infoblox

LOOKALIKE SALDIRILARINA DERİNLEMESİNE BAKIŞ

YENİ ÇALIŞMALAR EN SON TEHDİT VEKTÖRLERİNİ ORTAYA KOYUYOR

Nisan 2023

LOOKALIKE DOMAIN SALDIRILARI HERKESİ HEDEFLER

İÇİNDEKİLER TABLOSU

YÖNETİCİ ÖZETİ

Saldırganlar, internetin ortaya çıkışından bu yana kullanıcıları kandırarak kötü amaçlı web sitelerini ziyaret etmelerini sağlamak için görsel olarak benzer alan adları kullanmaktadır. Lookalike domains olarak adlandırılan bu alan adları kimlik avı saldırılarına o kadar benzerdir ki, güvenlik farkındalığı eğitimi bu gibi bağlantıları incelemeyi öğrenmeyi de içerir.

Bununla birlikte, farkındalık kampanyalarına ve teknolojideki ilerlemelere rağmen, lookalike domainler tüketiciler ve kuruluşlar için sürekli karşılaşılan ve saldırganların hızla adapte olduğu bir tehdit oluşturuyor. Tüketicilerden devletlere, büyük perakende markalarından küçük restoranlara, dünyaca ünlü teknoloji şirketlerinden daha az bilinenlere kadar herkes bir hedef. Bu makalede, gerçek alan adları ve kampanyalardan örneklerle "herkesin bir hedef olduğunu" göreceksiniz. Oldukça niş bir sektörde mütevazı büyüklükte bir şirket olarak biz bile hedef alınıyoruz.

Bu rapor, sektörler ve kullanıcı grupları genelinde gerçek dünya örneklerini sergileyerek mevcut tehdit ortamını açıklamaktadır. Infoblox yıllardır benzer etki alanlarını tespit etmekte ve yeni ve potansiyel tehditleri bulmak için günlük 70 milyardan fazla alan adı sistemi (DNS) olaylarını analiz etmektedir. Bu makale için Ocak 2022'den Mart 2023'e kadar olan tespitlere odaklandık. 300.000'den fazla benzer alan adından, bu saldırılarla ilişkili zorlukları ve riskleri vurgulayan bir liste oluşturduk.

Lookalike Domainler genellikle e-posta spam'i, reklam, sosyal medya ve SMS mesajları yoluyla tüketicilere yönelik geniş kapsamlı, hedefsiz saldırılarla ilişkilendirilir. Her gün popüler yazılımları, finans kurumlarını ve paket dağıtım hizmetlerini taklit eden binlerce yeni alan adı tescil ediliyor. Kullanıcı kimlik bilgilerini çalmayı veya makinelere kötü amaçlı yazılım bulaştırmayı amaçlayan kimlik avı saldırıları o kadar yaygın ve çoğu zaman o kadar basittir ki, "e-postanızı kontrol etmezseniz kimlik avı dolandırıcılığına kanmazsınız"; gibi çok sayıda özdeyişin kaynağı haline gelmiştir. Genellikle komik olarak tasvir edilse de, kimlik avı ciddi bir sektör. Kimlik Avıyla Mücadele Çalışma Grubu (APWG), kimlik avının 2022'nin üçüncü çeyreğinde rekor seviyeye ulaştığını bildirmektedir.[1]

[ ] ***Bu makaledeki tüm göstergeler, kötü niyetli veya meşru olma durumlarına bakılmaksızın değiştirilmiştir. Noktaların [.] etrafına parantezler yerleştirerek göstergeleri bozduk ve tıklanabilir bağlantı olmalarını engelledik.***

70+ MİLYAR

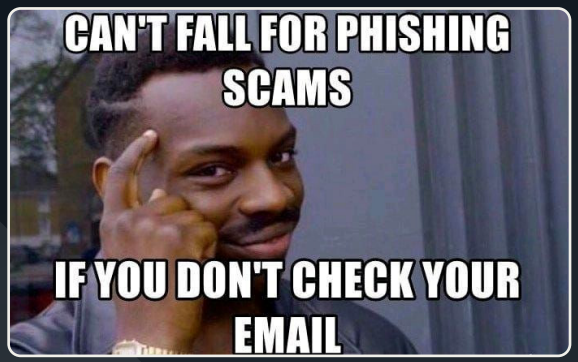
Infoblox, yeni tehditleri belirlemek için günlük 70 milyardan fazla DNS olayını analiz eder.

300K+

benzer alan adı, bu rapor için bu saldırıların zorluklarını ve riskini vurgulamak için seçildi.

KİMLİK AVI MEME'İNE BİR ÖRNEK.

Bir örnek, 2019'daki bu tweet'tir.[2]



Resim kredisi: Bu meme'in kökeni bilinmemektedir.

Ancak benzer alan adları sadece tüketiciler için bir tehdit değildir. Kurumsal ağlara erişim sağlamak için de kullanılırlar.

Son açıklamalar, kötü niyetli aktörlerin çalışanları çok faktörlü kimlik doğrulama (MFA) kimlik bilgilerini sağlamaları için kandırdığı hedefli saldırıları ortaya çıkardı. Çoğu durumda, benzer alan adları sadece şirketi taklit etmekle kalmadı, aynı zamanda MFA anahtar kelimelerini de içeriyordu. Bu durum daha fazla çalışanın bağlantının güvenli olduğuna inanmasını sağladı. Aktörlerin internet servis sağlayıcıları, bankacılık ve kripto para birimi, yazılım ve hizmetler ve sigorta şirketleri dahil olmak üzere birçok sektörde büyük ve küçük işletmeleri hedeflediğini belirledik. Bu saldırılar 2022 yılının başlarında başladı ve zamanla ivme kazandı.

Asimetrik bir saldırı olduğu için benzer alan adlarının kullanımı kârlıdır. Kullanıcılar kişisel mali durumlarını ve işverenlerinin bilgilerini korumak için her zaman tetikte olmalıdır. Ucuz alan adı kayıt fiyatları ve büyük ölçekli saldırıları dağıtma yeteneği aktörlere üstünlük sağlar. Saldırganlar ölçek avantajına sahiptir ve kötü niyetli faaliyetleri tespit etme teknikleri yıllar içinde gelişirken, savunmacılar buna ayak uydurmakta zorlanmaktadır.

Benzer alan adı kullanan kimlik avı yöntemleri gelişmekle kalmıyor, aynı zamanda benzerlerin kullanımı DNS kayıtlarında belirgin bir şekilde daha karmaşık hale geldi. Araştırmamız, benzer alan adlarının geleneksel kimlik avı ve yazım yanlışı amaçlarının ötesinde kullanıldığını gösteriyor. Ayrıca, daha önce bildirilmeyen şekillerde de kullanılıyorlar: örneğin, ad sunucuları olarak ve spear phishing posta dağıtımı için. Sadece benzer alan adlarına hizmet veren ve hem tüketicileri hem de kamu çalışanlarını hedefleyen büyük esnek ağlar vardır.

Infoblox benzer alan adlarını tanımlamak için birden fazla algoritma kullanmaktadır. Alışveriş, bankacılık, yazılım ve finans sektörlerindeki yaygın hedeflerin ve müşterinin belirlediği alan adlarının varyantlarını ve benzer alan adları konusunda uzmanlaşmış DNS altyapı aktörlerini izlemek gibi yöntemlerin bir kombinasyonunu kullanıyoruz. Bu çok yönlü yaklaşım bize tehdit ortamının geniş kapsamını sağlıyor.

> ***ÖNEMLİ NOT: Bu rapor, internet genelindeki benzer alan adlarının genişliğini ve derinliğini gösteren bir dizi örnek içermektedir; bunlar herhangi bir kuruluşa ilişkin başarılı saldırıları veya ihlalleri ima etmeyi amaçlamamaktadır.***

ARKA PLAN

Tüm iyi araştırma makaleleri gibi, bazı arka plan bilgileriyle başlayacağız. Bu çoğunlukla kelime bilgisini içeriyor. Çoğu okuyucunun arka plan bölümünü atladığını bildiğimiz için bu bölümü kısa tuttuk.

Kötü niyetli benzerler (bilinen bir alan adıyla aynı veya çok benzer görünen, saldırgan tarafından kaydedilmiş alan adları) siber ortamda iyi bilinen, kalıcı bir tehdittir. Genel anlamda, benzerlerin hem saldırı hem de savunma uygulamaları vardır. Saldırgan anlamda, insan gözünün olabileceği her yerde benzerlikler aldatma için kullanılır. Saldırganlar para çalmak, kimlik bilgileri veya erişim elde etmek, kişisel kimlik bilgileri toplamak, kötü amaçlı yazılım dağıtmak veya reklam geliri elde etmek için benzer alan adlarını kullanır. Ayrıca siyasi amaçlarla ve marka itibarını zedelemek için de kullanılmaktadırlar. Kısacası, siber suçlular için amaca giden bir yoldur. Savunma anlamında, birçok kuruluş saldırganların bu alan adlarını talep etmesini ve kullanmasını önlemek için kendilerininkine benzer alan adlarını proaktif olarak kaydettirmektedir.

Benzer alan adları farklı biçimler alır. DNS alanında, alan adları şunlar olabilir:

- **Homograflar**
- **Combosquat'lar**
- **Typosquat'lar**
- **Soundsquat'lar**

Orijinal hedef alan adından neredeyse ayırt edilemez veya nesnel olarak oldukça farklı olabilirler. Benzer alan adlarının bir saldırı vektörü olarak başarısının büyük bir kısmı, bireylerin üstündeki yükten kaynaklanmaktadır.

Göreceğimiz gibi, e-posta gönderen adreslerinden kimlik avı URL'lerine ve kötü amaçlı yazılım komuta ve kontrolüne (C2) kadar bir saldırının her unsurunda benzerler bulunabilir. Genellikle adres kayıtları (A/AAAA) ile ilişkilendirilmesine rağmen, ad sunucusu (NS), işaretçi (PTR) ve kanonik ad (CNAME) kayıtları için kullanılan benzerler bile bulduk. Bunlar e-posta, SMS veya kısa mesajlar, güvenliği ihlal edilmiş web siteleri, kötü amaçlı reklam ağları ve telefon görüşmeleri yoluyla dağıtılabilir. Aşağıdaki bölümde, farklı benzerlik biçimlerini kısaca açıklanmış ve her birine ilişkin örnekler verilmiştir.

DAKTILOYU SUÇLA

Aslında, bu modern sorunun izi daktiloların ilk günlerine kadar sürülebilir. Birçok eski daktiloda, 0 veya 1 tuşu yoktu, çünkü daktilo yazanların bu rakamları temsil etmek için büyük O ve küçük L harflerini kullanmaları bekleniyordu.[4]

HOMOGRAFLAR (HOMOGLİFLER)

İngilizce'de homograf kelimesi "aynı yazılışa sahip, ancak aynı şekilde telaffuz edilmesi gerekmeyen ve farklı anlamlara sahip iki kelime" anlamına gelse de, homograf terimi güvenlik araştırmaları literatüründe uzun yıllardır "görsel olarak aynı görünen iki alan" anlamında kullanılmaktadır.[3] Daha doğru bir terim homogliftir. Bu alan adları birbirine benzer ve bazı durumlarda neredeyse ayırt edilemez olabilir. *Araştırma literatürüyle tutarlılık sağlamak için bu makalede yanlış terim olan 'homograf'ı kullanacağız.*

Bu benzerlik biçimi, aynı karakter kümesindeki veya alfabedeki birçok karakterin birbirine benzemesinden yararlanır. Örneğin, 0 (sıfır rakamı) ve O (büyük harf "o") veya "l" (küçük harf "L") ve "I" (büyük harf "i"). Bazı yazı tipleri bu sorunu daha da vurgulamaktadır. Bunun klasik örnekleri, Google'daki "o" kelimesinin sıfır (0) ile değiştirildiği ve Infoblox'taki "i"nin sırasıyla küçük harf "L" ile değiştirildiği g0ogle.com ve Infoblox.com'dur.

İnternet olgunlaştıkça ve İngilizce bilmeyen daha fazla kişi World Wide Web'de oturum açmaya başladıkça, uluslararası alan adlarına (IDN'ler) olan ihtiyaç arttı. IDN, Latin alfabesinde bulunmayan en az bir karakter içeren bir alan adıdır; Unicode'un kullanılmaya başlanması, bu tür alan adlarının yükselişini sağladı. IDN'lerle birlikte yeni bir benzerlik biçimi ortaya çıktı: IDN homografı. Bu da bir homoɡrɑf olsa da benzer görünen diğer karakter kümelerinden veya alfabelerden karakterler kullanır. Gabrilovich ve Gontmakher, 2002 tarihli "The Homograph Attack" (Homograf Saldırısı) adlı makalelerinde IDN hoɱografının gücünü gösterdi. Yazarlar, gerçek Microsoft alan adı microsoft[.]com'un Kiril harfleri "c" ve "o" içeren bir benzerini tescil ettiler.[5] Sonuçta ortaya çıkan www.microsoft[.]com alan adı, gerçek Microsoft alan adından görsel olarak ayırt edilemez.

Unicode Konsorsiyumu, belirli bir dize için mevcut çok sayıda kafa karıştırılabilir karakteri gösteren bir araç yayınladı.[6] "hi" dizesi Unicode karakterli 684 varyasyona sahiptir; "infoblox" gibi bir dize için sayı 2,2 trilyonun üzerinde varyasyona yükselir. Bazı varyasyonlar, benzerler için diğerlerinden daha az etkilidir. Örneğin, Unicode Konsorsiyumu "৯" (genişletilmiş Arapça-Hint rakamı beş) karakterini "o" (Latince küçük harf "O") için potansiyel bir kafa karıştırılabilir karakter olarak listelemiştir.

Açıkça, inf৯bl৯x[.]com çok etkili bir benzerlik değil; ancak yaygın olarak kullanılan Arial yazı tipinde gösterildiğinde, {infoblox[.]com} ve {infoblox[.]com} (Belarusça veya Ukraynaca küçük "i" ve Ermenice "n" olarak yazılan küçük "vo" harfi içeren) aradaki farkı görebiliyor musunuz? Biz de göremiyoruz.

TYPOSQUAT'LAR

Typosquat alan adları, popüler alan adlarından ve kullanıcıların yaptığı veya bozuk klavyelerde yazmaktan kaynaklanan yazım hatalarından yararlanır. Bu terim genellikle reklam parası çekmek amacıyla kaydedilen ancak kullanılmayan alan adlarıyla ilişkilendirilir. Örneğin, yazarlardan biri yakın zamanda mülk yönetim grubunun appfolio[.]com (mülk yönetim gruplarına ve ev sahiplerine SaaS çözümleri sunan tanınmış bir yazılım şirketi) adresinde barındırılan çevrimiçi portalı üzerinden kira ödemeye çalışıyordu. Bunun yerine, yazım hatası yapıp neredeyse appfollio[.]com'u ziyaret ettiler. Bu 2013 yılında tescil edilmiş ancak şu anda park halinde olan bir alan adı.

İlginç bir şekilde, Appfolio için bir başka görünür typosquat alan adı, apfolio[.]com, Appfolio'ya ait gibi görünüyor. Doğru alan adına yönlendiriyor ve aynı tescil ettiren, tescil ettiren kuruluş ve tescil ettirene sahip. Yasal alan adı appfolio[.]com'dan sadece bir ay sonra tescil edilmiş. Bu, benzer alan adlarının savunma amaçlı kullanımına bir örnek. Ne yazık ki, kötü niyetli kişiler avantajlı durumda çünkü çok fazla olasılık olduğundan kuruluşların tüm benzer varyasyonları kaydetmesi mümkün değil.

Typosquat'lar öncelikle bir para kazanma yöntemi olarak algılanır, ancak kötü bir amaçları olabilir. Bunlar 3. taraf reklamlarını satmak veya yasal alan adı sahibine satış yapmak için kullanılırken, daha sonra göstereceğimiz gibi "blackhat" bağlı kuruluş pazarlama programları ve kötü amaçlı yazılım C2 alanları olarak da kullanılabilirler. Markalar ve şirketler, Anticybersquatting Tüketici Koruma Yasası kapsamında typosquatting'e karşı sivil korumaya sahiptir. Bu yasal işlem tehdidinden dolayı, typosquatting, alan adı çevirme/park etme topluluğunda para kazanmanın "blackhat" bir biçimi olarak görülmektedir ve iGoldRush gibi ciddi alan adı yüzücüler, kâr için typosquatting yapmamayı tavsiye etmektedir.[7]

TYPOSQUAT ÖRNEKLERİ

gikthub[.]com
5whatsapp[.]com
Hdfcbank[.]vip
royalbsank[.]com
sportybet[.]city
bamgkokbank[.]com
1337x[.]asia
moneycont5rol[.]com

kötüye kullanılan combosquatting alan adlarının 1000 günden fazla süredir aktif olanları

kötüye kullanılan combosquatting alan adlarının ilk çözümlemeden 100 gün sonra en az bir kamuya açık engelleme listesinde yer alanları

COMBOSQUATTİNG

Combosquatting, popüler marka veya şirket adlarını diğer anahtar kelimelerle birleştiren bir benzerlik biçimidir. Destek, yardım, güvenlik ve posta gibi terimler yaygındır. Örneğin, wordpresssupport[.]ru, wordpresssupport[.]store ve wordpress-security[.] cloud'u düşünün. Bu alan adlarının hepsi aynı Rusya merkezli IP adresi üzerinde barındırılıyor ve popüler web içerik yazılımı WordPress'e benziyor. Alan adına destek ve güvenliğin dahil edilmesi bunların WordPress kullanıcılarına yönelik olduğuna işaret ediyor. Bunlar, WordPress sitelerini ele geçirmek için kimlik bilgilerini veya ödeme ve kişisel tanımlanabilir bilgi (PII) ayrıntılarını toplamak için kullanılabilirler.

Saldırganlar, combosquat alan adlarını kendileri oluşturmanın yanı sıra, benzerlerini oluşturmak için sözlük alan adı oluşturma algoritmalarını (DDGA'lar) da kullanabilmektedir. Saniyeler içinde, çok sayıda marka veya şirket için binlerce aday alan adı oluşturulabilir. Şans eseri algoritma, alan adının etkili olabilmesi için doğru anahtar kelimelere sahip aday alan adları oluşturabilir. En iyi oyun platformlarından biri olan Steam'in kullanıcı topluluğu, combosquat DDGA'ları kullanan saldırganlar için ortak bir hedeftir. Yakın zamanda gözlemlenen bir kümedeki bazı alan adı örnekleri şunlardır: steamcommiunity[.]com[.]ru, steamcommucnity[.]com[.]ru, steamcommunityjp[.]top ve steamcommunityiq[.]top. Bu alan kümesinde typosquatting ve combosquatting arasındaki örtüşmeye dikkat edin.

Kitsin ve ark. 2017'de yaklaşık 468 milyar DNS kaydını (hem aktif hem de pasif veri kümelerinden kaynaklı) analiz ederek combosquatting üzerine boylamsal bir çalışma gerçekleştirdi ve rahatsız edici sonuçlara ulaştı:

- **Combosquat alan adları, typosquatting alan adlarından 100 kat daha yaygın**
- **Kötüye kullanılan combosquatting alan adlarının %60'ı 1.000 günden uzun süredir aktif**
- **Kötüye kullanılan combosquatting alan adlarının %20'si ilk çözümlerden 100 gün sonra en az bir genel engelleme listesinde görünmektedir**
- **Combosquat alan adı çözünürlüğü yıldan yıla arttı[8]**

Yazarların combosquat alanlarının yaygınlığına ilişkin bulgularına katılıyoruz. Analitiklerimiz aracılığıyla saf typosquats veya saf homoraflardan (IDN veya başka bir şey) daha fazla combosquat alanı buluyoruz.

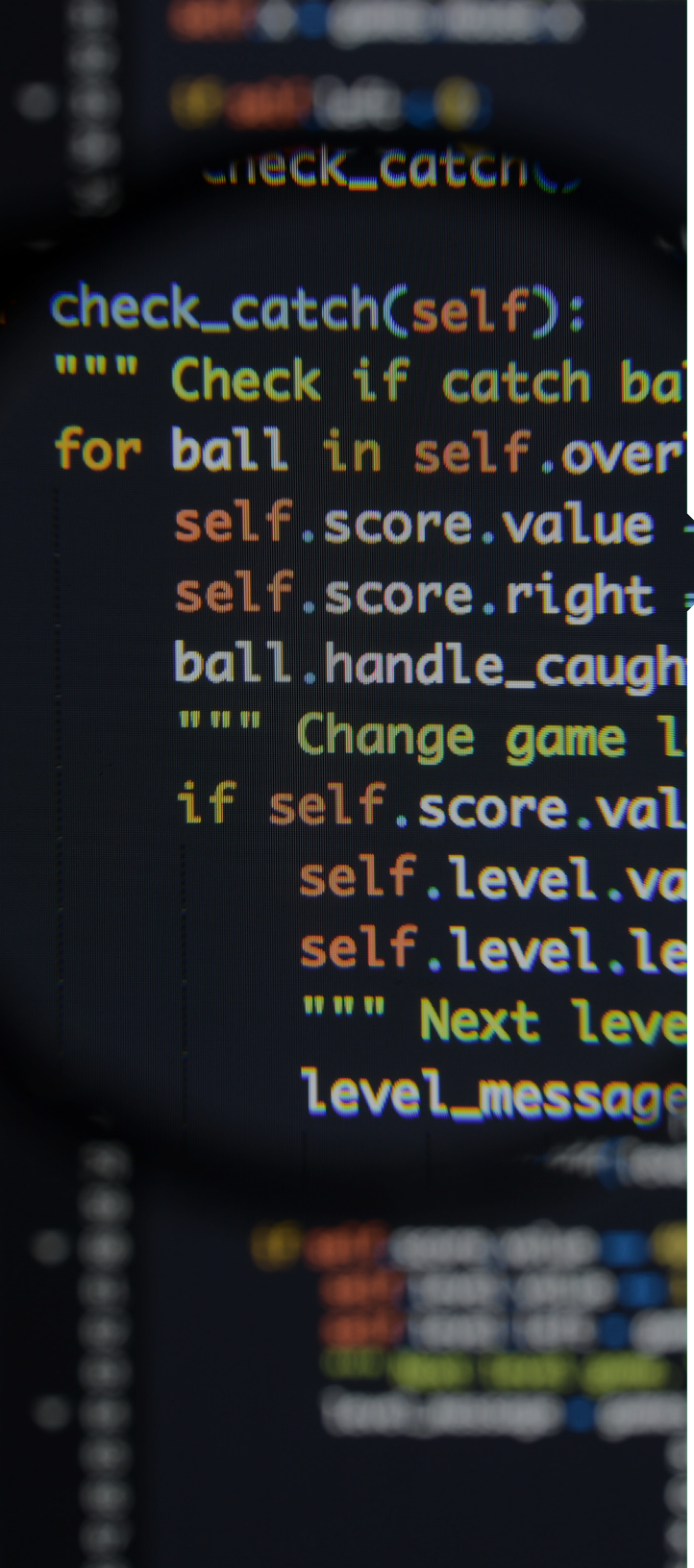
SOUNDSQUATTİNG

Soundsquat alan adları, kulağa aynı gelen ancak farklı bir yazıma sahip kelimeler olan homofonların kullanımından yararlanır. Soundsquatting, ilk olarak 2014 yılında literatürde ortaya çıkan en son tanımlanan benzerlik biçimidir.[9] Soundsquatting, Alexa, Siri ve Google Voice akıllı hoparlörlerin çoğalması nedeniyle son zamanlarda araştırmacıların daha fazla ilgisini çekti.[10] Soundsquat alan adları, diğer benzer alan adı türleriyle örtüşür, çünkü hem ses çıkarabilir hem de benzer görünebilirler. Görsel olarak benzer görünmeyen ancak aynı görünen saf ses alanlarının nadir olduğunu bulduk. Bu alan adları genellikle metin tabanlı benzerlik teknikleriyle de bulunabilir.

Vahşi doğadaki benzer adlarının genellikle burada belirttiğimiz gibi kolayca kategoize edilemeyeceğini belirtmek önemlidir. Bir benzer alan adının etkinliğini en üst düzeye çıkarmak için formların bir kombinasyonu kullanılır. Gördüğümüz combosquat alan adlarının çoğunda typosquat ve homograf (IDN veya başka türlü) unsurları bulunmaktadır. Typosquat'lar homografların unsurlarını, soundsquat'lar typosquat'ların unsurlarını vb. kullanır. Sonuç olarak, saldırganların savunuculara nefes aldırmayacağı asimetrik bir tehdit ortamı ortaya çıkıyor.

SES SALDIRISI

Soundsquatting'in yaygınlığı, Alexa, Siri ve Google Voice gibi sesle etkinleştirilen teknolojilerin ortaya çıkmasıyla başladı.



BENZER ALAN ADLARININ DİĞER BİÇİMLERİ

Bu makalenin odak noktası benzer alan adları ve bunların mevcut tehdit ortamındaki rolleri olsa da, savunmasız kullanıcıları istismar edebilen başka benzerlik türleri de mevcuttur. Bunların dikkate değer bir örneği yakın zamanda Python PyPi paketlerinde bulundu.

https://infosec.exchange/@tweedge@cybersecurity.theater/109846797159938702

Python gibi popüler programlama dilleri için paket yöneticileri, alan adları ile aynı zayıflıklara maruz kalmaktadır. Herkes herhangi bir adla (bu ad daha önce alınmadığı sürece) güvenlik riski içermeyen ya da içermeyen kod içeren bir paket yükleyebilir. 2016 yılında güvenlik araştırmacısı Nikolai Tschacher, 17.000'den fazla farklı ana bilgisayarı keyfi kod çalıştırmaya zorlamak için bu şekilde typosquatting kullanmıştır.[11] Ardından 2021 yılında güvenlik araştırmacısı Alex Birsan, Tschacher'in fikrini alıp genişleterek "bağımlılık karışıklığı" terimini ortaya atmıştır.[12]

Birsan, çeşitli açık kaynaklar aracılığıyla büyük şirketlerin özel, dahili paket adlarını buldu. Bu, web sitelerinde kaynak kodunu keşfetmeyi, GitHub'da paketleri aramayı ve hatta halka açık forumlarda paket adlarını bulmayı içeriyordu. Ardından, özel, dahili paketlerle aynı adı taşıyan paketleri genel paket yöneticilerine yükledi. Birsan, son olarak otomatikleştirilmiş CI/CD boru hatlarını kullanarak özel, dahili paketler için genel paketleri "karıştırdı". Otomatik boru hatları, özel paketleri içe aktarıp kurmak yerine Birsan'ın genel paketlerini bulup içe aktardı. Birsan daha sonra DNS sızıntısını kullanarak, amaçlanan özel paketin değil keyfi kodunun çalıştırıldığını kendisine bildirdi. Birsan'ın taklit tekniği, bazıları paketlerini yükledikten birkaç saat sonra olacak şekilde 35 kuruluşa sızmasını sağladı.

Görünümün türü veya benzerliğin kullanıldığı bailiwick ne olursa olsun, benzerlikler kalıcı bir tehdittir. Benzerleri incelemenin zorluklarından biri de tanımlanmamış olmalarıdır. Hesaplanamayacak kadar fazla olasılık vardır ve her şey bir hedeftir. Aşağıdaki bölümlerde, hedefler, dağıtım yöntemleri, altyapı, neden etkili oldukları, zorluklar ve Infoblox'un soruna yönelik çözümleri dahil olmak üzere vahşi doğadaki bu çeşitli benzerlik biçimlerinin spesifik örneklerini gösteriyoruz.

HERKES HEDEFTE

Örneklerimizde en az bir şaşırtıcı hedef bulacağınızı düşünüyoruz.

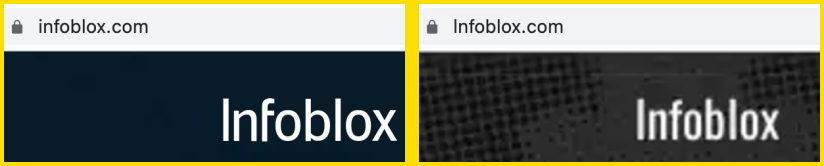
DNS'deki benzer alan adları incelememizden elde ettiğimiz en güçlü bulgulardan biri herkesin bir hedef olduğuydu: beklenen tüm hedeflerin yanı sıra daha küçük şirketler ve hizmetler için de benzer alan adları bulduk. Bu alan adları kötü niyetli kişiler tarafından iş yerinde ve evde bireyleri avlamak için kullanılmaktadır.

Akamai'nin yakın zamanda belirttiği gibi, benzer alan adı kampanyalarının çoğu ancak büyük bir hedef etkilendiğinde basında yer almaktadır.[13] Amacımız bu "tipik" hedeflerin yanı sıra az bildirilen ve gözden kaçan hedeflere ışık tutmaktır. Bu noktayı göstermek için burada birkaç seçkin örnek gösterilmiştir, ancak aynı zamanda farklı sektörler üzerindeki etkiyi de vurgulayacağız. Çeşitli metodolojilerin kullanımı daha sonra daha ayrıntılı olarak ele alınacaktır.

BİZİ HEDEF ALIYORLAR!

Infoblox dünya çapında 2000'den az çalışana sahip mütevazı büyüklükte bir şirkettir.

Topluca DDI olarak bilinen DNS, Dynamic Host Configuration Protocol (DHCP) ve IPAM pazarının büyük bir payına sahip olsak da, bu sektör oldukça spesifiktir ve Infoblox pek bilinen bir isim değildir. Kötü niyetli aktörlerin bizi benzer alan adlarıyla aktif olarak hedeflemeleri bir yana, bizden haberdar olmaları bile şaşırtıcı olsa gerek. Bununla birlikte, hem çalışanlarımızı hem de müşterilerimizi kandırmak için tasarlanmış birçok alan adı bulduk. Avantajlar portalımız da dahil olmak üzere dahili hizmetlerin görünümleri ve ürün adlarımız geçtiğimiz yıl tescil edilmiş.



Şekil 2. Resmi infoblox[.]com web sitesi (L) ile benzer Infoblox[.]com (R) arasındaki logoların karşılaştırması

Infoblox'a ait olmayan bazı kayıtlı alan adları şunlardır:

Homograf **Infoblox[.]com**	Büyük bir "i" taklidi yapmak için küçük bir "L" harfi kullanımı Temmuz 2022'de kaydedildi ve satışa sunulmasına rağmen, site sol üst köşede kurumsal web sitemizdekinden neredeyse ayırt edilemeyen bir render gösteriyor. *Şekil 2'deki bir karşılaştırmaya bakın.*
Typosquat **infobloxbenifits[.]com**	Bu alan adı Çin'de Nisan 2022'de tescil edilmiştir ve çalışanlara sağlanan avantajlar portalımızda küçük bir yazım hatasıdır. Bu alan adı şu anda Bodis ile park edilmiş durumda.
TLD Squat **infoblox[.]info**	Farklı üst düzey alan adı veya TLD, Ağustos 2022'de oldukça suistimal edilen kayıt şirketi Sav[.]com aracılığıyla kaydedildi. Kullanıcıların alan adı satmasına olanak tanıyan dan[.]com'a park edilmiştir.
Combosquat **infobloxgrid[.]com**	Dünya çapında binlerce müşteri tarafından kullanılan amiral gemisi şirket içi ürünümüze benzer bir combosquat. Patentli Grid teknolojimiz, ağ yöneticilerinin çeşitli ağ uygulamalarını tek bir sistemde birleştirmesine olanak tanır. Bu alan adı dan[.]com adresinde de mevcuttur ve Nisan 2022'de kaydedilmiştir.
Combosquat **infoblox-updater[.]com**	Alan adında "güncelleme" veya "destek" gibi yaygın yazılım kelimelerini kullanma tekniğine bir örnek. Bu durumda, bir müşteri, Infoblox sistem güncellemeleriyle ilgili olduğunu düşünerek yanlış bir sistemle bağlantı kurması için kandırılabilir. Kimlik avı alanı veya kötü amaçlı yazılım C2 olarak kullanılabilen bu tür combosquat alan adları için teknoloji şirketlerinin adları veya ürünleri sıklıkla kullanılır. Diğer örnekler arasında dev[.]gitlabs[.]me ve jira[.]atlas-sian[.]net bulunur. Her ikisi de gelişmiş kalıcı tehdit (APT) aktörü Iron Tiger tarafından SysUpdate kötü amaçlı yazılımlarında kullanılır.[14]

Bizimki gibi küçük teknoloji şirketlerini hedef almanın yanı sıra, restoranların, hukuk firmalarının ve diğer küçük işletmelerin aldatıcı türevleri olan çok çeşitli benzerler gördük.

Dahası, tek bir aktör hem tanınmış markaları hem de küçük işletmeleri kurbanları çekmek için kullanabilir. Infoblox'un bir süredir izlediği bir aktör, New York City restoranı Cotenna için benzer alan adları oluşturdu ve muhtemelen ziyaretçileri cezbetmek ve kredi kartlarıyla online rezervasyon yaptırmak için web sitelerini kopyaladı.[15] cotenna[.]nyc sitesi Nisan 2022'de kaydedilmiştir ve cotenna[.]com restoran web sitesinin bir benzeridir. Aynı aktörün Twitter gibi büyük sosyal medya şirketlerini hedef alan benzer alan adları da bulunmaktadır.

Takip eden bölümlerde, günümüzde en yaygın olarak hedef alınan sektörlerin yanı sıra alan adlarının başarılı bir saldırı için kullanılabileceği birçok yoldan bazıları hakkında daha derinlemesine bilgi vereceğiz. Herkes bir hedef olduğu için, 300.000 benzer alan adının incelenmesine dayanarak en çok kötü niyetli faaliyet gördüğümüz alanları vurgulayacağız.

BENZER ALAN ADLARI HERKESİ HEDEFLER

amėricafirst[.]com
ınstagram[.]dev,
caterpillarespaña[.]com
steamcommunltly.net[.]ru
boatairbuds[.]in
secure1-scotiabank[.]com
saveukraine[.]xyz
expressvpn-app[.]com

10K+ ORGS

Temmuz 2022'de Microsoft, kullanıcılardan MFA kimlik bilgilerini gerçek zamanlı olarak çalmak için tasarlanmış AiTM saldırılarının hedefi olduğu konusunda uyardı.

1.600+

Araştırmamız, 1.600'den fazla alan adının kurumsal ve MFA benzer özelliklerinin bir kombinasyonunu içerdiğini buldu.

ÇALIŞANLARI HEDEF ALIYORLAR

Yakın zamana kadar, birçok şirket, çok faktörlü kimlik doğrulama (MFA) kullanımının iç ağlarını kimlik avı saldırılarına karşı koruduğunu düşünüyordu.

Ancak 2023'ün başlarında Coinbase, çalışanlarının şirketin dahili MFA girişine benzer alan adlarını kullanan spear phishing saldırıları tarafından hedef alındığını açıkladı. Bu açıklamayı hızla benzer saldırıların hedefi olan diğer şirketlerden gelen doğrulayıcı raporlar izledi. Mağdur raporlarına dayanarak, kötü niyetli aktörlerin çalışanlara SMS mesajları ve e-postalar gönderdiğini ve onları dahili sistemlerde oturum açmaya çağırdığını biliyoruz. Bazı durumlarda, saldırganın çalışanın web tarayıcısında ziyaret etmesi için bir alan adı sağladığı telefon görüşmeleri de söz konusu olmuştur. Saldırganlar, çalışanlara şirketin gerçek ağıyla etkileşimde olduklarına dair güvence vermek için ortadaki rakip (AitM) tekniklerini kullandı. Çalışanlardan bir MFA kodu istenmiş ve bu kod daha sonra saldırgan tarafından ele geçirilerek dahili sistemlere erişim sağlamak için kullanılmıştır.

Microsoft, Temmuz 2022'de 10.000'den fazla kuruluşun, kullanıcılardan MFA kimlik bilgilerini gerçek zamanlı olarak çalmak için tasarlanmış AitM saldırılarının hedefi olduğu konusunda uyarmıştı.[16] Bu saldırılar Outlook 365 kimlik doğrulamasının kullanımına özeldi, ancak Microsoft ayrıca Şubat 2023'te MFA saldırılarına olanak tanıyan bir kimlik avı kitinin Temmuz 2022'de satışa sunulduğunu ve yaygın olarak kullanıldığını bildirdi.[17] Twilio da dahil olmak üzere diğer şirketler, 2022 yazında benzer saldırıları açıklamıştı, ancak saldırının genişliği, Coinbase ifşaatlarına kadar iyi bir şekilde duyurulmamıştı.[18]

Bu olayı araştırmak için, "mfa", "okta" ve "2fa" gibi anahtar kelimeler kullanarak MFA'yı taklit eden benzer alan adlarının geriye dönük bir analizini gerçekleştirdik. Araştırmamız, yılın başlarında bu saldırılar için önemli sayıda benzer alan adı kullanılmış olmasına rağmen, Temmuz 2022'den itibaren geniş bir hedef yelpazesi ve faaliyetlerde belirgin bir artış olduğunu ortaya koydu. 1.600'den fazla alan adı, kurumsal ve MFA benzeri özelliklerin bir kombinasyonunu içeriyordu. Hedefler Coinbase, Reddit ve Twilio gibi bildirilen büyük şirketlerden büyük bankalara, yazılım şirketlerine, internet servis sağlayıcılarına, devlet kurumlarına ve dünya çapında oyun platformlarına kadar uzanıyordu. Ayrıca hedeflenen, ancak yeterince rapor edilmedi, daha küçük teknoloji şirketleri, marketler ve perakendecilerdi.

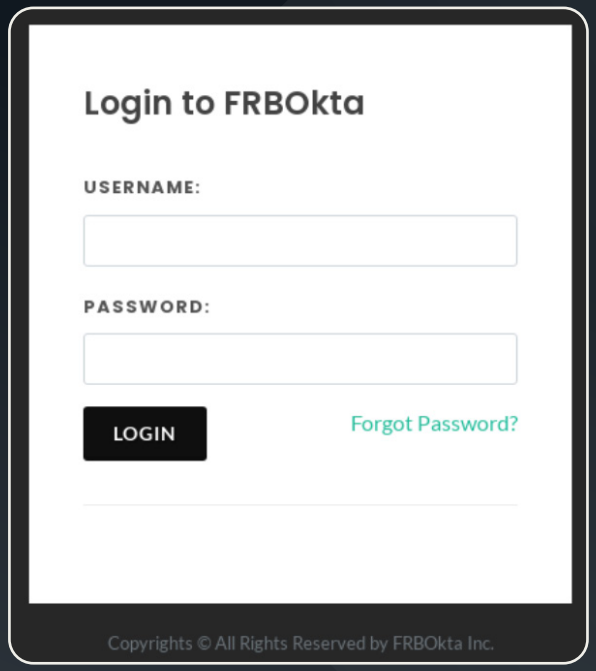
Daha az bilinen hedeflere bir örnek olarak, birden fazla MFA benzer alan adı Western Electricity Coordinating Council'ı (WECC) taklit etmiştir.
WECC, Batı Amerika Birleşik Devletleri'nin büyük bir kısmı için Toplu Elektrik Sistemi güvenilirliğini teşvik eder. Benzerler arasında wecc-okta[.]org, wecc-oktc[.]org ve wecc-okta[.]com vardı. Hepsi Şubat 2023'te tescil edilmiş ve aynı IP adresini paylaşıyor.

Bir başka şaşırtıcı örnek ise Feldman Auto Group'tur. Bu şirket Amerika Birleşik Devletleri'ndeki çeşitli otomobil bayilerinden oluşur.
Şirket, Amerikalı aktör Mark Wahlberg ile bir marka ilişkisine sahip olsa da, orta batıda 18 lokasyonu olan orta ölçekli bir şirkettir.[19] Bu alan adının bir MFA benzeri olan feldmanauto-okta[.]com, Ocak 2023'ün sonlarında tescil edilmiştir.

MFA'ya benzerlerinin şirket hedeflerinden bazıları daha belirsiz.
frb-okta[.]com alan adı, Federal Rezerv Bankası, First Reserve Bank veya Polonyalı giyim şirketi Farbokta gibi bir siteye benzeyen, sıradan bir FRBOkta logosu içeren bir oturum açma istemi gösteriyor.[20] Birçok durumda, hedefin ne olduğundan emin olamıyoruz ve kimlik avı kiti yalnızca kısa bir süre aktif olmuş olabilir. *Kendiniz tahmin edebilmeniz için Şekil 3'e giriş ekran görüntüsünü ekledik.*

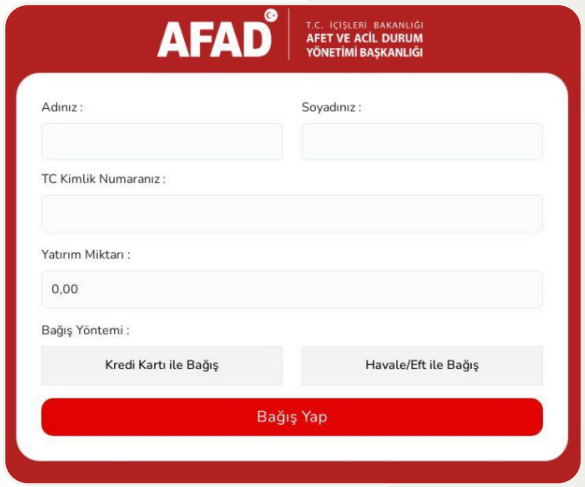
Bu AitM saldırıları, 2022'de tüketicilere, özellikle oyun içi satın alımlarını korumak için MFA kullanan oyun topluluğunda olanlara karşı da kullanıldı.
Yazarlar tarafından bilinen bir vakada, kurban popüler bir çevrimiçi oyunun Twitch canlı yayınından bir siteyi ziyaret etmesi için kandırılmıştır. MFA kimlik bilgilerini girdikten sonra, ev ağına karşı kısa bir hizmet reddi (DoS) saldırısı yaşadı ve bu durum birkaç dakika internet kesintisi yarattı. Oyun hesabına tekrar girebildiğinde tüm satın alma işlemlerinin çalındığını fark etti. *Oyuncuları ebeveynlerinin bodrumunda yaşayan gençler olarak düşünebiliriz, ancak uygulama içi satın alımlara harcanan para miktarı, Roblox'tan Counter-Strike'a kadar oyunları ve oyuncularını kazançlı bir hedef kitlesi haline getiriyor.*

FRBOKTA.COM MFA BENZERI

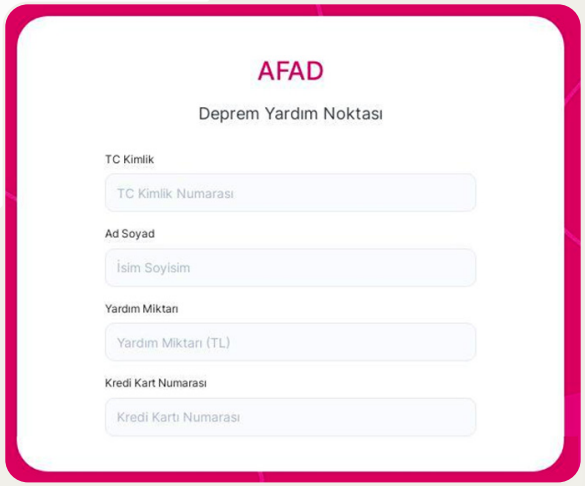


Şekil 3. frb-okta[.]com adresindeki web sitesi, FRBOkta'ya atıfta bulunan, tanımlanamayan bir giriş sayfası göstermektedir. Resim kredisi: URLScan.[21]

TÜRKİYE BAKANLIĞI BENZER SAYFASI



Şekil 4. AFAD benzeri afadestek[.]net
Resim kredisi: DomainTools.



Şekil 5. AFAD benzeri alan adı afadbagislari[.]net
Resim kredisi: DomainTools.

İYİLİK YAPANLARI HEDEF ALIYORLAR

Para çalmak isteyen dolandırıcılar, dünya olaylarını ve felaketleri haksız kazanç sağlamak için kullanmak söz konusu olduğunda genellikle "ilk müdahale edenlerdir".

Infoblox, dolandırıcıların COVID-19 gibi sağlık krizleri veya Rusya'nın Ukrayna'yı işgali gibi haberlerde yer alan herhangi bir olaydan faydalanmakta hızlı davrandıklarını tespit etmiştir. Ne yazık ki 2023, Şubat ayı başlarında Türkiye-Suriye depremi gibi bir insani kriz yaşandı.[22] 6 Şubat'taki ilk depremin ardından, birkaç dolandırıcı alan adı Türkiye İçişleri Bakanlığı Afet ve Acil Durum Yönetimi Başkanlığı'nın (AFAD) web sitelerini taklit etmeye çalıştı. Bu alan adları, afad[.]gov[.]tr meşru alan adı gibi görünmeye çalışarak tam nitelikli alan adındaki 'AFAD' kelimesinden yararlanmıştır. Aşağıdaki örnekler yeni kaydedilmiş alan adlarıdır ve uzun bir tam nitelikli alan adına (FQDN) sahip olsalar da, hepsi 'AFAD' ile başlar.

Daha uzun FQDN'lerin kullanılması, dolandırıcılara birden fazla AFAD temalı kampanyada kullanmak üzere meşru alan adının daha fazla permütasyonunu sunar:

- **afad-kizilay[.]yardim-yap[.]net**
- **afad-kizilay[.]yardimbagis[.]net**
- **afad-online-odeme-bagis[.]net**
- **afadtr[.]bagislama[.]net**

Combosquatting'e ek olarak, bu sitelerden bazıları ziyaretçileri sitelere bağış yapmaları için kandırmaya yardımcı olmak amacıyla yasal AFAD logosunu kullanmaktadır. Örneğin sahte site afadestek[.]net 7 Şubat'ta tescil edildi ve *Şekil 4*'te gösterildiği gibi meşru Türk AFAD sitesine benzer bir web tasarımı sergiledi. Makine çevirisine göre, elektronik para transferi, kredi kartı veya havale yoluyla bağış toplamanın yanı sıra ad ve soyad ve ulusal kimlik numaraları gibi kişisel bilgileri topladığı görülüyor.

Diğer sahte alan adları resmi AFAD logosunu kullanma zahmetine girmemiş ve bağışçılardan alabilecekleri para miktarını en üst düzeye çıkarmak için hızlıca oluşturulmuştur. Her ikisi de aynı IP adresinde barındırılan afadbagislari[.]net ve afadyardimyap[.]net buna iki örnektir. Benzerleri için özel altyapı yaygındır ve daha sonra daha ayrıntılı olarak ele alınacaktır. Her iki site de *Şekil 5*'te gösterilen aynı düzen ve içeriğe sahiptir ve kredi kartı ödemeleri yoluyla deprem yardımı için bağış istemektedir.

KRİPTOYU HEDEF ALIYORLAR

Hızlı para kazanmak isteyen dolandırıcıların yanı sıra benzer alan adları, kimlik bilgilerini çalmak için yoğun olarak kullanılır.

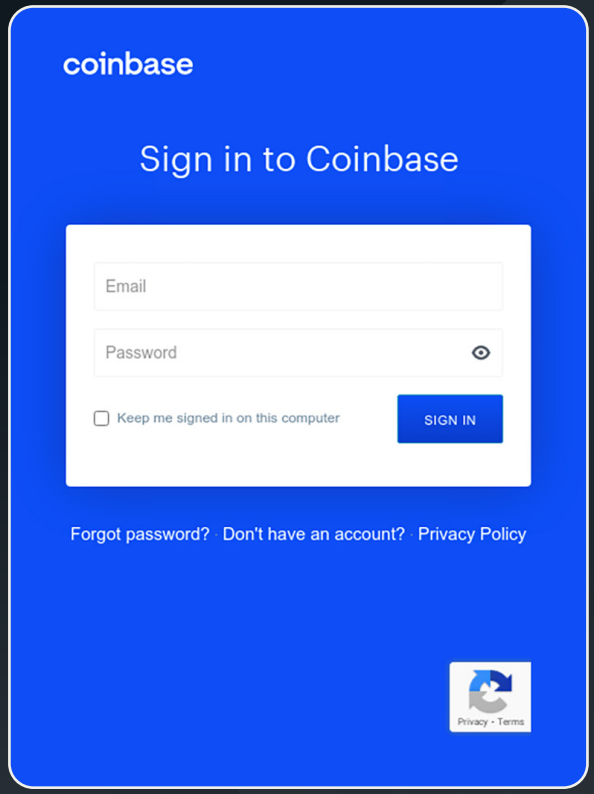
Kullanıcıların kimlik bilgilerini ele geçirmeye çalışan genel bir "kimlik avı" web sitesi dendiğinde muhtemelen en sıradan insanın aklına gelen şey benzer bir alan adıdır. Kripto paraların popülerliğinin artmasıyla birlikte saldırganlar pazar yerleri, cüzdanlar ve borsalar da dahil olmak üzere bu finansal hizmetleri hedef almaktadır. ABD merkezli popüler borsa Coinbase için çok ikna edici birkaç benzer site bulduk. Böyle bir site *Şekil 6*'da gösterilmektedir.[23]

Örneğin aşağıdaki tabloda yer alan alan adları Ocak 2023'te tescil edilmiştir:

Tablo 1. Coinbase kripto para borsasına benzeyen alan adlarına örnekler.	
securefinancialcoinbase[.]com	reconfirminfocoinbase[.]com
secureaccountreverify-coinbase[.]com	reconfirmaccount-coinbase[.]com
secure4-coinbase[.]com	kyc-reverifycoinbase[.]com
secure2reconfirm-accountcoinbase[.]com	ap-coinbase[.]com
secure2financial-coinbase[.]com	accountupdate-financialcoibase[.]com
secure2-financialcoinbase[.]com	2farecoverycoinbase[.]com
secure-2faupdatecoinbase[.]com	recovery-financialcoinbase[.]com
2fa-accountupdatecoinbase[.]com	2fa-updatecoinbase[.]com

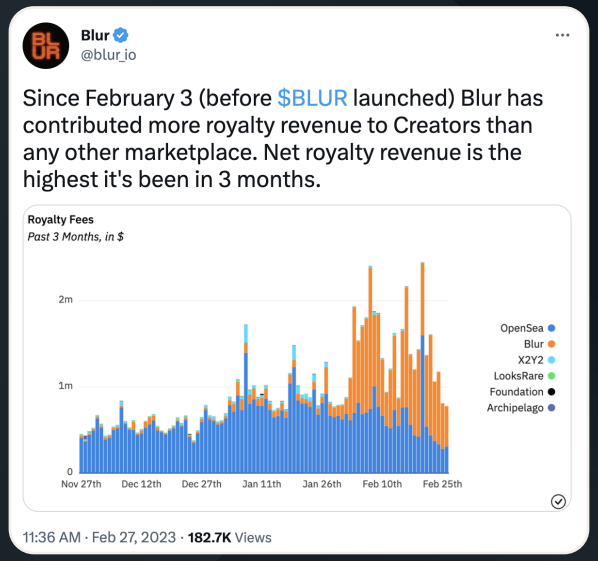
İşlemleri Şubat 2023'te 2 milyar doların üzerine ulaşan takas edilemeyen tokenlerin (NFT'ler) büyümesiyle birlikte, aktörler yatırımcılardan para çalma çabalarında geleneksel kripto para biriminin ötesine hızla genişledi.[24]
Örnek olarak, Blur pazaryeri Ekim 2022'de açıldı ve Blur token birkaç ay sonra piyasaya sürüldü. Mayıs 2022'den bu yana NFT'lere rekor bir yatırım yapıldı.[25] Ürün lansmanından kısa bir süre sonra Blur benzerlerini görmeye başladık ve ardından platformun popülaritesi arttıkça benzerlerde çarpıcı bir artış gördük.

COINBASE BENZERİ



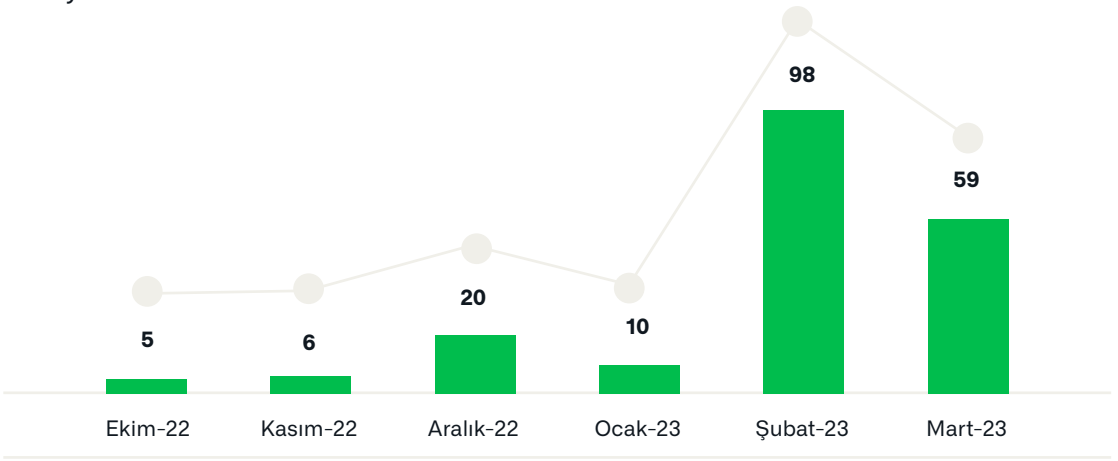
Şekil 6. Coinbase benzeri click-coinbase[.]com
Resim kredisi: DomainTools.

BLUR NFT BENZERİ



Şekil 7. Blur NFT piyasası, Şubat 2023'te görülen 2 milyar dolarlık NFT işlemlerinin önde gelen itici güçleri arasındadır.[26] Resim kredisi: Infoblox

Blur Token'ın 14 Şubat 2023'te piyasaya sürülmesine kadar, Blur'le ilgili benzerlerin sayısında beş ila altı kat artış gördük. Miktar düşerken bile Mart 2023'te bir şekilde ortaya çıkan bu model, aktörlerin kısa yoldan para kazanmak için kripto dünyasındaki trendlere ayak uydurma istekliliğini gösteriyor.



Şekil 8. Pazarın Ekim 2022'deki duyurusundan bu yana Blur ile ilgili benzerliklerde ciddi artış.

Infoblox, kripto para birimi ile ilgili benzerlerde uzmanlaşmış birden fazla aktörü izler. Bu aktörler, Blur ve rakipleri Yuga Labs, APEcoin'in ve popüler NFT Bored Ape Collection'ın sahibi de dahil olmak üzere pazardaki tüm büyük kuruluşları hedefliyor. Aşağıdaki tabloda, bu alanların küçük bir örneğini sunuyoruz. Bu aktörler tarafından kullanılan teknikler arasında üst düzey alan adında (TLD) basit değişiklikler, tek bir harfin eklenmesi ve tanınması özellikle zor olabilen Unicode alan adları bulunmaktadır. Aşağıdaki tabloda apecoíns[.]com'da "i" harfinin üzerinde bir aksan olduğuna dikkat edin. DNS'de bu alan, benzer bir şekilde tanınması biraz zor olan xn--apecons-cza[.]com'a benziyor, ancak bir web tarayıcısında orijinalinden neredeyse ayırt edilemez.

Tablo 2. Blur token ve Yuga Labs benzeri alan adı örnekleri.

Blur benzeri alan adları [blur.io]	**Yuga Labs benzeri alan adları [yuga.com]**
blurclaim[.]com	yugaslabs[.]com
blurdrop[.]com	apecoíns[.]com
blurnft[.]pw	apecoinstake[.]world
blur-nft[.]org	yugas[.]app
blur-coin[.]com	ape-claim[.]com

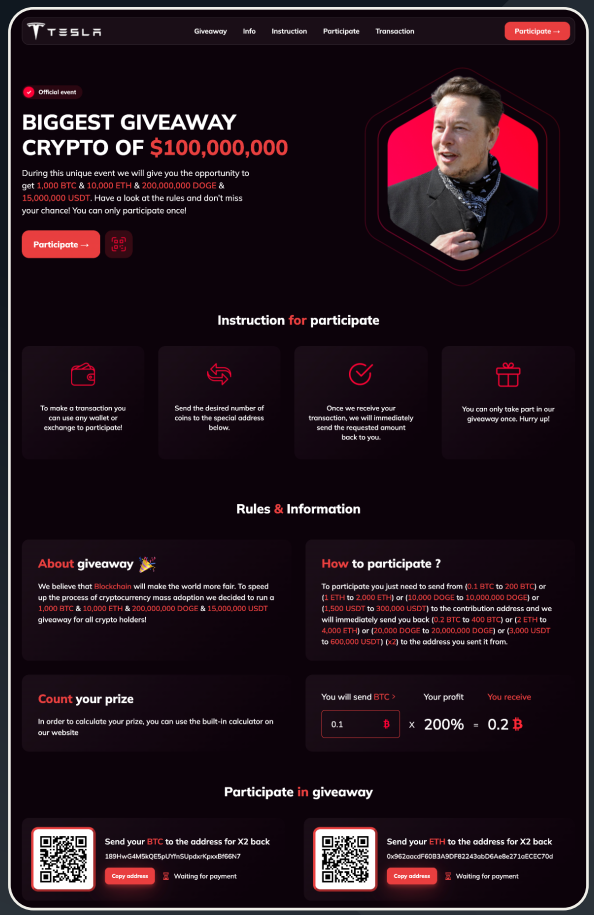
YouTube'u hedeflerini kendi alanlarına çekmek için bir vektör olarak kullanan daha az geleneksel kripto para birimi ile ilgili benzer alan adları da vardır.

Bu planlar, tehdit aktörlerinin, meşru ürünlerle ilgili görünen sahte sponsorluk tekliflerini kullanarak popüler YouTube içerik oluşturucularına saldırmasıyla başlar.[27] E-postalar, içerik oluşturucudan, tanıtılan yazılımın bir kopyası veya sponsorluk sözleşmesi içeren bir PDF dosyası gibi sponsorluk teklifiyle ilgili olduğu iddia edilen bir dosyayı indirip açmasını ister.[28] Gerçekte, bu dosyalar açıldığında kurbanın tarayıcısından oturum çerezlerini çalan kötü amaçlı yazılım yükleridir. Çalınan çerezler çok faktörlü kimlik doğrulama etkinleştirilse bile saldırganın kurbanın YouTube hesabına erişmesine imkan sağlar.

Saldırgan, içerik oluşturucunun YouTube hesabına eriştikten sonra, kanalın adını ve profil fotoğrafını saldırının temasıyla eşleşecek şekilde değiştirerek kanalın saldırıya uğradığı gerçeğini gizlemeye çalışır; bu genellikle Elon Musk veya onun şirketlerinden biriyle ilgilidir.[29]
Saldırgan ayrıca izlerini daha da gizlemek için kanalın mevcut videolarını silebilir veya gizleyebilir. Saldırgan daha sonra kanalın mevcut abonelerini cezbetmek için Elon Musk'ın Ark Invest konuşması gibi kripto parayla ilgili bir videonun düzenlenmiş bir versiyonunu yayınlamaya başlar.

Bu düzenlenmiş videolar, kullanıcıları saldırganın kripto parayla ilgili benzer alan adını ziyaret etmeye yönlendiren bir metin katmanı içerir ve alanın bağlantısı da akışın açıklamasına dahil edilir.
Alan adları, kurbanlardan belirli bir cüzdan adresine belirli bir miktarda kripto para göndermelerini isteyen ve karşılığında bu miktarın iki katını alacakları vaadinde bulunan standart "paranızı ikiye katlayın" dolandırıcılıklarıdır. Bu saldırılarda, benzer alan adının amacı, temasını düzenlenen video ve yeniden markalanan YouTube kanalıyla eşleştirerek teklifin inandırıcılığını artırmaktır.

TESLA BENZERİ



Şekil 9. Kripto para birimi ile ilgili Tesla benzer alan adı tesla-online[.]net, kullanıcılardan karşılığında iki kat daha fazla almak için belirli adreslere kripto para göndermelerini ister. Resim kredisi: Infoblox

SOSYAL MEDYA VE MOBİL KULLANICILARI HEDEFLİYORLAR

Apple gibi büyük markaların yanı sıra Instagram ve Twitter gibi sosyal medya platformları da kimlik avı saldırılarının popüler hedefleridir.

Her popüler marka ve hizmet bu saldırılarda sürekli olarak hedefleniyor, ancak mevcut tehdidin bir örneği olarak bu üç markadan sadece birkaç örnek kullanacağız. Kimlik bilgisi toplama yeni bir şey değil; sosyal medya ve Apple ID gibi evrensel kimlik platformları ortaya çıkmadan önce, kötü niyetli kişiler e-posta hesabınıza girmeye çalışıyordu. Ancak, sosyal medya ve evrensel kimlik platformlarının artık hayatımızla ne kadar iç içe geçtiği düşünüldüğünde, bu benzerler sürekli bir tehdit oluşturuyor.

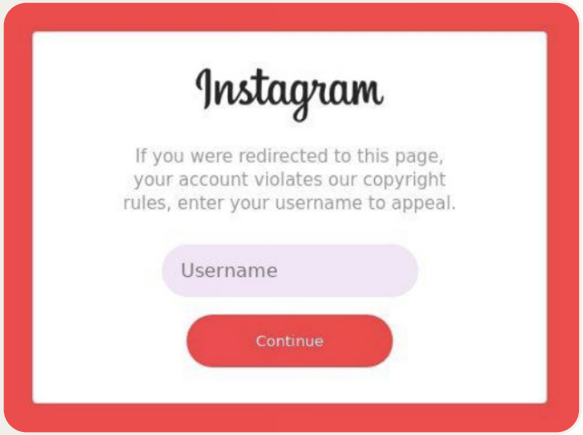
Tehdit aktörleri sadece fenomenlerin ve ünlülerin hesaplarının değil, herkesin sosyal medya hesabının peşine düşecektir. Instagram için pek çok benzer alan adı var. Bunlardan bazıları combosquat, diğerleri homograflar. Bu tür alan adları genellikle eşzamanlı olarak kaydedilen alan adlarından oluşan kümeler halinde ortaya çıkmaktadır ve bu da bunların bir DDGA kullanılarak oluşturulan koordineli bir kampanyanın parçası olduğunu düşündürmektedir. Aşağıdaki örneklerin tümü, markayı yardım ve geri bildirim gibi kelimelerle birleştiren bir Instagram setinin parçasıdır.

Tablo 3. Instagram destek benzer alan adlarına örnekler.

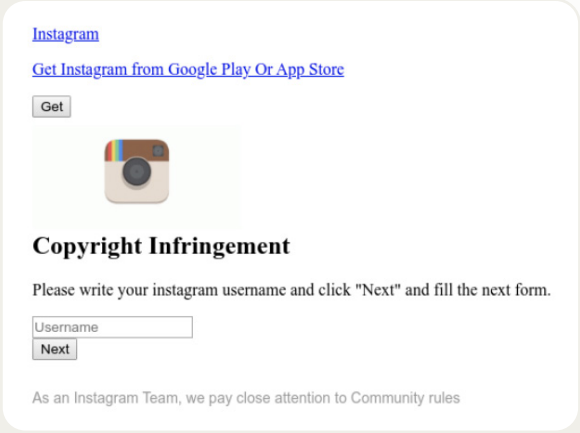
help-instagram-notice[.]com	help-instagram-about[.]com
feedback-instagram[.]com	help-Instagram-notice[.]com
help-Instagram-about[.]com	help-Instagram-notice[.]gq

Bu alan adlarındaki içerik, kullanıcının Instagram'ın telif hakkı kurallarını ihlal ettiğini iddia ediyor ve kullanıcıdan karara itiraz etmek için kullanıcı adını girmesini ister; *bkz. Şekil 10 ve 11.*

İNSTAGRAM BENZERİ

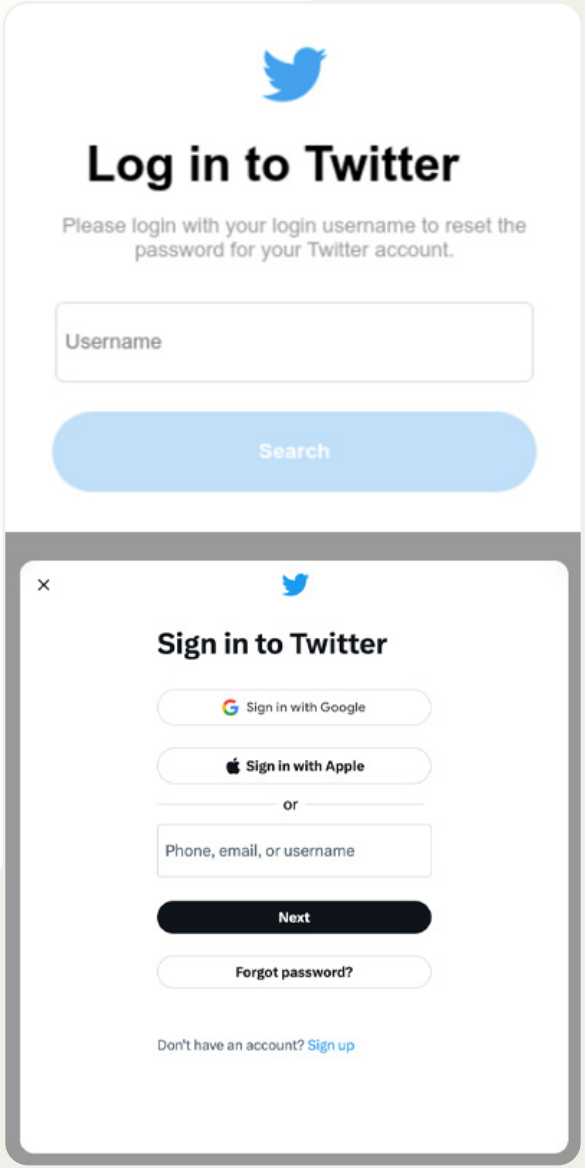


Şekil 10. Instagram benzeri help-Instagram-notice[.]com telif hakkı ihlali itirazı harekete geçirici mesajı görüntülüyor. Resim kredisi: DomainTools.[30z]



Şekil 11. Instagram benzeri help-instagram-about[.]com, başka bir telif hakkı ihlali itiraz harekete geçirici mesajı gösteriyor. Resim kredisi: URLScan.[31]

TWITTER BENZERİ



Şekil 12. Twitter'da ikna edici şifre sıfırlama portalı benzeri help-twitter-center[.]net. Kimlik avı görüntüsü üstte, meşru olan altta. Resim kredisi: DomainTools.[32]

Diğer Instagram benzerleri, büyük "i" harfi yerine küçük "L" harfi kullanarak gıpta edilen "mavi onay işaretini" (Instagram'ın kamuya mal olmuş bir kişi olarak doğrulama yaklaşımı) hedefliyor. İronik bir şekilde, Instagram mavi onay işaretini tanınmış kişilikler veya şirketler için taklitçilikle mücadele etmenin bir yolu olarak tanıttı. *Kötü niyetli aktörlerin benzerleri kullanarak benzerlik karşıtı çözümleri hedef almasına aldırmayın.*

Bazı örnekler:

Tablo 4. Instagram doğrulamaya benzeyen alan adlarına örnekler.	
Instagram-blueticket-form[.]ml	Instagram-contactbluebadge[.]ga
Instagram-verification-badges-service[.]com	Instagrambluetickverifcation[.]cf
Instagramverifybadge-contact[.]cf	Instagram-badgecentre[.]gq

Instagram benzerlerini takip ederken, saldırganların tüm yumurtalarını tek bir sosyal medya sepetine koymadıklarını gördük.

Twitter için benzer alan adları, Instagram "telif hakkı ihlali" görünümleriyle birlikte de barındırıldı. Bu Twitter benerleri, kullanıcıların kimlik bilgileri için kimlik avı yapan combosquat alanlarıydı ve açılış sayfaları meşru bir şifre sıfırlama portalı gibi görünüyordu; *bkz. Şekil 12.*

Sosyal medya benzerlerine ek olarak, araştırmamız sırasında Apple'ın Apple aygıtları arasında bulut depolama ve senkronizasyon sunan bulut hizmeti iCloud'un benzerlerini de sık sık gördük. Bu alan adları nispeten az sayıda anahtar kelimeden yararlanmıştır; en sık "apple", "findmy", "id" ve "icloud" kelimelerini gözlemledik. Apple ile ilgili benzer alan adları da sayıca çok fazlaydı.

Aşağıda, İspanyolca konuşan kullanıcıları hedefliyor gibi görünen bazıları da dahil olmak üzere birkaç örnek bulunmaktadır:

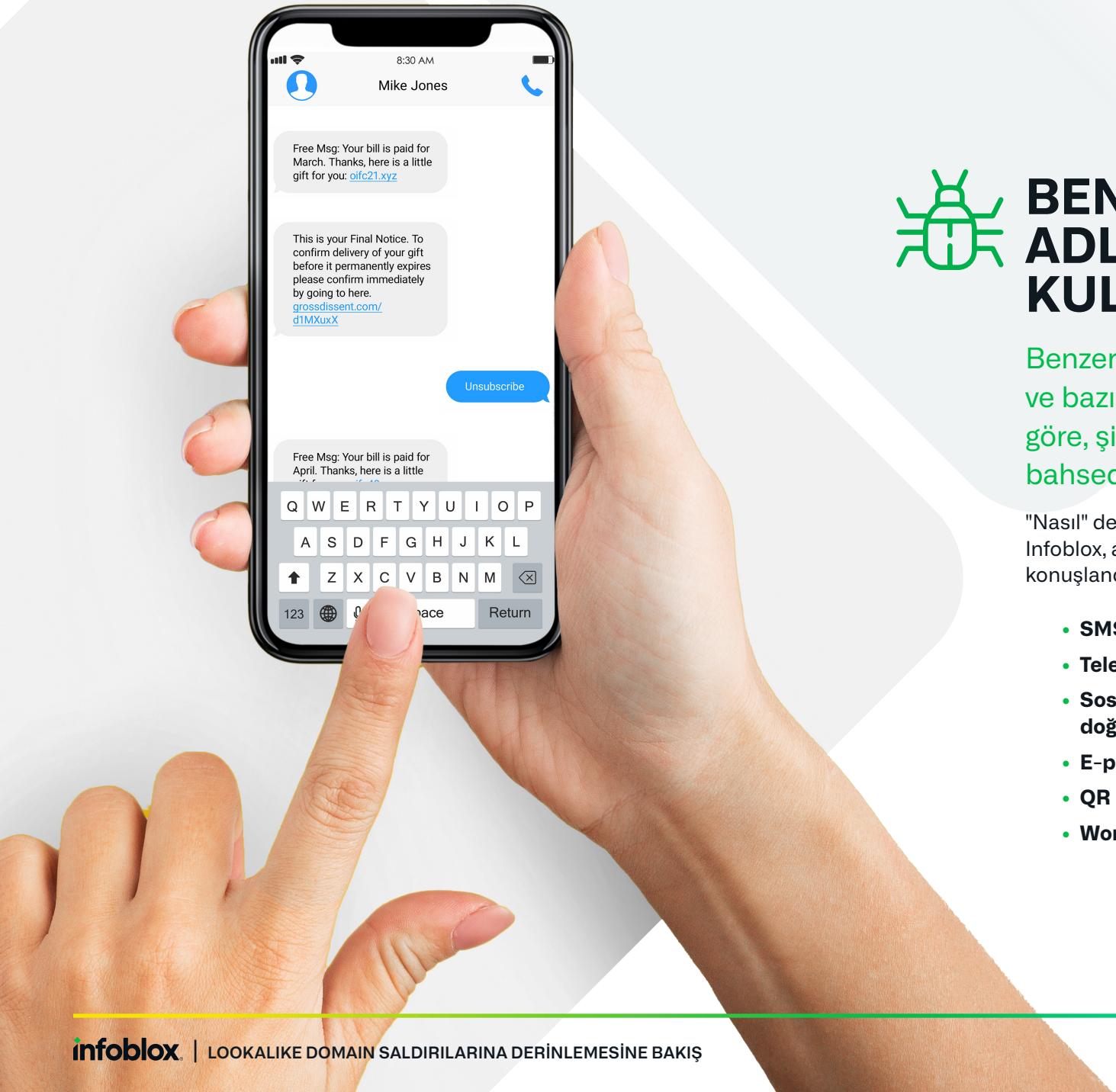
Tablo 5. Apple ile ilgili hizmetleri hedefleyen benzer alan adları.	
supportid-apple[.]com	sopport-apple[.]com
soporte-latam[.]us	soporte-appleid[.]com
Icloud-web-app[.]com	icloud-fndmy[.]com

HERKESİ HEDEF ALIYORLAR

Algılama algoritmalarımız her gün binlerce yeni benzer alan adı tespit etmektedir. Kötü niyetli kişilerin para veya kimlik çalabileceği büyük veya küçük her şirket veya hizmet hedef alınacaktır. Bu bölümü, genel olarak gözlemlediğimiz benzer alan adları ve bunların hedefleriyle kapatacağız.

Tablo 6. Benzer alan adları ve hedefleri.

Benzer alan adları	Benzer hedef
mee6bot[.]ru	Discord bot, Mee6
vulcan[.]pm	Discord bot, Vulcan
o365-outlook[.]com, ms-o365[.]com, o365-outlook[.]com, https-o365[.]com	Microsoft Office 365
myato-refund[.]online	Avustralya Vergi Dairesi
checkscam22[.]com, checkscams[.]online, checkscammer[.]xyz	Dolandırıcılık kontrolü web siteleri
xpressvpn[.]business, expressvpn-app[.]com, expressvpn-okta[.]com	Express VPN
anpost-paymentduty[.]com, ups-pay-deliveryfee[.]info, caddeliverypostca[.]com	Posta ve teslimat hizmetleri
crarebate-info[.]com	Kanada vergi iadesi
ebl-ch[.]com	İsviçreli enerji şirketi EBL
op-fi-palvelut[.]co, op-fi-io[.]in	Op[.]fi, Finlandiya dijital bankacılık ve sigorta hizmeti
boatairbuds[.]in, boatbudsmusc[.]in, boatflashsale[.]in, boatmusicairbud[.]in	Hintli teknoloji şirketi BoAt
pumauaeshoes[.]com, pumanzsale[.]com, pumaireland[.]com, vejaoutletcanada[.]ca	Ayakkabı şirketleri
secure1-scotiabank[.]com,r-scotiabank[.]com, chasebank-jpm[.]com, thetrustnationalbank[.]com, amėricafirst[.]com	Bankalar
sprint-ldg[.]com, tds-telecom[.]com, teistra[.]ne, 1111systems-okta[.]com, t-mobile-okta[.]us, vzw-sso[.]com	İnternet ve bulut hizmeti sağlayıcıları
sso-authentication[.]de, sso-securelogin[.]com, service-sys-2fa[.]com	Çok faktörlü kimlik doğrulama ve alan adlarında tek oturum açma



BENZER ALAN ADLARI NASIL KULLANILIR?

Benzer alan adlarının ne olduğunu ve bazı örnek hedefleri ele aldığımıza göre, şimdi nasıl kullanıldıklarından bahsedelim.

"Nasıl" derken, dağıtım yöntemlerini kastediyoruz. Infoblox, aşağıdakiler gibi çeşitli şekillerde konuşlandırılmış benzer alan adları belirledi:

- **SMS mesajları**
- **Telefon çağrıları**
- **Sosyal medya sitelerindeki doğrudan mesajlar**
- **E-postalar**
- **QR kodlarına gömülü**
- **World Wide Web'deki Alan Adları**

MESAJ GÖNDERİYORLAR

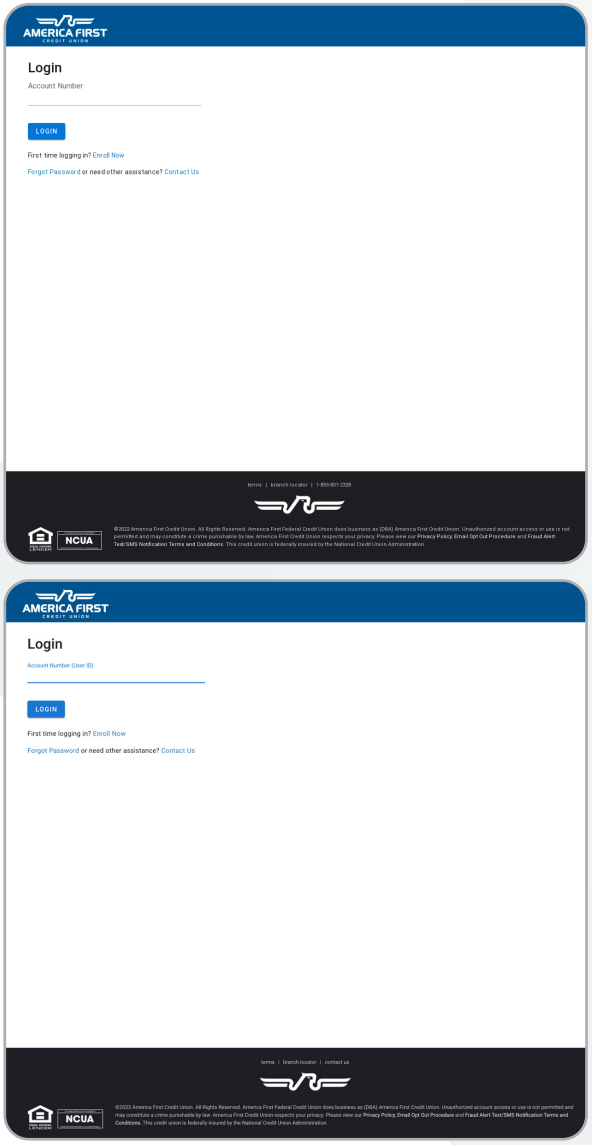
Cep telefonu kısa mesajlarına (SMS) yönelik spam filtrelerindeki gelişmelere rağmen, genellikle smishing olarak adlandırılan kimlik avı mesajlarını iletmek için SMS kullanımı artmaya devam etmektedir.

Saldırganlar çok sayıda mesajı hızlı bir şekilde dağıtarak e e-posta kimlik avı saldırılarına karşı korunmak için uygulanan bazı güvenlik mekanizmalarından kaçınabilir. SMS, hem geniş çaplı tüketici saldırılarında hem de kurumsal çalışanlara yönelik dar kapsamlı spearphishing saldırılarında kullanılmaktadır. Bu bölümde, tüketicilere ve kamu çalışanlarına saldırmak için SMS ve benzer alan adlarını kullanan iki tehdit aktörünü açıklayacağız.

Infoblox, neredeyse bir yıldır OpenTangle adını verdiğimiz ısrarcı bir benzer smishing saldırganını. Bildiğimiz kadarıyla bu saldırgan başka bir yerde rapor edilmemiştir. OpenTangle başlangıçta finans kurumları, internet sağlayıcıları ve çevrimiçi perakendecilerin benzerlerini kullanarak Batılı tüketicileri hedef aldı. Yakın zamanda devlet çalışanlarını ve yüklenicileri hedef almaya başladı. Yaklaşık iki yıl önce faaliyet göstermeye başladıklarından beri OpenTangle tarafından kontrol edilen 1.500'den fazla benzer alan adından haberdarız. OpenTangle'ın alan adlarından bazıları mtbsuportz0610[.]com, americafirst0nline[.]com ve mygov03-ato[.]com.

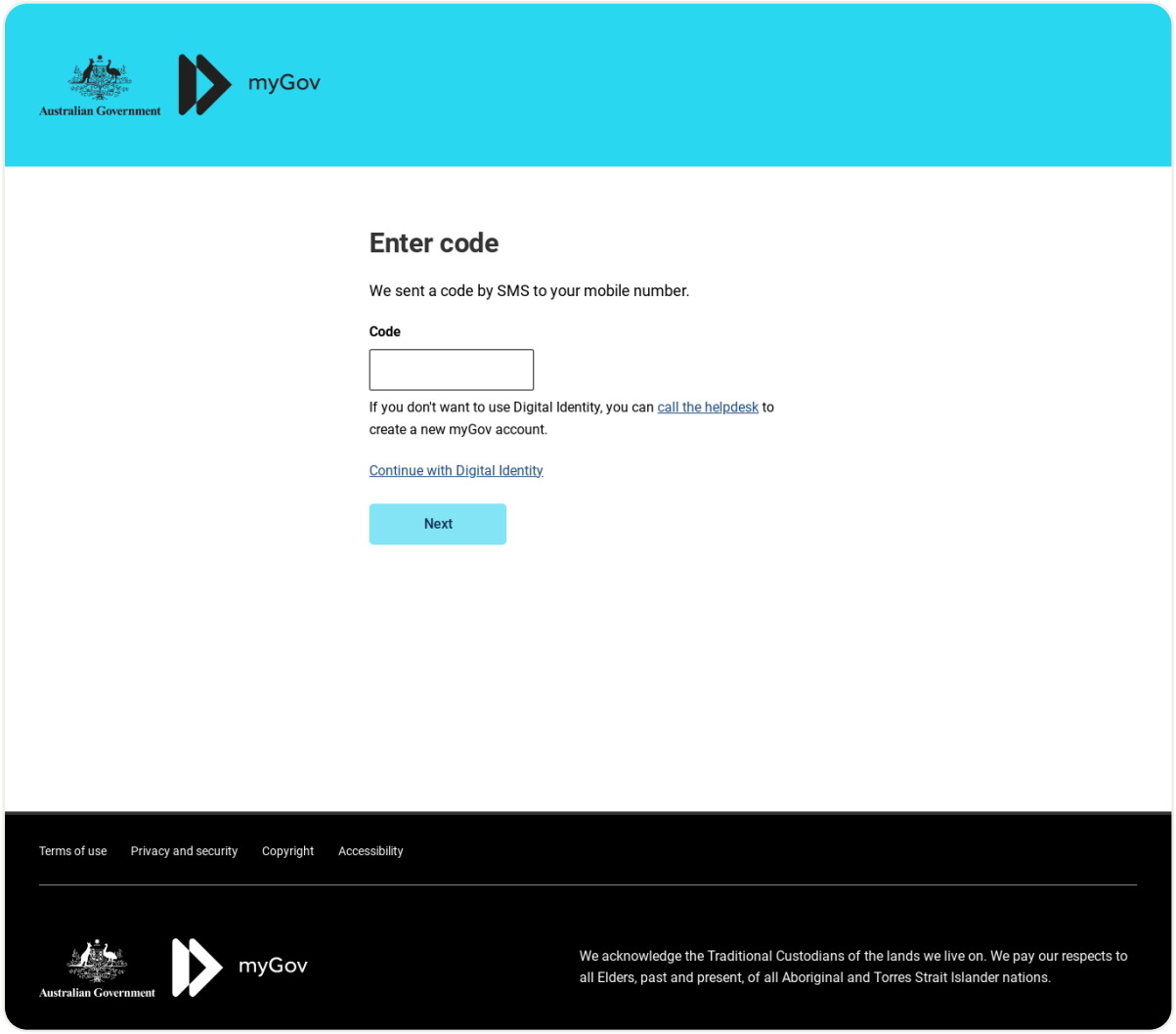
Farklı benzerlik teknikleri kullandıklarına dikkat edin.

Bu makalenin yazarlarından biri, OpenTangle'dan, yazarın hiçbir bağlantısı olmayan M&T Bank'ın benzerleri de dahil olmak üzere çok sayıda metin mesaj aldı. OpenTangle, kampanyalarının başlarında, belki de şaşırtmanın başarılı olacağını umarak, smishing metinlerine kısaltılmış URL bağlantıları ekledi. Ancak Mayıs 2022 itibarıyla benzer alan adlarına geçiş yaptılar. *Şekil 13*, kullanıcının kimlik bilgilerini talep ettikleri bankacılık kampanyalarından birinin bir örneğini göstermektedir.



Şekil 13. America First Credit Union hesap sahiplerini hedefleyen americafirst0nline[.]com alan adındaki bir kimlik avı sayfası. Üstteki resim kimlik avı sayfası, alttaki resim meşru sayfadır. Resim kredisi: URLScan.[33]

OpenTangle geçtiğimiz yıl içinde AitM kimlik avı kitlerini kullanarak MFA'yı istismar etmeye başladı. Daha önceki kampanyalarında standart kimlik avı giriş sayfaları kullanmış ve genellikle tüketicileri hedef almış olsalar da, *Şekil 14* kampanyalarını nasıl geliştirdiklerine dair bir örnek göstermektedir. Bu durumda Avustralya Devleti myGov hesap sahiplerini hedef almakta ve sadece giriş bilgileri yerine bir MFA kodu talep etmektedirler. Ayrıca, 2022'de kullanıcıları kötü amaçlı web sitelerini ziyaret etmeye ikna etmenin bir yolu olarak ortaya çıkan bir başka teknik olan yardım masasını aramak için bir bağlantı da eklediler.



Şekil 14. Avustralya Devleti'nin devlet bulutu için çevrimiçi portalı myGov'u taklit eden OpenTangle benzeri alan adı www.mygovsupport-ato[.]com. Resim kredisi: URLScan.[34]

Scamélie, benzerlerini yaymak için smishing mesajlarını kullanan bir başka saldırgan örneğidir.

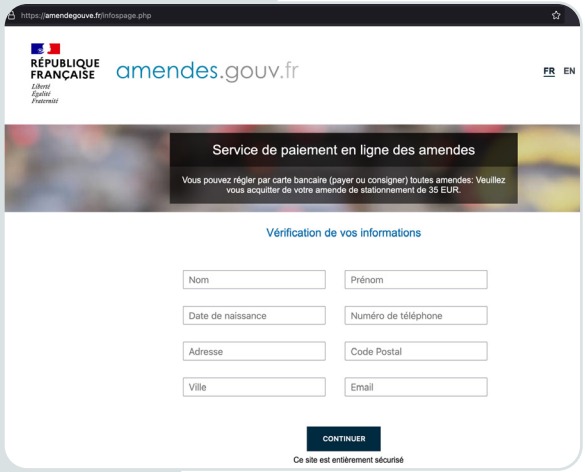
Scamélie olarak adlandırdığımız saldırgan, Fransızca konuşulan ülkelerden gelen ve özellikle Fransızca konuşulan ülkeleri hedef alan uzun bir dolandırıcılık listesine dahil olan gevşek bir şekilde bağlı gruplar ve bireylerden oluşuyor. Ayrıca Avrupa ve BAE genelinde daha genel bir hedefleme yaptıklarını da gördük. Scamélie'nin benzer alan adları öncelikle ISP'lerin, bankaların, devlet hizmetlerinin ve dağıtım şirketlerinin kimliğine bürünür. Grubun gevşek bağlılığı nedeniyle, seyahat şirketleri, spor giyim şirketleri ve marketler gibi daha az beklenen şirketler için dolandırıcılık da gördük.

Scamélie'nin benzer alan adları genellikle büyük bulut sağlayıcılarında veya "kurşun geçirmez" barındırma şirketlerinde barındırılır. Bazı durumlarda, dolandırıcılar kendi sağlayıcılarını kurmuşlardır veya diğer bağlı olmayan dolandırıcılar tarafından kurulan barındırma sağlayıcılarını kullanırlar. Hem hedeflenen alan adlarının hem de çalıntı kimliklerle kaydedilen ve sanal kredi kartları veya kripto para birimleriyle ödenen genel amaçlı alan adlarının (hesabım, sorun-giderme vb.) olduğunu gördük.

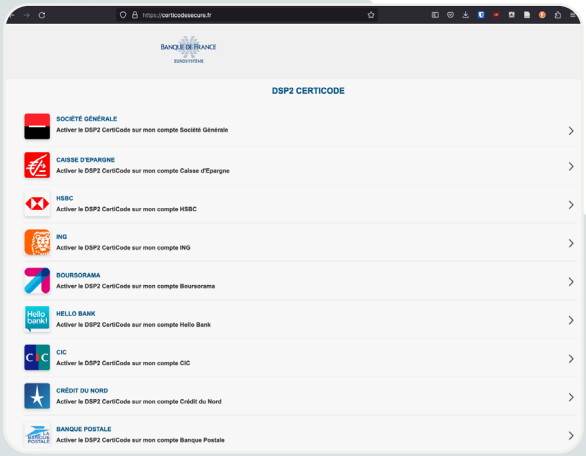
Saldırganlar kredi kartı bilgilerini çaldıktan sonra, kurbanın bankasının veya kredi kartı veren kuruluşun bir çalışanı gibi davranarak onu arar.
Kurbanın kredi kartı bilgilerinin çalındığını ancak sorunu çözmeye yardımcı olacaklarını söylerler. Arayan kişi daha sonra kurbana, hesap güvenliği için arayan kişiye geri okunması gereken iki MFA kodu verileceğini söyler. Gerçekte, saldırganın kurbandan gerçek zamanlı olarak para çalmak için MFA kodlarına ihtiyacı vardır. İlk MFA kodu havale tutarını artırır ve ikincisi işlemin gerçekleşmesini sağlar. Dolandırıcılar, aramalarının etkinliğini artırmak amacıyla arayanlar için ideal olarak genç kadınlardan ve/veya anadili İngilizce olan bir kişide şüphe uyandırmayacak şekilde Fransızca konuşan bireylerden oluşan bir kadro istihdam eder.

Örgütlenmemiş bir grup olan Scamélie'nin izlenmesi ve analiz edilmesi zordur. Çoğunlukla kurbanlarının bilgilerini gece vaktinde çalıyor ve birkaç saat ya da gün sonra alan adlarını kapatıyorlar. Güvenlik araştırmacılarını daha fazla engellemek için anti-bot ve anti-scraping komut dosyaları kullanıyorlar.

SCAMÉLIE BENZERLİK ÖRNEKLERİ



Şekil 15. Scamélie benzer alan adı amendegouve[.]fr bir Fransız devlet hizmet portalını taklit ediyor. Resim kredisi: Infoblox.



Şekil 16. Scamélie benzer sitesi certicodesecure[.]fr bir Fransız bankacılık hizmetini taklit ediyor ve kurbanları banka hesap bilgilerini ilişkilendirmeye davet ediyor. Resim kredisi: Infoblox.

GELENEKSEL TELEFON GÖRÜŞMELERİNİ KULLANIYORLAR

Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA), 26 Ocak 2023'te uzaktan izleme ve yönetim yazılımının (RMM) kötü amaçlı kullanımı hakkında bir Siber Güvenlik Danışmanı (CSA) yayınladı.[35]

CISA, Ekim 2022'de kötü niyetli kişilerin telefon numarası içeren kimlik avı e-postaları gönderdiği ve kullanıcılardan aramalarını istediği bir kampanya tespit etti. E-posta bir müşteri destek mesajı olarak tasarlanmıştı ve kullanıcılar telefon numarasını aradığında, aktörler onları kötü niyetli bir alan adını ziyaret etmeye yönlendirdi. Kullanıcı bunu yaptığında, çalıştırılabilir bir dosya indirildi ve ardından ek RMM yazılımının indirildiği ikinci bir kötü amaçlı alanla bağlantı kuruldu. Bu yazılım (AnyDesk ve ScreenConnect) yasaldı, ancak kalıcılık için saldırganın RMM sunucusuna bağlanmak üzere önceden yapılandırılmıştı.

Kullanılan alan adları, iyi bilinen hizmetlerin benzerleridir; senaryoları ve arayanların kişiliklerini oluşturmak için kullanılan ek sosyal mühendislik nedeniyle, telefonla aranan mağdurlar için alan adını kabul etme olasılığı daha da yüksektir. Verilerimiz üzerinde geriye dönük bir inceleme gerçekleştirdik ve saldırganın CSA'nın belirttiğinden daha uzun süredir aktif olduğuna dair kanıtlar bulduk.[36] Bu kampanyalar en azından 2021 İlkbaharından beri, yani CISA ve Silent Push'un ayrı bir makalede açıkladığı olaylardan bir yıldan fazla bir süre önce aktift. Ayrıca bazı alan adlarının yeniden kullanıldığını gördük. Örneğin amzsupport[.]live alan adını kullanan Amazon benzeri, Nisan 2020'de aktif bir kampanyanın parçasıydı ve daha sonra Ekim 2021'de tekrar kullanıldı.

2023'ün başlarında dahili kurumsal sistemlerinin MFA korumasına yönelik saldırılar gün yüzüne çıktığında, bazı durumlarda dolandırıcıların kurbanı kendi BT departmanları gibi davranarak aradıkları ortaya çıktı. Bu, kurban ilk soruya yanıt vermedikten sonra yapılmış ve kullanıcının benzer alan adını ziyaret etme ihtiyacına daha fazla meşruiyet sağlamak için kullanılmıştır. Buna uyan kullanıcılar, saldırganın kurumsal kimlik bilgilerini çalmasını sağladı.

SPAM GÖNDERİYORLAR

Kurnaz dolandırıcıların benzer alan adlarını dağıtmak ve kurbanları tuzağa düşürmek için smishing ve telefon aramalarını kullandığını görmüş olsak da, kimlik avı e-postasının modası hiç geçmedi.

Infoblox her gün on binlerce kötü amaçlı spam e-postasını analiz ederek benzer alan adlarını dağıtan görünüşte bitmeyen bir kampanya akışını ortaya çıkarıyor. Bu kampanyalardan birkaçının yanı sıra kuruluşların kimlik avı e-postalarını özenle takip etmelerinin önemini vurgulayacağız.

Bu kampanyalardan biri, büyük bir Amerikan telekomünikasyon şirketi olan Xfinity'yi hedef alıyor. Bu benzer alan adları DGA benzeri özelliklere sahiptir ve xfnity<kısa veya kısmi kelime>.com biçimindedir. "Xfinity"nin ilk "i" harfi eksik olduğu için yanlış yazıldığını unutmayın. Saldırgan ayrıca gönderen adının meşru görünmesini sağlamış ve Kiril alfabesinde büyük "X" harfi kullanan "Xfinity Mobile" olarak göstermiştir. Gönderen e-postalar kendi alan adlarını kullanmış ve kullanıcı adında da noreply-<anahtar kelime>, örneğin noreply-corporate@xfnitycard[.]com kalıbından oluşan DGA benzeri özelliklere sahip olduğu görülmüştür. Aktörler her e-posta için benzersiz alan adları kullanmadı. Bazı durumlarda, alan adları tekrarlandı ancak anahtar kelime değiştirildi, örneğin: noreply-corporate @xfnitycard[.]com ve noreply-active@xfnitycard[.]com.

Tablo 7. Xfinity'ye benzeyen alan adları.

xfnitykuri[.]com	xfnitycomp[.]com
xfnitystarter[.]com	xfnityhlaty[.]com
xfnityersa[.]com	xfnityothie[.]com
xfnitykaris[.]com	xfnityrkles[.]com
xfnityrayton[.]com	xfnitycard[.]com

Kampanyada tespit edilen alan adları tuzak park olarak adlandırdığımız bir tekniği kullanmaktadır: Bir alan adı doğrudan ziyaret edildiğinde park edilmiş gibi görünse de gerçekte alan adının posta sunucusu aktiftir ve kötü amaçlı e-postalar göndermektedir. Aldatıcı park etmenin oldukça yaygın olduğunu ve diğer sağlayıcılar tarafından rapor edilmediğini gördük. *Sahte park sayfasının bir örneği için Şekil 17'ye bakın.*

XFINITY BENZERİ

Şekil 17. Xfinity benzeri xfnityrayton[.]com tarafından sergilenen tuzak park sayfası. Resim kredisi: URLScan.[37]

WEDO MACHINERY BENZERİ

Dear you

Good day !
How are you?
How is your project going?
Do you receive my message?

Hope we can establish long term cooperation.

We got recommendation of your company from our UK partner about

below order as attached

Please confirm if your can deliver the products specifield

Mrs. ConnieXu
Mob: 0086 131 0941 7901 [WhatsApp/Wechat]

Wedo Machinery (Zhangjiagang) CO., LTD.

Add: Zhenbei Road, Leyu Town, Zhangjiagang City, Jiangsu Province, China.

Şekil 18. Yem olarak Wedo Machinery ve kötü amaçlı yazılım C2 olarak benzer alan adı acrobat-adobe[.]com kullanan malspam kampanyasının gövdesi.
Resim kredisi: Infoblox

Analizimiz bu Xfinity benzerlerini dağıtılmış kötü amaçlı Word belgelerinde buldu.

Kampanya konuları harekete geçirme çağrısı olarak buna eklendi ve ödemenin reddedilmesi veya hizmet sonlandırma tehdidi etrafında yoğunlaştı; örneğin "[Duyuru] Hizmetiniz feshedilme riski altında" veya "[İşlem Gerekiyor] Kartınızdan ücret almıyoruz, bu hatayı düzeltin" gibi. Bu e-postaların gövdesi müşteri destek ekibinden geliyormuş gibi gösterilmiş ve alıcılardan "konu ayrıntıları için eke bakmaları" istenmiştir.

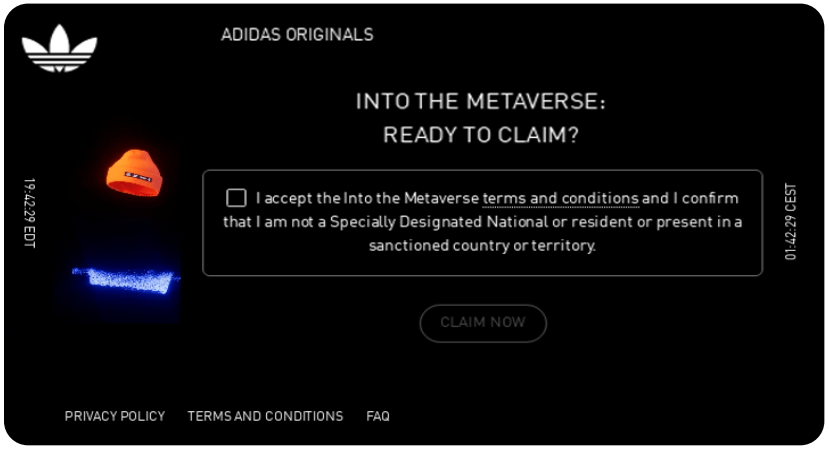
Infoblox'un tespit ettiği bir başka kampanyada fidye yazılımı yükleyicisi bırakmak için Çinli bir geri dönüşüm şirketi olan Wedo Machinery kullanılmıştır. Bu kampanyada, her biri Zmutzy olarak tanımlanan tek bir yürütülebilir dosya içeren bir .zip dosyası içeren 176 e-posta tespit ettik. *Kampanya dahilindeki bir e-posta örneği olarak Şekil 18'e bakın.* Kampanya dahilinde iki dosya adı gördük: PO-0097(1).zip ve PO-29862K.zip. Zmutzy yükleyicisi, ek yükleri indirmek için acrobat-adobe[.]com benzer alan adını kullanır.

QR KODLARI KULLANIYORLAR

Doğrudan kripto para birimi benzerlerine ek olarak şunu da gözlemledik: Kullanıcıları ücretsiz ödüller almaya ve kripto cüzdanı hesap bilgileri sağlamaya teşvik etmek için oluşturulan benzer alan adlarıyla birlikte, bir URL hedefini gizlemek ve kötü amaçlı içerik sunmak için bir QR kodunun kullanıldığı QR kimlik avı yönteminin kullanımı.

Bir örnekte, QR kodu kurbanı fon çalmak için kullanılan bir mekanizma olan bir bridge[.]walletconnect[.]com bağlantısına yönlendirdi. Bu dolandırıcılıkta, aktörler güvenilirlik oluşturmak ve benzer alan adlarını paylaşmak için @adidas_weare adlı bir Twitter hesabı kurdular; *bkz. Şekil 19*. Hesap 21 Şubat 2023 itibarıyla 16.000 takipçiye ulaşmış olsa da neyse ki şu anda silinmiş ya da kaldırılmıştır.

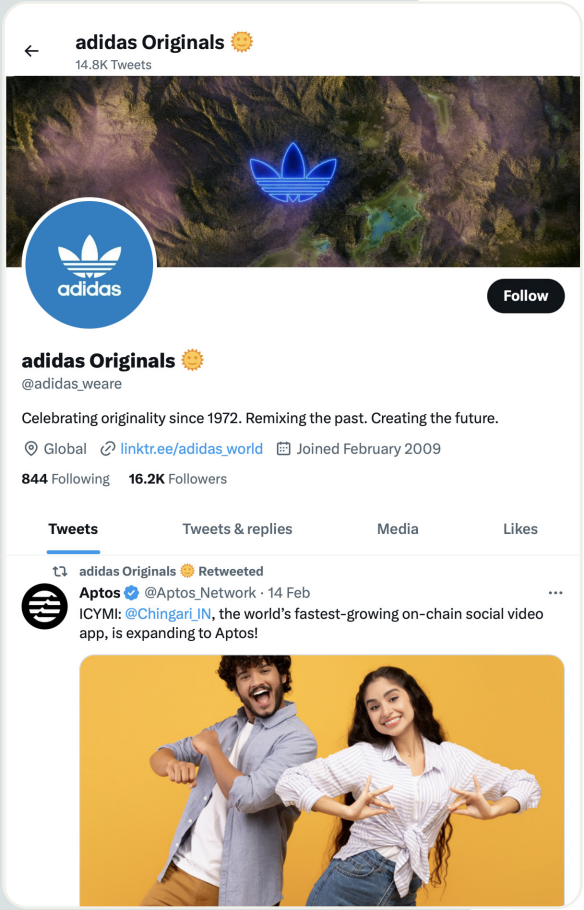
Dolandırıcılar, Porsche arabaları ve Adidas kıyafetleri veya ayakkabıları dahil olmak üzere farklı ürünlerin sahte hediyelerinin reklamını yaptı. Alan adları ağırlıklı olarak "adidas" veya "porsche" anahtar kelimelerini içeren combosquatlar'dı. Aşağıda *Şekil 20*'de gösterildiğigibi benzer alan adlarını ziyaret ettikten sonra, kullanıcılardan verilen hediyeyi talep etmelerini sağlayacak bir QR kodu taramaları istendi ve ardından onları saldırganın kullanıcının fonlarına erişmesini sağlayan merkezi olmayan uygulama WalletConnect'e yönlendirdi.



Şekil 20. Adidas benzeri alan adı adidas-go[.]com kullanıcıları ücretsiz bir ürün talep etmek için tıklamaya davet ediyor. Resim kredisi: URLScan.[39]

Kullanıcılar QR kodunu tarar ve kripto para cüzdanlarını merkezi olmayan uygulamaya bağlarsa dolandırıcılar kullanıcının kripto parasını gasp edebiliyor. Bu alan adları paylaşılan ad sunucuları kullanıyor ve 185[.]149[.]120[.]83 numaralı Rusya çözümlü IP adresinde barındırılıyor. Bu adres tamamen saldırganların kontrolünde ve Blur'un yanı sıra Ethereum akıllı sözleşmelerinin hızını ve ölçeklenebilirliğini artırmaya yönelik bir çözüm olan Arbitum'un da benzerlerini içeriyor.

ADIDAS BENZERİ



Şekil 19. Adidas Originals @adidasoriginals'a benzer Twitter hesabı @adidas_weare. Resim kredisi: Infoblox.

DNS KULLANIYORLAR

Benzer alan adları yalnızca web sitesi alan adı olarak oluşmaz.

Bunların aşağıdakiler de dahil olmak üzere çeşitli DNS kapasitelerinde kullanıldığını tespit ettik:

- **Ad sunucusu**
- **Posta sunucusu**
- **CNAME kayıtları**
- **PTR kayıtları**

Çoğu durumda, bu alan adları tipik bir A kaydına veya web sitesi varlığına sahip olmaz ve genellikle park edilmiş görünebilir (önceki bir bölümde açıkladığımız tuzak parkın bir uygulaması). Saldırganlar ayrıca DNS'de yeniden yönlendirme ve C2 iletişimi için benzer alan adları kullanırlar.

AD SUNUCULARI

Benzer ad sunucularına bir örnek olarak bitkeep[.]dev ve flutter[.]direct alan adları Kasım 2022'de kaydedilmiştir. Bunların her ikisi de farklı alan adlarına benzemektedir, ancak aynı altyapıyı paylaşmaktadır. BitKeep, tüm kripto para birimi işlemleri için tek bir merkez olmayı amaçlayan bir merkeziyetsiz çok zincirli bir kripto cüzdanıdır. BitKeep'in resmi alan adı bitkeep[.]com'dur ve şirket 8 milyondan fazla kullanıcısıyla beş yıldır faaliyet göstermektedir.[40] Flutter, tek bir kod tabanından mobil, web ve masaüstü için yerel olarak derlenmiş uygulamalar oluşturmaya yönelik Google'ın taşınabilir kullanıcı arayüzü (UI) araç setidir. Flutter için resmi alan adı flutter[.]dev şeklindedir.[41]

Her iki meşru alan da web içeriğini birincil alanda barındırır, ancak benzer alan adlarının hiçbiri bunu yapmaz. Her iki alan adı da ilk kaydedildiklerinde Flutter'ın bir başka benzeri get-flutter[.]com adlı başka bir alan adı için ad sunucusu olarak görev yapıyordu. O dönemde, alan adları İsviçreli offshore barındırma sağlayıcısı Private Layer'da barındırılıyordu. Bu ağ aynı zamanda flutter[.]vision'ı da barındırdı. Bu alan adlarını kötü niyetli faaliyetlerle kesin olarak ilişkilendiremesek de, geleneksel olmayan amaçlar için benzer alan adlarından yararlanma modelini göstermektedirler. Deneyimli araştırmacılar için bile analiz edilmesi oldukça zorlayıcıdır ve birçok tehdit istihbaratı algoritmasını tetikleme olasılıkları düşüktür.

POSTA SUNUCULARI

Ad sunucularına ek olarak, benzerlerinin posta sunucusu olarak kullanıldığını gördük. whirlpoolmxonline[.]com ve whirlpoolservicesmx[.]com alan adları, büyük cihaz markası Whirlpool'u hedefliyor ve aynı altyapıyı paylaşıyor. Seyşeller'de bulunan düşük kaliteli bir VPS ve barındırma sağlayıcısı olan Lyra Hosting'e ait aynı IP adresinde barındırılıyor ve aynı ad sunucularını paylaşıyorlar.

İkinci seviye alan adı (SLD) ile doğrudan Whirlpool'u hedef alsalar da, her bir alan adı içinde diğer büyük cihaz markalarını da hedef aldıklarını gösteren özellikler tespit ettik. SLD whirlpoolmxonline[.]com'un üç alt alan adı var: mabe-onlinemx[.]whirlpoolmxonline[.]com, samsung-onlinemx[.]whirlpoolmxonline[.] com ve lg-onlinemx[.]whirlpoolmxonline[.]com. Mabe, Meksikalı bir cihaz şirketidir. SLD whirlpoolservicesmx[.]com'un alt alanı olmasa da alan adıyla ilişkili geçmiş SSL sertifikaları zinciri, whirlpoolmxonline[.]com gibi benzer cihaz markalarının hedeflenmesine işaret ediyor: www[.]lgservicesmx[.]mabeservice[.]com ve *.lgservicesmx[.]com.

Benzer alan adlarını posta sunucuları olarak kullanmak, e-posta başlıklarına ilk bakışta meşru görünümü nedeniyle bir uç noktadaki kimlik avı e-postalarını tespit etmek için ek bir zorluk sunar.

MALWARE C2'LER

Daha önce e-posta dağıtımı bölümünde, Zmutzy fidye yazılımı yükleyicisini kaldıran tespit ettiğimiz bir malspam kampanyasının, benzer alan adı acrobat-adobe[.]com'u kötü amaçlı yazılım C2 sunucusu olarak nasıl kullandığından bahsetmiştik. Lookalikes, yasal etki alanlarının yanı sıra ağ trafiğine kolayca karışabildikleri için kötü amaçlı yazılım C2'ler için mükemmeldir. Bir Slovak güvenlik yazılımı şirketi olan ESET'teki araştırmacılar, Şubat 2023'te mesajlaşma uygulaması Telegram olarak poz veren FatalRat (uzaktan erişim truva atı) için kötü amaçlı yazılım C2'leri tespit etti.[42]

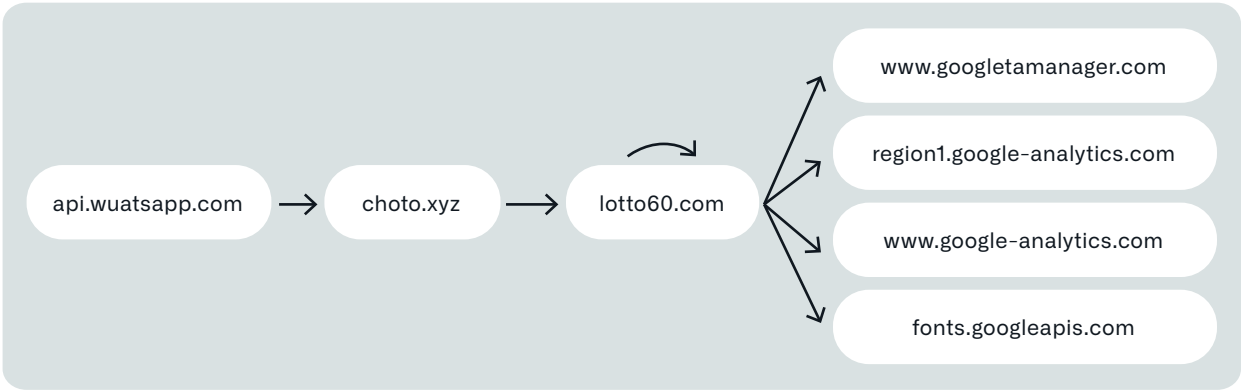
Tablo 8. Kötü amaçlı yazılım C2'leri olarak işlev gören Telegram benzerleri.

12-03.telegramxe[.]com	12-25.telegraem[.]org
12-25.telegraxm[.]org	12-25.telegraem[.]org

Kötü amaçlı .exe dosyasını barındıran alan adları Telegram'ın yanı sıra WhatsApp, Skype, Google Chrome ve Firefox'a da benziyordu.

YÖNLENDİRMELER

Benzer alan adları yönlendirme olarak da kullanılabilir. Ziyaretçileri, kurbanları koşullu olarak lotto60[.]com açılış alanına yönlendiren bir C2 alanı olan choto[.]xyz'ye yönlendiren geniş bir typosquat alan adı ağı tespit ettik. Saldırganlar, muhtemelen güvenlik araştırmacıları tarafından tespit edilmesini ve araştırılmasını önlemek için choto[.]xyz üzerinde ters proxy hizmetleri ve Cloudflare bot koruması kullanıyor. Açılış alan adı, hileli bir satış ortaklığı pazarlama programı yürütüyor gibi görünüyor. Belge nesne modelini (DOM) analiz ederek, HTML'nin ziyaretçi verilerini Google Analytics'e analitik kimliği G-DT4YWT5VP8 ile gönderen satır içi bir gtag() işlevi içerdiğini görebiliyoruz. Saldırganın bağlı kuruluş pazarlama numaralarını şişirmenin yanı sıra, lotto60[.]com'un HTTP üzerinden uzaktan erişim truva atı Nighthawk olduğu onaylanan dosya imzalarıyla eşleşen potansiyel kötü amaçlı dosyalar tarafından talep edildiğini gördük.[43]



Şekil 21. Bir typosquat alan adından Google Analytics'e örnek yönlendirme zinciri. Resim kredisi: URLQuery.[44]

Birinci aşama typosquat alan adları çeşitli şirketleri taklit eder. Bazı örnekler şunlardır:

Tablo 9. Sahte bir bağlı kuruluş pazarlama kampanyasında yönlendirme işlevi gören benzerler.

gi6hub[.]com	whatysapp[.]com
bankofamegica[.]com	babgkokbank[.]com
intuhit[.]com	scotiasbank[.]com

Bu typosquat'lar genellikle yönlendirme olarak kullanılmadan önce bir ila üç ay boyunca park edilir. Saldırganlar bu typosquat alan adlarını hazırlarken büyük özen gösterdi. Her yanlış karakter, ABD İngilizcesi, QWERTY klavyesindeki asıl karaktere doğrudan bitişik. Bunlar, ortalama bir kullanıcının bir günde birden çok kez yapabileceği hatalardır (hala "avlanıp gagalayan" kullanıcılar hariç).

NEDEN ETKİLİLER?

Sevgili Okur, şu ana kadar bu makalenin içine serpiştirdiğimiz 19 benzer kelimeyi fark ettiniz mi? Bazılarını görmek çok zor!

İpucu: 6 tane daha var. Bakalım onları bulabilecek misiniz?

Şimdiye kadar bazı belirli hedeflerin yanı sıra benzer alan adlarının dağıtım yöntemleri altyapısını ele aldık. Peki neden bu kadar etkililer? Onları bu kadar kalıcı bir tehdit haline getiren şey nedir?

Cevap karmaşıktır ve psikolojinin, teknik uygulamaların ve basit insan hatalarının yönlerini içerir. **Sonuçta bizi insan yapan da budur!**

PSIKODİLBİLİM

Psikolojik olarak, insan beyni okurken kısa devre yapar (bu durumda, bir akımın istenmeyen bir en az direnç yolunu seçmesinin gerçek tanımını kastediyoruz). Muhtemelen aşağıdaki gibi bir meme görmüşsünüzdür:

> ***Cmabrigde Uinervtsesi arşatırmasına gröe keliemede harflrein sıralmaası önelmi dğeildir, önmeli olan tek şey ilk ve son hafrin yeirnde olmsaıdır. Sonçuta ortyaa çıakn metin karmşaık olsa da kolyaca okuanbilir. Bnuun ndeeni, isnan zihinnin her hafri ayrcıa dğeil, keilmeyi bir btüün oalrak okumaısdır.***

İddia, Cambridge'de böyle bir araştırmanın yayınlanmadığı anlamında temelsiz olsa da, altta yatan kavramın değeri var gibi görünüyor. Örneğin, son araştırmalar, "karışık bir kelimeyi görüntülemenin bilinen kelimelerle karşılaştırılan görsel bir temsili etkinleştirdiğini" öne sürüyor.[45] Psikodilbilimin temel sorularını kanıtlamak veya çürütmek bu makalenin kapsamı dışında olsa da, psikodilbilimin görünüşün beğenilerinin etkinliğinde nasıl önemli bir rol oynadığını göstermek istiyoruz.

Spesifik olarak, insan beyninin kısa devresi, homoɢraf ve typosquat'lar söz konusu olduğunda rol oynar. Infoblox[.]com gibi bir alan adı gördüğünüzde, beyniniz o alan adındaki her bir harfi ayrıştırmaz ve bu nedenle ilk karakterin aslında büyük bir "i" değil küçük bir "L" olduğunu asla fark etmeyebilirsiniz.

Benzer nedenlerden dolayı, gooogle[.]com alan adını gördüğünüzde, beyniniz "o" harfinin iki yerine üç tane olduğunu fark etmeyebilir... en azından çok geç olana ve siz çoktan tıklayana kadar.

PUNYCODE DESTEĞİ: İSABETLER VE ISKALAR

Web tarayıcıları, kullanıcıları uluslararası alan adı (IDN) hom0grafik saldırılarına karşı savunmanın yollarını sunar. İlk ve en belirgin savunma hattı, Unicode alan adını, başındaki "xn--" ile tanınabilen ve çıplak gözle anlamsız görünen Punycode'a "çevirmektir". Bunun nedeni, Zayıf Kod'un Unicode karakterlerini yalnızca harf, rakam ve kısa çizgi içeren Amerikan Bilgi Değişimi Standart Kodu (ASCII) karakterlerinin çok daha sınırlı alt kümesiyle eşlemesidir. Tüm başlacı tarayıcı Punycode alan adlarını destekler. Google, Chromium'da bir alan adının uluslararasılaştırılmış veya Punycode sürümünün gösterilip gösterilmeyeceğini belirleyen algoritmada yer alan buluşsal yöntemlerin ayrıntılı bir açıklamasını verir.[46] Mozilla da benzer bir açıklama yapmıştır.[47]

Mozilla da IDN görüntüleme algoritmasının açıklamasında bu ilham verici metni sunuyor:

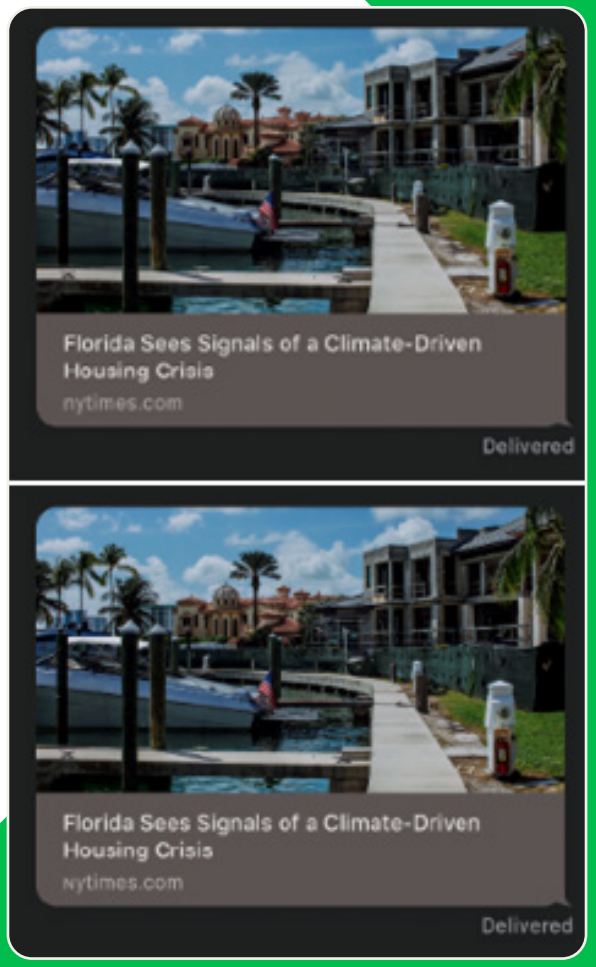
> ***Bu konuya cevabımız, sonuçta müşterilerinin birbirlerini dolandırmasına izin verip vermemenin kayıt kuruluşlarına bağlı olduğudur. Tarayıcılar bazı teknik kısıtlamalar getirebilirler ancak biz, web üzerinde Latin alfabesi olmayan alfabeler için eşit şartlar sağlamaya devam ederken bu işi onlar adına yapabilecek durumda değiliz. Kayıtlar, burada uygun kontrolü uygulayabilecek konumdaki tek kişilerdir. Bizim açımızdan, Latince olmayan yazılara ikinci sınıf vatandaş olarak davranmadığımızdan emin olmak istiyoruz.***

Güvenlik araştırmacısı Xudong Zheng 2017 yılında Punycode'da bir alan adı kaydetmiştir, xn--80ak6aa92e[.]com, "apple[.]com" anlamına gelmektedir ve "apple" kelimesindeki Latince karakterlerin görünümünü taklit eden Kiril karakterleri içermektedir.[48] O dönemde Internet Explorer, Microsoft Edge, Safari, Brave ve Vivaldi web tarayıcılarında güvenlik açığı olmasa da Chrome, Firefox ve Opera güvenlik açığına sahipti. Şu anda sadece Firefox Punycode'u çevirmeye devam etmektedir. Bu da kullanıcıları saldırılara karşı savunmasız bırakmaktadır (alan adını yakın zamanda Internet Explorer veya Microsoft Edge üzerinde test etmedik).

PUNYCODE NEDİR?

Punycode, Unicode karakterlerini daha küçük, kısıtlı bir karakter seti olan ASCII'ye dönüştürmek için kullanılan özel bir kodlamadır. Punycode, uluslararasılaştırılmış alan adlarını (IDN'ler) kodlamak için kullanılır.

IDN HOMOGRAFLARINI KULLANARAK İMESSAGE SMISHING



Şekil 22. Tyler Butler'dan alınan En İyi Resim, iMessage aracılığıyla gönderilen gerçek bir New York Times makalesini gösteriyor.
Alttaki Resim Tyler Butler'dan alınmıştır ve bir IDN homograf alan adında sahte bir NYT makalesini göstermektedir. Resim kredisi: Tyler Butler.

Hu ve ark. IDN homograf saldırılarına karşı tarayıcı tabanlı savunmaların etkinliği üzerine boylamsal ve nicel bir analiz gerçekleştirdi.[49]

Üç soruyu cevaplamak için yola çıktılar:

1. Başlıca tarayıcılar hangi politikaları uyguluyor ve bu politikaları ne kadar iyi uyguluyorlar?
2. Mevcut politikaları sistematik olarak atlamanın yolları var mı?
3. Web'de gezinenler IDN homograflarını ne kadar iyi tanıyabilir ve tarayıcı politikalarını atlayan bu IDN homografları az çok aldatıcı mı?

Yazarlar soruları yanıtlamak için beş yıl boyunca (Ocak 2015'ten Nisan 2020'ye kadar) beş ana akım tarayıcıyı (Chrome, Firefox, Safari, Microsoft Edge ve Internet Explorer) inceledi. İlk iki soruyu yanıtlamak için 9.000 test vakası oluşturdular ve üçüncü soruyu yanıtlamak için bir kullanıcı çalışması yürüttüler. Chrome ve Edge, karşılık gelen IDN homografları yerine Punycode'u görüntülemede en başarılı oldu; her iki tarayıcının da genel hata oranı (Punycode yerine IDN sürümünü gösterme) %20.62'ydi. Safari ve Firefox çok daha kötüydü; genel başarısızlık oranı sırasıyla %42,91 ve %44,46 oldu. Her tarayıcı, IDN kategorisine bağlı olarak farklı başarısızlık oranlarına sahipti. Ayrıca, yazarlar web'de gezinenlerin homograf IDN'leri tanımakta zorlandıklarını ve tarayıcıların engellediği IDN'lerin özgünlüğü belirlemede en sıkıntılı olanlar olduğunu bulmuşlardır: kullanıcıların %48,8'i gerçek olduklarını düşünürken, %48,5'i olmadıklarını düşünmüş ve %2,7'si arada farj görememiştir.

Şimdiye kadar yalnızca masaüstü tarayıcılara odaklandık. Ancak, bu makalenin önceki bölümlerinde açıklanan benzer smishing saldırılarında gördüğümüz gibi, IDN eş yazımlı alan adları da mobil cihazlarda oldukça rahattır. Aslında, daha tehlikeli olabilirler. Daha küçük ekran boyutları, daha küçük adres çubukları ve genel olarak bağlantı önizleme eksikliği, daha etkili benzer alan adı saldırılarına yol açabilir. Bağlantı önizlemesi olsa bile, IDN homografları mobil cihazlarda yine etkili olabilir. 2021'de güvenlik araştırmacısı Tyler Butler, iMessage'da IDN homograflarını kullanarak smishing yapmanın akla yatkınlığı üzerine bir makale yayınladı.[50] iMessage, bağlantıların zengin önizlemelerini sunar, ancak bilgili bir saldırgan, yeterince iyi bir benzer alan adı ve web sayfasının kendisi için biraz stil çalışması ile bunu oldukça kolay bir şekilde aşabilir. Bay Butler'ın belirttiği gibi, bu saldırı biçimi yanlış bilgi yaymak, kimlik bilgilerini çalmak veya hedefli kötü amaçlı yazılım veya casus yazılım göndermek için kullanılabilir.

Bay Butler, Apple'ın homoglaflarının "görsel olarak ayırt edilebili" olması nedeniyle güvenlik açığını ele almayacaklarını iddia ettiğini açıklıyor. *Şekil 22 göz önüne alındığında, ne düşünüyorsunuz? Farkı görebiliyor musunuz?*

HATA YAPMAK İNSANCA, AFFETMEK ULVİDİR... AMA OTOMATİKLEŞTİRMEK AKILLICADIR

World Wide Web'de, diğer bazı insanlar başkalarının hatalarını bu kadar affedici değildir. Daha önce de belirttiğimiz gibi, saldırganlar başkalarının doğal yazım hatalarını avlamak için typosquat alan adlarını kullanır. Bir saldırganın typosquat'in etkili olması için yapması gereken tek şey, makul bir alan adı kaydetmek ve beklemektir. Bu kadar. Er ya da geç, bir insan bu yazım hatasını yapacak ve hiç ziyaret etmek istemediği bir alana gidecektir. Elbette kötü niyetli kişiler sadece beklemekle kalmaz, proaktif olarak insanları tıklamaya ikna ederler. Hızla değişen dünyamızda çoğu zaman ilk etapta bir hata yaptığımızın farkına bile varmıyoruz.

Günün sonunda, benzer alan adları bir nedenden dolayı benzer olarak adlandırılır: bir insanı aldatmak amacıyla bilinen alan adlarına benzerler. Gördüğümüz gibi, bazı benzerlikler diğerlerinden daha etkilidir, ancak alan adı seçimi, benzerlerin etkinliğinin yalnızca bir parçasıdır. Benzer bir alan adının dağıtılma şekli, kampanyanın genel başarısı üzerinde de önemli bir etkiye sahip olabilir. Örneğin, okta[.]Infoblox[.]com veya okta-Infoblox[.]com gibi bir Okta veya MFA benzeri ele alalım. Ziyaret etmeden önce her alan adını üç kez kontrol eden seçici bir kişi (bu kişilerden birini bulmak için iyi şanslar), ikinci seviye alan adındaki (SLD) "i" in aslında küçük bir "L" harfi olduğunu fark edebilir. Ancak, örneğin işverenlerinin çevrimiçi profilinde sahip oldukları telefon numarasına iyi hazırlanmış bir SMS mesajıyla eşleştirilmiş bu benzerlik, fark yaratan şey olabilir. Denkleme acil bir harekete geçirici mesaj içeren bir telefon görüşmesi eklediğinizde oyun biter. Elbette bu, spearphishing'in kurgusal bir örneğidir (tüm bileşen parçalarıyla birlikte) ve benzerlikler kullanan genel bir kampanya değildir. Ancak mesele aynı: benzerlik teknikleri alan adlarına birden çok şekilde ve DNS altyapısının birden çok bölümüne etkili bir şekilde uygulanabilir.

Tüm bunlar, sıkça atıfta bulunulan "beni bir kez kandırırsan, sana; beni iki kez kandırırsan, bana yazıklar olsun" atasözünün benzerler için geçerli olmadığını söylemek içindir. En şahin gözlü, güvenlik bilincine sahip bireyler bile bir benzer alan adının kurbanı olabilir ve bunu tekrar tekrar yapabilir. Kötü niyetli kişiler bu savaşta üstünlüğe sahip, ama savaş henüz kaybedilmedi. Infoblox, kuruluşların kendilerini savaşma ve etkili bir şekilde savunma yeteneğine sahip olmasını sağlamak için DNS düzeyinde çözümlere sahiptir.

IOC'LER ***Bu makalenin tam listesi GitHub'da https://github.com/infobloxopen/threat-intelligence adresinde bulunabilir.***

INFOBLOX ÇÖZÜMLERİ

Benzer alan adları, etkinlikleri ve bunları geniş ölçekte tespit etmenin zorluğu nedeniyle saldırganlar arasında popüler olmaya devam ediyor. Bu zorluk, meşru bir hedefi taklit etmesi amaçlanan şüpheli bir alan adını otomatik olarak tanımlamanın zorluğuyla daha da artmaktadır. Bu durum, işletmelerin ve devlet kurumlarının kurumsal alan adlarını veya tedarik zincirlerini taklit eden benzer alan adları konusunda giderek daha fazla endişe duymalarına neden olmuştur.

Infoblox BloxOne Threat Defense (B1TD) Advanced, benzer tehditlere karşı benzersiz geniş ve kapsamlı bir çözüm sunar. Büyük ölçekli DNS'lerden yararlanan Infoblox, her gün yüz binlerce yeni SLD'ye bir dizi analiz uygulayabiliyor. Bu, IDN Homografilerindeki görsel benzerliklerin otomatik olarak değerlendirilmesi gibi benzerlik tespiti için çoklu analitikleri içerir.

Müşteriler, yaygın olarak hedeflenen alan adları arasından seçim yapabilir veya özel benzerlik izleme ve analizi için özel bir liste oluşturabilir. Bu derinlemesine analizin sonuçlarına, algılanan benzerin şüpheli veya kimlik avı etkinliğiyle ilişkili olduğu durumları da işaretleyen benzeralan adı Raporlama Kullanıcı Arayüzü aracılığıyla erişilebilir. Genel olarak, politikalar müşterinin özel ortamının ihtiyaçlarına ve risk toleransı düzeyine uyacak şekilde özelleştirilebilir. Ayrıntılı alan adı verileri, B1TD Gelişmiş Kullanıcı Arayüzleri ve API'leri aracılığıyla erişilebilen değerli ek açıklamalar içerir ve müşterilere tehdit araştırmalarını hızlandırabilecek ve olay yanıtlarını daha etkili hale getirebilecek bağlamı sağlar.

Bu benzer tehdit algılama özellikleri, BloxOne Threat Defense tarafından sunulan ve diğer çözümlerin algılayamadığı tehditleri görmesini ve tehdit yaşam döngüsünün erken dönemlerinde saldırıları durdurmasını sağlayan birçok hizmetten sadece biridir. Yaygın otomasyon ve ekosistem entegrasyonu sayesinde, SecOps'ta daha fazla verimlilik sağlayabilir, mevcut güvenlik yığınının etkinliğini artırabilir, dijital ve her yerden çalışma çabalarını güvence altına alabilir ve siber güvenlik için toplam maliyeti düşürebilir.

DAHA FAZLA BİLGİ İÇİN

Bu adresi ziyaret edin: infoblox.com

Bizi LinkedIn'de takip edin

Bizi Twitter'da takip edin

REFERANSLAR

[1] https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf

[2] https://twitter.com/kgroupcompanies/status/1188878363068391425

[3] https://en.wikipedia.org/wiki/IDN_homograph_attack

[4] https://i.imgur.com/68oL4U9.jpg

[5] https://www.researchgate.net/publication/220420915_The_Homograph_Attack

[6] https://util.unicode.org/UnicodeJsps/confusables.jsp

[7] https://www.igoldrush.com/domain-guide/domain-legal-issues/cybersquatting-and-typosquatting

[8] https://dl.acm.org/doi/pdf/10.1145/3133956.3134002

[9] https://core.ac.uk/download/pdf/34615371.pdf

[10] https://iris.polito.it/retrieve/handle/11583/2970511/1dd2efbb-9eed-4db5-be4f-ecfcc362572c/_Workshop__Data_driven_Soundsquatting_Generation%20(7).pdf

[11] https://incolumitas.com/2016/06/08/typosquatting-package-managers/

[12] https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

[13] https://www.akamai.com/blog/security-research/combosquatting-keyword-analysis-support

[14] https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/c/iron-tiger-sysupdate- reappears-adds-linux-targeting/IOCs-iron-tiger-sysupdate-reappears-adds-linux-targeting.txt

[15] https://urlscan.io/result/41e8b29f-55cc-4887-9186-41a064ffb2ac/

[16] https://thehackernews.com/2022/07/microsoft-warns-of-large-scale-aitm.html

[17] https://thehackernews.com/2023/03/microsoft-warns-of-large-scale-use-of.html

[18] https://www.hackread.com/hackers-employee-accounts-twilio-internal-system/

[19] https://www.feldmanauto.com/

[20] https://urlscan.io/result/98f407d6-96b4-4652-bd38-aa44470b5b78/

[21] https://urlscan.io/result/98f407d6-96b4-4652-bd38-aa44470b5b78/

[22] https://blogs.infoblox.com/cyber-threat-intelligence/scammers-first-on-the-scene-for-turkiyes-disaster-of-the-century/

[23] https://urlscan.io/result/4f295f57-7d46-49e9-94f6-d90858a4cfeb/

[24] https://www.coindesk.com/web3/2023/03/02/nft-trading-volumes-hit-2b-in-february-highest-since-luna-crash-thanks-to-blur/

[25] https://nftnow.com/guides/blurs-token-just-dropped-heres-what-you-need-to-know/

[26] https://twitter.com/blur_io/status/1630290782211981312/

[27] https://www.wired.com/story/youtube-bitcoin-scam-account-hijacking-google-phishing/

[28] https://twitter.com/FoolishBB/status/1627059614654279682

[29] https://www.bleepingcomputer.com/news/security/fake-crypto-giveaways-steal-millions-using-elon-musk-ark-invest-video/

[30] https://www.domaintools.com/

[31] https://urlscan.io/result/8e94bf31-7295-47e8-9de4-756743937f46/

[32] https://www.domaintools.com/

[33] https://urlscan.io/result/7f3c8f83-1922-4570-a9b1-1542e32ccc89/

[34] https://urlscan.io/result/f60f5548-4b54-4a97-add5-1f37a89f4e7e/#summary

[35] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a

[36] https://blogs.infoblox.com/cyber-threat-intelligence/cyber-campaign-briefs/dont-dial-that-number-distribution-of-phishing-lookalikes-through-fake-support-calls/

[37] https://urlscan.io/result/41a6ef99-fef1-4d08-80e1-623123280b6a/

[38] https://walletconnect.com/

[39] https://urlscan.io/result/a79ba8e3-9f9a-4a9c-b54b-b26a300afc23/

[40] https://bitkeep.com/

[41] https://docs.flutter.dev/

[42] https://www.welivesecurity.com/2023/02/16/these-arent-apps-youre-looking-for-fake-installers/

[43] https://www.virustotal.com/gui/file/ 271229d5d007baf5324fb2705b7a0b3751bd228bbdb08a86e7b7e2856bbf9b08

[44] https://urlquery.net/report/ef86060b-39e3-4e41-a480-a2b138ee0a49

[45] https://elifesciences.org/articles/54846

[46] https://chromium.googlesource.com/chromium/src/+/main/docs/idn.md

[47] https://wiki.mozilla.org/IDN_Display_Algorithm

[48] https://www.xudongz.com/blog/2017/idn-phishing/

[49] https://www.usenix.org/system/files/sec21-hu-hang.pdf

[50] https://tbutler.org/2021/04/16/considering-the-plausibility-of-idn-homograph-attacks

infoblox.

Infoblox, benzersiz performans ve koruma sağlamak için ağ ve güvenliği birleştirir. Fortune 100 şirketleri ve gelişmekte olan yenilikçiler tarafından güvenilen firmamız, ağınıza kimin ve neyin bağlandığı üzerinde gerçek zamanlı görünürlük ve kontrol sağlıyor. Böylece kuruluşunuz daha hızlı harekete geçerek tehditleri daha çabuk durdurabilir.

Kurumsal Merkez
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com