cpl.thalesgroup.com

THALES
Building a future we can all trust

Fidye yazılım saldırıları korumasız RDP protokollerini nasıl suistimal ediyor ve saldırılara karşı hangi önlemleri alabilirsiniz?

Çeşitli sektörlerde faaliyet gösteren işletmeleri hedef alan fidye yazılım (ransomware) saldırıları, 2020 yılının ilk yarısında hızla yükselişe geçmiştir. Bilgisayar korsanları kötü niyetli amaçlarını hayata geçirmek amacıyla; dijital haberleşme ve uzaktan çalışma uygulamalarını kullanmamızı fırsat bilerek bu durumu suistimal ediyorlar. Sonuç olarak, fidye yazılım olaylarının büyük bir çoğunluğunun **sınırlı sayıda saldırı vektörüyle** ilişkili olduğu söylenebilir; ilk üç sırada ise iyi korunmayan uzak masaüstü protokolü (RDP) uç noktaları, e-posta kimlik avcılığı (phishing) ve sıfır gün VPN güvenlik açıklarının kötüye kullanımı yer almaktadır.

Coveware, Emsisoft ve **Recorded Future** raporlarında "RDP'nin tek başına en büyük fidye yazılım saldırı vektörü olarak kabul edildiği" ve 2020 yılında çoğu fidye yazılım olaylarının kaynağı olduğu vurgulanmaktadır.

Bazıları RDP'nin fidye yazılımlar için en çok tercih edilen saldırı vektörü olmasının, mevcut evden çalışma kurgularıyla ilişkili olduğunu düşünebilir. Ancak, bu doğru değildir. Geçen yıldan bu yana fidye yazılım saldırısı yapan kişilerin tüketicileri hedef almaktan vazgeçip bunun yerine şirketleri ve kritik altyapıları hedef almaya başlamasıyla birlikte RDP en başta gelen saldırı vektörleri arasında yerini almıştır.

Bu olayın temel nedeni nedir?

RDP; uzak sistemlere bağlanmak için kullanılan en yaygın teknolojidir ve özel bir ağda kullanıldığında genel olarak emniyetli ve güvenli bir araç olarak kabul edilir. Bununla birlikte, RDP portları İnternet üzerinden açık kaldığı ve basit şifrelerle erişilebilir olduğu durumlarda ciddi güvenlik sorunlarına yol açabilir. Şifreler kolaylıkla çalınabilir ve bunun sonucunda korumasız kalan RDP protokolleri üzerinden kurumsal ağlara kötü niyetli ve yetkisiz erişim sağlanabilir.

RDP protokolleri üzerinden yetkisiz erişim, saldırıda bulunan kişilerin kurumsal sunuculara erişim kazanmasına ve böylece fidye yazılım saldırılarına davetiye çıkarmasına neden olabilir.

Dünya genelinde, RDP portları İnternet üzerinden açık ve saldırıya karşı korumasız milyonlarca bilgisayar bulunmakta; bu durum RDP portlarını her türlü kötü niyetli siber saldırı faaliyetleri ve sayısı her geçen gün artan fidye yazılım saldırıları için başlıca saldırı vektörü hâline getirmektedir. Söz konusu erişim noktalarını kötüye kullanmayı amaçlayan bilgisayar korsanları, "RDP pazarları" üzerinden ücretsiz olarak bulabiliyor. Bundan sonrası ise her zaman yaptıkları olağan faaliyetler. Kaba kuvvet veya sosyal mühendislik gibi iyi bilinen teknikleri kullanarak zayıf şifreleri arayıp buluyorlar. Saldırgan hedef sisteme erişim kazandıktan sonra ağ güvenliğini mümkün olduğu ölçüde devre dışı bırakmaya odaklanıyor.

Güvenlik sistemleri devre dışı bırakıldıktan ve ağ korumasız hale geldikten sonra ise saldırıdan sorumlu bilgisayar korsanları kötü niyetli yazılım paketini serbestçe uygulamaya koyabiliyor. Bu uygulamalar; fidye yazılım kurulumu, klavye tuşu kaydedici (keylogger) yazılım kurulumu, ele geçirilen bilgisayarların spam içerik göndermek için kullanımı, özel nitelikli kişisel verilerin ve hassas verilerin çalınmasından veya gelecekteki saldırılar için gizli erişim protokolleri vb. kurmaya kadar çeşitli faaliyetleri kapsayabilir.

RDP saldırılarını asgariye indirmek için en iyi uygulamalar

Yukarıda daha önce bahsedildiği üzere RDP protokolleri, kurumsal ağlara girmek için kullanılan erişim noktaları olduğundan; İnternet üzerinden gösterilmemeli veya korumasız bir biçimde yayınlanmamalıdır. Kullanıcıların kolaylığı düşünülerek uzak masaüstü protokollerinin korumasız bir şekilde yayınlanması, işletmelerin maruz kaldığı artan risk ve tehditlere mazeret olarak gösterilmemelidir.

RDP kullanımına ihtiyaç duyan işletmeler için aşağıdaki iyi uygulamalar; erişim noktasının güçlendirilmesine odaklanmakta ve RDP protokollerinin kaba kuvvet saldırılarına karşı güvenliğini korumada faydalıdır.

- Genel bir kural olarak, korumasız uzak masaüstünü İnternetüzerinden paylaşmayın. İnternet üzerinden paylaşılması mutlaksurette gerekli olduğu durumlarda, yalnızca kimliği doğrulanmış kullanıcıların RDP üzerinden erişim sağlamasını temin etmek içinRDP erişim noktasının çok faktörlü kimlik doğrulama (MFA) ile iskorunduğundan emin olun.
- RDP ağ geçitlerini kullanın. Standart RDP 3389 portunu gizlemek amacıyla; uzaktan masaüstü, ters vekil sunucu (proxy) ağ geçitleri arkasından korunmalıdır. RDP ağgeçitlerine; TLS şifreleme protokolüyle korunan HTTPSbağlantıları (port 443) üzerinden erişim sağlanır.
- RDP ağ geçidine erişmek için MFA kullanın. En güçlü şifrelerin bile çalınma ihtimali vardır. MFA tek başına tüm sorunların çözümü olmasa da kullanıcıların bir RDP oturumuna giriş yapması için kullanıcıları asgari olarak iki faktörlü kimlik doğrulama işleminetabi tutarak ek bir güvenlik mekanizması sunar.
- Ağda oturum açmak için MFA kullanın. Uzak masaüstüne erişimsağlandıktan sonra, diğer bir ek güvenlik önlemi olarak ağoturumu açma ekranında da MFA yöntemiyle kimlik doğrulamauygulayın.

Thales SafeNet Trusted Access, Saldırıların Asgariye İndirilmesine Nasıl Yardımcı Olur?

Thales SafeNet Trusted Access; iş ortamınızı RDP tabanlı fidye yazılım saldırılarına karşı korumaya yardımcı olabilir. SafeNet Trusted Access; kullanılan uç nokta cihazı ne olursa olsun, işletmelerin RDP erişim noktalarına, RDP ağ geçitlerine ve ayrıca bulut tabanlı ve eski sürüm uygulamalara uzaktan erişimi etkin bir şekilde güvence altına almasını sağlar.

SafeNet Trusted Access aşağıdaki avantajları sunar:

- Uyarlanabilir ve kademeli kimlik doğrulama, MFA ve donanımbazlı token dahil olmak üzere çeşitli kimlik doğrulama seçenekleriiçin destek
- Tüm işletim sistemleri (Windows/Mac/Linux) için esnek erişimpolitikaları
  –başka bir ifadeyle, hangi işletim sisteminde çalıştıklarınabakılmaksızın; bulut tabanlı uygulamaları ve tüm uzakmasaüstü erişim noktalarını korumak için tek bir erişimyönetimi ve kimlik doğrulama hizmetini kullanabilirsiniz.
- Tek bir Erişim Yönetimi/MFA hizmeti üzerinden bulut tabanlıuygulamaları ve ağda oturum açma işlemlerini merkezi olarakyönetin

Thales Hakkında

Gizliliğinizi koruması için güvendiğiniz kişiler, verilerini koruması için Thales'e güveniyor. Veri güvenliği söz konusu olduğunda, işletmeler her geçen gün daha fazla dönüm noktasıyla karşı karşıya kalıyor. Dönüm noktası niteliğindeki bu karar anlarında, bir şifreleme stratejisinin oluşturulması, bulut ortamına geçiş veya zorunlu mevzuat gerekliliklerini karşılamak gibi hangi kararı verirseniz verin, dijital dönüşümünüzü güvence altına almak için Thales'e güvenin.

Önemli karar anları için kararlı teknoloji.