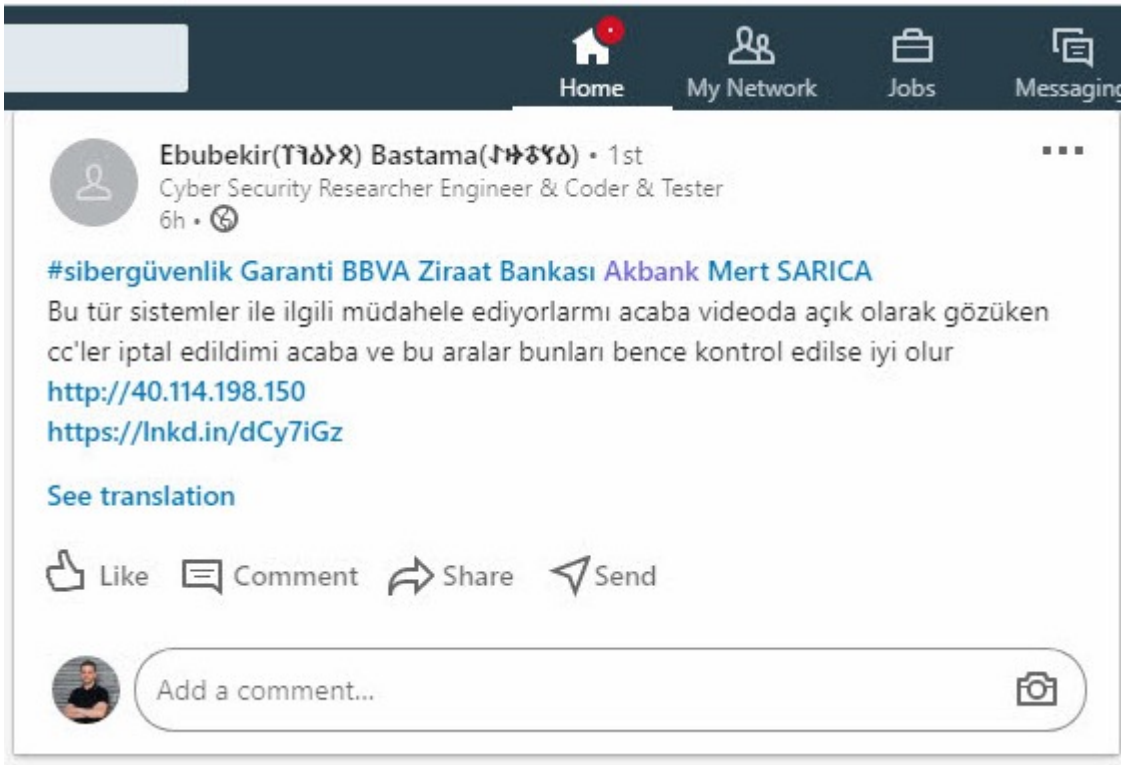
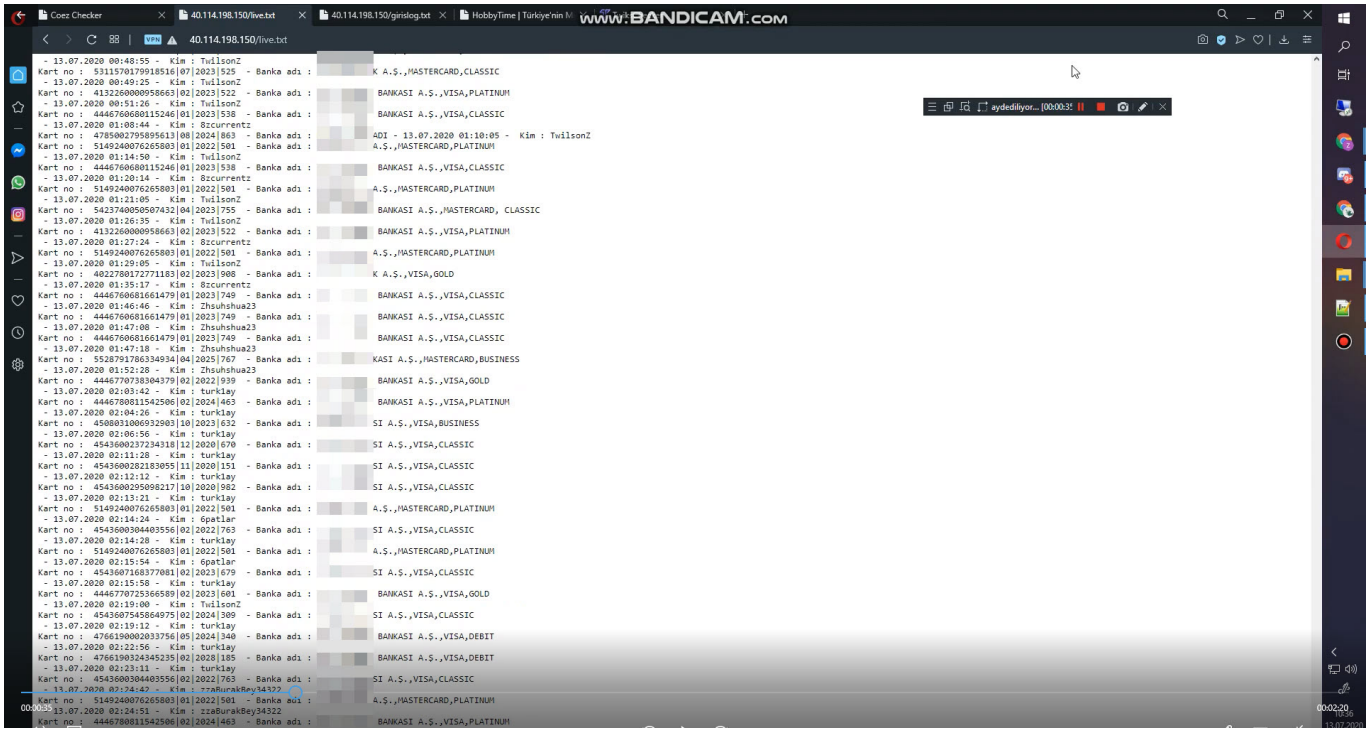
Çalıntı Kart Avı

written by Mert SARICA | 1 March 2022
If you are looking for an English version of this article, please visit here.

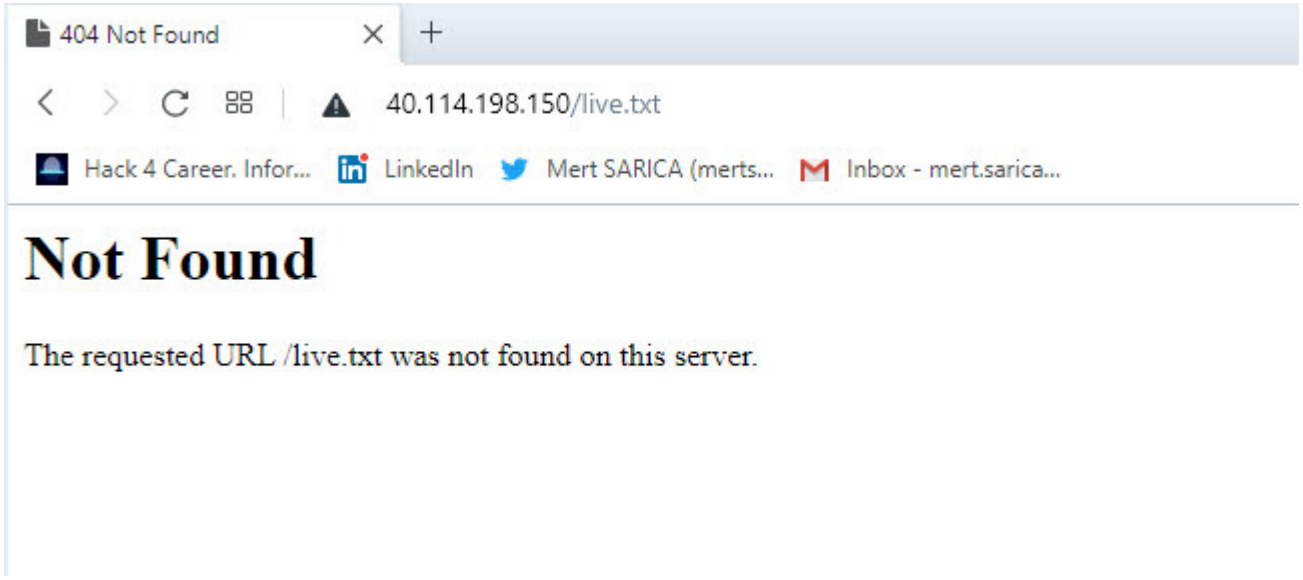
Sosyal medyayı oldukça etkin kullanan bir güvenlik araştırmacısı olarak bu zamana dek sosyal ağlar, e-postalar üzerinden aldığım mesajları güvenlik araştırmalarına ve ardından blog yazılarına, sunumlara çevirdiğimi biliyorsunuzdur. Çıkış noktası diğerleri ile aynı olan bu hikayede ise müşteri güvenliğini sağlamak amacıyla sosyal ağ üzerinden gelen bir siber tehdit istihbaratından nasıl faydalandığımı görebilirsiniz.

Her sabah olduğu 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 kişinin bankalar dışında beni de etiketlediği bir mesaj dikkatimi çekti. Mesajında bir videoda yer alan ve açık halde görülen kredi kartı bilgilerinin yer aldığını ve müşteri güvenliği adına bunların iptal edilip edilmediğini merak ediyordu.





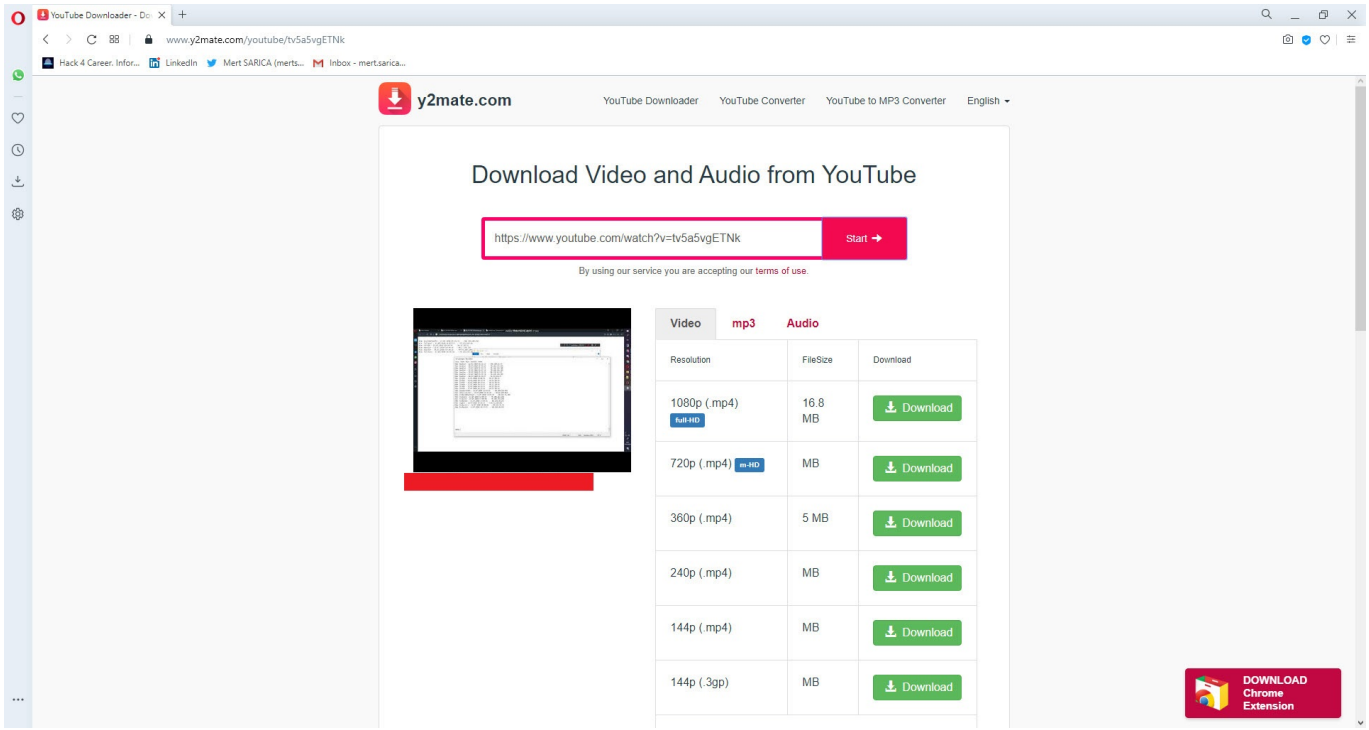
Videoyu izlemeye başladığımda Coez Checker isimli çalıntı kartları kontrol etmek amacıyla kullanılan bir servisin dolandırıcılar tarafından diğer dolandırıcılara mesaj vermek amacıyla hacklendiği anlaşılıyordu. Dolandırıcı, yaklaşık 3 dakikalık videonun 30 saniyesi boyunca sistem üzerinde kayıtlı olan 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 adresine ulaşmak istediğimde ise tahmin ettiğim üzere dosya çoktan yayından kaldırılmıştı ve elimde sadece bu video ile kalakalmıştım.



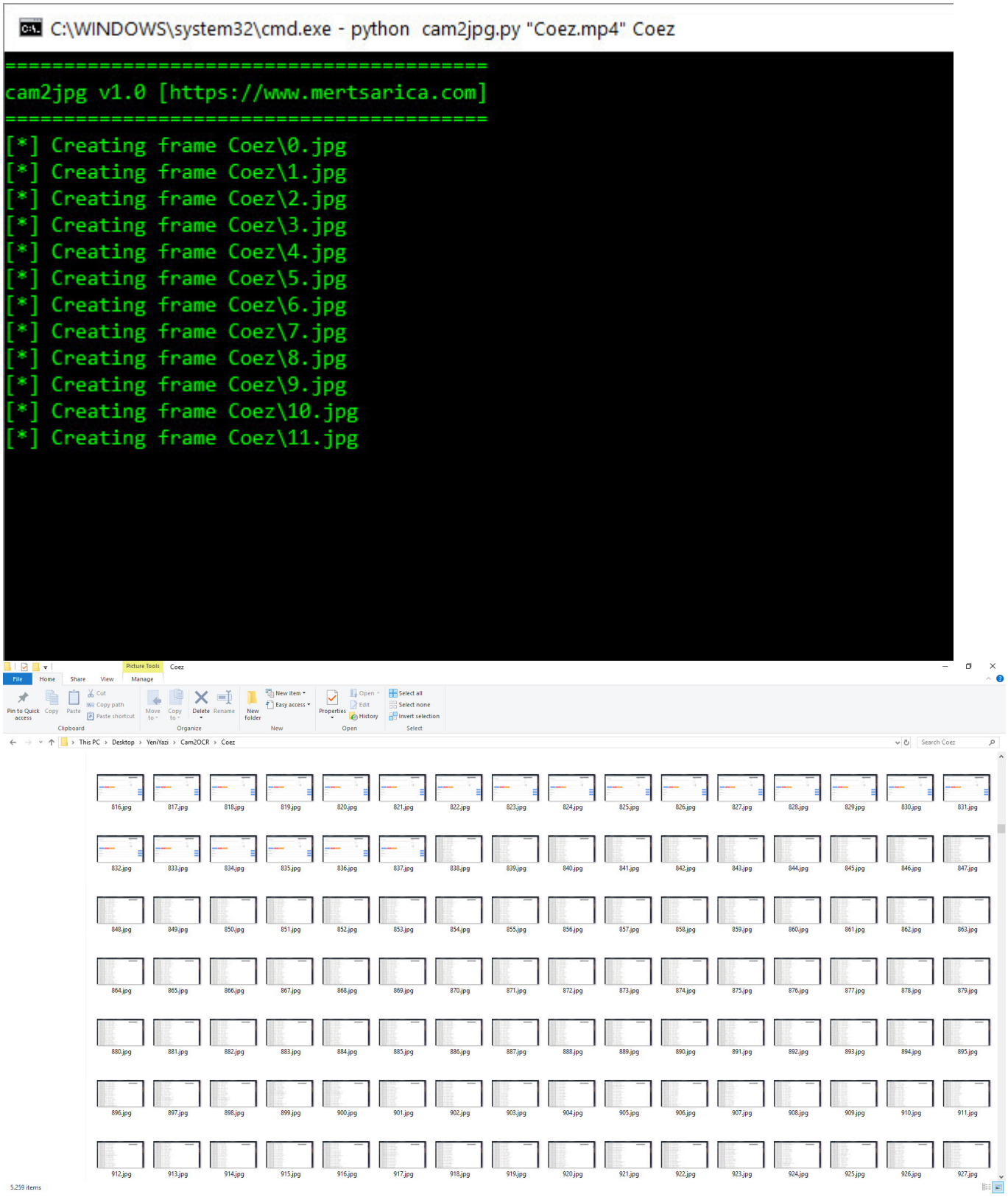
Vatandaşların dolandırıcılar tarafından mağdur edilmemesi adına bu videodaki kart bilgilerini başta Sektörel SOME/BDDK olmak üzere bankalarla da paylaşmak

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.

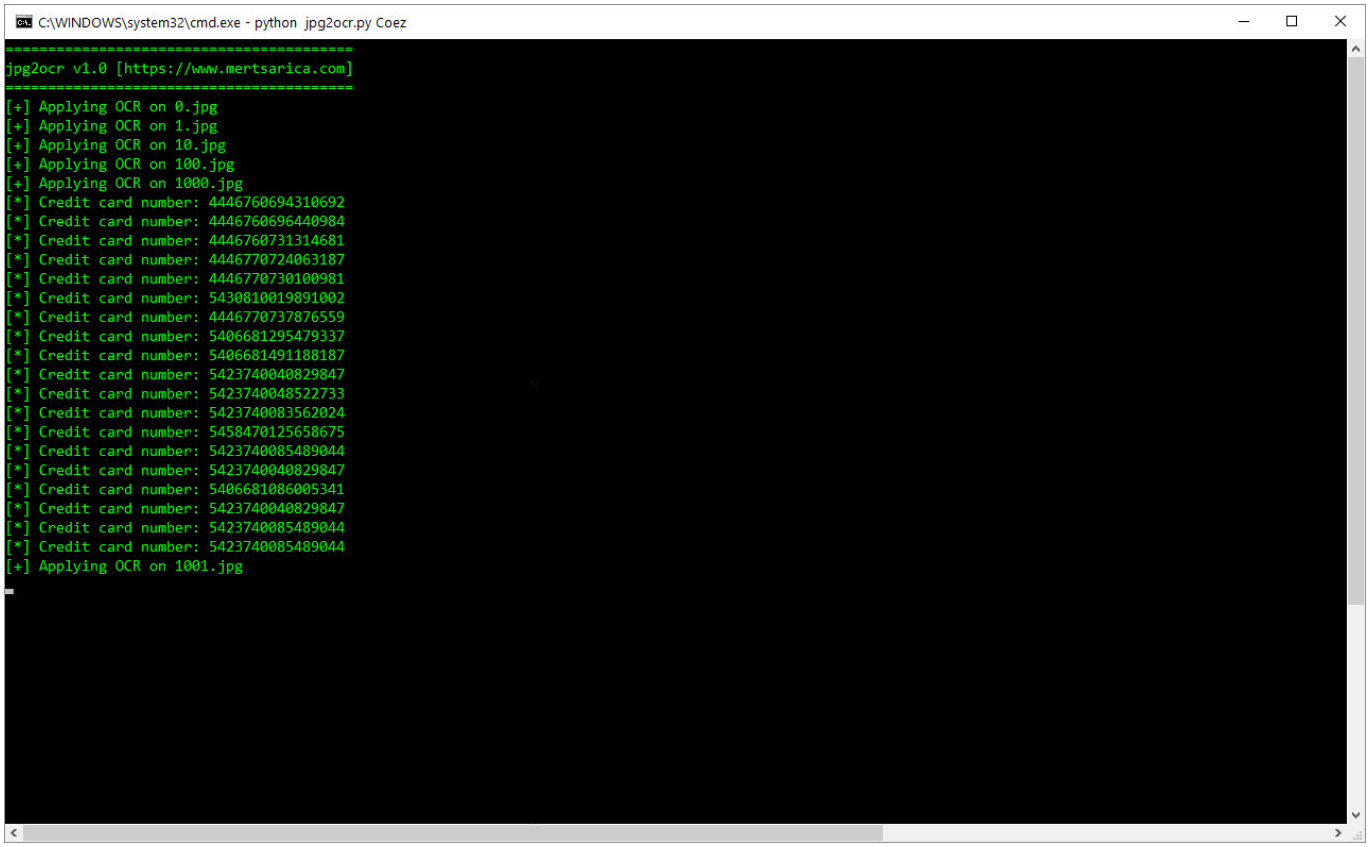
İlk iş olarak Y2mate YouTube Downloader web sitesinden faydalanarak Youtube üzerinden ilgili video dosyasını indirdim.



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.



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.



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.