**Logotipo

Descrição gerada automaticamente**

Serviço Nacional de Aprendizagem Industrial

SENAI “Gaspar Ricardo Junior”

Curso

TÉCNICO EM DESENVOLVIMENTODE SISTEMAS

*O que são malwares?*

GABRIELLA DEL vigna de moura

Julio cesar trigueiro filho

Natália oliveira martins dias

rafael oliveira senra

leandro Gaudio Rosa

VEDILSON DO PRADO DOS santos

Sorocaba

Abril – 2024

1. O que são malwares?

Malware, ou “software malicioso,” é um termo mais amplo que descreve qualquer programa ou código malicioso que seja prejudicial aos sistemas. Hostil, intrusivo e intencionalmente prejudicial, o malware invade, danifica ou desabilita computadores, sistemas de computador, redes, tablets e dispositivos móveis, geralmente assumindo o controle parcial das operações de um dispositivo. Assim como a gripe para os humanos, ele interfere no funcionamento normal

1. O que ele pode fazer?

Malware é uma maneira de ganhar dinheiro à sua custa de forma ilícita. Embora malware não possa danificar o hardware físico dos sistemas e equipamentos de rede, ele pode roubar, criptografar ou excluir seus dados, alterar ou sequestrar funções essenciais do computador e espionar a atividade de seu computador sem seu conhecimento ou permissão.

1. Como saber se houve uma infecção por malwares?

* Seu computador se torna mais lento. Um dos principais efeitos do malware é reduzir a velocidade de seu sistema operacional, seja ao navegar na Internet ou ao usar os aplicativos locais.
* Uma torrente de anúncios irritantes que não deveriam estar ali invadem sua tela. Anúncios em janelas pop-up inesperadas são um sinal típico de uma infecção por malware.
* Seu sistema desliga repetidamente, congela ou exibe BSOD (Tela Azul), o que pode ocorrer em sistemas Windows após um erro fatal.
* Você nota uma perda misteriosa de espaço em disco, provavelmente, causada por um malware invasor gigantesco que se oculta em seu disco rígido.

1. Tipos de malwares e como funcionam:

Temos oito tipos de malwares, que são:

O vírus: Este vírus geralmente vem como um anexos em um e-mail, e nele tem uma carga de vírus, ou parte do malware que executa uma ação maliciosa, depois que o usuário abre o arquivo o dispositivo está infectado.

Ransomware: Um dos mais convenientes, com isso, também o mais conhecido dos tipos de malware entre cibercriminosos é o ransomware. Esse malware se instala na máquina da vítima, criptografa seus arquivos e depois exige um resgate para o retorno dos dados do usuário, e o valor desse resgate geralmente é em Bitcoin.

Malware sem arquivo: É um tipo de software malicioso que usa programas autênticos para infectar o computador de um usuário, esse tipo de malware se torna difícil de detectar e remover já que, os ataques deles não deixam rastro de arquivos de malware a serem varridos ou processos mal-intencionados a serem detectados.

Worms: O tipo Worms não requer interação do usuário para funcionar, ele geralmente explora algum tipo de falha de segurança em um software ou sistema operacional, e com isso ele tem a capacidade de se copiar de máquina para máquina.

Cavalos de troia: Se trata de um malware que se disfarça ade um aplicativo inofensivo e desta forma, enganar o usuário para fazer o download e usarem o app. Ele age roubando dados pessoais, travam um dispositivo e espionam atividades.

Adware: Esses programas geralmente são instalados em troca de outro serviço, com o direito de usar um programa sem pagar por isso, o adware enviam anúncios indesejados aos usuários e geralmente exibem anúncios chamativos quando você executa uma determinada ação.

Scareware: Perante um golpe de scareware, você ira ver uma mensagem pop-up alarmante enquanto navega pela web com alguma mensagem informando que você tem algum vírus na máquina, fazendo com que pensemos que nosso computador estejam infectados, para convencer o alvo a comprar um aplicativo falso.

Spyware: É um software instalado sem que o usuário possa saber da presença dele, seja em um computador tradicional, um aplicativo no navegador ou aplicativo que reside em seu dispositivo. O spyware transmite suas informações pessoais, e confidenciais para o invasor.

1. Como se propagam:

Eles se podem através de arquivos corrompidos, além de oferecer arquivos infectados, que parecem legítimos, os criadores de Malwares usam outra técnica bem semelhante: contaminam programas “legítimos” com vírus. Dessa forma, colocam em sites de download da Internet uma versão de um aplicativo conhecido (o compactador Winrar, por exemplo), dizendo que é uma versão “especial” gratuita. Quando o programa é instalado, o Malware é instalado também.

1. Problemas do malware:

Atualmente, práticas de segurança rigorosas e recursos de proteção mais eficientes estão limitando consideravelmente as atividades dos malwares, embora este seja um problema longe de um fim. Em um passado não muito distante, algumas dessas pragas se destacaram tanto que "entraram para a história". Eis algumas delas:

\*Melissa: criado em 1999

\*ILOVEYOU: criado em 2000

\*Code Red: criado em 2001

\*MyDoom: lançado em 2004

1. Impactos e consequências:

O malware pode ter um impacto significativo, tanto em pessoas físicas quanto em empresas. Para pessoas físicas, o malware pode levar à perda de dados e roubo de identidade. Entretanto, também pode resultar em perdas financeiras se você for enganado a pagar por um resgate depois que seus arquivos forem criptografados pelo ransomware.

BIBLIOGRAFIA

[**https://www.mcafee.com/pt-br/antivirus/malware.html**](https://www.mcafee.com/pt-br/antivirus/malware.html)> Acessado em: 02/05/2024.

<https://br.malwarebytes.com/malware/> > Acessado em: 02/05/2024

<https://www.kaspersky.com.br/resource-center/threats/spyware> > Acessado em: 02/05/2024

<https://www.veritas.com/pt/br/information-center/malware> > Acessado em:

02/05/2024

<https://www.avast.com/pt-br/c-malware> > Acessado em: 02/05/2024