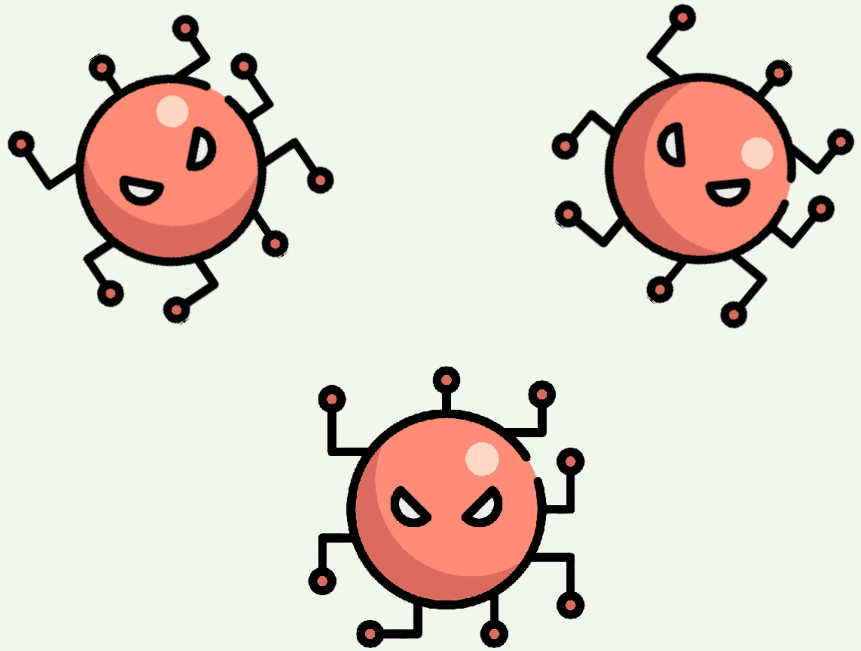
CÓDIGOS MALICIOSOS

* O que são
* Tipos Principais
* Cuidados a serem tomados



CÓDIGOS MALICIOSOS SÃO USADOS COMO INTERMEDIÁRIOS E POSSIBILITAM A PRÁTICA DE GOLPES, A REALIZAÇÃO DE ATAQUES E O ENVIO DE SPAM!!!

Também conhecidos como pragas e malware, códigos maliciosos são programas desenvolvidos para executar atividades danosas em equipamentos (computadores, roteadores, dispositivos móveis, switches, etc.).

Seus equipamentos podem ser infectados caso você:

>> acesse páginas web maliciosas

>> acesse mídias removíveis infectadas, como pen drives

>> execute arquivos infectados, obtidos em anexos de e-mail, páginas web, redes sociais ou diretamente de outros equipamentos

TIPOS PRINCIPAIS

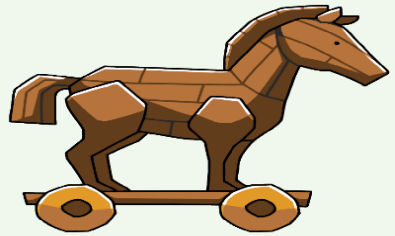
CÓDIGOS MALICIOSOS

VÍRUS

É um tipo de programa ou código malicioso criado para alterar a forma como um computador funciona. Atua fazendo cópias de se e inserindo-se a programas ou documentos legítimos a fim de executar seu código podendo danificar o sistema, corromper e destruir dados.

RANSOMWARE

É um tipo de malware de sequestro de dados, feito por meio de criptografia, que usa como refém, arquivos pessoais da própria vítima e cobra resgate para restabelecer o acesso a estes arquivos.

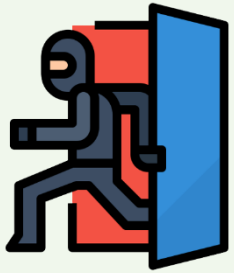


CAVALO DE TRÓIA (TROJAN)

Acessa seu dispositivo disfarçado de programa legítimo. Seu papel é possibilitar a abertura de uma "porta", de forma que usuários mal intencionados possam invadir seu computador.

Prefeitura de Manaus

CÓDIGOS MALICIOSOS

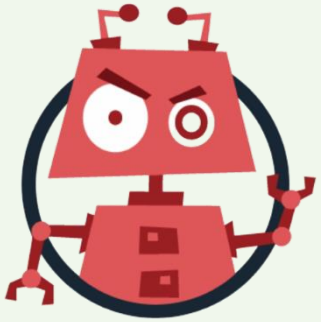


BACKDOOR

Programa que permite o retorno de um invasor a um equipamento comprometido, por meio de serviços criados ou modificados para este fim.

WORM

É um tipo de malware que se propaga rapidamente pela rede fazendo cópias de si mesmo com o objetivo de roubar dados do usuário ou de empresas.



BOT

Malware autopropagador, que infecta seu host e se conecta de volta a um servidor central, podendo ser controlado remotamente pelo invasor.

CÓDIGOS MALICIOSOS

SPYWARE

Malware destinado a infiltrar-se em um sistema para coletar informações pessoais de forma ilícita e encaminhar para uma entidade externa via internet para fins maliciosos.

KEYLOGGER

Programa criado para registrar as teclas pressionadas em um teclado, normalmente de maneira secreta para que a pessoa não saiba que suas ações estão sendo monitoradas.

SCREENLOGGER

Software capaz de armazenar a posição do mouse e da tela apresentada no monitor. A tela é capturada e salva como uma imagem ou vídeo, sendo enviada ao atacante.

Prefeitura de Manaus

CÓDIGOS MALICIOSOS

ADWARE

Programa de computador que executa automaticamente uma grande quantidade de anúncios sem a permissão do usuário.

ZUMBI

Equipamento infectado por um bot. Pode ser controlado remotamente sem o conhecimento do seu dono.

ROOTKIT

Pacote de software e técnicas malignas projetadas para oferecer acesso não autorizado à um computador e assegurar a presença do invasor.

CÓDIGOS MALICIOSOS

CUIDADOS A SEREM TOMADOS

CÓDIGOS MALICIOSOS

MANTENHA SEUS EQUIPAMENTOS ATUALIZADOS

>> Use apenas programas originais
>> Tenha sempre as versões mais recentes dos programas instalados
>> Instale todas as atualizações disponíveis, principalmente as de segurança
>> Crie um disco de recuperação e tenha-o por perto no caso de emergências

INSTALE UM ANTIVÍRUS (ANTIMALWARE)

>> Mantenha o antivírus atualizado
>> Configure o antivírus para verificar automaticamente qualquer extensão de arquivo, anexos de e-mails, discos rígidos e unidades removíveis
>> Verificar arquivos recebidos antes de executá-los
>> Evite o uso simultâneo de diferentes antivírus, pois podem afetar o desempenho do equipamento e afetar a capacidade de detecção
>> Crie um disco de emergência de seu antivírus: use-o se desconfiar que o antivírus esteja desabilitado ou que o comportamento do equipamento está estranho

USE UM FIREWALL PESSOAL

>> Assegure-se de ter um firewall pessoal instalado e ativo

AO INSTALAR APLICATIVOS

>> Baixe de fontes confiáveis
>> Escolha aplicativos bem avaliados e com grande quantidade de usuários
>> Verifique se as permissões de instalação e execução são coerentes

CÓDIGOS MALICIOSOS

FAÇA BACKUPS

>> Proteja seus dados fazendo backup regularmente
>> Nunca recupere um backup se desconfiar que ele contenha dados não confiáveis
>> Mantenha os backups desconectados do sistema

SEJA CUIDADOSO AO CLICLAR EM LINKS

>> Antes de acessar um link curto, procure usar complementos que permitam visualizar o link de destino
>> Não considere que as mensagens de conhecidos sejam sempre confiáveis

>> O campo do remetente de e-mail pode ter sido falsificado, ou
>> Elas podem ter sido enviadas de contas falsas ou invadidas

OUTROS

>> Use a conta de administrador apenas quando necessário
>> Cuidado com extensões ocultas
>> Desabilite a auto execução de mídias removíveis e de arquivos anexados

CÓDIGOS MALICIOSOS