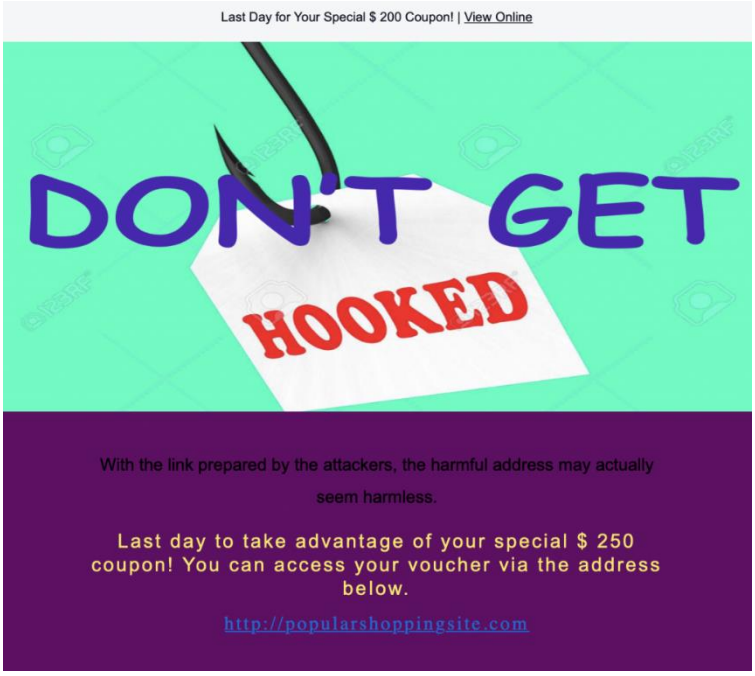
KİMLİK AVI E-POSTA **-Ahmet Arif Arslan-**

Kimlik Avına Giriş

Phishing saldırısı, kullanıcılara e-posta yoluyla kötü niyetli bağlantılara tıklayarak veya bilgisayarında kötü amaçlı dosyalar çalıştırarak genel olarak kullanıcının kişisel verilerini çalmayı amaçlayan bir saldırı türüdür.

Phishing saldırıları, siber saldırıları analiz etmek için oluşturulan **Cyber Kill Chain modelinde " Teslim** " aşamasına karşılık gelmektedir . Teslim aşaması, saldırganın önceden hazırladığı zararlı içerikleri kurban sistemlere/kişilere ilettiği adımdır.

Saldırganlar genellikle “hediye kazandınız”, “büyük indirimi kaçırmayın”, “e-postadaki bağlantıya tıklamazsanız hesabınız askıya alınacak” gibi postadaki zararlı bağlantıya tıklamayı amaçlar. ”, kullanıcıları postadaki bağlantılara tıklamaya yönlendirmek için.



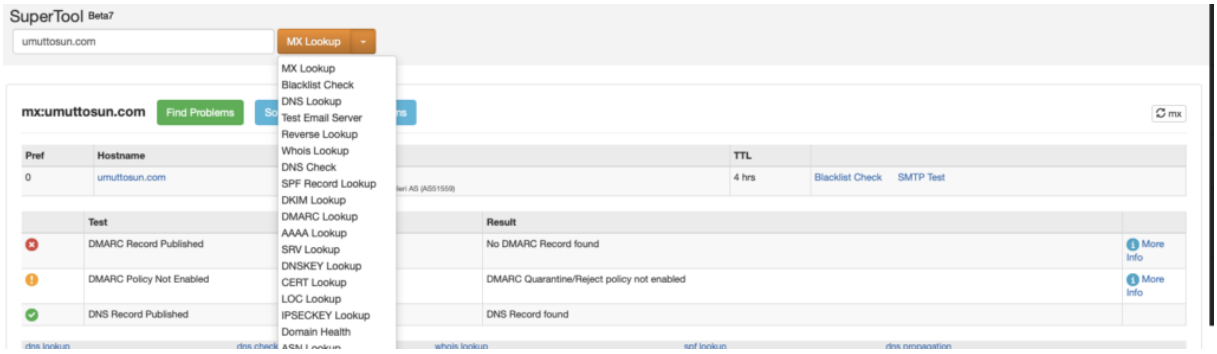
Bilgi toplama

yanıltma

Saldırganlar, e-postaların mutlaka bir kimlik doğrulama mekanizmasına sahip olmaması nedeniyle başkası adına e-posta gönderebilir. Saldırganlar, kullanıcıyı gelen e-postanın güvenilir olduğuna inandırmak için sahtecilik adı verilen tekniği kullanarak başkası adına posta gönderebilir. E-posta Spoofing tekniğini önlemek için çeşitli protokoller oluşturulmuştur. SPF, DKIM ve DMARC protokolleri yardımıyla göndericinin adresinin fake mi yoksa gerçek mi olduğu anlaşılabilir. Bazı mail uygulamaları bu kontrolleri otomatik olarak yapmaktadır. Ancak bu protokollerin kullanımı zorunlu değildir ve bazı durumlarda sorunlara neden olabilir.

- Gönderen Politikası Çerçevesi (SPF)
- Etki Alanı Anahtarları Tanımlı Posta (DKIM)

Mailin spoof olup olmadığını manuel olarak öğrenmek için öncelikle mailin SMTP adresinin öğrenilmesi gerekir. Mxtoolbox gibi araçlar kullanılarak domainin SPF, DKIM, DMARC ve MX kayıtları öğrenilebilir . Buradaki bilgiler karşılaştırılarak mailin sahte olup olmadığı öğrenilebilir.



Kendi mail sunucularını kullanan büyük kurumların IP adresleri kendilerine ait olacağından SMTP IP adresinin whois kayıtlarına bakılarak SMTP adresinin o kuruma ait olup olmadığı incelenebilir.

Burada önemli olan nokta, gönderici adresi sahte değilse, mailin güvenli olduğunu söyleyemeyiz. Kurumsal/kişisel e-posta adresleri hacklenerek güvenilir kişiler adına zararlı mailler gönderilebilir. Bu tür siber saldırılar zaten gerçekleşti, bu nedenle bu olasılık her zaman göz önünde bulundurulmalıdır.

E-posta Trafik Analizi

Bir kimlik avı saldırısını analiz ederken birçok parametreye ihtiyaç vardır. Mail ağ geçidi üzerinde yapılacak arama sonuçlarında saldırının boyutunu ve hedef kitleyi aşağıdaki parametrelere göre öğrenebiliriz.

- Gönderici Adresi(info@letsdefend.io)
- SMTP IP Adresi (127.0.0.1)
- @letsdefend.io (alan tabanı)
- Letsdefend (Saldırgan, gmail hesabının yanı sıra hotmail hesabından da göndermiş olabilir)
- Konu (gönderen adresi ve SMTP adresi sürekli değişiyor olabilir)

Arama sonuçlarında mail numaralarının yanı sıra alıcı adresleri ve saat bilgilerinin de öğrenilmesi gerekmektedir. Zararlı e-postalar sürekli

aynı kullanıcılara yönlendiriliyorsa, e-posta adresleri bir şekilde sızdırılmış ve PasteBin gibi sitelerde paylaşılmış olabilir.

Saldırganlar, Kali Linux'ta Harvester aracıyla e-posta adreslerini bulabilir. Kişisel posta adreslerinin web sitelerinde tutulması saldırganlar için potansiyel bir saldırı vektörü olacağından, bu tür bilgilerin açıkça paylaşılmaması önerilir.

E-posta Başlığı nedir?

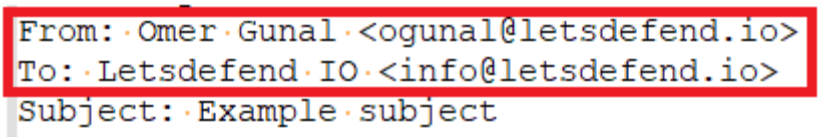
"Başlık" temelde postanın gönderen, alıcı ve tarih gibi bilgileri içeren bir bölümüdür. Ayrıca "Dönüş Yolu", "Yanıtla" ve "Alındı" gibi alanlar da vardır. Aşağıda örnek bir e-postanın başlık ayrıntılarını görebilirsiniz.

```
Delivered-To: info@letsdefend.io
Received: by 2002:ab4:8fc7:0:0:0:0:0 with SMTP id cs7csp1721687ecb;
        Mon, 21 Mar 2022 06:10:11 -0700 (PDT)
X-Received: by 2002:a05:620a:2416:b0:67d:7735:4bbf with SMTP id d22-20020a05620a241600b0067d77354bbfmr12659013qkn.501.1647868211414;
        Mon, 21 Mar 2022 06:10:11 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1647868211; cv=none;
        d=google.com; s=arc-20160816;
        b=ZxH9+3UjmlxSK/Y/LeaLuupLgQT9gWm7lZagKamcTCU/4Tp5WIYpwXZe7PKv4gz30h
        4jUc3QKlzmit8KREmbS4RRQQz8E7Varx+b2ZpejUltxWixYcoOWt25rWrX1UnUU29vdT
        OuGXWQYjqfJLoQeaDRSPoaPWKBrLbgf1uZv7R5A9sYjVgf9jE/JfY2HqBiHWvK/Z6v55
        FH7TBAvChCAdh7ronXI4FfxggfvGh7yEAko6qHmnTwA3CsuseMKh18P4M2ZLNaMtx2t0
        Ej5MiiM8BR/nJjetLwcuyNh37acMD7fuB4Atsu+4FS4sa8dFA9JSwR7wAUNtL4znh7bG
        vlpg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=mime-version:delivered-to:date:message-id:subject:to:from
        :dkim-signature;
        bh=HIAfgOlDaK3JQLpH5fJuRxhIvU9cb88FSU4V8MlV9sI=;
        b=DQbcXx7CopYCaegIw+c82nMDSTr6SGHNR4p+jqBAgtdIm3/TXsiJwKXJJv/Yj6HRp9
        YNm2RuORlLdAjcHuk1cl7wngpfLP2678iuQsZvzPBFEMbgjRZbh/2OeIaNBpkEMzlaDo
        4a6MNUzl/DJmLVQokqQ7s5hYePucKTGhpzijQDC/7aubWiaXuOzwXvNt9V2GsHOxvoRh
        dph2LsXWAdYDc6sAGCtWR7wwIve4zoDBw/evWoH/g55aChuX8KGB7OPuP3Gl2fo0F296
        EAVSovT/zvPl0/MN6oaSOwIYoYshyKm36ceOtbFZLqDYhxslD+NeXEak8seecPz14LGg
        lNEg==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@letsdefend.io header.s=google header.b=hRMOgQ3u;
       spf=pass (google.com: domain of ogunal@letsdefend.io designates 209.85.220.41 as permitted sender) smtp.mailfrom=ogunal@letsdefend.io
Return-Path: <ogunal@letsdefend.io>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id d7-20020ac85447000000b002de980041b8sor9866778qtq.15.2022.03.21.06.10.11
        for <info@letsdefend.io>
        (Google Transport Security);
        Mon, 21 Mar 2022 06:10:11 -0700 (PDT)
Received-SPF: pass (google.com: domain of ogunal@letsdefend.io designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@letsdefend.io header.s=google header.b=hRMOgQ3u;
       spf=pass (google.com: domain of ogunal@letsdefend.io designates 209.85.220.41 as permitted sender) smtp.mailfrom=ogunal@letsdefend.io
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=letsdefend.io; s=google;
        h=from:to:subject:message-id:date:delivered-to:mime-version;
        bh=HIAfgOlDaK3JQLpH5fJuRxhIvU9cb88FSU4V8MlV9sI=;
        b=hRMOgQ3uKL9FSba7f/J1WB2QkC0Rr8IR6YqQBJlHTp9egr9Vwpck6qHPYHskxOdgT0
        7vwxxkHhKrBLJwGjqXeVv+MNBXLK52fiLw3B3esnnMdrmyysJLuRuvyRV2LakLqY9gCc
        1W0yOlWFT/990p5h4GQMJOPSYQLPbZTwJEWC2UdfCHte4YHuxB1PUVZ261whpbqNdxGy
        jcKBbl4DN0AM3olu5tu6hVZr6kgreS7TTrShGz/73bTM0JnoExH/XU+V8RmYP60ei3Av
```

E-posta Başlığı ne işe yarar?

Gönderici ve Alıcı Kimliğini Etkinleştirir

Başlıktaki "Kimden" ve "Kime" alanları sayesinde bir e-postanın kimden kime gideceği belirlenir. Yukarıdaki "eml" formatında indirdiğiniz e-postaya bakarsak " ogunal@letsdefend.io "adresinden " info@letsdefend.io " adresine gönderildiğini görürüz.



Spam Engelleyici

Başlık analizi ve diğer çeşitli yöntemler kullanılarak spam e-postaları tespit etmek mümkündür. Bu, insanları SPAM e-postaları almaktan korur.

Bir E-postanın Rotasını İzlemeye İzin Verir

Bir e-postanın doğru adresten gelip gelmediğini görmek için izlediği rotayı kontrol etmek önemlidir. Yukarıdaki örnek e-postaya bakarsak " ogunal@letsdefend.io " adresinden geldiğini görüyoruz ama aslında "letsdefend.io" alan adından mı yoksa aynı adı taklit eden farklı bir sahte sunucudan mı geldi? Bu soruyu cevaplamak için başlık bilgisini kullanabiliriz.

Önemli Alanlar

İnternet başlığındaki " Kimden

" alanı, gönderenin adını ve e-posta adresini belirtir.

Kime

Posta başlığındaki bu alan, e-postanın alıcısının ayrıntılarını içerir.

Adlarını ve e-posta adreslerini içerir. CC (karbon kopya) ve BCC (kör karbon kopya) gibi alanlar da alıcılarınızın ayrıntılarını içerdiğinden bu kategoriye girer.
Karbon kopya ve kör karbon kopya hakkında daha fazla bilgi edinmek istiyorsanız, CC ve BCC'nin nasıl kullanılacağına bakın.

Tarih

Bu, e-postanın ne zaman gönderildiğini gösteren zaman damgasıdır. Gmail'de genellikle "gün gg ay yyyy hh:mmss" biçimini izler. Dolayısıyla, 16 Kasım 2021'de 16:57:23'te bir e-posta gönderilmiş olsaydı, 16 Kasım 2021 Çar olarak gösterilirdi 16 :57:23.

Konu Konu

, e-postanın konusundan bahseder. Tüm mesaj gövdesinin içeriğini özetler.

Dönüş Yolu

Bu posta başlığı alanı, Yanıt olarak da bilinir. Bir e-postayı yanıtlarsanız, Geri Dönüş Yolu alanında belirtilen adrese gidecektir.

Etki Alanı Anahtarı ve DKIM İmzaları

Etki Alanı Anahtarı ve Etki Alanı Anahtarı Tanımlanmış Posta (DKIM), e-posta hizmet sağlayıcılarının, SPF imzalarına benzer şekilde e-postalarınızı tanımlamasına ve doğrulamasına yardımcı olan e-posta imzalarıdır.

İleti Kimliği

İleti Kimliği başlık alanı, her postayı tanımlayan benzersiz bir harf ve

sayı kombinasyonudur. Hiçbir iki e-posta aynı Mesaj Kimliğine sahip olmayacaktır.

MIME Sürümü

Çok Amaçlı İnternet Posta Uzantıları (MIME), bir internet kodlama standardıdır. Görüntüler, videolar ve diğer ekler gibi metin olmayan içeriği metne dönüştürür, böylece bir e-postaya eklenebilir ve SMTP (Basit Posta Aktarım Protokolü) aracılığıyla gönderilebilir.

Alınan

Alan, alıcının gelen kutusuna ulaşmadan önce bir e-postadan geçen her posta sunucusunu listeler. Ters kronolojik sırada listelenmiştir - burada üstteki posta sunucusu, e-posta iletisinin geçtiği son sunucudur ve alt kısım, e-postanın geldiği yerdir.

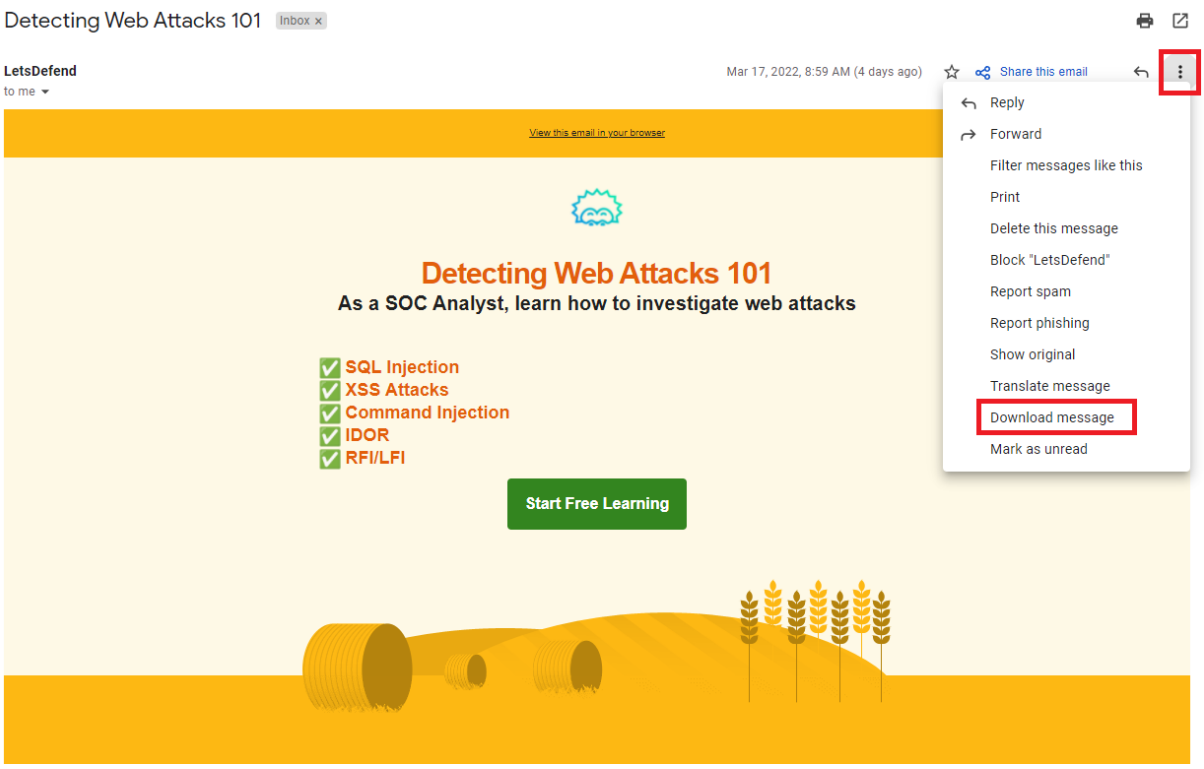
X-Spam Durumu

X-Spam Durumu size bir e-posta mesajının spam puanını gösterir. İlk olarak, bir iletinin spam olarak sınıflandırılıp sınıflandırılmadığı vurgulanır.
Ardından, e-postanın spam puanı ve e-postanın spam eşiği gösterilir. Bir e-posta, bir gelen kutusunun spam eşiğini karşılayabilir veya aşabilir. Çok spam içeriyorsa ve eşiği aşarsa, otomatik olarak spam olarak sınıflandırılır ve spam klasörüne gönderilir.

E-posta Başlığınıza Nasıl Erişilir?

Gmail

1- İlgili e-postayı açın
2- Sağ üstte bulunan 3 noktaya "..."
tıklayın 3- "Mesajı indir" butonuna tıklayın.

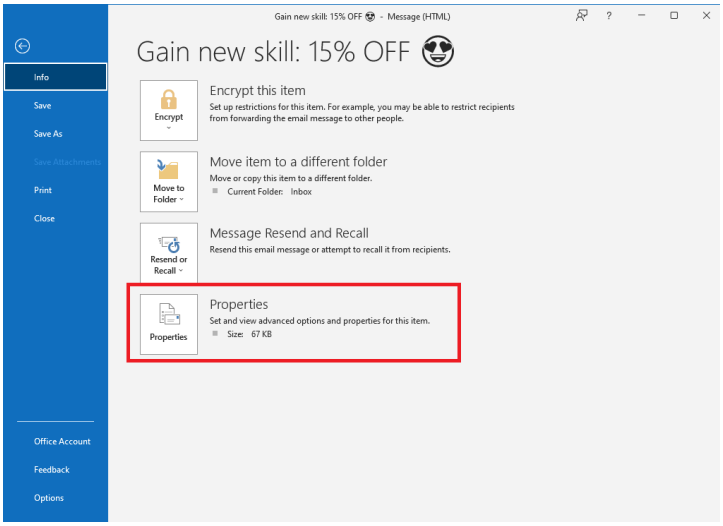


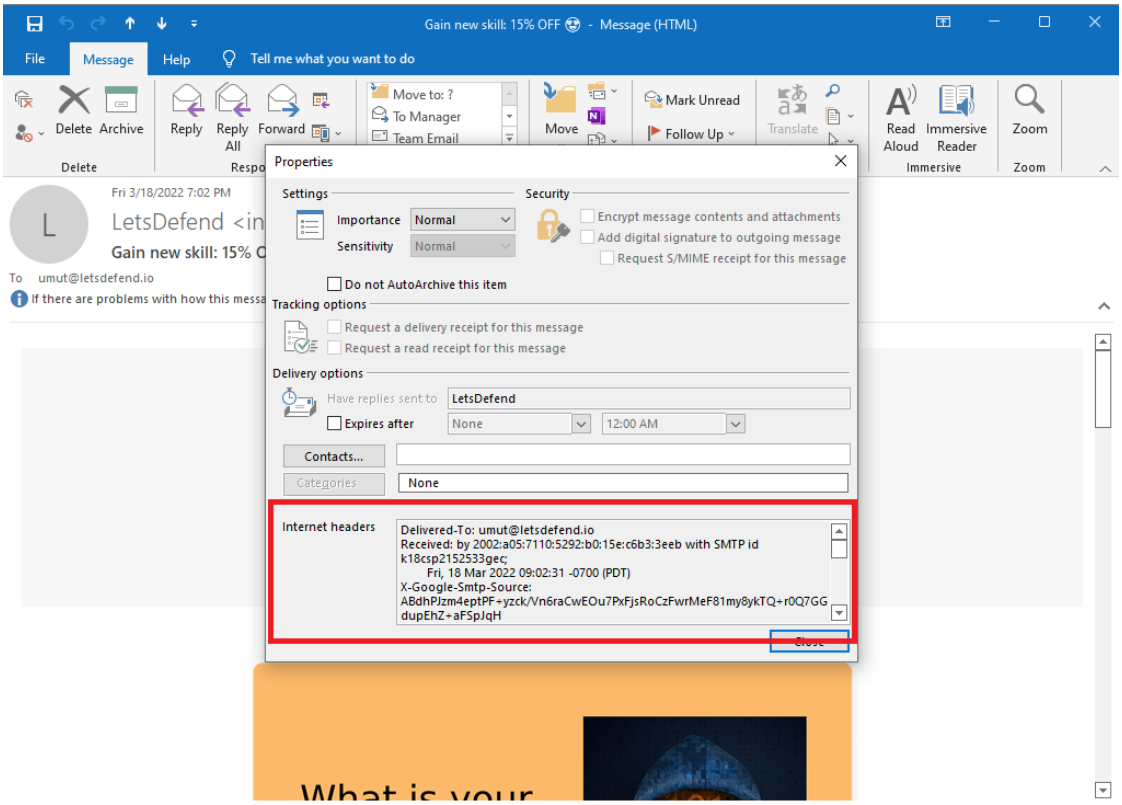
4- İndirildi ". Herhangi bir notebook uygulaması ile "eml" uzantılı dosyayı açın

Görünüm

1- İlgili e-postayı açın

2- Dosya - > Bilgi -> Özellikler - > İnternet başlıkları





E-posta Başlık Analizi

Önceki bölümlerde kimlik avı e-postasının ne olduğundan, başlık bilgisinin ne olduğundan ve ne yaptığından bahsetmiştik. Şimdi, bir e-postanın kimlik avı olduğundan şüphelendiğimizde, ne yapmamız gerektiğini ve analiz sürecinin nasıl olması gerektiğini bileceğiz.

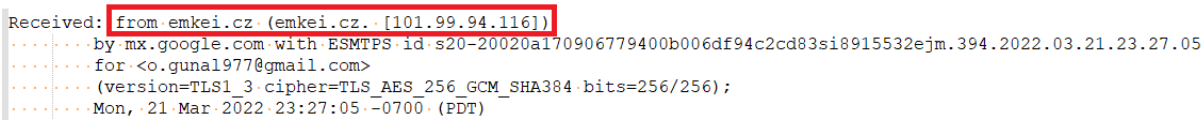
Kimlik Avı analizi sırasında başlıkları kontrol ederken yanıtlamamız gereken temel sorular şunlardır:

E-posta doğru SMTP sunucusundan mı gönderildi?

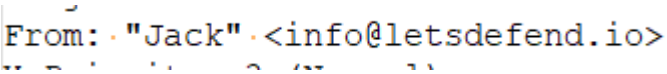
"Kimden" ve "Dönüş Yolu / Yanıt" verileri aynı mı?

E-posta doğru SMTP sunucusundan mı gönderildi?

Postanın izlediği yolu görmek için "Alındı" alanını kontrol edebiliriz. Aşağıdaki resimde görüldüğü gibi, posta IP adres sunucusundan "101[.]99.94.116"dır.

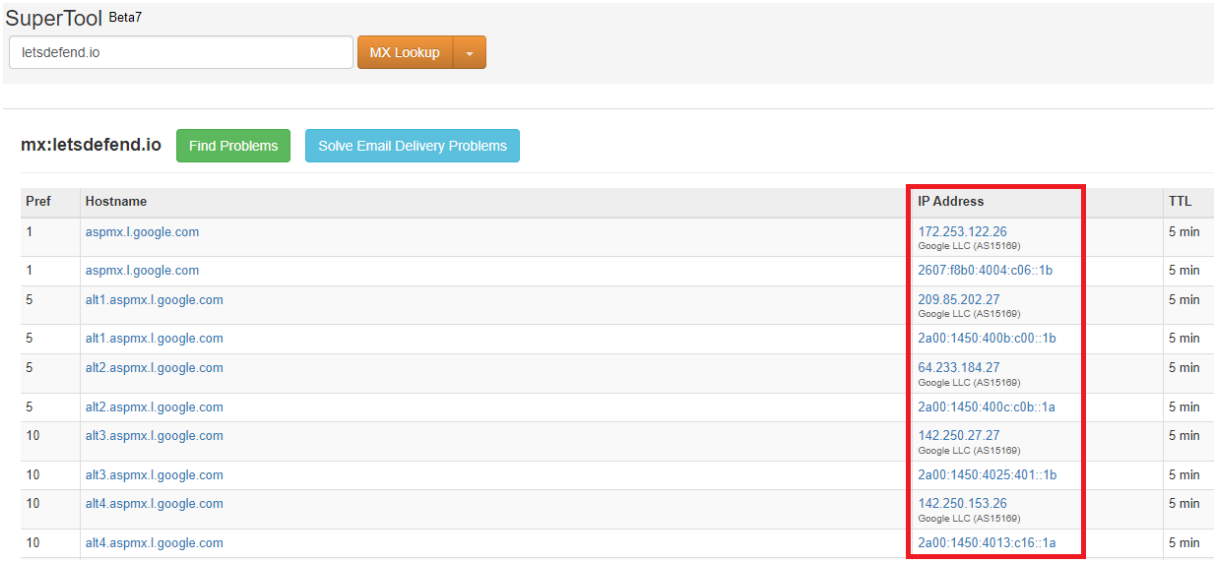


Postayı kimin ("gönderen") gönderdiğine bakarsak, Letsdefend.io alan adından geldiğini görürüz.



Yani normal şartlar altında, "letsdefend.io", posta göndermek için "101[.]99.94.116" kullanmalıdır. Bu durumu doğrulamak için "letsdefend.io" tarafından aktif olarak kullanılan MX sunucularını sorgulayabiliriz.

"mxtoolbox.com", aradığınız etki alanı tarafından kullanılan MX sunucularını size göstererek yardımcı olur.



Yukarıdaki resme bakarsak, "letsdefend.io" alan adı, e-posta sunucusu olarak Google adreslerini kullanır. Yani emkei[.]cz veya "101[.]99.94.116" adresleri ile hiçbir ilişkisi yoktur.

Bu kontrolde e-postanın asıl adresten gelmediği, sahte olduğu belirlendi.

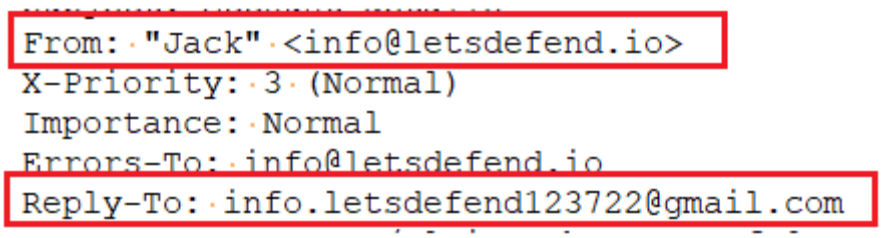
"Kimden" ve "Dönüş Yolu / Yanıt" verileri aynı mı?

İstisnai durumlar dışında, e-postayı gönderen ile yanıtları alan kişinin aynı olmasını bekleriz. Bu alanların Phishing saldırılarında neden farklı kullanıldığına dair bir örnek:

LetsDefend'e Google'da çalışan birinin soyadıyla aynı e-postayı (gmail, hotmail vb.) gönderen LetsDefend, çalışana faturayı kendisinin düzenlediğini ve ödemeyi XXX hesabına yapması gerektiğini söyler. Olası bir e-postaya cevap verilmesi durumunda sahte e-posta

adresinin öne çıkmaması için "Reply-to" alanına gerçek Google çalışanının e-posta adresini koyar.

Yukarıda indirdiğimiz e-postaya dönersek, tek yapmamız gereken "Kimden" ve "Yanıtla" alanlarındaki e-posta adreslerini karşılaştırmak.



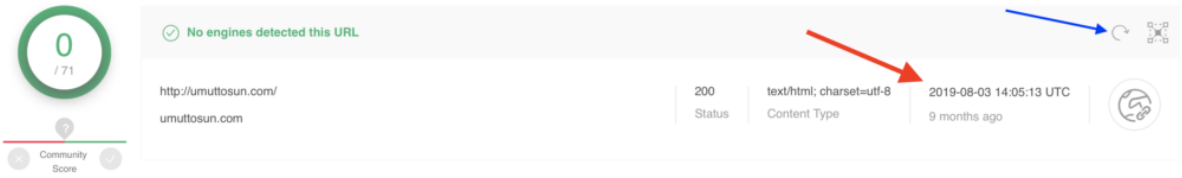
Gördüğünüz gibi, veriler farklı. Yani bu e-postaya cevap vermek istediğimizde aşağıdaki gmail adresine cevap göndereceğiz. Bu verilerin farklı olması her zaman kesinlikle bir kimlik avı e-postası olduğu anlamına gelmez, olayı bir bütün olarak ele almamız gerekir. Yani bu şüpheli duruma ek olarak e-posta içeriğinde zararlı bir ek, URL veya yanıltıcı içerik varsa e-postanın phishing olduğunu anlayabiliriz.

Statik Analiz

Düz metinden oluşan maillerin sıkıcı olduğu bir gerçektir. Bu nedenle mail uygulamaları HTML desteği sağlayarak kullanıcıların daha fazla ilgisini çekebilecek maillerin oluşturulmasına olanak sağlar. Tabii ki, bu özelliğin bir dezavantajı var. Saldırganlar, zararsız görünen butonların / metinlerin arkasına zararlı URL adreslerini gizleyerek HTML ile e-postalar oluşturabilirler.

Yukarıdaki resimde görüldüğü gibi linke tıklandığında kullanıcının gördüğü adres farklı olabiliyor (link üzerine gelindiğinde gerçek adres görülüyor).

VirusTotal üzerinde maildeki web adreslerini aratarak antivirüs motorlarının web adresini zararlı olarak algılayıp algılamadığını öğrenmek mümkündür. VirusTotal'da aynı adresi/dosyayı daha önce başka biri analiz etmişse, VirusTotal sıfırdan analiz yapmaz, size eski analiz sonucunu gösterir. Bu özelliği hem avantaj hem de dezavantaj olarak kullanabiliriz.



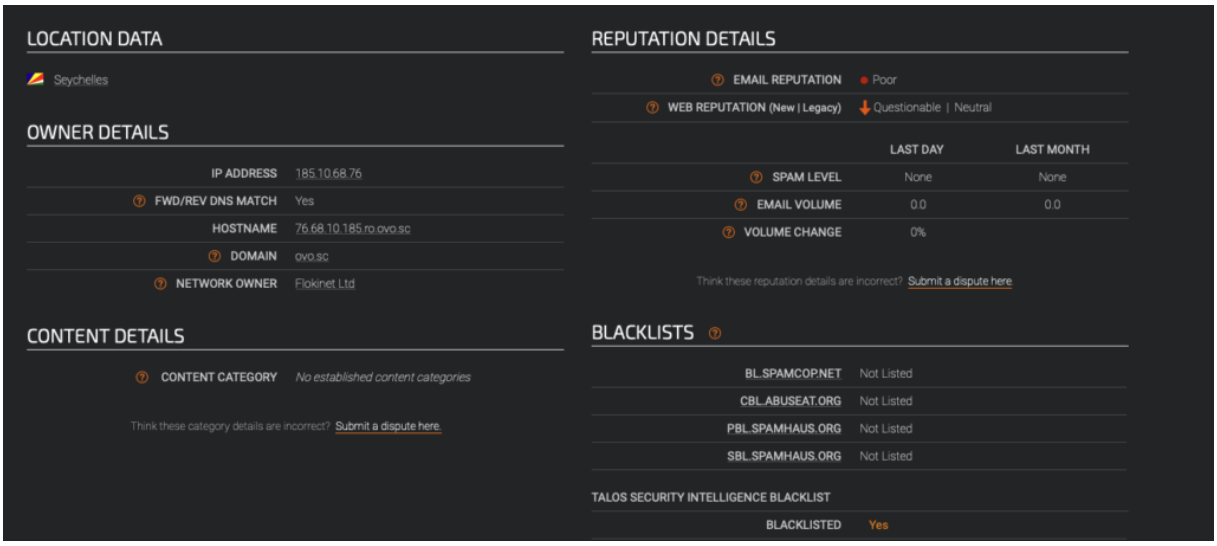
Saldırgan, VirusTotal'da zararlı içerik barındırmadan domain adresini ararsa, o adres VirusTotal'da zararsız görünür ve fark edilmezse, bu adresin zararsız olduğu yanılgısına düşebilirsiniz. Yukarıdaki resimde umuttosun.com adresinin zararsız göründüğünü görebilirsiniz ancak kırmızı ok ile işaretlenmiş bölüme bakarsanız bu adresin 9 ay önce

arandığını ve bu sonucun 9 ay önce olduğunu göreceksiniz. Tekrar analiz edilebilmesi için mavi ok ile işaretlenmiş butona basılması gerekmektedir.

Sayfa daha önce VirusTotal'da arandıysa, saldırganın hazırlık aşamasında sitenin tespit oranını görmek istediği anlamına gelebilir. Tekrar analiz edersek, antivirüs motoru bunu kimlik avı olarak algılar, bu da saldırganın analistleri kandırmak için bir hamlesi olduğu anlamına gelir.

Maildeki dosyaların statik analizini yapmak o dosyanın kapasitesinin/yeteneklerinin öğrenilmesini sağlayabilir. Ancak statik analiz uzun zaman aldığı için dinamik analiz ile ihtiyacınız olan bilgiye daha hızlı ulaşabilirsiniz.

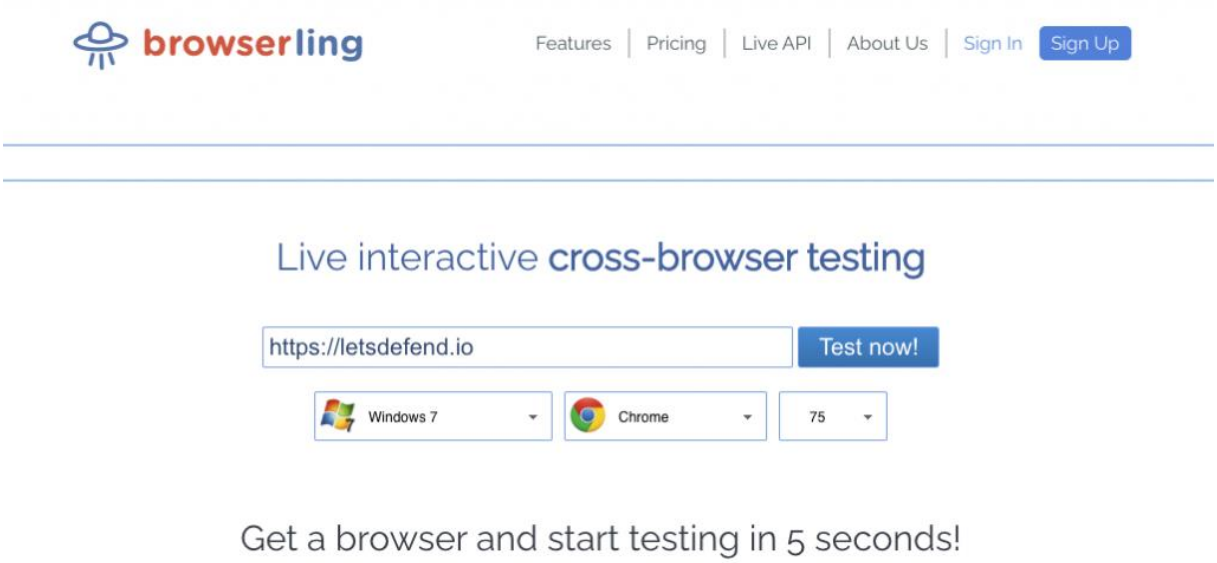
Cisco Talos Intelligence , IP adreslerinin itibarlarını öğrenebileceğimiz arama bölümlerine sahiptir. Talos üzerinde tespit ettiğimiz mailin SMTP adresini aratarak IP adresinin itibarını görebilir ve kara listede olup olmadığını öğrenebiliriz. SMTP adresi kara listedeyse, güvenliği ihlal edilmiş bir sunucuya saldırı yapıldığı anlaşılabilir.



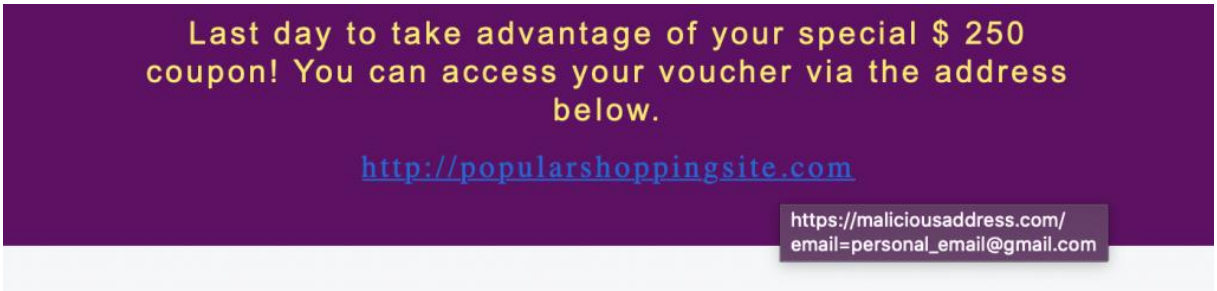
Aynı şekilde, IP adresinin daha önce kötü niyetli faaliyetlerde bulunup bulunmadığını belirlemek için SMTP adresi VirusTotal ve AbuseIPDB'de aranabilir.

Dinamik Analiz

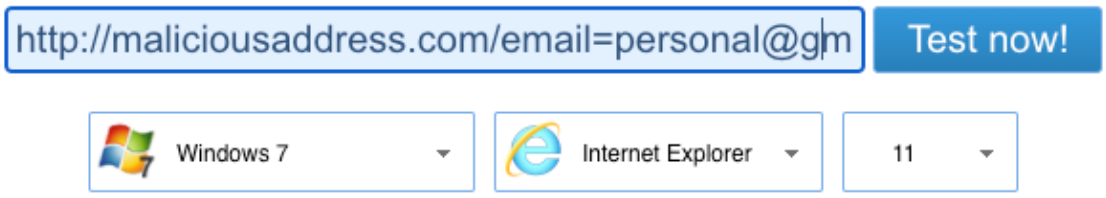
URL'ler ve dosyalar postada bulunabilir. Bu dosyalar ve URL adreslerinin incelenmesi gerekir. Bu dosyaları kişisel bilgisayarınızda çalıştırarak verilerinizin bilgisayar korsanları tarafından çalınmasını istemezsiniz. Bu nedenle maildeki web siteleri ve dosyalar sandbox ortamlarda çalıştırılmalı ve sistemde yapılan değişiklikler incelenmeli, zararlı olup olmadığı kontrol edilmelidir.



Postadaki web adreslerini hızlı bir şekilde kontrol etmek istiyorsanız, Browserling gibi çevrimiçi web tarayıcılarını kullanarak web sitesinin içeriğini görebilirsiniz . Bu tür hizmetlerle ilgili iyi olan şey, web sayfasına kendi bilgisayarınızdan gitmediğiniz için tarayıcıları etkileyen olası bir sıfır gün güvenlik açığından etkilenmemenizdir. Browserling gibi web tarayıcıları kullanmanın dezavantajı, kötü niyetli dosya siteye indirilirse bu dosyayı çalıştıramazsınız. Bu nedenle analiziniz kesintiye uğrayacaktır.



Maildeki adreslere gitmeden önce adreste önemli bilgiler olup olmadığı kontrol edilmelidir. Yukarıdaki görseldeki örneği incelediğimizde, kullanıcı popülershoppingsite[.]com'a tıkladığında aslında kullanıcının adresinin ziyaret edildiği, e-posta parametresinde ise kullanıcının e-posta adresinin olduğu görülmektedir. Kullanıcı phishing sayfasına şifresini girmese bile bu adrese ulaşıldığında maildeki bağlantıya ulaşıldığı ve saldırganın bu kullanıcının geçerli olduğunu anladığı anlamına gelir. Daha sonra gerçekleştireceği saldırılarda geçerli olan kullanıcılar üzerinde sosyal mühendislik saldırıları yaparak gerçekleştireceği saldırının başarı oranını artırabilir. Bu nedenle adreslere ulaşmadan önce e-posta adresi gibi bilgilerin değiştirilmesi gerekmektedir.



Sandbox ortamlarında şüpheli dosyaları ve web sitelerini inceleyebilirsiniz. Bu ortamlardaki dosyaları incelediğinizde, bilgisayarınıza kötü amaçlı yazılım bulaştırma riskini ortadan kaldırmış olursunuz. Birçok sandbox hizmeti / ürünü mevcuttur. Bu ürün/hizmetler ücretli ve ücretsiz olarak kullanılabilir. Bu hizmetlerden birini/birkaçını ihtiyaçlarınıza göre seçebilirsiniz.

Mailde url ve dosya olmaması bunun zararlı olmadığı anlamına gelmez. Saldırgan, analiz ürünlerine kapılmamak için resim olarak da gönderebilir.

Saldırganların kullandığı bir diğer teknik, normalde yasal siteleri kullanarak kimlik avı saldırıları gerçekleştirmektir. Bazıları aşağıdaki gibidir.

- **Google ve Microsoft gibi Bulut Depolama hizmetleri sunan hizmetleri kullanma**
    - Saldırganlar, sürücüye zararlı dosyalar yükleyerek kullanıcıya zararsız görünen Google/Microsoft sürücü adreslerine tıklamaya çalışırlar.

- **Microsoft, Wordpress, Blogspot, Wix gibi ücretsiz alt etki alanları oluşturmaya izin veren servisleri kullanma**
    - Saldırganlar, bu hizmetlerden ücretsiz bir alt etki alanı oluşturarak güvenlik ürünlerini ve analistleri aldatmaya çalışır. Whois bilgisi subdomain olarak aranamadığı için bu adreslerin geçmişte alındığı ve Microsoft, Wordpress gibi kurumlara ait olduğu görülüyor.>

- **Form başvuruları**
    - Serbest form oluşturmaya izin veren hizmetler mevcuttur. Saldırganlar, kendileri bir balıkçılık sitesi oluşturmak yerine bu hizmetleri kullanır. Domain normal şartlarda zararsız olduğu için antivirüs yazılımlarına takılmadan kullanıcıya geçebilir. Google Formu bu hizmetlere bir örnektir. Whois bilgilerine bakıldığında alan adının Google olduğu görülebilir, bu nedenle saldırgan analistleri yanıltabilir.