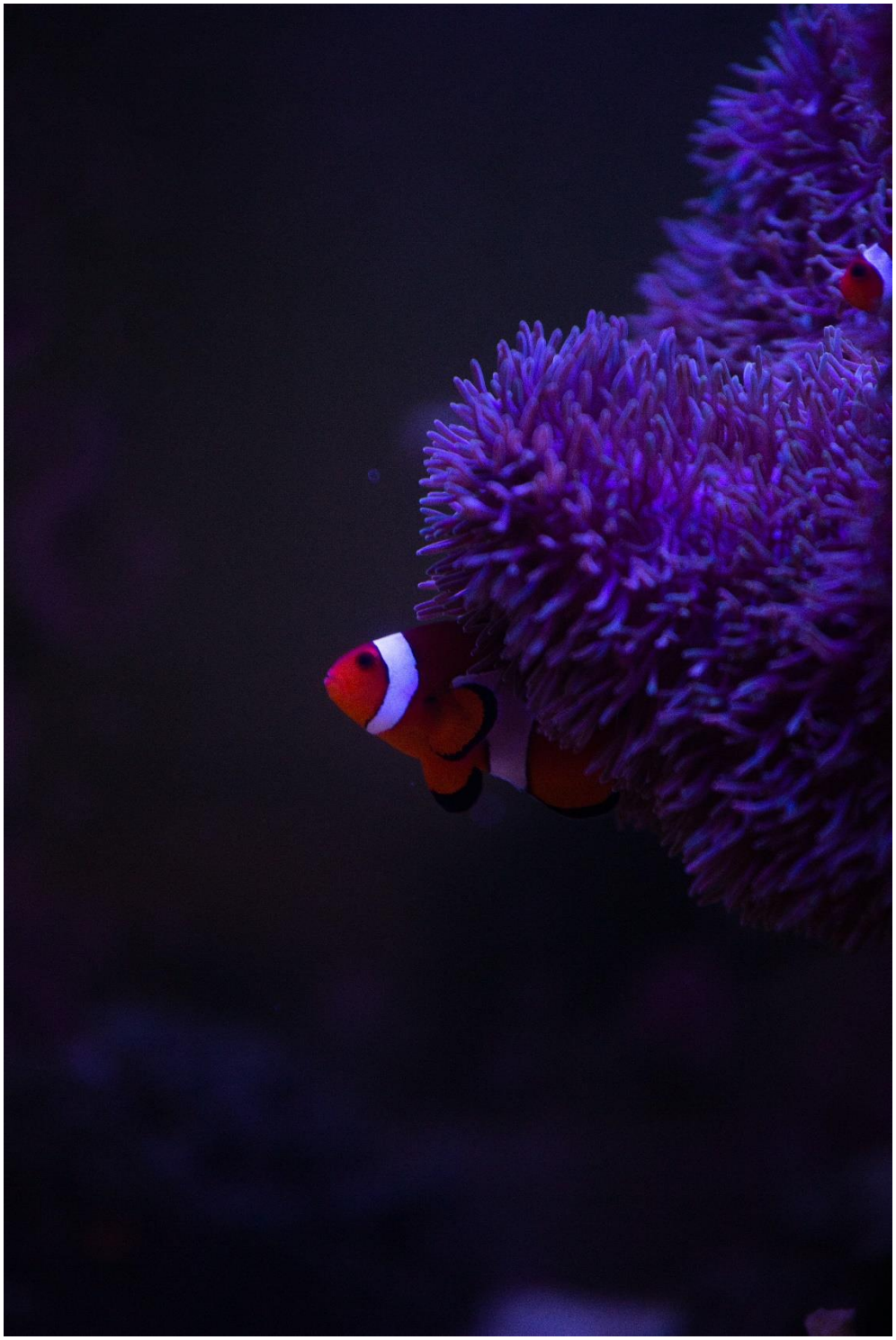


Phishing Analysis

BLUE TEAMS LABS

Sudenur MURATOĞULLARI

İçindekiler

Giriş(Introduction)

Bir kullanıcı kimlik avı e-postası aldı ve SOC'a iletti. Yararlı eserler toplamak için e-postayı ve ekini araştırıyoruz.

Metodoloji(Methodology)

Bu analizde e-postayı ve ekini incelerken not defteri, outlook araçlarının yanında URL2PNG, whois.domaintools.com ve groupdocs çevrimiçi sorgularını kullandık.

Bulgular ve Analiz(Findings and Analysis)

E-posta analizini yapmamız için bize verilen "Website contact from submission.eml" dosyasını not defterimde açıyorum.

Not Defteri'nde açılan tüm içeriği çevrimiçi posta analiz aracında analiz ediyorum.

Address Details

Mail From:	Mailer-Daemon@se7-syd.hostedmail.net.au	**Mail To:**	kinnar1975@yahoo.co.uk
Mail From Name:	Mail Delivery System	**Reply To:**	E1lMk2z-00086Y-Jw@se7-syd.hostedmail.net.au

Yukarıdaki veriler e-mail bu e-postanın birincil alıcısının kinnar1975@yahoo.co.uk olduğunu göstermekte.
Bu EML dosyasını groupdocs aracını kullanarak açacağım.
Bu, e-postayı daha net analiz etmek için önemli.

Sent: 03/19/2021 16:49 +00:00
To: john smith
Subject: Website contact form submission
Attachments: Website contact form submission

From: Mail Delivery System <Mailer-Daemon@se7-syd.hostedmail.net.au>
Sent: 18 March 2021 04:14
To: kinnar1975@yahoo.co.uk <kinnar1975@yahoo.co.uk>
Subject: Undeliverable: Website contact form submission

This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its recipients. This is a permanent error. The following address(es) failed:

kinnar1975@yahoo.co.uk
host mx-eu.mail.am0.yahoodns.net [188.125.72.73]
SMTP error from remote mail server after end of data:
554 30 Sorry, your message to kinnar1975@yahoo.co.uk cannot be delivered. This mailbox is disabled (554.30).

Burada postanın içeriğini daha net bir şekilde gözlemliyoruz.

Mailin konusu "Undeliverable: Website contact form submission". Ayrıca mailin gönderildiği tarih ve saatin 18 Mart 2021 04:14 olduğunu gözlemledik.

```
168
169 --_004_VI1PR0102MB31679BEF784B62C41CDAEDB282689VI1PR0102MB3167_
170 Content-Type: message/rfc822
171 Content-Disposition: attachment;
172         creation-date="Thu, 18 Mar 2021 04:14:19 GMT";
173         modification-date="Thu, 18 Mar 2021 04:14:19 GMT"
174 Content-ID: <5A9638EA6676A449B32643CFC62AAB5F@eurprd01.prod.exchangelabs.com>
175
176 Received: from c5s2-1e-syd.hosting-services.net.au ([103.9.171.10])
177         by se7-syd.hostedmail.net.au with esmtps (TLSv1.2:AES128-GCM-SHA256:128)
178         (Exim 4.92)
179         id 1lMk2r-0007vB-6O
180         for kinnar1975@yahoo.co.uk; Thu, 18 Mar 2021 15:14:06 +1100
181 Received: from markgard by c5s2-1e-syd.hosting-services.net.au with local (Exim 4.94)
182         id 1lMk2m-002w3b-NT
183         for kinnar1975@yahoo.co.uk; Thu, 18 Mar 2021 15:13:56 +1100
184 To: kinnar1975@yahoo.co.uk
```

Not defterinde metin ayrıntılarını incelerken kaynak IP adresine erişiyorum.

➔ 103.9.171.10

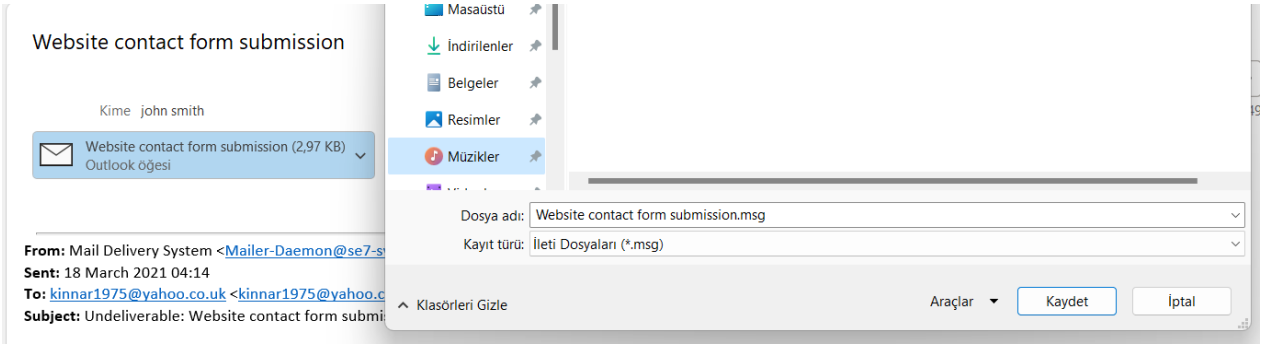
Bu IP adresini sorgumuzda kullanacağız.

IP Location	Australia Sydney Synergy Wholesale Pty Ltd
ASN	AS45638 SYNERGYWHOLESALE-AP SYNERGY WHOLESALE PTY LTD, AU (re
Resolve Host	c5s2-1e-syd.hosting-services.net.au
Whois Server	whois.apnic.net
IP Address	103.9.171.10
Reverse IP	7 websites use this address.

Sorgulamam sonucunda IP adresinin menşe ülkesinin Avustralya olduğunu ve "resolve host" değerinin c5s2-1e-syd.hosting-services.net.au olduğunu gözlemliyorum.

X-OriginatorOrg:	outlook.com

Birkaç adım önce yaptığım sorguda X-OriginatorOrg değerinin outlook.com olduğunu gözlemledim, bu nedenle dosyayı outlook kullanarak tekrar açacağım.



Dosyayı kaydetmeye çalıştığımda adını ve uzantısını açıkça görebiliyorum.

➔ Website contact form submission.msg

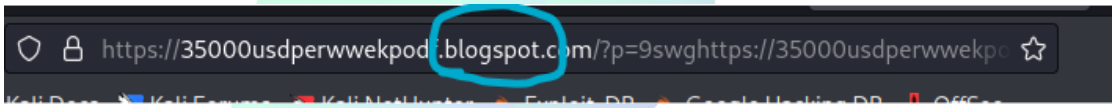
Ayrıca e-postaya eklenmiş bir dosya görüyorum.

Sent: Thursday, 18 March 2021 04:13
To: kinnar1975@yahoo.co.uk
Subject: Website contact form submission

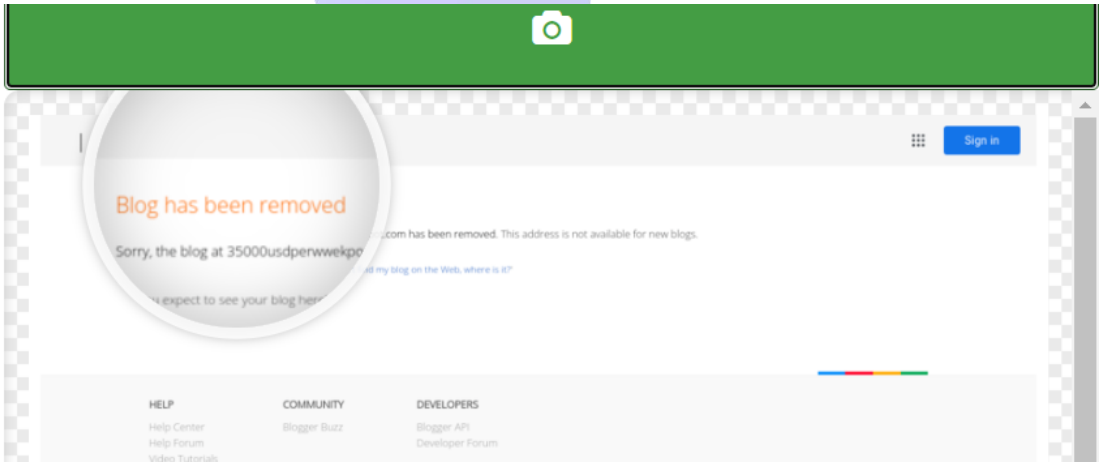
First Name: Robertbiolo
Last Name: Robertbiolo
Email Address: kinnar1975@yahoo.co.uk
Mobile: 85471397431
Booking Date: 1977-11-10
Booking Time: RobertbioloXE
Services Required:

Good earnings from $6500 per day >>>>>>>>>>
https://35000usdperwwekpodf.blogspot.sg?p=9swghttps://35000usdperwwekpodf.blogspot.co.il?o=0hnd <<<<<<<<<<

Burada "https://35000usdperwwekpodf.blogspot.sg?p=9swghttps://35000usdperwwekpodf.blogspot.co.il?o=ohnd " URL'i mevcut.



Bu URL'yi incelediğimde, bu web sayfasının blogspot hizmetinde barındırıldığını görüyorum.



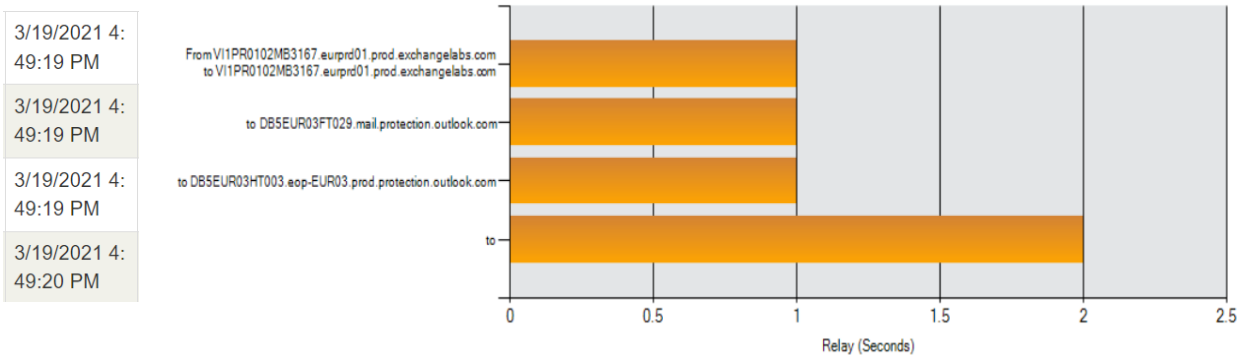
URL2PNG kullanarak, bu sayfadaki başlık metninin "Blog has been removed" olduğunu görüyorum.

Olay Zaman Çizelgesi(Timeline of Events)

- 18 Mart 2021 Cuma 04:14 :

Şüpheli e-postayı aldık.

- Aldığımız e-postanın içindeki teknik detayların tarih ve saat bilgileri.



Sonuçlar(Conclusions)

Aldığımız e-postanın şüpheli olup olmadığını analiz ettikten sonra, bunun kötü niyetli bir e-posta olduğu sonucuna ulaştık.

Bilgili personel sayesinde zararlı dosya analiz edilmeden açılmamış ve olası bir siber saldırının önüne geçilmiştir.