**O que é um malware?**

O termo malware é proveniente do inglês e é a forma contraída para a expressão “malicious software” (software malicioso). Refere-se a qualquer software capaz de infectar um sistema secretamente.

Sem o conhecimento do usuário, esse software intencionalmente causa danos, alterações e, até mesmo, rouba informações suas e da sua empresa. Pode também bloquear o acesso do usuário ao sistema.

Malware é um temo usado para definir uma variedade de softwares hostis, sendo um código executável, scripts de conteúdo ativo, ou outros softwares.

**Contexto Histórico**

Frequentemente projetado visando lucro, o malware por vezes é utilizado contra sites do governo e de empresas para coletar informações importantes e bloquear acessos ao sistema, interrompendo a continuidade de operações e, consequentemente, do negócio.

Porém, o início dos ataques cibernéticos é marcado pela tentativa de hackers testarem suas habilidades contra sistemas diversificados, os quais eram vistos como um desafio a eles.

O acesso generalizado à internet permitiu a popularização desses delitos. E como consequência, existem muitos desenvolvedores de software black hat que prestam serviços em troca de grandes quantias de dinheiro.

A contratação desse “profissional” é feita tanto por agências de inteligência que desejam acessar informações sigilosas, quanto por organizações criminosas em busca de novos meios para atuarem no mundo digital.

No entanto, o malware é também usado contra pessoas físicas a fim de obter informações diversas – detalhes de identificação pessoal, números bancários ou de cartão de crédito e senhas.

**Tipos de malware**

**Vírus**

São *softwares*que se prendem a arquivos limpos e infectam outros arquivos limpos. Eles têm a capacidade de se espalhar descontroladamente, danificando funções centrais de um sistema e excluindo ou corrompendo arquivos diversos. Geralmente aparecem na forma de um arquivo executável.

### Adware

Programas responsáveis por exibirem propagandas e anúncios sem a permissão do usuário, de modo a deixar lento tanto o computador, quanto a conexão de rede existente, comumente assumindo o formato de pop-up, abrindo janelas indesejadas no seu navegador.

Mesmo não sendo essencialmente malignos, tratam-se de *softwares* de publicidade **especialmente agressivos** que minam a sua segurança ao oferecerem anúncios, essa oferta de anúncios funciona como porta de entrada para vários outros *malwares.*

### Cavalo de Tróia

Um *Troian Horse* se passa por um programa que **simula alguma funcionalidade útil**quando, na verdade, **esconde um programa que pode causar diversos malefícios** aos computadores e seus usuários.

Esse *software* malicioso possibilita invasões e roubo de informações do usuário. A principal forma de propagação ocorre pela internet, onde são oferecidos como ferramentas úteis ou vitais para seu sistema.

Ou seja, ele se disfarça de *software* legítimo ou está incluído em um *software* legítimo que foi violado. Age discretamente e cria “portas dos fundos” em sua segurança para permitir a entrada de outros *malwares*.

### Spyware

Como o próprio nome sugere, o *spyware* trata-se de um *malware* projetado para espionar e coletar informações.

Ele se esconde em segundo plano e guarda todas as informações daquilo que você faz online, desde senhas e números de cartões até hábitos de navegação, por exemplo.

São normalmente instalados através de falhas na segurança, as quais podem ser proporcionadas por *malwares* do tipo *adware*. Podendo ser embalados junto de um *software* instalado pelo usuário (aplicações *peer-to-peer*).

Logo, um *spyware* tem como objetivo **coletar informações sobre atividades realizadas no sistema da sua empresa**. Sendo aplicado como *software malicioso*, seu uso está aliado a práticas ilegais.

No entanto, existem empresas de anúncio que se aproveitam de *spywares* para entender o consumo realizado pelo seu público e, assim, selecionar que tipo de anúncio vai lhe apresentar.

Contudo, vale lembrar: um *spyware* não-prejudicial é instalado mediante a autorização do usuário. Enquanto a instalação de um *spyware* maligno ocorre sem que você ou outro usuário percebam.

Sendo assim, esse é mais um *malware* muitas vezes embutido em programas fornecidos oficialmente por empresas, principalmente através de *download*vindos de site com **aparência** útil ou atraente

Mas uma aplicação oculta de rastreamento vem inclusa a esse arquivo fornecido, a qual reúne estatísticas e informações diversas obtidas através do uso do sistema da sua organização.

### Worm

Essa categoria de *malware* **infecta redes inteiras de dispositivos** – locais ou online. Ele usa as interfaces de rede para isso, além de usar cada máquina infectada consecutiva para infectar outra.

Desde 2003, a maioria dos *worms*gerados são projetados para assumir o controle de computadores dos usuários para fins ilícitos.

Depois de infectados, os dispositivos são usados para enviar *spams*, hospedar dados de contrabando ou se engajar em ataques distribuídos de negação de serviço, como uma forma de extorsão.

### Ransomware

O *ransomware* é uma categoria de destaque da atualidade. Logo, sua compreensão é vital para entender o que é *malware* e o quão prejudicial ele é para seu negócio.

Originado do inglês, *ransom + malware*, o termo refere-se a um *software* malicioso baseado em cripto virologia e é conhecido também como vírus de resgate ou *scareware*.

Esse tipo de *malware* age de modo a sequestrar (ao criptografar) seus dados ou o controle do sistema da sua empresa, exigindo o pagamento de um resgate para recuperar essas informações.

O usuário sofre um ataque de extorsão criptoviral para que não tenha a publicação dos dados obtidos através do sequestro realizado no sistema de rede em questão.

Em suma, o *scareware*tem a capacidade de bloquear seu computador, além de ter total controle sob os dados existentes na rede referente a esse dispositivo.

### Botnet

*Malwares* do tipo *botnet* são redes de computadores as quais foram infectadas e que são forçadas a trabalharem juntos sob o controle de um *hacker* invasor.

### Backdoor

O *backdoor* é um *malware* que permite a um *hacker* comandar o computador de forma remota e executar determinada ações.

Alguns exemplos de consequências do ataque desse *software* malicioso é: download de outros *malwares*; envio de dados do usuário e *spams* e ataques de negação de serviço (*Denial of Service*).

Você pode ver que são muitos os modelos atuais em destaque, e o quão importante e fundamental é conhecê-los para, então, ter ciência sobre o que é*malware*e como agir mediante tais situações.