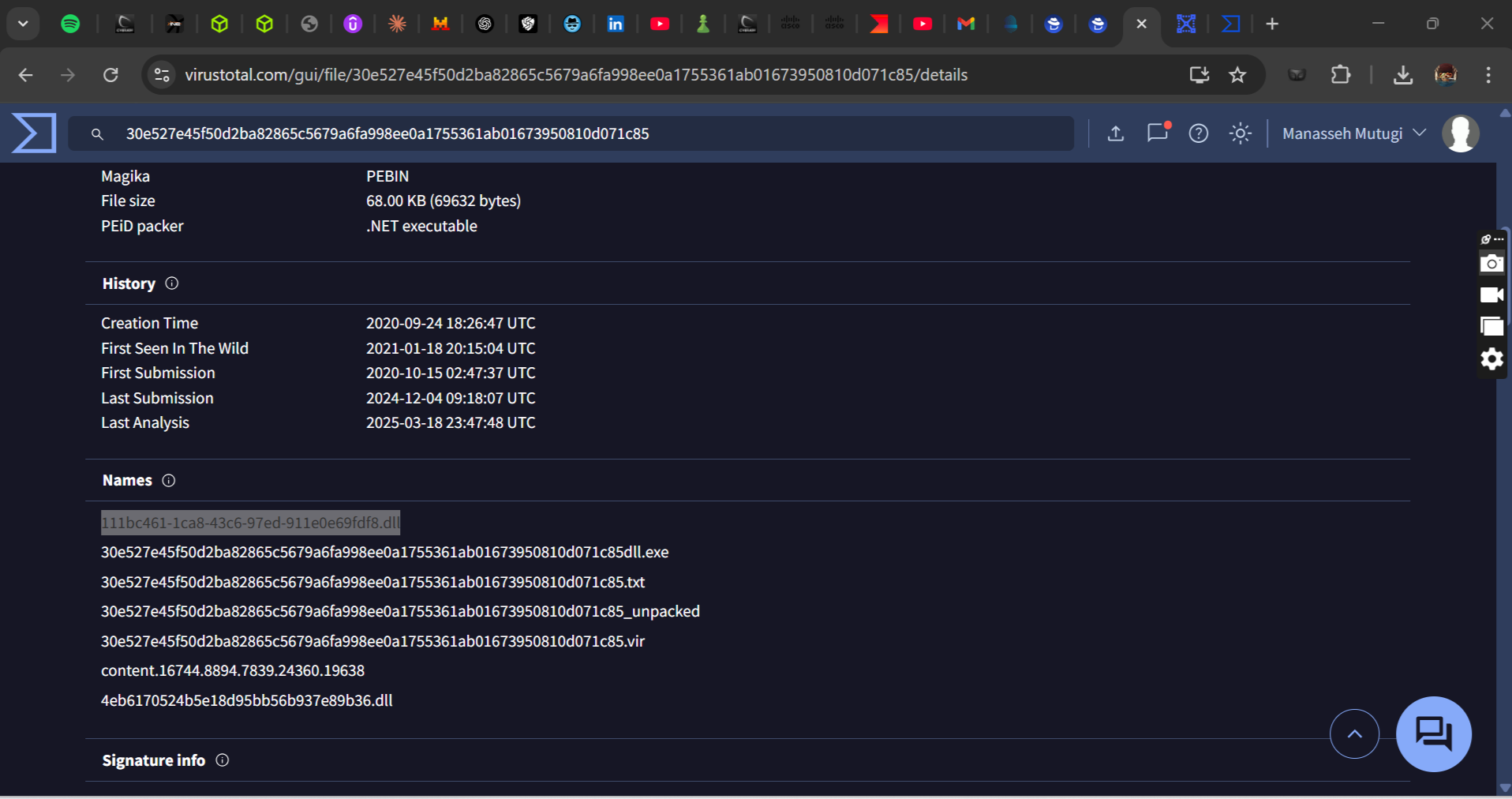
***During a regular IT security check at GlobalTech Industries, abnormal network traffic was detected from multiple workstations. Upon initial investigation, it was discovered that certain employees' search queries were being redirected to unfamiliar websites. This discovery raised concerns and prompted a more thorough investigation. Your task is to investigate this incident and gather as much information as possible.***

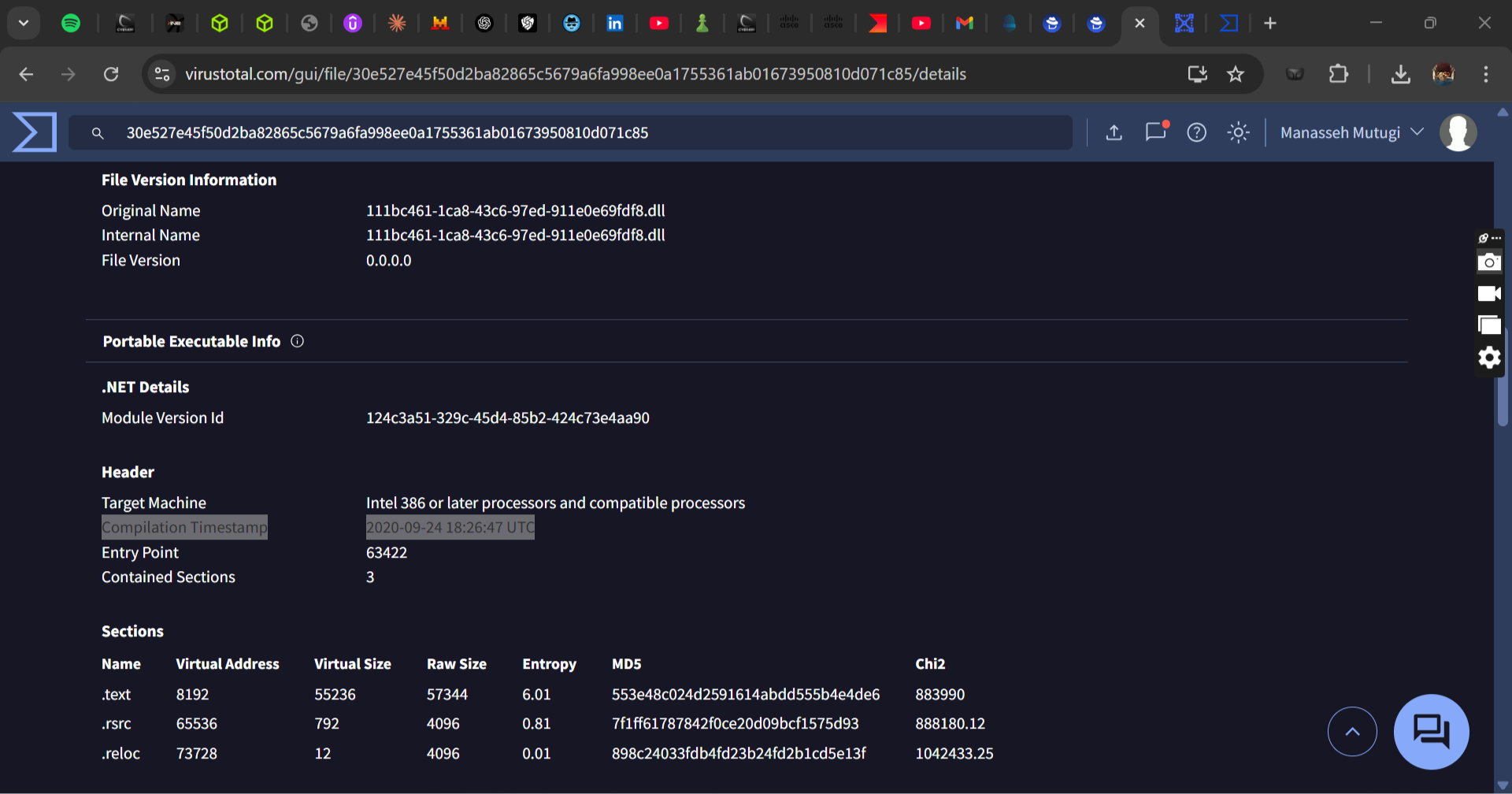
As part of our incident response, knowing common filenames the malware uses can help scan other workstations for potential infection. Upon uploading the hash on virusTotal, In the Details tab, look for the Names section.

**111bc461-1ca8-43c6-97ed-911e0e69fdf8.dll**



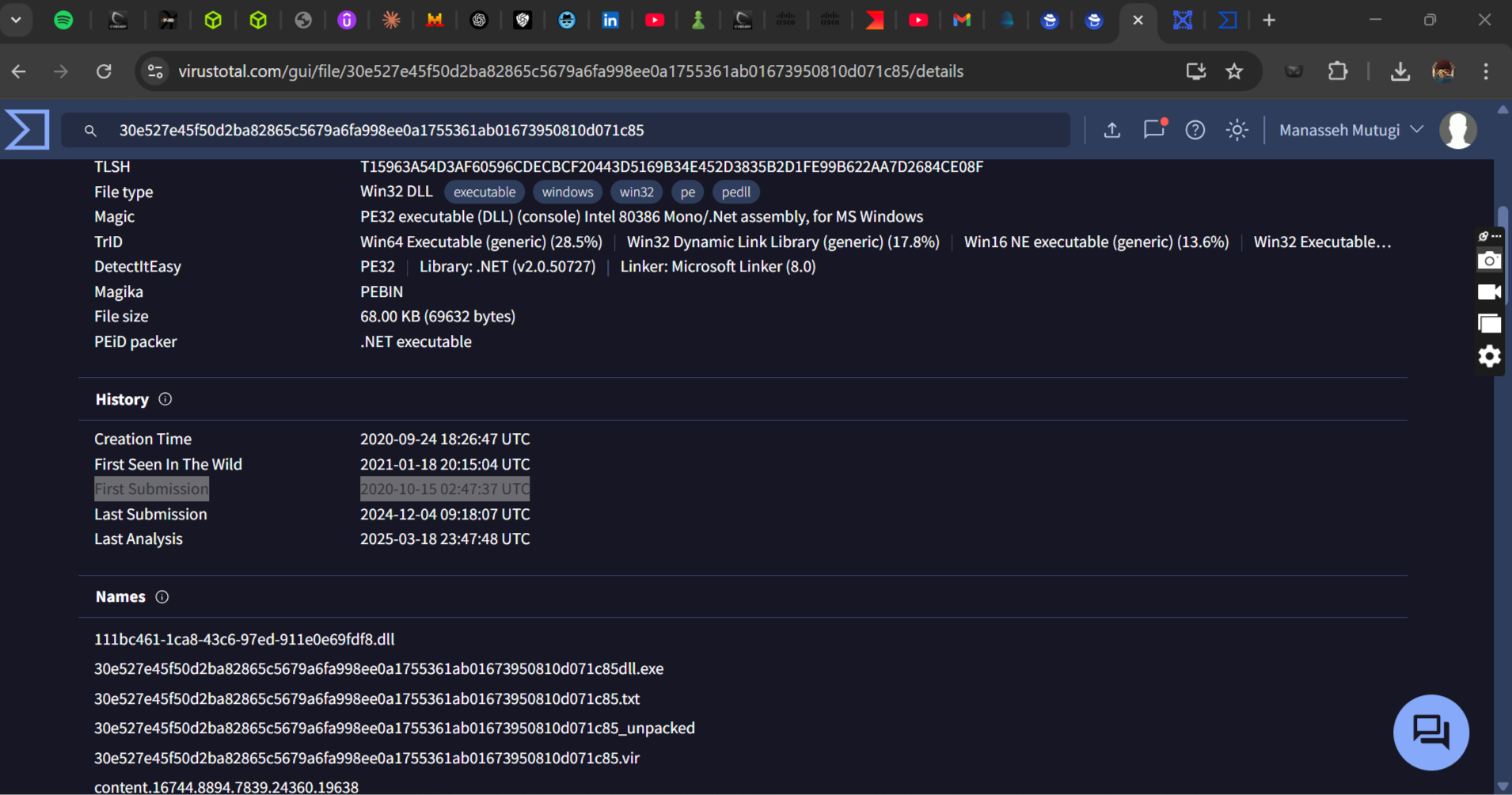
Determining the compilation timestamp of malware can reveal insights into its development and deployment timeline. In the Details tab, scroll down to the Portable Executable info section. Here, you will find the Compilation Timestamp which indicates when the malware was created.

**2020-09-24 18:26**



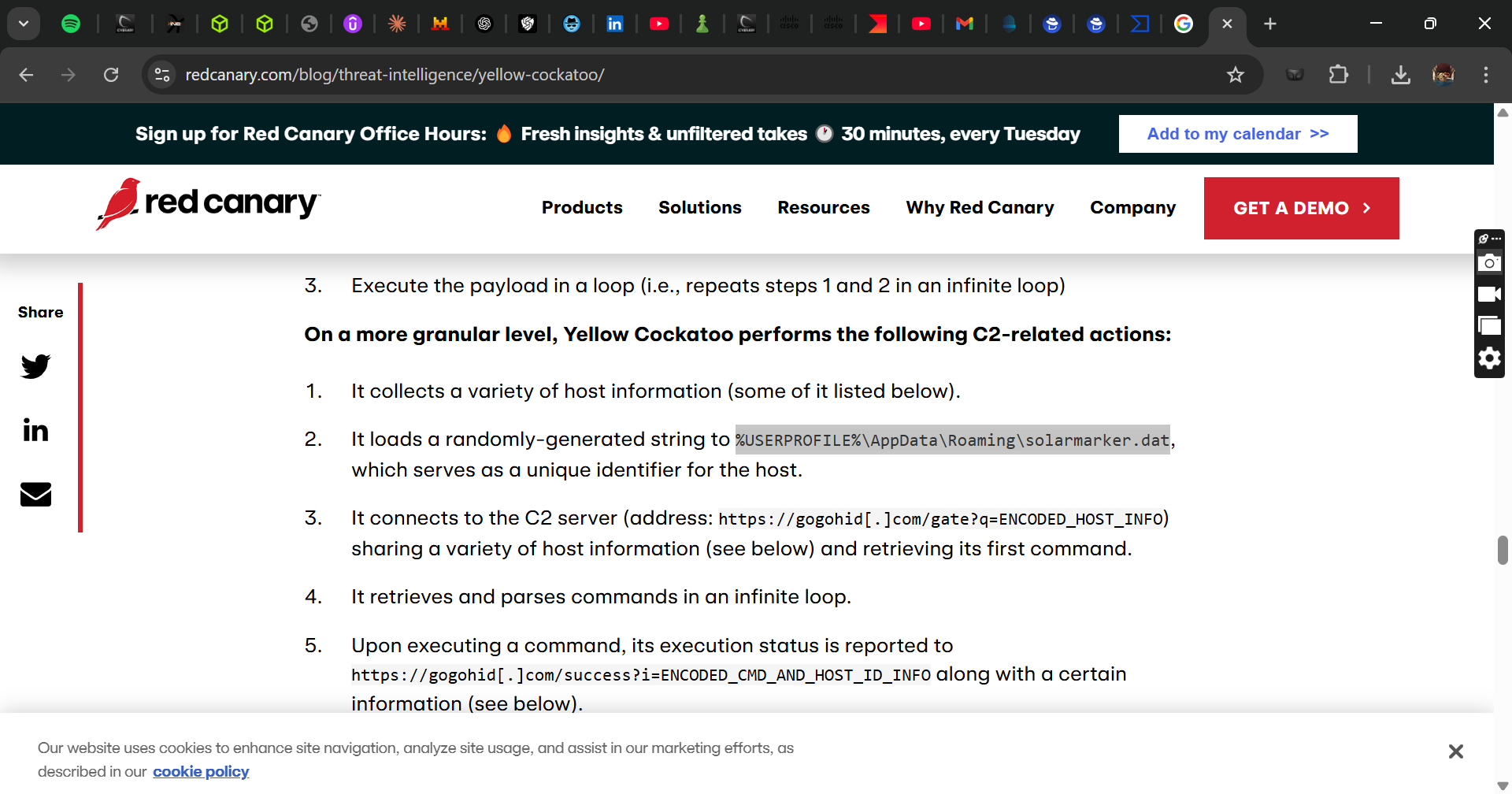
Understanding when the broader cybersecurity community first identified the malware could help determine how long the malware might have been in the environment before detection. In the Details tab, look for the First Submission date under the History section. This will tell you when the malware was first submitted to VirusTotal.

**2020-10-15 02:47**



To completely eradicate the threat from Industries' systems, we need to identify all components dropped by the malware. Review this Red Canary report for details on dropped files in the AppData folder: *https://redcanary.com/blog/threat-intelligence/yellow-cockatoo/*

**Solarmarker.dat**



It is crucial to identify the C2 servers with which the malware communicates to block its communication and prevent further data exfiltration. In the Behavior tab, go to the Activity Summary section and look under Network Communications Here, you'll find the Memory Pattern URLs which reveal the C2 server the malware is communicating with.

**https://gogohid.com**

