

Çalıntı Kart Avı

written by Mert SARICA | 1 March 2022

If you are looking for an English version of this article, please visit here.

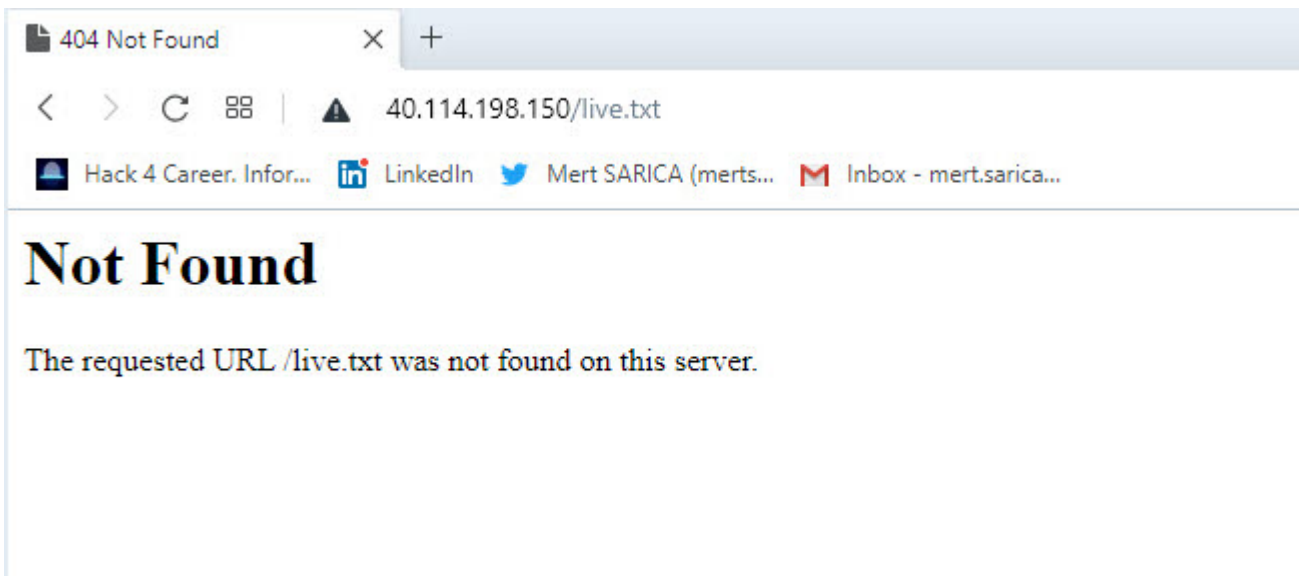
Sosyal medyayı oldukça etkin kullanan bir güvenlik arařtırmacısı olarak bu zamana dek sosyal aęlar, e-postalar üzerinden aldığım mesajları güvenlik arařtırmalarına ve ardından blog yazılarına, sunumlara çevirdiğimi biliyorsunuzdur. Çıkıř noktası dięerleri ile aynı olan bu hikayede ise müşteri güvenliğini saęlamak amacıyla sosyal aę üzerinden gelen bir siber tehdit istihbaratından nasıl faydalandığımı görebilirsiniz.

Her sabah olduęu gibi 17 Temmuz 2020 sabahı da uyandıktan hemen sonra telefonumu elime alıp siber güvenlik haberlerine göz atmak için sosyal medya hesaplarıma göz atmaya başladım. LinkedIn üzerinde Ebubekir BASTAMA isimli bir kiřinin bankalar dıřında beni de etiketledięi bir mesaj dikkatimi çekti. Mesajında bir videoda yer alan ve açık halde görülen kredi kartı bilgilerinin yer aldığını ve müşteri güvenlięi adına bunların iptal edilip edilmediğini merak ediyordu.



```
13.07.2020 00:40:55 - Kim : Tuilson2
Kart no : 5311570179918516|07|2023|525 - Banka adı : K A.S.,MASTERCARD,CLASSIC
13.07.2020 00:40:25 - Kim : Tuilson2
Kart no : 413226000958663|02|2023|522 - Banka adı : BANKASI A.S.,VISA,PLATINUM
13.07.2020 00:51:26 - Kim : Tuilson2
Kart no : 4446760680115246|01|2023|538 - Banka adı : BANKASI A.S.,VISA,CLASSIC
13.07.2020 01:10:44 - Kim : Tuilson2
Kart no : 4785802795895613|08|2024|863 - Banka adı : ADI - 13.07.2020 01:10:05 - Kim : Tuilson2
Kart no : 5149240076265803|01|2022|501 - Banka adı : A.S.,MASTERCARD,PLATINUM
13.07.2020 01:14:50 - Kim : Tuilson2
Kart no : 4446760680115246|01|2023|538 - Banka adı : BANKASI A.S.,VISA,CLASSIC
13.07.2020 01:20:14 - Kim : Sccurrentz
Kart no : 5149240076265803|01|2022|501 - Banka adı : A.S.,MASTERCARD,PLATINUM
13.07.2020 01:21:05 - Kim : Tuilson2
Kart no : 542374009507432|04|2023|755 - Banka adı : BANKASI A.S.,MASTERCARD, CLASSIC
13.07.2020 01:25:17 - Kim : Sccurrentz
Kart no : 5149240076265803|01|2022|501 - Banka adı : BANKASI A.S.,VISA,PLATINUM
13.07.2020 01:27:24 - Kim : Sccurrentz
Kart no : 413226000958663|02|2023|522 - Banka adı : BANKASI A.S.,VISA,PLATINUM
13.07.2020 01:29:05 - Kim : Tuilson2
Kart no : 4022780172771183|02|2023|908 - Banka adı : K A.S.,VISA,GOLD
13.07.2020 01:31:57 - Kim : Sccurrentz
Kart no : 4446760681661479|01|2023|749 - Banka adı : BANKASI A.S.,VISA,CLASSIC
13.07.2020 01:46:46 - Kim : Zhsuhshua23
Kart no : 4446760681661479|01|2023|749 - Banka adı : BANKASI A.S.,VISA,CLASSIC
13.07.2020 01:47:08 - Kim : Zhsuhshua23
Kart no : 4446760681661479|01|2023|749 - Banka adı : BANKASI A.S.,VISA,CLASSIC
13.07.2020 01:47:10 - Kim : Zhsuhshua23
Kart no : 4446760681661479|01|2023|749 - Banka adı : BANKASI A.S.,VISA,CLASSIC
13.07.2020 01:47:10 - Kim : Zhsuhshua23
Kart no : 4446760681661479|01|2023|749 - Banka adı : BANKASI A.S.,VISA,CLASSIC
13.07.2020 01:52:28 - Kim : Zhsuhshua23
Kart no : 5528791786334934|04|2025|767 - Banka adı : KASI A.S.,MASTERCARD,BUSINESS
13.07.2020 01:52:28 - Kim : Zhsuhshua23
Kart no : 4446760681661479|01|2023|749 - Banka adı : BANKASI A.S.,VISA,CLASSIC
13.07.2020 01:52:28 - Kim : Zhsuhshua23
Kart no : 4446760681661479|01|2023|749 - Banka adı : BANKASI A.S.,VISA,CLASSIC
13.07.2020 02:04:26 - Kim : turkiyay
Kart no : 4580831006932903|10|2023|632 - Banka adı : SI A.S.,VISA,BUSINESS
13.07.2020 02:06:56 - Kim : turkiyay
Kart no : 4543600295098217|10|2020|982 - Banka adı : SI A.S.,VISA,CLASSIC
13.07.2020 02:11:28 - Kim : turkiyay
Kart no : 4543600295098217|10|2020|982 - Banka adı : SI A.S.,VISA,CLASSIC
13.07.2020 02:12:12 - Kim : turkiyay
Kart no : 4543600295098217|10|2020|982 - Banka adı : SI A.S.,VISA,CLASSIC
13.07.2020 02:13:21 - Kim : turkiyay
Kart no : 4543600295098217|10|2020|982 - Banka adı : SI A.S.,VISA,CLASSIC
13.07.2020 02:14:24 - Kim : 6patlar
Kart no : 5149240076265803|01|2022|501 - Banka adı : A.S.,MASTERCARD,PLATINUM
13.07.2020 02:14:24 - Kim : 6patlar
Kart no : 454360030403556|02|2022|763 - Banka adı : SI A.S.,VISA,CLASSIC
13.07.2020 02:14:28 - Kim : turkiyay
Kart no : 454360030403556|02|2022|763 - Banka adı : SI A.S.,VISA,CLASSIC
13.07.2020 02:15:54 - Kim : 6patlar
Kart no : 5149240076265803|01|2022|501 - Banka adı : A.S.,MASTERCARD,PLATINUM
13.07.2020 02:15:58 - Kim : turkiyay
Kart no : 454360030403556|02|2022|763 - Banka adı : SI A.S.,VISA,CLASSIC
13.07.2020 02:15:58 - Kim : turkiyay
Kart no : 444677072566689|02|2023|601 - Banka adı : BANKASI A.S.,VISA,GOLD
13.07.2020 02:19:00 - Kim : Tuilson2
Kart no : 4543607545864975|02|2024|309 - Banka adı : SI A.S.,VISA,CLASSIC
13.07.2020 02:19:12 - Kim : turkiyay
Kart no : 476619002033761|05|2024|340 - Banka adı : BANKASI A.S.,VISA,DEBIT
13.07.2020 02:22:56 - Kim : turkiyay
Kart no : 476619002033761|05|2024|340 - Banka adı : BANKASI A.S.,VISA,DEBIT
13.07.2020 02:23:13 - Kim : turkiyay
Kart no : 476619002033761|05|2024|340 - Banka adı : BANKASI A.S.,VISA,DEBIT
13.07.2020 02:23:13 - Kim : turkiyay
Kart no : 454360030403556|02|2022|763 - Banka adı : SI A.S.,VISA,CLASSIC
13.07.2020 02:24:42 - Kim : zzaBurakRey34322
Kart no : 5149240076265803|01|2022|501 - Banka adı : A.S.,MASTERCARD,PLATINUM
13.07.2020 02:24:51 - Kim : zzaBurakRey34322
Kart no : 5149240076265803|01|2022|501 - Banka adı : A.S.,MASTERCARD,PLATINUM
13.07.2020 02:24:51 - Kim : zzaBurakRey34322
Kart no : 4446780811542506|02|2024|463 - Banka adı : BANKASI A.S.,VISA,PLATINUM
```

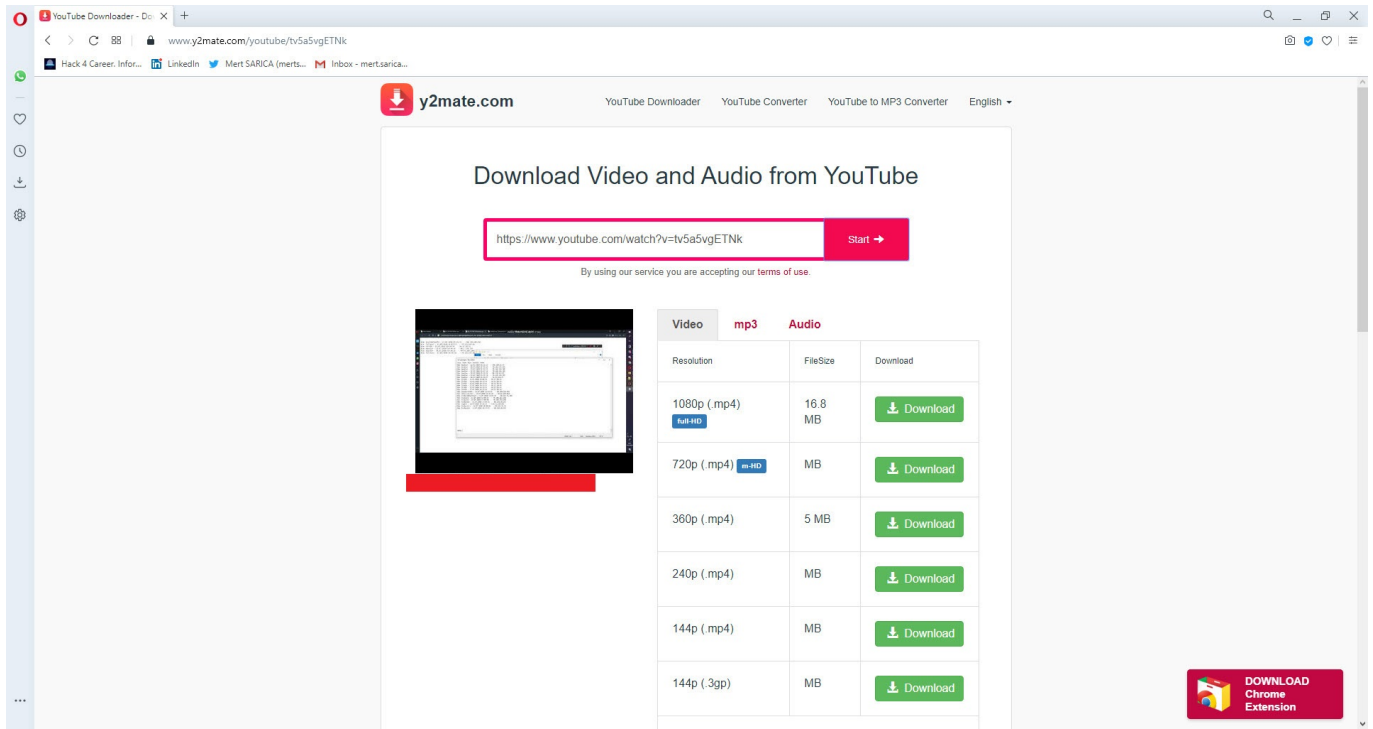
Videoyu izlemeye başladığımda Coez Checker isimli çalıntı kartları kontrol etmek amacıyla kullanılan bir servisin dolandırıcılar tarafından diğer dolandırıcılara mesaj vermek amacıyla hacklendiği anlaşılıyordu. Dolandırıcı, yaklaşık 3 dakikalık videonun 30 saniyesi boyunca sistem üzerinde kayıtlı olan 13 Temmuz tarihli çalıntı kart bilgilerini gösteriyor ve ardından diğer dolandırıcılara mesajını ilettikten sonra video kaydı sonlanıyordu. Videoda görünen çalıntı kart bilgilerinin yer aldığı [http://40\[.\]114.198.150/live.txt](http://40[.]114.198.150/live.txt) adresine ulaşmak istediğimde ise tahmin ettiğim üzere dosya çoktan yayından kaldırılmıştı ve elimde sadece bu video ile kalakalmıştım.



Vatandaşların dolandırıcılar tarafından mağdur edilmemesi adına bu videodaki kart bilgilerini başta Sektörel SOME/BDDK olmak üzere bankalarla da paylaşmak

için videodan nasıl elde edebileceğimi düşünmeye başladım. 2009 yılında X Finans Kuruluşu – Animated Captcha (GIF) başlık blog yazım için benzer bir çalışma yaptığımı anımsayarak bu defa video dosyasını karelere (frame) ayırmaya ardından da Sponsorlu Dolandırıcılık başlıklı blog yazımda olduğu gibi görüntü dosyalarını OCR ile analiz edip kart bilgilerini ortaya çıkarmaya karar verdim.

İlk iş olarak Y2mate YouTube Downloader web sitesinden faydalanarak Youtube üzerinden ilgili video dosyasını indirdim.



The screenshot shows the Y2mate website interface. At the top, there is a navigation bar with the Y2mate logo and links for 'YouTube Downloader', 'YouTube Converter', 'YouTube to MP3 Converter', and 'English'. The main heading is 'Download Video and Audio from YouTube'. Below this, there is a search bar containing the URL 'https://www.youtube.com/watch?v=lv5a5vgETNk' and a 'Start' button. A small disclaimer states 'By using our service you are accepting our terms of use.' Below the search bar, there is a video player thumbnail showing a video frame. To the right of the thumbnail is a table of download options for video and audio.

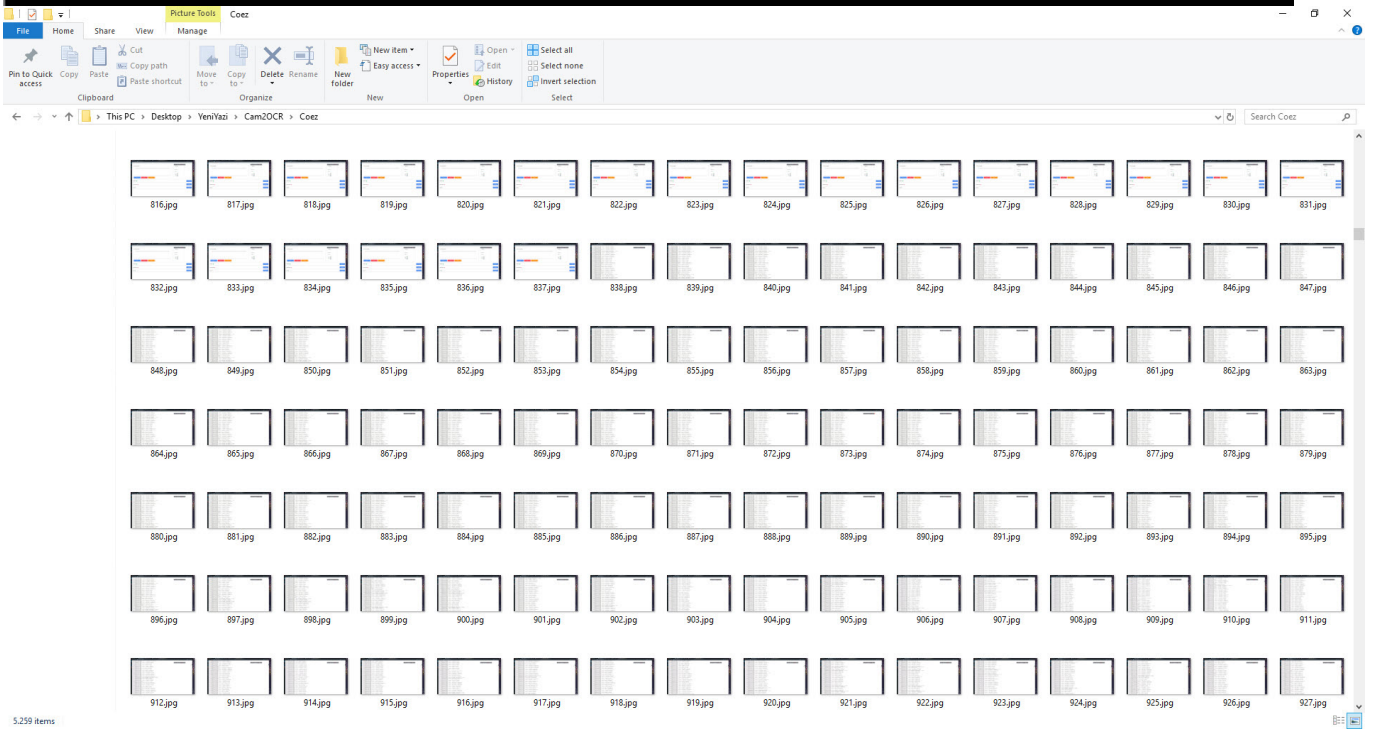
Video	mp3	Audio
Resolution	File Size	Download
1080p (.mp4) <small>Full HD</small>	16.8 MB	Download
720p (.mp4) <small>HD</small>	MB	Download
360p (.mp4)	5 MB	Download
240p (.mp4)	MB	Download
144p (.mp4)	MB	Download
144p (.3gp)	MB	Download

Python ile belirtilen video dosyasını karelere ayırıp, JPEG dosya biçiminde saklayan Cam2Jpg isimli bir araç geliştirip indirdiğim video dosyası üzerinde çalıştırdığımda ortaya 5000'den fazla görüntü dosyası çıktı.

C:\WINDOWS\system32\cmd.exe - python cam2jpg.py "Coez.mp4" Coez

```
=====  
cam2jpg v1.0 [https://www.mertsarica.com]  
=====
```

```
[*] Creating frame Coez\0.jpg  
[*] Creating frame Coez\1.jpg  
[*] Creating frame Coez\2.jpg  
[*] Creating frame Coez\3.jpg  
[*] Creating frame Coez\4.jpg  
[*] Creating frame Coez\5.jpg  
[*] Creating frame Coez\6.jpg  
[*] Creating frame Coez\7.jpg  
[*] Creating frame Coez\8.jpg  
[*] Creating frame Coez\9.jpg  
[*] Creating frame Coez\10.jpg  
[*] Creating frame Coez\11.jpg
```



Bu defa Python ile Python-tesseract projesinden faydalanarak görüntü dosyalarını analiz edip, kredi kartı numaralarını tespit eden Jpg2ocr (kötüye kullanılmaması adına aracı yayınlamama kararı aldım) isimli başka bir araç daha geliştirdim. Bu aracı görüntü dosyaları üzerinde çalıştırdığımda kısa süre içinde 1000'den fazla kredi kartı numarası ortaya çıkmış oldu.

```
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
```

Elde ettiğim tüm kredi kartı bilgilerini aynı gün içinde yetkili mercilerle paylaşarak daha fazla vatandaşımızın mağdur olmasını engellemenin verdiği sorumluluk bilinci ve mutluluk ile bir güvenlik araştırmamı daha tamamlamış oldum.

Kurum olarak bir veya birden fazla siber tehdit istihbaratı servisinden faydalansanız da istihbaratın gelmemesi veya gecikmeli gelmesi durumlarına karşı kendi imkanlarınızla da sosyal ağları yakından takip etmenizde her zaman fayda olacaktır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.