Türkiye'nin siber bekçileri nasıl çalışıyor?

OLAĞANÜSTÜ ŞÜPHELİLER!

'Beyaz hacker' Can Yıldızlı

Telefonumda WhatsApp bildirileri yanıp sönüyor... İsviçre'den, Can Yıldızlı isimli genç bir hacker'dan gelen mesaj evimdeki bilgisayarın çöktüğünü söylüyor. Bunlar bana ulaşan son mesajlar zaten... 10-15 dakika sonra, kullanabileceğim ne internet kalıyor ne de cep telefonu... Can Yıldızlı, fişi çekiyor... Dijital çöplüğe gidiyorum. Ta ki Yıldızlı, sistemimi yeniden açana kadar... Neyse ki, bu benim de haberdar olduğum bir deneme. Yine de paniğe kapılmadan edemiyorum; çünkü kendini 'beyaz hacker' yani sistemin açıklarını bulup sistem yöneticilerine bildiren biri olarak tanımlayan genç adamın yetenekleri korkutucu. Yıldızlı'nın sosyal medya hesabı yok; internete bağlanmayan bir cep telefonu kullanıyor ve kendi gibi yetenekli gençlerden kurduğu ekibiyle Türkiye'deki bankaların yüzde 90'ıyla çalışıyor. İşte bu ekiple beraber dijital dünyaya daldık; kendimizi 'sanalda' nasıl korumamız gerektiğini konuştuk.

Serkan Ocak S10

Beyaz hacker Can Yıldızlı anlattı

Sosyal medyada 'güvenli' diye bir şey yok

Can Yıldızlı'yla ilk kez dört yıl önce, İstanbul'da bir pastanede buluşmuştuk. Saniyeler içinde mekânın internetini kullananları tespit etti ve Facebook hesaplarına girdi. Şok geçirmiştim. Bu kez, İsviçre'de olduğundan WhatsApp üzerinden konuştuk. Cep telefonum üzerinden evimin internetini çökertmesi bir dakikasını almadı bile. 'Pentagon Hacker'ı diye tanınan CanYıldızlı, sistemin açıklarını bulup sistem yöneticilerine bildiren 'beyaz hacker'lardan. Kimlik fotokopileri, kredi kartı bilgileri, e-posta şifreleri çalınan kişileri tespit ediyor. Kurduğu ekiple 'siyah hacker'lara karşı mücadele veriyor. Cebinde ise internete bağlanmayan, eski model, 100 liralık bir mobil telefon taşıyor. Hiçbir sosyal medya hesabı yok. Çünkü biliyor ki internet varsa yüzde 100 güvenlik hiç bir zaman yok.

MUTLAKA

- İnternet bağlantısında ortak ağ kullanıyorsanız, önemli şifrelerinizi girmediğinizden emin olun.
- **Gizli olması gerektiğini düşündüğünüz belge, bilgi, fotoğraflarınızı, ücretsiz depolama hizmeti veren Dropbox gibi servisler yerine güvendiğiniz bir ortamda, örneğin çalıştığınız kurumun server'larında saklayın. Örneğin Can Yıldızlı'nın kurduğu şirketlerin server'ları Alp Dağları'nda eski bir askeri sığınakta. Sistemi kendileri kurdular ve 24 saat kamerayla izliyorlar.**
- Tüm e-postalar, sosyal medya hesapları için 'SMS doğrulama' gibi ikinci güvenlik yöntemlerini kullanın.
- **Cep telefonunuzu satarken geri dönüşümü olmayacak şekilde tüm bilgilerinizi silin.**
- Güvenli konuşma için 'Threema' gibi özel şirketlerin paralı yazılımlarını kullanın. Cep telefonu numarası girmeden hesap yaratılabiliyor. Dinlemeler kolay yakalanmıyor.
- **Cep telefonu veya bilgisayarınıza, tüm yazılımların güncel versiyonlarını indirin. Ne kadar güncel, o kadar güvenli.**
- Bilgisayarlarınız arasında uzaktan erişim kullanıyorsanız, işiniz bittiğinde bilgisayar ve modeminizin uzaktan erişime kapalı olduğundan mutlaka emin olun.
- **Çok güçlü şifreler kullanın ve şifrelerinizi sık sık değiştirin.**

ASLA

- Kafelerde, restoranlarda, otellerde sunulan, ortak kullanıma açık internet hizmetinden bankacılık işlemi yapmayın. Önemli bilgilerinizi, şifrelerinizi girmeyin.
- Telefonda birilerine kredi kartı bilgilerinizi veya başka bir şifrenizi vermeyin.
- Zararlı yazılım ihtimaline karşı format attırmadan ikinci el cep telefonu almayın.
- WhatsApp, Facebook, Twitter, Instagram gibi sosyal medya hesaplarının güvenliğinin yüzde 100 olduğuna güvenmeyin.
- WhatsApp web kullandıktan sonra güvenli çıkış yapmadan bilgisayarın başından ayrılmayın.
- WhatsApp ve Telegram gibi programların grup konuşmaları, birebir yazışmalara oranla daha güvensiz. Önemli yazışmalarınızı gruptan yapmayın.
- WhatsApp yazışmalarının uçtan uca şifrelenmesine güvenmeyin. Telefonun kendisi hack'lenebilir. Örneğin bir resimle gönderilen zararlı kod sayesinde yazışmalar okunabilir.
- Otomatik onayları, gizlilik ayarlarından kaldırmadan sosyal medya hesaplarını kullanmayın. Neredeyse tamamında 'bilgilerin reklam ve istatistik amaçlı kullanılması' bölümü önceden onaylı oluyor.
- Özellikle Instagram'da konum paylaşmayın. Avrupa'da son zamanlarda hırsızlıkların büyük kısmı bu şekilde yapılıyor. Hırsızlar sosyal medyayı takip ederek kimin ne zaman evde olmadığını tespit ediyor.
- Amerika'daki en büyük ilişki sitelerinden 'ashleymadison' hack'lendi. Sitenin Türkiyeli kullanıcılarına şantaj yapıldı. Üye olmadan önce tekrar düşünün.
- Antivirüs programlarına tamamen güvenmeyin. Bilgisayarlardaki antivirüs programları çok standart korumalar sağlıyor. En pahalı güvenlik antivirüs programları bile küçük bir yazılımla by-pass edilebiliyor.
- Ücretsiz yazılımlar indirmeyin.

Serkan Ocak
serkan.ocak@hurriyet.com.tr

Can Yıldızlı'yı dört yıl önce, bir siber güvenlik konferansında tanımıştım. Sabancı Üniversitesi Bilgisayar Mühendisliği bölümü mezunu. 1985 doğumlu. Pentagon'un açtığı yarışta, 25 sorudan 24'üne doğru yanıt verebilen dünyadaki tek 'hacker'dı. 25'inci soruya yanıt bulabilen hâlâ yok. Google'dan, Apple'dan iş teklifleri aldı ama geri çevirdi.

Bilgi Teknolojileri Kurumu (BTK), geçen ocak ayında, 'Türkiye siber yıldızlarını arıyor' duyurusu yaptı. BTK'nın açtığı bu yarışmaya tam 26 bin kişi başvurdu. Can Yıldızlı'nın kurduğu üç ekip, 1'inci, 4'üncü ve 6'ncı oldu. Geçen hafta yarışmanın ödül töreni vardı, BTK'nın bazı yarışmacılara iş teklif edeceği söyleniyor.

Yıldızlı ve ekibi, Türkiye'deki bankaların yüzde 90'ı ile çalışıyor. Kurdukları USTA (Ulusal Siber Tehdit Ağı) sistemi ile hizmet veriyorlar. Firmaların başına gelebilecek riskleri belirleyip onlara önceden haber veriyorlar. Tespit ettikleri bilgilerden bazıları şunlar:

71 2016'da tespit edilen zararlı mobil yazılım sayısı

Saatte 96 kredi kartının bilgisi çalınıyor

- Türkiye'de şu ana kadar 25 bin kişinin kimlik fotokopi görüntüsü çalınmış durumda. Sadece geçen yıl çalınan kimlik fotokopisi görüntü sayısı 1.019. Kimlik bilgisi ile kimlik fotokopisi arasında çok fark var. Yeraltı dünyasında fotokopilerin tanesi 25 TL'ye satılıyor. Boş nüfus cüzdanı şablonlarını doldurulup satıyorlar.
- Hacker'lar, araçların kaza bilgilerinin yer aldığı TRAMER kayıtlarının tamamına ulaşabiliyor.
- Her saat 96 kredi kartı bilgisi çalınıyor. Bugüne kadar yine hacker'ların eline geçen Türkiye vatandaşlarına ait kredi kartı bilgisi, 50 bin 339. Dünyada 2 milyon kişinin kredi kartı bilgisi yeraltı dünyasında sürekli el değiştiriyor. Sahte kredi kartlarının nakde çevrilmesi için kullanılan 3 bin 32 farklı yöntem var. Kredi kartı bilgilerinin yüzde 40'ı, e-ticaret sitelerinin hack'lenmesiyle ele geçiriliyor.
- 2016'da finans şirketlerinin adları kullanılarak 1984 sahte internet sitesi adresi tespit edildi.

Yenilmezler ekibi

Yıldızlı, Türkiye'de Invictus (Yenilmez) Bilişim Güvenlik, yurtdışında da 'Prodaft' adlı şirketler kurdu. 25 kişilik bir ekiple çalışıyor. Ekip, Teknopark İstanbul'da faaliyetlerini sürdürüyor. Komşularından bazıları ASELSAN, HAVELSAN, ROKETSAN gibi savunma teknolojileri mühendislik şirketleri. Invictus ekibi, tespitlerini danışmanlık yaptıkları kurumlara bildiriyor. Saldırılara engel olmaya çalışıyor. Kimi zaman saldırganların server'larına müdahale ediyor. Fişi çekiyor. Eğer saldırı yurtdışı kaynaklı ise o ülkenin güvenlik birimlerine bildiriyor. Ekibin tüm üyeleri birer siber istihbarat analisti. Mehmet D. İnce, sızma testleri konusunda uzman. Önay M. Kıvılcım'ın görevi 'sanal devriyelik'. Mazlum Ağar, güvenlik açıklarını tarıyor. Osman Erçelik'in işi 'otomatizasyon'. Çalıntı hesapları takip eden teknolojiler geliştiriyor. Ozan Yıldırım, siber suç keşif biriminden. Grubun tek kadın üyesi Havva F. Mete ise derin ağ analisti.

Silinen tweet'leri bile buluyorlar

Can Yıldızlı'nın ortağı Koryak Uzan (ortada), dijital iz bulma konusunda uzman. Birinin sildiği tweet'leri, bazı izleri takip ederek bulabiliyor. Tweet'lerini silip silmediğini de tespit edebiliyor. Suçlarını gizlemeye çalışan hacker'ları, insanların dijital ilişki ağlarını ortaya çıkarabiliyor.

İsviçre'den bağlanıp İstanbul'daki evimi hack'ledi!

Can Yıldızlı ile İsviçre'den WhatsApp aracılığıyla görüştük. Bir hacker saldırısı deneyimlemek istedim. Birkaç saniye sonra evimdeki tüm internet çöktü. 10-15 dakika cep telefonu ve bilgisayarları kullanamadım. "İstersen bağlandığın WiFi üzerinden çalıştığın kurumun tüm internetini çökertebilirim, kısa süreliğine test edelim mi?" diye sordu ya da düşünmeden "Hayır" dedim. Yıldızlı, aynı yöntemle bir hastanenin acil servisini, askeriyeyi, elektrik santrallarını, diğer kritik kurumları hack'leyebileceğini, bu tip olayların önüne geçmek için çalıştıklarını söyledi.

Diji-tele işbirliği

Yıldızlı, son dönemde dijital dolandırıcılarla telefon dolandırıcılarının işbirliği yaptığını belirtiyor. 'Deep web' denilen, internetin yeraltı dünyasını oluşturan 'Tor'da yeni ses kayıtları ele geçirdiklerini, dolandırıcıların işlerini nasıl yaptığını göstermek için bu ses kaydını 'Tor'da pazarlama aracı olarak kullandıklarını anlatıyor. Dijital dolandırıcılar, fiziksel olarak kredi kartı çalanlarla da ortak iş yapıyor.