CYBER SECURITY
WEEKLY BRIEFING **NO.169**

#HaftanınÖnerisi: Yalnızca güvenilir resmi kaynaklardan dosya indirin ve her zaman orijinal yazılım kullanın.

Haftalık bültenleri doğrudan e-postanıza almak için buradan kayıt olabilirsiniz.

■ FUJISTU SALDIRISINDA JAPON KAMU KURUMLARININ VERİLERİ ÇALINDI

Siber korsanlar, Fujitsu'nun proje yönetim platformuna sızarak birçok Japon kamu kuruluşundan veri çaldı. Kara, Altyapı, Ulaştırma ve Turizm Bakanlığı, Japonya Ulusal Siber Güvenlik Merkezi ve Narita Havaalanına ait veriler çalındı.

Devamını oku

■ INTERPOL MALİ SİBER SUÇLARLA MÜCADELEDE 83M DOLAR KURTARDI

Uluslararası Kriminal Polis Teşkilatı (INTERPOL), Eylül 2020 ile Mart 2021 tarihleri arasında çevrimiçi mali suç mağdurlarına ait 83 milyon doların fidyeci saldırganların hesaplarına aktarılmasını engelledi.

Devamını oku

■ KOBALT STRIKE SİBER SUÇLULARIN FAVORİ ARACINA DÖNÜŞTÜ

Açık kaynaklı Metasploit hack platformu, hem kendi ağlarını test etmek için bu araçlara ihtiyaç duyan hem de siber suçluların bunları kendilerine karşı kullanabileceğinden korkan güvenlik ekipleri tarafından 20 yıldır kullanılıyor.

Devamını oku

■ TREND MICRO GÜVENLİK AÇIKLARI EV AĞI GÜVENLİĞİNİ TEHDİT EDİYOR

Trend Micro'nun Ev Ağı Güvenliği sistemlerinde DoS, ayrıcalık yükseltme, kod yürütme ve kimlik doğrulama atlama işlemlerine izin verebilen açıklar bulundu. Sömürülebilir hataları iki yüksek önemde yığın arabellek taşması ve bir sabit kodlanmış parola sorunu oluşturuyor.

Devamını oku