NOTE: If you want to get a nice bird's-eye view of a lot of data at once, ask **Splunk** to show you its findings in a table format. The syntax isn't hard—just pipe your SPL search terms into a `table` command where you simply list the fields you want to display as a column. For example:

```
index=sysmon Computer="Daniel-PC" ProcessId=4652 | table _time, siem_event_id, Computer, source_ip, EventID, user, CurrentDirectory, process, ProcessId, Image, CommandLine, ParentProcessId, ParentImage, ParentCommandLine, SHA256
```

This is a quick way to drill down on a specific PID you're drilling down into, at a glance, without running a ton of **Splunk** queries to chase down PPIDs or timelines.

So, by pivoting between our two log sources, we can now reconstruct what happened:

1. `obommhdf.exe (PID 3764)` spawned a second instance of the `08875f1b...` Ramnit executable: `xwgrttjl.exe (PID 4652)`.
2. `xwgrttjl.exe (PID 4652)` then spawned the two rogue *(== without PPID of `services.exe (PID 500)`!)* `svchost.exe`'s: `svchost.exe (PID 4104)` and `svchost.exe (PID 2612)`.
3. `xwgrttjl.exe (PID 4652)` then exited the process list, having served its function.
4. `obommhdf.exe (PID 3764)`, `svchost.exe (PID 4104)` and `svchost.exe (PID 2612)` remain running.

This matches/corroborates the pattern we already saw in **ANY.RUN**'s process list from running the `08875f1b...` Ramnit executable sample in an earlier task.

#1. Ramnit's process execution trees

1a Ramnit's 2nd persistent execution (obommhdf.exe)

Note which **processes present or referenced within** this memory image are **involved with Ramnit in any way.**

Be sure to include the following information for each process: 1 **Process name** (*e.g.,* obommhdf.exe); 2 **PID & PPID** (in parentheses, after the Process name); 3 **How the process is related to Ramnit** (through inheritance or functionality or injection...).

e.g.: obommhdf.exe (PID 3764, PPID 472): Description of how Ramnit is related to this process.

System (PID: 272, PPID: 4)
- **smss.exe** (PID: 396, PPID: 272)
  - **winlogon.exe** (PID: 472, PPID: 396)
    - **obommhdf.exe** (PID: 3764, PPID: 472): Ramnit process child
    - **userinit.exe** (PID: 3744, PPID: 472)
      - **explorer.exe** (PID: 3824, PPID: 3744): hooker.dll is injected into this process and attempts to to map the configuration data into the browser's memory from shared memory sections
        - **chrome.exe** (PID: 2576, PPID: 3824): corroborates C2 communication
      - **xwgrttjl.exe** (PID 4652, PPID: 3764): responsible for installing/creating the svchost.exe processes (DLLs)
        - **svchost.exe** (PID: 2612, PPID: 4652): Injected DLL_2, communicates with C2
        - **svchost.exe** (PID: 4104, PPID: 4652): Injected DLL_1, requests/receives modules from DLL_2
          - **tracert.exe** (PID: 3908, PPID: 4104): listening on port 443, waiting for attacker to connect
        - **sdbinst.exe** (PID: 4232, PPID: 4652): this process is created to perform a silent installation with no visible window, status, or warning information to the user

1b Ramnit's 1st persistent execution (obommhdf.exe)

You will need to reference `sysmon`'s logs in the SIEM to reconstruct this, as it does not appear in your infected memory image from `Daniel-PC`.

System (PID: 272, PPID: 4)
smss.exe (PID: 396, PPID: 272)
winlogon.exe (PID: 492, PPID: 396)
obommhdf.exe (PID: 2292, PPID: 492)
xwgrttjl.exe (PID: 3804, PPID: 2292)
sdbinst.exe (PID: 3224, PPID: 3804)
svchost.exe (PID: 2156, PPID: 3804)
svchost.exe (PID: 2960, PPID: 3804)
tracert.exe (PID: 1800, PPID: 2960)
userinit.exe (PID: 2284, PPID: 492)
explorer.exe (PID: 2376, PPID: 2284)
obommhdf.exe (PID: 2740, PPID: 2376)
fgkhroxg.exe (PID: 3864, PPID: 2740)
obommhdf.exe (PID: 2756, PPID: 2376)
fgkhroxg.exe (PID: 3876, PPID: 2756)

1c Ramnit's initial execution (bilo400.exe)

You will need to reference `sysmon`'s logs in the SIEM to reconstruct this, as it does not appear in your infected memory image from `Daniel-PC`.

System (PID: 272, PPID: 4)
smss.exe (PID: 4924, PPID: 272)
winlogon.exe (PID: 1420, PPID: 4924)
userinit.exe (PID: 2364, PPID: 1420)
explorer.exe (PID: 728, PPID: 2364)
cmd.exe (PID: 1924, PPID:728): used for commands execution **bilo400.exe** (PID: 2148, PPID: 1924): the original malware executable containing Ramnit

---

#2. Corroborating & enriching previously-known IOCs

IOCs include **pivots you have already seen before in the SIEM during this your investigation**, such as IP addresses (+/- specific port), filenames (+/- filepaths), process names, process IDs, or usernames.

Be sure to note 1 which Volatility module(s) you saw this pivot corroborated in, 2 the pivot itself, and 3 whether any additional information is contained in the memory image that is not included within the SIEM (especially if it enriches the existing SIEM logs by giving further context).

e.g.: pslist, psscan, pstree: winlogon.exe (PID 472) is the parent process for obommhdf.exe (PID 3764). Evidence of persistence method for Ramnit. Exists in sysmon (sysmon logs contain more info).

shimcache: **Bilo400.exe (PID: 2148) -** original Ramnit malware executable dropped

---

#3. Entirely new pivots||IOCs

These are entirely newly-discovered-to-be-involved IOCs, including processes (such as Ramnit child processes or hooked processes) and filepaths. If you've found any, it is appropriate to include filepaths to hitherto-unknown files that may be worth following up on in the next task, when you have access to Daniel-PC's forensic disk image.

Be sure to note 1 which Volatility module(s) you saw this pivot corroborated in, 2 the pivot itself, and 3 whether this new pivot appears in any SIEM logs.

e.g.: pslist, psscan, pstree: winlogon.exe (PID 472) is the parent process for

obommhdf.exe (PID 3764). Evidence of persistence method for Ramnit. Exists in sysmon (sysmon logs contain more info).

N/A