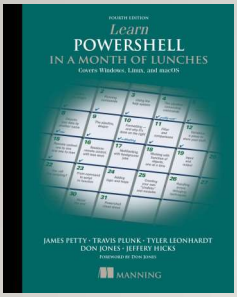
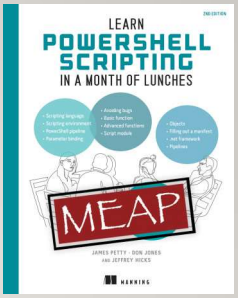

POWERSHELL SECURITY
AND BEST PRACTICES





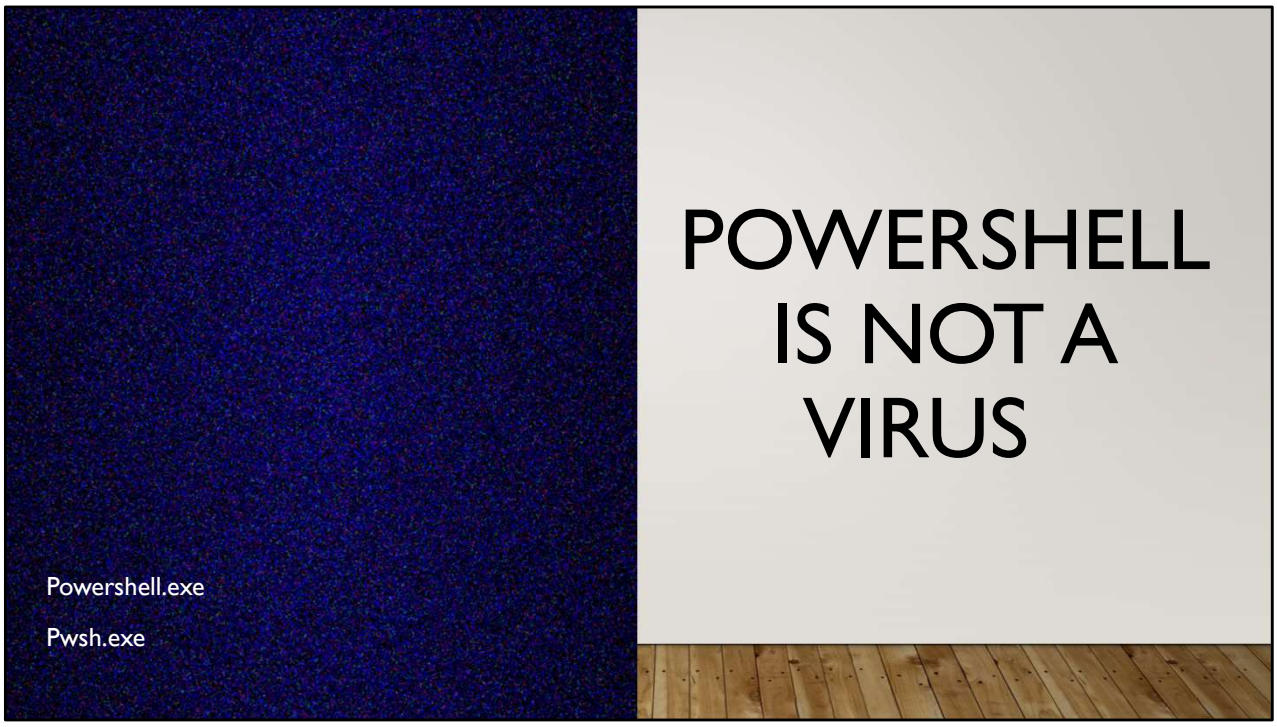
JAMES PETTY

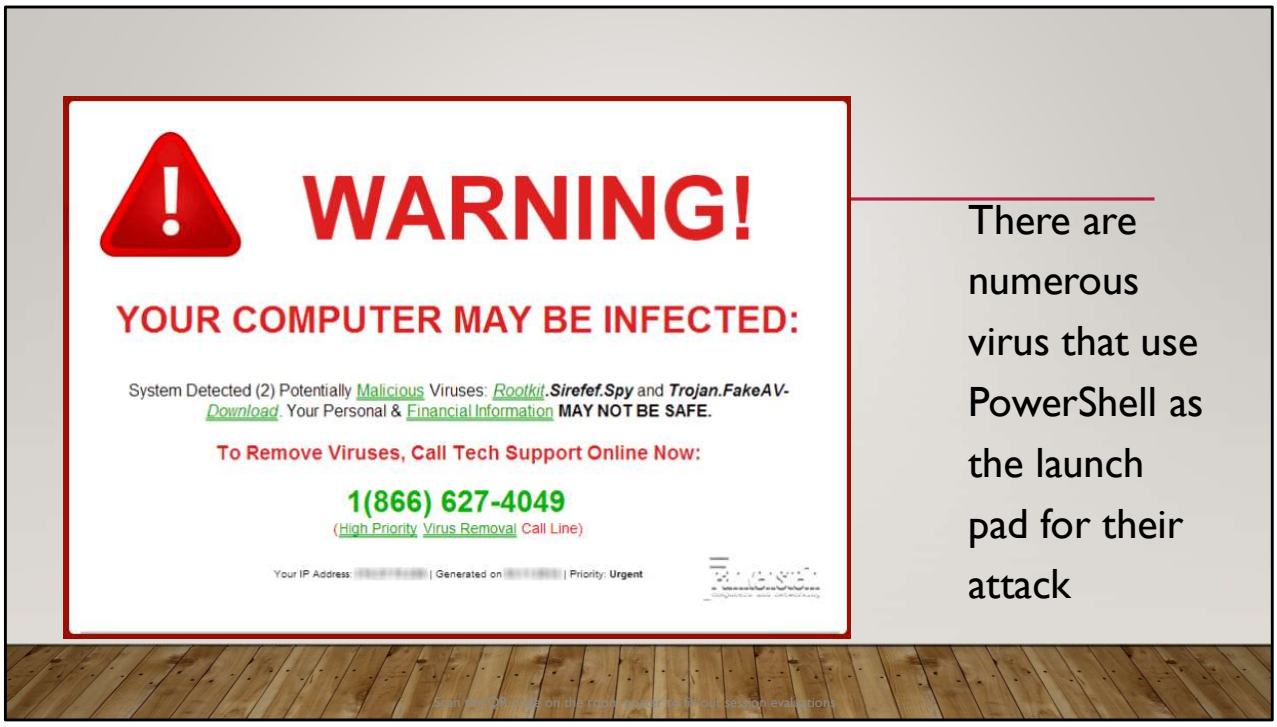
@psjamesp
Github.com/psjamesp

https://github.com/psjamesp/presentations/lopsa-knx

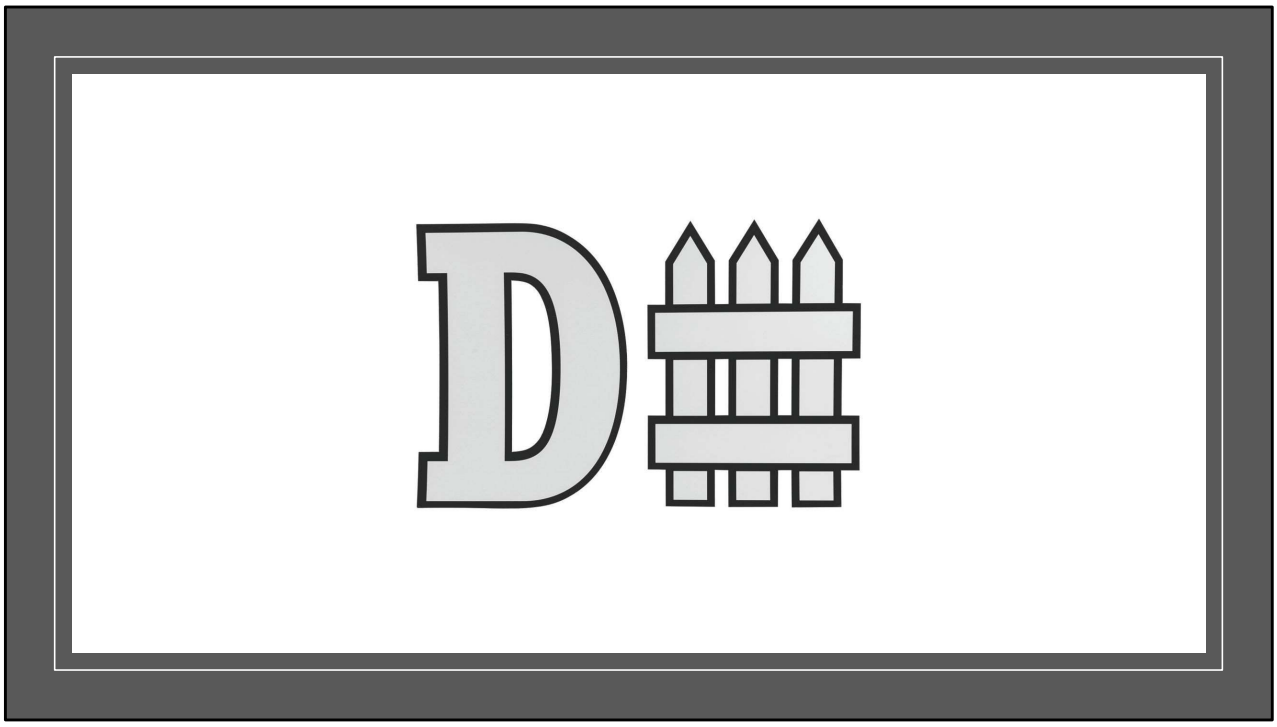
POWERSHELL

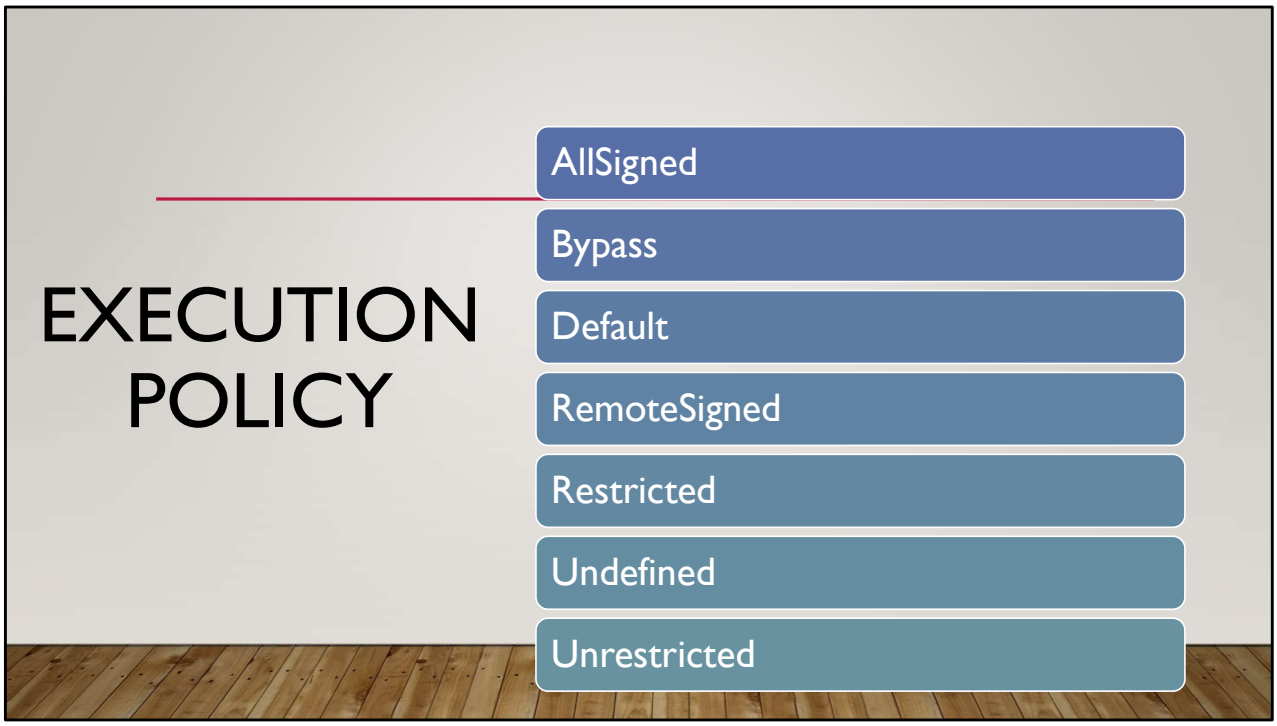
Windows PowerShell	PowerShell
5.1 – last release	7.4 – Latest
.Net	.Net Core


POWERSHELL IS NOT A VIRUS
Powershell.exe
Pwsh.exe

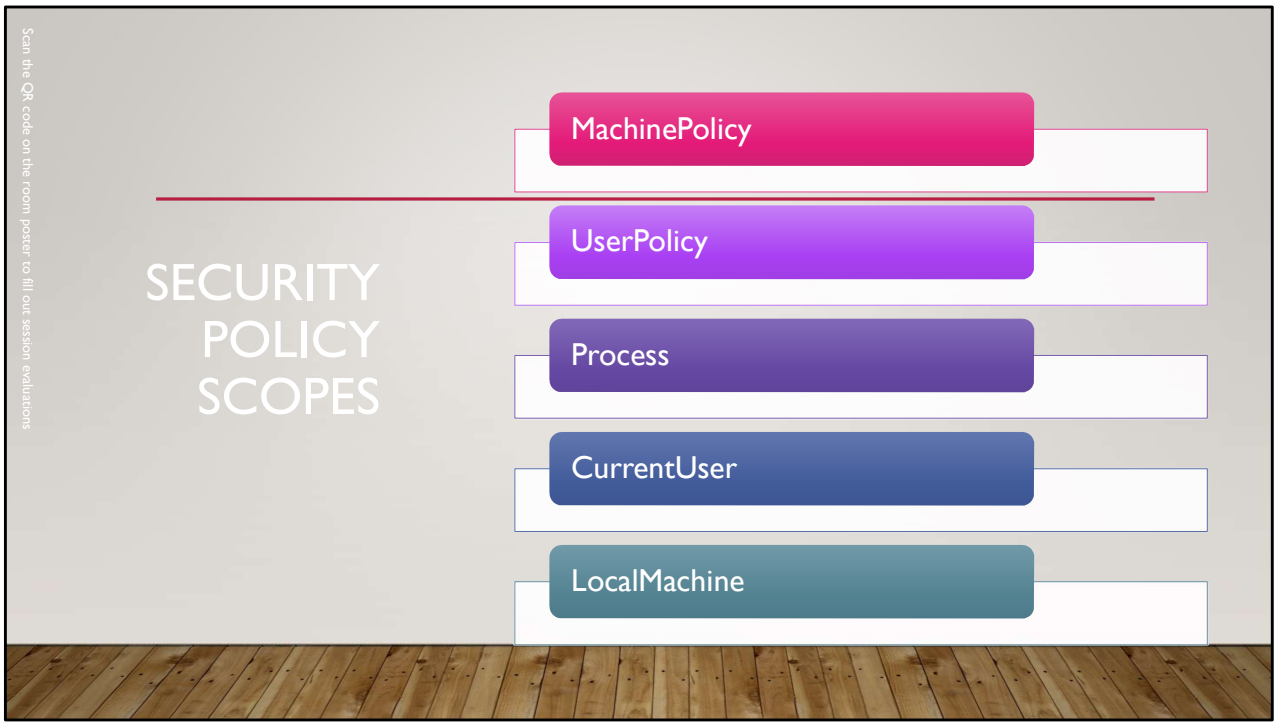


There are numerous virus that use PowerShell as the launch pad for their attack


D#



•**AllSigned**. Requires that all scripts and configuration files are signed by a trusted publisher, including scripts written on the local computer.
•**Bypass**. Nothing is blocked and there are no warnings or prompts.
•**Default**. Sets the default execution policy. **Restricted** for Windows clients or **RemoteSigned** for Windows servers.
•**RemoteSigned**. Requires that all scripts and configuration files downloaded from the Internet are signed by a trusted publisher. The default execution policy for Windows server computers.
•**Restricted**. Doesn't load configuration files or run scripts. The default execution policy for Windows client computers.
•**Undefined**. No execution policy is set for the scope. Removes an assigned execution policy from a scope that is not set by a Group Policy. If the execution policy in all scopes is **Undefined**, the effective execution policy is **Restricted**.
•**Unrestricted**. Beginning in PowerShell 6.0, this is the default execution policy for non-Windows computers and can't be changed. Loads all configuration files and runs all scripts. If you run an unsigned script that was downloaded from the internet, you're prompted for permission before it runs.


Scan the QR code on the room poster to fill out session evaluations
SECURITY POLICY SCOPES
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	WinRM
-HostName	-ComputerName


Thank you.