# Artefatos Maliciosos: Malwares - Forense Computacional - Ataques de Buffer Overflow - Ataques de Denial of Service



## Segurança da Informação

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### O que é malware?

Malware é um termo genérico para qualquer tipo de software malicioso projetado para prejudicar ou explorar qualquer dispositivo, serviço ou rede programável. Os criminosos cibernéticos costumam usá-lo para extrair dados que podem ser utilizados das vítimas para obter ganhos financeiros. Eles vão de dados financeiros, registros médicos a e-mails e senhas pessoais - as possibilidades de que tipo de informação pode ser comprometida se tornaram infinitas.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Por que os cibercriminosos usam malware?

Malware abrange todos os tipos de softwares maliciosos, incluindo vírus, e cibercriminosos o usam por muitas razões, tais como:

- Enganar a vítima para que forneça dados pessoais para roubo de identidade
- Roubar dados do cartão de crédito do consumidor ou outros dados financeiros
- Assumir controle de múltiplos computadores para lançar ataques de negação de serviço contra outras redes
- Infectar computadores e usá -los para minar bitcoin ou outros moedas virtuais

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Como o malware se espalha?

Desde o seu nascimento há mais de 30 anos, malware encontrou vários métodos de ataque. Eles incluem anexos de e-mail, anúncios maliciosos em sites populares (malvertising), instalações falsas de software, unidades USB infectadas, aplicativos infectados, e-mails de phishing e até mensagens de texto.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Tipos de malware?

Infelizmente, há um monte de malwares por aí, mas a compreensão dos diferentes tipos de malware é uma maneira de ajudar a proteger seus dados e dispositivos:

- **Vírus**

  Um vírus geralmente vem como um anexo em um e-mail que contém uma carga de vírus, ou parte do malware que executa a ação maliciosa. Depois que a vítima abre o arquivo, o dispositivo está infectado.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Tipos de malware?

- **Ransomware**

  Um dos mais rentáveis e, portanto, mais populares, tipos de malware entre os cibercriminosos é o ransomware. Esse malware se instala na máquina da vítima, criptografa seus arquivos e depois exige um resgate (geralmente em Bitcoin) para retornar esses dados ao usuário.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Tipos de malware?

- **Scareware**

  Os cibercriminosos nos fazem com que pensemos que nossos computadores ou smartphones foram infectados para convencer as vítimas a comprar um aplicativo falso. Em um golpe típico de scareware, você pode ver uma mensagem pop-up alarmante enquanto navega na Web com a mensagem "Aviso: seu computador está infectado!" ou "Você tem um vírus!" Os criminosos cibernéticos usam esses programas e práticas de publicidade antiéticas para assustar os usuários na compra de aplicativos não autorizados.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Tipos de malware?

- **Worms**

  Worms têm a capacidade de se copiar de máquina para máquina, geralmente explorando algum tipo de falha de segurança em um software ou sistema operacional e não exigem interação do usuário para funcionar.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Tipos de malware?

- **Spyware**

  Spyware é um programa instalado no seu computador, normalmente sem o seu conhecimento explícito, que captura e transmite informações pessoais ou de navegação na Internet hábitos e detalhes para o usuário. O Spyware permite que seus usuários monitorem todas as formas de comunicações no dispositivo alvo. O spyware é frequentemente usado pelas autoridades policiais, órgãos governamentais e organizações de segurança da informação para testar e monitorar as comunicações em um ambiente sensível ou em uma investigação. Mas spyware também está disponível para consumidores, permitindo que compradores espionem seus cônjuges, filhos e funcionários.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Tipos de malware?

- **Cavalos de troia**

  Os cavalos de troia se disfarçam de aplicativos inofensivos, enganando os usuários para que façam o download e os usem. Uma vez em funcionamento, eles podem roubar dados pessoais, travar um dispositivo, espionar atividades ou até mesmo iniciar um ataque.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Tipos de malware?

- **Adware**

  Os programas de adware enviam anúncios indesejados aos usuários e geralmente exibem anúncios piscantes ou janelas pop-up quando você executa uma determinada ação. Os programas de adware geralmente são instalados em troca de outro serviço, como o direito de usar um programa sem pagar por isso.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Tipos de malware?

- **Malware sem arquivo**

O malware sem arquivo é um tipo de software malicioso que usa programas legítimos para infectar um computador. Os ataques de registro de malware não deixam rastros de arquivos de malware a serem varridos ou processos maliciosos a serem detectados. Ele não depende de arquivos e não deixa pegadas, tornando difícil detectá-lo e removê-lo.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Como sei que fui infectado por malware?

Os sinais mais comuns de que seu computador foi comprometido por malware são:

- Desempenho lento do computador;
- O navegador o redireciona ou quando o seu navegador leva você a sites que você não pretendia visitar;
- Avisos de infecção acompanhados de solicitações para comprar algo para corrigir o problema;

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Como sei que fui infectado por malware?

- Problemas ao desligar ou iniciar o computador;
- Anúncios pop-up frequentes;
- Quanto mais sintomas comuns você notar, maior a probabilidade do seu computador ter uma infecção por malware. Redirecionamentos no navegador e um grande número de avisos pop-up afirmando que você tem um vírus são os indicadores mais fortes de que seu computador foi comprometido.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Como posso me proteger de malware?

Embora existam muitos tipos de malware por aí, a boa notícia é que existem muitas maneiras de se proteger contra malware. Confira estas dicas:

**Proteja seus dispositivos**

- Mantenha seu sistema operacional e aplicativos atualizados. Os criminosos cibernéticos procuram vulnerabilidades em softwares antigos ou desatualizados, portanto, instale as atualizações assim que elas estiverem disponíveis.

- Nunca clique em um link em um pop-up. Simplesmente feche a mensagem clicando em "X" no canto superior e saia do site que a gerou.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

## Como posso me proteger de malware?

**Proteja seus dispositivos**

- Limite o número de aplicativos em seus dispositivos. Instale apenas os aplicativos que você acha que precisa e que usará regularmente. E se você não usar mais um aplicativo, desinstale-o.

- Use uma solução de segurança móvel, disponível para Android e iOS. À medida que as campanhas de malware e adware continuam infectando aplicativos móveis, verifique se seus dispositivos móveis estão preparados para qualquer ameaça que ocorra.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

## Como posso me proteger de malware?

**Proteja seus dispositivos**

- Não empreste seu telefone ou deixe os seus dispositivos sem vigilância por motivo nenhum , e não se esqueça de verificar as configurações e os aplicativos. Se as configurações padrão foram alteradas ou um novo aplicativo apareceu misteriosamente, isso pode ser um sinal de que o spyware foi instalado.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

## Como posso me proteger de malware?

**Seja cuidadoso online**

- Evite clicar em links desconhecidos. Seja por e-mail, site de rede social ou mensagem de texto, se um link parecer estranho, não clique nele.

- Seja seletivo sobre os sites que você visita. Faça o seu melhor para usar apenas sites conhecidos e confiáveis, bem como usando um plug-in de pesquisa segura, para evitar quaisquer sites que podem ser maliciosos sem o seu conhecimento.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

## Como posso me proteger de malware?

**Seja cuidadoso online**

- Cuidado com e-mails solicitando informações pessoais. Se um e-mail parecer vir do seu banco e instruir você a clicar em um link e redefinir sua senha ou acessar sua conta, não clique nele. Vá diretamente para o seu site de banco online e inicie a sessão.

- Evite sites de risco, como os que oferecem protetores de tela gratuitos.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

## Como posso me proteger de malware?

**Seja cuidadoso online**

- Cuidado com e-mails solicitando informações pessoais. Se um e-mail parecer vir do seu banco e instruir você a clicar em um link e redefinir sua senha ou acessar sua conta, não clique nele. Vá diretamente para o seu site de banco online e inicie a sessão.

- Evite sites de risco, como os que oferecem protetores de tela gratuitos.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

## Como posso me proteger de malware?

**Preste atenção aos downloads e outras compras de software**

- Compre apenas software de segurança de empresas respeitáveis através do site oficial ou em uma loja de varejo.

- Atenha-se às lojas oficiais de aplicativos. Embora o spyware possa ser encontrado em lojas oficiais de aplicativos, eles prosperam em lojas obscuras de terceiros que promovem aplicativos não oficiais. Ao fazer o download de aplicativos para dispositivos com jailbreak, você ignora a segurança interna e essencialmente coloca os dados do dispositivo nas mãos de um estranho.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

## Como posso me proteger de malware?

**Preste atenção aos downloads e outras compras de software**

- Ao procurar seu próximo aplicativo favorito, faça o download apenas de algo que seja verificado. Leia as resenhas de aplicativos, utilize apenas lojas oficiais de aplicativos e, se algo soar vagamente suspeito, não faça download.

- Não abra um anexo de e-mail, a menos que saiba o que é, mesmo que seja de um amigo ou de alguém que você conheça.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

## Como posso me proteger de malware?

**Realize verificações regulares**

- Se você está preocupado com a possibilidade de seu dispositivo estar infectado, execute uma varredura usando o software de segurança que você instalou no seu dispositivo.

- Verifique suas contas bancárias e relatórios de crédito regularmente.

Com essas dicas e alguns softwares de segurança confiáveis, você estará no caminho certo para proteger seus dados e dispositivos de todos os tipos de malware.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### O que é computação forense?

A forense da computação, também conhecida como forenses digitais, ciência forense da computação ou forenses cibernéticos, combina a ciência da computação e forenses legais para coletar evidências digitais de maneira admissível em um tribunal de justiça.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### O que é computação forense?

Da mesma forma que os agentes da lei examinam cenas de crime em busca de pistas, os investigadores de computação forense procuram em dispositivos digitais por evidências que os advogados podem utilizar em investigações criminais, casos civis, investigações de cibercrimes e outras questões relacionadas à segurança corporativa e nacional. E, tal como os seus homólogos policiais, os investigadores de computação forense têm de ser especialistas não só na procura de provas digitais, mas também na recolha, manuseamento e tratamento para garantir a sua fidelidade e a sua admissibilidade em tribunal.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### O que é computação forense?

A computação forense está intimamente relacionada à cibersegurança. As descobertas da computação forense podem ajudar as equipes de cibersegurança a acelerar a detecção e a resolução de ameaças cibernéticas e a evitar futuros ataques cibernéticos. Uma disciplina emergente de cibersegurança, forense digital e resposta a incidentes (DFIR), integra forenses de computação e atividades de resposta a incidentes para acelerar a correção de ameaças cibernéticas, ao mesmo tempo em que garante que qualquer evidência digital relacionada não seja comprometida.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Como a computação forense evoluiu

A computação forense ganhou destaque pela primeira vez no início da década de 80 com a invenção do computador pessoal. Com a tecnologia tornando-se um elemento essencial na vida cotidiana, criminosos identificaram uma abertura e passaram a cometer crimes em dispositivos eletrônicos.

Logo em seguida, a internet conectou quase todos durante a noite, permitindo o acesso remoto e por e-mail a redes de computadores corporativas e organizacionais e abrindo portas para malware e ataques cibernéticos. Em resposta a essa nova fronteira de crime cibernético, as agências de segurança pública precisavam de um sistema para investigar e analisar dados eletrônicos e, portanto, nasceu a computação forense.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Como a computação forense evoluiu

Por exemplo, considere um acidente de carro. No passado, os policiais podem ter investigado a cena do crime em busca de evidências físicas, como marcas de desvio ou vidros estilhaçados; eles também podem ter verificado os telefones dos motoristas em busca de evidências de mensagens de texto enquanto dirigiam.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Como a computação forense evoluiu

Atualmente, os automóveis mais recentes geram e armazenam dados digitais e metadados que criam um registro detalhado da localização, velocidade e condição operacional de cada veículo a qualquer momento. Esses dados transformam os veículos modernos em ferramentas forenses poderosas adicionais, permitindo que os investigadores reconstruam eventos que antecederam, ocorreram durante e sucederam a um acidente; esses dados podem até mesmo ajudar a determinar quem foi responsável pelo acidente, mesmo na ausência de evidências físicas ou testemunhas oculares tradicionais.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Por que a computação forense é importante

Assim como as evidências físicas da cena do crime, as evidências digitais devem ser coletadas e tratadas corretamente. Caso contrário, os dados e metadados poderão ser perdidos ou considerados inadmissíveis em um tribunal.

Por exemplo, os investigadores e os procuradores têm de demonstrar uma cadeia de custódia adequada para as provas digitais – têm de documentar a forma como estas foram tratadas, processadas e armazenadas. E têm de saber como recolher e armazenar os dados sem os alterar – um desafio dado que ações aparentemente inofensivas, como abrir, imprimir ou guardar ficheiros, podem alterar os metadados permanentemente.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Por que a computação forense é importante

Por esse motivo, a maioria das organizações contrata investigadores de computação forense (também conhecidos pelas funções de especialista em computação forense, analista de computação forense ou examinador de computação forense) para coletar e lidar com evidências digitais associadas a investigações criminais ou criminosas cibernéticas.

Profissionais de informática geralmente têm um diploma de bacharel em ciência da computação ou justiça criminal, e combinam um sólido conhecimento funcional dos fundamentos de tecnologia da informação (TI) — por exemplo, sistemas operacionais, segurança da informação, segurança da rede, linguagens de programação — além de uma experiência nas implicações legais de evidências digitais e crime cibernético. Alguns podem se especializar em áreas como forenses móveis ou forenses do sistema operacional.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Como funciona a computação forense

Existem quatro etapas principais na computação forense.

- **Identificação de dispositivo**

  A primeira etapa é identificar os dispositivos ou mídia de armazenamento que podem conter dados, metadados ou outros artefatos digitais relevantes para a investigação. Esses dispositivos são coletados e colocados em um laboratório forense ou em outra instalação segura para seguir o protocolo e ajudar a garantir a recuperação adequada dos dados.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Como funciona a computação forense

- **Preservação de dados**

Especialistas forenses criam uma imagem, ou cópia bit a bit dos dados a serem preservados. Em seguida, armazenam com segurança a imagem e o original para protegê-los de serem alterados ou destruídos.

Especialistas coletam dois tipos de dados: dados persistentes armazenados no disco rígido local de um dispositivo e dados voláteis localizados na memória ou em trânsito (por exemplo, registros, cache e memória de acesso aleatório (RAM). Os dados voláteis devem ser manuseados com atenção, pois são efêmeros e podem ser perdidos se o dispositivo desligar ou perder energia.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Como funciona a computação forense

- **Análise forense**

  Em seguida, os investigadores forenses analisam a imagem para identificar evidências digitais relevantes. Isso pode incluir arquivos excluídos intencionalmente ou não, histórico de navegação na internet, e-mails e muito mais.

  Para descobrir dados "ocultos" ou metadados que outros podem perder, os investigadores usam técnicas especializadas, incluindo análise em tempo real, que avalia sistemas ainda em execução em busca de dados voláteis, e esteganografia reversa, que expõe dados ocultos usando esteganografia, uma técnica para ocultar informações confidenciais em mensagens comuns.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Casos de uso de forenses digitais

Existem várias áreas em que organizações ou autoridades policiais podem iniciar uma investigação forense digital:

- **Investigações criminais:** agências de segurança pública e especialistas em forenses de informática podem usar forenses de informática para resolver crimes relacionados ao computador, como cyberbullying, hackers ou roubo de identidade, bem como crimes no mundo físico, incluindo roubo, sequestro, assassinato e muito mais. Por exemplo, as autoridades policiais podem usar computação forense em um computador pessoal de um suspeito de assassinato para localizar possíveis pistas ou evidências ocultas em seus históricos de pesquisa ou arquivos excluídos.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Casos de uso de forenses digitais

Existem várias áreas em que organizações ou autoridades policiais podem iniciar uma investigação forense digital:

- **Investigações criminais:** agências de segurança pública e especialistas em forenses de informática podem usar forenses de informática para resolver crimes relacionados ao computador, como cyberbullying, hackers ou roubo de identidade, bem como crimes no mundo físico, incluindo roubo, sequestro, assassinato e muito mais. Por exemplo, as autoridades policiais podem usar computação forense em um computador pessoal de um suspeito de assassinato para localizar possíveis pistas ou evidências ocultas em seus históricos de pesquisa ou arquivos excluídos.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Casos de uso de forenses digitais

- **Processo judicial civil:** os investigadores também podem usar computação forense em casos de litígios civis, como fraude, disputas de emprego ou divórcios. Por exemplo, em um caso de divórcio, a equipe jurídica de um cônjuge pode usar computação forense em um dispositivo móvel para revelar a infidelidade de um parceiro e receber uma decisão mais favorável.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Casos de uso de forenses digitais

- **A proteção da propriedade intelectual:** A computação forense pode ajudar as autoridades policiais a investigar roubo de propriedade intelectual, como roubo de segredos comerciais ou material protegido por direitos autorais. Alguns dos casos de computação forense de maior destaque envolvem a proteção de propriedade intelectual, especialmente quando funcionários que estão saindo roubam informações confidenciais para vendê-las a outra organização ou estabelecer uma empresa concorrente.Ao analisar evidências digitais, os investigadores podem identificar quem roubou a propriedade intelectual e responsabilizá-la.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Casos de uso de forenses digitais

- **Segurança corporativa:** As empresas costumam usar a computação forense após um ataque cibernético, como uma violação de dados ou dados ou um ataque de ransomware, para identificar o que aconteceu e corrigir quaisquer vulnerabilidades de segurança. Um exemplo típico seria o de hackers que rompem uma vulnerabilidade no firewall de uma empresa para roubar dados confidenciais ou essenciais. O uso da computação forense para combater ataques cibernéticos continuará, à medida que os crimes cibernéticos continuam aumentando. Em 2022, o FBI estimou que os crimes de computador custaram aos americanos US$ 10,3 bilhões em perdas anuais, um aumento de US$ 6,9 bilhões em relação ao ano anterior.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Casos de uso de forenses digitais

- **Segurança nacional:** A computação forense tornou-se uma importante ferramenta de segurança nacional à medida que os crimes cibernéticos continuam aumentando entre as nações. Governos ou agências de aplicação da lei, como o FBI, agora usam técnicas de computação forense após ataques cibernéticos para descobrir evidências e reforçar vulnerabilidades de segurança.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Computação forense, cibersegurança e DFIR

Novamente, computação forense e cibersegurança são disciplinas estreitamente relacionadas que muitas vezes colaboram na proteção das redes digitais contra ataques cibernéticos. A cibersegurança abrange aspectos tanto proativos quanto reativos, enfocando a prevenção e detecção de ciberataques, além da resposta e correção a esses ataques cibernéticos.

A forense informática é quase totalmente reativa, entrando em ação no caso de um ataque cibernético ou crime. Mas investigações forenses de computação muitas vezes apresentam informações valiosas que as equipes de cibersegurança podem usar para evitar futuros ataques cibernéticos.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### DFIR: Computação forense + Resposta a incidentes

Quando os dados da computação forense e a resposta a incidentes, a detecção e mitigação de ataques cibernéticos em andamento, são conduzidos de forma independente, eles podem interferir uns com os outros, com resultados negativos para uma organização.

As equipes de resposta a incidentes podem modificar ou destruir evidências digitais enquanto eliminam uma ameaça da rede. Os investigadores forenses podem atrasar a resolução da ameaça enquanto perseguem e coletam evidências.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### DFIR: Computação forense + Resposta a incidentes

A computação forense digital e a resposta a incidentes, ou DFIR (Digital Forensics and Incident Response), combinam a computação forense e a resposta a incidentes em um fluxo de trabalho integrado que pode auxiliar as equipes de segurança a interromper ameaças cibernéticas de maneira mais rápida, ao mesmo tempo em que preservam evidências digitais que podem ser perdidas na urgência da mitigação de ameaças.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### DFIR: Computação forense + Resposta a incidentes

Em DFIR,

- A coleta de dados forenses ocorre juntamente com a mitigação de ameaças. As equipes de resposta a incidentes usam técnicas de computação forense para coletar e preservar dados enquanto contêm e erradicam a ameaça, garantindo que a cadeia de custódia adequada seja seguida e que evidências valiosas não sejam alteradas ou destruídas.

- A revisão pós-incidente inclui o exame de evidências digitais. Além de preservar evidências para ações legais, as equipes de DFIR as utilizam para reconstruir incidentes de cibersegurança do início ao fim, a fim de compreender o que ocorreu, como ocorreu, a extensão dos danos e como ataques semelhantes podem ser evitados.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### DFIR: Computação forense + Resposta a incidentes

A DFIR pode levar a uma atenuação mais rápida das ameaças, a uma recuperação mais robusta das ameaças e a evidências aprimoradas para a investigação de casos criminais, crimes cibernéticos, reclamações de seguros e muito mais.

# Segurança da Informação

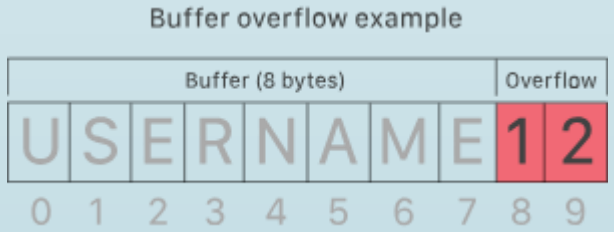
## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### O que é estouro de buffer?

O estouro de buffer é uma anomalia que ocorre quando o software gravando dados em um buffer estoura a capacidade do buffer, resultando na substituição de locais de memória adjacentes. Em outras palavras, muita informação está sendo passada para um container que não tem espaço suficiente e essa informação acaba substituindo os dados em containers adjacentes.

Os estouros de buffer podem ser explorados por invasores com o objetivo de modificar a memória de um computador para prejudicar ou assumir o controle da execução do programa.



# Segurança da Informação

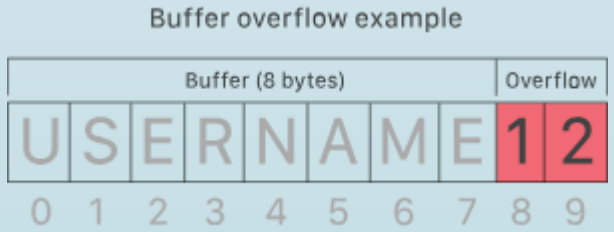
## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### O que é estouro de buffer?

O estouro de buffer é uma anomalia que ocorre quando o software gravando dados em um buffer estoura a capacidade do buffer, resultando na substituição de locais de memória adjacentes. Em outras palavras, muita informação está sendo passada para um container que não tem espaço suficiente e essa informação acaba substituindo os dados em containers adjacentes.

Os estouros de buffer podem ser explorados por invasores com o objetivo de modificar a memória de um computador para prejudicar ou assumir o controle da execução do programa.



# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### O que é um buffer?

Um buffer, ou buffer de dados, é uma área de armazenamento de memória física usada para armazenar dados temporariamente enquanto está sendo movida de um lugar para outro. Estes buffers normalmente vivem na memória RAM. Os computadores geralmente usam buffers para ajudar a melhorar a performance; a maioria dos discos rígidos modernos aproveitam o buffer para acessar dados de forma eficiente e muitos serviços on-line também usam buffers. Por exemplo, os buffers são geralmente utilizados em streaming de vídeos on-line para evitar a interrupção. Quando um vídeo é transmitido, o reprodutor de vídeo baixa e armazena, talvez, 20% do vídeo de cada vez em um buffer e depois transmite a partir desse buffer. Desta forma, pequenas quedas na velocidade da conexão ou interrupções rápidas de serviço não afetarão a performance do streaming de vídeo.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### O que é um buffer?

Os buffers são projetados para conter quantidades específicas de dados. A menos que o programa que utiliza o buffer tenha instruções incorporadas para descartar o excesso de dados enviados para o buffer, o programa substituirá os dados na memória adjacente ao buffer.

Estouros de buffer podem ser explorados por invasores para corromper software. Apesar de bem compreendidos, os ataques de estouro de buffer ainda são um grande problema de segurança que atormenta as equipes de segurança cibernética. Em 2014, uma ameaça conhecida como "heartbleed" expôs centenas de milhões de usuários a ataques devido a uma vulnerabilidade de estouro de buffer em software de SSL.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Como os invasores exploram os estouros de buffer?

Um invasor pode alimentar deliberadamente uma entrada cuidadosamente elaborada em um programa que fará com que o programa tente armazenar essa entrada em um buffer que não seja grande o suficiente, substituindo porções de memória conectadas ao espaço do buffer. Se o layout de memória do programa for bem definido, o invasor poderá sobrescrever deliberadamente áreas conhecidas por conterem código executável. O invasor pode então substituir esse código por seu próprio código executável, o que pode alterar drasticamente a forma como o programa foi projetado para funcionar.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Como os invasores exploram os estouros de buffer?

Por exemplo, se a parte sobrescrita na memória contiver um ponteiro (um objeto que aponta para outro local na memória), o código do invasor pode substituir esse código por outro ponteiro que aponta para uma carga de exploração. Isso pode transferir o controle de todo o programa para o código do invasor.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Como se proteger contra ataques de estouro de buffer

Felizmente, os sistemas operacionais modernos têm proteções de tempo de execução que ajudam a mitigar os ataques de estouro de buffer. Vamos explorar duas proteções comuns que ajudam a mitigar o risco de exploração:

- **Aleatorização do espaço de endereço** - reorganiza aleatoriamente os locais do espaço de endereço das principais áreas de dados de um processo. Os ataques de estouro de buffer geralmente dependem do conhecimento da localização exata do código executável importante, a aleatoriedade dos espaços de endereço torna isso quase impossível.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Como se proteger contra ataques de estouro de buffer

- **Prevenção de execução de dados** - Marca certas áreas da memória como executáveis ou não executáveis, evitando que uma exploração execute código encontrado em uma área não executável.

Os desenvolvedores de software também podem tomar precauções contra vulnerabilidades de estouro de buffer escrevendo em linguagens que tenham proteções internas ou usando procedimentos de segurança especiais em seu código.

Apesar das precauções, novas vulnerabilidades de estouro de buffer continuam a ser descobertas pelos desenvolvedores, às vezes após uma exploração bem-sucedida.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Quais são os diferentes tipos de ataques de estouro de buffer?

Existem vários ataques de estouro de buffer que empregam estratégias diferentes e visam diferentes partes de código. Abaixo estão alguns dos mais conhecidos.

- **Ataque de stack overflow -** Este é o tipo mais comum de ataque de estouro de buffer e envolve o estouro de um buffer na pilha de chamadas*.

- **Ataque de heap overflow -** Este tipo de ataque tem como alvo dados no pool de memória aberto conhecido como heap*.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Quais são os diferentes tipos de ataques de estouro de buffer?

- **Ataque de estouro de número inteiro** - Em um estouro de número inteiro, uma operação aritmética resulta em um integer (número inteiro) que é muito grande para o tipo de número inteiro destinado a armazená-lo; isso pode resultar em um estouro de buffer.

- **Unicode overflow** - Um unicode overflow cria um estouro de buffer inserindo caracteres unicode em uma entrada que espera caracteres ASCII. (ASCII e unicode são padrões de codificação que permitem que os computadores representem texto. Por exemplo, a letra "a" é representada pelo número 97 em ASCII. Enquanto os códigos ASCII cobrem apenas caracteres de idiomas ocidentais, o unicode pode criar caracteres para quase todos os idiomas escritos na Terra Como há muito mais caracteres disponíveis em unicode, muitos caracteres unicode são maiores que o maior caractere ASCII).

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Quais são os diferentes tipos de ataques de estouro de buffer?

** Os computadores contam com dois modelos de alocação de memória diferentes, conhecidos como pilha e heap; ambos vivem na RAM do computador. A pilha é bem organizada e contém dados em um modelo Last-In, First-Out. Qualquer que seja o dado que foi colocado mais recentemente na pilha será o primeiro a sair, mais ou menos como a última bala inserida em um pente de munição será a primeira a ser disparada. O heap é um conjunto desorganizado de memória extra, os dados não entram ou saem do heap em nenhuma ordem específica. Como acessar a memória a partir da pilha é muito mais rápido do que acessar a partir do heap, o heap geralmente é reservado para dados maiores ou dados que um programador deseja gerenciar explicitamente.*

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### O que é um ataque de negação de serviço?

Um ataque de negação de serviço (DoS) é um tipo de ataque cibernético em que um ator malicioso tem por objetivo tornar um computador ou outro dispositivo indisponível para os usuários a que se destinam, interrompendo o funcionamento normal do dispositivo. Os ataques DoS normalmente funcionam sobrecarregando ou inundando uma máquina visada com solicitações até que o tráfego normal não possa ser processado, resultando em negação de serviço para usuários adicionais. Um ataque DoS caracteriza-se pelo uso de um único computador para lançar o ataque.

Um ataque distribuído de negação de serviço (DDoS) é um tipo de ataque DoS que se origina em muitas fontes distribuídas, tais como um ataque DDoS de botnet.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

## Como funciona o ataque DDoS?

O foco principal de um ataque DDoS é saturar em excesso a capacidade de uma máquina visada, resultando em uma negação de serviço para pedidos adicionais. Os vários vetores de ataque dos ataques DoS podem ser agrupados por suas semelhanças.

Os ataques DoS normalmente se enquadram em duas categorias:

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

## Como funciona o ataque DDoS?

**Ataques de estouro de buffer**

Um tipo de ataque em que um estouro de buffer de memória pode fazer com que uma máquina consuma todo o espaço, memória ou tempo de CPU disponível no disco rígido. Essa forma de uso indevido frequentemente acarreta comportamento lento, falhas no sistema ou outros comportamentos prejudiciais do servidor, resultando em negação de serviço.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

## Como funciona o ataque DDoS?

**Ataques de inundação**

Ao saturar um servidor visado com uma enorme quantidade de pacotes, um ator malicioso pode saturar demais a capacidade do servidor, resultando em negação de serviço. Para que a maioria dos ataques de inundação DoS tenha sucesso, o ator malicioso deve ter mais largura de banda disponível do que o alvo.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

## Quais são alguns dos ataques DoS historicamente significativos?

Historicamente, os ataques DoS normalmente exploravam as vulnerabilidades de segurança presentes no projeto da rede, do software e do hardware. Esses ataques se tornaram menos predominantes, pois os ataques DDoS têm maior capacidade disruptiva e são relativamente fáceis de criar, devido às ferramentas disponíveis. Na realidade, a maioria dos ataques DoS também pode ser transformada em ataques DDoS.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

## Quais são alguns dos ataques DoS historicamente significativos?

Alguns ataques históricos comuns de DoS incluem:

- **Ataque Smurf** - um ataque DoS previamente explorado no qual um ator malicioso utiliza o endereço de broadcast da rede vulnerável enviando pacotes falsificados, resultando na inundação de um endereço de IP visado.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

## Quais são alguns dos ataques DoS historicamente significativos?

- **Inundação Ping** - esse ataque simples de negação de serviço baseia-se em sobrecarregar um alvo com pacotes ICMP (ping). Ao inundar um alvo com mais pings do que ele é capaz de responder com eficiência, pode ocorrer a negação de serviço. Esse ataque também pode ser usado como um ataque DDoS.

- **Ping da Morte** - muitas vezes confundido com um ataque de inundação ping, um ataque de ping da morte envolve o envio de um pacote malformado para uma máquina visada, resultando em comportamento prejudicial, como falhas do sistema.

# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

## Como é possível saber se um computador está sofrendo um ataque DoS?

Embora possa ser difícil separar um ataque de outros erros de conectividade de rede ou de consumo intenso de largura de banda, algumas características podem indicar que um ataque está em andamento.

Os indicadores de um ataque DoS incluem:

- Desempenho de rede atipicamente lento, como longos tempos de carregamento de arquivos ou sites
- Incapacidade de carregar um determinado site, como a sua propriedade da web
- Uma súbita perda de conectividade em dispositivos da mesma rede

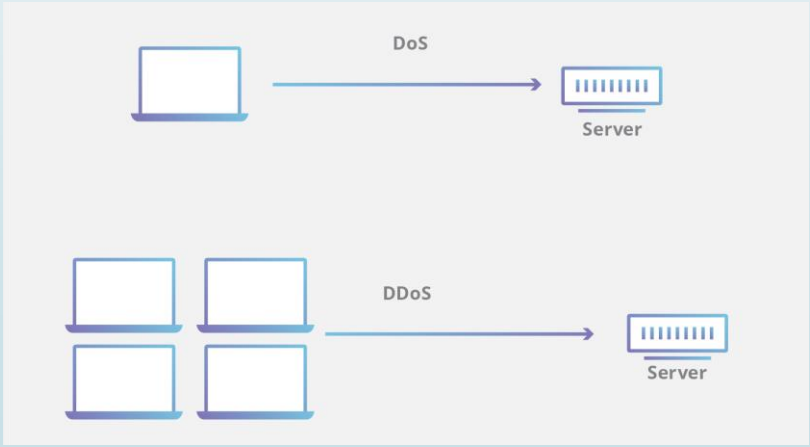
# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Qual é a diferença entre um ataque DDoS e um ataque DOS?

A diferença entre DDoS e DoS é o número de conexões utilizadas no ataque. Alguns ataques DoS, tais como o “low and slow" ou ataques como Slowloris, obtêm seu poder da simplicidade e dos requisitos mínimos necessários para que sejam eficazes.



# Segurança da Informação

## Malwares - Forense Computacional

## Ataques de Buffer Overflow - Ataques de Denial of Service

### Qual é a diferença entre um ataque DDoS e um ataque DOS?

O ataque DoS utiliza uma única conexão, enquanto um ataque DDoS utiliza muitas fontes de tráfego de ataque, muitas vezes na forma de uma botnet. De modo geral, muitos dos ataques são essencialmente similares e podem ser tentados usando mais uma das muitas fontes de tráfego malicioso.

# Referências


- **McAfee**

  https://www.mcafee.com/pt-br/antivirus/malware.html#:~:text=Malware%20é%20um%20termo%20genérico,vítimas%20para%20obter%20ganhos%20financeiros

- **IBM**

  https://www.ibm.com/br-pt/topics/computer-forensics

- **Cloudfire**

  https://www.cloudflare.com/pt-br/learning/security/threats/buffer-overflow/

  https://www.cloudflare.com/pt-br/learning/ddos/glossary/denial-of-service/