

nic.br cgi.br

20 anos
cert.br

6° Fórum Brasileiro de CSIRTs
São Paulo, SP
14 de setembro de 2017

Conscientização como uma Ferramenta para Diminuir a Efetividade de *Spear Phishing* e *Insider Threats*

Miriam von Zuben
miriam@cert.br


2014 cert.br nic.br egi.br

12 Email Attack on Vendor Set Up Breach at Target

FEB 14

Hackers atacam sistema de e-mails e de leitura de documentos do Itamaraty

RSA's SecurID Breach Started with Phishing Email

By: Fahmida Y. Rashid | April 04, 2011     

RSA's Art Coviello told analysts that the SecurID attackers used a phishing email with a malicious Excel spreadsheet to penetrate the company's network.

Home Depot hackers used vendor log-on to steal data, e-mails

Office 365 Users Increasingly Targeted by Credential-Stealing Phishing Campaigns

Phishers targeting LinkedIn users via hijacked accounts

<https://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/>

<http://politica.estadao.com.br/noticias/geral,hackers-atacam-sistema-de-e-mails-e-de-leitura-de-documentos-do-itamaraty,1172332>

<http://www.eweek.com/security/rsa-s-securid-breach-started-with-phishing-email>

<http://www.eweek.com/security/rsa-s-securid-breach-started-with-phishing-email>

<https://www.helpnetsecurity.com/2017/09/13/phishers-linkedin-hijacked-accounts/>

<http://mspmentor.net/security/office-365-users-increasingly-targeted-credential-stealing-phishing-campaigns>

Cenário atual

- **Ataques a usuários finais:**
 - visando serviços de autenticação
 - com foco em grandes corporações
 - levando a grandes vazamento de dados
 - repositórios de credenciais sendo confundidos com invasão de BD
- **Fruto da mudança de enfoque dos atacantes**
 - é mais fácil e “rentável” atacar um usuário
 - usuários com acesso a muitas e valiosas informações
 - ataques cada vez mais convincentes, explorando
 - engenharia social
 - grande quantidade de informações expostas na Internet
 - a confiança cega que as pessoas têm em contatos conhecidos
- **Credenciais com alto valor no mercado negro**

Underground Hacker Markets

<i>Large U.S. Airline Points Account varies based on amount</i>	<i>Price based on points in account 1,500,000 - \$450 / 200,000 - \$60</i>
<i>Large International Hotel Chain Points Account</i>	<i>Price based on points in account 1,000,000 - \$200 / 200,000 - \$40</i>
<i>Popular U.S. Email Accounts (Gmail, Hotmail, Yahoo)</i>	<i>\$129</i>
<i>Popular U.S. Social Media Accounts</i>	<i>\$129</i>
<i>Corporate email accounts</i>	<i>\$ 500 per mailbox</i>
<i>Remote Access Trojans (RATs)</i>	<i>\$5 – \$10</i>
<i>High Quality Bank Accounts with Verified Large Balances of \$70,000 – \$150,000</i>	<i>6% of the balance of the account</i>
<i>Hacking Website (stealing data)</i>	<i>\$350</i>
<i>Full business dossiers on companies located within the Russian Federation</i>	<i>\$547 - \$822</i>

Underground Hacker Markets Hacking Email Accounts

- ***“No prepayments, you pay only for visible results — we will present the necessary proof.”***
- ***“Complete Confidentiality— the victim will not even notice that their email account has been hacked.”***
- ***“Burglary of the email account will be carried out without changing the password, the victim, will access their email account noticing no suspicious activity.”***
- ***“Access to all the websites registered by the owner of the email account.”***

Como são obtidas as credenciais (1/2)



- **Phishing**

- *e-mails* enviados de forma massificada
- tentam induzir o usuário a fornecer credenciais, dados financeiros ou executar ações
- alguns tipos:
 - em cascata:
 1. uso de conta forjada/genérica para envio de *e-mails* aos funcionários
 2. uso de conta invadida para envio de *e-mails* a funcionários específicos
 - burlar sistemas de reputação (como SPF/DKIM)
 - responder conversas em andamento, incluindo *links*
 - usuários acreditam em contatos conhecidos (mesmo com conteúdo "estranho")
 - *spear phishing* - direcionados a grupos específicos
 - *whaling* - direcionados a alvos chave das organizações
 - *watering hole attacks* - direcionados a *sites* acessados pelos verdadeiros alvos
 - *SMiShing* - direcionados a usuários de dispositivos móveis

EMPRESAS ALEMÃS PERDEM MILHÕES DE EUROS EM “FRAUDE DO CEO”

📅 JUL 10, 2017 👤 ROBERTO CHU 📄 AMEAÇAS DIGITAIS 💬 NO COMMENTS YET

Empresas alemãs perderam milhões de euros para o crime organizado em um golpe apelidado de "fraude do CEO" que usa falsos memorandos de altos executivos para convencer funcionários de contabilidade à transferir fundos, disse nesta segunda-feira a agência federal de segurança cibernética da Alemanha (BSI).



A agência BSI disse que as autoridades que investigam a nova fraude receberam uma lista de 5 mil alvos potenciais, e notificaram as empresas envolvidas.

Organizações criminosas estão usando informações que conseguem em redes sociais, sites corporativos, sites de empregos e até ligações para as companhias para falsificar as informações de contato de altos executivos.

A BSI disse que a Polícia Federal Criminal alemã estimou que o golpe já custou milhões de euros a empresas nos últimos meses.

A fraude visa funcionários dos departamentos de contabilidade e auditoria de uma companhia que foi autorizada a transferir dinheiro, muitas vezes usando pressão de tempo e avisos sobre um suposto "projeto secreto" para manipulá-los à realizar os falsos pagamentos.

White House officials tricked by email prankster



By [Jake Tapper](#), Anchor and Chief Washington Correspondent

Updated 2309 GMT (0709 HKT) August 1, 2017



TRUMP'S WHITE HOUSE

PUNKED

TRUMP WHITE HOUSE

EMAIL PRANKSTER TRICKS WHITE HOUSE OFFICIALS

CNN

4:45 AM PT

TODAY BOSTON 81° NEW YORK 90° PHILADELPHIA 90°

0:00 / 1:44

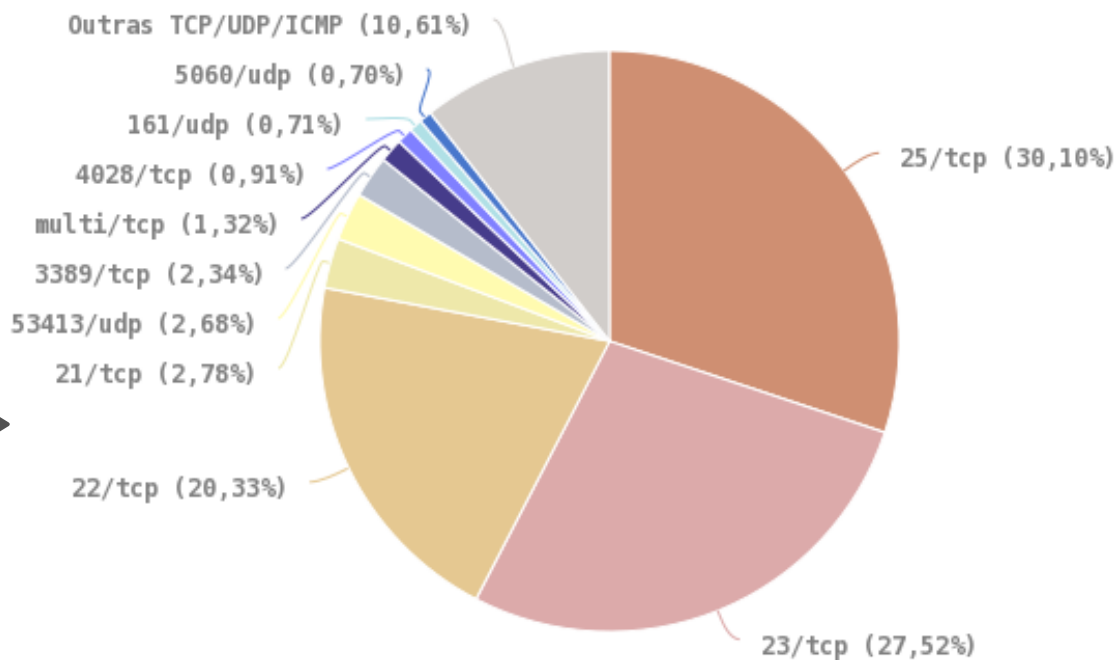
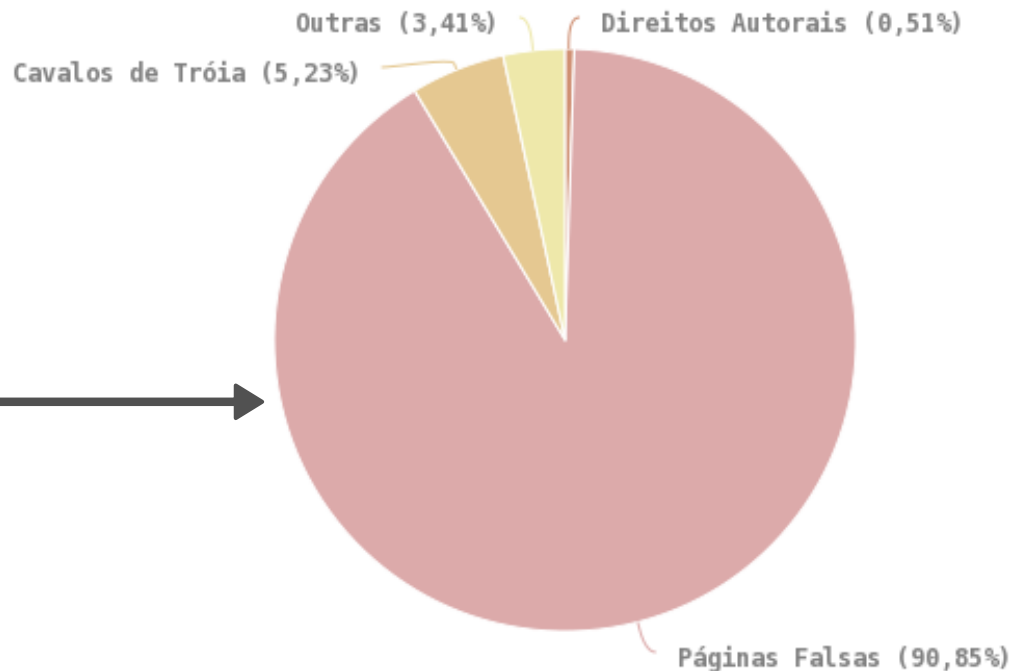
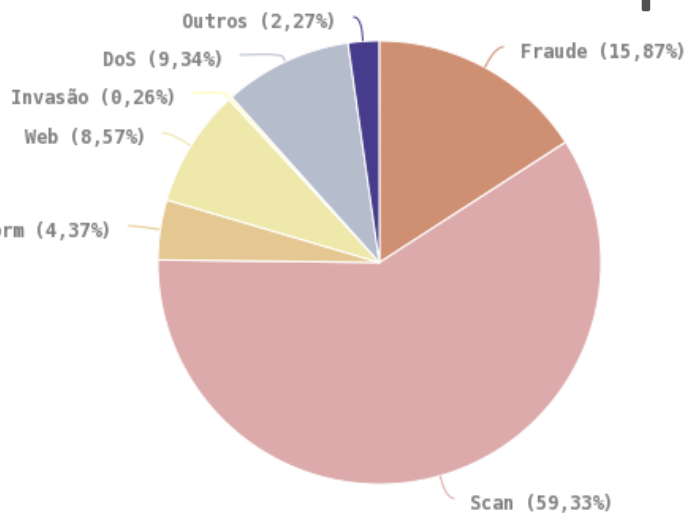
<http://edition.cnn.com/2017/07/31/politics/white-house-officials-tricked-by-email-prankster/index.html>

Como são obtidas as credenciais (2/2)

- **Instalação de *malware***
 - grande quantidade (variantes)
 - difíceis de serem detectados
 - venda de vulnerabilidades (*zero-days*)
- **Ataques de força bruta**
 - senhas fracas ou padrão
- **Falhas em sistemas**
 - transporte dos dados (não criptografados)
 - armazenagem (em texto claro, ataques a base de dados)
 - falhas de implementação
- **Informadas pelos próprios usuários (*insider threats*)**
 - forma intencional ou não intencional



Estatísticas 2016



*Insider Threat** (1/2)

**Potencial de um
(ex) funcionário, parceiro, prestador de serviços,
que tem (teve) acesso aos sistemas da organização,
de usar esse acesso,
com intuito malicioso ou não intencional,
de forma a colocar a organização em risco**

Baseado na definição do CERT-CC

<https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html>

Insider Threat (2/2)

- **Por que agem/não agem?**

- não intencionais

- ocorrem por erros humanos, displicência, preguiça, desconhecimento

- intencionais

- predisposição associada a oportunidade e motivo
- geralmente difíceis de serem detectados
 - utilizam acessos legítimos
- estão um passo à frente dos atacantes externos
- conhecem as joias da coroa
 - e principalmente as fraquezas
 - ex-funcionários conseguem persuadir mais facilmente os atuais

POLICY —

Former Energy Department employee admits trying to spear phish coworker

Feds say campaign was part of a plot to hack computers storing nuclear secrets.

DAN GOODIN - 2/3/2016, 7:33 PM



This carp was not paranoid enough. (The person pictured has nothing to do with the case reported in this post.)

A former Department of Energy employee has pleaded guilty to federal charges that he attempted to infect 80 current DOE employees with malware so foreign hackers could take control of computer systems that held sensitive information

One out of five employees is willing to sell work email passwords

0

By Kavita Iyer on MARCH 23, 2016

Security news, Technology

Scaring survey finds that one out five employees would sell corporate passwords, some for less than \$1000

According to the 2016 Market Pulse Survey, sponsored by an Austin-based security company, SailPoint Technologies, the biggest threat to a company's digital security seems to be its employees. The survey says that one in five employees would be willing to sell their work passwords to another organization, which is up from one in seven last year.

The data comes from a survey of 1,000 office workers at private organizations (with at least 1,000 employees) across the US, UK, Germany, France, the Netherlands and Australia.

The survey shows that one third (32 percent) of respondents said they share their passwords with their co-workers, and nearly two thirds (65 percent) said they only use a single password across multiple applications.

However, the most shocking revelation is that one in five employees globally said they would sell their passwords to an outsider. Of those who would sell their passwords, 44 percent would do it for less than \$1,000, and some for less than \$100.

<https://arstechnica.com/tech-policy/2016/02/former-energy-department-employee-admits-trying-to-spear-phish-coworkers/>
<https://www.techworm.net/2016/03/one-five-employees-willing-sell-work-email-passwords.html>

Como melhorar o cenário

cert.br nic.br cgi.br

Com melhorar o cenário



Conscientização

CSIRT

Preparação (1/2)

- **Conhecer a organização**
 - Identificar o *baseline*
 - conhecer o que é o “normal” da rede e dos usuários
 - fazer análise de risco, considerando
 - quais serviços, sistemas e dados são mais críticos
 - quais são os usuários chave
- **Criar um CSIRT**
- **Preparar funcionários para dar treinamentos**
 - conhecimento multidisciplinar



Preparação (2/2)

- **Definir políticas**

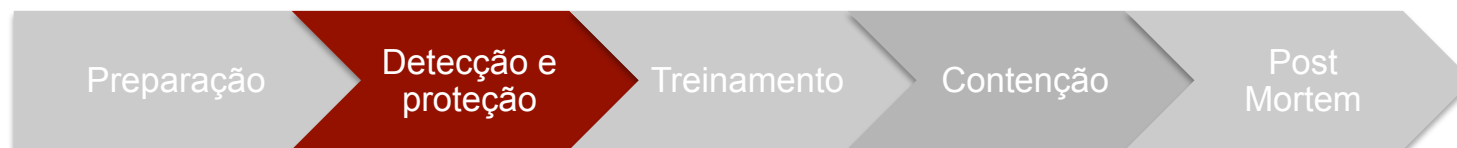
- segurança
 - contas
 - senhas / 2FA / privilégio mínimo
 - uso de equipamentos
 - BYOD
- proteção de dados
 - *backup* / engenharia social / confidencialidade (uso de redes sociais)
- contratação e demissão



Detecção e proteção

- **Implementar boas práticas**

- impedir que as mensagens cheguem aos usuários
 - monitoramento de rede (mudanças de padrão)
 - bloquear arquivos em anexo
 - implementar sistemas de combate a spam
 - listas de bloqueio, filtros de conteúdo, *greylisting*, SPF, DKIM, DMARC
- proteger os equipamentos dos usuários
 - manter os sistemas atualizados
 - usar mecanismos de segurança
 - *firewall*, antivírus, antispam, antiphishing, extensões (NoScript)
- implementar filtros de saída (*extrusion detection*)
 - netflow, DNS passivo, *data feeds*
 - gerência de porta 25



Treinamento (1/6)

- **Investir em pessoas**

- usuários essenciais para preservar a segurança da organização

- **Benefícios:**

- criar cultura de segurança na organização
 - casos não intencionais
 - reduzir e minimizar os problemas
 - casos intencionais
 - detectar os problemas
 - conhecer as consequências



Treinamento (2/6)

- **Para quem (público alvo)**

- geral
- segmentado por áreas da organização
- dedicado a funcionários:
 - área gerencial
 - com acesso privilegiado
 - com acesso a dados críticos



Treinamento (3/6)

- **Com qual periodicidade**

- prazo estipulado pela empresa (anual, semestral, etc)
- quando os casos estiverem aumentando
- quando um usuário solicitar ajuda
- quando funcionário começar a trabalhar na organização
- contínuo

- **Com qual nível de dificuldade**

- um único e grande módulo
- gradual – dividido em pequenos módulos



Treinamento (4/6)

- **Explicar de forma clara**

- qual é o problema
 - obtenção de credenciais / dados pessoais e financeiros
- quais são as consequências:
 - para a empresa
 - perdas financeiras / vazamento de dados, etc.
 - para o usuário
 - invasão de privacidade / furto de identidade / perda do emprego, etc.
- quais são os benefícios (motivação)
 - conhecimento também aplicado a vida pessoal
 - não é apenas “coisa da empresa”
- o que o usuário deve fazer
 - para se prevenir
 - em caso de cair no *phishing*



Treinamento (5/6)

- **Métodos que podem ser usados**

- um a um (quando o funcionário reportar algo)
- cartazes espelhados pela organização
- palestras (exemplos concretos / *storytelling*)
- simulações anunciadas
- simulações não anunciadas
 - ajudam na retenção
 - exploram a maior receptividade em momentos de aprendizagem (“*landing page*”)
- *gamification / active feedback*
 - participação voluntária
 - incentivo por meio de recompensas



The image shows a phishing education page from APWG (Anti-Phishing Working Group). It features a cartoon owl character and a 'WARNING!' section explaining that phishing pages try to steal personal information. The page is divided into several sections: 'How You Were Tricked' showing a phishing email from 'Wombank.com' with a 'My Inbox' attachment; 'How to Help Protect Yourself' with five numbered tips: 1. Don't trust links in an email (warning against clicking a suspicious link); 2. Never give out personal information upon email request (warning against providing credit card details); 3. Look carefully at the web address (warning against misspelled URLs); 4. Type in the real website address into a web browser; 5. Don't call company phone numbers in emails or instant messages; 6. Don't open unexpected email attachments or instant message download links. 'How Phishers Trick You Into Giving Out Personal Information' lists tactics like forging email addresses, provoking urgency, and adding suspicious links. 'How You Can Help' encourages reporting suspicious emails. The page includes a 'Legal Disclaimer' and a footer with navigation links.

<http://phish-education.apwg.org/r/en/index.htm>

Preparação

Deteção e
proteção

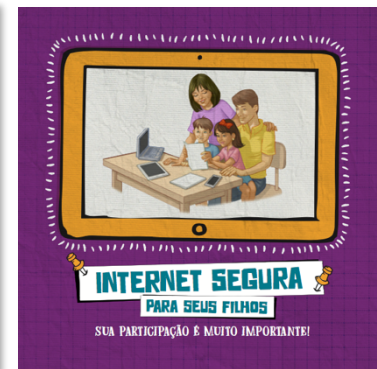
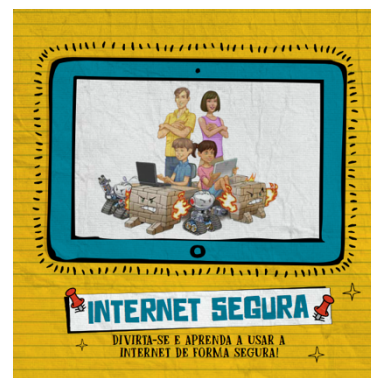
Treinamento

Contenção

Post
Mortem

Treinamento (6/6)

Cartilha de Segurança para Internet / Guias Internet Segura



<https://cartilha.cert.br/>
<http://internetsegura.br/>

Preparação

Deteção e
proteção

Treinamento

Contenção

Post
Mortem

Contenção (1/2)

- **Pro-atividade como forma de combate**
 - *“if you see something, say something”*
 - *“see phishing, report phishing”**
- **Quanto antes a empresa souber**
 - mais rápido poderá atuar
 - mais eficiente poderá ser a contenção
 - menores serão os danos
 - evitar outros casos (senhas sendo reutilizadas)

* <https://apwg.org/report-phishing/>



Contenção (2/2)

- **Funcionários devem ser incentivados a reportar**
 - quando suspeitarem:
 - que tenham instalado *malware*
 - que tenham caído em *phishing*
 - que o equipamento pode ter sido invadido
 - de algum comportamento ou situação estranha/suspeita
- **CSIRT pode ser o caminho para receber as notificações**
 - deve ser de fácil acesso e amigável
 - garantir a confidencialidade
 - implementar canais anônimos



Post Mortem

- **Analisar métricas**
 - considerar que decisões humanas são subjetivas e dependem do momento e das técnicas de persuasão usadas
- **Usar reforço positivo para os casos que foram notificados**
 - falsos positivos são bem vindos
- **Verificar o que deu errado em cada caso e usar isso para melhorar todo o processo**
 - refinar controles / customizar ferramentas
- **Rever as etapas anteriores**



Considerações finais

Se o usuário é realmente o elo mais fraco da segurança da informação, o que podemos fazer para que ele se torne um aliado?

Se a segurança é em camadas, não estaria a camada referente ao usuário sendo sobrecarregada com decisões de segurança?

O que podemos fazer ou o que deveríamos estar fazendo para auxiliá-los?

Referências

Advanced Persistent Training: Take Your Security Awareness Programme to the Next Level, Jordan Schroeder

Insider Threat The CERT Division

<http://www.cert.org/insider-threat/>

Common Sense Guide to Mitigating Insider Threats, Fifth Edition

http://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

Obrigada
www.cert.br

 miriam@cert.br

 [certbr](https://twitter.com/certbr)

14 de setembro de 2017

nic.br egi.br
www.nic.br | www.cgi.br