Exploits

Um exploit geralmente é uma sequência de comandos, dados ou uma parte de um software elaborados por hackers que conseguem tirar proveito de um defeito ou vulnerabilidade. O objetivo, neste caso, é causar um comportamento acidental ou imprevisto na execução de um software ou hardware, tanto em computadores quanto em outros aparelhos eletrônicos.

Para fins maléficos, um exploit pode dar a um cracker o controle de um sistema de computador, permitindo a execução de determinados processos por meio de acesso não autorizado a sistemas, ou ainda realizar um ataque de negação de serviço.

Diferente de outros meios de disseminação de vírus e ataques cibernéticos, um exploit não precisa que o usuário clique em um determinado link ou faça o download para a execução de algum arquivo. Por isso, os exploits são armas perigosas nas mãos de hackers mal intencionados.

Com a evolução dos computadores e dos sistemas de proteção, os hackers que utilizam exploits de maneira ilegal também desenvolveram novos métodos e diferentes ferramentas tornando processos que antes eram considerados seguros em obsoletos. Em informática, exploits e vulnerabilidades possuem exatamente o mesmo significado que no mundo real. Porém há dificuldades na definição de como uma vulnerabilidade específica aparece e o que os utilizadores realmente podem fazer para explorá-la.

Muitas vezes as vulnerabilidades são provenientes de erros na etapa de desenvolvimento de um produto. Em outros casos, já acontecem de maneira proposital para dar margem a um acesso secundário ao sistema depois que ele tenha sido lançado aos usuários. Contudo, um exploit pode ser utilizado de maneira legal para que um [hacker](https://canaltech.com.br/hacker/O-que-e-um-Hacker/) tenha acesso a uma determinada parte do produto.

São conhecidos como exploits também os comandos responsáveis por burlar o uso limitado de softwares, conhecidos mais popularmente como cracks.

Os exploits são classificados geralmente pelo tipo de vulnerabilidade que exploram, pela necessidade de serem executados na mesma máquina que o programa que tem a vulnerabilidade e através do resultado da execução do exploit (EoP, DoS, spooting e outros).

Os métodos para tentar evitar o contágio de exploits em seu computador são praticamente os mesmos para evitar os vírus mais comuns. É imprescindível possuir um bom antivírus e que ele e o sistema operacional do seu computador estejam sempre atualizados. Um firewall competente também ajudará muito nesta tarefa.

## 

## PRINCIPAIS VÍRUS DE COMPUTADOR

Na atualidade, os vírus se dividem em várias categorias e cada uma apresenta diferentes objetivos e formas de ataques. Veja a seguir alguns em destaque!

### KEYLOGGER

Os keyloggers são softwares de computador que visam monitorar, armazenar e enviar tudo o que foi digitado pela vítima para um terceiro. Nos dias de hoje, os keyloggers são inseridos em outros códigos prejudiciais como os trojans, que têm o objetivo de acessar dados bancários.

### ADWARE

O adware é qualquer programa cuja função é executar automaticamente e exibir um grande volume de anúncios, sem que o usuário tenha dado a devida permissão.

### BACKDOOR

É um mecanismo usado por vários malwares para promover acesso remoto a softwares ou à rede infectada. Esse programa busca explorar falhas problemáticas não documentadas em aplicações instaladas, desatualizadas e do firewall para ter acesso às [portas do roteador](https://blog.intnet.com.br/saiba-agora-o-que-e-virus-no-roteador-e-como-e-possivel-evitar/).

### BROWSER HIJACKER

Trata-se de um tipo de vírus de computador que tem por meta a mudança das principais configurações do navegador. Quando instalado, modifica a homepage e as formas de busca. Demonstram anúncios em páginas legítimas e redirecionam o usuário para sites maliciosos que podem apresentar exploits ou outras [pragas digitais](https://blog.intnet.com.br/o-que-deixa-a-sua-internet-lenta-confira-7-motivos-e-saiba-como-dribla-los/).

### TROJAN HORSES

Os Cavalos de Troia mantêm-se ocultos enquanto baixam e instalam ameaças em computadores e laptops. São conhecidos por responder pelo primeiro estágio de infecção de dispositivos digitais. Eles aparecem em mensagens de e-mail, arquivos de música, sites maliciosos, entre outros.

Além disso, esse tipo de vírus se aproveita de vulnerabilidades presentes no navegador para instalar softwares maliciosos no computador.

### ROOTKIT

Rootkit são trojans que usam mecanismos avançados de programação para serem instalados em classes profundas ou não documentadas do [sistema operacional](https://blog.intnet.com.br/saiba-o-que-e-e-como-proteger-seu-computador-contra-malware/). As suas funções mais devastadoras são: a sua capacidade de recuperação, reinstalando-se mesmo depois da limpeza do computador; e sua disseminação em alta velocidade.

### SPYWARE

Esse tipo de software apresenta a característica de espionagem e visa captar dados sobre os costumes dos usuários na [internet](https://blog.intnet.com.br/o-que-e-o-ping-e-como-ele-afeta-sua-conexao-com-a-internet/), com o objetivo de distribuir propaganda “customizada”.

### TIME BOMB

O Time Bomb é um tipo de malware que apresenta contagem regressiva. Ele é uma ameaça preordenada para ser executada em uma certa ocasião no sistema operacional, provocando sérios danos.

### WORM

Esse tipo de vírus de computador apresenta a função de se autorreplicar sem a necessidade de infectar arquivos legítimos, produzindo cópias funcionais de si mesmo. Tais características fazem com que os worms se espalhem rapidamente por redes de computadores e drives USB.

Além disso, eles podem ser repassados por mensagens de e-mail, criando anexos problemáticos e os enviando para as listas de contato da conta invadida.

### GREYWARE

É um malware que se encontra na chamada zona cinzenta, entre o software normal e um vírus, provocando mais irritação do que problemas, como programas de piada e adware. Assim, o Greyware refere-se a uma ampla gama de softwares que são instalados sem a permissão do usuário.

### JOKE PROGRAM

Tratam-se de mecanismos ou códigos criados para provocar danos temporários ao sistema operacional, como travamentos e alterações inesperadas de comportamento. Os códigos dessa natureza não causam nenhum dano real ao computador.

### MACROS

Os Macros são uma série de comandos coagidos que podem ser configurados em programas como Word e Excel. Desse modo, vários documentos com instruções prejudiciais podem ser criados, atingindo outros dados ou executando planos prejudiciais toda vez que eles forem realizados. Em sua grande parte, a ação é feita ao abrir ou fechar um documento dessa extensão.

### RANSOMWARE

São códigos maliciosos que retêm arquivos ou todo o sistema do usuário por meio de técnicas de criptografia. Após o “sequestro”, o malware apresenta mensagens exigindo o depósito de uma certa quantia ou a compra de alguma mercadoria, informando que em seguida fará o envio da senha que libera os arquivos. Contudo, mesmo depois do pagamento, o usuário não recebe senha alguma.

### TROJAN BANKING

É o trojan caracterizado pelo acesso a dados bancários, redes sociais, sites de compras e servidores de e-mail. As formas utilizadas são as mesmas de um trojan comum, sendo partilhado como um software ou arquivo legítimo, em sites infectados ou e-mails.