CyberDefenders: Yellow RAT

The following writeup is for Yellow RAT on CyberDefenders, it involves investigating a malware sample using VirusTotal (you are only provided the hash of the malware).

Scenario: 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.

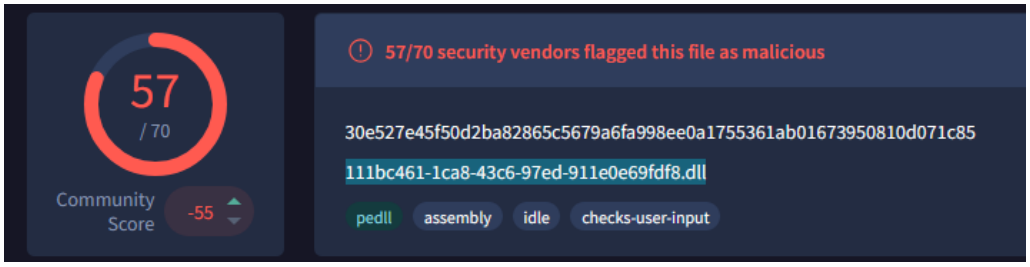
Understanding the adversary helps defend against attacks. What is the name of the malware family that causes abnormal network traffic?

Once you have entered the provided file hash into VirusTotal, you can navigate to the associations tab:

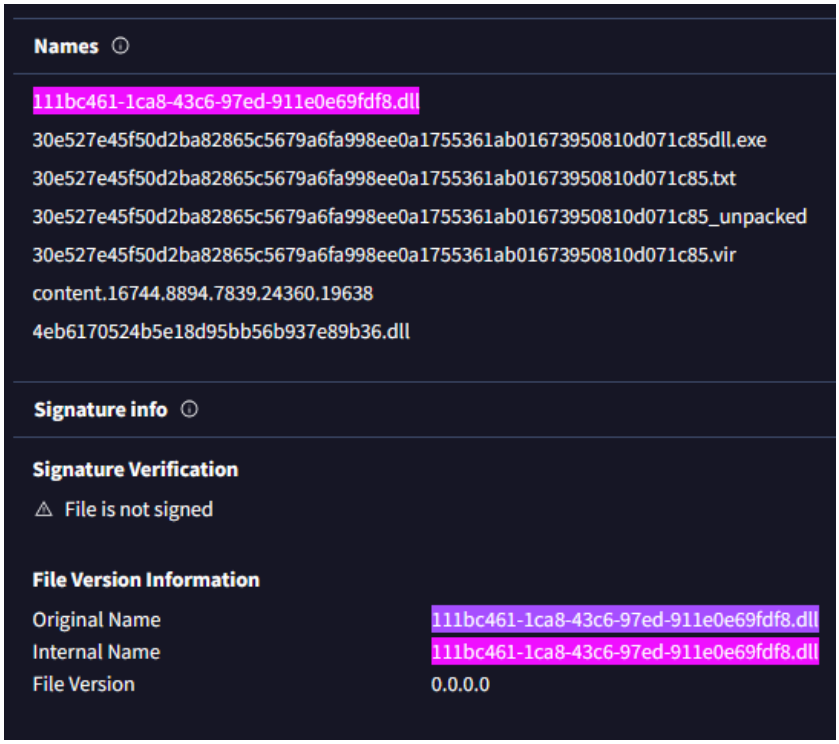
Here we can see several associations, however, the one of interest is Yellow Cockatoo RAT which is the answer.

As part of our incident response, knowing common filenames the malware uses can help scan other workstations for potential infection. What is the common filename associated with the malware discovered on our workstations?

There are several ways to identify common filenames associated with malware. The easiest way can be seen at the top of the screen next to the detection score:



You can also find the answer in the details tab:

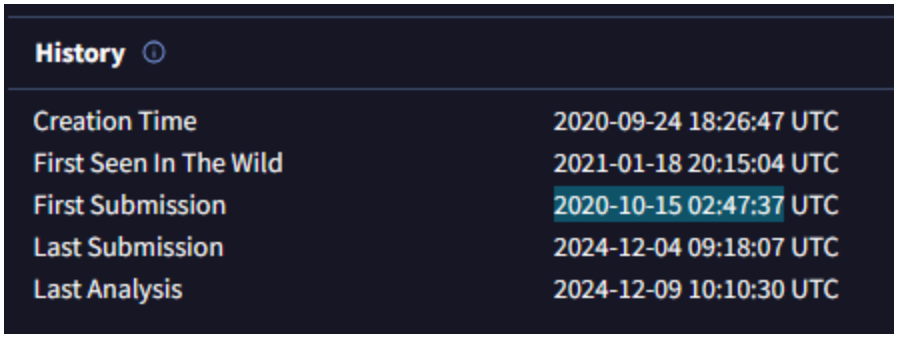


Determining the compilation timestamp of malware can reveal insights into its development and deployment timeline. What is the compilation timestamp of the malware that infected our network?

You can find the compilation timestamp in the Portable Execution Info section in the details tab:

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. When was the malware first submitted to VirusTotal?

This can also be found in the details tab:



To completely eradicate the threat from Indsutries' systems, we need to identify all components dropped by the mawalre. What is the name of the .dat file that the malware dropped in the AppData folder?

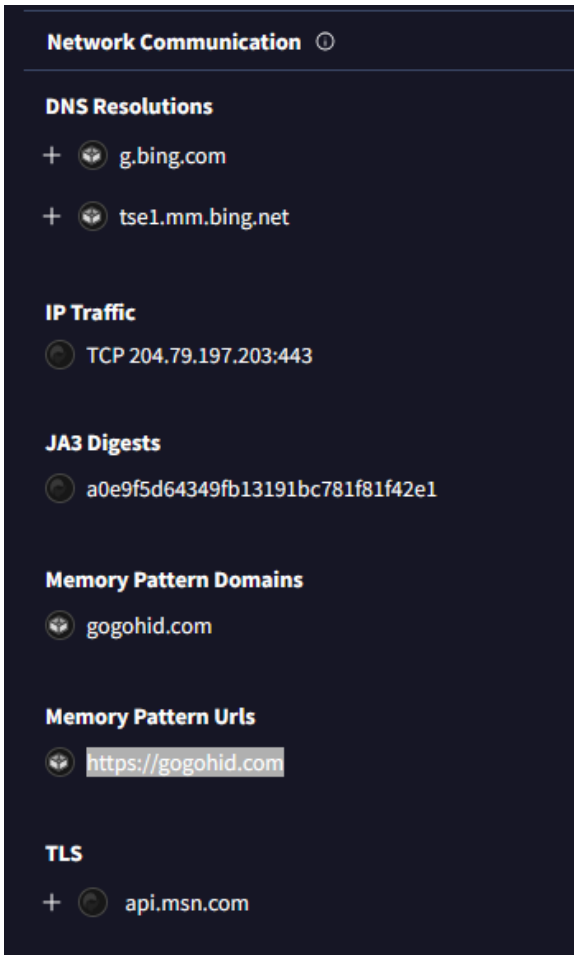
This required performing some external research. I was able to file a report by red canary that documents what .dat file was dropped in the AppData folder:

On a more granular level, Yellow Cockatoo performs the following C2-related actions:

1. It collects a variety of host information (some of it listed below).
2. It loads a randomly-generated string to `%USERPROFILE%\AppData\Roaming\solarmarker.dat`, which serves as a unique identifier for the host.
3. It connects to the C2 server (address: `https://gogohid[.]com/gate?q=ENCODED_HOST_INFO`) sharing a variety of host information (see below) and retrieving its first command.
4. It retrieves and parses commands in an infinite loop.
5. Upon executing a command, its execution status is reported to `https://gogohid[.]com/success?i=ENCODED_CMD_AND_HOST_ID_INFO` along with a certain information (see below).

It is crucial to identify the C2 servers with which the malware communicates to block its communication and prevent further data exfiltration. What is the C2 server that the malware is communicating with?

You can find the C2 domain by navigating to the Network Communication section in the behaviour tab:



This was a fun learning experience, although it is by no means an amazing lab experience. If, however, you have not used VirusTotal, this room is a great way to learn.