Uma Metodologia para Identificação Adaptativa e Caracterização de Phishing

Pedro Las-Casas, Osvaldo Fonseca, Elverton Fazzion,
Cristine Hoepers, Klaus Steding-Jessen, Marcelo H. P. Chaves,
Ítalo Cunha, Dorgival Guedes, Wagner Meira Jr.

31 de Maio de 2016

UFMG - ICEx
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO
e-speed DCC- UFMG
Winweb Instituto Nacional de Ciência e Tecnologia para a Web
nic.br

Introdução

- Phishing é uma das atividades criminosas mais lucrativas na Internet
- Phishing combina engenharia social e técnicas de ataque para enganar usuários
- Em geral, atacantes tentam ludibriar usuários, mascarando emails e páginas web para roubar informações sensíveis

Introdução

Dear Apple Customer,

Your Apple ID has been disabled due to several unsuccessful login attempts from the device listed below.

Date: 12/08/2015
Browser Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:37.0) Gecko/20100101 Firefox/37.0
Activity: 3 failed login attempts.
IP: 81.195.34.16
Country: Russian Federation

In order to restore your Apple ID we require you to verify your account information you can do this by clicking the l ink below.

Verify now >

If you have any questions or need help, please contact the Apple ID Support Team.

My Apple ID | Support | Privacy Policy
Copyright © 2015 iTunes Sarl 31-33, Rue Sainte Zithe, L-2763 Luxembourg All Rights Reserved.

Introdução

- Ataques de phishing contabilizam mais de 3,2 bilhões de dólares de prejuízo nos Estados Unidos em um ano
- Relatório da Kapersky Lab mostra que 37,3 milhões de pessoas foram vítimas de tais ataques em um ano

Introdução

- Apesar de haver grande esforço para combatê-lo, phishing persiste
- Phishers evoluem suas técnicas, ludibriando os diversos métodos de mitigação criados
- Necessário entender phishing a fundo para evoluir os mecanismos de defesa

Introdução

Objetivo

- Entender as principais características de phishing que norteiam sua disseminação atual
- Identificar phishing e separar dos demais tipos de spam

Coleta dos dados

- 13 honeypots de baixa interatividade, coletores de spam
  - 2 redes no Brasil
  - 2 redes nos Estados Unidos
  - Argentina, Áustria, Austrália, Chile, Equador, Hong Kong, Holanda, Noruega, Taiwan e Uruguai.

Coleta dos dados

- Honeypots são configurados para simular servidores vulneráveis
- Honeypots emulam:
  - *Proxy* HTTP aberto
  - *Proxy* SOCKS aberto
  - *Relay* SMTP aberto

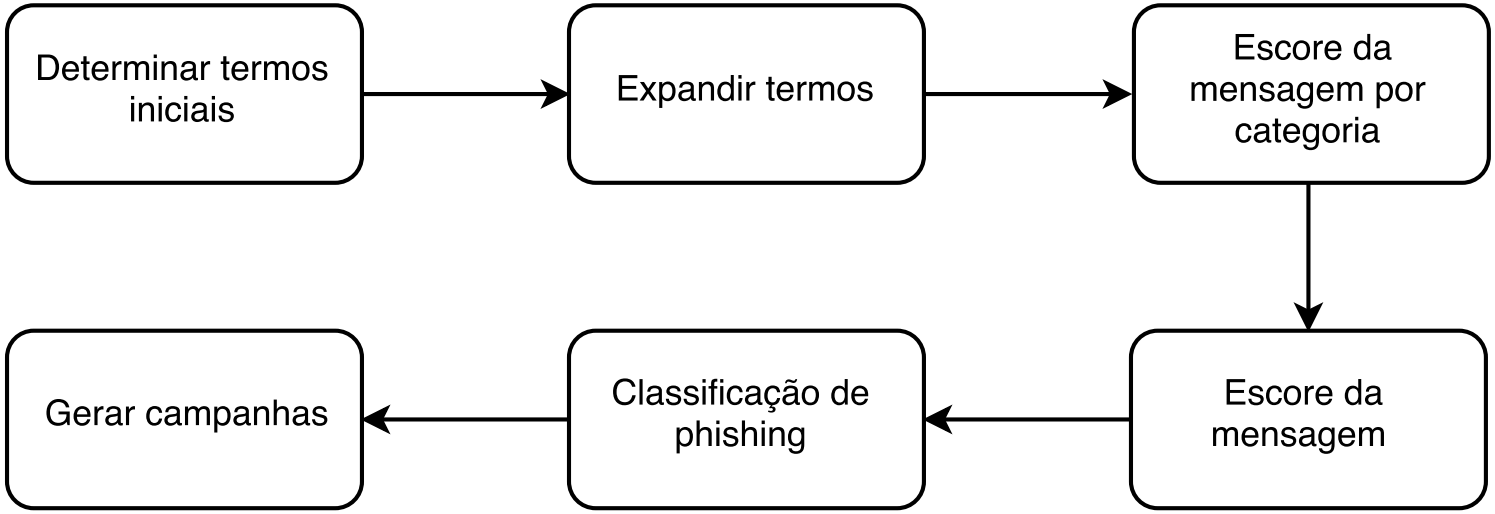
Coleta dos dados

- Honeypots não prestam serviço para nenhuma rede e não são anunciados publicamente
- Assumimos que todas as mensagens recebidas provém de spammers
- Analisamos mensagens recebidas entre **01/08/2015** e **31/10/2015**
- Em **91 dias**, coletamos **1,13 bilhão** de mensagens

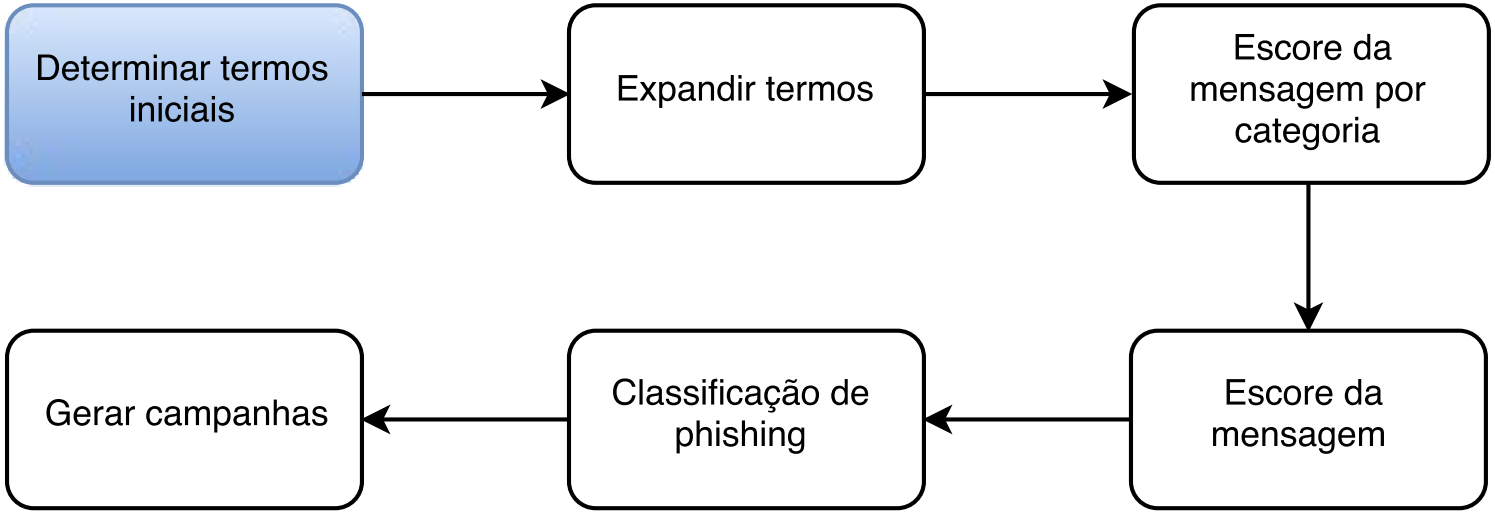
Pré-Processamento

- Mensagens são recebidas em diversos idiomas
- Selecionar apenas mensagens em inglês
  - Remoção tags HTML e URL's
  - Desconsidera-se anexos
  - Aplicar algoritmo para identificação de idiomas
  - De **1,13 bilhão** de mensagens, extraiu-se **13,21 milhões** em inglês

Identificação de Phishing



Identificação de Phishing



Identificação de Phishing

- **1. Determinação do conjunto inicial de termos**

Categoria	Conjunto Inicial
Tratamento	dear, friend, hello, please
Menção a dinheiro	bank, money, cash, dollar
Pedido de resposta	write, contact, reply, response, foward, send
Urgência	now, today, instantly, straightaway, directly, urgently, urgent, desperately, immediately, soon, shortly, quickly
Formulário	form, attach, attached, attachment
Segurança	security, violated

Identificação de Phishing

- **1. Determinação do conjunto inicial de termos**

Categoria	Conjunto Inicial
Tratamento	dear, friend, hello, please
Menção a dinheiro	bank, money, cash, dollar
Pedido de resposta	write, contact, reply, response, foward, send
Urgência	now, today, instantly, straightaway, directly, urgently, urgent, desperately, immediately, soon, shortly, quickly
Formulário	form, attach, attached, attachment
Segurança	security, violated

- Tratamento: Termos utilizados pelo spammer para se aproximar e ganhar a confiança da vítima

Identificação de Phishing

- **1. Determinação do conjunto inicial de termos**

Categoria	Conjunto Inicial
Tratamento	dear, friend, hello, please
Menção a dinheiro	bank, money, cash, dollar
Pedido de resposta	write, contact, reply, response, foward, send
Urgência	now, today, instantly, straightaway, directly, urgently, urgent, desperately, immediately, soon, shortly, quickly
Formulário	form, attach, attached, attachment
Segurança	security, violated

- Menção Monetária: Ataques relacionados à conta bancária ou relacinados à dinheiro fácil

Identificação de Phishing

- **1. Determinação do conjunto inicial de termos**

Categoria	Conjunto Inicial
Tratamento	dear, friend, hello, please
Menção a dinheiro	bank, money, cash, dollar
Pedido de resposta	write, contact, reply, response, foward, send
Urgência	now, today, instantly, straightaway, directly, urgently, urgent, desperately, immediately, soon, shortly, quickly
Formulário	form, attach, attached, attachment
Segurança	security, violated

- Pedido de resposta: Para o atacante roubar informações do usuário, é necessário que este responda a mensagem

Identificação de Phishing

- **1. Determinação do conjunto inicial de termos**

Categoria	Conjunto Inicial
Tratamento	dear, friend, hello, please
Menção a dinheiro	bank, money, cash, dollar
Pedido de resposta	write, contact, reply, response, foward, send
Urgência	now, today, instantly, straightaway, directly, urgently, urgent, desperately, immediately, soon, shortly, quickly
Formulário	form, attach, attached, attachment
Segurança	security, violated

- Senso de Urgência: Atacantes tentam induzir a vítima a responder o mais rápido possível

Identificação de Phishing

- **1. Determinação do conjunto inicial de termos**

Categoria	Conjunto Inicial
Tratamento	dear, friend, hello, please
Menção a dinheiro	bank, money, cash, dollar
Pedido de resposta	write, contact, reply, response, foward, send
Urgência	now, today, instantly, straightaway, directly, urgently, urgent, desperately, immediately, soon, shortly, quickly
Formulário	form, attach, attached, attachment
Segurança	security, violated

- Formulário: Mensagens pedem que usuário preencha formulário e envie de volta ao atacante

Identificação de Phishing

- **1. Determinação do conjunto inicial de termos**

Categoria	Conjunto Inicial
Tratamento	dear, friend, hello, please
Menção a dinheiro	bank, money, cash, dollar
Pedido de resposta	write, contact, reply, response, foward, send
Urgência	now, today, instantly, straightaway, directly, urgently, urgent, desperately, immediately, soon, shortly, quickly
Formulário	form, attach, attached, attachment
Segurança	security, violated

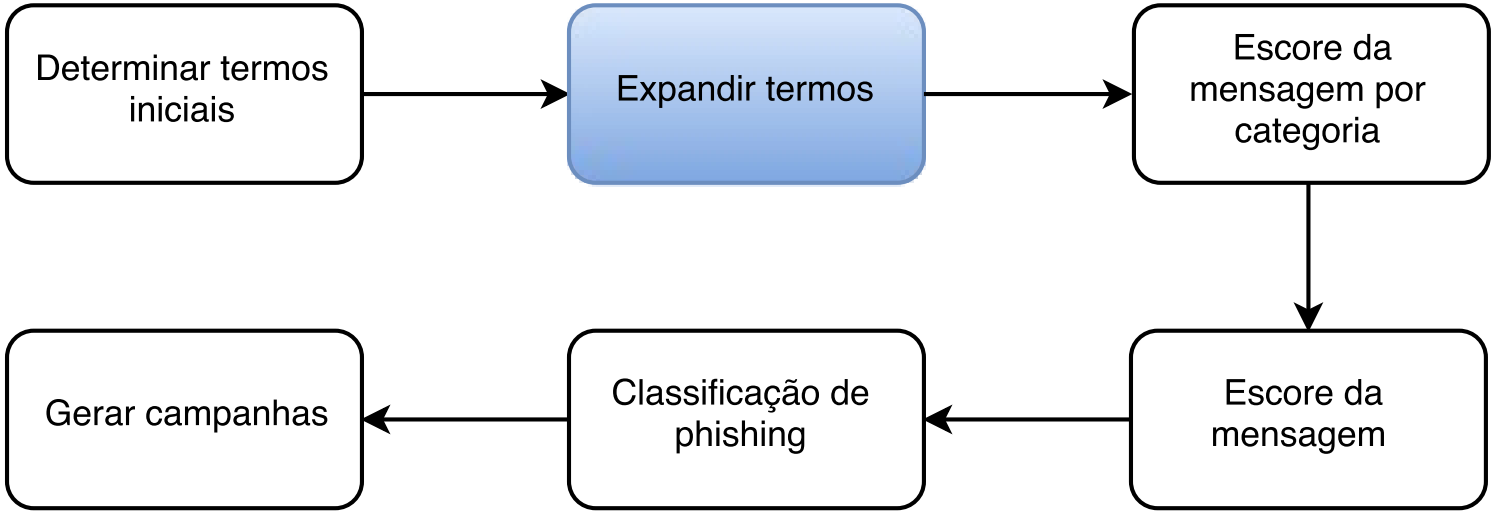
- Segurança: Menção de bloqueio à conta bancária ou algum serviço

Identificação de Phishing

- **1. Determinação do conjunto inicial de termos**
  - Baseados na literatura
  - Representativo mas incompleto

Categoria	Conjunto Inicial
Tratamento	dear, friend, hello, please
Menção a dinheiro	bank, money, cash, dollar
Pedido de resposta	write, contact, reply, response, foward, send
Urgência	now, today, instantly, straightaway, directly, urgently, urgent, desperately, immediately, soon, shortly, quickly
Formulário	form, attach, attached, attachment
Segurança	security, violated

Identificação de Phishing

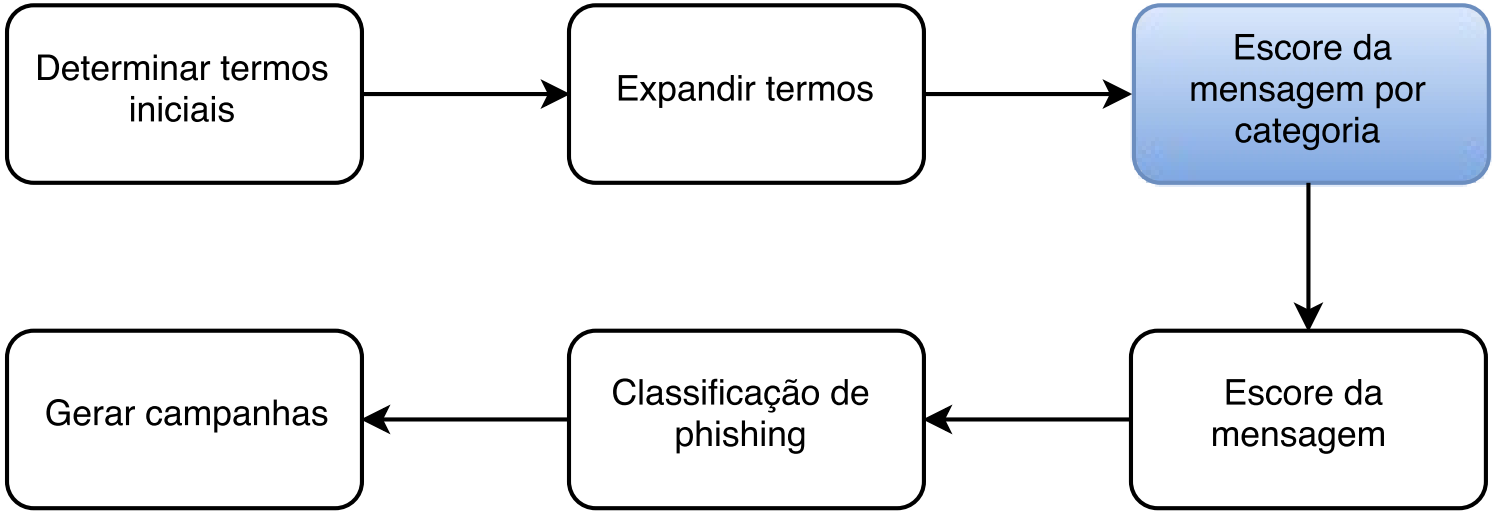


Identificação de Phishing

- **2. Expansão do conjunto de termos**
  - Utilizamos **Word2Vec** para expandir o conjunto de palavras
  - Identifica palavras mais semelhantes e mais relacionadas aos termos de entrada

Categoria	Termos Adicionados
Tratamento	congratulate, valuable, entrusted, congrats, sponsored, nontransferable, expires, regards, authentic, apologize, thank, inconvenience
Menção a dinheiro	credit, customer, funding, purchase, $, transfer, payment, millionaire, profits, accountability, dollars, donate
Pedido de resposta	communication, reapproved, reconfirm, confirming
Urgência	important
Formulário	information, address, occupation, documentations, subscriber, confidential, zipcode
Segurança	detected, correct, authorised, unauthorized, sign, reauthenticate, reliance, spamfiltered, recover, impostors, reactivate, suspects, account, verification

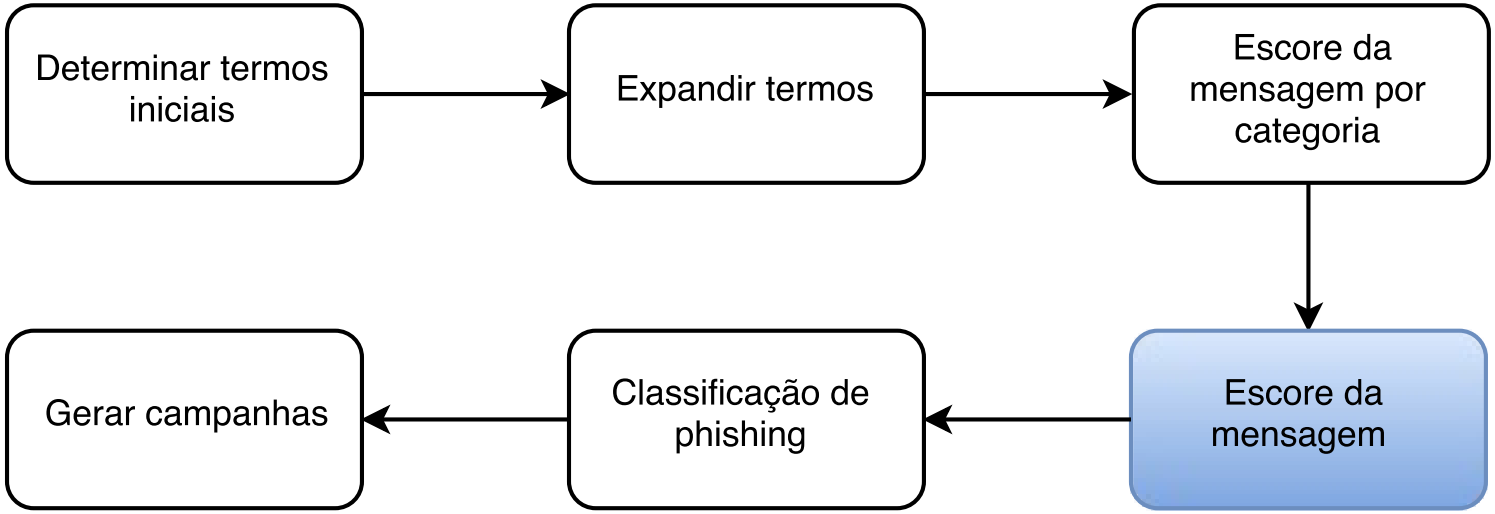
Identificação de Phishing



Identificação de Phishing

- **3. Escore da mensagem por categoria**
  - Estimar a pertinência de cada mensagem a cada categoria
  - Baseado em $TF - IDF$ [Baeza-Yates e Ribeiro-Neto 1999]
    - TF (*Term Frequency*) reflete a ocorrência de termos das categorias
      - Razão entre $numtermo_{msg,cat}$ e o maior $numtermo_{cat}$ que ocorre em alguma mensagem
      $$TF_{msg,cat} = numtermo_{msg,cat} / Max_{c \in categoria} numtermo_{msg,c}$$
    - IDF (*Inverse Document Frequency*) reflete a popularidade da categoria
      - Razão entre log do total de mensagens da base e número de mensagens assinaladas à categoria
      $$IDF_{cat} = log(nummsg_{*}) / nummsg_{cat}$$
    - $TFIDF_{msg,cat} = TF_{msg,cat} * IDF_{cat}$

Identificação de Phishing

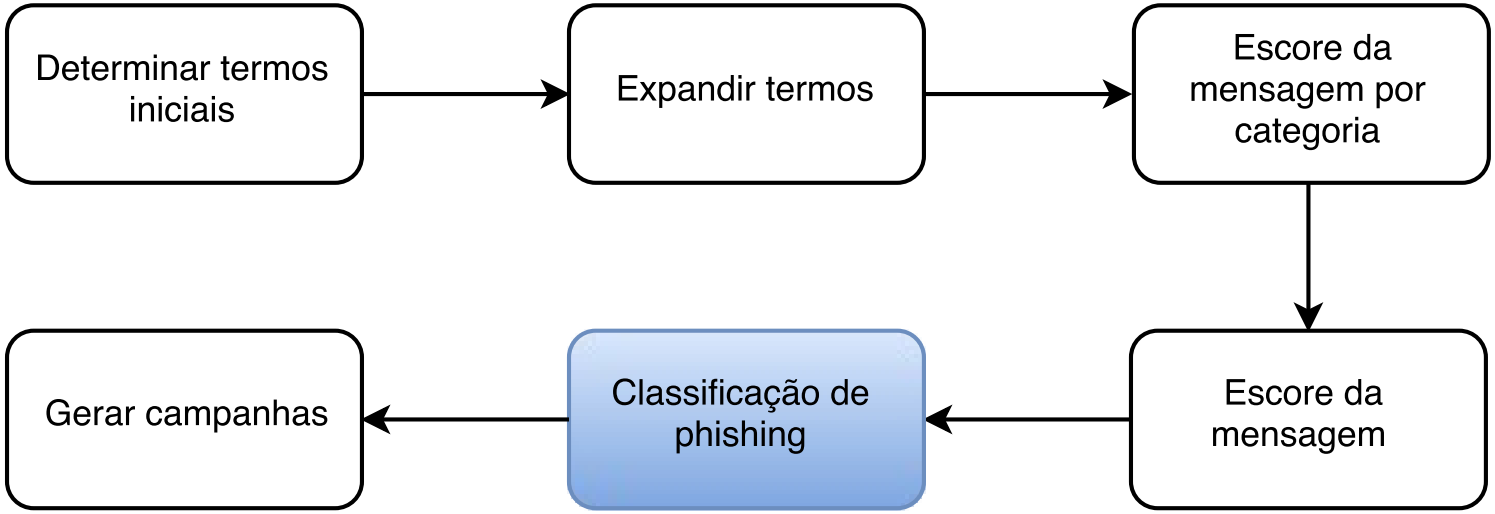


Identificação de Phishing

- **4. Escore da mensagem**
  - Gerar escore para cada mensagem
  - Soma dos $TF - IDF$ das categorias e constante α

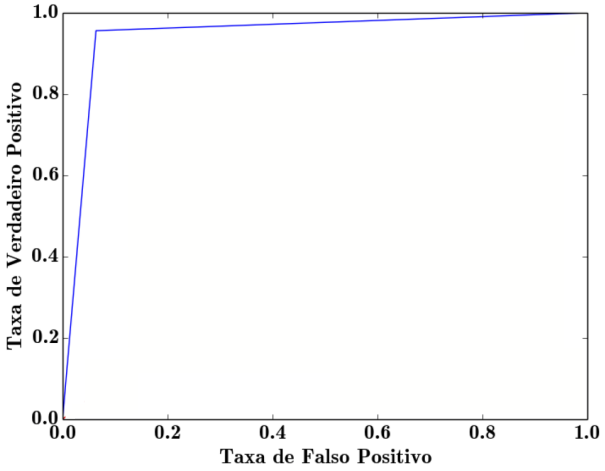
$$ESCORE_{msg} = \alpha + \sum_{cat \in categoria} TFIDF_{cat}$$

Identificação de Phishing



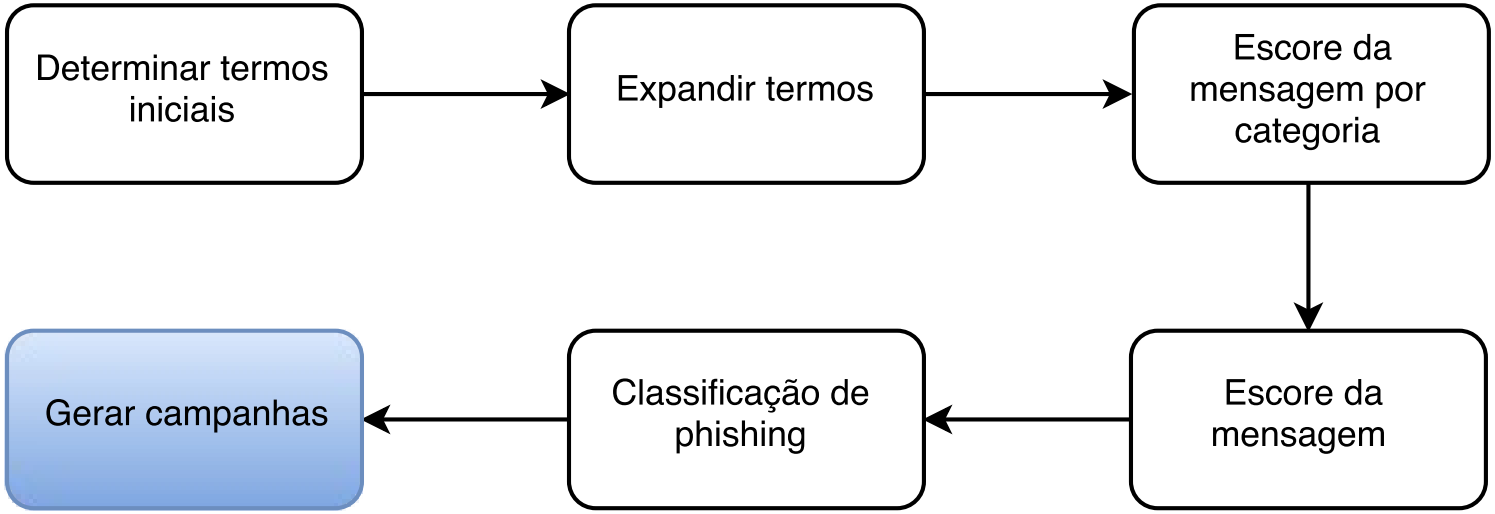
Identificação de Phishing

- **5. Classificação de Phishing**
  - Escore de cada mensagem é utilizado para classificar como phishing ou não
  - Metodologia baseada na curva ROC e medida AUC
    - Para amostragem, selecionamos **800** mensagens aleatórias
    - Nível de confiança de 95% e um erro amostral de $\pm 3,5\%$
    - Rotulamos manualmente mensagens como phishing ou não-phishing



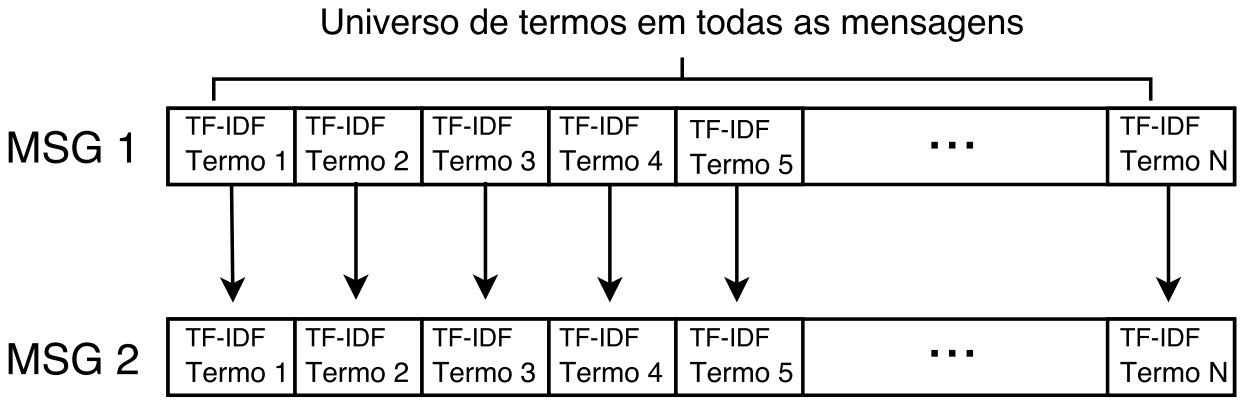
- Se $ESCORE_{msg} > lim$, mensagem é classificada como phishing

Identificação de Phishing



Identificação de Phishing

- **6. Determinação de Campanhas**
  - Após classificação de mensagens como phishing, agrupamos em campanhas (grupos de mensagens com mesma finalidade)
  - Utiliza $TF - IDF$, mas calculado no universo de todos os termos das mensagens.
  - $TF - IDF$ para cada termo compõe um vetor
  - Compara-se posição a posição de cada mensagem
  - Caso similaridade seja maior que 80%, agrupa mensagens



Resultados

- Caracterização do conjunto de mensagens de phishing
- Caracterização das campanhas de phishing

Visão Geral

Tabela : Visão Geral de *Phishing*

	SMTP(%)	SOCKS(%)	HTTP(%)	Total
Mensagens	9.757.096 (99,94%)	4.550 (0,04%)	807 (0,0%)	9.762.453
Endereços IP	6.651 (99,22%)	52 (0,77%)	4 (0,0%)	6.703
Sistemas Autônomos (AS)	1.701(99,35%)	35 (2,04%)	4 (0,23%)	1.712
***Country Codes* (CC)**	154 (100%)	16 (10,38%)	3 (1,94%)	154

Visão Geral

Tabela : Visão Geral de *Phishing*

	SMTP(%)	SOCKS(%)	HTTP(%)	Total
Mensagens	9.757.096 (99,94%)	4.550 (0,04%)	807 (0,0%)	9.762.453
Endereços IP	6.651 (99,22%)	52 (0,77%)	4 (0,0%)	6.703
Sistemas Autônomos (AS)	1.701(99,35%)	35 (2,04%)	4 (0,23%)	1.712
***Country Codes* (CC)**	154 (100%)	16 (10,38%)	3 (1,94%)	154

- Gerência da porta 25 ajudaria na mitigação do problema

Visão Geral

- Cerca de 60% enviou 10 mensagens ou menos
- 90% dos phishing foram enviados de 100 endereços IP distintos
- 40% destes e-mails estão concentrados em apenas 10 endereços IP

Tabela : Top 5 Endereços IP

IP	# de Mensagens	AS	CC	# de Campanhas
23.31.87.109	732.361	7922	US	6
212.227.94.138	524.056	8560	DE	2
65.29.192.68	500.351	10796	US	1
212.227.255.64	384.054	8560	DE	2
186.83.40.72	368.498	10620	CO	2

Visão Geral

Tabela : Top 5 Country Codes

CC	# de Mensagens	# de Endereços IP	# de AS's	# de Campanhas
US	3.605.904 (36,93%)	1.406 (20,97%)	302 (17,64%)	233
DE	2.308.181 (23,64%)	175 (2,61%)	53 (3,09%)	33
BA	480.317 (4,92%)	26 (0,38%)	2 (0,11%)	23
CO	388.093 (3,97%)	37 (0,55%)	9 (0,52%)	14
ZA	270.790 (2,77%)	41 (0,61%)	12 (0,70%)	11

- Mais de 60% das mensagens são provenientes dos Estados Unidos e Alemanha

Análise das campanhas de phishing

- 612 campanhas identificadas
- 8,5 milhões de mensagens
- 87% de todas as mensagens classificadas como phishing

Tabela : Visão geral das campanhas

Total de Campanhas	612
Média de mensagens	13.984
Média de IPs	3,16
Média de ASes	2,06
Média de CCs	1,82

Análise das campanhas de phishing

Tabela : Categoria das campanhas

	Abordagem	Dinheiro	Resposta	Urgência	Formulário	Segurança	Total
Campanhas	480	373	318	236	388	308	612
Mensagens	7.412.701	6.254.321	3.552.518	3.701.086	6.099.531	5.785.346	8.558.237

Análise das campanhas de phishing

Tabela : Categoria das campanhas

	Abordagem	Dinheiro	Resposta	Urgência	Formulário	Segurança	Total
Campanhas	480	373	318	236	388	308	612
Mensagens	7.412.701	6.254.321	3.552.518	3.701.086	6.099.531	5.785.346	8.558.237

- Uma maneira de evitar estes ataques é treinar e ensinar aos usuários as diferentes formas de ataque utilizada pelos phishers, minimizando a possibilidade de que estes se tornem vítima.

Principais campanhas de phishing

- Foram encontradas **612** campanhas
- **3** principais campanhas foram responsáveis por quase **24%** das mensagens

Tabela : Top 3 Campanhas

Características					Categorias					
	Mensagens	**IP**	**AS**	**CC**	**Abordagem**	**Dinheiro**	**Resposta**	**Urgência**	**Formulário**	**Segurança**
C 1	1.124.297	16	5	4	X	X			X	X
C 2	779.359	3	1	1	X			X	X	X
C 3	399.512	30	22	2	X	X	X		X	X

Campanha 1

Dear Apple Customer,

Your Apple ID has been disabled due to several unsuccessful login attempts from the device listed below.

Date: 12/08/2015
Browser Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:37.0) Gecko/20100101 Firefox/37.0
Activity: 3 failed login attempts.
IP: 81.195.34.16
Country: Russian Federation

In order to restore your Apple ID we require you to verify your account information you can do this by clicking the l ink below.

Verify now >

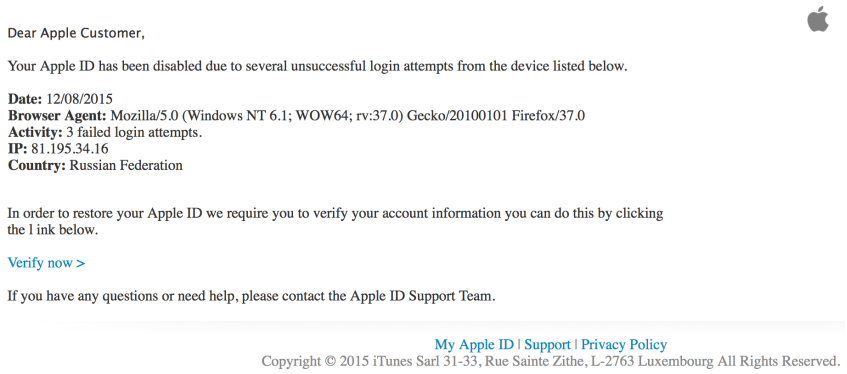
If you have any questions or need help, please contact the Apple ID Support Team.

My Apple ID | Support | Privacy Policy
Copyright © 2015 iTunes Sarl 31-33, Rue Sainte Zithe, L-2763 Luxembourg All Rights Reserved.

Campanha 1

Características					Categorias					
	Mensagens	**IP**	**AS**	**CC**	**Abordagem**	**Dinheiro**	**Resposta**	**Urgência**	**Formulário**	**Segurança**
C 1	1.124.297	16	5	4	X	X			X	X

- 16 endereços IP
- Localizados nos Estados Unidos, Alemanha, Colômbia e Grã-Bretanha
- 6 endereços enviaram poucas mensagens (menos de 1.000)
- Em contrapartida, IP 65.29.192.68 enviou mais de 500 mil mensagens de phishing



Dear Apple Customer,

Your Apple ID has been disabled due to several unsuccessful login attempts from the device listed below.

Date: 12/08/2015
Browser Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:37.0) Gecko/20100101 Firefox/37.0
Activity: 3 failed login attempts.
IP: 81.195.34.16
Country: Russian Federation

In order to restore your Apple ID we require you to verify your account information you can do this by clicking the l ink below.

Verify now >

If you have any questions or need help, please contact the Apple ID Support Team.

My Apple ID | Support | Privacy Policy
Copyright © 2015 iTunes Sarl 31-33, Rue Sainte Zithe, L-2763 Luxembourg All Rights Reserved.

Campanha 2

Bank of America

Important Notice

Starting from August 25th, 2015, we will be introducing new online banking authentication procedures in order to protect the information of our online banking customers.

You are required to complete our account verification process and confirm your information as you will not be able to have access to our online banking system untill this process has been completed. Please click the link below to get started.

Get Started

Please Note: Failure to complete our account verification process can lead to permanent restrictions being placed on your access to our online banking system.

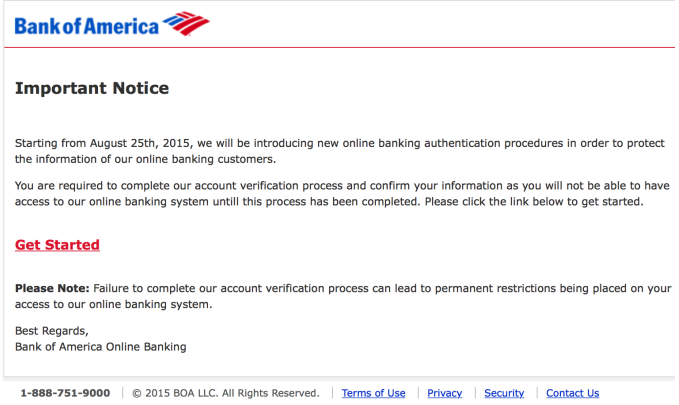
Best Regards,
Bank of America Online Banking

1-888-751-9000 | © 2015 BOA LLC. All Rights Reserved. | Terms of Use | Privacy | Security | Contact Us

Campanha 2

Características					Categorias					
	Mensagens	**IP**	**AS**	**CC**	**Abordagem**	**Dinheiro**	**Resposta**	**Urgência**	**Formulário**	**Segurança**
C 2	779.359	3	1	1	X			X	X	X

- Endereços IP: 212.227.94.138, 212.227.95.8 e 212.227.255.64
- Localizados na Alemanha (AS 8560)
- Cada endereços teve média de 259 mil phishings



Bank of America

Important Notice

Starting from August 25th, 2015, we will be introducing new online banking authentication procedures in order to protect the information of our online banking customers.

You are required to complete our account verification process and confirm your information as you will not be able to have access to our online banking system untill this process has been completed. Please click the link below to get started.

Get Started

Please Note: Failure to complete our account verification process can lead to permanent restrictions being placed on your access to our online banking system.

Best Regards,
Bank of America Online Banking

1-888-751-9000 | © 2015 BOA LLC. All Rights Reserved. | Terms of Use | Privacy | Security | Contact Us

Campanha 3

Dear Wells Fargo customer,
We have recently detected that a different computer user has attempted gaining access to your online account and multiple passwords were attempted with your user ID.
It is necessary to re-confirm your account information and complete a profile update.
You can do this by downloading the attached file and updating the necessary fields.
Note: If this process is not completed within 24-48 hours we will be forced to suspend your account online access as it may have been used for fraudulent purposes.
Completion of this update will avoid any possible problems with your account.
Thank you for being a valued customer.
(C) 2015 Wells Fargo. All rights reserved.

Campanha 3

Características					Categorias					
	Mensagens	**IP**	**AS**	**CC**	**Abordagem**	**Dinheiro**	**Resposta**	**Urgência**	**Formulário**	**Segurança**
C 3	399.512	30	22	2	X	X	X		X	X

- Campanha referente ao acesso a conta de bancos
  - Por exemplo Wells Fargo, Bank of America, Natwest
- Endereços IP presentes nos Estados Unidos e Grã-Bretanha

Dear Wells Fargo customer,
We have recently detected that a different computer user has attempted gaining access to your online account and multiple passwords were attempted with your user ID.
It is necessary to re-confirm your account information and complete a profile update.
You can do this by downloading the attached file and updating the necessary fields.
Note: If this process is not completed within 24-48 hours we will be forced to suspend your account online access as it may have been used for fraudulent purposes.
Completion of this update will avoid any possible problems with your account.
Thank you for being a valued customer.
(C) 2015 Wells Fargo. All rights reserved.

Conclusão e Trabalhos Futuros

- Apresentamos método adaptativo para identificação de mensagens de phishing
- Conseguimos identificar mais de **9,7 milhões** de mensagens de phishing, com taxa de acerto de aproximadamente **95%**
- Extensível para demais idiomas
- Mostramos características do phishing em inglês, como:
  - Mensagens são enviadas quase somente através do protocolo SMTP
  - Poucos endereços, comumente localizados na Alemanha e Estados Unidos, são responsáveis pela maior parte do tráfego
  - Poucas campanhas são responsáveis por grande parte das mensagens
- Como trabalho futuro, objetivamos aprimorar a técnica de identificação de phishing, estudando também os anexos e URL's das mensagens

Uma Metodologia para Identificação Adaptativa e Caracterização de Phishing

Pedro Las-Casas, Osvaldo Fonseca, Elverton Fazzion,
Cristine Hoepers, Klaus Steding-Jessen, Marcelo H. P. Chaves,
Ítalo Cunha, Dorgival Guedes, Wagner Meira Jr.

31 de Maio de 2016

UFMG - ICEx
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO
e-speed DCC- UFMG
Winweb Instituto Nacional de Ciência e Tecnologia para a Web
nic.br