23/10/2017

“Apps YILDIZ” ve “Mor Beyin” Adlı Uygulama Geliştirici Ekiplerin İnternetteki İzleri Hakkında Bilgi Notu

Sayın Av. Ali AKTAŞ,

Bu bilgi notu kendilerine “Yıldız Apps” ve “Mor Beyin” adlı mobil uygulama programı geliştirici ekipleri ile ilgili geçmişe dönük araştırma talebiniz üzerine kaleme alınmıştır.

Her iki uygulama gerliştiricisinin izleri WayBackMachine, Google Play ve VirusTotal servisleri kullanılarak aratılmıştır.

“Mor Beyin” adlı ekibin web sitesinin ve geliştirdikleri uygulamaların yayında olmadığı daha önceki bilgi notu için yapılan incelemede tespit edilmiştir.

Ancak “Apps Yıldız” tarafından yayınlanan bir kısım uygulama için yapılan bir çalışma sırasında elde edilen bulguların VirusTotal.com servisinde aratılması sırasında “Mor Beyin” hakkında da araştırma yapılmıştır.

İnceleme sonucunda karşılaşılan hususlar, teknik bilgiler ve önem arz eden diğer hususlar bu metinle bilgilerinize sunulmuştur.

Saygılarımla,
T. Koray Peksayar
Makine Müh. Lis. - Bilgi Tekn. Y. Lis.
Bilişim ve Adli Bilişim Uzmanı - Yeminli Adli Bilirkişi
İTÜ Y. Lis. Dip. No: 76-387

1. “Mor Beyin”

VirusTotal’da yapılan aramada “morbeyin.com” alan adıyla ilgili geçmişe dönük bilgiye ulabilinmiştir.[1]

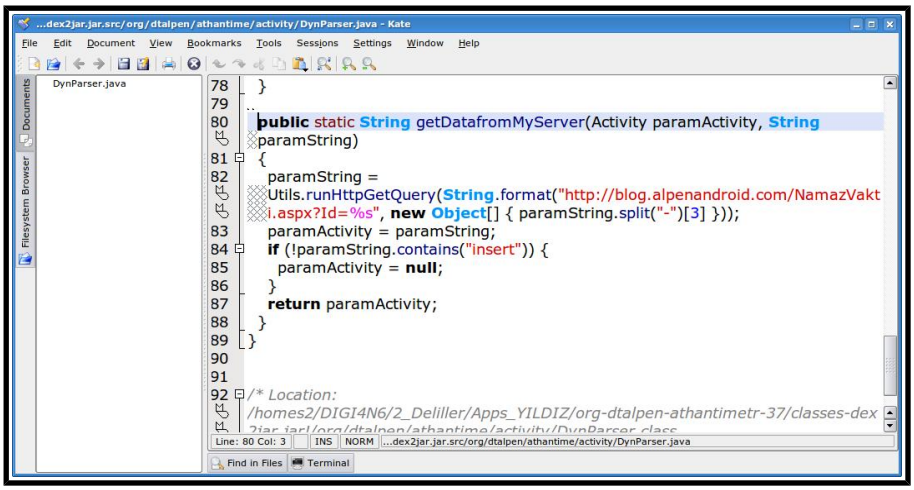
```
“Domain Name: MORBEYIN.COM
   Registrar: ENOM, INC.
   Sponsoring Registrar IANA ID: 48
   Whois Server: whois.enom.com
   Referral URL: http://www.enom.com
   Name Server: DNS1.NAMECHEAPHOSTING.COM
   Name Server: DNS2.NAMECHEAPHOSTING.COM
   Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Updated Date: 16-may-2016
   Creation Date: 18-may-2012
   Expiration Date: 18-may-2017
Domain Name: MORBEYIN.COM
Registry Domain ID: 1721266278_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.enom.com
Registrar URL: www.enom.com
Updated Date: 2017-05-13T07:42:23.00Z
Creation Date: 2012-05-18T12:47:00.00Z
Registrar Registration Expiration Date: 2017-05-18T11:47:49.00Z
Registrar: ENOM, INC.
Registrar IANA ID: 48
Reseller: NAMECHEAP.COM
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: AHMET ULUSOY
Registrant Organization:
Registrant Street: C.S.
Registrant City: IST
Registrant State/Province: IST
Registrant Postal Code: 80816
Registrant Country: TR
Registrant Phone: +90.212212212
Registrant Phone Ext:
Registrant Fax: +1.5555555555
Registrant Fax Ext:
Registrant Email: AHMETULSY@YANDEX.COM
Registry Admin ID:
Admin Name: AHMET ULUSOY
Admin Organization:
Admin Street: C.S
Admin City: IST
Admin State/Province: IST
Admin Postal Code: 80816
Admin Country: TR
Admin Phone: +90.212212212
Admin Phone Ext:
Admin Fax: +1.5555555555
Admin Fax Ext:
Admin Email: AHMETULSY@YANDEX.COM
Registry Tech ID:
Tech Name: AHMET ULUSOY
Tech Organization:
Tech Street: C.S.
Tech City: IST
Tech State/Province: IST
Tech Postal Code: 80816
Tech Country: TR
Tech Phone: +90.212212212
Tech Phone Ext:
Tech Fax: +1.5555555555
Tech Fax Ext:
Tech Email: AHMETULSY@YANDEX.COM
Name Server: DNS1.NAMECHEAPHOSTING.COM
Name Server: DNS2.NAMECHEAPHOSTING.COM
DNSSEC: unSigned
Registrar Abuse Contact Email: abuse@enom.com
Registrar Abuse Contact Phone: +1.4252982646”
```

1 https://www.virustotal.com/tr/domain/morbeyin.com/information/ adresinde mevcuttur

2. “Apps YILDIZ”

Söz konusu geliştiricinin yayınladığı “Namaz Vakitleri TR” adlı uygulamanın kaynak kodu dex2jar ve Java Decompiler (jd-gui) yazılımlarıyla elde edilmiştir.

Bu kaynak kodunda yapılan anlamlı veri dizileri aramasında, uygulamanın “http://blog.alpenandroid.com” adresine bağlantı kurarak bu adresteki ASP.NET ile yazılmış çeşitli program kodlarını kullanarak uygulamaya veri çektiği tespit edilmiştir.



VirusTotal’da yapılan aramada “alpenandroid.com” alan adıyla ilgili geçmişe dönük bilgiye ulabilinmiştir.[2]

```
“   Domain Name: ALPENANDROID.COM
    Registrar: 1 API GMBH
    Sponsoring Registrar IANA ID: 1387
    Whois Server: whois.1api.net
    Referral URL: http://www.1api.net
    Name Server: NS1.IWANTMYNAME.NET
    Name Server: NS2.IWANTMYNAME.NET
    Name Server: NS3.IWANTMYNAME.NET
    Name Server: NS4.IWANTMYNAME.NET
    Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
    Updated Date: 05-sep-2016
    Creation Date: 04-sep-2013
    Expiration Date: 04-sep-2017
Domain Name: ALPENANDROID.COM
Registry Domain ID: 1825636510_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.1api.net
Registrar URL: http://www.1api.net
Updated Date: 2016-12-25T09:26:38Z
Creation Date: 2013-09-04T21:30:02Z
Registrar Registration Expiration Date: 2017-09-04T21:30:02Z
Registrar: 1API GmbH
Registrar IANA ID: 1387
Registrar Abuse Contact Email: abuse@1api.net
Registrar Abuse Contact Phone: +49.68416984x200
Reseller: iwantmyname http://iwantmyname.com
Domain Status: clientTransferProhibited - http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: yasin alpen
Registrant Organization: alpen
Registrant Street: ankara
Registrant City: ankara
Registrant State/Province:
Registrant Postal Code: 06530
Registrant Country: TR
Registrant Phone: +90.90312444032
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: yasinalpen@gmail.com
Registry Admin ID:
Admin Name: c/o WHOIStrustee.com Limited
```

2 https://www.virustotal.com/tr/domain/alpenandroid.com/information/ adresinde mevcuttur

```
Admin Organization: Registrant of alpenandroid.com
Admin Street: 6 Thornes Office Park
Admin City: Monckton Road
Admin State/Province: Wakefield
Admin Postal Code: WF2 7AN
Admin Country: GB
Admin Phone: +49.68416984300
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: 1b839eebab@alpenandroid.com.whoistrustee.com
Registry Tech ID:
Tech Name: c/o WHOIStrustee.com Limited
Tech Organization: Registrant of alpenandroid.com
Tech Street: 6 Thornes Office Park
Tech City: Monckton Road
Tech State/Province: Wakefield
Tech Postal Code: WF2 7AN
Tech Country: GB
Tech Phone: +49.68416984300
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: 1b839eebab@alpenandroid.com.whoistrustee.com
Name Server: ns1.iwantmyname.net 62.116.159.99 2001:4178:0003:a357:0062:0116:0159:0099
Name         Server:         ns2.iwantmyname.net         217.160.113.131         83.169.55.71
2a01:0488:2000:0c02:0083:0169:0055:0071
Name Server: ns3.iwantmyname.net 89.146.248.96 2a01:0130:2000:0118:0089:0146:0248:0096
Name Server: ns4.iwantmyname.net 74.208.254.95
DNSSEC: unsigned”
```

Söz konusu geliştiricinin Google Play’deki kendisini tanıtan kaydı dönemsel olarak değiştirdiği, uygulamalarını sırasıyla;

1. alper yildiz
2. Apps YILDIZ
3. Heidi Mobil Apps

adlarıyla yayınladığı tespit edilmektedir.

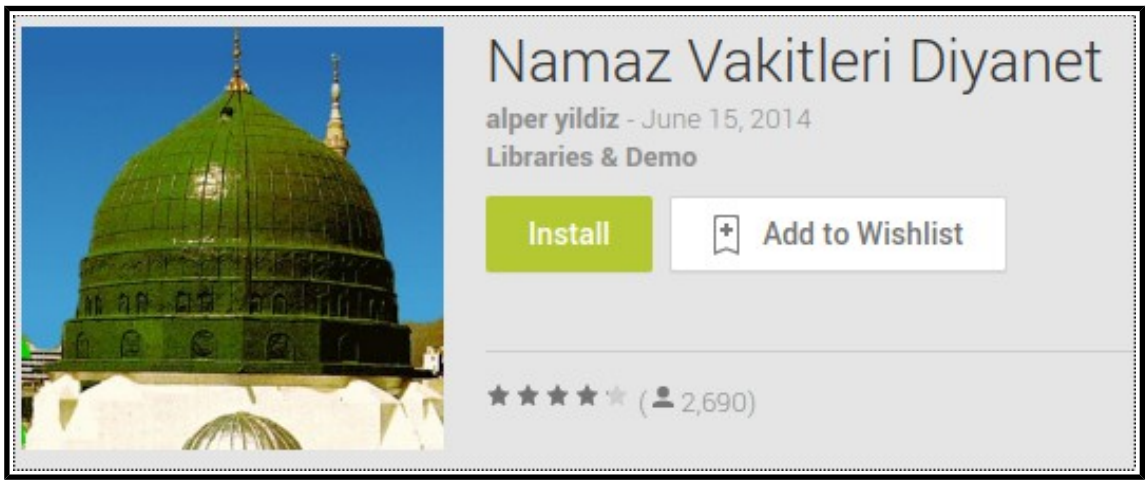
“Namaz Vakitleri TR” adlı uygulamanın Google Play sayfasının WayBack Machine arşive kaydına https://web.archive.org/web/*/https://play.google.com/store/apps/details?id=org.dtalpen.athantimetr adresinden ulaşılabilinir. Bu kayıtlara göre sayfa;

1. 06/08/2014
2. 11/06/2015
3. 07/02/2016
4. 12/10/2017

tarihlerinde arşivlenmiştir.

Arşivdeki uygulama tanıtım başlıklarının ekran görüntüleri aşağıdadır.

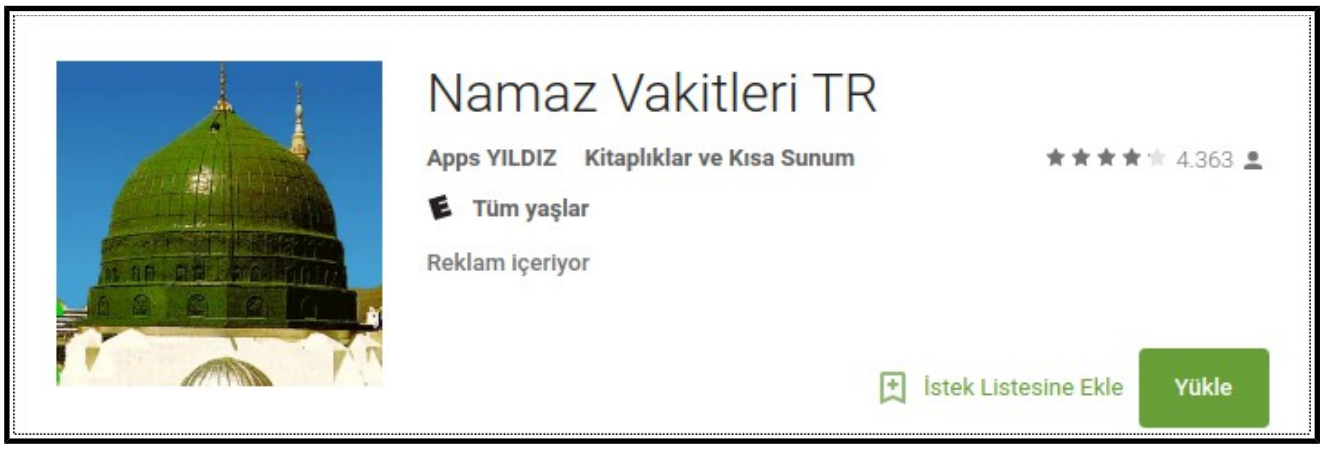
06/08/2014
https://web.archive.org/web/20140806145934/https://play.google.com/store/apps/details?id=org.dtalpen.athantimetr



11/06/2015
https://web.archive.org/web/20150611213657/https://play.google.com/store/apps/details?id=org.dtalpen.athantimetr

07/02/2016
https://web.archive.org/web/20160207214934/https://play.google.com/store/apps/details?id=org.dtalpen.athantimetr

12/10/2017
https://web.archive.org/web/20171012083609/https://play.google.com/store/apps/details?id=org.dtalpen.athantimetr



23/10/2017 Güncel hali
https://play.google.com/store/apps/details?id=org.dtalpen.athantimetr