DDoS Saldırılarının Sıklığı ve Karmaşıklığı Artıyor; Savunma Tarafında Olanlar Destek için Çareyi Otomasyonda ve Yönetilen Hizmetlerde Buluyor

NETSCOUT Arbor, 13. Yıllık Global Altyapı Güvenliği Raporunu (WISR) Yayınlıyor

BURLINGTON, Mass., 23 Ocak 2018 – NETSCOUT Arbor (NASDAQ: NTCT), dünyanın önde gelen hizmet sağlayıcı, bulut/barındırma ve kurumsal şirketlerde görevli ağ ve güvenlik uzmanlarının görüşlerini doğrudan sunan 13. Yıllık Global Altyapı Güvenliği Raporunu (WISR) bugün yayınladı. Raporda DDoS saldırılarının yanı sıra SDN/NFV ve IPv6'nin benimsenmesi gibi belli başlı sektörel trendlerden olay yanıtı eğitimi, personel idaresi ve bütçe gibi temel kurumsal sorunlara uzanan çok sayıda konu ele alınıyor. Rapor, ağ operatörlerinin siber tehditler nedeniyle her gün karşılaştığı operasyon güçlüklerine ve bunları azaltıp ortadan kaldırmaya yönelik stratejilere odaklanıyor.

NETSCOUT Arbor Teknolojiden Sorumlu Müdürü Darren Anstee, "Saldırganlar bu yıl hedeflerine ulaşmak için büyük kapsamlı saldırı hacminden uzaklaşarak IoT cihazların silahlandırılmasından yararlanan karmaşık saldırılara odaklandı. Saldırganlar oldukça etkili oldu ve DDoS saldırısı nedeniyle gelir kaybına uğrayan kuruluşların oranı bu yıl neredeyse iki katına çıkarak DDoS saldırısının önemini bir kez daha gösterdi," şeklinde belirti. "WISR anketinin sonuçları, ATLAS verilerimizle birlikte veri merkezinden buluta uzanan çok katmanlı entegre bir savunma sisteminin gerekli olduğunu gösterdi."

TEHDİT MANZARASI: IoT cihazların istismar edilmesi ve DDoS saldırısı hizmetlerinden daha yenilikçi saldırılara geçilmesi daha sık ve karmaşık saldırılara neden olmaktadır.

- **Boyut:** Kurumsal operatörlerin yüzde elli yedisi ve veri merkezi operatörlerinin yüzde kırk beşi, DDoS saldırıları nedeniyle internet bant genişliklerinin doygunluğa ulaşmasıyla karşılaşmıştır.
- **Sıklık:** Küresel internet trafiğinin yaklaşık üçte birini kapsayan Arbor'ın ATLAS altyapısına göre 2017 yılında 7,5 milyon DDoS saldırısı gerçekleşmiştir. Hizmet sağlayıcı katılımcılar daha çok hacimsel saldırı yaşarken kurumlar ise gizli uygulama katmanı saldırılarında yüzde otuz artış olduğunu bildirmiştir.
- **Karmaşıklık:** Çok vektörlü saldırıların sayısı önceki yıla göre yüzde yirmi artarak hizmet sağlayıcılarda yüzde elli dokuz ve kurumsal katılımcılarda yüzde kırk sekizi olmuştur. Çok vektörlü saldırılar yüksek hacimli floodları, uygulama katmanı saldırılarını ve TCP durumu kaybına neden olan saldırıları tek bir sürekli taarruz altında birleştirerek etki azaltmanın karmaşıklığını ve saldırganın başarı ihtimalini artırmaktadır.

SONUÇLAR: Başarılı DDoS saldırılarının operasyonel ve mali etkisi artmaktadır.

- Katılımcıların yüzde elli yedisi saldırının işe olan temel etkisini itibar/markaya gelen zarar olarak belirtilirken operasyonel harcamalar ikinci sırayı almıştır.
- 10.000 $ ile 100.000 $ arasında mali etki belirten katılımcıların oranı 2016'ya göre neredeyse ikiye katlanarak yüzde elli altıya çıkmıştır.

• Veri merkezi operatörlerinin yüzde kırk sekizi, başarılı bir saldırının ardından en önemli sorunun müşterinin kaçması olduğunu söylemiştir.

SAVUNMA: Birbirine bağlı dünyanın koruyucuları olan ağ ve güvenlik ekiplerinin karşısına aktif ve karmaşık bir tehdit manzarasının yanı sıra kalıcı personel sorunları da çıkmaktadır.

- Hizmet sağlayıcıların yüzde seksen sekizi Akıllı DDoS Etki Azaltma Çözümleri kullanmakta ve yüzde otuz altısı DDoS etkisini hafifleten teknolojiden yararlanmaktadır. Hizmet sağlayıcı ağlarında karşılaşılan saldırıların sayısı, özel otomasyon araçlarına yapılan yatırımları artırmaktadır.
- Saldırı sıklığı da yönetilen güvenlik hizmetlerine olan talebi tetiklemektedir. Önceki yıl üçüncü taraf ve dışarıdan hizmet alan kurumların oranı yüzde yirmi sekiz olurken bu yıl bu oran yüzde otuz sekiz olmuştur. Katılımcıların sadece yüzde otuzu savunma tatbikatları düzenlemiş ve en az her üç ayda bir tatbikat düzenleyen katılımcıların oranı yüzde yirmi düşmüştür.
- Kurumların yüzde kırk dördü ve hizmet sağlayıcıların yüzde kırk sekizi, kalifiye personelin işe alınmasında ve işte tutulmasında zorluk yaşamıştır.

Ek Kaynaklar

- Raporun tamamını buradan indirin (kayıt gerektirir).
- WISR'nin önemli bulguları hakkında daha fazla bilgi almak için NETSCOUT Arbor'un webinar serisine Kaydolun.
- Raporun farklı yönleri hakkındaki görüşler için NETSCOUT Arbor blog'unu ziyaret edin.
- Bizi Facebook'da beğenin ve diğer önemli bulgular için Twitter'da @ArborNetworks ile takip edin.

Anket Kapsamı ve Demografi

- WISR anketi verileri dünyanın her yerinden Katman 1, Katman 2 ve Katman 3 hizmet sağlayıcıların yanı sıra, barındırma, mobil, kurumsal ve diğer tür ağ operatörlerinin bir karması olan 390 katılımcının yanıtlarına dayanmaktadır.
- Katılımcıların üçte ikisi kendisini güvenlik, ağ veya operasyon profesyoneli olarak tanımlamaktadır.
- Veriler Kasım 2016 ile Ekim 2017 arasındaki süreyi kapsamaktadır.

NETSCOUT Hakkında

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT), işletmelerin dijital hizmetlerde yaşadıkları tüm kullanılabilirlik, performans veya güvenlik sorunlarına karşı güvence sağlar. Pazar ve teknoloji lideri konumumuzu, akıllı analizi patentli akıllı veri teknolojimizle birleştirerek elde ettik. Müşterilerin dijital dönüşümünü hızlandırmak ve güvenliğini sağlamak için gereken gerçek zamanlı ve yaygın görünürlüğü, bilgileri ve Wi-Fi araçlarını sağlıyoruz. Yaklaşımımız, kuruluşların hizmetleri ve uygulamaları planlama, sunma, entegre etme, test etme ve dağıtma biçimini değiştirir. nGenius hizmet güvencesi çözümlerimiz hizmet, ağ ve uygulama performansının gerçek zamanlı ve bağlamsal analizini sağlar. Arbor güvenlik çözümleri, kullanılabilirliği tehdit eden DDoS saldırılarına ve kritik iş varlıklarını çalmak için ağlara sızan gelişmiş tehditlere karşı koruma sağlar. Fiziksel/sanal veri merkezlerindeki veya buluttaki hizmet, ağ ve uygulama performansını arttırma hakkında bilgi almak ve NETSCOUT'un hizmet istihbaratından güç alan performans ve güvenlik çözümlerinin güvenli bir şekilde ilerlemenize nasıl yardımcı olabilece-

ğini öğrenmek için www.netscout.com adresini ziyaret edin veya Twitter, Facebook veya LinkedIn'de @NETSCOUT ve @ArborNetworks'ü takip edin.

Güvenli Liman

Bu bültendeki ileriye yönelik ifadeler, 1934 Sermaye Piyasası Kanununun 21E Bölümü ve diğer federal menkul kıymetler kanunlarının güvenlik liman hükümleri uyarınca yapılır. Yatırımcılar, Arbor'ın çözüm portföyünün avantajları ve özellikleri ile ilgili ifadeler de dahil ancak bunlarla sınırlı olmamak üzere, kesinlikle tarihsel olmayan ifadeler içeren bu basın bülteninde yer alan ifadelerin, riskler ve belirsizlikler içeren ileriye dönük ifadeler oluşturduğu konusunda uyarılmıştır. Gerçek sonuçlar, bilinen ve bilinmeyen riskler, belirsizlikler, varsayımlar ve diğer faktörler nedeniyle ileriye yönelik ifadelerden önemli ölçüde farklılık gösterebilir. NETSCOUT ile ilişkili risk faktörlerinin daha ayrıntılı bir açıklaması için, sona eren mali yıl için NETSCOUT'un Form 10-K Yıllık Raporu'na 31 Mart 2017 ve NETSCOUT'un Form 10-Q sonraki Üç Aylık Raporlarına bakın. Bunlar, Menkul Kıymetler ve Borsa Komisyonu'nda dosyalanır. NETSCOUT bu basın açıklamasında yer alan ileriye dönük bilgileri güncelleştirme veya burada açıklanan duyurularla ilgili güncelleştirme yükümlülüğünü üstlenmez.