Venona (2)

ÇETİN KAYA KOÇ

1943 yılında başlayan Venona programı, artık mesaj içeriklerinin önemi kalmamış olmasına rağmen 1980 yılına kadar devam etti ve o yıl kapatıldı. Sonunda Venona, 1944 yılında NSA'ye yardımcı başkanlık yapmış olan William Crowell'in çalışmaları sonucu 1995 yılında kamuoyuna açıklandı. Ben de geçen yıl bir Microsoft toplantısında Crowell'i dinlediğimde, Venona hakkında hayatımda ilk defa detaylı bilgi sahibi oldum. Tabii, projenin bir yöneticisinden olayı dinleyince çok farklı boyutlarının farkına varıyorsunuz.

Bu projenin çok uzun sürmesi ve sosyal ve politik etkilerinin çok yaygın olması dışında, benim ilginç bulduğum iki özelliği var. Birincisi teknik içerik, ikincisi ise insani boyutu. Bu yazımda teknik içerikten biraz bahsetmek istiyorum. Teknik boyut detayları, bir gün kriptanalist olarak çalışma (şifre kırarak hayatını kazanma!) arzusunda olanlara fikir verir umarım. Olayın teknik boyutları, Sovyetlerin kullandığı şifreleme algoritmaları, bu algoritmaların kırılması, metinlerin tercümesi ve takma adların (örneğin, "liberal") keşfedilmesi gibi konular.

1943-1946 arasında 3000e yakın şifreli mesaj elde edilmiş. Venona çalışanları, kırılması imkansız gibi görülen Sovyet şifreleme algoritmalarını çok zahmetli çalışmalar sonucunda kırarak, şifreli mesajları kelime kelime çözmüşler. Sadece algoritmaları kırmak yetmiyor, kod isimlerin kimlere karşılık geldiğini anlamak, Rusça'dan tercüme yapmak ve bu dilin nüanslarına vakıf olmak ve zaman içinde yavaşça olan değişimleri fark etmek gerekiyor. Venona ekibi hem kriptografinin matematiksel özelliklerine ve hemde mesajların dil ve kültür özelliklerine vakıf olmalıydılar. Belki bu bize 37 yılın gizemini biraz açıklayabilir. Venona ekibi prensip olarak 5 şifreleme algoritmasının varlığını keşfetmişler ve bu algoritmalar farklı alanlarda kullanılıyormuş. Şifreleme algoritmaları anlaşılınca, Sovyetlerin diplomatik alanlar dışında (KGB çalışmaları, ticari casusluk gibi) yaptığı şifreli mesajların içerikleri de elde edilmiş.

koc@cryptocode.net