

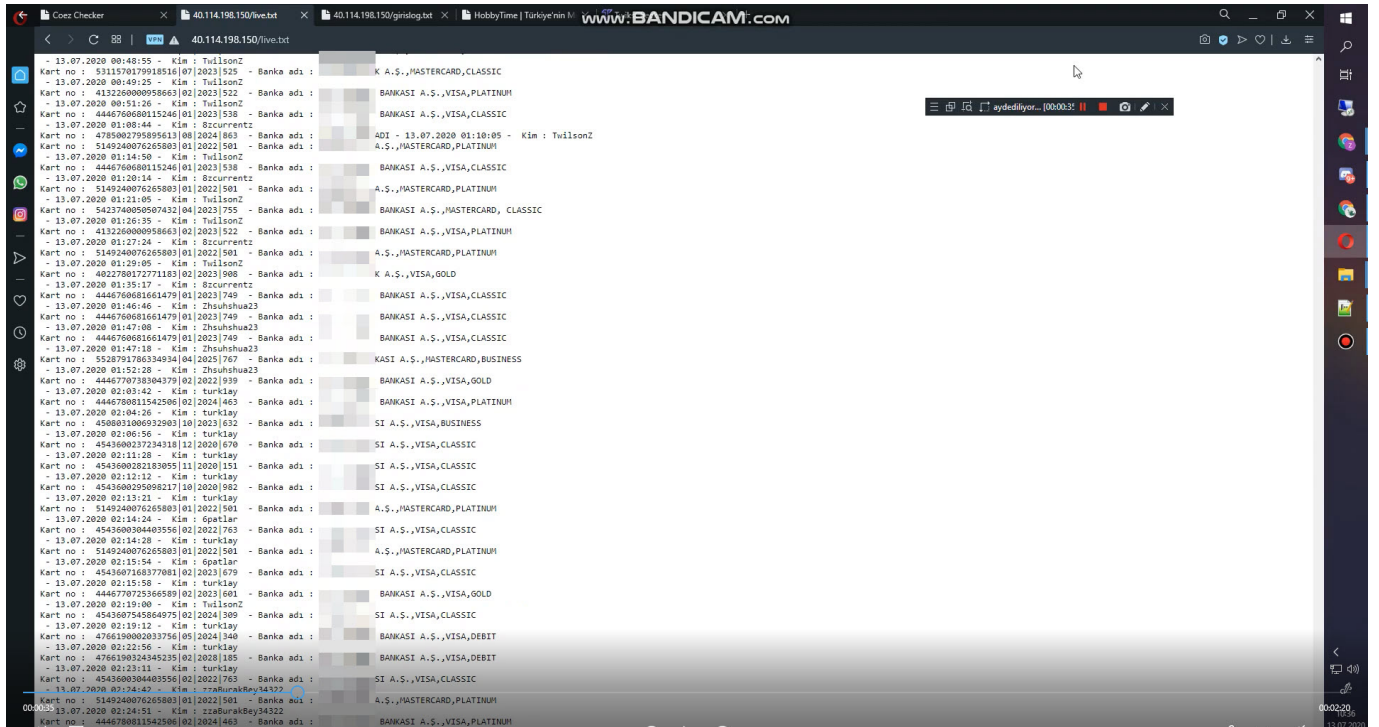
Stolen Credit Card Hunt

written by Mert SARICA | 1 March 2022

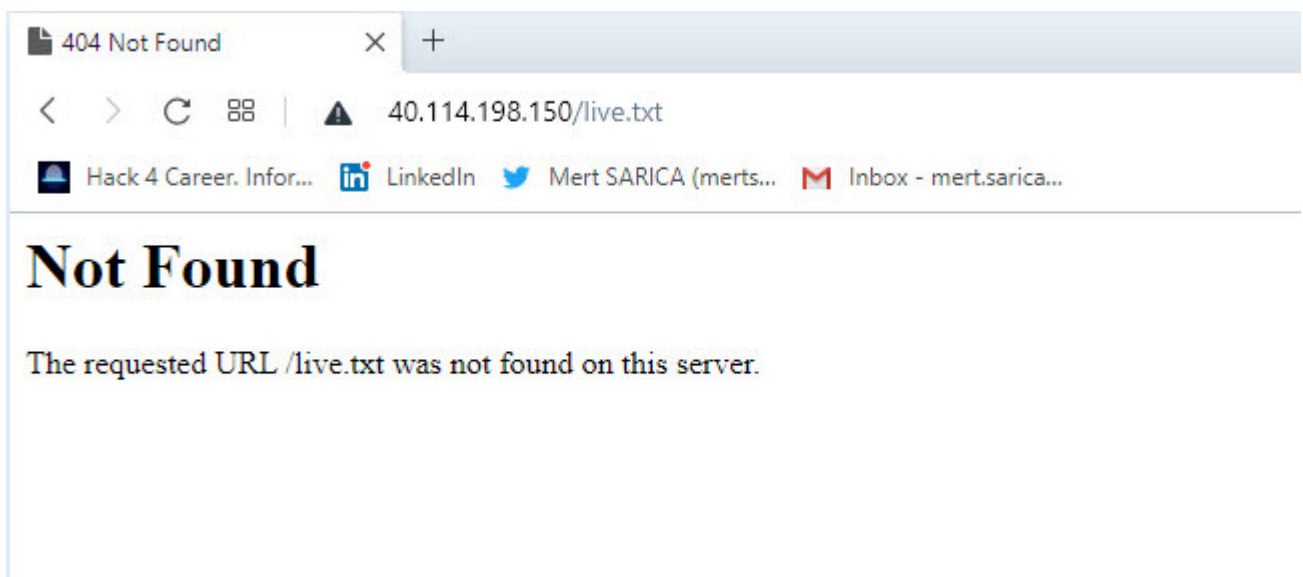
As a cybersecurity researcher who uses social media very effectively, you know that I have turned messages I have received through social networks and emails into security research, and then into articles and presentations. In this story, which has the same starting point as others, you can see how I benefited from a cyber threat intelligence received through a social network for the purpose of ensuring customer security.

As usual, on the morning of July 17, 2020, as soon as I woke up, I picked up my phone and started looking at my social media accounts to check cyber security news. A message from a person named Ebubekir BASTAMA on LinkedIn caught my attention, in which he tagged me in addition to banks. The message contained a video showing credit card information in plain sight and asked if they were canceled for customer security.





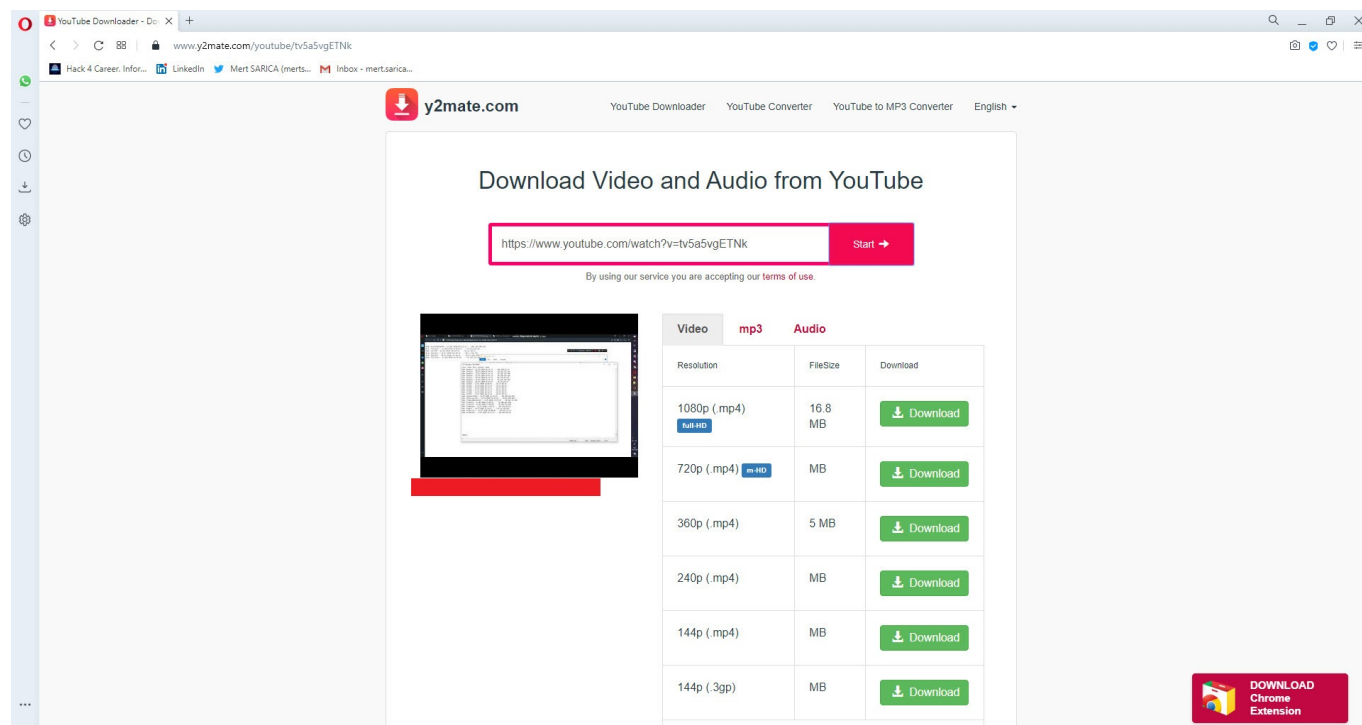
As I started watching the video, it seemed that a service called Coez Checker, which is used to check stolen cards, was hacked by scammers to message other scammers. The scammer showed the stolen card information registered on the system on July 13 for about 30 seconds of the approximately 3-minute video, and then ended the video recording after sending his message to other scammers. When I tried to access the address [http://40\[.\]114.198.150/live.txt](http://40[.]114.198.150/live.txt), where the stolen card information seen in the video is located, as I expected, the file had already been removed from the broadcast and I was left with only this video.



Thinking about how I could share the card information in this video with banks, including Banking Regulation and Supervision Agency (BRSA), in order

to prevent citizens from being victimized by scammers, I decided to split the video file into frames, and then analyze the image files with OCR, as I did in my blog post titled “Sponsored Scamming”, to reveal the card information. I remembered doing a similar study for the blog post titled “X Financial Institution – Animated Captcha (GIF)” in 2009.

First, I used the Y2mate YouTube Downloader website to download the relevant video file from YouTube.

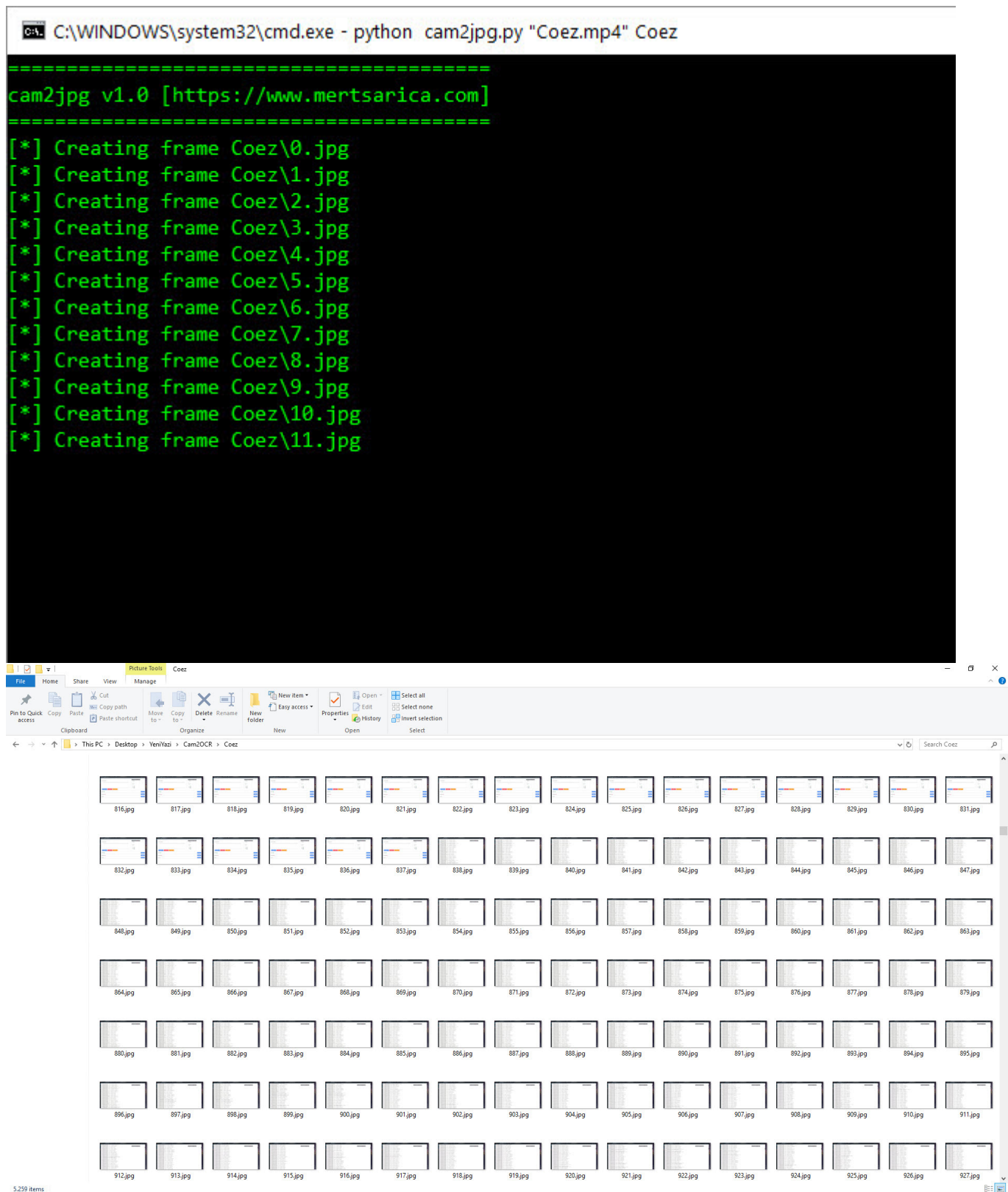


The screenshot shows the Y2mate website interface. At the top, there's a navigation bar with links to 'YouTube Downloader', 'YouTube Converter', and 'YouTube to MP3 Converter'. The main heading is 'Download Video and Audio from YouTube'. Below this, a text input field contains the URL 'https://www.youtube.com/watch?v=tv5a5vgETNk', and a red 'Start' button is to its right. A small disclaimer states, 'By using our service you are accepting our terms of use.' To the left of the download table is a video player showing a blurred screenshot of a document. The table on the right lists various download options:

Video	mp3	Audio
Resolution	FileSize	Download
1080p (.mp4) Full HD	16.8 MB	Download
720p (.mp4) HD	MB	Download
360p (.mp4)	5 MB	Download
240p (.mp4)	MB	Download
144p (.mp4)	MB	Download
144p (.3gp)	MB	Download

At the bottom right, there is a red button that says 'DOWNLOAD Chrome Extension'.

I developed and downloaded a tool called Cam2Jpg that splits the specified video file into frames and saves them in JPEG format, and when I ran it on the downloaded video file, it produced more than 5000 image files.



This time, using Python and the Python-tesseract project, I developed another tool called Jpg20cr (I decided not to publish the tool to prevent it from being misused) that analyzes the image files and detects credit card numbers. When I ran this tool on the image files, it produced more than 1000 credit card numbers in a short time.

```
C:\WINDOWS\system32\cmd.exe - python jpg2ocr.py Coez
jpg2ocr v1.0 [https://www.mertsarica.com]
[+] Applying OCR on 0.jpg
[+] Applying OCR on 1.jpg
[+] Applying OCR on 10.jpg
[+] Applying OCR on 100.jpg
[+] Applying OCR on 1000.jpg
[*] Credit card number: 4446760694310692
[*] Credit card number: 4446760696440984
[*] Credit card number: 4446760731314681
[*] Credit card number: 4446770724063187
[*] Credit card number: 4446770730100981
[*] Credit card number: 5430810019891002
[*] Credit card number: 4446770737876559
[*] Credit card number: 5406681295479337
[*] Credit card number: 5406681491188187
[*] Credit card number: 5423740040829847
[*] Credit card number: 5423740048522733
[*] Credit card number: 5423740083562024
[*] Credit card number: 5458470125658675
[*] Credit card number: 5423740085489044
[*] Credit card number: 5423740040829847
[*] Credit card number: 5406681086005341
[*] Credit card number: 5423740040829847
[*] Credit card number: 5423740085489044
[*] Credit card number: 5423740085489044
[+] Applying OCR on 1001.jpg
```

Feeling a sense of responsibility and happiness for preventing more of our citizens from being victimized by sharing all of the credit card information I obtained with the authorities on the same day, I completed another security research.

It is always useful to closely monitor social networks on your own, even if you benefit from one or more cyber threat intelligence services, in case the intelligence does not arrive or arrives late.

Hope to see you in the following articles.