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

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 maskeleme taktiğinden faydalanmaktadırlar. Ben de bu yazımda farkındalık yaratması adına maskeleme tekniklerinden en çok kullanılanlarına ve bunları basit bir şekilde atlatmak amacıyla yapay zekaya geliştirttiğim 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.

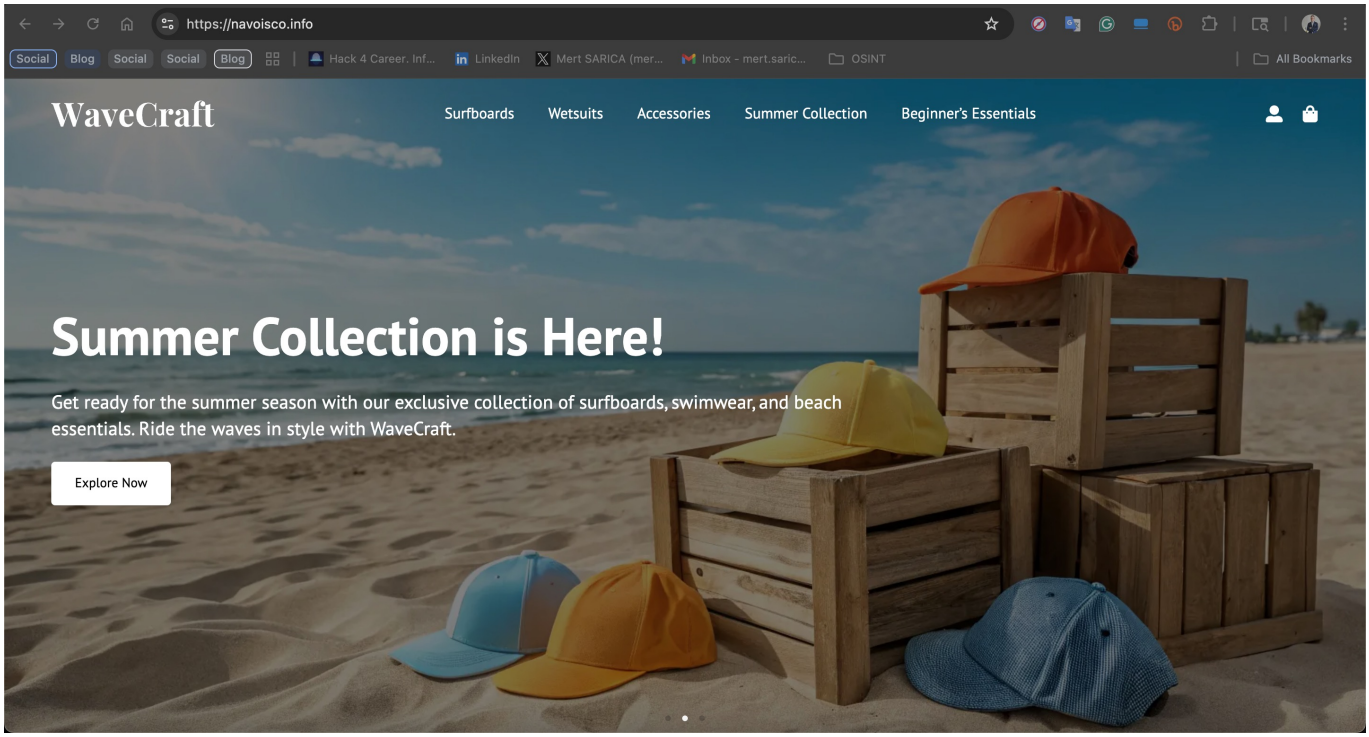
Öncelikle maskeleme tekniği kullanılan oltalama siteleri üzerinde güvenlik araştırması yapabilmek için oltalama sitelerinin kaynak koduna ihtiyacım vardı. Ha deyince bunlara ulaşmak pratikte pek mümkün olamayacağı için önceki yazılarımda olduğu gibi SOCRadar’ın yardımına başvurmaya verdim. :)

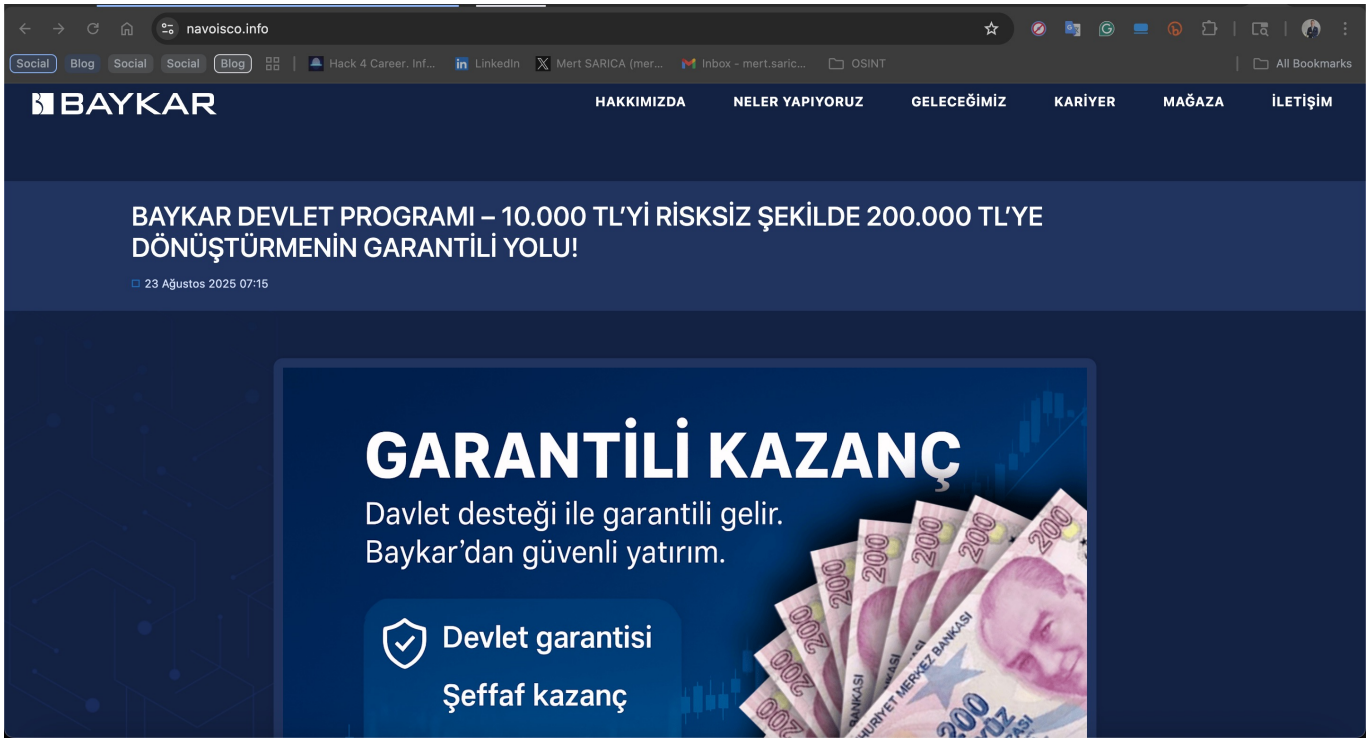
SOCRadar platformu oltalama (phishing) sitelerini sadece tespit etmekle kalmayıp bunların arkasındaki tehdit aktörlerine ulaşabilmek için yeri geldiğinde kaynak kodlarını da elde edebildiği için Türk vatandaşlarını hedef alan 500 tane oltalama sitesine ait kaynak kodunu temin edip, üzerinde güvenlik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

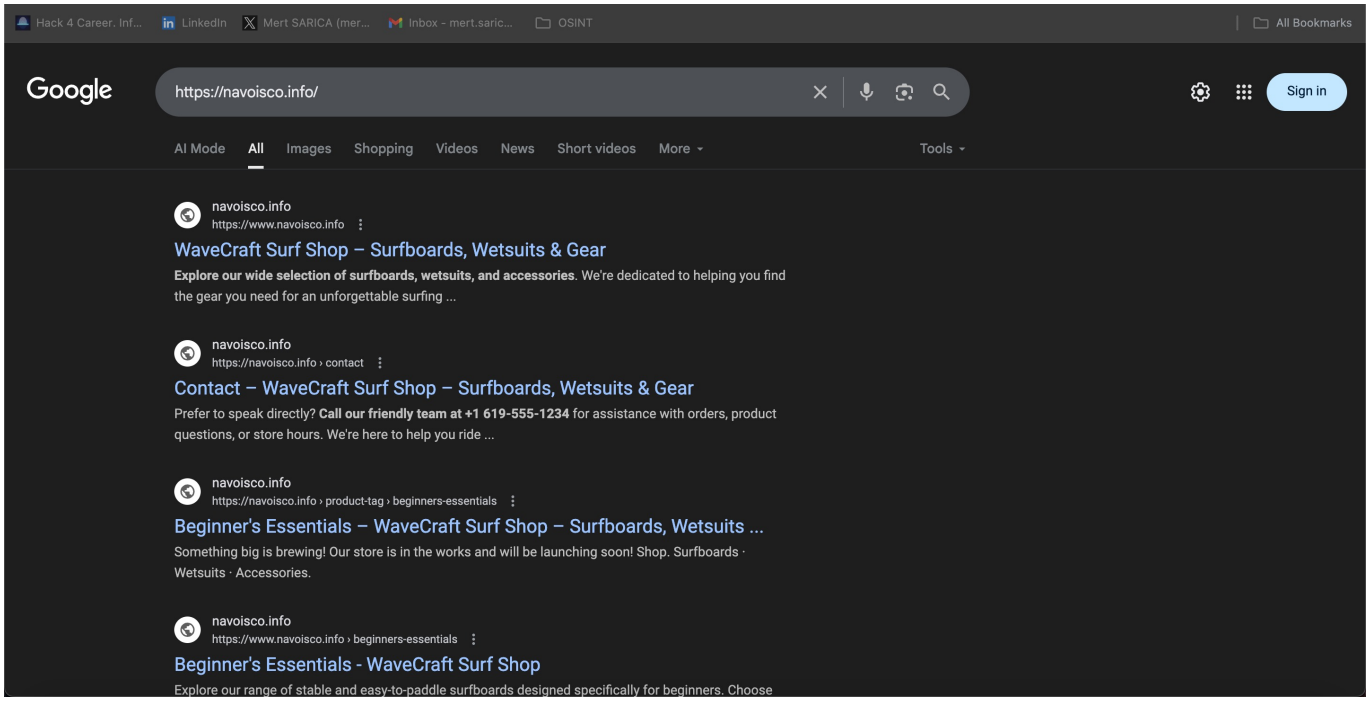
Coğrafi Maskeleme

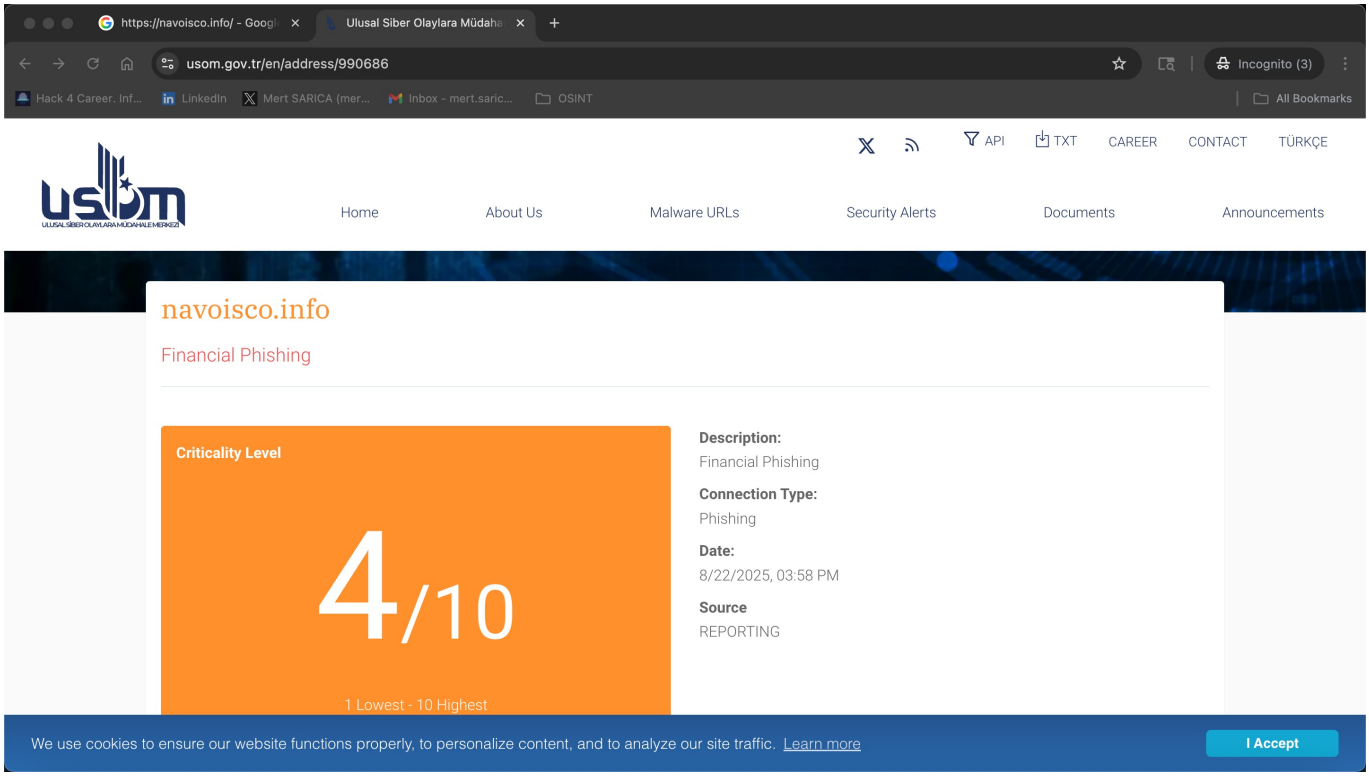
İlk olarak Yatırım Dolandırıcıları blog yazıma konu olan tehdit aktörüne ait bir web sitesini inceledim. Bir yıldır dolandırıcılık operasyonlarına hız kesmeden devam eden bu tehdit aktörü, 6 Ağustos 2025 tarihinde navoisco[.]info isimli alan adını kayıt edip, 13 Ağustos 2025 tarihinde ise web sitesini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

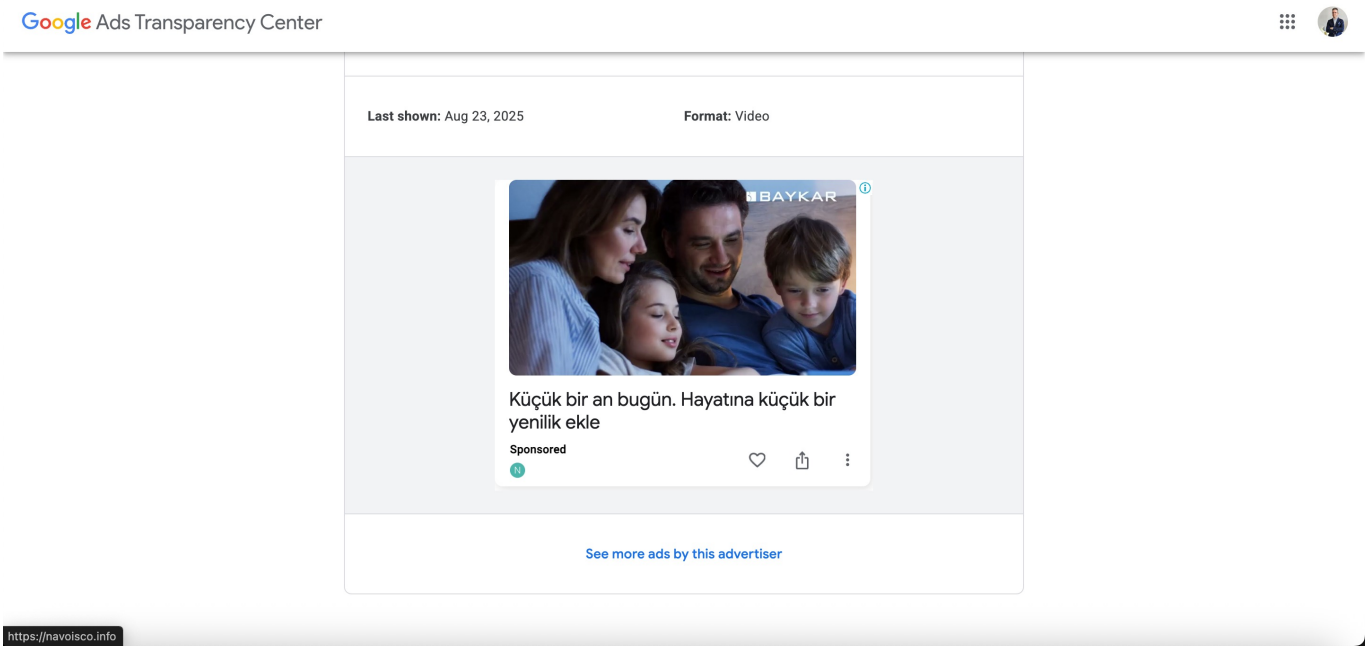
Bu web sitesini yurt dışından ziyaret ettiğinizde karşınıza sörf ürünleri satan bir içerik geliyordu fakat Türkiye'den ziyaret ettiğinizde bu defa Baykar savunma şirketinin adını kullarak dolandırıcılık faliyeti gerçekleştiren, kısaca Coğrafi Maskeleme tekniği kullanan bir web sayfası olarak karşınıza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





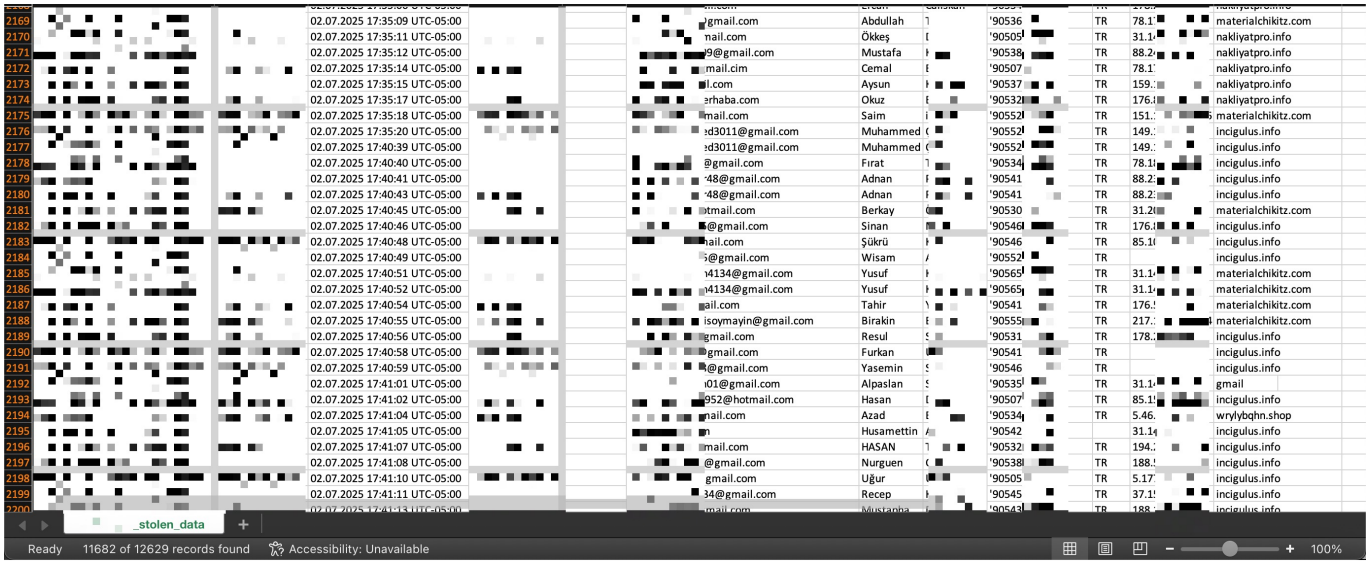

Hack 4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
OSINT
All Bookmarks
Google
https://navoisco.info/
Sign in
AI Mode
All
Images
Shopping
Videos
News
Short videos
More
Tools
navoisco.info
https://www.navoisco.info
WaveCraft Surf Shop – Surfboards, Wetsuits & Gear
Explore our wide selection of surfboards, wetsuits, and accessories. We're dedicated to helping you find the gear you need for an unforgettable surfing ...
navoisco.info
https://navoisco.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 ...
navoisco.info
https://navoisco.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.
navoisco.info
https://www.navoisco.info › beginners-essentials
Beginner's Essentials - WaveCraft Surf Shop
Explore our range of stable and easy-to-paddle surfboards designed specifically for beginners. Choose


https://navoisco.info/ - Googl
Ulusal Siber Olaylara Müdaha
usom.gov.tr/en/address/990686
Incognito (3)
Hack 4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
OSINT
All Bookmarks
API
TXT
CAREER
CONTACT
TÜRKÇE
Home
About Us
Malware URLs
Security Alerts
Documents
Announcements
navoisco.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



Not: Yaklaşık bir yılı aşkın süredir takip ettiğim ve Rus olduklarına kanaat getirdiğim, operasyonlarını ise ağırlıkla 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 oltalama (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	volumeviin.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	volumeviin.com
test@gmail.com	test	test	'380991292992	UA	185.237.75.100	volumeviin.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	тест	тест	'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

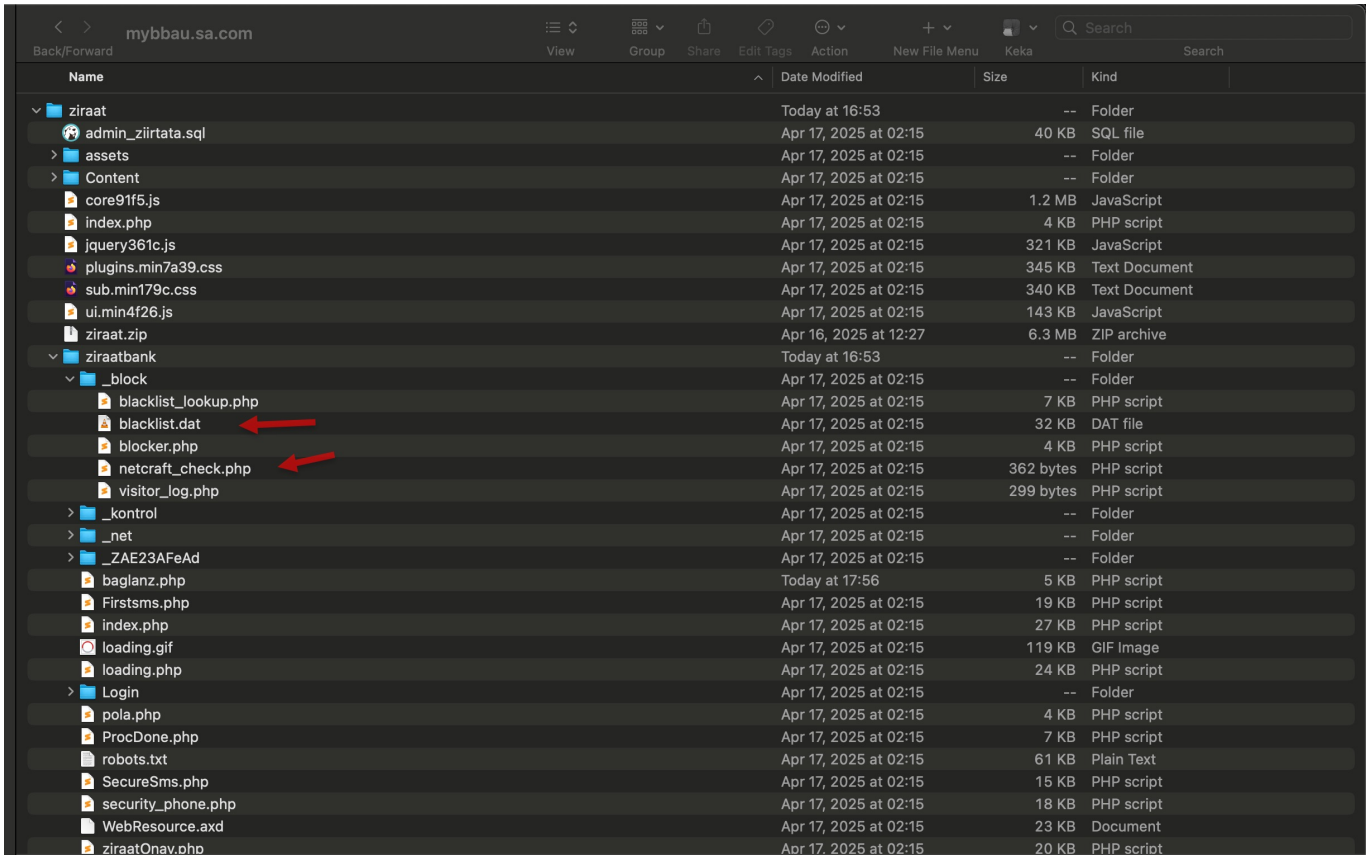


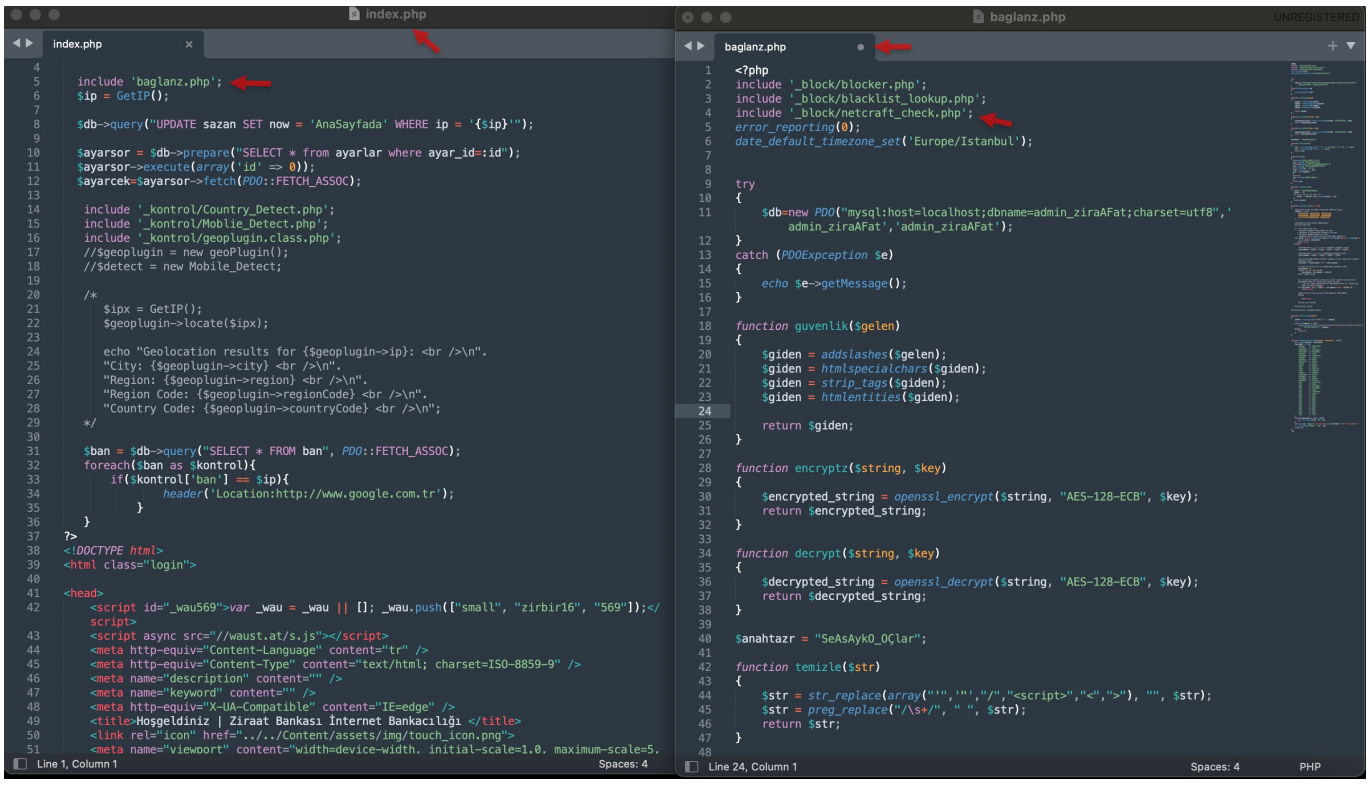
Kullanıcı Aracısı (User-Agent) Tabanlı Maskeleme

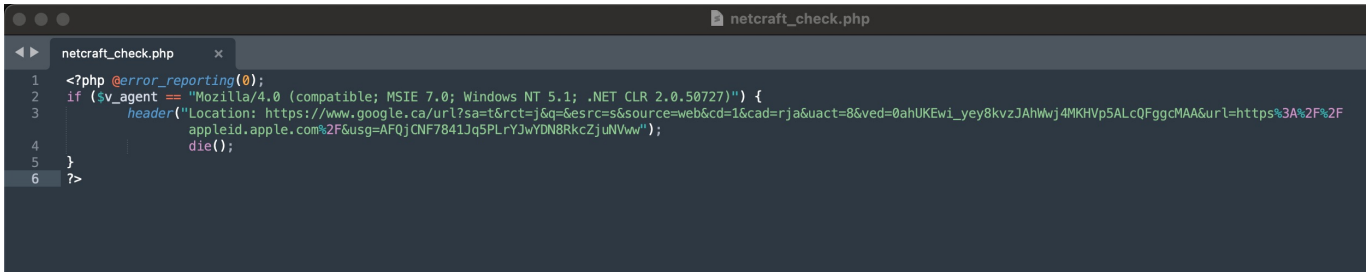
İkinci olarak 17 Nisan 2025 tarihinde Ziraat Bankası müşterilerini hedef alan mybbau[.]sa[.]com oltalama sitesine ait kaynak kodlarını incelemeye başladım ve dosyalar arasında netcraft_check.php isimli dosya dikkatimi çekti.

Netcraft, 1995’ten beri faaliyet gösteren İngiltere merkezli bir siber güvenlik ve internet ölçümleme 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 maskeleme işlemi gerçekleştiriyordu.

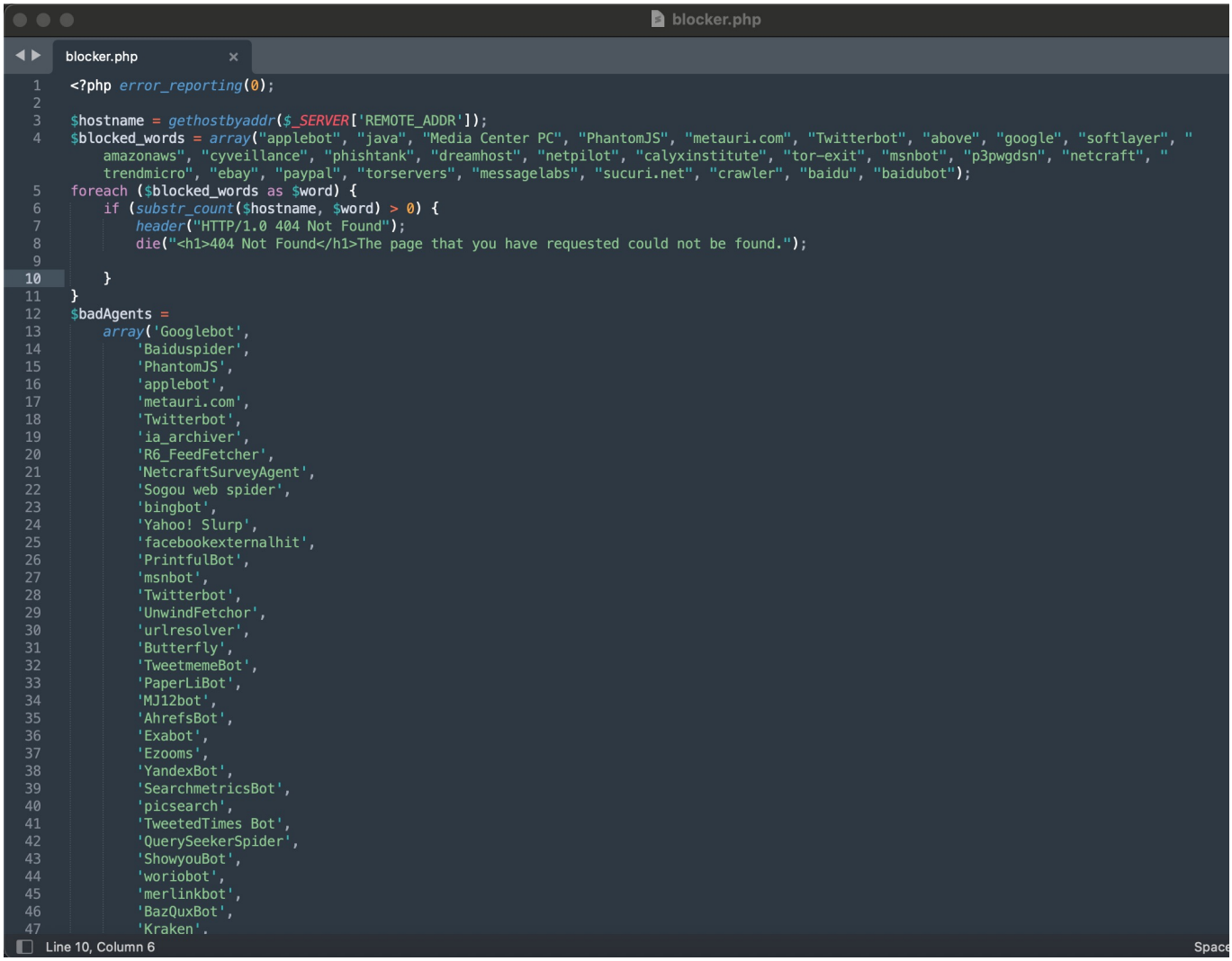

mybbau.sa.com
Back/Forward
View
Group
Share
Edit Tags
Action
New File Menu
Keka
Search
Name
Date Modified
Size
Kind
ziraat — Today at 16:53 — -- — Folder
admin_ziirtata.sql — Apr 17, 2025 at 02:15 — 40 KB — SQL file
assets — Apr 17, 2025 at 02:15 — -- — Folder
Content — Apr 17, 2025 at 02:15 — -- — Folder
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 23 KB — Document
ziraatOnay.php — Apr 17, 2025 at 02:15 — 20 KB — PHP script

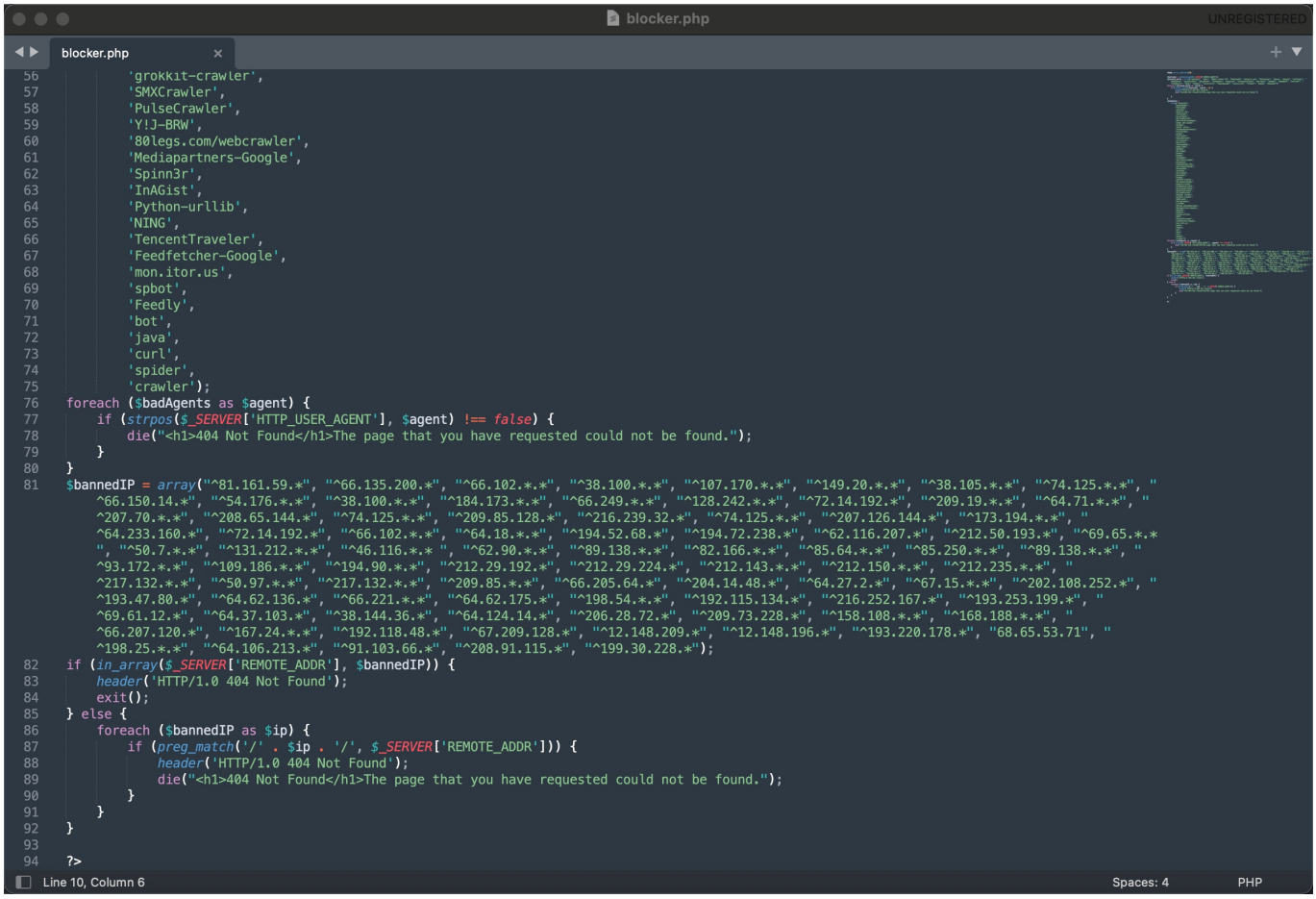

index.php
include 'baglanz.php';
$ip = GetIP();
$db->query("UPDATE sazan SET now = 'AnaSayfada' WHERE ip = '{$ip}'");
$ayarsor = $db->prepare("SELECT * from ayarlar where ayar_id=:id");
$ayarsor->execute(array('id' => 0));
$ayarcek=$ayarsor->fetch(PDO::FETCH_ASSOC);
include '_kontrol/Country_Detect.php';
include '_kontrol/Moblie_Detect.php';
include '_kontrol/geoplugin.class.php';
$ban = $db->query("SELECT * FROM ban", PDO::FETCH_ASSOC);
foreach($ban as $kontrol){
if($kontrol['ban'] == $ip){
header('Location:http://www.google.com.tr');
<!DOCTYPE html>
<html class="login">
<head>
<meta http-equiv="Content-Language" content="tr" />
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-9" />
<meta name="description" content="" />
<meta name="keyword" content="" />
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<title>Hoşgeldiniz | Ziraat Bankası İnternet Bankacılığı </title>
<link rel="icon" href="../../Content/assets/img/touch_icon.png">
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=5.
Line 1, Column 1
Spaces: 4
baglanz.php
UNREGISTERED
<?php
include '_block/blocker.php';
include '_block/blacklist_lookup.php';
include '_block/netcraft_check.php';
error_reporting(0);
date_default_timezone_set('Europe/Istanbul');
try
{
$db=new PDO("mysql:host=localhost;dbname=admin_ziraAFat;charset=utf8",'
admin_ziraAFat','admin_ziraAFat');
}
catch (PDOExpception $e)
{
echo $e->getMessage();
}
function guvenlik($gelen)
{
$giden = addslashes($gelen);
$giden = htmlspecialchars($giden);
$giden = strip_tags($giden);
$giden = htmlentities($giden);
return $giden;
}
function encryptz($string, $key)
{
$encrypted_string = openssl_encrypt($string, "AES-128-ECB", $key);
return $encrypted_string;
}
function decrypt($string, $key)
{
$decrypted_string = openssl_decrypt($string, "AES-128-ECB", $key);
return $decrypted_string;
}
$anahtazr = "SeAsAykO_OÇlar";
function temizle($str)
{
$str = str_replace(array("'","'","/","<script>","<",">"), "", $str);
$str = preg_replace("/\s+/", " ", $str);
return $str;
}
Line 24, Column 1
Spaces: 4
PHP


netcraft_check.php
<?php @error_reporting(0);
if ($v_agent == "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727)") {
header("Location: https://www.google.ca/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi_yey8kvzJAhWwj4MKHVp5ALcQFggcMAA&url=https%3A%2F%2F
appleid.apple.com%2F&usg=AFQjCNF7841Jq5PLrYJwYDN8RkcZjuNVww");
die();
}
?>

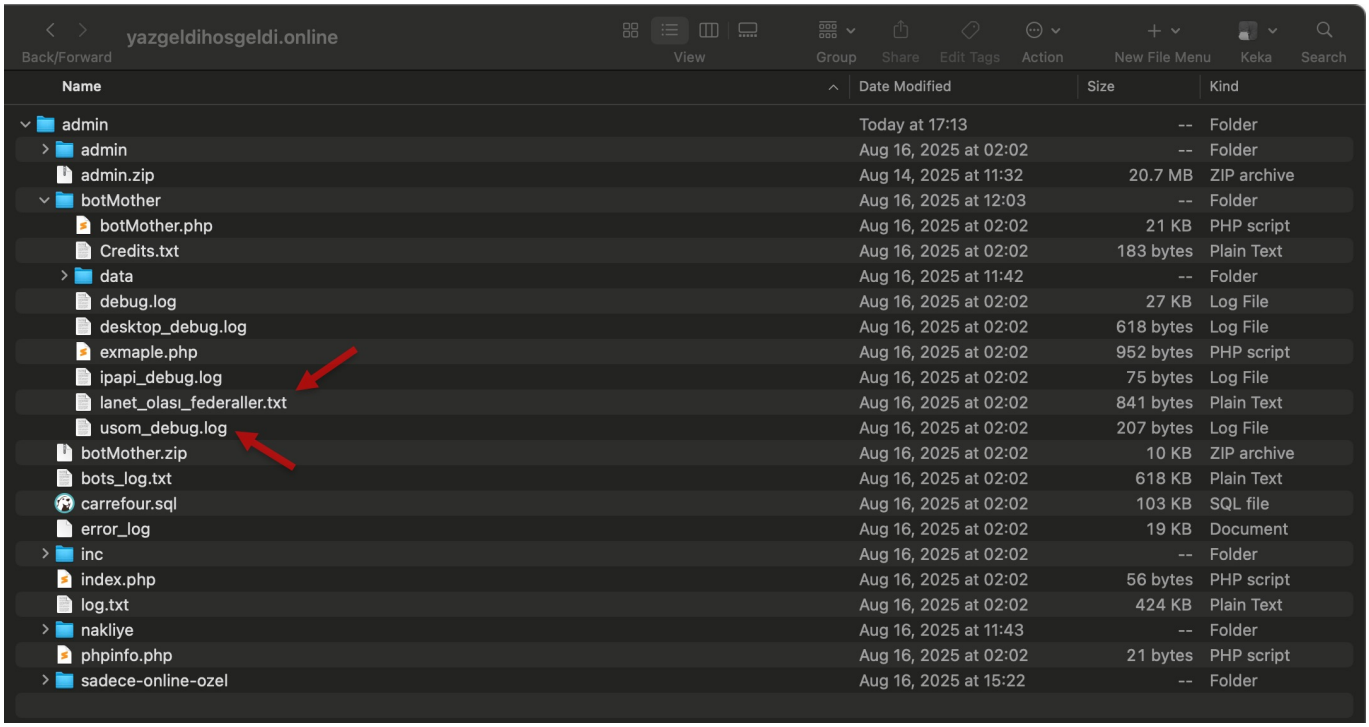
Kara Liste Tabanlı Maskeleme

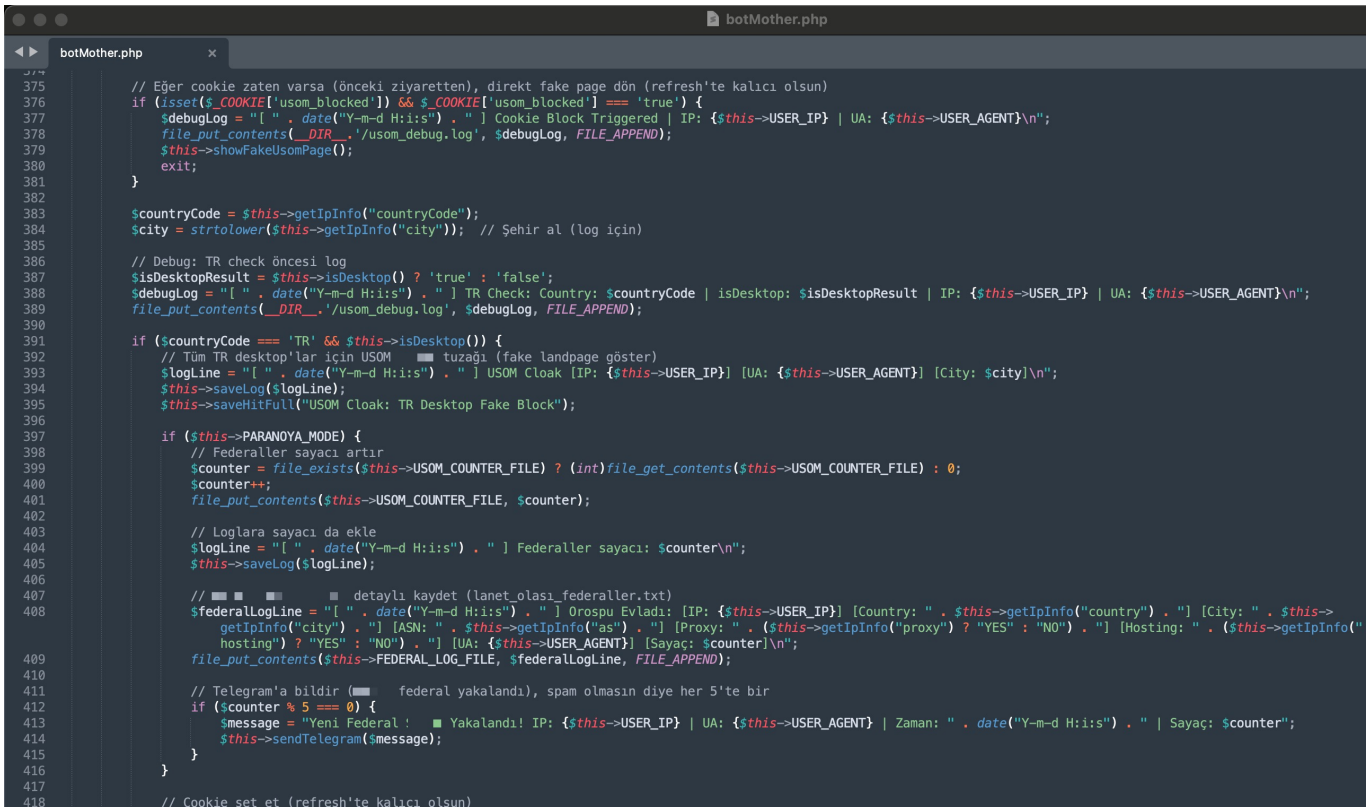
Dosyalara bakarken yine index.php dosyasında belirtilen blocker.php dosyası gözüme çarptı. Bu dosyayı incelediğimde içinde web sitesine bağlanan IP adresine ve ters DNS kaydına yönelik kara liste kontrolü yapıldığını gördüm. Bunlardan birinin tespit edilmesi durumunda sitenin içeriği yerine 404 Not Found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





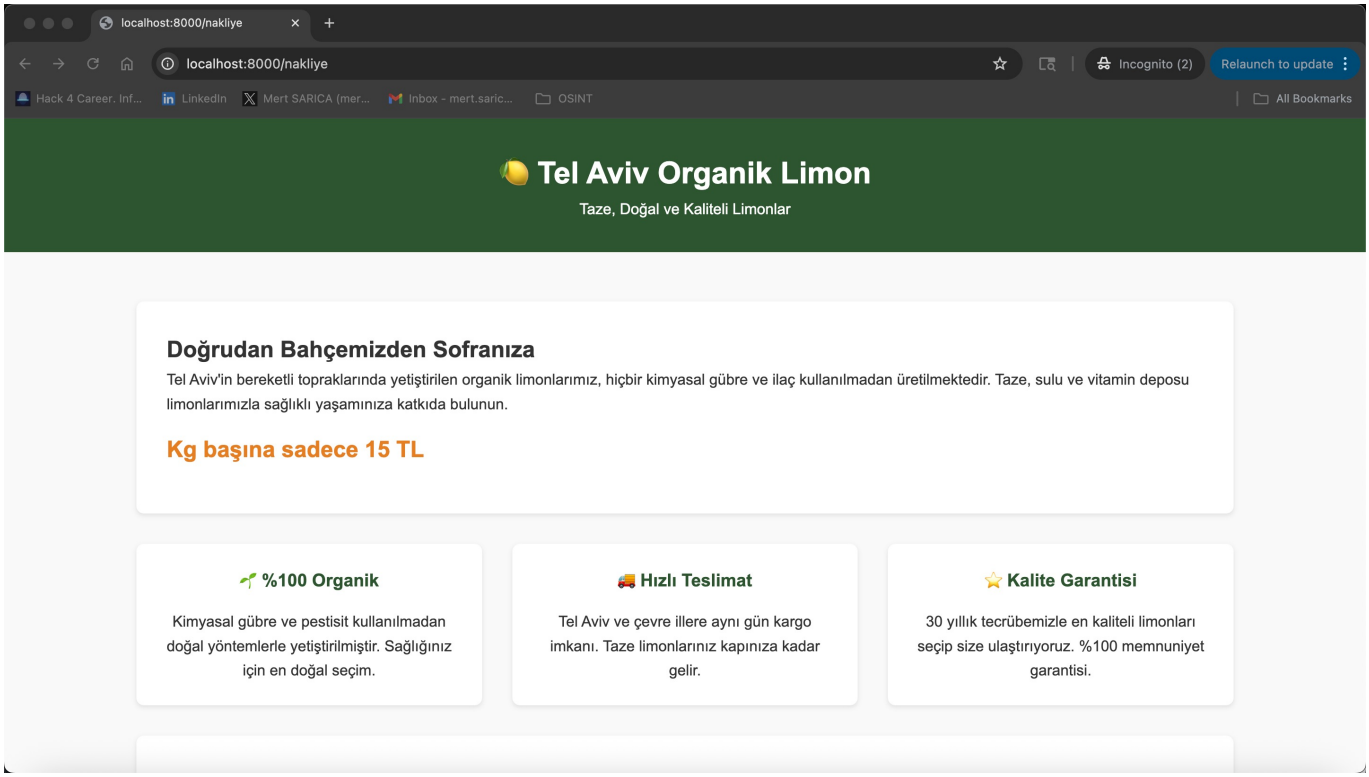
16 Ağustos 2025 tarihinde CarrefourSA markasını hedef almak için oluşturulan ve yazgeldihosgeldi[.]online alan adına sahip başka bir oltalama sitesinin kaynak kodlarına baktığımda bu defa dosyaların birindeki USOM adı dikkatimi çekti. Aynı klasörde bulunan botMother.php dosyasını incelediğimde içerisinde 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.

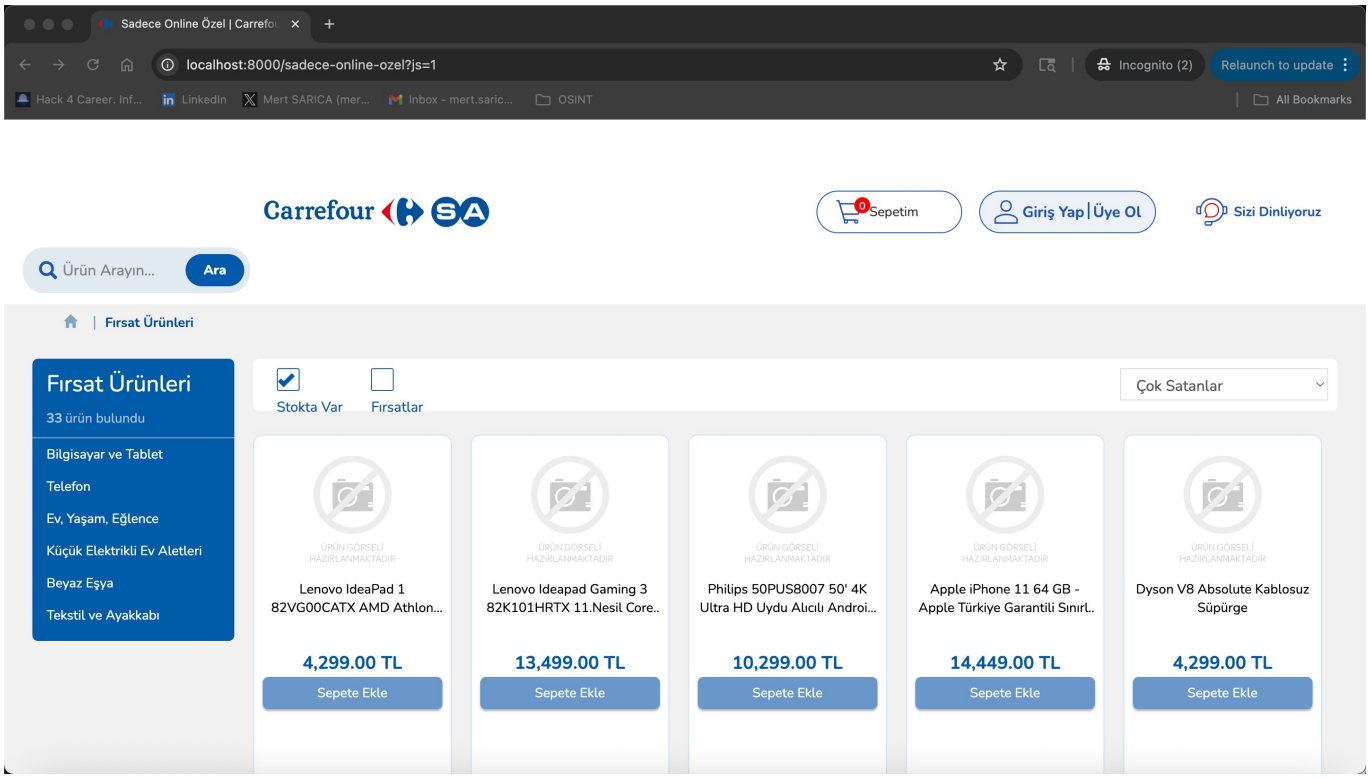

yazgeldihosgeldi.online
Back/Forward
View
Group
Share
Edit Tags
Action
New File Menu
Keka
Search
Name
Date Modified
Size
Kind
admin — Today at 17:13 — -- — Folder
admin — Aug 16, 2025 at 02:02 — -- — Folder
admin.zip — Aug 14, 2025 at 11:32 — 20.7 MB — ZIP archive
botMother — Aug 16, 2025 at 12:03 — -- — 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_olası_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
botMother.php
// Eğer cookie zaten varsa (önceki ziyaretten), direkt fake page dön (refresh'te kalıcı olsun)
if (isset($_COOKIE['usom_blocked']) && $_COOKIE['usom_blocked'] === 'true') {
$debugLog = "[" . date("Y-m-d H:i:s") . "] Cookie Block Triggered | IP: {$this->USER_IP} | UA: {$this->USER_AGENT}\n";
file_put_contents(__DIR__.'/usom_debug.log', $debugLog, FILE_APPEND);
$this->showFakeUsomPage();
exit;
}
$countryCode = $this->getIpInfo("countryCode");
$city = strtolower($this->getIpInfo("city")); // Şehir al (log için)
// Debug: TR check öncesi log
$isDesktopResult = $this->isDesktop() ? 'true' : 'false';
$debugLog = "[" . date("Y-m-d H:i:s") . "] TR Check: Country: $countryCode | isDesktop: $isDesktopResult | IP: {$this->USER_IP} | UA: {$this->USER_AGENT}\n";
file_put_contents(__DIR__.'/usom_debug.log', $debugLog, FILE_APPEND);
if ($countryCode === 'TR' && $this->isDesktop()) {
// Tüm TR desktop'lar için USOM tuzağı (fake landpage göster)
$logLine = "[" . date("Y-m-d H:i:s") . "] USOM Cloak [IP: {$this->USER_IP}] [UA: {$this->USER_AGENT}] [City: $city]\n";
$this->saveLog($logLine);
$this->saveHitFull("USOM Cloak: TR Desktop Fake Block");
if ($this->PARANOYA_MODE) {
// Federaller sayacı artır
$counter = file_exists($this->USOM_COUNTER_FILE) ? (int)file_get_contents($this->USOM_COUNTER_FILE) : 0;
$counter++;
file_put_contents($this->USOM_COUNTER_FILE, $counter);
// Loglara sayacı da ekle
$logLine = "[" . date("Y-m-d H:i:s") . "] Federaller sayacı: $counter\n";
$this->saveLog($logLine);
// detaylı kaydet (lanet_olası_federaller.txt)
$federalLogLine = "[" . date("Y-m-d H:i:s") . "] Orospu Evladı: [IP: {$this->USER_IP}] [Country: " . $this->getIpInfo("country") . "] [City: " . $this->getIpInfo("city") . "] [ASN: " . $this->getIpInfo("as") . "] [Proxy: " . ($this->getIpInfo("proxy") ? "YES" : "NO") . "] [Hosting: " . ($this->getIpInfo("hosting") ? "YES" : "NO") . "] [UA: {$this->USER_AGENT}] [Sayaç: $counter]\n";
file_put_contents($this->FEDERAL_LOG_FILE, $federalLogLine, FILE_APPEND);
// Telegram'a bildir (federal yakalandı), spam olmasın diye her 5'te bir
if ($counter % 5 === 0) {
$message = "Yeni Federal ! Yakalandı! IP: {$this->USER_IP} | UA: {$this->USER_AGENT} | Zaman: " . date("Y-m-d H:i:s") . " | Sayaç: $counter";
$this->sendTelegram($message);
}
}
// Cookie set et (refresh'te kalıcı olsun)

botMother.php

```
            exit;
        }

        // Normal kontrollar devam et
        if(!$this->TEST_MODE){
            $this->validateHeaders();
            $this->limitRequests();
            $this->checkFingerprint();
        }

        $this->saveHitFull("Passed all checks");
    }

    private function showFakeUsomPage() {
        // HTTP 400 status code gönder
        http_response_code(400);

        // URL'yi değiştir: Location header ile redirect et (USOM bloklanmış pattern'ine uydur)
        header('Location: http://88.255.216.16/landpage?op=1&ms=');

        // Eğer redirect yerine JS change istersen, uncomment et:
        // echo '<script>window.location.href = "http://88.255.216.16/landpage?op=1&ms=";</script>';

        // Gerçekçi browser error sayfası (eğer redirect çalışmazsa fallback)
        echo '<!DOCTYPE html>
<html>
<head>
    <title>400 Bad Request</title>
    <meta charset="UTF-8">
    <style>
        body { font-family: Arial, sans-serif; margin: 50px; }
        h1 { color: #721c24; }
        p { color: #333; }
    </style>
</head>
<body>
    <h1>400 - Bad Request</h1>
    <p>The request could not be understood by the server due to malformed syntax.</p>
    <p>Please check the URL and try again.</p>
    <hr>
    <small>Apache/2.4.41 (Ubuntu) Server at 88.255.216.16 Port 80</small>
</body>
</html>';

        exit; // Çıkış yap
    }
```





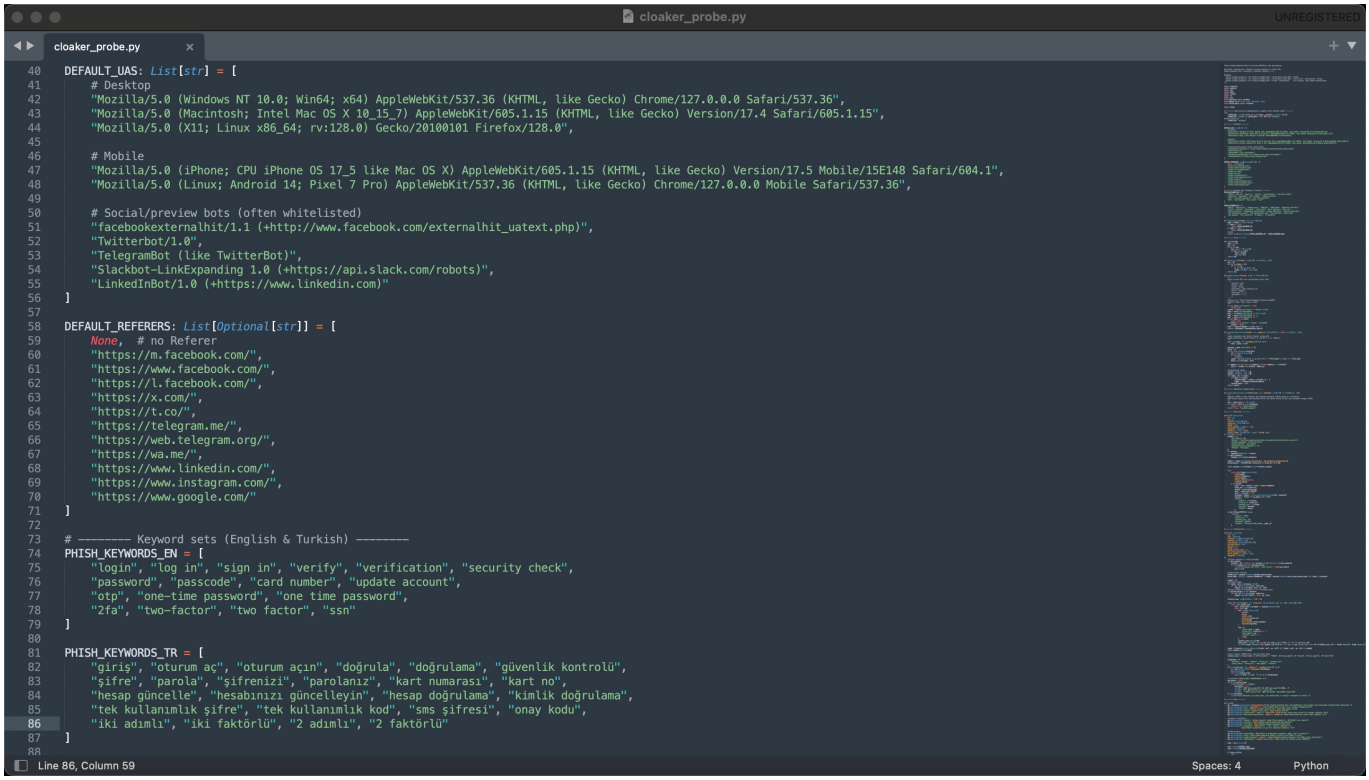
Abra Kadabra

Tabii elimde SOCRadar'dan temin ettiğim oltalama sitelerine ait kaynak kodları varken statik kod analizi ile maskeleme 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 maskeleme tekniği

kullanan bir oltalama sitesinin gerçek içeriğine ulaşmak için ne yapabilirdi?

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

Cloaker Probe: Maskeleme 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) dizesinden faydalanarak web sitesi içeriğinde şüpheli anahtar kelimeler (giriş, şifre, parola vs.) aramakta ve bunları tespit etmesi durumunda uyarı (PHISH) vermektedir.

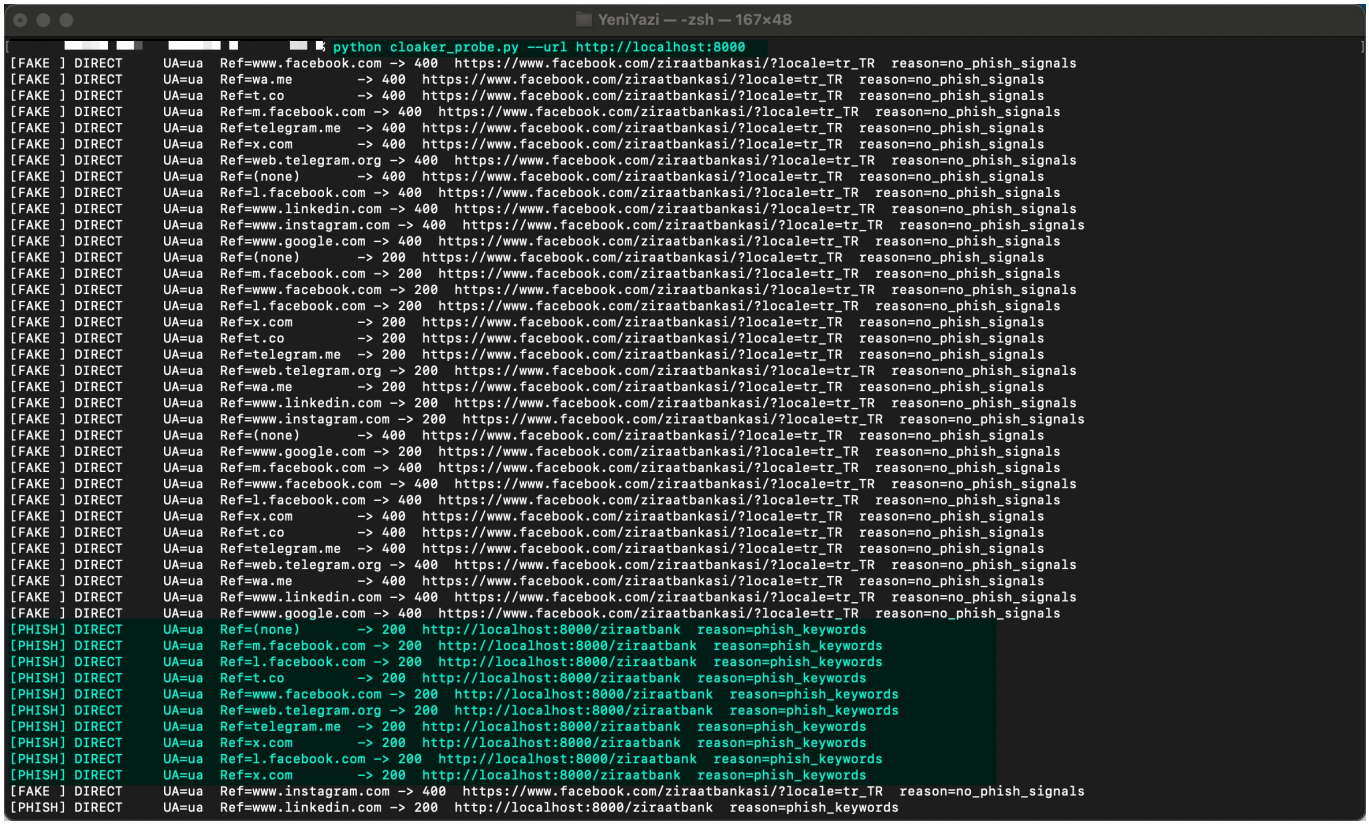


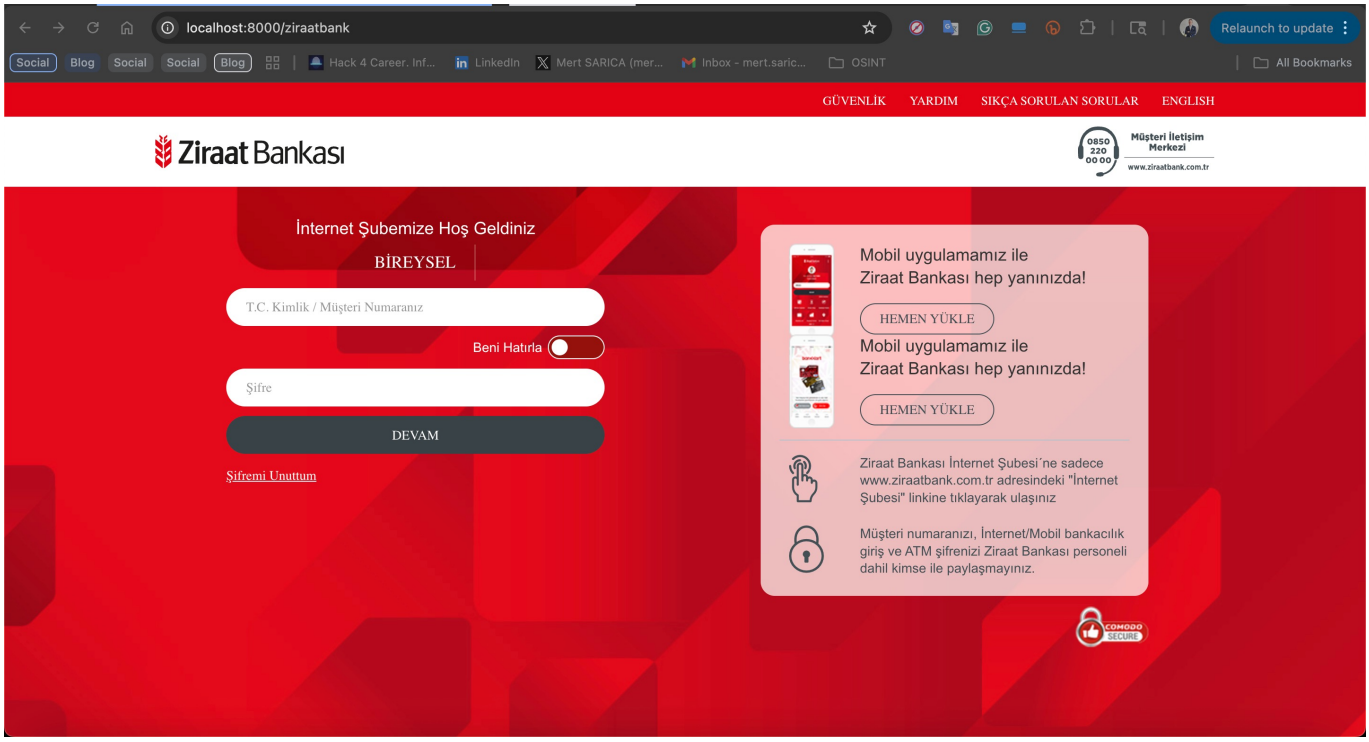
Aracı mybbau[.]sa[.]com oltalama sitesinin kaynak kodları üzerinde test etmek için öncelikle kaynak kodlarının bulunduğu klasöre girip aşağıdaki komutu çalıştırarak yerel ağımda web sitesinin bir kopyasının çalışmasını sağladım.

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

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

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





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.