

Dolandırıcıların Gizlenme Oyunları

written by Mert SARICA | 1 September 2025

If you are looking for an English version of this article, please visit [here](#).

İÇİNDEKİLER

1. Başlangıç
2. Coğrafi Maskeleye
3. Kullanıcı Aracısı (User-Agent) Tabanlı Maskeleye
4. Kara Liste Tabanlı Maskeleye
5. Abra Kadabra
6. Sonuç

Başlangıç

Yatırım Dolandırıcıları başlıklı blog yazımı okuyanlarınız, sosyal medya ve ağlar üzerinden dolandırıcıların sahte reklamlarla masum vatandaşları hangi yöntemlerle, nasıl ağlarına düşürmeye çalıştıklarını görmüşlerdir. O yazıda da olduğu gibi dolandırıcılık girişiminin önemli bir parçasında yer alan web siteleri, dolandırıcıların operasyonları açısından kritik bir yere sahiptir.

Çoğu vakada ikna yolu ile bir şekilde kurbanlarını web sitelerine getirebilen dolandırıcılar, kurbanlarına ait bilgileri buradan ele geçirmekte, ardından operasyonlarının diğer adımı olan çağrı veya WhatsApp, Telegram gibi kanallar üzerinden kurbanları ile iletişime geçmektedirler. Tahmin edilebileceği üzere bu son adımda da kurbanlarına para transferi yaptırmaya çalışarak kötü emellerine ulaşmayı hedeflemektedirler.

Tabii bu dolandırıcılardan biraz işi bilenler, SOCRadar, Netcraft gibi siber suçlarla mücadele eden şirketlerin ve USOM gibi birimlerin web sitelerini taradıklarını, raporladıklarını ve ardından da şüpheli/zararlı olanları kapattırdıklarını bildikleri için bu taramaları atlatma adına 1996 yılından beri SEO dünyasında kullanılan Cloaking dediğimiz maskeleye taktiğinden faydalanmaktadırlar. Ben de bu yazımda farkındalık yaratması adına maskeleye tekniklerinden en çok kullanılanlarına ve bunları basit bir şekilde atlatmak amacıyla yapay zekaya geliştirdiğim bir araca yer vermeye çalıştım.

Cloaking, bir web sitesinin arama motorlarına gösterdiği içeriğin, kullanıcılara gösterdiği içerikten farklı olmasıdır; bu, arama motoru optimizasyonu (SEO) kurallarına aykırı bir uygulamadır. Kullanıcılar ve arama motorları tarafından farklı içeriklerin sunulduğu bu yöntem, arama sonuçlarında avantaj sağlamak amacıyla kullanılır.

Cloaking'in Amacı ve Yöntemi

Arama Motoru Optimizasyonu (SEO):

Cloaking, bir web sitesinin arama motoru sonuçlarında daha üst sıralarda yer almasını sağlamak için kullanılan bir tekniktir.

Farklı İçerik Sunumu:

Arama motoru botları, web sitesinin daha zengin ve arama sorgularına uygun anahtar kelimelerle dolu bir içeriğe sahip olduğunu düşünür. Ancak, gerçek kullanıcılara sitenin farklı ve genellikle daha az optimize edilmiş bir sürümü gösterilir.

Kötü Niyetli Kullanım:

Bu yöntem, Google gibi arama motorlarının algoritmalarını kandırmak ve kullanıcılara spam veya yanıltıcı içerikler göstermek amacıyla kullanılır.

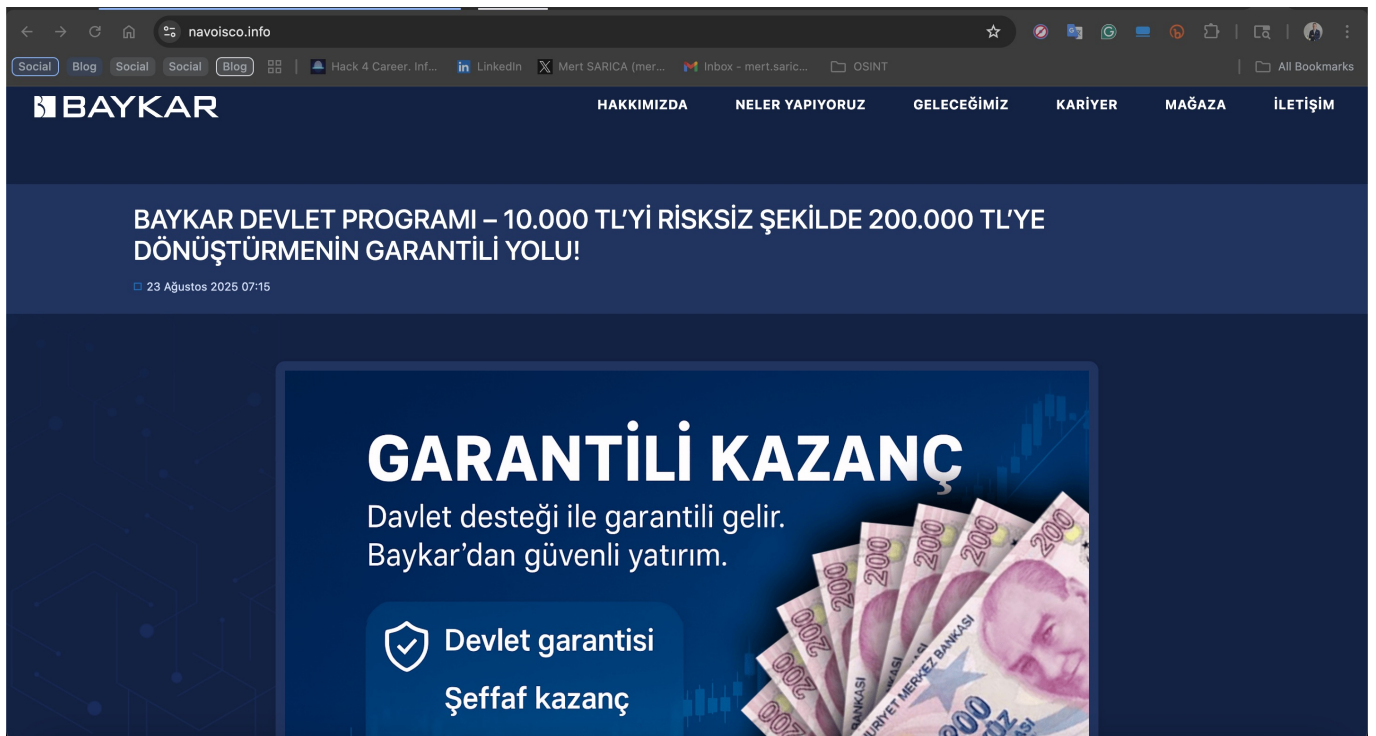
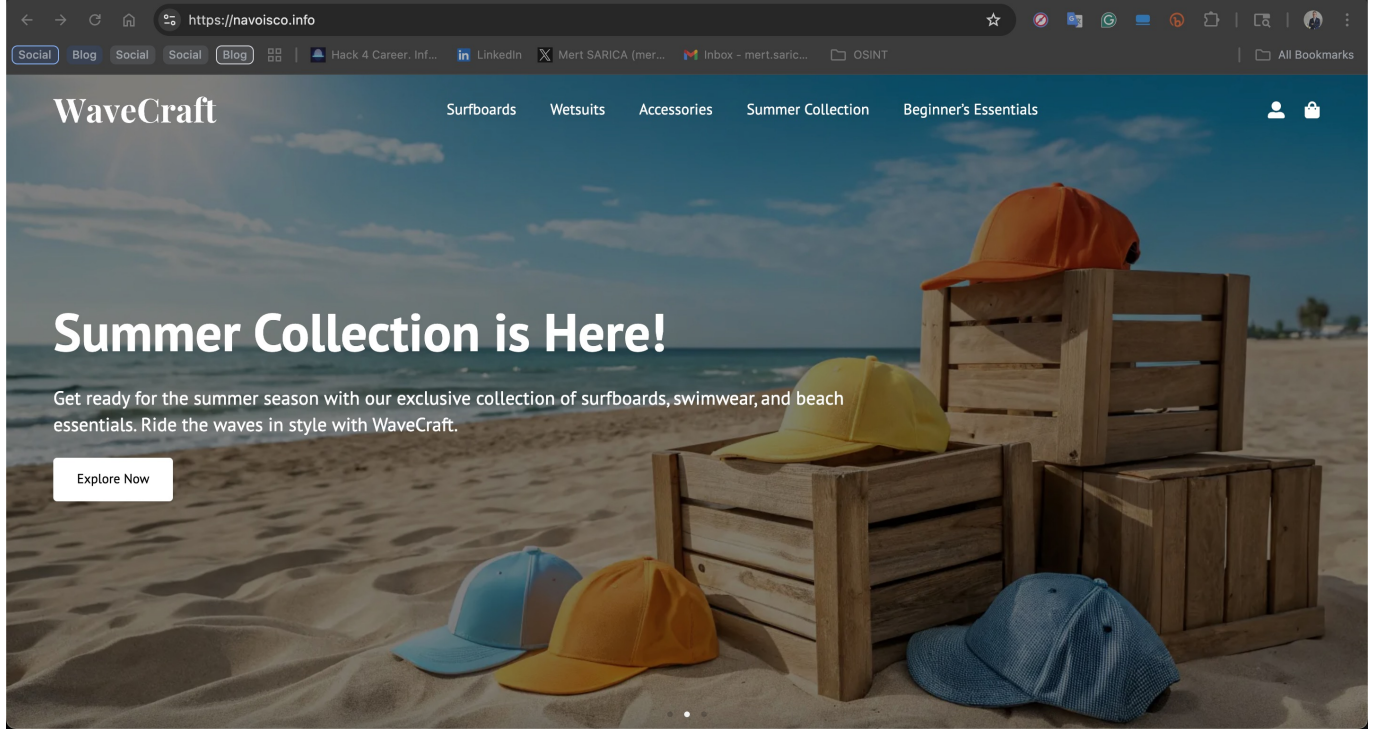
Öncelikle maskeleyme tekniği kullanılan ortalama siteleri üzerinde güvenlik araştırması yapabilmek için ortalama sitelerinin kaynak koduna ihtiyacım vardı. Ha deyince bunlara ulaşmak pratikte pek mümkün olamayacağı için önceki yazılarımda olduğu gibi SOCRadar'ın yardımına başvurmaya verdim. :)

SOCRadar platformu ortalama (phishing) sitelerini sadece tespit etmekle kalmayıp bunların arkasındaki tehdit aktörlerine ulaşabilmek için yeri geldiğinde kaynak kodlarını da elde edebildiği için Türk vatandaşlarını hedef alan 500 tane ortalama sitesine ait kaynak kodunu temin edip, üzerinde güvenlik araştırması yapmaya karar verdim.

Coğrafi Maskeleyme

İlk olarak Yatırım Dolandırıcıları blog yazıma konu olan tehdit aktörüne ait bir web sitesini inceledim. Bir yıldır dolandırıcılık operasyonlarına hız kesmeden devam eden bu tehdit aktörü, 6 Ağustos 2025 tarihinde navisco[.]info isimli alan adını kayıt edip, 13 Ağustos 2025 tarihinde ise web sitesini dolandırıcılık amacıyla kullanmaya başladı.

Bu web sitesini yurt dışından ziyaret ettiğinizde karşınıza sörf ürünleri satan bir içerik geliyordu fakat Türkiye'den ziyaret ettiğinizde bu defa Baykar savunma şirketinin adını kullanarak dolandırıcılık faaliyeti gerçekleştiren, kısaca Coğrafi Maskeleye tekniği kullanan bir web sayfası olarak karşınıza çıkıyordu. Google arama motorunda bu adresi arattığınızda ise dolandırıcıların kullandığı bu maskeleye tekniği sayesinde kayıtlara sörf ürünleri satan bir mağaza olarak girdiği görülmüştü.



Google search results for <https://navisco.info/>

- navisco.info**
<https://www.navisco.info/>
WaveCraft Surf Shop – Surfboards, Wetsuits & Gear
Explore our wide selection of surfboards, wetsuits, and accessories. We're dedicated to helping you find the gear you need for an unforgettable surfing ...
- navisco.info**
<https://navisco.info/contact>
Contact – WaveCraft Surf Shop – Surfboards, Wetsuits & Gear
Prefer to speak directly? Call our friendly team at +1 619-555-1234 for assistance with orders, product questions, or store hours. We're here to help you ride ...
- navisco.info**
<https://navisco.info/product-tag/beginners-essentials>
Beginner's Essentials – WaveCraft Surf Shop – Surfboards, Wetsuits ...
Something big is brewing! Our store is in the works and will be launching soon! Shop. Surfboards · Wetsuits · Accessories.
- navisco.info**
<https://www.navisco.info/beginners-essentials>
Beginner's Essentials - WaveCraft Surf Shop
Explore our range of stable and easy-to-paddle surfboards designed specifically for beginners. Choose

USBM (Ulusal Siber Olaylara Müdahale Birimi) website showing a security alert for navisco.info.

navisco.info
Financial Phishing

Criticality Level
4/10
1.Lowest - 10.Highest

Description:
Financial Phishing

Connection Type:
Phishing

Date:
8/22/2025, 03:58 PM

Source:
REPORTING

We use cookies to ensure our website functions properly, to personalize content, and to analyze our site traffic. [Learn more](#) [I Accept](#)

Last shown: Aug 23, 2025

Format: Video



Küçük bir an bugün. Hayatına küçük bir yenilik ekle

Sponsored


[See more ads by this advertiser](#)
<https://navisco.info>

Not: Yaklaşık bir yılı aşkın süredir takip ettiğim ve Rus olduklarına kanaat getirdiğim, operasyonlarını ise ağırlıklı Ukrayna IP adresleri (185.38.218.86, 185.237.75.100, 91.123.155.63) üzerinden gerçekleştiren tehdit aktörlerinin, Şubat 2025'ten bu yana 699 ortalama (phishing) web sitesi hayata geçirdiğini, yaklaşık 9000 Türk vatandaşını hedef alıp kişisel bilgilerini (isim, soyad, e-posta adresi, telefon numarası, ip adresi) ele geçirdiklerini tespit ettim.

test@gmail.com	test	test	'380503223522	UA	159.224.64.139	volumeiin.com
test@gmail.com	test	test	'380992182888	UA	185.237.75.100	wwwborusan.com
test@gmail.com	test	test	'380042124241	UA	159.224.64.139	volumeiin.com
test@gmail.com	test	test	'380991292992	UA	185.237.75.100	volumeiin.com
test@gmail.com	test	test	'380501284234	UA	31.148.245.242	breakoyclh.com
test@gmail.com	test	test	'380991292992	UA	185.237.75.100	breakoyclh.com
test@gmail.com	recr	recr	'380992929292	UA	185.237.75.100	breakoyclh.com
test@gmail.com	test	test	'380912992929	UA	185.237.75.100	breakoyclh.com
test@gmail.com	test	test	'380501929292	UA	185.237.75.100	breakoyclh.com
test@gmail.com	test	test	'380658454664	UA	159.224.64.139	noriochiai.com
test@gmail.com	Test	Mobile	'380656568864	UA	159.224.64.139	token-academ.com
test@gmail.com	test	test	'380912020020	UA	185.237.75.100	breakoyclh.com
test@gmail.com	test	test	'380991292999	UA	185.237.75.100	oliorossi.pro
test@gmail.com	test	test	'380501299299	UA	185.237.75.100	talentscanai.pro
test@gmail.com	test	test	'380991202002	UA	185.237.75.100	news.borusana.com
test@gmail.com	test	test	'380333333333	UA	91.123.155.63	www.greenexhome.com
test@gmail.com	test	test	'380919292999	UA	185.237.75.100	homogeubpz.shop
test@gmail.com	test	test	'380912902020	UA	185.237.75.100	talentscanai.pro
test@gmail.com	test	test	'380912902020	UA	185.237.75.100	talentscanai.pro
test@gmail.com	test	test	'380912902020	UA	185.237.75.100	talentscanai.pro
test@gmail.com	test	test	'380912902020	UA	185.237.75.100	talentscanai.pro
test@gmail.com	test	test	'380501299292	UA	185.237.75.100	talentscanai.pro
test@gmail.com	test	test	'380510292999	UA	185.237.75.100	gmail
test@gmail.com	test	teest	'380501229292	UA	185.237.75.100	gmail
test@gmail.com	test	test	'380912920020	UA	185.237.75.100	gmail
test@gmail.com	test	test	'380501239299	UA	185.237.75.100	gmail
test@gmail.com	test	test	'380500123912	UA	185.237.75.100	gmail
test@gmail.com	test	test	'380919239293	UA	185.237.75.100	gmail
test@gmail.com	test	test	'380991230230	UA	185.237.75.100	gmail
test@gmail.com	test	test	'380959120000	UA	185.237.75.100	perimasaliotel.pro
test@gmail.com	test	test	'380991230200	UA	185.237.75.100	gmail
test@gmail.com	tes	ttest	'380919239239	UA	185.237.75.100	gmail

Line	Time	IP	Country	IP	Country	IP	Country	IP	Country
2169	02.07.2025 17:35:09 UTC-05:00	192.168.1.1	TR	90536	TR	78.1	TR	materialchiktz.com	
2170	02.07.2025 17:35:11 UTC-05:00	192.168.1.1	TR	90505	TR	31.1	TR	nakiyatpro.info	
2171	02.07.2025 17:35:12 UTC-05:00	192.168.1.1	TR	90538	TR	88.2	TR	nakiyatpro.info	
2172	02.07.2025 17:35:14 UTC-05:00	192.168.1.1	TR	90507	TR	78.1	TR	nakiyatpro.info	
2173	02.07.2025 17:35:15 UTC-05:00	192.168.1.1	TR	90537	TR	159.1	TR	nakiyatpro.info	
2174	02.07.2025 17:35:17 UTC-05:00	192.168.1.1	TR	90532	TR	176.1	TR	nakiyatpro.info	
2175	02.07.2025 17:35:18 UTC-05:00	192.168.1.1	TR	90552	TR	151.1	TR	materialchiktz.com	
2176	02.07.2025 17:35:20 UTC-05:00	192.168.1.1	TR	90552	TR	149.1	TR	incigulus.info	
2177	02.07.2025 17:40:39 UTC-05:00	192.168.1.1	TR	90552	TR	149.1	TR	incigulus.info	
2178	02.07.2025 17:40:40 UTC-05:00	192.168.1.1	TR	90534	TR	78.1	TR	incigulus.info	
2179	02.07.2025 17:40:41 UTC-05:00	192.168.1.1	TR	90541	TR	88.2	TR	incigulus.info	
2180	02.07.2025 17:40:43 UTC-05:00	192.168.1.1	TR	90541	TR	88.2	TR	incigulus.info	
2181	02.07.2025 17:40:45 UTC-05:00	192.168.1.1	TR	90530	TR	31.2	TR	materialchiktz.com	
2182	02.07.2025 17:40:46 UTC-05:00	192.168.1.1	TR	90546	TR	176.1	TR	incigulus.info	
2183	02.07.2025 17:40:48 UTC-05:00	192.168.1.1	TR	90546	TR	85.1	TR	incigulus.info	
2184	02.07.2025 17:40:49 UTC-05:00	192.168.1.1	TR	90552	TR		TR	incigulus.info	
2185	02.07.2025 17:40:51 UTC-05:00	192.168.1.1	TR	90563	TR	31.1	TR	materialchiktz.com	
2186	02.07.2025 17:40:52 UTC-05:00	192.168.1.1	TR	90563	TR	31.1	TR	materialchiktz.com	
2187	02.07.2025 17:40:54 UTC-05:00	192.168.1.1	TR	90541	TR	176.1	TR	materialchiktz.com	
2188	02.07.2025 17:40:55 UTC-05:00	192.168.1.1	TR	90558	TR	217.1	TR	materialchiktz.com	
2189	02.07.2025 17:40:56 UTC-05:00	192.168.1.1	TR	90531	TR	178.1	TR	incigulus.info	
2190	02.07.2025 17:40:58 UTC-05:00	192.168.1.1	TR	90541	TR		TR	incigulus.info	
2191	02.07.2025 17:40:59 UTC-05:00	192.168.1.1	TR	90546	TR		TR	incigulus.info	
2192	02.07.2025 17:41:01 UTC-05:00	192.168.1.1	TR	90535	TR	31.1	TR	gmail	
2193	02.07.2025 17:41:02 UTC-05:00	192.168.1.1	TR	90507	TR	85.1	TR	incigulus.info	
2194	02.07.2025 17:41:04 UTC-05:00	192.168.1.1	TR	90534	TR	5.46	TR	wrybybqn.shop	
2195	02.07.2025 17:41:05 UTC-05:00	192.168.1.1	TR	90542	TR	31.14	TR		
2196	02.07.2025 17:41:07 UTC-05:00	192.168.1.1	TR	90532	TR	194.1	TR	incigulus.info	
2197	02.07.2025 17:41:08 UTC-05:00	192.168.1.1	TR	90538	TR	188.1	TR	incigulus.info	
2198	02.07.2025 17:41:10 UTC-05:00	192.168.1.1	TR	90505	TR	5.17	TR	incigulus.info	
2199	02.07.2025 17:41:11 UTC-05:00	192.168.1.1	TR	90545	TR	37.1	TR	incigulus.info	
2200	02.07.2025 17:41:13 UTC-05:00	192.168.1.1	TR	90543	TR	188.1	TR	incigulus.info	

Kullanıcı Aracısı (User-Agent) Tabanlı Maskeleye

İkinci olarak 17 Nisan 2025 tarihinde Ziraat Bankası müşterilerini hedef alan mybbau[.]sa[.]com oltalama sitesine ait kaynak kodlarını incelemeye başladım ve dosyalar arasında netcraft_check.php isimli dosya dikkatimi çekti.

Netcraft, 1995'ten beri faaliyet gösteren İngiltere merkezli bir siber güvenlik ve internet ölçüleme şirketidir. En çok phishing (oltalama) ve kötüye kullanım raporlama hizmetleriyle bilinir; barındırma analizi ve internet altyapısı istatistikleri sunar.

Oltalama sitesinin ziraatbank alt klasöründe yer alan index.php dosyasından çağrılan bu dosyada, Netcraft şirketi tarafından oltalama sitesini tespit etmek amacıyla kullanıldığı düşünülen kullanıcı aracısı dizesi (User-Agent) yer alıyordu. Bu dize ile web sitesine bağlantı yapıldığında kullanıcının web tarayıcısı google.ca adresi üzerinden https://appleid.apple.com web adresine yönlendirerek maskeleye işlemi gerçekleştiriyordu.

Name	Date Modified	Size	Kind
ziraat	Today at 16:53	--	Folder
admin_ziirtata.sql	Apr 17, 2025 at 02:15	40 KB	SQL file
assets	Apr 17, 2025 at 02:15	--	Folder
Content	Apr 17, 2025 at 02:15	--	Folder
core91f5.js	Apr 17, 2025 at 02:15	1.2 MB	JavaScript
index.php	Apr 17, 2025 at 02:15	4 KB	PHP script
jquery361c.js	Apr 17, 2025 at 02:15	321 KB	JavaScript
plugins.min7a39.css	Apr 17, 2025 at 02:15	345 KB	Text Document
sub.min179c.css	Apr 17, 2025 at 02:15	340 KB	Text Document
ui.min4f26.js	Apr 17, 2025 at 02:15	143 KB	JavaScript
ziraat.zip	Apr 16, 2025 at 12:27	6.3 MB	ZIP archive
ziraatbank	Today at 16:53	--	Folder
_block	Apr 17, 2025 at 02:15	--	Folder
blacklist_lookup.php	Apr 17, 2025 at 02:15	7 KB	PHP script
blacklist.dat	Apr 17, 2025 at 02:15	32 KB	DAT file
blocker.php	Apr 17, 2025 at 02:15	4 KB	PHP script
netcraft_check.php	Apr 17, 2025 at 02:15	362 bytes	PHP script
visitor_log.php	Apr 17, 2025 at 02:15	299 bytes	PHP script
_kontrol	Apr 17, 2025 at 02:15	--	Folder
_net	Apr 17, 2025 at 02:15	--	Folder
_ZAE23AFeAd	Apr 17, 2025 at 02:15	--	Folder
baglanz.php	Today at 17:56	5 KB	PHP script
Firstsms.php	Apr 17, 2025 at 02:15	19 KB	PHP script
index.php	Apr 17, 2025 at 02:15	27 KB	PHP script
loading.gif	Apr 17, 2025 at 02:15	119 KB	GIF Image
loading.php	Apr 17, 2025 at 02:15	24 KB	PHP script
Login	Apr 17, 2025 at 02:15	--	Folder
pola.php	Apr 17, 2025 at 02:15	4 KB	PHP script
ProcDone.php	Apr 17, 2025 at 02:15	7 KB	PHP script
robots.txt	Apr 17, 2025 at 02:15	61 KB	Plain Text
SecureSms.php	Apr 17, 2025 at 02:15	15 KB	PHP script
security_phone.php	Apr 17, 2025 at 02:15	18 KB	PHP script
WebResource.axd	Apr 17, 2025 at 02:15	23 KB	Document
ziraatOnav.php	Apr 17, 2025 at 02:15	20 KB	PHP script

```

4 include 'baglanz.php';
5 $ip = GetIP();
6
7
8 $db->query("UPDATE sazan SET now = 'AnaSayfada' WHERE ip = '{sip}'");
9
10 $sayarsor = $db->prepare("SELECT * from ayarlar where ayar_id=:id");
11 $sayarsor->execute(array('id' => 0));
12 $sayarcek=$sayarsor->fetch(PDO::FETCH_ASSOC);
13
14 include '_kontrol/Country_Detect.php';
15 include '_kontrol/Mobile_Detect.php';
16 include '_kontrol/geoplugin.class.php';
17 // $geoplugin = new geoplugin();
18 // $detect = new Mobile_Detect;
19
20 /*
21 $ipx = GetIP();
22 $geoplugin->locate($ipx);
23
24 echo "Geolocation results for {$geoplugin->ip}: <br />\n".
25 "City: {$geoplugin->city} <br />\n".
26 "Region: {$geoplugin->region} <br />\n".
27 "Region Code: {$geoplugin->regionCode} <br />\n".
28 "Country Code: {$geoplugin->countryCode} <br />\n";
29 */
30
31 $ban = $db->query("SELECT * FROM ban", PDO::FETCH_ASSOC);
32 foreach($ban as $kontrol){
33     if($kontrol['ban'] == $ip){
34         header("Location:http://www.google.com.tr");
35     }
36 }
37
38 <!DOCTYPE html>
39 <html class="login">
40
41 <head>
42 <script id="_wau569">var _wau = _wau || []; _wau.push(["small", "zirbir16", "569"]);</
43 script>
44 <script async src="//waust.at/s.js"></script>
45 <meta http-equiv="Content-Language" content="tr" />
46 <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-9" />
47 <meta name="description" content="" />
48 <meta name="keyword" content="" />
49 <meta http-equiv="X-UA-Compatible" content="IE=edge" />
50 <title>Hosgeliniz | Ziraat Bankasi Internet Bankaciligi </title>
51 <link rel="icon" href=" ../Content/assets/Img/touch_icon.png">
52 <meta name="viewport" content="width=device-width. initial-scale=1.0. maximum-scale=5.

```

```

1 <?php
2 include '_block/blocker.php';
3 include '_block/blacklist_lookup.php';
4 include '_block/netcraft_check.php';
5 error_reporting(0);
6 date_default_timezone_set('Europe/Istanbul');
7
8
9
10
11 try
12 {
13     $db=new PDO("mysql:host=localhost;dbname=admin_ziraAFat;charset=utf8",'
14     admin_ziraAFat','admin_ziraAFat');
15 }
16 catch (PDOException $e)
17 {
18     echo $e->getMessage();
19 }
20
21 function guvenlik($gelen)
22 {
23     $sgiden = addslashes($gelen);
24     $sgiden = htmlspecialchars($sgiden);
25     $sgiden = strip_tags($sgiden);
26     $sgiden = htmlentities($sgiden);
27
28     return $sgiden;
29 }
30
31 function encryptz($string, $key)
32 {
33     $encrypted_string = openssl_encrypt($string, "AES-128-ECB", $key);
34     return $encrypted_string;
35 }
36
37 function decrypt($string, $key)
38 {
39     $decrypted_string = openssl_decrypt($string, "AES-128-ECB", $key);
40     return $decrypted_string;
41 }
42
43 $sahahtazr = "SeAsAyK0_Qclar";
44
45 function temizle($str)
46 {
47     $sstr = str_replace(array("'", '"', "\\", "\r", "\n", "\t", "\f", "\z", "\0", "\x00", "\x01", "\x02", "\x03", "\x04", "\x05", "\x06", "\x07", "\x08", "\x09", "\x0A", "\x0B", "\x0C", "\x0D", "\x0E", "\x0F", "\x10", "\x11", "\x12", "\x13", "\x14", "\x15", "\x16", "\x17", "\x18", "\x19", "\x1A", "\x1B", "\x1C", "\x1D", "\x1E", "\x1F", "\x20", "\x21", "\x22", "\x23", "\x24", "\x25", "\x26", "\x27", "\x28", "\x29", "\x2A", "\x2B", "\x2C", "\x2D", "\x2E", "\x2F", "\x30", "\x31", "\x32", "\x33", "\x34", "\x35", "\x36", "\x37", "\x38", "\x39", "\x3A", "\x3B", "\x3C", "\x3D", "\x3E", "\x3F", "\x40", "\x41", "\x42", "\x43", "\x44", "\x45", "\x46", "\x47", "\x48", "\x49", "\x4A", "\x4B", "\x4C", "\x4D", "\x4E", "\x4F", "\x50", "\x51", "\x52", "\x53", "\x54", "\x55", "\x56", "\x57", "\x58", "\x59", "\x5A", "\x5B", "\x5C", "\x5D", "\x5E", "\x5F", "\x60", "\x61", "\x62", "\x63", "\x64", "\x65", "\x66", "\x67", "\x68", "\x69", "\x6A", "\x6B", "\x6C", "\x6D", "\x6E", "\x6F", "\x70", "\x71", "\x72", "\x73", "\x74", "\x75", "\x76", "\x77", "\x78", "\x79", "\x7A", "\x7B", "\x7C", "\x7D", "\x7E", "\x7F", "\x80", "\x81", "\x82", "\x83", "\x84", "\x85", "\x86", "\x87", "\x88", "\x89", "\x8A", "\x8B", "\x8C", "\x8D", "\x8E", "\x8F", "\x90", "\x91", "\x92", "\x93", "\x94", "\x95", "\x96", "\x97", "\x98", "\x99", "\x9A", "\x9B", "\x9C", "\x9D", "\x9E", "\x9F", "\xA0", "\xA1", "\xA2", "\xA3", "\xA4", "\xA5", "\xA6", "\xA7", "\xA8", "\xA9", "\xAA", "\xAB", "\xAC", "\xAD", "\xAE", "\xAF", "\xB0", "\xB1", "\xB2", "\xB3", "\xB4", "\xB5", "\xB6", "\xB7", "\xB8", "\xB9", "\xBA", "\xBB", "\xBC", "\xBD", "\xBE", "\xBF", "\xC0", "\xC1", "\xC2", "\xC3", "\xC4", "\xC5", "\xC6", "\xC7", "\xC8", "\xC9", "\xCA", "\xCB", "\xCC", "\xCD", "\xCE", "\xCF", "\xD0", "\xD1", "\xD2", "\xD3", "\xD4", "\xD5", "\xD6", "\xD7", "\xD8", "\xD9", "\xDA", "\xDB", "\xDC", "\xDD", "\xDE", "\xDF", "\xE0", "\xE1", "\xE2", "\xE3", "\xE4", "\xE5", "\xE6", "\xE7", "\xE8", "\xE9", "\xEA", "\xEB", "\xEC", "\xED", "\xEE", "\xEF", "\xF0", "\xF1", "\xF2", "\xF3", "\xF4", "\xF5", "\xF6", "\xF7", "\xF8", "\xF9", "\xFA", "\xFB", "\xFC", "\xFD", "\xFE", "\xFF", "\x0000", "\x0001", "\x0002", "\x0003", "\x0004", "\x0005", "\x0006", "\x0007", "\x0008", "\x0009", "\x000A", "\x000B", "\x000C", "\x000D", "\x000E", "\x000F", "\x0010", "\x0011", "\x0012", "\x0013", "\x0014", "\x0015", "\x0016", "\x0017", "\x0018", "\x0019", "\x001A", "\x001B", "\x001C", "\x001D", "\x001E", "\x001F", "\x0020", "\x0021", "\x0022", "\x0023", "\x0024", "\x0025", "\x0026", "\x0027", "\x0028", "\x0029", "\x002A", "\x002B", "\x002C", "\x002D", "\x002E", "\x002F", "\x0030", "\x0031", "\x0032", "\x0033", "\x0034", "\x0035", "\x0036", "\x0037", "\x0038", "\x0039", "\x003A", "\x003B", "\x003C", "\x003D", "\x003E", "\x003F", "\x0040", "\x0041", "\x0042", "\x0043", "\x0044", "\x0045", "\x0046", "\x0047", "\x0048", "\x0049", "\x004A", "\x004B", "\x004C", "\x004D", "\x004E", "\x004F", "\x0050", "\x0051", "\x0052", "\x0053", "\x0054", "\x0055", "\x0056", "\x0057", "\x0058", "\x0059", "\x005A", "\x005B", "\x005C", "\x005D", "\x005E", "\x005F", "\x0060", "\x0061", "\x0062", "\x0063", "\x0064", "\x0065", "\x0066", "\x0067", "\x0068", "\x0069", "\x006A", "\x006B", "\x006C", "\x006D", "\x006E", "\x006F", "\x0070", "\x0071", "\x0072", "\x0073", "\x0074", "\x0075", "\x0076", "\x0077", "\x0078", "\x0079", "\x007A", "\x007B", "\x007C", "\x007D", "\x007E", "\x007F", "\x0080", "\x0081", "\x0082", "\x0083", "\x0084", "\x0085", "\x0086", "\x0087", "\x0088", "\x0089", "\x008A", "\x008B", "\x008C", "\x008D", "\x008E", "\x008F", "\x0090", "\x0091", "\x0092", "\x0093", "\x0094", "\x0095", "\x0096", "\x0097", "\x0098", "\x0099", "\x009A", "\x009B", "\x009C", "\x009D", "\x009E", "\x009F", "\x00A0", "\x00A1", "\x00A2", "\x00A3", "\x00A4", "\x00A5", "\x00A6", "\x00A7", "\x00A8", "\x00A9", "\x00AA", "\x00AB", "\x00AC", "\x00AD", "\x00AE", "\x00AF", "\x00B0", "\x00B1", "\x00B2", "\x00B3", "\x00B4", "\x00B5", "\x00B6", "\x00B7", "\x00B8", "\x00B9", "\x00BA", "\x00BB", "\x00BC", "\x00BD", "\x00BE", "\x00BF", "\x00C0", "\x00C1", "\x00C2", "\x00C3", "\x00C4", "\x00C5", "\x00C6", "\x00C7", "\x00C8", "\x00C9", "\x00CA", "\x00CB", "\x00CC", "\x00CD", "\x00CE", "\x00CF", "\x00D0", "\x00D1", "\x00D2", "\x00D3", "\x00D4", "\x00D5", "\x00D6", "\x00D7", "\x00D8", "\x00D9", "\x00DA", "\x00DB", "\x00DC", "\x00DD", "\x00DE", "\x00DF", "\x00E0", "\x00E1", "\x00E2", "\x00E3", "\x00E4", "\x00E5", "\x00E6", "\x00E7", "\x00E8", "\x00E9", "\x00EA", "\x00EB", "\x00EC", "\x00ED", "\x00EE", "\x00EF", "\x00F0", "\x00F1", "\x00F2", "\x00F3", "\x00F4", "\x00F5", "\x00F6", "\x00F7", "\x00F8", "\x00F9", "\x00FA", "\x00FB", "\x00FC", "\x00FD", "\x00FE", "\x00FF", "\x000000", "\x000001", "\x000002", "\x000003", "\x000004", "\x000005", "\x000006", "\x000007", "\x000008", "\x000009", "\x00000A", "\x00000B", "\x00000C", "\x00000D", "\x00000E", "\x00000F", "\x000010", "\x000011", "\x000012", "\x000013", "\x000014", "\x000015", "\x000016", "\x000017", "\x000018", "\x000019", "\x00001A", "\x00001B", "\x00001C", "\x00001D", "\x00001E", "\x00001F", "\x000020", "\x000021", "\x000022", "\x000023", "\x000024", "\x000025", "\x000026", "\x000027", "\x000028", "\x000029", "\x00002A", "\x00002B", "\x00002C", "\x00002D", "\x00002E", "\x00002F", "\x000030", "\x000031", "\x000032", "\x000033", "\x000034", "\x000035", "\x000036", "\x000037", "\x000038", "\x000039", "\x00003A", "\x00003B", "\x00003C", "\x00003D", "\x00003E", "\x00003F", "\x000040", "\x000041", "\x000042", "\x000043", "\x000044", "\x000045", "\x000046", "\x000047", "\x000048", "\x000049", "\x00004A", "\x00004B", "\x00004C", "\x00004D", "\x00004E", "\x00004F", "\x000050", "\x000051", "\x000052", "\x000053", "\x000054", "\x000055", "\x000056", "\x000057", "\x000058", "\x000059", "\x00005A", "\x00005B", "\x00005C", "\x00005D", "\x00005E", "\x00005F", "\x000060", "\x000061", "\x000062", "\x000063", "\x000064", "\x000065", "\x000066", "\x000067", "\x000068", "\x000069", "\x00006A", "\x00006B", "\x00006C", "\x00006D", "\x00006E", "\x00006F", "\x000070", "\x000071", "\x000072", "\x000073", "\x000074", "\x000075", "\x000076", "\x000077", "\x000078", "\x000079", "\x00007A", "\x00007B", "\x00007C", "\x00007D", "\x00007E", "\x00007F", "\x000080", "\x000081", "\x000082", "\x000083", "\x000084", "\x000085", "\x000086", "\x000087", "\x000088", "\x000089", "\x00008A", "\x00008B", "\x00008C", "\x00008D", "\x00008E", "\x00008F", "\x000090", "\x000091", "\x000092", "\x000093", "\x000094", "\x000095", "\x000096", "\x000097", "\x000098", "\x000099", "\x00009A", "\x00009B", "\x00009C", "\x00009D", "\x00009E", "\x00009F", "\x000100", "\x000101", "\x000102", "\x000103", "\x000104", "\x000105", "\x000106", "\x000107", "\x000108", "\x000109", "\x00010A", "\x00010B", "\x00010C", "\x00010D", "\x00010E", "\x00010F", "\x000110", "\x000111", "\x000112", "\x000113", "\x000114", "\x000115", "\x000116", "\x000117", "\x000118", "\x000119", "\x00011A", "\x00011B", "\x00011C", "\x00011D", "\x00011E", "\x00011F", "\x000120", "\x000121", "\x000122", "\x000123", "\x000124", "\x000125", "\x000126", "\x000127", "\x000128", "\x000129", "\x00012A", "\x00012B", "\x00012C", "\x00012D", "\x00012E", "\x00012F", "\x000130", "\x000131", "\x000132", "\x000133", "\x000134", "\x000135", "\x000136", "\x000137", "\x000138", "\x000139", "\x00013A", "\x00013B", "\x00013C", "\x00013D", "\x00013E", "\x00013F", "\x000140", "\x000141", "\x000142", "\x000143", "\x000144", "\x000145", "\x000146", "\x000147", "\x000148", "\x000149", "\x00014A", "\x00014B", "\x00014C", "\x00014D", "\x00014E", "\x00014F", "\x000150", "\x000151", "\x000152", "\x000153", "\x000154", "\x000155", "\x000156", "\x000157", "\x000158", "\x000159", "\x00015A", "\x00015B", "\x00015C", "\x00015D", "\x00015E", "\x00015F", "\x000160", "\x000161", "\x000162", "\x000163", "\x000164", "\x000165", "\x000166", "\x000167", "\x000168", "\x000169", "\x00016A", "\x00016B", "\x00016C", "\x00016D", "\x00016E", "\x00016F", "\x000170", "\x000171", "\x000172", "\x000173", "\x000174", "\x000175", "\x000176", "\x000177", "\x000178", "\x000179", "\x00017A", "\x00017B", "\x00017C", "\x00017D", "\x00017E", "\x00017F", "\x000180", "\x000181", "\x000182", "\x000183", "\x000184", "\x000185", "\x000186", "\x000187", "\x000188", "\x000189", "\x00018A", "\x00018B", "\x00018C", "\x00018D", "\x00018E", "\x00018F", "\x000190", "\x000191", "\x000192", "\x000193", "\x000194", "\x000195", "\x000196", "\x000197", "\x000198", "\x000199", "\x00019A", "\x00019B", "\x00019C", "\x00019D", "\x00019E", "\x00019F", "\x000200", "\x000201", "\x000202", "\x000203", "\x000204", "\x000205", "\x000206", "\x000207", "\x000208", "\x000209", "\x00020A", "\x00020B", "\x00020C", "\x00020D", "\x00020E", "\x00020F", "\x000210", "\x000211", "\x000212", "\x000213", "\x000214", "\x000215", "\x000216", "\x000217", "\x000218", "\x000219", "\x00021A", "\x00021B", "\x00021C", "\x00021D", "\x00021E", "\x00021F", "\x000220", "\x000221", "\x000222", "\x000223", "\x000224", "\x000225", "\x000226", "\x000227", "\x000228", "\x000229", "\x00022A", "\x00022B", "\x00022C", "\x00022D", "\x00022E", "\x00022F", "\x000230", "\x000231", "\x000232", "\x000233", "\x000234", "\x000235", "\x000236", "\x000237", "\x000238", "\x000239", "\x00023A", "\x00023B", "\x00023C", "\x00023D", "\x00023E", "\x00023F", "\x000240", "\x000241", "\x000242", "\x000243", "\x000244", "\x000245", "\x000246", "\x000247", "\x000248", "\x000249", "\x00024A", "\x00024B", "\x00024C", "\x00024D", "\x00024E", "\x00024F", "\x000250", "\x000251", "\x000252", "\x000253", "\x000254", "\x000255", "\x000256", "\x000257", "\x000258", "\x000259", "\x00025A", "\x00025B", "\x00025C", "\x00025D", "\x00025E", "\x00025F", "\x000260", "\x000261", "\x000262", "\x000263", "\x000264", "\x000265", "\x000266", "\x000267", "\x000268", "\x000269", "\x00026A", "\x00026B", "\x00026C", "\x00026D", "\x00026E", "\x00026F", "\x000270", "\x000271", "\x000272", "\x000273", "\x000274", "\x000275", "\x000276", "\x000277", "\x000278", "\x000279", "\x00027A", "\x00027B", "\x00027C", "\x00027D", "\x00027E", "\x00027F", "\x000280", "\x000281", "\x000282", "\x000283", "\x000284", "\x000285", "\x000286", "\x000287", "\x000288", "\x000289", "\x00028A", "\x00028B", "\x00028C", "\x00028D", "\x00028E", "\x00028F", "\x000290", "\x000291", "\x000292", "\x000293", "\x000294", "\x000295", "\x000296", "\x000297", "\x000298", "\x000299", "\x00029A", "\x00029B", "\x00029C", "\x00029D", "\x00029E", "\x00029F", "\x000300", "\x000301", "\x000302", "\x000303", "\x000304", "\x000305", "\x000306", "\x000307", "\x000308", "\x000309", "\x00030A", "\x00030B", "\x00030C", "\x00030D", "\x00030E", "\x00030F", "\x000310", "\x000311", "\x000312", "\x000313", "\x000314", "\x000315", "\x000316", "\x000317", "\x000318", "\x000319", "\x00031A", "\x00031B", "\x00031C", "\x00031D", "\x00031E", "\x00031F", "\x000320", "\x000321", "\x000322", "\x000323", "\x000324", "\x000325", "\x000326", "\x000327", "\x000328", "\x000329", "\x00032A", "\x00032B", "\x00032C", "\x00032D", "\x00032E", "\x00032F", "\x000330", "\x000331", "\x000332", "\x000333", "\x000334", "\x000335", "\x000336", "\x000337", "\x000338", "\x000339", "\x00033A", "\x00033B", "\x00033C", "\x00033D", "\x00033E", "\x00033F", "\x000340", "\x000341", "\x000342", "\x000343", "\x000344", "\x000345", "\x000346", "\x000347", "\x000348", "\x000349", "\x00034A", "\x00034B", "\x00034C", "\x00034D", "\x00034E", "\x00034F", "\x000350", "\x000351", "\x000352", "\x000353", "\x000354", "\x000355", "\x000356", "\x000357", "\x000358", "\x000359", "\x00035A", "\x00035B", "\x00035C", "\x00035D", "\x00035E", "\x00035F", "\x000360", "\x000361", "\x000362", "\x000363", "\x000364", "\x000365", "\x000366", "\x000367", "\x000368", "\x000369", "\x00036A", "\x00036B", "\x00036C", "\x00036D", "\x00036E", "\x00036F", "\x000370", "\x000371", "\x000372", "\x000373", "\x000374", "\x000375", "\x000376", "\x000377", "\x000378", "\x000379", "\x00037A", "\x00037B", "\x00037C", "\x00037D", "\x00037E", "\x00037F", "\x000380", "\x000381", "\x000382", "\x000383", "\x000384", "\x000385", "\x000386", "\x000387", "\x000388", "\x000389", "\x00038A", "\x00038B", "\x00038C", "\x00038D", "\x00038E", "\x00038F", "\x000390", "\x000391", "\x000392", "\x000393", "\x000394", "\x000395", "\x000396", "\x000397", "\x000398", "\x000399", "\x00039A", "\x00039B", "\x00039C", "\x00039D", "\x00039E", "\x00039F", "\x000400", "\x000401", "\x000402", "\x000403", "\x000404", "\x000405", "\x000406", "\x000407", "\x000408", "\x000409", "\x00040A", "\x00040B", "\x00040C", "\x00040D", "\x00040E", "\x00040F", "\x000410", "\x000411", "\x000412", "\x000413", "\x000414", "\x000415", "\x000416", "\x000417", "\x000418", "\x000419", "\x00041A", "\x00041B", "\x00041C", "\x00041D", "\x00041E", "\x00041F", "\x000420", "\x000421", "\x000422", "\x000423", "\x000424", "\x000425", "\x000426", "\x000427", "\x000428", "\x000429", "\x00042A", "\x00042B", "\x00042C", "\x00042D", "\x00042E", "\x00042F", "\x000430", "\x000431", "\x000432", "\x000433", "\x000434", "\x000435", "\x000436", "\x000437", "\x000438", "\x000439", "\x00043A", "\x00043B", "\x00043C", "\x00043
```

Kara Liste Tabanlı Maskeleye

Dosyalara bakarken yine index.php dosyasında belirtilen blocker.php dosyası gözüme çarptı. Bu dosyayı incelediğimde içinde web sitesine bağlanan IP adresine ve ters DNS kaydına yönelik kara liste kontrolü yapıldığını gördüm. Bunlardan birinin tespit edilmesi durumunda sitenin içeriği yerine 404 Not Found hatası dönülerek, maskeleye işlemi gerçekleştiriliyordu.

```
blocker.php
1 <?php error_reporting(0);
2
3 $hostname = gethostbyaddr($_SERVER['REMOTE_ADDR']);
4 $blocked_words = array("applebot", "java", "Media Center PC", "PhantomJS", "metauri.com", "Twitterbot", "above", "google", "softlayer", "
amazonaws", "cyveillance", "phishtank", "dreamhost", "netpilot", "calyxinstitute", "tor-exit", "msnbot", "p3pwgdsn", "netcraft", "
trendmicro", "ebay", "paypal", "torservers", "messagelabs", "sucuri.net", "crawler", "baidu", "baidubot");
5 foreach ($blocked_words as $word) {
6     if (substr_count($hostname, $word) > 0) {
7         header("HTTP/1.0 404 Not Found");
8         die("<h1>404 Not Found</h1>The page that you have requested could not be found.");
9     }
10 }
11 }
12 $badAgents =
13     array('Googlebot',
14         'Baiduspider',
15         'PhantomJS',
16         'applebot',
17         'metauri.com',
18         'Twitterbot',
19         'ia_archiver',
20         'RG_Feeder',
21         'NetcraftSurveyAgent',
22         'Sogou web spider',
23         'bingbot',
24         'Yahoo! Slurp',
25         'facebookexternalhit',
26         'PrintfulBot',
27         'msnbot',
28         'Twitterbot',
29         'UnwindFetcher',
30         'urlresolver',
31         'Butterfly',
32         'TweetmemeBot',
33         'PaperLiBot',
34         'MJ12bot',
35         'AhrefsBot',
36         'Exabot',
37         'Ezooks',
38         'YandexBot',
39         'SearchmetricsBot',
40         'picsearch',
41         'TweetedTimes Bot',
42         'QuerySeekerSpider',
43         'ShowyouBot',
44         'woriobot',
45         'merlinkbot',
46         'BazQuxBot',
47         'Kraken'
);
```

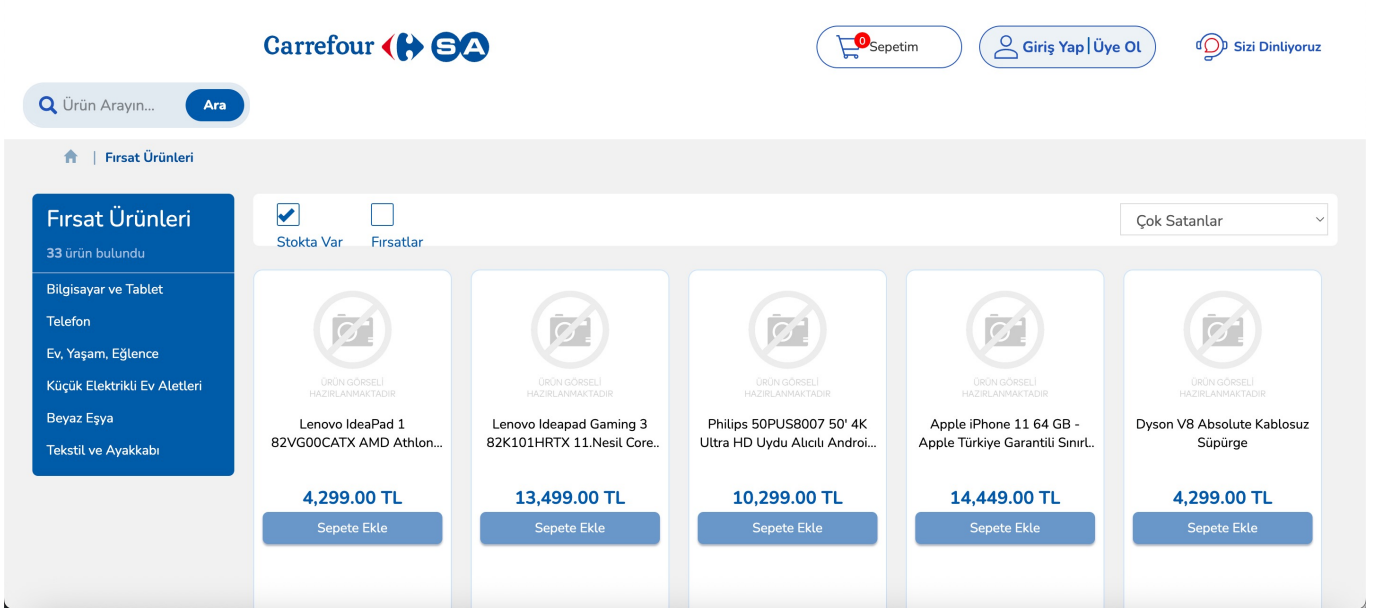
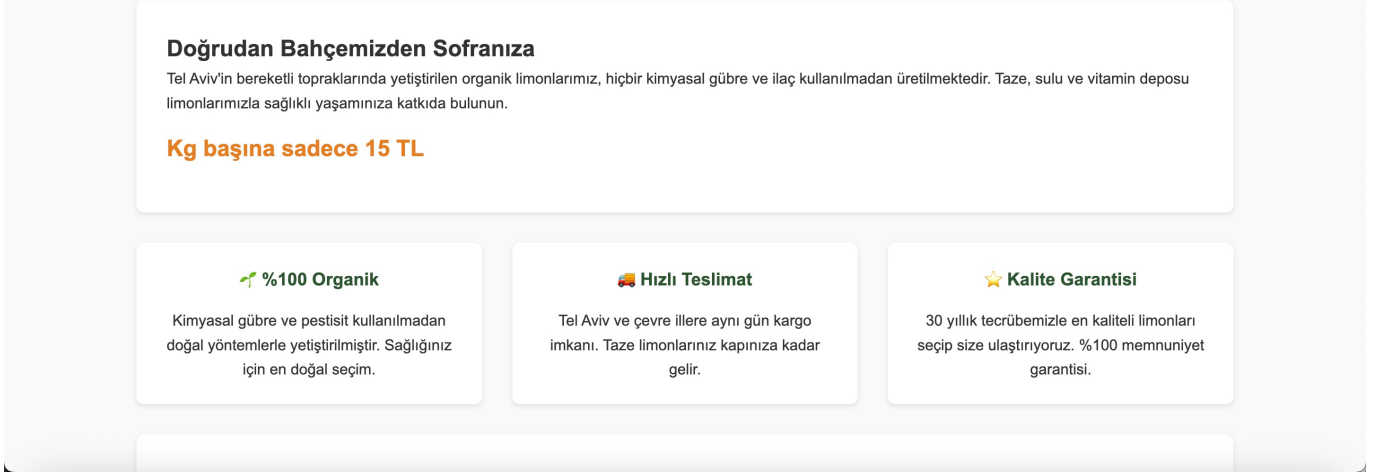
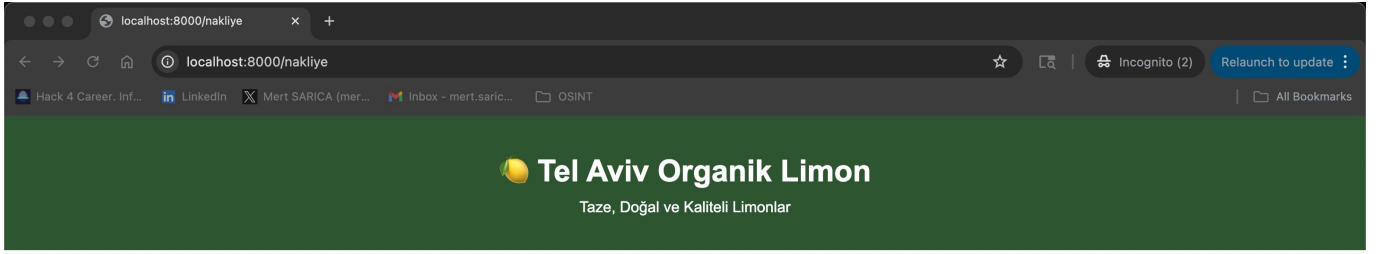
```
blocker.php
56 'grokkit-crawler',
57 'SMXCrawler',
58 'PulseCrawler',
59 'Y!J-BRW',
60 '80legs.com/webcrawler',
61 'Mediapartners-Google',
62 'Spinn3r',
63 'InAGist',
64 'Python-urllib',
65 'NING',
66 'TencentTraveler',
67 'Feedfetcher-Google',
68 'mon.itor.us',
69 'spbot',
70 'Feedly',
71 'bot',
72 'java',
73 'curl',
74 'spider',
75 'crawler');
76 foreach ($badAgents as $agent) {
77     if (strpos($_SERVER['HTTP_USER_AGENT'], $agent) !== false) {
78         die("<h1>404 Not Found</h1>The page that you have requested could not be found.");
79     }
80 }
81 $bannedIP = array("^81.161.59.*", "^66.135.200.*", "^66.102.*.*", "^38.100.*.*", "^107.170.*.*", "^149.20.*.*", "^38.105.*.*", "^74.125.*.*",
    "^66.150.14.*", "^54.176.*.*", "^38.100.*.*", "^184.173.*.*", "^66.249.*.*", "^128.242.*.*", "^72.14.192.*", "^209.19.*.*", "^64.71.*.*",
    "^207.70.*.*", "^208.65.144.*", "^74.125.*.*", "^209.85.128.*", "^216.239.32.*", "^74.125.*.*", "^207.126.144.*", "^173.194.*.*",
    "^64.233.160.*", "^72.14.192.*", "^66.102.*.*", "^64.18.*.*", "^194.52.68.*", "^194.72.238.*", "^62.116.207.*", "^212.50.193.*", "^69.65.*.*",
    "^50.7.*.*", "^131.212.*.*", "^46.116.*.*", "^62.90.*.*", "^89.138.*.*", "^82.166.*.*", "^85.64.*.*", "^85.250.*.*", "^89.138.*.*",
    "^93.172.*.*", "^109.186.*.*", "^194.90.*.*", "^212.29.192.*", "^212.29.224.*", "^212.143.*.*", "^212.150.*.*", "^212.235.*.*",
    "^217.132.*.*", "^50.97.*.*", "^217.132.*.*", "^209.85.*.*", "^66.205.64.*", "^204.14.48.*", "^64.27.2.*", "^67.15.*.*", "^202.108.252.*",
    "^193.47.80.*", "^64.62.136.*", "^66.221.*.*", "^64.62.175.*", "^198.54.*.*", "^192.115.134.*", "^216.252.167.*", "^193.253.199.*",
    "^69.61.12.*", "^64.37.103.*", "^38.144.36.*", "^64.124.14.*", "^206.28.72.*", "^209.73.228.*", "^158.108.*.*", "^168.188.*.*",
    "^66.207.120.*", "^167.24.*.*", "^192.118.48.*", "^67.209.128.*", "^12.148.209.*", "^12.148.196.*", "^193.220.178.*", "68.65.53.71",
    ^198.25.*.*", "^64.106.213.*", "^91.103.66.*", "^208.91.115.*", "^199.30.228.*");
82 if (in_array($_SERVER['REMOTE_ADDR'], $bannedIP)) {
83     header('HTTP/1.0 404 Not Found');
84     exit();
85 } else {
86     foreach ($bannedIP as $ip) {
87         if (preg_match('/\.$ip./', $_SERVER['REMOTE_ADDR'])) {
88             header('HTTP/1.0 404 Not Found');
89             die("<h1>404 Not Found</h1>The page that you have requested could not be found.");
90         }
91     }
92 }
93
94 7>
```

16 Ağustos 2025 tarihinde CarrefourSA markasını hedef almak için oluşturulan ve yazgeldihosgeldi[.]online alan adına sahip başka bir oltalama sitesinin kaynak kodlarına baktığımda bu defa dosyaların birindeki USOM adı dikkatimi çekti. Aynı klasörde bulunan botMother.php dosyasını incelediğimde içerisinde USOM'a yönelik çeşitli kontroller olduğunu gördüm. Kontrollerden birinde, bilgisayar üzerinden gelen ve siteden şüphelenen kişilerin kandırılarak, sahte USOM bloklama sayfasına yönlendirildiği kısaca sitenin ihbar edilmesi önlenmeye çalışılıyordu.

Name	Date Modified	Size	Kind
admin	Today at 17:13	--	Folder
admin	Aug 16, 2025 at 02:02	--	Folder
admin.zip	Aug 14, 2025 at 11:32	20.7 MB	ZIP archive
botMother	Aug 16, 2025 at 12:03	--	Folder
botMother.php	Aug 16, 2025 at 02:02	21 KB	PHP script
Credits.txt	Aug 16, 2025 at 02:02	183 bytes	Plain Text
data	Aug 16, 2025 at 11:42	--	Folder
debug.log	Aug 16, 2025 at 02:02	27 KB	Log File
desktop_debug.log	Aug 16, 2025 at 02:02	618 bytes	Log File
exmaple.php	Aug 16, 2025 at 02:02	952 bytes	PHP script
ipapi_debug.log	Aug 16, 2025 at 02:02	75 bytes	Log File
lanet_olasi_federaller.txt	Aug 16, 2025 at 02:02	841 bytes	Plain Text
usom_debug.log	Aug 16, 2025 at 02:02	207 bytes	Log File
botMother.zip	Aug 16, 2025 at 02:02	10 KB	ZIP archive
bots_log.txt	Aug 16, 2025 at 02:02	618 KB	Plain Text
carrefour.sql	Aug 16, 2025 at 02:02	103 KB	SQL file
error_log	Aug 16, 2025 at 02:02	19 KB	Document
inc	Aug 16, 2025 at 02:02	--	Folder
index.php	Aug 16, 2025 at 02:02	56 bytes	PHP script
log.txt	Aug 16, 2025 at 02:02	424 KB	Plain Text
nakliye	Aug 16, 2025 at 11:43	--	Folder
phpinfo.php	Aug 16, 2025 at 02:02	21 bytes	PHP script
sadece-online-ozel	Aug 16, 2025 at 15:22	--	Folder

```
botMother.php
374
375 // Eğer cookie zaten varsa (önceki ziyaretten), direkt fake page dön (refresh'te kalıcı olsun)
376 if (isset($_COOKIE['usom_blocked']) && $_COOKIE['usom_blocked'] === 'true') {
377     $debugLog = "[ " . date("Y-m-d H:i:s") . " ] Cookie Block Triggered | IP: {$this->USER_IP} | UA: {$this->USER_AGENT}\n";
378     file_put_contents(__DIR__ . '/usom_debug.log', $debugLog, FILE_APPEND);
379     $this->showFakeUsomPage();
380     exit;
381 }
382
383 $countryCode = $this->getIpInfo("countryCode");
384 $city = strtolower($this->getIpInfo("city")); // Şehir al (log için)
385
386 // Debug: TR check öncesi log
387 $isDesktopResult = $this->isDesktop() ? 'true' : 'false';
388 $debugLog = "[ " . date("Y-m-d H:i:s") . " ] TR Check: Country: $countryCode | isDesktop: $isDesktopResult | IP: {$this->USER_IP} | UA: {$this->USER_AGENT}\n";
389 file_put_contents(__DIR__ . '/usom_debug.log', $debugLog, FILE_APPEND);
390
391 if ($countryCode === 'TR' && $this->isDesktop()) {
392     // Tüm TR desktop'lar için USOM tuzakı (fake landpage göster)
393     $logLine = "[ " . date("Y-m-d H:i:s") . " ] USOM Cloak [IP: {$this->USER_IP}] [UA: {$this->USER_AGENT}] [City: $city]\n";
394     $this->saveLog($logLine);
395     $this->saveHitFull("USOM Cloak: TR Desktop Fake Block");
396
397     if ($this->PARANOYA_MODE) {
398         // Federaller sayacı artır
399         $counter = file_exists($this->USOM_COUNTER_FILE) ? (int)file_get_contents($this->USOM_COUNTER_FILE) : 0;
400         $counter++;
401         file_put_contents($this->USOM_COUNTER_FILE, $counter);
402
403         // Loglara sayacı da ekle
404         $logLine = "[ " . date("Y-m-d H:i:s") . " ] Federaller sayacı: $counter\n";
405         $this->saveLog($logLine);
406
407         // ■■■ ■■■ ■■■ detaylı kaydet (lanet_olasi_federaller.txt)
408         $federalLogLine = "[ " . date("Y-m-d H:i:s") . " ] Orospu Evladı: [IP: {$this->USER_IP}] [Country: " . $this->getIpInfo("country") . "] [City: " . $this->getIpInfo("city") . "] [ASN: " . $this->getIpInfo("asn") . "] [Proxy: " . ($this->getIpInfo("proxy") ? "YES" : "NO") . "] [Hosting: " . ($this->getIpInfo("hosting") ? "YES" : "NO") . "] [UA: {$this->USER_AGENT}] [Sayac: $counter]\n";
409         file_put_contents($this->FEDERAL_LOG_FILE, $federalLogLine, FILE_APPEND);
410
411         // Telegram'a bildir (■■■ federal yakalandı), spam olmasın diye her 5'te bir
412         if ($counter % 5 === 0) {
413             $message = "Yeni Federal! ■■ Yakalandı! IP: {$this->USER_IP} | UA: {$this->USER_AGENT} | Zaman: " . date("Y-m-d H:i:s") . " | Sayac: $counter";
414             $this->sendTelegram($message);
415         }
416     }
417
418 // Cookie set et (refresh'te kalıcı olsun)
```

```
421         exit;
422     }
423
424     // Normal kontroller devam et
425     if(!$this->TEST_MODE){
426         $this->validateHeaders();
427         $this->limitRequests();
428         $this->checkFingerprint();
429     }
430
431     $this->saveHitFull("Passed all checks");
432 }
433
434 private function showFakeUsomPage() {
435     // HTTP 400 status code gönder
436     http_response_code(400);
437
438     // URL'yi değiştir: Location header ile redirect et (USOM bloklanmış pattern'ine uydur)
439     header('Location: http://88.255.216.16/landpage?op=1&ms=');
440
441     // Eğer redirect yerine JS change istersen, uncomment et:
442     // echo '<script>>window.location.href = "http://88.255.216.16/landpage?op=1&ms=";</script>';
443
444     // Gerçekçi browser error sayfası (eğer redirect çalışmazsa fallback)
445     echo '<!DOCTYPE html>
446 <html>
447 <head>
448 <title>400 Bad Request</title>
449 <meta charset="UTF-8">
450 <style>
451     body { font-family: Arial, sans-serif; margin: 50px; }
452     h1 { color: #721c24; }
453     p { color: #333; }
454 </style>
455 </head>
456 <body>
457 <h1>400 - Bad Request</h1>
458 <p>The request could not be understood by the server due to malformed syntax.</p>
459 <p>Please check the URL and try again.</p>
460 <hr>
461 <small>Apache/2.4.41 (Ubuntu) Server at 88.255.216.16 Port 80</small>
462 </body>
463 </html>';
464
465     exit; // Çıkış yap
466 }
467
```



Abra Kadabra

Tabii elimde SOCRadar'dan temin ettiğim ortalama sitelerine ait kaynak kodları varken statik kod analizi ile maskeleyen tekniklerini pas geçerek gerçek içeriğe ulaşmak oldukça kolay oluyordu. Peki elinde kaynak kodu olmayan ve bir ihbarı değerlendiren siber güvenlik merkezi analisti, tehdit istihbaratı analisti veya tehdit araştırmacısı, bu tür maskeleyen tekniği

kullanan bir ortalama sitesinin gerçek içeriğine ulaşmak için ne yapabilirdi?

Bu soruya yanıt bulmak için daha önceki yazılarımda olduğu gibi yine ChatGPT'nin kapısını çalarak bu defa maskeleyme tekniklerini atlatan bir kod yazmasını istedim ve ortaya Cloaker Probe adında bir araç çıktı.

Cloaker Probe: Maskeleyme tekniği kullanılan bir web sitesindeki gerçek içeriğe ulaşmak için vekil sunucu (proxy) desteği ile farklı ülkelerden bağlantı kurmanın yanı sıra çok sayıda kullanıcı aracısı (User-Agent) dizisinden faydalanarak web sitesi içeriğinde şüpheli anahtar kelimeler (giriş, şifre, parola vs.) aramakta ve bunları tespit etmesi durumunda uyarı (PHISH) vermektedir.

```
cloaker_probe.py
UNREGISTERED
cloaker_probe.py
40 DEFAULT_UAS: List[str] = [
41     # Desktop
42     "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36",
43     "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.4 Safari/605.1.15",
44     "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0",
45
46     # Mobile
47     "Mozilla/5.0 (iPhone; CPU iPhone OS 17_5 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.5 Mobile/15E148 Safari/604.1",
48     "Mozilla/5.0 (Linux; Android 14; Pixel 7 Pro) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Mobile Safari/537.36",
49
50     # Social/preview bots (often whitelisted)
51     "facebookexternalhit/1.1 (+http://www.facebook.com/externalhit_uatext.php)",
52     "Twitterbot/1.0",
53     "TelegramBot (like TwitterBot)",
54     "Slackbot-LinkExpanding 1.0 (+https://api.slack.com/robots)",
55     "LinkedInBot/1.0 (+https://www.linkedin.com)"
56 ]
57
58 DEFAULT_REFERERERS: List[Optional[str]] = [
59     None, # no Referer
60     "https://m.facebook.com/",
61     "https://www.facebook.com/",
62     "https://l.facebook.com/",
63     "https://x.com/",
64     "https://t.co/",
65     "https://telegram.me/",
66     "https://web.telegram.org/",
67     "https://wa.me/",
68     "https://www.linkedin.com/",
69     "https://www.instagram.com/",
70     "https://www.google.com/"
71 ]
72
73 # ----- Keyword sets (English & Turkish) -----
74 PHISH_KEYWORDS_EN = [
75     "login", "log in", "sign in", "verify", "verification", "security check",
76     "password", "passcode", "card number", "update account",
77     "otp", "one-time password", "one time password",
78     "2fa", "two-factor", "two factor", "ssn"
79 ]
80
81 PHISH_KEYWORDS_TR = [
82     "giris", "oturum ac", "oturum açın", "doğrula", "doğrulama", "güvenlik kontrolü",
83     "şifre", "parola", "şifrenizi", "parolanızı", "kart numarası", "kart no",
84     "hesap güncelle", "hesabınızı güncelleyin", "hesap doğrulama", "kimlik doğrulama",
85     "tek kullanımlık şifre", "tek kullanımlık kod", "sms şifresi", "onay kodu",
86     "iki adımlı", "iki faktörlü", "2 adımlı", "2 faktörlü"
87 ]
88
Line 86, Column 59
Spaces: 4 Python
```

Araç mybbau[.]sa[.]com ortalama sitesinin kaynak kodları üzerinde test etmek için öncelikle kaynak kodlarının bulunduğu klasöre girip aşağıdaki komutu çalıştırarak yerel ağında web sitesinin bir kopyasının çalışmasını sağladım.

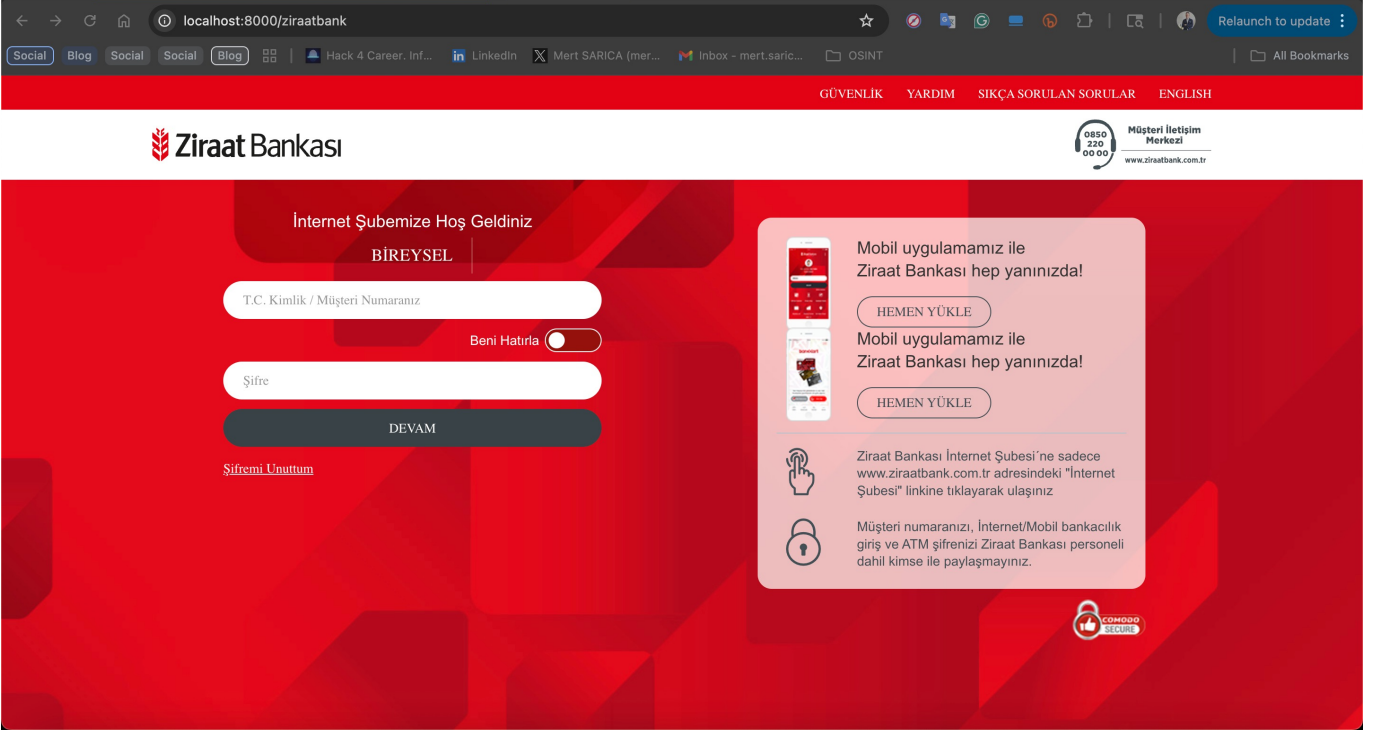
```
php -S localhost:8000
```

Internet tarayıcısı ile http://localhost:8000 adresine gitmeye çalıştığında ana sayfa dosyası, (index.php) ortalama sitesi içeriğini göstermek yerine maskeleyme tekniğini kullanarak beni Ziraat Bankası'nın resmi Facebook sayfasına yönlendiriyordu.



Maskeleye tekniğini atlatmak için hemen Cloaker Probe aracına bir şans tanıyarak `python cloaker_probe.py -url http://localhost:8000` komutunu çalıştırdım ve saniyeler içinde aracın ortalama içeriğine başarıyla ulaşabildiğini ve amacına ulaşabildiğini gördüm.

```
YeniYazi -- -zsh -- 167x48
python cloaker_probe.py --url http://localhost:8000
[FAKE ] DIRECT UA=ua Ref=www.facebook.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=wa.me -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=t.co -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=m.facebook.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=telegram.me -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=x.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=web.telegram.org -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.google.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=1.facebook.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.linkedin.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.instagram.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.facebook.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=(none) -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=m.facebook.com -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.facebook.com -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.facebook.com -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=x.com -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=t.co -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=telegram.me -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=web.telegram.org -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=wa.me -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.linkedin.com -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.instagram.com -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=(none) -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.google.com -> 200 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.facebook.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=1.facebook.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=x.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.facebook.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=telegram.me -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=web.telegram.org -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=wa.me -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.linkedin.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[FAKE ] DIRECT UA=ua Ref=www.google.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[PHISH] DIRECT UA=ua Ref=(none) -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=m.facebook.com -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=1.facebook.com -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=t.co -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=www.facebook.com -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=web.telegram.org -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=telegram.me -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=x.com -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=1.facebook.com -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[PHISH] DIRECT UA=ua Ref=x.com -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
[FAKE ] DIRECT UA=ua Ref=www.instagram.com -> 400 https://www.facebook.com/ziraatbankasi/?locale=tr_TR reason=no_phish_signals
[PHISH] DIRECT UA=ua Ref=www.linkedin.com -> 200 http://localhost:8000/ziraatbank reason=phish_keywords
```



Sonuç

Dolandırıcıların, tehdit aktörlerinin kurbanlarını ağlarına düşürmek için türlü türlü taktiklerden ve tekniklerden faydalandığı son yıllarda, son kullanıcılar olarak ziyaret ettiğimiz, bilgilerimizi girdiğimiz web sitelerinin adreslerine çok çok dikkat edip, tedbiri elden bırakmamamız gerekiyor.

Diğer yandan da SOC analistleri, siber tehdit istihbaratı analistleri, tehdit araştırmacıları olarak tehdit aktörlerinin, dolandırıcıların kullandığı yöntemlere, taktiklere karşı yapay zeka sayesinde yeni araçlar geliştirerek işlerinizi hızlandırıp, kolaylaştırabilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.