TERMODİNAMİK

Ayda bir yayımlanır • Eylül 2018 • Yıl: 27 • Sayı: 313 • 14 TL • ISSN 1302-6065 • www.termodinamik.info

dsyg

DSYG Dergilik
dergilerinize her yerden ulaşın...

SÖYLEŞİ
TÜRKONFED
Yönetim Kurulu Başkanı
Orhan Turan

Yangınla Mücadele Mevzuatı ve TSEN 12845+A2 & NFPA20 Karşılaştırması

Yaz Aylarında Veri Merkezi İklimlendirmesi için 5 Pratik Öneri

Isıtma Sistemlerinde Besleme Suyu Sıcaklığının Düşürülmesi

2018 · 09

İklimlendirme Sistemlerinde
Mikrobiyolojik Üremenin Azaltılması

Yayın Adı : Termodinamik
Referans No : 81087900
Dağıtım alanı : Ulusal
Yayın Periyot : Aylık
Yayın Tipi : Dergi
Yayın Tarihi : 01.09.2018
Sayfa : 24
Tiraj : 6000
Reklam E.($) : 483,33

AJANS PRESS

Haberler

Siber Saldırganlar, Klimaları Botnetlere Dönüştürüyor

Klimalar, sadece yaz sıcağından kurtulmak istediğimizde aklımıza geliyor. Ancak güncel bir araştırma, akıllı klima gibi internete bağlı ev cihazlarımızı hedefleyen siber saldırganların, milyonlarca kişiyi etkileyen büyük elektrik kesintileri yaratabileceğini gösteriyor. IoT cihaz üreticilerinin siber saldırılara karşı dayanıklı ürünler tasarlaması gerektiğini belirten Komtera Teknoloji güvenlik uzmanları, aksi takdirde evlerdeki akıllı cihazları hedef alan siber saldırganların büyük çapta elektrik kesintilerine sebep olabileceğini belirtiyor. Princeton Üniversitesi araştırmacılarının IoT cihazların güvenliğine dair oluşturduğu yeni rapor, akıllı klimalar gibi internete bağlı çalışan cihazlara yönelik siber saldırıların büyük kapsamlı elektrik kesintilerine sebep olabileceğini gösteriyor. Siber saldırganlar, yazın çok kullanılan klimaları botnetlere dönüştürerek elektrik tüketimlerini artırabiliyor. Yüz binlerce cihazla yapılan bu eylem, elektrik şebekesini etkisiz hale getirebilecek büyüklükte etkiler yaratabiliyor. Bilişim güvenliği alanında çözümler sunan Komtera Teknoloji güvenlik uzmanları, IoT cihazları hedef alan saldırıların bir ülkeyi kapsayacak büyüklükte elektrik kesintisine neden olabileceğini söylüyor. Kötü amaçlı yazılımları kullanarak IoT cihazlardan botnetler üreten hackerlerin yüz binlerce klimanın elektrik tüketimini sadece %1 artırması, 38 milyon kişiyi kapsayacak derecede büyük bir elektrik kesintisi yaratabiliyor. Bu sayı yaklaşık olarak Kanada ya da Kaliforniya gibi yaygın yerleşime sahip olan yerlerin nüfusuna denk geliyor. Bireysel günlük kullanımlar dışında, polis merkezlerinden hastanelere ya da tedavisi evde elektrikli cihazlarla süren hastaların cihazlarına kadar pek çok sistemin çalışması, böyle bir saldırıyla aniden aksayabiliyor.

Üretilen çoğu IoT cihazdaki güvenlik seviyesi yetersiz

Araştırma raporunda BlackIoT olarak adlandırılan saldırılarla klimanızın ya da diğer IoT cihazlarınızın botnet olarak kullanılması ile elektrik şebekelerinde büyük ölçekli ve birbiriyle bağlantılı saldırılar başlatılabiliyor. Talep manipülasyonu denilen teknikle siber saldırganlar elektrik tüketimini yükselterek şebekelerin çalışma dengesini bozuyor. Elektrik şebekesini çökertmek için kaç tane cihazın kullanılması gerektiğini görmek adına beş farklı simülasyon üreten araştırmacılar, ortaya çıkan senaryonun oldukça rahatsız edici olduğunu belirtiyor. Sonuçlara göre 38 milyon kişiye hizmet edecek kadar geniş bir elektrik ağı, ele geçirilmiş yüz binlerce klimadaki sadece %1 talep artışıyla çalışmaz hale gelebiliyor. Komtera Teknoloji'nin güvenlik uzmanları, konuyu "Elektrik şebekeleri, arz talebe eşit olduğu sürece stabildir. Ancak eğer güvenlik zafiyetlerinin bulunduğu IoT cihazlarını kullanarak oluşturulmuş çok büyük bir botnetiniz varsa arzı istediğiniz zaman hemen değiştirebilirsiniz. Bu nedenle IoT cihazlarda bulunan güvenlik zafiyetlerinin ortadan kaldırılması gerekiyor" sözleriyle açıklıyor.

Cihazlardaki varsayılan şifrelerin değiştirilmemesi en büyük etken

Mirai Botnet'in verdiği hasarı örnek gösteren Komtera Teknoloji uzmanları, evlerdeki çok sayıda internet yönlendiricisi ve web kamerası gibi IoT cihazlar aracılığıyla DDoS saldırısı yapılabildiğini hatırlatıyor. Komtera Teknoloji güvenlik uzmanları, "Ne yazık ki cihazların çoğu yetersiz güvenlik seviyesiyle tasarlanıp üretiliyor ve kullanılıyor. Ayrıca, üreticilerin güvenlik sistemi entegre etmediği bu cihazlar, genelde teslimat sırasında verilen şifreler değiştirilmeden çalıştırılıyor ve kötü niyetli kişilere kolay erişim imkanı doğuyor" ifadelerinde bulunuyor. Laptop gibi güvenliğine daha çok dikkat edilen cihazlar kadar diğerlerinin de bu anlamda ilgiyi hak ettiğini çünkü güvenlik ihmalinin eşit derecede zarara sebep olacağını söyleyen Komtera Teknoloji güvenlik uzmanları, "Elektrikli akıllı cihazlara yönelik siber saldırı bilincinin bir an önce oluşturulması, büyük önem taşıyor. Güvenliği önlemlerinin tüm cihazlarda takip edilmesi gerekiyor. Aksi takdirde, güvenlik veya gizlilik ile ilgili bireysel sorunlardan çok öteye giden yıkıcı etkiler görülebiliyor. Yakın gelecekte daha çok akıllı cihazın hayatımıza girecek olması, durumu daha kritik hale getirecek" sözleriyle tehlikenin boyutunu vurguluyor.

Yayın Adı : Termodinamik
Referans No : 81087900
Dağıtım alanı : Ulusal
Yayın Periyot : Aylık
Yayın Tipi : Dergi
Yayın Tarihi : 01.09.2018
Sayfa : 24
Tiraj : 6000
Reklam E.($) : 483,33

AJANS PRESS

Siber Saldırganlar, Klimaları Botnetlere Dönüştürüyor

Klimalar, sadece yaz sıcağından kurtulmak istediğimizde aklımıza geliyor. Ancak güncel bir araştırma, akıllı klima gibi internete bağlı ev cihazlarımızı hedefleyen siber saldırganların, milyonlarca kişiyi etkileyen büyük elektrik kesintileri yaratabileceğini gösteriyor. IoT cihaz üreticilerinin siber saldırılara karşı dayanıklı ürünler tasarlaması gerektiğini belirten Komtera Teknoloji güvenlik uzmanları, aksi takdirde evlerdeki akıllı cihazları hedef alan siber saldırganların büyük çapta elektrik kesintilerine sebep olabileceğini belirtiyor. Princeton Üniversitesi araştırmacılarının IoT cihazların güvenliğine dair oluşturduğu yeni rapor, akıllı klimalar gibi internete bağlı çalışan cihazlara yönelik siber saldırıların büyük kapsamlı elektrik kesintilerine sebep olabileceğini gösteriyor. Siber saldırganlar, yazın çok kullanılan klimaları botnetlere dönüştürerek elektrik tüketimlerini artırabiliyor. Yüz binlerce cihazla yapılan bu eylem, elektrik şebekesini etkisiz hale getirebilecek büyüklükte etkiler yaratabiliyor. Bilişim güvenliği alanında çözümler sunan Komtera Teknoloji güvenlik uzmanları, IoT cihazları hedef alan saldırıların bir ülkeyi kapsayacak büyüklükte elektrik kesintisine neden olabileceğini söylüyor. Kötü amaçlı yazılımları kullanarak IoT cihazlardan botnetler üreten hackerlerin yüz binlerce klimanın elektrik tüketimini sadece %1 artırması, 38 milyon kişiyi kapsayacak derecede büyük bir elektrik kesintisi yaratabiliyor. Bu sayı yaklaşık olarak Kanada ya da Kaliforniya gibi yaygın yerleşime sahip olan yerlerin nüfusuna denk geliyor. Bireysel günlük kullanımlar dışında, polis merkezlerinden hastanelere ya da tedavisi evde elektrikli cihazlarla süren hastaların cihazlarına kadar pek çok sistemin çalışması, böyle bir saldırıyla aniden aksayabiliyor.

Üretilen çoğu IoT cihazdaki güvenlik seviyesi yetersiz

Araştırma raporunda BlackIoT olarak adlandırılan saldırılarla klimanızın ya da diğer IoT cihazlarınızın botnet olarak kullanılması ile elektrik şebekelerinde büyük ölçekli ve birbiriyle bağlantılı saldırılar başlatılabiliyor. Talep manipülasyonu denilen teknikle siber saldırganlar elektrik tüketimini yükselterek şebekelerin çalışma dengesini bozuyor. Elektrik şebekesini çökertmek için kaç tane cihazın kullanılması gerektiğini görmek adına beş farklı simülasyon üreten araştırmacılar, ortaya çıkan senaryonun oldukça rahatsız edici olduğunu belirtiyor. Sonuçlara göre 38 milyon kişiye hizmet edecek kadar geniş bir elektrik ağı, ele geçirilmiş yüz binlerce klimadaki sadece %1 talep artışıyla çalışmaz hale gelebiliyor. Komtera Teknoloji'nin güvenlik uzmanları, konuyu "Elektrik şebekeleri, arz talebe eşit olduğu sürece stabildir. Ancak eğer güvenlik zafiyetlerinin bulunduğu IoT cihazlarını kullanarak oluşturulmuş çok büyük bir botnetiniz varsa arzı istediğiniz zaman hemen değiştirebilirsiniz. Bu nedenle IoT cihazlarda bulunan güvenlik zafiyetlerinin ortadan kaldırılması gerekiyor" sözleriyle açıklıyor.

Cihazlardaki varsayılan şifrelerin değiştirilmemesi en büyük etken

Mirai Botnet'in verdiği hasarı örnek gösteren Komtera Teknoloji uzmanları, evlerdeki çok sayıda internet yönlendiricisi ve web kamerası gibi IoT cihazlar aracılığıyla DDoS saldırısı yapılabildiğini hatırlatıyor. Komtera Teknoloji güvenlik uzmanları, "Ne yazık ki cihazların çoğu yetersiz güvenlik seviyesiyle tasarlanıp üretiliyor ve kullanılıyor. Ayrıca, üreticilerin güvenlik sistemi entegre etmediği bu cihazlar, genelde teslimat sırasında verilen şifreler değiştirilmeden çalıştırılıyor ve kötü niyetli kişilere kolay erişim imkanı doğuyor" ifadelerinde bulunuyor. Laptop gibi güvenliğine daha çok dikkat edilen cihazlar kadar diğerlerinin de bu anlamda ilgiyi hak ettiğini çünkü güvenlik ihmalinin eşit derecede zarara sebep olacağını söyleyen Komtera Teknoloji güvenlik uzmanları, "Elektrikli akıllı cihazlara yönelik siber saldırı bilincinin bir an önce oluşturulması, büyük önem taşıyor. Güvenliği önlemlerinin tüm cihazlarda takip edilmesi gerekiyor. Aksi takdirde, güvenlik veya gizlilik ile ilgili bireysel sorunlardan çok öteye giden yıkıcı etkiler görülebiliyor. Yakın gelecekte daha çok akıllı cihazın hayatımıza girecek olması, durumu daha kritik hale getirecek" sözleriyle tehlikenin boyutunu vurguluyor.