

# SUNBURST & Memory Analysis

Published: 2020-12-25 · Archived: 2026-04-05 17:05:37 UTC

The recent SolarWind's hack which resulted in a backdoor version of their SolarWind Orion product which counts 33,000 customers has been all over the news in the past few weeks - most things have been said and repeated, although there are few notes that I mentioned on Twitter which I would like to compile in a blogpost for perennality.

First of all, I would like to point out to the presence in the backdoor process blacklist (*the full list can be found on [Itay Cohen's repository](#)*) of several processes that can be used for either:

- creating system raw memory dump such as Belkasoft RAM Capturer,
- or creating Microsoft process crash dumps with some of the Sysinternals Tools such as ProcDump or Process Explorer.

```
13611814135072561278UL /* procdump64 (ProcDump - RE/Malware analysis) */,
2810460305047003196UL /* procdump (ProcDump - RE/Malware analysis) */,
2032008861530788751UL /* processhacker (Process Hacker - RE/Malware analysis) */,
27407921587843457UL /* procexp64 (Process Explorer - RE/Malware analysis) */,
6491986958834001955UL /* procexp (Process Explorer - RE/Malware analysis) */,
(...)
7775177810774851294UL /* ramcapture64 (Ram Capturer - Forensics) */,
16130138450758310172UL /* ramcapture (Ram Capturer - Forensics) */,
```

This makes sense given how powerful [memory analysis](#) and [memory forensics](#) are in general, and memory imaging was also included as a [DHS emergency directive \(21-01\)](#). (Thanks to Andrew Case for sharing this on LinkedIn).

This emergency directive requires the following actions:

Agencies that have the expertise to take the following actions immediately must do so before proceeding to Action

a. Forensically image system memory and/or host operating systems hosting all instances of SolarWinds Orion vers

Although, memory was completely dismissed by the Microsoft DART team in their [Advice for incident responders on recovery from systemic identity compromises](#) blogpost:

After you validate that no persistence mechanisms created by the attacker exist or remain on your system, sched

**BEFORE** you validate persistence, you always want to create a Microsoft full memory crash dump of the system (with DumpIt or any other tools) before rebooting. As an incident responder, you should not omit any artifacts that

may be useful for your investigation.

And the last point, I would like to highlight was a very good [tweet from Kim Zetter](#):

Kim is highlighting a very important point here which is the lack of logging in the critical infrastructure industry. Two years ago, [we wrote about a new logging paradigm](#) which we believe should be in place for critical assets across industries where instead of relying on logs/events (that are often missing context and information) - to periodically make memory images (such as Microsoft full memory crash dumps) and to archive them to be able to retro-investigate critical incidents such as those that we have seen over the past years (DOUBLEPULSAR, SUNBURST etc.).

If you haven't read it yet, go ahead: <https://www.comae.com/posts/rethinking-logging-for-critical-assets/>.

We are more than happy to share thoughts on this.

If you are interested by our [memory analysis platform Comae Stardust](#) also feel free to reach out if you are interested in testing or a custom deployment instance.

---

Source: <https://www.comae.com/posts/sunburst-memory-analysis/>