SİBER GÜVENLİK
HAFTALIK BÜLTEN **NO.138**

#Haftanın önerisi: Sahte bağlantılar çok farklı şekillerde zarar verebilir, bu nedenle her bir bağlantıyı kontrol ettiğinizden emin olun.! Bu bültenleri düzenli olarak almak istiyorsanız buradan kaydolun!

■ SAĞLIK FIRMASI, KRONAVIRÜS TEDAVILERINI TEST EDERKEN FIDYE SALDIRISINA UĞRADI.

Bir sağlık teknolojisi firmasına yapılan fidye yazılımı saldırısı, bazıları koronavirüs için tedaviler ve aşılar içeren bazı klinik denemeleri yavaşlattı. New York Times'a göre hedef, yüzlerce klinik denemede kullanılan yazılımları satan bir Philadelphia şirketiydi. Ancak hiçbir hasta etkilenmedi.

Daha fazlası

■ FACEBOOK, REKLAM ÇALIŞTIRARAK HESAPLARI ELE GEÇIREN ZARARLI YAZILIMLARI KAPATTI

Wired'e göre, bilgisayar korsanları ele geçirdikleri hesaplar üzerinden diyet hapları, sahte tasarım çantalar ve farklı eşyaların reklamını yapmak amacıyla 4 milyon dolar değerinde reklam satın aldı. Saldırganlar, ele geçirilmiş bir Facebook kullanıcısının hesabına..

Daha fazlası

■ CAPTCHA KULLANAN PHISHING SALDIRISI

Siber suçlular birden fazla CAPTCHA kullanarak hedeflerine saldırdı. Saldırı için oltalama sayfasından önce Office 365 kullanıcılarının tıklaması için çeşitli CAPTCHA'lar yüklediler. Bu saldırılar devam ediyor ve sağlık kurumlarını hedef alıyor. Suçlular,c engellenmemek ve gerçek görünmek için görsel CAPTCHA kullanıyor.

Daha fazlası

■ SAĞLIK SİGORTASI 2014 VERİ İHLALİNİ ÇÖZMEK İÇİN 48 MİLYON DOLAR ÖDEYECEK

30 Eylül'de, ülke çapında 78 milyondan fazla müşterinin kişisel bilgilerini içerdiği iddia edilen 2014 veri ihlalini çözmek için bir sağlık sigortası şirketi ile 42 eyalet başsavcısı ve Columbia Bölgesi arasında çok devletli bir anlaşmaya varıldı. Eyaletlere göre, siber saldırganlar bir kimlik avı e-postası aracılığıyla yüklenen kötü amaçlı yazılımları kullanarak...

Daha fazlası