Türk Korsan Gruplarının Siber Terörizmle Mücadelede Etkileri

Siber Güvenlik Teknolojileri Derneği

Öncelikle şunu belirtmeliyim ki, 2002 yılından bu yana bu alanın içinde olmama rağmen ilk defa bir konferansa konuşmacı olarak katılıyorum. Daha önce birçok davet aldım açıkçası, lakin ilk defa bir konferansa katıldım. Buradaki değerli konuşmacılar ve dinleyicilere saygılarımı sunuyorum. Bunun dışında bize bu imkanı sağlayan Gazi Üniversitesi yetkililerine de şükranlarımı sunarak, bir duyuru yapmak istiyorum. Uzun yıllardan bu yana hedeflediğimiz sistemi birkaç gün sonra hayata geçireceğiz. Ülkemizi desteklemek adına Siber Güvenlik Federasyonumuz birkaç gün sonra kendini resmi olarak ilan edecektir. Bu federasyonda genel sekreter görevini üstleneceğim. Bu göreve beni layık gören herkese de buradan teşekkürlerimi sunarım. Tüm siber güvenlik derneklerimizi de bu federasyona katılıma davet ediyorum.

Türkiye de aktif olarak faaliyet gösteren Hack Grupları

Türkiye de aktif hack gruplarına değinecek olursak bunları ikiye ayırabiliriz. Bunlardan birincisi kendilerini milli temele dayandıran gruplar ve diğeri ise Türkiye 'de faaliyet gösteren anti milli gruplar şeklinde sınıflandırılabilir.

Bunları aşağıdaki gibi listeleyebiliriz;

Milli Gruplar:

- Türk Hack Team
- Cyber Warrior
- Ayyıldız Tim

Anti Milli Gruplar:

- Redhack
- CMG " CooldHackers "

Milli Gruplar

Türk Hack Team

Kendilerini milliyetçi, muhafazakar ve Atatürkçü olarak tanımlayan ve genel itibariyle Uluslararası hack gruplarından Türkiye'ye dönük yapılan hack operasyonlarına karşı koymak üzere kendini tasarlamış bir grup, Türkiye de yeterince bilinmese de Uluslararası alanda en çok bilinen gruplardan biri diyebiliriz, bundan birkaç ay önce softpedia adlı otoriter bir sitede Dünya 'nın en etkili 2. hack grubu olarak seçilmiş, 1. sırada olan grup ise sizlere çok tanıdık gelecek olan Anonymous adlı Siber Terörizm grubu. Uluslararası basına da bakıldığında bu grup Washington Post, New York Times, Le Figaro gibi birçok uluslararası basın organında makalelerine rastlamaktayız.

Ayyıldız Tim

Türkiye de çok medyatik bir grup. Herkesin bu ismi tanıyacağını düşünüyorum. Çok eski bir grup 2002 yılından bu yana aktif olarak çalışmaktalar, nitekim diğer bir grup olan Türk Hack Team 'de aynı yıl aktif olmuş bir grup, bu grup'ta kendisini Atatürkçü temele dayandırıyor. Genel itibariyle Ulusal operasyonlar düzenliyorlar lakin uluslararası operasyonları da mevcut, son dönemlerde malum terör grubuna da ciddi sosyal medya operasyonları düzenlemektedir. Genel olarak sosyal mühendislik ve brute force yöntemleri ile çalışıyorlar.

Cyber Warrior

Kendilerini muhafazakar çerçeveye dayandıran bir grup, çok etkili olmakla beraber genel olarak uluslararası alanda çalışmalar yürütmekte, kendi timi içerisinde hack yapan bir de ayrı grupları daha bulunmaktadır, bu grubu da Akıncılar olarak nitelendiriyorlar. Bu grup ise 2003 yılından bu yana aktif olarak faaliyet göstermekte, hatta gruba ait bir de resmi dernek bulunuyor. Onu da hemen sizlerle paylaşayım, Bilişim Suçlarına Karşı Mücadele Derneği.

Yukarıda yazdığım timler dışında başka timler de mevcut, lakin bazıları pasif konumda olup, bazıları ise büyük ölçekli olmadığından buraya not almadım. Ancak onların da hakkını yemek istemem. Kısaca bu şekilde değinmiş olduk.

Anti Milli Gruplar

Redhack

Redhack Adlı grup kendisini Sosyalist, Marksist temele dayandıran bir grup, içinde genel olarak bu temelde insanları barındırıyor. Türkiye'ye karşı gerçekleştirmiş oldukları ciddi güvenlik tehditleri bulunmaktadır, bunların bir kısmını devletimizin yetkili organları ve yukarıda ismi yazılı olan hack timleri sayesinde önlenmektedir, hatta daha önce gruba ait isim listelerinin milli bazı gruplar tarafından ele geçirilerek devletin yetkili organlarına verildiğini söyleyebiliriz. Zaten milli gruplar sürekli olarak yetkili birimlere bilgi aktarmaktadır. Redhack 'in scada sistemleri üzerine vermiş olduğu zararlar bulunmaktadır, ayrıca daha önce birçok bakanlık sunucularına girerek zaafiyet uğratıldığını biliyoruz. Hatta bunun ötesinde pkk'ya da lokal bilgiler sızdırdığı biliniyor, pkk ile ortak çalışarak gerçekleştirdikleri bir terör operasyonu da mevcut bununla alakalı Redhack grubundan alınan terör yanlısı hackerlar olmuştu. Bununla alakalı çok fazla konuşmamın anlamı yok. Tehdit derecesinin seviyesini anlatmam açısından kısa bir bilgi paylaşmak istedim. Anonymous tehditinin çıkmasından sonra, Redhack bu uluslararası grupla da beraber çalışmaya başladı. Bunun sonucu olarak da son dönemlerde eylemlerini o grup üzerinden yapmaya başladıkları için bulunmaları ve tespit edilmeleri oldukça zorlaşmıştır. Anonymous ile beraber Türkiye 'de ciddi bir internet trafiği oluşturarak ülkemizdeki internet trafiğini kısmi kesintilere uğrattıkları da bilinmektedir.

COLDHACKERS

CMG adlı grup pkk temelli bir grup olup, devlete ait gizli bilgilere erişim maksadıyla bazı siber terör faaliyetleri sergilemektedir, bu bağlamda daha önce askeri bilgilerin ele geçirildiğini bilmekteyiz. Tehlikeli ve bir o kadar stratejik bilgilerin zafiyet'e uğratılması noktasında terörist faaliyetler sürdürmektedirler.

Siber Ordulara Katılım Süreci

Genel olarak hack forumlarında, askeriyede olduğu gibi rütbeleme sistemi uygulanmaktadır. Bu forumlara katılım sanıldığı kadar kolay değil, bir çoğunda davetiye sistemi ile üye olunuyor, bazı forumlarda ise üyelik alımı kapalı, bu forumlarda sistem ise sene de 10 ila 15 gün kadar üye alımını açıp kapatmak şeklinde gerçekleşiyor. Bu nedenle her önüne gelenin bu forumlara kayıt olması zor. Bu forumlarda birkaç gruptan oluşan timler mevcut, birinci grup genel forum ekibi,ikinci grup hack grubu, üçüncü grup ise istihbarat grubu şeklinde oluyor. Bu timlere girebilmek için değişik şartlar bulunmaktadır. Hacker grubuna girebilmek için sistem açıkları hakkında bilgi sahibi olmanız gerekiyor. Bu da genel olarak Zone-h gibi hack tescil sitelerinde kaydı olan hackerlardan seçiliyor. İstihbarat timlerine alım ise, genel forumda çok eski üyeliği olan güvenilir insanlardan seçilirken, genel foruma alım ise konu sayısı gibi kriterler göz önünde bulundurarak seçimler yapılıyor. Türk hack gruplarına katılım süreci farklı şekillerde olabilir. Bunların dışında farklı sitelerden transfer şekliye de bu sistemlere katılım olabiliyor.

Peki bu nasıl oluyor? Örneğin bir forumda ya da bireysel olarak çalışan bir kişinin yapmış olduğu saldırılar neticesinde transfer gerçekleşiyor.

Bunların tespiti nasıl oluyor? Hack kayıtlarını tutan siteler bulunmakta bunlardan en popüleri zone-h.org adlı sitede burada yapmış olduğu hack kayıtlarını alıyorlar buradan bakılarak yapmış olunan kayıtlar kolayca tespit edilip o kişinin yeteneği tespit edilebiliyor.

Zone-h demişken bu sistemi de kısaca anlatmak isterim. Zone-h.org adlı site 2000 yılından beri aktif olan bir portal, bu portalı oluşturan moderasyon ekibi yaklaşık 10 farklı ülke mensubu merkezi İtalya olarak biliniyor. Hackerlar hackledikleri siteleri burada tescil ediyorlar, aynı zamanda sistemde Special List ve Normal List olarak 2 adet de Dünya sıralaması mevcut, bu listede çok sayıda Türk de bulunmaktadır.

Zone-h Dünya Hacker Top 20

N°	Notifier	Single def.	Mass def.	Total def.	Homepage def.	Subdir def.
1.	Hmei7	139651	154657	294308	85376	208932
2.	d3b~x	84208	76964	161172	21102	140070
3.	Index Php	78588	74359	152947	8487	144460
4.	iskorpitx	78016	393409	471425	268014	203411
5.	Sejeal	52296	53936	106232	9880	96352
6.	1923Turk	43656	228832	272488	108143	164345
7.	misafir	29191	52504	81695	11195	70500
8.	GHoST61	23687	303670	327357	175302	152055
9.	Fatal Error	23308	50875	74183	67882	6301
10.	ZoRRoKiN	23242	40929	64171	35836	28335
11.	w4l3xzy3	21809	30595	52404	1909	50495
12.	Ashiyane Digital Security Team	21280	56755	78035	24598	53437
13.	muhmademad	19904	26625	46529	8335	38194
14.	SA3D HaCk3D	19373	66672	86045	17864	68181
15.	chinafans	19126	22721	41847	189	41658
16.	HighTech	18234	34407	52641	27899	24742
17.	KaMtiEz	14875	16437	31312	10011	21301
18.	jok3r	13852	11482	25334	1452	23882
19.	BD GREY HAT HACKERS	13103	52555	65658	33208	32450
20.	HolaKo	11949	7135	19084	1064	18020

Hack faaliyetleri ve kullandıkları yöntemler

Kullandıkları hack faaliyetleri, vermek istedikleri zarara göre değişkenlik göstermektedir.

Örneğin bir sistemi erişilmez hale getirmek için genelde DDOS adlı hack yöntemini kullanmaktadırlar. Lakin sistemden düzenli bir veriye ulaşmak istiyorlarsa burada arka kapı(backdoor) devreye girmektedir, tabi bunların dışında sisteme erişim sağlayabilmek için birçok yöntem kullanılmakta sql ve xml injection, xss, upload yöntemleri, SSL sertifikasından kaynaklanan güvenlik açıkları, domain ve hosting firmalarından kaynaklanan güvenlik açıkları üzerinden erişim sağlamak, script(betik) üzerinde bulunan açıklar ya da Zer0 Day güvenlik açıkları gibi sayısız birçok güvenlik açığı kullanılarak sisteme erişim sağlanabiliyor. Siber terör grupları genel olarak ddos yöntemini kullanmakta, çünkü en düşük maliyetle en büyük zarar bu şekilde verilebilir. Anonymous adlı Siber Terör grubu da Türkiye 'de bu tarz saldırılar düzenlemektedir. Birkaç terör faaliyeti hakkında da bilgi vermek isterim:

2007 Estonya Saldırısı

Estonya 'nın, Sovyet Rusya için önemli olan savaş anıtını yıkması sonrasında, Estonya'ya başlatmış olduğu ciddi saldırılardır. Bu saldırılarda Estonya milyarlarca dolar zarara uğramasının yanı sıra internet erişimi neredeyse kullanılmaz hale gelmiştir. Estonya 1.3 milyonluk küçük bir ülke böyle bir saldırının Türkiye'ye yapıldığını düşünün ciddi sonuçlar doğuracaktır. Bu saldırı nasıl tertiplendi bundan bahsetmek gerekirse, bir bölgeye ait ip aralıkları bellidir. O aralıklarda olması muhtemel tüm iplerin tespiti de oldukça kolaydır. Şöyle düşünelim 10 milyonluk bir zombi ordusu kurmak çok zor değildir. Böyle bir ordunun stratejik kurumlara ait iplere saldırdıklarını düşünürsek sadece 4 5 tane zombi bile bir internet bağlantısının kesilmesinde etkili olabiliyor. Yapılacak özel bir yazılım ile zombileri dağıtmak da çok zor bir teknik değil, yani 10 milyonluk bir zombi ağı ile internet erişimini felç etmek çok zor bir durum değildir.

2016 Rusya’nın Türkiye saldırısı

Rusya 'ya ait savaş uçağının, Türkiye kara sınırları içerisinde sınır tacizi yaptığı gerekçesi ile vurulmasından sonra, Rusya ile aramızda başlayan kriz neticesinde Rusya 'dan ciddi anlamda saldırılar gelmiştir. Bu saldırılar genel olarak ülkeye zarar verici stratejik alanlara gerçekleştirilmiştir. Yine bu saldırıların yöntemi de ddos şeklinde olmuştur. Bu saldırılar karşısında Türk hackerlar da aynı şekilde saldırılara cevap vermesinden sonra saldırılar çok uzun sürmeden kesilmiştir.

Görüleceği üzere bir saldırıyı önlemenin en kolay yolu karşı saldırıdır. Aksi takdirde bir ddos saldırısını durdurmak neredeyse imkansızdır.

Ulusal ve Uluslararası Siber Terörist Grupları ile ne gibi mücadeleler veriliyor?

Türkiye 'de bulunan hack grupları siber terörizme karşı genel olarak karşı atak yaparak cevap vermektedir. Diğer ülkelerden gelen siber saldırılar karşısında, saldırının geldiği locasyonlara dönük saldırılar düzenlemektedir. Bunun yanı sıra siyasi ve gündeme dönük saldırılar da gerçekleştirilmektedir.

Örneğin bir Ülkede Türkiye aleyhinde gerçekleştirilen olaylar karşısında o ülkelere yönelik saldırılar gerçekleştirmektedirler. Yukarıda da bazı anti gruplardan bahsetmiştik. Bu gruplara yönelik karşı tepki koymakta oldukça zordur, zira ülkemiz sınırları içerisinde bulunan ya da yurt dışında yaşayan vatandaşlarımız tarafından gerçekleştirilmektedir. Bunlara karşı önlem alırken genel olarak gruplara ait bilgilere ulaşılarak emniyet güçlerine vermek suretiyle gerçekleştiriliyor. Türkiye de bulunanlar için işlem yapılıyor, lakin yurt dışında yaşayan gruplar için bu işlem biraz daha zorlaşıyor.

Lakin diğer ülkelerden gelen saldırılara aynı şekilde karşı saldırıyla cevap veriliyor. Yukarıda Rusya uçak krizinden sonra gerçekleşen olaydan bahsetmiştik.

Türk Korsan Gruplarından Gelen Tehditlere Verilen Tepkisel Süreç

Ülkeye yönelen siber tehdit karşısında öncelikle tehdidin niteliği önem kazanmaktadır.

Örneğin Türkiye 'ye siyasi anlamda yapılan saldırılar karşısında, genel olarak Türk hackerların tepkileri o ülkeye ait internet sitelerine index atmak suretiyle gerçekleşirken, ülkeye yapılan finans ve stratejik olarak yapılan saldırılar karşısında ise, genelde Türk Hackerlar saldırının geldiği ülkelere karşı erişim kısıtlama şeklinde saldırılar yapmaktadır. Bir örnek vermek gerekirse 2007 yılında Avusturya'nın ülkemize yönelik çirkin bir baş örtülü çıplak kadın heykeli için Türk lokumu benzetmesi şeklinde bir siyasi saldırısı olmuştu. Bunun üzerine Türk Hackerlar belki tarihin en kitlesel saldırısını başlatarak yaklaşık 100 bin Avusturya sitesine index atmıştı.

Çin, Abd, Rusya Ve İsrail Siber Güvenlik Anlamında Neler Yapıyor?

Tabi ki tam anlamıyla bilmek mümkün değil, lakin bunlar kulağımıza gelen bazı bilgiler,

En iyi stratejiyi ABD 'nin kurguladığını söyleyebilirim. ABD genelde özel sektördeki güvenlik firmalarını fonlayarak sistemi kurmaya çalışıyor. ABD başkanı 1 yıl kadar önce Çin 'i uyararak, Çin 'den gelen siber saldırılar sonrasında bunun bir savaş sebebi sayılabileceğine değinmişti. Bu nedenle bu tür saldırıların gizlilik zemininde olması gerektiğini düşünüyorum.

Hackerlar savunmayı da, karşı saldırı olarak yapmaktadır. Bu hususa değindikten sonra ABD 'nin stratejisi de tam bunun üstüne kurgulanmış. Bir noktaya gelmiş firmalar ya da ihtiyaç duyulan siber alanlarda özel firmaları fonlayarak ciddi bir siber güvenlik ağı kurmaktadırlar. Tabi ki bu ağını ihtiyaç duyduğu anda devreye sokmaktadır.

Şimdi birkaç örnek daha vermek istiyorum.

Deep Web duymayanınız yoktur diye düşünüyorum. Deep Web 'de uyuşturucu ticaretinden, insan tacirliğine, kiralık katilden, çocuk pornosunun en üst seviyelerde döndüğü derin bir web diye nitelendirebilirim. Bu ağ üzerine farklı bir tarayıcı üzerinden erişim sağlanıyor. Şimdi akla gelen şu bu tarayıcı arkasında kim var, tabi ki de NSA, bütün kirli bilgiyi elinde tutuyor. Lakin ihtiyaç duyduğu anda devreye sokuyor. Bunun dışında off shore datacenterlar bulunuyor bunların çoğu da NSA tarafından fonlanmaktadır, bu sayede kirli internet trafiğini elinde tutuyor. Bir de Bitcoin adındak, para birimi var bu da kirli para trafiğinin kontrol altına alınmaması için tasarlanmış çok akılcı dijital para, bunun arkasında da NSA izlerine rastlamak mümkün, anlayacağınız ABD bu işi tam olması gerektiği gibi yapıyor. Bunun dışında ülke içinde fonladığı uluslar arası platformlara değinmedik bile.

Çin adeta kapalı bir kutu, daha önce İsrail 'in Demir Kubbe adı verdiği bombaları havadayken vuran sistemi çalmasıyla adını duyanlarınız olmuştur. Yani İsrail'e ait bir sistemi hackerları sayesinde çalmıştır.

Bunun dışında NSA 'in daha önce Lenova model bilgisayarları yasakladığını biliyor muydunuz?

Bilgisayarlara Superfish adı verdikleri özel bir izleme sistemi olduğunu Lenova'nın bizzat kabul ettiğini ve NSA 'in öncesinde Lenova bilgisayarları yasakladığını biliyor muydunuz?

Hatta NSA de ortaya çıkan bilgi sızdırma skandalının da LENOVA üzerinden yapıldığını destekleyen birçok da haber çıkmıştı. Yani düşünün teknik bir cihaz üzerinden bile bir bilgi operasyonu yapılabilmekte, bu sadece bir bilgisayarla da bitmemekte olup, bir flash bellek üzerinden bile veri transferi yapılabilmesi mümkündür. Bunların hepsi bir siber güvenlik stratejisidir, fakat siber güvenlik stratejilerinin çok gizli oluşturulması bir gerekliliktir.

Zira uluslararası alanda hedef haline gelebilirsiniz.

İsrail'in bu işi daha çok güvenlik duvarları üzerinden gerçekleştirdiği bilinmektedir. Siber güvenlik ile ilgili cihazlar üzerinden ciddi bir siber güvenlik stratejisi oluşturduğunu düşünmekteyiz.

Rusya aslında en tehlikeli ülkelerden biri olarak nitelendirilebilir. Rusya bir zamanlar Türkiye'de bulunan Hackerları adeta taşeron olarak kullanıyordu.

Peki nasıl yapılıyordu? Birçok kart bilgisi Türk hackerlar üzerinden parça başı olarak Rus hackerlara satılıyor. Rus hackerlar da bu kart bilgilerini kullanarak çekimler yapıyordu, hatta bununla alakalı Türkiye 'de bir hacker operasyonu yapılmıştı. Ruslar özellikle zararlı yazılımlar konusunda ciddi bir bilgiye sahip, Türk Hackerlara sorulduğunda bile en tehlikeli hackerlar olarak Rus hackerlar nitelendirilir. Bir çoğu illegal olarak nitelendirebileceğimiz dolandırıcılık faaliyetlerinin içinde yer alıyorlar. Rusya 'da bir siber ordu kurmaya bile gereklilik olduğunu düşünmüyorum.

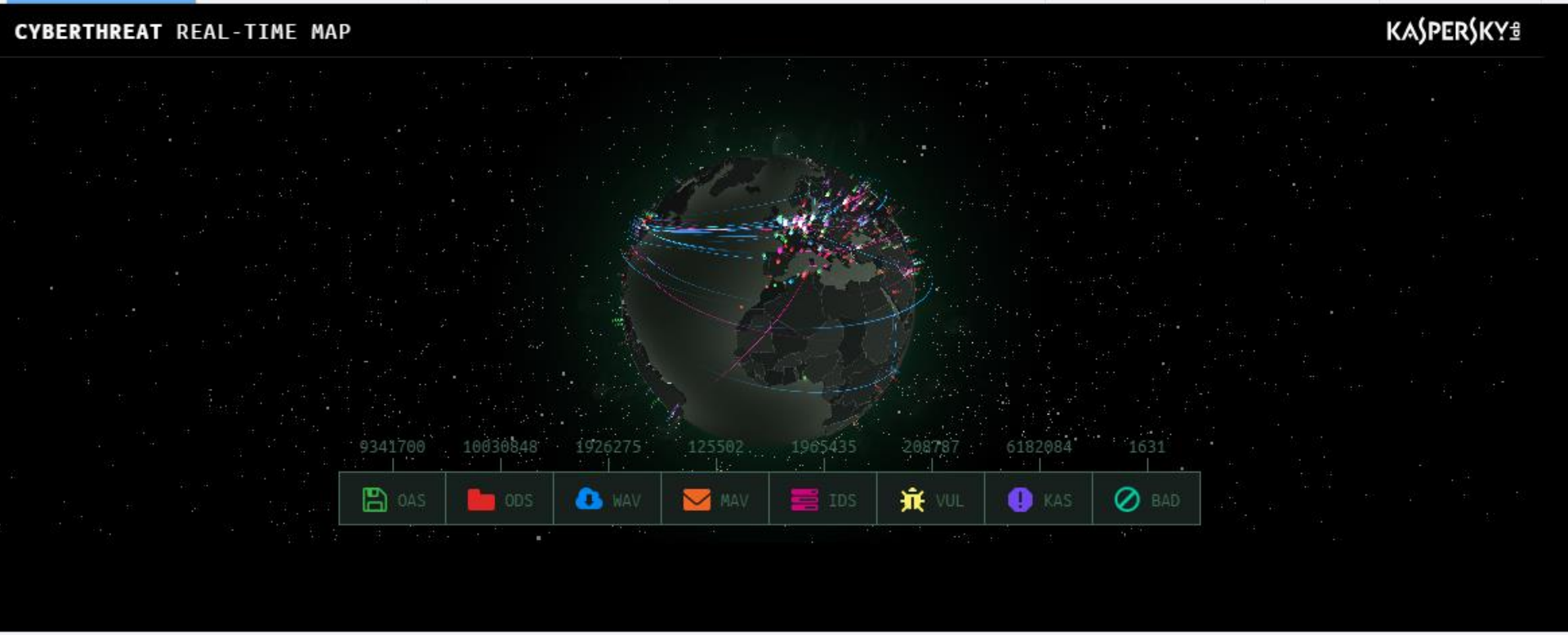
Arjantin'den bize örnek olması adına bahsetmek istiyorum. Arjantin de, bu konu üzerine oldukça iyi, birçok üst düzey hacker geçtiğimiz yıllarda Arjantin'den oldukça söz ettirmişti. Zannedersem Yetkili organlar da bunun farkına varmış ki Arjantin'de 2008 yılı sonrası adeta devrim yapılmış. Bununla alakalı liselerin bile kurulduğunu duymuştum. Hatta bizim tanıdığımız birkaç arkadaşımızın da orada olduğunu bizzat öğrendim. Bu arkadaşlara sorduğumda bu liselerden yetişen gençlerin ciddi anlamda donanım bilgisi sahibi olduğunu, hatta son zamanlarda birçok güvenlik cihazının ABD üzerinden Dünyaya pazarlandığını söylüyorlar.

Kısaca özetleyecek olursak, bir ülkenin siber saldırılardan korunmasında en büyük etken, o ülkenin caydırıcılığıdır. Türk Hackerlar en başından beri bu caydırıcılıkta üst düzey rol üstlendi. Bu nedenle de bazı ülkelerin hedefi olmadık.

Siber Güvenlik Teknolojileri Derneği

BİZE ULAŞIN

0282 654 4399 bilgi@sgt.org.tr



İlginiz için teşekkür ederim.

Vahap EREN
Dernek Başkanı
Siber Güvenlik Teknolojileri

Katkılarından dolayı A.Ufuk Yavuzer'e teşekkürler.