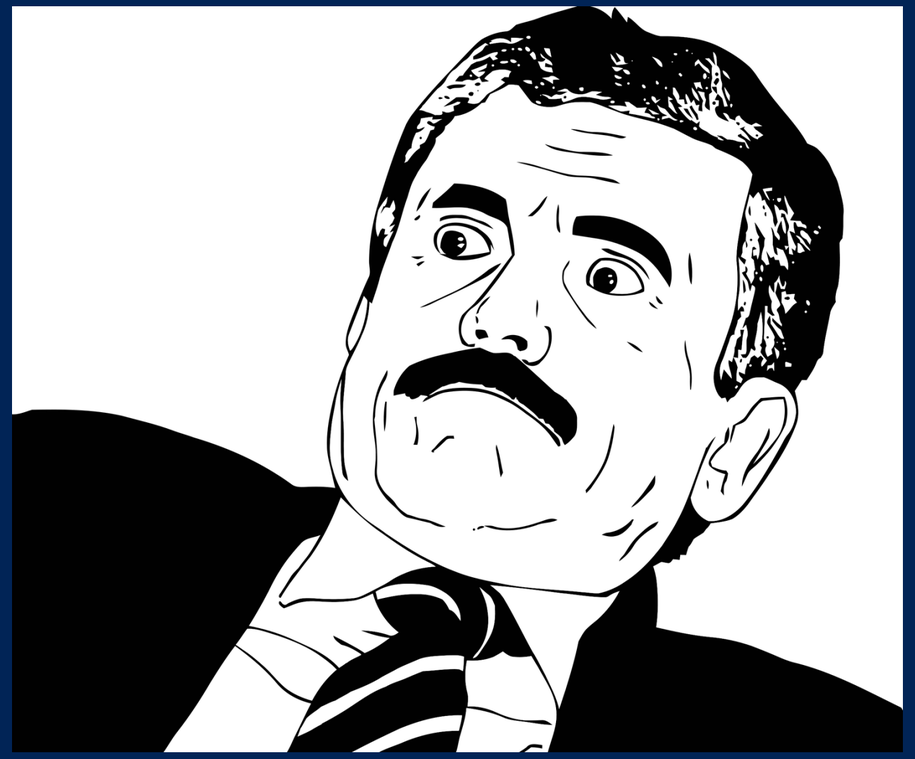
>_ Projeler

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



>_ Powershell > Powershell.exe





>_ Bırakılan İzler

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

>_ Kayıt Defteri

- Kalıcı Olmak (Persistent)

>_ Ağ Trafiği

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

>_ Memory

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

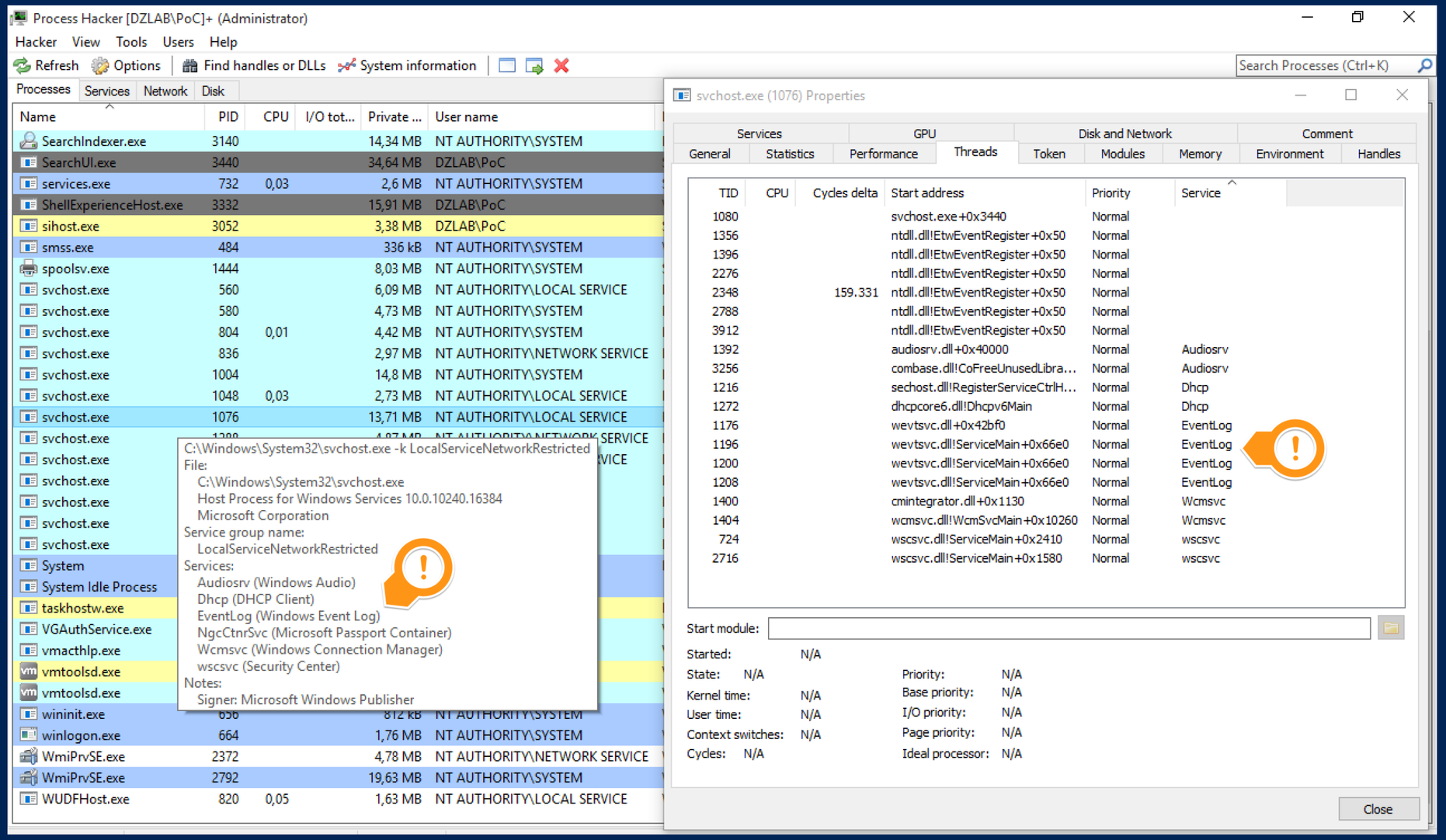
>_ svchost.exe

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.[1] 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



>_ Demo

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