Açıkların Peşinde

Yazılımcıların yaptığı yanlışlar, bulanlara para bulamayanlara risk getiriyor. ERSUN ERDİNÇ

Celil Ünüver ilk yazılım açığı keşfini 21 yaşında, Marmara Üniversitesi'nde iktisat öğrenimi görürken yaptı.

Haziran 2010, İran nükleer programı için önemli bir kesinti tarihiydi. Siber-solucan Stuxnet, Natanz'daki uranyum zenginleştirme tesislerinin İnternet bağlantısı olmayan ağına bir USB bellek yoluyla girmişti. Kendini sistemdeki bilgisayarlara kopyalayıp yayılarak nihayetinde SCADA sistemleri üzerinden U235 ve U238 izotoplarını birbirinden ayırmakta kullanılan Siemens merkezkaç cihazlarının dönüş hızını değiştirerek tahrip olmasına neden olmuştu. Basında yer alan bilgilere göre bin kadar cihaz devre dışı kalmış, Tahran'ın nükleer programı iki yıl geriye gitmişti.

Ağız dalaşı platformunda İran ve ABD'yi karşı karşıya getiren bu olay, 2007'deki Rusya - Estonya siber saldırılarıyla birlikte tarihin ilk siber savaş örneklerinden biri olarak niteleniyor.

Yıllar öncesinin bu saldırısı bizi niçin ilgilendiriyor? 2010'daki bu olayda ortaya çıkan önemli bir nokta daha önce hiç hedef alınmamış bir yapı üzerinden zahmetsizce sabotaj yapılabileceğini de gösterdi. SCADA (Uzaktan Kontrol ve Gözleme Sistemi) yapıları bilgisayarlardan, haberleşme aletlerinden, algılayıcılardan ve yardımcı cihazlardan oluşan ve yönetilip denetlenebilen sistemleri anlatıyor. Genel olarak elektrik, su ve doğalgazı içeren enerji SCADA'sı ile fabrika ve tesis otomasyonunu içeren süreç SCADA'sı biçiminde ikiye ayrılıyor. O tarihe kadar hiçbir üretici böyle bir tehdidi aklına getirmediği için SCADA yazılımlarında güvenliğe pek önem vermeden ürün geliştirdi. Dolayısıyla gereken önlemler alınmadığı sürece başta enerji santralleri olmak üzere hayatı kesintiye uğratacak pek çok endüstriyel tesis için bu tehdit varlığını sürdürüyor. Artık SCADA

sistemlerinde İnternet protokolleri kullanıldıkça tehdit artıyor.

SignalSec Bilgi Güvenlik Danışmanlık Yazılım ve Teknoloji şirketi kurucularından ve yazılım açığı araştırmacısı Celil Ünüver, Türkiye'de yakın zamana kadar SCADA güvenliğine pek önem verilmediğine ama özellikle Stuxnet'ten sonra yavaş yavaş kurumların bilinçlenmeye başladığına dikkat çekiyor. Ünüver genelde firmaların SCADA sistemlerine değil de, ağ sistemlerinin tehdit analizine yöneldiklerini belirtiyor.

Buradaki tehditler yazılımlardaki "sıfır gün açığı" denen hatalardan kaynaklanıyor. Ancak bu hataların özelliği, yazılımın pazara verildiği sırada ne üreticisinin ne de kullanıcısının fark etmesi. Kimsenin bilmediği bu açıkları fark edenler, bu açıktan bilgisayara erişip ilgilendiği yazılımları değiştirebilecek kodları sistemlere yerleştirme olanağına sahip oluyor. Dolayısıyla burada üç farklı pazar oluşuyor. İlki (beyaz pazar) yazılım üreticilerinin, açıklarını gidermek için para ödemesiyle oluşuyor. Kara pazar suiistimale yönelenlerin talebini karşılıyor örneğin para peşindeki siber korsanlar gibi. Gri pazar ise gizli bilgilerle ilgilenen istihbarat örgütlerinin paravan şirketler üzerinden yaptığı alımlardan oluşuyor.

Ünüver, firmaların özellikle Microsoft Windows ve Office, Internet Explorer, Mozilla Firefox, Google Chrome gibi çok yaygın kullanılan yazılımlardaki açıkları bulanlara her bir açık için 10 bin ila 300 bin dolara kadar değişen paralar ödeyerek bunları satın aldıklarını söylüyor. "Bu pazarı hacmin etmek zor ama şu an milyar doları bulmuştur" diyor. Sıfır gün açığını değerli kılan şey, yamasının olmaması ve yazılımın herkeste bulunması nedeniyle açığı bilenin pek çok bilgisayara sızabilmesine olanak vermesi. Ancak pazara dinamizm katan unsur açığı bulmanın bir adım ötesinde açığı kullanıp hedef sisteme sızabilen kodu hazırlamak. Bu durumda 10 bin dolarlık açığın fiyatı kodla beraber 100 bin dolara çıkıyor. Beyond Security, Netradar, Endgame gibi şirketlerin bir bölümü bu açıkları satın alıp kamu kuruluşlarına, istihbarat ve kolluk kuvvetlerine veri olarak servis ediyor. Ünüver, "Biz açıkları önce üretici firmaya bildiriyoruz. O bunu yamadıktan sonra yayımlıyoruz. Bu aslında etik yolu oluyor işin" diyor. Kamu kurumlarının piyasayı örneğin SecurityFocus gibi portallar üzerinden ciddi şekilde izlediğini belirten Ünüver, "Bu işlerle uğraşan şirketler ya da bireysel kişileri bünyelerine katabilmek için de ciddi emek sarf ediyorlar" diyor.

Stuxnet yazılımında çok karmaşık teknikler kullanılmış. Üzerinde uzun süre planlı olarak çalışılmış ve sonucunda güvenlik alanında çalışanların bile mühendisliğini ilgiyle incelediği bir yazılım ortaya çıkmış. Stuxnet'in içerisinde dört tane kritik sıfır gün açığı zafiyeti bulunmuş. Bunlar hem tesislerde kullanılan Siemens SCADA yazılımlarının hem de bunların üzerinde çalıştığı Microsoft yazılımlarının açıklarıydı. Dolayısıyla bir tesise sızmak için basit bir Internet Explorer açığı da yeterli olabiliyor. Ünüver, siber silahların bilinmeyen açıkları sömüren yazılımlar olduğuna dikkat çekiyor ve onları diğer silahlardan ayırıyor: "İran'a Stuxnet yerine fiziken saldırılsaydı, yapan devlet için çok sıkıntılı olurdu ama siber ortamdan yaptığı için 'ben yapmadım' diyebiliyorlar. Tam olarak kanıtlanabilir şeyler değil. Dolayısıyla şu anda o yüzden ABD'nin, İsrail'in, Rusya'nın çok fazla operasyon yaptığı risksiz bir alan."

Bazen de işler Stuxnet örneğindeki gibi planlı değil tamamen kontrol dışı bir risk yayılmasına dönüşüyor. SignalSec bir SCADA yazılımında açık buldu ve üreticisine bildirdi. Yazılım Norveç, Oslo trafik kontrol merkezinde kullanılıyordu. Şirket aynı yazılımı Çek Cumhuriyeti doğalgaz yönetim idaresine ve Kuala Lumpur Havaalanı'na da satmıştı. Açığı keşfedenler için (niyetine bağlı olarak) tek sistem üzerinden birkaç hedef kendiliğinden ortaya çıkıyordu.

> **"Popüler bir yazılımda, bilinmeyen ve yaması olmayan bir açığı sömüren zararlı yazılımlara siber silah diyoruz."**

Günümüzde kullanılan ağ tabanlı SCADA sistemleri açık sistem mimarisine dayanıyor. Bunların sistem protokolleri daha çokWAN üzerinden kullanıldığından siber savaşlara ve siber terörist girişimlere açık olması gibi bir güvenlik sorununu gündeme getiriyor. Ünüver, iyi haberlerden birinin TÜBİTAK ve TSE aracılığıyla SCADA sistem güvenliğini denetleyecek kişiler için sertifika programı olduğunu dikkat çekiyor. Ayrıca iki üç ay sonra endüstriyel sızma testi uzmanı sertifika programı da başlayacak.

Su, elektrik veya doğalgaz kesintilerinin ya da trafik sinyalizasyon aksaklıklarının günlük hayatı nasıl felç ettiği düşünüldüğünde günümüzde gittikçe daha fazla artan oranda otomasyon sistemlerine tabi bu altyapıların kritik pozisyonu ortaya çıkıyor. "Bir ülkeyi komple hack etmek bu yollardan geçiyor" diyor Ünüver...