



# WIRE ME THROUGH MACHINE LEARNING

Ankit Singh  
Threat Analyst Engineer, Symantec  
@ankit5934  
[Ankit\\_singh@Symantec.com](mailto:Ankit_singh@Symantec.com)



Vijay Thaware  
Security Response Lead, Symantec  
@021vj  
[Vijay\\_Thaware@Symantec.com](mailto:Vijay_Thaware@Symantec.com)

# AGENDA

- BEC scam walkthrough
- Social engineering, Social network hygiene and human psyche
- Recon and profiling
- Machine Learning – The attacker's way
- Design and Execution
- SOS : Defender's way
- Mitigation

## What's Not to Expect...

- This talk is about human hardware so NO exploits or codes are involved.
- Machine will not perform any magic here and start sending BEC attacks.
- You are welcome to disagree at our points, We are ok with it.

# AGENDA

- |   |  |
|---|--|
| 1 | BEC scam walkthrough                               |
| 2 | Social network hygiene and Defects in human psyche |
| 3 | Recon and profiling                                |
| 4 | Machine Learning – The attacker's way              |
| 5 | Design and Execution                               |
| 6 | SOS: Defender's way                                |
| 7 | Mitigation   |

# BUSINESS EMAIL COMPROMISE

## BEC ?

Umm..Never heard o'

### Features:

- Don't showcase strong technical exploit
- Use of high influential skills.
- Sent with short content sensing a need urgency.



Top 5 BEC Subject keyword

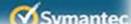
wire re:  
**transfer payment request**

Wire Me Through Machine Learning

Over 400 businesses are hit by BEC scams daily



At least 2 employees per business are targeted with an email



sent Monday to Friday, a standard working week



Organizations have lost over \$3 billion to BEC Scams

**\$3 Billion**

Source: FBI

>22,000 victims globally



# AGENDA

- 1 BEC scam walkthrough
- 2 Social engineering, social network hygiene and human psyche
- 3 Recon and profiling
- 4 Machine Learning – The attacker's way
- 5 Design and Execution
- 6 SOS: Defender's way
- 7 Mitigation

## Social engineering, Social network hygiene and Human psyche

"An art of exploiting human behavior in order to steal confidential or valuable information from people."

It is all about how we present ourselves on social network ...

## Defects in Human Psyche



Source: [www.jklossner.com](http://www.jklossner.com)

*"BEC attacks are highly targeted attacks and involve high level of research through social engineering."*

# AGENDA

- 1 BEC scam walkthrough
- 2 Social engineering, social network hygiene and human psyche
- 3 Recon and profiling**
- 4 Machine Learning – The attacker's way
- 5 Design and Execution
- 6 SOS: Defender's way
- 7 Mitigation

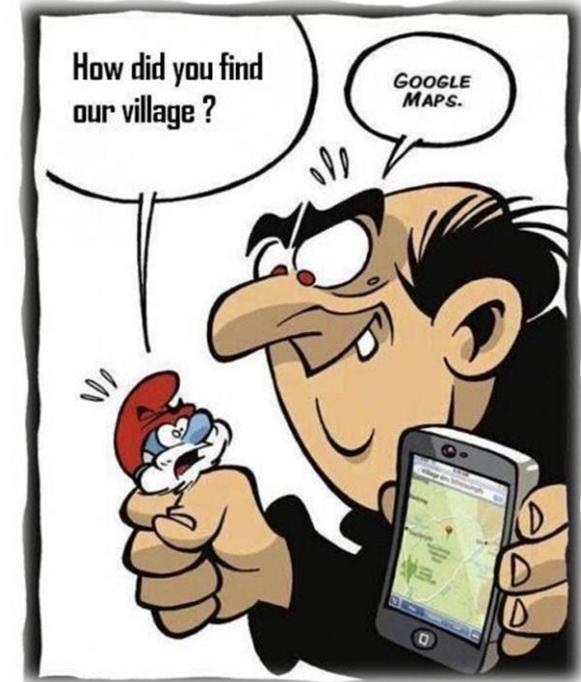
# RECON AND PROFILING

*Reconnaissance:* Preliminary surveying or research



## *Publicly available Data:*

- Social Media Profile
- Company website
- Current affairs
- Hierarchy of an Organization



Source:  
<https://www.pinterest.com/pin/414683078160855915/>

# GOOGLE SEARCH

**Google Dork:** “Chief Financial Officer” + “Email”

[Departments | Office of the Vice Chancellor - Chief Financial Officer](#)

[cfo.berkeley.edu/about-us](#) ▾

About the Vice Chancellor - Chief Financial Officer. Rosemarie Rae brings over ... Email:  
[jeanbednarz@berkeley.edu](mailto:jeanbednarz@berkeley.edu) (link sends e-mail) Phone: (510) 643-1888.

[Chief Financial Officer - Community ISD](#)

[www.communityisd.org/domain/80](#) ▾

Chief Financial Officer. Bill Moeller. Phone: 972-843-8440. Email:[William.Moeller@communityisd.org](mailto:William.Moeller@communityisd.org).  
Degrees and Certifications: MA School Administration ...

[Sidense Announces New Chief Financial Officer - Sidense Corp. OTP ...](#)

<https://www.sidense.com> › Company › Press Releases › 2015

Sidense Announces New Chief Financial Officer. Print; Email. Ottawa, Canada – (May 15, 2015) –  
Sidense Corp., a leading developer of non-volatile memory ...

[Justice/Branch Structure/CFO - Department of Justice](#)

[www.justice.gov.za/branches/organo/organo\\_CScfo.htm](#) ▾

Chief Financial Officer (CEO). Ms Louraine Rossouw Tel: 012 315 1775. E-mail:  
[LoRossouw@justice.gov.za](mailto:LoRossouw@justice.gov.za); PA: Ms Lerato Mdhluli, Tel: 012 315 4722, Email: ...

[Leadership: Office of the Vice President & Chief Financial Officer](#)

<https://vpcfo.iu.edu/leadership.html> ▾

Joan Hagen. Associate Vice President & University Controller. Office: Bryan Hall 114; Phone: (812) 856-2548; Email: [jhagen@iu.edu](mailto:jhagen@iu.edu); Website: ...

# RECON AND PROFILING

## Twitter Search

Twitter users with ""Chief finance officer"" in their bios only

Showing 1 - 50 of 71 results (order by relevance)

			tweets	following	followers	account age
<a href="#">follow</a>	 <b>Nickson maingi</b> @Nickyizzle	Nakuru, Kenya	1,415	6,198	6,299	5.65 years
Chief Finance Officer (CFO) from Machakos County willing to socialize with different people around the world. I Follow Back in 24 Hours. F4F U4U						
<a href="#">follow</a>	 <b>Loretta Outhwaite</b> @_outhwaite	Isle of Wight	7,684	1,932	1,300	4.83 years
CCG Chief Finance Officer, GPTW lead for Future Focused Finance & School Governor. Passionate about NHS, education & getting best out of life. Views are my own.						
<a href="#">follow</a>	 <b>Chrisha Alagaratnam</b> @chrishaal	London	741	746	921	4.17 years
Chief Finance Officer of Barts Health NHS Trust						
<a href="#">follow</a>	 <b>Aly</b> @ALYmentary	ust amv x tomcat	29,163	479	792	6.02 years
I remember everyone that leaves. @TOMCATust's Chief Finance Officer						

<https://moz.com>

## LinkedIn Search

Showing 21,961 results

	<b>Sara Maurice</b> • 2nd Senior Finance Manager at Washington federal saving Greater Seattle Area	<a href="#">Connect</a>
	<b>Sandhya Goel, CPA</b> • 2nd Senior Finance Manager at SPM Corporate Services Greater Philadelphia Area	<a href="#">Connect</a>
	<b>Ying Chen</b> • 2nd Senior ERP Finance Manager - ERP Tax Design Leader at GE Power Greater Boston Area	<a href="#">Connect</a>

See connections (500+) 

### Contact and Personal Info

 <a href="#">Profile</a>	<a href="https://linkedin.com/in/aj.../edit-profile">linkedin.com/in/aj.../edit-profile</a>
 <a href="#">Email</a>	<a href="mailto:anju[REDACTED]@gmail.com">anju[REDACTED]@gmail.com</a>
 <a href="#">Birthday</a>	December 4
 <a href="#">Connected</a>	
<a href="#">Show less ▾</a>	

# EMAIL VALIDATOR

<https://hunter.io>

- **To identify valid Email address**
- **Bulk Email Verifier**
- **API**

## Email Verifier

Verify the deliverability of any email address with the most complete email checker.

 Valid email address

The email format is good.  
The email address doesn't look gibberish.  
It seems not to be a disposable email address.  
We don't identify this domain as a webmail.  
MX records exist on this domain.  
Mail server exist on this domain.  
The email address is valid.  
The mail server doesn't accept all email addresses.

 We couldn't find this email address publicly available somewhere on the web.

## Email Verifier

Verify the deliverability of any email address with the most complete email checker.

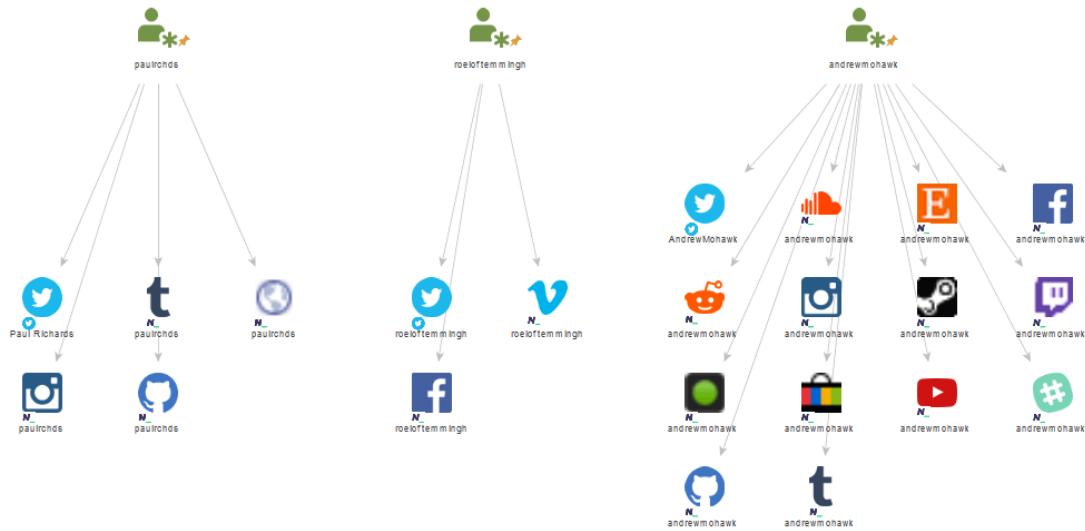
 Risky email address

The email format is good.  
The email address doesn't look gibberish.  
It seems not to be a disposable email address.  
We don't identify this domain as a webmail.  
MX records exist on this domain.  
Mail server exist on this domain.  
**The email address isn't valid.**  
The mail server doesn't accept all email addresses.

 We couldn't find this email address publicly available somewhere on the web.

# PROFILE FINGERPRINTING

- Maltego



- Recon-ng

CONFIGURATION FOR RECON-NG API'S LIST

Name	Value
bing_api	
builtwith_api	
facebook_api	
facebook_password	
facebook_secret	
facebook_username	
flickr_api	
fullcontact_api	
github_api	
google_api	
google_cse	
hashes_password	
hashes_username	
instagram_api	
instagram_secret	
ipinfodb_api	
jigsaw_api	
jigsaw_password	
jigsaw_username	
linkedin_api	
linkedin_secret	
pwnedlist_api	
pwnedlist_iv	
pwnedlist_secret	
shodan_api	
twitter_api	
twitter_secret	

hosts	
host	TEXT
ip_address	
region	
country	
latitude	
longitude	

contacts	
fname	TEXT
lname	
email	
title	
region	
country	

creds	
username	TEXT
password	
hash	
type	
leak	

dashboard	
module	TEXT
runs	INT

# AGENDA

- 1 BEC scam walkthrough
- 2 Social network hygiene and Defects in human psyche
- 3 Recon and profiling
- 4 **Machine Learning – The attacker's way**
- 5 Design and Execution
- 6 SOS: Defender's way
- 6 Mitigation

# WHY ML?

## Why Attackers Might Need ML

- To increase **success** rate
- Defeat other **machines** out there
- Acquire **target** list

# MACHINE LEARNING

## Objective

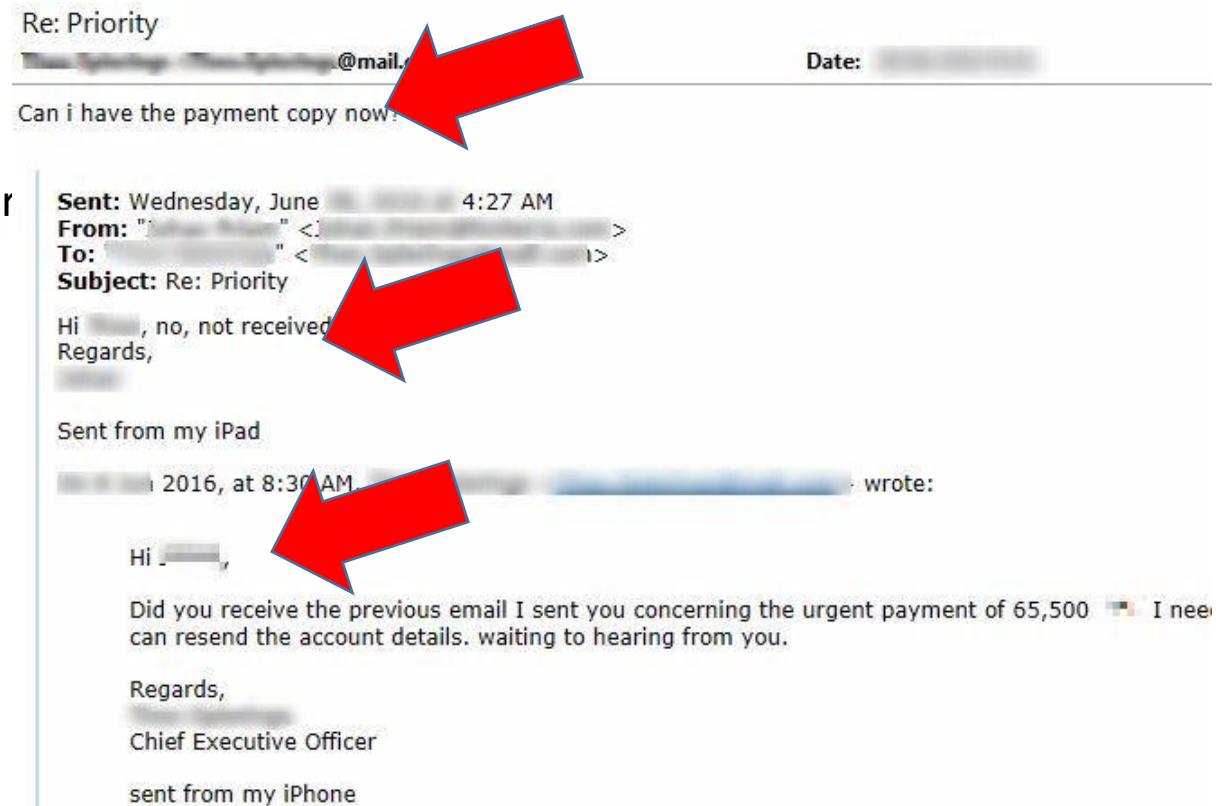
- To find the target for attack
- Obtain the model and test with real victim pr

## Machine Learning

- Supervised Machine learning
- Support Vector Machine
  - ✓ For possible Target profile prediction

## Ground Truth

- Anti Spam telemetry
- Profile of people who were attacked



# FEATURE SELECTION

Name	Age	Sex	No of LinkedIn Connection	Twitter Followers	No of Tweets	Spear Phished on Twitter	Spear Phished on LinkedIn	Victim
Lisa	45	F	2640	25	10871	1	1	True
John	40	M	241	4781	1472	0	0	False
Dave	50	M	357	5871	1571	1	0	False

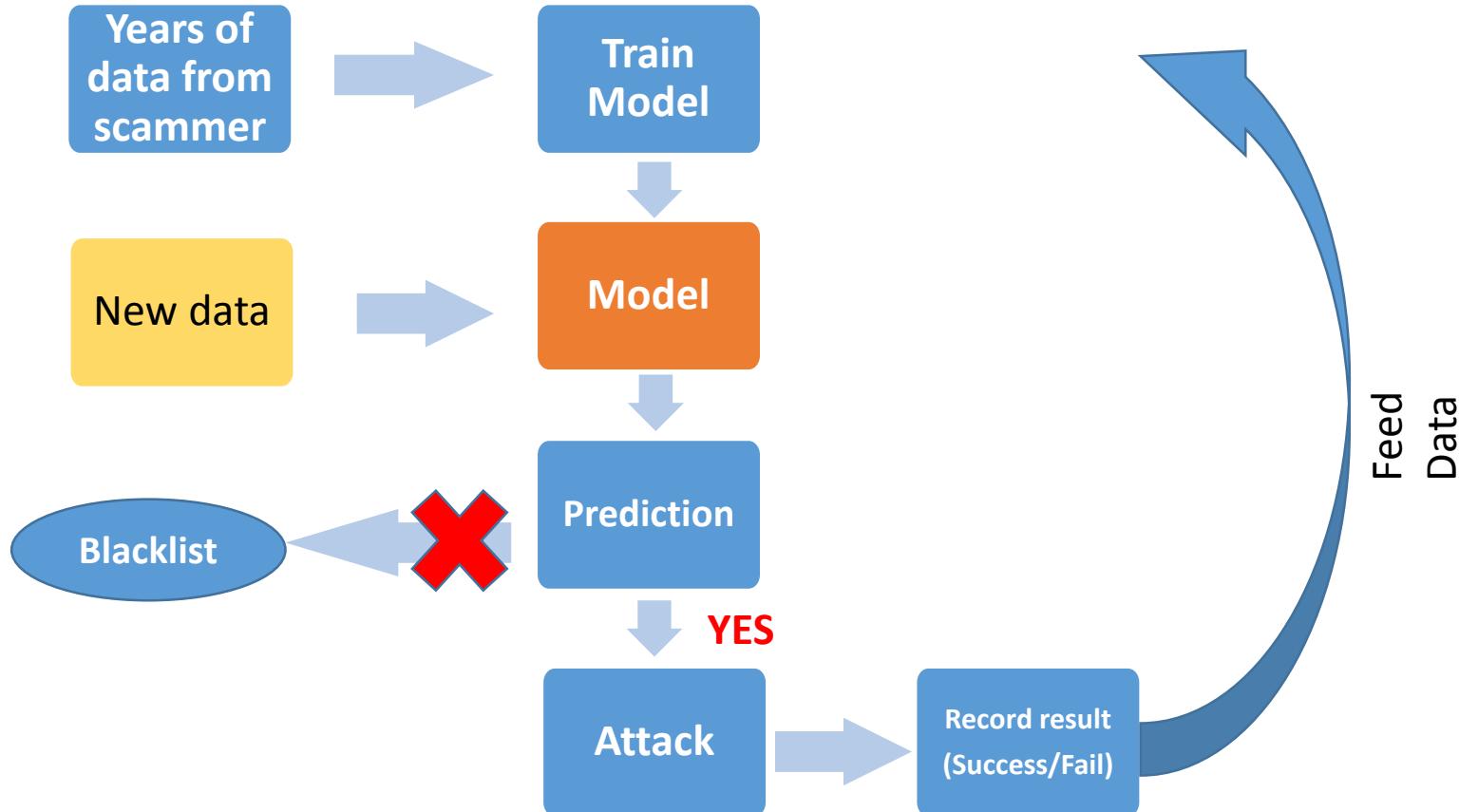
## Assumptions:

- The attacker has collected stats and data of all attacks that were conducted earlier
- The attacker is also labeling the profile for successful and failed attempts



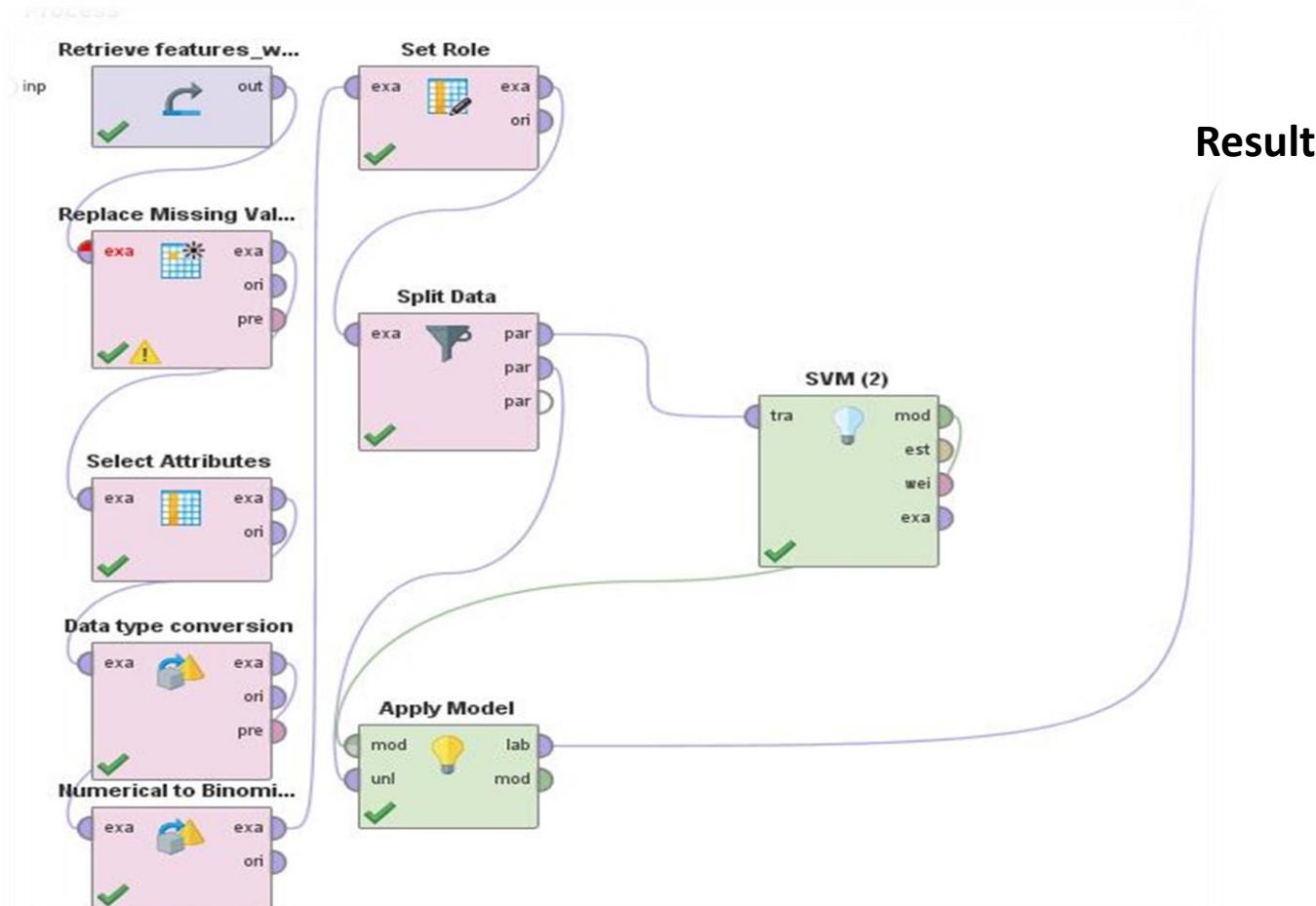
"You can't keep adjusting the data to prove that you would be the best Valentine's date for Scarlett Johansson."

# TRAINING MODEL



## Machine Learning Model:

- Data contains both Success and failed attempts of BEC
- SVM (Support Vector Machine)
- Model performance testing is done with Cross-validation



# TEST RESULTS

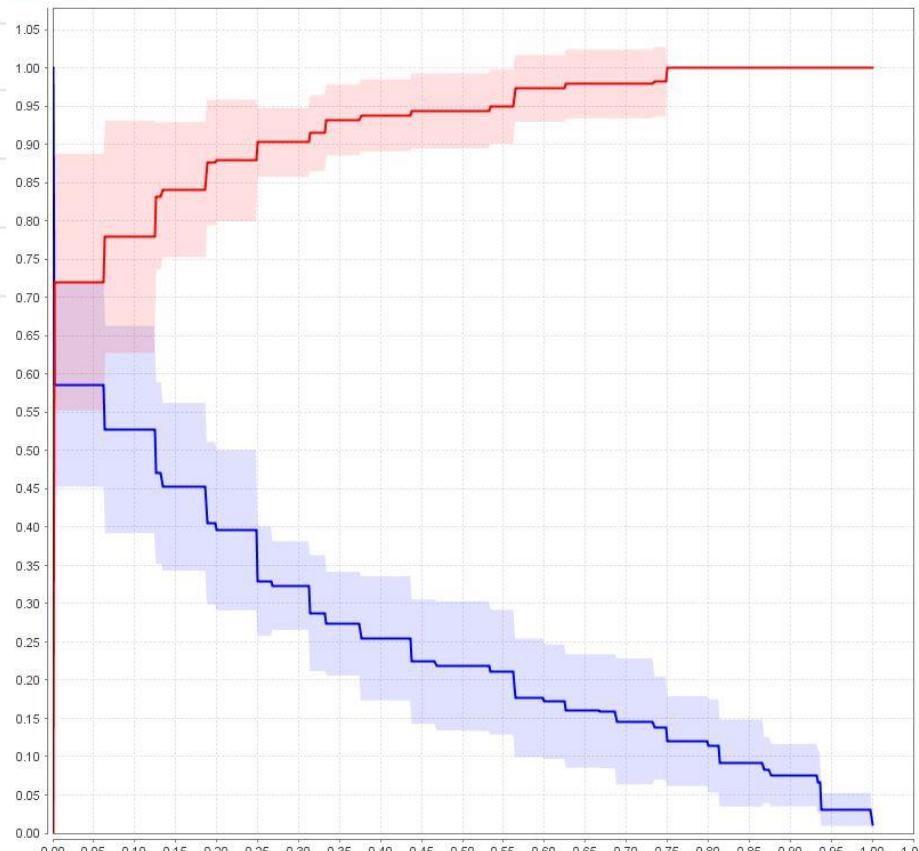
accuracy: 83.30% +/- 4.99% (mikro: 83.27%)

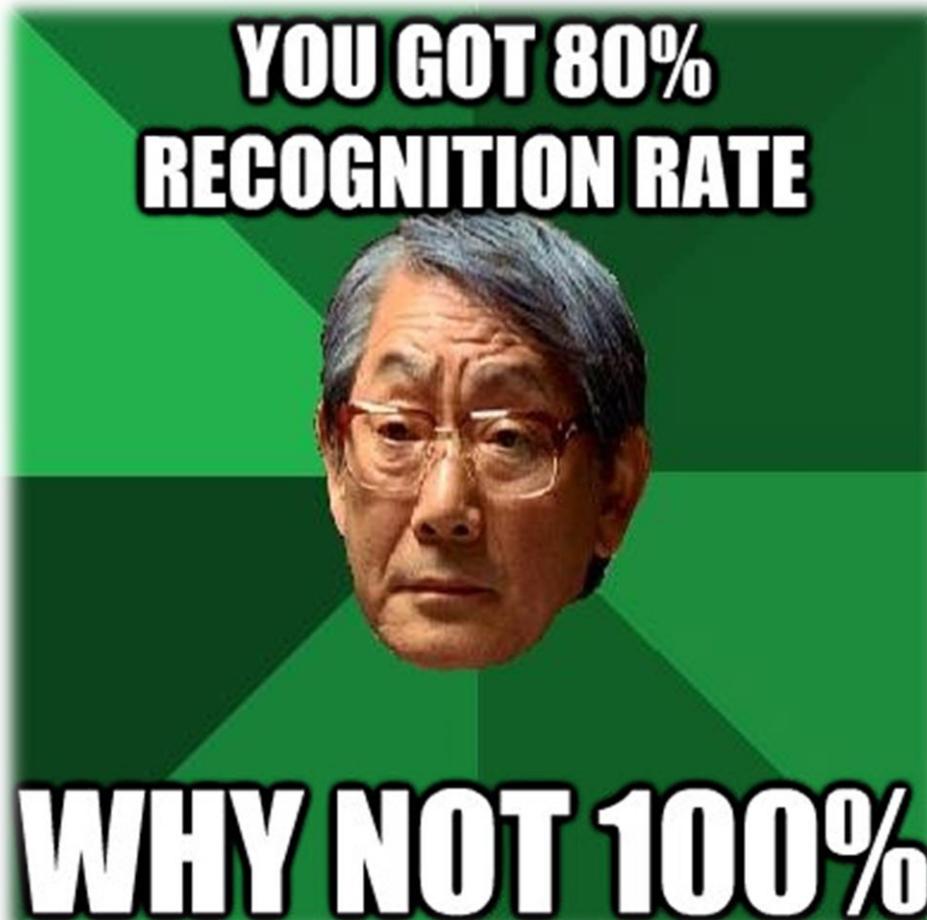
	true false	true true	class precision
pred. false	139	64	68.47%
pred. true	19	274	93.52%
class recall	87.97%	81.07%	

Attributes	Value
Precision	93.64% +/- 4.21%
Recall	81.08% +/- 5.59%
AUC	0.925 +/- 0.041
Accuracy	83.30% +/- 4.99%

AUC: 0.925 +/- 0.041 (mikro: 0.925) (positive class: true)

ROC ROC (Thresholds)





# AGENDA

- 1 BEC scam walkthrough
- 2 Social network hygiene and Defects in human psyche
- 3 Recon and profiling
- 4 Machine Learning – The attacker's way
- 5 **Design and Execution**
- 6 Mitigation

# Design and Execution

- Target Identified
- Email crafting
- Similar domain name registered



```
CAPTPhisher [v]0.0.3
Author: Mr. V
Web: ring0lab.com

SAGE:
atphish.rb -d domain [option,..]
-c, --custom      Custom level domain
-d, --domain     [REQUIRED ARGUMENT] Domain to analyze
-t, --type        Type of level domains: (popular, country, generic) -- Default: popular
-a, --all         Show all domains, including not available ones
```

Service	Term	Price	Subtotal	
<a href="#">symanteç.com</a> .COM Domain	1 Year ▾	\$15.00/yr* <a href="#">\$3.99</a> 	\$3.99	
			\$0.18	\$0.18
	<input type="checkbox"/> Keep my identity safe with Directnic Privacy		\$0.00	

\*Plus ICANN fee total charged at .18 per year per applicable TLD

Keep my identity safe with Directnic Privacy

[CLEAR CART](#) [REMOVE PRIVACY](#)



# Design and Execution

Service	Term	Price	Subtotal
symanteç.com .COM Domain	1 Year	\$15.00/yr* \$3.99 <small>i</small>	\$3.99
*Plus ICANN fee total charged at .18 per year per applicable TLD			
<input type="checkbox"/> Keep my identity safe with Directnic Privacy			
<a href="#">CLEAR CART</a>		<a href="#">REMOVE PRIVACY</a>	



# Design and Execution

Service	Term	Price	Subtotal
symanteç.com .COM Domain	1 Year	\$15.00/yr* \$3.99	\$3.99
Alt + 0231			
*Plus ICANN fee total charged at .18 per year per applicable TLD			\$0.18
<input type="checkbox"/> Keep my identity safe with Directnic Privacy			\$0.00
<a href="#">CLEAR CART</a>	<a href="#">REMOVE PRIVACY</a>		

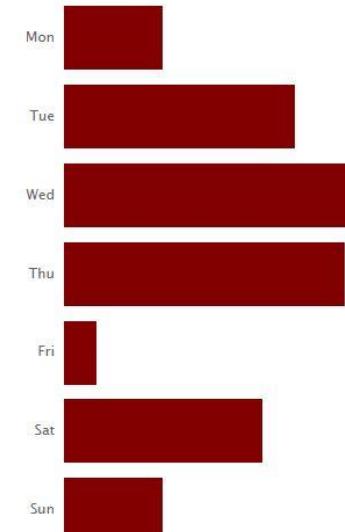
# TIMING

- Timing plays an important role in BEC attacks
- Attacks are launched mostly from Monday to Friday
- Attacker may plan the attack as per travel plan of CEO



→

Tweets by days of the week



Tweets by hours of the day



Source: <https://tweetchup.com/>

**Keynote Plan**



**Travel Plan**



**Norwich High** @NorwichHigh · Jun 19

We're thrilled that **@cherylGDST**, **CEO** @GDST will be joining us as AM **Keynote** speaker and panel leader at our @InspFemales Summit on Monday



**TwelveDotSecurity** @TwelveDotSec · Jun 19

Our **CEO** will be giving a **keynote** presentation entitled "IoT Security – Preventing a Global Disaster" tomorrow

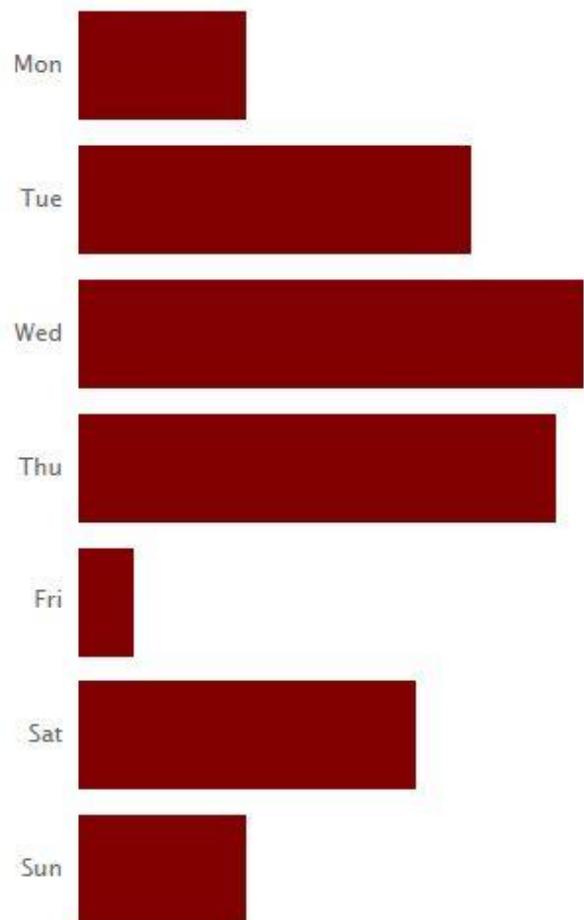


**Hilton Careers EMEA** @Hilton\_Careers · Apr 26

Chris Nassetta, President & **CEO** traveling to Saudi Arabia and meeting with **our** incredible Team Members

# TIMING

Tweets by days of the week



Tweets by hours of the day



Our Assumption

Bed Time

Ready for office/Walk

Travel to office

Lunch time

Bed Time

# Send Email and wait

# AGENDA

- 1 BEC scam walkthrough
- 2 Social network hygiene and Defects in human psyche
- 3 Recon and profiling
- 4 Machine Learning – The attacker's way
- 5 Design and Execution
- 6 SOS: Defender's way**
- 5 Mitigation

# SOS: Defender's way

- ✓ Check Social media hygiene
- ✓ Human pentesting inside organization
- ✓ Finding out potential targets inside the organization
- ✓ Educate and help hardening social media profile



# MITIGATIONS

- Protect your social network account, **Keep it clean**
- Do not click on emails and links which are **not** meant for you.
- Start reading emails from the “**FROM:**” field itself.
- **Cross check** before making any wire transfer and take time even if CEO says
- Training for **EVERYONE**...including top management.  
Most importantly... **TOP MANAGEMENT**

# Black Hat Sound Bytes

- ❖ More than enough personal data is available publically and can be used for social engineering
- ❖ Machine learning can be used offensively for target profiling or finding high value targets
- ❖ As the attackers may start labeling the profile with proper success and unsuccessful attack, the machine learning model may become more and more accurate.

# Thanks!!

Ankit Singh  
[@ankit5934](https://twitter.com/ankit5934)

Vijay  
[@021vj](https://twitter.com/021vj)