Malware Hunting 2026 Field Guide

Signatures are dead. Watch behavior. Watch memory. Watch chains.

The Family Tree — What You're Hunting

VIRUS	WORM	TROJAN	ROOTKIT	SPYWARE	RAT
Attaches to host file	Self-propagates	Disguised install	Kernel-level hide	Silent collector	Live remote control

LOLBin Watch List — Legit Tools, Malicious Use

- ☐ `powershell.exe` — Encoded/hidden execution
  `-nop -w hidden -enc`
- ☐ `wmic.exe` — Remote code execution
  `process call create`
- ☐ `certutil.exe` — File download from URL
  `-urlcache -f http://`
- ☐ `mshta.exe` — Remote HTA execution
  `http://... .hta`
- ☐ `regsvr32.exe` — Scriptlet download/execute
  `/s /u /i:http://`
- ☐ `bitsadmin.exe` — Background file download
  `/transfer /download`
- ☐ `rundll32.exe` — Inline JS execution
  `javascript:...`
- ☐ `msbuild.exe` — Arbitrary code via project file
  `*.xml (proj files)`

Process Tree Red Flags

winword.exe / excel.exe	outlook.exe	browser process	services.exe	*.tmp folder binary
→	→	→	→	→
powershell / cmd / wmic	any script interpreter	cmd / powershell	cmd from unusual paths	any network activity

Where to Look When the File System Is Empty

MEMORY
- ☐ Injected code (VirtualAllocEx)
- ☐ Hollowed processes
- ☐ Command line ☐ image path
- ☐ Suspicious loaded DLLs

REGISTRY
- ☐ Run / RunOnce keys
- ☐ Image File Execution Options
- ☐ Winlogon shell/userinit
- ☐ AppInit_DLLs

SCHEDULING
- ☐ Scheduled Tasks
- ☐ WMI event subscriptions
- ☐ COM object hijacking
- ☐ Startup folder items

NETWORK
- ☐ Beaconing intervals
- ☐ DNS to new domains
- ☐ TLS to unknown issuers
- ☐ Non-standard ports