

FireEye Cyber Defense Summit

written by Mert SARICA | 15 October 2017

Black Hat başta olmak üzere son 2 yılda 3 defa (#1, #2, #3) siber güvenlik konferanslarına katılmak için yolum Amerika'nın Nevada eyaletinin Las Vegas kentine düşmüştü. Tam 2017 yılını es geçeceğimi düşünürken FireEye Türkiye Sorumlusu Ümit NADİM'den Eylül ayında beni oldukça heyecanlandıran bir davet aldım. Davetinde, Türkiye'den bir siber güvenlik araştırmacısını FireEye'in her yıl Ekim ayı gibi düzenlenen FireEye Cyber Security Summit siber güvenlik konferansına götürmek istediğini belirtiyordu. Uzun yıllardır FireEye ürünlerini kullanıp Mandiant'ın da başarılı çalışmalarının yer aldığı tehdit raporlarını yakından takip eden bir güvenlik uzmanı olarak, Mandiant'ın sunumlarını yakından izleyebilme şansına erişebilecek olmak beni oldukça mutlu etti ve çok düşünmeden daveti kabul ettim.

8 Ekim tarihinde Ümit NADİM'in liderliğinde 8 kişilik bir katile olarak San Francisco aktarmalı olarak Las Vegas'a gitmek üzere yola çıktık. Seyahat her zaman olduğu gibi oldukça uzun ve yorucuydu. Saatte 30 KM hızla esen rüzgara karşı Las Vegas'ın McCarran Uluslararası Havalimanı'na pilotun uçağı oldukça zor şartlarda indirmesi, yüreğimizi ağzımıza getirdi. Havalimanından çıktığımızda her zaman olduğu gibi Las Vegas yine o müthiş ihtişamı ile bizi karşıladı. Sabah saat 9'da çıktığım evimden, Las Vegas'ın o meşhur Ocean's 11 filmine de konu olmuş Bellagio oteline yerleşmem tam tamına 28 saat sürmüştü.











9 Ekim sabahı konferans için kaydımızı yaptırmak için Ümit Bey ile otelin asansöründen çıktığımızda karşımızda bir anda FireEye'ın CEO'su Kevin Mandia'yı ve CTO'su Tony Cole'yi gördük. Kendileri ile kısa bir süre sohbet ettikten sonra Kevin Mandia ile o anı ölümsüzleştirmek için bir fotoğraf çekilmeyi de ihmal etmedik. :) Yolumuzun üzerinde olan Bellagio'nun botanik bahçesini de hızlıca gezdikten sonra konferansa kaydımızı yaptırmak için kayıt ofisinin yolunu tuttuk ve konferans programı ile yaka kartlarımızı aldık. Akşam düzenlenen Merhaba Resepsiyonu'na da katıldıktan sonra o günü güzel bir akşam yemeği ile tamamladık.







8:46 AM

October 10, 2017

BELLAGIO
CONVENTION
CENTER

MAP IT ►

Andrew's Distributing

WHEN: 9:00am - 12:00pm

WHAT: Meeting

WHERE: Executive Boardroom

MAP IT ►

Crounse and Skarshinski Wedding

WHEN: 1:00pm - 2:30pm

WHAT: Crounse and Skarshinski Wedding

WHERE: South Chapel

MAP IT ►

FireEye Cyber Defense Summit 2017

WHEN: 12:00pm - 8:00pm

WHAT: Registration

WHERE: Registration Desk 2

MAP IT ►

FireEye Cyber Defense Summit 2017

WHEN: 5:30pm - 7:30pm

WHAT: Exhibit Hall

WHERE: Grand Ballroom 4 - 9

Instructions:

Touch arrow keys to
manually advance through
event listings



MAP ►

Sales Office

Catering

Convention Services

Business Center

Registration

Restrooms

Wedding Chapel

Guest Elevators

Emergency Exits



FireEye

CYBER DEFENSE SUMMIT

MIRAGE | 2017

PROGRAM GUIDE



OCTOBER 10-12, 2017 | BELLAGIO | LAS VEGAS

SUMMIT AGENDA

At-A-Glance



TUESDAY, OCTOBER 10

TIME	SESSION	ROOM
NOON - 8:00PM	Registration Open	Registration Desk 2
5:30PM - 7:30PM	Welcome Reception / FireEye Expo	Grand Ballroom 4 - 9

WEDNESDAY, OCTOBER 11

TIME	SESSION	ROOM
6:30AM - 5:30PM	Registration Open	Registration Desk 2
7:00AM - 9:00AM	Breakfast / FireEye Expo	Grand Ballroom 4 - 9
9:00AM - 11:00AM	Keynote Presentations: Kevin Mandia FireEye Company Overview Grady Summers FireEye Technology Overview John Watters FireEye Services Overview	Bellagio Ballroom
11:00AM - 11:30AM	Coffee Break / FireEye Expo	Grand Ballroom 4 - 9
11:30AM - 12:30PM	Guest Speaker: Kurt Warner, Hall of Fame Quarterback, Football Analyst and Philanthropist	Bellagio Ballroom
12:30PM - 2:00PM	Lunch / FireEye Expo	Grand Ballroom 4 - 9
2:00PM - 4:00PM	Track One: Financial Track Two: Industrial Control Systems (ICS) Track Three: Government Track Four: Strategic Intelligence	Bellagio Ballroom Monet 3 & 4 Grand Ballroom 1 - 3 Monet 1 & 2
4:00PM - 4:30PM	Coffee Break / FireEye Expo	Grand Ballroom 4 - 9
4:30PM - 6:30PM	Track One: Financial Track Two: Industrial Control Systems (ICS) Track Three: Government Track Four: Strategic Intelligence	Bellagio Ballroom Monet 3 & 4 Grand Ballroom 1 - 3 Monet 1 & 2
6:30PM - 9:30PM	Cocktail Reception & Dinner	Bellagio Pool

THURSDAY, OCTOBER 12

TIME	SESSION	ROOM
7:00AM - 4:00PM	Registration Open	Registration Desk 2
7:00AM - 9:00AM	Breakfast / FireEye Expo	Grand Ballroom 4 - 9
9:00AM - 9:45AM	Keynote: David Hogue, Senior Technical Director NSA <i>A Day in the Life of NSA's Cybersecurity Operations Center (NCTOC)</i>	Bellagio Ballroom
9:45AM - 10:45AM	Customer Spotlight: Brian D. Cincera, Vice President, Global Information Security Pfizer <i>Cybersecurity Fitness: Keys to a Healthier Business</i>	Bellagio Ballroom
10:45AM - 11:15AM	Coffee Break / FireEye Expo	Grand Ballroom 4 - 9
11:15AM - 12:15PM	Industry Spotlight: Nadav Zafrir, Co-Founder, CEO Team8 <i>Change Your Cyber State of Mind</i>	Bellagio Ballroom
12:15PM - 1:15PM	Lunch / FireEye Expo	Grand Ballroom 4 - 9
1:15PM - 3:15PM	Mandiant on the Frontlines Track Five: Technical Track Track Six: Management Track	Monet 3 & 4 Monet 1 & 2
3:15PM - 3:45PM	Coffee Break / FireEye Expo	Grand Ballroom 4 - 9
3:45PM - 5:45PM	Mandiant on the Frontlines Track Five: Technical Track Track Six: Management Track	Monet 3 & 4 Monet 1 & 2
6:00PM - 8:00PM	Thank You Reception / FireEye Expo	Grand Ballroom 4 - 9

FRIDAY, OCTOBER 13 | SATURDAY, OCTOBER 14

TIME	SESSION	ROOM
8:00AM - 5:00PM	Post-Summit Training	Gauguin 1 Gauguin 2 Renoir 1 Renoir 2 Cezanne 1



10 Ekim olan konferansın ilk günü sabahında, Kevin Mandia'nın açılış konuşmasını dinlemek üzere hıncahınç dolu olan konferans salonunda yerimizi aldık. Oturan herkesin aksine size bol bol resim ve video çekmek için en

arkada dikilmenin karşılığını fazlasıyla aldım ve Kevin Mandia'nın konuşmasının ilk 5 dakikasını sizler için kayıt ettim. ;)

Bir diğer CT0 olan Grady Summers sunumunda, çok sayıda güvenlik alarmları ile boğuşan güvenlik ekiplerinin iş yükünü azaltma ve akıllı alarmlara odaklanabilmelerini sağlama adına, FireEye'in Helix ürününün yeni özelliklerinden bahsetti. Özellikle alarmları mobil arayüzünden görüntüleyebilme özelliği oldukça hoşuma gitti.









Açılış konuşmalarından sonra katılabileceğim çok sayıda paralel oturum vardı. Bir sonraki gün gerçekleştirilecek olan Mandiant'ın teknik oturumunu dört gözle beklediğim için o gün Finans oturumuna katılmaya karar verdim. Küçümseyerek girdiğim Finans oturumu beni ilk sunumdan son sunuma kadar oldukça şaşırtıp, ters köşe yaptı. Tony Cole'un sunumuyla başlayan Finans oturumunda, APT grupları ile FIN APT gruplarının gerçekleştirdiği siber saldırılardaki ortak noktalar ve farklılık gözler önüne serildiği gibi FIN APT gruplarının gerçekleştirdiği siber saldırılarda kullandıkları yöntemlere ve saldırılardan korunma adına izlenmesi gereken yollara dikkat çekildi.





Tracking Targets to Attribute Operations

FINANCIAL TRACK



Advanced Persistent Threat
APT Groups



- ✓ Track 30+ APT Groups
- ✓ Nation-state sponsored, sophisticated, determined, and coordinated attackers



Enterprise Financial Criminals
FIN Groups



- ✓ Track 10 FIN Groups
- ✓ Enterprise cyber criminals

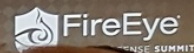


Identified Threat Groups



- ✓ Tracked 600+ other advanced threat actors
- ✓ Similar malware and activity to APT, tracking for development into FIN or APT group

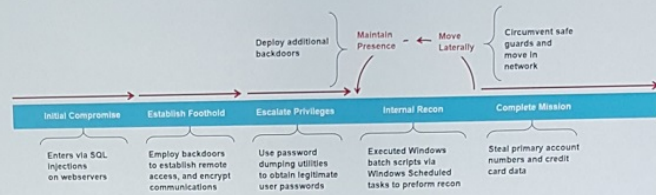
17 Copyright © FireEye, Inc. All rights reserved.



CHINA				RUSSIA / EASTERN EUROPE		KOREAN PENINSULA		HACKTIVISM	
33B Team	Talldoor Team	(APT24)		Koala Team	Fallout Team (South)		CYBERBERUT		
Bolo Team	Tailgaiter Team	TEMP-Tick		Sandstorm Team	DarkSide Activity (North)		SHALITA BOLTAI		
Barista Team	(APT17)	TEMP-Tombak		Tsai Team (APT28)	TEMP-Hermal (North)		CYBERCALPHATE		
(APT22)	Terrmille Team	TEMP-Tocuan		Turtle Team	Onoong Hwaleum (North)		UNBANKAN CYBER FORCES		
Calk Team (APT2)	Tevry Team	TEMP-Unclost		TEMP-Monkey (APT29)	TEMP-Raspeur (North)		ANONGHOSH		
Codicia Team	(APT20)	(APT26)		TEMP-Cossak			REDHACK		
Conic Team	Tamir Team	TEMP-Zhushuo				Vietnam			
Command Team	UPS Team (APT2)	(APT20)				OceanLotus (APT32)		YEMEN CYBER ARMY	
(APT1)	Walaby Team	TEMP-Zumbale		MIDDLE EAST				SYRIAN ELECTRONIC ARMY	
Conference Crew	(APT18)	TEMP-Waladomaru				SOUTH AMERICA		OPGREINIGHTS	
Conlimes Team	Wiggo Team (APT)	APT31				Andromeda Team		BITCH	
Cross Team	TEMP-Airmagars	APT6		Ajan Team (IR)		UNKNOWN		GODS SQUAD	
Flying Eagle Team	TEMP-Burthopper	APT7		Bassale Team (IR)				LAZARUS	
(APT15)	TEMP-Burmes	APT1		Bazari Team (IR)				GHIZAT SEC	
GREY Team (APT4)	TEMP-Battle	APT19		Chalor Team (IR)		Temp,Stratus		FINANCIAL CRIME	
Hippo Team (party)	(APT36)	APT16		Rammi/WhoDaddy (IR)		Zenithing Team			
to APT26)	TEMP-CCTV	APT23		TEMP-Lice (IR)				FIN6	
Mama Team	TEMP-DragonOK	APT27		TEMP-Omega (IR)		INDIA / PAKISTAN		FIN2	
Mompass Team	TEMP-Hus			TEMP-Schmittar (EGY)				FIN3	
(APT10)	TEMP-Hypnotize			TEMP-Hyena (LB)		Hangover Team (IR)		FIN4	
Nelson Team	TEMP-Hydrator			Handi Activity		TEMP-Angel (IR)		FIN5	
Roaming Tiger	(APT2)			Motelside Team (QW)		TEMP-Kalar (IR)		FIN6	
Sleets Campaign	TEMP-Overboard			Syrtaf Hwaleum Team (SY)		Hardcore Team (QW)		FIN8	
Social Network	TEMP-Pinkabook			APT33 (IR)		Tranchula Team (QW)		FIN9	
Team (APT15)	TEMP-Pleety Tiger					TEMP-Lapla (QW)		FIN10	

Cyber Crime Case: FIN2 Targeting Retail

FINANCIAL TRACK

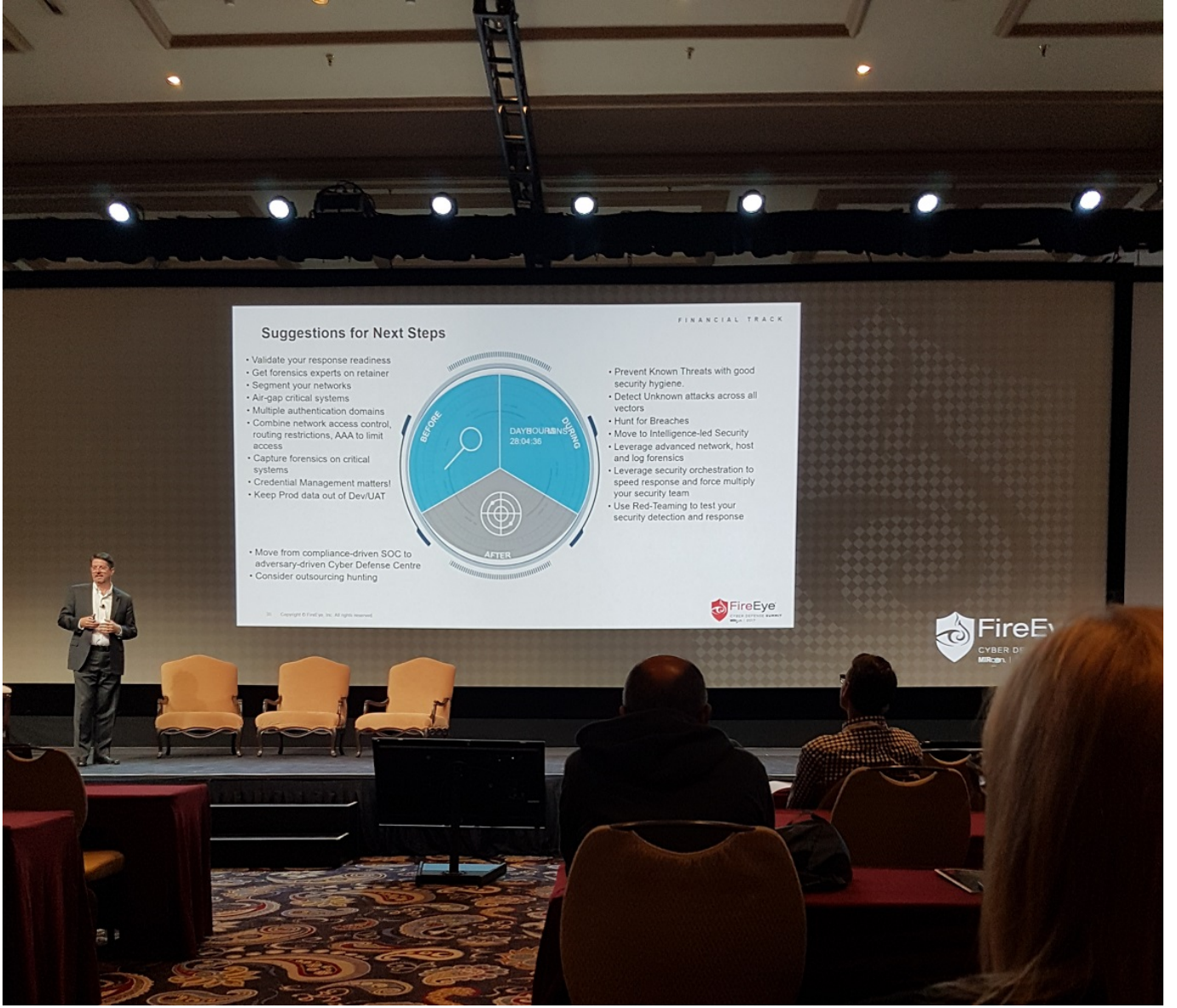


FIN2

- Targets: Financial sector and financial data
- Tools: Custom backdoors known as APOCALIPTO and LEAPFOG
- Tactics: Enters via SQL injections on web servers

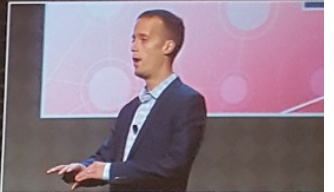
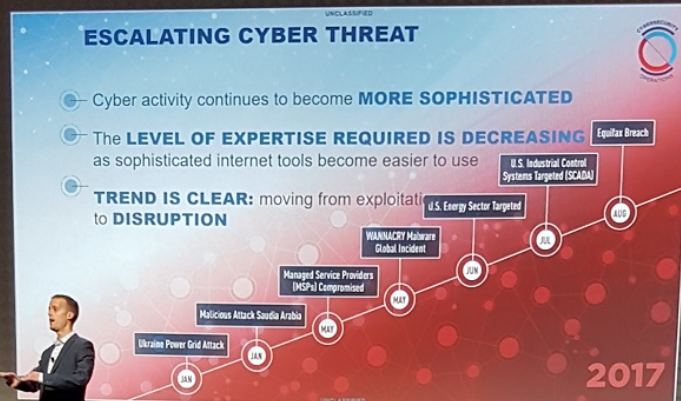
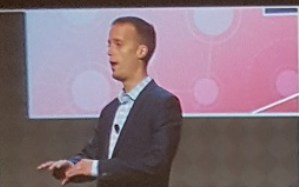
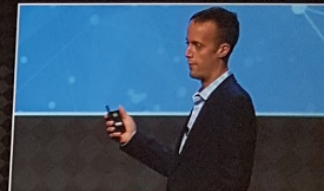
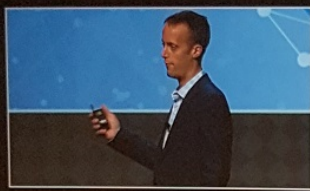
© 2013 FireEye, Inc. All rights reserved.





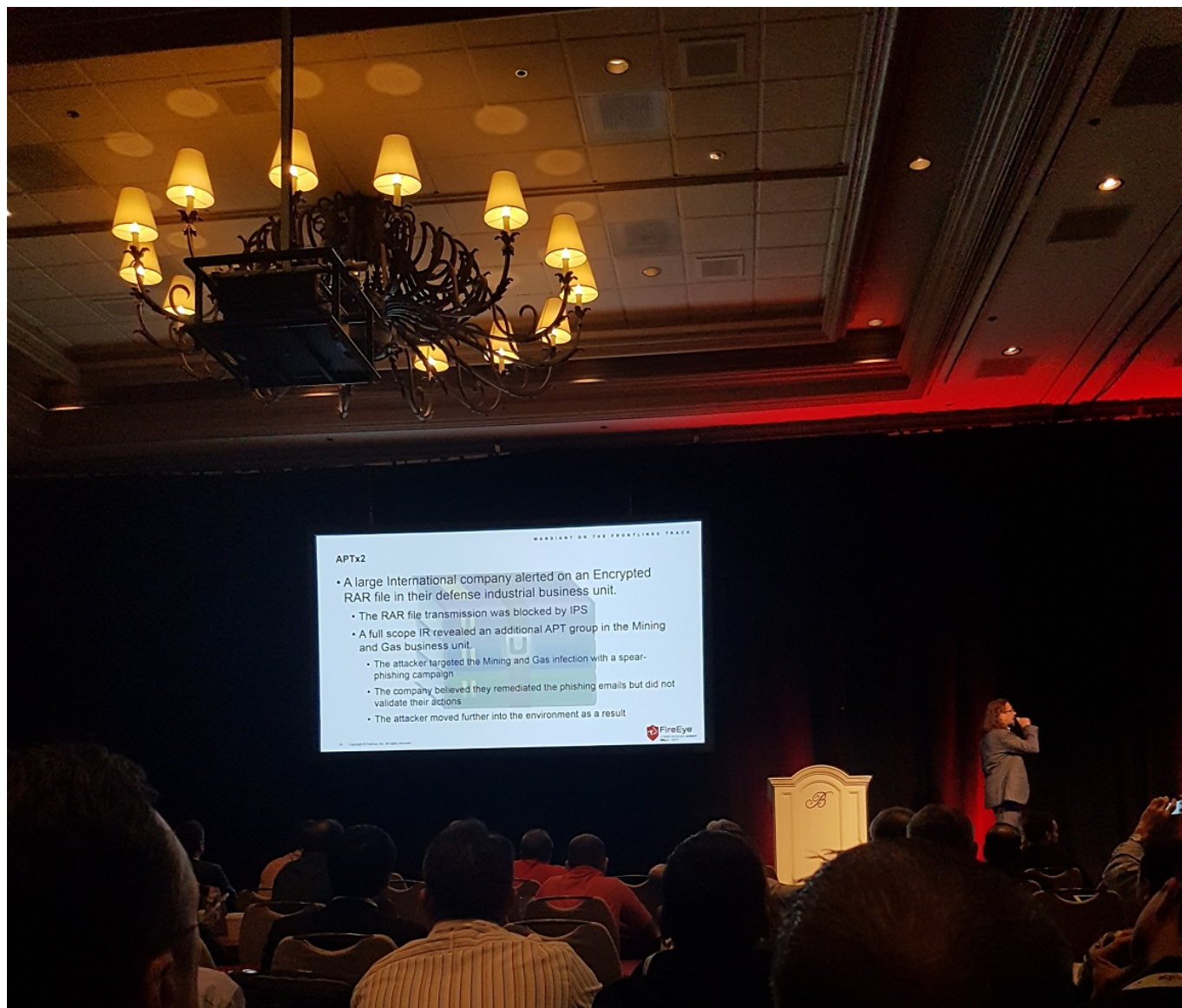
Konferansın ikinci gününde ise yine ilk olarak sahneye Kevin Mandia çıktı ve sözü çok uzatmadan konuşmasını yapmak üzere NSA'in SOC'undan sorumlu olan kıdemli teknik direktörü Dave Hogue'ye verdi. Söze ilk olarak NSA'in genele açık bir etkinlikte ilk defa sunum yaparak bir ilke imza attığını belirtti. İlk olmasından olsa gerek ki sunum oldukça sıradan ve sıkıcıydı. Aklımda kalan iki şeyden biri, bir zafiyet çıktığında tüm DoD'un veri merkezini 24 saat içinde zafiyete karşı tarayabildikleriydi. Diğeri ise izleyicilerden soru kabul etmeye başladığında bir izleyicinin "Peki son hacking vakalarından sonra nasıl toparlandınız?" sorusuna tabii ki "Yorum yok" yanıtını vermesiydi. :)







Sıra teknik oturuma geldiğinde ise sahneye ilk olarak Mandiant'ın en kıdemli bilgisayar olaylarına müdahale uzmanlarından Jeff Hamm çıktı. Yaptığı sunumda isim vermeden kurumların nasıl hacklendiklerini, hacklendiklerini nasıl öğrendiklerine, çıkarılan derslere ve bunlara karşı neler yapılması gerektiğine yer verdi. Anlatım dilinin esprili olmasının yanı sıra bilgisayar olaylarına müdahale esnasında geçen diyaloglara da sunumunda yer vermesi izleyenlere keyifli dakikalar geçirtti. Sunumunda özellikle kimi kurumların hacklendikten sonra bazı sistemlerinin varlığından o an itibariyle haberdar olmalarına dem vurarak, varlık envanterinin kurumlar tarafından sıkı takip edilmesi gerektiğinin altını önemle çizdi. (küresel sorun)



WANDERER ON THE FRONTLINES TRACK

APTx2

- A large International company alerted on an Encrypted RAR file in their defense industrial business unit.
- The RAR file transmission was blocked by IPS
- A full scope IR revealed an additional APT group in the Mining and Gas business unit.
- The attacker targeted the Mining and Gas infection with a spear-phishing campaign
- The company believed they remediated the phishing emails but did not validate their actions
- The attacker moved further into the environment as a result

FireEye





Broadcast Denied

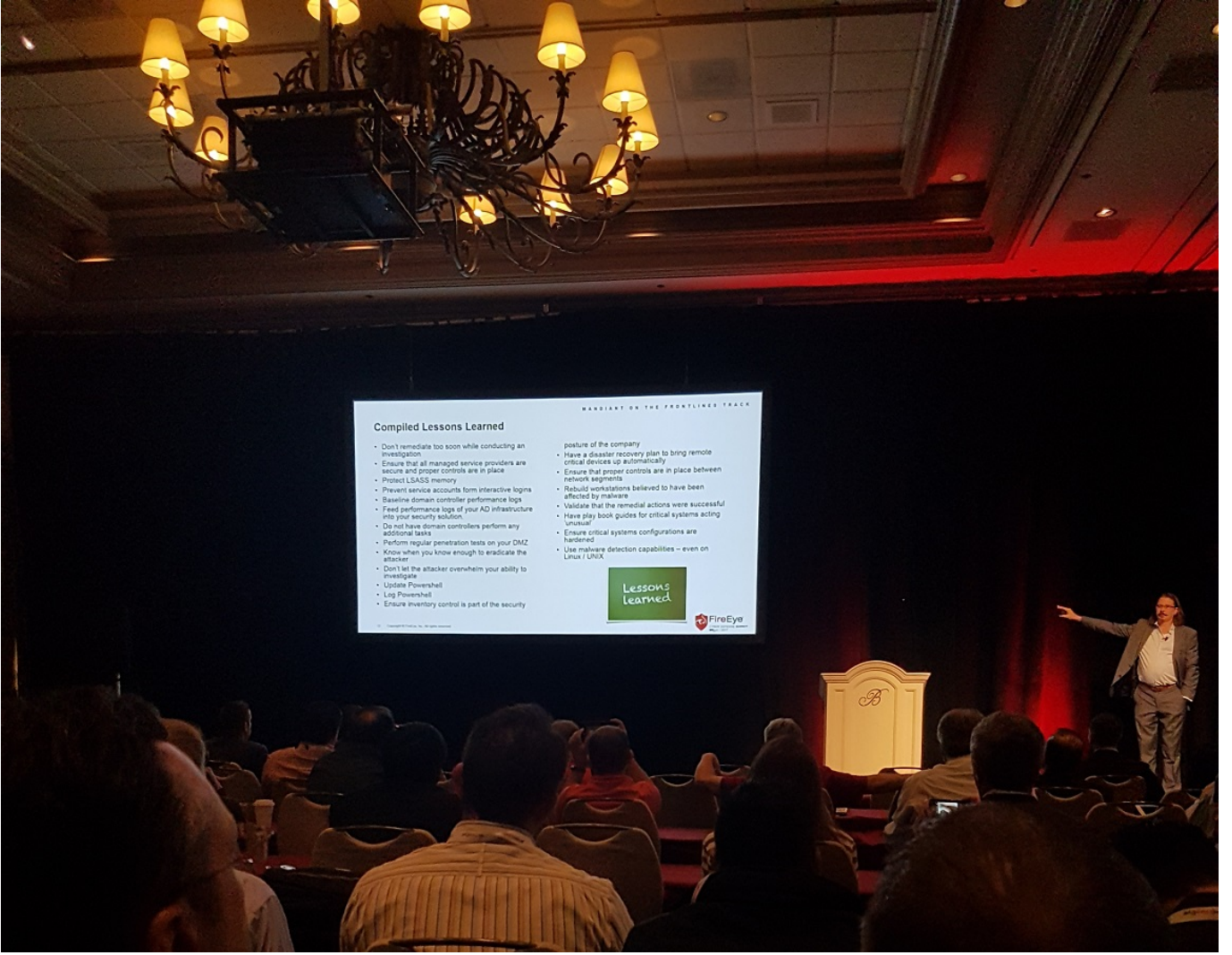
HARBINGER ON THE FRONTLINE TRACK

- Television Broadcasting Company had their repeaters crash just prior to an annual special event broadcast
- Proprietary systems were sent a remove network devices command
- The host name of the system sending the command was found early on
 - The IP address was unknown
 - The IP address assignment was DHCP and was not logged
 - A backup server had the mapping of the IP address, but the system was never located

© Copyright 2015, FireEye, Inc.

FireEye





Diğer bir sunumda ise Robert Wallace ve Alex Pennino sahneyi birlikte paylaştılar. Sunumlarında İran tarafından gerçekleştirildiği bilinen Newcaster APT saldırılarından elde ettikleri güncel bilgilere yer verdiler.

MANDIANT ON THE FRONTLINES | CYBER DEFENSE SUMMIT 2017

IRAN SO FAR AWAY

A VIEW FROM THE FRONTLINES OF RECENT IRANIAN
SPONSORED CYBER ATTACKS

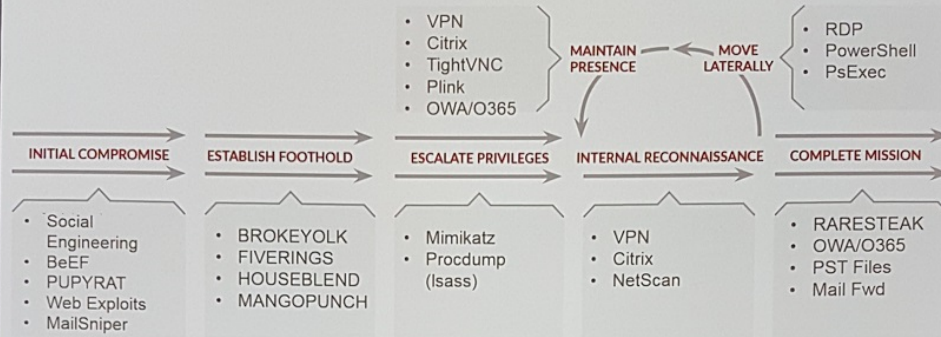
A ROBERT WALLACE + ALEX PENNINO JOINT | MANDIANT



COUNTRY PROFILE: IRAN

- Key cyber capabilities are suspected to be under control of IRGC
- Aggressive and destructive campaigns
- Contractors that conduct cyber warfare by proxy
- Continuing to grow their CNO capabilities
- What they lack in technical sophistication, they make up for in aggression

NEWSCASTER TEAM: ATTACK LIFECYCLE



MANDIANT ON THE FRONTLINES TRACK

NEWSCASTER TEAM MALWARE		
Family	Description	Availability
PUPYRAT	Pupy, a Python-based, open-source remote administration Trojan (RAT) used for post-exploitation environments, was leveraged on multiple occasions by Newscaster Team as a second-stage payload.	Public
BROKEYOLK	BROKEYOLK is a .NET downloader that downloads and executes a file from a hard-coded command and control (C&C) server. The malware communicates via SOAP (Simple Object Access Protocol) requests using HTTP.	Non-Public
FIVERINGS	FIVERINGS is a .NET data miner. This sample gathers system information and screen shots. It uploads the collected data to the command and control (C&C) server using HTTP web services.	Non-Public
HOUSEBLEND	HOUSEBLEND is a downloader also capable of executing shell commands provided by a hard-coded command and control (C2) server via HTTP.	Non-Public
MANGOPUNCH	MANGOPUNCH is a .NET backdoor that communicates using the HTTP POST method and encoded URI strings.	Non-Public
RARESTEAK	RARESTEAK is an uploader capable of sending .RAR files in the current directory to a command and control (C&C) address and port specified via the command line.	Non-Public

NEWSCASTER TEAM LESSONS

- *North Korea is new Iran and Iran is new China and China is new Russia and Russia is Fake News*
- Identified across almost every industry
- Massive email theft
- Simple to detect – difficult to remove

***These guys are like
the APT1 of 2017***

***– Alex Pennino,
March 2017***

NEWSCASTER TEAM LESSONS

- Disable Exchange ActiveSync (EAS) for privileged and service accounts
 - Review current policy to ensure only necessary domain accounts have EAS enabled
- Enforce Mailbox Audit Logging for specific high-value accounts
 - Logs mailbox access by owners, delegates and administrators
- Review Exchange Web Services (EWS) configuration
 - Potential for 2FA by-pass
 - Observed in the wild

Nick Carr ve Ben Withnell tarafından gerçekleştirilen bir diğer sunumda ise APT32 grubunun kullandığı taktik, teknik ve prosedürlere yer verildiği gibi bu saldırılarla nasıl mücadele edilebileceğine de sunum boyunca yer verildi.

MANDIANT ON THE FRONTLINES | CYBER DEFENSE SUMMIT 2017

APT32 and Beyond

Detecting the New Breed of Nation-State Attacks

Ben Withnell
Nick Carr

Copyright © 2017 FireEye, Inc. All rights reserved.



APT32 Targeting Private Sector Companies in Southeast Asia

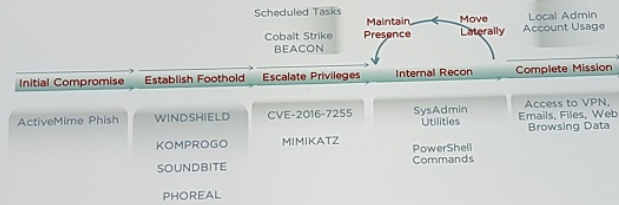
Year	Country	Sector	Malware
2016	US	Consumer Products	WINDSHIELD PHOREAL BEACON SOUNDBITE
2016	Vietnam	Media	WINDSHIELD
2016	China	Hospitality	WINDSHIELD
2016	Philippines	Technology Infrastructure	WINDSHIELD
2016	Vietnam	Banking	WINDSHIELD
2015	Philippines	Consumer products	KOMPROGO WINDSHIELD SOUNDBITE BEACON
2015	Vietnam	Media	WINDSHIELD
2014	Germany	Manufacturing	WINDSHIELD
2014	Vietnam	Network Security	WINDSHIELD

Table 1: Targeting table



APT32 Attack Lifecycle

MANDIANT ON THE FRONTLINES TRACK



How APT32 Gets In: Weaponized ActiveMime Phishing Docs

- 2017年员工工资性津贴统计报告.doc
 - (2017 Statistical Report on Staff Salary and Allowances)
- Thông tin.doc
 - (Information)
- Kế hoạch cứu trợ năm 2017.doc
 - (2017 Bailout Plan)
- Instructions to GSIS.doc
- Hoi thao truyền thông doc lập.doc
 - Traditional Games
- Phan Vu Tuân CV.doc
- HĐ DVPM-VTC 31.03.17.doc
- giấy yêu cầu bồi thường mới 2016 - hàng.doc
 - (New 2016 Claim Form)
- Hoa đơn chi tiết tiền nợ
 - (Debt Details)
- Danh sách nhân viên vi phạm kỷ luật.doc
 - (List of employee violations)
- Danh sách nhân viên làm việc sai quy định.doc
 - (List of employees working illegally)
- Nội dung quảng cáo.doc
 - (Internal content advertising)

MANDIANT ON THE FRONTLINES TRACK

-
- TRACKING IMAP FOLDER IMAP FILTERS MAIL MERGE GET STARTED...
- Search by email subject or recipient
- | | | | | | | |
|--|-----------------------|--|------------------------|--------------------|--|---|
| | an home.mateos@red.es | opened the attachment hola_1.0.jpg on May 6 | an subject: [redacted] | on May 6, 1:26 am | <input type="button" value="Stop Tracking"/> | <input type="button" value="All Emails"/> |
| | an home.mateos@red.es | opened the message on May 10, 3:27 am | an subject: [redacted] | on May 10, 3:29 am | <input type="button" value="Stop Tracking"/> | <input type="button" value="All Emails"/> |
| | an home.mateos@red.es | opened the message on May 10, 3:27 am | an subject: [redacted] | on May 10, 3:27 am | <input type="button" value="Stop Tracking"/> | <input type="button" value="All Emails"/> |
| | an home.mateos@red.es | opened the message on May 10, 3:26 am | an subject: [redacted] | on May 10, 3:26 am | <input type="button" value="Stop Tracking"/> | <input type="button" value="All Emails"/> |
| | an home.mateos@red.es | opened the message on May 10, 3:26 am | an subject: [redacted] | on May 10, 3:26 am | <input type="button" value="Stop Tracking"/> | <input type="button" value="All Emails"/> |
| | an home.mateos@red.es | opened the message on May 10, 3:10 am | an subject: [redacted] | on May 10, 3:10 am | <input type="button" value="Stop Tracking"/> | <input type="button" value="All Emails"/> |

```
1169 <p class=3D'JdHsoNormal'><span style=3D'mso-no-proof:yes'><img width=3D30155 height=3D30155
1170 id=3D'30'_x0000_11025' src=3D'http://job.supperpow.com:80/pd/fans/mitsumi/a550=
1171 .jpg'
1172 alt=3D'http://job.supperpow.com:80/pd/fans/mitsumi/a550.jpg'></span></p>
```



MANDIANT ON THE FRONTLINES TRACK

- 

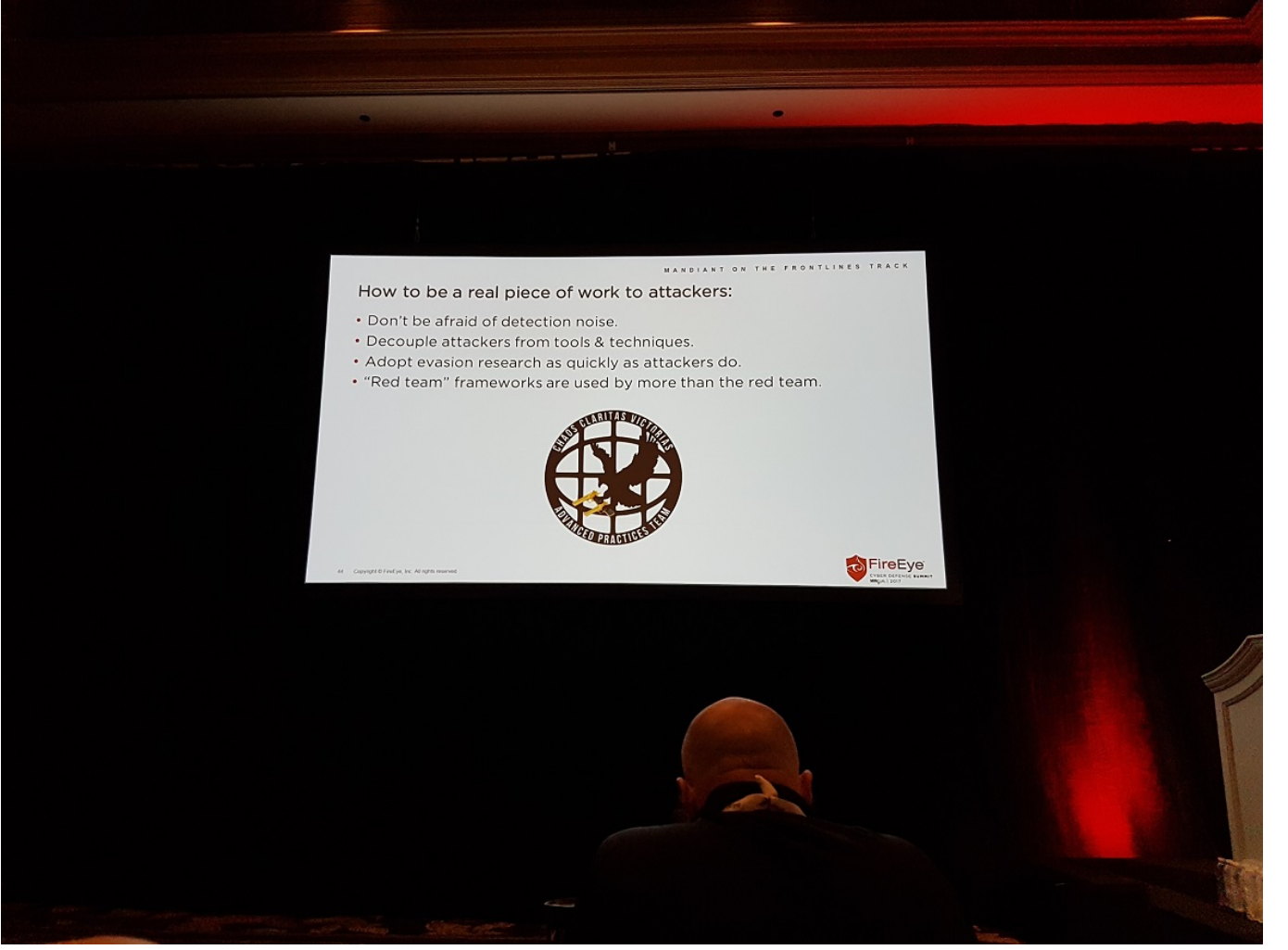
Casey Smith
Blogger

Following

[Blog Post]
Bypass Application Whitelisting Script
Protections - Regsvr32.exe & COM Scriptlet
(.sct files)
sub010x10.blogspot.com/2016/04/bypass ...
:-)

- 
- So @enigma0x3 found one of my new favorite new ways to execute COM Scriptlets
github.com/subTee/windows ...
 See GetObject at Line 68 of pubprm.vbs

- 3:34 PM - 27 Jun 2017



Kıssadan hisse, yüksek olan beklentilerimi fazlasıyla karşılayan FireEye Cyber Defense Summit güvenlik konferansından mutlu ve aydınlanmış bir şekilde evime dönerken, 12 saatlik uçak yolculuğunda sıcağı sıcağına kaleme aldığımı bu yazıyı yazarken bile etkinlikte olduğu kadar keyif aldım. Yazıma son noktayı koymadan önce, hem daveti için hem de seyahatin başından sonuna kadar tüm konuklarıyla yakından ilgilenip, misafirperverliği ile evimizi aratmayan Ümit NADİM'e teşekkürü bir borç bilirim. 2018'de tekrar bu konferansa katılma şansım olur mu bilinmez ama konferansa katılacakları şimdiden kıskanmaya başladığımı söyleyebilirim. :)

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.



Not: Etkinlik esnasında sosyal medya hesaplarımdan da duyurduğum üzere, LinkedIn ve Twitter hesaplarımı takip edenler arasında gerçekleştirilen hediye çekilişine buradan katılabilirsiniz.