

Common Symptoms of Compromise

Chapter 17

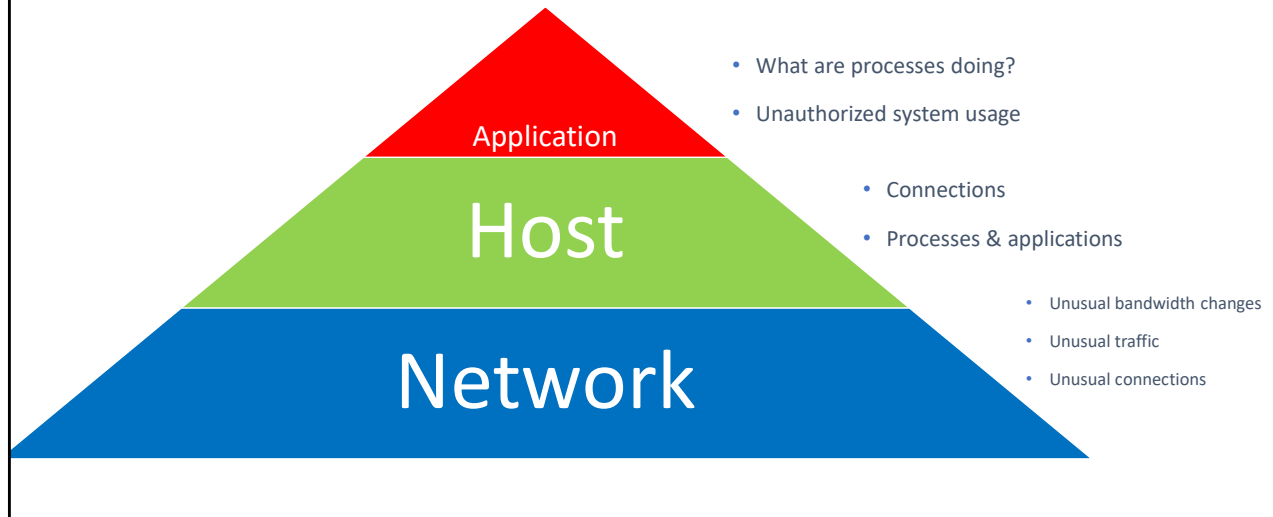
Episode 17.01

Network Symptoms

Objective: 4.3 Given an incident, analyze potential indicators of compromise.

- Network-related
 - Bandwidth consumption
 - Beaconsing
 - Irregular peer-to-peer communication
 - Rogue device on the network
 - Scan/sweep
 - Unusual traffic spike
 - Common protocol over non-standard port

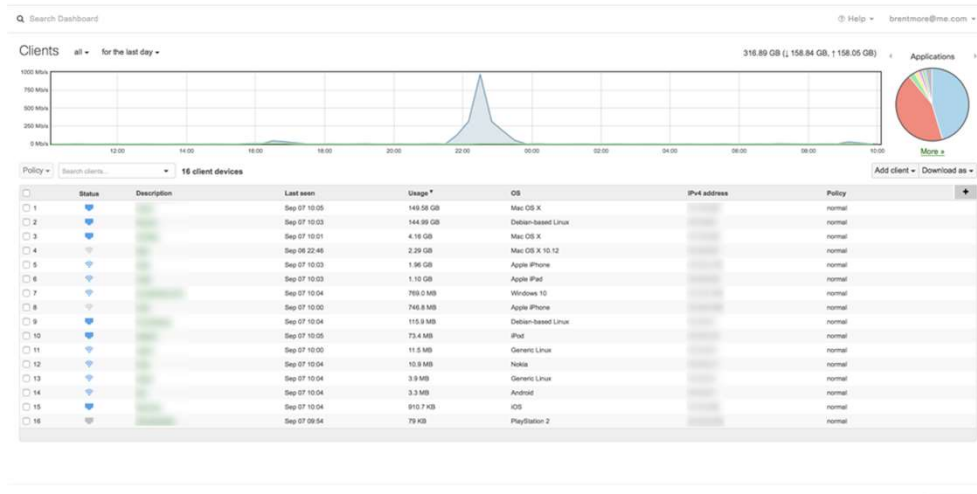
Diagnose Symptoms



Network-Related Symptoms

- Bandwidth consumption
- Traffic spikes
- Traffic irregularities

Bandwidth Consumption



Network-Related Symptoms

- Beaconing
- Peer-to-peer communications
- Rogue devices
- Scan sweeps

Scan Sweep

| Time | Source | Destination | Protocol | Length | Info |
|------------|-----------------|-------------|----------|--------|---|
| 1.88519000 | Vmware_4a:58:30 | Broadcast | ARP | 42 | who has 192.168.192.162? Tell 192.168.192.6 |
| 1.88528900 | Vmware_4a:58:30 | Broadcast | ARP | 42 | who has 192.168.192.163? Tell 192.168.192.6 |
| 1.88540000 | Vmware_4a:58:30 | Broadcast | ARP | 42 | who has 192.168.192.164? Tell 192.168.192.6 |
| 1.88555900 | Vmware_4a:58:30 | Broadcast | ARP | 42 | who has 192.168.192.165? Tell 192.168.192.6 |
| 1.88566200 | Vmware_4a:58:30 | Broadcast | ARP | 42 | who has 192.168.192.166? Tell 192.168.192.6 |
| 1.88574400 | Vmware_4a:58:30 | Broadcast | ARP | 42 | who has 192.168.192.167? Tell 192.168.192.6 |
| 1.88583400 | Vmware_4a:58:30 | Broadcast | ARP | 42 | who has 192.168.192.168? Tell 192.168.192.6 |
| 1.88591000 | Vmware_4a:58:30 | Broadcast | ARP | 42 | who has 192.168.192.169? Tell 192.168.192.6 |
| 1.88601800 | Vmware_4a:58:30 | Broadcast | ARP | 42 | who has 192.168.192.170? Tell 192.168.192.6 |
| 1.88610000 | Vmware_4a:58:30 | Broadcast | ARP | 42 | who has 192.168.192.171? Tell 192.168.192.6 |
| 1.88618800 | Vmware_4a:58:30 | Broadcast | ARP | 42 | who has 192.168.192.172? Tell 192.168.192.6 |
| 1.88626800 | Vmware_4a:58:30 | Broadcast | ARP | 42 | who has 192.168.192.173? Tell 192.168.192.6 |
| 1.88643300 | Vmware_4a:58:30 | Broadcast | ARP | 42 | who has 192.168.192.174? Tell 192.168.192.6 |
| 1.88654100 | Vmware_4a:58:30 | Broadcast | ARP | 42 | who has 192.168.192.175? Tell 192.168.192.6 |
| 1.88663100 | Vmware_4a:58:30 | Broadcast | ARP | 42 | who has 192.168.192.176? Tell 192.168.192.6 |
| 1.88671500 | Vmware_4a:58:30 | Broadcast | ARP | 42 | who has 192.168.192.177? Tell 192.168.192.6 |

Episode 17.02

Host Symptoms

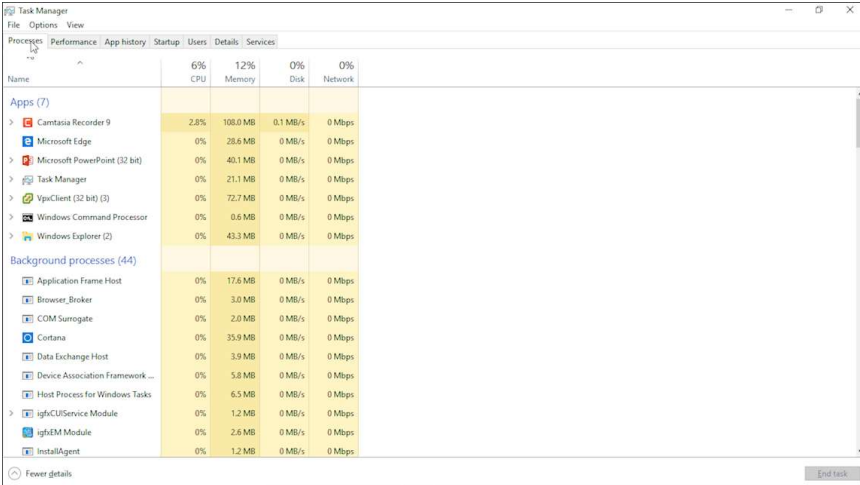
Objective: 4.3 Given an incident, analyze potential indicators of compromise.

- Host-related
 - Processor consumption
 - Memory consumption
 - Drive capacity consumption
 - Unauthorized software
 - Malicious process
 - Unauthorized change
 - Unauthorized privilege
 - Data exfiltration
 - Abnormal OS process behavior
 - File system change or anomaly
 - Registry change or anomaly
 - Unauthorized scheduled task

Host-Related Symptoms

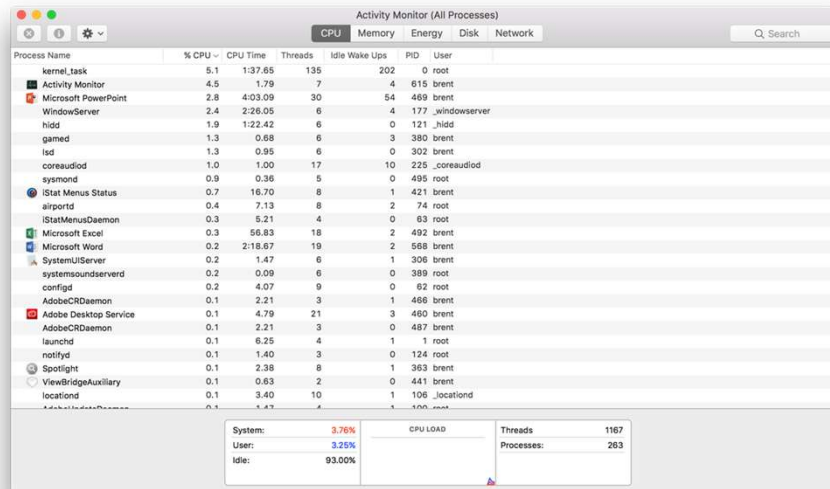
- Memory consumption
- Disk consumption
- Processor consumption
- Unauthorized applications or processes
- Unauthorized privileges
- Data exfiltration

Windows Task Manager



| Task Manager | | | | |
|---------------------------------|--------|------------|----------|------------|
| Processes | | | | |
| Name | 6% CPU | 12% Memory | 0% Disk | 0% Network |
| Apps (7) | | | | |
| Camtasia Recorder 9 | 2.8% | 108.0 MB | 0.1 MB/s | 0 Mbps |
| Microsoft Edge | 0% | 28.6 MB | 0 MB/s | 0 Mbps |
| Microsoft PowerPoint (32 bit) | 0% | 40.1 MB | 0 MB/s | 0 Mbps |
| Task Manager | 0% | 21.1 MB | 0 MB/s | 0 Mbps |
| VpnClient (32 bit) (3) | 0% | 72.7 MB | 0 MB/s | 0 Mbps |
| Windows Command Processor | 0% | 0.6 MB | 0 MB/s | 0 Mbps |
| Windows Explorer (2) | 0% | 43.3 MB | 0 MB/s | 0 Mbps |
| Background processes (44) | | | | |
| Application Frame Host | 0% | 17.6 MB | 0 MB/s | 0 Mbps |
| Browser_Broker | 0% | 3.0 MB | 0 MB/s | 0 Mbps |
| COM Surrogate | 0% | 2.0 MB | 0 MB/s | 0 Mbps |
| Cortana | 0% | 35.9 MB | 0 MB/s | 0 Mbps |
| Data Exchange Host | 0% | 3.9 MB | 0 MB/s | 0 Mbps |
| Device Association Framework... | 0% | 5.8 MB | 0 MB/s | 0 Mbps |
| Host Process for Windows Tasks | 0% | 6.5 MB | 0 MB/s | 0 Mbps |
| igfxCUServiceModule | 0% | 1.2 MB | 0 MB/s | 0 Mbps |
| igfxEMModule | 0% | 2.6 MB | 0 MB/s | 0 Mbps |
| InstallAgent | 0% | 1.2 MB | 0 MB/s | 0 Mbps |

macOS Activity Monitor



The screenshot displays the macOS Activity Monitor window, titled "Activity Monitor (All Processes)". The "CPU" tab is selected, showing a list of processes with columns for Process Name, % CPU, CPU Time, Threads, Idle Wake Ups, PID, and User. The processes are sorted by % CPU in descending order. At the bottom, a summary section provides system-wide statistics.

| Process Name | % CPU | CPU Time | Threads | Idle Wake Ups | PID | User |
|-----------------------|-------|----------|---------|---------------|-----|---------------|
| kernel_task | 5.1 | 1:37.65 | 135 | 202 | 0 | root |
| Activity Monitor | 4.5 | 1.79 | 7 | 4 | 615 | brent |
| Microsoft PowerPoint | 2.8 | 4:03.09 | 30 | 54 | 489 | brent |
| WindowServer | 2.4 | 2:26.05 | 6 | 4 | 177 | _windowserver |
| hidd | 1.9 | 1:22.42 | 6 | 0 | 121 | _hidd |
| gamed | 1.3 | 0.68 | 6 | 3 | 380 | brent |
| lsd | 1.3 | 0.95 | 6 | 0 | 302 | brent |
| coreaudiod | 1.0 | 1.00 | 17 | 10 | 225 | _coreaudiod |
| sysmond | 0.9 | 0.36 | 5 | 0 | 495 | root |
| iStat Menus Status | 0.7 | 16.70 | 6 | 1 | 421 | brent |
| airportd | 0.4 | 7.13 | 8 | 2 | 74 | root |
| iStatMenusDaemon | 0.3 | 5.21 | 4 | 0 | 63 | root |
| Microsoft Excel | 0.3 | 56.83 | 18 | 2 | 492 | brent |
| Microsoft Word | 0.2 | 2:18.67 | 19 | 2 | 568 | brent |
| SystemUIServer | 0.2 | 1.47 | 6 | 1 | 306 | brent |
| systemsoundserverd | 0.2 | 0.09 | 6 | 0 | 389 | root |
| configd | 0.2 | 4.07 | 9 | 0 | 62 | root |
| AdobeCRDaemon | 0.1 | 2.21 | 3 | 1 | 466 | brent |
| Adobe Desktop Service | 0.1 | 4.79 | 21 | 3 | 460 | brent |
| AdobeCRDaemon | 0.1 | 2.21 | 3 | 0 | 487 | brent |
| launchd | 0.1 | 6.25 | 4 | 1 | 1 | root |
| notifiyd | 0.1 | 1.40 | 3 | 0 | 124 | root |
| Spotlight | 0.1 | 2.38 | 8 | 1 | 363 | root |
| ViewBridgeAuxiliary | 0.1 | 0.63 | 2 | 0 | 441 | brent |
| locationd | 0.1 | 3.40 | 10 | 1 | 106 | _locationd |

| System: | | CPU LOAD | | Threads | |
|---------|--------|----------|--|------------|------|
| System: | 3.76% | | | Threads: | 1167 |
| User: | 3.25% | | | Processes: | 263 |
| Idle: | 93.00% | | | | |

Episode 17.03

Application Symptoms

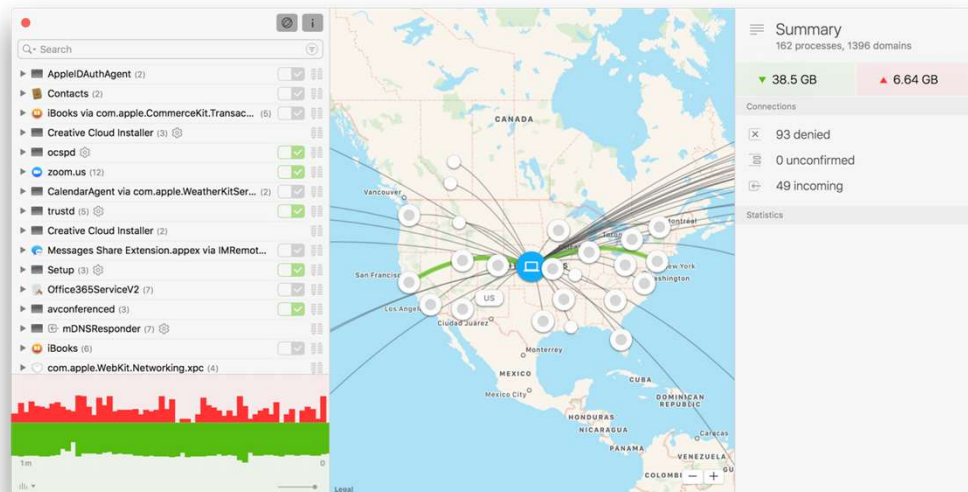
Objective: 4.3 Given an incident, analyze potential indicators of compromise.

- Application-related
 - Anomalous activity
 - Introduction of new accounts
 - Unexpected output
 - Unexpected outbound communication
 - Service interruption
 - Application log

Application-Related Symptoms

- Anomalous activity
- Unexpected error messages
- Out of memory alerts
- Unexpected outbound transmissions

Little Snitch



Windows Firewall

