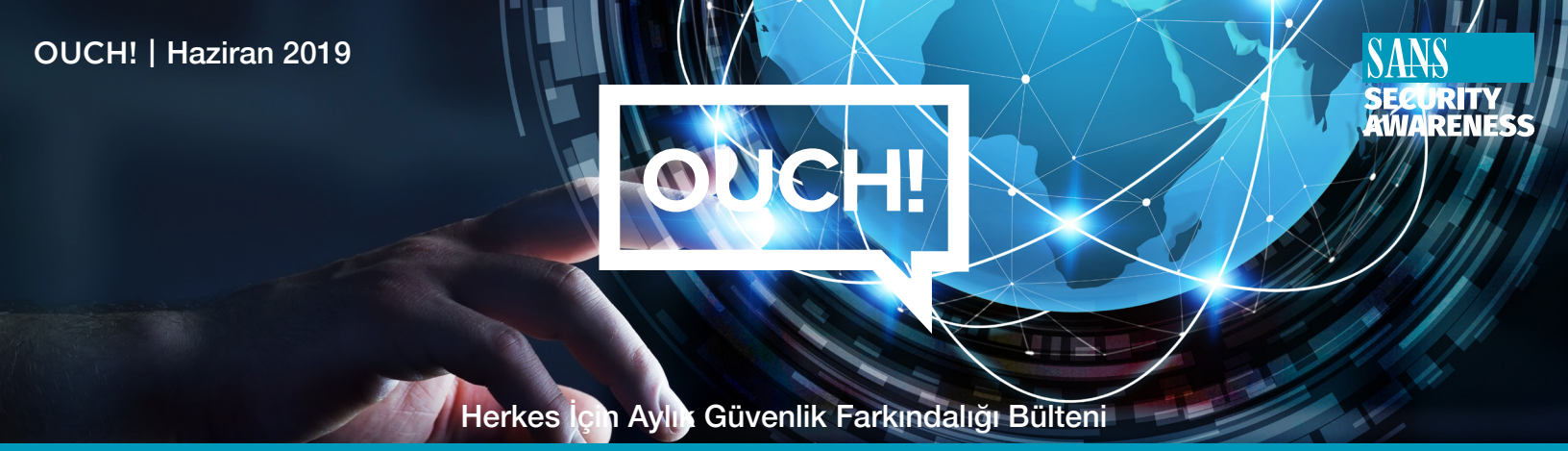


Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

# Dark Web (Karanlık Ağ)

## Genel Bakış

Daha önce başkalarından yada basında "Dark Web" terimini duydunuz ve "*Dark Web de nedir?*" yada "*Bu konuda herhangi bir şey yapmalı mıyım?*" sorularının cevabını merak ettiniz. Bugün Dark Web'in ne olduğunu ve sizin için ne ifade etmesi gerektiğini açıklıyoruz.

## Dark Web nedir?

Dark Web, İnternet üzerinde güvenli ve anonim olarak bilgi iletmek veya paylaşmak için tasarlanmış sistemlerdir. Tek bir "Dark Web" yoktur; Facebook gibi tek bir organizasyon tarafından yönetilen bir şey değildir. Dark Web, farklı amaçlar için kullanılan, farklı insanlar tarafından yönetilen, farklı sistem ve ağlar topluluğudur. Bu sistemler aktif olarak İnternet'e bağlı ve İnternet'in bir parçasıdır, ancak genellikle normal arama motorlarını kullanarak bulamazsınız. Bunları bulmak veya bunlara erişmek için genellikle bilgisayarınızda özel bir yazılıma ihtiyaç duyarsınız. Buna bir örnek Tor Projesidir. Dark Web'e erişmek için, Tor tarayıcısını indirip kurarsınız. Tor tarayıcısını kullanarak web sunucularına bağlandığınızda, şifrelenmiş veri trafiğiniz Tor kullanan diğer bilgisayarlardan geçer. Bu bilgisayarlardan geçerken, kaynak IP adresi değişir, web sitesine girdiğinizde çevrimiçi etkinliğiniz anonimleşir. Dark Web'lerin diğer örnekleri Zeronet, Freenet ve I2P'dir.

## Dark Web'i Kim Kullanır?

Siber suçlular Dark Web'in en büyük kullanıcılarıdır. İsimsiz ve güvenli bir şekilde uyuşturucu satın almak veya gigabaytlarca kanunsuzca ele geçirilmiş veri satmak gibi suç faaliyetlerini mümkün kılmak için web sitelerini ve forumlarını Dark Web üzerinden yönetirler. Örneğin, bir siber suçlu bir bankaya veya bir çevrimiçi alışveriş mağazasına saldırdığında, elinden geldiğince fazla bilgi çalar, daha sonra bu bilgileri sitesinde Dark Web üzerinden diğer siber suçlulara satar.

Dark Web'in meşru kullanımı da yaygındır. Örneğin, sansürün yaygın olduğu ülkelerdeki insanlar, gizliliklerini koruyarak ve kimliklerini saklı tutarak, bilgi paylaşmak ve dünyada başka neler olduğunu görmek için Dark Web ağlarını kullanabilirler. Gazeteciler, muhbirler ve mahremiyet odaklı insanlar, gizliliklerini artırmak ve sansürü aşmak için Dark Web'i kullanabilirler. Ek olarak, bu tarz kişiler Tor Tarayıcı gibi teknolojileri yalnızca Dark Web'e erişmek için kullanmakla kalmaz, aynı zamanda anonim olarak normal Internet'te de gezebilirler.

## Ne Yapmalıyım?

Dark Web'e erişmek için özel bir nedeniniz yoksa, kullanmamanız konusunda sizi uyarıyoruz. Bazı Dark Web siteleri yasadışı amaçlarla kullanılır. Sitelerin çoğu, hedeflerine ulaşmak için bilgisayarınızı kendi ağlarının bir parçası gibi kullanırlar ve bazı durumlarda bilgisayarınız bir uç nokta olarak kullanılabilir veya saldırıya uğrayabilir. Bazı şirketler, adınızın veya diğer bilgilerinizin siber suçlular tarafından çalınıp çalınmadığını ve Dark Web'de bulunup bulunmadığını size bildirmek için izleme hizmeti sunarlar. Bu hizmetlerin gerçekten alınmaya değer olup olmadığı üzerinde düşünülmelidir. Kendinizi korumanın en iyi yolu, bazı bilgilerinizin zaten Dark Web'de siber suçlular tarafından kullanılmakta olduğunu varsaymaktır. Sonuç olarak:

- **Resmi kuruluşlar gibi davranan para cezası ödemek gibi bir eylemde bulunmanız için baskı yapan telefon aramaları veya e-postalardan şüphelenin. Suçlular, kişiselleştirilmiş saldırı oluşturmak için hakkınızda buldukları bilgileri bile kullanabilirler.**
- **Kredi kartı ve banka hesap özetlerinizi kontrol edin. Belki de gerçekleşen işlemlerle ilgili günlük uyarılar bile ayarlanabilir. Bu şekilde, herhangi bir mali dolandırıcılığa maruz kaldığınızı tespit edebilirsiniz. Tespit etmeniz durumunda, hemen kredi kartı şirketinize veya bankanıza bildirin.**

## Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup Hawaii Üniversitesinde yazılım mimarileri ve yazılım güvenliği üzerinde doktora sonrası araştırma yapmaktadır.

Sema Yüce, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, finans, telekomünikasyon, sigortacılık, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, uyum, BT yönetişim/strateji, risk yönetimi, iş sürekliliği, hizmet yönetimi, altyapı hizmetleri, yazılım geliştirme ve program/proje yönetimi alanlarında yönetici ve danışman olarak 19 yılı aşkın süre görev yaptıktan sonra, Truth ISC (www.truth-isc.uk) adıyla kurduğu Türkiye ve İngiltere'de faaliyet gösteren danışmanlık şirketinde hizmet vermeye devam etmektedir.

## Konuk Editor

***Micah Hoffman*** *(@WebBreacher) Spotlight Infosec LLC de Lider Araştırmacı, sertifikalı SANS Enstitüsü eğitmeni ve SANS OSINT kurslarının yazarıdır. Micah'ın siber ve açık kaynaklı zekaya olan tutkusunu projeleri, eğitim yazılımı ve öğretim tarzı göstermektedir.*

## Kaynaklar

| | |
|---|---|
| Kişiselleştirilmiş Saldırılar: | https://www.sans.org/u/RfW |
| Sosyal Mühendislik: | https://www.sans.org/u/Rg1 |
| Kimlik Hırsızlığı: | https://www.identitytheft.gov |
| Tor Tarayıcı: | https://www.torproject.org/ |
| SANS OSINT Kursu: | https://sans.org/sec487 |