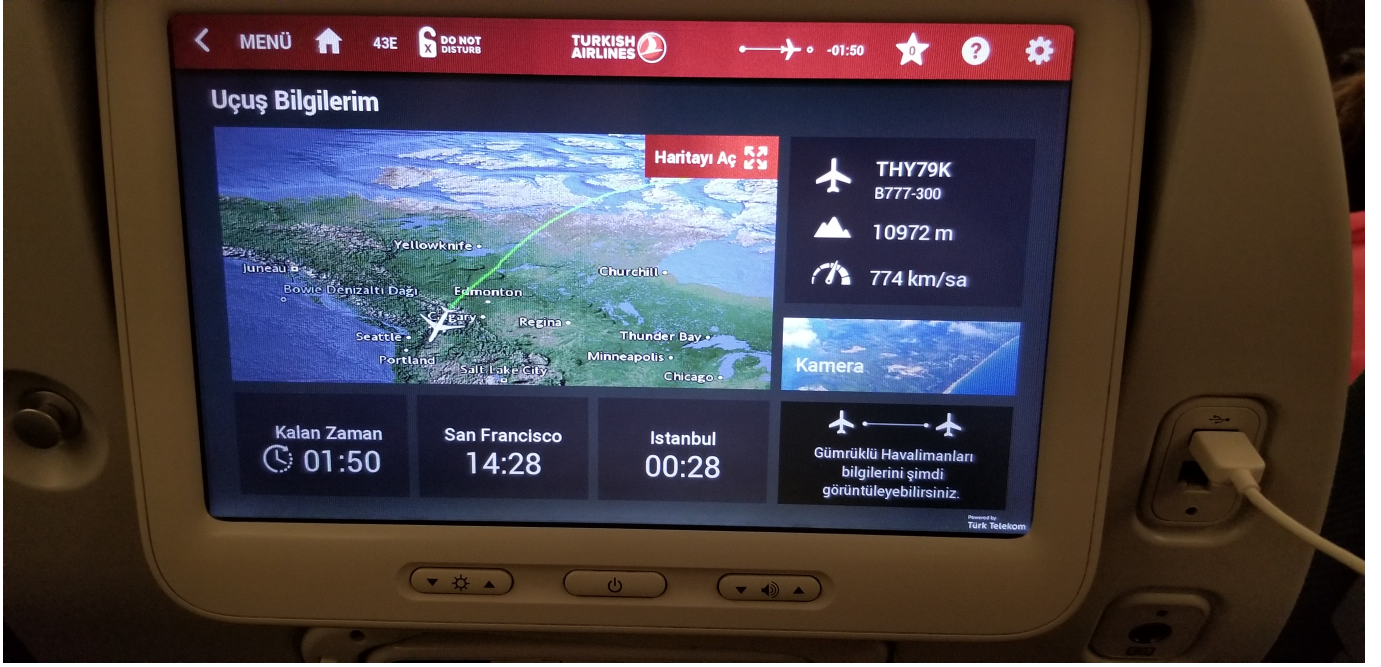


Black Hat USA 2018

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. :)









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 gözümünden 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. :)



Mert SARICA

@MertSARICA



İmkanım olsa uçak kaldırırim biliyorsunuz ama yok bu sebeple bloguma DoS saldırısı yapmazsanız sevinirim. :)

```
176.240.43.12 - - [08/Aug/2018:10:32:26 +0300] "GET /?q=bizi_black_hat_a_gotur HTTP/1.1" 301 178 "-"
"python-requests/2.18.4"
176.240.43.12 - - [08/Aug/2018:10:32:26 +0300] "GET /?q=bizi_black_hat_a_gotur HTTP/1.1" 301 178 "-"
"python-requests/2.18.4"
176.240.43.12 - - [08/Aug/2018:10:32:26 +0300] "GET /?q=bizi_black_hat_a_gotur HTTP/1.1" 301 178 "-"
"python-requests/2.18.4"
176.240.43.12 - - [08/Aug/2018:10:32:26 +0300] "GET /?q=bizi_black_hat_a_gotur HTTP/1.1" 301 178 "-"
"python-requests/2.18.4"
176.240.43.12 - - [08/Aug/2018:10:32:26 +0300] "GET /?q=bizi_black_hat_a_gotur HTTP/1.1" 301 178 "-"
"python-requests/2.18.4"
176.240.43.12 - - [08/Aug/2018:10:32:26 +0300] "GET /?q=bizi_black_hat_a_gotur HTTP/1.1" 301 178 "-"
"python-requests/2.18.4"
```

18:30 - 8 Ağu 2018

48 Beğeni



2



48



Konferans günü gelip çıktığında, 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 mdr Parisa Tabriz ıktı. Parisa Tabriz konuması esnasında getiđimiz ay hayata geen ve HTTPS olmayan sitelerin Chrome internet tarayıcısı tarafından gvensiz olarak etiketlenmesinin internet gvenliđi adına başarıya ulatıđından bahsetti. Benzer ekilde Project Zero'nun 90 gnlk zafiyet yayınlama politikasının (90 day disclosure policy) da bata reticiler tarafından memnuniyetsizlikle karılandıđını ancak Google'ın bu konuda geri adım atmaması sayesinde tespit ettikleri zafiyetlerin %98'inin 90 gn iinde reticiler tarafından giderildiđini belirtti. Dileyenler muazzam aılı videosunu aađıdan, aılı konumasının tamamını ise buradan izleyebilirler.



Getiđimiz yıllarda olduđu gibi yine paralelde ilgimi eken ok sayıda sunum olması sebebiyle Black Hat USA'in mobil uygulaması zerinden hangi sunumlara katılacađıma karar vermekte glk ektim.



Briefings

Çar 8

Per 9



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

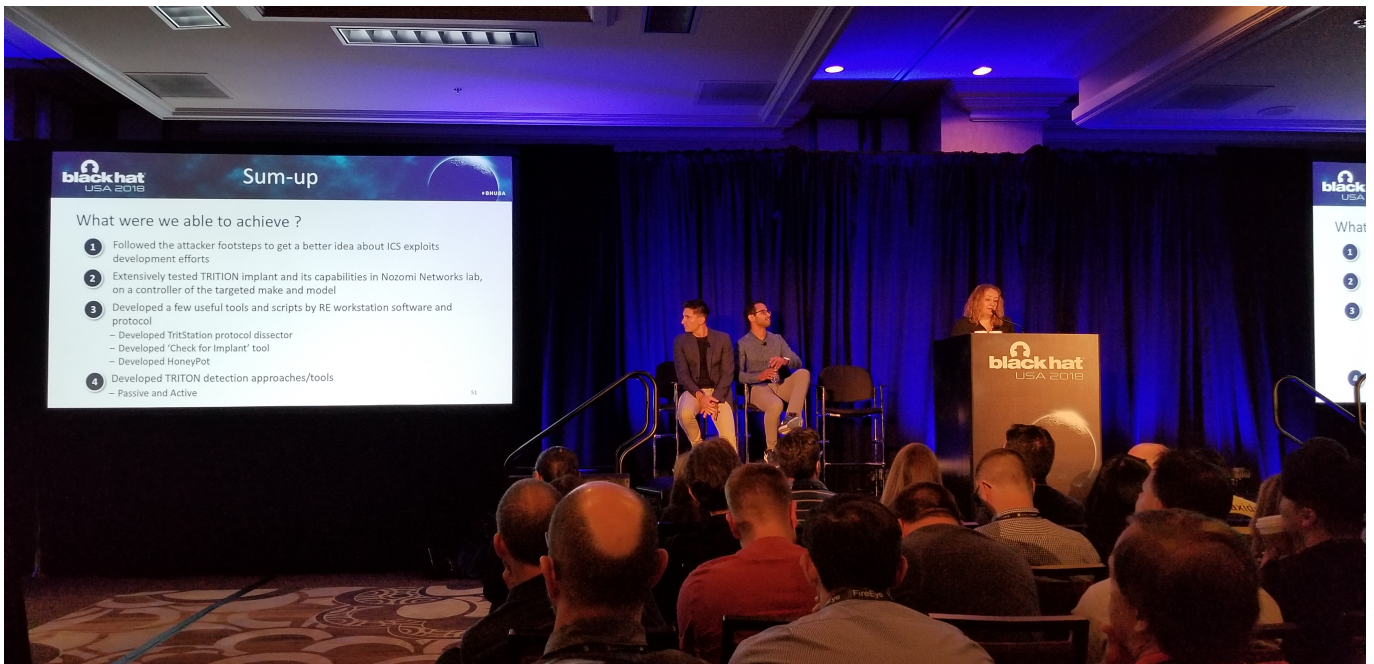


Çoğu sunumun, sunum dosyası yayınlandığı için her bir sunuma ayrı ayrı değinmeden her birinini ayrı ayrı incelemenizi tavsiye edebilirim. İlk günün en çok beğendiğim sunumlarını sıralayacak olursam;

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,



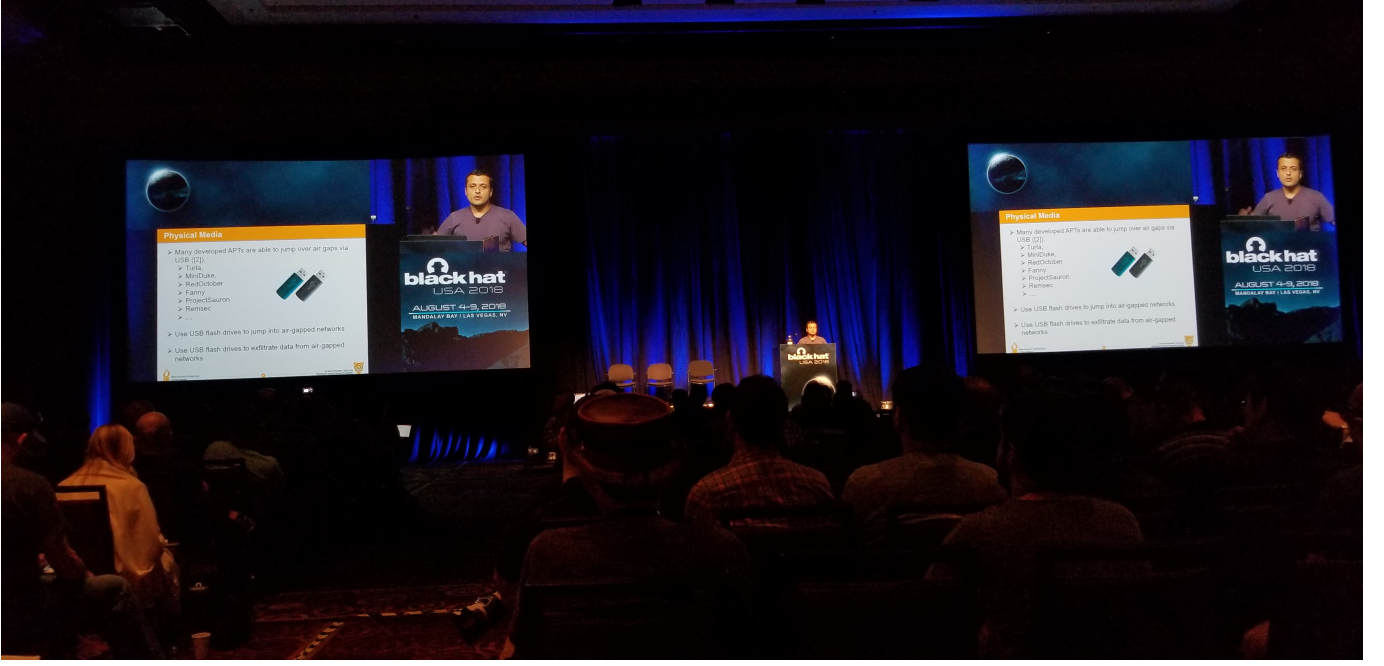
3. Donanım yazılımlarına (firmware) gerçekleştirilen çeşitli saldırı yöntemlerini ve tekniklerini konu alan Remotely Attacking System Firmware sunumu,



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



5. İsraili 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. :)











ARSENAL SCHEDULE

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	Lockpick by Joshua Pimpelli	Hunting Wargames with Arthur and Merlin in SC-land by Lior Kotlik	Hacking: An Attack Obfuscation Framework by Mike Hodges + Michelle Hodges	Micro-Renovator: Bringing Processor Firmware up to Code by Matt King	Deep Information Retrieval for Malware Searching System by Hongbin Ren + Wang Chao + Junyuan Zhao	DARWIN (Real World Use Cases for Covert Wireless) by Rob Miller + Ruzhishan D. Neukirch	MQT-PWN: Your IoT Sides-Army Knife by David Ables + Noora Zori	OWASP JoomScan Project by Mohammed Raza + Bilal Arif + Yehia Bahadran	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 Mmap Script Development by Simon Thomas	CyBot: Open-Source Threat Intelligence Chat Bot (Full Circle) by Terry Lee	OlympicSpy: Finding Data in Light Waves by Joe Grand	DELTA: SDN Security Evaluation Framework by Seungwon Lee + Jinsu Kim + Hwanseon Shin + Seungwon Woo	ML-Pat: An Effective Machine Learning Based Approach for PDF Malware Detection by Jason Chang	PA Tools: WireShark Plugins for Penetration by Jansen Matthei + Michael Stearns	BLE CTF Project by Ryan Hootman	ADA: Android Dynamic Analysis Tool by Andrius	Bloodhound 1.5 by Amy Robles + Roman Vachner	11:30-12:50
12:50-13:00	BREAK									12:50-13:00
13:00-14:20	VEX Validation Tool by Jonathan Peck + Remydij Armit	Codysmen Toolkit: Advanced System Monitoring Toolkit by Piotr Jaworski	ADFS: Active Directory Recon by Pieter Madsen	Armory by David Lamm	Objective-See's MacOS Security Tools by Patrick Wolfe	ANWI (ALL NEW WIRELESS IDS): THE 16 WIDS by Robert Korpe + Matthew Wells	WHID Injector and WHID Elite: A New Generation of HID Offensive Devices by Luke Bingham	Burp Replicator: Automate Reproduction of Complex Vulnerabilities by Paul Johnston	Walrus: Make the Most of Your Card Cloning Devices by Daniel Underlay + 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 Yi Wang + Jiahe Wang + Yu Zhou	Performing Live Forensics Without Killing Your Evidence by John Mann	POLAR: Accelerating the Search for Vulnerable Functions by Eric Cohn	Snake: The Malware Storage Zoo by Alex Fontaine	Firmware Audit: Platform Firmware Security Automation for BIOS, ROMs and OFW by Paul Smith + Lin Fisher	Dejavu: An Open Source Detection Framework by Brontis Harter + Hani Harter	Exploit: IoT Security Testing and Exploitation Framework by Brontis Harter + Hani Harter	Astra: Automated Security Testing For REST APIs by Arjun Bhargava + Sage Patel + Preet Kulkarni	SCODA: Smart Contract Defender and Analyzer by Ajit Hota	14:30-15:50
15:50-16:00	BREAK									15:50-16:00
16:00-17:20	ThreatPlaybook by Andrew Blagov + Shreshth Kumar	LogonTrac by Tomislav Hec + Shreshth Kumar	Redkiss OS (MM): A Virtual Machine for Adversary Emulation and Threat Hunting by Suchanhu Chaudhary	Chiron: An Advanced IPSEC Security Assessment and Penetration Testing Framework by Antonio Alsas	Kemon: An Open-Source Pre and Post-Exploitation Framework for macOS Kernel Monitoring by Yu Wang	Cloud Security Suite: One Stop Tool for AWS/GCP/Azure Security Audit by Jaganathan + David Lee + Shreshth Kumar	Damn Vulnerable iOS App: Swift Edition by Ramesh Ganesan	DataExploit 2.0 by Shubham Mittal	Puma Scan by Eric Johnson + Eric Mead	16:00-17:20
17:20-18:00	BUSINESS HALL RECEPTION									17:20-18:00

ARSENAL THEATER

Wednesday, August 8

10:00-11:00	TROMMEL by Kyle O'Meara
11:15-12:15	Archery: Open Source Vulnerability by Anand Tiwari
12:30-13:30	WarBerryPi by Yannis Ioannides + Stella Constantinou
13:45-14:45	Ghost Tunnel: Covert Data Transfer by Hongjian Cao + Kunzhi Chai + Yuhang Li
15:00-16:00	GRFICS: A Graphical Real-time Framework for Incident Response by David Forbny
16:15-17:15	Project Interceptor: Owning the Network by David Melerdez
17:30-18:00	Business Hall Reception

ARSENAL THEATER

Wednesday, August 8

10:00-11:00	TROMMEL by Kyle O'Meara
11:15-12:15	Archery: Open Source Vulnerability by Anand Tiwari
12:30-13:30	WarBerryPi by Yiannis Ioannides + Stella Constant
13:45-14:45	Ghost Tunnel: Covert Data Exfiltration by Honglan Cao + Kunshu Chai + Y
15:00-16:00	GRFICS: A Graphical Realistic Framework by David Formy
16:15-17:15	Project Interceptor: Owning the Network by David Melendez
17:30-18:00	Business Hall Reception

14:30-15:30	VWorks System by Yu Wang + Joshua Wang + Yu Zeng	Killing Your Evidence by John Moran	Vulnerable Functions by Eran Cattan	by Alex Komarov	Security Automation for Blue Teams and OSINT by Paul Fisher + Leo Fisher	Framework by Bhaskar Patel + Harsh Narasimhan	and Exploitation Framework by Aaron J. Storer	REST APIs by Arjun Bhargava + Rajat Patel + Pratik Kulkarni	and Analyzer by AJH Hall	14:30-15:30
15:30-16:00	BREAK									15:30-16:00
16:00-17:30	ThreatPlaybook by Nishu Shrivastava + Shashank Kumar	LogonTracer by Kenneth Tait + Stuart Tennings	RedHunt OS (VM): A Virtual Machine for Adversary Simulation and Threat Hunting by Ioan-Maria Ciocan	Chimera: An Advanced IPv6 Security Assessment and Penetration Testing Framework by Ioan-Maria Ciocan	Kernon: 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 Joseph Chaudhary + Shreyas + Shrinivas Madan	Damn Vulnerable iOS App: Swift Edition by Puneet Chaudhary	DataSploit 2.0 by Shashank Kumar	Puma Scan by Eric Johnson + Eric Most	16:00-17:30
17:30-19:00	BUSINESS HALL RECEPTION									17:30-19:00

Thursday, August 9

Open to All Pass Types

Station	1	2	3	4	5	6	7	8	9	Station
10:00-11:00	SQL by Kelly Cusack	PostgreSQL (Postgres): Collecting & Hunting for IOCs with Qusto and Data by Ioan-Maria Ciocan + Scott Suberland	DSP: Docker Security Playground by Simon Patro Romanos	PowerUpSQL: A Powercat Toolkit for Attacking SQL Servers in Enterprise Environments by Scott Suberland	ERTotal by Nishu Shrivastava + Nishu Shrivastava	MLSploit: Realistic ML Platform - Advanced Deep Learning Through Facial Recognition by Li Chen + Esh Vaid	Social Mapper: Social Media Correlation Through Facial Recognition by Esh Vaid	A Look at ModSec 3.0 for NGFW: A Software Web Application Firewall by Esh Vaid	OWASP Dependency-Check by Jeremy Long	10:00-11:00
11:00-11:30	BREAK									11:00-11:30
11:30-12:00	Jackhammer: One Security Framework to Rule Them All by Ioan-Maria Ciocan	Red: Do You Bro? Red Teaming to Export to Red Hat by Ioan-Maria Ciocan	RID Hijacking: Maintaining Access on Windows Machines by Sebastian Castro	Chimera: A Virtual Machine for Adversary Simulation and Threat Hunting by Ioan-Maria Ciocan	Art of Dealing with Shodan: Best Practices of API Abuse by Ioan-Maria Ciocan	Chimera: A Virtual Machine for Adversary Simulation and Threat Hunting by Ioan-Maria Ciocan	An Extensible Dynamic Analysis Framework for IoT Devices by Esh Vaid	WSAT by Ioan-Maria Ciocan	CoffeeShot: Avoid Detection with Memory Injection by Ioan-Maria Ciocan	11:30-12:00
12:00-13:00	BREAK									12:00-13:00
13:00-14:00	SQL by Kelly Cusack	PostgreSQL (Postgres): Collecting & Hunting for IOCs with Qusto and Data by Ioan-Maria Ciocan + Scott Suberland	DSP: Docker Security Playground by Simon Patro Romanos	PowerUpSQL: A Powercat Toolkit for Attacking SQL Servers in Enterprise Environments by Scott Suberland	ERTotal by Nishu Shrivastava + Nishu Shrivastava	MLSploit: Realistic ML Platform - Advanced Deep Learning Through Facial Recognition by Li Chen + Esh Vaid	Social Mapper: Social Media Correlation Through Facial Recognition by Esh Vaid	A Look at ModSec 3.0 for NGFW: A Software Web Application Firewall by Esh Vaid	OWASP Dependency-Check by Jeremy Long	13:00-14:00
14:00-14:30	BREAK									14:00-14:30
14:30-15:00	Jackhammer: One Security Framework to Rule Them All by Ioan-Maria Ciocan	Red: Do You Bro? Red Teaming to Export to Red Hat by Ioan-Maria Ciocan	RID Hijacking: Maintaining Access on Windows Machines by Sebastian Castro	Chimera: A Virtual Machine for Adversary Simulation and Threat Hunting by Ioan-Maria Ciocan	Art of Dealing with Shodan: Best Practices of API Abuse by Ioan-Maria Ciocan	Chimera: A Virtual Machine for Adversary Simulation and Threat Hunting by Ioan-Maria Ciocan	An Extensible Dynamic Analysis Framework for IoT Devices by Esh Vaid	WSAT by Ioan-Maria Ciocan	CoffeeShot: Avoid Detection with Memory Injection by Ioan-Maria Ciocan	14:30-15:00
15:00-15:30	SQL by Kelly Cusack	PostgreSQL (Postgres): Collecting & Hunting for IOCs with Qusto and Data by Ioan-Maria Ciocan + Scott Suberland	DSP: Docker Security Playground by Simon Patro Romanos	PowerUpSQL: A Powercat Toolkit for Attacking SQL Servers in Enterprise Environments by Scott Suberland	ERTotal by Nishu Shrivastava + Nishu Shrivastava	MLSploit: Realistic ML Platform - Advanced Deep Learning Through Facial Recognition by Li Chen + Esh Vaid	Social Mapper: Social Media Correlation Through Facial Recognition by Esh Vaid	A Look at ModSec 3.0 for NGFW: A Software Web Application Firewall by Esh Vaid	OWASP Dependency-Check by Jeremy Long	15:00-15:30

15:30-17:00

ARSENAL RECEPTION

15:00-16:00

GRFICS: A Graphical Realism

by David Farley

16:15-17:15

Project Interceptor: Owning A

by David Meisendor

17:30-19:00

Business Hall Reception

Thursday, August 9

10:00-11:00	Dradis Framework: Learn How to Use It by Daniel Martin
11:15-12:15	SimpleRisk by Josh Scott
12:30-13:30	JTAGulator: Uncovering the Achilles Heel by Joe Grand
13:45-14:45	Adversarial Robustness Toolbox for Machine Learning by Irena Năstăsescu
15:00-16:00	FireDrill: Adversarial Simulation Platform by Stephen Chavira
16:00-17:00	Arsenal Reception

ARSENAL ICON LEGEND

🟢 Tools

🟡 Hardware/Embedded

🔴 Tools

🟠 Social Engineering

🟢 Cryptography

🟡 Network

🔴 Malware

🟠 Deep OSINT/Security

🟢 Data Forensics and Incident Response

🟡 Digital Forensics

🔴 Malware Analysis

🟠 Mobile Security

🟢 Exploitation & Penetration Testing

🟡 Cloud

🔴 IoT

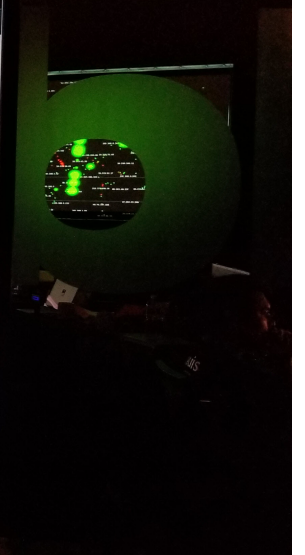
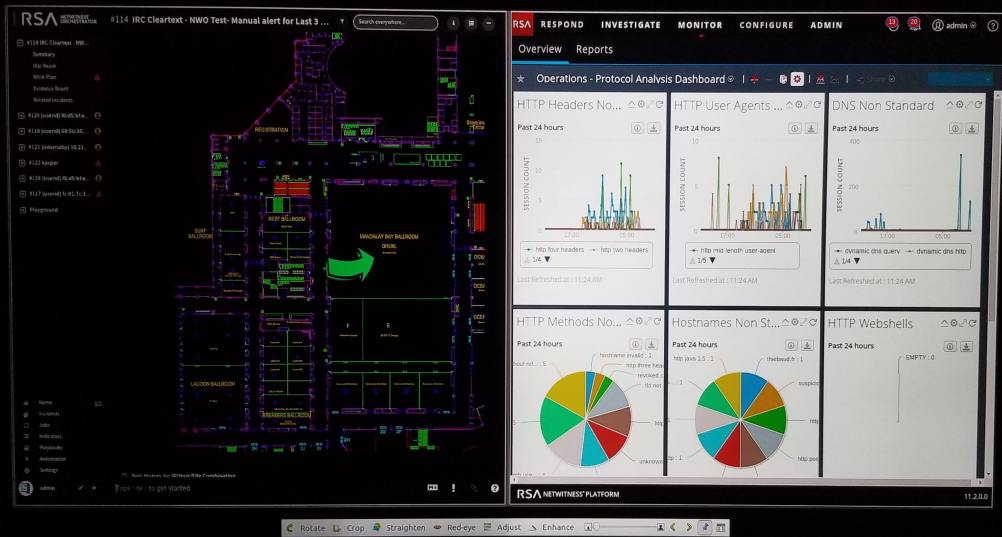
🟠 Web App



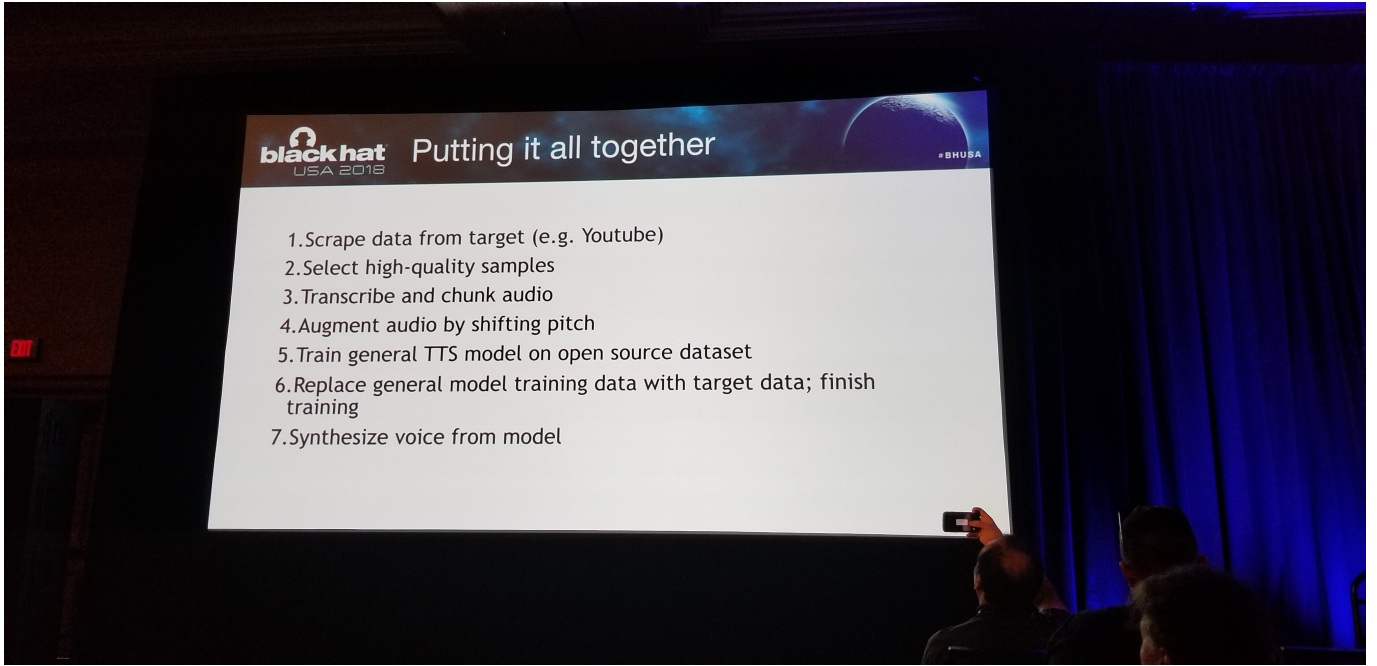
A black and white photograph of a sign on a chrome stand. The sign is for Black Hat USA 2018 and welcomes attendees to the Network Operations Center (NOC). The sign features a dark background with a moon in the top right and a mountain range at the bottom. The text is in white, with the main welcome message in large, bold, all-caps letters. The sign is mounted on a chrome stand with a circular base. The background shows a wooden door and a patterned carpet.

black hat
USA 2018

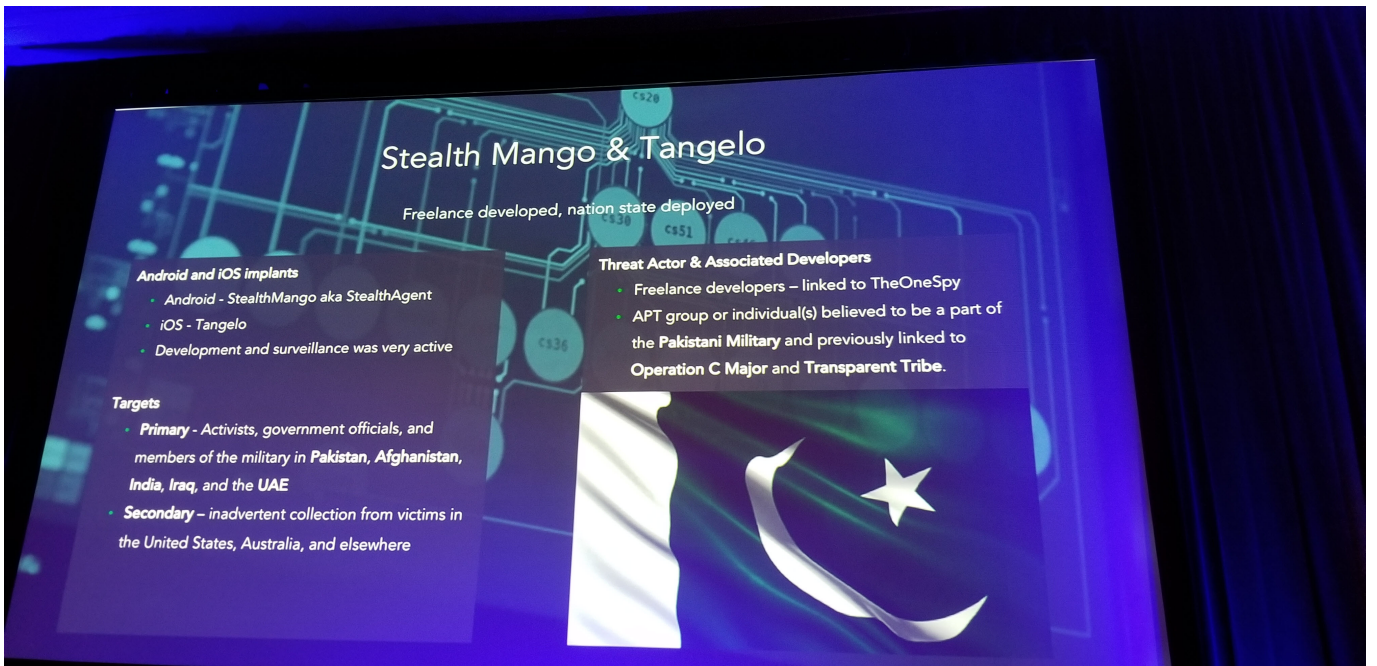
**WELCOME TO
THE BLACK HAT
NETWORK
OPERATIONS
CENTER (NOC)**







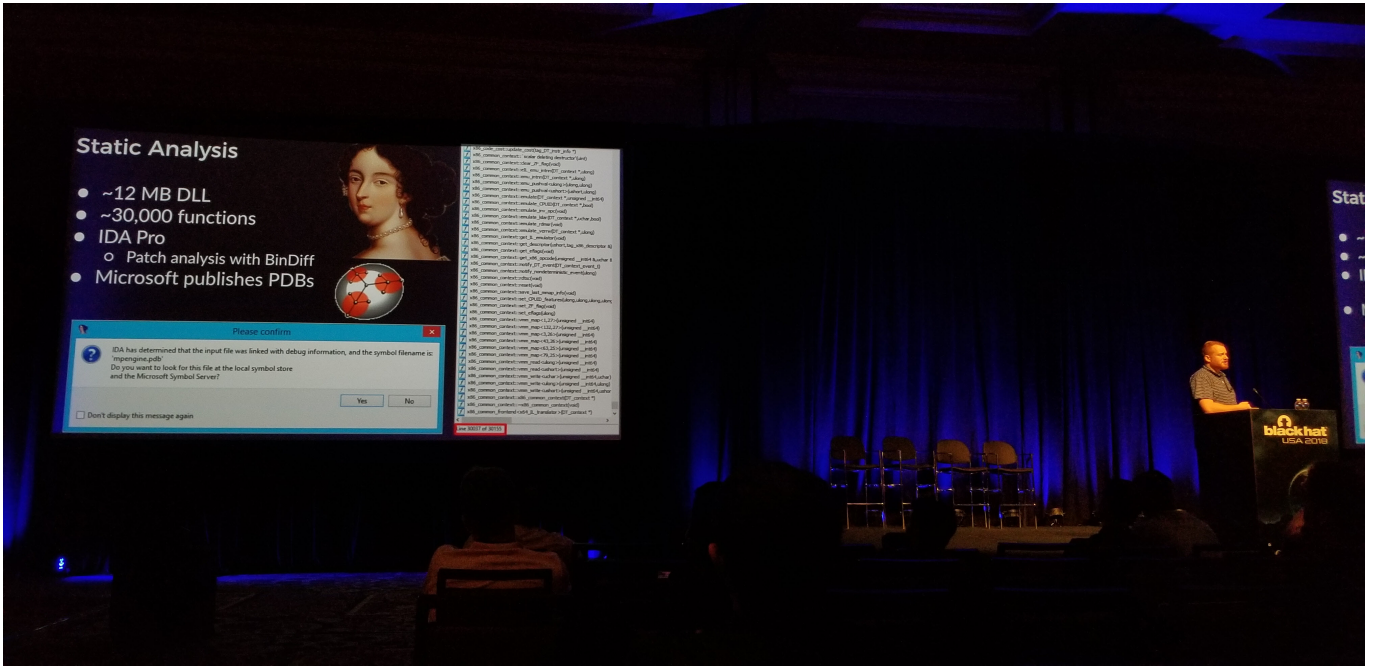
8. Devlet destekli siber saldırılarda kullanılan Stealth Mango ve Tangelo isimli mobil casus yazılımların analizini konu alan Stealth Mango and the Prevalence of Mobile Surveillanceware sunumu,



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 analizinizin 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 konferansı 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.



