**BASIN BÜLTENİ**

**Web kameraları yeterince güvenli mi?**

**Tüm dünyayı etkileyen COVID-19 salgınıyla birlikte video konferans hizmetlerinin, dolayısıyla web kameralarının da kullanımı önemli derecede arttı. Ancak web kameraları da siber suçluların hedefinde yer alıyor. Web kamerasının hala kullanıcının kontrolünde olduğuna altı yöntemle emin olmak mümkün.**

Şirketlerin güvenlik açıklarını bulma ihtiyacını kitle kaynak kullanımıyla hızlı ve şeffaf bir şekilde gideren BugBounter, içinde bulunduğumuz salgın döneminde sıkça kullanılan web kamerasının siber suçlular tarafından ele geçirildiğini gösteren 6 bulguyu paylaştı.

**1. Web kamerasının ışığı alakasız zamanlarda açılabilir**

Cihazların büyük çoğunluğunda web kameralarının yanında küçük bir ışık yer alıyor. Web konferansları ya da toplantıları gibi durumlarda web kamerası açıldığı zaman ışık da yanmaya başlar. Ancak özellikle kullanıcı kamerayı kullanmadığı zaman ışık yanıyorsa başka birisinin uzaktan kamerayı kontrol ediyor olabilir.

Öte yandan arkada çalışan uygulamalardan birisi de kamerayı çalıştırıyor olabilir. Bu yüzden kullanıcıların bu uygulamalara bakması ve çalışan uygulamaların izinlerini kontrol etmesi de önemli.

**2.Tarayıcı eklentileri kamerayı açıyor olabilir**

Tarayıcılara yüklenen eklentiler de kullanıcıların bilgisi dışında kamerayı açabilir. Eğer belirli bir tarayıcı çalıştırıldığında kamera sürekli çalışıyorsa, bu tarayıcıya yüklenen bir eklentinin kamerayı açtığı anlamına gelebilir. Hangisi olduğunu anlamak için kullanıcılar tüm eklentileri kapatıp tek tek açarak kontrol edebilir.

**3.Bilgisayarda web kamerasıyla çekilmiş video dosyaları oluşabilir**

Her ne kadar siber saldırganlar gelişmiş yazılımlarla web kamerasını ele geçirmiş olsa da kamerayla kaydedilen görüntüler bilgisayara kaydedilebilir. Bu yüzden bilgisayar içinde kullanıcının kaydetmediği görüntülere bakmak, web kamerasının siber saldırganlar tarafından ele geçirilip geçirilmediğini anlamanın en kolay yollarından birisi olarak öne çıkıyor.

**4.Güvenlik ayarları değişmiş olabilir**

Kötü amaçlı yazılımlar, web kamerasının kontrolünü daha kolay bir şekilde ele geçirmek için güvenlik ayarlarında değişiklik yapabilir. Kullanıcılar web kamerasının uygulaması üzerinden güvenlik ayarlarına bakarak detaylı bilgilere ulaşabilir. Ayrıca Windows 10’da uygulamaların web kamerasını kullanmasını engelleme özelliği de yer alıyor.

**5.Anti virüs programları şüpheli bir uygulama bulabilir**

Kullanıcılar, yüklü olması tavsiye edilen anti virüs programlarıyla manuel bir tarama yaparak cihazlarında kötü amaçlı bir yazılım olup olmadığını veya şüpheli hareketlerin gerçekleşip gerçekleşmediğini öğrenebilir. Ek olarak detaylara bakarak web kamerasının açığa çıkıp çıkmadığını da görebilir ve anti virüs programının şüpheli tüm içerikleri kaldırdığından emin olabilir.

**6.Kötü amaçlı hacker, kullanıcının cihazına mesaj gönderebilir**

Bilgisayara sızan hackerlar, cihaza bir mesaj göndererek web kamerasından elde edilen görüntülerle şantaj yapabiliyor. Bu mesajlara bir phishing (oltalama) gibi yaklaşmak gerekiyor. Bu mesajların neredeyse tamamı hackerın yaptığıyla veya eriştiği dosyalarla ilgili yalan bilgiler içeriyor. Dolayısıyla web kamerası görüntülerini görmeden kullanıcıların bu bağlantıya tıklamamaları çok önemli.

BugBounter Kurucu Ortağı Murat Lostar, konuyla ilgili şunları söyledi: “Web kameralarının güvenliği sadece COVID-19’la ortaya çıkan bir durum değil. Web kamerasını bantla kapatmak veya özel bir web kamerası kapağı kullanmak bireysel kullanıcılar için alışıldık bir durum. Ancak kurumlarda kullanılan kameralar 7/24 açık kalıyor. Etik bir hacker olan Avishai Efrat, az bir gayretle 15.000’den fazla potansiyel olarak erişebileceği kamera bulduğunu söylüyor. Bu noktada kameraların güvenliğinden emin olmak için donanım, yazılım ve ağ kontrollerinin yanı sıra kameralara sızma konusunda uzman bağımsız güvenlik araştırmacılarından da hizmet alarak doğrulama yapmak ve açıkları kapatmak mümkün.”

**İlgili Kişiler:**

Önder Kalkancı - Marjinal Porter Novelli

0533 927 23 95

onderk@marjinal.com.tr

Sezin Bulum - Marjinal Porter Novelli

0533 282 29 70

sezinb@marjinal.com.tr

**BugBounter hakkında**

Etik hackerların niteliksel ve niceliksel gücünü doğrulama süreçlerinden geçirerek sunan BugBounter, hacklenmeyen bir dünya vizyonuyla siber güvenlik uzmanlarından oluşan bir ekosistem kurmaktadır. Şirketlerin kendilerini siber saldırılara karşı güçlendirmesini sağlayan BugBounter, tüm süreci hem firmalar hem de hackerlar için demokratikleştiren tek platformun geliştiricisidir. <https://bugbounter.com/>