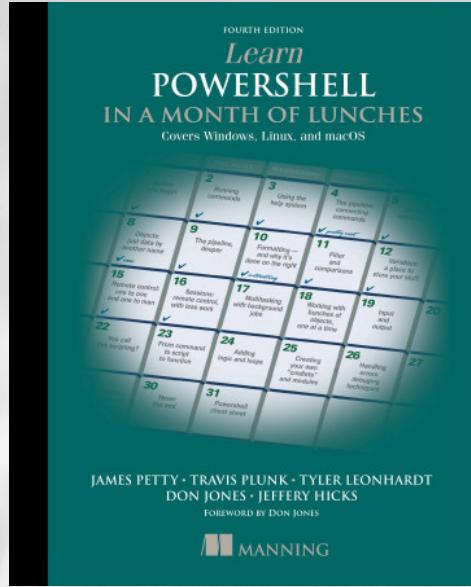
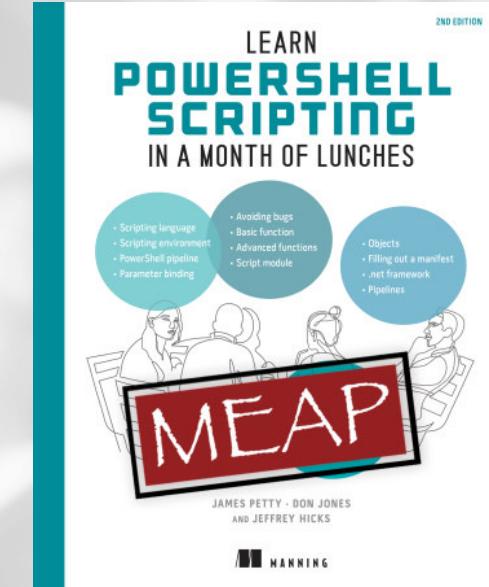


PowerShell Security and Best Practices



James Petty

@psjamesp



PowerShell

Windows PowerShell

5.1 – last release

.Net

PowerShell

7.6.3 – Latest

.Net Core

PowerShell is not a virus

Powershell.exe

Pwsh.exe

Scan the QR code on the room poster to fill out session evaluations



WARNING!

YOUR COMPUTER MAY BE INFECTED:

System Detected (2) Potentially Malicious Viruses: Rootkit.Sirefef.Spy and Trojan.FakeAV-Download. Your Personal & Financial Information MAY NOT BE SAFE.

To Remove Viruses, Call Tech Support Online Now:

1(866) 627-4049

(High Priority Virus Removal Call Line)

Your IP Address: [REDACTED] | Generated on [REDACTED] | Priority: Urgent

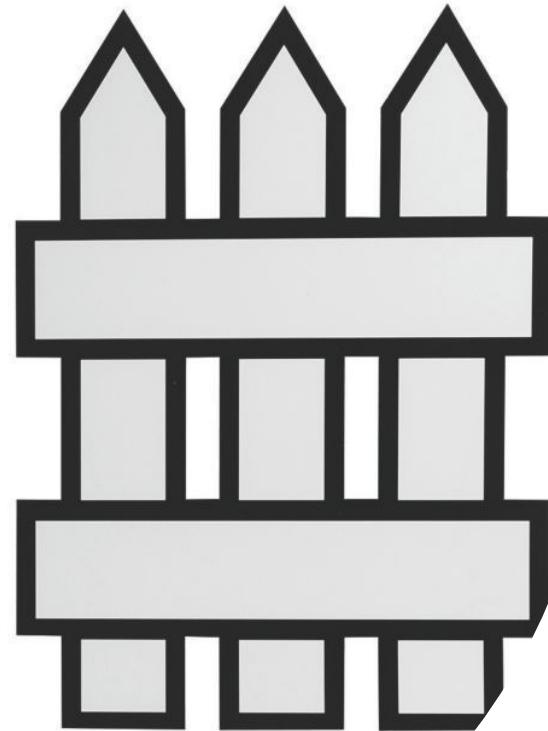


There are numerous virus that use PowerShell as the launch pad for their attack

#SPICEWORLD2023

Scan the QR code on the room poster to fill out session evaluations

D



SPICEWORLD
— IT CONFERENCE —

Security Policy

AllSigned

Bypass

Default

RemoteSigned

Restricted

Undefined

Unrestricted

MachinePolicy

UserPolicy

Process

CurrentUser

LocalMachine

PowerShell Remoting

Windows PowerShell

- WinRM
 - Port 5985 (HTTP)
 - Port 5986 (HTTPS)

PowerShell

- WinRM
 - Port 5985 (HTTP)
 - Port 5986 (HTTPS)
- SSH
 - Port 22

Remoting with PowerShell

SSH

-HostName

WinRM

-ComputerName

A blurred background image showing a large audience of people seated in rows, facing towards the left side of the frame, suggesting they are attending a presentation or conference.

#SPICEWORLD2023

Thank you.

THE HOTTEST I.T. CONFERENCE IN THE UNIVERSE

SPICEWORLD
— IT CONFERENCE —