
UNAERP
Universidade de Ribeirão Preto
Campus Ribeirão Preto · Campus Guarujá

Segurança da Informação

Tópicos Especiais em Engenharia

Medidas de Segurança Técnicas

Criptografia

Criptografia - Conceito

- ✘ Técnica usada para proteger informações / comunicações
- ✘ Códigos derivados de modelos matemáticos (algoritmos)
- ✘ Acessível apenas a quem possa ler/processar

Criptografia e Seg. Info.

- ✘ Confidencialidade
  - Somente quem tem a chave pode ler a informação
- ✘ Integridade
  - Informação não pode ser alterada no armazenamento/trânsito
- ✘ Irretratabilidade
  - Criador/emissor da informação não pode negar a criação/transmissão da informação
- ✘ Autenticação
  - Emissor e receptor podem confirmar suas identidades e origem/destino da informação

Criptografia – Componentes

- ✘ Algoritmo de criptografia
  - Instruções matemáticas para aplicar a criptografia
- ✘ Chave de criptografia
  - Sequência aleatória criada explicitamente para (des)criptografar dados

Criptografia - Componentes

- ✘ Algoritmo de criptografia
  - Pode ser público
- ✘ Chave de criptografia
  - Secreto!!!!!!!

Criptografia – Componentes

- ✘ Algoritmo de criptografia
  - RSA, AES, Triple DES....
- ✘ Chave de criptografia
  - 128 bits, 256 bits, 1024 bits...

Criptografia - Tipos de criptografia

- ✘ Simétrica
  - Única chave criptografa e descriptografa
- ✘ Assimétrica
  - Diferentes chaves para criptografar e descriptografar
- ✘ Unidirecional
  - Função hash, cálculo sem reversão
  - Usado principalmente para checar se dado foi alterado

Exemplo Unidirecional Hash

Windows

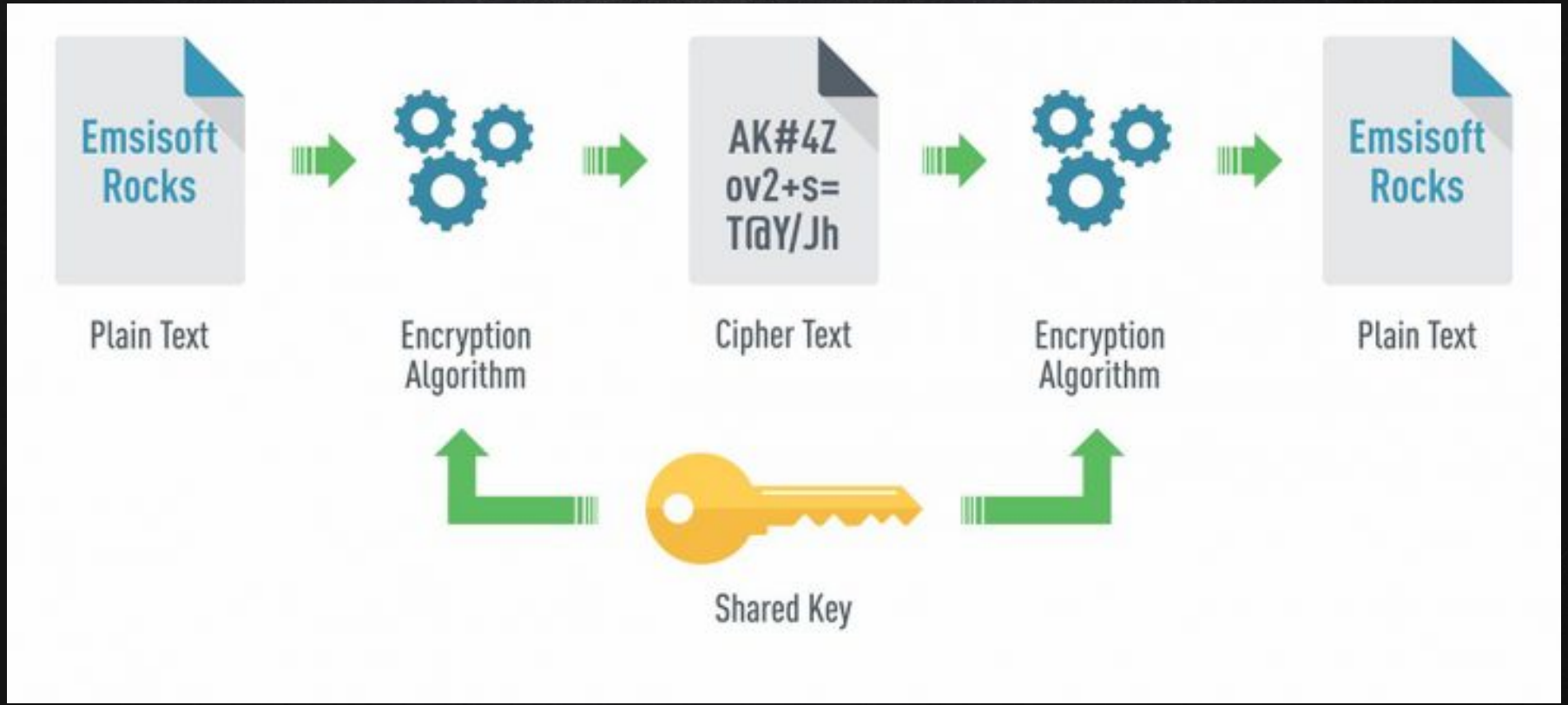
CertUtil –hashfile filename MD5 / CertUtil –hashfile filename SHA256 / CertUtil –hashfile filename XXX

Linux

md5sum filename / sha256sum filename / XXX

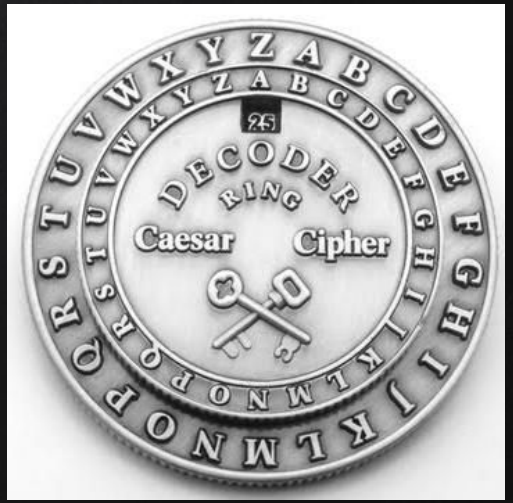
XXX -> algoritmo hash

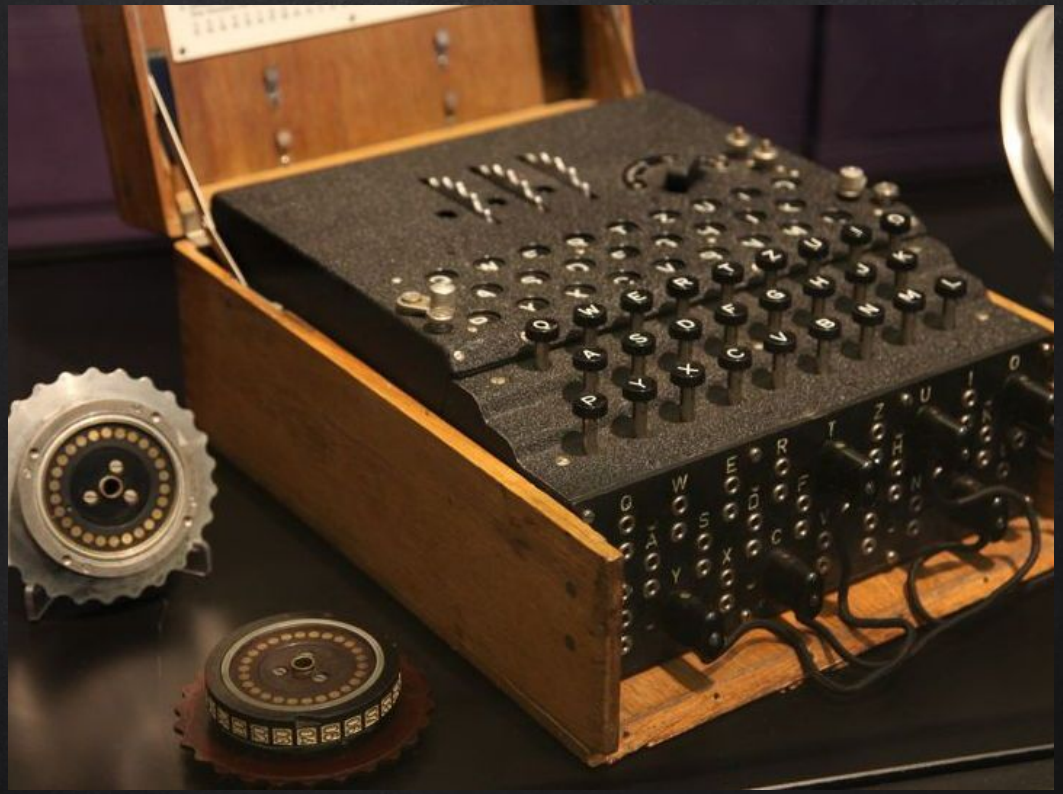
Criptografia Simétrica



A	B	C	D	E	F	G	H	I	J	K	L	M
ROT13	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

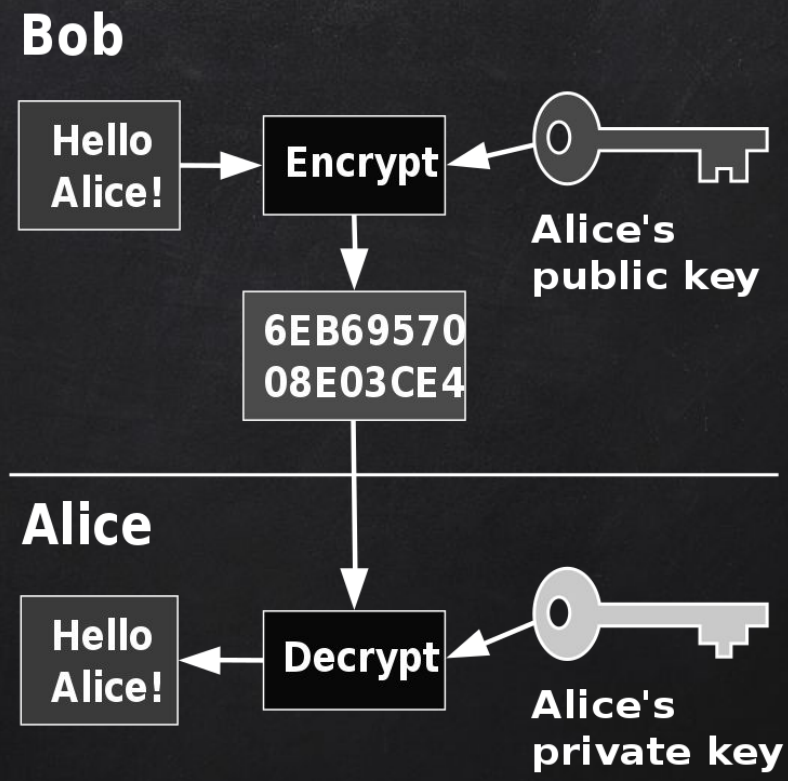
H	E	L	L	O
ROT13	↕	↕	↕	↕	↕
U	R	Y	Y	B





https://cryptii.com/pipes/enigma-machine

Criptografia Assimétrica



Comparativo Tipos de Criptografia

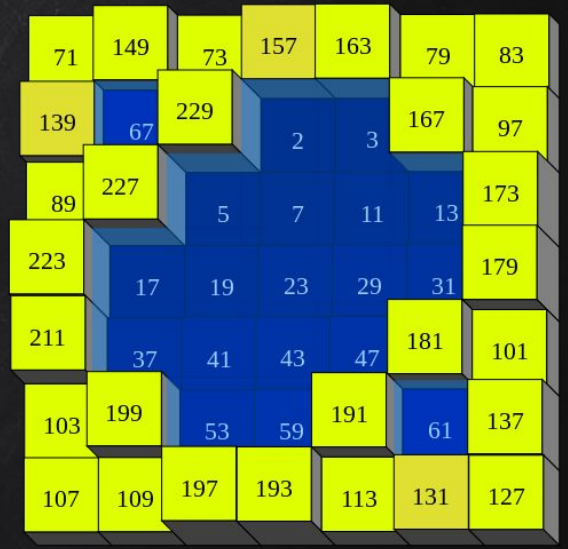
	Simétrica	Assimétrica
Chaves	Única chave	Par de chaves
Performance	Rápido	Mais lento
Quantidade de chaves	Cresce exponencialmente, de acordo com nº de usuários	Cresce linearmente, de acordo com nº de usuários
Garante	Confidencialidade	Confidencialidade, Integridade, Autenticação, Não-Repúdio

Rivest–Shamir–Adleman – RSA – Conceitos

<u>Número primo</u>

Divisível por 1 e por ele mesmo.

13 e 17 são primos.



<u>Números coprimos ou primos entre si</u>

Se o único divisor comum entre eles é o 1

8 e 15

Divisores de 8: 1, 2, 4, 8

Divisores de 15: 1, 3, 5, 15.

RSA – Conceitos

Função Phi (Função Totiente)

Para um número n, a função phi (n) é definida como a quantidade de números menores que n, coprimos de n.

Exemplo:

$\varphi(8) = 4$

Porque 1, 3, 5 e 7 (quatro números) são os números menores que 8 e coprimos de 8.

$\varphi(p*q) = \varphi(p) * \varphi(q)$

RSA – Conceitos

Se N é primo

$\varphi(N) = N-1$

Exemplo:

$\varphi(7) = 6$

$\varphi(11) = 10$

Se x e z são primos

$\varphi(x * z) = \varphi(x) * \varphi(z)$

$\varphi(x * z) = (x-1)*(z-1)$

Algoritmo RSA

Selecione dois números primos: p e q

Calcule

$n = p * q$

Escolha um inteiro e,

$1 < e < \varphi(n)$

de forma que "e" e $\varphi(n)$ sejam coprimos

Compute

$d = (2\ \varphi(n) + 1) / e$

Chave pública é composta por "n" e "e"

Chave privada é d

Algoritmo RSA

Cifrando a informação

$c = m^e \bmod n$

Decifrando a mensagem

$m = c^d \bmod n$

Onde

m é a mensagem a ser cifrada

c é a mensagem cifrada

Algoritmo RSA – Exemplo

Escolhemos dois números primos p e q

$p = 3$

$q = 7$

$n = p*q$

$n = 3*7$

$n = 21$

$\varphi(n) = (p-1)*(q-1)$

$\varphi(n) = 12$

$1 < e < \varphi(n)$

$1 < e < 12$

$e = 5$

"e" e $\varphi(n)$ são coprimos

"n" e "e" formam a chave pública

Algoritmo RSA – Exemplo

$d = (2\ \varphi(n) + 1) / e$

$d = ((2 * 12) + 1) / 5$

$d = 5$ (chave privada)

m = "AB" (mensagem)

Codificação da mensagem

A = 1

B = 2

$m = 12$

$c = m^e \bmod n$

$c = 12^5 \bmod 21$

$c = 248832 \bmod 21$

$c = 3$

$m = c^d \bmod n$

$m = 3^5 \bmod 21$

$m = 12$

Algoritmo RSA – Core

- ✘ p e q na prática são grandes
  - ordem de 10^100
  - https://pt.wikipedia.org/wiki/Googol
- ✘ Computadores tem facilidade para executar exponenciação (sequência de multiplicações)
- ✘ Descobrir chave privada exige fatorar números muito grandes, não é possível em tempo viável.
- ✘ Recomendado usar 4096 bits

Política de Criptografia

- ✘ Onde deve ser usado criptografia
- ✘ Quais tipos / Onde aplicações / serviços
- ✘ Gestão das chaves
- ✘ Backup de dados criptografados (e onde estão arquivos originais)
- ✘ Controle de Criptografia (medidas para evitar uso inadequado)

Certificado Digital

Certificado Digital

- ✘ Identidade Virtual
- ✘ Pessoa Física ou Jurídica
- ✘ Transações online
  - Garantia de Autenticidade
  - Proteção de informações trocadas

Certificado Digital

- ✘ Dados Identificado
- ✘ Dados Órgão Emissor
- ✘ Validade
- ✘ Assinatura Digital do Órgão Emissor
- ✘ Chave Pública Identificado

Infraestrutura de Chave Pública (ICP ou PKI)

- ✘ Estrutura de emissão de chaves públicas
- ✘ Princípio da "terceira parte confiável"
- ✘ Mediação de credibilidade e confiança entre partes que usam certificados digitais

Infraestrutura de Chave Pública (ICP ou PKI)

- ✘ Estrutura de emissão de chaves públicas
- ✘ Princípio da "terceira parte confiável"
- ✘ Mediação de credibilidade e confiança entre partes que usam certificados digitais

Infraestrutura de Chave Pública (ICP ou PKI)

- ✘ Estrutura de emissão de chaves públicas
- ✘ Princípio da "terceira parte confiável"
- ✘ Mediação de credibilidade e confiança entre partes que usam certificados digitais

Componentes da PKI

- Autoridade Certificadora (CA)
  - Armazena, assina e emite certificados digitais
  - CA assina a chave pública do usuário com sua chave privada

- Autoridade de Registro (RA)
  - Valida a identidade de entidades que solicitam que seus certificados sejam armazenados na CA

Proteção contra códigos maliciosos (malwares)

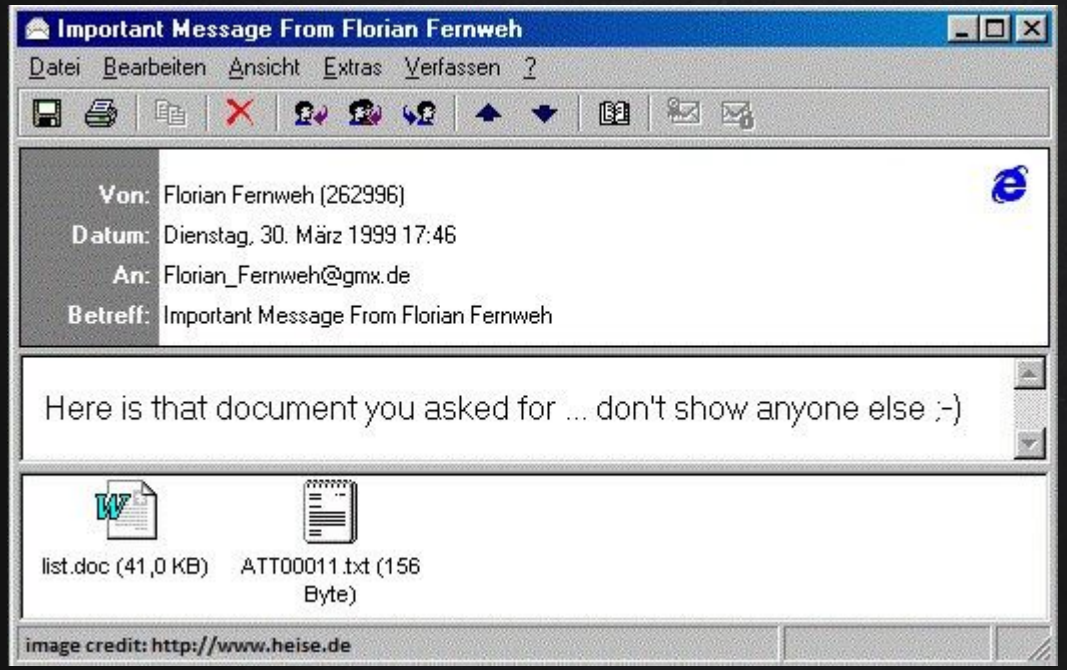
Proteção contra códigos maliciosos (malwares)

Malware: Códigos/Softwares criados para executar ações danosas em um sistema

Tipos de Malware – Vírus

Código que se propaga criando cópias de si mesmo e se tornando parte de outros programas/arquivos.

Se espalha somente quando encaminhado



David L. Smith
$80 MI

Tipos de Malware – Verme / Worm

Código que se propaga criando cópias de si mesmo e se tornando parte de outros programas/arquivos. Se espalha por execução direta ou exploração automática de vulnerabilidades.

Consomem muitos recursos computacionais.

Morris worm or Internet worm of November 2, 1988

```
#include "worm.h"
#include <stdio.h>
#include <signal.h>
#include <strings.h>
#include <sys/param.h>
#include <sys/types.h>
#include <sys/time.h>
#include <sys/resource.h>
#include <sys/socket.h>
#include <sys/fcntl.h>
#include <sys/stat.h>
#include <netinet/in.h>
#include <net/if.h>
#include <arpa/inet.h>

extern errno;
extern char *malloc();

int pleasequit;                         /* See worm.h */
int nobjects = 0;
int nextw;
char *null_auth;

object objects[69];                     /* Don't know how many... */

object *getobjectbyname();
```

Robert T. Morris
US$ 100 MI

Tipos de Malware – Trojan

Se esconde como parte de algum programa "útil".

Cartões virtuais, albuns, jogos etc.

Diferente do worm/virus, não se reproduz/espalha.

Enviar informações confidenciais/ativar backdoor.

remote access trojan (RAT)

DarkComet – Jean-Pierre LESUEUR (@DarkCoderSc) – 2008

Tipos de Malware – Bomba Lógica (Logic Bomb)

Código inserido em programa, que executa ações maliciosas quando um trigger (gatilho) é disparado.

Vírus/Worms geralmente contém *logic bombs*.

Exemplo: Dev insere um código para executar quando sair da empresa

Tipos de Malware - Hoax (Boato)

Não exatamente um código malicioso, mas um boato.

Enviado por e-mail ou apps de msgs instantânea.

Tenta convencer o usuário de sua veracidade.

Depende do recepctor da mensagem para execução e replicação.

WARNING

You should be alert during the next days: Do not open any message with an attached filed called "Invitation" regardless of who sent it. It is a virus that opens an Olympic Torch which "burns" the whole hard disc C of your computer. This virus will be received from someone who has your e-mail address in his/her contact list, that is why you should send this e-mail to all your contacts. It is better to receive this message 25 times than to receive the virus and open it.

If you receive a mail called "invitation", though sent by a friend, do not open it and shut down your computer immediately.

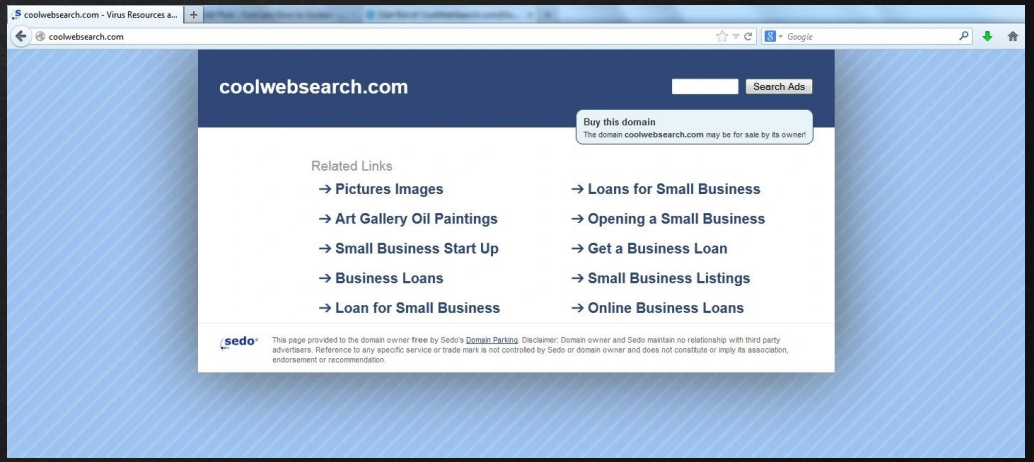
This is the worst virus announced by CNN, it has been classified by Microsoft as the most destructive virus ever. This virus was discovered by McAfee yesterday, and there is no repair yet for this kind of virus. This virus simply destroys the Zero Sector of the Hard Disc, where the vital information is kept. SEND THIS E-MAIL TO EVERYONE YOU KNOW, COPY THIS E-MAIL AND SEND IT TO YOUR FRIENDS AND REMEMBER: IF YOU SEND IT TO THEM, YOU WILL BENEFIT ALL OF US

✅ Olá, sou o Jélysson, diretor do WhatsApp Messenger, esta mensagem é para informar a todos os nossos usuários que temos apenas 530 contas disponíveis para novos celulares, e que, recentemente nossos servidores ficaram congestionados. Então, nós estamos pedindo a sua ajuda para resolver este problema. Precisamos de você. Nossos usuários ativos devem transmitir essa mensagem para cada uma das pessoas da sua lista de contatos, a fim de confirmar os nossos usuários ativos que usam WhatsApp, se você não enviar esta mensagem para todos os seus contatos, sua conta permanecerá inativa, com a consequência de perder todos os seus contatos. O símbolo de renovação, aparecerá automaticamente em seu smartphone, aparecem com a transmissão da mensagem. O smartphone será atualizado dentro de 24 horas, contará com um novo design, uma nova cor para bate-papo e seu ícone muda de verde para azul.Whatsapp se tornará pago, a menos que você é um usuário frequente. Se você tem pelo menos 10 contatos envie este sms e logo se tornará vermelho para indicar que você é um usuário freqüente Amanhã começam a receber mensagens para WhatsApp para 0,37 centavos. Envie esta mensagem para mais de 9 pessoas a partir de seus contatos WhatsApp. ♻️ Confirmando este é o novo ícone WhatsApp ☑️ Envie para todos os seus contatos para atualizar o aplicativo.✅ ATENCÃO Se achar que é mentira veja vc mesmo no googleOlá , o Whatsapp sera cancelado a partir do dia pois foi vendido para o FACEBOOK 💠 .Para que seu WhatsApp não seja cancelado, envie esta mensagem para 20 ou mais contatos, após a confirmação do envio o ícone ficará azul e você poderá usar o What'sBook normalmente.Obrigado!Equipe WhatsBook. ♻️ +55 88 99458494 : 🔵... Ja acabarão as mensagens gratis, amanha começarão a cobrar por whatsapp a 0.37 Reenvie esta mensagem a mais de 9 pessoas dos seus contatos, e tera gratuito por toda a vida. Fique atento na bolinha, pois ela ira ficar verde, faça e veja

08:54

Tipos de Malware – Spyware

- ✘ Coleta informações do dispositivo e envia para o atacante.
- ✘ Normalmente não danifica o dispositivo, mas viola a privacidade.
- ✘ Pode ter uso legítimo, quando instalado por admin para monitoramento e comunicação.



DÚVIDAS?

- ✘ Não esqueça de enviar sua maior dúvida pelo link que está no ClassRoom.
- ✘ Críticas/Sugestões: ezarpelao@unaerp.br
- ✘ Próxima aula: Bot, Botnet, Backdoor, Rootkit, e mais...

Credits

Special thanks to all the people who made and released these awesome resources for free:

- ✘ Presentation template by SlidesCarnival
- ✘ Photographs by Unsplash