

INTRODUÇÃO À FORENSE COMPUTACIONAL



Mariana Emerenciano

UFERN
UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

PROGRAD
PRÓ-REITORIA DE GRADUAÇÃO






SUMÁRIO

Conceitos iniciais e legislação

- 1 Introdução – forense;
- 2 Linha do tempo;
- 3 Legislação brasileira;
- 4 Conceitos básicos;

Ataques, investigação e evidências

- 5 Principais ataques;
 - 6 Etapas da investigação;
 - 7 Lidando com evidências;
 - 8 Boas práticas.
- 

INTRODUÇÃO

O que é ciência forense?

- Forensis: latim, “de antes do fórum”;
- "A aplicação dos princípios das ciências físicas ao direito na busca da verdade em questões cíveis, criminais e de comportamento social para que não sejam cometidas injustiças contra qualquer membro da sociedade" (Manual de Patologia Forense do Colégio de Patologistas Americanos, 1990).

INTRODUÇÃO



O que é forense computacional?

Forense computacional é a preservação, identificação, extração, interpretação e documentação de evidências computacionais, para incluir processos legais, integridade da evidência, relato dos dados encontrados e a opinião de um especialista num tribunal ou em outros processos legais e/ou administrativos.

LINHA DO TEMPO: CASOS INICIAIS ATÉ A LEGISLAÇÃO BRASILEIRA

1984



CART E SUPORTE AO
FBI EM BUSCA DE
EVIDÊNCIAS
COMPUTACIONAIS

LINHA DO TEMPO: CASOS INICIAIS ATÉ A LEGISLAÇÃO BRASILEIRA

1984



CART E SUPORTE AO
FBI EM BUSCA DE
EVIDÊNCIAS
COMPUTACIONAIS

1986

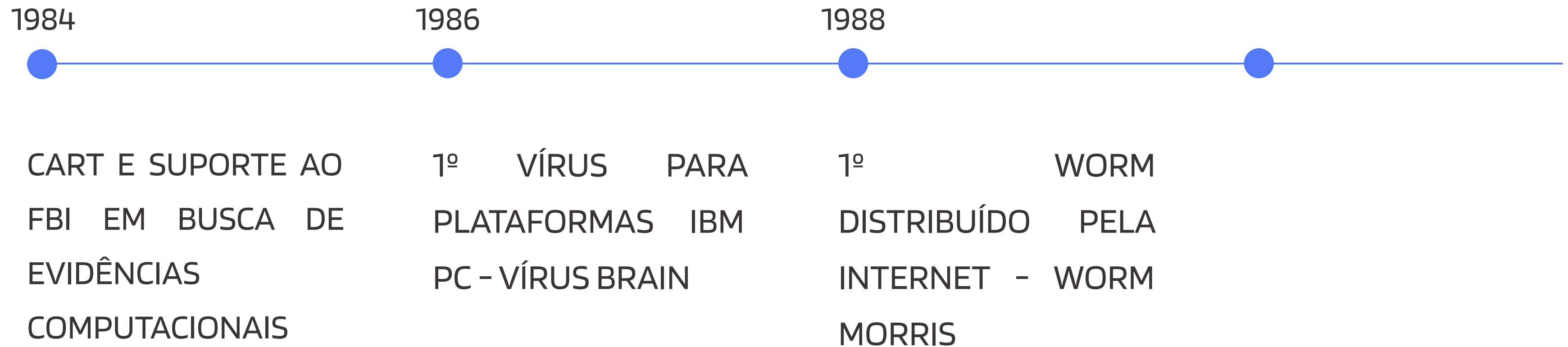


1º VÍRUS PARA
PLATAFORMAS IBM
PC - VÍRUS BRAIN

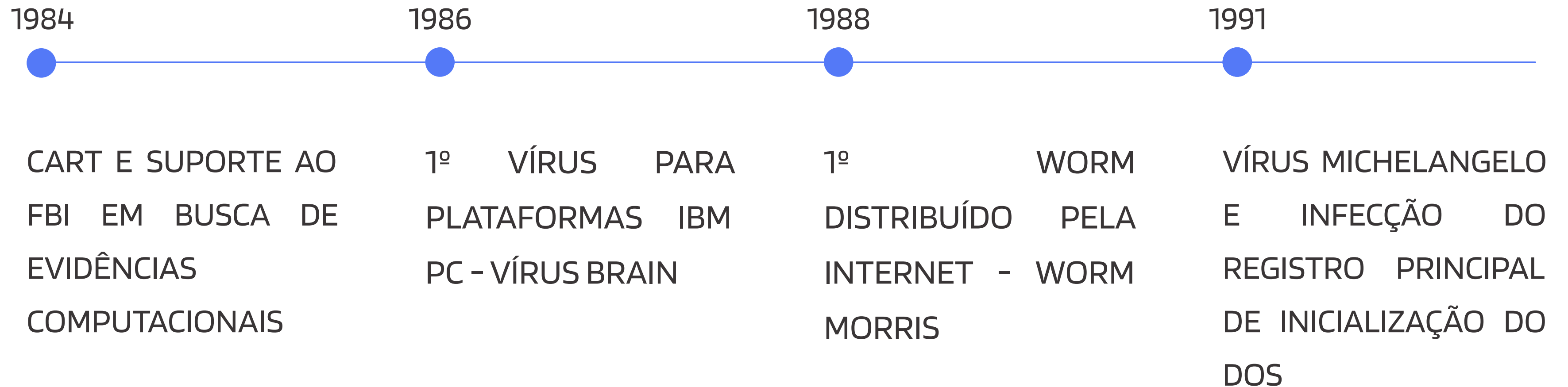


LINHA DO TEMPO:

CASOS INICIAIS ATÉ A LEGISLAÇÃO BRASILEIRA



LINHA DO TEMPO: CASOS INICIAIS ATÉ A LEGISLAÇÃO BRASILEIRA



LINHA DO TEMPO: CASOS INICIAIS ATÉ A LEGISLAÇÃO BRASILEIRA

1993



1ª CONFERÊNCIA
INTERNACIONAL
SOBRE EVIDÊNCIA
COMPUTACIONAL

LINHA DO TEMPO: CASOS INICIAIS ATÉ A LEGISLAÇÃO BRASILEIRA

1993



1ª CONFERÊNCIA
INTERNACIONAL
SOBRE EVIDÊNCIA
COMPUTACIONAL

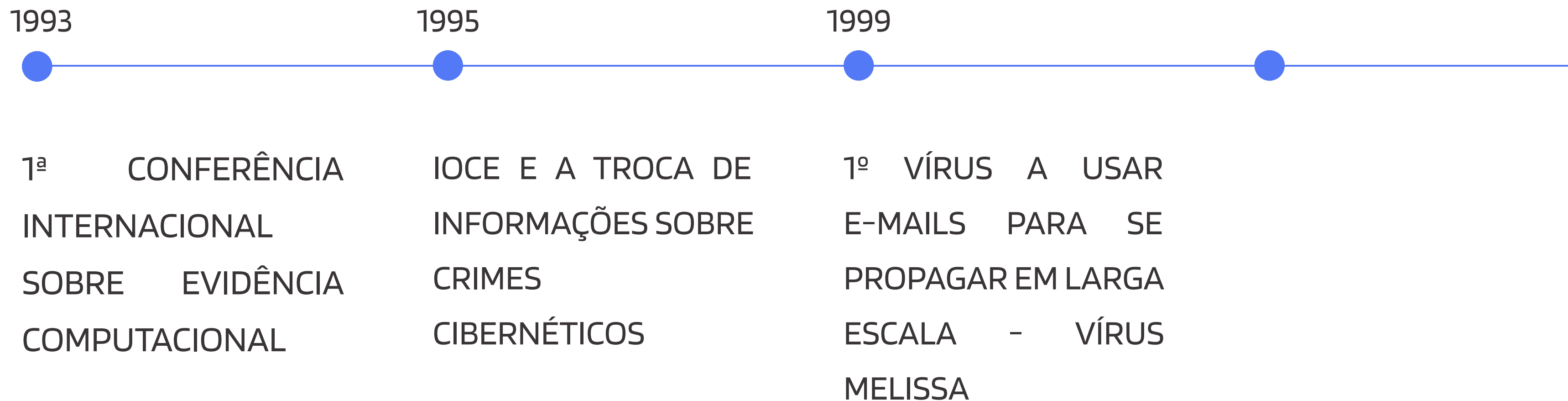
1995



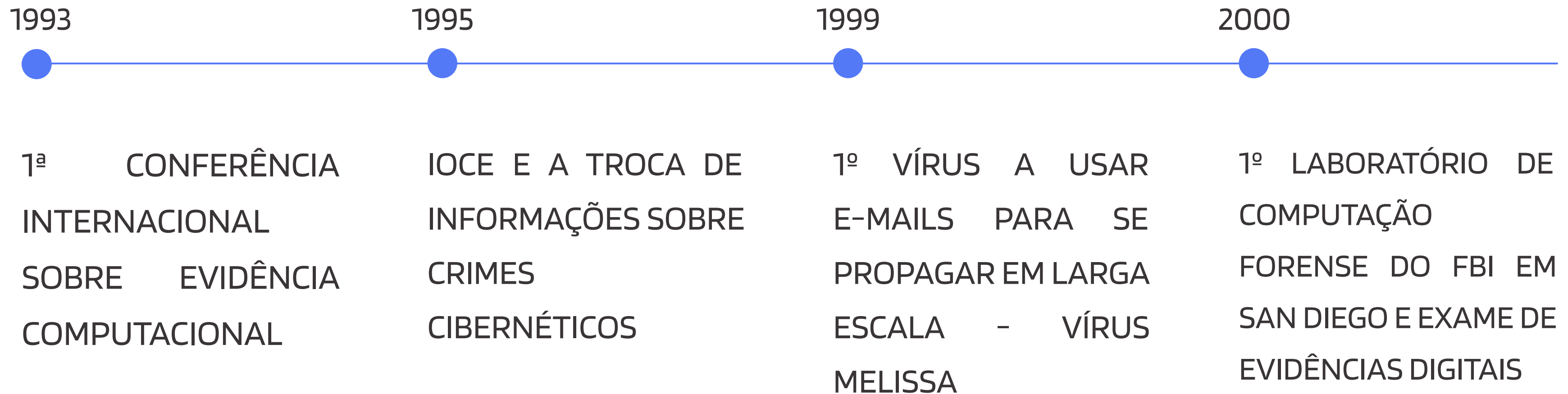
IOCE E A TROCA DE
INFORMAÇÕES SOBRE
CRIMES
CIBERNÉTICOS



LINHA DO TEMPO: CASOS INICIAIS ATÉ A LEGISLAÇÃO BRASILEIRA



LINHA DO TEMPO: CASOS INICIAIS ATÉ A LEGISLAÇÃO BRASILEIRA



LINHA DO TEMPO: CASOS INICIAIS ATÉ A LEGISLAÇÃO BRASILEIRA

2000



WORM LOVELETTER
E PROPAGAÇÃO 15x
MAIS RÁPIDA QUE O
VÍRUS MELISSA

LINHA DO TEMPO: CASOS INICIAIS ATÉ A LEGISLAÇÃO BRASILEIRA

2000



WORM LOVELETTER
E PROPAGAÇÃO 15x
MAIS RÁPIDA QUE O
VÍRUS MELISSA

2008



WORM CONFICKER E
SEUS IMPACTOS NO
MINISTÉRIO DE
DEFESA DO REINO
UNIDO

LINHA DO TEMPO: CASOS INICIAIS ATÉ A LEGISLAÇÃO BRASILEIRA

2000



WORM LOVELETTER
E PROPAGAÇÃO 15x
MAIS RÁPIDA QUE O
VÍRUS MELISSA

2008



WORM CONFICKER E
SEUS IMPACTOS NO
MINISTÉRIO DE
DEFESA DO REINO
UNIDO

2011



HACKER INVADE E
DIVULGA FOTOS
ÍNTIMAS DE CAROLINA
DIECKMANN

LEGISLAÇÃO DE CRIMES CIBERNÉTICOS NO BRASIL

Lei Carolina Dieckmann

Esta lei promoveu alterações no Código Penal Brasileiro, tipificando os delitos informáticos.

LEGISLAÇÃO DE CRIMES CIBERNÉTICOS NO BRASIL

Lei Carolina Dieckmann

Esta lei promoveu alterações no Código Penal Brasileiro, tipificando os delitos informáticos.

Lei Marco Civil da Internet

O Marco Civil da Internet disciplina o uso da internet no Brasil, por meio de direitos e deveres para quem faz uso da rede.

LEGISLAÇÃO DE CRIMES CIBERNÉTICOS NO BRASIL

Lei Carolina Dieckmann

Esta lei promoveu alterações no Código Penal Brasileiro, tipificando os delitos informáticos.

Lei Marco Civil da Internet

O Marco Civil da Internet disciplina o uso da internet no Brasil, por meio de direitos e deveres para quem faz uso da rede.

Lei Geral de Proteção de Dados (LGPD)

A LGPD é a legislação que regula as atividades de tratamento de dados pessoais, além de alterar alguns artigos do Marco Civil da Internet.

LEGISLAÇÃO DE CRIMES CIBERNÉTICOS NO BRASIL

Lei 14.155 de 2021

Esta lei tornou mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou via internet.

LEGISLAÇÃO DE CRIMES CIBERNÉTICOS NO BRASIL

Lei 14.155 de 2021

Esta lei tornou mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou via internet.

Lei 11.829, de 2008 (pornografia infantil)

Esta lei combate à produção, venda e distribuição de pornografia infantil, bem como criminaliza a aquisição/posse de tal material e outras condutas relacionadas à pedofilia na internet.

LEGISLAÇÃO DE CRIMES CIBERNÉTICOS NO BRASIL

Lei 14.155 de 2021

Esta lei tornou mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou via internet.

Lei 11.829, de 2008 (pornografia infantil)

Esta lei combate à produção, venda e distribuição de pornografia infantil, bem como criminaliza a aquisição/posse de tal material e outras condutas relacionadas à pedofilia na internet.

Lei 13.185 de 2015 (cyberbullying)

Esta lei institui o Programa de Combate à Intimidação Sistemática (bullying),

LEGISLAÇÃO DE CRIMES CIBERNÉTICOS NO BRASIL

Lei 14.155 de 2021

Esta lei tornou mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou via internet.

Lei 13.185 de 2015 (cyberbullying)

Esta lei institui o Programa de Combate à Intimidação Sistemática (bullying),

Lei 11.829, de 2008 (pornografia infantil)

Esta lei combate à produção, venda e distribuição de pornografia infantil, bem como criminaliza a aquisição/posse de tal material e outras condutas relacionadas à pedofilia na internet.

Lei 14.132 de 2021 (stalking)

Esta lei acrescenta um artigo à seção dos crimes contra a liberdade pessoal no Código Penal, visando prever o crime de perseguição.

CONCEITOS BÁSICOS

Cookies

Cookies são arquivos que contêm fragmentos de dados trocados entre o computador de um usuário e um servidor web para identificar usuários.

CONCEITOS BÁSICOS

Cookies

Cookies são arquivos que contêm fragmentos de dados trocados entre o computador de um usuário e um servidor web para identificar usuários.

SQL

Structured Query Language é a linguagem de pesquisa declarativa padrão para banco de dados relacional.

CONCEITOS BÁSICOS

Cookies

Cookies são arquivos que contêm fragmentos de dados trocados entre o computador de um usuário e um servidor web para identificar usuários.

Arquivo log

Descreve o processo de registro de eventos relevantes em um sistema computacional.

SQL

Structured Query Language é a linguagem de pesquisa declarativa padrão para banco de dados relacional.

CONCEITOS BÁSICOS

Cookies

Cookies são arquivos que contêm fragmentos de dados trocados entre o computador de um usuário e um servidor web para identificar usuários.

SQL

Structured Query Language é a linguagem de pesquisa declarativa padrão para banco de dados relacional.

Arquivo log

Descreve o processo de registro de eventos relevantes em um sistema computacional.

Patch de correção

Patch de correção é um programa criado especificamente para corrigir determinados erros presentes em um software.

CONCEITOS BÁSICOS

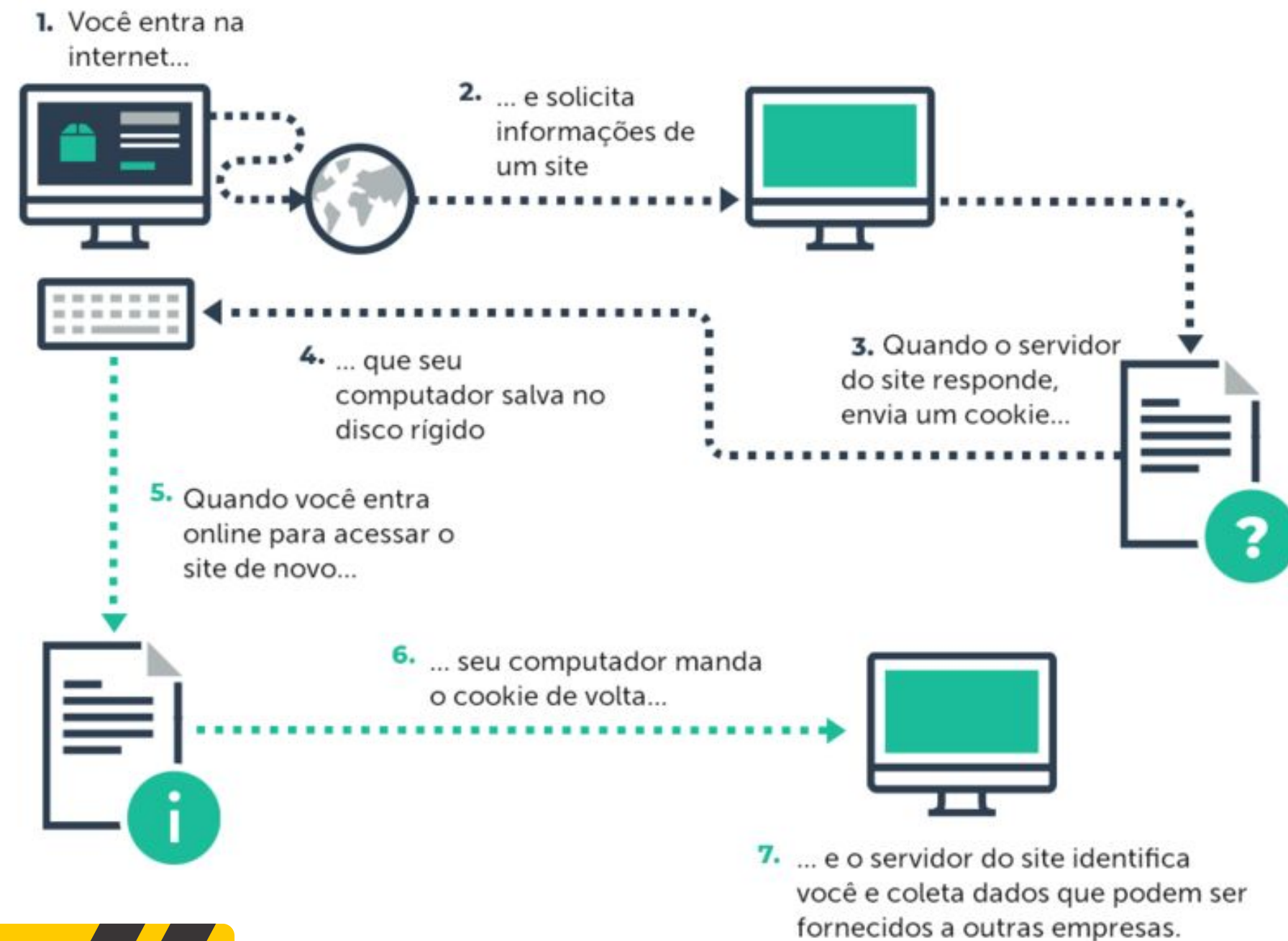


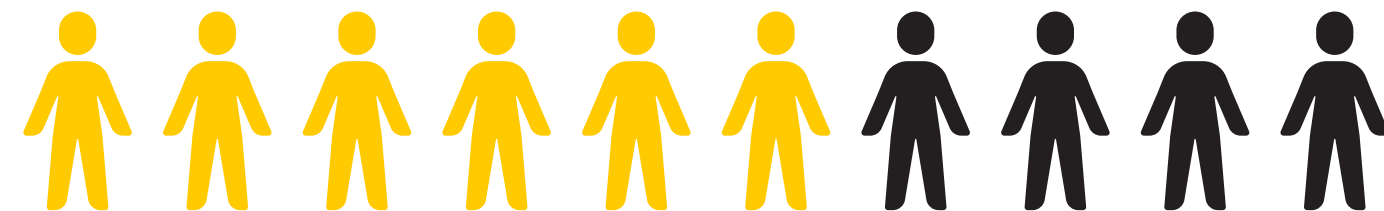
Imagem fornecida por PixelPrivacy, 2022.

PRINCIPAIS TIPOS DE ATAQUES



O que é um cyber crime?

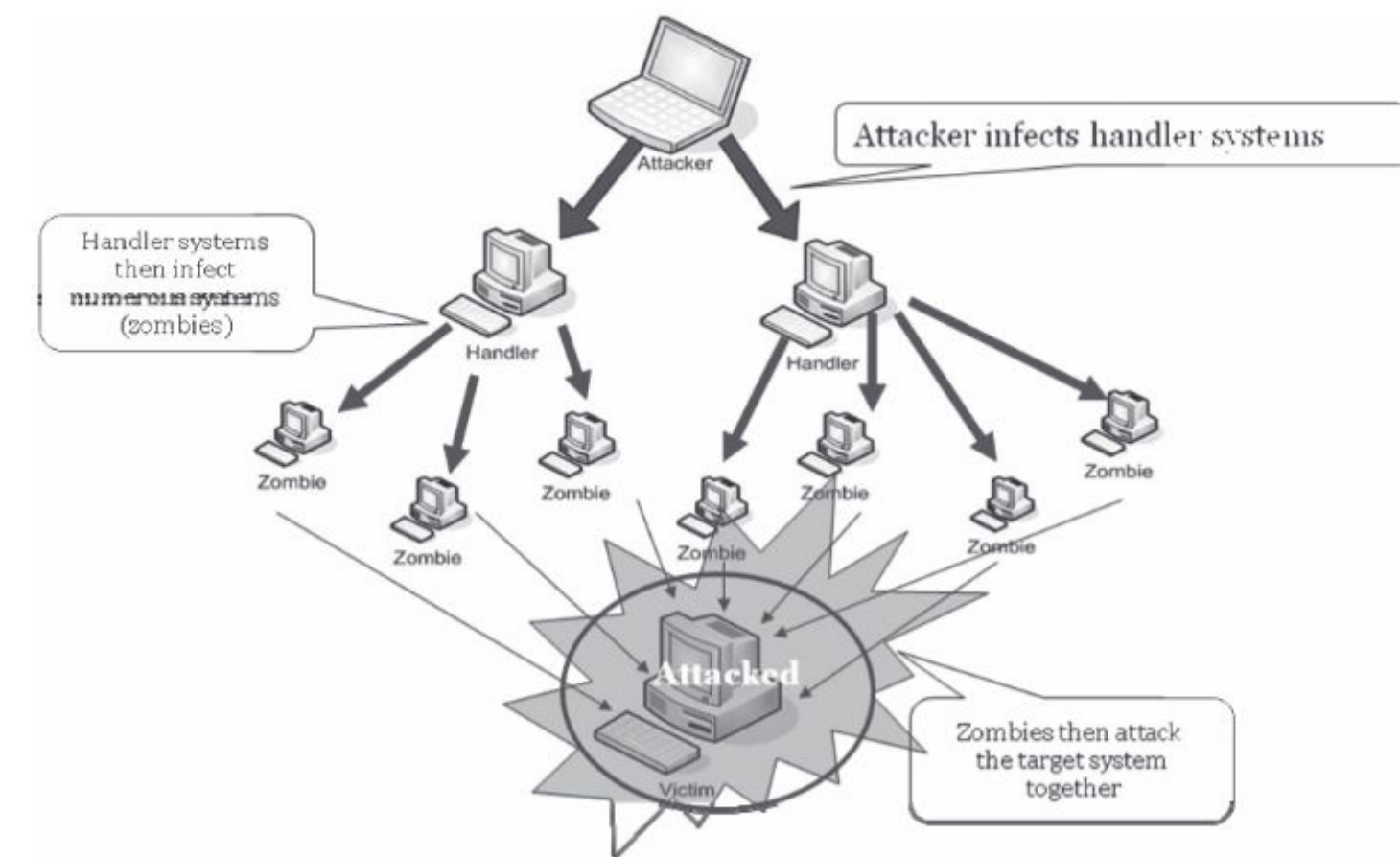
- Cyber crime pode ser definido como "qualquer ato ilegal que envolva um computador, seus sistemas ou suas aplicações.";
- Segundo uma pesquisa realizada pela empresa de cibersegurança Norton, 58% dos brasileiros entrevistados afirmam ter sofrido um cyber crime em 2021



PRINCIPAIS TIPOS DE ATAQUES:

DENIAL OF SERVICE

- Um ataque DoS ocorre quando um invasor tenta sobrecarregar a comunicação de um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores;

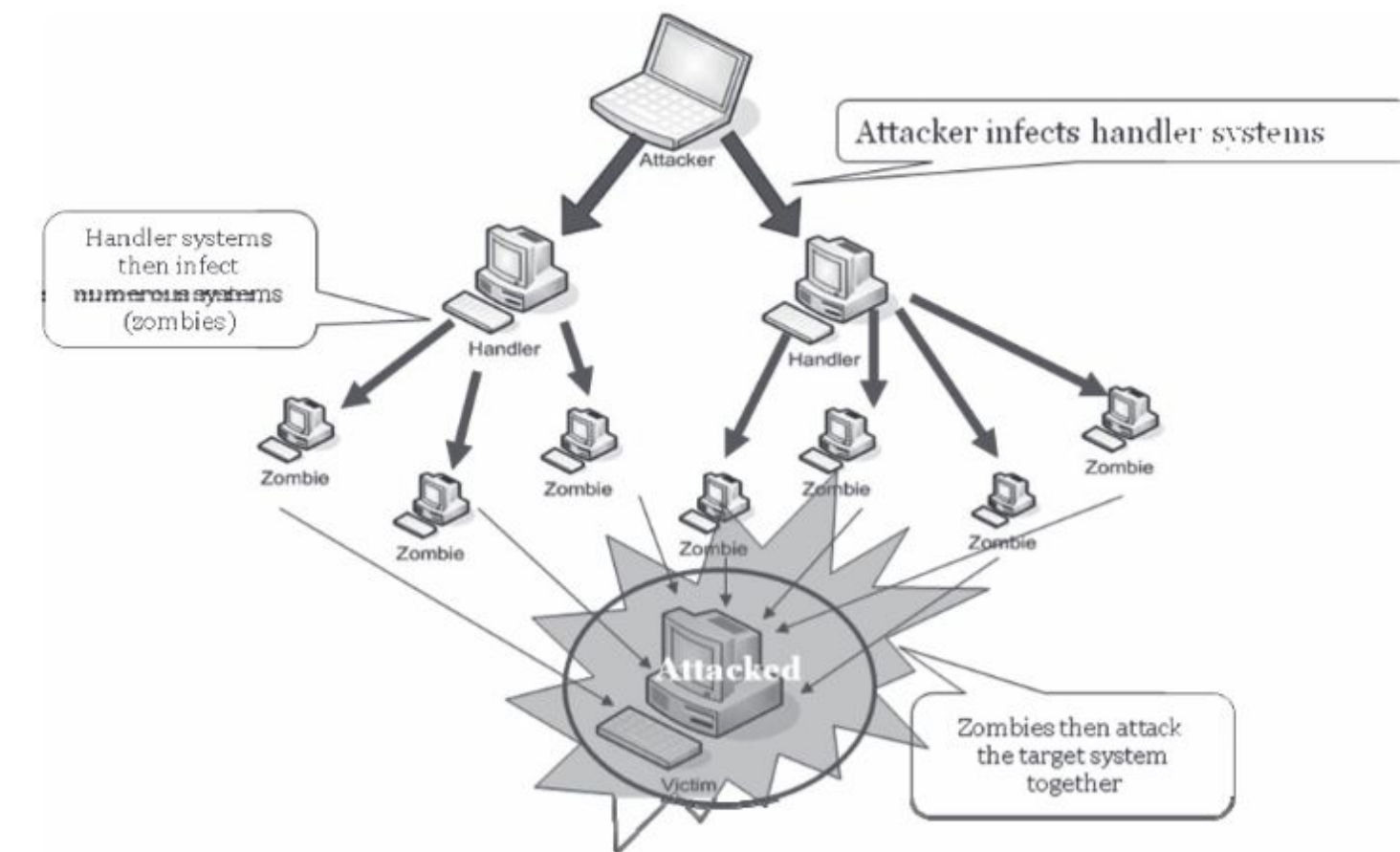


Copyright © by EC-Council

PRINCIPAIS TIPOS DE ATAQUES:

DENIAL OF SERVICE

- Um ataque DoS ocorre quando um invasor tenta sobrecarregar a comunicação de um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores;
- Os objetivos deste ataque são o consumo dos próprios recursos e a destruição ou alteração de informações, programas e arquivos de um sistema.

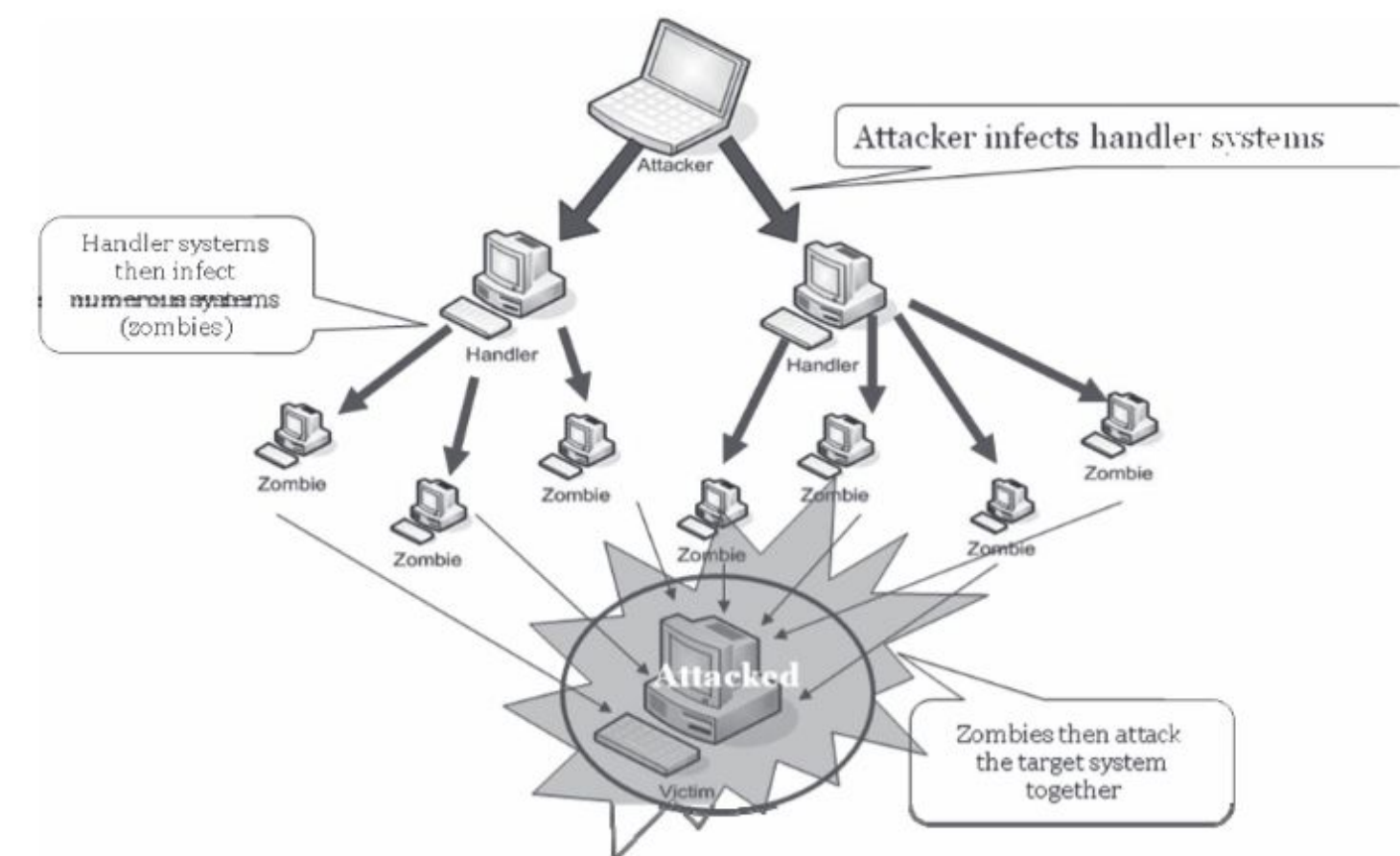


Copyright © by EC-Council

PRINCIPAIS TIPOS DE ATAQUES:

DENIAL OF SERVICE

- Um ataque DoS ocorre quando um invasor tenta sobrecarregar a comunicação de um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores;
- Os objetivos deste ataque são o consumo dos próprios recursos e a destruição ou alteração de informações, programas e arquivos de um sistema.
- Há também os ataques "denial of service distribuídos" (DDoS), nos quais uma grande quantidade de sistemas atacam um único alvo.



Copyright © by EC-Council

PRINCIPAIS TIPOS DE ATAQUES: CROSS-SITE SCRIPTING (XSS)

- O ataque XSS ocorre quando uma página contendo um código malicioso do invasor é executada no sistema da vítima.



PRINCIPAIS TIPOS DE ATAQUES: CROSS-SITE SCRIPTING (XSS)

- O ataque XSS ocorre quando uma página contendo um código malicioso do invasor é executada no sistema da vítima.
- Os tipos de ataque XSS podem ser armazenados (stored) ou refletidos (reflected).



PRINCIPAIS TIPOS DE ATAQUES: CROSS-SITE SCRIPTING (XSS)

- O ataque XSS ocorre quando uma página contendo um código malicioso do invasor é executada no sistema da vítima.
- Os tipos de ataque XSS podem ser armazenados (stored) ou refletidos (reflected).
- Invasores podem coletar dados pessoais, roubar cookies, redirecionar usuários para outras páginas ou executar outros códigos maliciosos no sistema da vítima.



PRINCIPAIS TIPOS DE ATAQUES:

SQL INJECTION

- O ataque SQL Injection ocorre quando um invasor passa um código SQL malicioso para uma página web como "input" (entrada) e, caso o sistema valide o código sem checá-lo, ele pode ser submetido ao banco de dados, dando o controle dos dados ao criminoso.



Imagem fornecida por Avast, 2022.

PRINCIPAIS TIPOS DE ATAQUES: COOKIE POISONING

- Os aplicativos Web usam cookies para armazenar informações como IDs de usuário, senhas e afins, na máquina do usuário;



PRINCIPAIS TIPOS DE ATAQUES:

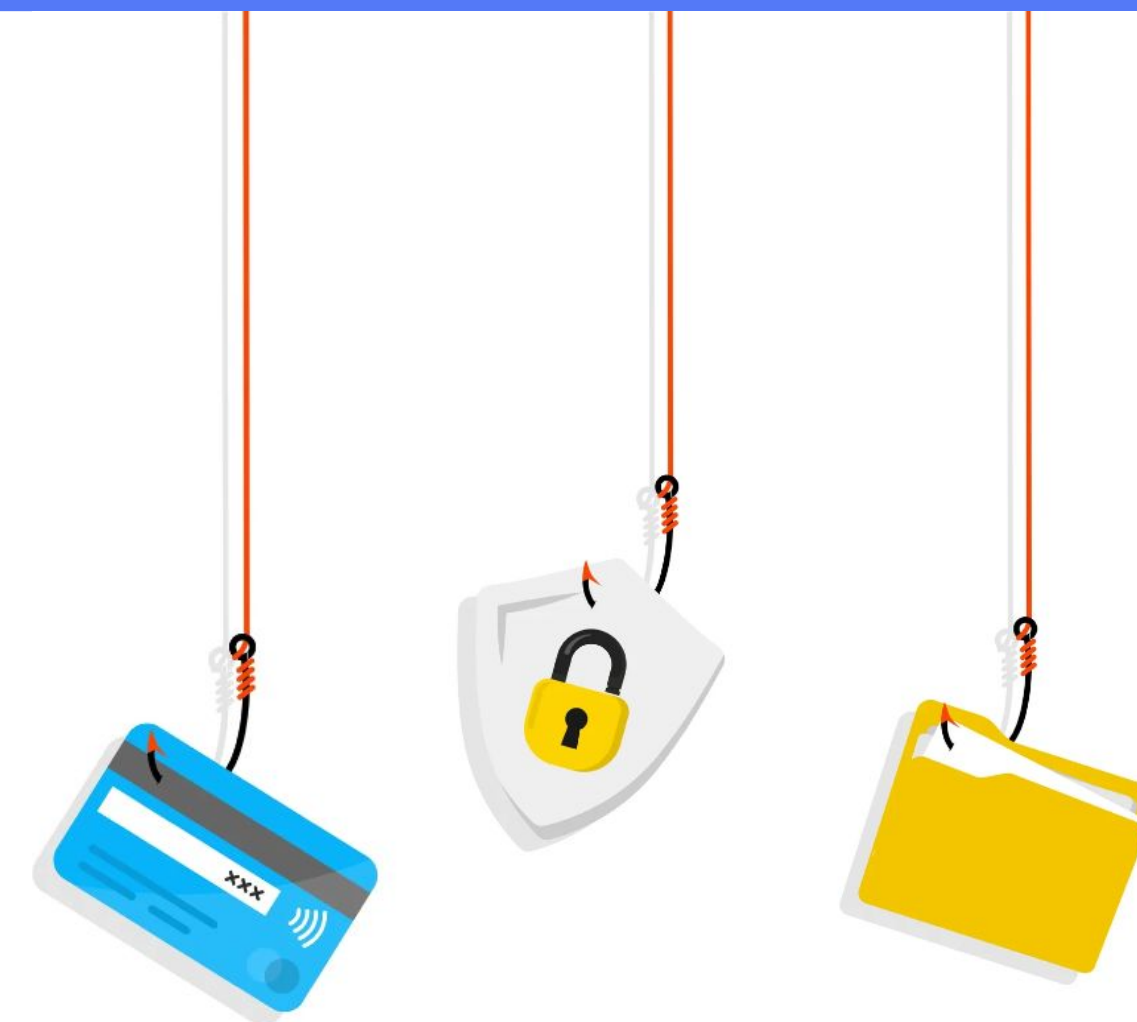
COOKIE POISONING

- Os aplicativos Web usam cookies para armazenar informações como IDs de usuário, senhas e afins, na máquina do usuário;
- Em um ataque de envenenamento por cookie, o invasor modifica o conteúdo de um cookie para roubar informações pessoais sobre um usuário ou fraudar sites.



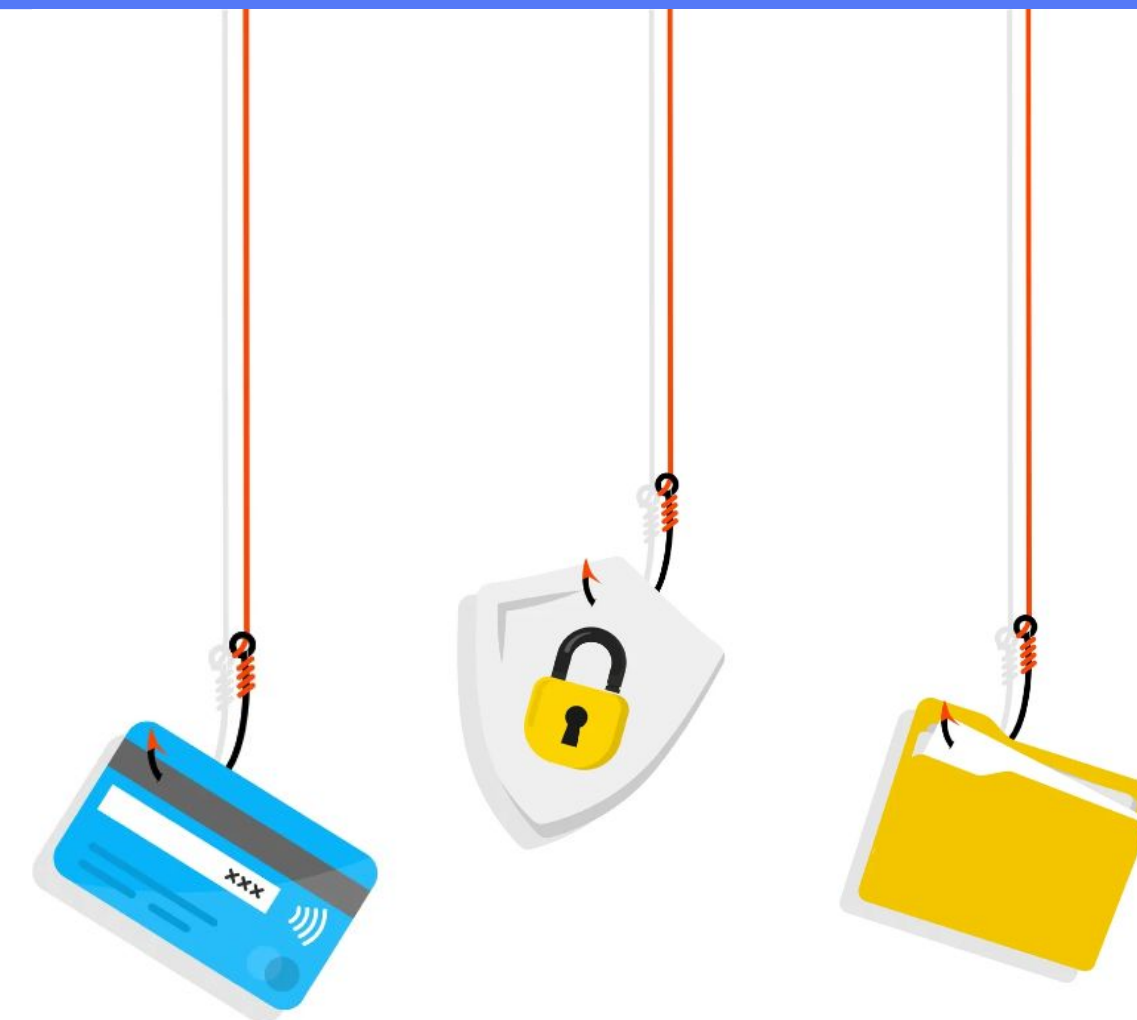
PRINCIPAIS TIPOS DE ATAQUES: PHISHING

- Phishing é um método de fraude por e-mail em que o criminoso envia um e-mail de aparência oficial às possíveis vítimas, fingindo ser de seu banco ou estabelecimento comercial, para coletar informações pessoais e financeiras;



PRINCIPAIS TIPOS DE ATAQUES: PHISHING

- Phishing é um método de fraude por e-mail em que o criminoso envia um e-mail de aparência oficial às possíveis vítimas, fingindo ser de seu banco ou estabelecimento comercial, para coletar informações pessoais e financeiras;
- Durante esse processo, os usuários são solicitados por e-mail a visitar um site da Web para atualizar suas informações pessoais.



PRINCIPAIS TIPOS DE ATAQUES:

MANIPULAÇÃO DE LOGS

- Os aplicativos Web mantêm logs para rastrear os padrões de uso de um aplicativo, incluindo logins, recursos acessados e outras informações específicas do aplicativo;

```
11:56:54 User login: juser  
12:34:07 Administrator account created: drevil  
12:36:43 Administrative access: drevil  
12:45:19 Configuration file accessed: drevil
```

```
11:56:54 User login: juser  
12:50:14 User logout: juser
```

Imagem fornecida por EC-Council, 2010.

PRINCIPAIS TIPOS DE ATAQUES:

MANIPULAÇÃO DE LOGS

- Os aplicativos Web mantêm logs para rastrear os padrões de uso de um aplicativo, incluindo logins, recursos acessados e outras informações específicas do aplicativo;
- Esses logs são usados para comprovação de transações, cumprimento de requisitos legais, análise de marketing e análise de incidentes forenses. A integridade e a disponibilidade dos logs são especialmente importantes quando o não repúdio é necessário;

```
11:56:54 User login: juser  
12:34:07 Administrator account created: drevil  
12:36:43 Administrative access: drevil  
12:45:19 Configuration file accessed: drevil
```

```
11:56:54 User login: juser  
12:50:14 User logout: juser
```

Imagem fornecida por EC-Council, 2010.

PRINCIPAIS TIPOS DE ATAQUES:

MANIPULAÇÃO DE LOGS

- Os aplicativos Web mantêm logs para rastrear os padrões de uso de um aplicativo, incluindo logins, recursos acessados e outras informações específicas do aplicativo;
- Esses logs são usados para comprovação de transações, cumprimento de requisitos legais, análise de marketing e análise de incidentes forenses. A integridade e a disponibilidade dos logs são especialmente importantes quando o não repúdio é necessário;
- Para cobrir seus rastros, os invasores geralmente modificam logs e destroem as evidências do ataque.

```
11:56:54 User login: juser  
12:34:07 Administrator account created: drevil  
12:36:43 Administrative access: drevil  
12:45:19 Configuration file accessed: drevil
```

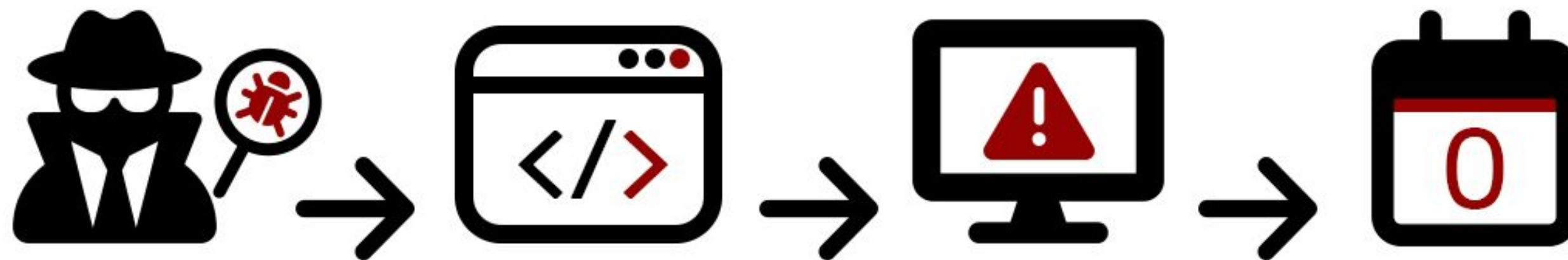
```
11:56:54 User login: juser  
12:50:14 User logout: juser
```

Imagem fornecida por EC-Council, 2010.

PRINCIPAIS TIPOS DE ATAQUES:

ATAQUE DE DIA ZERO

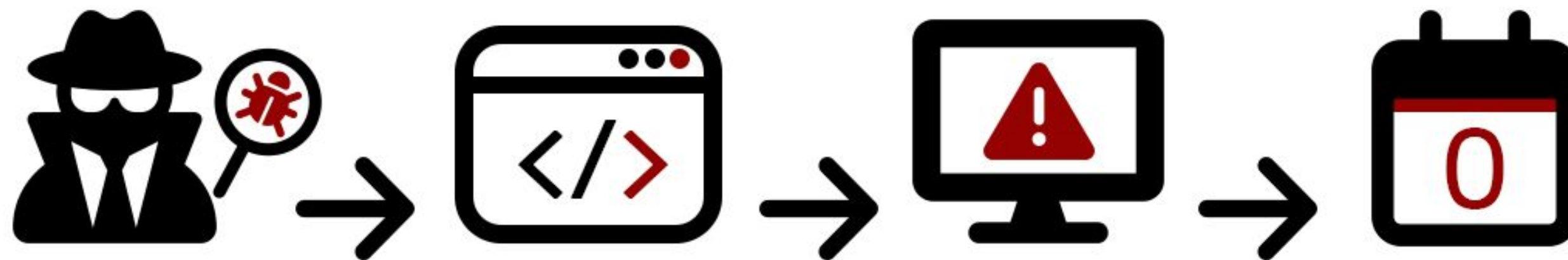
- Ataques de dia-zero exploram vulnerabilidades previamente desconhecidas, sendo por isso especialmente perigosos, pois medidas prévias não podem ser tomadas;



PRINCIPAIS TIPOS DE ATAQUES:

ATAQUE DE DIA ZERO

- Ataques de dia-zero exploram vulnerabilidades previamente desconhecidas, sendo por isso especialmente perigosos, pois medidas prévias não podem ser tomadas;
- Por não existir um método de segurança específico para ataques de dia-zero, uma janela de tempo até o patch de correção ser desenvolvido pode ser aproveitada pelos invasores.



PRINCIPAIS TIPOS DE ATAQUES:

ATAQUES RANSOMWARE

- Ransomware é um código malicioso de extorsão que consiste na criptografia de arquivos individuais ou de todo o sistema operacional e, em seguida, um resgate é exigido às vítimas para recuperar os dados;



Imagem fornecida por Trend Micro, 2020.

PRINCIPAIS TIPOS DE ATAQUES:

ATAQUES RANSOMWARE

- Ransomware é um código malicioso de extorsão que consiste na criptografia de arquivos individuais ou de todo o sistema operacional e, em seguida, um resgate é exigido às vítimas para recuperar os dados;
- Assim, os ataques ransomware ocorrem da seguinte maneira:
 1. Infecção;
 2. Criptografia;
 3. Resgate.



Imagem fornecida por Trend Micro, 2020.

ETAPAS DA FORENSE COMPUTACIONAL

PRESERVAÇÃO

ETAPAS DA FORENSE COMPUTACIONAL

PRESERVAÇÃO

IDENTIFICAÇÃO

ETAPAS DA FORENSE COMPUTACIONAL

PRESERVAÇÃO

IDENTIFICAÇÃO

EXTRAÇÃO

ETAPAS DA FORENSE COMPUTACIONAL

PRESERVAÇÃO

IDENTIFICAÇÃO

EXTRAÇÃO

INTERPRETAÇÃO

ETAPAS DA FORENSE COMPUTACIONAL

PRESERVAÇÃO

IDENTIFICAÇÃO

EXTRAÇÃO

INTERPRETAÇÃO

DOCUMENTAÇÃO

ETAPAS DA FORENSE COMPUTACIONAL

- Preservação: O investigador deve preservar a integridade da evidência;

ETAPAS DA FORENSE COMPUTACIONAL

- Preservação: O investigador deve preservar a integridade da evidência;
- Identificação: O examinador deve identificar a evidência e sua localização;
 - Ex.: a evidência pode estar em um disco rígido, pendrive ou log file;

ETAPAS DA FORENSE COMPUTACIONAL

- Preservação: O investigador deve preservar a integridade da evidência;
- Identificação: O examinador deve identificar a evidência e sua localização;
 - Ex.: a evidência pode estar em um disco rígido, pendrive ou log file;
- Extração: Após a identificação, o examinador deve extrair dados da cópia da evidência original;

ETAPAS DA FORENSE COMPUTACIONAL

- Preservação: O investigador deve preservar a integridade da evidência;
- Identificação: O examinador deve identificar a evidência e sua localização;
 - Ex.: a evidência pode estar em um disco rígido, pendrive ou log file;
- Extração: Após a identificação, o examinador deve extrair dados da cópia da evidência original;
- Interpretação: O investigador deve analisar e inspecionar o que foi encontrado;

ETAPAS DA FORENSE COMPUTACIONAL

- Preservação: O investigador deve preservar a integridade da evidência;
- Identificação: O examinador deve identificar a evidência e sua localização;
 - Ex.: a evidência pode estar em um disco rígido, pendrive ou log file;
- Extração: Após a identificação, o examinador deve extrair dados da cópia da evidência original;
- Interpretação: O investigador deve analisar e inspecionar o que foi encontrado;
- Documentação: Do início ao fim da investigação, o perito deve manter a documentação relativa às provas.

LIDANDO COM AS EVIDÊNCIAS

ENCONTRAR DADOS RELEVANTES

Deve ficar claro ao investigador quais dados devem ser coletados. É uma perda de tempo coletar dados desnecessários, pois dados mais relevantes podem ser perdidos se forem voláteis;

LIDANDO COM AS EVIDÊNCIAS

ENCONTRAR DADOS RELEVANTES

Deve ficar claro ao investigador quais dados devem ser coletados. É uma perda de tempo coletar dados desnecessários, pois dados mais relevantes podem ser perdidos se forem **voláteis**.

ORDEM DE VOLATILIDADE

Certas evidências são chamadas de **voláteis** pois não duram muito. Durante a coleta, o investigador deve preparar uma ordem de volatilidade, como por exemplo:

- ☐ Registros e cache;
- ☐ Tabela de roteamento;
- ☐ Cache ARP;
- ☐ Tabela de processo.

LIDANDO COM AS EVIDÊNCIAS

COLETAR A EVIDÊNCIA

Um investigador precisa seguir uma série de passos quando estiver coletando a evidência considerada relevante para o caso, tais como fotografar e identificar com a data da coleta da evidência.

LIDANDO COM AS EVIDÊNCIAS

COLETAR A EVIDÊNCIA

Um investigador precisa seguir uma série de passos quando estiver coletando a evidência considerada relevante para o caso, tais como fotografar e identificar com a data da coleta da evidência.

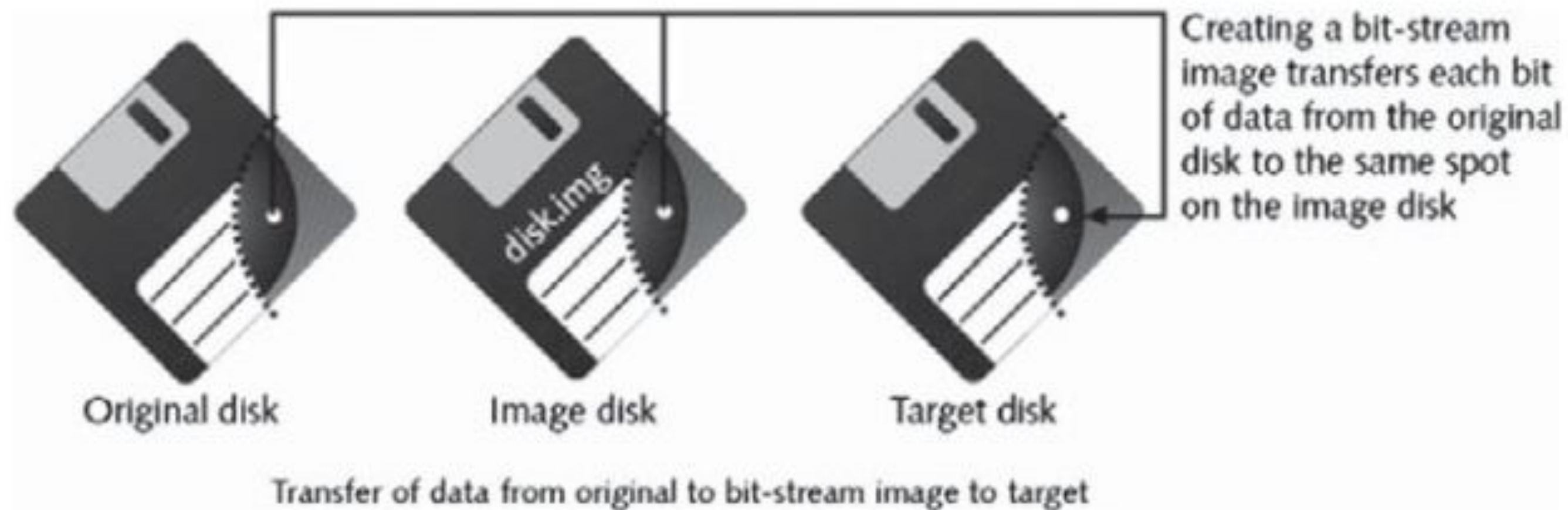
EXAMINAR E DOCUMENTAR

O investigador deve examinar as evidências em uma cópia bitstream em vez do computador original. Durante a documentação, o investigador deve usar um sistema preciso de data e hora.

LIDANDO COM AS EVIDÊNCIAS

- Como verificar a autenticidade da cópia bitstream em relação à evidência original?

LIDANDO COM AS EVIDÊNCIAS



Copyright © by **EC-Council**

LIDANDO COM AS EVIDÊNCIAS

- Como verificar a autenticidade da cópia bitstream em relação à evidência original?
- Função hash: uma função matemática que, via algoritmo, mapeia dados de comprimento variável para dados de comprimento fixo;

LIDANDO COM AS EVIDÊNCIAS

- Como verificar a autenticidade da cópia bitstream em relação à evidência original?
- Função hash: uma função matemática que, via algoritmo, mapeia dados de comprimento variável para dados de comprimento fixo;
- Um hash é uma sequência de bits geradas por um algoritmo de dispersão que busca identificar um arquivo ou uma informação unicamente;

LIDANDO COM AS EVIDÊNCIAS

Encryption

(used to protect sensitive information)



Plain text



Encryption



Encrypted text



Decryption



Plain text

Hashing

(used to validate information)



Plain text



Hash Function



Hashed Text

okta

LIDANDO COM AS EVIDÊNCIAS

- Como verificar a autenticidade da cópia bitstream em relação à evidência original?
- Função hash: uma função matemática que, via algoritmo, mapeia dados de comprimento variável para dados de comprimento fixo;
- Um hash é uma sequência de bits geradas por um algoritmo de dispersão que busca identificar um arquivo ou uma informação unicamente;
- Assim, caso os valores da cópia e da evidência original sejam idênticos, ambas devem ser tratadas com mesmo peso em um Tribunal da Justiça.

BOAS PRÁTICAS DE SEGURANÇA



O que fazer para se defender?

As boas práticas de segurança vão desde a atualização de softwares até a implementação de uma política de segurança da informação. Alguns passos importantes são:

- Realizar backups e atualizações frequentes;
- Controlar acessos dos usuários às funcionalidades específicas;
- Investir em serviços e equipamentos voltados para a segurança.

DÚVIDAS?

REFERÊNCIAS

- EC-Council. **Computer Forensics: Investigation Procedures and Response**. New York, NY: Course Technology, 2010. v.1.
- EC-Council. **Computer Forensics: Investigating Network Intrusions and Cybercrime**. New York, NY: Course Technology, 2010. v.4.
- https://www.planalto.gov.br/ccivil_03/
- NortonLifeLock. **2022 Cyber Safety Insights Report**. Disponível em <http://www.nortonlifelock.com/us/en/newsroom/press-kits/2022-norton-cyber-safety-insights-report-special-release-online-creeping/> Acesso em 14 set. 2022.
- [/www.kaspersky.com.br/](http://www.kaspersky.com.br/)