UNIVERSIDADE DO EXTREMO SUL CATARINENSE

CURSO DE CIÊNCIA DA COMPUTAÇÃO

TIAGO DAL TOÉ WESTRUP

ANALISANDO O SISTEMA OPERACIONAL WINDOWS *XP* DIANTE DO ATAQUE DOS *SPYWARES*

CRICIÚMA, DEZEMBRO DE 2006.

TIAGO DAL TOÉ WESTRUP

ANALISANDO O SISTEMA OPERACIONAL WINDOWS *XP* DIANTE DO ATAQUE DOS *SPYWARES*

Trabalho de Conclusão de Curso apresentado para obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. MSc. Paulo João Martins

CRICIÚMA, DEZEMBRO DE 2006.

Dedico esse trabalho ao meu pai, pois sempre ofereceu educação para seus filhos, e à minha mãe, pela compreensão e carinho dado ao longo do curso.

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus que me iluminou durante esta caminhada. Aos meus pais, Aloísio Westrup e Anildes Salete Dal Toé Westrup que de forma carinhosa me deram forças e coragem, me apoiando nos momentos de dificuldades, e a minha namorada Mariana por sua atenção a mim.

Ao meu orientador Paulo João Martins e por todos os professores, pelo conhecimento proporcionado em todo este período do curso.

Aos meus irmãos e amigos, pois sem o apoio destes, dificilmente teria concluído este curso.

“O ser humano não pode deixar de cometer erros;

é com os erros, que os homens de bom senso

aprendem a sabedoria para o futuro”.

Plutarco

RESUMO

O anseio das empresas em busca de novos clientes é evidente a cada dia e no comércio eletrônico isto não é diferente, diminuindo a privacidade dos usuários de Internet, já que toda informação fica disponibilizada nos servidores e circula pela rede. Grande parte destes dados, capturados por *spywares* são usados por exemplo na área do marketing de forma rápida e direta para obtenção de lucros. Com a contaminação de tal software há ainda grandes perdas nos recursos do computador infectado, causando lentidão dos sistemas e mudanças na área de trabalho. Por este motivo, o presente trabalho realizou análises no sistema operacional Windows XP, tanto na parte visível ao usuário quanto nas linhas de registro do sistema, a fim de documentar e demonstrar a maneira como os *spywares* realizam suas infecções, e ainda estruturas de proteção do sistema e remoção destes programas.

Palavras-Chave: Segurança da informação, Windows XP, Spyware.

ABSTRACT

The yearning of the companies in search of new customers is evident to each day and, in the electronic commerce this is not different, diminishing the privacy of the users of Internet, since all information is available in the servers and circulates through the net. Great part of these data, captured by spywares, are used for example in the marketing area in a fast and direct way for profit gain. With the contamination of such software there is still great losses in the resources of the infected computer, causing slowness of the systems and changes in the work area. For this reason, the present work carried through analyses in the operational system Windows XP, as the visible part to the user as in the lines of register of the system, in order to document and to demonstrate the way of how spywares carries through its infections, and still structures of protection of the system and removal of these programs.

Key-words: Security of the information, Windows XP, Spyware.

LISTA DE FIGURAS

Figura 1. Selo GoodPriv@cy 21

Figura 2 Como trabalha um *spyware* 23

Figura 3. Como trabalha um *adware* 26

Figura 4. Instalando controle ActiveX 28

Figura 5. Instalando *softwares* na Internet baseado em ActiveX no Internet Explorer .. 28

Figura 6. Sistema do computador 30

Figura 7. Interface do regedit.exe 34

Figura 8. Configuração de extensões de arquivos 36

Figura 9. Extensões de arquivos no registro do Windows 37

Figura 10. Tela do programa Registry Monitor 39

Figura 11. Tela do programa RegistryProt 40

Figura 12. Pasta Run do registro HKEY_LOCAL_MACHINE 42

Figura 13. Pasta Run do registro HKEY_CURRENT_USER 42

Figura 14. Processos do sistema 42

Figura 15. Configuração padrão do Internet Explorer no registro 43

Figura 16. Complementos do Internet Explorer 43

Figura 17. Pop-up instalado pelo spyware 44

Figura 18. Arquivos encontrados no sistema 44

Figura 19. Detecção do lopdotcom pelo Spy Sweeper 45

Figura 20. Página inicial modificada pelo *spyware* 47

Figura 21. Registro do Windows mostrando as páginas modificadas 47

Figura 22. HijackThis detalhando o registro alterado por meio do looktome 48

Figura 23. Detecção do looktome pelo Spy Sweeper 49

Figura 24. Aviso de Segurança avisando usuário sobre instalação do Gator..... 51

Figura 25. SpySweeper avisando sobre mudanças no registro 51

Figura 26. Detecção do Gain pelo Spy Sweeper Parte 1 52

Figura 27. Detecção do Gain pelo Spy Sweeper Parte 2 52

Figura 28. Detecção do Gain pelo Spy Sweeper Parte 3 53

Figura 29. Detecção de arquivos do Gain pelo HijackFree 53

Figura 30. Sistema travado e aviso de infecção 54

Figura 31. Gerenciador de tarefas bloqueado..... 54

Figura 32. Detecção do spysheriff pelo Spy Sweeper 55

Figura 33. HijackThis detalhando o registro modificado por meio do spysheriff 55

Figura 34. Detecção de arquivos do Gain pelo HijackFree 56

Figura 35. Software Ad-Aware 56

Figura 36. HijackThis detalhando o registro modificado após da 1ª. remoção..... 57

Figura 37. Linha de registro detectando arquivo na inicialização..... 57

Figura 38. Barras de ferramentas inseridas e página inicial alterada 58

Figura 39. Ícones dos *spyware*s na bandeja do sistema..... 58

Figura 40. Complementos carregados no Internet Explorer 59

Figura 41. Aviso do Spy Sweeper de linhas inseridas no registro 59

Figura 42. Pasta Run no registro HKEY_LOCAL_MACHINE com infecções..... 60

Figura 43. Pasta Run no registro HKEY_CURRENT_USERS com infecções..... 60

LISTA DE TABELAS

Tabela 1. Estudo realizado pela Earthlink..... 16

Tabela 2. Softwares anti-*Spywares*..... 22

Tabela 3. Ranking de *spywares*..... 25

Tabela 4. Estrutura do registro. 35

Tabela 5. Tabela do HijackThis..... 63

LISTA DE SIGLAS

AVI	*Audio Video Interleave*
BHO	*Browser Helper Object*
CPU	*Central Processing Unit*
DDI	Discagem Direta Internacional
DLL	*Dynamic Link Library*
DNS	*Domain Name Service*
DPP	*Data Protection and Privacy*
EXE	*Executable (arquivos executáveis)*
HTML	*HyperText Markup Language*
IBM	*International Business Machines*
IE	*Internet Explorer*
INI	*Initialize (arquivos de inicialização)*
IP	*Internet Protocol*
MP3	*MPEG-1 Audio Layer-3*
NT	*New Technology*
OLE	*Object Linking and Embedding*
ONU	Organização das Nações Unidas
UDP	*User Datagram Protocol*
XP	*eXPerience*

SUMÁRIO

1 INTRODUÇÃO.....13

1.1 OBJETIVO GERAL 14

1.2 OBJETIVOS ESPECÍFICOS 14

1.3 JUSTIFICATIVA..... 15

1.4 ESTRUTURA DO TRABALHO 16

2 A PRIVACIDADE NA INTERNET.....18

2.1 POLÍTICAS DE PRIVACIDADE..... 20

3 HISTÓRICO DOS SPYWARES.....22

3.1 TIPOS DE *SPYWARES* 25

3.2 SISTEMAS OPERACIONAIS NO CONTEXTO..... 30

3.3 REGISTRO DO WINDOWS, O SPYWARE NA SUA RAIZ 32

3.4 FORMAS DE PROTEÇÃO NO REGISTRO 38

4 TRABALHO DESENVOLVIDO: ESTUDOS DE CASOS.....41

4.1 AO INSTALAR O WINDOWS XP 41

4.2 PRIMEIRO CASO: LOOPDOTCOM 44

4.3 SEGUNDO CASO: LOOKTOME 46

4.4 TERCEIRO CASO: GATOR 50

4.5 QUARTO CASO: SPYSHERIFF..... 54

4.6 QUINTO CASO: INFECÇÕES DIVERSAS..... 58

4.7 RESULTADOS OBTIDOS..... 64

CONCLUSÃO.....66

REFERÊNCIAS.....67

APÊNDICE A - Logs do Software Spy Sweeper.....70

APÊNDICE B - Logs do Software HijackThis 83

ANEXO A - Política de Privacidade On-Line do Banco Itaú S.A. 86

1 INTRODUÇÃO

Atualmente as organizações vivem cercadas de tecnologia dentre elas a Internet, com recursos aprimorados a cada dia, porém os problemas relacionados são inevitáveis. Vírus[1], s*pam*[2] e o objeto deste estudo, o s*pyware* ou programa espião, que tentam ocultar-se nos sistemas e secretamente monitorar as atividades.

O dia-a-dia das empresas é permeado por ameaças rotineiras. Há alguns anos eram apenas vírus, que apagavam arquivos e afetavam redes no mundo todo. Depois empresas começaram a se aproveitar da propaganda fácil na Internet e encher as caixas de correio dos usuários com *spam*. Agora, junto com os *spam* e *sites* não confiáveis, os *spywares* formam um novo cenário, pois diferentes dos vírus, são mais complexos de ser removidos mudando suas formas de infecção.

O aumento pelo interesse comercial na obtenção de dados com o poder de identificar perfis dos usuários vem se mostrando como uma crescente preocupação dos usuários de Internet a respeito da proteção à privacidade.

Existem desenvolvedores que trabalham para empresas que demandam a obtenção de dados confidenciais sem respeitar a ética e a boa conduta. Práticas deste tipo aumentam o uso do *spyware* visto que as aplicações são projetadas cada vez mais para capturar informações dos usuários. Alguns destes programas podem extrair o perfil detalhado de um usuário incluindo, por exemplo, os hábitos de navegação, tempo gasto em cada conexão com o provedor, equipe favorita de futebol, religião, preferências sexuais entre outras.

---

[1] Vírus: programa malicioso desenvolvido por programadores para infectar sistemas.
[2] Spam: envio em massa de mensagens não-solicitadas na comunicação eletrônica.

Todas estas ações, naturalmente, são comportamentos indesejados que caracterizam a violação da confidencialidade e muitas vezes da integridade das informações. Conversas monitoradas, documentos roubados, senhas de contas correntes capturadas para o desvio de dinheiro por meio do Internet *Banking*, dentre outros atos maliciosos. Infelizmente, um panorama onde a tendência do *spyware* é de proliferação, principalmente pelo descuido dos usuários que não tem noção da necessidade de boas práticas durante o uso da Internet, como algumas descritas no decorrer deste trabalho. O problema *spyware* é tecnológico, mas a principal forma de combate e retenção do avanço da praga é humana.

Enquanto a forma de combate humana é superficial, a tecnológica é a única que está ao alcance. Desta forma, este trabalho compreende a utilização de ferramentas para análise dos spywares instalados nos computadores e onde ocorrem as infecções para o combate e remoção, onde os resultados poderão servir para desenvolvimento na área.

1.1 OBJETIVO GERAL

Analisar alterações no Sistema Operacional *Windows XP* provocadas por *spywares.*

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos desta pesquisa consistem em:

a) compreender o funcionamento dos *spywares*;

b) demonstrar as conseqüências dos *spywares;*

c) analisar o Sistema Operacional *Windows XP,* juntamente com seu registro, quando manipulado por um *spyware*;

d) verificar softwares de correção do registro, remoção e controle de ataque dos *spywares*;

1.3 JUSTIFICATIVA

O *spyware*, na maioria das vezes, é uma tecnologia que não infringe a lei, e é instalado junto a programas *freewares*[3] e *sharewares*[4] como tocadores de mp3[5], programas *peer-to-peer*[6], e outros, revelando sua funcionalidade secundária nas licenças de uso. A descrição do componente *spyware* é muito ambígua para deixar claro sobre o que ele faz. Em alguns casos estes *softwares* são instalados através das páginas na Internet não confiáveis por meio de códigos maliciosos, e assim, ficam escondidos do usuário.

Conforme a EarthLink (2006), após um estudo em conjunto com a empresa de segurança Webroot, cada computador conectado a Internet tem em média vinte e oito *spywares* instalados no sistema, conforme Tabela 1. O que vem cada vez mais assustando usuários em todo mundo é o fato da maioria desse programas capturarem dados sobre sua navegação, deixando a questão de privacidade principalmente na computação quase impossível. Foram constatados mais de 29 milhões de *spywares* e que corresponde a 90% dos computadores conectados a Internet no mundo.

---

[3] Freewares: programa de computador gratuito para o público sem a necessidade de pagamento por qualquer tipo de licença de uso.
[4] Sharewares: programa de computador para ser usado experimentalmente por um determinado período.
[5] Mp3: tipo de arquivo digital que comprime áudio com perda de dados mantendo a eficiência.
[6] Peer-to-peer: tecnologia para o compartilhamento de arquivos na Internet.

Tabela 1. Estudo realizado pela Earthlink

Computadores verificados	Spywares encontrados	Média de Spywares por micro
1.062.756	29.540.618	27,79%

Fonte: EARTHLINK (2006)

Dados da *Federal Trade Commission* (2005) mostram que 10 milhões de americanos têm sua informação pessoal coletada por *hackers*[7], e atingem um prejuízo de 5 bilhões de dólares para consumidores, e mais de 48 bilhões de dólares para negócios envolvendo cartões de crédito.

Os armazenamentos de informações de programas e periféricos instalados estão no registro na plataforma do Sistema Microsoft Windows; num grande banco de dados; além de informações de preferências dos usuários como a página inicial do Internet Explorer, por exemplo. O Sistema Operacional *Windows XP* é o que há de mais novo no cenário Microsoft para usuários domésticos e estações de redes, e é neste sistema que os *spywares* são instalados, modificando várias linhas no registro, e assim monitorando o controle do computador.

A documentação dos *logs*[8] das linhas de registro é essencial para que programadores possam elaborar *softwares* para proteção do sistema operacional, fazendo isto, automaticamente, sendo uma das formas de diminuir a possibilidade dos *spywares* contaminar o sistema.

1.4 ESTRUTURA DO TRABALHO

Essa pesquisa de Análise do Sistema Operacional Windows XP diante de ataque dos *spywares* é apresentado em dois capítulos de fundamentação teórica, um

[7] Hacker: qualquer pessoa que tem como objetivo investigar a integridade e a segurança de um sistema.
[8] Logs: registro das atividades armazenadas em arquivos por alguns *softwares*.

capítulo mostrando cinco estudos de casos da pesquisa, as considerações finais e dois apêndices.

O capítulo dois aborda sobre a privacidade, cada dia menor para os usuários de Internet, e sem uma lei atualizada para manter a ordem nesta questão.

No capítulo três tem-se o estudo de *spywares*, abordando seu histórico, e detalhes sobre alguns tipos mais famosos destes softwares que trazem muitos danos nos sistemas atuais. Além disso, são comentados itens do Sistema Operacional pouco seguro, como os processos que conduzem à instalação fácil dos *spywares* e o registro do Windows, onde ficam armazenadas as informações.

O estudo desenvolvido no capítulo quatro apresenta primeiramente o Windows depois de instalado e configurado, e em seguida cinco casos de infecções por spywares no sistema, sempre detalhando as linhas no registro modificadas.

A conclusão apresenta comentários dos resultados obtidos com esta pesquisa e sugestões para futuros trabalhos.

O Apêndice A apresenta os rastros deixados por *spywares* no sistema catalogados pelo anti-spyware SpySweeper da Webroot, e Apêndice B fornece informações analisadas das entradas de registro do Windows por meio do software HijackThis da Merijn.

2 A PRIVACIDADE NA INTERNET

Privacidade, por definição sugerida pela comunidade *Privacilla.ORG (2006)* de que uma pessoa precisa ter controle sobre suas informações e exercer este controle de forma consistente com seus interesses e valores pessoais. A privacidade está ligada diretamente ao controle, quanto menos controle um indivíduo exerce sobre suas informações, menos privacidade apresenta.

Porém na Internet, o domínio das informações é muito complicado, pois vários cadastros de usuários e organizações são efetuados a cada dia. E estes documentos não permanecem isolados, havendo constantes trocas de informações entre base de dados que crescem assustadoramente.

Os princípios do direito de privacidade são assegurados pela Constituição Brasileira de 1988.

> Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (CONSTITUIÇÃO BRASILEIRA, 1988, Art. 5º).

De acordo com a Declaração Universal dos Direitos Humanos, a privacidade do indivíduo é um direito fundamental a ser respeitado.

> Artigo 12° - Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei. (ONU, 1948, Art. 12º)

Toda vez que o usuário conecta em um servidor de um *site* na Internet, este obtém informações da máquina, sistema operacional instalado, número IP, além de criar um *cookie* no computador local. Isto acontece para proteção do *site* caso aconteça um episódio de invasão hacker, por exemplo, para que a empresa tenha como elaborar relatórios das pessoas que acessaram o serviço por um determinado período de tempo para investigações.

Segundo a Wikipedia (2006), os *cookies* são informações que ficam armazenadas no computador do usuário no momento da navegação por um *site* qualquer na Internet. Geram arquivos com informações de preferências do usuário, *logins* e senhas de acesso, dentre outras.

Invasões de computadores, acessando dados sigilosos é a forma mais explícita de invasão de privacidade. Usando falhas em sistemas, ou más configurações, os conhecedores de informática denominados crackers[9] tem acesso total a computadores, violando a privacidade, lendo e-mail e até mesmo revelando senhas dos usuários.

A visão capitalista das empresas na busca de lucro tira a privacidade das pessoas, usando o poder da imagem e comercializando produtos em escala mundial, sempre lutando por maior espaço no mercado. Disponibilizam algum serviço "grátis" buscando o *marketing* digital, como *e-mail*, por exemplo, e depois carregam a caixa postal do usuário de propagandas para fins de comércio eletrônico, gerando *spam*.

Além disso, desenvolvem programas com a finalidade de observar os assuntos dos *sites* visitados por usuários com o pretexto de melhorar a qualidade dos serviços ofertados. A comercialização de informações na Internet é outro fator de

---

[9] Cracker: qualquer pessoa que utiliza seus conhecimentos avançados de programação com o objetivo de prejudicar uma rede.

preocupação, como venda de listas com e-mails e cadastros diversos que transitam pela rede.

2.1 POLÍTICAS DE PRIVACIDADE

Informar dados para cadastro em algum *site* na Internet é bem comum, mas o que o usuário desconhece é que muitos destes *sites* não têm uma política de privacidade. Segundo Gaertner (2005), a política de privacidade de uma organização deve mostrar como são armazenados e tratados os dados de seus clientes e como serão utilizadas posteriormente. Além disso, a empresa responsável por elaborar sua política deve informar que tipos de sistemas de segurança são utilizados, que tipo de informação é coletado e ainda se o usuário tem o direito de escolher se quer ou não que suas informações sejam compartilhadas com uma terceira parte.

Para ajudar as organizações na questão da política de privacidade, há um selo internacional de privacidade chamado *GoodPriv@cy* bastante utilizado no Brasil, no qual empresas como o Banco Bradesco e Itaú são certificadas, como mostra a Figura 1. A política de privacidade do Banco Itaú S.A. é demonstrada no Anexo A, esclarecendo como é coletado e tratado os dados individuais de cada cliente.

A *IQNet* é uma organização certificadora do selo *GoodPriv@cy* para clientes interessados na proteção das suas companhias. Proteção de dados e privacidade (DDP) estão se tornando fatores de qualidade crescente e significante para os negócios. A especificação de IQNet *GoodPriv@cy* integra proteção de dados e exigências de segurança de informação. Sua função é apoiar organizações que desejam administrar a proteção de dados e segurança da informação de forma eficaz.

FUNDAÇÃO VANZOLINI

CERTIFICADO

A FUNDAÇÃO CARLOS ALBERTO VANZOLINI

certifica que a empresa

BANCO ITAÚ S/A

no campo de atividade:

Privacidade Online – Gestão da captação de dados fornecidos por clientes e não clientes aos servidores do Banco Itaú S.A. através das páginas componentes do site www.itau.com.br

Av. do Estado, 5533 – São Paulo – SP – Brasil

implementou e mantém um

Sistema de Gestão de Proteção de Dados

Através de auditoria da Fundação Vanzolini foi comprovado que esse Sistema de Gestão cumpre os requisitos da especificação:

GoodPriv@cy Data Protection Label (2002 edition)

Data Protection IQNet GoodPriv@cy

Este certificado é válido até : 12 de dezembro de 2007

Número do Certificado : GP@-4106

São Paulo, 13 de dezembro de 2004

FUNDAÇÃO CARLOS ALBERTO VANZOLINI

PROC – GP@ – M01521

Figura 1. Selo GoodPriv@cy
Fonte: IQNET (2006)

No próximo capítulo, será abordado sobre o que são os *spywares*, um pouco da história de como surgiram estes *softwares*[10] e, além disso, os tipos mais conhecidos na Internet. Ainda o sistema operacional, que é onde acontece a infecção por suas falhas de segurança e o registro do Windows que é alterado na execução do *spyware*.

[10] Softwares: programa de computador, no qual é necessário pagar a licença de uso do mesmo.

3 HISTÓRICO DOS SPYWARES

Em outubro de 1996, foi encontrado o primeiro *spyware* postado na Usenet para ridicularizar o *site* de negócios da Microsoft. Em 1999, o fundador da Zone Labs, Gregor Freund usa o termo *spyware* para anunciar a imprensa o ZoneAlarm Personal Firewall, desde então, usuários de computadores do mundo usam este termo.

Posteriormente, aparece a primeira versão de um *freeware* com um *spyware* embutido, um jogo de humor muito circulado pela Internet chamado *Elf Bowling*. Muitas pessoas ficaram surpresas, pois o programa transmitia informações pessoais ao criador do jogo enquanto se divertiam no jogo.

No começo de 2000, Steve Gibson da Gibson Research publicou no jornal uma matéria de um programa que era suspeito de capturar informações pessoais em seu sistema. Após analisarem o *software* e descobrir que tinham componentes extras de uma companhia chamada Aureate (que depois virou Radiate) e Conducent. O *software* de anúncios coletava informações sobre a cultura do usuário, além de instalar *spywares* no sistema e dificultar a remoção destes.

Com esta análise no ano 2000, Gibson desenvolveu o primeiro *software* anti-*spyware*, o OptOut, e muitos outros *softwares* do gênero tem aparecido desde então, tais como os principais anti-*spywares* no site Superdownloads (2006), conforme Tabela 2.

Tabela 2. Softwares anti-*Spywares*

Nome do anti-*Spyware*	Empresa	Download disponível em:
Ad-aware SE Personal	Lavasoft	www.lavasoft.com
Spy Sweeper	Webroot	www.webroot.com
HijackThis 1.99.1	Merijn	www.merijn.org
a-squared HijackFree Analysis	Emsi	www.hijackfree.com

Fonte: SUPERDOWNLOADS (2006)

Spyware, de modo geral, é um *software* automático que recolhe informações pessoais e envia a uma entidade externa, altera a forma em que o computador e o navegador estão configurados e aumenta o número de anúncios de publicidade durante o uso da Internet (WIKIPEDIA, 2006).

A Figura 2 detalha como um *spyware* funciona:

1º - Instalado nos sistemas através da Internet;

2º - Computador funciona normalmente já que o programa ocupa apenas alguns Kbytes[11] na memória;

3º - Informações são enviadas à empresa que desenvolveu o *spyware*.

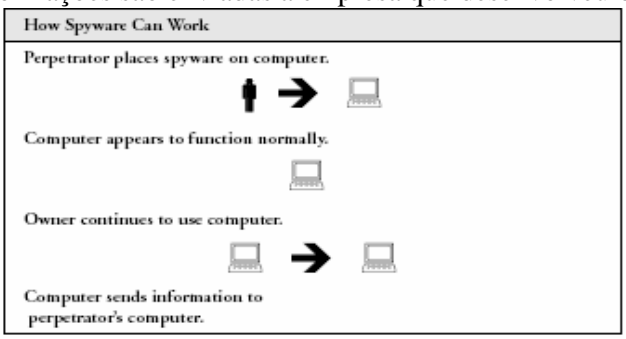


Figura 2 Como trabalha um *spyware*
Fonte: ERBSCHLOE, M (2004)

Em Segurança Máxima (2000, p.335), é relatado que os computadores com base no Windows apresentam segurança precária, assim sendo facilmente infectados por *spywares*, logo os usuários notam redução no desempenho do sistema. Criam significante e não desejado uso de CPU, a quantidade de informações armazenadas no disco por estes programas aumenta, além de limitar o tráfego na rede, causando falhas na conexão a Internet. A utilização de recursos torna-se lento e paradas de sistema são bastante comuns, ocasionando muitas vezes a "*Blue Screen of Death*", a famosa tela azul de erro do Windows.

[11] Kbyte: conjunto de 1024 bytes.

Infecções de *spywares* fazem os usuários procurarem suporte em assistências técnicas, ou revendedores. Muitas vezes o usuário não tem a consciência do *spyware*, e pensa que o problema está no Windows ou no *hardware*. Em casos de grandes infecções, muitas vezes a reinstalação do sistema é fundamental para a normalidade. Geralmente o *spyware* é um processo, e desabilitam Antivírus, *firewalls*[12], diminuindo a segurança do navegador, com isso o sistema fica vulnerável para futuras infecções.

Existem basicamente dois modos dos *spywares* aparecerem no sistema. O primeiro deles, através de *freewares* com arquivos *spywares* embutidos, e o outro por meio do navegador, geralmente no Internet Explorer da Microsoft. Estes programas espiões geralmente são ativados sempre que o Windows é iniciado, e ainda quando executado o BHO[13]. (WIKIPEDIA, 2006)

Usado para descobrir todo tipo de informação como teclas digitadas no teclado, páginas visitadas recentemente na Internet pelo usuário e aplicações instaladas no sistema. *Spywares* podem ainda coletar nomes, e-mails, números e senhas de cartão de crédito, dados bancários e todo tipo de informação. Tudo isto fica em um banco de dados para criar um perfil individual, de uma família, ou de uma empresa, e por meios de publicidade, criam perfis de usuários para a venda de um serviço ou mercadoria concretizar-se mais rápido. Por exemplo, se um *spyware* obtém a informação de que um usuário irá fazer uma viagem para Bahia, ele relaciona pacotes promocionais de empresa de turismo, e dessa forma facilita atingir o mercado específico.

---

[12] Firewalls: sistema de segurança que protege a rede de entradas ilegais.
[13] Browser Helper Object: programas executados ao mesmo tempo em que é iniciado o Internet Explorer.

3.1 TIPOS DE *SPYWARES*

Existem milhões de *spywares* e a cada dia surgem novos, assim como vírus, se modificam para dificultar a remoção. A Tabela 3 detalha o *ranking* dos 10 *spywares* mais predominantes.

Tabela 3. Ranking de *spywares*

Spyware	%
Gator	4,78
CoolWebSearch	4,03
180 Search Assistant	3,13
HuntBar	2,65
Cydoor	2,58
ISTbar	2,53
WhenU-DesktopBar	2,44
New.Net	1,91
IEPlugin	1,86
BargainBuddy	1,65

Fonte: SPYWAREGUIDE (2006)

O *adware* inicialmente instalado em *freewares*, como o Kazaa[14], gera propagandas para que o usuário compre um outro programa ou a versão completa (este sem propagandas) do programa inicialmente grátis. Em seguida os *adwares* monitoram o comportamento dos usuários de Internet, fazendo publicidades personalizadas de acordo com o perfil de cada um, tendo assim funções de *adwares* e *spywares*.

Adwares nem sempre são arquivos maliciosos, muitos deles apenas buscam informações do usuário para trabalhar com marketing. A remoção do *adware* é o que incomoda muitos usuários, pois não funciona como os demais programas simplesmente tendo um arquivo de desinstalação.

O *adware* geralmente é instalado através de um *site* de Internet que o usuário acessa para que a empresa responsável monitore o computador, com o sistema

[14] Kazaa: programa peer-to-peer de músicas.

funcionando normalmente, assim como na Figura 3. A maioria dos spywares seja qual for sua classificação, além de sua característica padrão, acrescenta *adwares* em sua instalação. (ERBSCHLOE, 2004)

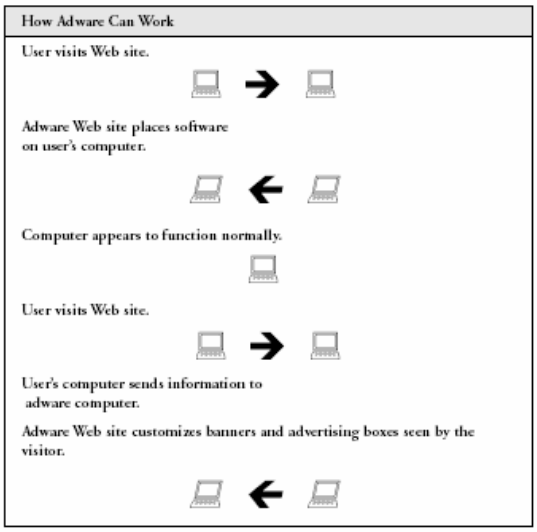


Figura 3. Como trabalha um *adware*
Fonte: ERBSCHLOE, M (2004)

Porém com o passar do tempo, os *adwares* sofisticaram-se, com o surgimento de inúmeras variantes, e é grande o mistério por trás do funcionamento destes programas, pois muitos utilizam nomes aleatórios para dificultar na remoção e a busca de informações de tal arquivo na Internet.

Além disso, conforme o *site* WIKIPEDIA (2006), os *spywares* realizam alterações no registro do Windows e a seguir se escondem no sistema para garantir que as alterações não sejam desfeitas, exigindo então não mais a ação de um antivírus, mas sim de um programa específico. Por vezes os *adwares* exibem propagandas pornográficas, falsos avisos de infecção do sistema por vírus e propagandas para venda de produtos causando instabilidade no sistema, principalmente no navegador.

O *stealware,* outro programa do gênero, que segundo Laufer et al (2004) é um programa "ladrão de audiência". Na Internet muitas vezes o *site* de uma organização possui um link[15] para o *site* de um patrocinador e a organização é remunerada pelos números de acessos que são efetuados através de seu *site* pelo patrocinador. O *stealware* engana este mecanismo de forma a contabilizar acessos originados de uma outra organização diferente da legítima. A identificação da organização é geralmente realizada por informações armazenadas na estação do usuário, como *cookies*, ou através do próprio endereço da página *web* acessada.

Normalmente, o *stealware* é embutido em *softwares* que alguns *sites* forçam o usuário a instalar, com a finalidade de liberar o acesso do usuário a seções restritas do portal. O usuário, ao executar o *software*, habilita o código malicioso. Tudo o que o *stealware* tem a fazer então é modificar os *cookies* na máquina do usuário ou forjar o endereço da página acessada.

Segundo Hunter (2005), o *Hijacker* modifica as configurações do navegador de Internet, como página inicial, página de busca padrão e arquivos de *hosts*[16], como o DNS[17]. Este tipo de código é instalado no uso da Internet em *site* que utilizam os controles *ActiveX*[18] para o Microsoft Internet Explorer como mostra a Figuras 4 e 5. Logo após a instalação de *ActiveX* que contém *Spywares*, as configurações do Internet Explorer e algumas configurações do Windows, como o papel de parede e a proteção de tela podem ser modificados automaticamente. Mesmo se o usuário retornar a configuração inicial, o *hijacker* executa como seu arquivo .DLL ou executável quando o sistema é reiniciado, e o mesmo volta a ativa.

---

[15] Link: seu significado é atalho, mais na Internet designa partes clicáveis em forma de texto ou imagem, que levam a outras página do mesmo site ou para sites diferentes.
[16] Hosts: qualquer dispositivo ou computador conectado na rede.
[17] DNS: Sistema de nomes de domínio, serve para resolver nomes em endereços de rede.
[18] ActiveX: conjunto de tecnologias para facilitar a integração entre diversas aplicações.

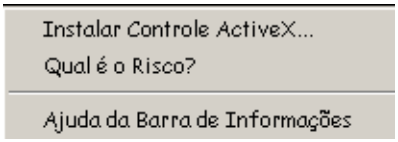


Figura 4. Instalando controle ActiveX
Fonte: MICROSOFT (2005)

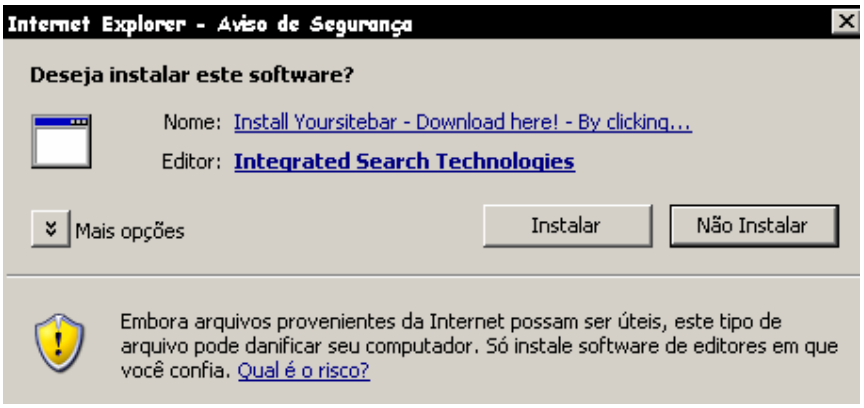


Figura 5. Instalando *softwares* na Internet baseado em ActiveX no Internet Explorer
Fonte: MICROSOFT (2005)

O *logging keystrokes*[19], conforme Hunter (2005) é um tipo de *spywares* que grava todas as informações em *logs,* entre teclas digitadas, cópia das telas, e uma lista dos programas acessados durante a sessão, além das caixas do correio eletrônico. Então, o programa é configurado para enviar estas informações para um *hacker* ou à empresa que desenvolveu o *software*. Usuários que costumam acessar bancos, ou outro tipo de acesso de comércio eletrônico tem de ter muito cuidado, pois *logins*[20], números de cartão de crédito, códigos de bancos e todo tipo de senha podem ser repassados e causar grandes prejuízos.

Em muitos casos, a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como por exemplo, o acesso a um *site* específico de comércio eletrônico ou

[19] Keystrokes: o ato de teclar.
[20] Login: conjunto de caracteres solicitados para o acesso em sistemas computacionais.

Internet Banking[21]. Normalmente, o keylogger contém mecanismos que permitem o envio automático das informações capturadas para terceiros.

Para segurança, instituições financeiras desenvolveram os teclados virtuais para evitar que os *keyloggers* pudessem capturar informações sensíveis de usuários. Então, foram desenvolvidas variantes mais avançadas de *keyloggers* também conhecidas como *screenloggers*, que gravam os pontos vetoriais em que a posição do mouse foi pressionada em um determinado momento, por este motivo várias instituições bancárias modificam os números de posição no teclado virtual.

Conforme o Wikipedia (2006), discadores ou *dialers* são *spywares* usados para ligar automaticamente para números de telefones que permitem o acesso a determinados serviços por computador, com atos lesivos. Tem crescido o uso destes programas de forma fraudulenta, ao serem utilizados para discar para números pagos sem o conhecimento dos usuários, geralmente relacionado à pornografia disponível via números de telefone com altas taxas de uso por minuto. Para facilitar o acesso, as empresas com estes serviços desenvolveram discadores próprios, e se usados são altamente lucrativos.

Foi assim que os discadores passaram a ser inseridos em páginas da *web* criadas para fazer o *download*[22], instalar e executar os programas sem que os usuários afetados percebessem. Um ataque com um *dialer* é iniciado normalmente quando o usuário visita determinadas páginas da *web*, como as que possuem conteúdo pornográfico, assuntos *hacker*, *cracks* para programas[23] e *downloads* ilegais. As principais conseqüências dos ataques com discadores é a criação de uma nova conexão, que será usada para se conectar a Internet com número diferente, que ao invés de fazer a

---

[21] Internet Banking: tipo de serviço utilizado para realizar transações bancárias por meio da Internet ou da Intranet da instituição.
[22] Download: é a transferência de dados de um computador remoto para um computador local.
[23] Cracks para programas: transforma o programa de demonstração numa cópia idêntica a original.

discagem para o servidor habitual, conecta a serviços pagos e cobrados em conta telefônica, geralmente com código DDI.

3.2 SISTEMAS OPERACIONAIS NO CONTEXTO

De acordo com Tanenbaum (2000), o Sistema Operacional é um *software* básico que torna o *hardware* utilizável para funcionamento pelos usuários, e um gerenciador de recursos.

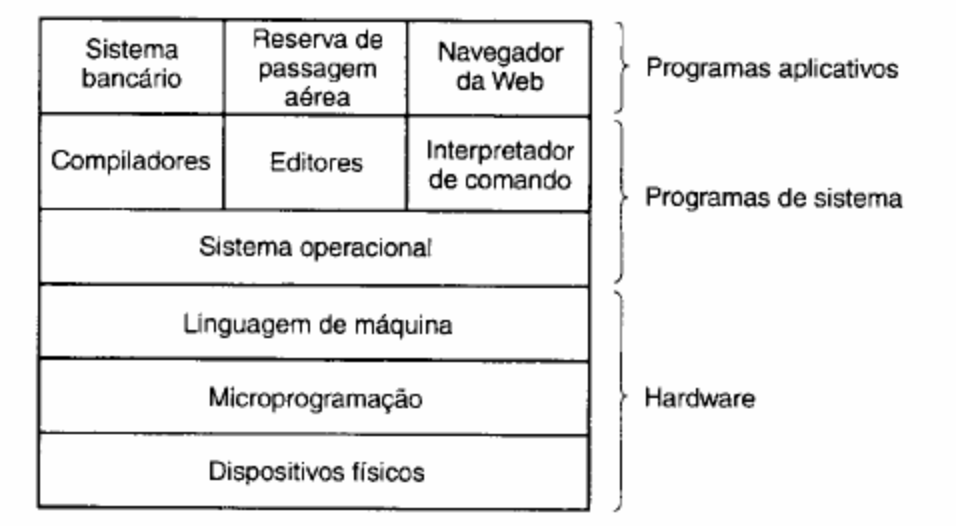


Figura 6. Sistema do computador
Fonte: TANENBAUM, A (2000)

O conjunto do Sistema Operacional é constituído por um núcleo e um conjunto de *softwares* que executam operações simples, mas que juntos desempenham um grande potencial.

Segundo Cardozo e Magalhães (2002), a primeira geração do Sistema Operacional era máquina de cálculo que utilizavam válvulas na década de 40, um pequeno grupo de pessoas projetava, construía, programava, operava e mantinha cada

máquina. Toda programação era feita em linguagem de máquina, muitas vezes interligando tomadas para controlar funções básicas.

Na segunda geração, na metade dos anos 50, a utilização do transistor tornou os computadores mais seguros, sendo empregado em atividades múltiplas. Para executar um processo, o programador produzia um conjunto de cartões perfurados, e entregava ao operador que dava entrada do programa no computador, finalmente retornava ao programador o código fonte de forma impressa. A maioria dos computadores nesta geração foi criada para cálculo de engenharia e científicos.

No início dos anos 60, a IBM realizou a junção da arquitetura e conjunto de instruções para o mesmo computador para atender tanto aplicação científica como comerciais. Assim na terceira geração surgiu o conceito da multi-programação, e o armazenamento das leituras de cartões perfurados em discos, reduzindo a espera nos resultados.

A principal evolução nos Sistemas Operacionais foi sem dúvida na quarta geração, com os computadores pessoais é possível utilizar o processador para várias tarefas simultâneas comutadas de programa em programa na ordem de milisegundos, por exemplo: navegar na Internet enquanto imprime um texto, e silenciosamente um processo convocando um *spyware* ou vírus, e infectando o sistema.

Um processo é basicamente um programa em execução na memória principal do sistema. Ele consiste do executável, os dados e a pilha do programa, o descritor do programa, ponteiro da pilha, e outros registradores, e todas as outras informações necessárias para rodar o programa, um processo pode estar em um determinado estado; entre ativo, bloqueado ou executando (TANENBAUM, 2000).

Os processos fazem todo o serviço que o *spyware* solicita, enviam dados importantes a um servidor em qualquer parte do mundo, ou então gravam tudo o que for

digitado para um *hacker* sem o consentimento do usuário, assim como mudam configurações de área de trabalho e navegador da Internet.

Para realizar o compartilhamento da CPU entre vários processos, um Sistema Operacional, necessita de critérios para delimitar, qual o próximo processo será executado primeiramente, esse modo de seleção é realizado pelo escalonador.

Toda informação referente a processos é controlada por uma parte do sistema chamada núcleo ou kernel. Este representa apenas uma pequena parte da programação do Sistema Operacional, mas é o código mais utilizado, e por esta razão permanece na memória principal do sistema.

A segurança nos Sistemas Operacionais é uma preocupação freqüente, e são grandes os valores orçamentários que como, por exemplo, a Microsoft investe nesta área. A cada dia novas correções são elaboradas para que o sistema esteja sempre protegido de ataques. Muitos usuários ignoram estas atualizações que ajudam muito a combater spywares e outros *bugs*[24] provenientes do sistema.

Segundo a própria Microsoft, não existe um sistema operacional 100% seguro e livre de falhas, e através do site Windows Update Service disponibiliza aos usuários a atualização de seus softwares à medida que *bugs* surgem.

3.3 REGISTRO DO WINDOWS, O SPYWARE NA SUA RAIZ

Conforme Kokoreva (2002), quando o Windows 3.1 surgiu, este veio com três tipos de arquivos de configurações diferentes. O primeiro é os arquivos de inicialização de sistemas, que tinha os arquivos Control.ini, Progman.ini, Protocol.ini

[24] Bug: falha no programa que o impede de funcionar como o esperado.

System.ini, Win.ini, e Winfile.ini. O Win.ini era onde ficavam as configurações de *software*, onde cada nova aplicação instalada pelo usuário, era acrescentada linhas neste arquivo, e com o passar do tempo ficava muito carregado e algumas seções eram ignoradas pelo sistema, então usuários avançados criavam arquivos .ini privados.

System.ini era responsável pela parte do *hardware*, criava um banco de dados com toda a configuração do Sistema e seus respectivos *drivers*[25]. Progman.ini continha as configurações de inicialização do ambiente do Windows e o Winfile.ini arquivos de administração do Windows, se algum destes eram perdidos, toda a configuração do usuário retornava ao padrão do Windows. Control.ini era responsável por configurações do painel de controle. O Protocol.ini era para ambiente de redes e nele continham configurações da rede local.

Além dos arquivos .ini privados, onde eram instalados junto com outras ferramentas para configurações específicas, incluindo tamanho e local das aplicações do Windows e listas de arquivos utilizados pelos usuários recentemente.

Segundo Kokoreva (2002), finalmente surge o Reg.dat, que depois virou o registro dos outros Sistemas Operacionais da Microsoft. Um hierárquico banco de dados que compreende numa estrutura de *root*: HKEY_CLASSES_ROOT, neste estão contidas outras estruturas, no qual armazenam informações de suporte OLE e arquivos associados. Os arquivos de registro permitem usuários de modificar o comportamento do sistema e ver a lista de aplicações no Ambiente Windows.

O registro torna-se sucessor dos arquivos .INI, que conforme Torres (1998) possuía sérios defeitos e limitações e era muito inconveniente para o uso. O Windows

---

[25] Drivers: programas que disponibilizam a comunicação entre o sistema operacional e dispositivos ligados a um computador.

NT 3.5 foi o primeiro a conter um registro similar ao atual, com quatro chaves *root*[26]: HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER, HKEY_CLASSES_ROOT, e HKEY_USERS.

O registro atual do Windows é um banco de dados de forma hierárquica, e apresenta praticamente todas as funções como as configurações dos programas, o *kernel*[27], *Plug* and *Play*[28], *driver* de dispositivos, perfil de usuário, perfil de *hardware* e outros.

A partir do Windows 95, a Microsoft desenvolveu o editor de registro com o nome de regedit.exe para administradores de sistema realizar modificações no registro.

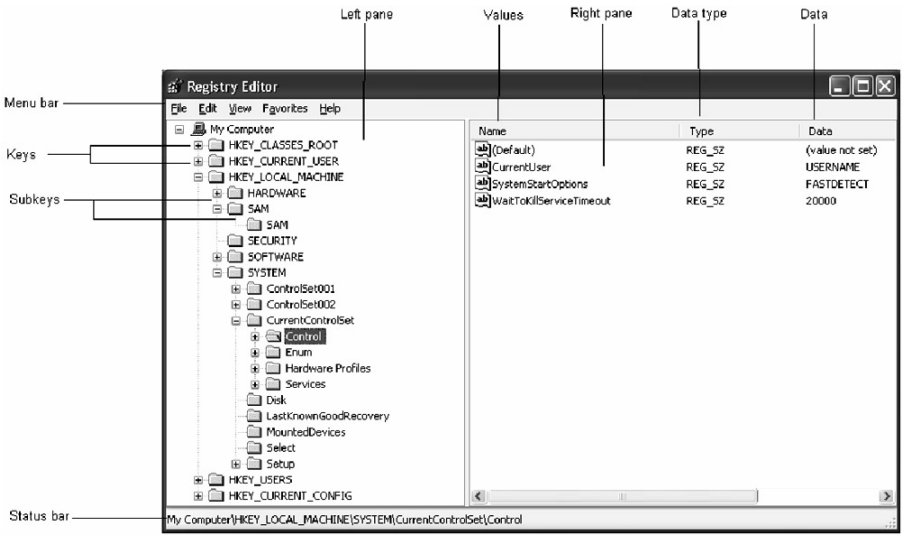


Figura 7. Interface do regedit.exe
Fonte: MICROSOFT (2006)

A interface do regedit.exe é composto por meio dos itens como detalha a Figura 7, com o nome, o valor e o tipo de dado da chave. A estrutura atualmente do

[26] Root: mais alto nível da hierarquia.
[27] Kernel: núcleo do sistema operacional que representa a camada mais baixa de interface com o hardware.
[28] Plug and Play: tecnologia para a facilitação do reconhecimento de um dispositivo conectado ao equipamento.

registro compreende em cinco chaves de *root*: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, e HKEY_CURRENT_CONFIG.

Tabela 4. Estrutura do registro.

Chave Root	Descrição
HKEY_CLASSES_ROOT	Informações de tipos de arquivos e suas associações, para que o sistema conheça qual programa é necessário para abrir um tipo de arquivo, ou seja, uma extensão. Esta chave na verdade é um atalho para HKEY_LOCAL_MACHINE\Software\Classes.
HKEY_CURRENT_USER	Perfil do usuário ativo no sistema, incluindo todo o ambiente, configurações da área de trabalho, da rede e de aplicações.
HKEY_LOCAL_MACHINE	Informações globais de *drivers* e dados do Sistema Operacional, incluindo tipo de barramento, sistema de memória, *driver* de dispositivos e outras informações usadas durante o processo de inicialização.
HKEY_USERS	Todo o perfil dos usuários ativos, incluindo HKEY_CURRENT_USERS.
HKEY_CURRENT_CONFIG	Informações do perfil atual do *hardware* instalado. As modificações são introduzidas desde a configuração padrão de serviços e dispositivos instalados na chave HKEY_LOCAL_MACHINE. Esta chave na verdade é um atalho para HKEY_LOCAL_MACHINE\ System\CurrentControlSet\HardwareProfiles\Current.

Fonte: MICROSOFT (2006)

Para o estudo dos *spywares*, as chaves de registro mais importantes são a HKEY_LOCAL_MACHINE\Software que é responsável por todo o banco de dados de *softwares* instalados no Windows e HKEY_LOCAL_MACHINE\System onde ficam registrados desde controle de inicialização, *drivers*, serviços de sistema e o comportamento do Sistema Operacional.

Assim como a chave HKEY_CLASSES_ROOT merece um entendimento, onde o Windows associa a extensão do arquivo a um determinado programa instalado

no computador. Muitos códigos maliciosos modificam estas chaves deixando o sistema confuso.

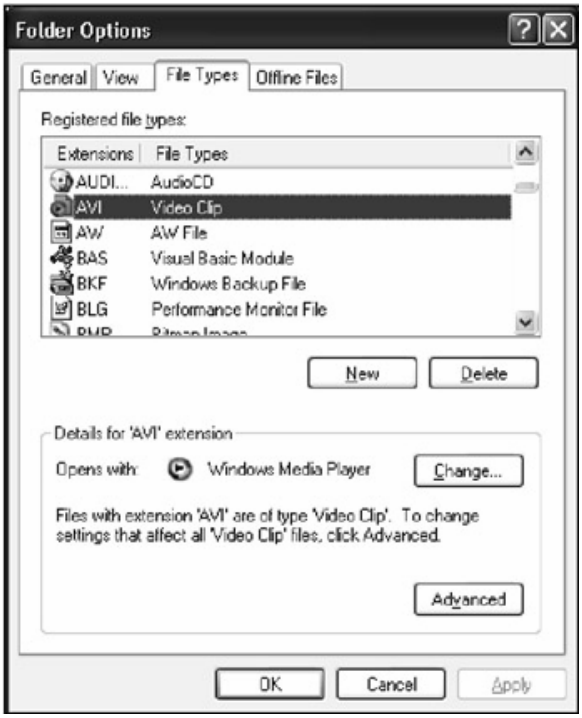


Figura 8. Configuração de extensões de arquivos
Fonte: MICROSOFT (2006)

A configuração de arquivos do sistema operacional é efetuada graficamente como mostra na Figura 8, e fica na chave HKEY_CLASSES_ROOT do registro do Windows, podendo adicionar ou excluir uma nova extensão, alterar os ícones e mudar o aplicativo padrão para execução.

No caso arquivo AVI, uma extensão de vídeo famosa por usuários de computador, configurado inicialmente para executar pelo programa Windows Media Player da própria Microsoft.

Na Figura 9, mostra-se o mesmo exemplo da Figura 8, mas desta vez no ambiente do registro, na chave HKEY_CLASSES_ROOT, onde todas as extensões estão presentes. Aqui é mostrado a mesma extensão .AVI, e ao abrir as propriedades nas

pastas do regedit, nota-se que as configurações estão iguais ao modo gráfico, porém mais complexas de serem modificadas.

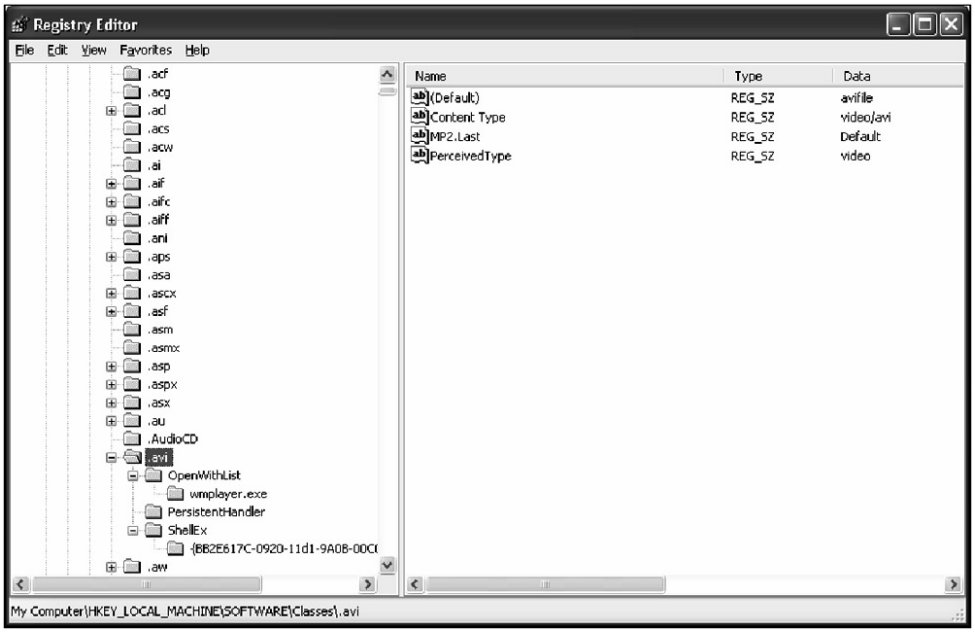


Figura 9. Extensões de arquivos no registro do Windows
Fonte: MICROSOFT (2006)

Spywares são executados como serviços do sistema, configurados para iniciar junto ao Sistema Operacional, e incluir seus atributos na chave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\nome_do_serviço.

Podem iniciar como arquivos de programas, estes na chave HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Nestes dois casos, mesmo que o usuário altere alguma configuração em seu computador, logo após a inicialização do sistema, executará novamente o processo ou arquivo, e o *spyware* voltará a ativa e mudará as configurações conforme sua programação.

O BHO malicioso, da mesma forma que processos e arquivos, depois que executado retorna as configurações programadas do *spyware*, porém, neste caso ele fica

como um objeto do Internet Explorer e apenas ao abrir o navegador que infectará o sistema. Este tipo de configuração fica armazenado na chave HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ Browser Helper Objects do registro do Windows.

No caso de processos, arquivos configurados na inicialização do Windows e do BHO, eles são executados e podem infectar o sistema. Depois do sistema infectado o *spyware* altera muitas configurações, incluindo *ToolBar*[29] no navegador Internet Explorer armazenados na chave HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Internet Explorer\Toolbar e altera as configurações de páginas padrões em HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\Internet Explorer\Main.

Modifica configurações de DNS da rede na chave HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ Interfaces, insere menus extras em HKEY_CURRENT_USER\Software\ Microsoft\Internet Explorer\MenuExt, configura protocolos adicionais na chave HKEY_CLASSES_ROOT\ PROTOCOLS\Handler\msnim, e vários outros tipos de configuração desde mudança no papel de parede até proxy[30] de rede.

3.4 FORMAS DE PROTEÇÃO NO REGISTRO

A principal e mais fácil maneira de proteger o registro do Windows XP é bloqueá-lo, não deixando editar ou inserir nenhuma linha sequer, o que deixaria o sistema limitado, pois nenhum programa poderia ser instalado. Muitos administradores

---

[29] ToolBar: régua de ferramentas para funções específicas.
[30] Proxy: software intermediário entre o computador cliente e servidores com alto poder de armazenamento.

de sistema configuram contas de usuários limitadas, para que estes tenham acesso a apenas algumas configurações e a instalação dos programas é executada apenas com a permissão do responsável, assim, *spywares* e vírus tem dificuldade de manipularem arquivos neste sistema.

Além desta forma básica de proteger o registro para não ser atingido por programas maliciosos, existem vários outros para este fim que informam ao usuário quando qualquer alteração está sendo feita no registro. Um *software* encontrado para *download* na Internet é o Registry Monitor da empresa Sysinternals, mostrado na Figura 10, ele detalha todos os processos sendo executados no momento e a chave de registro que está abrindo para efetuar tal operação.

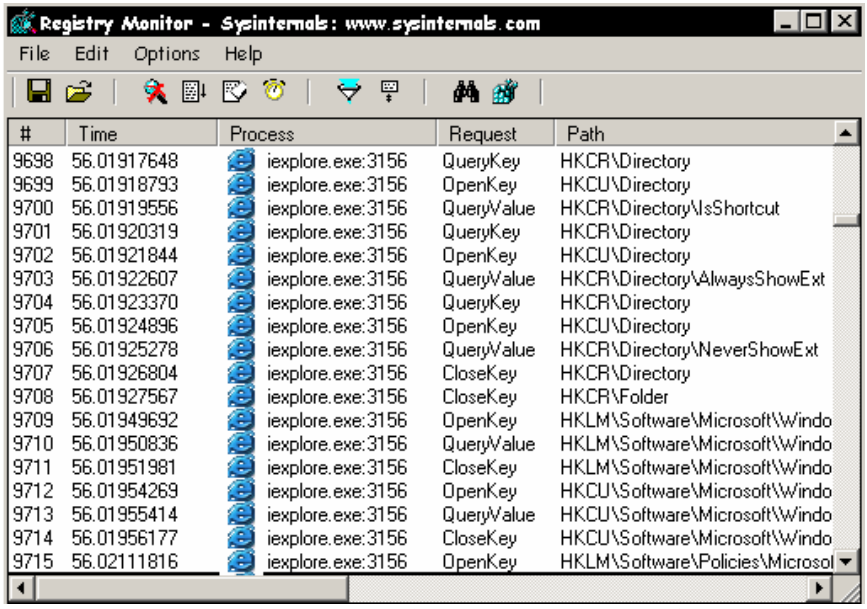


Figura 10. Tela do programa Registry Monitor
Fonte: SYSINTERNALS (2005)

Muitas são as análises feitas neste programa, e com ele tem-se uma forma de verificar vírus, *spywares* ou outros códigos maliciosos sendo implantados no sistema. Quando o processo do iexplore.exe, no caso o Internet Explorer é executado, são mostradas as chaves responsáveis por iniciar *Toolbar*, BHO e botões extras do navegador.

Outro *software* semelhante é o RegistryProt da DiamondCS, porém este atua de forma diferente, para cada mudança no registro que causa suspeita, aparece um aviso ao usuário, e este aceita ou não a alteração do registro. No caso da Figura 11, um controle ActiveX foi instalado através de uma página de *crack* e tentou instalar um *spyware* no sistema, então o programa aparece ao usuário com a pergunta sobre a mudança no registro, caso queira deletar a entrada do arquivo bedlbxwr.exe da chave HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\ Run.

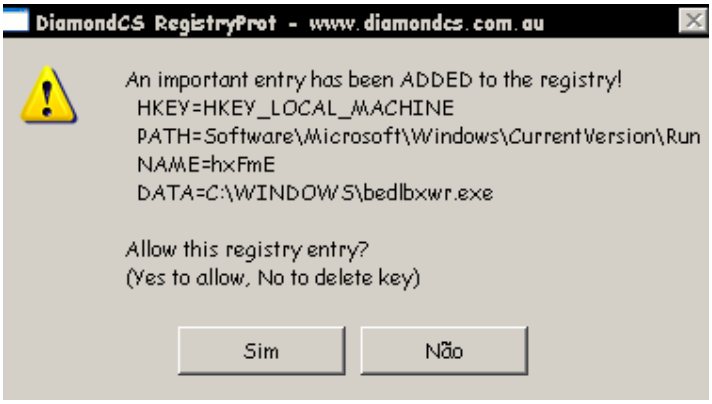


Figura 11. Tela do programa RegistryProt
Fonte: DIAMONDCS (2005)

Agora que já se obteve as informações sobre os spywares, a parte onde ele ataca o sistema operacional e detalhes da maneira como funciona o registro do Windows, pode-se então iniciar os testes no computador para verificar as formas de infecção dos spywares para um estudo mais amplo do assunto. E, no capítulo 4 será iniciado o estudo de casos com algumas infecções de *spywares* conhecidos e um sistema repleto de contaminações por estes softwares.

4 TRABALHO DESENVOLVIDO: ESTUDOS DE CASOS

Para um maior conhecimento do contexto, de como atuam estes *softwares* dentro do sistema, onde se alojam e a forma mais simples de remoção foram realizados cinco estudos de casos. Para início do projeto foi escolhido um computador AMD *Athlon* XP 2700+ com 512MB de memória e disco rígido de 80GB, e instalado o Sistema Operacional Microsoft Windows XP Professional com *Service Pack* 2.

A fim de realizar o estudo, alguns sites considerados perigosos na Internet foram acessados dentre eles o www.cracks.am e www.astalavista.box.sk para possibilitar a contaminação por spywares. Ainda, foi acessado o site www.gator.com para fazer o *download* de *freewares* desenvolvidos pela empresa Gator, que segundo a Tabela 3 no Capítulo 3, é considerado o *spyware* com maior índice de infecção no mundo. Para a análise e remoção dos spywares, foram utilizados os softwares já mencionados na Tabela 2 do Capítulo 3.

4.1 AO INSTALAR O WINDOWS XP

Após a instalação do Sistema Operacional *Windows XP e* configuração dos *drivers*, a pasta *Run* tanto do sistema como do usuário específico não possuem programas em execução como detalha as Figuras 12 e 13. Apenas processos de redes e outros processos que precisam ser utilizados para o funcionamento do Windows, assim referido na Figura 14.

Por enquanto, é praticamente impossível um *spyware* surgir no sistema, pois o disco rígido do computador estava formatado anteriormente e nesta ocasião possui apenas o sistema operacional, e após o usuário iniciar suas atividades, principalmente na Internet, iniciará as infecções.

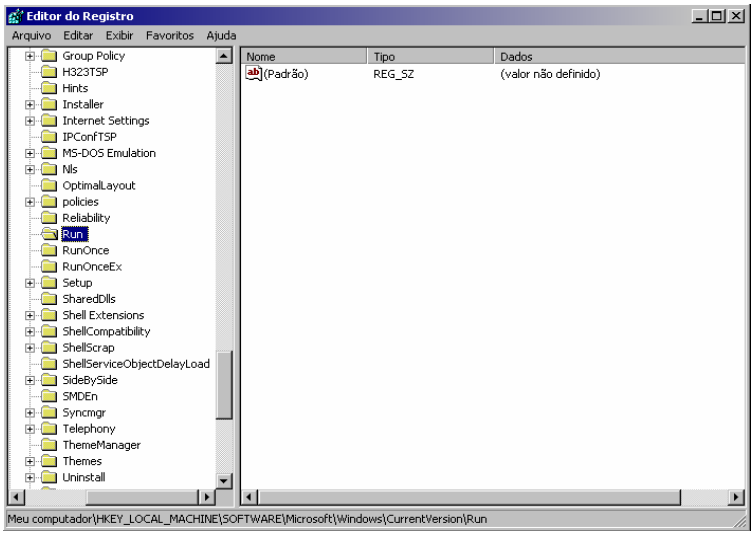


Figura 12. Pasta Run do registro HKEY_LOCAL_MACHINE
Fonte: MICROSOFT (2006)

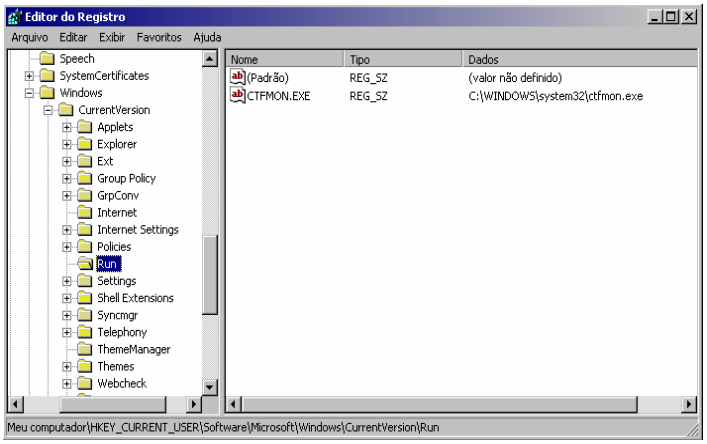


Figura 13. Pasta Run do registro HKEY_CURRENT_USER
Fonte: MICROSOFT (2006)

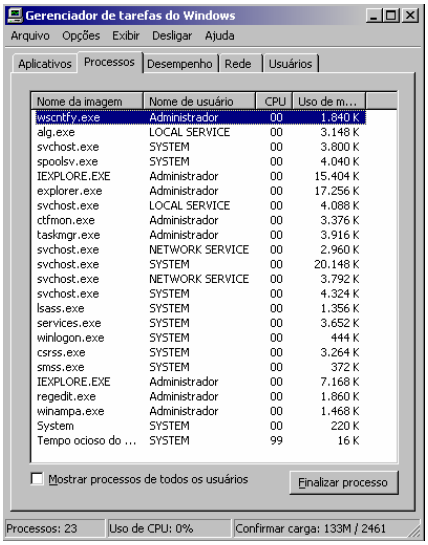


Figura 14. Processos do sistema
Fonte: MICROSOFT (2006)

O navegador, no caso o Internet Explorer da Microsoft, todas as páginas principais estão com os padrões do Windows XP, que são configurados após a instalação do mesmo (Figura 15), e que somente dois complementos[31] estão ativos junto ao navegador, que são o Windows Messenger [32]e o Shockwave[33], mostrado na Figura 16.

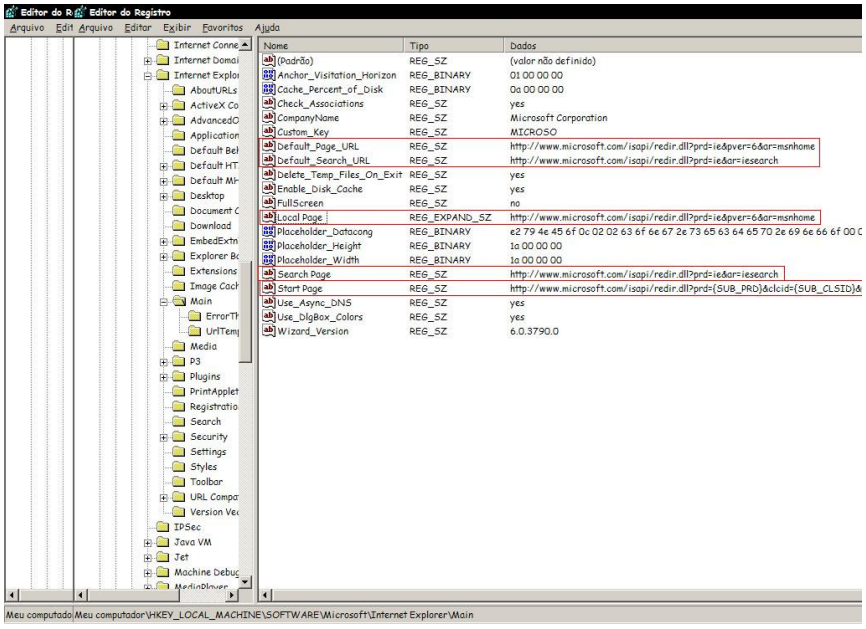


Figura 15. Configuração padrão do Internet Explorer no registro
Fonte: MICROSOFT (2006)

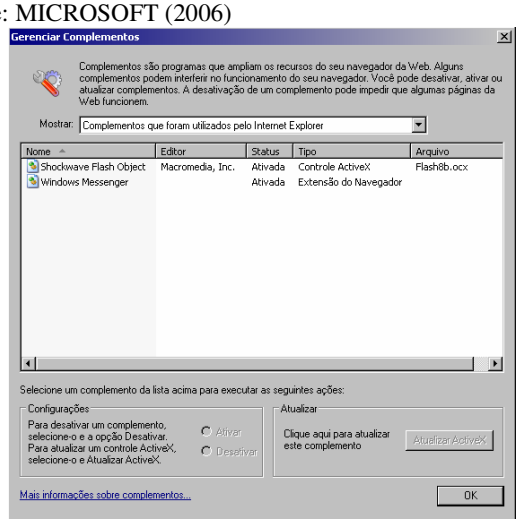


Figura 16. Complementos do Internet Explorer
Fonte: MICROSOFT (2006)

---

[31] Complementos: Programas iniciados junto ao Internet Explorer.
[32] Windows Messenger: Software de mensagens instantâneas da Microsoft.
[33] Shockwave: Software para visualização de animações na Internet.

4.2 PRIMEIRO CASO: LOOPDOTCOM

Até o momento, não existia o risco de infecção no sistema e só aparecerão apenas se o usuário visitar *sites* não-confiáveis ou instalar *Softwares* desconhecidos.

Após a visita do *site* www.cracks.am[34], o computador portou-se de maneira estranha, aparecendo páginas na tela como exibido na Figura 17.

Figura 17. Pop-up instalado pelo spyware
Fonte: MICROSOFT (2006)

Arquivos desconhecidos foram encontrados no Windows XP na pasta Documents and Settings\Administrador\Dados dos aplicativos, como mostra a Figura 18, assim provavelmente havia um *Spyware* na máquina.

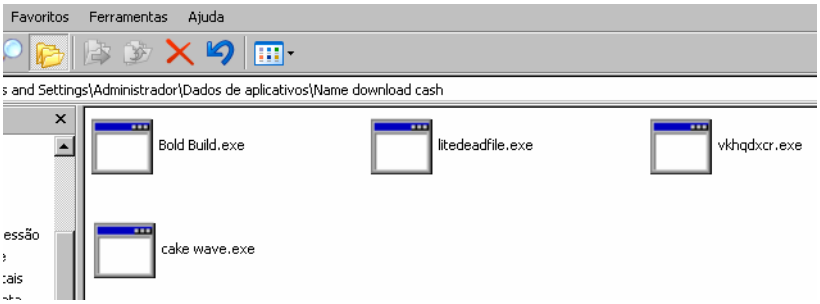


Figura 18. Arquivos encontrados no sistema
Fonte: MICROSOFT (2006)

[34] www.cracks.am: site cracker.

Para realmente ratificar possibilidade de infecção, foi usado o anti-*spyware* Spy Sweeper da empresa Webroot, que além de remover *spywares* e gravar *logs*, atua diretamente avisando ao usuário algum efeito estranho no computador, como novas entradas no registro, por exemplo.

Assim, foi obtida a seguinte informação como mostra a Figura 19 que realmente há arquivos infectados pelo loopdotcom, além de outros cookies. Um dos arquivos encontra-se em *Temporary* Internet Files, local destinado ao armazenamento de todo acervo que o usuário acessa na Internet, desde arquivos HTML até imagens, com grande chance de aparecer vírus e *spywares* nesta pasta.

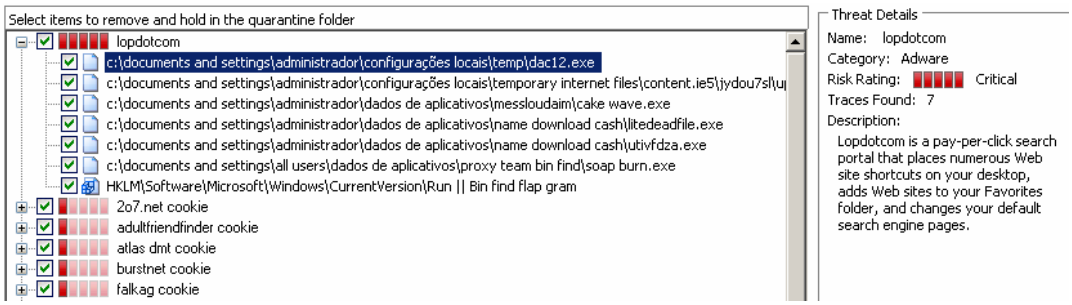


Figura 19. Detecção do lopdotcom pelo Spy Sweeper
Fonte: WEBROOT (2006)

O *spyware* encontrado é o *lopdotcom*, desenvolvido pela C2Media, um portal on-line com serviço *pay-per-click*[35], justamente porque usa o usuário para o portal obter lucros pelos cliques com os *pop-ups* instalados no sistema. Segundo a empresa *Webroot (2006)* tem risco crítico para os usuários, modificando as páginas iniciais e de busca do Internet Explorer e Mozilla[36], e gerando *pop-ups* de *sites* para buscas de mp3, *sites* pornográficos, entre outros.

[35] Pay-per-click: Serviço de publicidade onde o anunciante paga uma quantia de acordo com o número de acessos efetuados por usuários na Internet.
[36] Mozilla: Navegador de Internet com código livre e multi-plataforma.

O objetivo de tudo isto é gerar infinitas ligações com o sistema de busca do portal www.lop.com.br, e cada vez que o usuário visita o *site* ou outros vinculados, a C2MEdia ganha bonificações de *marketing*. Toda vez que um *site* for digitado incorretamente ou simplesmente quando aberto navegador, é acionada uma página com a publicidade do *spyware*, pois tanto página inicial quanto a de busca foram alteradas.

Variantes do *lopdotcom* usam nomes diferentes em inglês em seus arquivos, fazendo que toda infecção embaralhe estes nomes, enganando os usuários na busca de informações na Internet referente aquele arquivo.

Analisando o registro do Windows, três arquivos diferentes do *spyware* foram encontrados. Na chave Run do registro de nomes soap burn.exe e Bold Build.exe, além do BHO cake wave.exe que funciona junto ao Internet Explorer. Assim, toda vez que o usuário inicia o Windows ou o navegador, o processo referente ao *spyware* retorna a ativa, executando suas funções.

4.3 SEGUNDO CASO: LOOKTOME

Após navegar algum tempo na Internet, em *sites crackers*, uma nova infecção é encontrada no computador, se trata do *looktome*, um programa malicioso que monitora todos os *sites* visitados pelo usuário e envia essas informações para um servidor. Além disso, realiza o *download* de diversos outros componentes *spywares*.

Conforme mostra a Figura 20, note que a página inicial do navegador mudou para www.findthewebsiteyouneed.com, que se trata de um *adware* instalado junto ao *looktome*.

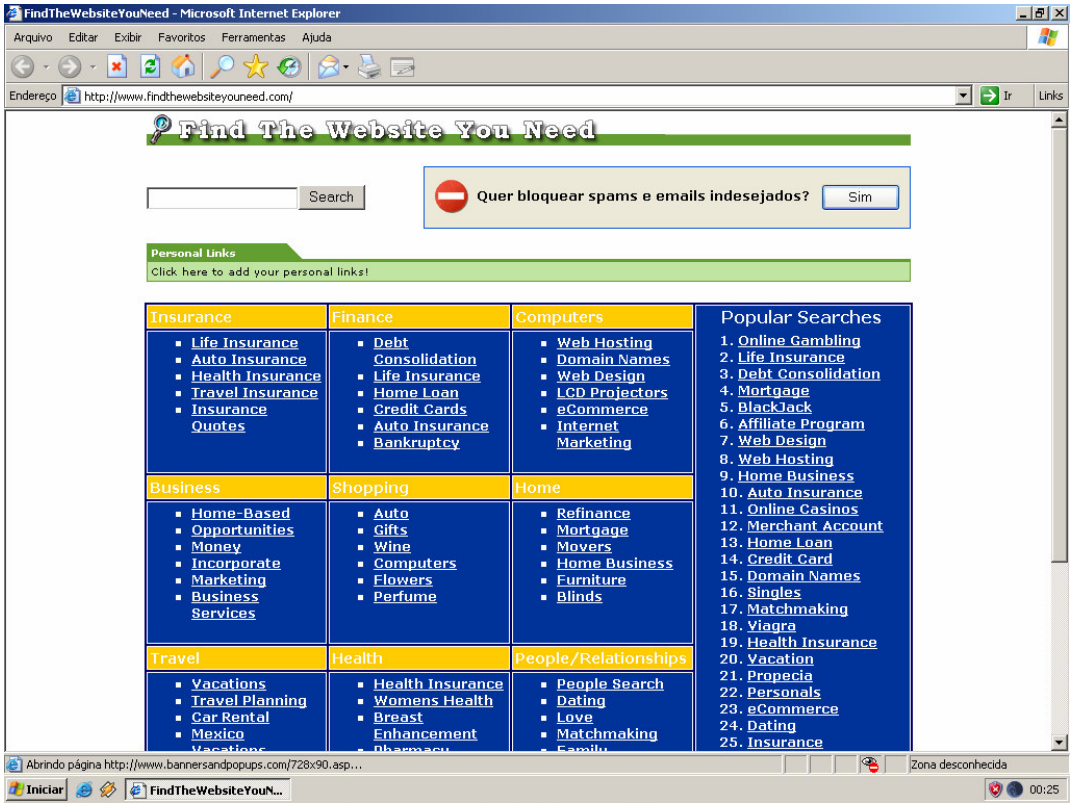


Figura 20. Página inicial modificada pelo *spyware*
Fonte: MICROSOFT (2006)

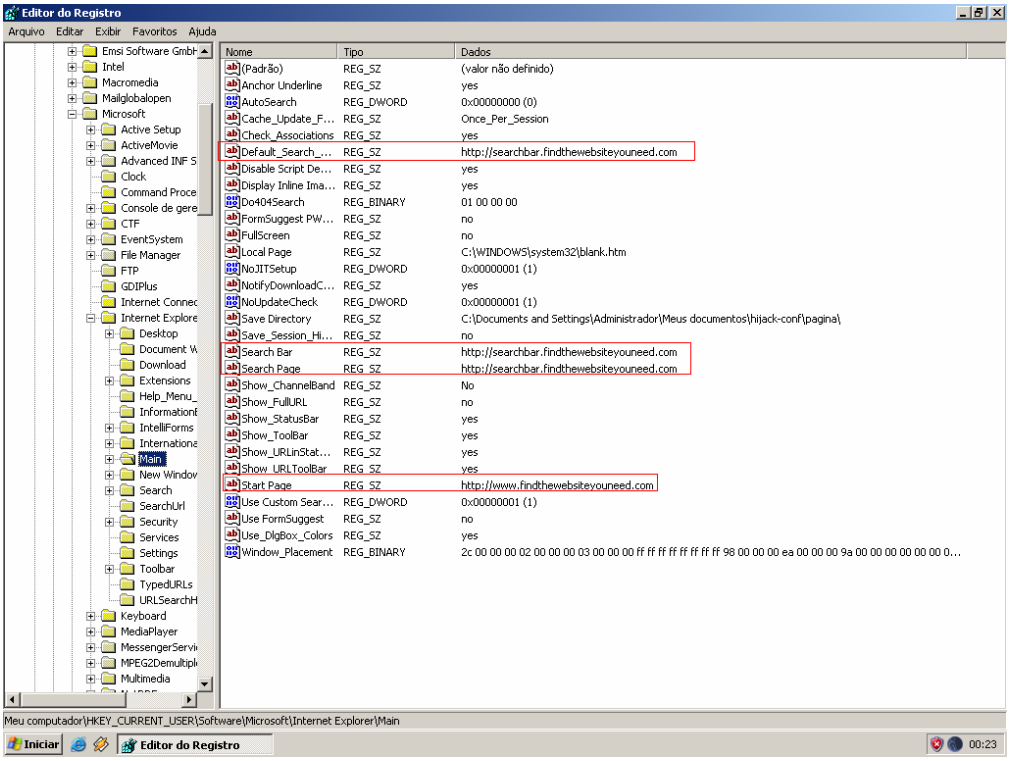


Figura 21. Registro do Windows mostrando as páginas modificadas
Fonte: MICROSOFT (2006)

A mesma informação é detalhado na Figura 21, só que por meio do registro do Windows, alterado pelo programa espião. Tanto a página inicial, como as de busca são modificadas para o *site* patrocinador do *spyware*.

Agora, usando o Software HijackThis 1.99.1 da empresa Merijn, um aplicativo para usuários avançados que detalha as informações mais importantes do registro onde os *spywares* atacam como as páginas principais do navegador, inicializações de processos do Windows, *Toolbar*, números do DNS, dentre outros.

Na Figura 22, nas seis primeiras linhas as informações referentes a configurações das páginas principais do navegador, todas elas, com o *site* www.findthewebsiteyouneed.com, logo abaixo, três arquivos são ativados na pasta Run do registro, são eles: defender19a.exe, keyboard19.exe e newname19.exe. Outro arquivo encontrado é o ctfmon.exe, um arquivo instalado junto ao Microsoft Office, que já era encontrado anteriormente as infecções.

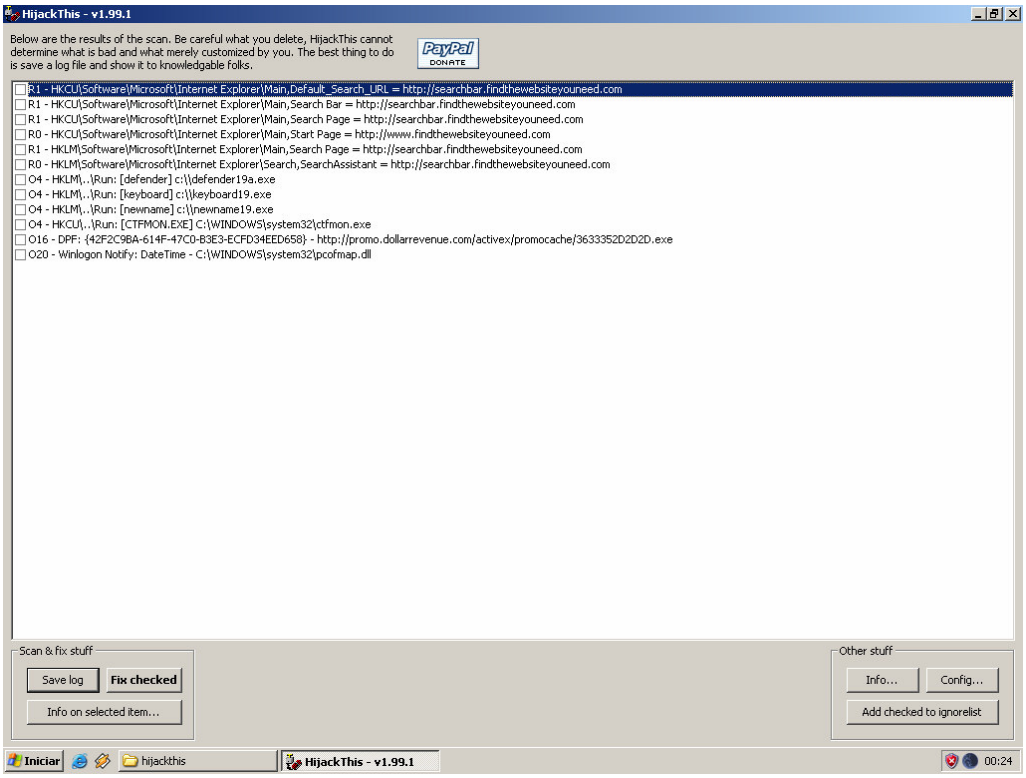


Figura 22. HijackThis detalhando o registro alterado por meio do looktome
Fonte: MERIJN (2006)

A próxima linha da Figura 22 remete o usuário a um site na Internet com um arquivo de extensão .EXE, onde provavelmente seja o programa de instalação do *spyware*, caso o usuário removê-lo do computador, cada vez que iniciar o Windows esta linha busque-o outra vez no meio externo ao computador e infecte novamente o sistema.

No final a DLL pcofmap na pasta System32 referindo-se a notificação do Winlogon, outra linha perigosa, pois este arquivo não existe em nenhum software da Microsoft e apareceu depois da infecção.

Já no *software* Spy Sweeper, muitos arquivos DLL são incluídos na pesquisa como mostra a Figura 23, muitos deles usados para serem executados junto ao navegador da Internet afim de publicidade das organizações financiadoras dos *spywares*, e a mesma informação do programa HijackThis, onde nos informa que os links principais do navegador foram alterados.

O arquivo localizado no HijackThis chamado pcofmap.dll surgi como um aviso de infecção, e apresenta a certeza que o arquivo é parte de um *spyware*. Por estes motivos, é recomendável a utilização de vários *softwares* anti-*spywares*.

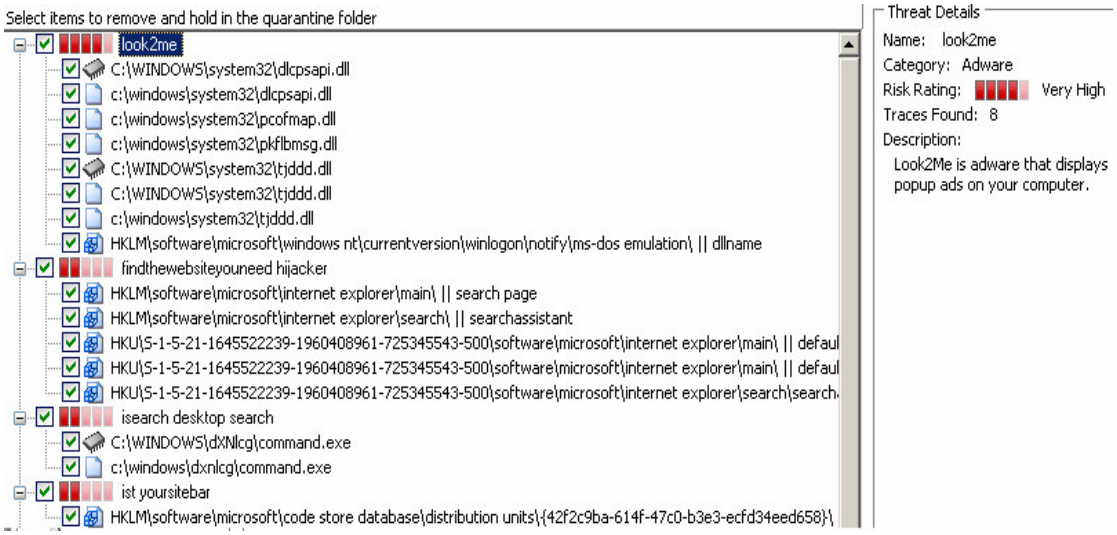


Figura 23. Detecção do looktome pelo Spy Sweeper
Fonte: WEBROOT (2006)

Quatro são os *spywares* encontrados na pesquisa, o principal deles: looktome, que ao conectar-se ao servidor www.a-d-w-a-r-e.com, instala novos componentes que são reconhecidos no anti-*spyware.*

O *Adware isearch desktop sea*rch é encontrado referindo-se ao arquivo command.exe, para enganar ao usuário que fica com medo de delatá-lo, pois este se encontra na pasta c:\Windows\dxnlcg\command.exe e o arquivo da *Microsoft* instalado junto ao *Windows* fica na pasta c:\Windows\system32\command.com, além de a extensão não ser a mesma, pois o *spyware* usa .EXE e a *Microsoft* usa .COM.

O *looktome* é um *spyware* tratado como risco muito alto segundo a *Webroot* (2006) e responsável por mostrar *pop-ups* na tela do computador, e monitorar os *sites* e submeter *logs* ao servidor responsável.

4.4 TERCEIRO CASO: GATOR

No terceiro estudo de casos, o *spyware* em questão é o Gator, o mais famoso de todos, e o primeiro em maior número de infecção conforme a Tabela 3.

O programa Gator (www.gator.com), que serve para armazenar senhas e informações pessoais no computador, pode alterar radicalmente o mercado de publicidade on-line: um novo recurso do software, que muitas vezes vem embutido em outros programas e é instalado sem que o usuário perceba, permite trocar os anúncios exibidos em páginas da Internet.

O sistema funciona da seguinte maneira: depois de monitorar os hábitos de navegação, o Gator seleciona anúncios que supostamente interessariam ao usuário e os sobrepõe à propaganda original dos *sites* visitados.

Os anúncios sobrepostos podem até mesmo promover o concorrente de uma empresa que pagou pelos anúncios originais.

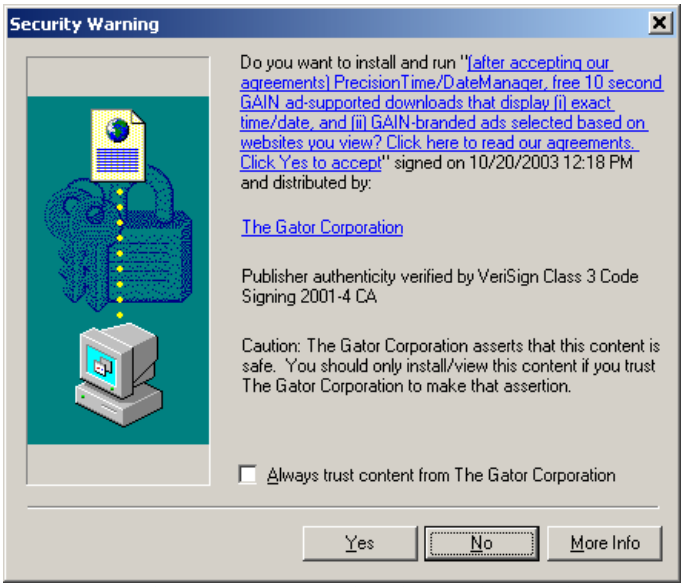


Figura 24. Aviso de Segurança avisando usuário sobre instalação do Gator
Fonte: MICROSOFT (2006)

Embora as faixas sobrepostas possam ser fechadas, revelando os anúncios originais, o novo recurso é visto com receio por publicitários e advogados dos EUA, que consideram exagerados e ilegais. A empresa responsável pelo "Gator" diz que a sobreposição de anúncios é normal.

Logo após aceitar a instalação do Gator, o Spy Sweeper que estava iniciado na bandeja do sistema já previu alterações no registro e informa um aviso ao usuário, conforme a Figura 25, mostrando três arquivos do Gator pedindo para escolher alguma das opções, entre remover a linha e aceitar.

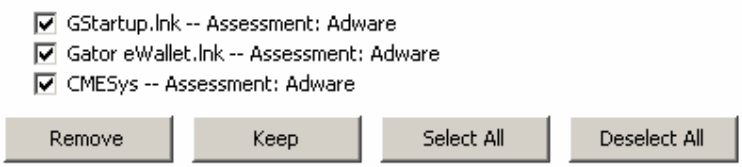


Figura 25. SpySweeper avisando sobre mudanças no registro
Fonte: WEBROOT (2006)

Depois de já infectado, usando o mesmo Spy Sweeper foi detectado muitos arquivos do *spyware* Gator, da empresa Gain Computers, como mostra as Figuras 26, 27 e 28.

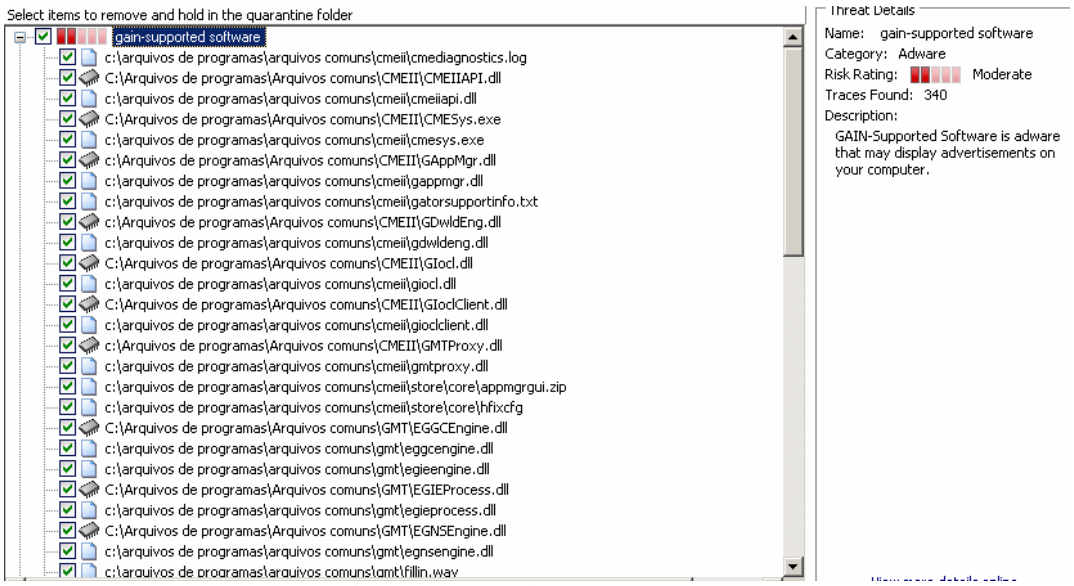


Figura 26. Detecção do Gain pelo Spy Sweeper Parte 1
Fonte: WEBROOT (2006)

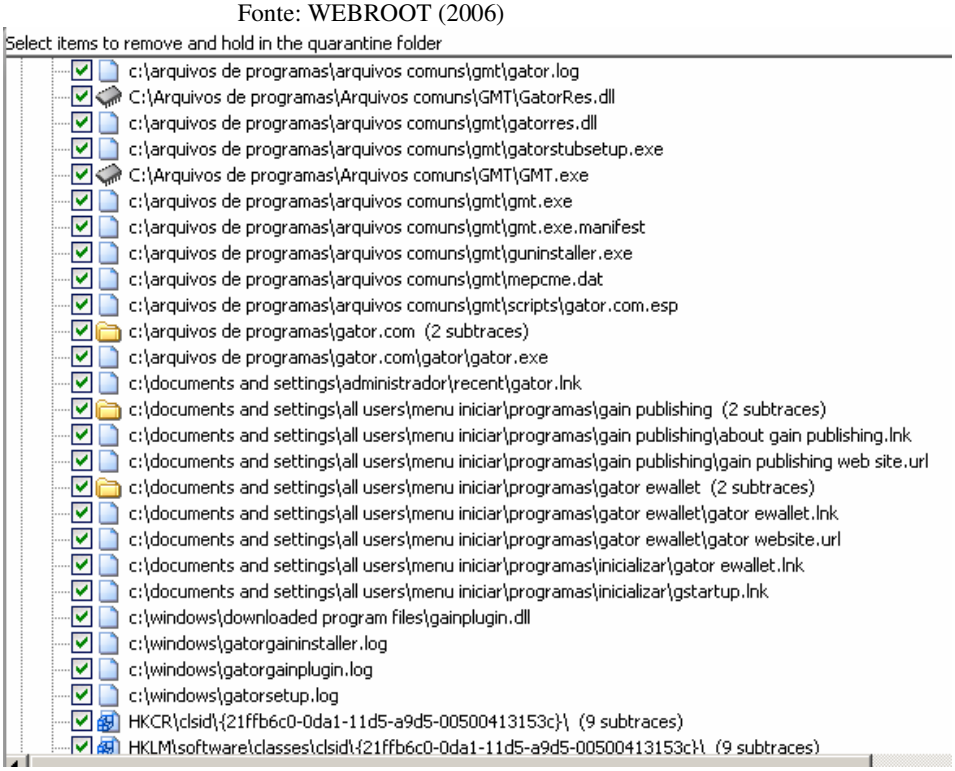


Figura 27. Detecção do Gain pelo Spy Sweeper Parte 2
Fonte: WEBROOT (2006)

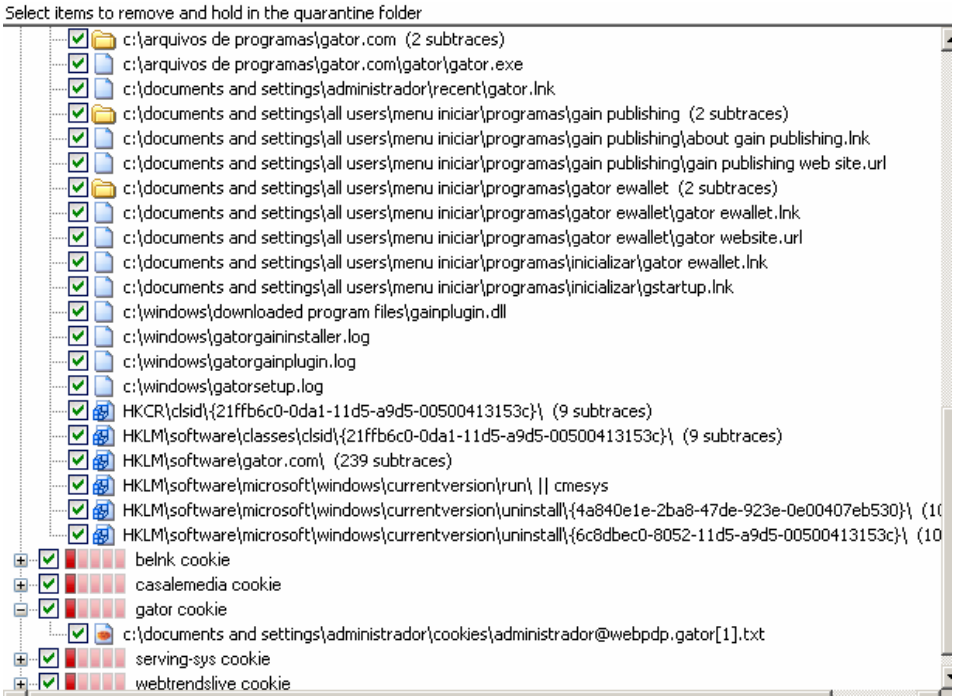


Figura 28. Detecção do Gain pelo Spy Sweeper Parte 3
Fonte: WEBROOT (2006)

Informações de outro software para manipulação do registro desenvolvido pela Emsi com o nome de a-squared HijackFree Analysis, mostra o arquivo CMESys, que encontra-se na pasta do sistema C:\Arquivos de programas\Arquivos comuns\CMEII \CMESys.exe, e é iniciado no registro HKLM\SOFTWARE\Microsoft\Windows \CurrentVersion\Run, envia informações a Gain Computers, e cria uma DLL com *Back Orifice* na porta UDP 1349, como mostra a Figura 29.

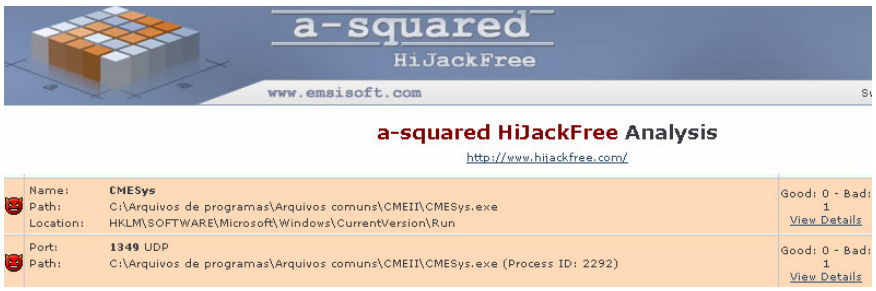


Figura 29. Detecção de arquivos do Gain pelo HijackFree
Fonte: EMSISOFT (2006)

4.5 QUARTO CASO: SPYSHERIFF

O Spysheriff é um falso anti-*spyware*, que faz a máquina parar de responder e avisar sobre a ocorrência de infecção na bandeja do sistema, como mostra a Figura 30, fazendo o usuário comprar a versão completa do programa e pagar licenças de uso.

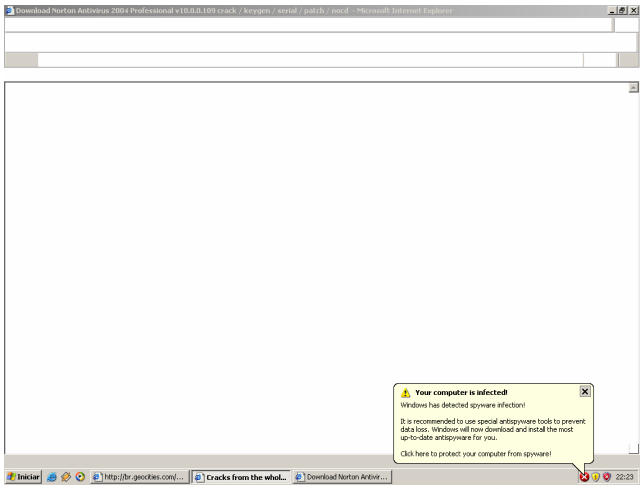


Figura 30. Sistema travado e aviso de infecção
Fonte: MICROSOFT (2006)

Com o travamento da máquina, com o objetivo de finalizar alguma tarefa, ao entrar no Gerenciador de Tarefas com Ctrl + Alt + Del, o sistema aponta a mensagem conforme a Figura 31.

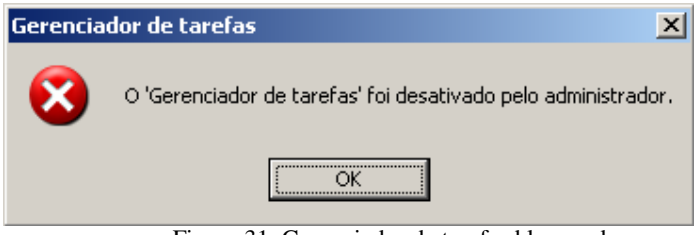


Figura 31. Gerenciador de tarefas bloqueado
Fonte: MICROSOFT (2006)

Com tudo isto, o que resta é verificar o sistema com o Spy Sweeper e observar os arquivos infectados, o software nos dá o resultado de que o *spyware* SpySheriff instalou na máquina, junto com alguns outros componentes como o vezbiz downloader, o 180 search assistant/zango, dentre outros, como mostra a Figura 32.

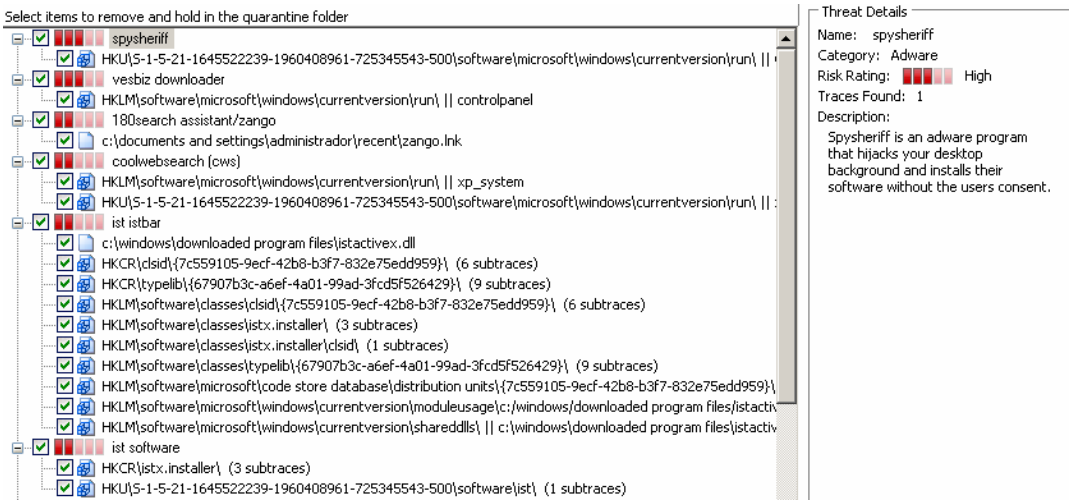


Figura 32. Detecção do spysheriff pelo Spy Sweeper
Fonte: WEBROOT (2006)

Para aumentar mais a confiança na remoção do *spyware*, então é executado o HijackThis a fim de detectar entradas no sistema para obstruir infecções no futuro, que mostrado na Figura 33, alguns arquivos estranhos apareceram, como o service.exe, e o objeto de *browser* winnuts.dll.

O arquivo winmuse.exe, e na raiz do sistema o winstall.exe. Localizado ainda uma instalação de classe que o *spyware* busca na Internet na página www.tbcode.com.br. E mais um arquivo para confundir o usuário encontrado, o cmd32.exe, de nome parecido com o cmd.exe da Microsoft.

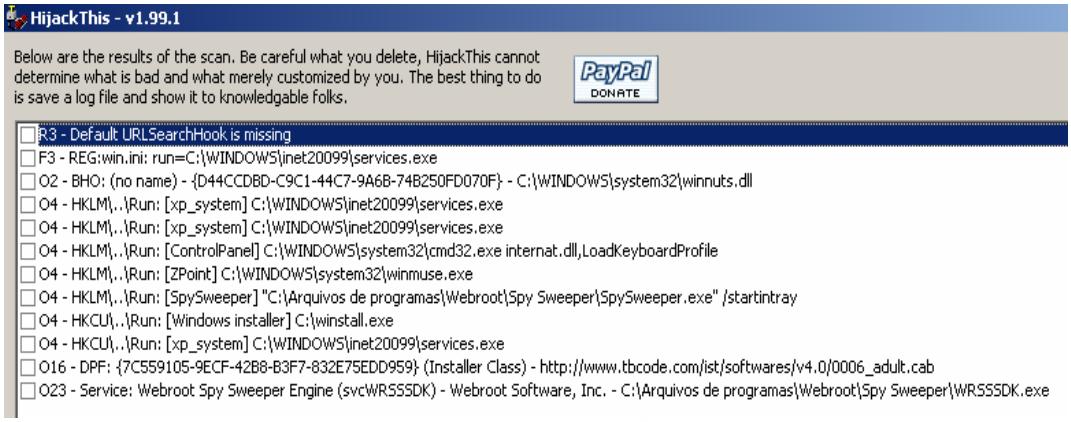


Figura 33. HijackThis detalhando o registro modificado por meio do spysheriff
Fonte: MERIJN (2006)

Para uma maior certeza dos arquivos infectados, foi executado agora o HijackFree que informa, conforme a Figura 34 que alguns arquivos estão com total desconfiança, inclusive o cmd32.exe, com o nome de Painel de Controle, e apontando mais uma DLL, com o nome de internat. Em amarelo, dois arquivos service.exe que o software pede atenção.

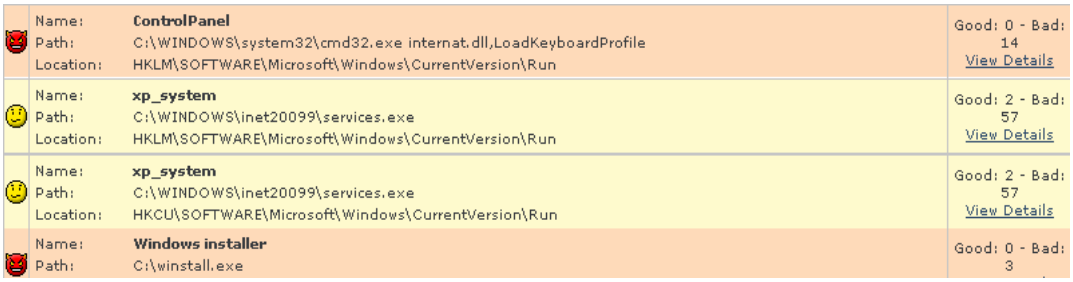


Figura 34. Detecção de arquivos do Gain pelo HijackFree
Fonte: EMSISOFT (2006)

Depois que o Spy Sweeper removeu os arquivos que encontrou, outro software anti-*spyware* foi utilizado, o AD-aware SE Personal Edition 1.06 (Figura 35) desenvolvido pela Lavasoft, e este removeu mais alguns arquivos como z15.exe, z16.exe, zlbw.dll, taskdir.dll (arquivo que muitos podem se confundir com o taskdir.exe da Microsoft), todos da pasta system32 do diretório c:\windows).

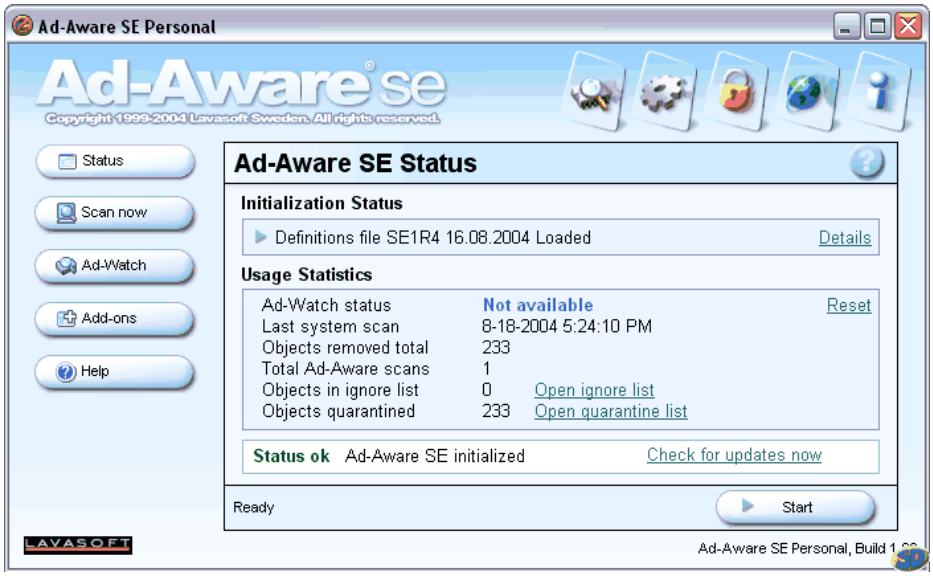


Figura 35. Software Ad-Aware
Fonte: LAVASOFT (2006)

Muitos arquivos encontravam-se no Windows depois da remoção pelo Spy Sweeper e do Ad-Aware, como os arquivos z12.exe, z11.exe, z14.exe, dentre outros, na pasta c:\windows\system32.

Depois de todo este procedimento, é executado o HijackThis novamente, e encontrado arquivos suspeitos como mostra na Figura 36, e excluída as linhas do registro no qual fazem referência aos *spywares*.

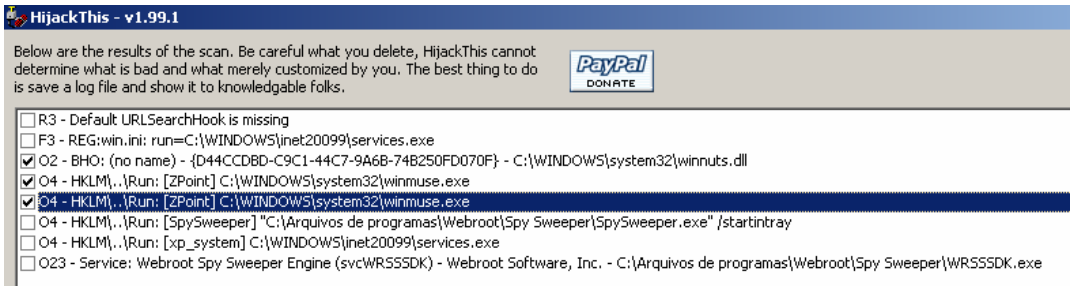


Figura 36. HijackThis detalhando o registro modificado após da 1ª. remoção
Fonte: MERIJN (2006)

O sistema é reiniciado e, logo iniciado em Modo de Segurança para executar o Spy Sweeper, que encontra mais uma linha de registro executando um arquivo infectado na pasta Run, conforme a Figura 37.

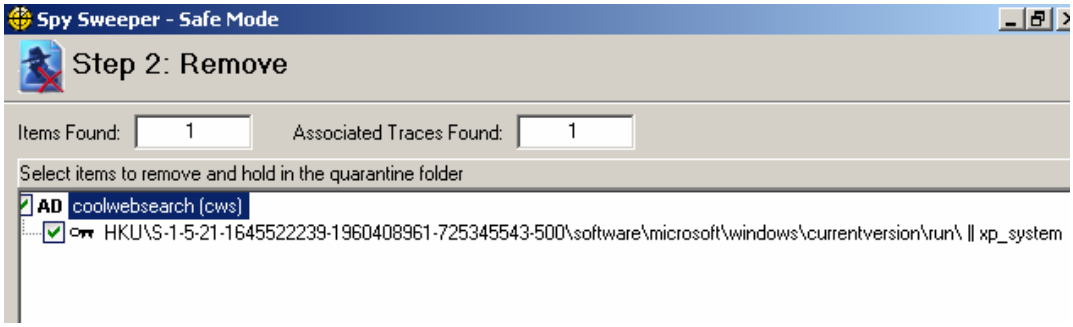


Figura 37. Linha de registro detectando arquivo na inicialização
Fonte: WEBROOT (2006)

Então, executando o HijackThis novamente, e informado na tela que já não existe mais nenhum arquivo infectado nos principais campos de registro do Windows, apenas o software Spy Sweeper sendo executado junto ao Windows.

Logo após todo este procedimento, o sistema ficou normal e não possui nenhuma infecção conhecida pelos anti-*spywares*.

4.6 QUINTO CASO: INFECÇÕES DIVERSAS

Modificações no computador sem que o usuário as faça, sempre são indícios de *spywares*, e neste caso, barras de ferramentas instaladas no navegador Internet Explorer e a troca da página inicial como mostrado na Figura 38, além de ícones na bandeja de entrada do Windows como mostra a Figura 39.

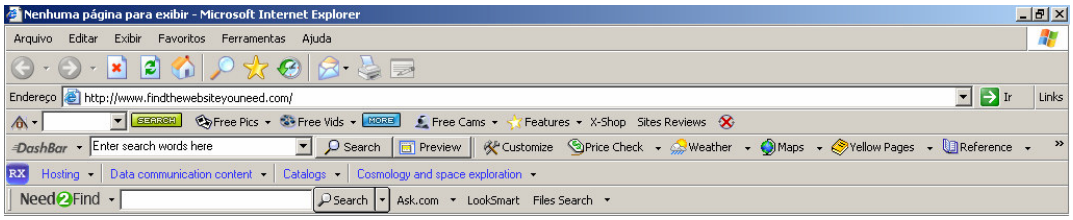


Figura 38. Barras de ferramentas inseridas e página inicial alterada
Fonte: MICROSOFT (2006)

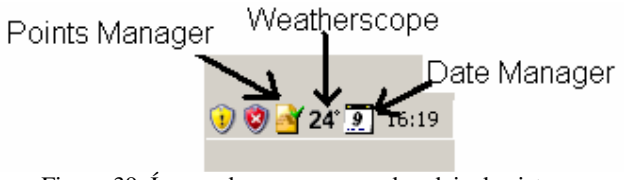


Figura 39. Ícones dos *spywares* na bandeja do sistema
Fonte: MICROSOFT (2006)

Um outro item importante para verificar a existência de *spywares* é o gerenciador de complementos do Internet Explorer, como mostra a Figura 40, ele informa todos os itens, botões, *toolbar*, e outros arquivos do navegador.

A barras de ferramentas como o DashBar, ISTbar e RXToolbar estão ativas, além de objetos auxiliares responsáveis por gerar publicidade na tela do computador do usuário.

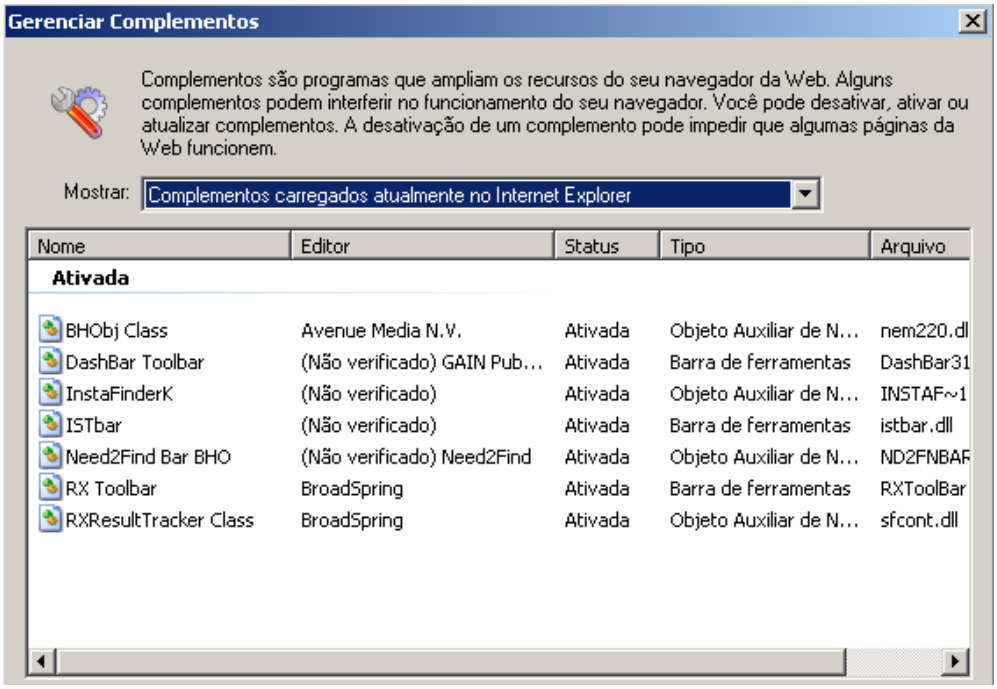


Figura 40. Complementos carregados no Internet Explorer
Fonte: MICROSOFT (2006)

Assim, faz-se necessário o uso dos softwares anti-*spyware*s para análise e remoção das infecções com execução do Spy Sweeper, logo na sua execução surgem avisos de mudanças no registro como mostra a Figura 41.

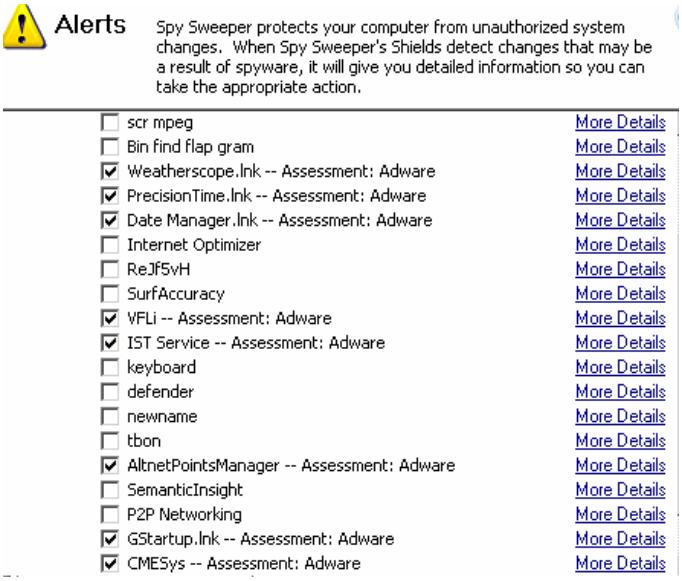


Figura 41. Aviso do Spy Sweeper de linhas inseridas no registro
Fonte: WEBROOT (2006)

Arquivos como o Weatherscope, PrecisionTime e Date Manager da empresa Gain Publishing, e outros serviços são acusados como *spywares*.

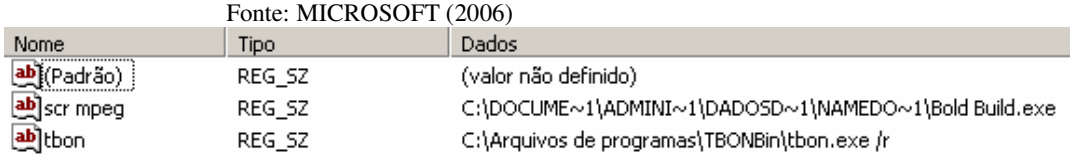
O *log* gravado pelo programa Spy Sweeper no Apêndice A, informa todos os *spyware*s instalados na máquina, catalogado através de um banco de dados que é atualizado semanalmente pela empresa responsável pelo software.

No Apêndice A, após iniciar o teste na memória, o software anti-*spyware* detecta os processos infectados, posteriormente começa o teste no registro, procurando as entradas modificadas pelos *spywares*. Depois, o Spy Sweeper começa a encontrar os *cookies* do sistema e depois os arquivos infectados.

Quando termina a primeira fase do processo, é catalogado tudo o que foi encontrado, inicia-se o processo de exclusão (alguns arquivos, como estão na memória, serão apenas excluídos após o reinício do sistema) e por fim os arquivos ficarão em Quarentena[37].

Nome	Tipo	Dados
(Padrão)	REG_SZ	(valor não definido)
AltnetPointsMana...	REG_SZ	C:\Program Files\Altnet\Points Manager\Points Manager.exe -s
Bin find flap gram	REG_SZ	C:\Documents and Settings\All Users\Dados de aplicativos\proxy team bin find\Face view.exe
defender	REG_SZ	C:\\defender25.exe
Internet Optimizer	REG_SZ	"C:\Program Files\Internet Optimizer\optimize.exe"
IST Service	REG_SZ	C:\Arquivos de programas\ISTsvc\istsvc.exe
keyboard	REG_SZ	C:\\keyboard25.exe
newname	REG_SZ	C:\\newname25.exe
P2P Networking	REG_SZ	C:\WINDOWS\system32\P2P Networking\P2P Networking.exe /AUTOSTART
ReJf5vH	REG_SZ	C:\WINDOWS\ojponyb.exe
SemanticInsight	REG_SZ	C:\Arquivos de programas\RXToolBar\Semantic Insight\SemanticInsight.exe
SpySweeper	REG_SZ	"C:\Arquivos de programas\Webroot\Spy Sweeper\SpySweeper.exe" /startintray
SurfAccuracy	REG_SZ	C:\Arquivos de programas\SurfAccuracy\SAcc.exe
Trickler	REG_SZ	"c:\windows\temp\bic_gatordm.exe"
VFLi	REG_SZ	C:\WINDOWS\nsyrfx.exe

Figura 42. Pasta Run no registro HKEY_LOCAL_MACHINE com infecções
Fonte: MICROSOFT (2006)



Nome	Tipo	Dados
(Padrão)	REG_SZ	(valor não definido)
scr mpeg	REG_SZ	C:\DOCUME~1\ADMINI~1\DADOSD~1\NAMEDO~1\Bold Build.exe
tbon	REG_SZ	C:\Arquivos de programas\TBONBin\tbon.exe /r

Figura 43. Pasta Run no registro HKEY_CURRENT_USERS com infecções
Fonte: MICROSOFT (2006)

[37] Quarentena: Período de Quarenta dias no qual o programa não deixará executar os arquivos.

Nas Figuras 42 e 43, a pasta *Run* das chaves de registro HKEY_LOCAL_MACHINE e HKEY_CURRENT_USER, detalham todas inicializações presentes no Sistema Operacional, estes muito parecidos com a da Figura 45, como o caso do RXToolBar, o Gator, e o ISTTolbar, e os arquivos newname, defender e keyboard.

No mesmo exemplo, Points Manager.exe refere-se ao *spyware* TopSearch, da empresa Altnet, é instalado junto ao software *Kazaa*, e gera propagandas aos seus usuários. Os arquivos face view.exe, e Bold Build.exe são responsáveis pelo *spyware* Lopdotcom, já detalhado no desenvolvimento do trabalho. Assim como os arquivos defender25.exe, keyboard25.exe e newname25.exe chamado de Looktome, que no outro caso, ao invés do final 25 nos arquivos, foi instalado no sistema como 19, fazendo com que os usuários confundam-se na busca de informações na Internet.

O Internet Optimizer, apontando o arquivo optimize.exe, outro *spyware* com *links pop-up* periodicamente na tela do computador, e que se torna a página de busca principal do navegador.

O IST Service, como o arquivo istsvc.exe é uma barra de ferramentas instalado por meio de controles ActiveX em *sites* de afiliados ao sistema. Criado por Integrated Search Technologies/CDT Inc, cria botões rápidos no navegador para *sites* pornográficos, e segundo o portal SpywareGuide (2006) além da barra de ferramentas, o *spyware* mostra propagandas em *pop-ups* e modifica as configurações do navegador.

P2P networking.exe é responsável por compartilhamento de arquivos na Internet em serviços como Imesh, Kazaa, e não tem perigo de infecção, assim como o arquivo SpySweeper.exe do próprio anti-*spyware* que inicia ao Windows para proteção.

Os arquivos nsyrfx.exe e ojponyb.exe não foram encontrados em nenhuma referência, e por isso, devem ser removidos junto com a linha de registro, pois muitos

*spyware*s embaralham os nomes dos arquivos em letras estranhas para dificultar a remoção.

SemanticInsight.exe, um BHO responsável pela execução da barra de ferramentas RXToolbar, outro *spyware* responsável por publicidade, além de criar *logs* de páginas visitadas pelo usuário para enviar ao servidor responsável. O arquivo SAcc.exe da empresa Surf Accuracy, tem a mesma função de enviar relatórios de *sites* visitados, para ser fonte de propaganda para o próprio usuário, que receberá apenas a área de seu interesse.

Outro arquivo, o bic_gatordm.exe, da empresa Gator, já relatado, é recorde em infecções no mundo todo, e sempre está fazendo aprimoramentos para novas versões. A Gator disponibiliza vários *sofwares* em seu *site*, apenas com a propósito de capturar informações dos usuários.

No *site* www.gainpublishing.com, *freewares* de todos os tipos, como por exemplo, o Date Manager que apenas informa a data na bandeja de sistema do Windows, ou o Precision Time, que efetua conexões na Internet para acertar o relógio do sistema.

O mais famoso de todos os softwares Gain, o Gator eWallet guarda informações de *login* e senhas do usuário para nunca serem perdidos. E até um *freeware* de previsão de tempo, o Weatherscope, que cria um ícone na bandeja de sistema para informar o tempo em qualquer cidade do mundo no dia atual, e a previsão dos próximos três dias.

Detalhado na chave HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Run o tbon.exe, responsável pelo *spyware* BestOffers, que no próprio nome já diz Melhor Oferta, outro que faz publicidade por meio de *pop-ups* para o comércio eletrônico.

O sistema descrito está repleto de *spywares* causando lentidão e não é confiável ao usuário fornecer informações pessoais em *sites* com este panorama, e buscar o mais rápido *softwares* que possam remover as infecções.

Para compreender melhor o que acontece, *logs* do software HijackThis resultam informações das entradas de registro no quais os *spywares* infectam e manipulam o sistema para seu controle. Toda informação gerada pelo programa encontra-se no Apêndice B.

Na Tabela 5, todos os tipos de itens de registro que podem ser catalogados pelo software HijackThis, alguns encontrados neste estudo de caso, como barra de ferramentas, BHO e mudanças nas configurações do navegador.

Tabela 5. Tabela do HijackThis

Código	
R0, R1, R2 e R3	Página Inicial e de busca do Internet Explorer
F0, F1	Programas auto executáveis
N1,N2,N3,N4	Página Inicial e de busca do Netscape/Mozilla
O1	Redirecionamento dos arquivos de hosts
O2	Browser Helper Object
O3	Barra de ferramentas do navegador
O4	Programas auto executáveis através do registro
O5	Ícones não visíveis no IE
O6	Opções restritas pelo administrador
O7	Acesso restrito do registro pelo administrador
O8	Itens extra do navegador
O9	Botões extras do navegador
O10	Winsock hijacker
O11	Grupo extra nas opções avançadas do IE
O12	Plugins do IE
O13	Prefixo padrão do hijack do IE
O14	Opção de resetar padrões do hijack
O15	*Site* não confiável
O16	Objetos ActiveX
O17	Domínios do hijacker lop.com
O18	Protocolos extras e hijackers
O19	Estilo do usuário
O20	DLL auto executáveis
O21	ShellService auto executáveis
O22	Tarefas executáveis
O23	Serviços do Windows NT

Fonte: MERIJN (2006)

O *log* do Apêndice B detalha o Sistema Operacional instalado na máquina: Windows XP SP2, o navegador Internet Explorer 6.0 SP2, todos os processos do sistema, inclusive do Windows NT, e programas e arquivos DLL iniciados, além de outros.

4.7 RESULTADOS OBTIDOS

Após o quinto estudo de caso, verifica-se que *spywares* geralmente agem de forma semelhante ao atacarem o sistema, gerando arquivos executáveis na inicialização do Windows e do navegador, e caso o usuário remover alguns arquivos, outros deles atuam na reinstalação do programa espião.

Quanto um sistema é encontrado infectado, é recomendável uma ampla análise do cenário, utilizar *softwares* para verificar o registro como o HijackThis, e programas anti-*spyware* para a remoção e combate, deixando os arquivos causadores da infecção totalmente isolados para a não execução dos mesmos, e o sistema livre dos *spywares*.

Para o combate dos *spywares* enquanto não há um *software* eficiente, é aconselhável algumas recomendações:

- Cuidar no acesso a sites deconhecidos;
- Não abrir e-mails de estranhos ou que possuem desconfiança;
- Instalar um anti-spyware confiável;
- Atualizar Sistema Operaciona, anti-vírus e anti-*spyware* frequentemente;
- Ler políticas de privacidade ao utilizar serviços na Internet;

Para as empresas, uma forma de amenizar a quantidade de arquivos maliciosos na rede de uma organização é a instalação de um servidor *proxy.* Este faz o controle no acesso dos usuários a Internet, como por exemplo, os *sites* permitidos, bloqueio dos programas usados para *download* de músicas, e liberação ao enviar e receber *e-mail*.

Com o projeto desenvolvido, foi possível verificar as formas de um spyware contaminar o sistema, que são:

- Através de programas *freewares* com *spywares* embutidos;
- Na Internet por meio de sites que instalam controles ActiveX;
- Por *bugs* do sistema e outros softwares.

O objetivo deste trabalho na análise das alterações no Sistema Operacional Microsoft Windows XP provocadas por *spywares* obtiveram resultados satisfatórios. O estudo amplo destes *softwares* auxiliou para compreender seu funcionamento e suas conseqüências no momento em que atacam o sistema. Além disto, após as informações dos anti-*spywares* e programas para análise de registro, todos os *spywares* dos cinco casos foram removidos com sucesso.

Logo, a pesquisa dos cinco estudos de casos com toda a documentação e demonstração das infecções, foi essencial para verificar as alterações tanto no ambiente gráfico quanto nas linhas de registro do Windows.

Esta documentação e as demonstrações feitas darão apoio aos usuários, técnicos de informática, administradores de redes e programadores, quando estes precisarem de informações dos *spywares* em suas atividades.

CONCLUSÃO

Com base neste estudo, é possível afirmar que os *spywares* são *softwares* fantasmas, no qual se instalam por meio de *bugs* do sistema e da falta de conhecimento do usuário. Pouco do assunto foi encontrado tanto em livros quanto na Internet, porém com o auxílio de um computador e alguns softwares, a análise das infecções de *spywares* teve um amplo resultado.

No decorrer deste trabalho foram alcançados os objetivos no conhecimento dos spywares, mostrando seu funcionamento, suas conseqüências e análises de registro para combate e remoção dos arquivos maliciosos.

Diferentes dos vírus, que apresentavam como finalidade interromper serviços nas organizações e *sites* da Internet, os *softwares* espiões têm a intenção de deixar os sistemas funcionando sem suspeitas para capturar informações confidenciais, diminuindo a privacidade das pessoas e organizações.

Com a análise do Sistema Operacional Windows XP, tanto no ambiente gráfico, quanto em *logs* do registro, foi possível verificar os meios de infecção e onde se alojam os *spywares* após a instalação. Um *sniffer* pode ser usado para controlar as entradas e saídas do computador local para a Internet em trabalhos futuros, a fim de verificar as informações que os *spywares* coletam. Este trabalho colaborará para que programadores e administradores de redes continuem trabalhando a favor da segurança, e juntos desenvolverem softwares mais completos, para a prevenção dos *spywares* antes mesmo de atacarem o sistema.

REFERÊNCIAS

ACTIVITY LOGGER, Disponível em: < http://www.softactivity.com/> Acesso em: 12 nov. 2005.

ANCHIESCHI, Olavo José Gomes. **Segurança Total:** Protegendo-se contra os hackers. São Paulo: Makron Books, 2000

CARDOZO, Eleri; MAGALHÃES, Maurício F. **Indrodução aos Sistemas Operacionais.** São Paulo: 2002.

CERT.Br -- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, Disponível em: <http://www.cert.br/> Acesso em: 22 nov. 2005.

CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. Disponível em <http://www.planalto.gov.br/> Acesso em 10 fev. 2006.

CRACKS.AM. Disponível em: <http://www.cracks.am/> Acesso em: 20 nov. 2005.

DIAMONDCS. Disponível em: <http://www .diamondcs.com.au/> Acesso em: 10 nov. 2005.

EARTHLINK. EARTHLINK AND WEBROOT TRACK THE GROWTH OF SPYWARE. EarthLink Press Roam Atlanta, 15 abr. 2004. Disponível em: <http://www.earthlink.net/about/press/pr_spyAudit/> Acesso em: 08 set. 2005.

EMSISOFT HIJACKFREE, Disponível em: < http://www.emsisoft.com/> Acesso em: 01 fev. 2006.

ERBSCHLOE, Michael. **Trojans, Worms and Spywares:** A computes Security Professional's Guide to Malicious Code. Washington: Butterworth-Heinemann, 2004.

FEDERAL TRADE COMMISSION. Disponível em: <http://www.ftc.gov/> Acesso em 1 out. 2005.

FEISTEIN, Ken. **Faça de Tudo para Combater Spam, Vírus, Pop-up & Spyware.** Rio de Janeiro: Altas Book, 2005.

FERNANDES, Carlos Henrique; FILHO, Fernando Mario de O. A Privacidade na Sociedade da Informação, 2003.
Disponível em: < http://www.linux.ime.usp.br/> Acesso em 10 mar. 2006.

GAERTNER, Adriana; DA SILVA, Helena Pereira. Privacidade da informação na Internet: Ausência de normalização, 2005. Disponível em: < http://dici.ibict.br> Acesso em 10 mar. 2006.

GREGORY, Peter; Michael, A. Simon. **Blocking Spam & Spyware for dummies.** 1 ed. Indianapolis: Wiley Publishing, Inc, 2005.

HUNTER, Laura E. **Stopping Spyware.** Boston: Addison Wesley, 2005.

IQNET. **Selo GoodPriv@cy**. Disponível em <http://www.iqnet-certification.com/> Acesso em 20 mar. 2006.

KÖCHE, José Carlos. **Fundamentos de Metodologia Científica.** 17 ed. Petrópolis: Vozes, 1997.

KOKOREVA, Olga. **Windows XP Registry**. A-List Publishing, 2002.

LAVASOFT AD-AWARE, Disponível em: <http://www.lavasoft.com/> Acesso em: 10 nov. 2005.

LAUFER, Rafael P. et al. **Negação de serviços: ataques e contramedidas.** Rio de Janeiro. Disponível em <http://www.gta.ufrj.br/> Acesso em: 10 out. 2005.

MERIJN HIJACKTHIS, Disponível em: < http://www.merijn.org/> Acesso em: 01 fev. 2006.

METZ, Cade. *Spy Stoppers.* **Pc Magazine**, New York, v.1, p.79-94, mar.2004.

MICROSOFT, Disponível em: <http://www.microsoft.com/> Acesso em: 20 set. 2006.

ONU. **Declaração dos Direitos Humanos.** Disponível em < http://www.onu-brasil.org.br/> Acesso em 10 fev. 2006.

PRIVACILLA.ORG. Disponível em: <http://www.privacilla.org/> Acesso em 02 fev. 2006.

PROCESSLIBRARY. Disponível em: <http://www.processlibrary.com/> Acesso em: 20 out. 2005.

SEGURANÇA MÁXIMA. Tradução de Edson Furmankiewizs e Joana Figueiredo. Rio de Janeiro: Campus, 2000. 826p. Tradução de: *Maximum Security.*

WEBROOT SPY SWEEPER, Disponível em: <http://www.webroot.com/> Acesso em: 01 fev. 2006.

SPYWAREGUIDE. Disponível em: <http://www.spywareguide.com/> Acesso em: 10 jun. 2006.

SPYWAREINFO. Disponível em: <http://www.spywareinfo.com/> Acesso em: 25 jul. 2006.

SUPERDOWNLOADS, Disponível em: <http://www.superdownloads.com.br/> Acesso em: 10 set. 2006.

SYSINTERNALS, Disponível em: <http://www.sysinternals.com/> Acesso em 13 set. 2005.

TANENBAUM, Andrew S; WOODHULL, Albert S. **Sistemas Operacionais:** Projeto e Implementação. 2 ed. Porto Alegre: Bookman, 2000.

TITTEL, Ed. Fighting *Spyware, Viruses and malware.* **Pc Magazine**, New York, v.1, p.1-349, dec.2004.

TORRES, Gabriel. **O Registro do Windows 9.x**. Rio de Janeiro, 1998.

WIKIPEDIA, Disponível em: <http://www.wikipedia.com/> Acesso em: 20 set. 2006.

ZELLER JR, Tom. ***Black Market in Credit Cards Thrives on Web. The New York Times, New York, 21 jun. 2005***. Section A, p.1.

APÊNDICE A - Logs do Software Spy Sweeper

****
16:40: | Start of Session, sexta-feira, 12 de maio de 2006 |
16:40: Spy Sweeper started
16:40: Sweep initiated using definitions version 556
16:47: Starting Memory Sweep
16:47: Found Adware: look2me
16:47: Detected running threat: C:\WINDOWS\system32\e402ledo1h0c.dll (ID = 163672)
16:48: Detected running threat: C:\WINDOWS\system32\awtiveds.dll (ID = 163672)
16:48: Memory Sweep Complete, Elapsed Time: 00:01:01
16:48: Starting Registry Sweep
16:48: Found Adware: altnet
16:48: HKCR\adm.adm.1\ (3 subtraces) (ID = 103441)
16:48: HKCR\adm.adm\ (5 subtraces) (ID = 103442)
16:48: HKCR\adm4.adm4.1\ (3 subtraces) (ID = 103443)
16:48: HKCR\adm4.adm4\ (3 subtraces) (ID = 103444)
16:48: HKCR\adm25.adm25.1\ (3 subtraces) (ID = 103445)
16:48: HKCR\adm25.adm25\ (3 subtraces) (ID = 103446)
16:48: HKCR\appid\adm.exe\ (1 subtraces) (ID = 103448)
16:48: HKCR\appid\altnet signing module.exe\ (1 subtraces) (ID = 103449)
16:48: HKCR\appid\{8b0fef15-54dc-49f5-8377-8172de975f75}\ (1 subtraces) (ID = 103453)
16:48: HKCR\appid\{99a8e2b2-3405-4c0d-9110-131c14caaf62}\ (1 subtraces) (ID = 103454)
16:48: HKCR\clsid\{1d3bce37-7834-4579-8169-e67681420a98}\ (12 subtraces) (ID = 103458)
16:48: HKCR\clsid\{3f4d4f88-0198-4921-b630-957f3eb814e0}\ (1 subtraces) (ID = 103460)
16:48: HKCR\clsid\{9bbcf06c-dcd7-495d-80df-cdd5399d0ff8}\ (11 subtraces) (ID = 103461)
16:48: HKCR\clsid\{3646c2bd-3554-49ca-8125-44deefb881de}\ (1 subtraces) (ID = 103462)
16:48: HKCR\clsid\{c15b7ea2-a360-43e8-a591-5faedc7c4e1d}\ (24 subtraces) (ID = 103466)
16:48: HKCR\clsid\{def37997-d9c9-4a4b-bf3c-88f99eaceec2}\ (12 subtraces) (ID = 103467)
16:48: HKCR\clsid\{e813099d-5529-47f4-9b37-4afafcb00a43}\ (4 subtraces) (ID = 103468)
16:48: HKCR\interface\{ad5bc1f0-72d8-44b3-8e3d-8e8fecce43fb}\ (5 subtraces) (ID = 103472)
16:48: HKCR\interface\{e813099d-5529-47f4-9b37-4afafcb00a43}\ (5 subtraces) (ID = 103474)
16:48: HKCR\signingmodule.signingmodule.1\ (3 subtraces) (ID = 103476)
16:48: HKCR\signingmodule.signingmodule\ (5 subtraces) (ID = 103478)
16:48: HKLM\software\altnet\ (29 subtraces) (ID = 103481)
16:48: HKLM\software\classes\adm.adm.1\ (3 subtraces) (ID = 103482)

16:48: HKLM\software\classes\adm.adm\ (5 subtraces) (ID = 103483)
16:48: HKLM\software\classes\adm4.adm4.1\ (3 subtraces) (ID = 103484)
16:48: HKLM\software\classes\adm4.adm4\ (3 subtraces) (ID = 103485)
16:48: HKLM\software\classes\adm25.adm25.1\ (3 subtraces) (ID = 103486)
16:48: HKLM\software\classes\adm25.adm25\ (3 subtraces) (ID = 103487)
16:48: HKLM\software\classes\appid\adm.exe\ (1 subtraces) (ID = 103488)
16:48: HKLM\software\classes\appid\altnet signing module.exe\ (1 subtraces) (ID = 103489)
16:48: HKLM\software\classes\appid\{8b0fef15-54dc-49f5-8377-8172de975f75}\ (1 subtraces) (ID = 103490)
16:48: HKLM\software\classes\appid\{99a8e2b2-3405-4c0d-9110-131c14caaf62}\ (1 subtraces) (ID = 103491)
16:48: HKLM\software\classes\clsid\{1d3bce37-7834-4579-8169-e67681420a98}\ (12 subtraces) (ID = 103492)
16:48: HKLM\software\classes\clsid\{9bbcf06c-dcd7-495d-80df-cdd5399d0ff8}\ (11 subtraces) (ID = 103493)
16:48: HKLM\software\classes\clsid\{c15b7ea2-a360-43e8-a591-5faedc7c4e1d}\ (24 subtraces) (ID = 103495)
16:48: HKLM\software\classes\signingmodule.signingmodule.1\ (3 subtraces) (ID = 103496)
16:48: HKLM\software\classes\signingmodule.signingmodule\ (5 subtraces) (ID = 103497)
16:48: HKLM\software\classes\typelib\{676f6d1d-c559-42a9-860b-27c1477b7179}\ (9 subtraces) (ID = 103502)
16:48: HKLM\software\classes\typelib\{5830698f-7fc0-40cd-a453-9a0cafdf3a64}\ (9 subtraces) (ID = 103503)
16:48: HKLM\software\classes\typelib\{bff4f684-677e-44f4-8c74-1d575c950e10}\ (9 subtraces) (ID = 103504)
16:48: HKLM\software\microsoft\windows\currentversion\run\ || altnetpointsmanager (ID = 103518)
16:48: HKLM\software\microsoft\windows\currentversion\uninstall\altnetdm\ (2 subtraces) (ID = 103531)
16:48: HKCR\typelib\{676f6d1d-c559-42a9-860b-27c1477b7179}\ (9 subtraces) (ID = 103535)
16:48: HKCR\typelib\{bff4f684-677e-44f4-8c74-1d575c950e10}\ (9 subtraces) (ID = 103536)
16:48: Found Adware: cws-aboutblank
16:48: HKCR\protocols\filter\text/html\ (2 subtraces) (ID = 114343)
16:48: HKLM\software\classes\protocols\filter\text/html\ (2 subtraces) (ID = 115907)
16:48: Found Adware: gain-supported software
16:48: HKCR\clsid\{21ffb6c0-0da1-11d5-a9d5-00500413153c}\ (9 subtraces) (ID = 126731)
16:48: HKCR\clsid\{cc90cda0-74a0-45b4-80ef-d89ca8c249b8}\ (11 subtraces) (ID = 126734)
16:48: HKCR\dashbartoolbar.searchscoutbandobj.1\ (3 subtraces) (ID = 126736)
16:48: HKCR\dashbartoolbar.searchscoutbandobj\ (5 subtraces) (ID = 126737)
16:48: HKCR\interface\{a2ba5e71-5be3-4007-ac48-157823fb63fb}\ (8 subtraces) (ID = 126746)
16:48: HKLM\software\classes\clsid\{21ffb6c0-0da1-11d5-a9d5-00500413153c}\ (9 subtraces) (ID = 126751)

16:48: HKLM\software\classes\clsid\{cc90cda0-74a0-45b4-80ef-d89ca8c249b8}\ (11 subtraces) (ID = 126752)
16:48: HKLM\software\classes\dashbartoolbar.searchscoutbandobj.1\ (3 subtraces) (ID = 126753)
16:48: HKLM\software\classes\dashbartoolbar.searchscoutbandobj\ (5 subtraces) (ID = 126754)
16:48: HKLM\software\classes\interface\{a2ba5e71-5be3-4007-ac48-157823fb63fb}\ (8 subtraces) (ID = 126755)
16:48: HKLM\software\classes\typelib\{8642d0f2-37cc-46b7-aa5b-399e6e68c626}\ (9 subtraces) (ID = 126759)
16:48: HKLM\software\microsoft\internet explorer\toolbar\ || {cc90cda0-74a0-45b4-80ef-d89ca8c249b8} (ID = 126761)
16:48: HKLM\software\microsoft\windows\currentversion\run\ || cmesys (ID = 126779)
16:48: HKLM\software\microsoft\windows\currentversion\uninstall\dashbar\ (3 subtraces) (ID = 126799)
16:48: HKLM\software\microsoft\windows\currentversion\uninstall\date manager\ (3 subtraces) (ID = 126800)
16:48: HKLM\software\microsoft\windows\currentversion\uninstall\precisiontime\ (3 subtraces) (ID = 126802)
16:48: HKLM\software\microsoft\windows\currentversion\uninstall\weatherscope\ (3 subtraces) (ID = 126803)
16:48: HKLM\software\microsoft\windows\currentversion\uninstall\{4a840e1e-2ba8-47de-923e-0e00407eb530}\ (10 subtraces) (ID = 126804)
16:48: HKCR\typelib\{8642d0f2-37cc-46b7-aa5b-399e6e68c626}\ (9 subtraces) (ID = 126812)
16:48: Found Adware: ist software
16:48: HKCR\clsid\{5f1abcdb-a875-46c1-8345-b72a4567e486}\ (14 subtraces) (ID = 127191)
16:48: Found Adware: instafinder
16:48: HKCR\clsid\{4e7bd74f-2b8d-469e-90f0-f66ab581a933}\ (6 subtraces) (ID = 128654)
16:48: HKLM\software\classes\clsid\{4e7bd74f-2b8d-469e-90f0-f66ab581a933}\ (6 subtraces) (ID = 128656)
16:48: HKLM\software\classes\instafink.instafink\ (3 subtraces) (ID = 128660)
16:48: HKLM\software\microsoft\windows\currentversion\uninstall\instafink\ (2 subtraces) (ID = 128664)
16:48: HKCR\instafink.instafink\ (3 subtraces) (ID = 128669)
16:48: Found Adware: internetoptimizer
16:48: HKCR\clsid\{00000010-6f7d-442c-93e3-4a4827c2e4c8}\ (11 subtraces) (ID = 128881)
16:48: HKLM\software\avenue media\ (27 subtraces) (ID = 128888)
16:48: HKLM\software\classes\clsid\{00000010-6f7d-442c-93e3-4a4827c2e4c8}\ (11 subtraces) (ID = 128892)
16:48: HKLM\software\microsoft\windows\currentversion\policies\ameopt\ (ID = 128912)
16:48: HKLM\software\microsoft\windows\currentversion\run\ || internet optimizer (ID = 128916)
16:48: HKLM\software\microsoft\windows\currentversion\uninstall\internet optimizer\ (3 subtraces) (ID = 128921)

16:48: HKLM\software\microsoft\windows\currentversion\uninstall\kapabout\ (2 subtraces) (ID = 128924)
16:48: HKLM\software\policies\avenue media\ (ID = 128929)
16:48: Found Adware: ist istbar
16:48: HKCR\interface\{dc065fa6-08f9-4c50-99dc-275d16cfc5bd}\ (8 subtraces) (ID = 129069)
16:48: HKCR\pugi.pugiobj.1\ (3 subtraces) (ID = 129074)
16:48: HKCR\pugi.pugiobj\ (5 subtraces) (ID = 129075)
16:48: HKLM\software\classes\interface\{dc065fa6-08f9-4c50-99dc-275d16cfc5bd}\ (8 subtraces) (ID = 129092)
16:48: HKLM\software\classes\pugi.pugiobj\ (5 subtraces) (ID = 129099)
16:48: HKLM\software\classes\typelib\{89a10d64-83bf-41a4-86a3-7aaf1f8f3d1b}\ (9 subtraces) (ID = 129102)
16:48: HKLM\software\istsvc\ (24 subtraces) (ID = 129111)
16:48: HKLM\software\microsoft\windows\currentversion\moduleusage\c:/windows/downloaded program files/istactivex.dll\ (2 subtraces) (ID = 129124)
16:48: HKLM\software\microsoft\windows\currentversion\run\ || ist service (ID = 129146)
16:48: HKLM\software\microsoft\windows\currentversion\shareddlls\ || c:\windows\downloaded program files\istactivex.dll (ID = 129174)
16:48: HKLM\software\microsoft\windows\currentversion\uninstall\istbaristbar\ (2 subtraces) (ID = 129182)
16:48: HKLM\software\microsoft\windows\currentversion\uninstall\istsvc\ (7 subtraces) (ID = 129183)
16:48: HKCR\typelib\{89a10d64-83bf-41a4-86a3-7aaf1f8f3d1b}\ (9 subtraces) (ID = 129188)
16:48: Found Adware: moneytree
16:48: HKCR\dyfuca_bh.bhobj.1\ (3 subtraces) (ID = 135175)
16:48: HKCR\dyfuca_bh.bhobj\ (5 subtraces) (ID = 135176)
16:48: HKLM\software\classes\dyfuca_bh.bhobj\ (5 subtraces) (ID = 135194)
16:48: HKLM\software\classes\typelib\{40b1d454-9ca4-43cc-86aa-cb175eac52fb}\ (9 subtraces) (ID = 135201)
16:48: HKLM\software\microsoft\windows\currentversion\uninstall\dyfuca\ (ID = 135214)
16:48: HKCR\typelib\{40b1d454-9ca4-43cc-86aa-cb175eac52fb}\ (9 subtraces) (ID = 135217)
16:48: Found Adware: rx toolbar
16:48: HKCR\rxtoolbar.tbinfo\ (5 subtraces) (ID = 140294)
16:48: HKCR\rxtoolbar.tbinfo.1\ (3 subtraces) (ID = 140295)
16:48: HKLM\software\classes\rxtoolbar.tbinfo.1\ (3 subtraces) (ID = 140296)
16:48: HKLM\software\classes\rxtoolbar.tbinfo\ (5 subtraces) (ID = 140297)
16:48: HKCR\clsid\{25d8bacf-3de2-4b48-ae22-d659b8d835b0}\ (11 subtraces) (ID = 140299)
16:48: HKCR\typelib\{66b20295-dc57-42b6-acdf-52d916e86464}\ (9 subtraces) (ID = 140300)
16:48: HKLM\software\classes\clsid\{25d8bacf-3de2-4b48-ae22-d659b8d835b0}\ (11 subtraces) (ID = 140302)
16:48: HKLM\software\classes\typelib\{66b20295-dc57-42b6-acdf-52d916e86464}\ (9 subtraces) (ID = 140303)

16:48: HKLM\software\microsoft\internet explorer\toolbar\ || {25d8bacf-3de2-4b48-ae22-d659b8d835b0} (ID = 140304)
16:48: HKLM\software\microsoft\windows\currentversion\uninstall\rxtoolbar\ (6 subtraces) (ID = 140305)
16:48: HKLM\software\classes\clsid\{5f1abcdb-a875-46c1-8345-b72a4567e486}\ (14 subtraces) (ID = 141834)
16:48: HKLM\software\microsoft\internet explorer\toolbar\ || {5f1abcdb-a875-46c1-8345-b72a4567e486} (ID = 141840)
16:48: HKCR\interface\{1c01d150-91a4-4de0-9bf8-a35d1bdf1001}\ (8 subtraces) (ID = 169495)
16:48: HKLM\software\classes\interface\{1c01d150-91a4-4de0-9bf8-a35d1bdf1001}\ (8 subtraces) (ID = 169496)
16:48: Found Adware: surf accuracy
16:48: HKLM\software\sacc\ (9 subtraces) (ID = 203068)
16:48: HKLM\software\microsoft\windows\currentversion\run\ || surfaccuracy (ID = 203069)
16:48: HKLM\software\microsoft\windows\currentversion\uninstall\sacc\ (7 subtraces) (ID = 203070)
16:48: HKLM\software\avenue media\internet optimizer\ (26 subtraces) (ID = 394594)
16:48: HKLM\software\gator.com\ (286 subtraces) (ID = 528933)
16:48: HKCR\rxresult.rxresultfilter\ (3 subtraces) (ID = 729537)
16:48: HKCR\rxresult.rxresultfilter\clsid\ (1 subtraces) (ID = 729539)
16:48: HKCR\rxresult.rxresultfilter.1\ (3 subtraces) (ID = 729541)
16:48: HKCR\rxresult.rxresultfilter.1\clsid\ (1 subtraces) (ID = 729543)
16:48: HKCR\rxresult.rxresulttracker\ (3 subtraces) (ID = 729545)
16:48: HKCR\rxresult.rxresulttracker\clsid\ (1 subtraces) (ID = 729547)
16:48: HKCR\rxresult.rxresulttracker.1\ (3 subtraces) (ID = 729549)
16:48: HKCR\rxresult.rxresulttracker.1\clsid\ (1 subtraces) (ID = 729551)
16:48: HKCR\clsid\{2ab289ae-4b90-4281-b2ae-1f4bb034b647}\ (10 subtraces) (ID = 729553)
16:48: HKCR\clsid\{59879fa4-4790-461c-a1cc-4ec4de4ca483}\ (8 subtraces) (ID = 729564)
16:48: HKCR\typelib\{05563f82-69a7-40a6-8670-153b635a7ef6}\ (9 subtraces) (ID = 729573)
16:48: HKLM\software\rxresults\ (4 subtraces) (ID = 729611)
16:48: HKLM\software\classes\rxresult.rxresultfilter\ (3 subtraces) (ID = 729616)
16:48: HKLM\software\classes\rxresult.rxresultfilter\clsid\ (1 subtraces) (ID = 729618)
16:48: HKLM\software\classes\rxresult.rxresultfilter.1\ (3 subtraces) (ID = 729620)
16:48: HKLM\software\classes\rxresult.rxresultfilter.1\clsid\ (1 subtraces) (ID = 729622)
16:48: HKLM\software\classes\rxresult.rxresulttracker\ (3 subtraces) (ID = 729624)
16:48: HKLM\software\classes\rxresult.rxresulttracker\clsid\ (1 subtraces) (ID = 729626)
16:48: HKLM\software\classes\rxresult.rxresulttracker.1\ (3 subtraces) (ID = 729628)
16:48: HKLM\software\classes\rxresult.rxresulttracker.1\clsid\ (1 subtraces) (ID = 729630)
16:48: HKLM\software\classes\clsid\{2ab289ae-4b90-4281-b2ae-1f4bb034b647}\ (10 subtraces) (ID = 729632)

16:48: HKLM\software\classes\clsid\{59879fa4-4790-461c-a1cc-4ec4de4ca483}\ (8 subtraces) (ID = 729643)
16:48: HKLM\software\classes\typelib\{05563f82-69a7-40a6-8670-153b635a7ef6}\ (9 subtraces) (ID = 729652)
16:48: Found System Monitor: active keylogger
16:48: HKU\S-1-5-21-1645522239-1960408961-725345543-500\software\winsoul\ (17 subtraces) (ID = 102578)
16:48: HKU\S-1-5-21-1645522239-1960408961-725345543-500\software\winsoul\keylogger\ (ID = 102579)
16:48: Found Adware: findthewebsiteyouneed hijacker
16:48: HKU\S-1-5-21-1645522239-1960408961-725345543-500\software\microsoft\internet explorer\main\ || default_search_url (ID = 125236)
16:48: HKU\S-1-5-21-1645522239-1960408961-725345543-500\software\microsoft\internet explorer\toolbar\webbrowser\ || {5f1abcdb-a875-46c1-8345-b72a4567e486} (ID = 127195)
16:48: HKU\S-1-5-21-1645522239-1960408961-725345543-500\software\instafink\ (21 subtraces) (ID = 128666)
16:48: HKU\S-1-5-21-1645522239-1960408961-725345543-500\software\avenue media\ (ID = 128887)
16:48: HKU\S-1-5-21-1645522239-1960408961-725345543-500\software\policies\avenue media\ (ID = 128928)
16:48: HKU\S-1-5-21-1645522239-1960408961-725345543-500\software\ist\ (4 subtraces) (ID = 129108)
16:48: HKU\S-1-5-21-1645522239-1960408961-725345543-500\software\istbar\ (21 subtraces) (ID = 129109)
16:48: HKU\S-1-5-21-1645522239-1960408961-725345543-500\software\rx toolbar\ (8 subtraces) (ID = 140298)
16:48: HKU\S-1-5-21-1645522239-1960408961-725345543-500\software\microsoft\internet explorer\toolbar\webbrowser\ || {25d8bacf-3de2-4b48-ae22-d659b8d835b0} (ID = 140301)
16:48: HKU\S-1-5-21-1645522239-1960408961-725345543-500\software\gator.com\ (70 subtraces) (ID = 528932)
16:48: HKU\S-1-5-21-1645522239-1960408961-725345543-500\software\microsoft\internet explorer\search\searchassistant explorer\main\ || default_search_url (ID = 555437)
16:48: HKU\S-1-5-21-1645522239-1960408961-725345543-500\software\microsoft\windows\currentversion\policies\ameopt\ (ID = 654042)
16:48: HKU\S-1-5-21-1645522239-1960408961-725345543-500\software\microsoft\internet explorer\main\ || default_search_url (ID = 790269)
16:48: Registry Sweep Complete, Elapsed Time:00:00:12
16:48: Starting Cookie Sweep
16:48: Found Spy Cookie: 217.73.66 cookie
16:48: administrador@217.73.66[1].txt (ID = 1949)
16:48: Found Spy Cookie: 66.220.17 cookie
16:48: administrador@66.220.17[1].txt (ID = 1991)
16:48: Found Spy Cookie: 7search cookie
16:48: administrador@7search[2].txt (ID = 2011)
16:48: Found Spy Cookie: 888 cookie
16:48: administrador@888[1].txt (ID = 2019)
16:48: administrador@888[2].txt (ID = 2019)

16:48: Found Spy Cookie: yieldmanager cookie
16:48: administrador@ad.yieldmanager[2].txt (ID = 3751)
16:48: Found Spy Cookie: adultfriendfinder cookie
16:48: administrador@adultfriendfinder[2].txt (ID = 2165)
16:48: Found Spy Cookie: adultrevenueservice cookie
16:48: administrador@adultrevenueservice[2].txt (ID = 2167)
16:48: Found Spy Cookie: falkag cookie
16:48: administrador@as1.falkag[2].txt (ID = 2650)
16:48: Found Spy Cookie: atlas dmt cookie
16:48: administrador@atdmt[2].txt (ID = 2253)
16:48: Found Spy Cookie: belnk cookie
16:48: administrador@belnk[1].txt (ID = 2292)
16:48: Found Spy Cookie: enhance cookie
16:48: administrador@c.enhance[1].txt (ID = 2614)
16:48: Found Spy Cookie: goclick cookie
16:48: administrador@c.goclick[1].txt (ID = 2733)
16:48: Found Spy Cookie: casalemedia cookie
16:48: administrador@casalemedia[2].txt (ID = 2354)
16:48: Found Spy Cookie: cassava cookie
16:48: administrador@cassava[1].txt (ID = 2362)
16:48: Found Spy Cookie: xhit cookie
16:48: administrador@count.xhit[1].txt (ID = 3714)
16:48: Found Spy Cookie: sextracker cookie
16:48: administrador@counter1.sextracker[1].txt (ID = 3362)
16:48: administrador@counter2.sextracker[1].txt (ID = 3362)
16:48: administrador@counter3.sextracker[2].txt (ID = 3362)
16:48: Found Spy Cookie: epilot cookie
16:48: administrador@epilot[1].txt (ID = 2621)
16:48: Found Spy Cookie: fastclick cookie
16:48: administrador@fastclick[2].txt (ID = 2651)
16:48: Found Spy Cookie: findwhat cookie
16:48: administrador@findwhat[1].txt (ID = 2674)
16:48: Found Spy Cookie: wegcash cookie
16:48: administrador@free.wegcash[1].txt (ID = 3682)
16:48: Found Spy Cookie: hotlog cookie
16:48: administrador@hotlog[2].txt (ID = 2801)
16:48: Found Spy Cookie: lopdotcom cookie
16:48: administrador@lop[1].txt (ID = 2936)
16:48: administrador@media.fastclick[1].txt (ID = 2652)
16:48: Found Spy Cookie: morwillsearch cookie
16:48: administrador@morwillsearch[2].txt (ID = 3008)
16:48: Found Spy Cookie: overture cookie
16:48: administrador@overture[1].txt (ID = 3105)
16:48: Found Spy Cookie: 2o7.net cookie
16:48: administrador@partygaming.122.2o7[1].txt (ID = 1958)
16:48: Found Spy Cookie: partypoker cookie
16:48: administrador@partypoker[2].txt (ID = 3111)
16:48: Found Spy Cookie: passion cookie
16:48: administrador@passion[2].txt (ID = 3113)
16:48: Found Spy Cookie: paycounter cookie

16:48: administrador@paycounter[1].txt (ID = 3115)
16:48: administrador@programs.wegcash[1].txt (ID = 3682)
16:48: Found Spy Cookie: realtracker cookie
16:48: administrador@project2.realtracker[1].txt (ID = 3242)
16:48: Found Spy Cookie: dashbar cookie
16:48: administrador@results.dashbar[1].txt (ID = 2496)
16:48: Found Spy Cookie: revenue.net cookie
16:48: administrador@revenue[2].txt (ID = 3257)
16:48: Found Spy Cookie: rn11 cookie
16:48: administrador@rn11[2].txt (ID = 3261)
16:48: Found Spy Cookie: adjuggler cookie
16:48: administrador@rotator.adjuggler[1].txt (ID = 2071)
16:48: Found Spy Cookie: findthewebsiteyouneed cookie
16:48: administrador@searchbar.findthewebsiteyouneed[2].txt (ID = 2673)
16:48: administrador@sextracker[1].txt (ID = 3361)
16:48: Found Spy Cookie: spylog cookie
16:48: administrador@spylog[1].txt (ID = 3415)
16:48: Found Spy Cookie: onestat.com cookie
16:48: administrador@stat.onestat[1].txt (ID = 3098)
16:48: Found Spy Cookie: statcounter cookie
16:48: administrador@statcounter[1].txt (ID = 3447)
16:48: Found Spy Cookie: tribalfusion cookie
16:48: administrador@tribalfusion[2].txt (ID = 3589)
16:48: administrador@web2.realtracker[1].txt (ID = 3242)
16:48: Found Spy Cookie: webpower cookie
16:48: administrador@webpower[2].txt (ID = 3660)
16:48: administrador@www.888[1].txt (ID = 2020)
16:48: administrador@www.lop[1].txt (ID = 2937)
16:48: Found Spy Cookie: xxxcounter cookie
16:48: administrador@xxxcounter[1].txt (ID = 3733)
16:48: Found Spy Cookie: xxxtoolbar cookie
16:48: administrador@xxxtoolbar[2].txt (ID = 3739)
16:48: Cookie Sweep Complete, Elapsed Time: 00:00:01
16:48: Starting File Sweep
16:48: c:\documents and settings\all users\menu iniciar\programas\weatherscope (2 subtraces) (ID = -2147480947)
16:48: c:\arquivos de programas\istsvc (1 subtraces) (ID = -2147480800)
16:48: c:\arquivos de programas\surfaccuracy (4 subtraces) (ID = -2147478266)
16:48: c:\documents and settings\all users\menu iniciar\programas\gain publishing (2 subtraces) (ID = -2147480950)
16:48: c:\arquivos de programas\weatherscope (5 subtraces) (ID = -2147480938)
16:48: c:\documents and settings\all users\menu iniciar\programas\date manager (2 subtraces) (ID = -2147480952)
16:48: c:\documents and settings\administrador\configurações locais\temp\fsg_tmp (ID = -2147480935)
16:48: c:\arquivos de programas\date manager (6 subtraces) (ID = -2147480943)
16:48: c:\arquivos de programas\dashbar (25 subtraces) (ID = -2147480944)
16:48: c:\documents and settings\all users\menu iniciar\programas\dashbar (1 subtraces) (ID = -2147480953)
16:48: c:\arquivos de programas\instafink (6 subtraces) (ID = -2147480836)

16:48: Found Adware: commonname
16:48: c:\windows\temp\adware (2 subtraces) (ID = -2147481214)
16:48: c:\arquivos de programas\rxtoolbar (33 subtraces) (ID = -2147476417)
16:48: c:\documents and settings\administrador\configurações locais\temp\admcache (ID = -2147481437)
16:48: c:\arquivos de programas\istbar (6 subtraces) (ID = -2147480319)
16:48: c:\windows\temp\altnet (18 subtraces) (ID = -2147481435)
16:48: Found Adware: bullguard popup ad
16:48: c:\windows\temp\bullguard (1 subtraces) (ID = -2147476409)
16:48: c:\documents and settings\all users\menu iniciar\programas\precisiontime (2 subtraces) (ID = -2147480948)
16:48: c:\arquivos de programas\precisiontime (8 subtraces) (ID = -2147480939)
16:48: egieengine.dll (ID = 61343)
16:48: gmt.exe.manifest (ID = 61434)
16:48: peer points manager.lnk (ID = 49852)
16:48: altnetuninstall.exe (ID = 49794)
16:48: about gain publishing.lnk (ID = 61270)
16:48: dminfo3.cab (ID = 49823)
16:48: asmend.exe (ID = 49803)
16:48: jsinstall.cab (ID = 49835)
16:48: dminstall7.cab (ID = 49829)
16:49: guninstaller.exe (ID = 61468)
16:49: cmesys.exe (ID = 61297)
16:49: date manager.lnk (ID = 61325)
16:49: dashbar website.lnk (ID = 61317)
16:49: eggcengine.dll (ID = 61340)
16:49: date manager.lnk (ID = 61325)
16:49: awtiveds.dll (ID = 163672)
16:49: instafinderk_inst.exe (ID = 63654)
16:49: asmps.dll (ID = 49808)
16:49: egnsengine.dll (ID = 61346)
16:49: skin.xml (ID = 49876)
16:49: Found Adware: isearch desktop search
16:49: command.exe (ID = 144946)
16:49: gstartup.lnk (ID = 61450)
16:49: gappmgr.dll (ID = 61377)
16:49: adm4.dll (ID = 49779)
16:49: Found Adware: cydoor peer-to-peer dependency
16:49: cd_clint.dll (ID = 57300)
16:49: bulldownload.exe (ID = 52017)
16:49: gioclclient.dll (ID = 61432)
16:49: adm.exe (ID = 111765)
16:49: dmfiles.cab (ID = 49818)
16:49: adm4005.exe (ID = 111765)
16:49: Found Adware: lopdotcom
16:49: cake wave.exe (ID = 91)
16:49: litedeadfile.exe (ID = 90)
16:49: pmfiles.cab (ID = 49856)
16:49: pminstall.cab (ID = 49857)
16:49: asmfiles[1].cab (ID = 49805)

16:49: gatorstubsetup.exe (ID = 61412)
16:49: giocl.dll (ID = 61431)
16:49: weatherscope.lnk (ID = 61643)
16:49: datemanager.exe (ID = 61322)
16:49: weatherscope.lnk (ID = 61643)
16:49: istbar.dll (ID = 76139)
16:49: cmeiiapi.dll (ID = 61293)
16:49: fillin.wav (ID = 61352)
16:49: istbar[1].dll (ID = 157825)
16:49: gmtproxy.dll (ID = 61439)
16:49: Found Adware: hot as hell
16:49: xml_adultbar.php (ID = 62265)
16:49: dashbarsetup.log (ID = 61315)
16:49: istsvc.exe (ID = 64660)
16:49: HKLM\Software\Microsoft\Windows\CurrentVersion\Run || IST Service (ID = 0)
16:49: egieprocess.dll (ID = 61344)
16:49: help.xml (ID = 49830)
16:49: dminfo3.cab (ID = 49824)
16:49: dminstall7.cab (ID = 49829)
16:49: pmexe.cab (ID = 49854)
16:49: Found Adware: dialer access
16:49: loader[1].cab (ID = 58235)
16:49: istrecover[1].exe (ID = 64496)
16:49: nem220[1].dll (ID = 64043)
16:49: nem220.dll (ID = 64043)
16:49: e402ledo1h0c.dll (ID = 163672)
16:49: precisiontime.lnk (ID = 61563)
16:49: weatherscope.exe (ID = 61640)
16:49: gatorres.dll (ID = 61405)
16:49: gdwldeng.dll (ID = 61425)
16:49: points manager.exe (ID = 49861)
16:49: HKLM\Software\Microsoft\Windows\CurrentVersion\Run || AltnetPointsManager (ID = 0)
16:49: asmfiles.cab (ID = 49805)
16:49: admdata.dll (ID = 49784)
16:49: admdloader.dll (ID = 49786)
16:49: admfdi.dll (ID = 49789)
16:49: admprog.dll (ID = 49790)
16:50: precisiontime.lnk (ID = 61563)
16:50: nsyrfx.exe (ID = 64496)
16:50: HKLM\Software\Microsoft\Windows\CurrentVersion\Run || VFLi (ID = 0)
16:50: wsuninstaller.exe (ID = 61652)
16:50: admprog.dll (ID = 49790)
16:50: adm4.dll (ID = 49779)
16:50: adm25.dll (ID = 49782)
16:50: altnet.css (ID = 49792)
16:50: gatorgaininstaller.log (ID = 61390)
16:50: gmt.exe (ID = 61437)
16:50: appmgrgui.zip (ID = 61281)

16:50: ptuninstaller.exe (ID = 61570)
16:50: setup.exe (ID = 49875)
16:50: points manager.exe.manifest (ID = 49859)
16:50: setup.cab (ID = 49872)
16:50: sysdetect.dll (ID = 49877)
16:50: local_firstuse.html (ID = 49844)
16:50: local_points.html (ID = 49846)
16:50: local_redeem.html (ID = 49846)
16:50: local_start.html (ID = 49844)
16:50: local_wallet.html (ID = 49846)
16:50: instafinderk_inst.exe (ID = 63654)
16:50: Found Adware: topsearch
16:50: topsearch.dll (ID = 79735)
16:50: dbau.exe (ID = 61334)
16:50: admdloader.dll (ID = 49786)
16:50: admdata.dll (ID = 49784)
16:50: admfdi.dll (ID = 49789)
16:50: adm25.dll (ID = 49782)
16:50: gainplugin.dll (ID = 61363)
16:50: gatorgainplugin.log (ID = 61391)
16:50: istactivex.dll (ID = 64599)
16:50: precisiontime.exe (ID = 61561)
16:50: message.xml (ID = 49847)
16:50: dmuninstaller.exe (ID = 61338)
16:50: date manager website.url (ID = 61333)
16:50: cmediagnostics.log (ID = 61291)
16:50: dashbarwebsite.url (ID = 61318)
16:50: precisiontimewebsite.url (ID = 61569)
16:50: weatherscope website.url (ID = 61649)
16:50: selectdir.txt (ID = 49864)
16:50: gain publishing web site.url (ID = 61372)
16:50: gator.log (ID = 61386)
16:50: mepcme.dat (ID = 61517)
16:50: gatorsupportinfo.txt (ID = 61414)
16:50: selectdir1st.txt (ID = 49865)
16:51: Found System Monitor: activity logger
16:51: activity logger configuration.lnk (ID = 48839)
16:51: visit activity logger website.lnk (ID = 48875)
16:51: activity loggert help.lnk (ID = 48841)
16:51: uninstall activity logger.lnk (ID = 48871)
16:51: Found Adware: 180search assistant/zango
16:51: zango.lnk (ID = 91109)
16:51: gator.lnk (ID = 61385)
16:53: alogcfg.exe (ID = 48846)
16:53: logexp.dll (ID = 119925)
16:53: readme.txt (ID = 119926)
16:53: license.txt (ID = 119927)
16:53: alogcfg.hlp (ID = 119928)
16:53: emailer.dll (ID = 119932)
16:53: scrview.exe (ID = 119933)

16:53: swkbhkl.dll (ID = 119935)
16:53: slgrl.dll (ID = 119936)
16:53: alaware.dll (ID = 119937)
16:53: alsys.exe (ID = 119938)
16:53: alogger.url (ID = 48848)
16:53: buyal.url (ID = 48852)
16:53: Found System Monitor: activity monitor 2002
16:53: url.html (ID = 48873)
16:53: bottom.html (ID = 48906)
16:53: first.html (ID = 48855)
16:53: head.html (ID = 48856)
16:53: last.html (ID = 48857)
16:53: log.xls (ID = 48859)
16:53: logrec.html (ID = 48861)
16:53: scrshot.html (ID = 48865)
16:53: header.csv (ID = 48918)
16:53: delim.csv (ID = 48912)
16:53: Sweep Canceled
16:53: File Sweep Complete, Elapsed Time: 00:04:43
16:53: Traces Found: 1724
16:54: Removal process initiated
16:54: Quarantining All Traces: look2me
16:54: Warning: Launched explorer.exe
16:54: Warning: Quarantine process could not restart Explorer.
16:54: look2me is in use. It will be removed on reboot.
16:54: awtiveds.dll is in use. It will be removed on reboot.
16:54: e402ledo1h0c.dll is in use. It will be removed on reboot.
16:54: C:\WINDOWS\system32\e402ledo1h0c.dll is in use. It will be removed on reboot.
16:54: C:\WINDOWS\system32\awtiveds.dll is in use. It will be removed on reboot.
16:54: Quarantining All Traces: altnet
16:55: Quarantining All Traces: cws-aboutblank
16:55: Quarantining All Traces: gain-supported software
16:55: Quarantining All Traces: ist software
16:55: Quarantining All Traces: instafinder
16:55: Quarantining All Traces: internetoptimizer
16:55: Quarantining All Traces: ist istbar
16:56: Quarantining All Traces: moneytree
16:56: Quarantining All Traces: rx toolbar
16:56: Quarantining All Traces: surf accuracy
16:56: Quarantining All Traces: active keylogger
16:56: Quarantining All Traces: findthewebsiteyouneed hijacker
16:56: Quarantining All Traces: 217.73.66 cookie
16:56: Quarantining All Traces: 66.220.17 cookie
16:56: Quarantining All Traces: 7search cookie
16:56: Quarantining All Traces: 888 cookie
16:56: Quarantining All Traces: yieldmanager cookie
16:56: Quarantining All Traces: adultfriendfinder cookie
16:56: Quarantining All Traces: adultrevenueservice cookie
16:56: Quarantining All Traces: falkag cookie

16:56: Quarantining All Traces: atlas dmt cookie
16:56: Quarantining All Traces: belnk cookie
16:56: Quarantining All Traces: enhance cookie
16:56: Quarantining All Traces: goclick cookie
16:56: Quarantining All Traces: casalemedia cookie
16:56: Quarantining All Traces: cassava cookie
16:56: Quarantining All Traces: xhit cookie
16:56: Quarantining All Traces: sextracker cookie
16:56: Quarantining All Traces: epilot cookie
16:56: Quarantining All Traces: fastclick cookie
16:56: Quarantining All Traces: findwhat cookie
16:56: Quarantining All Traces: wegcash cookie
16:56: Quarantining All Traces: hotlog cookie
16:56: Quarantining All Traces: lopdotcom cookie
16:56: Quarantining All Traces: morwillsearch cookie
16:56: Quarantining All Traces: overture cookie
16:56: Quarantining All Traces: 2o7.net cookie
16:56: Quarantining All Traces: partypoker cookie
16:56: Quarantining All Traces: passion cookie
16:56: Quarantining All Traces: paycounter cookie
16:56: Quarantining All Traces: realtracker cookie
16:56: Quarantining All Traces: dashbar cookie
16:56: Quarantining All Traces: revenue.net cookie
16:56: Quarantining All Traces: rn11 cookie
16:56: Quarantining All Traces: adjuggler cookie
16:56: Quarantining All Traces: findthewebsiteyouneed cookie
16:56: Quarantining All Traces: spylog cookie
16:56: Quarantining All Traces: onestat.com cookie
16:56: Quarantining All Traces: statcounter cookie
16:56: Quarantining All Traces: tribalfusion cookie
16:56: Quarantining All Traces: webpower cookie
16:56: Quarantining All Traces: xxxcounter cookie
16:56: Quarantining All Traces: xxxtoolbar cookie
16:56: Quarantining All Traces: commonname
16:56: Quarantining All Traces: bullguard popup ad
16:56: Quarantining All Traces: isearch desktop search
16:56: Quarantining All Traces: lopdotcom
16:56: Quarantining All Traces: hot as hell
16:56: Quarantining All Traces: dialer access
16:56: Quarantining All Traces: topsearch
16:56: Quarantining All Traces: activity logger
16:56: Quarantining All Traces: 180search assistant/zango
16:56: Quarantining All Traces: activity monitor 2002
16:56: Removal process completed. Elapsed time 00:02:22
16:57: | End of Session, sexta-feira, 12 de maio de 2006 |

APÊNDICE B - Logs do Software HijackThis

Logfile of HijackThis v1.99.1
Scan saved at 16:17:07, on 12/5/2006
Platform: Windows XP SP2 (WinNT 5.01.2600)
MSIE: Internet Explorer v6.00 SP2 (6.00.2900.2180)

Running processes:
C:\WINDOWS\System32\smss.exe
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\System32\svchost.exe
C:\WINDOWS\system32\spoolsv.exe
C:\WINDOWS\system32\rundll32.exe
C:\WINDOWS\Explorer.EXE
C:\defender25.exe
C:\windows\temp\bic_gatordm.exe
C:\Arquivos de programas\ISTsvc\istsvc.exe
C:\WINDOWS\nsyrfx.exe
C:\Arquivos de programas\Internet Explorer\iexplore.exe
C:\Arquivos de programas\SurfAccuracy\SAcc.exe
C:\WINDOWS\ojponyb.exe
C:\Program Files\Internet Optimizer\optimize.exe
C:\WINDOWS\system32\P2P Networking\P2P Networking.exe
C:\WINDOWS\dXNlcg\command.exe
C:\Arquivos de programas\RXToolBar\Semantic Insight\SemanticInsight.exe
c:\arquiv~1\intern~1\iexplore.exe
C:\Program Files\Altnet\Points Manager\Points Manager.exe
C:\Arquivos de programas\Network Monitor\netmon.exe
C:\Arquivos de programas\TBONBin\tbon.exe
C:\Arquivos de programas\Webroot\Spy Sweeper\WRSSSDK.exe
C:\Arquivos de programas\Date Manager\DateManager.exe
C:\Arquivos de programas\PrecisionTime\PrecisionTime.exe
C:\Arquivos de programas\Weatherscope\Weatherscope.exe
C:\PROGRA~1\Altnet\DOWNLO~1\asm.exe
C:\WINDOWS\system32\wscntfy.exe
C:\Documents and Settings\Administrador\Desktop\hijackthis\HijackThis.exe

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Default_Search_URL = http://searchbar.findthewebsiteyouneed.com
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar = http://results.dashbar.com/search?c=27440&b=29905&t=0&ce=DI&m=NjA3MjEzNzg3&ver=3.1.0.0&lang=en
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page = http://searchbar.findthewebsiteyouneed.com

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = http://www.findthewebsiteyouneed.com
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page = http://searchbar.findthewebsiteyouneed.com
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant = http://searchbar.findthewebsiteyouneed.com
R3 - URLSearchHook: (no name) - _{CFBFAE00-17A6-11D0-99CB-00C04FD64497} - (no file)
O2 - BHO: BHObj Class - {00000010-6F7D-442C-93E3-4A4827C2E4C8} - C:\WINDOWS\nem220.dll
O2 - BHO: Need2Find Bar BHO - {4D1C4E81-A32A-416b-BCDB-33B3EF3617D3} - C:\Arquivos de programas\Need2Find\bar\1.bin\ND2FNBAR.DLL
O2 - BHO: InstaFinderK - {4E7BD74F-2B8D-469E-90F0-F66AB581A933} - C:\ARQUIV~1\INSTAF~1\INSTAF~1.DLL
O2 - BHO: RXResultTracker Class - {59879FA4-4790-461c-A1CC-4EC4DE4CA483} - C:\Arquivos de programas\RXToolBar\sfcont.dll
O3 - Toolbar: ISTbar - {5F1ABCDB-A875-46c1-8345-B72A4567E486} - C:\Arquivos de programas\ISTbar\istbar.dll
O3 - Toolbar: DashBar Toolbar - {CC90CDA0-74A0-45b4-80EF-D89CA8C249B8} - C:\Arquivos de programas\DashBar\DashBar31.dll
O3 - Toolbar: RX Toolbar - {25D8BACF-3DE2-4B48-AE22-D659B8D835B0} - C:\Arquivos de programas\RXToolBar\RXToolBar.dll
O4 - HKLM\..\Run: [SpySweeper] "C:\Arquivos de programas\Webroot\Spy Sweeper\SpySweeper.exe" /startintray
O4 - HKLM\..\Run: [Bin find flap gram] C:\Documents and Settings\All Users\Dados de aplicativos\proxy team bin find\Face view.exe
O4 - HKLM\..\Run: [newname] C:\\newname25.exe
O4 - HKLM\..\Run: [defender] C:\\defender25.exe
O4 - HKLM\..\Run: [keyboard] C:\\keyboard25.exe
O4 - HKLM\..\Run: [Trickler] "c:\windows\temp\bic_gatordm.exe"
O4 - HKLM\..\Run: [IST Service] C:\Arquivos de programas\ISTsvc\istsvc.exe
O4 - HKLM\..\Run: [VFLi] C:\WINDOWS\nsyrfx.exe
O4 - HKLM\..\Run: [SurfAccuracy] C:\Arquivos de programas\SurfAccuracy\SAcc.exe
O4 - HKLM\..\Run: [ReJf5vH] C:\WINDOWS\ojponyb.exe
O4 - HKLM\..\Run: [Internet Optimizer] "C:\Program Files\Internet Optimizer\optimize.exe"
O4 - HKLM\..\Run: [P2P Networking] C:\WINDOWS\system32\P2P Networking\P2P Networking.exe /AUTOSTART
O4 - HKLM\..\Run: [SemanticInsight] C:\Arquivos de programas\RXToolBar\Semantic Insight\SemanticInsight.exe
O4 - HKLM\..\Run: [AltnetPointsManager] C:\Program Files\Altnet\Points Manager\Points Manager.exe -s
O4 - HKCU\..\Run: [scr mpeg] C:\DOCUME~1\ADMINI~1\DADOSD~1\NAMEDO~1\Bold Build.exe
O4 - HKCU\..\Run: [tbon] C:\Arquivos de programas\TBONBin\tbon.exe /r
O4 - Global Startup: Date Manager.lnk = C:\Arquivos de programas\Date Manager\DateManager.exe
O4 - Global Startup: PrecisionTime.lnk = C:\Arquivos de programas\PrecisionTime\PrecisionTime.exe

O4 - Global Startup: Weatherscope.lnk = C:\Arquivos de programas\Weatherscope\Weatherscope.exe
O16 - DPF: {1D6711C8-7154-40BB-8380-3DEA45B69CBF} (Web P2P Installer) -
O18 - Filter: text/html - {2AB289AE-4B90-4281-B2AE-1F4BB034B647} - C:\Arquivos de programas\RXToolBar\sfcont.dll
O20 - Winlogon Notify: ThemeManager - C:\WINDOWS\system32\g8040idqe80e0.dll
O23 - Service: Command Service (cmdService) - Unknown owner - C:\WINDOWS\dXNlcg\command.exe
O23 - Service: Network Monitor - Unknown owner - C:\Arquivos de programas\Network Monitor\netmon.exe
O23 - Service: Webroot Spy Sweeper Engine (svcWRSSSDK) - Webroot Software, Inc. - C:\Arquivos de programas\Webroot\Spy Sweeper\WRSSSDK.exe

ANEXO A - Política de Privacidade On-Line do Banco Itaú S.A.

Política de Privacidade
Privacidade das informações
Política de Privacidade On-line do Banco Itaú S.A.

A Política de Privacidade On-Line foi criada para reafirmar o compromisso do Itaú com a segurança e a privacidade das informações coletadas dos usuários de seus produtos e serviços interativos. Como essa política está sujeita a eventuais atualizações, recomendamos que ela seja consultada periodicamente.

Você pode visitar nosso site e conhecer os produtos e serviços que oferecemos, verificar oportunidades de carreiras, ler relatórios, obter informações e notícias, sem precisar fornecer nenhuma informação pessoal. Mas, caso isso aconteça, esta política procura esclarecer como o Itaú coleta e trata seus dados individuais.

1- Qualquer informação fornecida pelos usuários será coletada e guardada de acordo com os mais rígidos padrões de segurança e confiabilidade.
2- Todas as informações coletadas dos usuários trafegam de forma segura, utilizando processo de criptografia padrão da Internet.
3- As informações pessoais que nos forem fornecidas pelos usuários serão coletadas por meios éticos e legais. Essa coleta poderá ter um ou mais propósitos, sobre os quais nossos usuários serão informados.
4- Os usuários serão avisados sobre que dados seus estão sendo coletados, ficando a seu critério fornecê-los ou não, e serão informados também sobre as conseqüências de sua decisão.
5- A menos que tenhamos determinação legal ou judicial, as informações dos usuários jamais serão transferidas a terceiros ou usadas para finalidades diferentes daquelas para as quais foram coletadas.
6- O acesso às informações coletadas está restrito a funcionários autorizados para o uso adequado desses dados. Os funcionários que se utilizarem indevidamente dessas informações, ferindo nossa Política de Privacidade, estarão sujeitos às penalidades previstas em nosso processo disciplinar.
7- Manteremos a integridade das informações que nos forem fornecidas.
8- Nossos sites contêm links para outros sites externos cujos conteúdos e políticas de privacidade não são de responsabilidade do Itaú ,sendo que nós não temos acesso às informações coletadas por "cookies" (*) presentes nesses sites.
9- Será exigida de toda organização contratada para prover serviços de apoio, o cumprimento aos nossos padrões de privacidade e segurança da informação.
10- Para fins operações de crédito e gerenciamento de riscos, poderemos trocar informações sobre nossos clientes com fontes respeitáveis de referência, órgãos reguladores e serviços de compensação.
11- Eventualmente, poderemos utilizar cookies (*) para confirmar sua identidade, personalizar seu acesso e acompanhar a utilização de nosso website visando o aprimoramento de sua navegação e funcionalidade.
12- O Itaú coloca à disposição de seus usuários, canais de atendimento ao cliente, para esclarecer qualquer dúvida que possa surgir.

---

*Cookie: pequeno arquivo colocado em seu computador para rastrear movimentos dentro dos websites, como visitas a páginas e anúncios.
Cookies não armazenam informações pessoais sem que você as tenha fornecido e não coletam informações registradas em seu computador.
A maioria dos browsers possibilita que o usuário, a qualquer instante, ative mecanismos para informá-lo quando os cookies estiverem acionados ou para evitar que sejam acionados, embora isso possa afetar a utilização de algumas funções de nosso site.