Windows Memory Forensics — Case Notes (Suspicious PowerShell Beaconing)

Luis Camacho Jr. — Junior SOC/DFIR

Executive Summary

During routine threat hunting, anomalous PowerShell activity was observed on a Windows host. Memory analysis revealed an injected PowerShell process initiating periodic DNS-based beaconing. The host was isolated, persistence removed, and IOCs pushed to detection watchlists.

Environment

```
OS: Windows 10 (Lab)
User Context: Standard user
Logging: Sysmon (operational), Windows Security, Zeek (SPAN capture)
Tools: FTK Imager, Volatility, Zeek, RITA/AC-Hunter, Splunk
```

Triage Timeline

```
T0  — Alert: Unusual PowerShell parent/child chain
T+5 — Host isolated from network
T+10 — Memory acquired; volatile artifacts preserved
T+25 — Volatility triage and process tree reconstruction
T+45 — Beaconing confirmed via Zeek + RITA
T+60 — Persistence keys removed; IOCs distributed; report drafted
```

Acquisition

Disk image captured with FTK Imager (logical) and RAM captured via winpmem. Hashes recorded (SHA256). All actions executed under a minimal-change, documented workflow.

Memory Analysis (Volatility)

```
Commands executed:
  - windows.pslist / pstree — establish process lineage
  - windows.netscan — enumerate network sockets
  - malfind — search for code injection
  - cmdline — recover command-line parameters
  - handles — enumerate suspicious handles

Highlights:
  • powershell.exe (PID 2316) spawned by explorer.exe with encoded command
  • Suspicious remote DNS queries observed during netscan window
  • malfind detected RWX region inside powershell.exe (entropy high)
```

Network Findings (Zeek + RITA/AC-Hunter)

Zeek dns.log revealed periodic queries to subdomains matching a fast-flux pattern. RITA scored the destination as beacon-like (elevated periodicity & low jitter). PCAP reconstruction showed small, regular payloads over DNS with base64-like lengths.

SIEM Investigation (Splunk)

```
Sample SPL used:
  1) Suspicious child processes:
     index=win EventCode=4688 New_Process_Name=powershell*
     | stats count by Account_Name, Parent_Process_Name, New_Process_Name,
Command_Line

  2) Beaconing heuristic:
     index=zeek sourcetype=dns
     | bin _time span=1m
     | stats count by src_ip, query, _time
     | eventstats avg(count) as avg stdev(count) as sd by src_ip,query
     | where count > avg + 3*sd
```

Indicators of Compromise (IOCs)

```
Domains: *.example-beacon.com (lab)
IP: 10.10.10.50 (C2 in lab range)
Hash (suspicious DLL): d41d8cd98f00b204e9800998ecf8427e (placeholder)
Command-line pattern: powershell.exe -enc
```

Persistence & Remediation

Persistence located in HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Value: 'Updater' → powershell -enc
Actions: Removed autorun key; rotated creds; cleared cached tokens; restored host from clean snapshot; pushed IOCs to watchlists; added DNS sinkhole for lab domain.

MITRE ATT&CK; Mapping

T1059.001 PowerShell • T1055 Process Injection • T1071.004 Exfiltration over Uncommonly Used Port (DNS) • T1053 Scheduled Task/Job (if applicable) • T1060 Registry Run Keys/Startup Folder

Recommendations

- Harden PowerShell with Constrained Language Mode and script block logging
- Expand Sysmon coverage (parent-child + network GUIDs)
- Create detections for encoded PowerShell, abnormal DNS query periodicity, and autorun anomalies
- User awareness on phishing/attachments; enforce least privilege
- Regular memory acquisition drills in IR runbooks

Lessons Learned

Early correlation between host artifacts (Volatility) and network telemetry (Zeek/RITA) shortened time-to-containment. Maintaining ready-to-run SPL and Sigma templates accelerated triage and documentation.