



McAfee Systems Protection

Contagem de Detecções de Spywares

Impressões e Realidade

Índice

Índice	2
O mito do número de assinaturas	3
Truques	3
Quando uma ameaça é contada como exclusiva	3
Mas espere, ainda tem mais!	5
Confundindo a situação	6

Como os produtos devem ser comparados?	6
Próximas Etapas	7
Cooperação do Ramo	7
Testes Independentes Melhorados	7

Conclusão	7
Sobre a AVERT	8

O mito do número de características

Truques!

Nos primórdios do ramo de antivírus, era comum que os fornecedores se vangloriassem do número de assinaturas que reconheciam e escondessem suas amostras dos outros fornecedores de antivírus para impedir que estes os alcançassem. Por fim, todos perceberam que isso estava levando a afirmações enganosas e prestando um mau serviço para o mercado. Essa prática levou, de muitas formas, ao surgimento dos organismos de testes independentes, tais como ICSA Labs, VTC, AV-Test.org e outros.

Infelizmente, o ramo do anti-spyware, de maneira geral, ainda não atingiu esse nível de maturidade. Muitos fornecedores contam cada executável, arquivo de dados, chave de registro e outros pertencente a um pacote como nova característica. Também há uma grande variação nos tipos de ameaças detectadas. Alguns detectam backdoors, cavalos de Tróia e worms, ao passo que outros contam com numerosas detecções de cookies, os quais não possuem qualquer impacto sobre a segurança e implicações discutíveis sobre a privacidade.

Quando uma ameaça é contada como exclusiva

O ponto de vista do antivírus

Há muito tempo a indústria de antivírus faz confusão sobre a nomenclatura dos vírus, e há uma ampla disparidade não apenas quanto ao número de detecções que um produto afirma ser capaz de realizar, mas também quanto à maneira como as ameaças são nomeadas e contadas. Essa discrepância ocorre no mundo dos antivírus por diversas razões, a saber:

- Convenções tradicionais
- Falta de tempo para sincronizar nomes durante as epidemias
- Por simples teimosia
- Diferenças na tecnologia de detecção genérica e heurística

Para compreender o último aspecto, imagine que os quatro arquivos a seguir, consistindo apenas em seis seqüências de letras, fossem todos vírus:

1. ABCDEF
2. ACCDEF
3. AACDEF
4. AACDFF

Agora, imagine um grupo de fornecedores de antivírus escrevendo programas para detectar todos eles (programas de detecção executados na ordem mostrada a seguir):

Fornecedor X:

- Detecta A*CD*F como Vírus 1

Fornecedor Y:

- Detecta AACD*F como Vírus 1
- Detecta A*CDEF como Vírus 2

Fornecedor Z:

- Detecta ABCD** como Vírus 2
- Detecta ACCD** como Vírus 3
- Detecta AACD** como Vírus 4

Acabamos tendo o seguinte:

Tabela 1: Concordância hipotética de nomenclatura de antivírus

Arquivo	Fornecedor X:	Fornecedor Y:	Fornecedor Z:
	Núm. Carac. 1	Núm. Carac. 2	Núm. Carac. 3
ABCDEF	Vírus 1	Vírus 2	Vírus 2
ACCDEF	Vírus 1	Vírus 2	Vírus 3
AACDEF	Vírus 1	Vírus 1	Vírus 4
AACDFF	Vírus 1	Vírus 1	Vírus 4

Portanto, neste caso supersimplificado, três fornecedores com variação de 200% no número de características detectam todas as quatro amostras, mas com nomes diferentes.

A ferramenta VGrep, mantida pela McAfee para o Boletim de Vírus (<http://www.virusbtn.com/resources/vgrep/index.xml>) ajuda a reduzir essa confusão, realizando uma referência cruzada dos nomes dos fornecedores com um grande corpo de amostras.

Par ver um exemplo mais realista, em um recente teste da AVComparatives (http://www.avcomparatives.org/seiten/ergebnisse_2004_08.php), os produtos testados afirmam reconhecer de pouco menos de 53 mil características (Dialogue Science) até quase 123 mil

características (Frisk Software). Mas, ao final das contas, quase todos os produtos testados detectaram mais de 300 mil de 323 mil amostras únicas. Portanto, uma grande diferença no número de características pode ter relação apenas com pequenas diferenças nos recursos reais de detecção.

Agora, esse nível de confusão ocorre em um ramo que:

- Existe há quase 20 anos, de uma forma ou de outra
- Possui definições uniformes do que é e do que não é um vírus ou um cavalo de Tróia (a definição de vírus pode ser expressa em termos matemáticos, de tão precisa que é. Adleman, 1988, "An Abstract Theory of Computer Viruses")
- Possui vários organismos profissionais (AVPD, CARO, AVED, AVAR, EICAR) para promover cooperação e uniformidade
- Possui uma rotina de troca de coleções entre a maioria dos fornecedores
- Possui vários organismos de testes de boa reputação (por exemplo, ICSA, VTC, VB, AV-Test.org, AVComparatives.org) com coleções de alta qualidade

Na verdade, toda a base da classificação dos recursos de detecção dos fornecedores de antivírus depende do fato de haver pessoas e organizações com coleções ortodoxas ou, pelo menos, muito completas. Dessa forma, podemos comparar maçãs com maçãs em relação aos produtos antivírus, de forma que elas não apresentem ambigüidades, apesar da inerente falta de uniformidade na contagem e na nomenclatura.

O ponto de vista do anti-spyware

Agora, passemos ao ramo dos programas espíões (*spyware*), no qual uma recente (setembro de 2004) pesquisa interna da McAfee apresentou os seguintes números "crus" de características:

Tabela 2: Número de característica detectada pelos produtos anti-spyware

Concorrente	Produto	Nº de detecções
Aluria	Spyware Eliminator	18625
Lavasoft	Ad-Aware	9637
Computer Associates	PestPatrol	118060
Safer Networking Ltd	Spybot S&D	17679

Spycop	SpyCop	467
Webroot	Spyware Sweeper	31104
Javacool	SpywareBlaster	3183
PC Tools.com Ltd	Spyware Doctor	10684
Giant Company Software‡	GIANT Antispyware	> 100.000
McAfee	VirusScan Enterprise	3175*
McAfee	Antispyware**	384

* Conta apenas detecções de Programas Potencialmente Indesejáveis

** Produto anti-spyware da McAfee para o mercado consumidor

‡ Atual Microsoft Anti-spyware

Isso demonstra uma diferença de três ordens de magnitude entre as contagens mais alta e mais baixa de característica nos diferentes produtos. Agora, vamos levar em conta a velocidade desses produtos na varredura da coleção APPS da McAfee (detecções que não são nem de vírus nem de cavalos de Tróia):

Tabela 3: Detecção dos produtos anti-spyware com a coleção APPS da McAfee

Fornecedor	Número de Detecções	Tempo Gasto
McAfee VirusScan Enterprise	11288	0:19:50
Spyware Doctor	135	0:00:24
SpySweeper	951	0:02:54
Adwaresafe	151	0:00:57
Adaware	356	0:03:19
PestPatrol	2601	0:25:00
McAfee Antispyware*	270	0:03:53
Aluria Spyware Eliminator	358	0:12:07
Giant Antispyware	617	0:22:19
SpyBot	0	0:03:08

* Produto anti-spyware da McAfee para o mercado consumidor

ATENÇÃO:

- Este é um teste horrível e não deve ser usado para comparações reais ou avaliações competitivas.
- O McAfee Anti-Spyware Enterprise (produto para empresas) não estava disponível para inclusão no momento dos testes.

A única coisa que os resultados acima provam é que é MUITO fácil realizar um teste sem qualquer significado. Por que esse é um teste horrível?

- Ele inclui amostras recolhidas por apenas um fornecedor (McAfee) e é EXTREMAMENTE tendencioso em favor do VirusScan Enterprise, pois se trata da coleção usada para verificar se detectamos o que devemos em termos de PUPs (Programas Potencialmente Indesejáveis) antes de cada DAT ser liberado.
- Ele é extremamente tendencioso CONTRA produtos que dependem de mais de um arquivo para disparar a detecção. Por exemplo, o SpyBot detecta PUPs APENAS quando um pacote corretamente instalado (inclusive entradas de registro *et. al.*) está presente em um sistema. Uma coleção de arquivos “sem inteligência” não disparará nada. Na verdade, o SpyBot actually é um produto anti-spyware decente contra PUPs ativos, e isso não pode ser determinado com este teste.
- Ele não possui detecção de cookies e entradas de registro, os quais podem compor grandes partes dos bancos de dados de características de alguns produtos.
- Ele não possui cavalos de Tróia e outros programas mal-intencionados “tradicionais”, que, muitas vezes, conseguem driblar os produtos anti-spyware. Por exemplo, quase 70% dos arquivos listados na *Pest Encyclopedia* do *Pest Patrol* (<http://research.pestpatrol.com/search/browse.aspx>), ou seja, mais de 25 mil pragas, estão em categorias que a AVERT geralmente trata como cavalos de Tróia. Em outras palavras, quase ¾ do seu banco de dados de característica podem consistir em itens já detectados pelo McAfee VirusScan Enterprise.
- Ele não possui uma coleção de mais de 200 mil programas discadores diferentes que são detectados por menos de 100 características nos arquivos DAT da McAfee.

Mas espere, ainda tem mais!

Contudo, essas não são as únicas dificuldades da tentativa de entender um pouco o jogo dos números do anti-spyware. A maioria dos vírus e cavalos de Tróia consiste em programas autônomos – eles normalmente consistem em um único arquivo, ou até mesmo algumas linhas de código dentro de outro arquivo. Embora o polimorfismo e o parasitismo tornem o campo dos vírus um pouco mais complexo e possam causar acaloradas discussões entre os

fornecedores de antivírus sobre o nome correto das famílias, eles são, de muitas formas, menos complexos que os PUPs.

Muitos PUPs são pacotes completos de *software*. Eles possuem instaladores, desinstaladores, arquivos “leia-me”, contratos de licença, arquivos de dados, DLLs de apoio, atalhos e a parafernália comum aos aplicativos do Windows. Nas nossas primeiras experiências com os spywares coletados pela equipe MAS (McAfee Anti-Spyware) para consumidores, percebemos o seguinte:

- Há algo em torno de 14 mil arquivos (somente cerca de cinco mil são deixados após a exclusão dos arquivos de dados, tais como txt, jpg, registry e outros.) presentes na coleção MAS, pertencentes às apenas 400 (mais ou menos) detecções únicas que o produto contém. Portanto, embora os DATs contem com três mil características para detectar 11 mil arquivos (perto de três arquivos por característica), a coleção MAS precisa de apenas 400 para dar conta de cerca de 14 mil (aproximadamente 35 por característica).
- Uma única detecção da coleção MAS contém, muitas vezes, arquivos detectados sob cinco a dez nomes completamente diferentes nos DATs.
- Há muito mais reutilização de código nos PUPs, de forma que exatamente o mesmo binário pode existir em 15 ou mais pacotes individuais de PUPs. Ainda pior, os mesmos binários podem existir em pacotes que NÃO possuem absolutamente nenhuma característica de PUP, os quais não queremos detectar nesse contexto.

Em resumo, **não há absolutamente qualquer correspondência entre o número de características em um banco de dados e a eficiência desse produto contra qualquer conjunto de ameaças específico.**

Há muito pouca uniformidade sobre como as detecções são contadas entre os fornecedores de anti-spyware, e nenhum deles está em condições de assumir isso, porque ninguém possui uma coleção abrangente. A AVERT calcula que existam em torno de sete mil a dez mil PUPs realmente exclusivos para detectar, contando-os mais ou menos da forma que fazemos na área de antivírus. Então, vamos pressupor que os fornecedores dedicados a antivírus vejam apenas metade do quadro geral, dupliquem-no e acrescentem alguma variabilidade nas convenções de nomenclatura e níveis diferentes de detecção genérica entre os fornecedores. Qualquer coisa acima de cerca de 20 mil deverá disparar o alarme de uma possível “inflação”.

Confundindo a situação

Pode haver várias maneiras de indicar detecções em um produto anti-spyware baseado em host:

- Por número de nomes diferentes de detecção
- Por nomes e variantes de detecção
- Por número de arquivos e itens de registro detectados
- Por número de arquivos e itens de registro excluídos

De certa maneira, nenhum desses métodos é intrinsecamente mais correto que qualquer outro. Entretanto, a comparação de um relatório de um fornecedor que utiliza o primeiro método com o relatório de um fornecedor que utiliza o último método gerará resultados aparentemente assimétricos, mesmo que detectem e excluam exatamente os mesmos objetos!

Alguns produtos detectam chaves de registro existentes normalmente em sistemas Windows, que podem ser contadas como “omissão” por outros produtos.

Alguns produtos indicarão o mesmo objeto várias vezes. Em um teste, uma única DLL foi listada 50 vezes em um único relatório. Muitos produtos anti-spyware indicam chaves de registro várias vezes, uma para cada grupo por meio do qual elas podem ser endereçadas, por exemplo:

- HKEY_CLASSES_ROOT\ProgID
- HKEY_LOCAL_MACHINE\Software\Classes\ProgID

Alguns produtos indicam cada subchave ou valor de registro presente ao excluir uma chave ascendente, levando um único objeto “sabidamente nocivo” gere uma dezena ou mais de itens em um log de correção.

Já vimos casos em que diferentes produtos anti-spyware indicaram de 5 a 96 “itens” durante a detecção e a correção de um único pacote de adware, com resultados praticamente idênticos, ou seja, todos eles eliminaram os mesmos arquivos e as mesmas entradas do registro.

Em outras palavras, não há qualquer correspondência entre o número de objetos indicados por dois produtos e a sua eficiência.

Como os produtos devem ser comparados?

A finalidade de um teste de detecção é determinar quais entre um grupo de produtos são capazes de localizar mais “material ruim” de maneira eficiente e eficaz. Há alguns pré-requisitos para que uma comparação seja válida:

- Todos os produtos testados estão de acordo sobre o que é “material ruim”. Na pior das hipóteses, devem ser incluídas apenas as amostras sobre as quais todos os produtos concordam categoricamente. A menos que o objetivo de todos os produtos seja eliminar cavalos de Tróia ou programas de compartilhamento de arquivos por P2P, eles não devem fazer parte do conjunto de teste.
- O conjunto de amostra deve ser o maior possível. As amostras do conjunto devem vir de um período de tempo bem-definido, e devem ser verificadas por um especialista na área. Em condições ideais, o conjunto de amostra do examinador deve ser um superconjunto extraído de fontes do ramo, de especialistas independentes e das suas próprias pesquisas, a fim de evitar parciaisidades injustas no teste.
- Quando o conjunto de amostras precisar ser limitado, as amostras deverão ser escolhidas de acordo com alguns critérios significativos – por exemplo, predominância, risco potencial ou carga, dificuldade de remoção. Um pequeno conjunto de amostras mal-escolhidas mascarará os aspectos tanto positivos quanto negativos dos produtos testados, por meio do simples acaso.
- Tanto os falsos positivos COMO os falsos negativos devem ser testados. É muito fácil escrever rotinas de detecção que apanhem cada uma das amostras, mas isso cria muitos falsos positivos ou problemas de velocidade.
- Os critérios de sucesso ou fracasso devem se basear na medição independente das alterações em arquivos, processos ou no registro, NÃO no desempenho de algum produto de “referência”.

Devido à falta de uniformidade e de definições no mercado de anti-spyware em geral, a maioria dos testes até hoje foi mal-projetada e mal-implementada. Os conjuntos de

amostras são pequenos e escolhidos arbitrariamente. As amostras usadas e seus efeitos sobre o sistema foram mal documentados. Muitas vezes, as medições consistem na listagem de quantos itens o produto indicou, estejam eles ou não sequer relacionados às amostras em questão.

Próximas Etapas

Cooperação do Ramo

Atualmente, o ramo de anti-spyware está envolvido em um grande jogo de pôquer no qual nenhum jogador pode ver as cartas dos outros. Todos estão blefando com seus clientes, esperando que ninguém pague para ver, porém essa situação é insustentável. A McAfee começará a tentar estabelecer o mesmo tipo de alianças entre os integrantes de boa reputação da comunidade anti-spyware que já temos nas comunidades antivírus. Já há alguma troca limitada de coleções de PUPs entre alguns grandes fornecedores de antivírus.

Procuraremos ampliar essa iniciativa para que possamos começar a ter uma idéia mais clara do panorama competitivo e começar realmente a medir nosso progresso em uma escala que tenha alguma relação com a realidade. Naturalmente, essa abordagem é um pouco arriscada, pois as outras empresas também terão acesso às nossas coleções. Em vários anos de trocas de coleções de vírus, não houve nenhum grande abalo causado por essa prática; as empresas que já estavam no jogo ainda estão, e as empresas menos organizadas ainda estão atrás. Esperamos que isso também valha para o mercado anti-spyware. Em todo caso, estaremos em melhores condições que qualquer outra empresa de absorver novos conteúdos devido às ferramentas e técnicas que já desenvolvemos na área de antivírus.

Testes Independentes Melhorados

Finalmente, o ramo de anti-spyware precisa incentivar o aumento das medidas e dos testes dos programas anti-spyware. Em um ambiente no qual falhas em testes decidem a superioridade dos fornecedores, não há uma maneira racional de determinar a forma de melhorar ou de medir o quanto se melhora. É necessário definir quais metodologias de teste possuem maior probabilidade de gerar resultados precisos e significativos, e trabalhar com organizações de teste independentes para implementar essas técnicas. É preciso ajudar os analistas independentes a superar seu medo de repercussões legais e criar coleções úteis.

Até que isso aconteça, entretanto, ainda estaremos no Velho Oeste dos testes. Clientes, analistas mal informados, parceiros e OEMs realizarão testes provisórios mal concebidos que complicarão mais a situação do que a esclarecerão. Os analistas devem:

- Sempre que possível, usar dados baseados em predominância para orientar seus conjuntos de teste. Extrair dados de predominância de PUPs de relatórios de clientes, de logs de suporte, de relatórios de predominância de fornecedores, praticamente qualquer coisa tem mais validade que testes realizados em relação a N PUPs que possam estar bem confortáveis no computador da mamãe de alguém, ou que possam ser instalados durante a visita a alguns sites nada confiáveis.
- Muitos analistas inexperientes realizarão um teste no qual instalarão um monte de PUPs aleatórios e, em seguida, aplicarão um produto anti-spyware, depois aplicarão um segundo produto, e “descerão a lenha” no fornecedor do primeiro produto por qualquer coisa que ele tenha deixado passar. Os resultados da análise da Spyware Warrior acima indicam que os fornecedores tendem a detectar TUDO ou NADA de um determinado pacote, mas todos eles deixam passar um número considerável de pacotes. A menos que um pesquisador de segurança que possua bom-senso tenha confirmado se tudo o que passou é relevante (e não falsos positivos) e o teste tenha sido realizado também na ordem inversa, os dados gerados não terão qualquer significado.
- Quando é indicado um falso negativo, falso positivo ou erro de correção em um produto, as respectivas amostras devem ser colocadas à disposição do fornecedor para reproduzir ou refutar a afirmação. Com não há nenhuma definição padronizada, seja legalmente ou no ramo, do que é um *spyware*, qualquer desvio entre os produtos poderá ser intencional. Na pior das hipóteses, o fornecedor deve ter a oportunidade de corrigir versões futuras qualquer problema apresentado.

Conclusão

O mercado de anti-spyware se assemelha muito a como o mercado de antivírus era há dez anos. As oportunidades são grandes, mas os riscos também são. O mercado está começando a dar sinais de maturidade. A atividade legislativa e de fiscalização nos EUA e em outros países pode redefinir completamente o campo de jogo no médio prazo. E o comportamento das organizações que criam PUPs pode facilitar ou dificultar muito o trabalho da comunidade de segurança. Contudo, esse ambiente de mudanças frequentes e grandes riscos/prêmios é um ambiente ao qual a McAfee está muito acostumada.

Sobre a AVERT

A McAfee AVERT é uma das organizações de pesquisa antivírus e de vulnerabilidades mais respeitadas do mundo, empregando pesquisadores em 13 países dos cinco continentes. A McAfee AVERT combina o que há de melhor em pesquisa de programas mal intencionados e vírus com o conhecimento em pesquisas de prevenção de invasões e vulnerabilidades das organizações McAfee®

IntruShield®, McAfee® Enterccept® e McAfee® Foundstone® Professional Services. A McAfee AVERT protege os clientes, fornecendo as vacinas desenvolvidas por meio da combinação dos esforços dos pesquisadores da McAfee AVERT com a tecnologia AutoImmune, que aplica heurística avançada, detecção genérica e a tecnologia ActiveDAT para gerar vacinas contra vírus ainda não descobertos.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, www.mcafee.com

McAfee, AVERT, VirusScan e outras são marcas comerciais, registradas ou não, da McAfee, Inc. e/ou das suas afiliadas nos EUA e/ou em outros países. A cor vermelha usada em relação à segurança é marca distintiva dos produtos que levam a marca McAfee®. Todas as outras marcas comerciais, registradas ou não, mencionadas neste documento pertencem exclusivamente aos seus respectivos titulares. ©2004 Network Associates Technology, Inc. Todos os direitos reservados

6-sps-avecounting-001-0305