

**Estratégia para combate de pragas eletrônicas**  
Por André Fucs, CISSP

## **Introdução:**

Há algum tempo, prestávamos consultoria para uma grande empresa, cuja Política de Segurança praticamente inviabilizava o uso de notebooks de terceiros dentro de sua rede. Para não causar impactos no cronograma do projeto, decidimos utilizar as estações de trabalho da empresa ao invés de negociar o uso de nossos notebooks.

Ao preparar as estações de trabalho para receber informações sensíveis foram detectados nada mais do que três códigos maliciosos, sendo um vírus, um verme e um cavalo de tróia/back-door. Como recomendado pelo cliente, chamamos a equipe de suporte da empresa que rapidamente nos atendeu, passou o antivírus e nos entregou o micro para que pudéssemos recomeçar do zero a preparação do sistema operacional. Novamente, foram detectados os três códigos maliciosos.

O fenômeno até então desconhecido pela equipe de help-desk era na verdade uma infecção em grande escala de uma rede corporativa. Ao ignorar esse fato, o help-desk realizava as tarefas sem coordenação e conhecimento, cerca de 100% das máquinas desinfectadas foram novamente contaminadas em até 24 horas.

O objetivo desse documento é apresentar de forma introdutória as características de vermes, vírus de computador e cavalos de tróia assim como descrever os mecanismos de infecção mais comuns nos dias de hoje assim como apresentar estratégias de combate à proliferação desenfreada de pragas eletrônicas em redes de computador.

## **Códigos maliciosos**

### ***O que são***

São considerados códigos maliciosos qualquer código adicionado, modificado ou removido de um sistema com a intenção de dano ou enganar o funcionamento correto de um sistema.[MCGRAW01]. Sendo sub-classificados da seguinte forma:

- Vírus;
- Cavalos de Tróia;
- Vermes.

**Vírus** - São denominados assim aqueles programas que se anexa a, sobre-escreve ou substitui outro programa com objetivo de se reproduzir sem o conhecimento do usuário. [ACV01]

**Cavalos de tróia** – Termo que classifica programas que por trás de uma função aparentemente útil realizam ações maliciosas.

**Vermes** – Tipo de código malicioso que infecta sistemas através de redes de computador com o objetivo de executar ações pré-programadas e de se copiar em outras máquinas de uma rede.

Apesar dessas definições, nos últimos três anos o mercado de segurança acompanhou uma fusão dos códigos maliciosos. Não é raro hoje um dia um vírus fazer uso de técnicas tipicamente adotadas por vermes.

## **Formas de infecção**

Além dos mecanismos mais tradicionais tais como o Setor de Boot, macros e memória, três vetores são frequentemente encontrados em diferentes tipos de código malicioso:

- Correio eletrônico;
- Compartilhamento de arquivos;
- Falhas do sistema operacional.

Curiosamente enquanto os vírus antigos faziam uso de mecanismos extremamente complexos para se infectar, hoje em dia vários dos vermes e vírus fazem uso dos próprios recursos do sistema operacional. Surge portanto a necessidade de uma estratégia de combate de vírus que envolva o próprio sistema operacional e é esse justamente o ponto com o qual o suporte não contava.

Na história apresentada na introdução desse documento, os códigos maliciosos não estavam usando a conta de correio eletrônico para se infectar e sim um compartilhamento de arquivos do ambiente de rede Microsoft. Por desconhecer esse mecanismo de infecção o técnico do suporte executava uma limpeza com a última versão do anti-vírus e entregava a máquina ao usuário! Em nenhum momento o técnico demonstrou estar orientado à necessidade de identificar e remover compartilhamentos de disco presentes naquela estação de trabalho!

Essa seria apenas uma história de despreparo não fosse um motivo, o atendimento de usuários era uma atividade terceirizada, cujo contrato previa um número limitado de atendimentos com cobrança adicional para àqueles que estivessem acima da cota mensal pré-estabelecida. Tão ou mais assustador é o fato de que dezenas de funcionários perdiam praticamente seu dia de trabalho inteiro esperando a desinfecção do micro, isso quando não perdiam arquivos.

### **Estratégias de combate**

Sem dúvida alguma é interessante para o combate de pragas de computador que equipes de resposta à emergência, *CERT*, sejam criadas dentro da estrutura da empresa. Entretanto esse não será o tema desse documento.

#### ***Estratégia I – Prevenção***

Sem dúvida alguma a estratégia de mais longo prazo é a prevenção. Usuários, suporte e administradores devem ser alertados para os riscos de vírus de computador e mecanismos eficazes, em acordo com a política de segurança da empresa devem ser colocados em prática.

- **Desenvolva checklists para o suporte!** Muitos gestores de segurança reclamam do tamanho de suas equipes. Porque não usar outras equipes para executar trabalhos voltados à segurança da informação? Lembre-se incluir:
  - Análise e remoção de compartilhamento de redes Microsoft;
  - Análise e atualização sistema operacional;
  - Análise e atualização do sistema de antivírus do usuário;Se sua empresa possuir um mecanismo automatizado de gerenciamento de estações, boa parte dessa tarefa poderá ser feita remotamente!
- **Faça campanhas de conscientização.** Em geral usuários de informática gostam de receber treinamentos e orientação sobre vírus. Alerta-os sobre os perigos de abrir arquivos executáveis por correio eletrônico, compartilhar arquivos, etc.
- **Aplique a sua política de segurança na prática!** Tecnologia sem política de segurança não funciona, mas política de segurança sem tecnologia também não! Coloque em prática as definições de sua política de segurança. É verdade que em muitos casos o sistema operacional não será capaz de oferecer senhas fortes, inibir a modificação de arquivos de configuração mas o bom é inimigo do ótimo e esperar que as mudanças ocorram pode demorar demais.
- **Trabalhe em conjunto!** Segurança da Informação é um assunto em voga hoje em dia, mas muitas equipes ainda não estão preparadas para atuar nessa área da informática. Popularize seu conhecimento e traga para perto de você áreas como suporte e telecomunicações.

#### **Estratégia II – Reação**

Nem sempre a prevenção funciona e geralmente quando ela falha estamos completamente despreparados para o problema. Caso isso ocorra, calma. De nada adianta sair aplicando vacinas de antivírus se você ainda não sabe do que aquele vírus é capaz. Antes de tudo informe-se e procure descobrir quais os mecanismos de propagação da praga.

#### ***Correio Eletrônico***

No caso de pragas que se propagam exclusivamente através de correio eletrônico três passos devem ser seguidos:

1. Atualize o antivírus do servidor de correio eletrônico;
2. Execute processo de remoção do vírus;

3. Verifique se o sistema de email do usuário já foi atualizado e se as configurações de segurança do email do usuário são adequadas! Boa parte das pragas eletrônicas descobertas no último ano eram na verdade variações de pragas conhecidas que faziam uso de falhas do sistema de correio eletrônico!
4. Registre o incidente e apresente um breve relatório para sua equipe de suporte

#### **Compartilhamento de arquivos;**

Hoje em dia tornam-se cada vez mais comuns os vírus e vermes que fazem uso do compartilhamento de arquivos para infectar outros micros. Esses programas necessitam de maiores cuidados e sua capacidade de reprodução em redes corporativas é imensa. O motivo encontra-se no fato de que ao contrário das redes domésticas, as redes de grandes empresas possuem servidores de arquivos que nem sempre possuem antivírus e diversos ambientes de workgroup não autorizados. É relativamente comum encontrar nessas redes, grupos departamentais que fazem uso compartilhado de arquivos e impressoras. O uso inseguro de compartilhamentos é inclusive apontado como o quarto mais grave em ambientes Windows pelo FBI e pelo Sans Institute [SANS02].

Para combater a propagação de vírus e vermes que façam uso dessa forma de infecção, uma estratégia semelhante àqueles utilizadas por militares no combate faz-se necessária. É preciso isolar o inimigo suprimindo sua capacidade de fuga. Parece complicado mas é muito fácil de ser feito do que parece. A chave dessa estratégia está na compreensão da topologia da rede de sua empresa. É preciso segmentar, nem que temporariamente, partes da rede com o objetivo de enclausurar a praga. Filtros aplicados em equipamentos de rede tais como switches são uma boa opção. Uma vez identificados os focos já existentes os procedimentos tradicionais de combate a vírus podem ser aplicados.

1. Aplique a vacina na máquina infectada;
2. Verifique a atualização e estado do sistema operacional. É importante observar que alguns vírus de computador tais como o **W32/FLCSS** são capazes de corromper os mecanismos de segurança do sistema operacional.
3. Registre o incidente e apresente um breve relatório para sua equipe de suporte.

Nós da CFSEC Security Architects não acreditamos que soluções exclusivamente tecnológicas são capazes de resolver os problemas de Segurança da Informação. Sabemos que durante muitos anos investiu-se em tecnologia e gestão isoladamente. Com o passar do tempo ambas as opções demonstraram ser pouco eficientes na solução dos problemas existentes. No caso de vírus de computador e demais pragas digitais essa incapacidade de solucionar definitivamente os problemas torne-se ainda mais nítida.

Há mais de dez anos as empresas de antivírus afirmam que seus produtos são capazes de prever novas pragas e há mais de dez anos que se deve atualizar as bases de dados dos programas de antivírus diariamente. Apesar disso, esses sistemas realmente oferecem uma boa proteção aos usuários.

O que questionamos é até onde essa proteção vai sem a ação de um indivíduo capacitado e de uma boa estratégia de combate às pragas. Observamos que em setembro de 2001, uma entidade de análise e engenharia de tráfego conhecida como CAIDA registrou quase meio milhão de endereços IPs propagando o vírus Nimda. O assustador número é apenas uma pequena fração do problema real pois diversas das máquinas infectadas estavam dentro de ambiente corporativos, escondidos por firewalls e dispositivos de NAT.

Leve essa discussão para dentro de sua empresa e discuta com seus colegas a solução para esse problema dentro de seu ambiente de rede. Trabalhe em equipe e oriente as demais áreas da empresa. A Segurança da Informação não deve ser sinônimo de Auditoria de Sistemas. Definir critérios, mecanismos e procedimentos de proteção ao ambiente computacional de sua empresa são fundamentais para o sucesso de sua área!

**Bibliografia**

[MCGRAW01] <http://www.cigitallabs.com/resources/presentations/sans01/sld003.htm>

[ACV01] [http://www.bocklabs.wisc.edu/~janda/acv\\_faq.html](http://www.bocklabs.wisc.edu/~janda/acv_faq.html)

[SANS02] <http://www.sans.org/top20/#W4>

PROPIEDADES