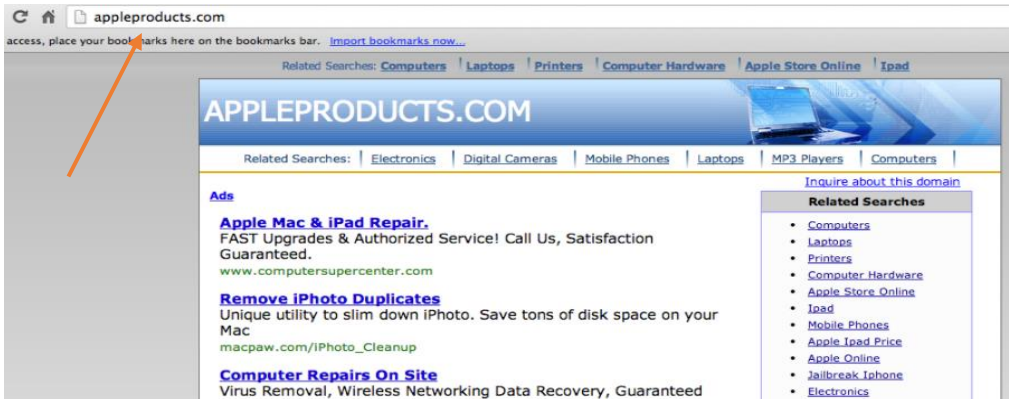
ALAN ADI İHLALLERİ – E-POSTA SAHTECİLİĞİ ÇÖZÜM YOLLARI VE ALINABİLECEK TEDBİRLER

CYBERSQUATTING – EMAIL SPOOFING – EMAIL FORGING

Cybersquatting, mevcut bir ticari markaya benzeyen bir alan adının kafa karıştırıcı bir şekilde kötü niyetli tescili ve kullanımıdır. Örneğin AppleProducts.com (*Şekil 1*) gibi "Apple" genel bir terim olsa da burada açıkça Apple, Inc.'e atıfta bulunulmaktadır. Cybersquatter 'lar çok çeşitli yasa dışı ve gayrı meşru uygulamalar yürütebilmekte olup bu kapsamda kötü amaçlı yazılım gönderebilir, sahte ürünler satabilir, kimlik avı düzenleri barındırabilir, kimlikleri çalabilir ve aldatıcı reklam hilelerinden para kazanabilirler. Ayrıca internet alan adlarını büyük ölçekte elde etmek için genellikle oldukça gelişmiş otomatik programlar kullanırlar, bu da internet kullanıcılarını büyük ölçekte istismar ettikleri anlamına gelir.



Şekil 1. Benzer alan adı üreterek dünya çapında bir markayı taklit örneği

Aynı şekilde majör tehditlerden birisi de **Email Impersonation Scamming** ya da **Email Spoofing** adı verilen bir şirketin ya da kişinin yerine geçerek gerçeğine çok yakın bir algı yaratacak yöntemlerle sahte bir mail kimliği kullanarak potansiyel veya halihazırdaki kontaklarla iletişime geçmek amacı ile yapılan siber ataklardır. Bu atak daha çok yukarıda tanımlanan Cybersquatting yapılarak önce alan adı satın alınarak yapılır. Biraz daha ileri bilgiyle bu satın alma olmadan da direkt sahte uzantıyla mail atılabilir, bu mümkündür. Ancak bu tip mailler %99 oranla sistem tarafından spam olarak algılanır ve junk (gereksiz e-posta) klasörüne düşer. Dolayısıyla bu tip dolandırıcılık vakalarında kayıtlı legit (meşru) mail adresleri kullanılır.

Bu atakta da amaç aslından ayırt edilmesi çok güç olan bir alan adı satın alınarak ya da alan adının önüne ya da devamına alakalı bir ek getirerek -asıl yani jenerik ismi aynen kapsayacak bir şekilde, benzer e-postaları üretmek ve bunları kullanarak işletme sahiplerini ve yöneticilerin kimliklerini taklit etmektir. Hedeflenen genellikle yetkili pozisyonlardaki üst düzey çalışanlardır ve

bu etkin kimliklerle kurbanlardan para transferi yapmalarını, fatura ödemelerini veya saldırgana hassas veriler göndermelerini istenebilir. Bu atak ***CEO Fraud*** olarak da bilinir. *(Şekil 2)*

Şekil 2- Email Impersonating Örneği

Bunların yanında bir email adresinin "from" *(kimden)* kısmı değiştirilerek yapılabilen bir atak daha vardır. Buna **Email Forging** denir. Kural olarak her e-postanın iki farklı göndericisi vardır. Bir e-posta adresi "zarf gönderen" (envelope sender) olarak adlandırılır ve bir diğeri e-posta başlığında ayarlanır. İkincisi, normalde Microsoft Outlook gibi e-posta istemcileri tarafından görüntülenen 'Kimden:' başlığı olarak bilinir. Ne yazık ki siber suçlular, e-posta istemcilerini işletmenize ait bir ad ve e-posta adresi göstermeleri için kandırmak için 'Kimden:' başlığını taklit edebilir. Bunu önleme yöntemleri de (SPF, DKIM ve DMARC kayıtlarını kayıt ve teyit ettirmek) mevcuttur ancak bunlar ileri seviye sayılabilecek teknik detaylar olduğu için bu bilgi notunda ayrıntıya girilmeyecektir.

ÇÖZÜM ÖNERİLERİ

GELENEKSEL YÖNTEMLER

SEÇENEK # 1: WIPO KANALI ile KARŞI BİR TAHKİM YOLU İZLEME

WIPO- World Intellectual Property Organization (Dünya Fikri Mülkiyet Örgütü) alan adı ve ticari marka konularında söz konusu çevrimiçi suiistimallerle mücadele için öneriler ve yöntemler geliştirmek için kurulmuş, marka sahiplerinin haklarını korumak ve küresel e-ticarette tüketici güvenini oluşturmak için kanallara sahip dünya çapında bilinen ve yetki sahibi bir kuruluştur. Kurum başvuru süreci olarak zaman içinde optimize ettiği UDPR (Uniform Domain Name Dispute Resolution Policy) ile oldukça başarılı ve etkili bir çevrimiçi araç üretmiş başarısını kanıtlamıştır.

Yine de WIPO başvuru süreci oldukça zahmetli, uzun süren ve bir o kadar da maliyetli bir yöntem olarak değerlendirilebilir. Kurumun kendisi dahi zaman zaman siber işgaller ve marka ihlalleri konusunda vakıanın şartlarına göre daha hızlı, oldukça verimli, uygun maliyetli bir kanal olarak dünyadaki tüm alan adlarının ilk günden beri zorunlu olarak kaydedildiği en üst seviye organizasyon olan ICANN (Internet Corporation for Assigned Names and Numbers) başvuru

yolunu önermektedir. *WIPO son dönemde WIPO 3.0 adı verdiği daha hafif ve hızlı bir model üzerinde de çalışmaktadır.*

SEÇENEK # 2: ICANN KANALI ile UDRP ŞİKAYETİNİN DÜZENLENMESİ

Hak sahipleri, ICANN 'in anlaşmazlıkları çözmek için geliştirdiği bir dizi işlem ile Tekil Alan Adı Anlaşmazlık Çözümü Politikası (UDRP) 'nı kullanarak ihlal şikayetinde bulunabilirler. UDRP, bir şikayetçinin şu üç unsuru mevcut bulundurmasını gerektirir:

- Alan adı, şikayetçinin ticari markasına kafa karıştıracak şekilde benzer olmalıdır.
- Tescil ettirenin alan adı üzerinde hiçbir hakkı veya meşru menfaati olmamalıdır.
- Alan adı tescil edilmiş ve "kötü niyetle" kullanılıyor olmalıdır.

UDRP şikayetçisi iddiasında haklı çıkmayı başarırsa, ihtilaflı alan adının kendi kontrolüne aktarılmasını veya iptal edilmesini sağlayabilir ancak maddi tazminat söz konusu değildir. Şikâyette bulunmak için ICANN web sitesinde bulunan aşağıdaki linkteki online form doldurulur; ***https://survey.clicktools.com/app/survey/response.jsp***

Ancak ICANN 'a başvurmadan önce tüketilmesi gereken yollar vardır. Kötüye kullanım içeren bir alan adıyla ilgili şikayetler önce üst kayıt kuruluşuna (registrar) bildirilmelidir. ICANN 'e kötüye kullanım şikayetinde bulunmadan önce kayıt operatörünün yayınladığı kötüye kullanım iletişim bilgilerini kullanarak kayıt operatörüne bir kötüye kullanım raporu göndermek ve kayıt operatörünün inceleyip yanıt vermesi için yeterli süre tanımak ve bunu belgelemek gerekmektedir. Bir alan adının üst (registrar) kayıt kuruluşunu belirlemek için **https://lookup.icann.org/** adresinde bir arama yapılabilecek olup (kötüye kullanım amaçlı kişiler "Kayıt Şirketi Bilgileri" alanında listelenmiştir) kötüye kullanım iletişim bilgileri, kayıt operatörünün web sitesinde de görüntülenmelidir.

NOT: Marka sahiplerinin her ihlale karşı bir UDRP başvurusunda bulunmaları adet arttıkça maliyetli olacaktır. Yapmış olsalar bile, UDRP kapsamında izin verilen en ağır ceza, bir siber saldırganı o anda başvuru konusu ihtilaflı alan adını bırakmaya zorlamaktır. Bu, binlerce alan adına sahip siber saldırganlar için caydırıcı değildir ve kaybettikleri alan adını başka bir hak ihlalinde bulunan siteyle kolayca değiştirebilirler.

SEÇENEK # 3: SAVUNMA ARACI OLARAK TÜM İLGİLİ ALAN ADLARINI KAYDETMEK

Marka sahipleri, onları kötü aktörlerin elinden uzak tutmak için düzenli olarak savunma alan adları kaydetmektedir. Bununla birlikte, kötü aktörler, yazım hataları içeren veya ticari markaları başka kelimelerle birleştiren sonsuz sayıda olası alan adı tasarlayabilir. Saldırganlar kurumun web alan adlarına benzer yer değiştirmiş harflerle çeşitli alan adlarını satın alabilir veya

homografik karakterler kullanarak yazımı taklit edebilirler *(.com yerine .conn gibi)*. Yine komut dosyası sahteciliği ve Kiril veya İbranice gibi başka bir dilin karakterleri ustaca kullanılarak da URL'de fark edilmesi zor ihlal içeren benzer adlar üretilebilir. Çözümlerden biri de kendini saldırganın yerine koyarak yeri değiştirilmiş veya ortak Kiril harfli web sitelerini içeren web sitelerini satın almak ve bunları kuruluşun ana sayfasına geri yönlendirmektir.

DESTEKLEYİCİ FAALİYETLER

YENİ NESİL YÖNTEMLER

Burada tavsiye edilen aksiyonlar tamamen hukuk büromuz tarafından zaman içinde geliştirilmiş teknik ve sosyal tabanlı pro-aktif çözümlerdir. İnternetin kuralsız, sınırsız ve sayısız varyasyonlu seçenekler ortamı olması dolayısı ile zaman zaman gerilla hareketi olarak dahi tabir edebileceğimiz yöntemler kullanmak kaçınılmaz olmaktadır. Saldırganın -sosyal mühendislik olarak da adlandırılan aldatıcı ataklarını önceden kestirebilmek için onun yerine geçmek ve bir saldırganın düşünce yapısına bürünerek müşterilerimiz, potansiyel ilişkilerimiz hatta ailemiz ve çevremizi korumak adına ondan bir adım önde olmak gerekmektedir.

QR Code/ Çözümü

E-postalarımıza BT/IT ekibi tarafından kolaylıkla oluşturulacak bir barkod ya da QR Code ile gönderilen her e-postaya otomatik olarak (bir mail imzası gibi) eklenecek, e-postanın bizden geldiği ve iletişimin kaynağının resmi olarak biz olduğu karşı tarafça teyit edilebilecektir. QR Code okutmak artık çok kolay ve pandemi sürecinde kafelerde ve restoranlarda sıklıkla prova edildiği için yaygın olarak uygulanan ve bilinen bir işlemdir. Hemen her telefon hiçbir uygulama indirmeden sadece kodu kamerasına göstererek QR Code'u saniyeler içinde okuyabilmektedir.

Bu noktayı da yine e-maillerde bir üst bilgi olarak (*lütfen bu e-mailin bizden geldiğine emin olmak için QR Code 'u okutunuz)* ve bunun yanında imzanın altındaki mail disclaimer 'ına mutlaka not ederek bildirmemiz bizi hukuki olarak birçok soruna ve husumete karşı koruyacaktır. Ancak her ihtimali düşünmek adına da şirketimizin özellikle yurt dışı bağlantılı banka hesaplarına ve yüksek meblağlı hareketlere karşı kontrol ve onay metotları eklemek bu tarz kaçak para çıkışları için tamamlayıcı bir önlem olacaktır.

Bu kapsamda gerçekleştirilen IBAN dolandırıcılıkları en sık karşılaşılan sahtekarlık yöntemlerinden biridir. QR kod çözümünün benzer bir versiyonu ise oltalama/phishing kodu olarak da uygulanabilir. Oltalama kodu, gönderilen veya alınan e-postanın kendi kurumunuzdan veya güvenli göndericiden gönderildiğinden emin olmanızı sağlayan bir ek güvenlik katmanıdır. Bu kapsamda kurumunuz veya kötü niyetli karşı taraflarca paylaşılmış izlenimi verilerek e-posta aracılığıyla gönderilen oltalama (phishing) iletilerinin oluşturabileceği zararlar

engellenebilecektir. Oltalama Kodu'nu belirlediğinizde, bu kod, kurumunuzca gönderilen tüm iletilere eklenecektir. E-postalarda yer alacak kod sayesinde aynı QR kod gibi iletinin sahte olup olmadığını belirlemek kolaylaşır ve oltalama girişimleri engellenebilir. Sahtecilik girişimleri ile gönderilen mesajlarda bu kod yer alamayacaktır. Sınır ötesi iletişimler için bu uygulama kullanılabilecek olup aynı zamanda kurumsal itibarı da arttırıcı nitelik gösterebilecektir.

Periyodik Keşif ve Savunma Yazışmaları

Dünya üzerindeki sayısız bölgede çok fazla sayıda alan adı sağlayıcısı mevcuttur. Yine de bunları saldırgan bulabiliyorsa bizler de erişebiliriz demektir. Konunun zor kısmı bazı bölgelerin uluslararası anlaşmalardan -dolayısıyla uluslararası icra ve ihtar yollarından, muaf olmalarıdır. Bu sebeple buradaki kayıt kuruluşları ile direkt olarak ya da sitelerindeki formlar vasıtasıyla yazışmak ve kendimizi tanıtmak gerekli ve yerinde bir aksiyon olacaktır. İyi haber ise bir bölümüne en üst seviyede bulunan yukarıda bahsettiğimiz ICANN örgütü vasıtasıyla bu bildirimlerin yapılabilmesidir.

Bu kurumlardan kötü niyetli kayıtların (bad-faith registrations) talep edilmesi anında kendimizi tanıtmış olmamız, belirleyeceğimiz anahtar kelimelerle (keywords) bu kurumların kontrol listelerine muhtemel ihlal kayıtlarını işletmiş olmak ve alarm mekanizmalarını *(gerek sözleşmelerle gerekse centilmenlik anlaşmaları ile)* oluşturmak markaları ve ticari işaretleri ciddi bir yayılımla korunur hale getirecektir. Tabi bunun için en az bir çalışanın düzenli olarak bu kurumları listelemesi, güncellemesi ve onlarla yazışması gereklidir. Bunun yanında alan adı taramaları ile benzer isimlerin saldırıya uğrayıp uğramadığı da sık aralıklarla kontrol edilmelidir.

Bilgi Notları ve Disclaimer Gönderimleri

Müşteri ve *(henüz müşteri olmamış ya da hiçbir zaman müşteri olmayacak olsa da)* sair kontaklara çeşitli vesilelerle *(kutlama, newsletter, katalog, bilgi notu vb.)* tarafınızdan kurulacak ekstra iletişimler yukarıda *QR Code* başlığı altında bahsettiğimiz tedbir ve tembihleri aktarabilmek ve Kurumunuzun e-posta biçimini belirli aralıklarla karşı tarafa tanıtma fırsatı verecektir. Bu tür iletişimler karşı network 'te kendiliğinden yayılma potansiyeli olan viral bir etkileşim ihtimali içermekle birlikte sizden haber alma formatına alışık bir kontağınızı, söz konusu aldatıcı atak anı geldiğinde bu biçimsel farklılığı hissederek harekete geçirme ve savunma noktasında sizin uç birimdeki takım arkadaşınız haline getirme yeteneği de çok yüksektir.

SON SÖZ

İnternet suçlarında idrak edilmesi gereken en talihsiz konu internetin çıkış noktasında bireyler için tasarlanmış olmasıdır. İlk ve en büyük mottosu *özgürlükler ülkesi* ütopyası olduğu için kuralları ve etiği uzun süre sonra oluşturulmaya başlamıştır. Gerek alt yapı olarak gerekse kültürel olarak bu

kadar büyüyeceği kesinlikle kestirilmemiş ve güvenlik kaygıları söz konusu bile olmamıştır. İnternet ağı büyüdükçe, kitlelere ve son kullanıcılara erişim yeteneği fark edildikçe bu platformun reklam ve satış için kullanılabileceği akıllara gelmeye başladığında ise kuralları koymak için maalesef geç kalınmıştır. Şirketler ve kamu kurumları ise oyuna oldukça sonradan dahil oldukları için iş işten geçmiş ve internet anayasası tabir edilen *kuralsızlığın kuralı* ortamı bir türlü ticari ilişikler ve sofistike iletişim için gereken basiret ve uyumluluk seviyesine çıkamamıştır. Bu da ihlal ve suç hallerinde hukuksal süreçlerin reel hayattaki gibi seyretmemesine ve çoğu zaman havada kalması ile sonuçlanmaktadır.

Saygılarımızla,

GRC | LEGAL