What is GootLoader?

gootloader.wordpress.com/2023/01/05/what-is-gootloader/

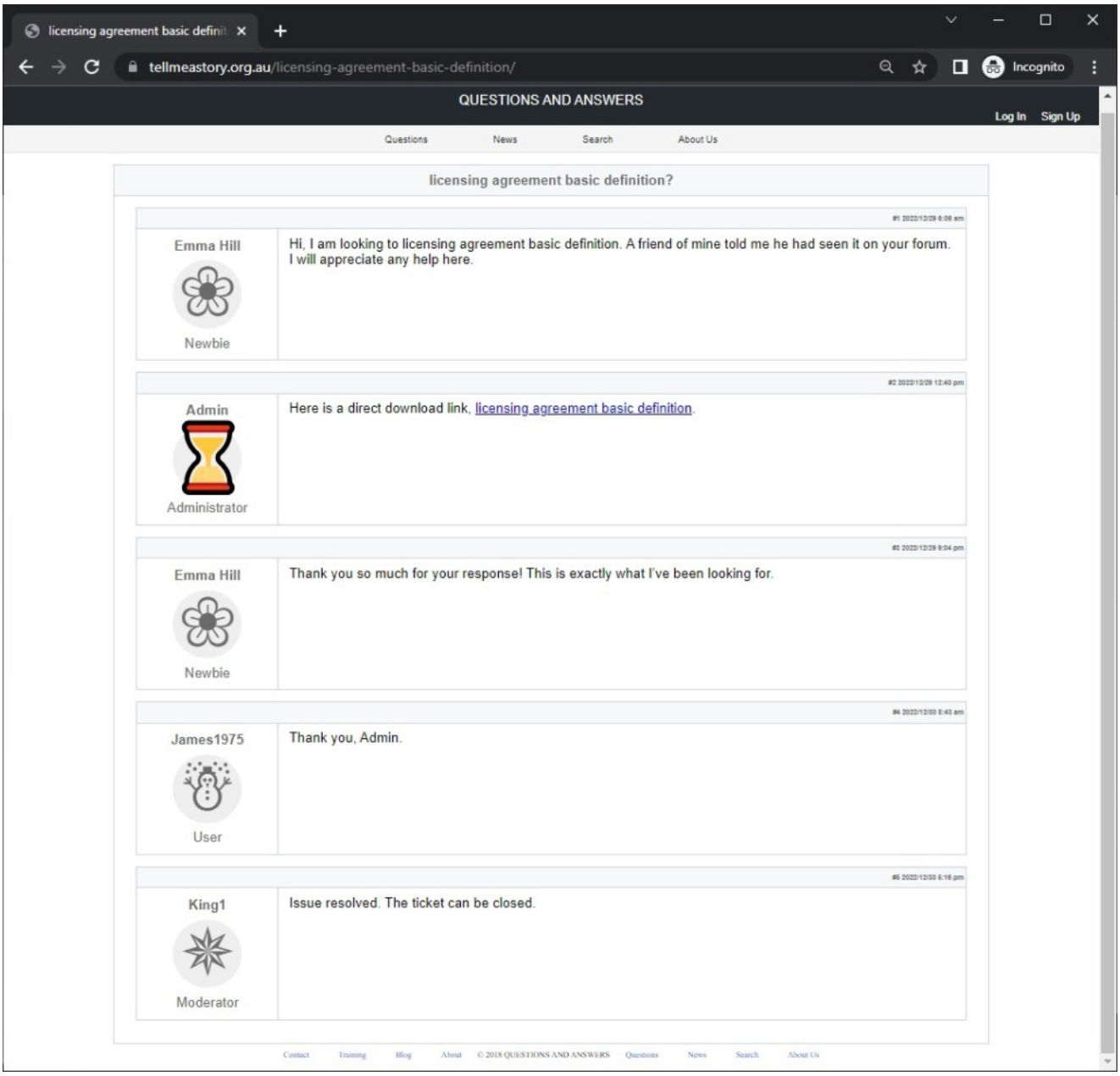
January 5, 2023

Gootloader is a malware that falls into the class of “Initial Access as a Service”. Basically, it infects a host (in this case Windows), maintains access, and (presumably) sells access for further compromise of the system and/or network.

Gootloader spreads via SEO poisoning (Search Engine Optimization), on compromised WordPress blogs, predominantly targeting “agreement/form/contract” type terms. Poisoned terms have been observed in Korean and French as well. In the past we have seen over a million terms be poisoned, across thousands of compromised blogs.

Gootloader has been around for a number of years and is constantly evolving to evade detection. But the behavior has hasn’t changed, that much, over the years.

A user searches for a term, ex: “licensing agreement basic definition” in Google or Bing and click on a compromised site. As long as they are visiting the site from a Windows computer, and an English-speaking country, the page will be redrawn to look like a forum, with a link of exactly what they searched for (see below).



When they click the link, a zip file will download, and inside of the zip file, a malicious .JS file resides. Currently (as of 5Jan2023), when the user runs the malicious .JS, it creates a scheduled task, and runs PowerShell code to call out to 10 domains with various info about the system.

Gootloader keeps calling out to these domains, waiting for code to run. The next stage is usually CobaltStrike, but that depends on who the access was passed off (or sold) to. Unfortunately, this has led to ransomware in many cases.