# Black Hat Macerası

written by Mert SARICA | 9 August 2015

1997 yılından bu yana, dünyadan bilgi ve bilişim güvenliği uzmanlarının, hackerların, istihbarat elemanlarının akın ettiği dünyaca ünlü Black Hat konferansına Ağustos ayında katılma ve eğitim alma şansını yakaladım. Şansını yakaladım diyorum çünkü bu konferansa katılmak ve eğitim almak için ya çok paranızın olması gerekiyor (uçak bileti, otel konaklama ve Black Hat bileti ~10.000 TL) ya da sizi bu konuda destekleyen sponsorlarınızın, bu konferansa katılmanız ve eğitim almanız gerektiğine inanan IBTech ve Finansbank gibi vizyoner işverenlerinizin olması gerekiyor. Ben de herşeyden önce bu konferansa katılmama ve eğitim almama destek olan, yardımlarını esirgemeyen herkese teşekkür etmek istiyorum.

Black Hat günlüğümün sayfalarını aralamadan önce 15 yıl aradan sonra bu defa farklı bir eyaletini ziyaret ettiğim Amerika'nın Nevada eyaletinin Las Vegas kenti hakkında kısaca gözlemlerime yer vermek istiyorum.

Birincisi insanların gerçekten mutlu, yardımsever, cana yakın ve kibar olduğunu söyleyebilirim. Özgürlükler ülkesi olan Amerika'da insanların kendi halinde olduklarını görebiliyorsunuz. Elinde bira kutusuyla gezen de var, ponpon kız kıyafetiyle sokağa çıkıp turistlerle fotoğraf çektirip bu işten para kazanan da var, üst geçitlerin sağında solunda dilenmeyen ancak elinde döviz ile yardım isteyen evsizler de var. Hatta bir evsizin dövizinde, "evsizim çünkü eski eşimin daha iyi bir avukatı vardı" gibi esprili yazılara rastlayabiliyorsunuz. İşin en güzel yanı herkes kendi dünyasında yaşıyor. Kimsenin kimseyle bir derdi, sorunu bulunmuyor. Yolda, toplu taşımada giderken kimse kimseyi rahatsız etmiyor, mahalle baskısına veya tacize maruz kalmıyorlar. Kurallara uyuyorlar, düzenliler, çevreye saygılılar ve siz de bunlara aç bir ülkeden geldiğiniz için hemen bu kurallara ve düzene memnuniyetle uyum sağlıyorsunuz.

İnsanlar sıraya girmesi gerektiğini biliyorlar. Sırada işleri uzun sürerse arkasında sıra bekleyenlere dönüp özür diliyorlar. Karşıdan karşıya geçecekseniz adımızını yola attığınız anda yoldan geçen araç duruyor ve sizin karşıya geçmenizi bekliyor. Beş şeritli yollarda oldukça lüks, spor araçlar göze çarpıyor ve hiç biri ne slalom yapıyor ne de birbirleriyle yarışıp, insanların canını tehlikeye atıyor. Yolda yürürken, bir restorana veya bir dükkana girdiğinizde, merhaba, nasılsınız ?, keyifler yerinde mi ? Vegas'ı

beğendiniz mi ? neredensiniz ? gibi sorular soran ve sizle sohbet eden cana yakın insanlarla karşılaşıyorsunuz. Türkiye'denim dediğinizde müslüman olduğunuz için size farklı davranmıyorlar. Yabancılar müslümanları ve Türkler'i sevmezler sözünün ön yargıdan ibaret olduğunu, Vegas için geçerli olmadığını hemen anlayabiliyorsunuz. Kendi fotoğrafınızı çekmeye çalıştığınızda yanınızdan geçen biri fotoğrafınızı isterseniz çekebilirim diye yardım eli uzatabiliyor.

Yaşlı istihdamına da gerçekten önem veriyorlar. Black Hat'e kayıt olurken biletinizi ve çantanızı size verenlerin yaş ortalamasının 50-60 arası olduğunu görebiliyorsunuz. Çok sayıda kadın otobüs şoförü var ve onların da yaş ortalamaları kimi zaman 50 ile 60 yaş arasında olabiliyor.

Kıssadan hisse, Avrupa ülkelerinde de olduğu gibi özgürlükler ülkesindeki bu yaşama ve medeniyet seviyesine, kıraathane sayısının kütüphane sayısının 285 katı olduğu bir ülkede erişilmesinin epey zaman alacağı anlaşılıyor.

Black Hat konferasına gelecek olursam, eğitimlere ve sunumlara katılımın oldukça yüksek olduğunu söyleyebilirim. Zaten etkinlik yeri için neden Mandalay Bay otelinin dev kongre merkezinin seçildiğini etkinlik tarihi gelince anlayabiliyorsunuz. Black Hat konferansı toplamda 6 gün sürüyor. İlk 4 gün boyunca eğitimler düzenleniyor, geri kalan iki günde ise neredeyse bir sene boyunca yapılan araştırmaların sunulduğu can alıcı sunumlara (Black Hat Briefings) ve güvenlik araçlarının tanıtıldığı (Black Hat Arsenal) tanıtım sunumlarına yer veriliyor.

Black Hat'te bu sene toplamda 63 tane eğitim verildi ve ben de 1-2 Ağustos tarihlerinde, Saumil Shah tarafından verilen Exploit Laboratory: Black Belt adındaki eğitimi aldım. Eğitimin temeli, internet tarayıcısı istismarına dayanıyordu. Eğitim esnasında use after free zafiyetlerinin ROP (return oriented programming) ve heap spray yöntemleri ile, Windows'un güvenlik kontrollerinin (DEP gibi) nasıl aşılarak istismar edilebileceğini gösterildi. Sınıfın mevcudu 30 kişiydi ve daha önce bu eğitmenden eğitim alanların bu eğitimi tercih ediyor olmaları da zaten eğitmenin başarılı olduğunu kanıtlar nitelikteydi.


Konferans ve eğitim esnasında güvenlik uzmanı dediğin biraz paranoyaktır örneklerine de rastlamadım değil :) Misal eğitim esnasında tuvalete giden birinin bilgisayarını kapatıp, çantasına koyup, yanına aldığını da gördüm, yaka kartında soyadını gizleyen kişileri de gördüm. (Mert S. gibi)

Black Hat'in açılış konuşmasının yapıldığı ilk günde, 1000 kişilik olduğunu düşündüğüm salonda Black Hat ve Defcon konferanslarının organizatörü Jeff Moss sözü aldı ve bu sene, katılımcı sayısının en yüksek olduğu Black Hat konferansını düzenlediklerini belirtti.

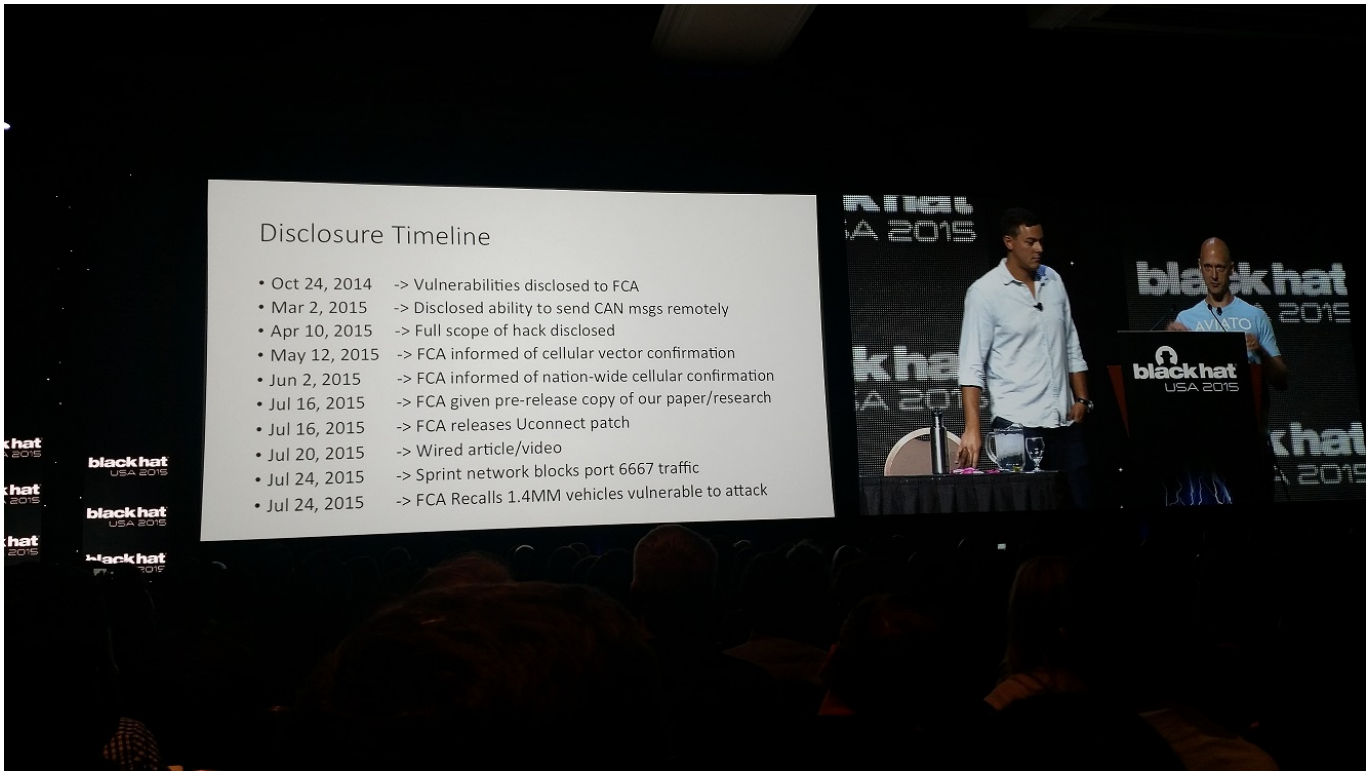

Verilen Black Hat tanıtım ve sunum kitapçığında kendime hangi sunumlara gireceğimle ilgili bir plan çıkarttım. Paralelde ilgimi çeken 3-4 sunumun olması ve aralarından sadece bir tanesini seçmek zorunda olmam beni oldukça zorladı.


Back Doors and Front Doors Breaking the Unbreakable System
by James Denaro + Matthew Green
South Seas ABE
Big Game Hunting: The Peculiarities of Nation-State Malware Research
by Morgan Marquis-Boire + Marion Marschalek + Claudio Guarnieri
Mandalay Bay GH
Distributing the Reconstruction of High-Level Intermediate Representation for Large Scale Malware Analysis
by Rodrigo Branco + Gabriel Negreira Barbosa + Alexander Matrosov + Eugene Rodionov
South Seas GH
Remote Exploitation of an Unaltered Passenger Vehicle
by Charlie Miller + Chris Valasek
Mandalay Bay EF
Stagefright: Scary Code in the Heart of Android
by Joshua Drake
Mandalay Bay BCD
Stranger Danger! What is the Risk from 3rd Party Libraries?
by Kymberlee Price + Jake Kouns
Switches Get Stitches
by Colin Cassidy + Robert Lee + Eireann Leverett
Targeted Takedowns: Minimizing Collateral Damage Using Passive DNS
by Paul Vixie
WSUSpect - Compromising the Windows Enterprise via Windows Update
by Paul Stone + Alex Chapman
#BHUSA

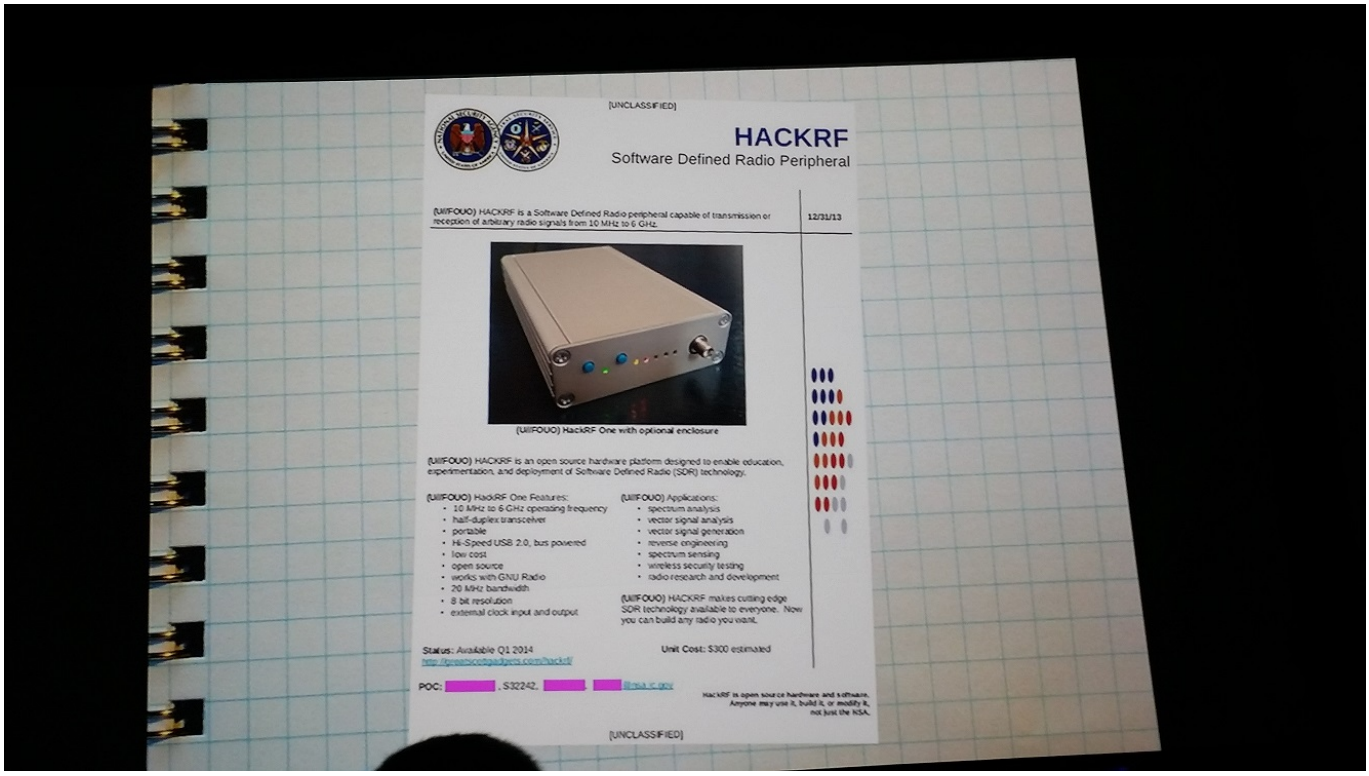

black hat
WEDNESDAY
BRIEFINGS
Wednesday, August 5 • 09:00-18:00
Keynote
09:00-10:00
The Lifecycle of a Revolution
by Jennifer Granick
Mandalay Bay Ballroom
Briefings
10:20-11:10
Android Security State of the Union
by Adrian Ludwig
Mandalay Bay GH
Bring Back the Honeypots...
by Haroon Meer + Marco Slaviero
South Seas ABE
How to Hack Government: Technologists as Policy Makers
by Ashkan Soltani + Terrell McSweeny
Lagoon K
Internet Plumbing for Security Professionals:
The State of BGP Security
by Wim Remes
Mandalay Bay BCD
Server-Side Template Injection: RCE for the Modern
Web App
by James Kettle
Jasmine Ballroom
Spread Spectrum Satcom Hacking: Attacking the
GlobalStar Simplex Data Service
by Colby Moore
South Seas GH
Unicorn: Next Generation CPU Emulator Framework
by Nguyen Anh Quynh + Hoang-Vu Dang
South Seas IJ
Why Security Data Science Matters and How It's Different:
Pitfalls and Promises of Data Science Based Breach
Detection and Threat Intelligence
by Joshua Saxe

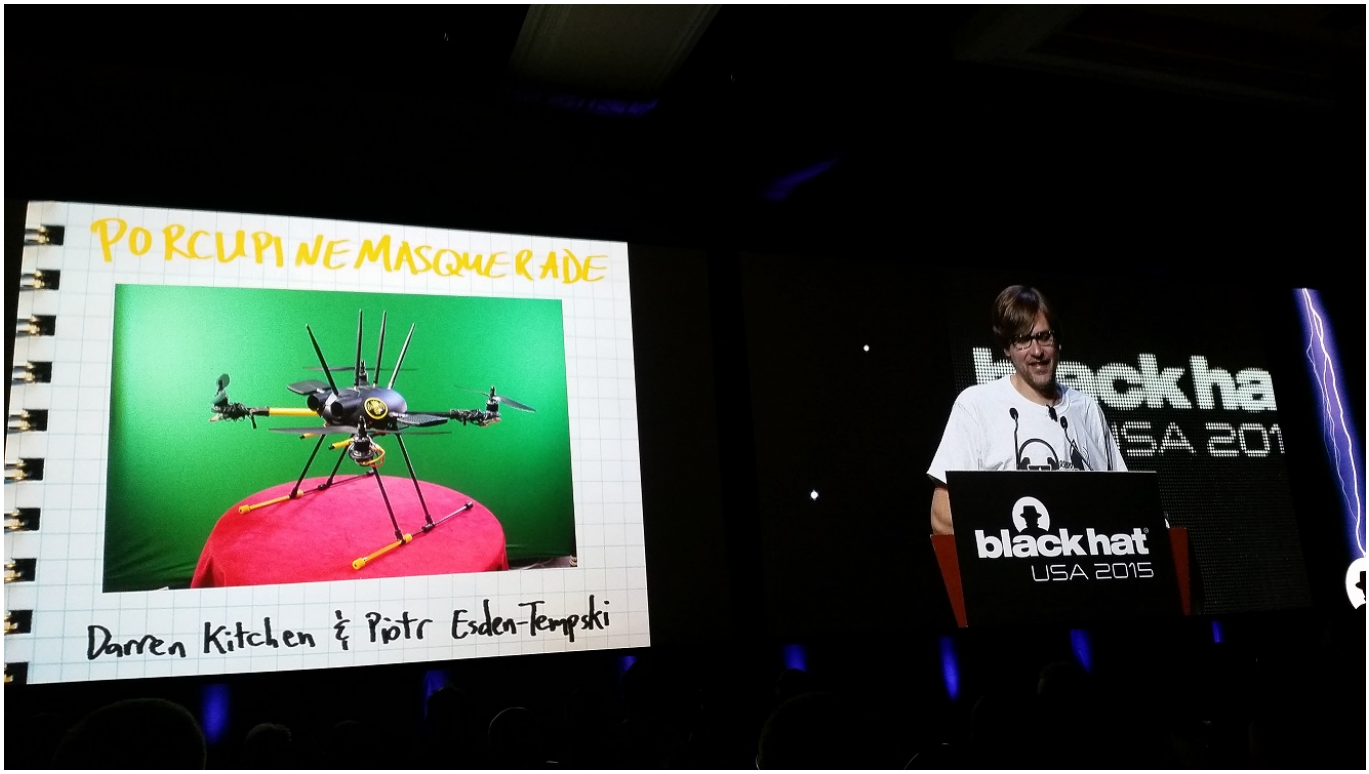
Katıldıklarım arasında en çok beğendiğim sunumlar; Charlie Miller ve Chris Valasek'in sunduğu Remote Exploitation of an Unaltered Passenger Vehicle, Michael Ossman'ın The NSA Playset sunumu, Sean Metcalf'in Red vs Blue: Modern Active Directory Attacks Detection and Protection sunumu ile Eric Evenchick ve Mark Baseggio'nın sunduğu Breaking Access Controls with BLEKey sunumları oldu.

Charlie Miller ile Chris Valasek'in yaptığı sunum oldukça keyifliydi. Sunum esnasında, imzalanmamış bir donanım yazılımı (firmware) sayesinde uzaktan bir arabayı nasıl hackleyebileceklerini oldukça renkli bir şekilde sundular. 1-2 sene arası süren bu zahmetli güvenlik araştırmalarının karşılığını, 1000 kişi olduğunu düşündüğüm hınca hınç dolu olan salonda müthiş bir alkış kopunca aldıklarını düşünüyorum. Sunum başlamadan önce yanında boş yer olanlar ellerini kaldırsınlar diye anons yapılması da sunuma olan ilginin bir göstergesiydi. Sunum sonunda Charlie Miller attığı bir tweet ile kendi sunumları esnasında oldukça değerli başka sunumların da paralelde gerçekleştiğini söyleyerek, sunumlarına katılanlara da teşekkür etmeyi ihmal etmediler. Yabancıların bu mütevaziliğini her zaman takdir etmişimdir.

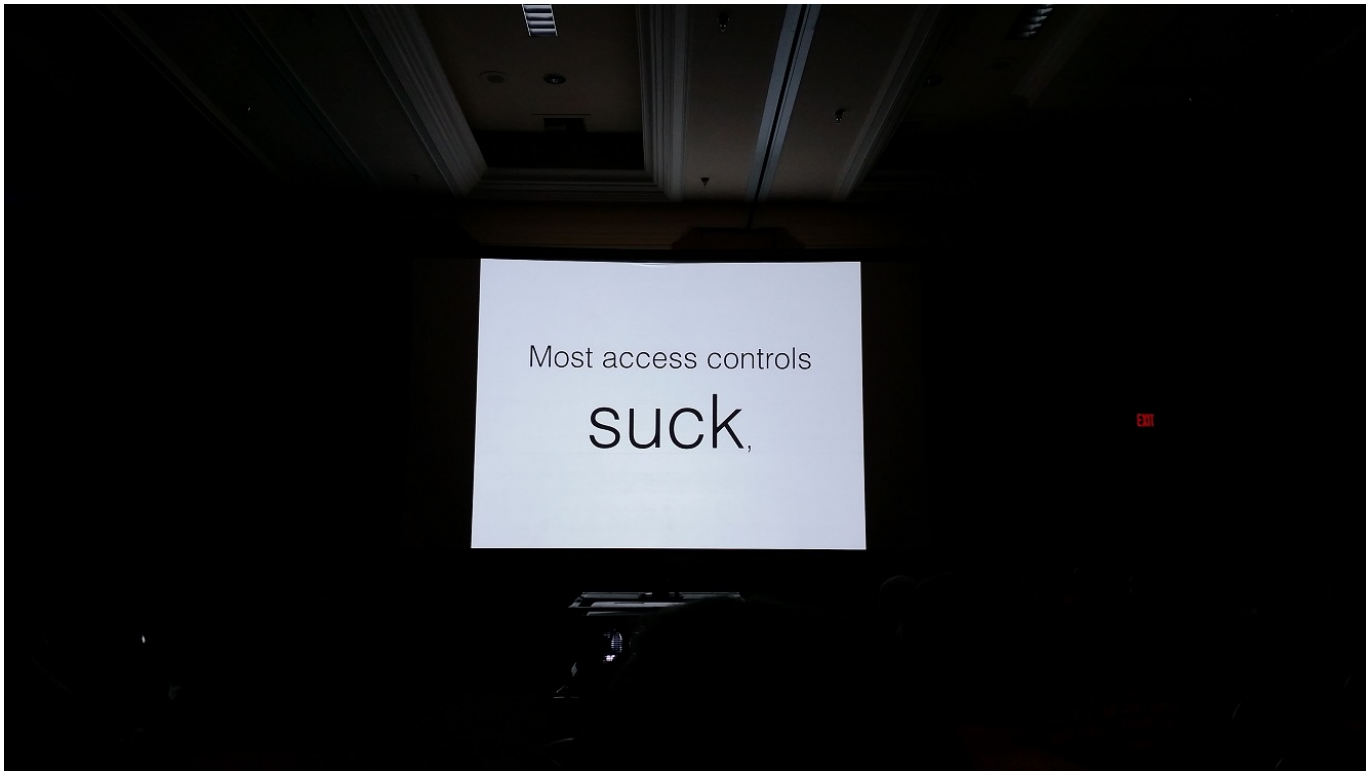



Hackrf One, (ben de sonunda bir tane alabildim :)) Ubertooth One ve bunun gibi birçok değerli donanıma imza atan Michael Ossman'ın sunumu da benim için oldukça değerliydi. NSA Playset adını verdiği sunumda, Edward Snowden tarafından sızdırılan NSA'in gizli belgelerinden esinlenerek güvenlik araştırmacıları tarafından hazırlanan donanımların tanıtımına kısaca yer verdi.



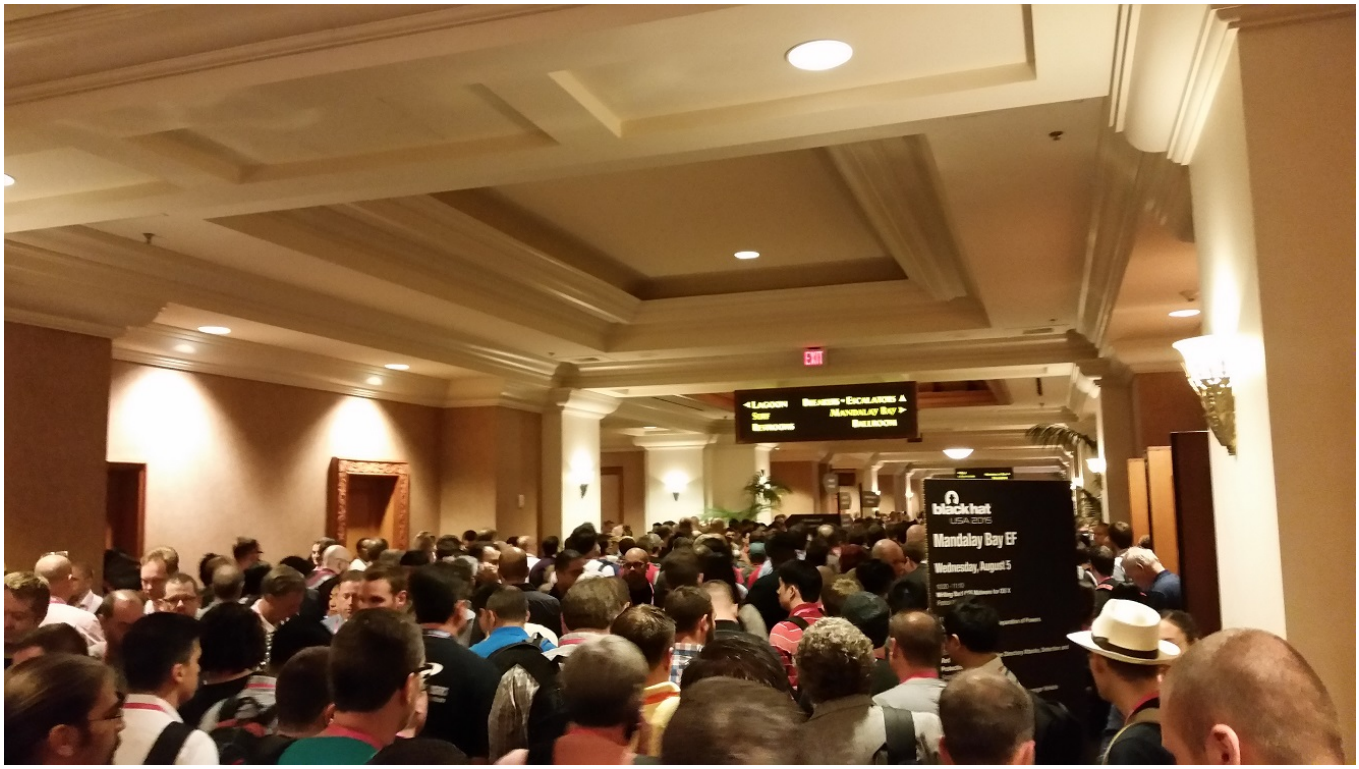




Eric Evenchick ve Mark Baseggio'nun RFID kapı kartları üzerine yapmış oldukları çalışma esnasında, kart kopyalamak için 10$'a mal ettikleri BLEKey cihazını da ilk 200 kişiye ücretsiz olarak dağıtmaları beni oldukça mutlu etti. (ben de bir tane kaptım :))


Most access controls
suck.
EXIT


POCKET GUIDE
black hat
USA 2015
AUGUST 1 - 6, 2015 WWW.BLACKHAT.COM
SUSTAINING PARTNERS
FireEye
FORTINET
iboss
LogRhythm
Microsoft

Her ne kadar katılamamış olsam da, bu sunumlar dışında geçen sene Gökhan ALKAN ve Bahtiyar BİRCAN'ın, bu sene ise sadece Bahtiyar BİRCAN'ın Black Hat Arsenal'de bizleri Heybe sunumu ile gururlandırdıklarını da unutmamak gerekiyor.
Bu arada sunumlar demişken, Black Hat'te bir sunumdan diğer bir sunuma yetişmek için adeta depar atmanız gerekebiliyor çünkü çoğunlukla koridorlar, metrobüslere benzer bir hal alabiliyor :)




Sunumlar dışında güvenlik dünyasının dev markalarının yer aldığı standları da (Business Hall) gezme imkanım oldu ve bunlar arasında dikkatimi en çok çeken FBI'ın standı oldu. FBI'ın standına gidip tweet atmak için broşürlerine bir göz atmak istediğimde, bir hanım ablamızın (artık ajan mıdır bilinmez :)), Amerikan vatandaşı mısın ? diye sormadan önce FBI'a katılmak ister misin ?, yetenekli misin diye laf atması da beni şaşırtmadı değil. Bu standı görünce insan, "eee adamlar nereden eleman almaları gerektiğini gayet iyi biliyorlar, sonuçta koskoca FBI" demeden geçemiyor.


Sonuç olarak Black Hat konferansı benim için gerçeğe dönüşen bir hayal oldu. Sunumlarıyla ve eğitimiyle oldukça verim aldığımı söyleyebilirim. Gönül ister

her firma, her sene güvenlik uzmanlarını Black Hat, Defcon gibi konferanslara göndersin, orada eğitim aldırsın, hem ülkeye hem de güvenlik sektörüne katkısı olsun ancak sığ vizyon, bol bol mesai yapsın kendini geliştirecek zamanı olmasın, ne iş olsa yapsın ama bir alanda uzmanlaşmasın, ekonomi de zaten kötü, maaş verdiğimize dua etsin eğitim falan istemesin zihniyeti ile önümüzdeki 5 yıl içinde bu sayının ne kadar artacağını hep birlikte göreceğiz.

Şartların, imkanların ve bilgiye ulaşmanın sınırlı olduğu ülkemizde, Charlie Miller ile Chris Valasek'in çalışması gibi güvenlik araştırmalarına yer verilmesi pek kolay olmuyor dolayısıyla Black Hat ve Defcon gibi konferanslarda bu tür can alıcı sunumlar yapan Türkler'e pek rastlamıyoruz. Umuyorum ki ülkemizde siber güvenliğe verilen önem ile bu tür araştırmalara verilen destek ve teşvik de artacak ve yakın gelecekte Black Hat ve Defcon gibi dünyaca ünlü konferanslarda bizleri gururlandıran sunumları görüyor olacağız.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Black Hat sunum dosyalarına erişmek için bu sayfayı ziyaret edebilirsiniz.