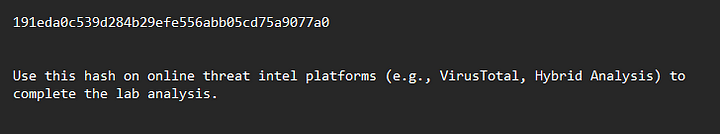
### **IcedID — CyberDefenders**

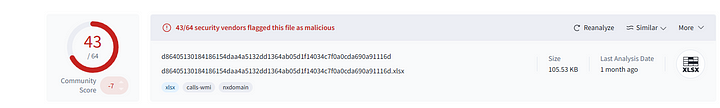
**Scenario:** A cyber threat group was identified for initiating widespread phishing campaigns to distribute further malicious payloads. The most frequently encountered payloads were IcedID. You have been given a hash of an IcedID sample to analyze and monitor the activities of this advanced persistent threat (APT) group.



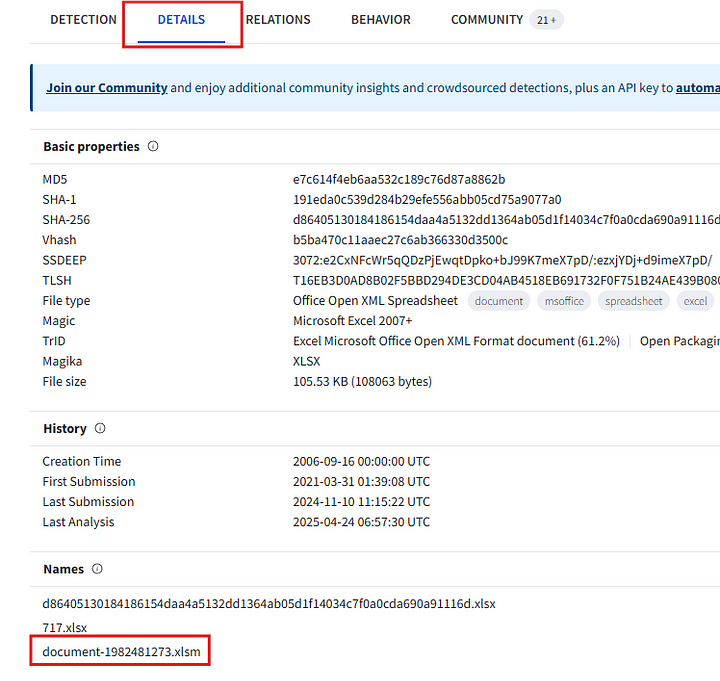
**TASKS**

1. **What is the name of the file associated with the given hash?**

Submit the hash to VirusTotal.



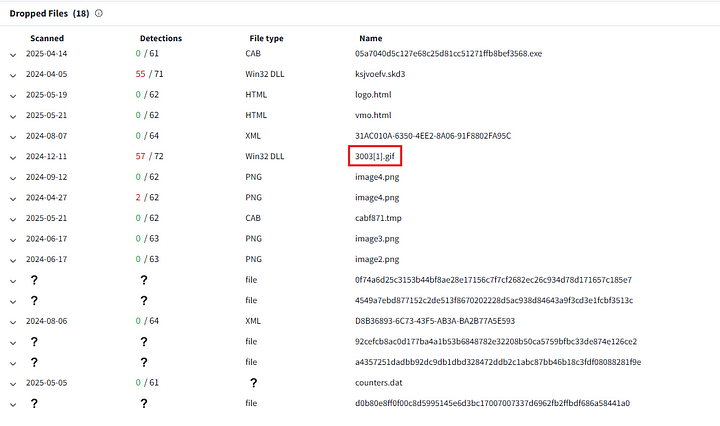
Now head to details tab to check the file name.



**Answer:** document-1982481273.xlsm

**2. Can you identify the filename of the GIF file that was deployed?**

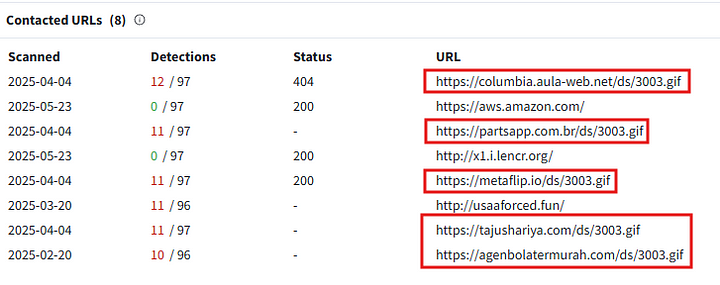
On VirusTotal, head to the “Relations” tab and look at dropped files section.



**Answer:** 3003.gif

**3. How many domains does the malware look to download the additional payload file in Q2?**

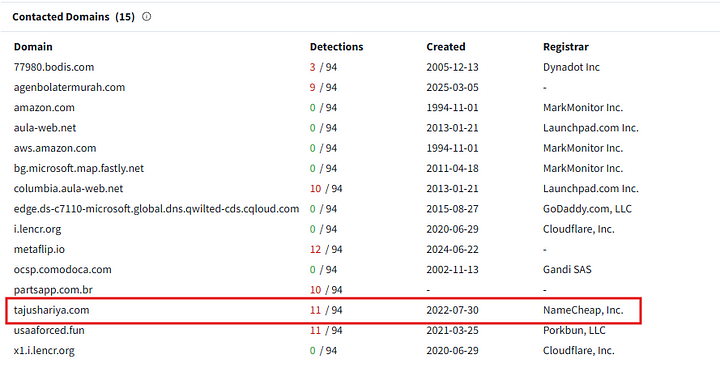
Under the Relations tab, we can look at the contacted URL’s, which download the above file.



**Answer:** 5

**4. From the domains mentioned in Q3, a DNS registrar was predominantly used by the threat actor to host their harmful content, enabling the malware’s functionality. Can you specify the Registrar INC?**

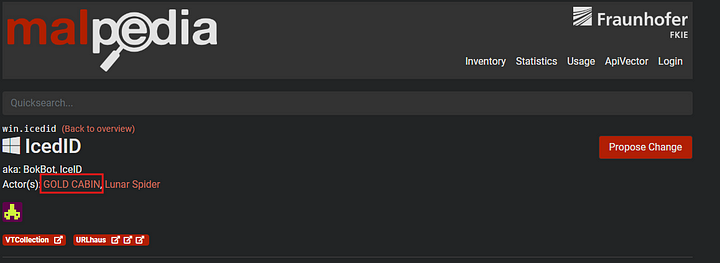
In the VirusTotal relations tab, check for the registrar name that has appeared most times for the above identified domains.



**Answer:** NAMECHEAP

**5. Could you specify the threat actor linked to the sample provided?**

Searching for IcedID on Malpedia gave a lot of reports relating to the malware. These reports contained the malware family.



**Answer:** Gold Cabin

**6. In the Execution phase, what function does the malware employ to fetch extra payloads onto the system?**

The report at<https://tria.ge/240417-nn49gaeh9t/behavioral1>, lists out the function used for fetching the extra payload.



**Answer:** URLDownloadToFileA

This is the end of the investigation.