Bahtiyar M. PALTACI **Cyber Security Analyst**

DergiPark AKADEMİK

Orta Doğu ve Orta Asya Kafkaslar Araştırma ve Uygulama Merkezi Dergisi (ODAK)

SİBER DOLANDIRICILIK VAKALARI, TEKNİK-TEORİK SENARYOLAR VE ACI SONUÇLAR: PHISHING, HOAX SALDIRILARINA GENEL BAKIŞ VE ALINABİLECEK ÖNLEMLER

ÖZET

Günümüzde sosyal medya aracılığıyla veya diğer sanal iletişim araçları vasıtasıyla pek çok dolandırıcılık vakasına şahit olmaktayız. Kullanıcıların net ortamında sık kullandığı uygulamalar veya işlemler detaylandırılarak phishing (oltalama saldırısı) dediğimiz yöntemle manipüle edilmekte. Kullanıcıların sık ziyaret ettiği sistemler veya uygulamaların birebir kopyası yapılıp çeşitli hoax (aldatıcı, asparagas mesaj) yöntemleriyle kullanıcılara gerçek veriymiş gibi gösteriliyor. Peki bu Hoax verilerinden veya yapılan phishing sistemlerden korunmak için ne kadar etkili çalışmalar var veya neler yapıyoruz ? Ve bu yöntemlerin boyutu ne kadar derine iniyor ? Bu makalede bu sorulara cevap arayarak sanal dolandırıcılık yöntemlerini teorik olarak inceleyip arada teknik detaylar ile son kullanıcının anlayabileceği şekilde aktarmaya gayret gösterilmiştir.

ABSTRACT

Today, we witness many fraud cases through social media or other virtual communication tools. Frequently used applications or transactions by users in the online environment are manipulated through a method known as phishing. Systems or applications frequently visited by users are replicated exactly, then presented to users as real data through various hoax methods. So, what effective efforts exist to protect us from these Hoax data or phishing systems? How deep do these methods go? This article aims to answer these questions by theoretically examining virtual fraud methods and attempts to communicate this information in a way that the end user can understand, with some technical details interspersed.

Anahtar Kelimeler : Sanal İletişim Araçları, Oltalama Saldırıları, Siber Dolandırıcılık, Sahte Haber, Manipülasyon ve İnandırma, Siber Dolandırıcılık Korunma ve Savunma Yöntemleri, Teknik Teorik Siber/Sanal Dolandırıcılık Senaryo ve Vakaları,

Keys : Virtual Communication Tools, Phishing Attacks, Cyber Fraud, Fake News, Manipulation and Persuasion, Cyber Fraud Protection and Defense Methods, Technical Theoretical Cyber/Virtual Fraud Scenarios and Cases

[ORCİD : 0000-0002-8626-6146] **[DergiPark : @bbmnr]** **[E-Posta: bmnrpltci@gmail.com]**

GİRİŞ : Hoax Nedir ?

İçerisinde aldatıcı bilgiler ile dikkat çekecek biçimde hazırlanmış mesajlar bütünüdür.[1] Genellikle mail yoluyla hedefe gönderilir ve hedef manipüle edilmeye çalışılır. Mail yolu dışında; artık sosyal medyanın da hayatımızın bir parçası olmasıyla birlikte bir çok adreste (Facebook, Twitter, Instagram, Blogspot, Tumblr v.b) bu tür hoax verilerine en inandırıcı biçimde rastlayabilirsiniz.

Mail üzerinden, Facebook üzerinden, Twitter üzerinden, Whatsapp üzerinden, Instagram üzerinden ve bütün bunların alternatifi olabilecek (Telegram, Vk, Signal, Snapchat) uygulamalar üzerinden bile Hoax artık günümüzde çok rahat bir biçimde uygulanmaktadır.

Çeşitli yollarla, ilgili uygulamalarla da bütünleşik biçimde istenilen hedefe yönelik %99 başarılı sonuçlar alınabilecek Hoax türleri vardır.[2] Tabiki bunlar Sosyal Mühendislik ve biraz da teknik siber güvenlik bilgileri gerektirmektedir. Günümüzde siyah şapkalı hackerlar dediğimiz kötü niyetli bireyler ve dolandırıcılar hedeflerini analiz ederek kişisel veya topluca yöntemler belirleyip, manipüle edici verileri hazırlayarak bunları uygun sosyal mühendislik yöntemleriyle birleştirip doğrudan hedefi veya hedefleri profesyonel bir biçimde ele geçirmekte.

Peki Nasıl ? Örnek bir Hoax/Phishing Senaryosu

* Senaryo uygulamada Hoax, Sosyal Mühendislik, Phishing ve Web Security/Design ağırlıklı gidilmiştir.

Ziraat Bankası üzerinden bir senaryo gerçekleştirelim. Biliyorsunuz Ziraat Bankası Kurumsal

URL : https://www.ziraatbank.com.tr

Online Bankacılık işlemleri baz alınsın. Onunda URL adresi aşağıdadır.

https://bireysel.ziraatbank.com.tr/Transactions/Login/FirstLogin.aspx?customertype=rtl

Buraya kadar her şey normal. Girdiğimiz adresler belli, hangi işlemleri yapacağımız belli. Giriş yaptıktan sonra ödeme kanalları, hesap bilgileri gibi arayüzleri biliyoruz.

Hedef orta yaşlarda, devlette çalışan bir personel veya personeller olsun.

Şimdi hedefe yönelik araştırmalar yapalım. Twitter veya Facebook aracılığıyla online satış sayfaları, e-ticaret sayfaları, gruplar, twitter aktiviteleri detaylıca araştırıldıktan sonra kullanıcıya/kullanıcılara yönelik bilgiler harmanlanır. Bu bilgilere yönelik Ziraat Hesabı olan kişi veya kişiler bulunur. Bu kişilerin mailleri toplanır.

Mail toplamanın farklı yönleri elbette var. Bir çok mail datası nette kolaylıkla bulunabilir. Yine her hangi bir devlet kurumuna yönelik yapılan saldırılarda çeşitli “data” bilgiler ele

geçirilebilir. İçeriden veya dışarıdan yapılacak bu tür saldırıların neticelendirilmesi sonucunda kötü niyetli kişiler kolaylıkla bu dataları pazarlayabilir veya direkt provake amaçlı paylaşabilir.

Asıl konumuza devam edelim.

Bkz : Bazı devlet kurumlarından alınan maaşların Ziraat Bankasından verilmesi örneği.

Bankaların hangi devlet kurumları ile anlaşmalı olduğundan yola çıkarak hangi kurumun hangi bankadan maaş verdiği de çok kolay bir şekilde tespit edilebilmekte.

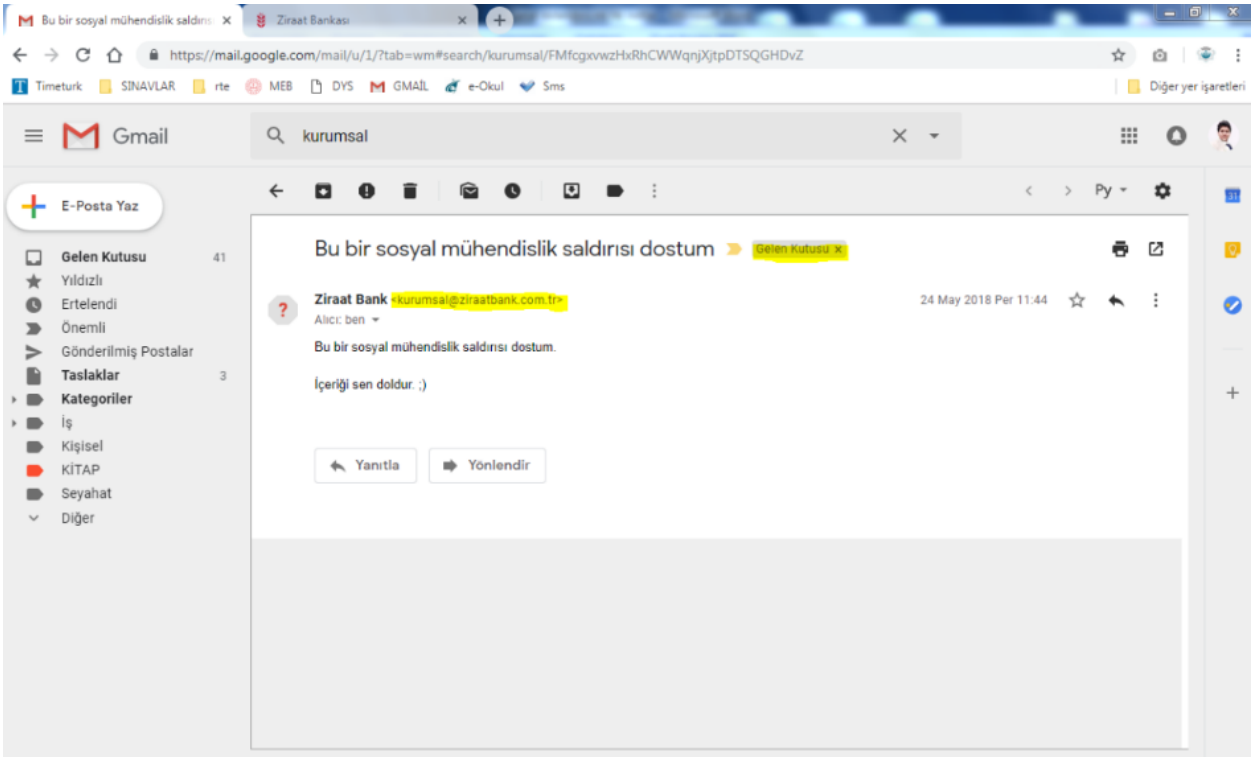
Bkz : Alınan bilgiler doğrultusunda hedefin çalıştığı kurum tespit edilir ve saldırı senaryosu üzerinden fikirler geliştirilir.

Bkz : Geliştirilen fikirler artık yavaş yavaş uygulamaya alınır. Bunlar için gerekli birkaç teknik yöntemler oluşturulur.

Bu yöntemler nelerdir hemen inceleyelim.

 # Kurumsal Mail

Hedefe doğrudan etkili bir mesajla, “hedefe gönderilecek veriye” en yakın şekilde ya da direk aynı isimde bir mail üzerinden ilk iletişime geçilir.



Not : Görüntü tarafımdan 2018 yılında uygulamalı eğitim üzerinden gerçekeştirilen senaryoda kayda geçmiştir.

Yukarıda ki örnekte sosyal mühendislik saldırısı için kurumsal@ziraatbank.com.tr adresinden direk gelen kutusuna düşecek biçimde mail gönderildiğini görüyorsunuz. Günümüzün hacking yöntemlerinde sıklıkla kullanılan bir yöntem. İstediğiniz adresten direk gelen kutusuna istediğiniz mesajı gönderebiliyorsunuz.

Bilinçli bir kullanıcının ilk yapacağı mail adresini kontrol etmektir. Peki yeterli mi ? Tabiki hayır.

 # Mail İçeriği

Mail içeriği kullanıcıya yönelik bir kampanya, çekiliş v.b yöntemler ile manipüle için kullanılır. Örnek için, hemen Ziraat Bankası'nın e-bülten servisinden bir içerik bulalım.

http://ebulten.ziraatbank.com.tr/trimages/taksitlendirme_012019/taksitlendirme_012019.html

Yukarıda ki kampanya detayları, güzelce hazırlanır ve tıpkı Ziraat Bankasının resmi mail hesabından (yukarıda ki gördüğünüz adres) bire bir gelen kutusuna; ve mail içeriği tıpkı ziraat bankasının gönderdiği kampanyalar gibi...

Buraya kadar, normal bir son kullanıcı ziraat bankasından mail geldiğine emin olmuş olmalı ?

Normal bir mail aldığınızı düşünmeniz ilk etapta geçerli. Ama bu gördüğünüz gibi kesinlikle sizi yanıltıcı biçimde hazırlandı. Devam edelim...

 # Phishing Attack (İçerik-Tasarım)

Artık kötü niyetli şahısların oltasını atıp bekleyeceği sistemin son aşaması, Phshing sayfası ve bu sayfanın orjinaliyle bire bir aynı olacak şekilde kodlanıp; ilgili security adımlarını atlatması.

Bunu nasıl yapabilirler veya nasıl yapıyorlar ?

Şöyle ki bir web sayfasının bire bir kopyasının çıkartılması uzmanlarca dakikalar alabilecek bir konu. Web tasarım konusunda görsellik önemli bir konudur; web sitesinin kullanılabilir kılınmasında büyük rol oynar.[3] Bu hususta senaryoya göre uzmanın sahte web sayfasını logosundan içeriğine, içeriğinden Hoax da kullanılan detaylara kadar inandırıcı ve %100 aynı tasarım ile sizlerin önüne getirilebilmesi çok kolay bir iştir. Ve çeşitli doğrulama adımları da Sponsorlu bağlantı örnekleri veya kullanıcı dikkatsizliği nedeniyle es geçiliyor.

Burada ki püf noktası ve son kullanıcıların çoğunun dikkat etmediği nokta bu veriler hangi sunucuda, bu veriler hangi url adresi ile önünüze geliyor ? Çoğunlukla önceki aşamalarda hazırlanan Hoax'da ki verilerin inandırıcılığı ile; son aşamada önünüze gelen aldatıcı sayfanın güvenilirliğinde gözden kaçan detaylar sonucu bir çok mağduriyet malasef ki yaşanmakta.

Artık çoğu kullanıcının işlerini mobil sistemlerden yapması ve akıllı telefonların büyük bir çoğunlukta olması tüm bu anlatılanların gerçekleşmesinde de en büyük etkenlerden biri.

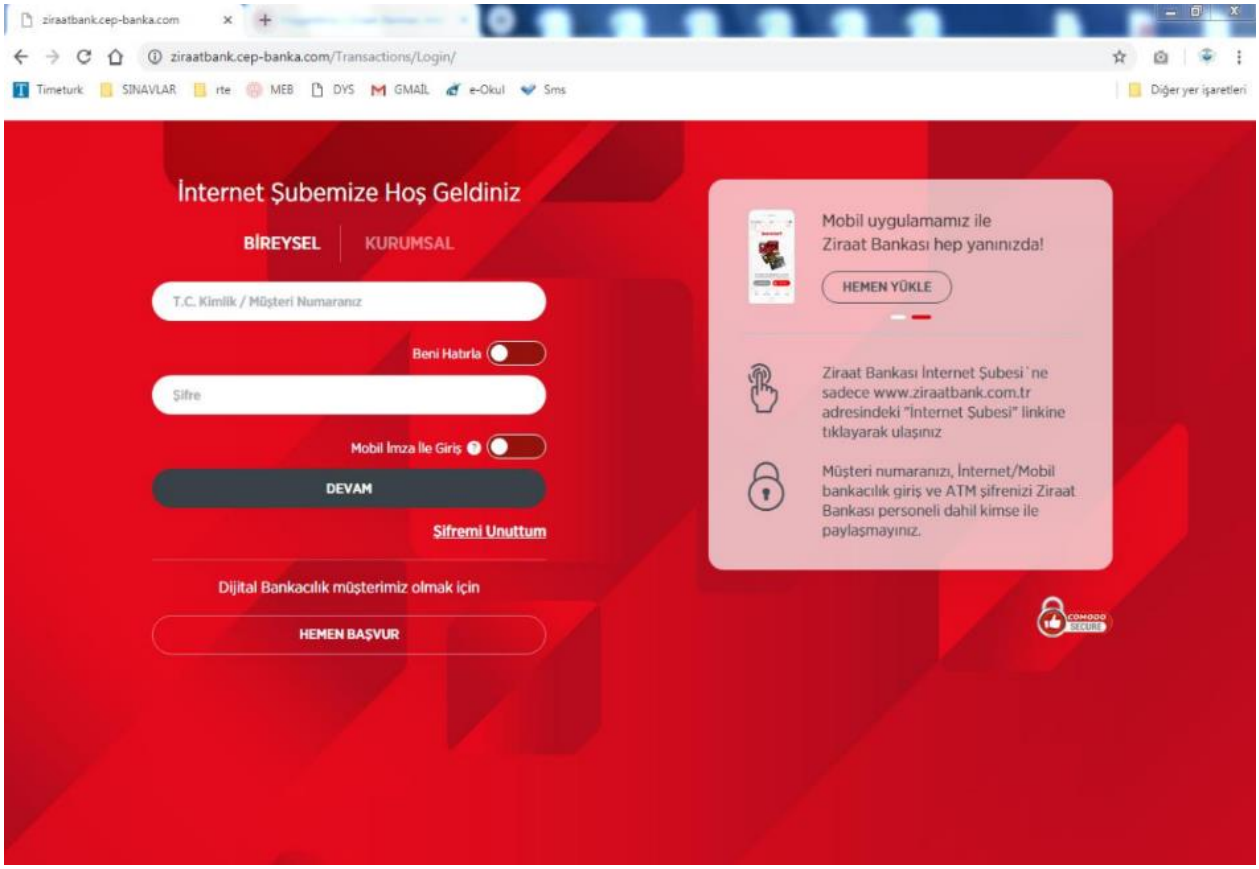
Akıllı Telefonlar üzerinden yapılan E-Ticaret alışverileri, bankacılık işlemleri ve aklınıza

gelebilecek bir çok şey ne yazık ki çok büyük bir bilinçsizlik içerisinde yapılmakta. Bunu bilen; zafiyetinizi açığa çıkarır ve kötü sonuçlar ve deneyimler yaşamanıza sebebiyet verir.

Şimdi ilk paragrafta değindiğimiz kopya sistemler üzerinden devam edelim. Mail içeriğimiz Kampanya detayları hakkındaydı. Mail'den girilen bağlantılar aşağıda ki görselde gördüğünüz adrese *eğer onay verdiğiniz takdirde, yönlenecektir. Ve siz gelen mailin güvenilirliğine yönelik sorgulama yapmadan bu adrese rahatlıkla gidebilmenin deneyimini yaşadığınızı zannediyor durumdasınız.

"Kampanya hakkında ayrıntılı bilgi için tıklayınız."

Tıklayalım...



Böyle bir içeriğe yönlendiriliyorsunuz. Gördüğünüz URL adresi ise bilinçsiz kullanıcıların en büyük zafiyetlerinden birisini oluşturuyor. Bu adrese girdiğiniz bilgiler direkt olarak scripte gömülmüş dolandırıcı mail adreslerine iletiliyor ve anında işlem yapılarak telefonunuza gelen kodu aynı kurumsal mail adresinden iletmeleri isteniyor. Ve karşı tarafa kodu verdiğiniz andan itibaren dolandırıcılar artık ziraat bankası bireysel işlemler sayfasından hesabınıza erişmiş oluyor.

Maalesef ki bu son aşama ile bir çok mağduriyet yaşanıyor. En sık kullanılan yöntemlerden ziyade daha etkili ve nokta atışı bir senaryo ile karşı karşıya olduğunuzu düşünürsek Facebook,

Instagram ve benzeri yerlerde ki sponsorlu bağlantı hileleri ile dolandırılan vatandaşların sayısını size bırakıyorum...

Görmüş olduğunuz gibi; senaryolar üzerinden ve teknik kısımların araya serpiştirilmesi ile bu vakaların yaşanmasına şahit oluyoruz. Bu olayın her kısımdan yapılabilmesi (mobil cihazlardan / laptolardan / tabletlerden) de ne yazık ki acı bir gerçek. En büyük sorunumuz araştırmamak ve bilinçsiz teknoloji kullanımı.

SONUÇ VE ÖNERİLER: Ne yapılmalı ?

Dolandırıcılık vakalarının analizi çıkarılarak hangi kesime yönelik olduğu yüzde ile belirlenip; bu kesime gerekli uyarıcı makale ve bildiriler yayınlanmalı.

• Her çeşit yaş aralığında görülse de genel uyarılar ve makaleler ile vatandaşlar bilgilendirilmeli.

• Teknik olarak bir mesajın hoax olduğunu anlayabilmek için; yazı dili – içeriklerin dizilimi – verilen mesaj ve en önemlisi sizden istenenin ne olduğunu daima sorgulayarak hareket edin.

• E-ticaret sistemleri'nde doğrulanmamış web siteleri veya bilinmeyen adreslerden alışveriş yapmayın.

• Sosyal Medya'yı bilinçli kullanın.

• Tespit ettiğiniz dolandırıcılık vakalarını ilgili birimlere bildirin.

• Şüphelendiğiniz adresleri USOM kanallarına bildirin. [4]

KAYNAKÇA

[1] Hoax, Hacettepe Üniversitesi – https://yunus.hacettepe.edu.tr/~ncokca/kmlst/hoax.htm
[2] Aldatmaca Türleri, KasperSky – https://www.kaspersky.com.tr/blog/what-is-hoax-report/6087/
[3] Paltacı M. Bahtiyar, WordPress Tema Geliştirme, Level Kitap – Sayfa: 15
[4] Usom İhbar – Ulusal Siber Olaylara Müdahale Merkezi – https://www.usom.gov.tr/ihbar