[REDACTED] : GATOR Detection (11998)

InfoSec Analysis & Notes – 08/24/2017

Background

From malware.wikia.com/wiki/Claria_Corporation:

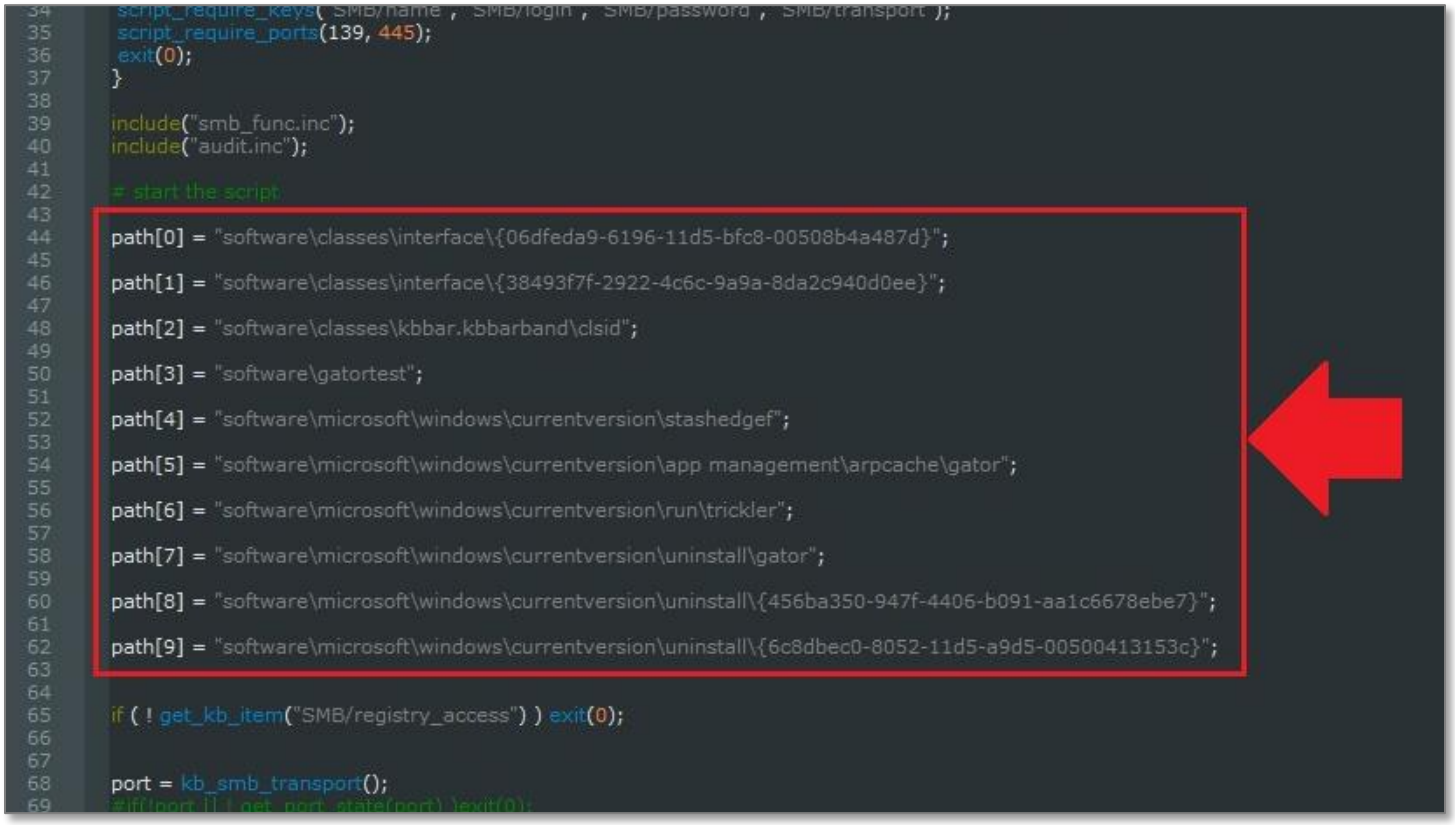
Claria Corporation (formerly known as Gator Corporation) was a media marketing software company based in Redwood City, California with products many considered spyware.

It was established in 1998 by Denis Coleman. Its name was often used interchangeably with its Gain advertising network, which it claimed serviced over 40 million users.

Claria exited the adware business at the end of second quarter 2006, and eventually shut down completely in October 2008. However, its software still remains installed on millions of PCs.

Analysis

Nessus plugin 11998 is for detecting GATOR malware. If we inspect the NASL file for this plugin, we can identify the criteria that is used to determine if there is a finding for this item:



We can see in the images above that it is looking for 10 specific registry keys. However, the issue with this Nessus plugin is that it does not give any output to help us see which of these keys were detected.

Using the information from the NASL file, we can create a small script to look for these same keys and help us identify 1) if a machine does indeed have signs of GATOR being installed and 2) which key or keys were found.

References

- https://www.tenable.com/plugins/index.php?view=single&id=11998
- https://vuldb.com/?id.89232
- https://nvd.nist.gov/vuln/detail/CVE-2002-0317
- http://www.securityfocus.com/bid/4161/info
- https://exchange.xforce.ibmcloud.com/signature/Spyware_Gator_Detected
- https://exchange.xforce.ibmcloud.com/vulnerabilities/12598
- https://marc.info/?l=bugtraq&m=101438671922874&w=2
- https://www.vulnerabilitycenter.com/#!vul=3464
- https://en.wikipedia.org/wiki/Claria_Corporation
- http://malware.wikia.com/wiki/Claria_Corporation
- http://www.pcpitstop.com/gator/default.asp
- http://www.pchell.com/support/gator.shtml
- https://malwaretips.com/blogs/adware-win32-gator-removal/