NÖHÜ Müh. Bilim. Derg. / NOHU J. Eng. Sci., 2021; 10(2), 450-455

Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi
Niğde Ömer Halisdemir University Journal of Engineering Sciences

Araştırma makalesi / Research article

www.dergipark.org.tr/tr/pub/ngumuh / www.dergipark.org.tr/en/pub/ngumuh

Web sitesi tabanlı oltalama saldırılarının adli analizi

Forensic analysis of web-based phishing attacks

İlker Kara[1,*]

[1]*Çankırı Karatekin Üniversitesi Eldivan Sağlık Hizmetleri Meslek Yüksek Okulu, Çankırı, Türkiye.*

Özet

Teknolojide yaşanan gelişmeler insan hayatını kolaylaştırmakta ve birçok faaliyetleri internet ortamında gerçekleştirme imkânı sunmaktadır. İnternet teknolojisi ve uygulamalarının kullanımının artması beraberinde bazı riskleri de içermektedir. Güvenlik açıkları yâda siber saldırı yöntemleri (zararlı yazılımlar, oltalama saldırıları gibi) her geçen gün yeni mağdurların oluşmasına neden olmaktadır. Web tabanlı oltalama saldırıları, sahte web siteler kullanarak kurbanların kredi kartı bilgileri veya kişisel şifreler gibi önemli bilgilerini ele geçirmek için tasarlanmış saldırılar olarak bilinmektedir. Kurbanların günlük yaşantısında internet ortamında yaptığı faaliyetleri hedef alarak (internet bankacılığı, sosyal medya kullanımı, kurumsal işlemler, aldatıcı kampanyalar gibi) tasarlanan sahte web sitelerine kişisel bilgilerini giriş yapmasını sağlamak için yönlendirmektedirler. Web tabanlı oltalama saldırı önlemeye yönelik çeşitli araştırmalar ve çalışmalar yapılmakla birlikte başarı oranı tartışmalıdır. Web tabanlı oltalama saldırılarıyla mücadelede saldırganların kullandığı bilinen araç, yöntem ve yaklaşımları tanımlanması ve incelenmesi mücadelede önemli katkılar sağlayacaktır. Bu çalışma web tabanlı oltalama saldırıların adli bilişim yöntemleriyle analizlerine odaklanmaktadır. Çalışmada gerçek bir web tabanlı oltalama saldırısı seçilerek saldırıda kullanılan web sitesinin adli analizi yapılmıştır. Çalışmanı sonuçlarından saldırgana ait bilgilere ulaşılabilir olduğu görülmüştür.

Anahtar kelimeler: Oltalama saldırısı, Adli analiz, Saldırı tespiti ve analiz metodu.

Abstract

Developments in technology offer many opportunities to make activities on the internet for making human life easier. Increasing use of internet technology and applications also involves some risks. Some risks are involved in the increasing use of internet technology applications due to security weaknesses or cyber-attack methods (such as malware, phishing attacks) which cause new victims to occur every day. Web-based phishing attacks are known as attacks designed to obtain victims' vital information, such as credit card information or personal passwords, using fake websites. The victims' daily life activities (such as internet banking, social media usage, corporate transactions, and deceptive campaigns) were monitored in the internet environment to enable them to enter their personal information into fake websites designed. Even though various researches and studies have been piloted to avoid web-based phishing attacks, the success rate is provocative. Identifying and examining the known tools, methods and approaches used by attackers in struggling web-based phishing attacks will provide important contributions to combat. This study was focused on the analysis of web-based phishing attacks with forensic methods. In this study, a real web-based phishing attack was selected and forensic analysis of the website used in the attack was analyzed. It could be concluded from the results of the study that the information about the attacker might be reachable.

Keywords: Phishing attack, Forensic analysis, Attack detection and analysis method.

1 Giriş

Dünya genelinde, kişisel kullanıcıları, ticari şirketleri veya resmi kurumları hedef alan sayısız oltalama (phishing) saldırılarına maruz kalmaktadır [1]. Oltalama saldırısı, saldırganların hedefteki kullanıcıları korkutma, merak uyandırma veya sahte vaatlerde (para, hediye, indirim gibi) bulunarak önemli bilgilerini ele geçirmek üzerine tasarlanmış siber saldırılardır [2]. Bu saldırıların en önemli özelliği saldırganın mağduru çok kolayca tuzağa düşürmesi ve istediği bilgileri ele geçirebilmesidir [3]. Oltalama saldırı yöntemleri sürekli gelişmektedir. Saldırganlar, güncel olaylar ve gelişmelerden (salgın, politika yâda toplumsal ihtiyaçlar gibi) ilham alarak kişilerin dikkatini çekmek üzerine saldırı stratejisini belirleyebilmektedir [4]. En popüler saldırı yöntemi ise mağdura sahte bir e-posta ile ulaşarak hedef bilgisayar veya cep telefonuna zararlı yazılım (malware) indirmesine yönlendirmesidir [5] . Zararlı yazılım kurban sistemde kayıtlı şifreleri veya kimlik bilgilerini ulaşarak saldırgana iletebilmekte veya mağduru e-posta içerisinde bulunan sahte bir web sitesine yönlendirerek bu bilgileri girmesi isteyebilmektedir [6].

Diğer bir yöntem ise resmi bir kurumdan ya da finansal bir şirkettin web sitesini taklit ederek mağdurdan bu sitede bulunan sahte bir formu doldurması (kimlik bilgileri veya bankacılık bilgileri gibi) istenmektedir. Bu tuzağa düşen mağdurun banka hesaplarını boşaltılmakta veya bu değerli bilgileri kötüye kullanılabilmektedir [7]. Oltalama web siteleri, taklit ettikleri web sitelerinde bulunan (logo, resim

* Sorumlu yazar / Corresponding author, e-posta / e-mail: ilkerkara@karatekin.edu.tr (İ.Kara)
Geliş / Recieved: 04.03.2021 Kabul / Accepted: 31.05.2021 Yayımlanma / Published: 27.07.2021
doi: 10.28948/ngmuh.891261

veya şekiller gibi) görselini birebir kopyalamakta mağdurun kurumsal web sitede işlem yaptığına hiçbir şüphe bırakmamaktadır. Oltalama web siteleri hazırlanırken hedef kişileri aldatmak için alan adı benzetmesi kullanılarak basitçe karıştırabilecek harfler ("k" yerine "h" veya "a" yerine "o" harfleri gibi) yer değiştirilerek kullanılabilmektedir.

Geçmişten günümüze yapılan araştırmalarda, oltalama suçu ile mücadele için yeni yöntemler geliştirilmekle birlikte oltalama saldırıları da tüm dünyada büyük bir hızla artmaktadır. Anti-oltalama saldırıları çalışma grubu (APWG) yayınladıkları rapora göre, 2020'nin üçüncü çeyreğinde tespit edilen oltalama saldırıları için hazırlanmış web sitelerinin sayısı 571.764 ve kişiler veya şirketleri hedef alan oltalama saldırıları için hazırlanmış e-posta sayısının 367.287 olduğunu yayınlamışlardır [8].

Varshney ve arkadaşları yapmış oldukları çalışmada, oltalama saldırısı için tasarlanmış web sitelerinin tespiti için Google arama motoruna girilen kelimeleri inceleyerek tespit edilen URL (Uniform Resource Loader)'den gelen dizeler ve belirtilen bir web sayfası başlıklarını incelemişlerdir [9]. Çalışma sonucunda erişim sağlanan web sayfalarının % 99.5 oranında pozitif (doğru web sayfası) olduğunu görülmüştür. Smadi ve arkadaşları, bir evrişimsel sinir ağları (CNN) modeli kullanarak oltalama saldırıları için hazırlanmış (12.266 e-postadan oluşan bir veri seti) e-postaların tespitini incelemişlerdir [10]. Önerilen model ilk gün açıkları (zeroday) ile başa çıkabileceğini ve oltalama saldırıları için tasarlanmış e-posta içeriklerini % 98.63 oranında doğruluk elde etmişlerdir. Web sitesi tabanlı oltalama saldırılarının tespit ve saldırı engellemesine yönelik çalışmalar önemli olmakla birlikte saldırı sonrası yapılacak adli analizler suçluların tespitinde önemli bir yer tutmaktadır. Ayrıca, web sitesi tabanlı oltalama saldırılarının adli analiz sonuçlarından saldırı stratejileri, kullanılan tekniklerin belirlenmesi ve saldırganın izinin sürülebilmesi gibi önemli bilgilere ulaşılabilmektedir.

Tüm bunları göz önünde bulundurarak, bu çalışmada, oltalama saldırıları için hazırlanmış web sitesinin adli analizlerinde katkıda bulunmak için bir yaklaşım sunuyoruz. Bu çalışma esas olarak üç katkıyı sunmaktadır:

(1) Çalışma, web sitesi tabanlı oltalama saldırılarında gözlemlenen son kullanıcı davranışını,
(2) Bankacılık bilgilerini el geçirmek için tasarlanmış gerçek bir web sitesi tabanlı oltalama saldırısının adli analizi,
(3) Çalışmada seçilen örnek web sitesi tabanlı oltalama saldırı vakası analizinden elde edilen sonuçları değerlendirildi.

Bu çalışma aşağıdaki gibi düzenlenmiştir: bölüm 2'de, ilgili çalışmalardan birkaçı gözden geçirilmiştir. Bölüm 3'te, web sitesi tabanlı oltalama saldırı vakası adli analizlerini gerçekleştirilmiştir. Sonraki bölümde 4'te çalışmada kullanılan yaklaşımı değerlendirilmiştir. Son olarak, bölüm 5'te çalışma tamamlanmış ve gelecekteki olası web sitesi tabanlı oltalama saldırıyla mücadele için değerlendirmeler yapılmıştır.

2 Literatür çalışması

Literatürde web sitesi tabanlı oltalama saldırı tespiti ve analiz alanında çalışmalar olmakla beraber bu bölümde, önemli olan bazılarına odaklanarak kısaca gözden geçirilmiştir.

Web sitesi tabanlı oltalama saldırıları ile mücadelede sezgisel yaklaşımla kullanılarak şüpheli web sitelerin tespiti etkili bir yöntemdir. Bu yöntem, şüpheli web sitelerinin URL (Uniform Resource Loader) ve HTML (Hypertext Markup Language) içeriklerini makine öğrenmesi veya derin öğrenme gibi yöntemlerle inceleyerek sahte olanları tespit edip engellemek mantığına dayanmaktadır [11]. Ludl ve arkadaşları yapmış oldukları çalışmada sezgisel tabanlı bir yaklaşım kullanarak web sitesi tabanlı oltalama siteleri tespit etmek ve sınıflamak için özellikle HTML ve URL hedef alan bir yöntem önermişlerdir [12]. Bu çalışmada, veri seti olarak 18 farklı oltalama web sitesi kullanılmış ve çalışma sonucunda HTML içeriklerinde % 16.9 ve URL içeriklerinde ise % 0.4 oranında yanlış algılama olduğu görülmüştür.

Diğer bir çalışmada Pan ve arkadaşları, web sitesi tabanlı oltalama tespiti için öncelikle web sitelerin gerçek kimliklerini analiz etmeyi önermişlerdir [13]. Web sitesinde bulunan başlık, açıklama, telif hakkı vb. gibi özelliklerin oltalama web sitelerinde değişebileceğini varsayımını kullanmışlardır. Çalışma sonucunda % 29 oranında önerilen yöntemin başarısız olduğu görülmüştür.

Benzer olarak diğer bir çalışmada Cantina web sitelerinde bulunan sözcüklerin tespiti ve analizi için sezgisel bir yöntem kullanılarak yanlış yazılmış veya ad benzetmesi kullanılmış web sitelerini tespit etmeyi amaçlamıştır [14]. Analizler sonucunda % 89 doğruluk oranında sonuçlar elde etmiştir. Metin tabanlı değişiklikler yapmak oltalama saldırısı için tasarlanmış web sitelerinde en sık kullanılan yöntem olduğunu ve bu yöntemle hazırlanmış siteler tespit edilebilmesi ve içeriğin engellemesi bu suçla mücadelede önemli katkı sağlayacağını vurgulamıştır.

Diğer bir çalışmada Yi ve arkadaşları kullanıcı adı, kimlik bilgileri ve kredi kartı bilgileri çalmak için tasarlanmış oltalama amaçlı web sitelilerin tespiti için bir yöntem önermişlerdir [15]. Çalışmada derin öğrenme yöntemi kullanarak şüpheli web sitelerinin IP numaraları ve URL adresini tespit ederek bu web sitelerini engellemek mantığına amaçlanmıştır. Çalışmada, veri seti olarak ISS (İnternet servis sağlayıcısı) 24 saat süre içerisinde gerçek veriler kullanılmıştır. Çalışma sonucunda önerilen yöntemin oltalama amaçlı web sitelerinin % 90 başarı oranına sahip olduğu görülmüştür.

Benzer bir çalışmada Moghimi ve arkadaşları özellikle bankacılık bilgilerini çalmak için tasarlanmış oltalama amaçlı web sitelerin tespiti için bir yöntem önermişlerdir [16]. Bu yöntem şüpheli web sitelerinin IP numaraları ve URL adreslerinin özelliklerini tespit ederek sınıflandırma işlemi uygulanmıştır. Çalışmada veri seti olarak şüpheli 3066 web sitesi incelenmiş olup önerilen yöntem % 99.14 oranında başarılı olduğu görülmüştür.

Diğer bir çalışmada Al Mutawa ve arkadaşları akıllı cep telefonlarında oltalama amaçlı web sitelerin (Facebook, Twitter, MySpace gibi) adli inceleme araçları kullanarak (Forensic Tools Kit, Wireshark vb.) adli analizleri

yapılmıştır [17]. Önerilen yöntemin benzer adli vakalar için uygulanabilir olmakla beraber çalışmada kullanılan örneklerin dışında farklı model ve marka akıllı cep telefonları ile analizlerin genişletilmesi gerekliliği vurgulamışlardır.

3 Gereç ve yöntemler

Bu bölümde, web sitesi tabanlı oltalama saldırıları için hazırlanmış vaka örneğini ve analizlerde kullanılan iş bilgisayarı ve analiz araçlarını tanıtılmıştır.

3.1 Veri seti

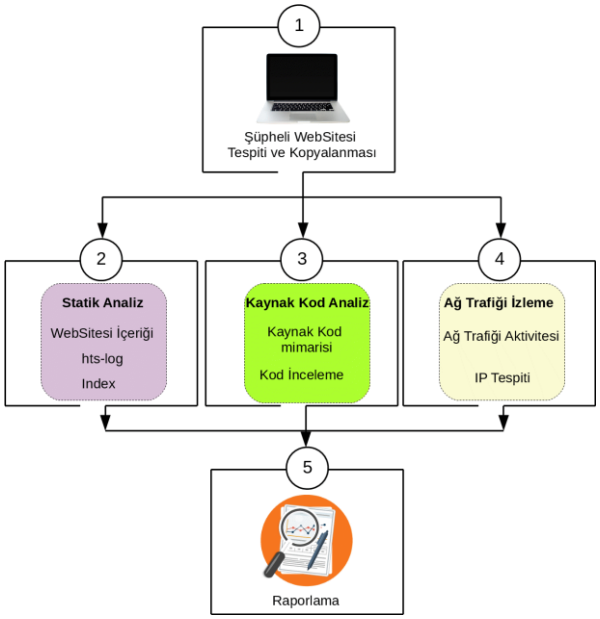
Vaka analiz çalışmalarında, seçilen örneğin konunu tam olarak içermesi ve mümkünse günlük hayatta karşımıza çıkan gerçek bir örnek olması son derece önemlidir. Böyle uygun bir vaka örneğine için Türkiye'de faaliyet gösteren bir bilgi güvenliği şirketi ile işbirliği yapılmıştır.

3.2 Analiz yöntemi

Bu bölümde, tüm analiz yaklaşımının iş akışı ve sistemi ayrıntılı olarak açıklanmıştır. Genel çalışma beş aşamadan oluşmaktadır (Şekil 1).

3.2.1 Şüpheli web sitesinin tespiti ve kopyalanması

Web tabanlı oltalama saldırıların adli incelemelerinin ilk adımı şüpheli web sitesinin tespitidir. Tespit edilen şüpheli web sitesi adli incelemesi yapılabilmesi için uygun programlar kullanılarak iş bilgisayarına kopyalanır. Bu adım tamamlandıktan sonra analiz aşamasına geçilir.



Şekil 1. Analiz yaklaşımın genel iş akışı.

3.2.2 Statik analiz

Statik analiz yaklaşımı, şüpheli içerikler çalıştırılmadan yapılan analizleri kapsamaktadır. Şüpheli web sitesinin içerikleri hakkında hızlı bir şekilde bilgi toplanmasına imkan sağlamaktadır. Statik analiz yöntemiyle şüpheli web sitesinin içeriği, hts-log bilgileri ve index bilgileri gibi bilgilere ulaşılabilmektedir. Bununla birlikte web sitesini oluşturan dosyaların amacını tam olarak belirlemek için static anaiz yaklaşımı yeterli değildir. Statik analiz aşamada elde edilen bilgiler diğer adımlarda yapılacak analizler için rehber niteliğindedir.

3.2.3 Kaynak kod analizi

Kaynak kod analizi, şüpheli web sitesini oluşturan kaynak kodun çalıştırtılmadan basit olarak yapılan analizleri içermektedir. Kaynak kod analizi sayesinde şüpheli web sitesinin kaynak kod mimarisi analizi ve web sitesinin kod yapısı incelenerek, mevcut yapısı ve olası hataların tespitinin yapılması amaçlanmaktadır.

3.2.4 Ağ trafiği izleme

Ağ trafiği izleme yöntemi adli bilişim incelemelerinde sıklıkla kullanılmaktadır. Ağ izleme süreci boyunca şüpheli web sitesinin gerçek zamanlı ağ trafiği verileri toplanabilmektedir. Bu veriler analiz edilerek anormallikleri tespit edebilme imkânı sağlamaktadır. Ağ trafiği analizleri sonucunda şüpheli web sitesi ile saldırgana arasında iletişim bilgilerini içerebilmesinden dolayı son derece önemlidir. Ağ trafiği verilerinden saldırgana ait IP (İnternet Protokolü) numarası tespit edilebilirse saldırganın izinin sürülebilmesine imkân sağlamaktadır. IP numarası sayesinde bağlı olan abone ve lokasyon (Whois) bilgilerine ulaşmak mümkün hale gelmektedir.

3.2.5 Raporlama

Raporlama aşaması şüpheli web sitesi adli analizi sonucunda ulaşılan bulguların rapor olarak hazırlanması aşamasını ifade etmektedir. Analiz rapor içeriğinde, analiz zamanı, analiz sonucunda şüpheli web sitesi hakkında ele geçen bulgulara ilişkin bilgiler detaylı olarak yer almaktadır.

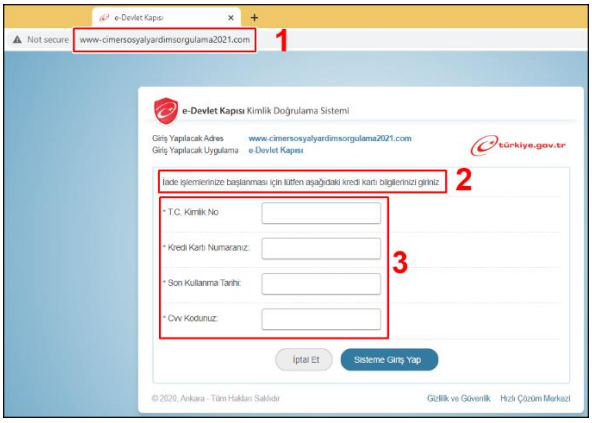
3.3 Örnek vaka analizi

Seçilen örnekte saldırgan, web sitesi tabanlı oltalama saldırısı için son zamanlarda tüm dünya genelinde görülen korona virüs salgını konusunu kullanmıştır. Tüm dünyayı etkisi altına alan Koronavirüs salgını derin ekonomik etkileri olduğu ülkemizde de görülmektedir. Söz konusu salgının ekonomik etkileri ve yol açtığı maddi kayıplar nedeniyle resmi kurumlar tarafından sosyal yardımlar yapılmaktadır. Saldırgan bu hizmeti taklit etmek için bir senaryo tasarlanmış ve Türkiye vatandaşlarına devlet tarafından verilen hizmetlerin elektronik ortamda sunulması kurumsal web sitesi (e-devlet) oltalama saldırısı yapmak için taklit edilmiştir (Şekil 2).

Şekil 2'de oltalama saldırıları için hazırlanmış şüpheli web sitesi içeriği görülmektedir. Web sitesi tabanlı oltalama saldırı içeriği incelendiğinde e-devlet logosunun kullanılarak mağdurda kurumsal e-devlet web sitesinde işlem yaptığını izlemini oluşturmak amaçlanmıştır.

Şekil 2'de (1) kısımda, saldırgan tarafından hazırlanan web sitesi alan adı görülmektedir. Alan adı hazırlanırken "https://www-cimersosyalyardimsorgulama2021.com" içerisinde CİMER (Cumhurbaşkanlığı İletişim Merkezi) kelimesi özellikle vurgulandığı görülmüştür. Şekil 2'de (2) kısımda, Mağdurun kişisel ve bankacılık bilgilerini hazırlanmış forma girmesi için yönlendirme mesajını göstermektedir. Şekil 2'de (3) kısımda, mağdurdan siteme

girmesi istenen bilgileri neler olduğunu ve ilgili alanlar görülmektedir.



Şekil 2. Oltalama saldırıları için hazırlanmış web sitesinin ekran görüntüsü.

HTTrack Website Copier, web sitesini bütünüyle bilgisayara indirmeyi sağlayan ve indirilen web sitenin çevirim dışı olarak kullanılmasını sağlayan bir web site kopyalama aracıdır (Chowdhury, vd. 2013). Şüpheli web site içeriğinin incelemesi için HTTrack Website Copier 3.49-2 programı kullanılmıştır. HTTrack Website Copier programı kullanılarak şüpheli web sitesi "https://www-cimersosyalyardimsorgulama2021.com" inceleme bilgisayarına bütünüyle indirilerek inceleme aşamasına geçilmiştir. (Şekil 3).

Şekil3."https://www.cimersosyalyardimsorgulama2021.com" web sitesi içeriği ekran görüntüsü.

Şekil3'de"https://www.cimersosyalyardimsorgulama2021.com" web sitesinin içeriği görülmektedir.

Şekil 3'de (1) kısım web sitesi içeriğinde kullanılan dosya ve dizinler görülmektedir. "cdn.e-devlet.gov.tr klasörü içeriğinde web sitesinde kullanılan e-devlet logo ve ifadeleri bu klasör içerisinde bulunduğu tespit edilmiştir. hts-cache (historical traffic search-cache) klasörü ise web sitesinin HTML sayfalarını, içerisindeki görselleri ve dokümanları bulundurmaktadır. Şekil 3'de (2) kısımda "hts-log" dosyası ise mağdurların forma giriş yaptığı bilgilerin tutulduğu kayıtları göstermektedir. Şekil 3'de (3) kısımda ise "index" klasörü ise HTTrack Website Copier programıyla kullanılarak indirilen şüpheli web sitesinin içeriğine çevrimdışı ulaşılmasını sağlamaktadır.

"https://www-cimersosyalyardimsorgulama2021.com" web sitesinin içeriği ve kaynak kod mimarisini incelemek ve web sitesi hakkında daha fazla bilgiye ulaşmak için kaynak kod içeriği analiz edilmiştir (Şekil 4).

Şekil 4'de şüpheli web sitesinin içeriği ve kaynak kod mimarisini inceldiğinde (1) kısımda "WordPress" kullanarak web sitesinin oluşturulduğu görülmüştür. Şekil 4'de (2) kısımda web sitensin ana sayfa adresi erişim linkin göstermektedir. Şekil 4'de (3) kısımda web sitesinin kayıtlarının tutulduğu klasörü olan "hts-log" olduğu tespit edilmiştir.

Şekil4."https://www.cimersosyalyardimsorgulama2021.com" web sitesinin kaynak kod mimarisinin ekran görüntüsü.

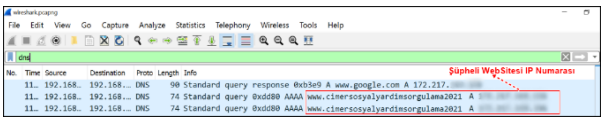
Web sitelerin log kayıtları çok değerli bilgiler içerdiğinden adli analizlerde önemlidir. "https://www-cimersosyalyardimsorgulama2021.com" web sitesinin "hts-log" dosyası analizi yapılmıştır (Şekil 5).

Şekil 5."hts-log" dosyası içeriğinin ekran görüntüsü.

"hts-log" dosyası içeriği görüntülendiğinde mağdurlar tarafından"https://www.cimersosyalyardimsorgulama2021.com" web sitesinin girilen bilgilere ulaşılabileceği görülmüştür. Şüpheli web sitesinin ağ trafiği incelemeleri adli analizlerde gerek failin gerekse lokasyonun belirlenmesi için IP adres bilgisine ihtiyaç bulunduğu kuşkusuzdur [18]. Ağ trafiği adli incelmelerde uluslararası standartlar geçerliliği olan analiz araçlarından birisi "Wireshark" programıdır [19-25]. Bu nedenle şüpheli, web sitesinin IP numarasının tespiti için "Wireshark" programı tercih edilmiştir. İnceleme bilgisayarında Wireshark programı çalıştırıldıktan sonra şüpheli "https://www-cimersosyalyardimsorgulama2021.com" web sitesine Goo gle arama motoru kullanılarak giriş yapılmıştır. Wireshark programı çalıştığı bilgisayarda tüm internet ve ağ paket trafiğini görüntüleyeceğinden sadece şüpheli "https://www-cimersosyalyardimsorgulama2021.com" web sitesine ait internet ve ağ paket trafiği bilgileri filtrelenmiştir. (Şekil 6.)

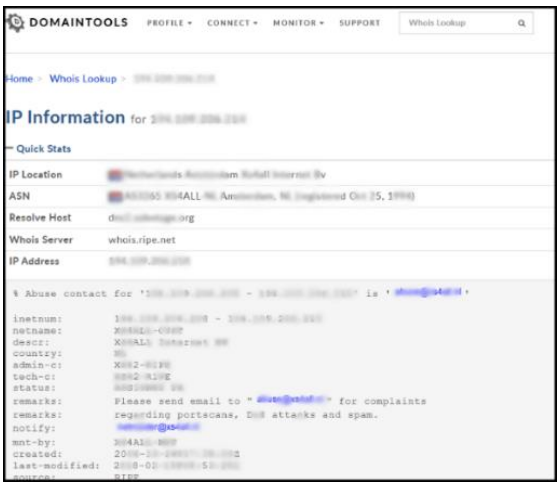
Analizler sonucunda şüpheli web sitesine ait IP numarası tespit edilmiştir. Ancak şüpheli IP numarasının tespiti yoluyla saldırganın izinin sürebilme süreci bazı zorluklar

ihtiva etmektedir. Tespit edilen IP numarasının gerçek faile ait olup olmadığı teyit edilmelidir [18]. 5271 sayılı Ceza Muhakemesi Kanununda 134. Maddesi gereğince tedbirler (şüpheli cihazlarda içerik araması yapılması, adreste arama, el koyma ve delil elde etme yöntemleri) uygulanarak desteklenmelidir. IP (statik veya dinamik) adreslerinin de çeşitli yöntemlerle (VPN, ZenMate vb.) kullanarak gerçek numarası gizlenebilmektedir [26]. Bu durumun önüne geçebilmek için Türk Ceza Kanununda ve Ceza Muhakemesi Kanununda düzenlemelere gidilmiştir [18]. Ayrıca tespit edilen şüpheli IP numarasının çeşitli programlar (VPN, ZenMate vb.) kullanarak gizlenmesi tespit edilmesi ve söz konusu IP numarasıyla suç işlendiği yönünde kuvvetli şüphe olması halinde ilgili şirketlerden gerçek IP numarasının talep edilebilmektedir [27].



Şekil 6. Wireshark programı ile "https://www-cimersosyalyardimsorgulama2021.com" sitesi IP numara tespitinin ekran görüntüsü.

Şüpheli IP numarasının tespit edilmesinden sonra IP numarasının ait bilgiler ulaşmak amacıyla "https://whois.dom aintools.com" adresinden alan adı sorgulaması yapılmıştır (Şekil 7).



Şekil 7. Şüpheli IP numarasının "https://whois domaintools.com" sorgusunun ekran görüntüsü.

Tespit edilen şüpheli IP numarasının sorgusu sonucunda saldırgana ait Whois (alan adı sorgulaması) bilgilere ulaşılabileceği görülmüştür.

4 Tartışmalar

Bu çalışmada web tabanlı oltalama saldırıları ele alınarak gerçek bir vaka analizi yapılarak mevcut durumda yaşanan zorluklar değerlendirilmiştir. Seçilen güncel ve gerçek bir saldırı örneği üzerinde saldırganın saldırı stratejisi ve kullandığı yöntemler incelenmiştir. Analiz sonuçları (1) seçilen örnek web tabanlı oltalama saldırısının çalışma mantığını, (2) saldırgana ait bilgilerinin izinin sürülmesi gibi iki önemli avantaj sunmaktadır. Öte yandan web tabanlı oltalama saldırılarının adli vaka analizleri bazı zorluklarda içermektedir. Saldırganlar her saldırıda farklı tasarımlar kullanabileceğinden tespit ve analiz yaklaşımları incelenen vakaya göre farklılıklar içerebilmektedir. Ayrıca bazı durumlarda tespit edilen şüpheli IP numaraları çeşitli yöntemlerle gizlenebilmektedir. Bu durumlarda tespit edilen IP numaralarının yürütülen soruşturma kapsamında kanuni düzenlemelerden faydalanılması mümkündür.

Web tabanlı oltalama saldırılarıyla mücadelede gerçek vaka analizleri büyük katkı sağlamakla birlikte ilgili alanda çalışan uzmanlarda farkındalık oluşturması açısından önemlidir.

Bu çalışmada önerilen yaklaşımın güçlendirilmesi ve desteklemek için daha fazla güncel örneklerle tekrarlanması gerektirdiğine inanıyoruz.

5 Sonuçlar

Bu çalışma, web tabanlı oltalama saldırılarının adli analizlerinde kullanılabilecek bir yaklaşım sunmaktadır. Dahası, analiz sonuçlarından web tabanlı oltalama saldırı sitesinin içerik analizini, saldırı stratejisinin belirlenmesi ve saldırgana ait bilgilere ulaşılabileceğini göstermiştir. Çalışmada kullanılan yaklaşım özellikle web sitesi tabanlı oltalama saldırıları analizlerinde kullanılabilecek uygun bir yöntem olabileceği görülmüştür.

Son olarak, çalışma web sitesi tabanlı oltalama saldırıları ile mücadelede farkındalık yaratacağına inanıyoruz. Gelecek çalışma olarak web sitesi tabanlı oltalama saldırıları tespiti ve analizlerinde farklı örnek veri setleriyle araştırmayı planlıyoruz.

Çıkar çatışması

Yazarlar çıkar çatışması olmadığını beyan etmektedir.

Benzerlik oranı (iThenticate): %17

Kaynaklar

[1] J. Lopez, J. E. Rubio, Access control for cyber-physical systems interconnected to the cloud, Computer Networks, 134, 46-54, 2018. doi: 10.1016/j.conmet 2018. 01.037.

[2] O. K, Sahingoz, E. Buber, O. Demir, B. Diri, Machine learning based phishing detection from urls, Expert Systems with Applications, 117 (1), 345-357, 2019. doi :10.10 16/ j.eswa.2018.09.029.

[3] C. N. Gutierrez, T. Kim, Della R. Corte, J. Avery, D. Goldwasser, M. Cinque, S. Bagchi, Learning from the ones that got away: Detecting new forms of phishing attacks. IEEE Transactions on Dependable and Secure Computing, 15 (6), 988-1001, 2018. doi: 10.1109.TDSC. 2018.2864993.

[4] B. Kesler, H. Drinan, N. Fontaine, News briefs. IEEE Security and Privacy, 4 (6), 8-13, 2006. doi: 10.28948/ngumuh.649969.

[5] I. Kara, Truva atı zararlı yazılımlarına yaklaşım ve çözüm önerileri. Bilgi Yönetimi, 2 (1), 28-33, 2019.

[6] I. Kara, Türkiye'de zararlı yazılımlarla mücadelenin uygulama ve hukuki boyutunun değerlendirilmesi.

Akademik Bakış Uluslararası Hakemli Sosyal Bilimler Dergisi, 52, 87-98, 2015.
[7] V. Bhavsar, A. Kadlak, S. Sharma, Study on phishing attacks. Int. J. Comput. Appl, 182, 27-29, 2018. doi:10.5120/ijca2018918286.
[8] APWG, Phishing Activity Trends Report: 3rd Quarter 2020. Anti-Phishing Working Group, Retrieved. Available online: https://apwg.org/trendsreports/ (Accessed on 06 Nisan 2021).
[9] G. Varshney M. Misra, P. K. Atrey. A phish detector using lightweight search features, Computers & Security, 62, 213-228, 2016. doi:10.1016/j.cose. 2016.08.003.
[10] S. Smadi, N. Aslam, L. Zhang, Detection of online phishing email using dynamic evolving neural network based on reinforcement learning. Decision Support Systems, 107, 88-102, 2018. doi:10.1016/j.dss.2018.01.001.
[11] M. R. Natadimadja, M. Abdurohman, H. H. Nuha, A Survey on Phishing Website Detection Using Hadoop. Jurnal Informatika Universitas Pamulang, 5 (3), 237-246, 2020. doi:10.32493/informatika.v5i3.6672.
[12] C. Ludl, S. Mcallister, E. Kirda, C. Kruegel. On the effectiveness of techniques to detect phishing sites. In DIMVA '07: Proceedings of the 4th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, Berlin, Heidelberg, 4579, 20-39, 2007. doi:10.1007/978-3-540-73614-1_2.
[13] Y. Pan, X. Ding, Anomaly based web phishing page detection. In ACSAC '06: Proceedings of the 22nd Annual Computer Security Applications Conference, IEEE Computer Society. 1, 381-392, 2006. doi:10.1019/ACSAC.2006.13.
[14] Y. Zhang, J. I. Hong, Cranor. Cantina: a content-based approach to detecting phishing web sites. In www '07: Proceedings of the 16th International Conference on World Wide Web, 8 (12), 639-648, 2007. doi:10.1145/1242572.1242659.
[15] P. Yi, Y. Guan, F. Zou, Y. Yao, W. Wang, T. Zhu, Web phishing detection using a deep learning framework. Wireless Communications and Mobile Computing, 9, 1-9, 2018. doi:10.1155/2018/4678746.
[16] M. Moghimi, A. Y. Varjani, New rule-based phishing detection method. Expert Systems with Applications, 53, 231-242, 2016. doi:10.1016/j.eswa.2016.01.028.
[17] A. Mutawa, N. Baggili, I. A. Marrington, Forensic analysis of social networking applications on mobile devices. Digital Investigation, 9, 24-33, 2012. doi:10.1016/j.diin.2012.05.007.
[18] D. Gedik, Bilişim suçlarında ıp tespiti ile ekran görüntüleri çıktılarının ispat değeri. Bilişim Hukuku Dergisi, 1 (1), 51-84.
[19] [wireshark] http://wireshark.org (Accessed on 06 Nisan 2021)
[20] S. Sandhya, S. Purkayastha, E. Joshua, A. Deep, assessment of website security by penetration testing using Wireshark. In 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE. 4, 1-4, 2017. doi:10.1109/CICN.2017.8319360.
[21] H. Kim, H. Lee, H. Lim, Performance of packet analysis between observer and wireshark. In 2020 22nd International Conference on Advanced Communication Technology (ICACT), IEEE. 2020, 268-271, 2020. doi:10.23919/ICACT48636.2020.9061452.
[22] J. C. Vega, M. A. Merlini, P. Chow, FFShark: a 100G FPGA implementation of BPF filtering for Wireshark. In 2020 IEEE 28th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM), IEEE. 47-55, 2020. doi:10.1109/FCCM 48280.2020.00016.
[23] K. M. Fathima, N. Santhiyakumari, A survey on network packet ınspection and arp poisoning using wireshark and ettercap. In 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), IEEE. 1136-1141, 2021. doi:10.1109/ICAIS50930.2021.9395852.
[24] https://www.iso.org/standard/44406.htm (Accessed on 06 Nisan 2021)
[25] https://www.iso.org/standard/44407.html (Accessed on 06 Nisan 2021)
[26] N. M. Al-Fannah, One leak will sink a ship: WebRTC IP address leaks. In 2017 International Carnahan Conference on Security Technology (ICCST), IEEE. 1-5, 2017. doi: 10.1109/CCST.2017.8167801.
[27] Ö. Murat, Avrupa konseyi siber suç sözleşmesi ışığında siber suçlarla mücadelede uluslararası işbirliği. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 19(2), 1229-1270, 2013.