

Grupo de Resposta a Incidentes de Segurança

Conficker *A Ameaça Continua*

por:
Augusto Cesar da F. dos Santos

gris@gris.dcc.ufrj.br
augusto@gris.dcc.ufrj.br



conficker

Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro



Sumário



Introdução

Sistemas Vulneráveis

Estatísticas

Principais Vetores de infecção

Atualização do Malware

Geração de Domínios

Peculiaridades da Infecção

Técnicas de Autodefesa

A Comunicação P2P (Peer-to-Peer)

Requisições HTTP

O Processo SVCHOST.EXE

O Conficker como uma Botnet

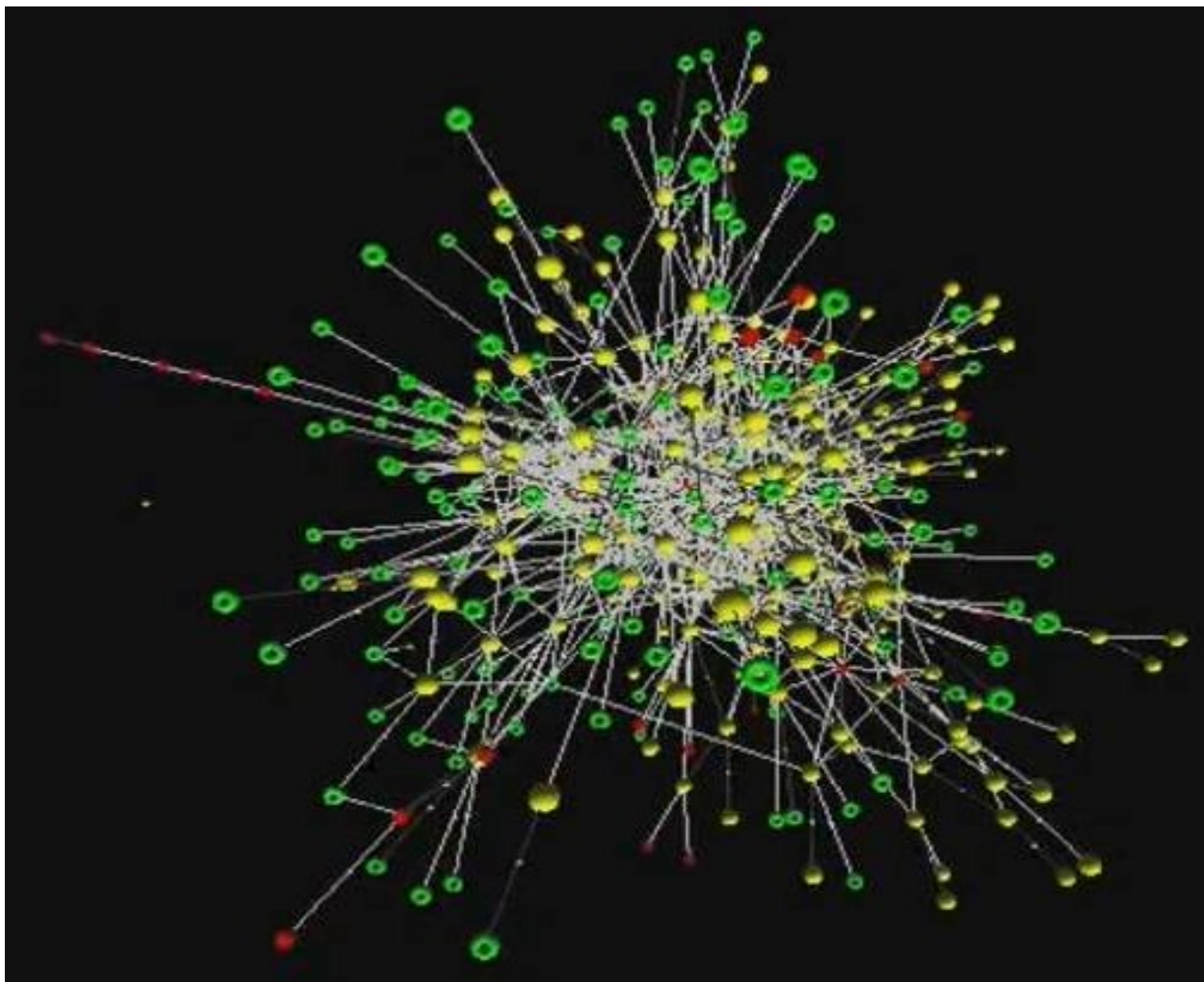
Protegendo-se da Infecção

Removendo a Infecção

Resumo da Remoção (Passo a Passo)



Estrutura do Malware



Introdução



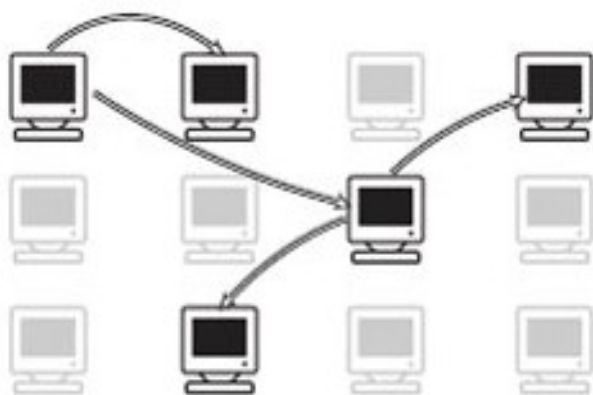
- Família de **Worms** mutantes que infectam Sistemas Operacionais **Windows**;
- Além das variantes .A, .B, .C, .D, .E são também conhecidas as variantes Downadup ou Kido, além de outros aliases;
- O ataque viabiliza-se em explorar uma vulnerabilidade em uma função de RPC (Remote Procedure Call), instala-se no hospedeiro, faz cópias de si e além de espalhar-se, atualiza-se para novas versões;
- Foi primeiramente detectado em um “telescópio de rede” na Califórnia;
- Principal peculiaridade de agir como Bot (Zumbi);
- Infectou mais de 12 milhões de sistemas ao redor do mundo em Janeiro de 2009;



Introdução

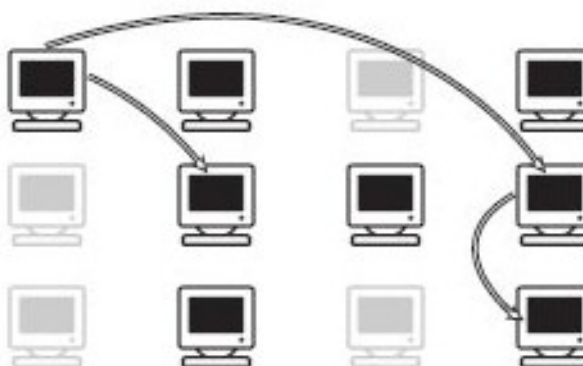


- **O Conficker em Ação:**



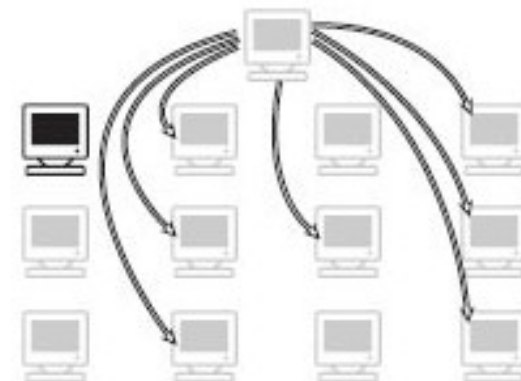
20 DE NOVEMBRO DE 2008

A primeira cepa do Conficker espalha-se rapidamente através da internet e das redes locais.



29 DE DEZEMBRO DE 2008

Uma segunda variedade é liberada. Ela pode se propagar também pela porta USB.



15 DE MARÇO DE 2009

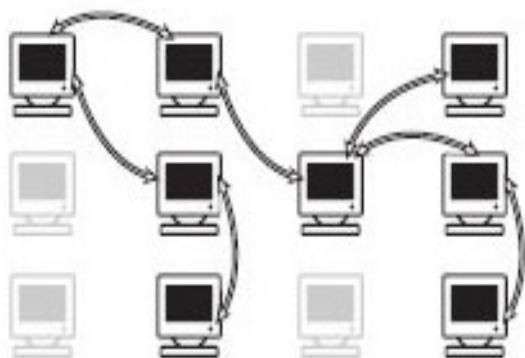
Os computadores infectados conectam-se a um servidor e baixam mais uma versão do worm.



Introdução

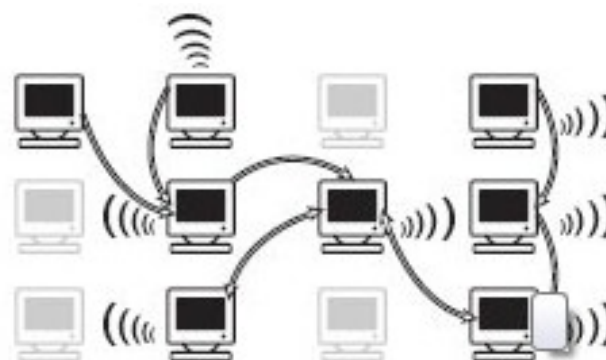


- **O Conficker em Ação:**



7 DE ABRIL DE 2009

Os micros escravos passam a atualizar o programa maligno por meio de conexões peer-to-peer.



HOJE

A rede com milhões de PCs zumbis está ativa enviando spam a destinatários do mundo inteiro.

<http://info.abril.com.br/noticias/seguranca/a-historia-secreta-do-conficker-14092009-14.shl>



Sistemas Vulneráveis



Microsoft Windows 2000 Service Pack 4

Windows XP Service Pack 2

Windows XP Service Pack 3

Windows XP Professional x64 Edition

Windows XP Professional x64 Edition Service Pack 2

Windows Server 2003 Service Pack 1

Windows Server 2003 Service Pack 2

Windows Server 2003 x64 Edition

Windows Server 2003 x64 Edition Service Pack 2

Windows Server 2003 com SP1 para sistemas baseados no Itanium

Windows Server 2003 com SP2 para sistemas baseados no Itanium

Windows Vista e Windows Vista Service Pack 1

Windows Vista x64 Edition e Windows Vista x64 Edition Service Pack 1

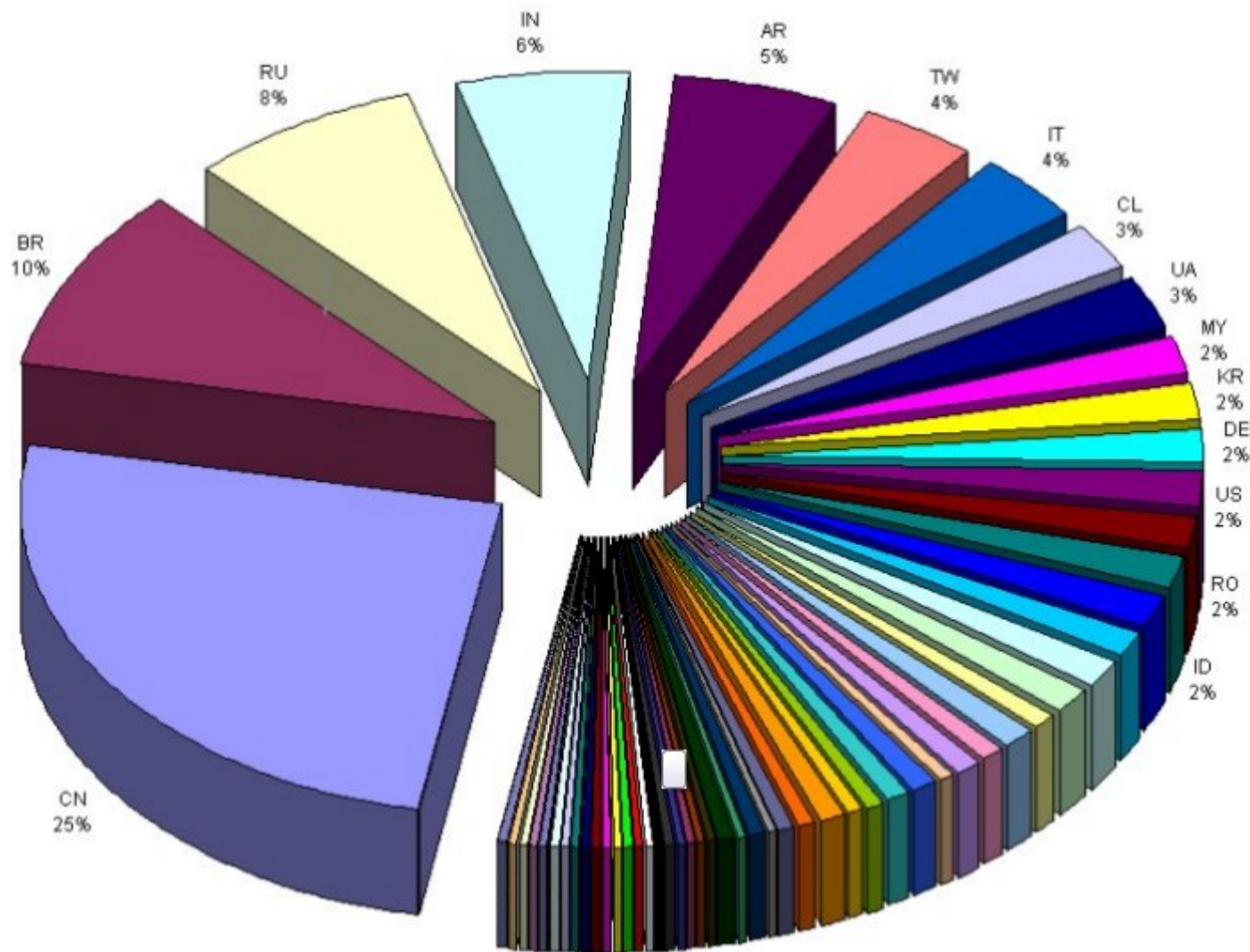
Windows Server 2008 para

Windows Server 2008 para sistemas baseados em x64*

Windows Server 2008 para sistemas baseados no Itanium



Estatísticas



Total Count: Total IP Addresses Infection Count for Conficker A and B
Conficker.A: IP Addresses Infection Count for Conficker A only
Conficker.B: IP Addresses Infection Count for Conficker B only
Q-Cumm A: Cumulative Q(*) values for Conficker.A
Q-Cumm B: Cumulative Q(*) values for Conficker.B



Estatísticas



Country	Total Count	Conficker.A	Conficker.B	Q-Cumm A	Q-Cumm B
CN	2,649,674	1,265,792	1,558,286	10,923,793	6,361,262
BR	1,017,825	314,574	786,014	10,346,477	18,122,278
RU	835,970	229,497	718,883	8,034,341	23,747,378
IN	607,172	296,544	423,945	22,056,407	11,801,841
AR	569,445	458,403	240,301	59,452,966	17,800,596
TW	413,762	311,305	125,779	15,621,086	4,572,295
IT	374,513	94,210	290,102	2,070,977	11,119,862
CL	280,182	208,514	136,799	90,467,237	35,357,299
UA	274,411	35,422	255,889	1,173,346	7,915,761
MY	212,477	102,099	135,737	4,029,677	2,960,225
KR	201,107	38,340	169,911	939,117	2,657,482
DE	195,923	76,154	122,682	2,635,577	6,931,439
US	191,531	121,323	75,262	10,909,836	4,607,551
RO	182,790	38,497	153,666	2,319,680	7,263,286
CO	169,597	99,603	94,134	10,252,126	5,435,429
TH	165,080	39,000	135,546	4,259,999	2,831,264
ID	164,794	66,623	123,717	6,664,631	3,637,131
MX	151,861	95,694	72,287	4,227,442	1,250,216
PH	126,594	37,477	102,012	2,502,421	2,771,099
VE	102,073	63,165	48,137	11,160,434	3,139,896



Principais Vetores de Infecção



- Exploração da vulnerabilidade no serviço “Servidor” do Windows (**SVCHOST.EXE** – TCP/445 [SMB] e TCP/139 [NetBios]);
Falha corrigida pelo alerta 958644 MS08-067 da Microsoft
- Ataques de “Brute Force” contra máquinas que executam serviços compartilhados;
- Tentativa da quebra de senha de administrador com ataques de dicionário;
- Infecção através de dispositivos removíveis que contenham reprodução automática através da criação de trojans em formato DLL (pen-drive, cartões de memória USB e etc...)

OBS: A variante Win32/Conficker.D não se espalha para unidades removíveis nem pastas compartilhadas em uma rede. O Win32/Conficker.D é instalado por variantes anteriores do Win32/Conficker.



Atualização do Malware



- **Requisição HTTP:**

Downloads diários de 250 domínios pseudo-aleatórios

OBS: Conforme realizam atualizações, outras variantes aumentam o número de domínios de requisições, que podem chegar a 5000 diárias

- **NetBios:**

Remove o patch **MS08-067** para reinfecção da máquina

- **P2P (Peer-to-Peer):**

Executa varreduras por peers infectados via UDP e executa transferências por UDP



Geração de Domínios



→ **“downatool2.exe”**

- Esta ferramenta foi desenvolvida com o intuito de auxiliar na detecção de máquinas que estejam infectadas principalmente pelas variantes .A, .B e .C em uma rede;
- Auxilia na detecção de hosts que se conectam a domínios maliciosos;

Pode ser encontrada no site:

<http://net.cs.uni-bonn.de/wg/cs/applications/containing-conficker/>



Geração de Domínios



```
C:\Windows\system32\cmd.exe

/*-----*/
/* Downadup/Conficker Domain Name Generation */
/*-----*/
/* by Felix Leder, Tillmann Werner @ University of Bonn 2009 */
/* {leder,werner}@cs.uni-bonn.de */
/*-----*/
Generating domains for Conficker.A
Generating domains for 2009-11-11

nyrzvygjm.info
pxvnqzykc.biz
juansxqgosa.org
mxybtrgx.com
esjisi.com
avlasxoe lx.biz
xsbldzugj.info
leozejny.net
caysd.biz
ltprvcdge.net
btucsjfy.info
qwdcevsrn.info
cxayd.info
uqjlt.org
srybgvlyn.com
kvsznlr.net
yfnuxnru.info
maknmk.net
rdrwbqeiz.info
fobuidf.biz
wnxyp.com
tvsnptqjmk.net
suxtebttpm.net
vdwvrhrn.com
ndomngjsoud.biz
irlrhwd.info
hvidxghm.org
vtgxbrzsp.org
kuoycduy.com
yrennen.net
wzebykuuksm.com
gqntepifw.org
aebsumoma.info
owfhdelv.net
yaplerpp.org
ttbkmaj.com
vnhflul.info
zegeurtuxjq.org
mpitalzh.net
inowbaq.info
```





Peculiaridades da Infecção e Sintomas

→ A Infecção traz possibilidades de mal uso da rede, como:

- Transmissão de dados ou materiais ilegais;
- DDoS (Distributed Denial of Service);
- Envio de Spams;
- Atividades que causem esgotamento de recursos da rede;
- Diversos sites relacionados a segurança são restritos por palavras pertinentes;
- Ferramentas de Segurança não conseguem ser inicializadas em loco;
- Transferência de dados sem autorização através de **Comunicação P2P**;

<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fConficker.B>
<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fConficker.D>





Técnicas de Autodefesa

→ **Alguns Serviços de Segurança falham ao ser inicializados:**

- Windows Update Service;
- Background Intelligent Transfer Service;
- Windows Defender;
- Windows Error Reporting Services;
- Usuários ficam desabilitados a se conectarem em sites que contenham em sua string:

Virus, spyware, malware, rootkit, defender, Microsoft, symantec, norton, mcafee, trendmicro, sophos, panda, etrust, networkassociates, computerassociates, f-secure, kaspersky etc..





Técnicas de Autodefesa

- **Desativa Atualizações automáticas;**
- **Executa varreduras por processos anti-malware, modificando e diagnosticando ferramentas a cada um segundo**



A Comunicação P2P(Peer-to-Peer)



- Principal comunicação realizada por máquinas infectadas pelo worm na sua segunda versão, onde:
- O mesmo pode se atualizar para novas versões sem necessitar de uma central;
- Único worm a usar **Criptografia MD6** na sua comunicação para ocultar o conteúdo do tráfego;
- Realiza levantamento de informações do host infectado e da rede local, como velocidades de banda, redes vizinhas, país de origem e etc...





A Comunicação P2P

- As primeiras variantes do Worm tentam conectar-se nos seguintes endereços para informações sobre a máquina (data/hora/etc...):
- <http://getmyip.co.uk>
 - <http://www.whatsmyipaddress.com>
 - <http://www.whatismyip.org>
 - <http://checkip.dyndns.org>
 - <http://schemas.xmlsoap.org/soap/envelope/>
 - <http://schemas.xmlsoap.org/soap/encoding/>
 - <http://schemas.xmlsoap.org/soap/envelope/>
 - <http://schemas.xmlsoap.org/soap/encoding/>
 - <http://trafficconverter.biz/4vir/antispysware/loadadv.exe>
 - <http://trafficconverter.biz>
 - <http://www.maxmind.com/download/geoip/database/GeoIP.dat.gz>



Requisições HTTP



- Nas primeiras versões do Malware tenta-se fazer requisições HTTP:

Ex: <http://IP/search?q=%d>

- Sendo que “%d” representa o número de máquinas infectadas na rede explorada.

<http://143.215.143.11/search?q=269>

<http://83.68.16.6/search?q=98>

<http://149.20.56.32/search?q=194>



O Processo **SVCHOST.EXE**



- Arquivo de Sistema são carregado na inicialização do sistema e estes não podem ser apagado;
- Processo de Host Genérico onde DLL´s são carregadas;
- Perspectiva de reusabilidade em termos de programação;
- Função dividida em diversas instâncias lógicas e criadas por cada grupo;



O Processo **SVCHOST.EXE**

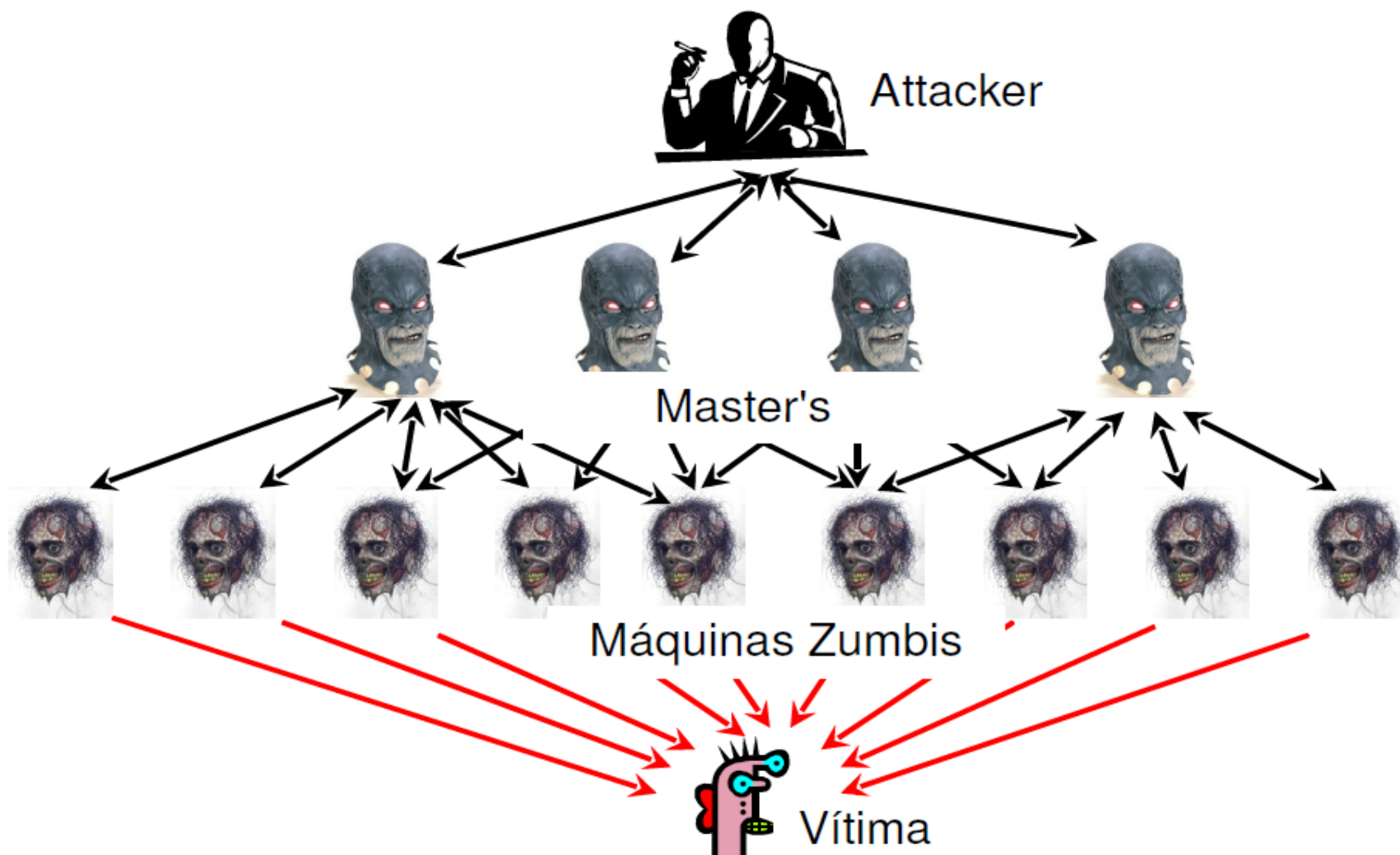


```
C:\Windows\system32\cmd.exe
C:\Users\Augusto>cd ..
C:\Users>cd ..
C:\>tasklist /SVC
```

Nome da imagem	Identifi	Serviços
System Idle Process	0	N/A
System	4	N/A
smss.exe	400	N/A
csrss.exe	536	N/A
wininit.exe	580	N/A
csrss.exe	592	N/A
services.exe	628	N/A
lsass.exe	640	KeyIso, SamSs
lsm.exe	648	N/A
winlogon.exe	752	N/A
svchost.exe	844	DcomLaunch, PlugPlay
svchost.exe	920	RpcSs
svchost.exe	956	WinDefend
svchost.exe	1052	AudioSrv, Dhcp, Eventlog, lmhosts, wscntfrg
svchost.exe	1080	AudioEndpointBuilder, EMDMgmt, Netman, PcaSvc, SysMain, TabletInputService, TrkWks, UxSms, WdiSystemHost, Wlansvc, WPDBusEnum, wudfsvc
svchost.exe	1096	AeLookupSvc, Appinfo, BITS, EapHost, IKEEXT, iphlpsvc, LanmanServer, MMCSS, ProfSvc, RasMan, Schedule, seclogon, SENS, ShellHWDetection, Themes, Winmgmt, wuauserv
audiodg.exe	1216	N/A
svchost.exe	1244	gpsvc
SLsvc.exe	1280	slsvc
svchost.exe	1324	EventSystem, FDRessPub, LanmanWorkstation, netprofm, nsi, SSDPSRV, upnphost, W32Time, WebClient
svchost.exe	1524	CryptSvc, Dnscache, KtmRm, NlaSvc, TapiSrv, TermService



O Conficker atua como uma Botnet



Protegendo-se da Infecção



- Instalação da atualização Crítica de Segurança MS08-067 da Microsoft
<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>
- Instalar um bom antivírus. Sugestão:
 1. Avira Antivir
 2. BitDefender
 3. Avast Home Free
<http://www.inexistentman.net/2009/03/02/os-12-melhores-antivirus-de-2009/>
- Ativar o Firewall do Windows
- Use senhas de administrador fortes que sejam exclusivas para todos os computadores;
- Verifique se as atualizações de segurança mais recentes foram aplicadas a todos os sistemas.
- Desative o recurso de Reprodução Automática.



Removendo a Infecção



- Ferramentas para usuários domésticos:
- Kaspersky Removal Tool

```
C:\Users\Augusto\Documents\My DAP Downloads\KK.exe
Net-Worm.Win32.Kido removing tool, Kaspersky Lab 2009
version 3.4.5   Apr 13 2009 09:14:32
scanning      jobs ...
scanning      processes ...
scanning      threads ...
scanning      modules in svchost.exe...
scanning      modules in services.exe...
scanning      modules in explorer.exe...
scanning      C:\Windows\system32 ...
scanning      C:\Program Files\Internet Explorer\ ...
scanning      C:\Program Files\Movie Maker\ ...
scanning      C:\Program Files\Windows Media Player\ ...
scanning      C:\Program Files\Windows NT\ ...
scanning      C:\Users\Augusto\AppData\Roaming ...
scanning      C:\Users\Augusto\AppData\Local\Temp\ ...

completed
Infected jobs:           0
Infected files:          0
Infected threads:        0
Splices functions:        0
Cured files:              0
Fixed registry keys:      0

Pressione qualquer tecla para continuar. . . _
```



Removendo a Infecção



→ Ferramentas para Administradores:

- Nmap

Melhor ferramenta para identificar computadores infectados na rede e que não possuem o patch de vulnerabilidade.

Após instalado, use a linha de comando abaixo:

```
nmap -PN -T4 -p139,445 -n -v --script smb-check-vulns,smb-os-discovery - --script-args unsafe=1 [ip_do_pc]
```

Se o pc estiver infectado, ele mostrará a mensagem:

Conficker: **Likely INFECTED**

Se não estiver infectado, mostrará a mensagem:

Conficker: **Likely CLEAN**



Removendo a Infecção



- Abaixo, a evidência que mostra que o vírus aplicou o seu próprio patch -> MS08-067: PATCHED (possibly by Conficker)

The screenshot shows the Zenmap application window. The 'Alvo' field contains '192.168.153.128'. The 'Comando' field contains the Nmap command: `nmap -p 139,445 -T4 -v -n -PN --script smb-check-vulns,smb-os-discovery --script-args unsafe=1 192.168.153.128`. The 'Hosts' tab is selected, showing a list of hosts with '192.168.153.128' listed. The 'Details' tab is selected, showing the Nmap output. The 'Host script results' section is highlighted, showing the following results:

```
Host script results:
| smb-os-discovery: Windows XP
| LAN Manager: Windows 2000 LAN Manager
| Name: JONES\ATACANTE
|_ System time: 2009-04-07 20:21:19 UTC-3
| smb-check-vulns:
| MS08-067: PATCHED (possibly by Conficker)
| Conficker: Likely INFECTED
|_ regsvc DoS: FIXED
```

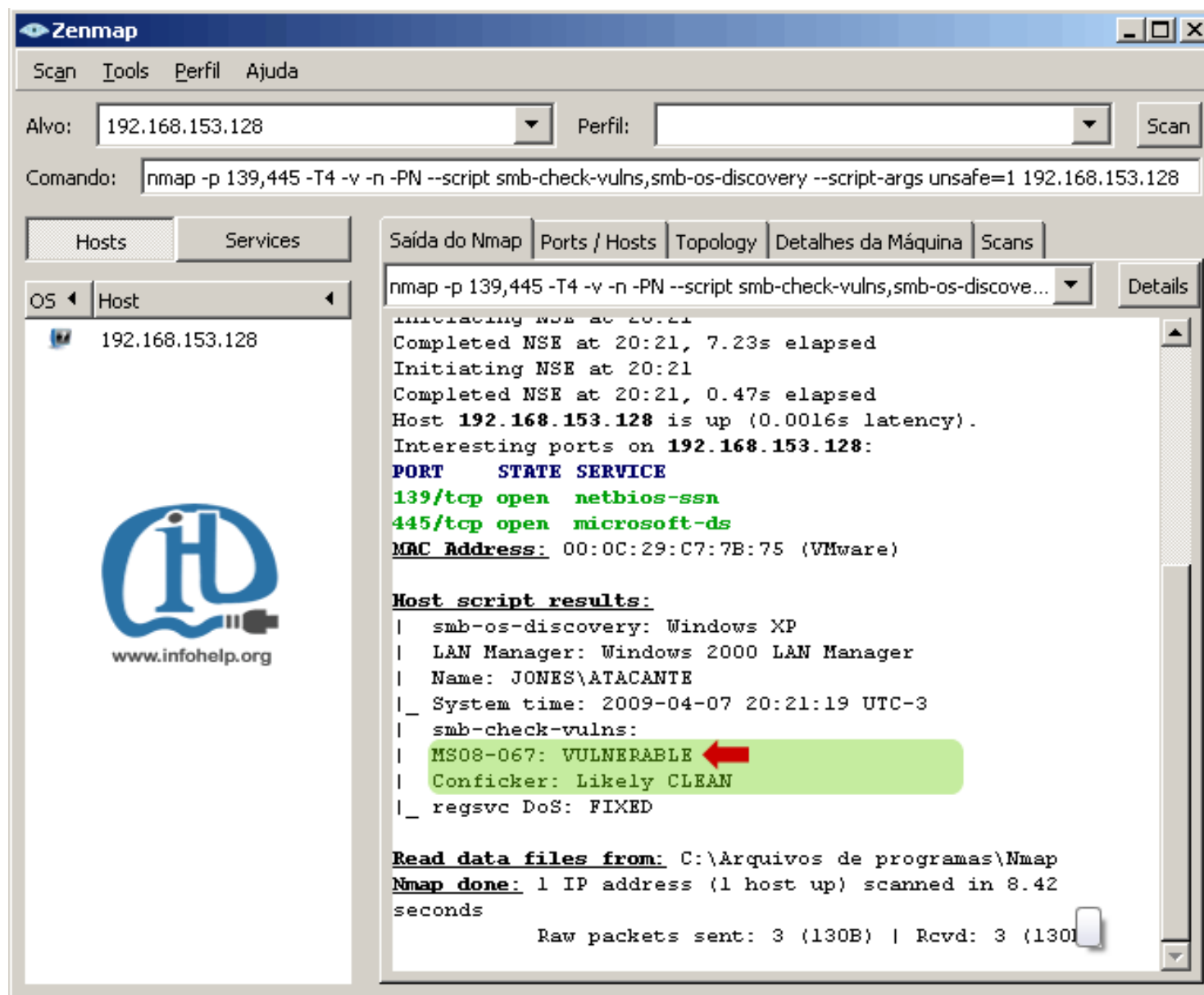
A red arrow points to the line 'MS08-067: PATCHED (possibly by Conficker)'. The 'Read data files from' section shows the path 'C:\Arquivos de programas\Nmap'. The 'Nmap done' section shows '1 IP address (1 host up) scanned in 8.42 seconds'. The 'Raw packets sent' section shows '3 (130B) | Rcvd: 3 (130B)'.



Removendo a Infecção



- Depois de remover o vírus do PC, teremos a seguinte tela com a informação que o conficker foi limpo, mas o computador continua sem o patch da microsoft -> **MS08-067: VULNERABLE**



Removendo a Infecção



- Após aplicar o patch teremos a tela abaixo mostrando que o computador não está mais vulnerável
-> MS08-067: FIXED

Zenmap

Scan Tools Perfil Ajuda

Alvo: 192.168.153.128 Perfil: Scan

Comando: nmap -p 139,445 -T4 -v -n -PN --script smb-check-vulns,smb-os-discovery --script-args unsafe=1 192.168.153.128

Hosts Services

OS Host

192.168.153.128

www.infohelp.org

Saída do Nmap Ports / Hosts Topology Detalhes da Máquina Scans

nmap -p 139,445 -T4 -v -n -PN --script smb-check-vulns,smb-os-discovery --script-args unsafe=1 192.168.153.128 Details

Initiating NSE at 21:02
Completed NSE at 21:02, 7.16s elapsed
Initiating NSE at 21:02
Completed NSE at 21:02, 0.72s elapsed
Host 192.168.153.128 is up (0.0054s latency).
Interesting ports on 192.168.153.128:

PORT	STATE	SERVICE
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds

MAC Address: 00:0C:29:C7:7B:75 (VMware)

Host script results:

- | smb-os-discovery: Windows XP
- | LAN Manager: Windows 2000 LAN Manager
- | Name: JONES\ATACANTE
- |_ System time: 2009-04-07 21:02:45 UTC-3
- | smb-check-vulns:
- | MS08-067: FIXED
- | Conficker: Likely CLEAN
- |_ regsvc DoS: FIXED

Read data files from: C:\Arquivos de programas\Nmap

Nmap done: 1 IP address (1 host up) scanned in 10.02 seconds

Raw packets sent: 3 (130B) | Rcvd: 3 (130B)




Removendo a Infecção



- McAfee – Conficker Detection Tool

Conficker Detection Tool - Ver. 1.0.8 - Copyright © McAfee, Inc. 2009

This is a free utility provided by McAfee, Inc. to aid in the detection of the Conficker.b/c/e worm. For further information on the Foundstone enterprise vulnerability management solution click on this image.



IPs

Hostname/IP: -> Start IP: End IP:

Start IP: ☒ 192 . 168 . 200 . 20 -> End IP: ☒ . . .

Read IPs from file:

Start IP: 192.168.200.20

Scan Control

☒ Randomize scan order
☒ Ping before checking (no response, no check)
☒ Show both infected and not infected systems
☐ Show non-responding systems
☒ Resolve IP addresses to names
☐ Send message to infected systems

Timeout (ms):
Max. concurrent checks:

IP	DNS Host Name	Computer Name	Status
192.168.200.20	notebook.nce.ufrj.br	NOTEBOOK	Not infected

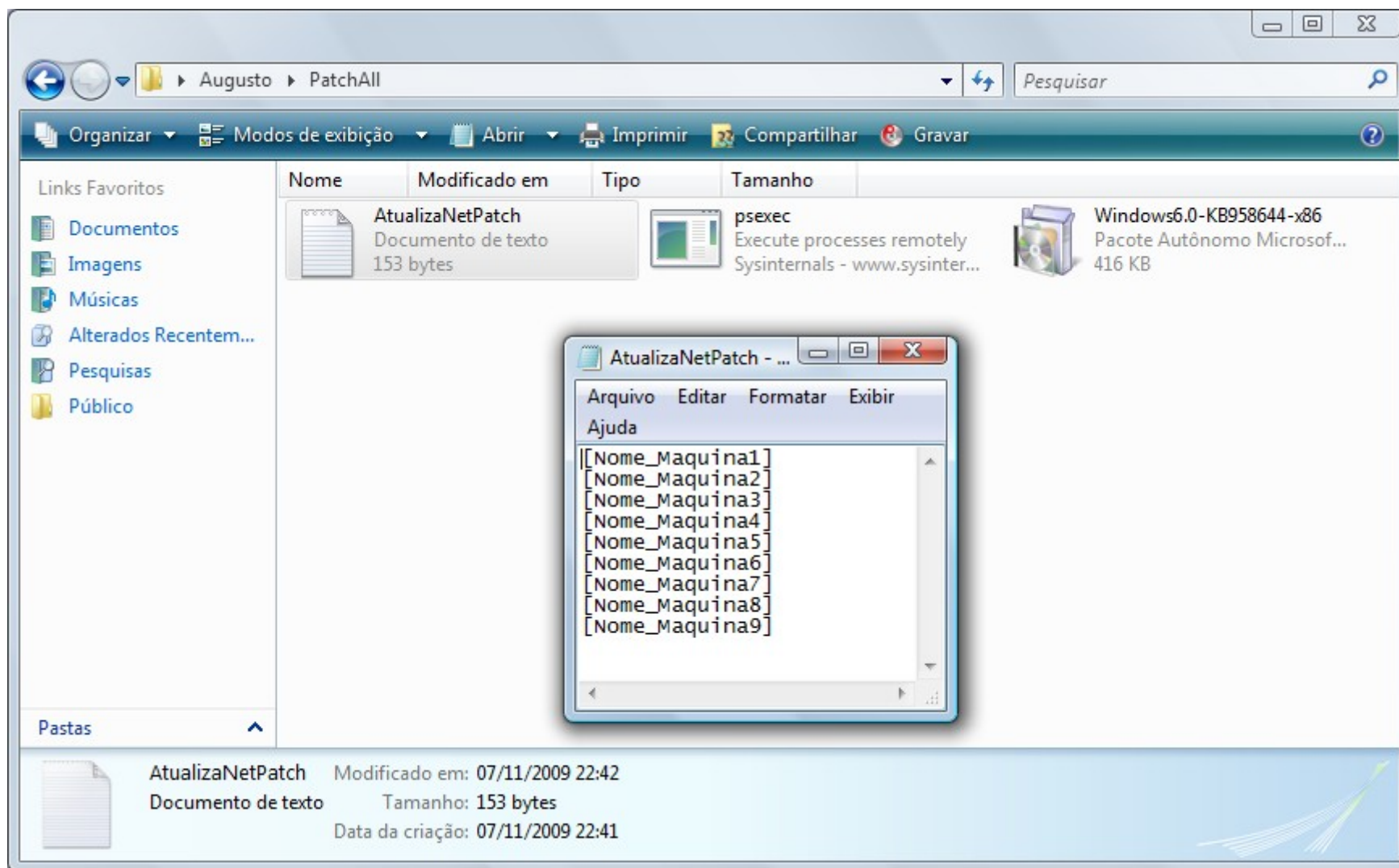
Scanned: 1/1 Infected: 0



Removendo a Infecção



- Fazendo o deploy do Patch na Rede com **PSEXEC**



<http://download.sysinternals.com/Files/PsTools.zip>



Removendo a Infecção



- Fazendo o deploy do Patch na Rede com **PSEXEC**

```
C:\Windows\system32\cmd.exe

C:\Users\Augusto\PatchAll>psexec @AtualizaNetPatch.txt -u seudominio\usuario -p
suassenha -c -d WindowsVista-KB950644-x06-PTB.exe /quiet /norestart

PsExec v1.96 - Execute processes remotely
Copyright (C) 2001-2009 Mark Russinovich
Sysinternals - www.sysinternals.com

The specified application is not on the path.

C:\Users\Augusto\PatchAll>
```





Resumo de Remoção

1. Faça um deploy na rede para instalação do patch de segurança e peça para os usuários reiniciarem os computadores;
 2. Rode o nmap para procurar algum computador infectado na rede;
 3. Rode o arquivo de remoção da Kaspersky caso ache algum vírus;
 4. Reinicie e faça um full scan com o seu antivírus;
- **Mantenha seu sistema operacional e seu antivírus sempre atualizado para evitar problemas como este.**



Dúvidas ???



Obrigado !!!



<http://norberto3d.files.wordpress.com/2009/05/obrigado.jpg>



Bibliografias



Know Your Enemy: Containing Conficker

To Tame A Malware

The Honeynet Project

<http://honeynet.org>

Felix Leder, Tillmann Werner

Last Modified: 7th April 2009 (rev2)

Conficker - Guia definitivo de remoção

<http://www.infohelp.org/tales-laray/conficker-guia-definitivo-de-remocao/>

Guia de detecção e remoção do bot Conficker

<http://www.csirt.pop-mg.rnp.br/docs/conficker.html>

A história secreta do Conficker

<http://info.abril.com.br/noticias/seguranca/a-historia-secreta-do-conficker-14092009-1>

Alerta de vírus sobre o worm Win32/Conficker

<http://support.microsoft.com/kb/962007/pt-br>



Bibliografias



Containing Conficker

<http://net.cs.uni-bonn.de/wg/cs/applications/containing-conficker/>

<http://www.skullsecurity.org/blog/?p=230>

Descoberto novo virus de computador – "CONFICKER"

<http://www.youtube.com/watch?v=IJsD7zdoGHM>

GRIS

