Endüstriyel ağlara fidye yazılımı **saldırılarının önlenmesi**

Fidye Yazılımı, Westrock ve diğer endüstriyel kuruluşları vurdu. OTD BİLİŞİM uzmanları endüstriyel ağlara fidye yazılımı saldırılarının nasıl önleneceğini paylaşıyor.

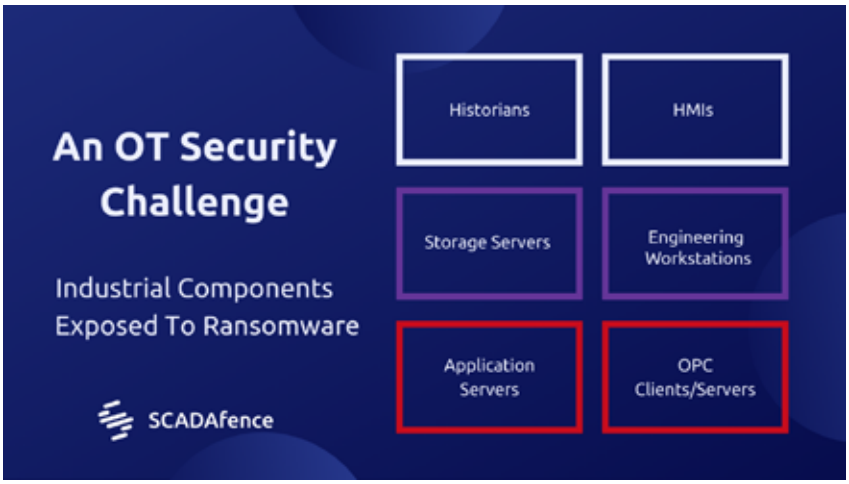
Bu haftanın başlarında, 17 milyar dolarlık ambalaj firmasındaki WestRock operasyonlar, hem BT hem de OT (operasyonel teknoloji) ağlarını etkileyen bir fidye yazılımı saldırısıyla sekteye uğradı. İki gün sonra, 27 milyar dolarlık büyük bir zincir operatörü Dairy Farm Group de fidye yazılımı tarafından saldırıya uğradı ve saldırganlar 30 milyon dolar fidye talep etti. Bunlar sadece bu haftanın başarılı fidye yazılım saldırılarının bir örneğidir.
2017 'deki Wannacry & NotPetya fidye yazılımı saldırılarının patlak vermesinden bu yana, BT tarafından kaynaklanan OT ağlarını etkileyen günlük saldırılara tanık oluyoruz. ABD Ulusal Güvenlik Ajansı (NSA) da bu çok basit nedenden dolayı bu konuyu vurguladı. İşe yaradı.

FİDYE YAZILIMI ÇALIŞMALARI

Bu, görünürde bir son olmamasına karşın, fidye yazılımı saldırıları olaylarının neden son bir yıl içinde keskin bir şekilde arttığını açıklamanın en basit yoludur. PurpleSec'in son raporuna göre, fidye yazılımı saldırılarının sayısı 2018 'den bu yana yüzde 350 arttı, ortalama fidye ödemesi bu yıl yüzde 100' den fazla arttı, kesinti süresi yüzde 200 arttı ve olay başına ortalama maliyet artıyor. Egregor, Conti, Ragnar Locker Ryuk ve diğer birçok isme sahip tehdit aktör grupları acımasızdır, iyi finanse edilir ve COVID -19 aşı üreticilerinden, otomotiv üreticilericilerinden, kritik altyapıdan, hükümetlerden ve hastanelerden ödemelerini almak için herkesi hedef almaya isteklidir. Aslında, ilk fidyeye bağlı ölüm geçen Eylül ayında, bir Alman hastanesine fidye yazılımı bulaştığında ve Kovid -19 salgını sırasında hastaları tedavi edilemediğinde gerçekleşti. SCADAfence'ın sivillerin hayatını ve güvenliğini koruma misyonunun bir parçası olarak, endüstriyel organizasyonunuzdaki fidye yazılımlarını önlemenize yardımcı olmak için bu kılavuzu hazırladık.

FİDYE YAZILIMI ŞİFRELEME SÜRECİ

En başa geri dönelim ve bu saldırıların



▲ *Şema #1 - Bir OT Güvenlik Sorunu: Şifrelemeye Maruz Endüstriyel Bileşenler*

sistemleri nasıl şifrelediğini ele alalım. Araştırdığımız önceki fidye yazılımı saldırılarından, saldırganların ilk erişimlerinden itibaren birkaç saat içinde tüm ağı şifreleyebileceklerini öğrendik. Diğer durumlarda, saldırganlar hangi varlıkları şifrelemek istediklerini değerlendirmek için daha fazla zaman harcayacaklar ve depolama ve uygulama sunucuları gibi önemli sunuculara ulaştıklarından emin olacaklardı. Haberlerde okuduğunuz son fidye yazılımı saldırılarının çoğu, şifreleme işlemlerinin kesintiye uğramayacağından emin olmak için antivirüs işlemlerini sonlandırmaya çalışır.
SNAKE DoppelPaymer VE LockerGoga gibi son fidye yazılım türleri ve hatta Siemens SIMATIC WinCC, Beckhoff TwinCAT, Kepware KEPServerEX ve OPC iletişim protokolü gibi OT ile ilgili süreçleri sonlandırarak daha da ileri gitti. Bu, endüstriyel sürecin kesintiye uğramasını sağladı ve bu, mağdurların fidyeyi ödeme ihtimalini artırdı. Bu tür fidye yazılımı saldırıları son Honda ve ExecuPharm saldırılarında görülmüştür. Gördüğümüz kadarıyla fidye yazılımı genellikle Windows ve Linux makinelerini şifreliyor. Hala şifrelenen bir PLC görmedik. Ancak, historianlar, HMI'lar, depolama, uygulama sunucuları, yönetim portalları ve OPC istemcisi/sunucuları gibi birçok endüstriyel hizmet Windows / Linux makinelerinde çalıştırılmaktadır. Birçok durumda, fidye yazılımı işlemleri BT ağında durmayacak ve ayrıca OT segmentlerine saldıracaktır. Daha fazla şifreli cihaz, saldırganlardan daha yüksek bir parasal fidye talebi anlamına gelir. Kuruluşlar, süreç açısından kritik son noktalara ulaşmadan önce riskleri etkili bir şekilde tanımlamak için BT/OT sınırındaki tehditleri izleyebilmeli ve tespit edebilmelidir.
Fidye yazılımı operatörlerinin kullandığı bazı araçlar ve teknikler, ulus - devlet tehdit aktörlerinin hedefli casusluk kampanyalarında kullandığı seviyededir. Kuruluşların, öldürme zincirinin her adımında fidye yazılımı enfeksiyonu riskini en aza indirmek için bu ortak güvenlik prosedürlerini uygulamalarını öneririz:

İLK ERİŞİM:

1. RDP

a. Mümkünse, RDP'yi iki faktörlü kimlik doğrulama gerektiren uzaktan erişim çözümü ile değiştirin, artık birçok VPN bunu desteklemektedir. Bu, saldırganların, örneğin, SMS ile gönderilen bir kod ile doğrulanmasını gerektirir.
b. RDP kullanmaya devam etmeyi seçerseniz, Windows Güncellemesinin etkin ve çalışır durumda olduğundan emin olun.

2. E-posta Kimlik Avı (Email Phishing)
a. Kuruluşun çalışanlarını kimlik avı saldırıları hakkında eğitin. Çalışanlar doğru görünmeyen e - postalardan şüphelenmeli ve şüpheli bağlantılara tıklamamalıdır.
b. Kimlik avı önleme çözümü yükleyin.

3. İnternet Yüzeyli Sunucuların Yazılım Güvenlik Açıkları
a. Kuruluşunuzun IP aralığını ağ dışından tarayın. Açıkta kalan tüm IP/bağlantı noktalarının beklediğiniz gibi olduğundan emin olun.
b. Maruz kalan hizmetleriniz için otomatik güvenlik güncellemelerinin etkinleştirildiğinden emin olun. Hizmetlerinizden biri (örneğin web sunucuları gibi) bu özelliğe sahip değilse, bu özelliğe sahip benzer bir hizmetle değiştirmeyi düşünün.

YANAL HAREKET:

1. Güvenlik Duvarları ve Windows Güncellemesi
Tüm iş istasyonlarınızda ve sunucularınızda güvenlik duvarlarını etkinleştirin. Windows Güncellemesi'nin etkinleştirildiğinden emin olun. Bu durum, makinelerinizin en son güvenlik açıkları için kaynaklı olmasını ve ayrıca yanal hareket tekniklerine daha az eğilimli olmasını sağlayacaktır. Microsoft, güvenlik politikalarını ve güvenlik duvarı kurallarını sürekli günceller. İyi bir örnek, 'at' komutunu kullanarak süreçlerin uzaktan oluşturulmasını devre dışı bırakmalarıdır.

2. Uç Nokta Koruması
Uç nokta koruma işleri. Klasik bilgisayar korsanlarının tekniklerini engellemenin ötesinde, bazıları fidye yazılımlarına karşı da savunmaya sahiptir ve verilerinizi şifrelemeden koruyacaktır.

3. Ağ Segmentasyonu
İdeal olarak, bir fidye yazılımı saldırısına maruz kaldığınızda endüstriyel ağınızın etkilenme riskini en aza indirmek istersiniz.
a. Mümkün olduğunca BT ağını OT ağ segmentinden ayırın. Segmentler arasındaki erişimi izleyin ve sınırlayın.
b. OT ve BT ağları için farklı yönetim sunucuları kullanın (Windows domainleri vb.). Bunu yaparak, BT etki alanından ödün vermek OT etki alanından ödün vermeyecektir.

4. Sürekli Ağ İzleme
Sürekli bir ağ izleme platformu (çok iyi bir tane biliyoruz.), ağ trafiğini analiz ederken tehditleri tanımlamanıza yardımcı olacak ve ağınızda neler olup bittiğinin daha büyük resmini görmenize yardımcı olacaktır.

5. Veri Boşaltma
Ağınızı olağandışı giden trafiğe karşı izleyin. Günlük kullanıcı etkinliği, kullanıcı başına yaklaşık 200 MB/gün'den daha yüksek yükleme bağlantısı etkinliği oluşturmamalıdır.

SCADAfence SİZE NASIL YARDIMCI OLUR?

Sizinki gibi endüstriyel kuruluşları endüstriyel siber saldırılardan (fidye yazılımı dahil) korumak için oluşturulan kapsamlı bir çözüm olan SCADAfence platformunu sunuyoruz . Ayrıca yerleşik özellikleri arasında uluslararası güvenlik standartlarını uygulamanıza yardımcı olur. Bunlardan bazıları şunlardır:
❖ Varlık Yönetimi
❖ Ağ Haritaları
❖ Trafik Analizörleri
Bu araçlar, kuruluşunuzun daha iyi ağ segmentasyonu uygulamasına, güvenlik duvarlarınızın düzgün çalıştığından ve OT ağındaki her aygıtın yalnızca iletişim kurması gerekenlerle iletişim kurduğundan emin olmanıza yardımcı olacaktır. Ayrıca, olması gereken yerde olmayan varlıkları da tespit edebileceksiniz, örneğin, DMZ'deki unutulmuş varlıklar. Aynı zamanda en yüksek puanlı OT ve IoT güvenlik platformu olan platform, tipik fidye yazılımı saldırılarında bulunanlar da dahil olmak üzere herhangi bir tehdit için ağ trafiğini izler; örneğin:
❖ Güvenlik ihlalleri ağ üzerinden gönderiliyor.
❖ En son teknikleri kullanarak yanal hareket girişimleri.
❖ Ağ taraması ve ağ keşfi.
Bir güvenlik ihlali durumunda, SCADAfence'ın ayrıntılı uyarıları bu tehditleri en kısa sürede kontrol altına almanıza yardımcı olacaktır. Sonuçta, endüstriyel kuruluşların saldırı yüzeylerini anlamalarına yardımcı olmak, herhangi bir kötü niyetli veya anormal aktivite için etkili segmentasyon ve sürekli ağ izlemesi uygulamak için bu aracı geliştirdik.

▲ *Şema #2 - Fidye Yazılımının Önlenmesi: Endüstriyel Ağlarınıza Fidye Yazılımı Saldırılarının Önlenmesi*

▲ *Şema #3 - Fidye Yazılımı Saldırılarında En Sık Kullanılan Taktikler, Teknikler ve Prosedürler*

VİDEO: HEDEFLENEN FİDYE YAZILIMI SALDIRISININ ANATOMİSİ:

Endüstriyel bir fidye yazılımı siber saldırısına verdiğimiz son olay yanıtının gerçek bir hikâyesini sizinle paylaşmak istiyoruz. SCADAfence'ın olay müdahale ekibi siber güvenlik acil durumlarında şirketlere yardımcı olmaktadır. Bu videoda, katıldığımız son bir olay müdahale etkinliğini inceleyeceğiz. Bu araştırma, kuruluşların bu tür etkinlikleri planlamalarına ve hedeflenen endüstriyel fidye yazılımlarının ağlarındaki etkisini azaltmalarına yardımcı olmak amacıyla yayınlanmıştır.

Bu hikâye hakkında daha ayrıntılı bilgi ve ürün hakkında detaylı bilgi almak isterseniz, OTD BİLİŞİM satış ekibi ile iletişime geçebilirsiniz.