

# Black Hat USA 2016

written by Mert SARICA | 8 August 2016

İlk defa geçtiğimiz yıl katılma fırsatını yakaladığım dünyaca ünlü Black Hat güvenlik konferansına, NormShield firması sayesinde bu sene tekrar katılacağımı büyük bir mutlulukla geçtiğimiz ay sizlerle paylaşmıştım. Konferans ve öncesinde aldığım kısa notları, 12 saatlik dönüş yolunda sizler için derleyerek daha önce olduğu gibi merak edenler için yazıya dökmeye karar verdim.

Benden kimseye zarar gelmeyeceğini üçüncü defada artık anlamış olsalar gerek ki, bu defa ABD'ye girişim Intel Security Focus Güvenlik Konferansı başlıklı blog yazımda yaşadıklarımın aksine oldukça rahat oldu. 20 Temmuz itibariyle Los Angeles şehrinde başlayan ABD tatilim, 30 Temmuz itibariyle yerini Las Vegas şehrinde gerçekleşen Black Hat güvenlik etkinliğine bıraktı. Takip edemeyenleriniz için, Black Hat USA 2016 güvenlik etkinliği, bu sene 30 Temmuz – 4 Ağustos tarihlerinde gerçekleştirildi.

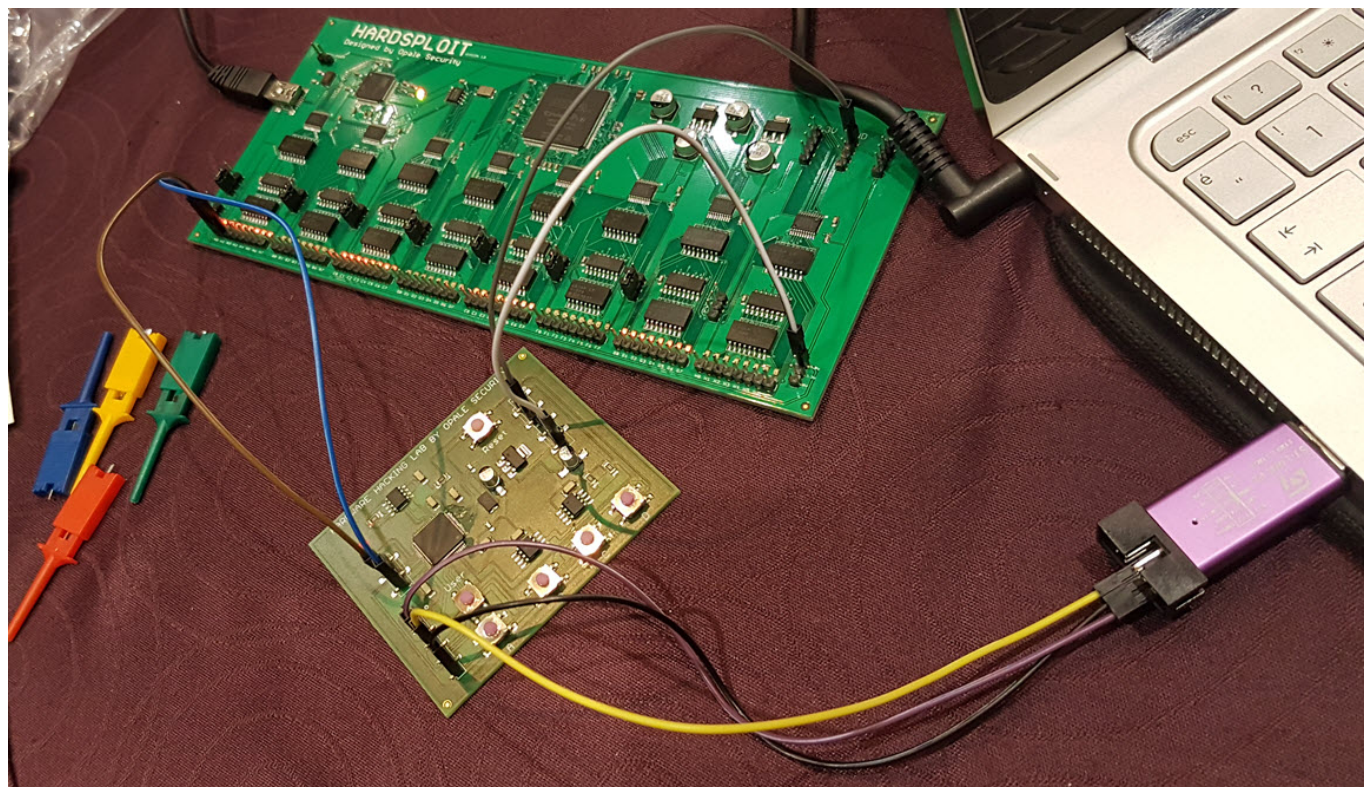


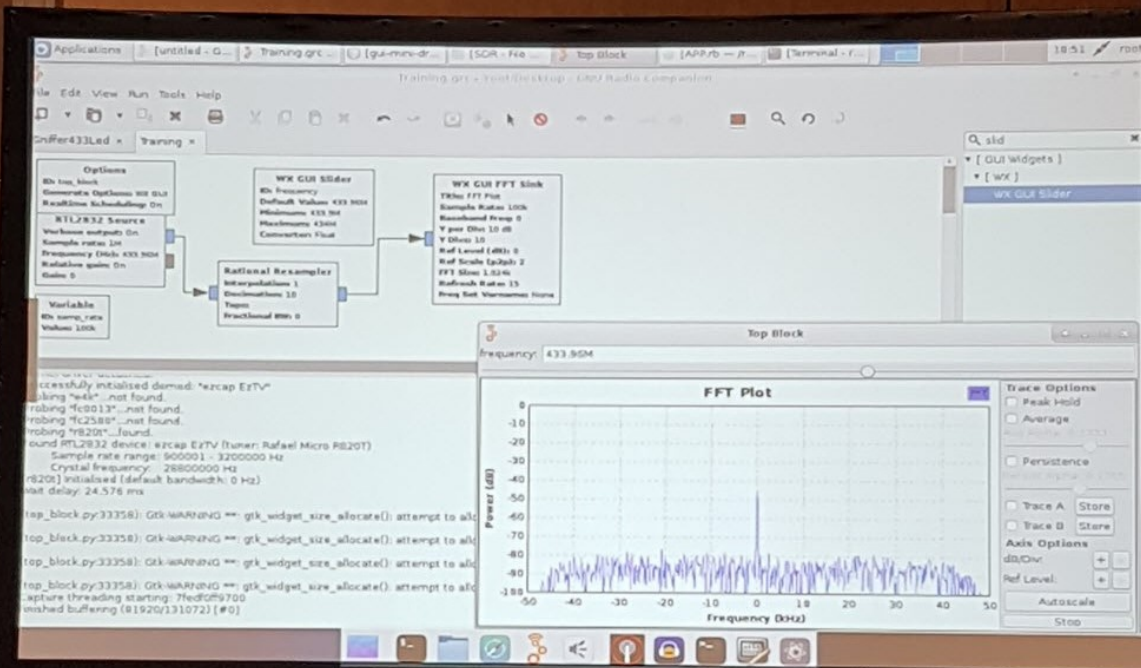
3 ve 4 Ağustos tarihlerinde yapılan sunumlar öncesindeki 4 günde, geçtiğimiz senelerde olduğu gibi birbirinden güzel 70'e yakın güvenlik eğitimi verildi. Ben de, değerli yöneticilerim ve işverenim IBTech sayesinde donanım güvenliği

üzerine yoğunlaşan iki günlük Hardware Hacking With Hardsploit Framework eğitimine katılabildim.

Geçtiğimiz aylarda işim gereği elektronik ATM kasa kilidi için sızma testi gerçekleştirmiş bir güvenlik uzmanı olarak, bu eğitimin benim için oldukça verimli geçtiğini ve ufkumu açtığını söyleyebilirim.

Opale Security firması tarafından verilen bu eğitime farklı ülkelerden (Tayvan, Kore, Brezilya, Fransa, Avusturalya), farklı profillerde (yazılımcı, sızma testi uzmanı) katılan yaklaşık 25 kişi vardı. Özellikle Amerikan Hava Kuvvetleri'nden üç kişinin katılması ve bazı katılımcıların eğitimin kendini tanıtmada diğer katılımcılar ile sadece isimlerini paylaşması (Acaba neden? :)) da dikkatimden kaçmadı. Eğitimin ilk günü, Hardsploit aygıtı ile SPI ve I2C belleklerden bilgi toplama (dump), SWD bağlantı noktasından donanım yazılımını (firmware) elde etme (dump) gibi uygulamalar gerçekleştirildi. Eğitimin ikinci gününde ise öğleden önce GNU Radio ve RTL2832U dijital tv alıcısı ile neler yapılabileceği gösterildi. Öğleden sonra ise 1.5 günde öğrenilen bilgilerin pekiştirildiği oldukça keyifli bir çalışma gerçekleştirildi. Katılımcılardan takımlar oluşturuldu ve daha sonra eğitmenler tarafından özel olarak oluşturulmuş quadcopterler (drone) takımlara dağıtıldı. Her bir takımdan drone'a üzerinde bulunan bağlantı noktaları üzerinden cihaza bağlanmaları, donanım yazılımını indirmeleri (dump), zafiyet tespit etmeleri ve diğer ekiplerin mevcut zafiyeti istismar etmesinden önce dronelerindeki bu zafiyeti gidermeleri istendi. Bunlara ilave olarak ayrıca her ekibe dağıtılan ve drone'a komut göndermek için kullanılan vericinin Hardsploit ile incelenmesi ve ardından eğitmenlerin sahip olduğu drone'a komut göndererek (belli periyotlarda eğitmenler kendi dronelerına sinyal göndererek bunu elde etmemizi sağladılar) havalandırmaları istendi. Kısa sürede son derece yoğun geçen bu eğitimden oldukça memnun kaldığımı söyleyebilirim.





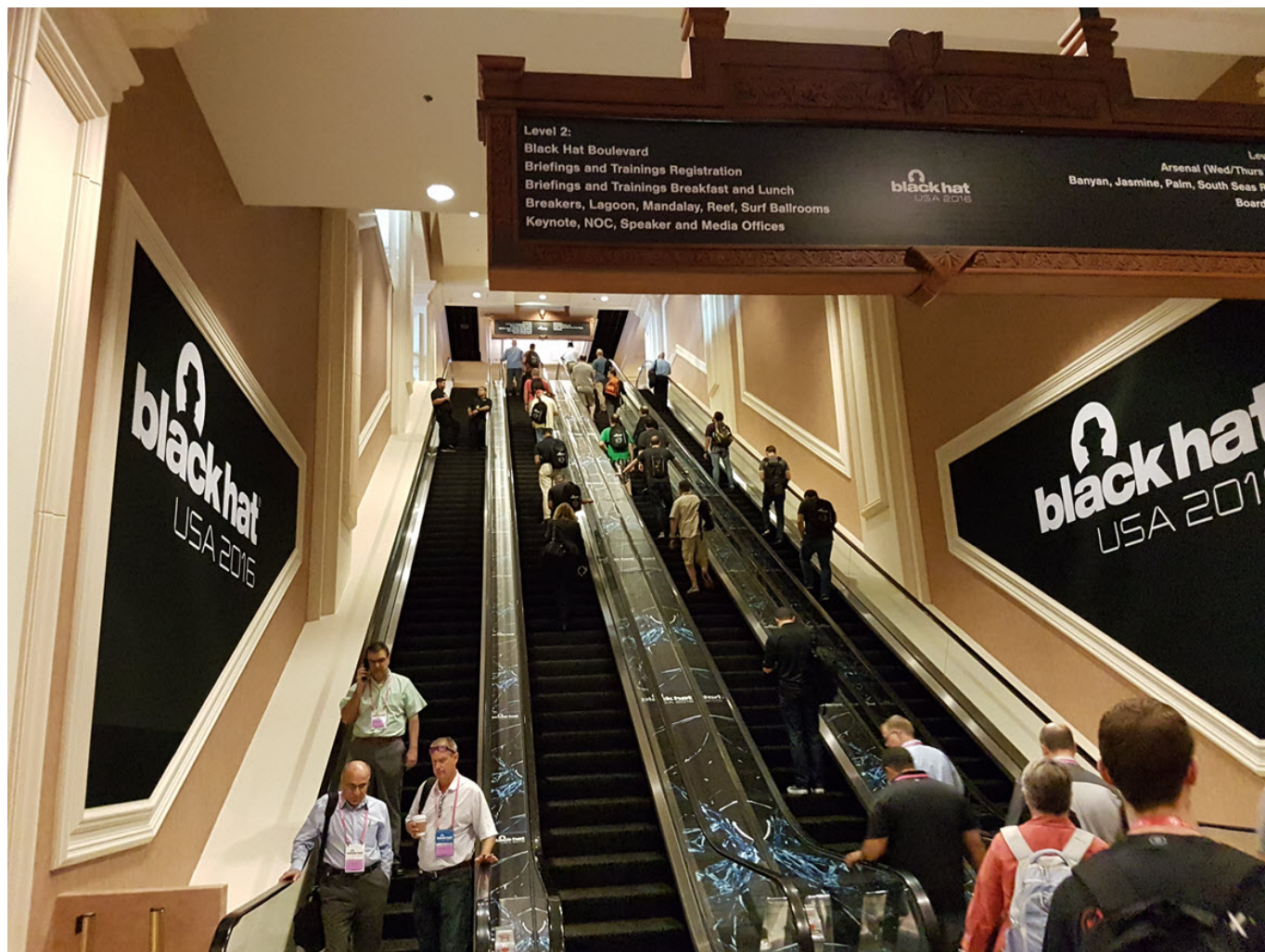




Black Hat Konferansı, geleneksel olarak konferansın kurucusu olan Jeff Moss'un açılış konuşması ile başladı. Yaklaşık 8 dakika boyunca konuştuktan sonra sözü Dan Kaminsky'e verdi. Jeff Moss konuşmasında bazı istatistiklere de yer verdi. İlk olarak Black Hat USA 2016'ya tarihi bir katılım olduğunu ve açılış konuşmasında salonda yaklaşık 6400 kişi olduğunu açıkladı! Ardından da 194 öğrenciye burs verdiklerini belirtti. (Açılış konuşmasını merak edenler, aşağıda onlar için kayıt ettiğim videoyu izleyebilirler.)



Geçtiğimiz sene olduğu gibi yine paralelde birbirinden ilgi çekici sunumlar olduğu için hangisine katılacağıma karar vermekte oldukça zorlandım. Sunum sayfasındaki kategori bazlı filtreden faydalanarak “Tersine Mühendislik” ve “Zararlı Yazılım” konularını işleyen sunumlara katılmaya gayret ettim. İkinci gün katıldığım sunumların ilk günkü sunumlara kıyasla benim için daha tatminkar olduğunu söyleyebilirim. Katılım oldukça yüksek olduğu için yine bir sunumdan diğerine gitmek için metrobüs kalabalığını aratmayan bir kalabalığın arasından yolumu bulmaya çalıştım. Bazı sunumlarda işitme engelli katılımcılar için işaret dili ile anlatım yapılmasını da çok takdir ettim.





Briefings

13:50-14:40



**Adaptive Kernel Live Patching: An Open Collaborative Effort to Ameliorate Android N-Day Root Exploits**

by Yulong Zhang + Tao Wei

Jasmine Ballroom



**CANSPY: A Platform for Auditing CAN Devices**

by Jonathan-Christofer Demay + Arnaud Lebrun

South Seas CDF



**Certificate Bypass: Hiding and Executing Malware from a Digitally Signed Executable**

by Tom Niprinsky

South Seas IJ



**Drone Attacks on Industrial Wireless: A New Front in Cyber Security**

by Jeff Melrose

Lagoon K



**GATTacking Bluetooth Smart Devices - Introducing a New BLE Proxy Tool**

by Slawomir Jasek

South Seas GH



**HEIST: HTTP Encrypted Information can be Stolen Through TCP-Windows**

by Tom Van Goethem + Mathy Vanhoef

South Seas ABE



**Secure Penetration Testing Operations: Demonstrated Weaknesses in Learning Material and Tools**

by Wesley McGrew

Mandalay Bay EF



**Towards a Holistic Approach in Building Intelligence to Fight Crimeware**

Katıldığım sunumlardan, Breaking Payment Points Of Interaction (POI) sunumunda POS cihazının tuş takımına (Pinpad) ortadaki adam saldırısı (MITM) yapılarak müşteriden Pin girmesini istemeleri ve daha sonrasında aradaki

haberleşme şifreli olmadığı için çalabilmeleri, müşteriye gösterilen ekranlara kendi mesajlarını enjekte edebilmeleri oldukça ilginçti.



## The Basics of EMV

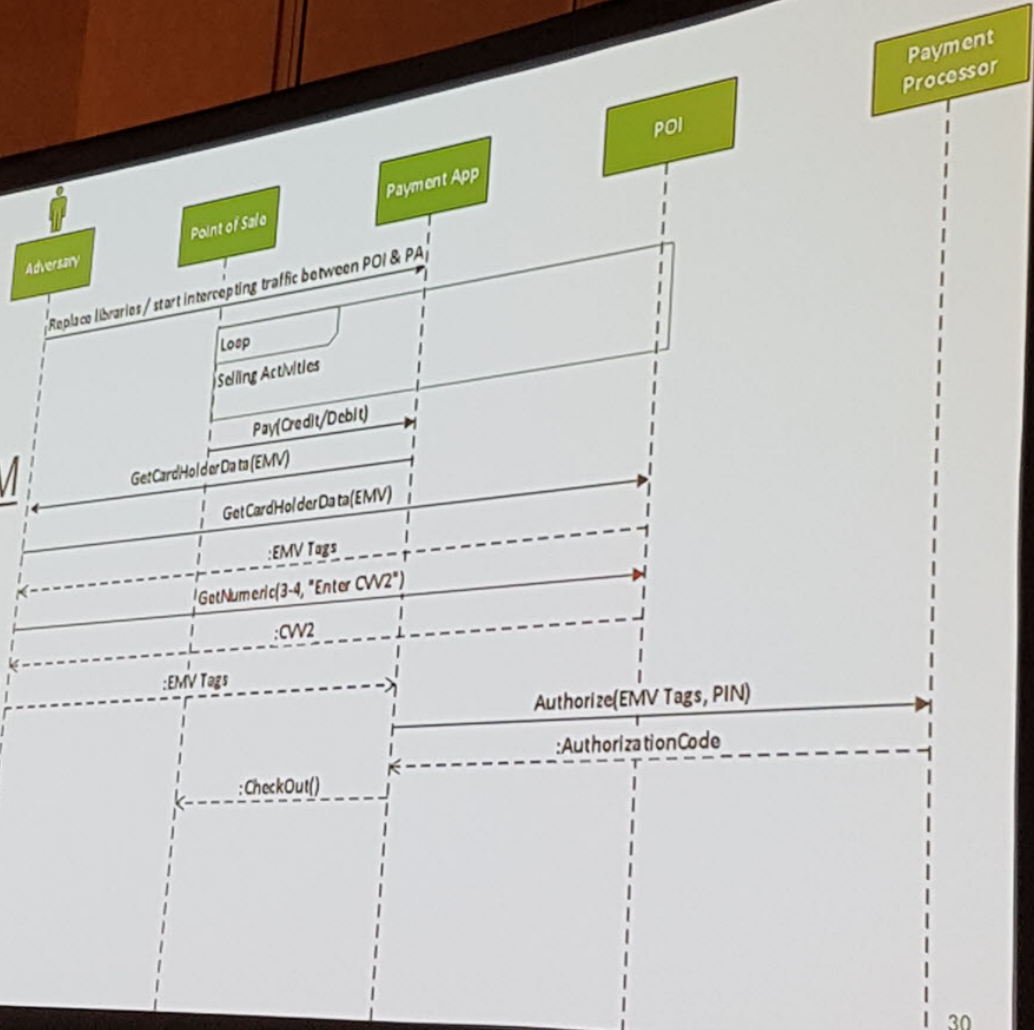
|      |                         |                         |
|------|-------------------------|-------------------------|
| 0000 | 08 00 27 75 54 3b ec f4 | bb 49 59 94 08 00 45 00 |
| 0010 | 00 a1 03 d1 40 00 80 06 | 74 33 c0 a8 00 64 c0 a8 |
| 0020 | 00 9e 9d ff 1b 8b ea cb | b1 6a 07 d0 41 73 50 18 |
| 0030 | 01 01 1c c0 00 00 00 77 | 02 43 33 31 30 30 00 6d |
| 0040 | 4f 08 a0 00 00 00 25 01 | 08 01 9f 12 00 50 10 41 |
| 0050 | 4d 45 52 49 43 41 4e 20 | 45 58 50 52 45 53 53 5f |
| 0060 | 30 02 02 01 5f 20 10 41 | 45 49 50 53 20 33 31 2f |
| 0070 | 56 45 52 20 32 2e 30 57 | 13 37 42 45 00 13 61 00 |
| 0080 | 4d 19 03 20 11 50 41 23 | 45 00 00 0f 5a 08 37 42 |
| 0090 | 45 00 13 61 00 4f 5f 24 | 03 19 03 31 5f 34 01 00 |
| 00a0 | 5f 25 03 15 04 01 9f 39 | 01 05 c2 01 31 03 04    |

```

.. 'uT;.. .IY...E.
....@... t3...d..
..... .j..AsP.
.....w .C3100.m
O.....%. ....P.A
MERICAN EXPRESS_
0..._ .A EIPS 31/
VER 2.0W .7BE..a.
M.. .PA# E...Z.7B
E..a.O_$ ...1_4..
%.....9 ....1..

```

## Active MITM Track 2 & CVV2 Compromise



Captain Hook: Pirating AVs To Bypass Exploit Mitigations sunumunda ise antivirüs yazılımlarının çengelleme (hook) yöntemini hatalı kullanmaları sebebiyle yüklü oldukları sistemlerin güvenliğini nasıl zayıflattığı ile ilgili kısımlar da oldukça önemliydi.

## Captain Hook:

### Pirating AVS to Bypass Exploit Mitigations

JULY 30 - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS

## MICROSOFT DETOURS

- The most popular hooking engine in the world
- Microsoft's App-V uses Detours which is integrated into Office
- We were surprised to find out that it has problems too...

### Features:

- ARM support
- ...

### Security Issues:

- Predictable RX (Universal).

\* Details won't be revealed until the patch is released (September)

| Products/Vendors     | UnSafe Injection | Predictable RWX(Universal) | Predictable RX(Universal) | Predictable RWX | RWX Hook code stubs | RWX Hooked Modules | Time To Fix (Days)  |
|----------------------|------------------|----------------------------|---------------------------|-----------------|---------------------|--------------------|---------------------|
| Symantec             |                  |                            |                           | X               |                     |                    | 90                  |
| McAfee               |                  |                            |                           | X               | X                   |                    | 90                  |
| Trend Micro          |                  | X                          | X (Initial Fix)           |                 | X                   |                    | 210                 |
| Kaspersky            |                  |                            | X                         | X               |                     |                    | 90                  |
| AVG                  |                  |                            |                           | X               |                     |                    | 30                  |
| BitDefender          |                  |                            |                           |                 | X                   | X                  | 30                  |
| WebRoot              |                  |                            | X                         |                 |                     | X                  | 29                  |
| AVAST                |                  |                            | X                         |                 | X                   |                    | 30                  |
| Emsisoft             |                  |                            |                           |                 | X                   |                    | 90                  |
| Citrix - Xen Desktop |                  |                            |                           |                 | X                   | X                  | 90                  |
| Microsoft Office*    |                  |                            | X                         |                 |                     |                    | 180                 |
| WebSense             | X                |                            |                           | X               |                     | X                  | 30                  |
| Vera                 | X                |                            |                           | X               |                     |                    | ?                   |
| Invincea             |                  | X(64-bit)                  |                           |                 | X                   | X                  | ?                   |
| Anti-Exploitation*   |                  |                            |                           | X               |                     |                    | ?                   |
| BeyondTrust          |                  |                            | X                         | X               |                     |                    | Fixed Independently |
| TOTALS               | 2                | 2                          | 6                         | 8               | 7                   | 5                  | 79.9                |

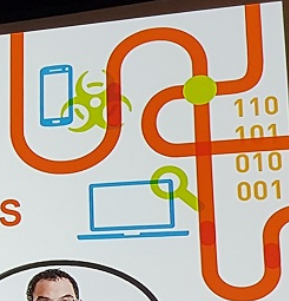
Konferansa damgasını vuran sunumlardan biri olan Hacking Next-Gen ATMs: From Capture To Cashout sunumunda ise Shimmer dediğimiz aygıtlar ile dolandırıcılar tarafından banka hesaplarının ATM üzerinden nasıl boşaltılabildiği gözler önüne serildi. Ayrıca son zamanlarda dolandırıcıların temassız kredi kartı bilgilerini de satın almaya başladıkları bilgisi, dikkat çeken bir diğer önemli noktaydı.

Shimmer, ATM'de kart okuyucu yuvasına yerleştirilen ve günümüzde güvenli olarak kabul edilen Çip & Pin destekli EMV kartın çipi ile ATM'nin çip okuyucusu arasındaki bilgiyi çalan ve dolandırıcılara bu bilgiyi anlık olarak gönderen bir aygıttır. Bu bilgiyi alan dolandırıcı, başka bir ATM'den bu bilgi ile müşterinin banka hesabını boşaltabilmektedir.

**RAPID7**

## HACKING NEXT-GEN ATMS FROM CAPTURE TO CASHOUT

Senior Security Consultant/Senior Pentester  
TWITTER, LinkedIn @westonhecker  
Rapid7 www.rapid7.com



### Buy Stolen Credit Card Data

Chain Fed Creditcard/EMV Data



HOME

COLLECTIONS

COLLECTIONS

ABOUT

CONTACT

BLOG



Buy EMV/Chip Card  
Data

+ VIEW MORE



Buy RFID Data

+ VIEW MORE



Show More

Buy Classic Track  
1,2,3 Data  
W/out PIN

+ VIEW MORE



Buy Devices  
Skimmers/Shimmers  
Cashout Devices

+ VIEW MORE

Buy Credit Card Data for all your scamming needs. Hotprice Carder Site has the

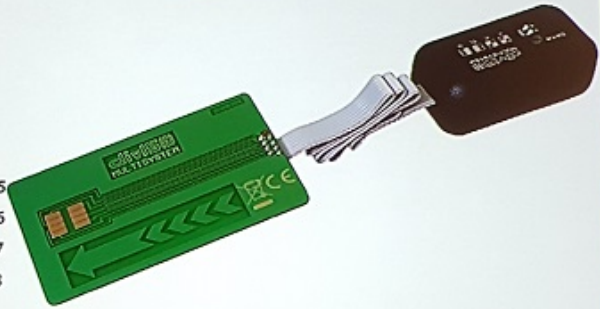
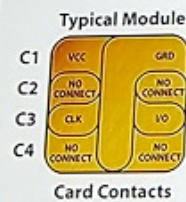
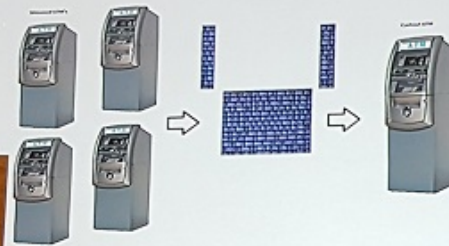
Buy Small Batch Skims



## Cashout Device Standalone?



## La-Cara Swiss army knife



Cherokee Jeep'i hackleyerek ünlerine ün katan Charlie Miller ile Chris Valasek'in Advanced Can Injection Techniques For Vehicle Networks sunumuna geçen sene olduğu gibi yine yoğun bir ilgi vardı. Bu iki güvenlik araştırmacısı sunumlarında, araba üreticilerinin güvenlik adına sistemlerine koydukları kontrolleri nasıl aşabildiklerine ve bunun için hangi adımlardan geçtiklerine yer verdiler.

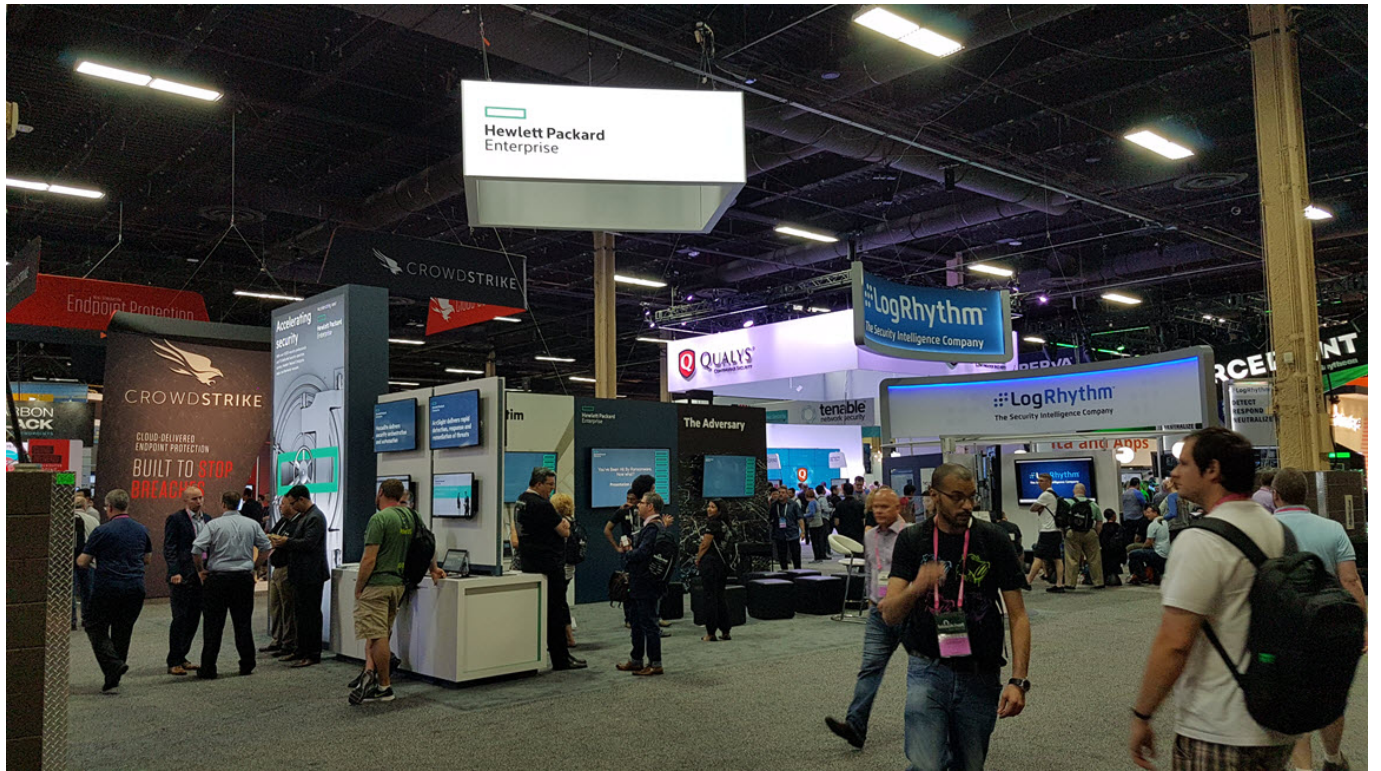




### State of art CAN injection – Physical systems

|               | 2009 Chevy Malibu | 2012 Ford Escape | 2012 Toyota Prius | 2014 Jeep Cherokee (previous) | 2014 Jeep Cherokee (now) |
|---------------|-------------------|------------------|-------------------|-------------------------------|--------------------------|
| Engage brakes | Yes               | < 5mph           | Yes               | < 5mph                        | Yes                      |
| Stop brakes   | Yes               | < 5mph           | No                | < 5mph                        | < 5mph                   |
| Steering      | No                | < 5mph           | Partly            | < 5mph                        | Yes                      |
| Acceleration  | No                | No               | No                | No                            | Yes                      |

Sunumlar dışında pek tabii yine Business Hall, güvenlik dünyasının markalarına ve bu markaların görkemli stantlarına ev sahipliği yaptı. Black Hat USA 2016'da, Türkiye'de olduğu gibi "madem sponsor oldum o halde ben de konuşacağım" diyen, mikrofonu eline alıp etkinlik programını ve katılımcıların vakitlerini hiçe sayarak uzun süreler konuşup programı sarkıtan sponsor sunumları yoktu. Güvenlik etkinliği düzenlemeye niyetlenip sponsorların kaprisleri ile karşı karşıya kalanlar, sponsorları ikna etme adına aşağıdaki fotoğrafları kendileri ile paylaşabilirler. :)

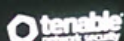
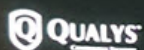
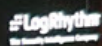
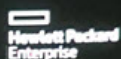




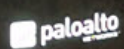
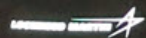
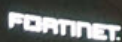
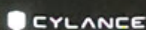
# black hat<sup>®</sup>

USA 2016

## DIAMOND SPONSORS



## PLATINUM PLUS SPONSORS



Black Hat mağazasına her zaman olduğu gibi Black Hat hayranlarının oldukça yoğun ilgisi vardı. Birbirinden ilginç hediyeelik eşyalar arasında gezinirken, Twitter takipçilerime yönelik düzenleyeceğim hediye çekilişi için ufak tefek hediyeler almayı ihmal etmedim. :)







Eğitimleriyle, sunumlarıyla, atmosferiyle ve anılarıyla beni her daim büyüleyen Black Hat USA konferansı benim için yine oldukça verimli geçti. Umarım bilgi güvenliğine meraklı olan herkes, imkanları dahilinde veya işverenlerinin desteğiyle bu konferansa katılma imkanını birgün yakalar. Black Hat 2017 USA blog yazısı ile tekrar görüşebilir miyiz bilmiyorum fakat görüşebilmeyi ümit ederek herkese güvenli günler dilerim. :)



black hat®



