SUNBURST & Memory Analysis

comae.com/posts/sunburst-memory-analysis/

Posted by *Matt Suiche* | Published on December 25, 2020

Categories: `apt` `stardust`
Tags: `solarwinds` `sunburst`
Reading time: 3 minutes. Table Of Contents:
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 perenniality.

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.

```
    136118141350725612 78UL     /* procdump64 (ProcDump - RE/Malware analysis) */,
    281046030504700319 6UL      /* procdump (ProcDump - RE/Malware analysis) */,
    203200886153078875 1UL      /* processhacker (Process Hacker - RE/Malware
analysis) */,
    27407921587843457UL         /* procexp64 (Process Explorer - RE/Malware analysis)
*/,
    649198695883400195 5UL      /* procexp (Process Explorer - RE/Malware analysis)
*/,
    (...)
    777517781077485129 4UL      /* ramcapture64 (Ram Capturer - Forensics) */,
    161301384507583101 72UL     /* 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 2. Agencies without this capability shall proceed to
Action 2.

a. Forensically image system memory and/or host operating systems hosting all
instances of SolarWinds Orion versions 2019.4 through 2020.2.1 HF1]. Analyze for new
user or service accounts, privileged or otherwise.
```

Although, memory was completly 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, schedule a restart. This can assist with removing memory
resident malware.
```

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:

> New: SolarWinds backdoor infected at least 15 entities in critical infrastructure incl electric/oil/gas/manufacture + 3 managed service providers for crit infr. No evidence hackers used backdoor to enter but may be difficult to tell due to lack of logging https://t.co/v3qnUMurEH
>
> — Kim Zetter (@KimZetter) December 24, 2020

Kim is highlighting a very important point here which is the lack of logging in the critical infrastucture 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.