2020

#evdekalbilgiliol

Bahtiyar PALTACI

covld19.com – bg.org.tr

COVID-19 DATABANK

BİLİŞİM GÜVENLİĞİ

BİLİŞİM SUÇLARINA KARŞI MÜCADELE DERNEĞİ

[COVID-19 SİBER RİSK RAPORU]

[Küresel olarak etkisini gösteren Covid-19 Pandemisi'nin dünya çapında oluşturduğu siber tehditleri ve Türkiye'nin pandemi kapsamında siber risk boyutunu, önlemleri ve önerileri kapsar.]

İÇİNDEKİLER

[1] Covid-19 Pandemisinin Çıkışı

[1.1] Pandeminin çıkış tarihi ve siber ortamdaki durum

1 Aralık 2019 tarihinde Çin'in Vuhan kentinde meydana gelen virüs salgınının Ocak 2020 ortasında dünya geneline yayılmaya başladığı ve konu hakkında tedbirler alındığı görülmektedir.

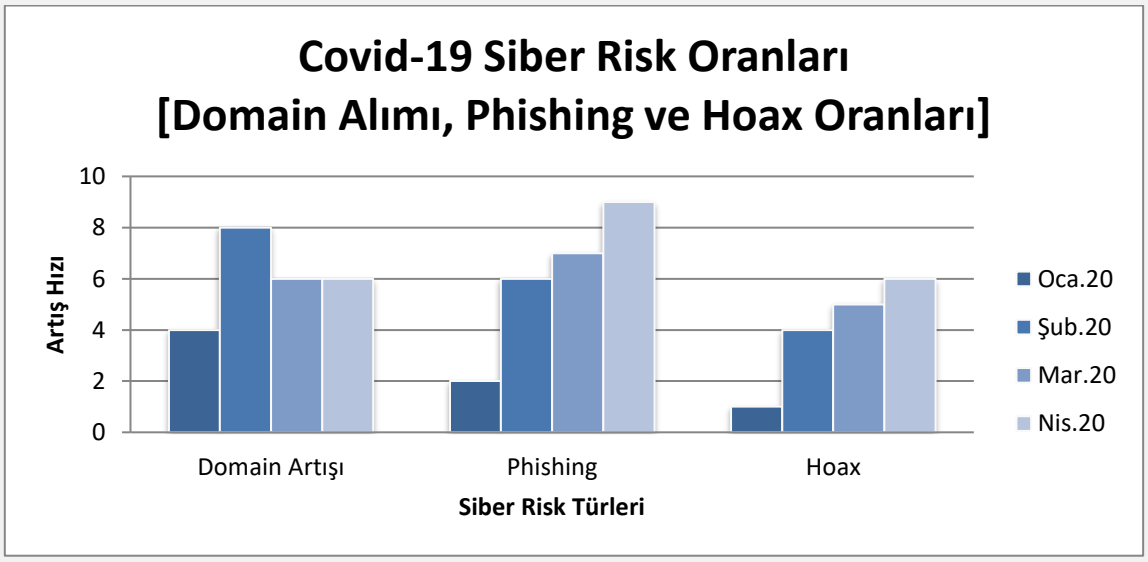
Aralık-Ocak ayı içerisinde Covid-19 hakkında ortaya çıkan bilgiler çoğunlukla siber ortamda resmi kaynaklar ve sosyal mecra üzerinden takip edilmekteydi. Şubat 2020'den itibaren covid19, covid-19, coronavirüs, coronapandemi v.b domainlerin artışında patlama yaşandı.

Ortaya çıkan tabloda çeşitli sağlık sektörüne hizmet veren kurumlar veya temizlik kuruluşlarının da dahil olduğu reg şirketlerinin ise daha çok ön planda olduğu görülmekte. Domainlerin reglenerek daha sonra da belirli şirketlerce satın alındığı da görülmekte.

Siber ortam da ortaya çıkan vakaların başlangıç noktası Şubat 2020 olarak tanımlanabilir. Domain sayısının artışı beraberinde bir çok hoax ve phishing olayını da meydana getirmiştir.

[1.2] Öngörülen / Gerçekleşen Siber Riskler

Aşağıda ki grafikte Covid-19 Pandemisine ilişkin siber ortamda Phishing, Hoax ve Domain Artışı ele alınmıştır. Ocak-Nisan arası olup kaynaklarla desteklenen grafik 10 üzerinden [Artış Hızı] derecelendirilip 3 konuda [Risk Türleri] siber risk alanında ki artışı göstermek maksadıyla hazırlanmıştır.



Ülkemiz bazında gerçekleşen genel siber olaylar ele alındığında, çoğunlukla sanal dolandırıcılık ve sahte sayfalar üzerinden yapılan etkileşimler görülmektedir. Bu kapsamda değerlendirilen risklerde Phishing oranı %70 Hoax oranı %80 ve beraberinde getirdiği dolandırıcılık olayları silsilesi bir hayli fazladır.

Hoax vakalarının en çok gerçekleştiği ortamlar sırasıyla :

- Whatsapp
- Twitter
- Instagram
- Facebook
- Görsel Medya
- Yazılı Medya

Phishing vakalarında en çok rol alınan kuruluşlar :

- E-Devlet
- Bankalar
- Cumhurbaşkanlığı İletişim Ofisi
- Çeşitli belediyeler ve valilikler
- Medya kuruluşları

Vaka oluşum süreçlerinde saldırganlarca amaçlanan hedefler/amaçlar :

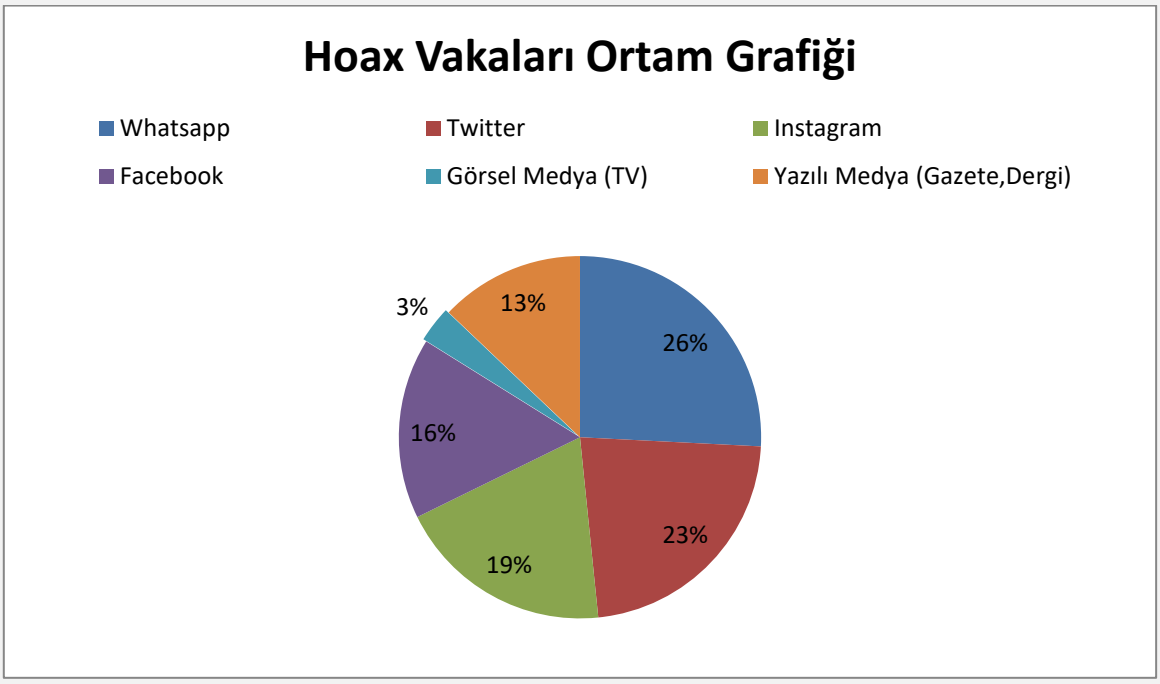
- Fidye isteme, gayriresmi para kazanma
- Kişisel bilgileri ele geçirme, kötüye kullanma
- Şantaj ve kötüye kullanım ile kurban profili oluşturma
- Hacktivizm, Black Hat senaryoları

Sırasıyla oluşan siber riskler :

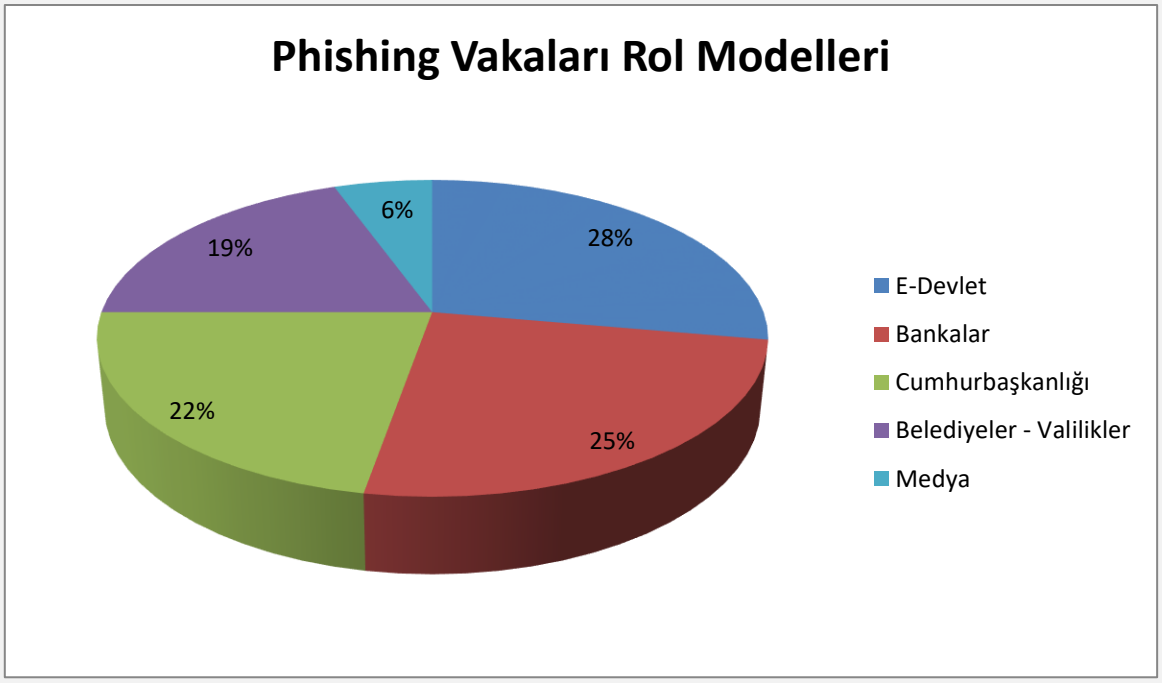
- Phishing
- Hoax
- Ransomware
- Keylogging
- RCE

Aşağıdaki grafiklerde siber vakalara göre çeşitli oranlar ele alınmıştır.

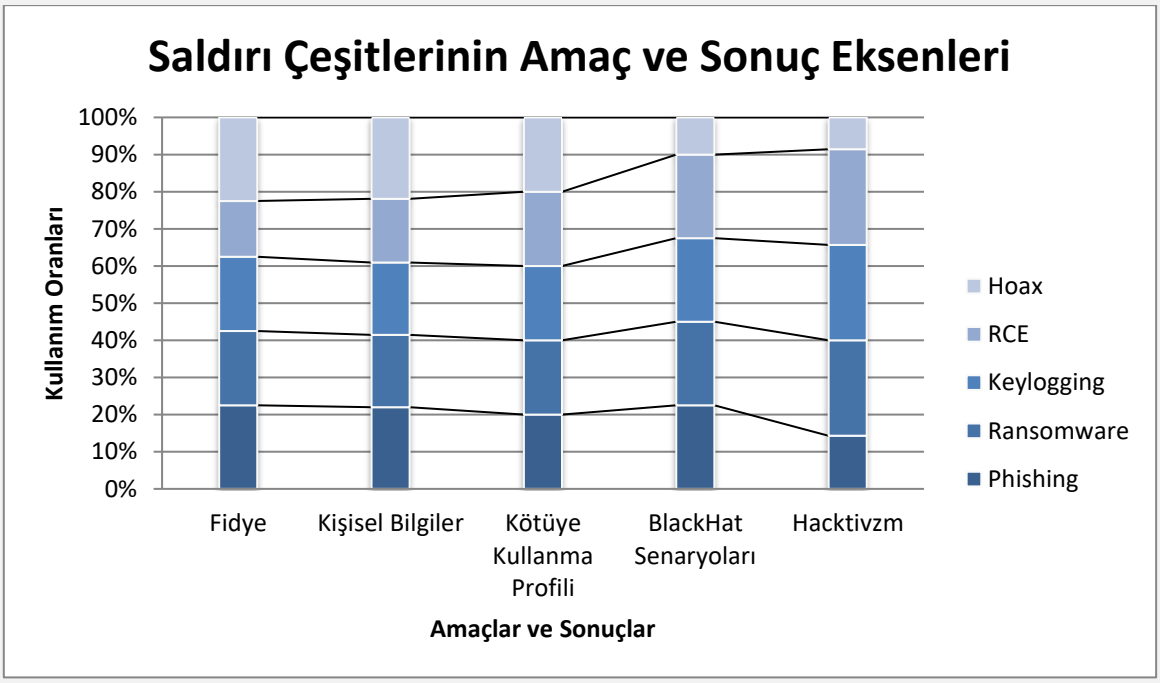
Hoax Vakaları Ortam Grafiği: Gerçekleşen spekülasyon ve yalan haberlerin ve beraberinde getireceği sorunların hangi ortamlar üzerinden yapıldığının oranlarını içerir.



Phishing Vakaları Rol Modelleri Grafiği: Gerçekleşen oltalama saldırılarının, en çok hangi kurum ve kuruluşların rol model alınarak yapıldığını göstermektedir.



Bu grafik gerçekleşen siber saldırıların Covid19 kapsamındaki amaçlarının ve sonuçlarının ele alındığı oranları içermektedir.

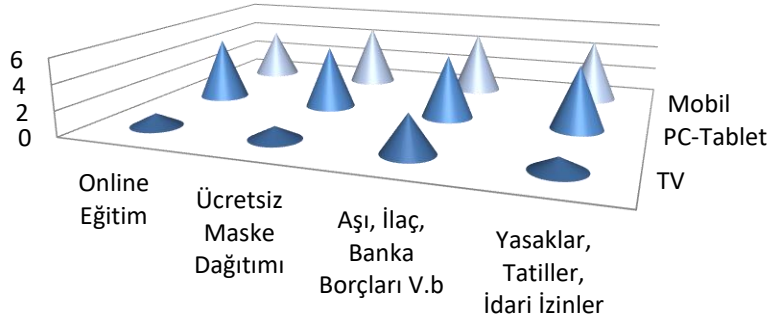


Genel olarak siber risklere baktığımızda yaşanan vakaların amaç ve sonuçları değerlendirildiğinde; ortaya çıkan Covid19 Pandemisi'nin getirdiği endişe ve merak duygusu

kullanılarak vakaların artışı ve genel amaçların değişmediği görülmektedir. Grafikte yer alan unsurlara ek olarak siber ortamdan “Korku Yayma, Spekülasyon” oranları da bir hayli fazladır.

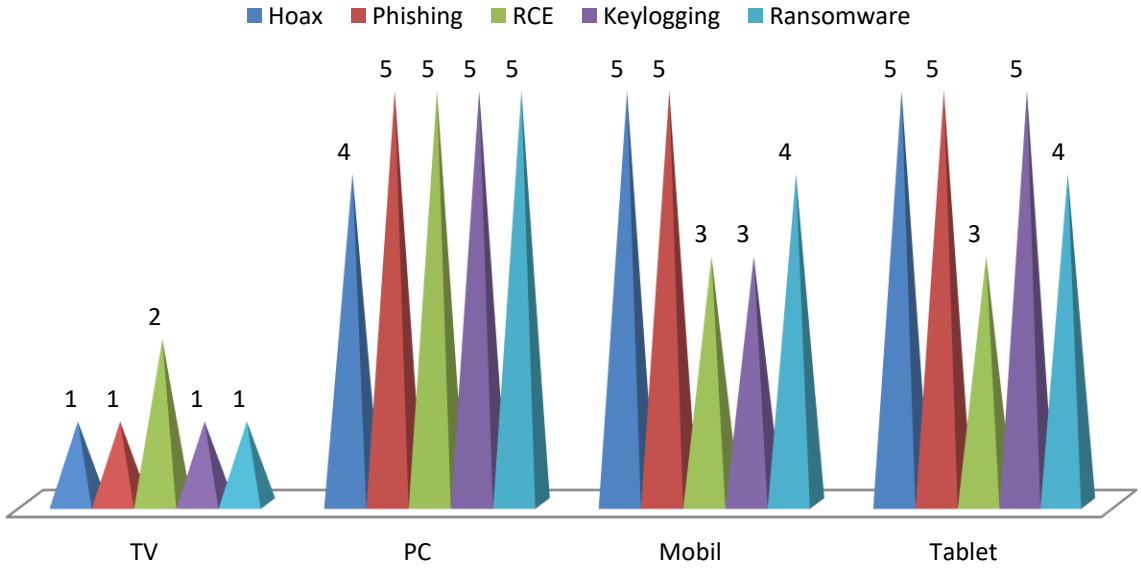
Devam eden salgın sürecinde ülkemizde ki gündeme göre siber ortam koşullarında ortaya çıkabilecek vaka ve risklerin ortam/unsur incelemeleri ve sonuç endeksi aşağıdaki grafikte toplanmıştır.

Gündem Konularına Göre Öngörülen Risklerin Ortam Grafiği [1]



	Online Eğitim	Ücretsiz Maske Dağıtımı	Aşı, İlaç, Banka Borçları V.b	Yasaklar, Tatiller, İdari İzinler
TV	1	1	3	1
PC-Tablet	5	5	5	5
Mobil	4	5	5	5

Gündem Konularına Göre Öngörülen Risklerin Ortam Grafiği [2]



Covid-19 Pandemisi Siber Risk Raporu – Bahtiyar PALTACI

Yukarıda belirtilen iki grafik de amaç-sonuç nedeni ilişkisi içerisinde bir bütün olarak değerlendirilmelidir. Şöyle ki ; Televizyon, PC ve Tablet, Mobil ortamlardan gelecek siber

risklerin [gündem konuları] bütününde bu konular kapsamınca gerçekleşecek [siber saldırılar] dağılımları 4 madde üzerinden [TV,Mobil,PC-Tablet] değerlendirilerek oranlanmıştır.

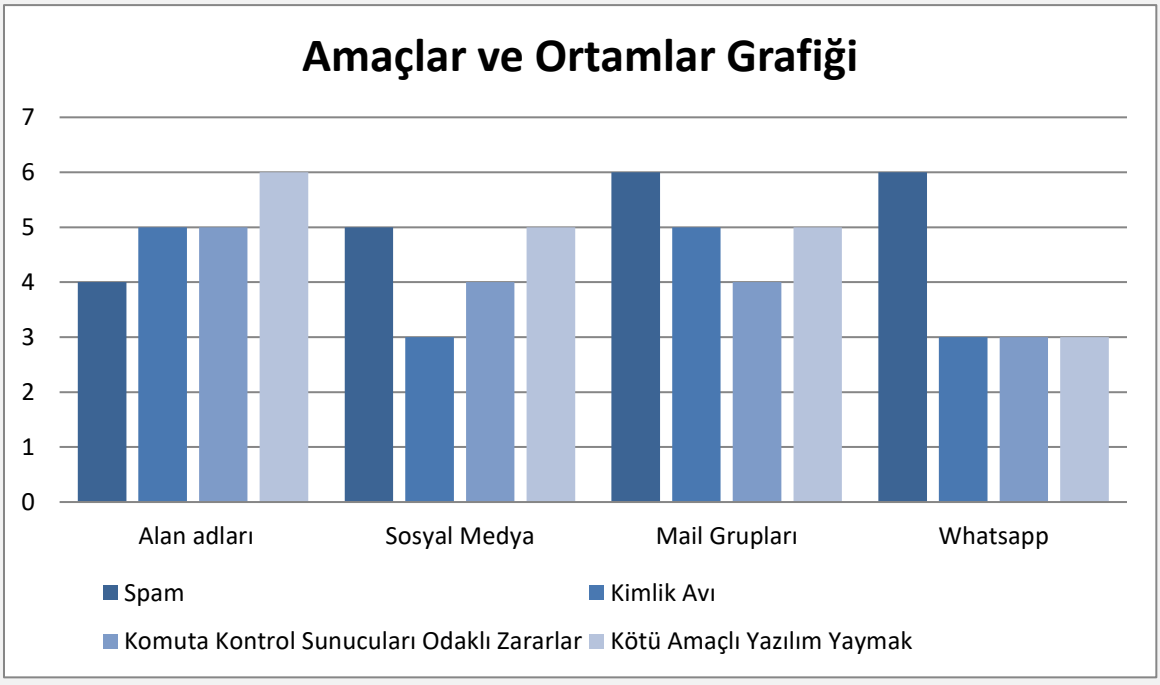
[2] Covid-19 Pandemisinin Yayılışı

[2.1] Dünya Genelinde Dijital Sirkülasyon

Covid-19 çıkış tarihinden yayılma sürecine kadar dünya genelinde dijital sirkülasyon da çok fazla artış görülmektedir. Domain ve web sistemleri alımları, kurulumları liste dahilinde olmakla birlikte, çevrimiçi eğitim metodları, çevrimiçi siparişler, online görüşmeler genel olarak artış listesindedir.

[2.3] Açılan Covid-19 Domainleri Ve Amaçları

Aşağıda ki grafikte açılan Covid-19 domainlerinin amaçlarını göstermek üzere diğer ortamlar ile de mükayese yapılarak sonuçlar listelenmiştir.



Covid-19 Pandemisi Siber Risk Raporu – Bahtiyar PALTACI

Açılan domainlerin meşru olduğu kadar gayrimeşru olanları da bir hayli fazladır. Amaçlar spam, kimlik avı, komuta kontrolsunucuları odaklı saldırılar, kötü amaçlı yazılım yaymak gibi faktörleri kapsamaktadır.

[2.4] Hoax Ve Phishing Vakalarının Artışı

Dünya genelinde dijital sirkülasyon da gerçekleşen siber vakalarda hoax ve phishing vakalarına ayrı bir başlık açmak gereklidir. Bu tür saldırıların çoğunluğa hitap edecek şekilde ve dağıtık olması risk faktöründe kaos odaklı yükselişler gösterir. Sonuç ve önlemlerde ki makaleleri bu bağlamda değerlendirip; Hoax ve Phisihing vakalarının önüne geçmek için kendinizi geliştirmelisiniz. Bunun için dikkat en önemli konu olmakla beraber teknik kavramlara da az da olsa aşina olmak gerekir.

[2.5] Resmi ve Faydalı Covid-19 Kaynakları

Açılan domainler de dünya genelinde bir çok gayrimeşru domain olduğunu söylemiştik. Alan adı ve sosyal medya bazında zararlı domainleri takip etmek yerine aşağıda bulunan kaynakları kullanabilirsiniz. Twitter üzerinde bulunan bazı fenomen Twitter hesaplarının da bu konuda olumlu çalışmaları olsa da çok fazla itibar edilmemesi gerektiğini unutmayalım.

Kurum	Amaçlar	Kaynak
INTERPOL	Covid 19 Siber Tehditler	https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats
DSO – DÜNYA SAĞLIK ÖRGÜTÜ	Covid 19 Siber Tehditler	https://www.who.int/about/communications/cyber-security
COE – AVRUPA KONSEYİ	Covid 19 Siber Suçlar	https://www.coe.int/en/web/cybercrime/cybercrime-and-covid-19
USOM – TR CERT	Covid 19 Siber Tehditler	https://twitter.com/trcert
SAĞLIK BAKANLIĞI TR	Covid 19 Güncel Durum	https://covid19.saglik.gov.tr/
ANADOLU AJANSI – AA – TR	Covid 19 Gelişmeler	https://www.aa.com.tr/tr/koronavirus
CB - DİJİTAL DÖNÜŞÜM OFİSİ	Dünya geneli harita	https://corona.cbddo.gov.tr/
COVİD 19 INFO LIVE	Canlı karşılaştırmalar	https://covid19info.live/
ROYLAB STATS	Canlı izleme	https://www.youtube.com/watch?v=SLV1B5Lzy48&feature=emb_rel_err
DSO – DÜNYA SAĞLIK ÖRGÜTÜ	Veriler, Grafikler	https://who.sprinklr.com/
MELBOURNE UNIVERSITY	Tahminler	https://covid19forecast.science.unimelb.edu.au/
IHME – ARAŞTIRMA ENST.	Tahminler, Sosyal Uzak.	https://covid19.healthdata.org/projections
DATACAT	Etkileşimli karşılaştırma	https://www.datacat.cc/covid/
COVID-19 TR DATABANK	Siber, Genel, Timeline	https://www.covld19.com
ANNUAL REVIEWS	Bilimsel Kaynak	https://www.annualreviews.org/ - search> coronavirüs
CAMBRIDGE UNIVERSTY	Bilimsel Kaynak	https://www.cambridge.org/gb/academic/covid-19-resources-and-information
DERGİPARK	Bilimsel Kaynak	https://dergipark.org.tr/tr/search?q=covid+OR+coronavir*&section=articles
COCHRANE LIBRARY	Bilimsel Kaynak	https://www.cochranelibrary.com/covid-19
DYNAMED	Bilimsel Kaynak	https://www.dynamed.com/condition/covid-19-novel-coronavirus
ELSEVIER	Bilimsel Kaynak	https://www.elsevier.com/connect/coronavirus-information-center
EMERALD PUBLISHING	Bilimsel Kaynak	https://www.emeraldgrouppublishing.com/promo/coronavirus.htm
IEE XPLORE DIGITAL LIBRARY	Bilimsel Kaynak	https://innovate.ieee.org/covid-19_related_research/
IOP PUBLISHING	Bilimsel Kaynak	https://ioppublishing.org/ news> coronavirüs
KARGER	Bilimsel Kaynak	https://www.karger.com/Tap/Home/278492
THE LANCET	Bilimsel Kaynak	https://www.thelancet.com/coronavirus
PROJECT MUSE	Bilimsel Kaynak	https://about.muse.jhu.edu/resources/freeresourcescovid19/
PUBLMED	Bilimsel Kaynak	https://www.ncbi.nlm.nih.gov/research/coronavirus/
BIORXIV	Bilimsel Kaynak	https://connect.biorxiv.org/relate/content/181
OXFORD ACADEMIC	Bilimsel Kaynak	https://academic.oup.com/cid
SEMANTIC SCHOLAR	Bilimsel Kaynak	https://www.semanticscholar.org/
SCIENCE MAG	Bilimsel Kaynak	https://www.sciencemag.org/ search> coronavirüs
SIAM	Bilimsel Kaynak	https://epubs.siam.org/page/EpidemiologyCollection

SPRINGER NATURE	Bilimsel Kaynak	https://www.springernature.com/gp/researchers/campaigns/coronavirus
TAYLOR – FRANCIS	Bilimsel Kaynak	https://taylorandfrancis.com/coronavirus/
TR DİZİN GOV	Bilimsel Kaynak	https://www.trdizin.gov.tr search> coronavirüs
UPTODATE	Bilimsel Kaynak	https://www.uptodate.com/ contents> coronavirüs
CLARIVATE	Bilimsel Kaynak	https://clarivate.com/coronavirus-resources/
WILEY ONLINE LIBRARY	Bilimsel Kaynak	https://novel-coronavirus.onlinelibrary.wiley.com/

[2.6] Online Eğitim'e Geçiş Süreci Ve Getirmiş Olduğu Riskler

[2.7] En Çok Kullanılan Online Araçlar

Ülkemiz ve dünya genelinde online eğitim sürecine geçilmiş olması sebebiyle artan online riskler saptanmıştır. En çok kullanılan Zoom uygulamasının kullanılmaması tavsiye edilir. Aşağıda ki liste de online eğitim araçları ve kapsamları listelenmiştir.

Araç	Limit	Toplantının Kaydı	Ekran Paylaşım	Dosya Paylaşım			Mesajlaşma Özelliği	Sanal Tahta
				Video	Ses	Dosya		
Zoom	45 dk 100 kişi	EVET	EVET	EVET	EVET	EVET	EVET	
Google Hangouts	10 kişi	EVET	EVET	EVET	EVET	EVET	EVET	
Uber Conference	45 dk 10 kişi	EVET		EVET	EVET	EVET		
TrueConf Online	3 kişi	EVET				EVET		EVET
Skype	10 kişi	EVET	EVET				EVET	
FreeConference	5 kişi		EVET			EVET	EVET	
Appear in	4 kişi		EVET				EVET	
Slack Video Calls	15 kişi						EVET	
Cisco Webex Meeting	100 kişi		EVET					

Bunlar dışında Microsoft Teams uygulaması da kullanım tercihi olabilir.

[3] Sonuç ve Önlemler

[3.1] Online İletişim İçin Önlemler

Türkiye'de en çok kullanılan mesajlaşma uygulaması Whatsapp'ın log tutması mümkün mü? Temel mantıkla tüm içeriklerin ilgili yazılımın sunucusunda loglanabileceği mümkündür.

Bu konuya açıklık getirmek açısından daha çok öne çıkan özelliklere bir bakalım. Bilindiği gibi Whatsapp telefona kurulurken bazı izinler ister bu izinlerin birçoğu programın getirdiği özelliklerin tam olarak kullanılabilmesi içindir. Bu özellikler nedir inceleyelim.

•Take Photo or Video (Foto-Video Çekim)

•Choose Photo or Video (Foto Video Seçim)

•Share Location (Konum Paylaşma)

•Share Contact (Kişi Paylaşma)

•Send Document (Döküman Yollama)

•Find Images (Resim Arama)

•Broadcast (Toplu Mesaj)

•Groups (Grup oluşturma)

Bu tür özelliklerin kullanılabilmesi için Whatsapp'ın telefon kullanıcısından gerekli Android/iOs izinlerinin listesini uzun uzun yazmaya gerek yok. Fakat şunu rahatlıkla söyleyebiliriz ki bu tür izinlerin bir çok riski mevcut.

Hackerların gözünden basit bir senaryo kuracak olursak bu tür erişim yetkilerine Whatsapp aracılığı ile ulaşıldığı takdirde; kişi-rehber bilgileriniz, telefon kayıtlarınız, son çağrılarınız ve sık kullandığınız görüşme kayıtları, izinsiz fotoğraf çekimi, ses kaydı, aile fotoğrafları, sms kaydı, telefon aracılığı ile kişisel bilgisayara erişim, senkronizasyon ile google hesaplarına erişim… kötü niyetli kullanıcılar tarafından ele geçirilebilir.

Tabiî ki bütün bunların yapılması kapsamlı bir senaryo ile oluşturulur ve gerekli teknik bilgi ile pekiştirilir. Bütün bunlar sosyal mühendislik yöntemiyle de yapılabilir fakat Whatsapp'ın teknolojik olarak nelere izin istediğini ve bu izinlerin güvenliğini sağladığını söylese de kapalı kapılar ardında neler olabileceğini bir üstteki paragrafta belirttik.

Daha güvenli iletişim için ne yapmalıyım?

Teknoloji çağında ne yazık ki %100 güvenli iletişim söz konusu değildir. Tabii ki konu son kullanıcılar yani halk olarak ele alındığında…

Fakat daha güvenli bir iletişim kurmak için azami düzeyde risklerin önlenmesi mümkündür. Bunları liste/karışık halde ele alalım.

•Uygulama izinlerinin en aza indirilmesi.

•Kişisel, mahremiyet taşıyan bilgilerin bu tür iletişim kanallarında kullanılmaması.

•Farklı aplikasyonlar kurarak ana aplikasyona erişim söz konusu olabilir (izinlerin açılması v.b)

•Bunu önlemek için kullandığınız telefonun yazılımsal olarak temiz olması çok önemli.

•Kullandığınız cihaz rootluysa kernel kodlarına erişim yapılabiliyor. Yine yan uygulamalar sayesinde iletişim kanallarını da etkileyerek çok çeşitli zararlar vermek mümkün.

•Bilgi düzeyiniz sınırlıysa kesinlikle telefonunuzu rootlamayın.

•Çeşitli antivirüs yazılımları kullanmanız tercih sebebiniz olabilir.

•Yine yan uygulamalar aracılığı ile network advertising ismini verdiğimiz yollarla bulaşan reklam türünde ki zararlı yazılımlar telefonunuza bulaşabilir; bunun sonucunda da kullandığınız Whatsapp türevi iletişim uygulamasını etkileyebilir.

•Url/apk ile tanımlanmış, Whatsapp aplikasyonunun arayüzü dışında ki bu tür reklam yoluyla bulaşan zararlı yazılımları çalıştırmayın veya onaylamayın.

•Sosyal sorumluluk bilinci bakımından gerekli önlemlerinizi alarak başta çocuklarınızın iletişim araçlarını hangi amaçlarla kullandığını mutlaka gözden geçirin.

[3.2] Phishing ve Hoax Saldırılarına Karşı Önlemler

Günümüz de 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.

Hoax Nedir ?

İçerisinde aldatıcı bilgiler ile dikkat çekecek biçimde hazırlanmış mesajlar bütünüdür. 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. 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.

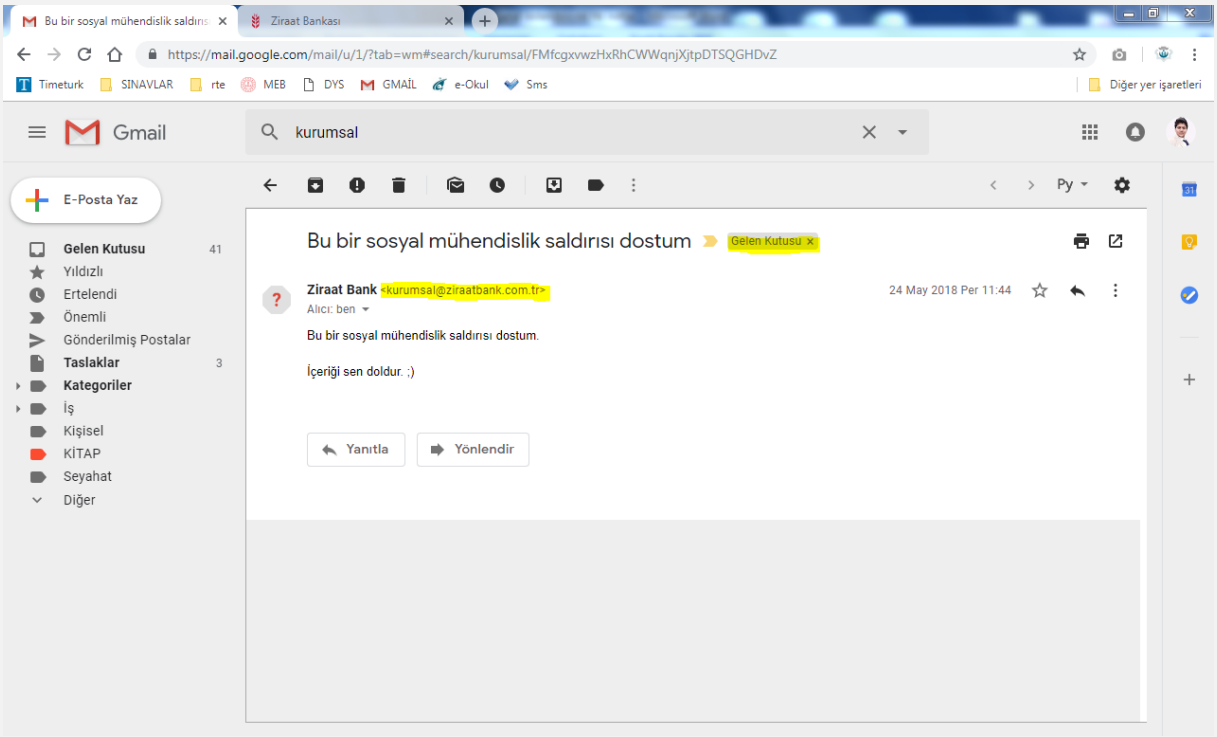
Bkz : Alınan bilgiler doğrultusunda hedefin çalıştığı kurum tespit edilir ve saldırı senaryosu üzerinden fikirler geliştirilir.

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.



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.

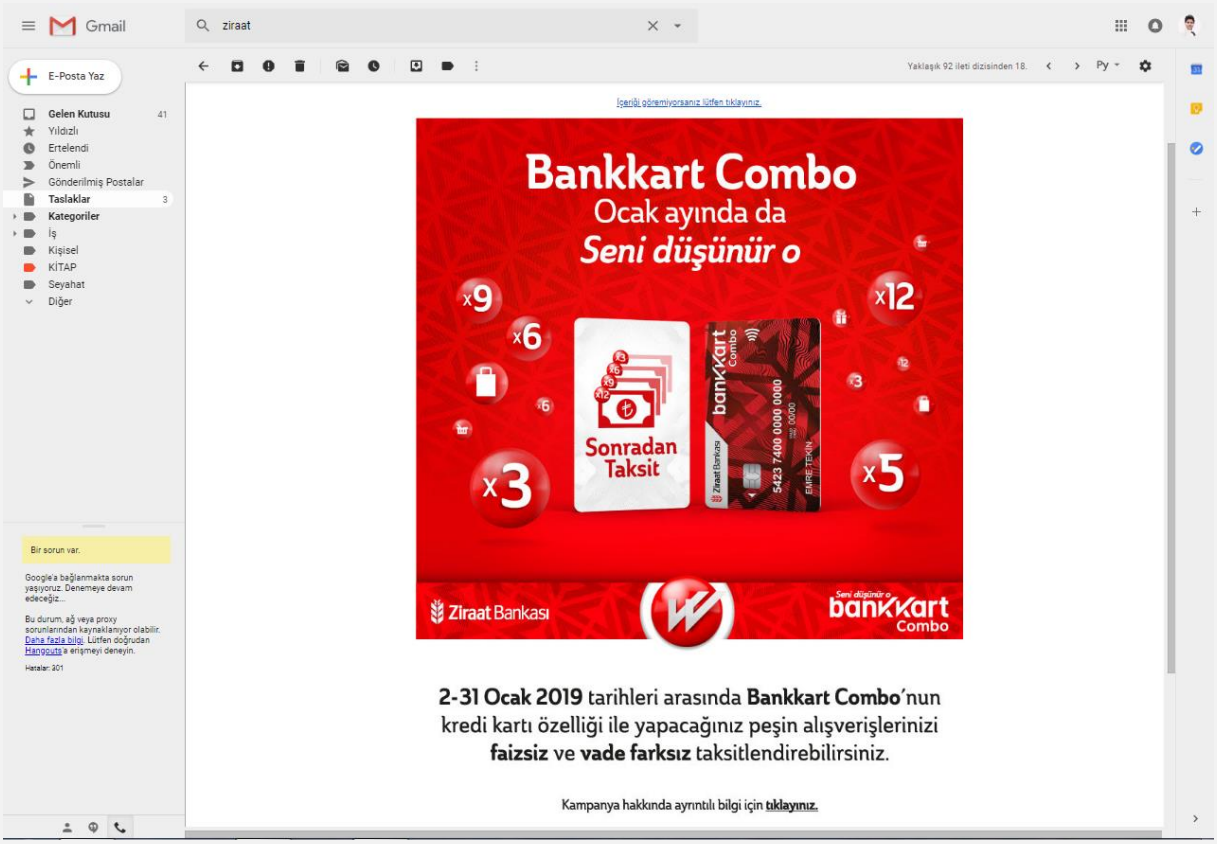
Mail İçeriği

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. 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

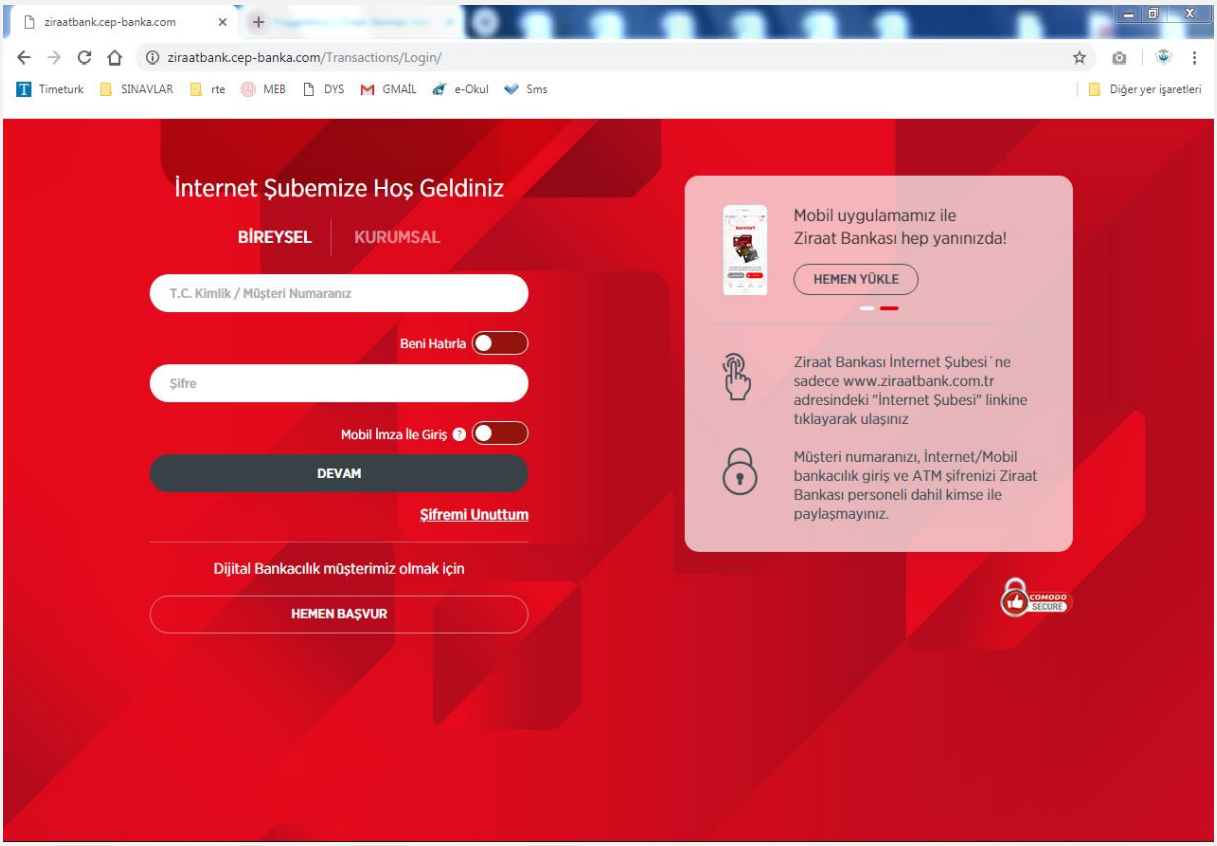
hazırlanan Hoax'da ki verilerin inandırıcılığı ile; son aşamada önünüze gelen aldatıcı sayfanın güvenilirliğinde gözden kaçan detaylar sonucu bir çok mağduriyet malasef ki yaşanmakta.

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.

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 BG kanallarına yazabilirsiniz.