Tech Info - 02

Vírus - Natureza e Actuação

Pluridata, Informática e Gestão, Lda.

Juntos trabalhamos melhor

JANEIRO / 2009
V.A.01.01

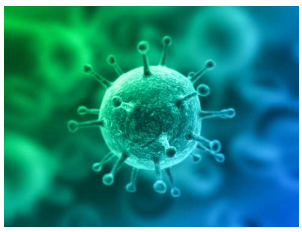
Vírus e spyware são talvez hoje em dia uma das causas mais frequentes de perturbações no funcionamento dos sistemas informáticos.

Procuramos neste memorando fazer uma descrição de natureza não excessivamente técnica dos seus tipos e mecanismos de funcionamento.

INTRODUCÇÃO

De acordo com a sua raiz etimológica latina, um vírus é um veneno. Na realidade, se observarmos os efeitos (por vezes devastadores) que um vírus informático pode causar num sistema, esta definição ajusta-se perfeitamente.

Os parasitas informáticos são chamados de vírus devido às semelhanças dos seus mecanismos de propagação com os dos vírus biológicos.



Diz-se que na origem do aparecimento dos vírus de computador esteve uma disputa entre programadores para criar programas que se assemelhassem a seres vivos.

Surgiram assim as aplicações que uma vez colocadas num ecossistema adequado (neste caso, o ambiente de trabalho de um computador) fossem capazes de multiplicar-se, crescerem e perpetuar-se.

De seguida, sabe-se que programadores manipularam um desses "seres", para que ultrapassasse o mero jogo em recintos fechados e se estendesse pelo mundo, com o fim de infectar sistemas alheios. Assim nasceram os vírus.

Os vírus de computador não passam de programas, tal como o Word ou o Photoshop, que em vez de terem sido criados para fazer algo útil, foram concebidos com o objectivo especifico de se propagarem em sistemas informáticos, podendo neste processo causar ou não danos aos dados e aplicações nos mesmos contidos.

Este tipo de programa apresenta-se normalmente oculto, dentro de outro programa, web page, ficheiro ou volume e executa-se automaticamente ao ser aberto, criando cópias de si mesmo dentro de outros programas e deste modo infectando-os. Esta capacidade de auto-cópia gera um efeito de propagação exponencial, que implica normalmente alterações no comportamento da máquina infectada.

OUTROS TIPOS DE VÍRUS

Os vírus propriamente ditos não estão sós, e têm alguns parentes próximos que podem causar tanto ou mais dano que eles mesmos: os worms (vermes), os trojans (troianos) , os backdoors e os spyware. Existem ainda vírus que combinam características destes tipos, e que são normalmente conhecidos como blended threats (ameaças combinadas).

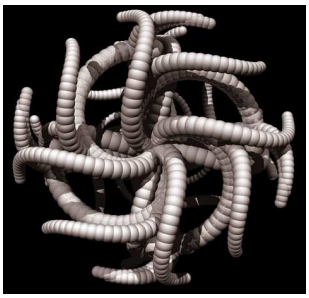
Soluções para a produtividade

Pluridata, Informática e Gestão, Lda.

R.da Eira, nº18,
Letra I/J
1495-050 Algés

Tel.: 214 121 294
Fax: 214 109 112
Email: marketing@pluridata.com
www.pluridata.com

Worms



Designa-se genericamente por worms uma família de vírus que se caracteriza principalmente por se multiplicarem por auto-cópia, não necessitando de infectar outros ficheiros para se reproduzir.

Os worms limitam-se, basicamente, a realizar cópias de si mesmos sem danificar nenhum outro ficheiro, mas reproduzem-se a uma velocidade tal que podem produzir um colapso devido à saturação das redes e ao esgotamento do espaço em disco disponível dos sistemas em que se infiltram. Transmitem-se muitas vezes através do e-mail, vindo escondidos dentro de um qualquer anexo executável.

Trojans

Um trojan ou troy horse é um tipo de vírus que normalmente se apresenta como disfarçado sob a forma de um qualquer utilitário de interesse, e que executa uma acção predeterminada ao ser executado pela primeira vez. Este tipo de acção pode ir desde a simples multiplicação do mesmo por envio por email à destruição dos dados existentes.

São conhecidas ainda situações que podem incluir acções tais como capturar todos os textos introduzidos pelo teclado ou registar as passwords introduzidas pelo utilizador.

Backdoors

Um backdoor é um programa que infecta o computador de maneira muitas vezes encoberta, e que muitas vezes não apresenta sintomas nem causa danos, directamente, ao sistema infectado. Aquilo que faz é estabelecer uma "porta das traseiras" através da qual é possível entrar no computador infectado e controla-lo remotamente e ainda utilizar os seus recursos.

Torna-se assim possível ao intruso, realizar acções tais como, a eliminação de ficheiros, a destruição do disco rígido, a captura e envio de dados confidenciais para um endereço electrónico externo ou o envio de spam.

Spyware

Spyware refere toda uma família de vírus cujo objectivo é transmitir, de forma encoberta e não dependendo de autorização especifica, informação sobre a utilização que é dada a um determinado sistema informático

A informação transmitida pode ir desde o histórico de páginas web visitadas à lista de contactos existente no programa de e-mail ou até ao histórico de transacções de compra e venda efectuados. O spyware é muitas vezes contraído por navegação na Internet em sites de conteúdo menos ortodoxo.

ESCONDERIJOS HABITUAIS DOS VÍRUS

Web pages: que por estarem escritas em determinadas linguagens de programação (HTML, Java, PHP, etc) podem conter elementos (applets, Java e ActiveX) que permitem aos vírus esconder-se. A infecção dá-se ao visitar a página.

E-mails: são o esconderijo preferido dos vírus, já que se tratam do meio de propagação mais rápido. Estas mensagens podem conter ficheiros infectados ou até produzir a infecção caso o utiliza-

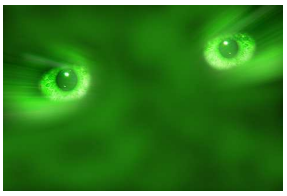
dor abra algum anexo que traga um vírus escondido.

A memória do computador: é onde se escondem os vírus e ameaças combinadas à espera que ocorra um evento que lhes determine que devem entrar em acção.

O sector de arranque: trata-se de uma área especial do disco rígido, em que está armazenada informação sobre as suas características e conteúdo. Os vírus, mais especificamente os de boot, alojam-se aqui para depois infectar o computador.

Os ficheiros com macros: as macros são pequenos programas que ajudam a realizar determinadas tarefas e estão incorporadas dentro de documentos Word, folhas de cálculo Excel ou apresentações PowerPoint. Por serem programas, as macros podem ser infectadas por vírus.

ATAQUES DE VÍRUS



Apenas um sistema completamente isolado que nunca troque informação com terceiros nem actualize aplicações existes está realmente a salvo.

Contudo as características actuais da utilização dos sistemas informáticos estão muito relacionadas com a comunicação e partilha de dados por interligação de sistemas, atributos sem os quais a sua utilidade seria muito reduzida.

A maior parte dos vírus não escolhe quem ataca, o seu comportamento é indiscriminado e afectam todos os sistema que podem, motivo pelo qual ninguém está isento de ser infectado.

ANATOMIA DE UM VÍRUS

- Multiplicação e Encobrimento;
- Ogiva, consiste numa "armadilha" ou código criado para causar danos no sistema infectado;
- Encriptação, um código adicional de mecanismos, de envio de e-mail e de encriptação, necessários para fazer "correr" a ogiva;
- Código Estranho, cujo único objectivo é tornar o ficheiro maior e mais difícil de analisar;
- SMTP (Protocolo de envio de e-mail).