



# PHISHING SALDIRILARININ TAKİBİ

**Baskı: 2019**

## İÇİNDEKİLER

<b>PHİSHİNG NEDİR? .....</b>	<b>4</b>
OLTALAMA (PHİSHİNG) SALDIRILARININ ÖNEMİ.....	4
<b>SPEAR PHİSHİNG NEDİR?.....</b>	<b>5</b>
<b>VİSHİNG NEDİR? .....</b>	<b>6</b>
<b>PHİSHİNG KİT NEDİR? NASIL TESPİT EDİLİR? .....</b>	<b>8</b>
PHİSHİNG KİTLER (OLTALAMA SALDIRISI SETLERİ) NERELERDEN ELDE EDİLİR? .....	8
Phishing Kitler Nereleden Elde Edilebilir?.....	9
PHİSHİNG KİT KULLANIMI .....	9
PHİSHİNG KİT NASIL TESPİT EDİLİR? .....	11
Phishing Kitler Yapısal Olarak İki Tür Dosya İçerir. ....	12
Phishing Kitlerin Tespiti Zorlaştırmak İçin Saldırganların Aldığı Bazı Önlemler .....	14

## Giriş

Phishing, internet tarihinin en eski ve en etkili saldırı türlerinden biridir. Ortalama saldırıları olarak bilinen bu saldırı türünde genel olarak kurbanların e-posta hesaplarına; hediye, indirim veya benzeri cezbedici sahte iletiler gönderilerek parola, kimlik bilgisi veyahut benzeri hassas verilerin çalınması amaçlanır.

İletilen e-posta mesajlarındaki zararlı bağlantılar tıklandığı zaman kurbanın av olması sağlanabildiği gibi e-postalar ile ek olarak gönderilen virüslü dosyaların çalıştırılması ile de kurbanların bilgisayarları saldırganlar tarafından ele geçirilebilir.

## Phishing Nedir?

Phishing, genel olarak bir kişinin parolasını, banka hesabını veya kredi kartı bilgilerini öğrenmek amacıyla kullanılır. Saldırgan tarafından özel olarak hazırlanan phishing e-postası resmi bir kurumdan geliyormuş gibi ya da gerçek bir e-posta şeklinde görülür. Hazırlanan e-posta yardımıyla bilgisayar kullanıcıları sahte sitelere yönlendirilerek parolalarını vermeleri sağlanır. Diğer bir yandan bu e-postalara eklenen dosyaların çalıştırılması ile kurbanların bilgisayarları ele geçirilerek saldırının kontrolü altına girebilir.

Phishing saldırılarında saldırıya geçen kişi bir “yem” hazırlar ve bu yeme kurbanların takılmasını amaçlar. Yem genelde maaş zammı, hediye, ücretsiz tatil, para ödülü şeklinde cezbedici senaryolardan oluşturulur. Kurumlar için büyük riskler oluşturan bu saldırı türüne karşı büyük kayıplar yaşanmaması için kurum çalışanlarının bilgilendirilmesi ve özel olarak eğitilmesi gereklidir.

## Ortalama (Phishing) Saldırıların Önemi

İnternet kullanımı yaygınlaştıkça, kurum çalışanları veya bireysel kullanıcılar daha fazla çevrimiçi olmak, ürün veya hizmetlere erişimde interneti kullanmayı talep etmektedir. Bu noktada internet kullanımının yaygınlaşması ile alışverişlerimiz, bankacılık işlemlerimiz, finansal işlemlerimiz, kurum içi iletişimlerimiz ve benzeri birçok kritik veri internet üzerinde yaygın olarak kullanılmaya başlanmıştır. Doğal olarak bu durum siber saldırıların bakiş açısını değiştirerek hedefli saldırıların artmasına sebep olmuştur.

Siber saldırıların phishing yöntemleri ile bilinçsiz kullanıcıları hedefleyerek büyük zararlara sebep olmaktadır. Phishing saldırıları hedefli olarak yapıldığı takdirde ise büyük bir başarı oranına sahiptir. Doğal olarak siber saldırıların internet tarihinin en eski ve en etkili yöntemlerinden biri olan phishing saldırılarını sıklıkla kullanmaktadır. Sosyal mühendislik saldırıları ile birlikte gerçekleştirilen spear phishing saldırıları ise maalesef ki siber saldırıların elinde korunması zor ve tehlikeli bir siber silah olarak kurumları tehdit etmektedir.

Phishing saldırıları hem sosyal mühendislik hem de teknik altyapı kullanılarak gerçekleştirilen bir suç olarak tanımlanır. Yaygın olarak e-posta aracılığıyla gerçekleştirilen bu saldırılar günümüz sosyal ağlarının popüler olması ile evrim geçirerek çok daha büyük kitlelere ulaştığını, virüs worm gibi zararlı kodların yayılmasında etkili rol oynadığını göstermiştir.

## Spear Phishing Nedir?

Spear Phishing hedefli ortalama saldırıları olarak tanımlanır. Amaç siber korsanlar tarafından seçilen kurbanların mahrem bilgilerin, finansal verilerini, banka hesapları gibi benzeri kritik verilerin çalınmasıdır. Rastgele kurban seçilebileceği gibi bir kişi veya kurum da hedef alınabilir. Bu durum phishing saldırılarının kurbanı göre özelleştirilerek hazırlanmasını gerektirmektedir.

Bu saldırı yöntemi ile bir kuruluşun çalışanlarına ait kimlik bilgileri, sosyal medya hesapları, bankacılık işlemlerinde kullanılan bilgiler elde edilmeye çalışabilir. Biraz daha ileri boyutta geçtiğini düşünürsek ticari sırlar ve gizli bilgiler elde edilebilir. İnternet dünyasında ortaya çıkan phishing saldırılarına baktığımız zaman dünyanın en önemli kurumların dahi bu saldırılar karşısında yenik duruma düştüğünü görmekteyiz.

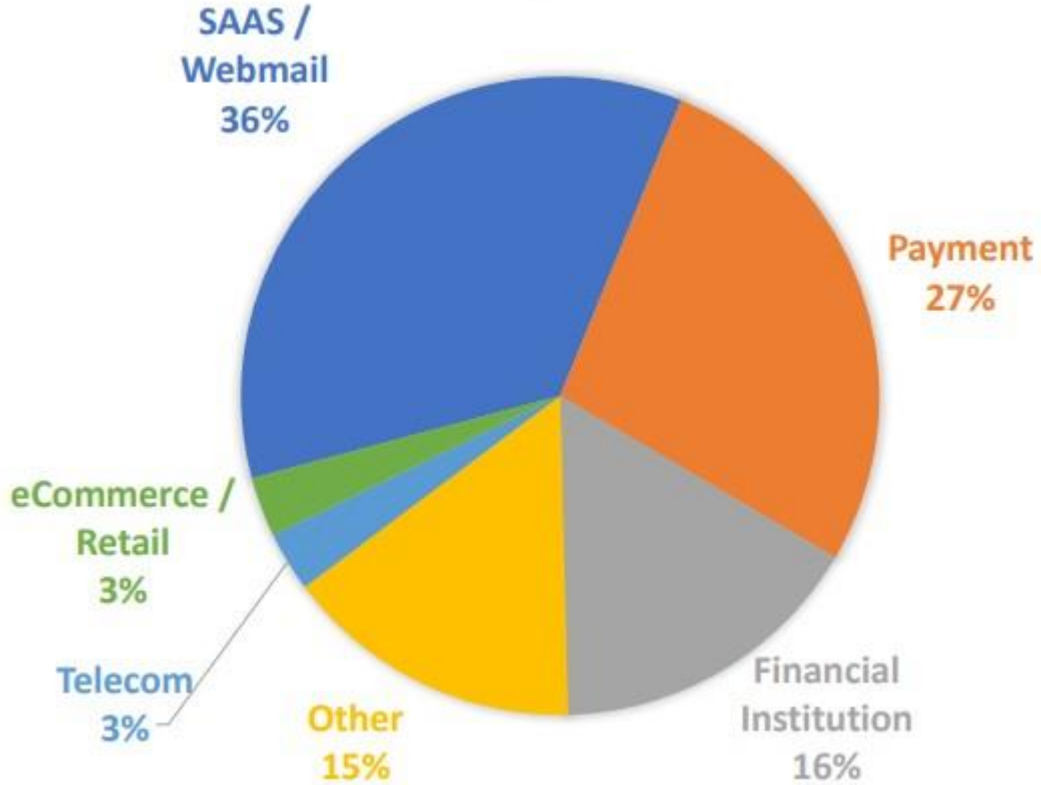
Spear Phishing saldırılarında öncelikle kurban olarak seçilen kişi ya da kuruluş hakkında bilgi toplanır. Bilgi toplama Spear Phishing saldırılarında (hedefli ortalama saldırıları) ilk ve en önemli adımdır. Kurbanı iletilen e-posta da kullanılan isimler gerçek kişilere aittir. E-postayı gönderen kişi olarak, yöneticiler, iş arkadaşları veya kurbanın tanıdığı kişiler kullanılır. Aynı zamanda e-postanın içeriğini belirleyebilecek / etkileyebilecek yetkili bir kişi adı ve unvan da seçilir. Bu yöntem sayesinde kurbanı, olağan akışta gelebilecek bir e-posta izlenimini verilerek şüphe edilebilecek durumlar ortadan kaldırılır.

## Vishing Nedir?

Vishing, telefonla gerçekleştirilen phishing saldırıları için kullanılan teknik bir kavramdır. Hedef net olarak belirlenerek, doğrudan kurbanı ulaşılır. Telefon ile yapılan bu saldırı türünde duygusal tetikleyiciler kullanılır. Vishing saldırılarına örnek olarak teknik destek dolandırıcılığı verilebilir. Her iki tür phishing saldırısında da ana amaç kullanıcıdan kritik bilgileri çalabilmektir.

Telefon ile gerçekleştirilen Vishing saldırıları genel olarak belirtilen işin acil olduğunu, aksi durumda çalışan bir servisin durması, veri kaybı olabileceği gibi ciddi zararlar yaşanabileceğini vurgulanarak kurbanı korku verilir. Bu sayede karşıdaki kişiye yardım etmek istiyormuş izlenimi verilmiş ve güven sağlanmış olur. Aynı zamanda başarılı bir saldırı için kurbanın merak duygusu da tetiklenebilir.

Phishing saldırılarının etkinliği son yıllarda hızla değişmiştir; iyi tanımlanmış, küçük ölçekli bir işlemde, iyi tanımlanmış rollere sahip birden fazla oyuncuyu içeren, büyük ölçüde otomatikleştirilmiş bir işleme dönüşmüştür. Bu sayede Phishing kitleri yapılmaya başlanmış ve Deep Web adı verilen illegal internet dünyasında satışa sunulmuştur.



APWG Kimlik Avı Etkinliği Trend Raporu'na göre 2019 ilk çeyreğinde en fazla phishing saldırısı alan SaaS ve mail servisleri oldu.

APWG Kimlik Avı Etkinliđi Trend Raporu'na g re 2019 ilk  eyređinde en fazla phishing saldırısı alan SaaS ve mail servisleri oldu. Aynı zamanda 2018'in 3. ve 4.  eyređine g re phishing saldırıları artıř g stermiřtir. Saldırılarda kullanılan SSL sertifikaları ise kurum  alıřanlarına verilen farkındalık eđitimlerine paralel oranla y kseliře ge miřtir.

BGA Bilgi G venliđi olarak kurum  alıřanlarınızın bilgi g venliđi farkındalıđını artırarak phishing (oltalama) saldırılarına karřı daha dikkatli olmanızı sađlıyoruz. Bilgi G venliđi Farkındalık Eđitimlerimiz ve Sim lasyon Testlerimiz ile kurumların phishing saldırılarına karřı durumlarını analiz ederek  alıřanlarınızın durumları i in  zel raporlar sunmaktayız. Bu konuda **bilgi@bga.com.tr** adresimiz ile iletiřime ge erek fiyat teklifi veya teknik ekibimiz ile kurumunuza  zel   z mler i in bilgi alabilirsiniz.

## Phishing Kit Nedir? Nasıl Tespit Edilir?

Phishing kit, bir çeşit web bileşenidir. Ortalama saldırıları için kullanılan teknik ekipman olarak tanımlanabilir. Teknik bilgisi az olan kişiler tarafından da kullanılabilen bir yapıda tasarlanarak hazır paketler halinde sunulur. Bazı Phishing kitler satır değiştirilerek konfigüre edilip kullanılabilirken, bazı kitler için oluşturulmuş ayrıntılı kullanım talimatları mevcuttur. Bugüne kadar phishing (ortalama) saldırıların yaygınlaşmasında kitlerin kullanımı etkili olmuştur. Kitler ücretsiz olarak tanıtılıp dağıtılabildiği gibi ücretli olarak da illegal dünyada satılmaktadır.

Saldırganlar phishing kitler ile bilindik markaların ya da kuruluşların web sitesini kolayca kopyalayabilirler. Kuruluş portalları, bankalar, Google, Twitter, Instagram, Microsoft gibi firmalar sıklıkla kullanılmaktadır. Bu kitlerde genel olarak web sitelerinde kullanılan mahrem bilgilerin ele geçirilmesi amaçlanmaktadır. Genellikle SSL sertifikaları ile desteklenerek inandırıcılık artırılmaktadır. Bu kitleri kullanan saldırganların fark edilmesi zordur ve bu kitlerin yayından kaldırılmadan önce genel olarak 36 saat boyunca faaliyet gösterdiği tespit edilmiştir.

Kurumunuzun güvenlik önlemleri yeterli ve güncelse uygun tespit yöntemleri kullanılarak, kullanıcıların maillerine düşmeden, mail sunucularında phishing kitler tespit edilip bloklanabilir.

**BGA Security olarak bu konuda ülkemiz kurumlarına Phishing saldırıları ve kitleri için özel çözümler sunmaktayız.**

## Phishing Kitler (Ortalama Saldırısı Setleri) Nereleden Elde Edilir?

Saldırganlar phishing için genelde birçok alan adı alıp, birinin engellenmesi durumunda diğerlerini otomatik olarak devreye sokar. Kullanılan sunucu iplerinin itibarları yüksek olduğu için genelde pasif taramalara takılmazlar.

Gerçek web sitesinde kullanıcıdan istenilen bilgiler hazırlanan phishing web sitelerinde de istenir. Genellikle, bilgiler alındıktan sonra kullanıcılar, hiçbir şey olmamış gibi gerçek web sitesine yönlendirilir. Örneğin kurbanın mail adresine düşük faizli kredi gibi düzenlenen bir saldırı gelebilir. Kurban maili açtığında bankanın kopyalanmış, gerçeğiyle birebir aynı sahte web sitesine erişir. Giriş için kullanılan bilgilerin doldurulmasının ardından, kurban sms sayfasına yönlendirilir. Saldırgan bu sırada kullanıcının bilgilerini kullanarak gerçek web sitesine giriş yapmış ve kullanıcıya sms gelmesini beklemektedir. Telefonuna sms gelen kullanıcı, bu bilgiyi de phishing siteye girecektir. Daha sonra hazırlanan phishing sitesinin içeriğine göre gerçek siteye yönlendirilebilir ya da daha farklı bilgiler de talep edilebilir. Bu sayede fark edilmesi güçleşmiş olacaktır.




## Phishing Kitler Nereleden Elde Edilebilir?

Darnet, Dark Web, Deep Web adını verdiğimiz internetin karanlık ortamındaki bazı forumlar, IRC kanalları, Github, phishing kit tespit eden araçlar (örneğin stalkphish) ve özellikle bu bu işin dağıtımını yapan siteler örnek olarak gösterilebilir. Dağıtım yapan sitelerin kapatılması phishing sitelerin kapatılmasından çok daha uzun sürmektedir.

## Phishing Kit Kullanımı

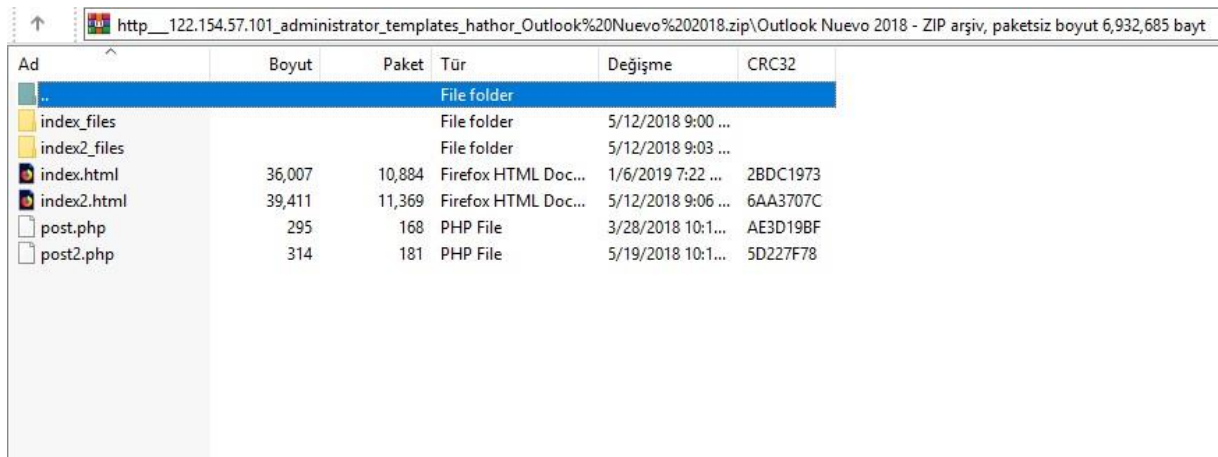
Phishing kiti, genellikle bir arşiv dosyasında (örneğin bir zip, rar dosyası, tar dosyası gibi) bulunur ve donanımlı bir phishing web sitesi oluşturmak için kullanılabilecek dosyaları içerir. HTML / PHP sayfa şablonları, otomatik çalıştırma komut dosyaları, gömülü resimler ve benzeri içeriklerin bulunduğu bu kitler çok kapsamlıdır. Hazır ve otomatize edildikleri için kullanmak isteyenlerin neredeyse sıfıra yakın bir teknik becerisi olması yeterlidir. Tüm teknik ayarlamalar bu kitler içerisinde otomatik olarak yapılmaktadır.

Friedphish tarafından tespit edilen ve incelenen, İspanyol dili kullanan kişilerin hedef alındığı bir phishing kit, Github' tan indirilmiş ve dosya içeriği aşağıdaki gibi paylaşılmıştır.



Ad	Boyut	Paket	Tür	Değişme	CRC32
..			File folder		
_MACOSX			File folder	1/6/2019 7:25 ...	
Outlook Nuevo 2018			File folder	5/12/2018 9:10 ...	

İçerik kontrol edildiğinde MAC OS işletim sistemi kullanılarak hazırlanmış bir kit olduğu ekran görüntüsündeki gibi tespit edilmiştir.



Ad	Boyut	Paket	Tür	Değişme	CRC32
..			File folder		
index_files			File folder	5/12/2018 9:00 ...	
index2_files			File folder	5/12/2018 9:03 ...	
index.html	36,007	10,884	Firefox HTML Doc...	1/6/2019 7:22 ...	2BDC1973
index2.html	39,411	11,369	Firefox HTML Doc...	5/12/2018 9:06 ...	6AA3707C
post.php	295	168	PHP File	3/28/2018 10:1...	AE3D19BF
post2.php	314	181	PHP File	5/19/2018 10:1...	5D227F78

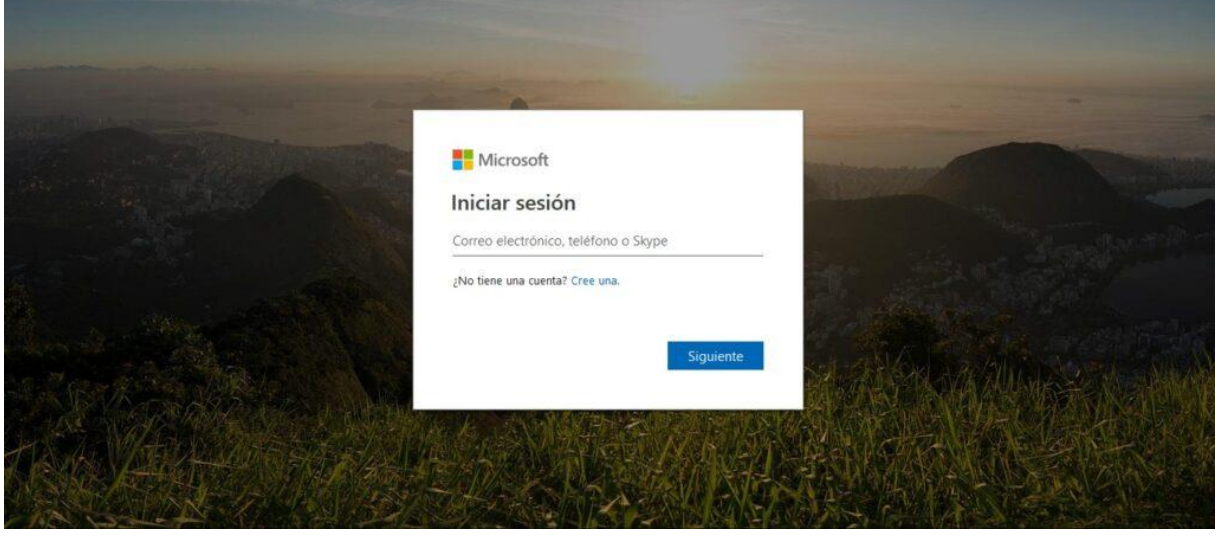
Bu kiti incelediğimiz zaman Python ile geliştirilmiş olduğu görülüyor. Bu phishing kit basit bir çalışma mantığında hazırlanmış. Kurbandan alınan girdiler post.php dosyasına gönderiliyor. Post.php kurbanlardan aldığı girdiyi usernames.txt dosyasına kaydediyor ve kurbanları index2.html sayfasına yönlendirerek işlemini tamamlıyor.

```
1 <?php
2 header ('Location:index2.html');
3 $handle = fopen("usernames.txt", "a");
4 foreach($_POST as $variable => $value) {
5     fwrite($handle, $variable);
6     fwrite($handle, "=");
7     fwrite($handle, $value);
8     fwrite($handle, "\r\n");
9 }
10 fwrite($handle, "\r\n");
11 fclose($handle);
12 exit;
13 ?>
```

Yukarıdaki kodu incelediğimiz zaman kurbanlardan gelen şifreler post2.php dosyasına iletilmektedir. Kurbanlardan alınan parola password.txt dosyasına yazılıyor ve kurbanlar fark etmemesi için Outlook'un ana sayfasına yönlendiriliyor.

```
1 <?php
2 header ('Location: https://outlook.live.com/owa/');
3 $handle = fopen("passwords.txt", "a");
4 foreach($_POST as $variable => $value) {
5     fwrite($handle, $variable);
6     fwrite($handle, "=");
7     fwrite($handle, $value);
8     fwrite($handle, "\r\n");
9 }
10 fwrite($handle, "\r\n");
11 fclose($handle);
12 exit;
13 ?>
```

Kiti kullanan saldırganın yapması gereken tek şey kiti sunucuya koymak ve bağlantıyı bir şekilde kurbanın tıklamasını sağlamaktır. Herhangi bir teknik bilgi gerektirmeden kurulup hazır hale getiriliyor. Sayfa açıldığında orijinal sayfanın birebir kopyası alındığı için kurban sahte bir sayfada olduğunu bağlantıyı kontrol etmeden anlayamayacaktır.



Yukarıdaki örnekte belirtmiş olduğumuz gibi bu phishing kit ve benzeri birçok araç internette bulunabilmekte ve illegal dünyada çok sayıda phishing kite ulaşılabilir.

## Phishing Kit Nasıl Tespit Edilir?

Phishing kitlerini sunucu tarafından çalıştığı için kaynak kod, eğer sunucu tarafından eksik-yanlış bir konfigürasyon yapılmadıysa görülmeyecektir. Bazı saldırganlar bu duruma dikkat etmediği için orjinal zip dosyasını genelde sunucuda bırakırlar ve indirilebilir bir yapıda olur. Bu da tespit edilmelerini kolaylaştıran bir hatadır. Kullanılan kitlerden bazılarında, izin indeksleme etkin olduğu için dosyalar daha kolay görülebilmektedir. Phistank, clean-mx in tespit ettiği URL <http://x.x.x.x/outlook/index.php> şeklindeyse <http://x.x.x.x/outlook.zip> şeklinde talepte bulunarak bazı durumlarda phishing kit kaynak kodu elde (kit) edilebilir.

Otomatik araçlarla yapılan phishing kit elde etme işleminde bu durum, tar.gz gibi türlerle de denenmektedir. Phishing kitin kaynak kodunun elde edilmesi analiz yapan kişilere daha fazla bilgi verecektir. Ancak phishing kit elde edilmeden de çeşitli yöntemler kullanılarak tespitler yapılabilir.

## Phishing Kitler Yapısal Olarak İki Tür Dosya İçerir.

- Hedeflenen web sitesinin bir kopyasını görüntülemek için gereken kaynak dosyaları.
- Çalınan bilgileri kaydetmek ve saldırganlara göndermek için kullanılan işleme komut dosyaları.

Bir site de phishing kit kullanılıp kullanılmadığının tespiti için bazı parametreler kullanılır. Bu parametreler daha önce bir saldırıda kullanılmış phishing kitlerden elde edilmiştir. Bir web sitesinde bu kitlerden birisi kullanılmışsa ücretsiz araçlar, ticari yazılımlar ile taranarak hangi kitin kullanıldığı belirlenebilir. Tespit esnasında kullanılan yöntemler araçlara göre değişiklik göstermektedir.

**Bir Phishing Kit'in tespiti için genel olarak kullanılabilecek parametreler aşağıdaki gibi verilmiştir;**

- Phishing kitin adı
- Phishing kitin içerdiği dosyaların listesi
- Phishing kitin içerdiği dosyaların hash bilgisi
- Phishing kitin boyutu
- Phishing kitin geliştiricisi hakkında bilgi (isim, mail vb.)
- Elde edilen bilgilerin (kullanıcı adı, şifre v.b) iletileceği mail adresi (regex kullanılıyor)
- Phishing kit geliştiricisinin imzası
- Coğrafi konum scriptleri
- Şaşırtma teknikleri

Aşağıdaki örnekte Kit-Hunter ile gerçekleştirilen kontrolün sonucundan bir bölüm paylaşılmıştır. Şüpheli bulunan dosyalar ve bu dosyaların bulunmasını sağlayan etiketler verilmiştir.



```
kit_hunter_report.log
~/Downloads/kit_hunter

/root/Downloads/kit_hunter/assets/includes

-----
SUSPECT FILENAME IS:

language.php
functions.php
language.mob.php
start_.php

-----
SUSPECT FILE DETECTED BY THE FOLLOWING PHISHING TAG:

geoplugin

-----
ACTUAL LINE OF CODE RESPONSIBLE FOR THIS ALERT:

$ipDetails = json decode(file get contents("http://www.geoplugin.net/json.gp?ip=" . $ipAddress), true);
$jsonip = file get contents('http://www.geoplugin.net/json.gp?ip='.$ipadr);
$jsonip = file get contents('http://www.geoplugin.net/json.gp?ip='.$ipeh);

=====
END OF BLOCK
=====
```

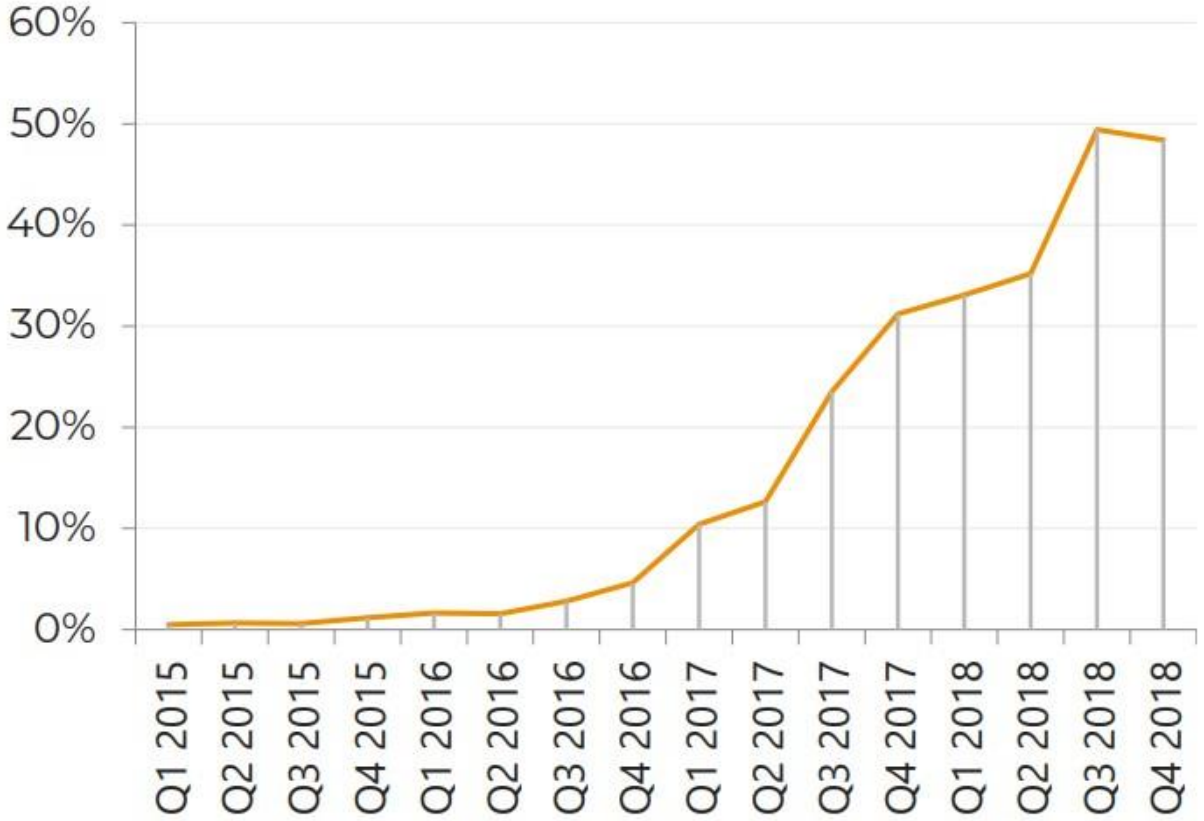
Aşağıda verilen ekran görüntüsü phishing web sitesi hazırlamış bir saldırganın hangi phishing kiti kullandığının tespiti yapılmaya çalışılmakta ve sık kullanılan dosyalar aranmaktadır.

```
- - [2019 17:39:15] "GET /htdocs.php HTTP/1.1" 404 -  
directory traversal attempt detected from: [REDACTED]  
- - [2019 17:39:18] "GET /b.php HTTP/1.1" 404 -  
directory traversal attempt detected from: [REDACTED]  
- - [2019 17:39:19] "GET /sane.php HTTP/1.1" 404 -  
directory traversal attempt detected from: [REDACTED]  
- - [2019 17:39:42] "GET /wpc.php HTTP/1.1" 404 -  
directory traversal attempt detected from: [REDACTED]  
- - [2019 17:39:43] "GET /wpo.php HTTP/1.1" 404 -  
directory traversal attempt detected from: [REDACTED]  
- - [2019 17:39:43] "GET /t6nv.php HTTP/1.1" 404 -  
directory traversal attempt detected from: [REDACTED]  
- - [2019 17:39:44] "GET /muhstik.php HTTP/1.1" 404 -  
directory traversal attempt detected from: [REDACTED]  
- - [2019 17:39:46] "GET /text.php HTTP/1.1" 404 -  
directory traversal attempt detected from: [REDACTED]  
- - [2019 17:39:50] "GET /wp-config.php HTTP/1.1" 404 -  
directory traversal attempt detected from: [REDACTED]  
- - [2019 17:39:51] "GET /muhstik.php HTTP/1.1" 404 -  
directory traversal attempt detected from: [REDACTED]  
- - [2019 17:39:51] "GET /muhstik2.php HTTP/1.1" 404 -  
directory traversal attempt detected from: [REDACTED]  
- - [2019 17:39:52] "GET /muhstiks.php HTTP/1.1" 404 -  
directory traversal attempt detected from: [REDACTED]  
- - [2019 17:39:54] "GET /muhstik-dpr.php HTTP/1.1" 404 -  
directory traversal attempt detected from: [REDACTED]  
- - [2019 17:39:55] "GET /lol.php HTTP/1.1" 404 -  
directory traversal attempt detected from: [REDACTED]  
- - [2019 17:39:55] "GET /uploader.php HTTP/1.1" 404 -  
directory traversal attempt detected from: [REDACTED]
```



## Phishing Kitlerin Tespiti Zorlaştırmak İçin Saldırganların Aldığı Bazı Önlemler

İnandırıcılık seviyesini artırmak için saldırganlar SSL sertifika kullanımı yoluna da gitmektedir. Ücretsiz edinilen sertifikalar, kurbanların ikna edilmesinde avantaj sağladığı için kullanımında da artış görülmektedir. Phislab'ın 2019 raporuna göre tespit edilen kitlerde SSL sertifikasının kullanım grafiği aşağıda verilmiştir.



Phishing sitelerin tespit edilmesi durumunda tarayıcılar tarafından engelleme yapılır. Bu amaçla, tarayıcı tabanlı engellemenin etkinliğini azaltmak amacıyla bazı kitler her ziyaretçi için sitelerinin URL'sini dinamik olarak değiştiren teknikler kullanır.

Bu tekniklere örnek olarak; dizin oluşturma ve randomize URL parametreleri oluşturulması verilebilir.

Dizin oluşturma; her yeni mağdur siteyi ziyaret ettiğinde, sunucuda yeni bir dizin oluşturulur ve phishing sitesini oluşturan tüm bileşenler kopyalanır. URL her ziyaretçi için farklı olacaktır, ancak phishing ana yolu değişmeden kalacaktır. Randomize URL, yeni bir ziyaretçi geldiğinde phishing web sitesi sayfasının URL'inin sonuna eklenmiş olan randomize parametreleri kullanır. Dizin oluşturmada olduğu gibi, bu yöntem de URL'yi her ziyaretçiye özel kılar. Ancak,

dizin oluşturma işleminden farklı olarak, bu teknik dosyaların sunucuda kopyalanmasını veya oluşturulmasını gerektirmez.

Finans sektöründe bir banka için saldırı gerçekleştiriliyorsa, hesap/kart numarasının doğru olup olmadığına dair kontrolün yapılması, hane sınırlaması konulması, şifre de girilecek minimum karakter sayısının sabit tutulması gibi özelliklerin phishing kitlere eklendiği de görülmüştür. görülmüştür.

Oluşturulan bazı phishing kitleri birden fazla coğrafya için kullanılabilecek şekilde tasarlanabilir. Örneğin kurban Türkiye’ den giriş yapıyorsa Türkçe, Japonya’dan giriş yapıyorsa Japonca dille sayfayı açma teknikleri kullanılır.

Tespiti azaltmak için kullanılan bir başka teknik ise aynı ip adresinin phishing sayfayı sadece bir kere ziyaret edebilmesidir. Sayfaya istekte bulunan kurbanın ip adresi kaydedilir. Tespit için yapılan denemelerde sayfayı tekrar ziyaret etmemiz, sayfa bulunamadı uyarısı ile karşılaşır ya da başka bir sayfaya yönlendirilir.

Phishing ile mücadelenin etkinliğinin artması saldırganları da değişik noktalarda kontrole itmiştir. Birçok phishing kitinde, güvenlik araştırmacıları ve güvenlik şirketleri tarafından kullanıldığı bilinen IP adresleri saldırganlar tarafından kara listeye alınır. IP adreslerinin yanı sıra, user-agent ve hostname’lerinde kodlanmış bir listesi bulundurulur. Kurban listeye alınmış bir IP veya user-agent ise, phishing kit web sitesinin içeriğini göstermeyecektir. Bazı durumlarda, kodlanmış IP adresleri listesiyle birlikte, kurbanın IP’sinin proxy olup olmadığını görmek için bazı çevrimiçi servisler kullanılarak kontrol işlemleri yapılmaktadır.

Phishing kitler, web sayfasını analiz etmeyi ve algılamayı zorlaştırmak için, HTML özniteliklerinin sayfa değerlerini her ziyarette rastgele oluşturarak, tespit edilmeyi engellemeye çalışabilir.

Bu ve benzeri birçok teknik de tespit edilmesini zorlaştırmaya yönelik uygulamalar arasında gelmektedir. Bir Phishing saldırısına maruz kalındığında destek almak, çalışanlarınız için farkındalık eğitimleri gibi hizmetlerimizden faydalanmak için bilgi@bga.com.tr adresimiz ile iletişime geçerek bilgi ve fiyat teklifi alabilirsiniz.

## REFERANSLAR

<https://www.csoonline.com/article/3290417/csos-guide-to-phishing-and-phishing-kits.html>  
<https://www.imperva.com/blog/our-analysis-of-1019-phishing-kits/>  
<https://research.checkpoint.com/a-phishing-kit-investigative-report/>  
<https://www.globalsign.com/en/blog/warning-advanced-phishing-kits-now-available-on-the-dark-web/>  
<https://cofense.com/enterprise-phishing-susceptibility-report/>  
[http://docs.apwg.org/reports/apwg\\_trends\\_report\\_q1\\_2019.pdf](http://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf)  
[http://static.usenix.org/event/woot08/tech/full\\_papers/cova/cova.pdf](http://static.usenix.org/event/woot08/tech/full_papers/cova/cova.pdf)  
<https://steemit.com/technology/@balor/an-example-of-an-outlook-phishing-attack>  
<https://github.com/friedphish/phishkits/blob/master>  
<https://jordan-wright.com/blog/2014/07/30/how-to-hunt-down-phishing-kits/>  
<https://www.zscaler.com/blogs/research/evolution-phishing-kits>  
<https://docs.apwg.org/ecrimeresearch/2018/5349207.pdf>



## BGA Bilgi Güvenliđi A.Ş. Hakkında

BGA Bilgi Güvenliđi A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliđi sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliđi, stratejik siber güvenlik danışmanlıđı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliđe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA’da sürdüren BGA Bilgi Güvenliđi’nin ilgi alanlarını **“Sızma Testleri, Red Teaming, Güvenlik Denetimi, SOME, SOC Danışmanlıđı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri”** oluşturmaktadır.

Gerçekleştirdiđi başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliđi, kurulduđu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına **1.000’den fazla eğitim ve danışmanlık** projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliđi, kurulduđu 2008 yılından beri ülkemizde bilgi güvenliđi konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

## BGA Bilgi Güvenliđi AKADEMİSİ Hakkında

BGA Bilgi Güvenliđi A.Ş.’nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliđi AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalıđını arttırıcı gönüllü faaliyetleri yürütölmesinden sorumludur. Bilgi Güvenliđi AKADEMİSİ markasıyla bugüne kadar **“Siber Güvenlik Kampları”, “Siber Güvenlik Staj Okulu”, “Siber Güvenlik Ar-Ge Destek Bursu”, “Ethical Hacking yarışmaları” ve “Siber Güvenlik Kütüphanesi”** gibi birçok gönüllü faaliyetin destekleyici olmuştur.