Malware Patrol

Os desafios de coletar e monitorar URLs
que apontam para Malwares

GTS-13 – 20/06/2009

André D. Corrêa, CISSP, ITIL Certified
www.malwarepatrol.net

Agenda

- Histórico e motivação
- Estatísticas
- Arquitetura da solução
- Captura e monitoramento de URLs e sistema de alerta
- Colaboração com CSIRTs, grupos de segurança e a comunidade
- Listas disponíveis
- Malware vs. AdWare, PoC, HackTool, etc
- Técnicas de ofuscamento de URLs
- Samples não classificados
- Desafios atuais
- Próximos desenvolvimentos

Malware Patrol

- "**Malware** Patrol is a free, automated and user contributed system for verifying URLs for the presence of Viruses, Trojans, Worms, or any other software considered **Malware**."
- Nossos objetivos:
  - **Coletar:** Um sistema de *crawling* automatizado coleta as URLs que apontam para extensões perigosas;
  - **Analisar:** Cada URL é analisada para detectar a eventual presença de **Malware**;
  - **Bloquear:** Disponibilizamos listas em 29 formatos para que administradores possam bloquear o acesso a URLs infectadas;
  - **Alertar:** Administradores de domínios e de servidores que hospedam **Malware** recebem alertas por e-mail. Alguns grupos de segurança e CSIRTs também são avisados;
  - **Monitorar:** URLs infectadas são monitoradas para garantir que as listas de bloqueio estejam sempre atualizadas e confiáveis. Todas as URLs na base de dados é visitada diariamente;

Malware Patrol

- Não é apenas uma *block list*, realiza colaboração com outros grupos e procura remover **Malwares** da Internet;
- Acessos originados de diversos países e TLDs, sendo os mais comuns:
  - Brazil
  - IP – sem DNS reverso;
  - .com
  - .net
  - Germany
  - Italy
  - USA Educational
  - Switzerland
  - USA Military
- Grande quantidade de acessos efetuados durante o minuto zero de cada hora e picos extras nas horas 00, 06, 12 e 18. Este comportamento causa alguma lentidão no site durante estes períodos. Existem outros 59 minutos a cada hora;
- Operando praticamente sem *downtime* por 4 anos;

Histórico e motivação

- Junho/2005 - motivado por uma discussão na GTS-L, o projeto iniciou com uma pequena lista de URLs maliciosas que circulavam entre os membros do grupo. Devido à dificuldade de monitorar essas URLs de forma manual, foi desenvolvido um sistema simples que disponibilizava a lista de URLs apenas nos formatos texto e para o *Squid Proxy*;
- Março/2007 - a empresa Kaspersky doa para o projeto, licença de seu Anti-Virus;
- Junho/2008 - a empresa F-Prot doa para o projeto, licença de seu Anti-Virus;
- Outubro/2008 - o projeto passa a se chamar **Malware Patrol** – **www.malwarepatrol.net**;

Histórico e motivação

- Listas de bloqueio são serviços baseados na **confiança** dos usuários. É preciso demonstrar confiabilidade e estabilidade. Não são aceitos erros (ex: bloqueio indevido de sites importantes);
- Atitude positiva quando recebemos pedidos de remoção de domínios das listas;
- O bloqueio de *downloads* por extensão (ex: exe, scr, pif, etc) não é uma solução totalmente eficaz. Extensões que "não podem" ser bloqueadas apresentam riscos;
  - Bugs Adobe Acrobat Reader (pdf);
  - Bugs Flash Player (swf);
  - Bug libpng;
  - Etc...;

Histórico e motivação

Release date: June 9, 2009
Vulnerability identifier: APSB09-07
Platform: All Platforms

Summary

Critical vulnerabilities have been identified in Adobe Reader 9.1.1 and Acrobat 9.1.1 and earlier versions. These vulnerabilities would cause the application to crash and could potentially allow an attacker to take control of the affected system.

This update resolves a stack overflow vulnerability that could potentially lead to code execution (CVE-2009-1855).

This update resolves an integer overflow that leads to a Denial of Service (DoS); arbitrary code execution has not been demonstrated, but may be possible (CVE-2009-1856).

This update resolves a memory corruption vulnerability that leads to a Denial of Service (DoS); arbitrary code execution has not been demonstrated, but may be possible (CVE-2009-1857).

This update resolves a memory corruption vulnerability in the JBIG2 filter that could potentially lead to code execution (CVE-2009-1858).

This update resolves a memory corruption vulnerability that could potentially lead to code execution (CVE-2009-1859).

This update resolves a memory corruption vulnerability in the JBIG2 filter that leads to a Denial of Service (DoS); arbitrary code execution has not been demonstrated, but may be possible (CVE-2009-0198).

This update resolves multiple heap overflow vulnerabilities in the JBIG2 filter that could potentially lead to code execution (CVE-2009-0509, CVE-2009-0510, CVE-2009-0511, CVE-2009-0512, CVE-2009-0888, CVE-2009-0889).

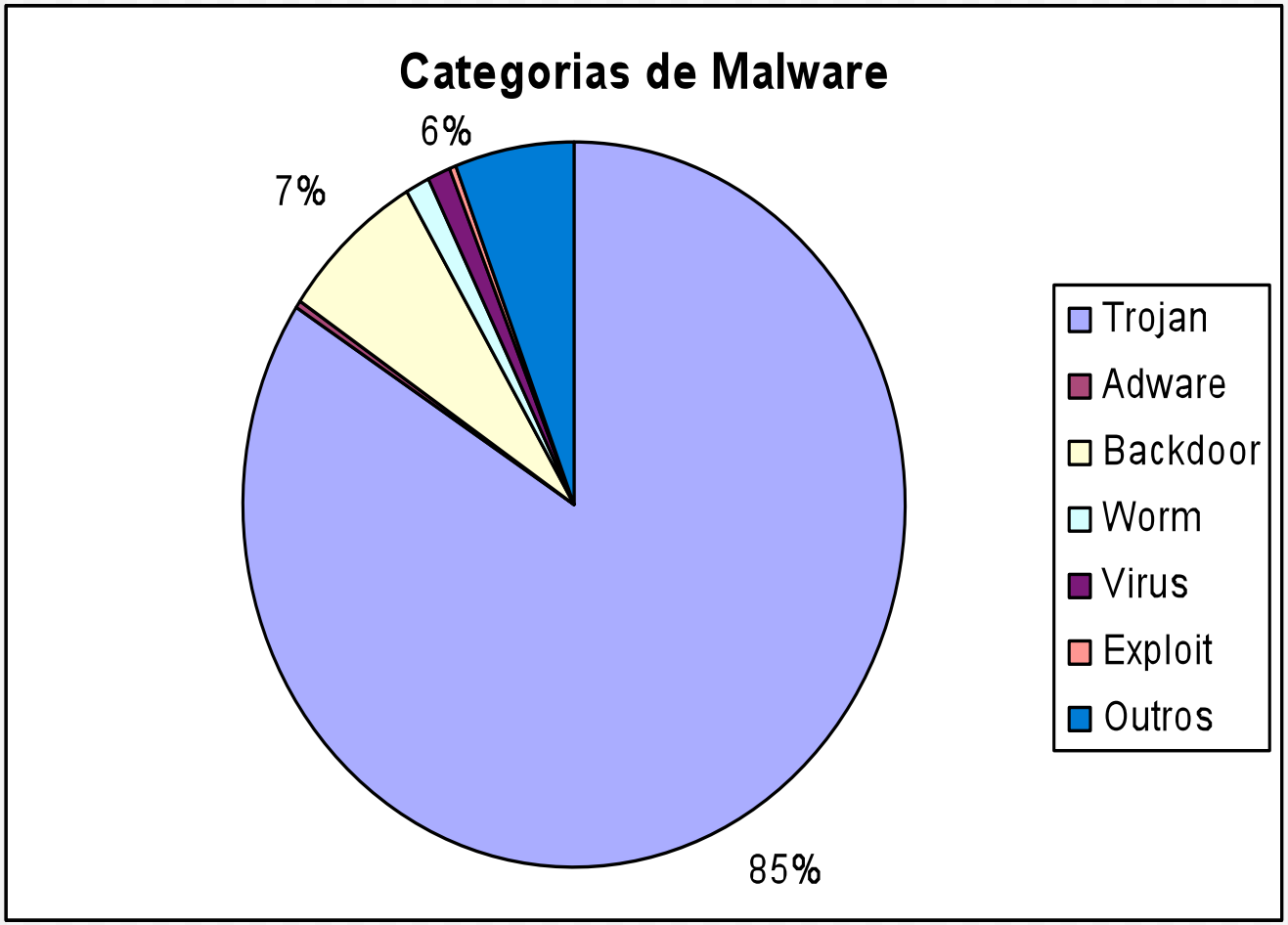
This update resolves multiple heap overflow vulnerabilities that could potentially lead to code execution (CVE-2009-1861).

Additionally, this update resolves Adobe internally discovered issues.

Estatísticas

- URLs ativas: ~4200;
- URLs “periogosas”: ~112.000;
- Total de URLs no BD: ~3.800.000;
- Hits por mês: ~4.000.000;
- TLDs hospedando Malware: ~50;
- ASNs hospedando Malware: ~93;
- Hosts/domains hospedando Malware: ~862;
- Malwares identificados únicos: 8.900;
- Extensões consideradas perigosas: ad, ade, adp, bas, bmp, cab, chm, cmd, com, cpl, crt, exe, hlp, inf, ins, isp, jar, lnk, msc, msi, msp, mst, pcd, pdf, pif, rar, reg, scr, sct, shb, shs, swf, url, vb, vbe, vbs, vss, vst, vsw, ws, wsc, wsf, wsh, zip;
- Listas de bloqueio disponíveis para uso não comercial;

Estatísticas



Estatísticas

- Alguns Malwares que foram inicialmente identificados devido ao envio de binários coletados pelo projeto:
  - Trojan-Downloader.Win32.Dadobra.nr
  - Trojan-Downloader.Win32.Banload.ack
  - Trojan-Downloader.Win32.Banload.wln
  - Trojan-Downloader.Win32.Banload.bmq
  - Trojan-Downloader.Win32.Banloade.boz
  - Trojan-Downloader.Win32.Banload.azy
  - Trojan-Downloader.Win32.Banload.bxt
  - Trojan-Spy.Win32.Banbra.oc
  - Trojan-Spy.Win32.Banker.cfd
  - Trojan-Spy.Win32.Banker.chz
  - Trojan-Spy.Win32.Banker.ceu
  - Trojan-Downloader.Win32.VB.awm
  - Trojan-Banker.Win32.Agent.br
  - Trojan-Downloader.Win32.Small.dli
  - Trojan-Downloader.Win32.VB.atz
  - Trojan-Spy.Win32.Banker.cfx
  - Trojan-Spy.Win32.Bancos.zm
  - ...

Estatísticas

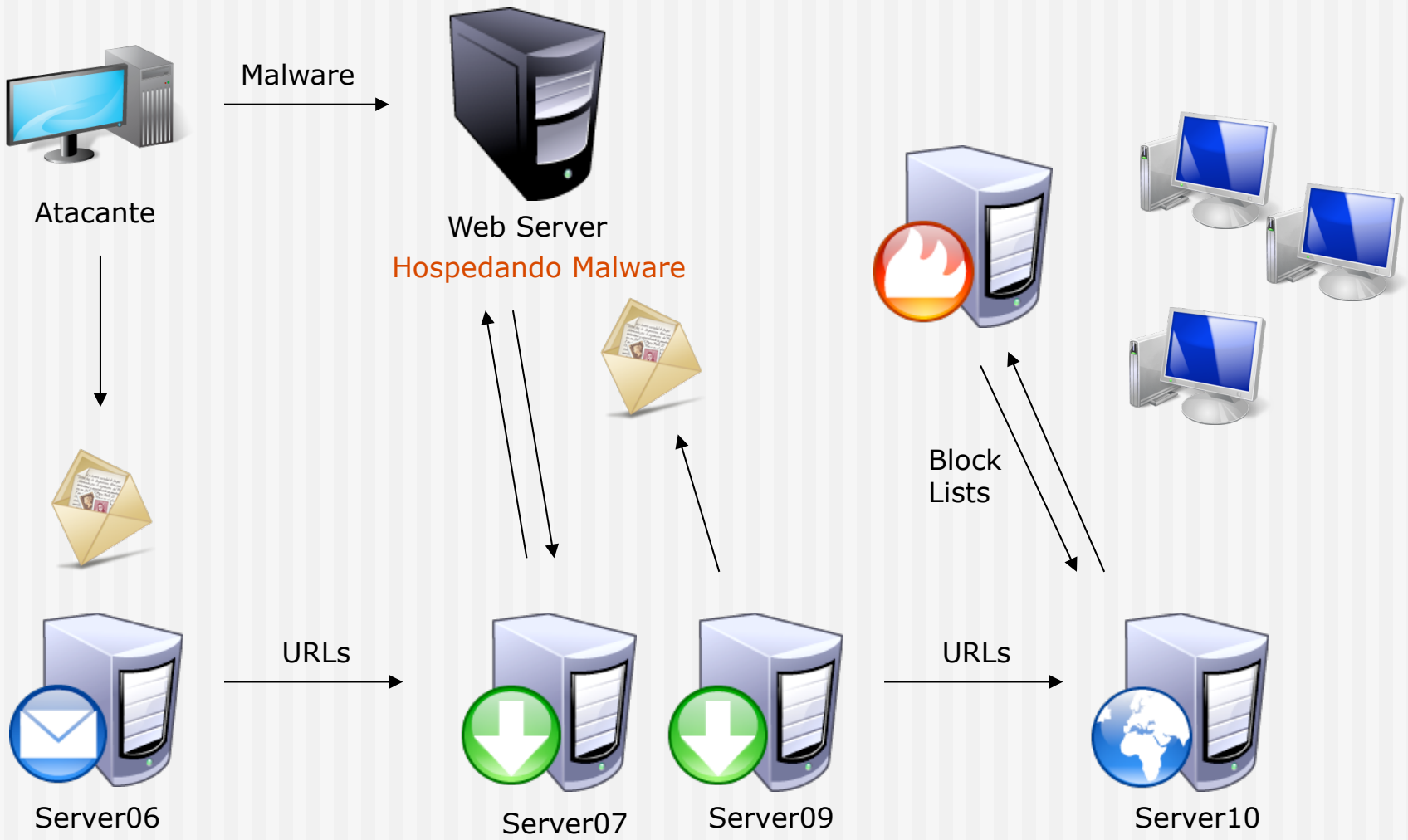
- A maioria dos binários coletados foram gerados e “packed”. Identificamos aproximadamente 150 packers diferentes, entre eles:

- ACProtect
- Alloy
- Armadillo
- ASPack
- ASProtect
- BeRoEXEPacker
- Cexe
- Crypto-Lock
- CRYPToCRACks
- DalKrypt
- Ding Boys PE-lock
- EXE Shield
- EXECryptor
- eXPressor
- EZIP
- FreeBASIC
- FreeJoiner
- Freshbind
- FSG
- Goats Mutilator
- iPB Protect
- kkrunchy
- Krypton
- MicroJoiner
- MinGW
- MoleBox
- nPack
- NsPack
- Obsidium
- Packman
- PC Shrinker
- PEBundle
- PECompact
- PESpin
- PureBasic
- RLPack
- ShellModify
- Ste@lth
- tElock
- Themida
- Upack
- UPX
- Xtreme-Protector
- yodas Crypter

Estatísticas

- Domínios .br hospedando Malware:
  - ig.com.br
  - hpg.com.br
  - hpgvip.com.br
  - yahoo.com.br
  - theblog.com.br
  - thomas.org.br
  - networker.com.br
  - **mte.gov.br - Trojan-Downloader.Win32.Agent.rqk**
  - diariodeeditais.com.br
  - topoevn.com.br
  - **diamantino.mt.gov.br - Trojan-Downloader.Win32.Banload.dts**
  - bandleader.com.br
  - plughosting.com.br
  - emes.com.br
  - euqueromeusite.com.br
  - k8.com.br
  - ...

Arquitetura da solução



Arquitetura da solução

- O sistema é composto por servidores, hospedados em 3 Data Centers nos EUA:
- Todos os softwares utilizados são Open Source, exceto os Anti-Virus da Kaspersky e F-Prot:
  - Linux Slackware;
  - FreeBSD;
  - Apache HTTPd;
  - LightHTTPd;
  - NGNIX;
  - MySQL;
  - Exim;
  - Stunnel;
  - Nagios;
  - RRDTool;
  - Perl + modulos;
  - VSFTPd;

Captura e monitoramento de URLs

- As URLs são recebidas através dos seguintes sistemas:
  - Formulário no site (com validação);
  - E-mail para recebimento de mensagens suspeitas – void@malware.com.br;
  - *SPAM traps*;
  - Contribuições de CSIRTs e grupos de Segurança;
  - Monitoramento de listas de discussão e newsgroups que tratam de botnets e segurança de IRC;
  - *Web crawling*;
  - Monitoramento de IRC;
- Todas as URLs recebidas e que apontam para extensões consideradas perigosas são adicionadas a uma *queue*;
- Essa *queue* é visitada de hora em hora por um *crawler* que tenta coletar os binários suspeitos;
- Todos os binários coletados são avaliados por sistemas de Anti-Virus. Caso um **Malware** seja encontrado, a URL é incluída nas listas de bloqueio;

Captura e monitoramento de URLs

- Se o binário coletado não for classificado como **Malware**, uma análise superficial é realizada. Essa análise inclui:
  - Sistema de pontuação para tentar identificar com maior precisão possíveis **Malwares**;
  - Probabilidade por extensão (ex: scr, pif, bat);
  - Probabilidade por domínio (whitelist e blacklist);
  - Probabilidade por string (ex: vídeo.scr, amor.exe);
  - Detecção de *Packers*;
  - Uso de *PeFile* na análise;
- Binários com fortes características de **Malware** são enviados a *vendors* de Anti-Vírus para análise detalhada;
- Os binários podem também ser submetidos a serviços on-line como Vírus Total e Jotti para análise por múltiplos Anti-Vírus;
- Não utilizamos *sandbox* por ser de difícil automatização e requerer muitos recursos de hardware;

Captura e monitoramento de URLs

- As URLs visitadas podem adquirir os seguintes status:
  - *Unexpected Content-Type*;
  - Arquivo sem perigo (white list);
  - Aguardando confirmação de e-mail (formulário web);
  - *404 - Not Found*;
  - *Fila de verificação*;
  - *Malware confirmado*;
  - *Malware não detectado*;
  - URL de domínio banido;
  - Badware;
- Todas as URLs cadastradas, com exceção dos arquivos considerados sem perigo e domínios banidos, são visitadas diariamente para assegurar que seus status não mudaram;
- Realizamos revisão diária dos binários não classificados;
- Todos os *crawlers* são escritos em Perl e trabalham em *multi-thread*;

Captura e monitoramento de URLs

```
bash-2.05b# perl scripts/m-spider.pl -single_thread  -browser ie6_w2k -grab_follow 1 -grab_URL "http://www. smktm.net/v2/view/sys_/
        Relatorio-Nov-2008.doc"

#### Running in single thread mode... ####

Starting Malware Spider 1.28-lppqF ( ) UA: ie6_w2k ...

-------------------------------------------------
Grabbing (http://www.smktm.net/v2/view/sys_/Relatorio-Nov-2008.doc - doc)
REDIRECT: 301 - ->Connection: close
->Date: Fri, 21 Nov 2008 15:02:32 GMT
->Location: http://www.smktm.net/v2/view/sys_/Relatorio-Nov-2008.doc/
->Server: Apache/1.3.37 (Unix) mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 PHP/4.4.6 FrontPage/5.0.2.2635.SR1.2
        mod_ssl/2.8.28 OpenSSL/0.9.8a
...

Following Redirects (0)

->Date: Fri, 21 Nov 2008 15:02:40 GMT
->Location: http://www.smktm.net/v2/view/sys_/Relatorio-Nov-2008.doc/Relatorio-Quinzena-Nov-2008.exe
->Server: Apache/1.3.37 (Unix) mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 PHP/4.4.6 FrontPage/5.0.2.2635.SR1.2
        mod_ssl/2.8.28 OpenSSL/0.9.8a
...
Sending localtion to void - http://www.smktm.net/v2/view/sys_/Relatorio-Nov-2008.doc/Relatorio-Quinzena-Nov-2008.exe - to
        void@malware.com.br

Grabbed URLs: 1
New URLs found: 1
Done!!!
```

Sistema de Alerta

- Sempre que verificamos uma URL que aponta para um **Malware**, são enviados e-mails de alerta para:
  - Contato cadastrado no *whois* para o domínio;
  - Contato cadastrado para o *ASN* onde está hospedado o servidor do domínio;
  - CERT/CSIRT responsável pelo *TLD* correspondente;
  - Outros contatos de CSIRTs ativos para o domínio ou *TLD*;
- Menos de 15% dos alertas enviados são respondidos:
  - Aproximadamente 70% destes, informam que o **Malware** foi removido e o site/conta de acesso suspensos;
  - Os demais pedem que se registre a ocorrência por formulários web ou que sejam incluídas informações como cabeçalhos de e-mail;
- Nossa caixa postal de alerta passou a receber SPAM e *Phishing Scams* depois de poucos meses de uso;

Sistema de Alerta

The Malware Patrol Team (www.malwarepatrol.net) discovered a Malware hosted in the domain: entre-panas.net

Please review the following information and take the appropriate measures to remove the Malware as soon as possible. If you are not responsible for the domain, please forward this message to whom it may concern.

- MBL# 99356
- Malware found: Trojan-Banker.Win32.Banker.bbb
- Insertion date: 08:00:48 17/Nov/2008 UTC
- URL: http :// www.entre-panas.net/fashionbaby.exe
- Host/Domain: entre-panas.net
- Host country: US
- Protocol: http
- Extension: exe
- Malware MD5: 30ac25bf2b47ad613741aa6c71516df8
- Malware SHA1: 2b6e1fac3bd9e9fdd88ba7f0ae81a0127c7ce907

We believe this URL is being used in Phishing Scams. Contact the local authorities to investigate the criminal activity right away.

If you have any questions or additional information, feel free to contact us at: alert (at) malware.com.br or visit our web site.

The Malware Block List Team

http://www.malware.com.br

Sistema de Alerta

Hello,

Thank you very much for the information that you have provided. I will terminate this site and corresponding hosting account right away.

Best Regards,
Peter
Support@Freehostia.com
http://www.freehostia.com

Sistema de Alerta

Dear,

We are BELNET CERT, the Computer Emergency Response Team for the BELNET community. BELNET CERT coordinates investigations and information flow regarding security incidents in which its constituency is involved, whether as source or as victim of an incident.

The device at maggiedeblock.be does not belong to our constituency and thus we have no control nor authority on this host.

However, we have contacted Schedom Europe and asked them to deal with this issue.

Best Regards,
The BELNET CERT Team.

Sistema de Alerta

Thank you for reporting spam to the MSN Support Team. This is an auto-generated response to inform you that we have received your submission. Please note that you will not receive a reply if you respond directly to this message.

Unfortunately, in order to process your request, MSN Support needs a valid MSN hosted account.

We can help you best when you forward the spam/abusive mail as an attachment to us. The attachment should have full headers / message routing information displayed. This means that the complete “From” address of the offending message should be displayed. If you need help to do this, please visit the following website:

http://safety.msn.com/articles/junkmail.armx

If you have deleted or no longer have the message, you can still resubmit your report by sending the name of the violating MSN hosted account and a description of your concerns. If your submission does not involve a third party, please include your own account name in the body of your message along with the description of your concerns so we can process your report.

For further instructions on how to submit spam and abusive emails to MSN please visit:

http://postmaster.msn.com/cgi-bin/dasp/postmaster.asp?ContextNav=Guidelines

For more information about MSN's efforts and technologies used to fight spam and abusive e-mails please visit:

http://postmaster.msn.com/cgi-bin/dasp/postmaster.asp?ContextNav=FightJunkEmail

...

Sistema de Alerta

...
Bonjour,

-- Attention -- attention -- attention -- attention -- attention --

Votre email a été reçu sur notre support mais NE PEUT PAS
être traité. En effet, il manque des informations concernant
votre domaine et le type de support que vous demandez.

Merci DE COMPLETER votre requête via cette url
http://www.ovh.com/fr/espaceclients/support/supportv2.cgi?id=2KZ3UKJ7JYB2PH9EBKDR
Il vous permettra aussi de suivre le traitement de votre
requête en temps réel.

Cordialement,

Support Client OVH
Support Technique : 08.99.70.17.61 (1.349 Euro/appel + 0.337 Euro/min)
Support Commercial : 08.20.32.03.63 (Numéro Indigo 0.118 Euro/min)
Fax : 03.20.20.09.58
Email: support@ovh.com
Du lundi au vendredi : 8h - 20h
Le Samedi : 9h - 17h
...

Colaboração

- Colaboramos com diversos grupos de segurança, CSIRTs e a comunidade. Entre eles, podemos destacar:
  - CAIS – RNP;
  - Grupo Cymru;
  - CastleCops;
  - SURBL;
  - WOT;
  - Kaspersky;
  - F-Prot;
  - Contribuições pessoais:
    - > 8500 usuários únicos que contribuem;
    - Nomes não divulgados;

Listas disponíveis

- Atualmente estão disponíveis listas de bloqueio em 29 formatos diferentes;
- Estas listas são “sanitized”, ou seja, contém:
  - Protocolo (http / ftp);
  - Host name e domínio (www. dominio. com. br);
  - Diretórios (/teste_dir_1/teste_dir_2/);
- As listas disponibilizadas não contém os nomes dos binários maliciosos;
- Somente enviamos binários e URLs completas para grupos de segurança reconhecidamente sérios e atuantes na remoção de **Malwares** da Internet;
- As listas estão sendo utilizadas indevidamente por empresas que comercializam sistemas/*applicances* de bloqueio de URLs;

Listas disponíveis

- Formatos disponíveis:
  - BIND like DNS Servers;
  - Clamav (basic e extended);
  - DansGuardian;
  - FireKeeper;
  - Hashes (MD5/SHA-1);
  - Hosts file;
  - Mailwasher block filters;
  - MaraDNS;
  - Microsoft DNS Server;
  - Mozilla cookie filtering;
  - Mozilla Firefox AdBlock;
  - Plain Text;
  - Postfix MTA;
  - SmoothWall;
  - SpamAssassin;
  - Squid Web Proxy;
  - SquidGuard;
  - Symantec Security for SMTP;
  - Symantec WebSecurity
  - XML;

malwarepatrol

MalwarePatrol

Malware is everywhere!

Updated **every hour**
Online since **06/2005** - 3.000.000 hits/month

Home | Stats | Block Lists | News/Blog | Contribute | ToDo | FAQ | Terms

Please Sign in or Register

Search MBL#: Search

Access Denied !!!

Access Denied!!!

The site you are trying to access is listed in the **Malware** Patrol - Block List as a host for some kind of software considered **Malware**. The administrator of your network decided to block access to this site. **Malwares** like these, are developed to cause some kind of damage to computers, servers or networks and can be classified as Viruses, Worms, Trojans, Spywares, Backdoors or Rootkits.

If you think the site you are tying to access has been added to the list by mistake, please contact your network administrator.

Please support us. Make a Donation!

Please Donate any amount of money and help us block and remove **Malware** from the Internet.

Your donation is very important and will be used to pay for server hosting and bandwidth needed to keep this project freely available for non-commercial use.

PayPal Donate

Ads by Google

Search results

These are the information stored in our database for **Backdoor.Win32.Bifrose.cnx** - 42 result(s):

URL status	Active Malware
MBL#	99573
Malware found	Backdoor.Win32.Bifrose.cnx
Insertion date	23:02:51 21/Nov/2008 UTC
URL	http://members.lycos.co.uk/ridaxxl/<sanitized>
Host/Domain	members.lycos.co.uk
Host country	- DE
Protocol	http
Extension	exe
Malware MD5	516b2a665e8318eb7b94ae20ae42502b
Malware SHA1	668831c9bff27f8248188d2243c76e13dc6df3e9
Last alert sent	23:50:00 21/Nov/2008 UTC

URL status	Not Found
MBL#	87563
Malware found	Backdoor.Win32.Bifrose.cnx
Insertion date	01:50:50 09/Apr/2008 UTC
URL	http://members.lycos.co.uk/crazy9999/up_rr/ar/<sanitized>

Malware vs. Badware

- Depois de analisados, os binários são classificados em uma entre as diversas categorias:
  - Adware;
  - Backdoor;
  - Downloader
  - HackTool;
  - PoC;
  - Rootkit;
  - SpamTool;
  - Trojans;
  - Worm;
  - ...

Malware vs. Badware

- Não é simples definir quais categorias incluem softwares considerados **Malwares** e quais são *Badwares*;
- *"**Malware** is software designed to infiltrate or damage a computer system, without the owner's informed consent. The term is a portmanteau of "mal-" (or perhaps "malicious") and "software", and describes the intent of the creator, rather than any particular features. **Malware** is commonly taken to include computer viruses, worms, Trojan horses, spyware and some adware. In law, malware is sometimes known as a computer contaminant..."*

  Font: Wikipedia

- Caso de PoC mal classificado: http://aluigi.altervista.org/poc.htm

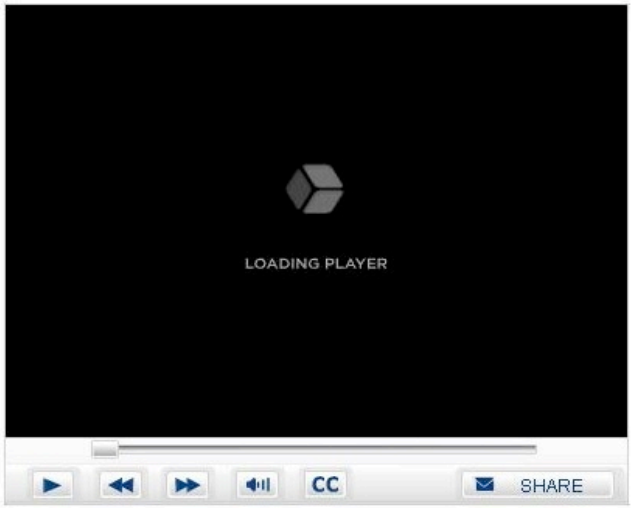
Técnicas de "ofuscamento"

- Diversas técnicas para "ofuscar" as URLs tem sido utilizadas em Phishing Scams;
  - Nomes de domínio parecidos com domínios legítimos;
  - Nomes de domínio muito longos contendo em seu início partes de domínios legítimos (http://www.google.com.xxxx.yyy...zzz.com/www...);
  - URL encoding total ou parcial
  - Redirecionamentos HTML/HTTP;
  - Bugs de browsers;
  - Uso de Content-Disposition;
  - Uso de JavaScript;
  - Sites forjados com links para **Malwares**;
  - Softwares forjados (Anti-Virus, Anti-Malware, etc);
  - Serviços de *short URLs* (NotLong, TinyURL, etc);
    - YouSendIt.com

Barack Obama Elected 44th President of United States

Barack Obama, unknown to most Americans just four years ago, will become the 44th president and the first African-American president of the United States. Obama, a senator from Illinois, and his running mate Joe Biden will take the oath of office on January 20, 2009.

Look Amazing Speech of New President



This America.gov Video Player requires the Adobe Flash 8 plugin or higher.
Download the most recent Adobe Flash Player here.

Run installation by clicking downloaded file. Installation time : 4-6 seconds.

By Organization

- A-Z Agency Index
- Federal Government
- State Government
- Local Government
- Tribal Government

Contact Government

- Online Services
- Frequently Asked Questions
- E-mail
- Web Chat
- Phone
- In Person
- Forms

By Topic

- Benefits and Grants
- Consumer Guides
- Defense and International
- Environment, Energy, and Agriculture
- Family, Home, and Community
- Health and Nutrition
- History, Arts, and Culture
- Jobs and Education
- Money and Taxes
- Public Safety and Law
- Reference and General Government
- Science and Technology
- Travel and Recreation
- Voting and Elections

Video: Scandal in the USA - McCain Lawyers Want to Stop Obama!

Access U.S. government services from your computer.

Get ADOBE® MEDIA PLAYER

Adobe® Media Player software provides control and flexibility to view what you want, when you want — whether online or offline.

Get ADOBE® MEDIA PLAYER

Installation: Double-click on the .exe file that you just downloaded. The .exe file appears as an icon on your desktop. After a few seconds the installer finishes loading and the Untangle for Windows Setup Wizard launches.

Change text size: A A A

- E-mail this page
- Print this page
- Receive updates by e-mail
- USA.gov RSS feeds
- Tutorials: Find government info
- BOOKMARK

In Focus

- Online Services by Topic – Government online services organized by topic.
- Register to Vote – Register to vote by mail, visit your State election website, or get an absentee ballot.
- Does the Government Owe You Money? – The federal or state government could owe you. Check failed banks, credit unions, pensions, mortgage refunds, unclaimed property, tax refunds, and more.

Local Weather Forecast

Enter City or ZIP Code:

Go

Featured Sites

- Forms Online
- Grants Finder
- Hold My Mail
- Locate Services Nearby
- Medicare Card Replacement
- Selective Service
- Stamps Online
- What Time Is It?
- ZIP Code Lookup
- Embassy Registration for Americans Abroad

Page Las

Técnicas de "ofuscamento"

CODIN / Ministério do Trabalho e Emprego / Consulta Processual

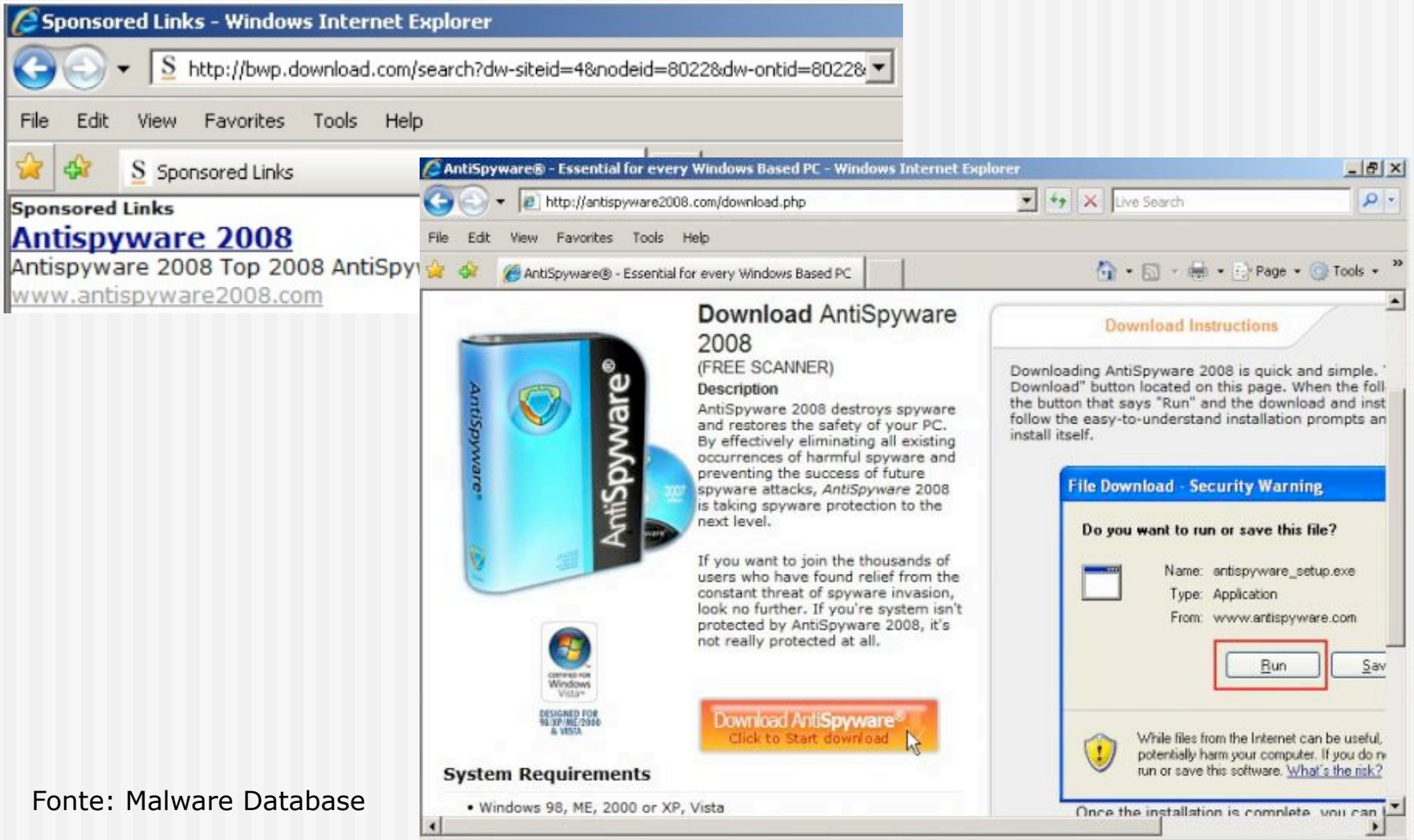
Aguarde o processamento do arquivo em anexo, caso o mesmo não abra, por gentileza abra-o manualmente logo abaixo:

Processo n.º 40925/2008 - anexos relacionados abaixo:

Despacho_409252008

*** Para a visualização desse conteúdo é necessário aceitar o plugin do Adobe Flash Player

Técnicas de "ofuscamento"



Fonte: Malware Database

Air France voo 447: reconhecimento de corpos.

Segundo helicóptero com vítimas de acidente chega a Noronha.

O helicóptero Super Puma, da Força Aérea Brasileira, pousou em Fernando de Noronha no fim da manhã desta terça-feira (9). A aeronave transportava oito corpos de vítimas do acidente do voo 447, da Air France, que estavam na Fragata Constituição. **Com Autorização dos familiares estamos enviando fotos dos corpos encontrados para reconhecimento dos mesmos, caso puder contribuir sua ajuda seria de extrema importância para todos entes queridos dos falecidos do trágico acidente.**

Para fazer o reconhecimento dos corpos acessem o link abaixo e confira as fotos.

Link: http://g1.informacoes/voo447/airbus.php?cod=CORPOS+VOO+447

Caso algum corpo for identificado nos informe através do e-mail: voo447@globo.com com o assunto: Reconhecimento de Corpos.

Ficamos muito grato com a sua ajuda e esperamos seu contato. Desculpe o incomodo mas esperamos que entendam a nossa extrema preocupação com esta tragédia.

Fonte:
http://g1.globo.com/

Samples não classificados

- Muitos binários coletados não são classificados como **Malwares** pelos Anti-Vírus, mas possuem fortes características (nome, extensão, packer, etc);
- Quando enviados aos *vendors* de Anti-Vírus, são analisados e assinaturas são criadas. No entanto, os não existem formas simples e automatizáveis para o envio e posterior recebimento de sua classificação;
- Atualmente temos aproximadamente 4500 *samples* não classificados mas com fortes características de **Malware**;
  - .../disco_virtual/card/cartao.exe
  - .../ternura.exe
  - .../novidadejoia/visualizar.exe
  - .../webinf10/visual.cmd
  - .../bradesco/sisret/instalar.exe
  - .../vale_presente.pif
  - ...

Desafios atuais

- Aumento da quantidade de URLs na base de dados;
- Aumento do volume de SPAM recebido;
- Alto consumo de banda;
- Freqüentes ataques de (D)DoS;
- Grande volume de *samples*;
- Uso de *Content-Disposition*;
- Necessidade de *crawling* recursivo;
- Custos de manutenção/*hosting* dos servidores;
- Falta de recursos para desenvolvimento de novas funcionalidades / correção de bugs;
- Atrair empresas interessadas em patrocinar o projeto e doações de usuários;

Próximos desenvolvimentos

- Aperfeiçoamento do sistema de extração de URLs em e-mails, web sites, newsgroups, IRC e binários;
- Aumentar a velocidade do sistema de *crawling* recursivo;
- Melhorar a captura e tratamento de URLs que utilizam *Content-Disposition*;
- *Thumbnail* dos e-mails e sites utilizados em *Phishing Scams* com **Malware**;
- Criar novas listas de bloqueio;
- Aprimorar o sistema de análise superficial dos binários coletados;
- Criar novos *SPAM traps*;
- Novas estatísticas e informações aos usuários;
- Criar novos mecanismos de cooperação com a comunidade (forum, blog, mailing list, etc);
- Implementar sistema de autenticação para *download* das listas;
- Geração automática de novas estatísticas;
- Estreitar a colaboração com *vendors* de Anti-Virus;

Próximos desenvolvimentos

- Monitorar extensões muito comuns e a princípio sem perigo (ex: pdf, jpg, ASP, HTML). Estas são utilizadas por exemplo, por *downloaders* ou com *Content-Disposition*. Não são bloqueadas em *proxies*;
- Monitorar *JavaScript* malicioso (ex: ataques do tipo *cross site scripting*). Como detectar?
- Disponibilizar para visualização, aproximadamente 5000 *Phishing Scams* coletados;
- Permitir pesquisas por URLs e/ou domínios (cuidado com *SQL injection*);
- Integração com algum *sandbox* online;

Agradecimentos

Perguntas

Perguntas, sugestões e críticas

Contato

André D. Corrêa, CISSP, ITIL Certified
andre.correa@pobox.com
andre@malware.com.br
(11) 9187-1906
http://www.malwarepatrol.net
Follow us on Twitter – MalwarePatrol