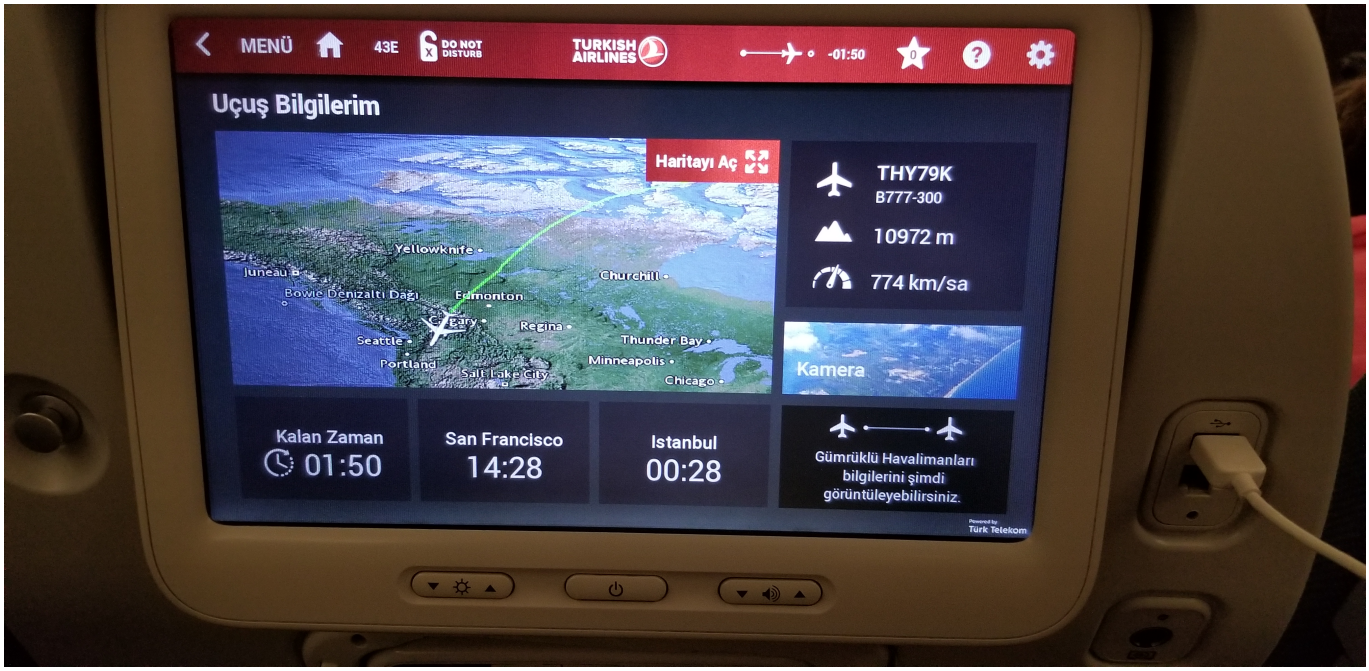
Black Hat USA 2018

written by Mert SARICA | 26 August 2018

Sevgili işverenim Akbank'ın ve yöneticilerimin destekleri ile 2 yıl aradan sonra yeni bir Black Hat USA serüveni için 3 Ağustos, sabah saat 05:00'da yolculuk için hazırlanmaya başladım. Akbank sponsorluğunda (ilk fotoğrafa dikkat :)) başlayan ilk uçak yolculuğunun ardından San Francisco aktarmalı olarak Las Vegas'ta, konferansın gerçekleşeceği Mandalay Bay oteline vardığımda, Türkiye saati ile saat 23:00 olmuş ve jet lag olmamak için tam 17+ saat uyumamış olmanın verdiği yorgunlukla tam anlamıyla pestilim çıkmıştı. Seyahat öncesinde Türk Lirası'nın aşırı değer kaybetmesi ile Amerikan Doları'nın 5.11 TL'ye kadar yükselmesi nedeniyle hayatımın en pahalı soğuk suyunu (5$ / 25 TL) otele vardığımda içerek hızlıca ayıldım. :)



4 Ağustos sabahı, saat 10:00'da başlayacak olan 2 günlük The Security Automation Lab eğitiminin heyecanı ile güne erken başladım. İlk iş olarak Black Hat kayıt alanına gidip yaka kartımı ve kayıt esnasında verilen Black Hat çantasını aldıktan sonra hızlıca eğitim alacağım sınıfın yolunu tuttum. Yolda giderken de her zaman olduğu gibi sizler için bol bol fotoğraf çekmeyi ihmal etmedim. :)

Your Badge/
On-Site Registration
UBM Check-In
Registration Customer Service/
Sustaining Partner Check-In
black hat
USA 2018
AUGUST 4-9, 2018
EMAIL ADDRESS OR CONFIRMATION NUMBER NOT FOUND
CREATE NEW ATTENDEE REGISTRATION

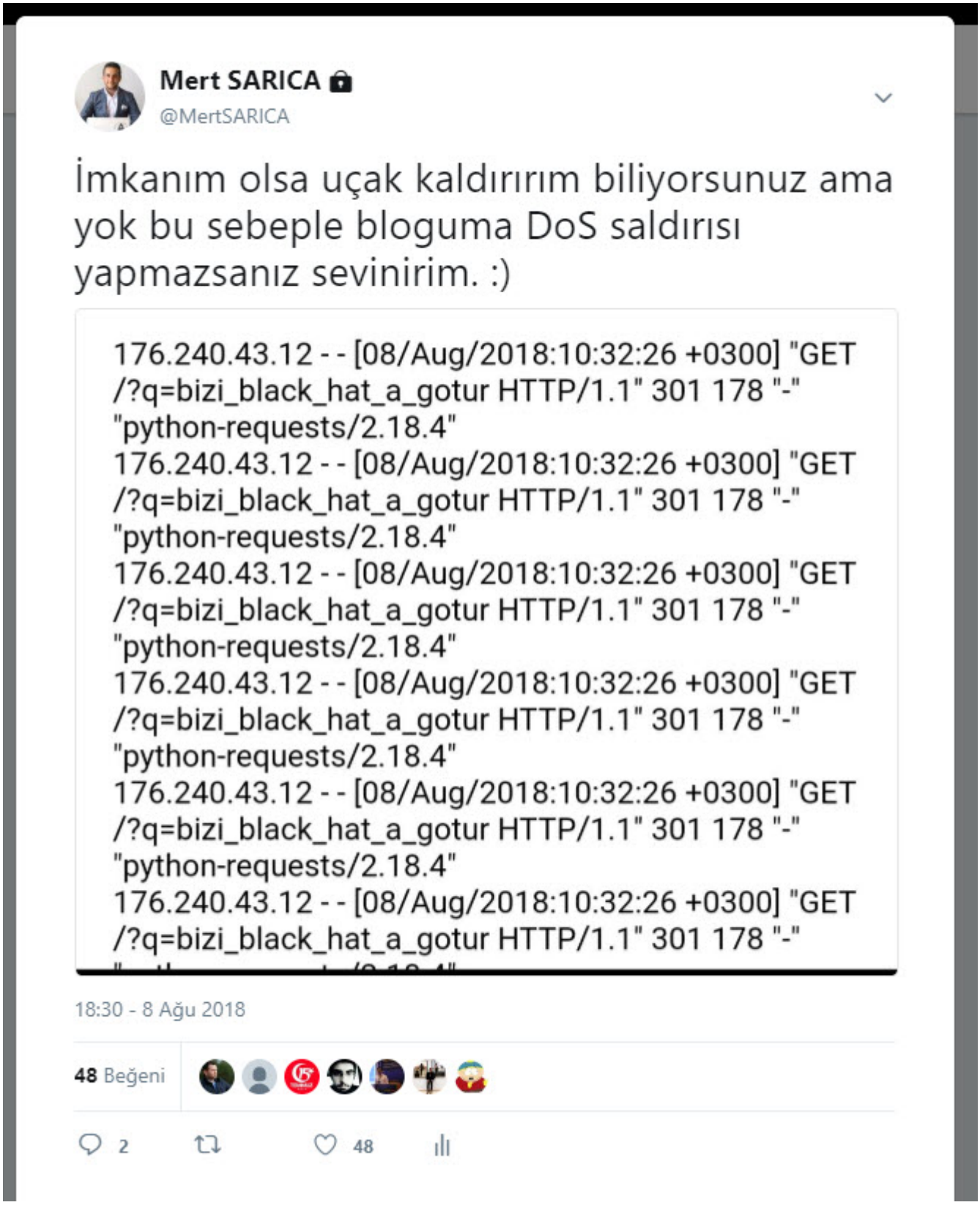
CYLANCE
black hat
USA 2018
blackhat USA 2018
Mert SARICA
Cyber Security Manager
TRAININGS,BRIEFINGS

Daha önce almış olduğum tekik eğitimlere göre oldukça hafif olan 2 günlük bu eğitim boyunca güvenlik otomasyon platformu olarak kullanılan Evolve platformu üzerinde, tehdit istihbaratı toplamaktan sistem üzerinde tespit

edilen bir zararlı yazılıma müdahaleye kadar bir çok senaryonun uygulamasını gerçekleştirdik. Entegrasyon adına manuel gereksinimi çok olsa da özellikle IBM’in Resilient gibi bir güvenlik otomasyon platformu satın alacak bütçesi olmayan kurumların Evolve platformuna göz atmalarını, eğitimden edindiğim tecrübeye istinaden söyleyebilirim.

black hat
USA 2018
The Security
Automation Lab
BY THREAT INTELLIGENCE
PTY LTD

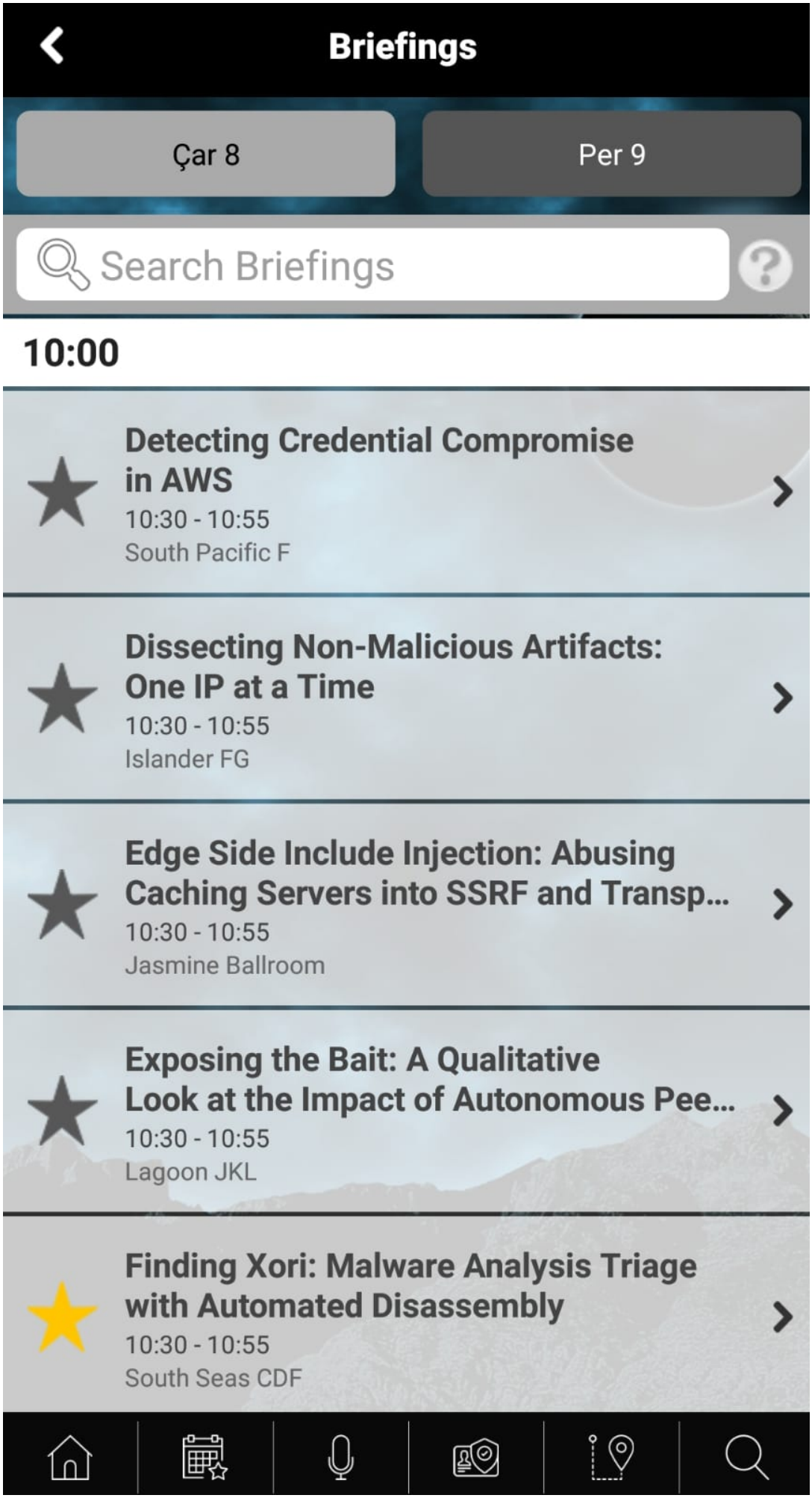
Önceki yıllarda olduğu gibi Black Hat USA ile ilgili olarak orada bulunduğum süre boyunca Twitter ve LinkedIn sosyal medya hesaplarımdan merak edenler için bol bol paylaşımda bulunmaya gayret ettim. Tabii bu paylaşımlara istinaden biri veya birileri de “bizi_black_hat_e_gotur” mesajı ile bloguma DoS saldırısı yaptığı da gözümden kaçmadı. Her daim okurları ve takipçileri için imkanları dahilinde hediye çekilişleri yapan birinin imkanı olsa emin olun Black Hat’e uçak kaldırırdı ama maalesef imkansızlıklar. :)



Konferans günü gelip çattığında, açılış konuşması için 2016 yılındaki ana balo salonu yerine bu defa kendimi Mandalay Bay'in 12.000 kişilik etkinlik merkezinde buldum. 12.000 kişilik etkinlik merkezi dolar mı diye biran olsun kendi kendime yanılgıya düşsem de açılış konuşmasına dakikalar kala boş koltuk sayılarını seçmekte oldukça zorlandım. Açılış konuşmasını yapmak için her zaman olduğu gibi ilk olarak sahneye Jeff Moss ardından da Google'ın

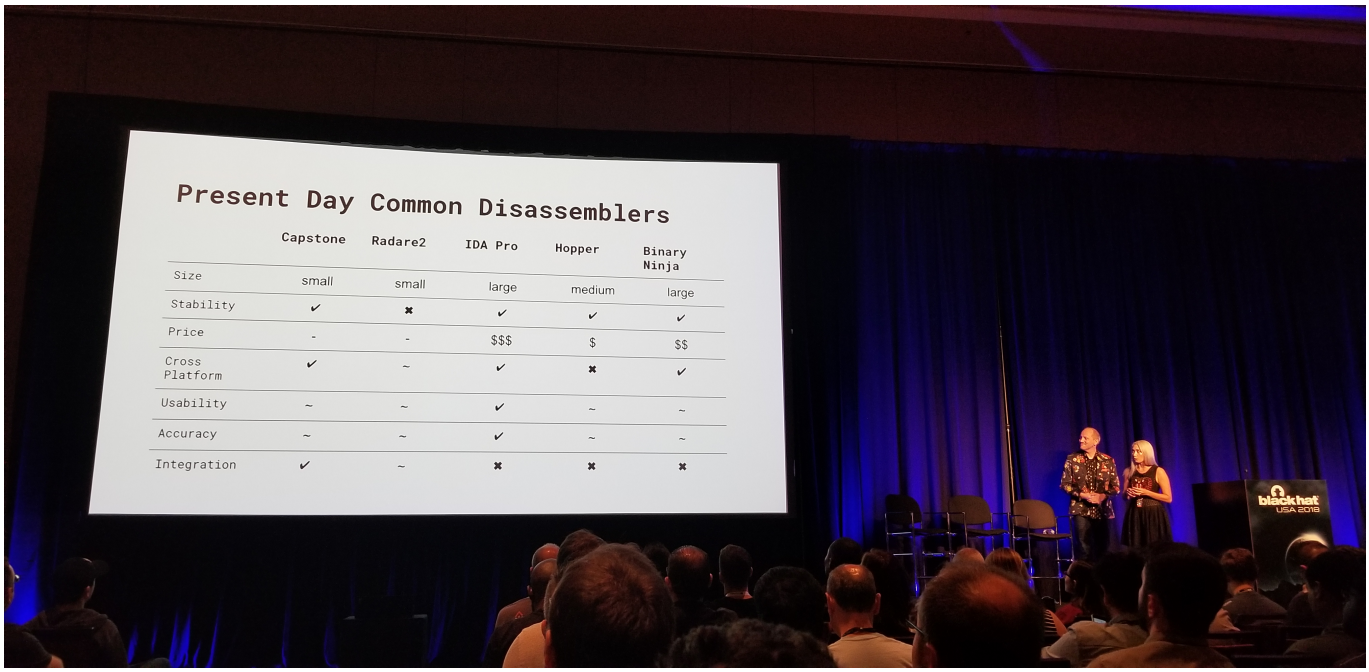
Project Zero müdürü Parisa Tabriz çıktı. Parisa Tabriz konuşması esnasında geçtiğimiz ay hayata geçen ve HTTPS olmayan sitelerin Chrome internet tarayıcısı tarafından güvensiz olarak etiketlenmesinin internet güvenliği adına başarıya ulaştığından bahsetti. Benzer şekilde Project Zero'nun 90 günlük zafiyet yayınlama politikasının (90 day disclosure policy) da başta üreticiler tarafından memnuniyetsizlikle karşılandığını ancak Google'ın bu konuda geri adım atmaması sayesinde tespit ettikleri zafiyetlerin %98'inin 90 gün içinde üreticiler tarafından giderildiğini belirtti. Dileyenler muazzam açılış videosunu aşağıdan, açılış konuşmasının tamamını ise buradan izleyebilirler.

Geçtiğimiz yıllarda olduğu gibi yine paralelde ilgimi çeken çok sayıda sunum olması sebebiyle Black Hat USA'in mobil uygulaması üzerinden hangi sunumlara katılacağıma karar vermekte güçlük çektim.


Briefings
Çar 8
Per 9
Search Briefings
10:00
Detecting Credential Compromise in AWS
10:30 - 10:55
South Pacific F
Dissecting Non-Malicious Artifacts: One IP at a Time
10:30 - 10:55
Islander FG
Edge Side Include Injection: Abusing Caching Servers into SSRF and Transp...
10:30 - 10:55
Jasmine Ballroom
Exposing the Bait: A Qualitative Look at the Impact of Autonomous Pee...
10:30 - 10:55
Lagoon JKL
Finding Xori: Malware Analysis Triage with Automated Disassembly
10:30 - 10:55
South Seas CDF

Çoğu sunumun, sunum dosyası yayınlandığı için her bir sunuma ayrı ayrı değinmeden her birinini ayrı ayrı incelemenizi tavsiye edebilirim. İlk günün en çok beğendiğim sunumlarını sıralayacak olursam;

1. Zararlı yazılım analizi alanında da çalışmaları ile tanınan Amanda Rousseau'nun geliştirip tanıttığı disassembler aracını içeren Finding Xori: Malware Analysis Triage with Automated Disassembly sunumu,

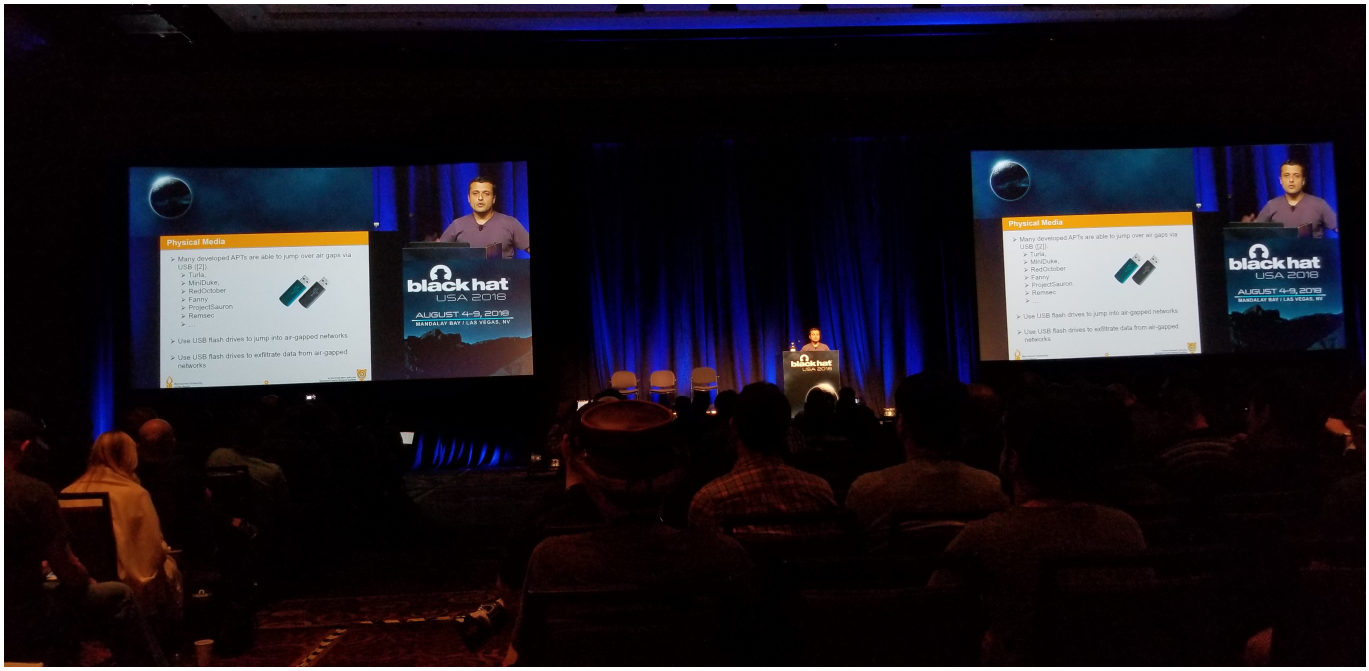


2. Güvenlik Enstrümanlı Sistemi (safety instrumented system) hedef alan ilk zararlı yazılım olarak tarihe geçen Triton hakkında detaylı bilgilerin yer aldığı TRITON: How it Disrupted Safety Systems and Changed the Threat Landscape of Industrial Control Systems, Forever sunumu,

3. Donanım yazılımlarına (firmware) gerçekleştirilen çeşitli saldırı yöntemlerini ve tekniklerini konu alan Remotely Attacking System Firmware sunumu,

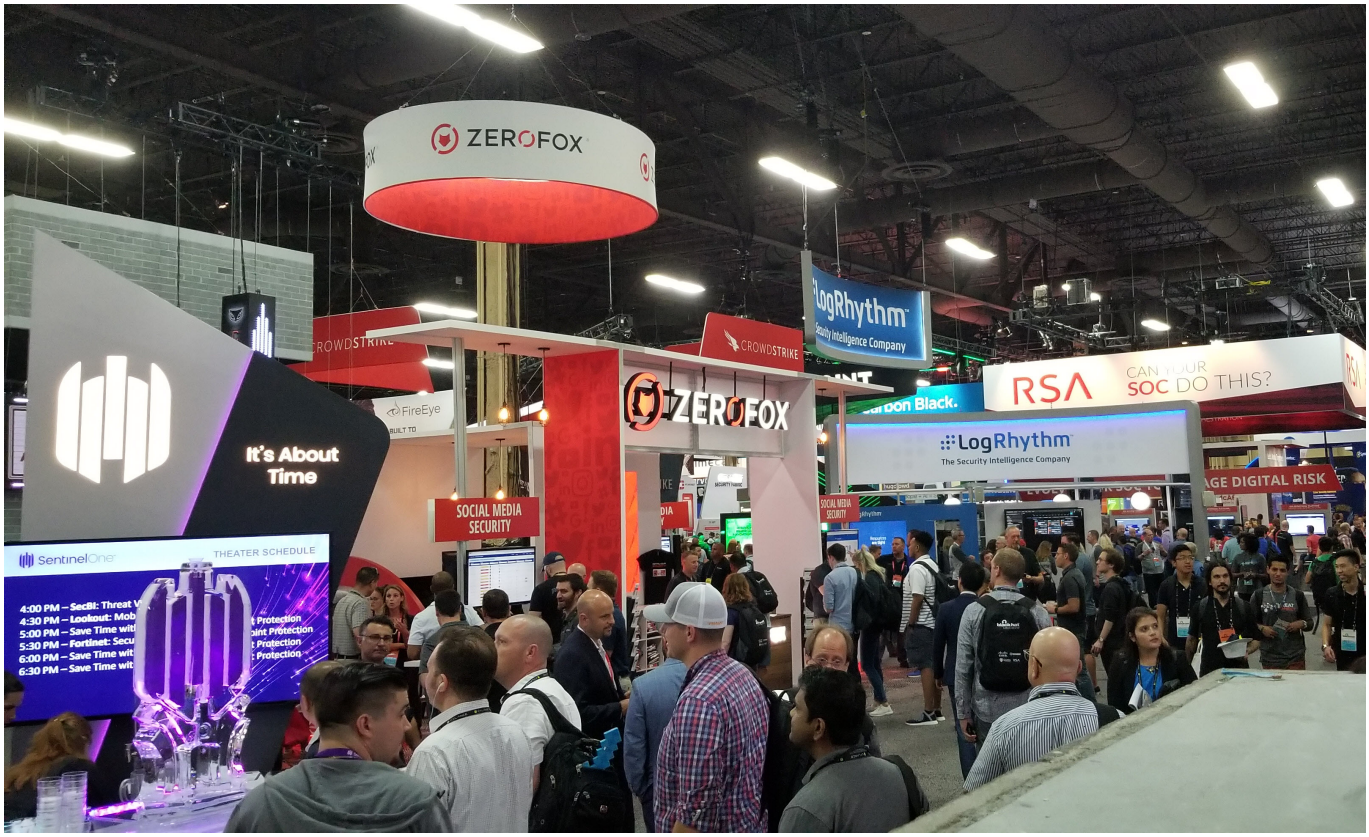
4. Microfost'un sesli asistan uygulamasının kötüye kullanımını gözler önüne seren Open Sesame: Picking Locks with Cortana sunumu,

5. İsrailli güvenlik araştırmacısının air gap denilen, yerel ağlara ve internete bağlı olmayan sistemlerden (faraday kafesindeki de dahil) nasıl veri sızdırılabildiğini çok sayıda yöntemle gösterdiği The Air-Gap Jumpers sunumu

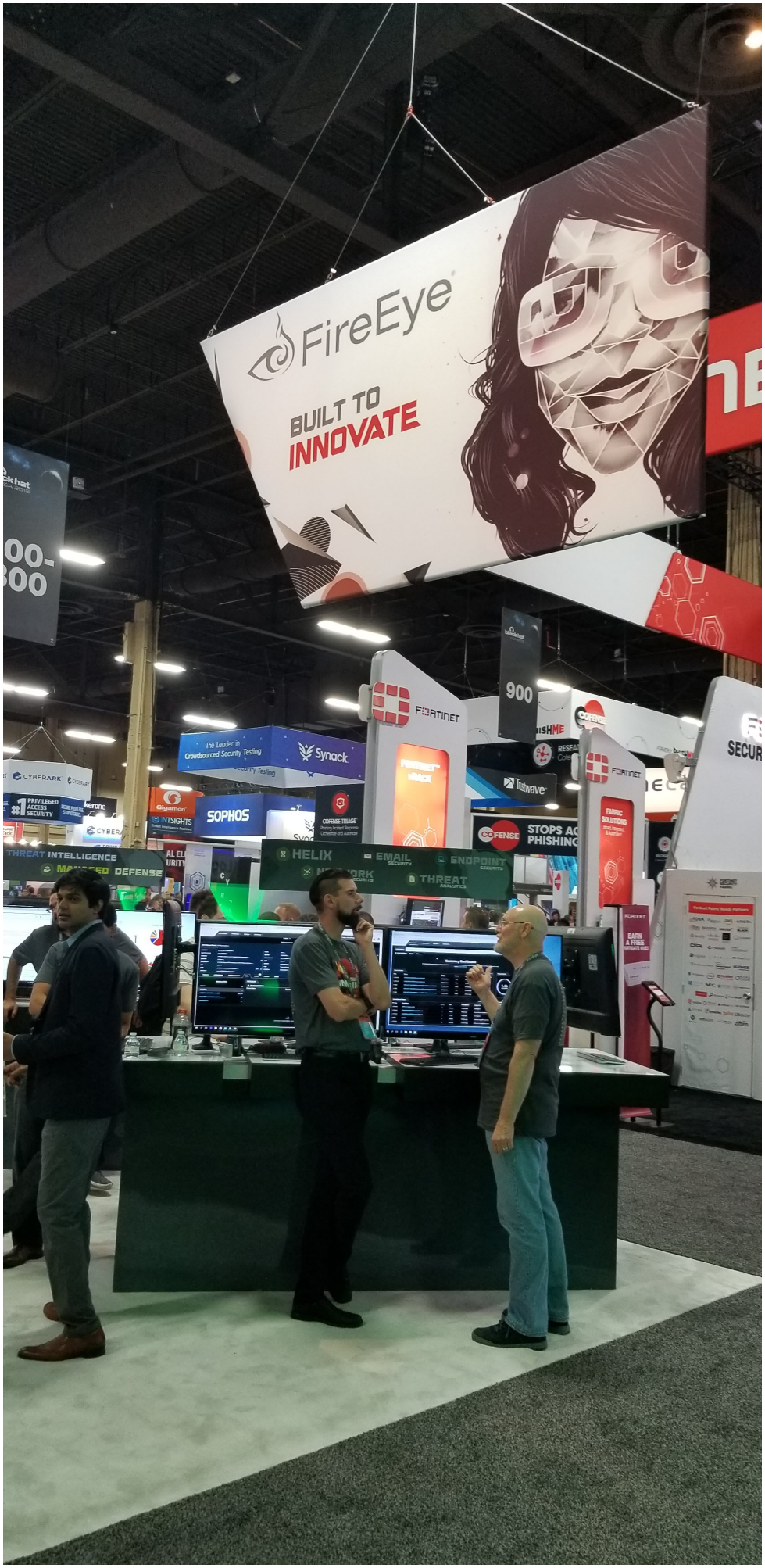


Sunumlar arası yine her Black Hat'te olduğu gibi hıncahınç kalabalığın arasında 3 farklı katta gerçekleştirilen sunumlara ulaşabilmek için epey çaba sarfettim. Sunumlardan arda kalan zamanlarda da yine güvenlik dünyasının büyük üreticilerinin yer aldığı Business Hall'a, güvenlik araçlarının tanıtıldığı meşhur Black Hat Arsenal'e, Black Hat ağına gerçekleştirilen siber saldırıları izleyen Black Hat NOC odasına, kitapçısına ve pek tabii ki okurlarım, takipçilerim için düzenleyeceğim hediye çekilişi için Black Hat mağazasına çam sakızı çoban armağanı hediyeler almak için uğradım. :)

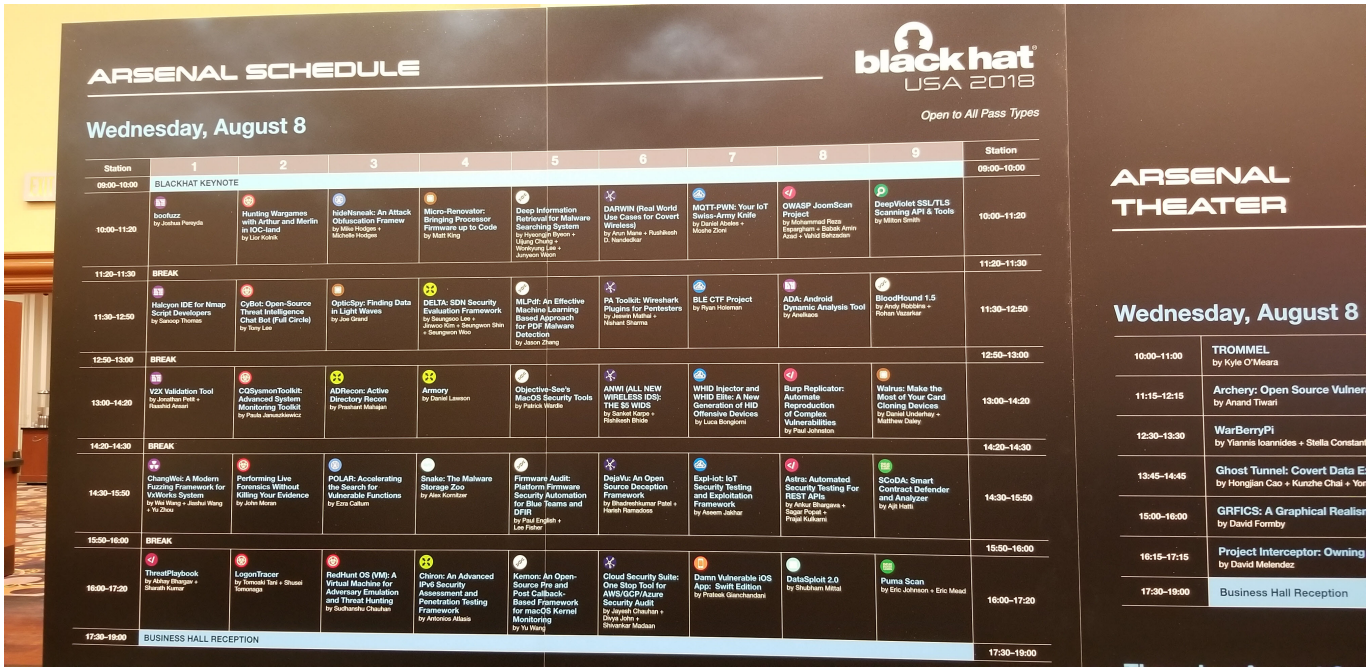
black hat
USA 2018

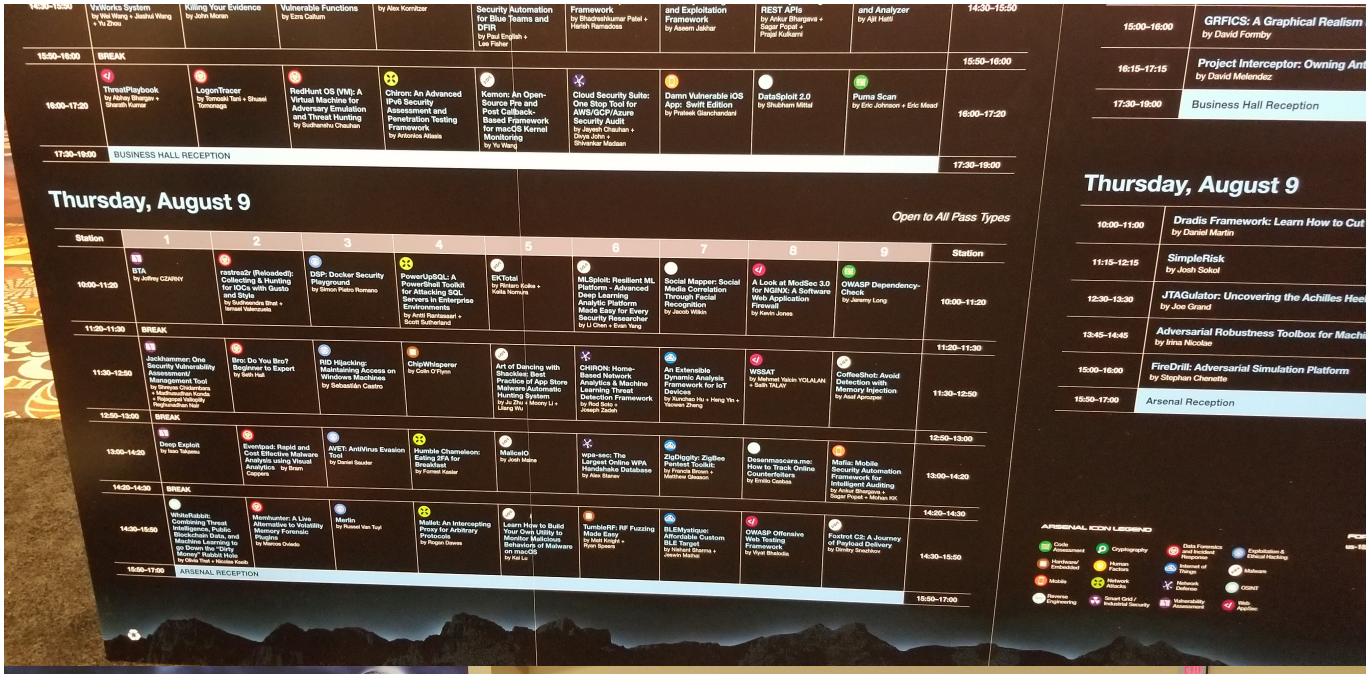

ZEROFOX
It's About Time
SentinelOne
THEATER SCHEDULE
SOCIAL MEDIA SECURITY
CROWDSTRIKE
FireEye
LogRhythm
Security Intelligence Company
RSA
LogRhythm
The Security Intelligence Company

Introducing
Community Edition
Sign up. It's FREE
qualys.com/ce
Qualys
tenable
Nessus
1600
black hat
USA 2018
Thank You to Our
Sustaining Partners
accenture
CROWDSTRIKE
cybereason
DARKMATTER
Qualys

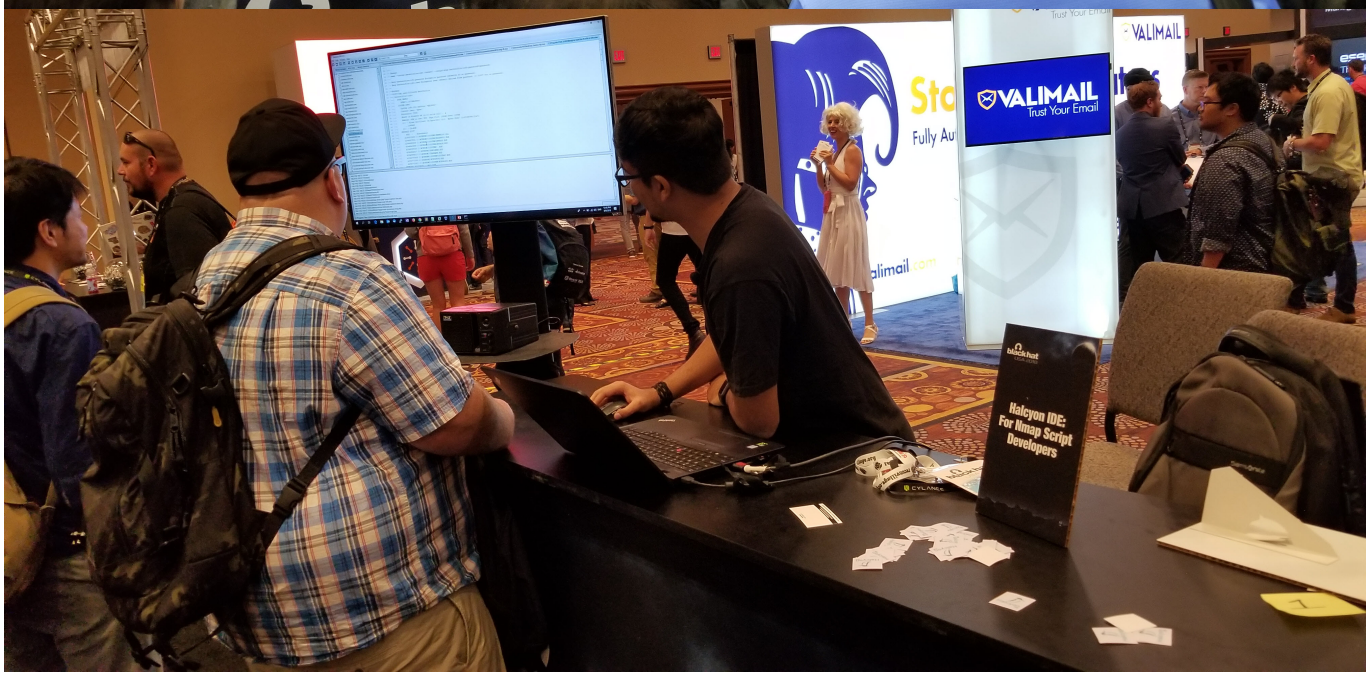

FireEye
BUILT TO
INNOVATE
FORTINET
Synack
The Leader in
Crowdsourced Security Testing
CYBERARK
#1 PRIVILEGED ACCESS SECURITY
SOPHOS
Tenable
Tnswave
COFENSE
STOPS AC
PHISHING
HELIX
EMAIL
ENDPOINT
THREAT
THREAT INTELLIGENCE
DEFENSE
900

1200
bugcrowd
#1 Crowdsourced Security Platform
SecurityScore
mimecast
spirent
eset CYBERSECURITY EXPERTS ON YOU
bugcrowd
AIRBRUSH Tattoos
cybereflood


ARSENAL SCHEDULE
black hat USA 2018
Open to All Pass Types
Wednesday, August 8
Station 1 2 3 4 5 6 7 8 9 Station
09:00–10:00 BLACKHAT KEYNOTE 09:00–10:00
10:00–11:20 boofuzz by Joshua Pereyda | Hunting Wargames with Arthur and Merlin in KOC-land by Lior Kolnik | hideNsneak: An Attack Obfuscation Framew by Mike Hodges + Michelle Hodges | Micro-Renovator: Bringing Processor Firmware up to Code by Matt King | Deep Information Retrieval for Malware Searching System by Hyeongjin Byeon + Ujjung Chung + Wonkyung Lee + Junyeon Won | DARWIN (Real World Use Cases for Covert Wireless) by Arun Manu + Rushikesh D. Nandedkar | MQTT-PWN: Your IoT Swiss-Army Knife by Daniel Abeles + Moshe Zioni | OWASP JoomScan Project by Mohammad Reza Espargham + Babak Amin Azad + Vahid Behzadan | DeepViolet SSL/TLS Scanning API & Tools by Milton Smith 10:00–11:20
11:20–11:30 BREAK 11:20–11:30
11:30–12:50 Halcyon IDE for Nmap Script Developers by Sanoop Thomas | CyBot: Open-Source Threat Intelligence Chat Bot (Full Circle) by Tony Lee | OpticSpy: Finding Data in Light Waves by Joe Grand | DELTA: SDN Security Evaluation Framework by Seungsoo Lee + Jinwoo Kim + Seungwon Shin + Seungwon Woo | MLPdf: An Effective Machine Learning Based Approach for PDF Malware Detection by Jason Zhang | PA Toolkit: Wireshark Plugins for Pentesters by Jeswin Mathai + Nishant Sharma | BLE CTF Project by Ryan Holeman | ADA: Android Dynamic Analysis Tool by Anshaos | BloodHound 1.5 by Andy Robbins + Rohan Vazarkar 11:30–12:50
12:50–13:00 BREAK 12:50–13:00
13:00–14:20 VZX Validation Tool by Jonathan Petit + Rwashid Ansari | CQSysmonToolkit: Advanced System Monitoring Toolkit by Paula Januszkiewicz | ADRecon: Active Directory Recon by Prashant Mahajan | Armory by Daniel Lawson | Objective-See's MacOS Security Tools by Patrick Wardle | ANWI (ALL NEW WIRELESS IDS): THE $5 WIDS by Sanket Kanjar + Rahikesh Bhide | WHID Injector and WHID Elite: A New Generation of HID Offensive Devices by Luca Bongiorni | Burp Replicator: Automate Reproduction of Complex Vulnerabilities by Paul Johnston | Walrus: Make the Most of Your Card Cloning Devices by Daniel Underhay + Matthew Daley 13:00–14:20
14:20–14:30 BREAK 14:20–14:30
14:30–15:50 ChangWei: A Modern Fuzzing Framework for VxWorks System by Wei Wang + Jiashui Wang + Yu Zhou | Performing Live Forensics Without Killing Your Evidence by John Moran | POLAR: Accelerating the Search for Vulnerable Functions by Ezra Caltum | Snake: The Malware Storage Zoo by Alex Kornitzer | Firmware Audit: Platform Firmware Security Automation for Blue Teams and DFIR by Paul English + Lee Fisher | DejaVu: An Open Source Deception Framework by Bhadreshkumar Patel + Harish Ramadoss | Expl-iot: IoT Security Testing and Exploitation Framework by Aseem Jakhar | Astra: Automated Security Testing For REST APIs by Ankur Bhargava + Sagar Popat + Prajal Kulkarni | SCoDA: Smart Contract Defender and Analyzer by Ajit Hatti 14:30–15:50
15:50–16:00 BREAK 15:50–16:00
16:00–17:20 ThreatPlaybook by Abhay Bhargav + Shanth Kumar | LogonTracer by Tomoki Tani + Shusei Tomonaga | RedHunt OS (VM): A Virtual Machine for Adversary Emulation and Threat Hunting by Sudhanshu Chauhan | Chiron: An Advanced IPv6 Security Assessment and Penetration Testing Framework by Antonios Atlasis | Kemon: An Open-Source Pre and Post Callback-Based Framework for macOS Kernel Monitoring by Yu Wang | Cloud Security Suite: One Stop Tool for AWS/GCP/Azure Security Audit by Jayesh Chauhan + Divya John + Shivankar Madaan | Damn Vulnerable iOS App: Swift Edition by Prateek Gianchandani | DataSploit 2.0 by Shubham Mittal | Puma Scan by Eric Johnson + Eric Mead 16:00–17:20
17:30–19:00 BUSINESS HALL RECEPTION 17:30–19:00
ARSENAL THEATER
Wednesday, August 8
10:00–11:00 TROMMEL by Kyle O'Meara
11:15–12:15 Archery: Open Source Vulner by Anand Tiwari
12:30–13:30 WarBerryPi by Yiannis Ioannides + Stella Constant
13:45–14:45 Ghost Tunnel: Covert Data E by Hongjian Cao + Kunzhe Chai + Yor
15:00–16:00 GRFICS: A Graphical Realisr by David Formby
16:15–17:15 Project Interceptor: Owning by David Melendez
17:30–19:00 Business Hall Reception


Thursday, August 9
Open to All Pass Types
Station
1
2
3
4
5
6
7
8
9
10:00–11:20
11:20–11:30 BREAK
11:30–12:50
12:50–13:00 BREAK
13:00–14:20
14:20–14:30 BREAK
14:30–15:50
15:50–17:00 ARSENAL RECEPTION
BUSINESS HALL RECEPTION
BSTA by Jeffrey CZARNY
rastrea2r (Reloaded!): Collecting & Hunting for IOCs with Gusto and Style by Sudhanshu Bhat + Ismael Valenzuela
DSP: Docker Security Playground by Simon Pietro Romano
PowerUpSQL: A PowerShell Toolkit for Attacking SQL Servers in Enterprise Environments by Antti Rantasaari + Scott Sutherland
EKTotal by Ryan Kalke + Keita Nomura
MLSploit: Resilient ML Platform - Advanced Deep Learning Analytic Platform Made Easy for Every Security Researcher by Li Chen + Sian Yang
Social Mapper: Social Media Correlation Through Facial Recognition by Jacob Wilkin
A Look at ModSec 3.0 for NGINX: A Software Web Application Firewall by Kevin Jones
OWASP Dependency-Check by Jeremy Long
Jackhammer: One Security Vulnerability Assessment/Management Tool by Shreyas Chidrawar + Madhusudhan Konda + Rajagopal Vellaichy Raghunadhan Nair
Bro: Do You Bro? Beginner to Expert by Seth Hall
RID Hijacking: Maintaining Access on Windows Machines by Sebastián Castro
ChipWhisperer by Colin O'Flynn
Art of Dancing with Shadows: Best Practice of App Store Malwares Automatic Hunting System by Ju Zhu + Mozmy Li + Lilang Wu
CHIRON: Home-Based Network Analytics & Machine Learning Threat Detection Framework by Rod Soto + Joseph Zadeh
An Extensible Dynamic Analysis Framework for IoT Devices by Xunchao Hu + Heng Yin + Yaowen Zheng
WSSAT by Mehmet Yalcin YOLALAN + Salih TALAY
CoffeeShot: Avoid Detection with Memory Injection by Asaf Aprosper
Deep Exploit by Isao Takaesu
Eventpad: Rapid and Cost Effective Malware Analysis using Visual Analytics by Bram Cappers
AVET: AntiVirus Evasion Tool by Daniel Sauder
Humble Chameleon: Eating 2FA for Breakfast by Forrest Kasler
MalicaIO by Josh Maine
wps-sec: The Largest Online WPA Handshake Database by Alex Stanev
ZigDiggity: ZigBee Pentest Toolkit by Francis Brown + Matthew Gleason
Dosenmascara.me: How to Track Online Counterfeiters by Emilio Cedeo
Mafia: Mobile Security Automation Framework for Intelligent Auditing by Ankur Bhargava + Sagar Popat + Mohan KK
WhiteRabbit: Combining Threat Intelligence, Public Blockchain Data, and Machine Learning to go Down the Rabbit Hole Money" Russell Hay by Olivia Thet + Nicolas Keeb
Memhunter: A Live Alternative to Volatility Memory Forensic Plugins by Marcos Oviedo
Merlin by Russel Van Tuyl
Mallet: An Intercepting Proxy for Arbitrary Protocols by Rogan Dawes
Learn How to Build Your Own Utility to Monitor Malicious Behaviors of Malware on macOS by Kai Lu
TumbleRF: RF Fuzzing Made Easy by Matt Knight + Ryan Speers
BLEMystique: Affordable Custom BLE Target by Nikhil Sharma + Jitesh Mishra
OWASP Offensive Web Testing Framework by Yuvi Bhaskola
Foxtrot C2: A Journey of Payload Delivery by Dmitry Snezhkov
Thursday, August 9
10:00–11:00 Dradis Framework: Learn How to Cut by Daniel Martin
11:15–12:15 SimpleRisk by Josh Sokol
12:30–13:30 JTAGulator: Uncovering the Achilles Heel by Joe Grand
13:45–14:45 Adversarial Robustness Toolbox for Machi by Irina Nicolae
15:00–16:00 FireDrill: Adversarial Simulation Platform by Stephan Chenette
15:50–17:00 Arsenal Reception
15:00–16:00 GRFICS: A Graphical Realism by David Formby
16:15–17:15 Project Interceptor: Owning Ani by David Melendez
17:30–19:00 Business Hall Reception
ARSENAL ICON LEGEND
Code Assessment
Cryptography
Data Forensics and Incident Response
Exploitation & Ethical Hacking
Hardware/ Embedded
Human Factors
Internet of Things
Malware
Mobile
Network Attacks
Network Defense
OSINT
Reverse Engineering
Smart Grid / Industrial Security
Vulnerability Assessment
Web Application

STATION 9
What Is BloodHound?
BloodHound 1.5


VALIMAIL
Trust Your Email
Halcyon IDE: For Nmap Script Developers

ADA: Android Dynamic Analysis Tool
blackhat USA 2018
ADA: I'll repeat the presentation in 5 minutes
https://github.com/ANELKAOS/ada
ANELKAOS@Gmail.com
@Sergio_Security
Kudos to Anthony Desnos, Ole Andre, Sergi Alvarez
cisco
tenable
Qualys.
RSA

NLP-dl: An Effective Machine Learning Based Approach for PDF Malware Detection

black hat
USA 2018
WELCOME TO
THE BLACK HAT
NETWORK
OPERATIONS
CENTER (NOC)

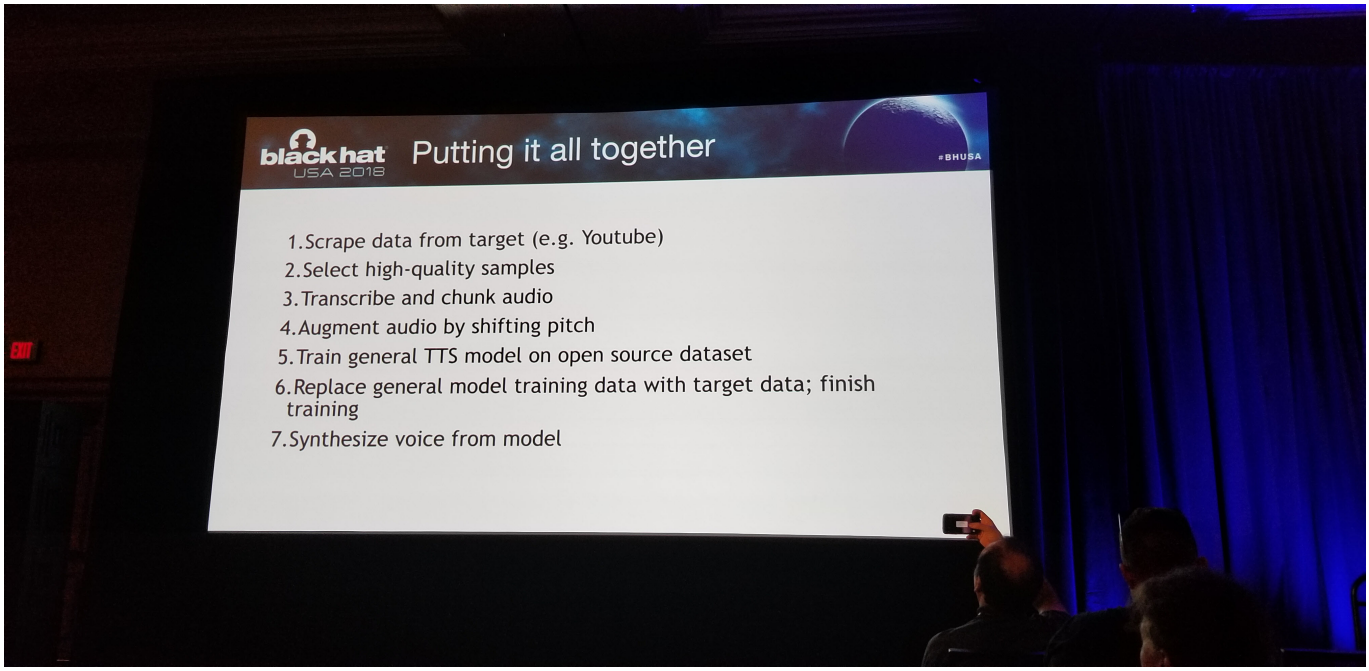
EXIT
RSA
#114 IRC Cleartext - NWO Test- Manual alert for Last 3 ...
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
Overview
Reports
Operations - Protocol Analysis Dashboard
HTTP Headers No...
HTTP User Agents ...
DNS Non Standard
HTTP Methods No...
Hostnames Non St...
HTTP Webshells
Past 24 hours
RSA NETWITNESS PLATFORM
11.2.0.0
Rotate
Crop
Straighten
Red-eye
Adjust
Enhance

SHIP YOUR BOOKS HOME
HIDING FROM THE INTERNET
OPEN SOURCE INTELLIGENCE TECHNIQUES
RESOURCES FOR SEARCHING AND ANALYZING ONLINE INFORMATION
SIXTH EDITION
MICHAEL BAZZELL
CEH v9
CCSP
OFFICIAL PRACTICE TESTS
Mike Meyers' CompTIA Security+ CERTIFICATION GUIDE (EXAM SY0-501)
<WOMEN IN TECH>
TARAH WHEELER VAN VLACK
TAKE YOUR CAREER TO THE NEXT LEVEL
with Practical Advice and Inspiring Stories
Includes:
THE SECRETS OF SALARY NEGOTIATION
THE BEST FORMAT FOR TECH RESUMES
HOW TO ACE A TECH INTERVIEW
HOW TO START YOUR OWN COMPANY

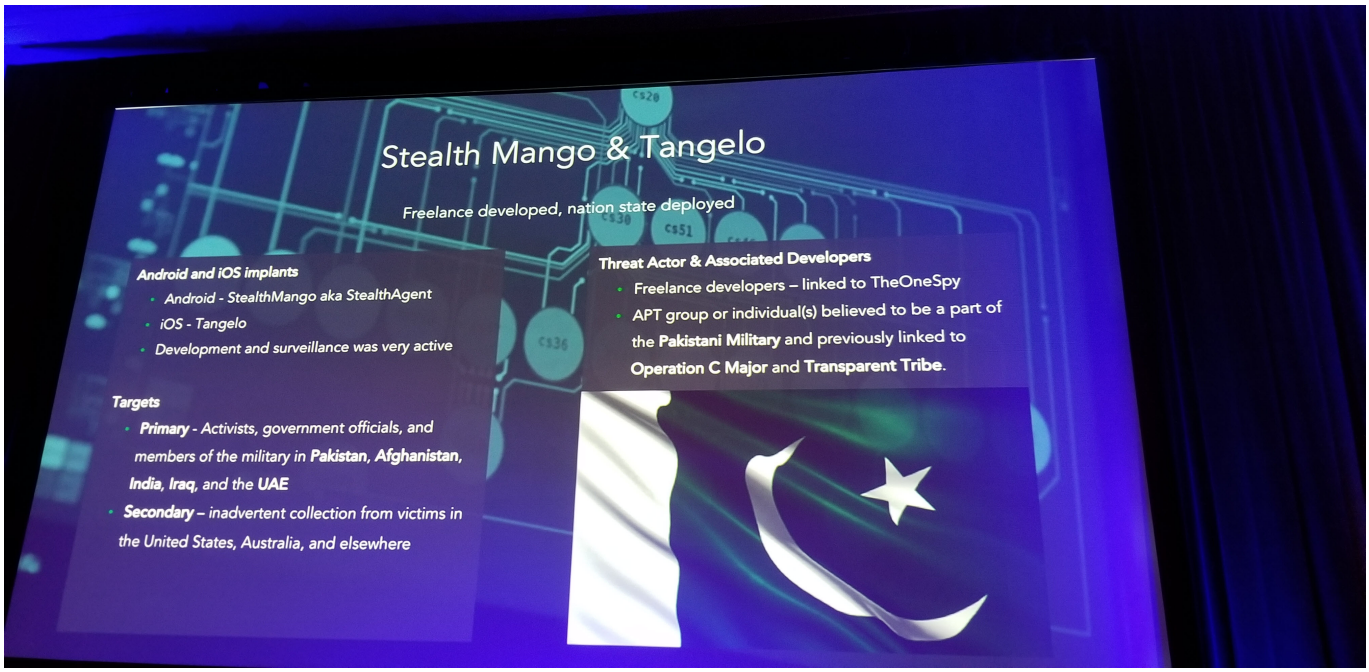
İkinci gün ise yine aynı yoğunlukta ve tempoda kaldığı yerden devam etti. İkinci günün en çok beğendiğim sunumları ise;

6. Son yıllarda oldukça popüler olan yanıltma (deception) teknolojilerinin nasıl tespit edilip atlatılabileceğini konu alan Real Eyes, Realize, Real Lies: Beating Deception Technologies sunumu,

7. Sesli doğrulama/tanıma sistemlerinin makine öğrenmesi (machine learning) ile nasıl atlatılabildiğini gösteren Your Voice is My Passport sunumu,

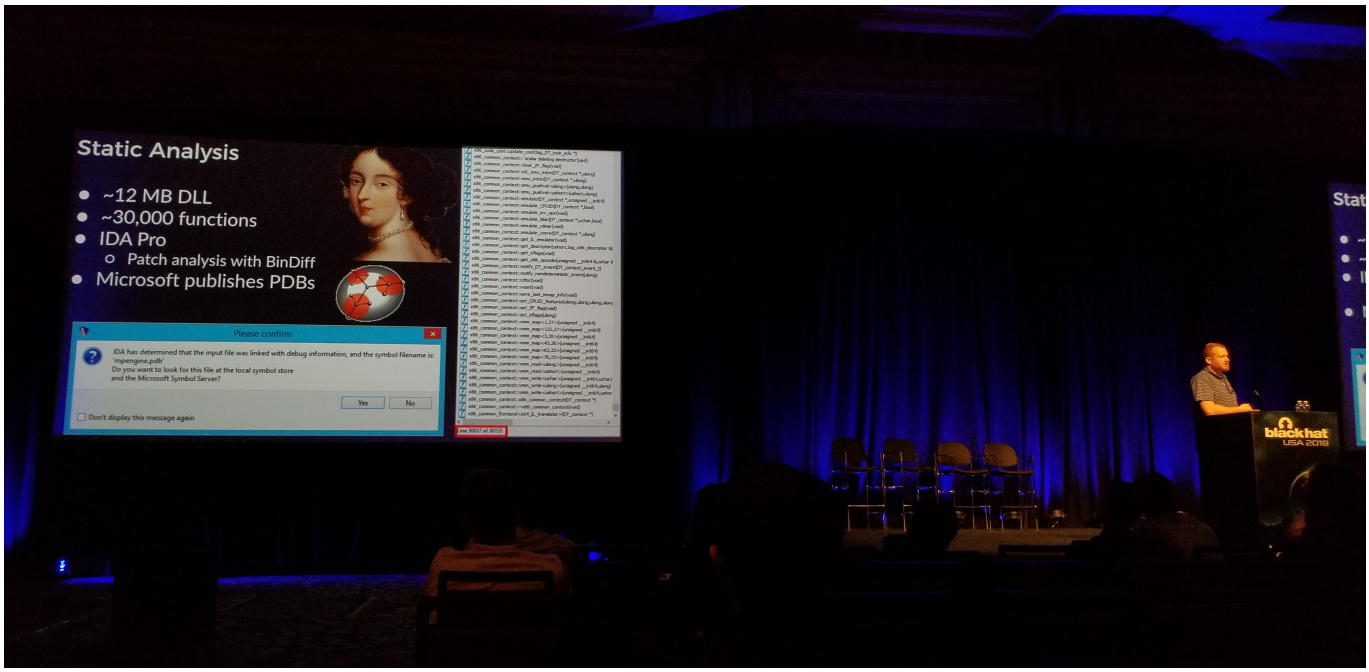


8. Devlet destekli siber saldırılarda kullanılan Stealth Mango ve Tangelo isimli mobil casus yazılımların analizini konu alan Stealth Mango and the Prevalence of Mobile Surveillanceware sunumu,



9. Sızma testlerinde sıklıkla kullanılan meşhur mimikatz aracının geliştiricisi Benjamin Delpy'in gerçekleştirdiği, DCShadow saldırısı ile Active Directory'i ele geçirmeye imkan tanıyan So I became a Domain Controller sunumu,

10. Windows Defender'ın antivirüs öykünücüsünün (emulator) derinlemesine analinizin yer aldığı Windows Offender: Reverse Engineering Windows Defender's Antivirus Emulator sunumu,



Emek ve zaman harcanarak gerçekleştirilen güvenlik araştırmalarını konu alan birbirinden faydalı, değerli sunumları, atmosferi ve anıları ile beni oldukça tatmin ve memnun eden bir Black Hat USA konferası daha geride kaldı. 2016 yılındaki blog yazımın sonunda, Cherokee Jeep'i hackleyerek ünlerine ün katan Charlie Miller ve Chris Valasek ile olan fotoğrafıma yer vermiştim. Bu yazının kapanışını da siber güvenlik camiasının yakından tanıdığı, F-Secure firmasının CRO'su Mikko Hyppönen ile olan fotoğrafım ile son vermek istedim.

3-8 Ağustos 2019’da Black Hat USA’de görüşmek hayaliyle (totem) herkese güvenli günler dilerim.

black hat
USA 2019
SAVE THE DATE
AUGUST 3–8, 2019
MANDALAY BAY CONVENTION CENTER
HOTEL LOBBY
CASINO
EVENT CENTER
RESTAURANTS
PARKING GARAGE
TRAM
EXIT
EXIT
WEBROOT