

Derinlemesine Savunma Stratejisi

MFA2+

Hack

Teknikleri

El Kitabı

İçindekiler

Özet	3
Giriş	3
Çok Faktörlü Kimlik Doğrulama Temelleri	4
Kimlik Doğrulama Temelleri	4
kimlik	4
Doğrulama	4
Erişim Kontrol Simgesi	5
Yetkilendirme	5
Tek Yönlü ve İki Yönlü Kimlik Doğrulama	6
Kimlik Doğrulama Faktörleri	7
Tek Faktörden Çok Faktöre	7
Bant İçi ve Bant Dışı Kimlik Doğrulama	8
Çok Faktörlü Kimlik Doğrulamayı Hackleme	9
MFA 9	
Oturum Ele Geçirme	9
Oturum Benzersiz Tanımlayıcı Tahmini	10
Oturum Ele Geçirme Proxy Saldırısı	10
Kevin Mitnick MFA Video 10	
Sahte Kimlik Doğrulama	11
Uç Noktadaki Adam Saldırıları	12
Banco Truva Atları	12
Kötü Amaçlı MFA Yazılımında Değişiklik	13
Kötü Amaçlı MFA Donanım Değişiklikleri	13
SIM Değiştirme Saldırıları	14
SMS Hileli Kurtarma	16
Yinelenen Kod Üreticileri	19
Omuz Sörfü	21
Göz Atma Saldırıları	22
Düşürme ve Kurtarma Saldırıları	24
Kurtarma Soru Saldırıları	25
Sosyal Mühendis Teknik Destek	27
Konu Ele Geçirme	28
Microsoft Akıllı Kart Kimliğini Ele Geçirme Saldırısı	28
Yeniden Oluşturulan Biyometri	37
Çalınan Biyometri	38
Kaba Kuvvet Saldırıları	39
Buggy MFA	40
ROCA Güvenlik Açığı	40
Diğer Fiziksel Saldırılar	40
Elektron Mikroskobu Saldırısı	41
Soğuk Önyükleme Saldırıları	41
MFA Saldırılarına Karşı Savunmaları Özetleme	42
Sosyal Savunma	42
Teknik Savunma	42

Sonuç

Özet

Tüm çok faktörlü kimlik doğrulama (MFA) mekanizmaları tehlikeye girebilir ve bazı durumlarda, geleneksel bir kimlik avı e-postası göndermek kadar basittir. Bu teknik inceleme, çeşitli MFA türlerini hacklemenin bir düzineden fazla farklı yolunu ve bu saldırılara karşı nasıl savunulacağını kapsar.

giriş

Oturum açma adları ve parolalar gibi tek faktörlü kimlik doğrulama yöntemlerine karşı onlarca yıl süren başarılı saldırılar, daha güvenli, çok faktörlü kimlik doğrulama (MFA) çözümlerine yönelik geniş çaplı bir hareketi tetikliyor. MFA çözümleri on yıllardır çeşitli nedenlerle mevcut olmasına rağmen, artık hem kurumsal ortamlarda hem de internet web sitelerinde MFA'nın devam eden, geniş ölçekli ve hızlı bir şekilde benimsenmesi söz konusudur.

Bu eğilim, son birkaç yılda Google, Microsoft, Facebook ve Twitter'a ait olanlar da dahil olmak üzere en popüler web siteleri ve hizmetlerin müşterilerine MFA çözümleri sunması gerçeğiyle örneklenmektedir. Pek çok internet sitesi ve hizmet artık hem geleneksel oturum açma adı/şifre çözümleri hem de daha güvenli MFA seçenekleri sunuyor.

Google gibi bazı büyük şirketler

(<https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/>) , kullanıcı tabanını tek faktörlüden çok faktörlüye taşıyarak bazı yaygın bilgisayar korsanlığı saldırılarına karşı savunmada büyük başarı bildiriyor. faktör doğrulama MFA çözümleri, en popüler işletim sistemlerinde varsayılan olarak desteklenir ve yüzlerce üçüncü taraf satıcı tarafından ek MFA çözümleri sunulur. FIDO Alliance (<https://fidoalliance.org/>) tarafından desteklenenler gibi ortak açık MFA standartları geniş çapta benimsenmektedir.

MFA daha önce (çoğunlukla) en yüksek güvenlik güvencesine ihtiyaç duyan kuruluşlar ve web siteleri için kullanılıyordu. Bugün, MFA jetonları sıradan kuruluşlar ve web siteleri tarafından sunuluyor veya kullanılıyor ve MFA jetonları cihaz başına birkaç dolar gibi düşük bir fiyattan satın alınabiliyor. Pek çok tüketici, MFA çözümlerinin güvenliğine o kadar çok güveniyor ki, mümkünse ve izin verildiğinde, buna izin veren tüm web sitelerinde ve hizmetlerde MFA satın alıyor ve kullanıyorlar.

MFA'nın daha geniş çapta benimsenmesi, bilgisayar savunmaları için olumlu bir gelişmedir ve aksi takdirde tek faktörlü kimlik doğrulama çözümlerine karşı daha kolay başarılı olabilecek birçok tehdidi yenecektir. Diğer her şey eşit olarak kabul edilir, tüm yöneticiler ve kullanıcılar, hassas verileri korumak için tek faktörlü kimlik doğrulama çözümleri yerine MFA çözümlerini düşünmeli ve kullanmalıdır.

Bununla birlikte, MFA'nın bilgisayar güvenlik riskini azaltma yeteneği, birçok satıcı ve savunucu tarafından aşırı derecede ifade edildi ve MFA uygulamasının, tek faktörlü kimlik doğrulamaya karşı başarılı olan tüm saldırıların MFA'ya karşı başarılı olamayacağı anlamına geldiğinin yanlış anlaşılmasına yol açtı. Örneğin, birçok MFA yöneticisi ve kullanıcısı, e-posta kimlik avının artık bir tehdit olmadığına inanmaktadır, çünkü kullanıcılar oturum açma kimlik bilgileriyle kimlik avı yapılamaz. Bu doğru değil.

MFA belirli bilgisayar güvenlik risklerini azaltır ve bazı durumlarda önemli ölçüde azaltırken, tek faktörlü kimlik doğrulamaya karşı başarılı olabilecek saldırıların çoğu MFA çözümlerine karşı da başarılı olabilir. Bu yazıda, farklı MFA çözümlerine saldırmanın bir düzineden fazla yolunu tanıtıyoruz. Çoğu zaman, tek bir MFA çözümü, çoklu kullanım yöntemlerine karşı hassastır. Bu belge tüm yöntemleri içermese de, dahil

edilen bilgisayar korsanlığı yöntemleri, MFA'nın tek faktörlü kimlik doğrulama çözümlerinden daha güvenli olmasına rağmen kırlamaz olmadığını gösterecek kadar temsilidir .

Bu teknik inceleme, MFA çözümlerini hacklemenin bir düzineden fazla farklı yolunu ve bu saldırılara karşı nasıl savunulacağını açıklamaya adanmıştır. MFA'yı hacklemek için kullanılan farklı yöntemleri anlamak için, kimlik doğrulama ve MFA'nın temel bileşenlerini anlamaya yardımcı olur.

Çok Faktörlü Kimlik Doğrulama Temelleri

Bu bölüm, genel anlamda kimlik doğrulama temellerini tartışır ve ardından özellikle MFA'yı kapsar.

Kimlik Doğrulama Temelleri

Kimlik doğrulama, belirli bir kimliğin sahipliğini kanıtlayan bir öznenin (örneğin, kullanıcı, cihaz, grup, hizmet, vb.) sürecidir. Daha da parçalayalım.

Kimlik

Kimlik, belirli bir konuyu tanımlayan herhangi bir benzersiz (ilgili ad alanına) etikettir. Bir kimlik genellikle bir oturum açma adı (ör. rogerg), e-posta adresi (ör.

rogerg@knowbe4.com) veya benzersiz bir karakter dizisi olabilir, ancak aynı ad alanı içinde daha önce üzerinde anlaşmaya varılan herhangi bir benzersiz etiket olabilir.

Ad alanı, belirli varlıkları ve bunlarla ilgili nitelikleri toplamaya, tanımlamaya ve yerleştirmeye yardımcı olan organize bir sistemdir. Ortak ad alanları, Etki Alanı Adlandırma Sistemi (DNS), Microsoft Active Directory ve Hafif Doğrudan Erişim Protokolü (LDAP) veritabanlarıdır. Bir ad alanı, konu başına birden fazla kimlik etiketi içerebilir (örneğin, Active Directory DNS, LDAP, e-posta adresi ve Kullanıcı Asıl Adını (UPN) kullanabilir), ancak her etiket aynı ad alanında benzersiz olmalıdır ve yalnızca tek bir kimlik etiketini temsil edebilir. ders.

Tüm kimlik doğrulama ve erişim denetimi adımları, bir veya daha fazla kimlik içerir. Tüm kimlik doğrulama, kimlik doğrulamayı yapan özneyi benzersiz şekilde tanımlayan bir kimlik etiketi içerir. Kimlikler, ilk kimlik doğrulama sürecinin bir parçası olarak veya öncesinde oluşturulmalıdır. Kimlik, kimliğin sahipliğini kanıtlamak için sağlanandan farklı olmalıdır. Örneğin, Microsoft Windows'ta, bir özne kimlik doğrulaması yapmak (yani kimliğin sahipliğini kanıtlamak) için bir parmak izi kullanabilse de, bir kimlik doğrulama girişimine eklenen etiket muhtemelen kullanıcının Active Directory oturum açma adı, UPN'si veya e-posta adresi olacaktır. . Kimlik etiketi, kimlik doğrulama sürecinde çok önemlidir.

kimlik doğrulama

Kimlik doğrulama, kimliğin ve ilgili izinlerin, üyeliklerin, hakların ve ayrıcalıkların bu ad alanıyla ilgili erişim kontrolü yetkilendirme işlemlerinde kullanılması için bir ad alanı içindeki bir kimlik doğrulama kimliğinin (tek) sahipliğini kanıtlayan bir özne sürecidir. .

Kimlik ve kimliğin sahiplik kanıtı, gelecekteki kimlik doğrulama zorluklarında kullanılmak üzere, en az bir konumda (örn. tablo, veritabanı, kayıt defteri girişi vb.) güvenli bir şekilde önceden saklanmış olmalıdır. Kimlik doğrulama kanıtlarının depolanması genellikle kimlik doğrulamaya doğrudan dahil olan sunucu/hizmet/sitede depolanmaz ve bunun yerine kimlik doğrulamaya dahil olan ve her iki tarafın da (sunucu ve istemci) güvendiği üçüncü taraf sunucu/hizmet/sitelerde depolanır.

Her depolama konumu, kimlik doğrulamasından ödün vermek için potansiyel bir saldırı vektörüdür. Kimlik doğrulamayı kullanan herkes, kimlik doğrulama kanıtlarının nerede saklandığını, bu konumlara

kimin erişimi olduğunu ve bu kimlik bilgilerinin saklanması ne kadar güvenilir olduğunu düşünmelidir. Kimlik doğrulama sırlarının depolanması her zaman yalnızca gerekli sayıda yöneticiyle sınırlandırılmalı ve agresif bir şekilde izlenmeli ve denetlenmelidir. Kimlik doğrulama sırlarının güvenliği ihlal edilirse, kimlik doğrulama işlemine artık tam olarak güvenilemez.

Kimlik doğrulama başarılı veya başarısız olabilir. Yalnızca başarılı, meşru kimlik doğrulamanın bir sonraki işleme yol açması beklenir.

Erişim Kontrol Simgesi

Başarılı bir kimlik doğrulamasından sonra, çoğu durumda, erişim kontrol süreci, bir erişim kontrol nesnesini (örneğin, belirteç, bilet, vb.) test edilen kimliğe ilişkilendirir. Bu erişim denetimi belirtecinin içeriği, sisteme ve protokole göre değişir. Bazı sistemlerde, yalnızca bir dizi sayı veya karakter gibi başka bir benzersiz tanımlayıcı içerebilir. Diğer sistemlerde, grup üyelikleri, izinler, ayrıcalıklar ve diğer gerekli bilgilerin bir listesini içerebilir.

Belirteç, önceden belirlenmiş bir maksimum ömre sahip olabilir veya olmayabilir; bu, sona erdiğinde, özneyi "etkin" bir oturumda kalmaya yeniden kimlik doğrulamaya zorlar. Microsoft Windows'ta, bir erişim denetimi belirteci, bir Kerberos bileti veya bir NTLM veya LM belirteci biçiminde gelebilir. Web sitelerinde ve hizmetlerde, çoğu erişim kontrol belirteci, basit bir metin dosyası olan bir HTML tanımlama bilgisi ile temsil edilir.

Başarılı bir kimlik doğrulamasından sonra, kullanıcıya daha sonra kimlik doğrulama döngüsünün geri kalanı için kullanılan bir oturum erişim kontrol belirteci verilir.

yetki

Yetkilendirme, öznenin bu nesnelere erişimini belirlemek için, şimdi başarıyla kimliği doğrulanmış öznenin erişim denetimi belirtecini önceden izin verilen/güvenli kaynaklarla karşılaştırma işlemidir. Çoğu durumda, bir özneye bir erişim kontrol belirteci verildikten sonra, özne (veya gerçekte özne adına bir süreç veya program) yetkilendirme için erişim kontrol belirtecini gönderir ve öznenin, sona erme tarihine kadar yeniden kimlik doğrulaması yapması gerekmez. jeton. Bir erişim kontrol belirteci verildikten sonra, her yetkilendirme erişim girişimi için kimlik doğrulama test edilmez. Erişim denetimi belirtecine sahip olmak, başarılı kimlik doğrulamanın kanıtı olarak kabul edilir.

ÇOK ÖNEMLİ NOKTA!

Basit parola, biyometrik veya çok faktörlü kimlik doğrulama jetonu olsun, bir kişinin nasıl başarılı bir şekilde kimlik doğrulaması yaptığı önemli değil, kimlik doğrulama başarılı olduğunda, kimliğe atanan kimlik doğrulama jetonu genellikle tüm kimlik doğrulama yöntemleri için aynıdır ve genellikle çok az benzerlik gösterir . kullanılan kimlik doğrulama yöntemi.

Örneğin, bir öznenin dizüstü bilgisayarını ve dizüstü bilgisayarın yerleşik parmak izi tarayıcısını kullanarak Windows ve Active Directory'de oturum açmak için parmak izini kullandığını varsayalım. Kimlik doğrulama işlemi, dizüstü bilgisayarda yerel olarak gerçekleşir. Dizüstü bilgisayarın parmak izi tanıma ve kimlik doğrulama yazılımı ve donanım kombinasyonu, kullanıcının kimliğini başarıyla doğrular. Bu

noktada, kullanıcının parmak izi artık kullanılmamaktadır. Parmak izi, erişim kontrol işlemlerine dahil olmak için ağ çevresinde gönderilmez. Kullanıcının parmak izi kopyalanmaz veya ağa bağlı başka bir bilgisayara gönderilmez, böylece kullanıcı bir dosyaya veya klasöre erişebilir.

Bunun yerine, kullanıcının parmak izi (veya her neyse) kullanılarak kimliği başarılı bir şekilde doğrulandıktan sonra, Windows işletim sistemi onlara bir Kerberos bileti veya NTLM veya LM belirteci verir. Kullanıcının (veya daha doğru bir şekilde yazılmış, kullanıcı adına hareket eden işlemler veya programların) tüm erişim kontrol yetkileri için kullandığı sonuçtaki bilet veya jetondur. Ve eğer bir saldırgan erişim kontrol belirtecine erişebilirse, kimliğinizi nasıl doğruladığınızla ilgilenmezler. Jetonun yasal yollardan sahip olunması veya olmaması, genellikle, o jetonun sahibinin kimliğini başarıyla doğrulamış gibi, yetkilendirme süreçleri tarafından ele alınır. Yetkilendirme sürecinin, o erişim kontrol belirtecinin mevcut sahibinin meşru kullanıcı olup olmadığını veya başarılı bir şekilde kimliği doğrulanmış olup olmadığını bilmenin bir yolu yoktur. Bu önemli gerçek, genellikle bilgisayar korsanları tarafından çok faktörlü kimlik doğrulamasını tehlikeye atmak için kullanılır.

Kimlik doğrulaması için kullanılan kimlik doğrulama yöntemi ile daha sonra yetkilendirme için kullanılan sonuçtaki erişim kontrol belirteci arasında büyük bir fark vardır.

Bu aynı kavram daha genel olarak tüm kimlik doğrulama süreci için geçerlidir. Kimlik doğrulamasından yararlanan saldırganlar, genellikle tüm süreç boyunca uygulamalarda zayıf noktalar ararlar. Kimlik, kimlik doğrulama ve yetkilendirme arasındaki bağlantılarda boşluklar olup olmadığına bakacaklardır... ve aşağıda göreceğiniz gibi genellikle vardır.

MFA'yı hacklemenin önemli bir yolu, kimlik kaydı, kimlik doğrulama gizli depolama, kimlik doğrulama ve yetkilendirmeden tüm kimlik doğrulama sürecindeki zayıflıkları aramaktır.

Tek Yönlü ve İki Yönlü Kimlik Doğrulama

Kimlik doğrulama normalde, genellikle sunucu (kimliği doğrulanan nesne/uygulama/işlem) ve istemci (sunucuya nesne kimlik doğrulaması) olarak adlandırılan iki veya daha fazla taraf arasında gerçekleştirilir ve tek yönlü veya iki yönlü olabilir. Birçok kimlik doğrulama nesnesi, kimlik doğrulama nedenine bağlı olarak hem sunucu hem de istemci görevi görebilir. Bu, fiziksel bir sunucunun her zaman bir sunucu gibi davranmadığını ve bunun tersini söylemektir. Kimlik doğrulama işlemine ek sunucular dahil olabilir ve bu nedenle tek bir kimlik doğrulama olayı sırasında meydana gelen birden fazla kimlik doğrulama olabilir. Buna iyi bir örnek, istemcinin, amaçlanan hedef sunucunun yanı sıra Kerberos kimlik doğrulama sunucusunda kimlik doğrulaması yapması gereken Kerberos'tur.

Çoğu kimlik doğrulama tek yönlüdür, yani istemci sunucuya kimlik doğrulaması yapar veya sunucu istemciye kimlik doğrulaması yapar, ancak en azından aynı kimlik doğrulama olayı sırasında bunun tersi doğru değildir. Bunun çok yaygın bir örneği HTTPS kullanan web sunucularıdır. HTTPS söz konusu olduğunda, web sunucusunun kimliğiyle (genellikle DNS adresi) bağlantılı bir HTTPS/TLS dijital sertifikası vardır. Bir istemci HTTPS üzerinden web sunucusuna bağlandığında, sunucu, kimliğini kanıtlamak ve simetrik anahtarlama materyali oluşturmak için şifreli bir kanalı güvence altına almak için HTTPS dijital sertifikasını istemciye gönderir. İstemci, web sunucusunun HTTPS dijital sertifikasını alır ve güvenilirliğini doğrular. Başarılı olursa, istemci sunucunun söylediği sunucu olduğuna güvenecektir (deneğin kimliğine göre). Tek yönlü kimlik doğrulamada, istemci, en azından aynı işlem içinde, kimliğini sunucuya kanıtlamaz.

İki yönlü, "karşılıklı" kimlik doğrulama ile hem istemci hem de sunucu, aynı kimlik doğrulama sürecinin bir parçası olarak birbirinin kimliğini doğrular. Bir taraf başarısız olursa, diğer taraf otomatik olarak başarısız olur.

Kimlik Doğrulama Faktörleri

Bir kimliğin sahipliğinin kanıtı, kimliği ve bir veya daha fazla kimlik doğrulama faktörünü sağlayan bir özne tarafından yapılır. Kimlik doğrulama faktörü, yalnızca öznenin bildiği veya sağlayabileceği sağlanan bir şeydir ve bunu yaparak, kimliği doğrulanmış kimliğin tek sahibi olduğunu kanıtlar. Genel olarak, yaygın olarak bilinen yalnızca üç temel kimlik doğrulama faktörü türü vardır:

- Bildiğin bir şey

Örnekler şunları içerir: Şifre, PIN, Noktaları Birleştir

- sahip olduğun bir şey

Örnekler şunları içerir: USB belirteci, akıllı kart, RFID verici, dongle

- Sen bir şeysin

Örnekler şunları içerir: Biyometri, parmak izleri, retina taraması

Yukarıda açıklandığı gibi, yalnızca üç ana kimlik doğrulama faktörü türü vardır. Bazen üçten fazla faktöre sahip (örneğin, beş faktörlü) MFA çözümlerini duyacaksınız, ancak bu çözümlerin atıfta bulunduğu şey, aynı üç faktörün birden çok örneğidir. Bir MFA çözümünde faktörlerin en koruyucu olması için faktörlerin farklı olması gerekir.

Tek Faktörden Çok Faktöre

Konsept, bu faktörlerin iki veya üçünün kullanılmasının bir bilgisayar korsanının işini daha zor hale getirmesidir. Örneğin, bilgisayar korsanı sizi bir paroladan mahrum bırakabilir, ancak bir MFA çözümünde kullanılıyorsa, donanım simgenizi çalmak için ek çaba gerektirecektir. Veya kötü niyetli bir kişi MFA donanım jetonunuzu alırsa, onu kullanmak için gerekli olan ilişkili PIN'inize de sahip değilse, bu onun için faydasız olacaktır.

MFA çözümü gibi görünen ancak ek bir faktör gerektirmeyen tek faktörlü donanım çözümleri vardır. Örneğin, Google Security Keys™ ve Yubikeys™'in mevcut sürümleri, tek faktörlü veya çok faktörlü için kullanılabilir. Tek faktörlü uygulamalarında, eğer bir kişi bu donanım cihazlarını bulursa, başka bir şekilde güvende değilse, onları kullanabileceği ve token ile ilişkili dijital kimliği devralabileceği anlamına gelir. Bir bilgisayar korsanı için başka bir kişinin tek faktörlü donanım belirtecini elde etmek, onu çevrimiçi bir paroladan kimlik avına çıkarmaktan daha zor olabilir, ancak bir kez elde edildiğinde, bu kimliğin derhal tehlikeye atılması anlamına gelir. Diğer her şey eşit olduğunda, MFA'ya tüm senaryolarda evrensel olarak

nadiren izin verilmesine rağmen, daha iyi güvenlik için MFA her zaman tek faktörlü kimlik doğrulamadan daha iyidir.

MFA çözümleri her zaman birden çok faktör türü gerektirmeye çalışmalıdır, ancak aynı faktör türünün birden çok örneği bile, tek faktörlü kimlik doğrulama çözümlerine göre güvenliği artırabilir. Ancak okuyucular, aynı kimlik doğrulama faktörünün birden fazla kullanımını, ek kimlik doğrulama faktörü türleri tarafından verilen güvenliğe eşdeğer olarak görmemelidir. Örneğin, bir kullanıcının oturum açmak için hem bir parola hem de bir PIN kullanması gerekiyorsa (her ikisi de aynı türde kimlik doğrulama faktörü ("Bildiğiniz Bir Şey")), o zaman neredeyse bir kullanıcı kadar kolay bir şekilde her ikisinden de kimlik avı yapılabilir. En fazla korumayı sağlayan ek faktör türleridir çünkü başarılı olmak için bilgisayar korsanının tamamen farklı bir şey yapmasını gerektirirler.

Bant İçi ve Bant Dışı Kimlik Doğrulama

Kimlik doğrulama faktörleri, bant içi veya bant dışı olarak kabul edilebilir. Bant içi kimlik doğrulama, kullanılan kimlik doğrulama faktörü yönteminin, birincil oturum açma yöntemiyle aynı iletişim kanalı üzerinden yürütüldüğü anlamına gelir. Bant dışı kimlik doğrulama, kimlik doğrulama faktörünün birincil oturum açma kanalından farklı bir kanal üzerinden gönderilmesidir.

Örneğin, bir internet hizmeti uygulamasında oturum açmaya çalışıyorsanız ve aynı tarayıcıda bir parola ve bir parola kurtarma yanıtı yazmanız gerekiyorsa, bu, her ikisi de bant içi olmak üzere aynı faktörün iki örneği olarak kabul edilir. Ancak, bilgisayarınızda bir şifre ve ayrıca harici cep telefonunuza gönderilen ikinci bir PIN kodunu girmeniz gerekiyorsa, ikinci faktör bant dışı olarak kabul edilir.

Daha da iyisi, YALNIZCA bu kanallarda her iki ayrı bant doğrulama faktörüne de yanıt vermeniz gerekiyorsa ve bunlar “kanallar arası” değilse (yani, bant dışı size gönderilen kimlik doğrulama faktörüne yalnızca diğer faktörle aynı bant), o zaman daha da fazla güvenlik güvencesi sağlar. Aynı cihaz üzerinden gönderilen kimlik doğrulama faktörleri, farklı kanallarda olsa bile, farklı cihazlar üzerinden farklı kanallar kullanan kimlik doğrulama yöntemleri kadar güvenli kabul edilmez.

Ayrı kimlik doğrulama faktörlerinin ve iletişim bantlarının sayısı arttıkça güvenlik güvencesi de artar. Çoğu senaryoda, bir MFA çözümü kullanmak yalnızca güvenliği artırabilir ve MFA, mantıklı olduğu yerde ve zamanda kullanılmalıdır. Ne yazık ki, hepsi değil kimlik doğrulama senaryoları MFA'ya izin verir ve çoğu zaman aynı MFA çözümü değildir. En azından şimdilik (2018 ve önümüzdeki birkaç yıl), kullanıcıların birçok senaryoda yine de tek faktörlü bir kimlik doğrulama yöntemi kullanmaları gerekecek.

MFA'ya izin verildiğinde ve kullanıldığında bile, bazen tek faktörlü kimlik doğrulama çözümleri kadar kolay bir şekilde saldırıya uğrayabilir. MFA iyidir, ancak güvenlik güvencenize fazla güvenmeyin. Güvenliği artırmak için iyi bir araçtır, ancak MFA'nın güvenlik güvencesini geliştirmesi ile MFA'nın hacklenemez olması arasında büyük bir fark vardır. Farkı anlamak, MFA çözümlerine güvenen tüm varlıklar ve güvenlik yöneticileri için çok önemlidir. Anahtar, bir güvenlik kurtarıcısı olarak MFA'ya aşırı derecede güvenmemektir.

Bunu bir perspektife oturtmak gerekirse, MFA çözümlerini kullanan çoğu şirket hala saldırıya uğruyor. Bunun nedeni, güvenliğin ihlal edilmesinin en popüler nedenlerinin (örneğin, sosyal mühendislik, istemci tarafı saldırıları, yama uygulanmamış yazılımlar ve kodlama hataları) MFA tarafından tam olarak azaltılamamasıdır. MFA, bazı bilgisayar korsanlığı biçimlerini bazen önemli ölçüde azaltabilir. Ancak ilgili

şirketler başarılı bir şekilde saldırıya uğramalarının en büyük nedenlerini ortaya koymazsa, MFA bilgisayar korsanlarının ve kötü amaçlı yazılımların başarılı olmasını engelleyemez. MFA iyidir, ancak çözülmesi gereken büyük bir bulmacanın yalnızca bir parçasıdır. MFA tek başına bir şirketi “ hacklenemez ” hale getiremez. Gerçekten de, MFA'nın kendisi hacklenemez değildir . MFA kullanan çoğu şirket hala başarılı bir şekilde saldırıya uğruyor.

Çok Faktörlü Kimlik Doğrulamayı Hackleme

Teknik incelemenin bu bölümü, MFA çözümlerini hacklemenin bir düzineden fazla yolunu tartışacaktır. Bu saldırıların çoğu, milyonlarca MFA korumalı kullanıcıya karşı başarıyla kullanılmıştır. Saldırı yöntemlerinin çoğu, haber raporlarına bağlantılar ve bunlardan yararlanma örnekleri içerecektir. Henüz halka açık bir saldırıda kullanılmayan teorik saldırılar bu şekilde not edilir.

Çoğu durumda, belirli bir MFA çözümü türü birden fazla bilgisayar korsanlığı yöntemine karşı hassastır ve bu nedenle saldırılar yalnızca tek bir MFA çözümü türüne karşı 1:1 değildir. Her saldırı, sıklıkla kendisine karşı kullanıldığı ancak çoğu zaman diğer MFA çözümlerine karşı da kullanılabileceği MFA yöntemine karşı gösterilir.

MFA'yı Hacklemenin Genel Yolları

MFA çözümlerinin nasıl saldırıya uğradığını düşünürken üç genel yol vardır:

- Sosyal mühendislik
- Teknik
- Karışık

Sosyal mühendislik, MFA çözümünü yanlışlıkla baypas veya yanlış kullanıma neden olacak şekilde kullanan ilgili insan unsuruna atıfta bulunur. Teknik manipülasyon, insan kullanıcının bir hata yapmasını gerektirmeyen sömürü ve manipülasyon yöntemlerini ifade eder. Aşağıda sunulan bilgisayar korsanlığı yöntemlerinin çoğu, hem insan hem de teknik zayıflıkların bir karışımını gerektirir.

Bilgisayar korsanlığı yöntemleri ne olursa olsun, kimlik, kimlik doğrulama gizli depolama, kimlik doğrulama veya yetkilendirme gibi kimlik doğrulama adımları arasındaki zayıflıklardan yararlanma girişimleridir. Saldırıları, bu adımlardan birinin veya daha fazlasının kötü niyetli olarak kesilmesi, değiştirilmesi veya yanlış temsil edilmesi veya bu adımlar arasında geçiş yapılmasıdır.

Not: Çoğu zaman bir MFA çözüm sağlayıcısı, MFA çözümünün kendisinin başarısız olmadığını söyleyerek çözümlerini başarılı bir kanıtlanmış saldırıya karşı savunur. Bu teknik anlamda doğru olsa da, MFA çözümleri yalnızca doğrudan saldırıların sayıldığı steril laboratuvarlarda nihai olarak test edilmez. MFA çözümü herhangi bir nedenle kullanıcıyı başarısızlığa uğratırsa, kullanıcının kafasında MFA çözümü başarısız olur. MFA çözümünün kendisinin teknik olarak sorumlu olup olmadığına dair ayrıntılarla pek ilgilenmez. Kullanıcı sadece kendisinin başarısız olduğunu bilir.

Oturum çalma

Oturum kaçırma, başarılı, meşru bir kimlik doğrulamanın ardından meşru kullanıcının oturumunun yetkisiz bir tarafça ele geçirildiği bir bilgisayar korsanlığı yöntemidir. Bunun nedeni genellikle ortaya çıkan erişim kontrol belirtecinin çalınmasıdır. Başlangıçta kullanıcı için şeffaf olabilir veya kullanıcı, geleneksel bir kimlik avı e-postası kadar basit bir şeye yanıt vererek farkında olmadan kendi bilgisayar korsanlığına katılabilir. Nasıl yapılırsa yapılsın, yetkisiz saldırgan erişim kontrol belirtecinin kontrolünü ele geçirdikten

veya kopyaladıktan sonra, yetkisiz davetsiz misafir oturumu meşru kullanıcıdan uzaklaştırabilir veya hileli bir şekilde manipüle edebilir. Bir oturum ele geçirildiğinde, saldırgan esasen oturumun tamamı için saldırıya uğramış kullanıcının kimliğini varsayar. Oturum kaçırma onlarca yıldır var ve kimlik doğrulama korsanlığının en yaygın biçimlerinden biridir ve MFA'ya karşı kullanıldığında da aynı derecede başarılı olabilir. Oturum kaçırma, aşağıdakiler de dahil olmak üzere çeşitli farklı yöntemler kullanılarak gerçekleştirilebilir:

- Oturum Benzersiz Tanımlayıcı Tahmini
- Ağ iletişim kanalında oturum belirtecinin çalınması
- Son noktada oturum belirtecinin çalınması

Oturum Benzersiz Tanımlayıcı Tahmini

Bir kullanıcı, MFA kullanarak veya kullanmayarak bir web sitesinde başarılı bir şekilde kimlik doğrulaması yaptığında, benzersiz bir oturum belirteci (yani, çerez) veya URL dizesi olması gereken ve her ikisinin de rastgele seçilmiş birer içermesi gereken URL dizesi geri gönderilir, meşru kullanıcıyı ve web sitesindeki oturumunu belirten benzersiz tanımlayıcı. Benzersiz tanımlayıcının, diğer üçüncü tarafların (yani bilgisayar korsanları) diğer kişilerin belirteçlerinin veya URL dizelerinin ne olduğunu veya olacağını tahmin edebilmesi için yeterince tahmin edilebilir olmaması önemlidir.

Oturum korsanları, öngörülebilir benzersiz tanımlayıcılara sahip web sitelerini arar. Bilgisayar korsanları bunu genellikle hedeflenen bir web sitesine birden çok, farklı, kimliği doğrulanmış kullanıcı olarak katılarak yapar ve her kullanıcı için çerez veya URL dizesine yerleştirilen benzersiz tanımlayıcılar arasındaki ortak noktaları arar. Bazen rastgelelik yoktur ve sayılar farklı kullanıcılar arasında mükemmel bir şekilde sıralıdır ve tahmin edilebilir. Saldırgan kalıbı tanıdığında, hangilerinin kendisine istenen hedef hesabı veya erişimi vereceğini görmek için farklı tanımlayıcı numaraları deneyecektir.

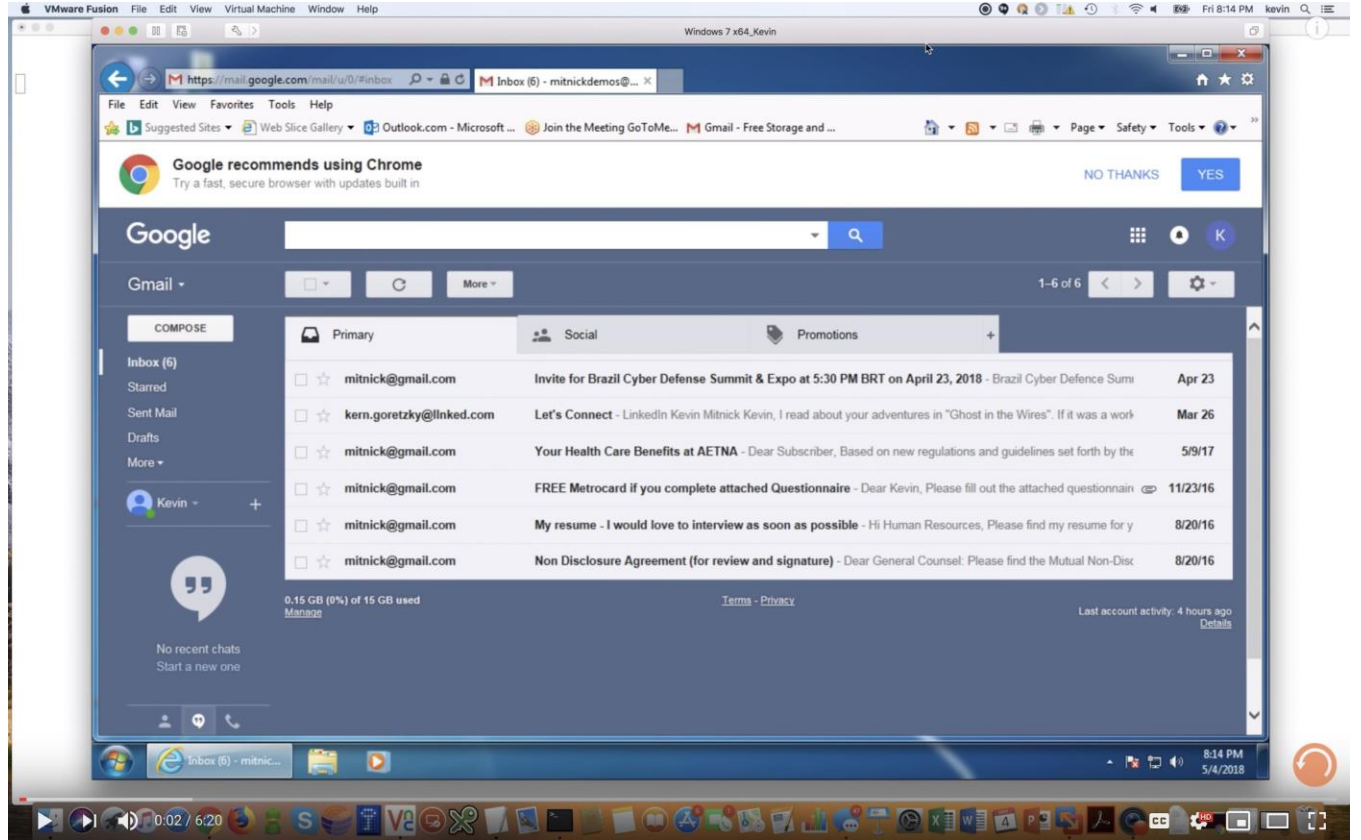
Bu tür bir saldırı ile saldırgan, hedeflenen kurbanı hiç dahil etmeden her kullanıcıyı kendi konumunun güvenliğinden "tahmin edebilir". Dolayısıyla, MFA dahil olsun veya olmasın, saldırgan başarılı bir kimlik doğrulamasından sonra sözde benzersiz tanımlayıcı bilgileri tahmin edebiliyorsa, tüm oturumlar için olmasa da en azından oturum için esasen "kullanıcı olur". Bu tür güvenlik kodlama hatası, onlarca yıl önce olduğu kadar popüler olmasa da, tüm web sitesi kodlayıcıları sorunun farkında olmadığı için hala yeterince sık oluyor.

Oturum Ele Geçirme Proxy Saldırısı

Bu tür bir saldırıda, bilgisayar korsanının önce istemci ve sunucu arasında başarılı bir şekilde yer alması gerekir (yani, ortadaki adam saldırısı (MitM)). Bir MitM saldırısı oluşturmak çoğu insanın düşündüğü kadar zor değildir. Bir kafede olduğu gibi, herhangi bir paylaşılan kablosuz ağ ortamında, çeşitli ücretsiz bilgisayar korsanlığı araçları kullanılarak yerel olarak gerçekleştirilebilir. Uzaktan, internet üzerinden, kurbanı sahte "benzer" veya "benzer" bir URL web sitesini ziyaret etmeye ikna etmek için bir kimlik avı e-postası göndererek gerçekleştirilebilir. Kullanıcı bir MitM kurbanı olduğunda , kullanıcının gönderdiği her şey MitM proxy hizmeti tarafından ele geçirilebilir.

Kevin Mitnick MFA Videosunu Hackliyor

Ancak bu tür bir saldırıyı açıklamanın en iyi yolu, birini çalışırken izlemektir.



İşte KnowBe4'ün Hacking Baş Sorumlusu Kevin Mitnick tarafından hazırlanan bir video,

(<https://blog.knowbe4.com/heads-up-new-exploit-hacks-linkedin-2-factor-auth.-see-this-kevin-mitnick-video>) bir kurbanın MFA çözümünde nasıl kimlik avı yapılacağını gösteriyor. Kevin altı dakika içinde size bunun ne kadar kolay olduğunu gösterecek. Videoyu izledikten sonra, nasıl yapıldığının özet adımlarını görmek için buraya geri gelin. Bu örnekte Kevin şunları yapar:

1. Kevin, gerçekten kötü bir vekil olan sahte bir benzer/ses benzerliği web sitesi kurdu
2. Kullanıcıyı kötü proxy web sitesini ziyaret etmesi için kandırdı
3. müşteriymiş gibi davranan proxy'nin meşru web sitesine sunulan kimlik bilgilerini girdi
4. kullanıcının oturumunu devralmak için tekrar oynattığı meşru oturum belirtecini geri gönderdi

Kevin, Evilginx'i kullandı (<https://breakdev.org/evilginx-advanced-phishing-with-two-factor-authentication-bypass/>) MitM proxy hack aracı için , ancak aralarından seçim yapabileceğiniz düzinelerce araç var. Bu, MFA dahil olsa bile, yüzlerce olmasa da düzinelerce oturum ele geçirme yönteminden yalnızca bir örnektir . Hepsinin ortak noktası, oturumu çalmak için oturum bilgilerinin yakalanmasıdır.

Sahte Kimlik Doğrulama

Hack'leri gerçekleştirmenin en kolay yollarından biri hiç hack'lememektir. Bu özel senaryoda, kullanıcıya sunulan tüm kimlik doğrulama deneyimi , tamamen veya kısmen sahte bir benzer web sitesi tarafından taklit edilir. Kurban, MFA belirtecine sahip olduğu bir siteyi ziyaret etmesi için kandırılır. Sahte site daha sonra tüm normal oturum açma deneyimini simüle eder. Kullanıcı bir oturum açma adı ve/veya parola girebilir ve ardından MFA çözüm yanıtı için (sahte) istenebilir. Sahte web sitesi daha sonra giriş deneyimi başarılı gibi davranır ve kurbanı saldırganın istediği açılış sayfasına götürür.

Örneğin, kullanıcı, Google'a katılan bir web sitesinin kimliğini doğruladığını düşünüyor.

Doğrulayıcı MFA uygulaması. Kullanıcı Google Authenticator MFA uygulamasını açtığında, web sitesi gerçekten Google Authenticator MFA kimlik doğrulamasına katılıp katılmadığına bakılmaksızın herhangi bir web sitesinde kullanılabilecek ve yazılabilecek 6 basamaklı bir kod sunar. Kullanıcıdan Google Authenticator kodlarını girmesi istenir ve tüm deneyimin sahte olduğunu bilmeden bunları girer.

Bu tür bir saldırı kullanarak, sahte, haydut web sitesi, kullanıcının ortaya çıkan oturum belirticini yakalamaz. Ve bu nedenle, kullanıcının gerçek web sitesine giriş yapamazlar veya kullanıcının gerçek oturumunu kontrol edemezler. Ayrıca, kullanıcının genellikle görmeyi beklediği normal, kullanıcıyla ilgili içeriği görüntüleyemezler. Saldırganın web sitesi, ek güvenlik bilgileri gerekiyormuş gibi davranabilir ve kullanıcıdan, parola kurtarma sıfırlama soruları ve/veya yanıtları, sosyal güvenlik bilgileri, kredi kartı bilgileri gibi saldırıyanın yakalamak istediği ek "nitelikli" bilgileri girmesini isteyebilir. vb. Kullanıcının gizli bilgilerini ele geçirdikten sonra saldırıyan, web sitesinde bir hata yaşamış gibi gösterebilir ve kullanıcıyı gerçek web sitesine yönlendirebilir.

Bazı MFA çözümleri, önceden kaydedilmiş gerçek web sitesi dahil olmadıkça bir MFA yanıtı göndermeyerek bu tür bir tuzaktan kaçınmaya çalışır. Bu şekilde, istek güvenilir bir web sitesi tarafından başlatılmadığı sürece, kullanıcıya sahte kimlik doğrulamaya katılması için bir kod bile verilmez. Hileli web siteleri, kullanıcının beklediği gibi bir kod oluşturmak için MFA çözümünü elde etmek için kullanıcının yazdığı bilgileri kullanıcının gerçek, önceden kayıtlı web sitesine göndererek bu korumayı aşmıştır. Bu hack, kullanıcı sahte web sayfasıyla etkileşime girdiğinde diğer amaçlanan, meşru web sitesinde oturum açmak için bile kullanılabilir.

Bazı MFA çözümleri, çeşitli farklı yöntemler kullanarak bu tür saldırılarla savaşıyor. Birincisi, MFA çözümü, kullanıcının tespit edilen konumuyla birlikte oturum açmakta olan web sitesinin URL'sini gönderebilir. Bir MitM saldırıyanı muhtemelen kurbandan farklı bir konuma sahip olacaktır. Bu nedenle, kullanıcı varsayılan oturum açma cihazını tamamen farklı bir konumda görürse, bir MitM saldırısının gerçekleştiğinden şüphelenebilir. Ancak, bilgisayar korsanları kullanıcının mevcut konumunu da aktarabilir ve gerçek web sitesi bundan daha akıllıca olmaz. Başka olası korumalar da vardır, ancak her biri artan kullanıcı sürtünmesi, hayal kırıklığı yaratır ve oturum açma sürecini uzatır. MFA çözümü gerçekten saldırıya uğramadığından, bu tür MFA kesmesinden kaçınmak çok zordur.

Uç Noktadaki Adam Saldırıları

Bu genel bir saldırı kategorisidir ve temelde, saldırıyanın bir cihazda yönetici erişimi elde etmesi durumunda cihazın yaptığı hiçbir şeye güvenilemeyeceğini söyleyen bir genel saldırı kategorisidir. Bilgisayar korsanı, oturum açmış kullanıcının yapabileceği her şeyi yapabilir, bu nedenle kullanıcı bir web sitesinde veya uygulamada kimlik doğrulaması yaparsa, bilgisayar korsanı, meşru kullanıcının yapabileceği her şeyi yapmak için esasen bu kimlik doğrulamaya geri dönebilir. "Yerel" bir bilgisayar korsanı, verilen oturum belirteçlerini doğrudan çalabilir ve önceki bölümde açıklanan saldırıları taklit edebilir, ancak önce bir MitM saldırısı yapmak zorunda kalmadan.

Banco Truva Atları

Bir Uç Noktadaki Adam saldırıyanı, meşru kimliği doğrulanmış kullanıcı ilk oturumu kullanırken ikinci bir gizli tarayıcı oturumu da başlatabilir. Bu genellikle bankacılık truva atları (Güney Amerika'da çok popüler olan bancos trojanları olarak da bilinir) tarafından kullanılan bir yöntemdir. Bancos truva atı, sosyal mühendislik veya yama uygulanmamış yazılım gibi geleneksel kötü amaçlı yazılımların girmek için kullandığı herhangi bir yöntemi kullanarak yerel bilgisayarı sömürebilir. Ardından truva atı, geçerli

kullanıcının tarama seçimlerini izleyerek “banka”, “Bank of America” gibi önceden tanımlanmış anahtar sözcükleri arar.

Bancos , kullanıcının hedeflenen bir finans kurumuna giriş yaptığını gösteren izlenen bir anahtar kelime tespit ettiğinde, bancos trojan ikinci, gizli bir tarayıcı oturumu başlatır. Meşru kullanıcı, MFA'yı kullanarak veya oturum açmayarak, sadece hesabına bakarken, bancos trojanı iletişim bilgilerini değiştirir ve kullanıcının fonlarının başka bir sahte banka hesabına büyük bir elektronik transferini başlatır. Banka teyit etmek için ararsa veya e-posta gönderirse, yeni, sahte iletişim bilgilerini kullanırlar.

Bankalar, günümüzün SMS MFA mesajlarına çok benzeyen ve yalnızca belirli bir işlem için iyi olan “doğrulama kodları” göndererek karşılık verdiler. Bancos truva atları, kullanıcının bir kod gerektiren bir işlem yapmasını bekleyip ardından yalnızca sahte işlemi göndererek yanıt verdi. Kullanıcının kastettiği şeyin banco trojan işlemi olmadığını bilmeyen banka, son kullanıcıya sadece banco trojan işlemi için çalışan bir MFA kodu gönderir. Son kullanıcı, ikinci bir gizli tarayıcı oturumu olduğundan habersizdir ve bancos trojanının mutlu bir şekilde kullandığı kodu yazar.

Bancos truva atları, Güney Amerika bankalarını MFA çözümlerini erken ve sık kullanmaya itti. Dünyanın habercisi olan bancos truva atları, MFA kullanımına yeni adapte oldu ve yüz milyonlarca dolar çalmaya devam etti. Bu tür saldırılara karşı savunma, bankaların yalnızca onay kodunu değil, sözde işlemin tüm detaylarını (örneğin dolar tutarı, işlem türü vb.) onay koduyla birlikte göndermesidir. Kullanıcının ne yapmak için bir onay kodu aldığını anlaması gerekir. İki taraf da birbirine güvenmemeli.

Mali işlem MFA onay mesajları, kullanıcının onaylamadan önce ayrıntıları görebilmesi için her zaman sözde işlemin kritik ayrıntılarını göndermelidir.

Kötü Amaçlı MFA Yazılımında Değişiklik

Bir bilgisayar korsanının kurbanın cihazına veya işletim sistemine yönetici erişimi varsa, yazılım ve donanımın yapabileceği her şeyi yapabilir. Tüm MFA çözümleri, MFA seçeneğini etkinleştirebilmek ve kullanabilmek için ilgili bir yazılım parçasına (örn. program, API, arayüz vb.) ihtiyaç duyar. MFA seçeneğinizi yazılımda yüklemesiniz ve “başlatmasanız” bile, bu birileri tarafından yapılmıştır veya varsayılan olarak etkinleştirilmiştir.

Bilgisayar korsanları, MFA yazılım programını veya arabirimini (Microsoft Windows'ta Şifreleme Hizmet Sağlayıcıları (CSP) veya Anahtar Depolama Sağlayıcıları (KSP) olarak bilinir) kötü niyetli olarak değiştirebilir, böylece MFA programı tarafından sağlanan koruma zayıflatılabilir veya tamamen devre dışı bırakılabilir. Bu özel saldırı türünün, bu makalenin yazarı tarafından halka açık olarak kullanıldığı bilinmiyor, ancak kolaylıkla kullanılabilir. Kolluk kuvvetleri ve istihbarat teşkilatları tarafından kullanılan ilgili bir saldırı, katılan bir hedefin ağ düğümünü tehlikeye atmak ve hedefin şifrelenmiş içeriğini okuyabilmeleri için iletişimleri şifrelemek için kullanılan özel veya simetrik anahtarları çalmaktır.

Kötü Amaçlı MFA Donanım Değişiklikleri

Kolluk kuvvetleri ve istihbarat teşkilatları, aksi takdirde güvenilen MFA donanım donanımını, hedeflerin bu donanıma olan güveninin daha kolay tehlikeye atılabilmesi için değiştirmiştir. Bazı durumlarda, MFA donanım çözümleri, normalde sağlanan korumanın hiçbirini sağlamayacak şekilde fiziksel olarak

değiştirildi. Diğerlerinde, yetkililer tarafından bilinen önceden tanımlanmış şifreleme anahtarları, daha sonra amaçlanan hedeflere yönlendirilen MFA çözümlerine yerleştirildi. Amaçlanan hedefler daha sonra, ya çok az koruma sağladıklarında ya da hiç koruma sağlamadıklarında ya da yetkililer tarafından istendiğinde uzlaşmaya izin verdiklerinde, tamamen güvenli olduklarını düşünerek MFA çözümlerini kullanırlar.

Savunma: Son kullanıcıların kötü niyetli bir şey yüklemek için sosyal mühendislik yapmamalarını sağlamak ve cihaz ile yazılımın tamamen yamalandığından emin olmak da dahil olmak üzere, uç noktadan kötü niyetli olarak yararlanılmasını önlemeyi içerir.

Önemli bir vakada, Birleşik Krallık ve ABD hükümet casuslarının, 2011 yılında dünyanın en büyük SIM kart üreticisi Gemalto'da üretilen beş milyardan fazla cep telefonu SIM kartı özel şifreleme anahtarının güvenliğini ihlal ettiği belgelendi (<https://www.theregister.co.uk>). /2015/02/19/nsa_and_gchq_hacked_worlds_largest_sim_card_company_to_steal_keys_to_kingdom /) (aşağıdaki bir sonraki bölümde daha ayrıntılı olarak ele alınmıştır). Muhtemelen cep telefonunuzun şifreleme anahtarını içerir. Aşağıda 2015 yılında *The Register*'in hırsızlığı hatırlatan bir başlığı var :

Did NSA, GCHQ steal the secret key in YOUR phone SIM? It's LIKELY

Snowden leaks reveals how spies can crack encryption on calls worldwide

By Iain Thomson in San Francisco 19 Feb 2015 at 22:50

149

SHARE ▼

SIM Değiştirme Saldırıları

Çoğu cep telefonu ve hücresel ağ sağlayıcısı, bir abonenin kişisel ve cep telefonu benzersiz tanımlayıcılarını, bir abonenin kişisel ve cep telefonu benzersiz tanımlayıcılarını, fiziksel (veya giderek sanallaşan) küçük bir bellek kartında saklar.

Abone Kimlik Modülü (SIM). Ayrıca, kullanıcının resimleri ve iletişim bilgileri gibi uygulama verilerini tutan cep telefonu için depolama işlevi görebilir. Çoğu aşağıdaki resme benzer:

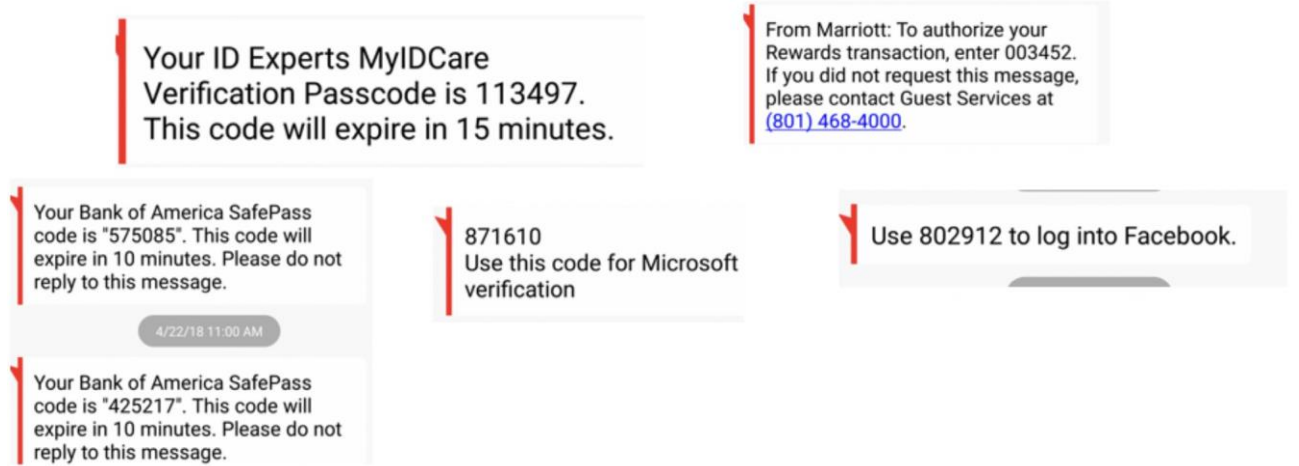


Bir kullanıcı yeni bir cep telefonu aldığında, genellikle mevcut SIM kartını yeni telefona taşıması veya SIM'deki bilgileri yeni telefona aktarması gerekir (SIM takas olarak bilinir). SIM, cep telefonunu belirli bir hücresel şebeke sağlayıcısına (örneğin, AT&T, Verizon Wireless, vb.) "bağlayan" ve abonenin cep telefonu numarasını cep telefonuna iliştiren şeydir.

On yıldan uzun bir süredir bilgisayar korsanları meşru bir abonenin SIM bilgilerini elde ediyor ve bu bilgileri ellerindeki bir telefona aktarıyor. Bu, bilgisayar korsanının yerel bir cep telefonu mağazasına şahsen gitmesi ve cep telefonunu yükseltmeye veya değiştirmeye çalışan meşru abone gibi davranması da dahil olmak üzere birçok yolla yapılabilir. Ayrıca, hücresel ağ sağlayıcısının teknik desteği aracılığıyla uzaktan yapıldı ve cep telefonu mağazalarındaki çalışanlara kötü niyetli SIM takaslarına bilerek katılmaları için rüşvet bile verildi. SIM değişimi yapıldığında, cep telefonunuz çalışmayı durdurur ve telefonunuza gönderilen her arama ve Kısa Mesaj Servisi (SMS) artık bilgisayar korsanının telefonuna gönderilir.

Kötü amaçlı SIM takasları genellikle bilgisayar korsanının önce hedeflenen kurbandan bazı özel bilgiler toplamasını gerektirir. Bir hücresel ağ sağlayıcısının teknik desteğini kandırmak veya yerel bir mağazaya girmek için genellikle kurbanın telefon numarasına, adına, çevrimiçi oturum açma adına ve/veya kimlik bilgilerine ve ev adresine ihtiyaç duyacaktır. Bunu genellikle, kurbanı yönelik önceki bir veya daha fazla kimlik avı saldırısından gerekli bilgileri alarak veya bilgileri güvenliği ihlal edilmiş başka bir veritabanından alarak başarır.

Hileli SIM takasları milyonlarca kez gerçekleşti. Bu, çoğunlukla yalnızca bir kullanıcının sesli arama hizmetini etkilerken, kullanıcının SMS mesajlarını kötü niyetli bir şekilde yeniden yönlendirmek için daha sık yapılmaktadır. Bu bir sorundur, çünkü hemen hemen her küresel hizmet sağlayıcı tarafından kullanılan, gezegendeki en popüler MFA seçeneği SMS tabanlıdır. Her cep telefonu kullanıcısı, güvenilir satıcılardan şüpheli sahte işlemleri doğrulamasını isteyen veya bir MFA oturum açma işlemini tamamlamak için tarayıcılarına MFA tarafından oluşturulan kodları yazmalarını isteyen mesajlara alışkındır. Aşağıda bazı yaygın örnekler verilmiştir:



Bu nedenle, bir bilgisayar korsanı kötü niyetli bir SIM takası yaptığında, bu SMS tabanlı MFA mesajları sizinki yerine bilgisayar korsanının cep telefonuna gönderilir. Bilgisayar korsanı daha sonra yanlış yönlendirilmiş SMS tabanlı MFA mesajını kullanarak çevrimiçi hesabınızı tehlikeye atabilir. Bu o kadar çok oldu ki, bilgisayar güvenliği ve kimlik doğrulama için federal yönergeler yayınlayan ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), son Dijital Kimlik Yönergeleri, NIST Özel Yayını 800-63'te söyledi.

(<https://pages.nist.gov/800-63-3/>) , SMS tabanlı MFA çözümlerini meşru kimlik doğrulama olarak kabul etmeyecektir. Bu, yıllar sonra neredeyse her büyük satıcının, daha güçlü ve daha iyi çözümlere sahip olanlar da dahil olmak üzere, SMS tabanlı MFA çözümlerini kullanması gerçeğiyle karmaşılaşıyor. SMS tabanlı MFA çözümleri, MFA kullanan dünyanın en büyük satıcılarının çoğu için ya varsayılan ya da yedekleme seçeneğidir.

Dünyanın en büyük ve en kötü şöhretli hacklerinden bazıları SIM değiştirmeyi içeriyor. Bir kripto para milyoneri kripto cüzdanından 24 milyon dolardan fazla çalındı

(<https://www.bankinfosecurity.com/att-sued-over-24m-cryptocurrency-sim-hijack-attacks-a-11365>)

çünkü SMS tabanlı MFA'ya dayanıyordu. SIM bilgilerini izinsiz aktardıkları için AT&T'ye 224 milyon dolar dava açtı. 2018'de Reddit'in şirket ağını tehlikeye atmak için SIM tabanlı bir saldırı da kullanıldı; bu saldırı Reddit'in kaynak kodunun ve ağ oturum açma kimlik bilgilerinin tehlikeye atılmasına neden oldu. İşte ilgili bazı saldırı bağlantıları:

- Reddit saldırı bilgisi:

[https://www.wired.com/story/reddit-hacked-thanks-to-woefully-insecure-two-factor-](https://www.wired.com/story/reddit-hacked-thanks-to-woefully-insecure-two-factor-setup)

- Bir başka harika SIM takas örneği:

<https://krebsonsecurity.com/2018/08/florida-man-arrested-in-sim-swap-conspiracy/>

<https://coolwallet.io/smartphone-crypto-hack/>

https://motherboard.vice.com/en_us/article/a3q7mz/hacker-allegedly-stole-millions-bitcoin-sim-swapping

<https://krebsonsecurity.com/2018/08/reddit-breach-highlights-limits-of-sms-based-authentication/>

En azından SMS tabanlı MFA çözümlerinin MFA olmayan çözümlerden (örneğin şifreler) daha iyi olduğu konusunda çok gerçek bir iddia var. Bir saldırganın SIM takası yapması, birinin oturum açma adı ve şifresini phishing'den çok daha fazla iş gerektirir, ancak NIST'e göre, yeterince güvenilir değil. Yeterince güvenilir değilse, neden kullanıyorsunuz? Ne yazık ki, bugünün dünyasında, daha iyi, tıpkı yaygın bir çözüm gelene kadar muhtemelen buna zorlanacaksınız.

Savunmalar: Kişisel bilgilerinizi dağıtmak için sosyal mühendislik uygulanmayın, cep telefonu satıcınızın kötü niyetli SIM takaslarını önleyen politika ve prosedürleri olduğundan emin olun ve daha da önemlisi, mümkün olduğunda SMS tabanlı MFA yerine application-MFA kullanın.

SMS Hileli Kurtarma


SMS mesajı oluşturma meşruiyetinin, SMS'in içinde izleyici tarafından kolayca doğrulanamamasında doğal bir sorun vardır. Herkes herhangi biri olduğunu iddia edebilir ve herhangi bir mesaj gönderebilir. Bu zayıflık, bilgisayar korsanlarına potansiyel kurbanlara sahte talimatlar gönderme fırsatı verir. Bu tür bir saldırıya örnek olarak SMS Rogue Recovery korsanlığı denir. SMS Rogue Recovery korsanlığının çalışması için bilgisayar korsanının yalnızca kurbanın e-posta adresini (zorla SMS kurtarmaya izin veren bir hizmetin) ve ilgili telefon numarasını bilmesi gerekir. Bunlar, erişilmesi zor bilgi parçaları değildir.

Bu bilgilerle bilgisayar korsanı, kurbanın e-posta sağlayıcısından geldiğini iddia ederek kurbanı sahte bir SMS kurtarma mesajı gönderir. Mesaj yanlışlıkla, kurbanın e-posta hesabının meşru sahipliğini ve kullanımını doğrulamak için kurbanın SMS göndericisine gönderilen bir yetkilendirme kodunu yazmasını gerektirecek bir olayın gerçekleştiğini gösteriyor (aşağıdaki örnek sahte SMS kurtarma mesajına bakın) .

Adım 1: Örnek: Hacker, kurbanı gelecek yasal SMS kurtarma koduna hazırlamak için sahte SMS kurtarma mesajı gönderir.

Bu sahte mesajın neredeyse her şey olabileceğini unutmayın. SMS mesajlarının kendileri, belki HTTP/HTTPS bağlantıları veya listelenen e-posta adresleri ile yalnızca düz metindir. Bir SMS mesajında, gönderenin veya mesajının meşru olup olmadığını gösteren hiçbir şey yoktur.

Ön uyarı mesajını gönderdikten sonra, bilgisayar korsanı, e-posta sağlayıcısına şifresini unutmuş meşru kullanıcıymış gibi



From Google Security: We have detected a rogue sign-in to your goodguy@gmail.com account credentials. In order to determine the legitimate login we're going to send a verification code to your previously registered phone number from another Google support number. Please re-type the sent verification code in response to this message or your account will be permanently locked.

davranarak kurbanın e-posta hesabını kasıtlı olarak SMS kurtarma moduna gönderir (aşağıdaki adımlara bakın): e-posta sağlayıcısının, e-posta hesabını kurtarma moduna sokan bilgisayar korsanının meşru kullanıcı olup olmadığını bilmesinin hiçbir yolu yoktur.

Adım 2: Örnek: Hacker kurbanın e-posta sağlayıcısının oturum açma sayfasına gider ve kurban oturum açma parolasını unutmuş gibi davranır.

Hizmet genellikle bir veya daha fazla oturum açma kurtarma yöntemi sunar.

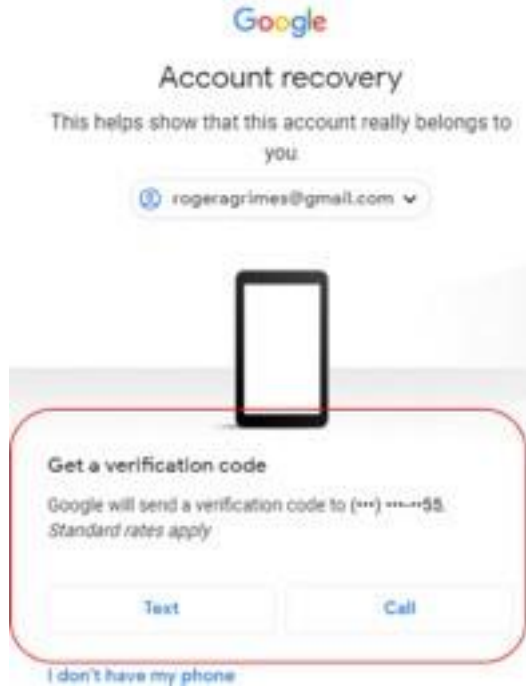
Adım 3: Örnek: Bilgisayar korsanı, kurbanın e-posta hizmetinden alternatif kurtarma seçeneğini seçer.

Hacker, kullanıcının önceden tanımlanmış telefon numarasına bir SMS doğrulama kodu göndermeyi seçer.

Adım 4:
Örnek:
Hacker,

telefon

Meşru



Google

Account recovery

This helps show that this account really belongs to you.

rogeragrimes@gmail.com

Get a verification code

Google will send a verification code to (***). Standard rates apply.

Text Call

[I don't have my phone](#)



Google

Account recovery

rogeragrimes@gmail.com

Enter the last password you remember using with this Google Account

Enter last password

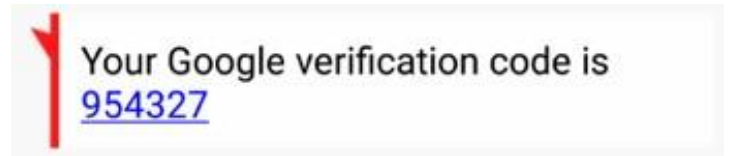
Try another way

Next

kullanıcının önceden tanımlanmış numarasına bir SMS doğrulama kodu göndermeyi seçer.

kullanıcı, e-posta satıcısından SMS kurtarma doğrulama kodu alır.

Örnek: Adım 5: Kullanıcıya meşru kurtarma yöntemi doğrulama kodu gönderilir.



Your Google verification code is

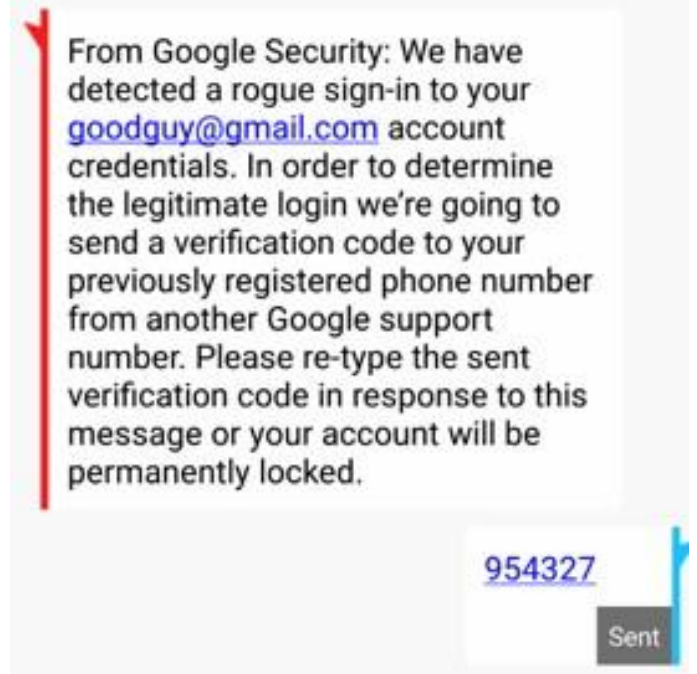
954327

Örnek: Adım 6: Kullanıcı, bilgisayar korsanının orijinal ön uyarı SMS mesajına yanıt olarak meşru SMS kurtarma doğrulama kodunu geri yazar.

Hacker gönderilen meşru kurtarma SMS doğrulama kodunu alır ve bunu e-posta sağlayıcısının web formuna yazarak hesabın kontrolünü ele geçirir.

SMS Rogue Recovery Hacking'e Karşı Savunma

- Hileli kurtarma mesajlarının farkında olun
- SMS kurtarma PIN'lerinin (genellikle) tekrar SMS'e değil, tarayıcılara ne zaman yazılması gerektiğini öğrenin
- Mümkün olduğunda MFA kullanın
- Alternatif e-posta tabanlı kurtarma yöntemlerinden kaçınmaya çalışın
- SMS tabanlı kurtarma tabanlı yöntemlerden kaçınmaya çalışın
- Kurtarma hesabı yöntemlerinizle ilgili telefon numaralarının herkese açık olarak gönderilmesini en aza indirmeye çalışın

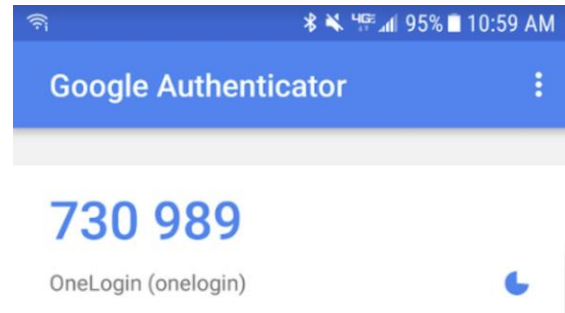


Not: Özellikle bu örnekte kullanılan Google, SMS doğrulama kodlarının ötesinde, kullanıcının yalnızca meşru olarak kabul etmeye karar verebileceği birçok farklı kurtarma yöntemi sunmakta ve böylece bu özel saldırı örneğini engellemektedir. Ancak, genellikle Google'ı ve diğer benzer e-posta hizmetlerini, varsayılan olarak birçok farklı yöntem sunuyorsa, yalnızca sizinle belirli bir kurtarma yöntemi kullanmaya zorlamanın bir yolu yoktur.

Not: FIDO U2F ve ilgili kurtarma yöntemlerini kullanan bu yöntemin halka açık gösterimlerini de gördüm.

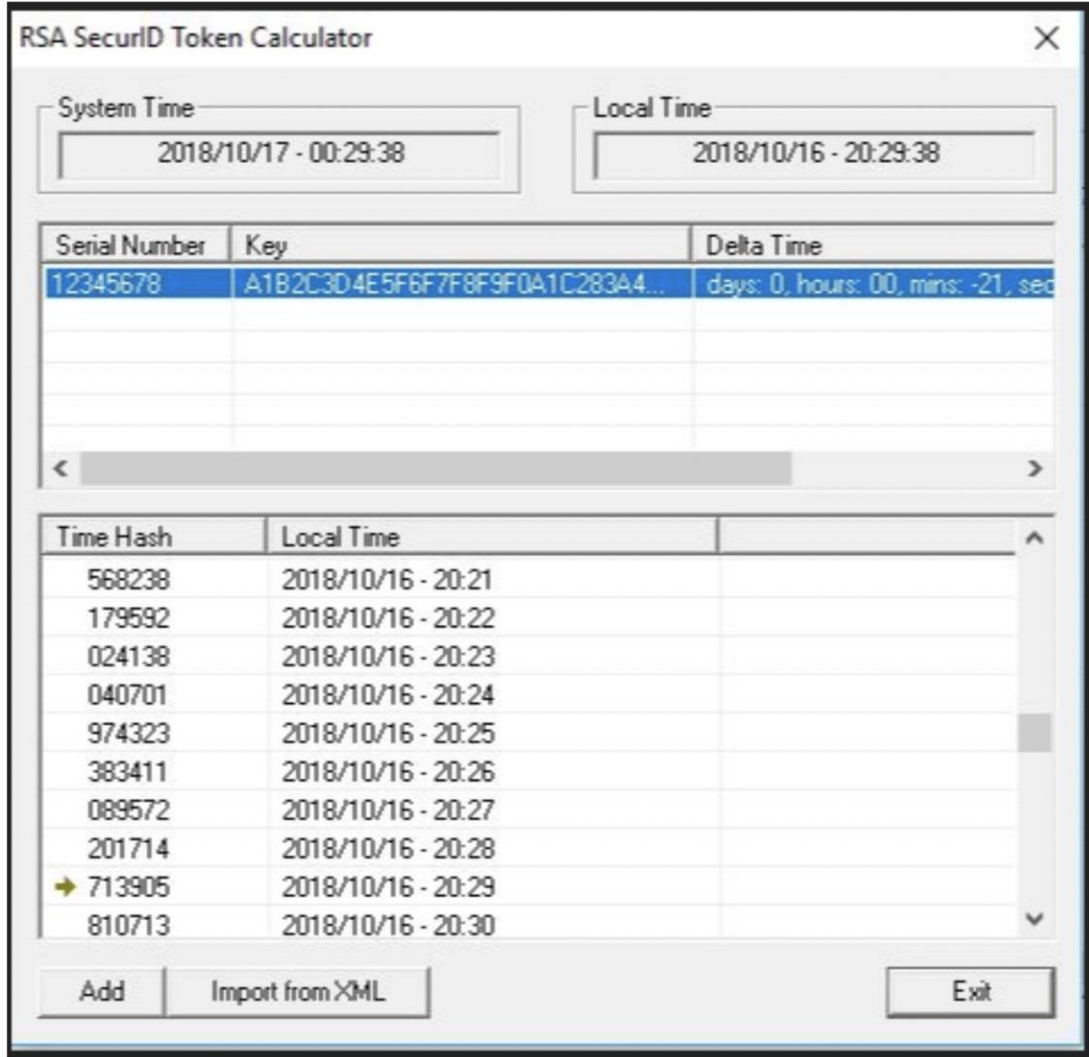
Yinelenen Kod Üreticileri

Pek çok MFA çözümü, kullanıcıya, oturum açma deneyiminin bir parçası olarak istendiğinde girdiği, zaman geçerli bir kodla sunulan "kod oluşturucuları" içerir. Kodlar genellikle rastgele rakamlar veya karakterler olarak görünür ve MFA çözümünün çalışması için gösterildikten sonra 30 – 600 saniye içinde girilmelidir. Popüler örnekler, RSA SecurID™'ler (donanım) ve Google'ın Google Kimlik Doğrulamasıdır (yazılım).



Bu zaman-geçerli kodlar aynı zamanda "tek seferlik şifreler" (OTP) veya

“zamana dayalı tek seferlik şifreler” (TOTP). Her durumda, kullanıcının cihazı veya uygulama örneği benzersiz bir şekilde tanımlanır (ör. Seri numarası vb.) ve bir başlangıç (rastgele oluşturulmuş) "çekirdek değeri" içerir. Sistem için nihai paylaşılan kimlik doğrulama sırrı olan bu tohum değeri, bir veya daha fazla kontrol eden kimlik doğrulama veritabanında saklanır ve ilgili cihazın benzersiz kimliğine bağlanır. Çekirdek değeri veritabanı, cihazın satıcı üreticisi ve/veya kurumsal kullanıcı ortamı gibi bir veya daha fazla paydaşa aittir/güvence altına alınır/korunur. Bir saldırgan tohum değeri veritabanına erişirse, dahil edilen herhangi bir kullanıcı için yinelenen, simüle edilmiş bir kod oluşturucu oluşturabilir. Saldırı, tohum değerini, cihazın benzersiz tanımlayıcı numarasını, geçerli zaman damgasını alabilir ve geçerli OTP'leri oluşturmak için bu değerleri cihazın bilinen nesil algoritmasıyla birlikte kullanabilir. Örneğin, Cain & Abel (<http://www.oxid.it/cain.html>) gibi en az 2001'den beri mevcut olan ve bir RS SecurID öykünücüsü içeren ücretsiz yazılım korsanlığı araçları vardır. Aşağıda bu işlevin bir ekran görüntüsü bulunmaktadır.

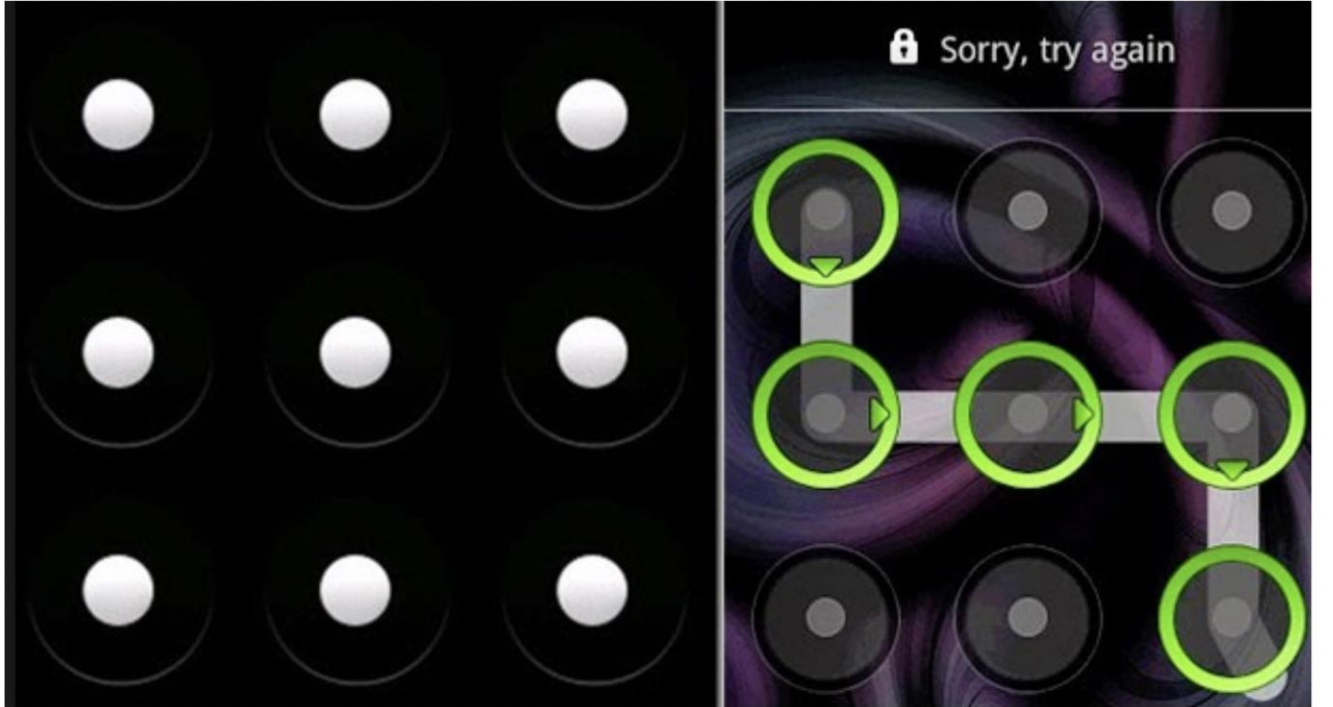


Bu tür saldırılar teorik değildir. Örneğin, 2011'de Çinli Gelişmiş Kalıcı Tehdit (APT) saldırganları RSA'ya girdi (<https://gcn.com/articles/2011/06/07/rsa-confirms-tokens-used-to-hack-lockheed.aspx>) ve Lockheed Martin de dahil olmak üzere birçok müşteri için RS SecurID tohum değerlerini çaldı. Ardından Çinli APT, bu çalıntı kodları kullanarak Lockheed Martin'e girdi ve çok hassas askeri sırları kopyaladı.

omuz sörfü

Bazı MFA çözümleri o kadar kötüdür ki, kullanıcının yazdıklarına veya bunu yaparken ne yaptığına rastgele bakarak "sırrı" görebilirsiniz. Bu durumda MFA genellikle kullanıcının sahip olduğu bir jeton, kart, cihaz veya başka bir nesne ile birlikte kullanıcının yazması gereken bir şey (örneğin, PIN, vb.) şifre" vb.).

Aşağıdaki ilk grafik bir Microsoft Windows Picture Password™ örneği ve ikincisi ise bir Apple iPhone oturum açma örneğidir.



Davetsiz misafir sırda gezinebilir ve cihaza erişebilirse, kurbanın MFA çözümünü kullanarak giriş yapabilir. Bu, uzun zamandır parolalara ve PIN'lere karşı geçerli bir saldırı biçimi olmuştur ve bilgisayar korsanları başarılı olmak için gözlemlediklerini ezberlemek, kullanıcının ne yazdığını filme almak veya daha sonra bir "aşınma düzeni" gözlemleyerek tahminde bulunmak gibi birçok farklı yöntem kullanmıştır. kodun veya eylemin gerçekleştirildiği cihazda.

Neredeyse bu tür bir saldırıyı dahil etmedim çünkü ilk önce saldırganın başarmak için hem faktörleri (kullanıcı tarafından tamamlanan kısım) hem de ilgili cihazı elde etmesini gerektiriyor. Ancak, artan popüler bir MFA çözümü, yukarıdaki grafiklerde gösterildiği gibi, "noktaları birleştir" veya önceden tanımlanmış "hızlı kaydırma" desenleridir; burada, kullanıcılar belirli bir deseni noktalar veya seçilen bir resim arasında kaydırmak için parmağını kullanır. , giriş yapmak için. Bu tür MFA çözümleri, olabilecek en kötü MFA çözümleridir.

Herhangi bir kullanıcının nasıl kaydırmayı seçtiği, bilgisayar korsanı bunu gözlemlemese bile oldukça tahmin edilebilir. Ancak gözlemlenirse, çoğu zaman kolayca, kolayca, hatta bir bilgisayar korsanı olmasa bile, başkalarının kopyalaması basittir. Başka bir "kimlik doğrulama" seçeneği yoktur, buna dünyanın büyük bir yüzdesinin kaydırmayı on metre öteden görebildiği ve ardından yürüyüp başarılı bir oturum açmayı yeniden oluşturabildiği başka bir "kimlik doğrulama" seçeneği yoktur. Bu "MFA" çözümlerini kullanmayın.

Savunma: Herhangi bir kritik veri için kaydırma, desen tabanlı MFA çözümleri kullanmayın.

Göz Atma Saldırıları

Skimming, kullanım sırasında MFA çözümünün sırlarının çalındığı bir hacker saldırı yöntemidir. Bu senaryoların çoğunda, MFA çözümündeki sırlar çok zayıf bir şekilde korunur veya hiç korunmaz. MFA kartında saklanan sırlar, işlem sırasında korumasız durumdayken kaydedilebilecek şekilde açığa çıkar. Gözden geçirme, fiziksel (bilgileri doğrudan MFA cihazından kaydeden bir cihaz kullanılarak) veya kablosuz (örneğin, RFID veya NFC kayması) dahil olmak üzere birçok farklı yolla yapılabilir.

Normalde gözden geçirme saldırılarını MFA'ya karşı bir saldırı olarak düşünmeseniz de, genellikle öyledir. Örneğin, çok yaygın bir gözden geçirme saldırısı ATM nakit akışı makinelerine yöneliktir. Meşru kullanıcı, hesap bilgilerine ve parasına erişmek için hem ATM kartını (yani birinci fiziksel faktör) ibraz etmeli hem de bir PIN (ikinci faktör) yazmalıdır. Saldırgan genellikle kartın manyetik şeridinden bilgi kaydetmek için normal ATM tuş takımı alanını taklit eden fiziksel bir kayıt cihazı yerleştirir, aynı zamanda kaydederken, düğmeye elektronik olarak basar veya gizli bir "gözetleme deliği" kamera kullanır. (aşağıdaki örnek kayma aygıtlarına bakın).



Gözden geçirme saldırıları, marketlerde ve benzin istasyonlarında da çok popüler bir şekilde kullanılmaktadır. Çoğu zaman, skimming saldırılarının bir parçası olan bankalar ve mağazalar (ve çalışanlar), skimming cihazlarının yerleştirilmesiyle suç teşkil etmemektedir. Birçok skimming cihazı, şirket veya çalışanlar farkında olmadan kısa bir süre içinde yerleştirilebilir. İşte harika bir video (<https://www.youtube.com/watch?v=5b1axnNK-wl>) , mağaza görevlisinin dikkatinin bir suç ortağı tarafından başka yöne çevrildiği çok kalabalık bir markete üç saniyeden kısa bir sürede gizlice kurulan bir kaymağını gösteren bir cihaz.

Bilgisayar güvenliği köşe yazarı Brian Krebs, muhtemelen başka herhangi bir gazeteciden daha fazla kayma hakkında araştırma yaptı ve yayınladı. Gözden geçirmeyle ilgili bilgilerine şu adresten göz atın: <https://krebsonsecurity.com/category/all-about-skimmers/> .

Savunma: Kayma ve gözden geçirme donanımının farkında olun. Kayma önleme teknolojilerini kullanan satıcıları kullanmaya çalışın.

Sürüm Düşürme ve Kurtarma Saldırıları

Herkese açık, yaygın olarak kullanılan MFA çözümlerinin çoğu (örneğin, Google, Microsoft, vb.), kullanıcılar tarafından birincil oturum açma yöntemi olarak gerekli olabilir. Ne yazık ki, aynı çözümlerin tümü, devre dışı bırakamayacağınız çok daha az güvenli bir yedekleme kimlik doğrulama alternatifine de sahiptir. Bunun nedeni, bu MFA çözümlerinin daha karmaşık olması ve bu karmaşık etkileşimler nedeniyle daha sık başarısız olmasıdır. Fiziksel MFA cihazları kaybolur, aktarılır ve bozulur. Yazılım tabanlı MFA çözümleri çalışmayı durdurur, kilitlenir ve kontrolleri dışındaki bir dizi başka nedenden dolayı yeniden yapılandırılmaları gerekir. Sonuç, bu mega-MFA sağlayıcılarının otomatik veya manuel, alternatif oturum açma veya kurtarma yöntemine sahip olmaması durumunda, birincil MFA çözümünün sağlanması çok pahalı olacaktır.

Örneğin, Microsoft O365 veya Google Gmail hesaplarınızda ve hizmetlerinde oturum açmak için MFA'ya "gerektiğinizi" varsayalım. Bir bilgisayar korsanı, MFA yöntemini kullanarak oturum açamıyormuş gibi davranabilir (belki üç kez dener) ve MFA ana bilgisayar hizmeti, kimlik doğrulamanızı onaylamanız için size otomatik olarak alternatif bir yol (genellikle e-posta, otomatik sesli onay veya SMS mesajı). Aşağıdaki grafik, popüler bir MFA sağlayıcısı tarafından sunulan yedek kimlik doğrulama yöntemlerini göstermektedir.

Account recovery options

If you forget your password or cannot access your account, we will use this information to help you get back in.

Recovery email

roger@[REDACTED]



Recovery phone

([REDACTED]) [REDACTED]



Aşağıda, bir bilgisayar korsanı tarafından alındığında MFA tarafından korunan hesabın güvenliğinin ihlal edilmesine izin verecek olan kurtarma güvenlik kodunun bir örneği verilmiştir.

Microsoft account

Security code

Please use the following security code for the Microsoft account [ro*****@hotmail.com](#).

Security code: **0152772**

If you don't recognize the Microsoft account [ro*****@hotmail.com](#), you can [click here](#) to remove your email address from that account.

Thanks,
The Microsoft account team

Kurtarma Soru Saldırıları

Kurtarma sorusu saldırıları, sürüm düşürme saldırı sınıfının özellikle kötü bir uzantısıdır. Birçok web sitesine kaydolurken, birden fazla "kurtarma sorusu" ve/veya yanıt oluşturmanızı GEREKTİRECEKTİR (aşağıdaki örneğe bakın). Bu soruların yanıtlarını kullanmayı ve doldurmayı kabul etmeden ilk hesabı oluşturamazsınız. Bu kurtarma soruları genellikle "Annenin Kızlık soyadı", "Babanın Orta Adı", "Favori Öğretmen", "İlk Araba" gibi soruları içerir.

Your Security Questions

Question: What is the name of the camp you attended as a child? ▼

Answer:

Repeat Answer:

Question: What is the first name of your favorite Aunt? ▼

Answer:

Repeat Answer:

Question: What is the zip code of the address where you grew up? ▼

Answer: ■ Special characters, such as / and -, are not allowed

Repeat Answer:

Question: What is the name of the street where you grew up? ▼

Answer:

Repeat Answer:

Sorun, kurtarma sorularının ve cevaplarının genellikle kolayca tahmin edilmesi ve bunları gönderen meşru kullanıcılar tarafından genellikle doğru şekilde hatırlanamamasıdır. Google'da Sırlar, Yalanlar ve Hesap Kurtarma: Google'da Kişisel Bilgi Sorularının Kullanımından Dersler adlı harika, dönüm noktası niteliğinde bir Google tanıtım belgesi var (<http://www.a51.nl/sites/default/files/pdf/43783.pdf>). İçinde Google, kurtarma sorularının tamamen yabancılar (örneğin, bilgisayar korsanları) tarafından tahmin edilmesinin genellikle oldukça kolay olduğunu ve genellikle onları oluşturan veya yanıtlayan kullanıcılar tarafından doğru şekilde hatırlanmadığını ortaya koydu.

Örneğin:

- Bazı kurtarma soruları ilk denemede %20 oranında tahmin edilebilir
- İnsanların %40'ı kendi kurtarma yanıtlarını başarıyla hatırlayamadı
- Cevapların %6'sı bir kişinin sosyal medya profilinde bulunabilir

Not: Kimlik doğrulama için kurtarma sorularının ne kadar kötü olduğunu anlayan Google, Microsoft ve diğer satıcılar artık bunları kullanmıyor.

MFA çözümünüz daha az güvenli alternatif kimlik doğrulama yöntemlerinin kullanılmasına izin veriyorsa, kimlik doğrulamanız yalnızca en zayıf yöntem kadar güçlüdür.

Çözüm, onlardan kaçınıbiliyorsanız onları asla kullanmamaktır. Gerekiyorsa, asla doğru yanıtlamayın. Bunun yerine, uzun bir parolaya benzer bir şey oluşturun (çoğu senaryoda karmaşıklık gerekmez), her kurtarma yanıtı için benzersiz, hiçbir yanıtı tekrarlamaz ve parola yöneticisinde veya başka bir yerde "temsilci" biçimde saklayın.

İkincisine bir örnek, pizzapizza\$vgad2@M1 şeklinde bir kurtarma yanıtı seçmektir (aşağıdaki örneğe bakın) ve kurtarma yanıtını yazmanız gerekirse, bunu pp\$vgad2@M1 olarak saklayın, burada yalnızca pp'nin geçerli olduğunu bilirsiniz. pizzapizza için . Bu şekilde, yetkisiz bir kişi kurtarma cevap listenize erişirse, doğru cevabı öğrenemezler.

Question:	What was your high school mascot?
Answer:	pizzapizza\$vgad2@M1
Repeat Answer:	*****
Question:	What is your mother's middle name?
Answer:	*****
Repeat Answer:	*****
Question:	What is your father's birthdate? (mmdd)
Answer:	*****
Question:	What is the name of your best friend from high school?
Answer:	*****
Repeat Answer:	*****

Çoğu şifre yöneticisi, ihtiyaç duyduğunuz her site için sorularınızı ve ilgili yanıtları güvenli bir şekilde saklayabileceğiniz "not alanları"na sahiptir ve bazıları, gerektiğinde doğru "yanıtları" saklar ve otomatik olarak yeniden doldurur.

Bir MFA sağlayıcısı, alternatif bir kimlik doğrulama yöntemi olarak kurtarma sorularına ve yanıtlarına izin verdiğinde, aslında sizi biraz daha güvenli bir çözümünden, oturum açma adı ve parola gibi normal bir tek faktörlü kimlik doğrulama yöntemini kullanmaktan çok daha kötü bir şeye götürüyorlar. MFA çözümünüz daha az güvenli alternatif kimlik doğrulama yöntemlerinin kullanılmasına izin veriyorsa, kimlik doğrulamanız yalnızca en zayıf yöntem kadar güçlüdür.

Savunmalar: Bir MFA satıcısı tarafından sürüm düşürme kimlik doğrulama teknolojilerine izin verilmesini önlemeye çalışın ve asla gerçek yanıtlarınızı kurtarma yanıtları için vermeyin.

Sosyal Mühendis Teknik Destek

Bir şirketin teknik destek mühendisleri yalnızca insandır ve ellerinden geldiğince yardımcı ve çözüm sağlayıcı olmak üzere eğitilmiş kişilerdir. Bir şirketin MFA'nın sosyal olarak tasarlanmasını önlemek için

belirli teknik ve politika kontrolleri olsa bile, aşırı yardımcı teknik destek çalışanları bunları atlayabilir. Bu, insanlara diğer insanlarla etkileşime girmeleri söylendiği sürece ortadan kalkmayacak bir risktir.

Mevcut MFA çözüm korumalarını devre dışı bırakmak veya atlamak için teknik destek almak için birçok sosyal mühendislik tekniği vardır. Bunlar arasında "kullanıcı" (yani bilgisayar korsanı) şunları söyler:

- Mevcut MFA çözümünü kaybetti veya hasar gördü
- Mevcut PIN'ini veya şifresini hatırlamıyor
- MFA çözümünü atlamayı gerektiren bir şeyi yapamadığı için ona çok kızgın
- O patrondur ve kritik bir şey yapmak için acil baypasa ihtiyacı vardır.

Sosyal mühendislik bilgisayar korsanları, genellikle, hemen çözülmesi gereken kritik bir görev veya mali sorun gibi yapay olarak oluşturulmuş "stres etkeni olayları" kullanır. En sevdiğim sosyal mühendislik gösteri hacklerinden biri, sosyal mühendisliği kullanan bir kadının, bir şey yapmadığı için kocasıyla başı belada olan ağlayan bir bebeği olan bir anne olduğunu iddia ederek bir kullanıcının cep telefonu hesabını devralmasını içeriyor.

Şuna bir göz atın: <https://www.youtube.com/watch?v=lc7scxvKQOo> . Videonun en sonunda NSFW (iş için Güvenli Değil) , hesabı ele geçirilen adamdan bir küfür var.

Savunma: MFA satıcınızın, teknik desteğine karşı sosyal mühendislik riskini anladığından ve kötü niyetli sosyal mühendisliği önlemek için araçlar, politikalar ve prosedürler kullandığından emin olun .

Konu Ele Geçirme

Her MFA çözümü, kullanıcının veya cihazın oturum açma adı, e-posta hesabı, kullanıcı asıl adı (UPN) veya ilgili ad alanındaki diğer bazı benzersiz tanımlayıcı gibi benzersiz bir kimliğe bağlıdır. Bazı MFA senaryolarında, ad alanında MFA kullanıcısının tanımlayıcısını değiştirebilerseniz, ilgili MFA'yı devralabilir veya atlayabilirsiniz. Bu, özellikle, sunulan başarılı MFA çözümünün kullanılan kimliğe gerçekten bağlı olup olmadığına bakmayan MFA çözümleri için geçerlidir (yani, MFA tanımlayıcısı ad alanında saklanmaz veya belirli bir kullanıcıya ait olduğu doğrulanmaz).).

İşte bu tür bir saldırının harika bir örneği. Microsoft Active Directory, kullanıcının UPN'si ve akıllı kartları içerir. Bu saldırı, yazarın bildiği kadarıyla, gerçek dünyadaki bir hedefe karşı bilerek "vahşi doğada" istismar edilmemesine rağmen, onlarca yıldır mümkün olmuştur. Microsoft'a bildirildi, doğrulandı ve "tasarlandığı gibi" çözünürlük verildi. Ayrıca, ayrıcalık saldırısının potansiyel bir içeriden değerlendirmesidir. İşte nasıl çalıştığı:

Microsoft Akıllı Kart Kimlik Hijack Saldırısı

Bu özel saldırı senaryosu için, yöneticilerin kimlik doğrulaması için akıllı kartlar gerektiren standart bir Active Directory orman ortamı olduğunu varsayacağız. Kötü adamın iki kritik gereksinime ihtiyacı var:

- Herhangi bir kullanıcı akıllı kartı ve kurbanın Active Directory ormanı tarafından güvenilen kimlik doğrulama PIN'i
- Amaçlanan kurbanın UPN'sini bir değerden diğerine değiştirebilme

Not: İlk madde işareti noktasında gerektiği gibi kullanıcı akıllı kartı, orman tarafından güvenilen herhangi bir sertifika yetkilisi (CA) tarafından verilen herhangi bir güvenilir kullanıcı akıllı kartı olabilir. Akıllı kart,

bir kullanıcıyı ve hedeflenen ormanda gerçekte var olmayan bir UPN'yi bile içerebilir, ancak bu gösterim için kullanıcı mevcut, geçerli, güvenilir bir kullanıcı olacaktır.

Bu hackin anahtarı, saldırganın kurbanın UPN'sini kendi UPN'si ile güncellemesidir. İçinde Active Directory, birçok yönetici kullanıcı hesabı bilgilerini güncelleyebilir. Varsayılan olarak, Microsoft'a göre, aşağıdaki gruplar ve bireysel izinler UPN'leri güncelleyebilir: Yöneticiler (etki alanı denetleyicilerinde), Etki Alanı Yöneticileri, Kurumsal Yöneticiler, Şema Yöneticileri ve ilgili kullanıcı hesapları üzerinde Genel Bilgi Yazma özelliğine sahip herhangi bir kullanıcı.

Bu bilgisayar korsanlığı senaryosu için, HelpDesk adlı daha düşük ayrıcalıklı bir kullanıcının, Süper Yöneticiler, UPN adlı yüksek ayrıcalıklı bir yöneticiyi güncelleme yeteneğine sahip olduğunu varsayacağız. Yardım Masası , Süper Yönetici'nin güvenlik hesabı izinlerini, grup üyeliklerini ve ayrıcalıklarını tamamen devralmak için bu değişikliği kullanabilir. İşte hack adımlarının bir özeti:

1. Düşük ayrıcalıklı HelpDesk yöneticisi, Süper Yönetici ile UPN'leri değiştirir.
2. HelpDesk yöneticisi kendi HelpDesk akıllı kartını ve PIN'ini kullanarak oturum açar.
3. Viyola! HelpDesk yöneticisi, tüm grup üyelikleri dahil olmak üzere Süper Yönetici olur.
4. HelpDesk kötü niyetli eylemler gerçekleştirir.
5. Sistem tüm işlemleri Süper Yönetici olarak takip eder.
6. HelpDesk bittiğinde , oturumu kapatır ve UPN'leri tekrar değiştirir. Farkı kimse bilmiyor .

Günlük yönetim sisteminiz UPN güncellemelerini izliyor ve uyarıyor mu? SuperAdmin'in her türden yükseltilmiş gruba ait olduğunu doğrulayalım (aşağıya bakın) kaydedilmiş bir videosunu izleyebilirsiniz .

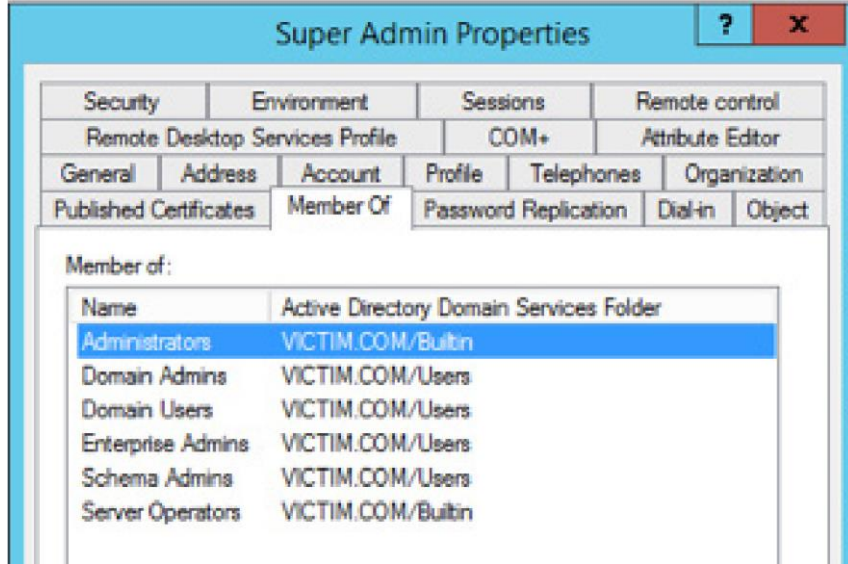
SuperAdmin'in yükseltilmiş gruplara ait olduğu doğrulanıyor .

demo of this attack at: <https://youtu.be/OLQ3IAMuokI>.

All unique subject/identity attributes used in the authentication process, such as UPN, need to be as protected and monitored as the other authentication secrets like password hashes.

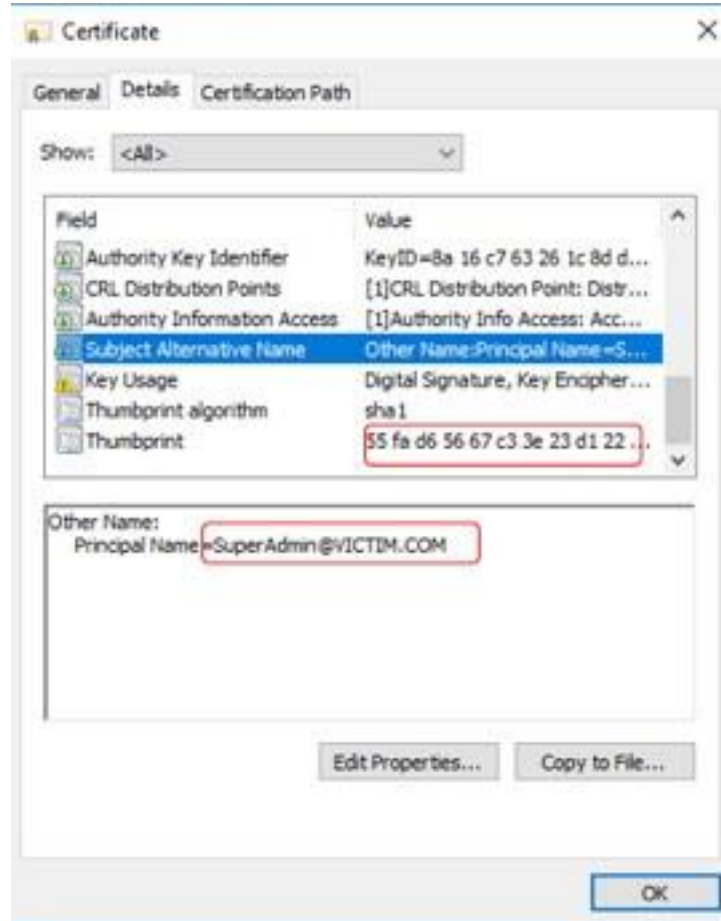
First, let's verify Super Admin's UPN (which is represented as User Logon Name in Active Directory) is SuperAdmin:





Ardından, Süper Yönetici'nin akıllı kartıyla ilgili benzersiz dijital sertifika parmak izi de dahil olmak üzere Süper Yönetici'nin UPN'sinin Süper Yönetici'nin akıllı kartına bağlı olduğunu doğrularız.

Süper Yönetici'nin akıllı kartının UPN'sini ve benzersiz dijital sertifika parmak izini doğrulama.



Süper Yöneticinin akıllı kartını ve PIN kodunu kullanarak Süper Yönetici olarak oturum açma.



Süper Yönetici'nin, Süper Yönetici'nin akıllı kartını ve PIN'ini kullanarak başarıyla oturum açtığını doğrulama.

Süper Yönetici olarak oturum açtığını doğrulamak için Whoami komutunu çalıştırma .

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\windows\system32>whoami
victim\superadmin

C:\windows\system32>
```

SuperAdmin'in yüksek grup üyeliklerine sahip olduğunu doğrulamak .

Süper Yöneticinin ait olduğu yükseltilmiş grupları doğrulamak için Whoami /groups kullanma .


```
Administrator: Command Prompt

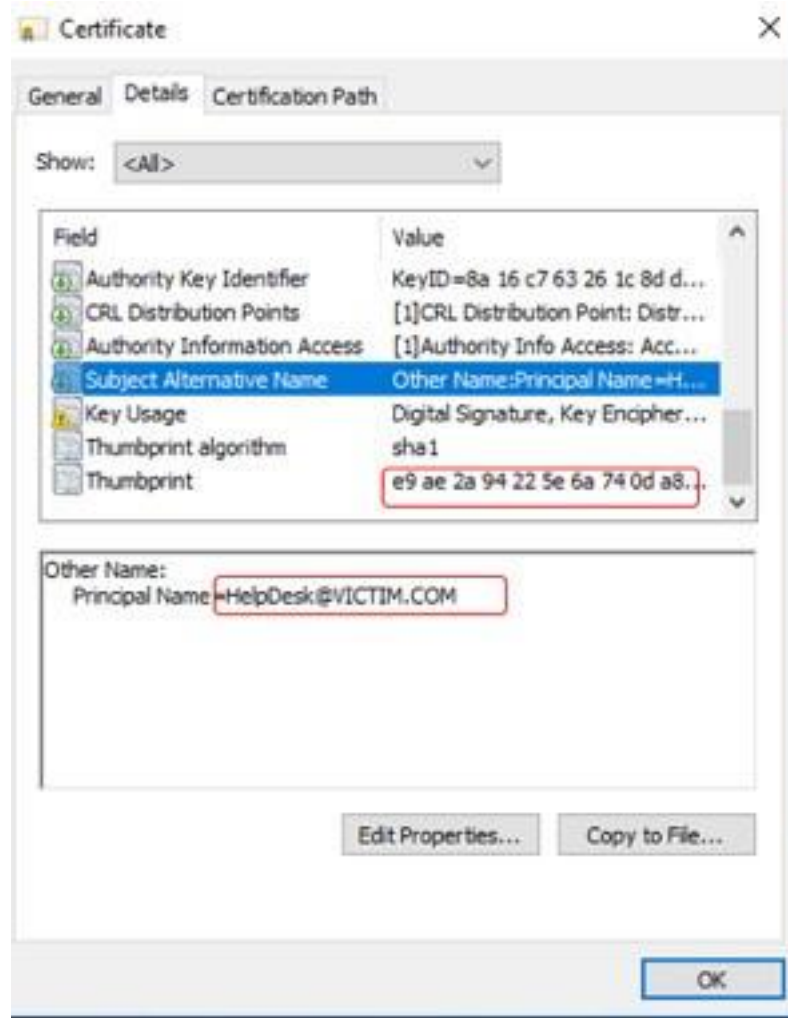
-----
Everyone Well-known group S-1-1-0
up, Enabled by default, Enabled group
BUILTIN\Administrators Alias S-1-5-32-544
up, Enabled by default, Enabled group, Group owner
BUILTIN\Users Alias S-1-5-32-545
up, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE Well-known group S-1-5-4
up, Enabled by default, Enabled group
CONSOLE LOGON Well-known group S-1-2-1
up, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11
up, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15
up, Enabled by default, Enabled group
LOCAL Well-known group S-1-2-0
up, Enabled by default, Enabled group
VICTIM\Domain Admins Group S-1-5-21-98619
up, Enabled by default, Enabled group
VICTIM\Enterprise Admins Group S-1-5-21-98619
up, Enabled by default, Enabled group
VICTIM\Schema Admins Group S-1-5-21-98619
up, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1
```

Daha sonra örnek, daha az ayrıcalıklı HelpDesk kullanıcısını kendi akıllı kartı ve PIN'ini kullanarak oturum açarken gösterecektir (saldırı tamamlanmadan önce mevcut durumu göstermek için).

HelpDesk kullanıcısı.



HelpDesk'in helpdesk@victim.com UPN ve HelpDesk'in benzersiz dijital sertifika parmak izini gösteren akıllı kart bilgileri.



HelpDesk'in kurban.com etki alanında oturum açtığını göstermek için Whoami'yi kullanma .

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\windows\system32>whoami
victim\helpdesk

C:\windows\system32>
```

HelpDesk yöneticisinin ait olduğu daha düşük ayrıcalıklı grupları göstermek için Whoami /groups kullanma .

```
Administrator: Command Prompt
C:\windows\system32>whoami /groups

GROUP INFORMATION
-----

Group Name                                     Type                                     SID
-----
Everyone                                     Well-known group S-1-1-0
oup
BUILTIN\Administrators                       Alias                                   S-1-5-32-544
oup, Group owner
BUILTIN\Users                               Alias                                   S-1-5-32-545
oup
NT AUTHORITY\INTERACTIVE                     Well-known group S-1-5-4
oup
CONSOLE LOGON                               Well-known group S-1-2-1
oup
NT AUTHORITY\Authenticated Users             Well-known group S-1-5-11
oup
NT AUTHORITY\This Organization               Well-known group S-1-5-15
oup
LOCAL                                        Well-known group S-1-2-0
oup
Authentication authority asserted identity Well-known group S-1-18-1
oup
NT AUTHORITY\This Organization Certificate    Well-known group S-1-5-65-1
oup
Mandatory Label\High Mandatory Level        Label                                   S-1-16-12288
```

Şimdi daha düşük ayrıcalıklı HelpDesk kullanıcısı, UPN'sini kullanarak SuperAdmin kullanıcısı ile değiştirecek.

Aktif Dizin kullanıcıları ve bilgisayarları. Bunu yapmak için, Active Directory iki hesabın aynı UPN'yi aynı anda paylaşmasına izin vermeyeceğinden, Yardım Masası kullanıcısının önce başka bir değerle UPN'sine geçmesi gerekir. Ardından HelpDesk kullanıcısı, SuperAdmin'in UPN'sini helpdesk@victim.com'u okuyacak ve kendi akıllı kartında tuttuğu UPN ile aynı olacak şekilde günceller.

HelpDesk , UPN'sini başka bir şeyle değiştirir ve ardından SuperAdmin UPN'sini HelpDesk akıllı kartında depolandığı ve doğrulandığı şekilde UPN'ye günceller.

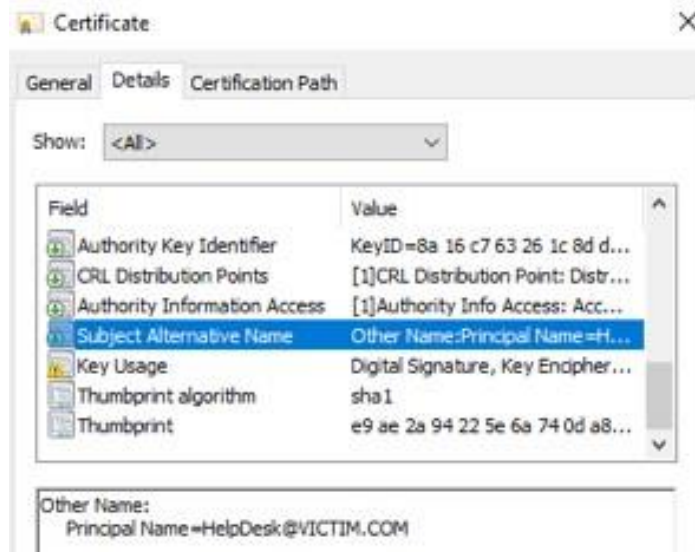


Ardından, HelpDesk Kullanıcısı oturumu kapatır, Active Directory replikasyonunun gerçekleşmesi için birkaç dakika bekler ve ardından tekrar oturum açar.

HelpDesk kullanıcısı, geçerli akıllı kartını ve PIN'ini kullanarak tekrar oturum açar.



HelpDesk akıllı kartının ve PIN'inin kullanıldığını doğrulamak için tekrar oturum açmak için kullanılan HelpDesk akıllı kartının ayrıntıları .



HelpDesk kullanıcısı ilgili HelpDesk akıllı kartını ve PIN'ini kullanarak oturum açsa da, SuperAdmin artık helpdesk@victim.com UPN'sine sahip olduğundan Active Directory onları SuperAdmin kullanıcısı ile ilişkilendirmiştir .

HelpDesk kullanıcısının artık Active Directory tarafından SuperAdmin olarak görüldüğünü doğrulamak için Whoami'yi kullanma .

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\windows\system32>whoami
victim\superadmin

C:\windows\system32>_
```

Oturum açmış olan HelpDesk kullanıcısının artık SuperAdmin grup üyeliklerine sahip olduğunu göstermek için Whoami /groups kullanma .

```
Administrator: Command Prompt
C:\windows\system32>whoami /groups

GROUP INFORMATION
-----

Group Name                                     Type
-----
Everyone                                     Well-known group
Authenticated Users                          Well-known group
Administrators                               Alias
Users                                         Alias
NT AUTHORITY\INTERACTIVE                     Well-known group
CONSOLE LOGON                               Well-known group
NT AUTHORITY\Authenticated Users             Well-known group
NT AUTHORITY\This Organization                Well-known group
LOCAL                                         Well-known group
VICTIM\Domain Admins                         Group
VICTIM\Enterprise Admins                    Group
VICTIM\Schema Admins                        Group
```

Bu noktada, HelpDesk kullanıcısı SuperAdmin'in şu anda yapabileceği her şeyi yapabilir ve Microsoft Windows ve Active Directory, tüm Windows Event Log olaylarını HelpDesk kullanıcısından değil SuperAdmin'den gerçekleşiyormuş gibi izler. Yardım Masası kullanıcısı , güvenlik bilgilerini her zaman yükseltebileceğini onaylamak gibi diğer yetkisiz eylemleri gerçekleştirdikten sonra , UPN'leri geri alabilir ve UPN güncellemeleri günlüğe kaydedilmediği ve bu belirli eylemlerin önemi fark edilmediği sürece, gerçekte ne olduğunu kolayca görmek zor.

Not: Etki alanı denetleyicilerinde kayıtlı olan ve sağlanan her akıllı kartın parmak izini içeren bazı oturum açma olayları vardır; bunlar, HelpDesk kullanıcısının akıllı kartının artık bir şekilde SuperAdmin hesabıyla ilişkili olduğunu ortaya çıkarmak için gözden geçirilebilir, ancak adli tıp müfettişlerinin bilmesi gerekir ve bu özel hack senaryosunu doğrulamaya çalışıyorum. Gerçekten ne olduğunu tartışmaya çalışırken bunu keşfetmek kolay olmayacaktı.

Açık olmak gerekirse, bu gerçekten bir hack veya hata değil. Bu, Active Directory ile tümleşik akıllı kartların çalışma şeklinin "tasarlandığı gibi" bir sonucudur. Bu tür bilgisayar korsanlığı hilelerini en aza indirmenin yolları olsa da, Microsoft muhtemelen bunu "düzeltmeyecektir". Sonuç olarak, geçerli, güvenilir akıllı kart, kimliği başarıyla doğrulanmış kullanıcının helpdesk@victim.com olduğunu söylüyor. Active Directory artık helpdesk@victim.com'un SuperAdmin'e ait olduğunu anlıyor .

Daha önce aktif olarak ele alındığı gibi, bir kimlik doğrulama dolandırıcılığının doğrulanması ve çoğu zaman, sonuçta ortaya çıkan yetkilendirme ve erişim kontrol süreçlerinden ayrıdır. Bu özel bilgisayar korsanlığı senaryosunda, akıllı kart kimlik doğrulama süreci (yani, kullanıcının doğru bir UPN'ye sahip geçerli, güvenilir bir akıllı kart sunması ve ilgili PIN'i bilmesi) ve erişim kontrolü ve yetkilendirme süreci ("doğrulanmış" kullanıcıya grubunun teslim edildiği yer). bir erişim kontrol belirtecindeki üyelikler ve ayrıcalıklar", Active Directory için neredeyse tamamen ayrı olaylardır. Geçerli, güvenilir bir akıllı kart ve doğru PIN girildikten sonra, Active Directory'nin (en yaygın akıllı kart senaryolarında) bunu yapmasının hiçbir yolu yoktur. sağlanan doğrulanmış UPN'nin, onu içeren kullanıcı hesabıyla eşleştirilmemesi gerektiğini bilin.

Bu tür MFA suistimallerine karşı genel koruma, bir kimlik doğrulama çözümünün parçası olarak konu adı gibi bir özneteliği her kullandığınızda, ilgili özneteliğin bir kimlik doğrulama sırrıymış gibi korunması ve izlenmesi gerektiğini anlamaktır. Çoğu yöneticiye, sanki krallığın anahtarlarıymış gibi parola karmaları gibi diğer kimlik doğrulama sırlarını korumaları öğretilir; ve onlar. Ancak çoğu yöneticiye, kötü niyetli değişikliklerinin benzer güvenlik etkilerine sahip olmasına rağmen, ilgili diğer kimlik doğrulama özneteliklerini korumaları ve izlemeleri öğretilmez.

Yeniden Oluşturulan Biyometri

Biyometrik nitelikler, diğer deneklerle eşleşmeyen (sözde) evrensel olarak benzersiz fiziksel özellikleri içerir. Bunlar şunları içerir: parmak izleri, retina taramaları, parmak-el geometrisi, DNA, ses, koku, yüz, damar desenleri, vücut şekilleri, vücut parçaları (yani kulaklar) şekilleri ve hatta imza, fare tıklamaları ve hatta hareket temelli biyomekanikler. klavye yazma özellikleri ("es" yazarken "e"-tuşundan "s"-tuşuna geçmenizin ne kadar sürdüğü gibi), vb. Hiçbir biyometrik özelliğin kanıtlanmadığı bir an için göz ardı etmek küresel olarak benzersiz, başka sorunlar da var. Bize belirli bir biyometrik tanımlayıcının taklit edilemez olduğu söylendiğinde, birileri bunları genellikle bir gün içinde, 100 dolardan daha az bir para alarak kolayca uydurdu ve dünyanın görmesi için YouTube'da yayınladı. İşte Apple'ın iPhone'unun yüz tanıma özelliğini kıran birinin harika bir örneği

(<https://www.youtube.com/watch?v=sYSQBleC4fs>) . Parmak izi tarayıcıları, jelatin ve Silly Putty™ yeniden yaratımları tarafından kandırıldı.

Biyometrik kimliklerin başarılı bir şekilde taklit edilmesi daha kolay hale getirilmiştir, çünkü biyometrik kimlikler (neredeyse) küresel olarak benzersiz olsa da, biyometrik okuma cihazları, algılama değişikliklerinde daha az hassas olmaları için "de-tuned" olmalıdır, aksi takdirde çok fazla yanlış negatifler olacaktır (yani, biyometrik kimliğin meşru sahibini reddetme).

Örneğin, parmak izleriniz küresel olarak benzersiz olsa bile, kaydı ve sonraki ölçümü mümkün olan en iyi ayırım çözünürlüğünde yapılamaz. Bunun nedeni, parmak izlerimizin her gün küçük kesikler, sıyrıklar ve dokunduğumuz, hatta terlediğimiz şeylere yapışması nedeniyle birçok “mikro değişikliğe” sahip olmasıdır. Parmak izi okuyucu çok hassas bir şekilde ayarlanmışsa, yöneticilerin ve kullanıcıların kabul edebileceği çok fazla yanlış-negatif inkar olurdu. Böylece, her biyometrik cihazın ayarı bozulur, olabileceğinden çok daha az hassas hale getirilir, bu da onları aynı biyometrik kimliklerin yakın benzerliklerine karşı daha duyarlı hale getirir.

Bir sorun olarak, ayarı bozma, gerçekten benzersiz olan farklı biyometrik niteliklerin belirli bir benzersiz kimlik için yanlış-pozitif olarak kabul edilebilmesine neden olur. Örneğin, fiziksel kimlik doğrulama için parmak izi analizini kullanan 500'den biraz fazla çalışanı olan bir şirket biliyorum. Üç çalışanın parmak izinin daha önce kayıtlı diğer çalışanlarla “eşleştiği” tespit edildi. Bu üç çalışan aynı parmak izlerini paylaşmıyor, hatta yakın değil. Ancak ayarsız parmak izi okuyucusu bunların aynı olduğunu düşünüyor. Bu tür sorunların çözümü, biyometrik okuyucuları değişikliklere karşı daha duyarlı hale getirmektir, ancak bunu yapmak, çoğu ortamın çalışmak istemediği bir sorun olan çok daha fazla yanlış negatife neden olacaktır. Tüm biyometrik özellikler çoğaltılabilir veya çalınabilir. Ve bir kez yapıldığında, gelecekteki kimlik doğrulama için biyometrik öznitelige güvenilemez. On yıllar boyunca, sözde unutulmaz her biyometrik kimliğin, sözde olduğu meşru kişiden geldiği için tamamen güvenilir olduğu kanıtlanmıştır.

Savunmalar: Biyometrinin doğasında var olan yanılabirliği kabul edin ve kullanılıyorsa, bunların her zaman ikinci, biyometrik olmayan bir faktörle kullanıldığından emin olun.

Çalınan Biyometri

Tüm biyometrik öznitelikler, bir kez kaydedildikten sonra, ya alındıkları bilgisayarda yerel olarak ya da ağ üzerinden erişilebilen bir veri tabanına kaydedilir. Çoğu zaman bu biyometrik kimlikler, ülke veya dünya çapında birden fazla veri tabanında depolanır. Bilgisayar korsanları veritabanlarını çalmak için kullanılır. Bir biyometrik öznitelik çalındığında (veya başarıyla yeniden oluşturulduktan sonra), gelecekteki herhangi bir kimlik doğrulama senaryosunda artık güvenilir olamaz.

Örneğin, 2015 yılındaki tek bir saldırıda ABD'den 5,6 milyon kişinin parmak izi çalındı.

Personel Yönetimi Ofisi

Bu çalınan parmak izleri, ABD hükümetinin güvenlik izni için başvuran herkesi içeriyordu (https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach) . Bu makalenin yazarının parmak izlerini içeriyordu. Yazarın karısının parmak izlerini, 1980'lerin başında bir tersanede çalışırken kaydettiği parmak izlerini içeriyordu. Çok gizli casuslarımızın parmak izlerini içeriyordu. Bir saldırıda, yaklaşık altı milyon insanın parmak izlerine artık güvenilemez.

Bugün dünyamız yüz tanıma tarayıcılarıyla dolu. ABD FBI'nın 117 milyondan fazla yüzü var (<https://www.digitaltrends.com/cool-tech/feds-facial-recognition-database-over-100-million/>) . İngiltere ve Çin yüz tanıma sistemlerinin de on milyonlarca yüz içerdiği düşünülüyor. Bilmediğimiz kaç tane biyometrik öznitelik veri tabanı tavizi var?

Çalınan biyometrik özelliklerle ilgili sorun, bir kez ele geçirildiklerinde onları değiştirememenizdir. Parolamızı, PIN kodumuzu, akıllı kartımızı veya MFA simgemizi değiştirebiliriz, ancak vücudumuzu

(kolayca) değiştiremeyiz. Bu nedenle, biyometrik olmayan başka bir faktör olmaksızın tek başına biyometri, biyometrikle ilgili herhangi bir MFA çözümünün parçası olmalıdır.


Kaba Kuvvet Saldırıları

Birçok MFA çözümü, parolalar ve PIN'ler gibi "bildiğiniz bir şey" faktörlerine sahiptir. Çoğu zaman bir bilgisayar korsanı, "Bilddiğiniz bir şey" faktörüyle eşleştirilmiş MFA cihazını ele geçirirse, kırana kadar "bildiğiniz bir şey" kısmını tahmin edebilir. Geleneksel şifre dünyasında, hesap kilitlenmeden önce az sayıda yanlış tahminle sınırlandırılmaya alışkınız (hesap kilitleme olarak bilinir) ve bazı MFA çözümleri tekrarlanan yanlış tahminleri yapay olarak yavaşlatır (hız sınırlama denir). Ancak çoğu zaman, her iki savunma dahil edilmeden yeni bir MFA çözümü sunulur, böylece hacker haklı olana kadar tahminde bulunabilir. Bu her zaman olur.

İşte Slack'in MFA çözümüyle ilgili Kasım 2017 tarihli bir hata raporu: <https://hackerone.com/reports/121696>.

hackerone

FOR BUSINESSFOR HACKERSHACKTIVITYCOMPANYTRY HACKERONE







**Takashi (kamikaze)**

366Reputation- Rank2.02Signal72ndPercentile10.36Impact76thPercentile

22

#121696

Bypass two-factor authentication

Share:      

State Resolved (Closed)


Disclosed publicly **November 18, 2017 7:00am -0500**

Reported To **Slack**

Weakness **Improper Authentication - Generic**

Bounty **\$500**


Severity No Rating (---)

Participants 

Visibility **Public (Full)**

Collapse

TIMELINE

**kamikaze** submitted a report to **Slack**. Mar 9th (3 years ago)

If a user set 2FA, a user has to enter verification code when a user tries to reset password.

Under the "Password Reset" page, a user can enter wrong two-factor authentication code many times. I said "many times" because your bug bounty policy stated...

Exclusions

Issues found through automated testing

So, I may not be allowed to brute force in order to check how many times a user can enter wrong 2FA codes. I didn't use any automated tools and didn't brute force for my testing.

I tested that I could still reset my password after I entered wrong 2FA codes 20 times manually. It seems that a user can brute force 2FA codes.

-----step to reproduce-----

1. A user sends a password reset message to user's registered email.
2. Go to "Password Reset" page from #1's message.
3. Set a new password and Brute force two-factor auth code

Ekim 2018'de başka bir MFA çözümüne yönelik bir başka kaba kuvvet saldırısı: <https://www.cloudfoundry.org/blog/cve-2018-11082/> . Biri onları bir hata olarak bildirene kadar kaldıkları yeni MFA sistemlerinde olağandışı değildirler.

Savunma: Tüm MFA seçenekleri, hız azaltma veya hesap kilitleme özelliklerini içermelidir.

Buggy MFA

İnsanoğlu kusursuz kod yazamaz. MFA çözümleri her zaman yazılım içerir ve bu yazılım kodlama hataları içerecektir. Bu hatalardan biri veya daha fazlası, güvenlik hatalarına dönüşecek kadar önemli hatalar içerebilir. Bazı güvenlik hataları o kadar şiddetlidir ki, MFA çözümünün tamamen atlanmasına izin verir ve bazıları o kadar kötüdür ki yüz milyonlarca bireysel örneğin güvenliği ihlal edilir.

Örneğin, Ocak 2018'den itibaren Uber'i içeren bir kodlama hatası nedeniyle bir MFA atlama:

<https://www.zdnet.com/article/uber-security-flaw-two-factor-login-bypass/> . Uber'in gönderilen baypas hatasını düzeltilmesi gereken gerçek bir sorun olarak kabul etmesi bile haftalar aldı. İşte bazı MFA baypas hataları:

- <https://www.youtube.com/watch?v=eFD89QrcRg8>
- https://www.youtube.com/watch?v=IPrhImqN_7E
- <https://hackerone.com/reports/264090>
- <https://blog.elcomsoft.com/2017/11/breaking-apple-icloud-reset-password-and-bypass-two-factor-authentication/>

ROCA Güvenlik Açığı

Belki de en meşhur, yaygın MFA atlama hatası (şimdiye kadar) 2017 ROCA güvenlik açığıdır.

(https://en.wikipedia.org/wiki/ROCA_vulnerability) . Bu durumda, bir Infineon Technologies RSALib şifre kitaplığıyla oluşturulan her 2048 bit RSA özel/genel anahtar çifti bu güvenlik açığını içerir. Yüz milyondan fazla akıllı kart ve Güvenilir Platform Modülü (TPM) yongaları gibi diğer ilgili kriptoloji cihazları. Hata o kadar şiddetliydi ki, eğer bir saldırgan özel/genel anahtar çiftinin (normalde dünyadaki herkesin bir güvenlik sorunu yaratmadan sahip olabileceği) açık anahtarını elde edebilirse, ilgili özel anahtarı kolayca yeniden oluşturabilirdi. Bu, esasen çok şeffaf şifreleme kullanan yüz milyondan fazla akıllı kart ve diğer cihazlar yapma etkisine sahipti.

Savunma: Sıfırdan güvenlik ve hata minimizasyonu içeren kodlama yöntemleri ve geliştiriciler kullanan MFA çözümlerini kullanın. Güvenlik Geliştirme Yaşam Döngüsü de dahil olmak üzere bunu yapan birkaç programlama yöntemi vardır.

(<https://www.microsoft.com/en-us/sdl>), Microsoft ve diğer önde gelen satıcılar tarafından kullanılır. SDL benzeri güvenlik tasarımına sahip satıcılar, güvenlik açıkları olan ancak olmayan yazılımlardan daha az güvenlik açıklarına sahip ürünler yaratmaya devam edecekler.

Diğer Fiziksel Saldırıları

Bilgisayar güvenliği dünyasında, bir saldırganın fiziksel kontrolü altındaki bir bilgisayar cihazının asla güvenli olmadığına dair bir söz vardır. Bu söz asla kriptografi ve MFA çözümleri dünyasına uygulandığında olduğu kadar doğru değildir. Bir MFA çözümünün gizli şifreleme anahtarları, bir yerde saklanmalı ve kimlik doğrulamada başarılı bir şekilde kullanılabilmesi için şifresi çözülmüş, düz metin durumunda gösterilmelidir.

Elektron Mikroskobu Saldırısı

Saldırganlar, çiplerde veya cihazlarda saklanan gizli şifreleme anahtarlarının moleküler seviyeye bakılarak keşfedilebileceğini öğrendi. Bir durumda, bir bilgisayar bilimcisi Elektron Mikroskobu kullandı (<https://gcn.com/articles/2010/02/02/black-hat-chip-crack-020210.aspx>) yalnızca şifreleme anahtarlarını güvenli bir şekilde saklamak için tasarlanmış özel bir şifreleme çipinde gizli şifreleme anahtarlarını bulmak için. Bu tür saldırılara karşı savunmasız olmayacak hiçbir MFA donanım çözümü yoktur.

Soğuk Önyükeme Saldırıları

Soğuk başlatma saldırıları, saklanan gizli anahtarların yakalanabildiği, analiz edilebildiği ve bazıları doğal ve olağan olaylar ve diğerleri doğal olmayan ve olağan olan bir dizi farklı eylemle açığa çıkarılabildiği bir saldırı sınıfıdır. Bu tür saldırıların çoğu, koruma sürecine dahil olan diğer bilgi işlem cihazlarının veya çiplerin doğal özelliklerine dayanır.

Örneğin, bilgisayar belleği verilerin şifresini çözmek için kullanılan şifrenlenmemiş gizli anahtarın bir kopyasını içeriyorsa, bellekteki veriler "dondurulabilir", ardından başka bir bilgisayara alınabilir ve tehlikeye atılabilir. En iyi bilinen örneklerden birinde, araştırmacılar, bellek yongalarında buz görünene kadar herhangi bir büro malzemeleri mağazasından satın alabileceğiniz, çalışan bir bilgisayara düzenli, çok yaygın olarak kullanılan bilgisayar belleğini basınçlı hava ile püskürttüler.

Daha sonra bu donmuş bellek yongalarını, özel adli yazılım içeren başka bir bilgisayara kaldırdılar. Yeni bilgisayarı diğer bellek yongalarıyla birlikte kullanarak, şifreleme gizli anahtarını bulup çıkarabildiler. Soğuk önyükeme saldırıları hakkında daha fazla ayrıntı için aşağıdaki bağlantılara bakın:

- https://en.wikipedia.org/wiki/Cold_boot_attack
- <https://www.zdnet.com/article/cryogenically-frozen-ram-bypasses-all-disk-encryption-methods/>
- <https://www.wired.com/story/cold-boot-break-pc-encryption/>

Savunma: MFA çözümlerinin bilgisayar korsanlarının eline geçmesini önlemeye çalışın ve iki farklı faktör türü gerektiren MFA çözümlerini kullanın, böylece fiziksel olarak birini kazanırlarsa diğerine otomatik olarak sahip olmazlar.

MFA'ya karşı başarılı olan veya başarılı olabilecek 15'ten fazla saldırının önceki listesi kapsamlı bir liste değildir. Yan kanal saldırıları ve elektromanyetik radyasyon (EMR) dinlemesi gibi iyi bilinen birçok yöntemi kapsamadı. Ancak, kullanıcıların ve yöneticilerin MFA çözümlerini seçip uygularken bilmeleri gereken saldırı türlerinin harika bir temsili özetidir.

Bu, bazı MFA çözümlerinin diğerlerinden daha güvenli olmadığı anlamına gelmez. İşin püf noktası, senaryolarınızın çoğu için doğru miktarda korumaya sahip MFA çözümünü seçmektir. Tüm çözümler ve senaryolar için “doğru cevap” yoktur. Sadece sizin ve ihtiyaçlarınız için en uygun olanı seçin. En iyi MFA çözümünüzü bulmaya başlamak için harika bir yer, aşağıdaki bağlantıları ziyaret etmektir:

Parolaları Değiştirme Görevi teknik incelemesi <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/QuestToReplacePasswords.pdf>

NIST Dijital Kimlik Kılavuzları <https://pages.nist.gov/800-63-3/>

Bir web sitesinin 2FA'yı destekleyip desteklemediğini kontrol edin

<https://twofactorauth.org/>

MFA Saldırılarına Karşı Savunmaları Özetleme

Daha önce tartışılan her MFA saldırı türü, bölümün sonunda bir veya daha fazla özetlenmiş savunma içeriyordu. Bu bölüm, hızlı başvuru için kullanılacak bu yöntemlerin yalnızca yeniden özetidir.

Sosyal Savunmalar

- Herhangi bir MFA çözümü de dahil olmak üzere hiçbir şeyin hacklenemez olduğunun farkına varın
- Güvenlik farkındalığı eğitiminize MFA korsanlığı farkındalığını dahil edin
- Bu teknik incelemeyi iş arkadaşlarınızla ve yönetimle paylaşın
- Hileli bağlantılara tıklamak için kandırılmayın
- Hileli bağlantıları mümkün olduğunca engelleyin
- Bir URL'nin meşru olduğundan emin olun

Teknik Savunma

- Mümkün olduğunda GEREKLİ MFA'yı etkinleştirin
- Mümkün olduğunda SMS tabanlı MFA kullanmayın
- İstemci tarafının sunucuya önceden kaydedilmesini gerektiren "1:1" MFA çözümlerini kullanın
- Mümkün olduğunda iki yönlü, karşılıklı, kimlik doğrulama kullanın/gerektirin
- Eski. FIDO U2F'nin Kanal veya Token Bağlaması
- MFA çözümünüz özellikle oturum belirteci hırsızlığı ve/veya kötü amaçlı tekrar oynatmalarla (yani , tekrar oynatmaya dayanıklı) mücadele ediyor mu?
- MFA satıcınızın desteği sosyal olarak tasarlanabilir mi?
- MFA satıcılarının programlamalarında güvenli geliştirme yaşam döngüsü (SDL) kullandığından emin olun
- MFA'nın "kötü deneme kısıtlaması" veya "hesap kilitleme" özelliğinin etkinleştirildiğinden emin olun
- Farklı "kanallar" veya "bantlar" (bant içi/bant dışı) arasında yayılma faktörleri
- MFA oturum açmalarının benzersiz tanımlaması için MFA tarafından kullanılan kimlik özniteliklerini koruyun ve denetleyin
- Dürüst yanıtları kullanarak parola sıfırlama sorularını yanıtlamayın
- ek faktörlerin istendiği yerlerde dinamik kimlik doğrulamayı kullanmak için siteleri ve hizmetleri teşvik edin ve kullanın
- "Paylaşılan gizli" sistemlerin risklerini anlayın
- İşlem tabanlı kimlik doğrulama için, onay iletilmeden/gerekli olmadan önce kullanıcıya tüm kritik ayrıntıları bant dışı göndermeniz gerekir.

Çözüm

Bu makaleden elde edilen temel çıkarımlar şunları içerir:

- MFA hacklenemez değildir .
- MFA, kimlik avı veya sosyal mühendisliğin başarılı olmasını engellemez.
- MFA iyidir. Herkes elinden geldiğince kullanılmalı ama kırılmaz değil.
- MFA'yı kullanır veya kullanmayı düşünüyorsanız, güvenlik bilinci eğitimi, genel güvenlik savunmanızın hala büyük bir parçası olmalıdır.