online (and offline) banking, phishing and other types of fraud

luiz eduardo

agenda

- intro/ history
- evolution of phishing
- atm fraud
- videos
- conclusion

intro / history

- nothing new (and won't go away)
- .com's marketing helped the scam industry
- in some places it got extended outside the webspace world

phishing

- a means to a fraud
  - spam/ forged emails
  - fake sites
  - trojans/ malware
  - voice
  - sms
  - wi-fi phishing (bad dns entries again)
  - web 2.0 (javascript, ajax, xss, etc)
- why some third world countries banks had to keep up with this?
- APWG breaks it down into:
  - financial, retail, isps, other

phishing / financial

- identity theft
- account withdrawn
- buying stuff with someone else's $
- and, for some financial institutions, security is an after thought

- but, why?
  - high roi
  - risk free *
  - lack of human interaction
  - lack of user knowledge

spam

- someone will fall for it
- out of 1 million spam messages, 0.01%
- spams do get better too

fake websites

- usually not hosted in the US
- usually not up for more than a few days
- reason why the emails go out in batches/ seasonal *

trojans/ malware

- email
- email directing to a fake site
- social networking websites
- im's

after download of the malicious binary

- user could be redirected to bad site instead of good one (pharming)
- the drive-by pharming case (poisoning the gateway, not the machine)
- simply logging data and sending to a site/ email

voice phishing

SecureWorks® the information security experts Client Su

Home | Services | Solutions | Research | Media | Company | Partners | Contact

Research

Threat Analyses
Blog
Newsletter
Webcasts
Articles

Home › Research › Threat Analyses › Call Forwarding Phishing Attack

Call Forwarding Phishing Attack

- **URL:** http://www.secureworks.com/research/threats/callforward
- **Date:** April 25, 2007
- **Author:** Don Jackson

SecureWorks discovered a new Phishing scheme this week which uses a "Call Forwarding" component. The victim receives an email from the phisher telling them that their bank needs to verify their phone number immediately. If they do not confirm their phone number their account will be suspended. The instructions are as follows:

Step 1- Go to your phone and Dial *72 Step 2- Dial 7075314910 (XYZ Bank Secure Line)
Step 3- Your phone is confirmed.

You will receive a call from us in 1 h for final verification!

If you have confirmed your phone, you can continue the update process:

- or email
- spit
- eavesdropping (mim)
- for example:



LAYER one

sms

- person receives a sms asking to visit a webpage, call a number, free stuff, etc

wi-fi phishing

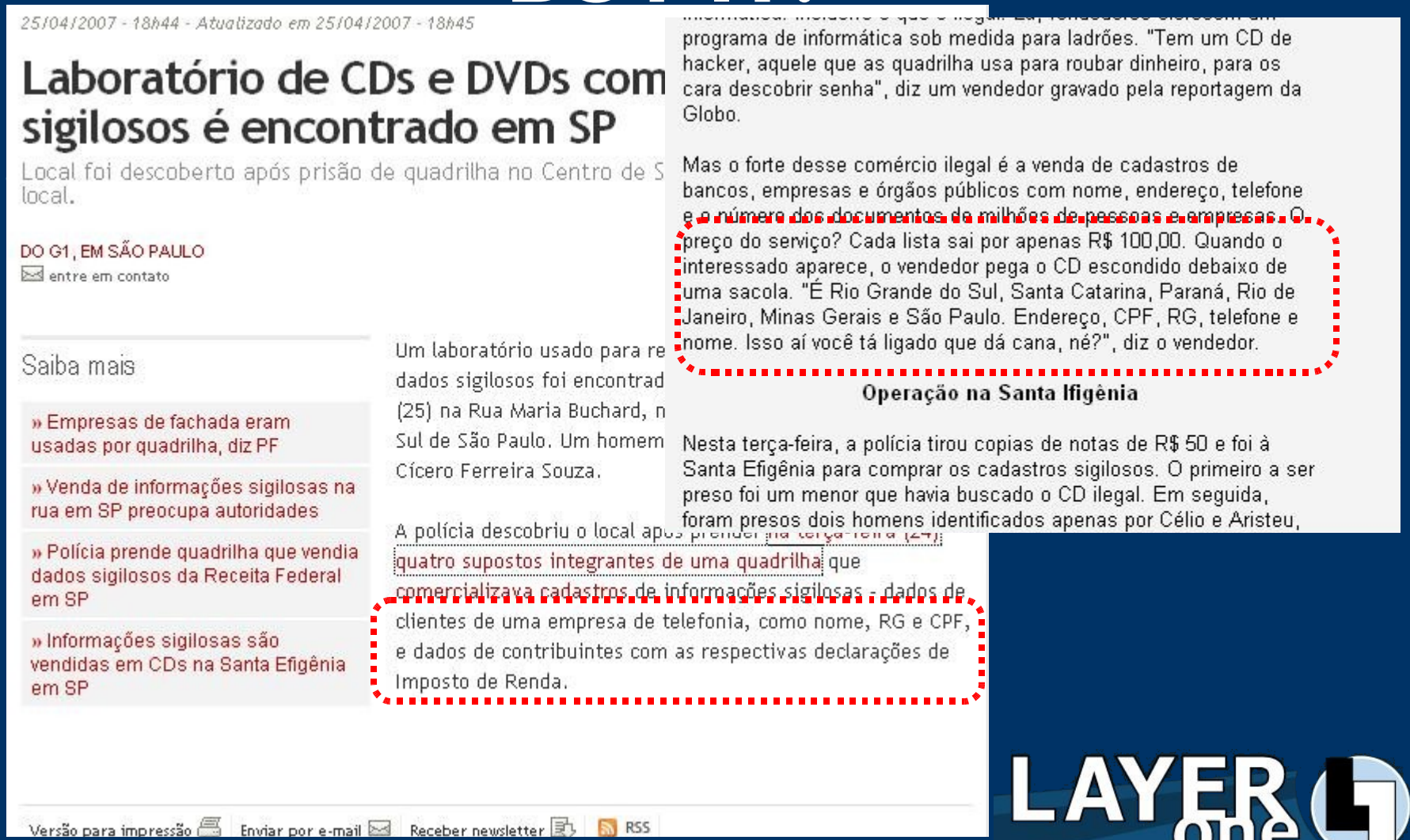
- evil twin
  - (better be) specially in hotspots
  - the user will be handled an ip for a dns with bad entries for “known-desired” sites (aka: banks, ebay, paypal, amazon, etc)
  - or a simple mim attack

web 2.0

- javascript
- ajax
- xss
- mim

- check comments from Billy Hoffman on his shmoocon 07 talk

but, if you need people's information, why can't you just BUY IT?



25/04/2007 - 18h44 - Atualizado em 25/04/2007 - 18h45

Laboratório de CDs e DVDs com sigilosos é encontrado em SP

Local foi descoberto após prisão de quadrilha no Centro de S local.

DO G1, EM SÃO PAULO

entre em contato

Saiba mais

» Empresas de fachada eram usadas por quadrilha, diz PF

» Venda de informações sigilosas na rua em SP preocupa autoridades

» Polícia prende quadrilha que vendia dados sigilosos da Receita Federal em SP

» Informações sigilosas são vendidas em CDs na Santa Efigênia em SP

Um laboratório usado para re
dados sigilosos foi encontrad
(25) na Rua Maria Buchard, n
Sul de São Paulo. Um homem
Cícero Ferreira Souza.

A polícia descobriu o local após prender na terça-feira (24) quatro supostos integrantes de uma quadrilha que comercializava cadastros de informações sigilosas - dados de clientes de uma empresa de telefonia, como nome, RG e CPF, e dados de contribuintes com as respectivas declarações de Imposto de Renda.

Versão para impressão | Enviar por e-mail | Receber newsletter | RSS

programa de informática sob medida para ladrões. "Tem um CD de hacker, aquele que as quadrilha usa para roubar dinheiro, para os cara descobrir senha", diz um vendedor gravado pela reportagem da Globo.

Mas o forte desse comércio ilegal é a venda de cadastros de bancos, empresas e órgãos públicos com nome, endereço, telefone e o número dos documentos de milhões de pessoas e empresas. O preço do serviço? Cada lista sai por apenas R$ 100,00. Quando o interessado aparece, o vendedor pega o CD escondido debaixo de uma sacola. "É Rio Grande do Sul, Santa Catarina, Paraná, Rio de Janeiro, Minas Gerais e São Paulo. Endereço, CPF, RG, telefone e nome. Isso aí você tá ligado que dá cana, né?", diz o vendedor.

Operação na Santa Ifigênia

Nesta terça-feira, a polícia tirou copias de notas de R$ 50 e foi à Santa Efigênia para comprar os cadastros sigilosos. O primeiro a ser preso foi um menor que havia buscado o CD ilegal. Em seguida, foram presos dois homens identificados apenas por Célio e Aristeu,

LAYER one

06/12/2006 - 09h52m - Atualizado em 06/12/2006 - 12h26m

AGÊNCIA ESTADO

RSS
Imprimir
Enviar por e-mail
Receber Newsletter

CAMELÔ OFERECE SOFTWARE PIRATA A DIRETOR DA MICROSOFT EM SP

Executivo se impressionou com "sinceridade" dos vendedores.
Preço de "tabela" do Windows Vista é R$ 10 nas ruas da cidade.

Tamanho da letra A- A+

O diretor mundial de Propriedade Intelectual
americana Microsoft, Keith Beeman, comanda
exército de 150 funcionários contra a falsificação
softwares em um escritório envidraçado, com vista
as congeladas Montanhas Cascade, na cobertura de
dos cem prédios que compõem o conglomerado
empresa em Seattle (EUA). O fio da meada com q
equipe tece a complexa rede mundial de pirat
termina, no Brasil, nas mãos de um garoto de 20 a
mulato de cabelos rastafári, 2º grau incompleto,
passa os dias atrás de uma barraca de pap
vendendo cópias toscas no maior centro de eletrôn
do país, a Santa Ifigênia, e atende pelo sugestivo no

Na terça-feira (5), as duas pontas dessa rede, esp
convite do jornal "O Estado de S. Paulo", Beema

LAYER one

how to resolve the problem

it all comes down to

WHO IS RESPONSIBLE FOR THE THEFT?

solutions

- ssl on all banks initial page
- some sort of client application pushed by the banks website (hmm)
- captchas
- anti-spam / anti-spyware/ anti-malware
- enterprise (appliances)
- home (applications/ os flavors/ webbrowser flavors and smaller appliances)
- some banks outsourced phishing incident response handling

won't ssl protect you?

- not if
  - trojan installed (ssl connection still trusted/safe)
  - and... human factor

virtual keyboards

- click / screen shot loggers

sitekey?

- great paper explaining why not...

http://cr-labs.com/publications/SiteKey-20060718.pdf

the “security card”

real tokens

- expensive
- for high profile customers
- or if the client is willing to pay for it

atm fraud

- again, take money from someone else
  - card / pin stealing
  - card cloning
  - fake atm machines
  - fake atm machine covers
  - hacking the atm itself (programming codes, tests, insider info, etc) *
  - money stealing on the spot
  - people hijacking
- or simply from the bank *


Bradesco
Tarifas de
Serviços Bancários
Multi Expresso

atm fraud solutions (?)

- smartcards
  - still needs the magstripe
  - clonable? (or at least readable?) *
  - compatibility
- integration with cellphones
  - initially for sms'ing an one time password (also for online banking)
  - later for real internet banking (which could possibly open a whole new can of worms)
  - cellphone banking available in some places in Europe, South Africa, New Zeland, Brazil and Japan
  - apparently cingular to offer cellphone banking in the US
  - convergence and phones doing lots of stuff, user able to install crap
- 10,000 steps for the person to be able to take out money (or do another transaction via online banking for that matter)
- restrictions: daily amounts (or by time)
- and...

FUJITSU THE POSSIBILITIES ARE INFI Fujitsu Introduces New Biometric Security Soluti

Home > News > Press Releases > Archives > By Month
Brazil

*This is an English-language summary of

Fujitsu Introduces New Biometric Sec
Brazil

Fujitsu PalmSecure ™ biometric palm vein aut
financial corporations requiring high-level secu

Sao Paulo, July 12, 2006 — Fujitsu do Brasil Ltda. tod
biometric security solution featuring a compact, high-perf
patterns to verify user identification in bank ATM transacti
is already being tested internally at Banco Bradesco S.A.
Latin America, with general operation scheduled to start s

After researching various biometric technologies, Bradesc
features, such as high levels of verification accuracy and l
it easier to be accepted by customers of the bank.

PalmSecure was developed by Fujitsu as the world's first
authentication system. The sensor captures the palm vei
with pre-registered data to authenticate the user's identity
35mm) and can be safely and flexibly used in a wide rang
and for building and room access.

For more information about Fujitsu do Brasil Ltda.: http://

For more information about Fujitsu PalmSecure palm vein
http://www.fujitsu.com/global/about/rd/200506palm-vein.ht

About Fujitsu

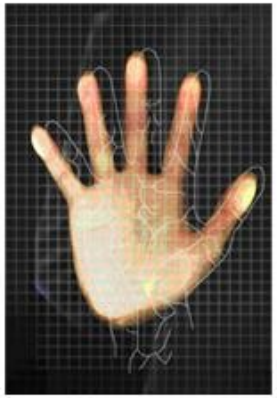
Fujitsu is a leading provider of customer-focused IT and c
marketplace. Pace-setting device technologies, highly rel
products, and a worldwide corps of systems and services
deliver comprehensive solutions that open up infinite poss
Headquartered in Tokyo, Fujitsu Limited (TSE:6702) repo
trillion yen (US$40.6 billion) for the fiscal year ended Mar
further information.

About Bradesco

Bradesco has the leadership in the Brazilian private financ
corporate customers. Its customer service network has m
Branches, Service Branches, Bank Postal (Post Office Br
more than 23,000 Automated Teller Machines in the Rede

R&D
Fujitsu Palm Vein Technology

How secure are your assets? Can your personal identification number be easily guessed? As we increasingly rely on computers and other machines in our daily lives, ensuring the security of personal information and assets becomes more of a challenge. If your bank card or personal data falls into the wrong hands, others can profit at your expense. To help deal with this growing problem, Fujitsu has developed a unique biometric security technology that puts access in the palm of your hand and no one else's.



Fujitsu's palm vein authentication technology consists of a small palm vein scanner that's easy and natural to use, fast and highly accurate. Simply hold your palm a few centimeters over the scanner and within a second it reads your unique vein pattern. A vein picture is taken and your pattern is registered. Now no one else can log in under your profile. ATM transactions are just one of the many applications of this new technology.

Fujitsu's technology capitalizes on the special features of the veins in the palm. Vein patterns are unique even among identical twins. Indeed each hand has a unique pattern. Try logging in with your left hand after registering with your right, and you'll be denied access. The scanner makes use of a special characteristic of the reduced hemoglobin coursing through the palm veins — it absorbs near-infrared light. This makes it possible to take a snapshot of what's beneath the outer skin, something very hard to read or steal.

Besides the high accuracy of a false rejection rate of 0.01% and a false acceptance rate of less than 0.00008 %(as of February, 2005), Fujitsu's contactless palm vein authentication offers a range of advantages over other biometric technologies.

"Fingerprint scans and face recognition ID methods are associated with the police by some people on a psychological level," says Shigeru Sasaki, director of Fujitsu's Media Solutions Laboratory. (Interview date: Feb 2nd, 2005) "In public areas, others don't like the thought of touching what everyone else has touched for sanitary reasons. This is why we created a contactless palm vein scanner."

ATM with PalmSecure™

The near-infrared rays in the palm vein scanner have no effect on the body when scanning. To protect the privacy and personal information of the user, the registered biometric information itself can be stored in bank cards. Bank of Tokyo-Mitsubishi ATMs in Japan are already equipped with palm vein scanners developed by Fujitsu. Users access their accounts by having a scan of their palm compared to a pre-registered scan stored on their bank card. This is expected to help reduce the growing cases of bank card thefts and fraudulent financial transactions.

Amid the heightened security climate in recent years and fears of terrorism, there has been a

end user education / awareness

- websites
- ads on magazines
- ads on billboards
- prime time ads on tv

examples

- taking cash from an atm in the US
  - insert the card
  - punch the pin number
  - select operation
  - remove the card
  - take cash

examples cont.

- taking cash from an atm in Brazil
  - insert the card
  - punch the pin number
  - select operation
  - use password # XYZ from the poor man's security token
  - insert card again
  - take cash and run

examples cont.

- taking cash, again in Brazil
  - insert card
  - punch pin number
  - select operation
  - punch the date / month/ year/ day of birth
  - insert card
  - take cash and run

examples cont.....

- taking cash in Venezuela
  - insert the card
  - punch pin number
  - punch your id's first (or last) 3 digits
  - ??????????????????????????????????????
  - (find another atm)
  - (cry for help)
  - take cash

videos

con clusion

- it's probably gonna get worse
- evolution accross the board
- and, some places will not change
- never travel without cash :-)

questions?

luiz eduardo
le (at) atelophobia.net