1.Vírus e Worms

Assim como um vírus biológico, um vírus de computador tem a capacidade de se replicar e se espalhar de um sistema para outro. No entanto, para que um vírus seja ativado, geralmente é necessário que um usuário realize alguma ação, como clicar em um link ou executar um arquivo infectado. Uma vez ativado, ele pode se espalhar pelo sistema de arquivos do computador e até mesmo para outros dispositivos conectados à rede. Os vírus são frequentemente associados a falhas e paralisações do sistema, mas alguns podem operar silenciosamente em segundo plano sem que o usuário perceba.

Devido à ameaça que representam, os vírus são uma preocupação constante para os usuários e, por isso, a maioria dos sistemas operacionais modernos já inclui softwares antivírus. Essas soluções de segurança monitoram continuamente os arquivos e processos em execução, buscando padrões que indiquem a presença de malware. Para serem eficazes, os antivírus dependem de **assinaturas**, que são bases de dados contendo informações sobre vírus já conhecidos. É fundamental manter essas assinaturas sempre atualizadas para garantir a detecção de novas ameaças.

Os vírus podem assumir diversas formas. Alguns requerem a execução de um programa infectado, enquanto outros atacam o setor de inicialização do sistema, sendo ativados assim que o computador é ligado. Além disso, certos vírus exploram scripts executados por navegadores e sistemas operacionais, enquanto outros utilizam macros de softwares como o Microsoft Office para disseminar códigos maliciosos. Uma variante particularmente perigosa é o **vírus fileless, que não grava arquivos infectados no disco rígido. Em vez disso, ele opera inteiramente na memória RAM, dificultando sua detecção por antivírus tradicionais**.

O processo de infecção por um *vírus fileless* geralmente começa quando um usuário clica em um link malicioso em um e-mail ou em um site comprometido. O ataque pode explorar vulnerabilidades conhecidas em softwares como Flash, Java ou no próprio sistema operacional. Assim que o vírus é executado, ele pode utilizar ferramentas legítimas do próprio sistema, como o PowerShell, para baixar e executar novos scripts maliciosos diretamente na memória. Como esse tipo de vírus não cria arquivos físicos, ele pode evitar muitas das proteções baseadas em análise de disco e assinaturas de malware.

Além dos vírus tradicionais, existem os **worms**, **que se diferenciam por não exigirem interação do usuário para se propagarem. Eles são projetados para se replicar automaticamente e infectar o maior número possível de dispositivos conectados à rede**. Como a maioria dos sistemas modernos está constantemente conectada à internet, os worms podem se espalhar rapidamente, explorando vulnerabilidades sem a necessidade de ações diretas dos usuários.

Um exemplo famoso desse tipo de ataque foi o **WannaCry**, um worm que se espalhou mundialmente em 2017, explorando uma falha no protocolo SMB do Windows. Após infectar um computador, o WannaCry procurava automaticamente outros dispositivos vulneráveis na mesma rede e repetia o processo. Além disso, ele não apenas se replicava, mas também instalava ransomware, criptografando arquivos do usuário e exigindo pagamento para restaurá-los. Esse ataque demonstrou como worms podem ser devastadores quando combinados com outras formas de malware.

A melhor defesa contra vírus e worms é manter o sistema operacional e os aplicativos sempre atualizados, garantindo que as vulnerabilidades conhecidas sejam corrigidas antes que possam ser exploradas por atacantes. Além disso, firewalls, sistemas de prevenção contra intrusões e backups regulares de arquivos são fundamentais para reduzir os danos em caso de infecção. Como novas ameaças surgem constantemente, a segurança digital exige uma abordagem proativa para minimizar os riscos e proteger os dados contra ataques cibernéticos.

2.Vírus - Extras

Um ***vírus*** é um tipo de malware que se espalha inserindo uma cópia de si mesmo em outro programa. Depois que o programa é executado, os vírus se espalham de um computador para o outro. A grande maioria requer ajuda humana para se espalhar e eles podem se instalar na primeira linha de código em um arquivo executável.

Quando ativado, o vírus pode verificar o disco em busca de outros executáveis para que ele possa infectar todos os arquivos que ainda não foram infectados. Eles podem ser inofensivos ou destrutivos, além de serem programados para evitar a detecção. O simples ato de abrir um arquivo pode ativar um vírus. Uma vez ativado, o programa normalmente afetará outros programas no computador ou outros computadores da rede.

3.Worms - Extras

Worms de computadores são semelhantes aos vírus porque se replicam e podem causar o mesmo tipo de dano, porém, eles exploram vulnerabilidades nas redes de forma independente e podem retardá-las à medida que se espalham de sistema para sistema. Enquanto um vírus requer ação humana, worms tem ações independentes e ainda nos dias de hoje representam ameaças persistentes. Geralmente se instalam usando um mecanismo de exploração como um anexo de e-mail, arquivo executável ou cavalo de Tróia. Eles habilitam uma vulnerabilidade, uma maneira de se propagar e todos contêm uma carga (*payload*).