RANSOMWARE

(Sequestro de Dados)

O que fazer?

Instituto Federal de Educação, Ciência e Tecnologia do RN
Câmpus Currais Novos

Ransomware

Pra quem ainda não sabe o que é (!?)

O que é Ransomware?

- Ransom = Resgate
- Software = programa / sistema computacional
- Ransom + software → Ransonware

  → Software (malicioso!?) programado para alterar o funcionamento de sistemas computacionais e cobrar resgate para restabelecer o seu funcionamento !?

- Tipo de malware que restringe o acesso ao sistema infectado e cobra um valor de "resgate" para que o acesso possa ser reestabelecido.

Ransomware (Evolução!?)

Sequestro de Sistema Computacional com pagamento de resgate

Hacker é preso no RN após invadir sites e assinar recibo

14/09/2011

- Sócio de uma Lan House
- Invasão a sites
- Telefonema à vítima
- Cobrança de “resgate”
- R$ 500,00 !!??
- 2 anos de “trégua”...
- “Me divirto invadindo sites”
- “Não existem leis contra isso...” !!??
- Ameaças e Extorsão !!!

http://www.tribunadonorte.com.br/noticia/hacker-e-preso-apos-invadir-sites-e-assinar-recibo-comprovando-extorsao/195856

Ransomware

Pra quem ainda não sabe o que é (!?)

- http://cartilha.cert.br/ransomware

- Você sabe o que é Ransomware?
- Ransomware é um tipo de código malicioso...
- ...que torna inacessíveis os dados armazenados em um equipamento...
- ...geralmente usando criptografia...
- ...e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário.

Ransomware
Classificação / Tipos

- http://cartilha.cert.br/ransomware

- Existem dois tipos de Ransomware:
  - Ransomware Locker
  - Ransomware Crypto

Ransomware
Classificação / Tipos

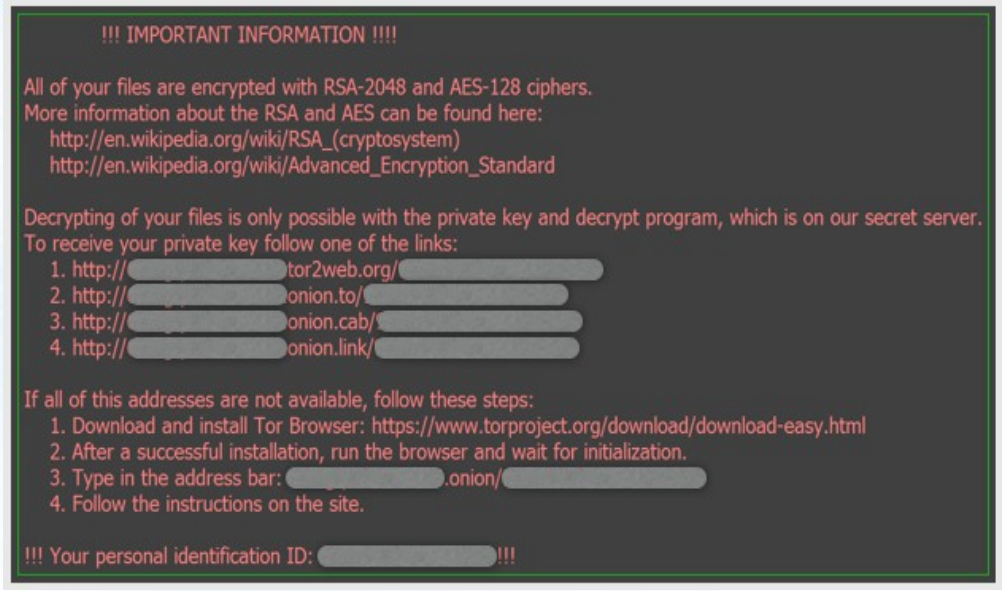
- Ransomware Locker: impede que você acesse o equipamento infectado.

- Ex.01: FBI Ransomware (Desktops com MS-Windows)
- Ex.02: Cyber Police Ransomware (Mobile)
  - Tipo conhecido como “Android Lockscreen”

Ransomware
Classificação / Tipos

- Ransomware Crypto: impede que você acesse aos dados armazenados no equipamento infectado, geralmente usando criptografia.

Crypto-Ransomware



- Ex.01: Locky Ransomware
  - Mail c/anexo → Word (ativa macros) → Download Malware
- Ex.02: TorLocker Ransomware
  - Desenvolvedores usam a rede Tor para esconder suas identidades

Ransomware

Principais "sintomas" (Eu fui/sou/serei vítima!?)

- Os principais sinais da presença de malwares do tipo ransomware em uma máquina são:
  - Identificação de arquivos criptografados;
  - Identificação de arquivos renomeados;
  - Bloqueios em Navegador(es) Web;
  - Bloqueio de tela;
  - Nota/alerta emitido pelo próprio ransomware (pedindo o resgate).

Ricardo Kléber

Ransomware
Evolução (Marcos Históricos)

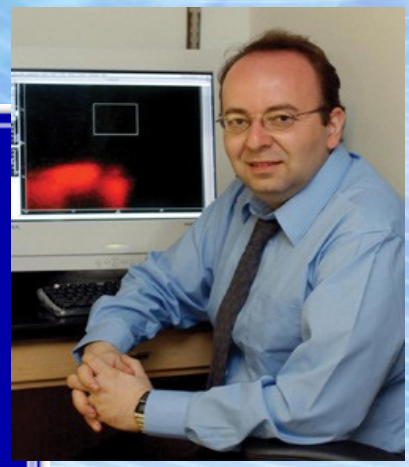
• AIDS Trojan — 1989

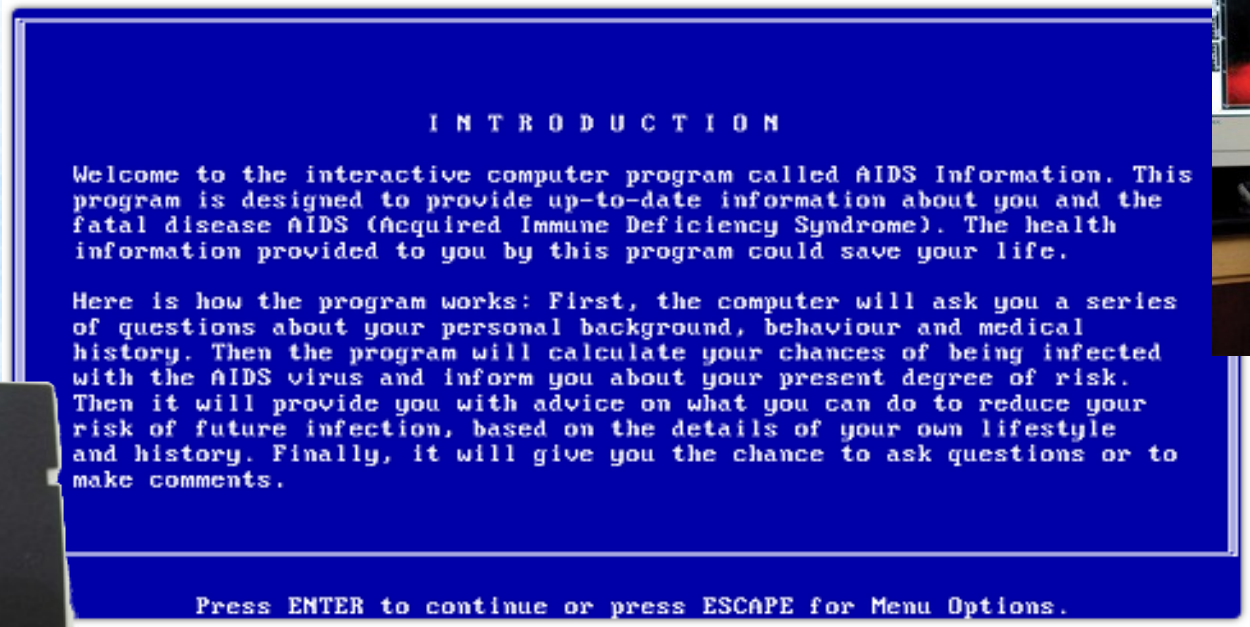
- Também conhecido como PC Cyborg Trojan (PC Cyborg Corporation);
- Enviado por carta (correio) em disquetes de 5¼";
- Criptografava arquivos e solicita ao usuário uma "renovação de licença";
- Objetivo financeiro claro → Sequestro de dados cobrando resgate (ranson)
- Resgate = U$ 189 (envio para uma caixa postal no Panamá);
- Na verdade, só substituía o Autoexec.bat, ocultava pastas e criptografava os nomes de arquivos na unidade C;
- Autor Dr. Joseph Popp Biólogo com PhD em Harvard
  - Preso, alegou que o dinheiro seria encaminhado para pesquisas sobre a cura da Aids.

Ransomware
Evolução (Marcos Históricos)

- **AIDS Trojan**

1989

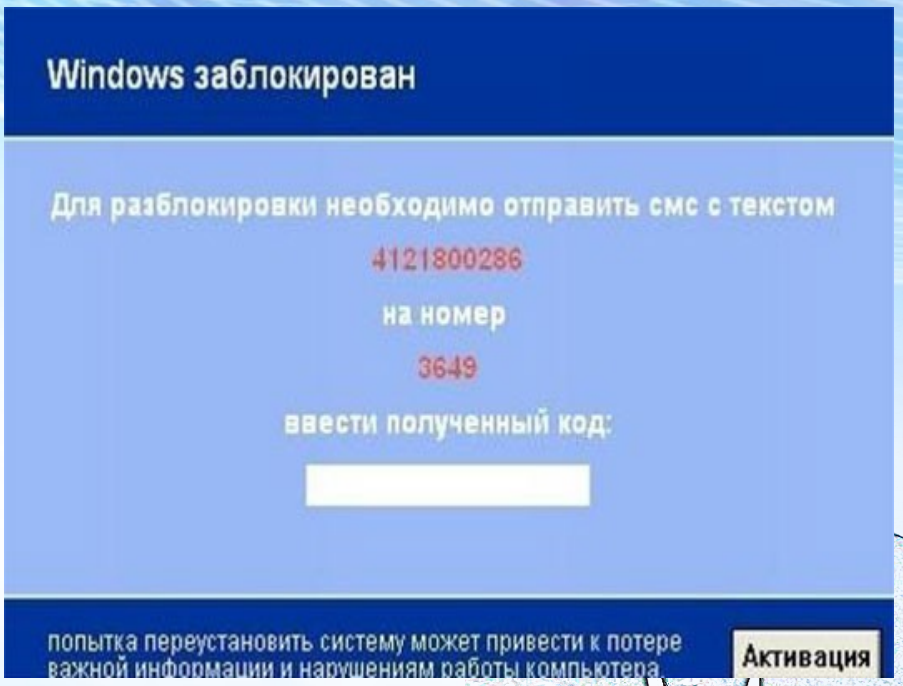




Ricardo Kléber

Ransomware
Evolução (Marcos Históricos)

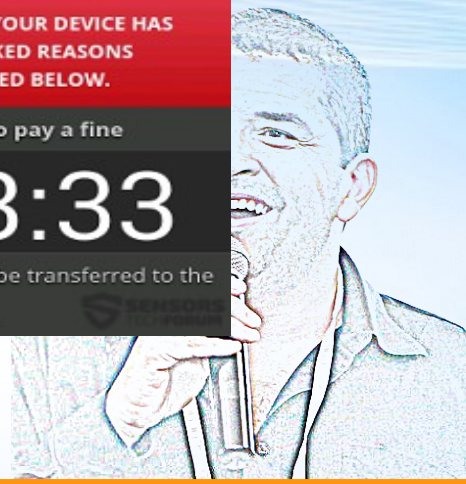
- **WinLocker (Rússia)** **2009**
  - Também conhecido como SMSLock
  - Bloqueio (locker) do equipamento
  - Exigência de envio de um SMS Premium
    - Usuário recebe SMS de resposta com o código para desbloquear
  - Custo médio de cada SMS = U$ 10
  - Lucro até a prisão do grupo = U$ 16 Milhões



Ransomware

Evolução (Marcos Históricos)

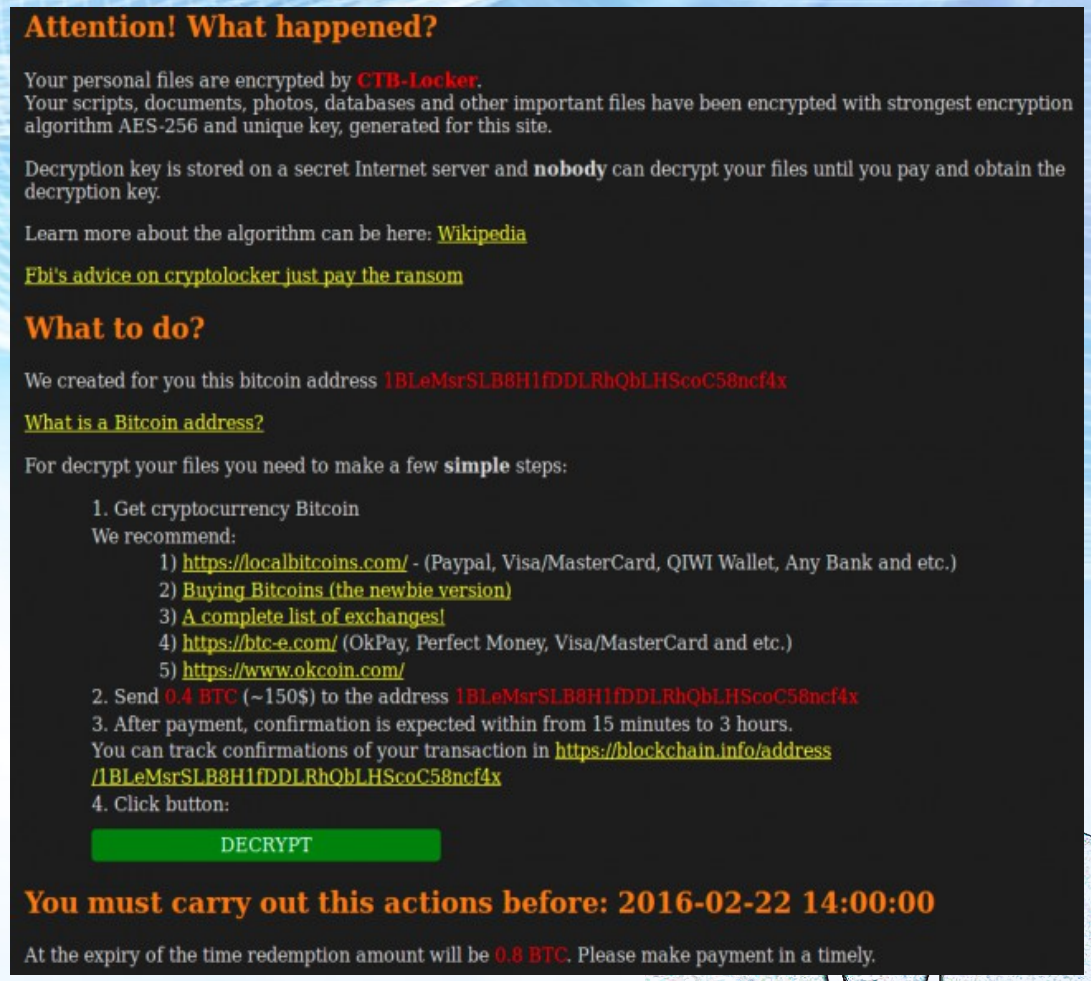
- **Scareware** — 2012
  - **Police Ransomware**
  - **Fake FBI / Police Locker Screen**



Scare = Susto / Medo / Pânico

Ransomware
Evolução (Marcos Históricos)

- **Pagamento com Bitcoins** **2013**
  - Moeda digital (“criptomoeda”) independente de instituições financeiras
  - Valor de 1 Bitcoin (08/12/2016) = R$ 2.656,22



Attention! What happened?

Your personal files are encrypted by CTB-Locker.
Your scripts, documents, photos, databases and other important files have been encrypted with strongest encryption algorithm AES-256 and unique key, generated for this site.

Decryption key is stored on a secret Internet server and **nobody** can decrypt your files until you pay and obtain the decryption key.

Learn more about the algorithm can be here: Wikipedia

Fbi's advice on cryptolocker just pay the ransom

What to do?

We created for you this bitcoin address 1BLeMsrSLB8H1fDDLRhQbLHScoC58ncf4x

What is a Bitcoin address?

For decrypt your files you need to make a few **simple** steps:

1. Get cryptocurrency Bitcoin
   We recommend:
   1) https://localbitcoins.com/ - (Paypal, Visa/MasterCard, QIWI Wallet, Any Bank and etc.)
   2) Buying Bitcoins (the newbie version)
   3) A complete list of exchanges!
   4) https://btc-e.com/ (OkPay, Perfect Money, Visa/MasterCard and etc.)
   5) https://www.okcoin.com/
2. Send 0.4 BTC (~150$) to the address 1BLeMsrSLB8H1fDDLRhQbLHScoC58ncf4x
3. After payment, confirmation is expected within from 15 minutes to 3 hours.
   You can track confirmations of your transaction in https://blockchain.info/address/1BLeMsrSLB8H1fDDLRhQbLHScoC58ncf4x
4. Click button:

DECRYPT

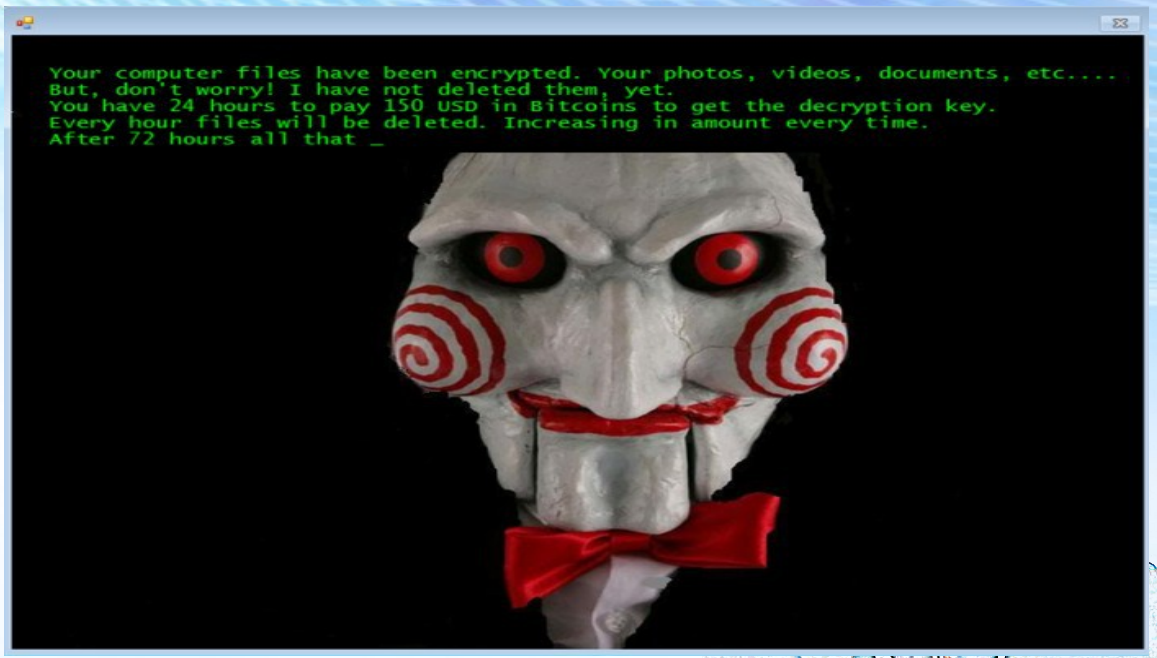
You must carry out this actions before: 2016-02-22 14:00:00

At the expiry of the time redemption amount will be 0.8 BTC. Please make payment in a timely.

Ransomware
Evolução (Marcos Históricos)

2015

- **ChirCrypt**
  - Humilhação / Pressão psicológica → Se prazo não for cumprido todos os arquivos serão deletados !!!
  - 2016: Jigsaw (inspirado no filme “Jogos Mortais”)
    - 72 horas para pagar
    - A cada hora uma parte dos arquivos é/era deletada.



https://blogs.technet.microsoft.com/mmpc/2016/05/18/the-5ws-and-1h-of-ransomware/

Ransomware
Evolução (Marcos Históricos)

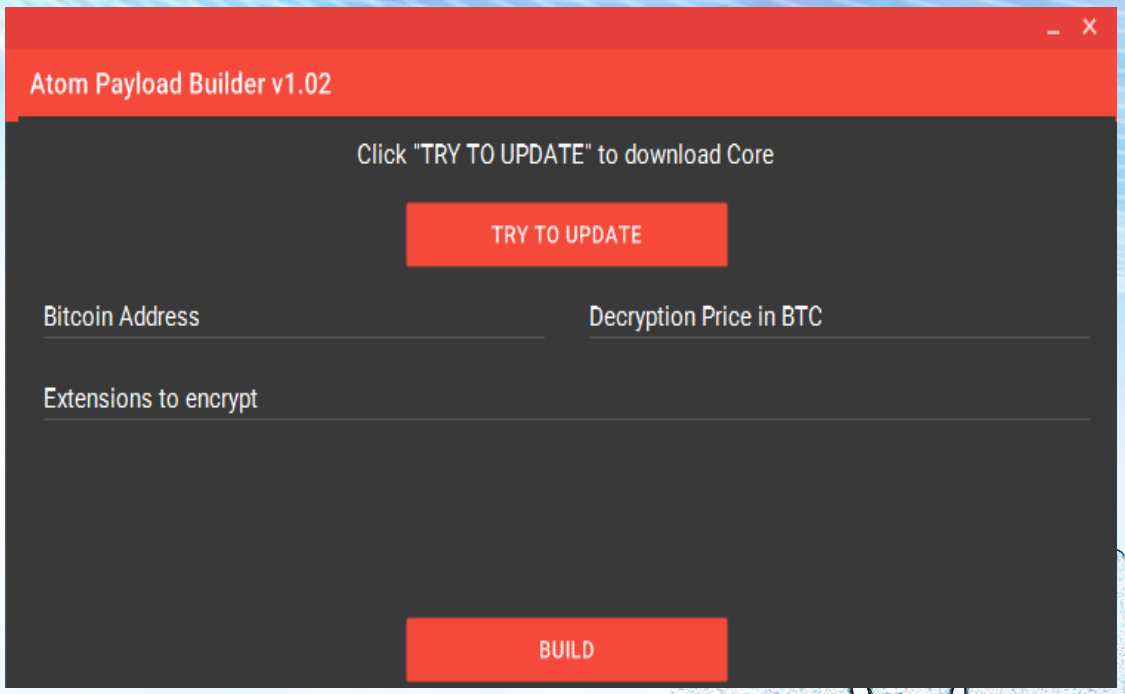
- **Samas Ransomware (Targeted Attack)** — 2016
  - Após infecção e ativação → busca por infecção de novos alvos conectados ao equipamento
- **RaaS (Ramsonware As A Service)**
  - Oferecido e negociado na "Deep Web"
  - Tarefa do "cliente" → Disseminar o malware
  - Até 80% de comissão/repasse para cada golpe bem sucedido
    - Shark Ransomware → Projeto Atom (Agosto/2016)

Ransomware
Evolução (Marcos Históricos)

- **RaaS (Ramsonware As A Service)** **2016**

- Bitcoin Address: Campo onde o "Cliente" cadastra sua "conta" para receber sua parte do lucro.
- Decryption Price in BTC: Valor que o ransomware vai exigir para o resgate.
- Extensions to encrypt: Lista de extensões de arquivos que o cryptovirus irá procurar para criptografar.

Interface de Interação do Projeto Atom "Ransomware Affiliate Program"



Ransomware
Proteção (Recomendações do CERT.BR)

Cartilha de Segurança para Internet

- http://cartilha.cert.br/ransomware

cert.br
Cartilha de Segurança para Internet

- Como devo me proteger de ransomware?
  - Para se proteger de ransomware você deve tomar os mesmos cuidados que toma para evitar os outros códigos maliciosos...
    - como ter um antivírus instalado e ser cuidadoso ao clicar em links ou abrir arquivos.
  - Fazer backups regularmente também é essencial para proteger os seus dados.
    - Se seu equipamento for infectado, a única garantia de que você conseguirá acessá-los novamente é possuir backups atualizados.
    - O pagamento do resgate não garante que você conseguirá restabelecer o acesso aos dados.

Ricardo Kléber

Ransomware

Países mais afetados (registros de ocorrências)

Countries	Machine count
United States	320948
Italy	78948
Canada	45840
United Kingdom	38068
Spain	35992
Turkey	32714
France	27941
Australia	25949
Brazil	24953
Taiwan	20448
Germany	19984
Republic of Korea	19842
Netherlands	18594
Mexico	16525
Russian Federation	13980
India	13783
Korea	13347
South Africa	10830
Romania	10220
Japan	9738

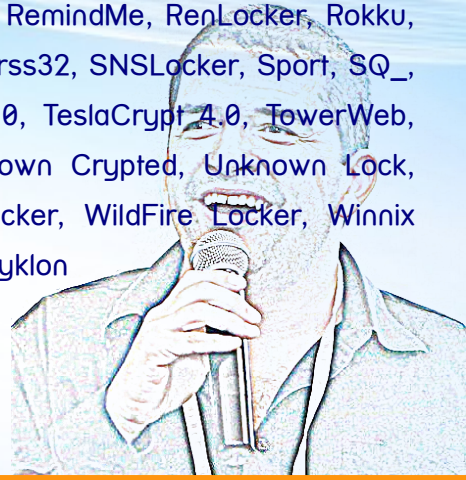
http://blogs.technet.microsoft.com/mmpc/2016/05/18/the-5ws-and-1h-of-ransomware/

Ransomware

Lista de Ransomware Identificados (ID-Ransomware)

7777, 7ev3n, 7h9r, 8lock8, ACCDFISA v2.0, Al-Namrood, Al-Namrood 2.0, Alcatraz, Alfa, Alma Locker, Alpha, AMBA, AngryDuck, Anubis, Apocalypse, Apocalypse (New Variant), ApocalypseVM, ASN1 Encoder, AutoLocky, AxCrypter, BadBlock, Bandarchor, BankAccountSummary, Bart, Bart v2.0, BitCrypt, BitCrypt 2.0, BitCryptor, BitStak, Black Feather, Black Shades, Blocatto, Booyah, Brazilian Ransomware, BTCLocker, Bucbi, BuyUnlockCode, Cerber, Cerber 2.0, Cerber 3.0, Cerber 4.0 / 5.0, CerberTear, Chimera, CHIP, CockBlocker, Coin Locker, CoinVault, Comrade Circle, Coverton, Cripton, Cryakl, CryFile, CryLocker, CrypMic, CrypMic, Crypren, Crypt0, Crypt0L0cker, Crypt38, CryptFuck, CryptInfinite, CryptoDefense, CryptoFinancial, CryptoFortress, CryptoHasYou, CryptoHitman, CryptoJoker, CryptoLuck, CryptoMix, Crypton, CryptorBit, CryptoRoger, CryptoShocker, CryptoTorLocker, CryptoWall 2.0, CryptoWall 3.0, CryptoWall 4.0, CryptoWire, CryptXXX, CryptXXX 2.0, CryptXXX 3.0, CryptXXX 4.0, CryPy, CrySiS, CTB-Faker, CTB-Locker, Deadly, DEDCryptor, Dharma, DirtyDecrypt, DMA Locker, DMA Locker 3.0, DMA Locker 4.0, Domino, Done, DXXD, ECLR Ransomware, EduCrypt, El Polocker, EncrypTile, EncryptoJJS, Encryptor RaaS, Enigma, Exotic, Fabiansomware, Fantom, FenixLocker, Flyper, FS0ciety, FuckSociety, GhostCrypt, Globe, GoldenEye, Gomasom, HadesLocker, Heimdall, HelpDCFile, Herbst, Hi Buddy!, HollyCrypt, HolyCrypt, Hucky, HydraCrypt, IFN643, iRansom, Ishtar, Jack.Pot, Jager, JapanLocker, Jigsaw, Jigsaw (Updated), JobCrypter, JuicyLemon, Karma, KawaiiLocker, KeRanger, KeyBTC, KEYHolder, KillerLocker, KimcilWare, Kolobo, Kostya, Kozy.Jozy, KratosCrypt, Kriptovor, KryptoLocker, LeChiffre, Lock93, LockLock, Locky, Lortok, LowLevel04, Magic, Maktub Locker, MarsJoke, Matrix, MirCop, MireWare, Mischa, Mobef, n1n1n1, NanoLocker, NCrypt, Negozl, Nemucod, Nemucod-7z, NMoreira, Nuke, NullByte, ODCODC, OMG! Ransomcrypt, OzozaLocker, PadCrypt, PaySafeGen, PClock, PClock (Updated), Philadelphia, PopCornTime, PowerLocky, PowerShell Locker, PowerWare, PrincessLocker, PrincessLocker 2.0, Protected Ransomware, R980, RAA-SEP, Radamant, Radamant v2.1, RansomCuck, RarVault, Razy, REKTLocker, RemindMe, RenLocker, Rokku, RotorCrypt, Russian EDA2, Sage, SamSam, Sanction, Satana, ShellLocker, ShinoLocker, Shujin, Simple_Encoder, Smrss32, SNSLocker, Sport, SQ_, Stampado, SuperCrypt, Surprise, SZFLocker, Team XRat, Telecrypt, TeslaCrypt 0.x, TeslaCrypt 2.x, TeslaCrypt 3.0, TeslaCrypt 4.0, TowerWeb, ToxCrypt, Trojan.Encoder.6491, Troldesh / Shade, TrueCrypter, UCCU, UmbreCrypt, UnblockUPC, Ungluk, Unknown Crypted, Unknown Lock, Unknown XTBL, Unlock92, Unlock92 2.0, USR0, Uyari, VaultCrypt, VenisRansomware, VenusLocker, VindowsLocker, WildFire Locker, Winnix Cryptor, WinRarer, WonderCrypter, XCrypt, Xorist, Xort, XRTN, XTP Locker 5.0, zCrypt, ZeroCrypt, ZimbraCryptor, Zyklon

252 (em 07/12/2016)



https://id-ransomware.malwarehunterteam.com

Ransomware Decryptor

Tabu 01: Não é possível desencriptar sem pagar o resgate (1/4)

Situações reversíveis (total ou parcialmente)

- Locker Ransomware
  - O autor do ransomware publicou todas as chaves de desencriptação;
  - Sucesso no uso de decryptor em 100% dos casos (até o momento).
- TorLocker
  - Pesquisadores descobriram erros no código (métodos utilizados para criptografar);
  - Sucesso no uso de decryptor em 70% dos casos.
- TeslaCrypt
  - Embora a mensagem informe que utiliza RSA-2048 usa, na verdade, AES;
  - Equipe da Cisco analisou, descobriu e desenvolveu um decryptor.

http://www.tripwire.com/state-of-security/security-data-protection/ransomware-happy-ending-10-known-decryption-cases/

Ransomware Decryptor

Tabu 01: Não é possível desencriptar sem pagar o resgate (2/4)

Situações reversíveis (total ou parcialmente)

- CoinVault e BitCryptor
  - Equipe da Kaspersky juntamente com a unidade de crimes de alta tecnologia da Holanda (NHTCU) e o Ministério Público dos Países Baixos analisaram e desenvolveram um decryptor.
- CryptoLocker
  - Versões iniciais deste Ransomware foram analisadas por equipes das empresas FireEye e Fox-IT que criaram um decryptor (DecryptCryptoLocker) que ajudou milhares de pessoas e empresas;
  - Novas versões foram produzidas e o decryptor não é mais eficaz (até o momento).

http://www.tripwire.com/state-of-security/security-data-protection/ransomware-happy-ending-10-known-decryption-cases/

Ransomware Decryptor

Tabu 01: Não é possível desencriptar sem pagar o resgate (3/4)

Lista (não exaustiva) de CryptoRansomware

com ferramentas de desencriptação (Decryptor)

- 777
- AI-Namrood
- Apocalypse
- ApocalypseVM
- Autolocky
- BadBlock
- CrypBoss
- CryptInfinite
- CryptoDefense
- CryptoLocker
- DMALocker2
- DMALockerCrypBoss
- Fabiansomware
- FenixLocker
- Globe
- Globe2
- Gomasom
- Harasom
- HydraCrypt
- KeyBTC
- LeChiffre
- Nemucod
- Nmoreira
- Operation Global III
- OzozaLocker
- PClock
- Petya
- Philadelphia
- Radamant
- Stampado
- TeslaCrypt
- UmbreCrypt
- Xorist
- XPan.XratTeam

http://www.thewindowsclub.com/list-ransomware-decryptor-tools

Ransomware Decryptor

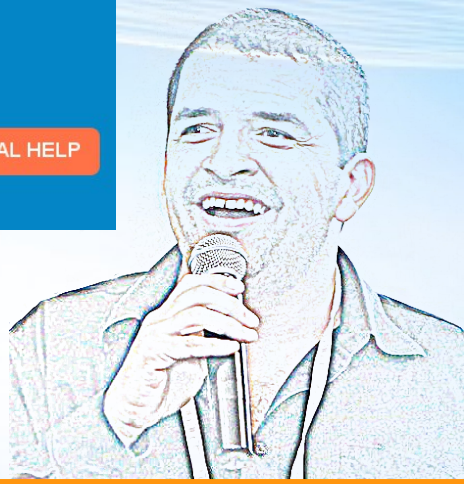
Tabu 01: Não é possível desencriptar sem pagar o resgate (4/4)

[Kaspersky Ransomware Decryptor (website)]

- **http://noransom.kaspersky.com**

[Emsisoft Decrypter (website)]

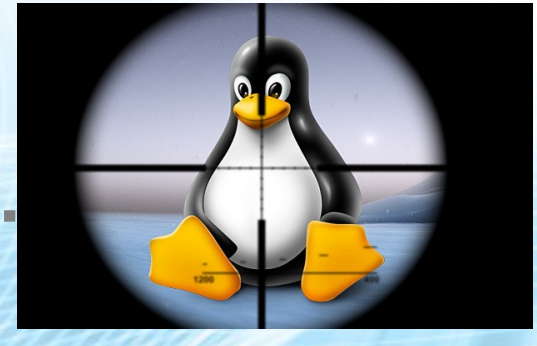
- **http://decrypter.emsisoft.com**



http://www.thewindowsclub.com/list-ransomware-decryptor-tools

Ransomware para Linux !!??

Tabu 02: O Pinguim está livre desse tipo de praga



- Linux/Ransm-C
  - Plataformas-alvo: Linux, System V Unix e FreeBSD (32 e 64 bits)
  - Alvos: Servidores Web e Bancos de Dados (encripta diretórios específicos)
  - Estaticamente compilados (não possui dependências)
- Fairware Ransomware
- Linux.Encoder.1

README_FOR_DECRYPT-2.txt

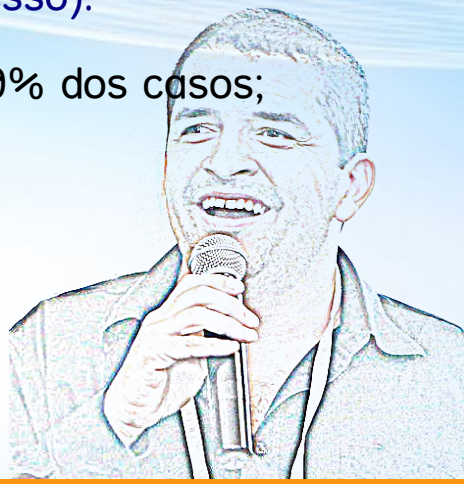
```
Your personal files are encrypted! Encryption was produced using a unique public key RSA-2048
generated for this computer.

To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow to decrypt the files, located on a secret
server at the Internet. After that, nobody and never will be able to restore files...

To obtain the private key and php script for this computer, which will automatically decrypt
files, you need to pay 1 bitcoin(s) (~420 USD).
Without this key, you will never be able to get your original files back.



!!!!!!!!!!!!!!!!!!!! PURSE FOR PAYMENT(ALSO AUTHORIZATION CODE):
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx !!!!!!!!!!!!!!!!!!!!
WEBSITE: https://z54n57pg2el6uze2.onion.to

INSTRUCTION FOR DECRYPT:
```

```
YOUR SERVER HAS BEEN INFECTED BY FAIRWARE | YOUR SERVER HAS BEEN INFECTED BY FAIRWARE
Hi,
Your server has been infected by a ransomware variant called FAIRWARE.
You must send 2 BTC to: 1DggzWksE2Y6DUX5GcNvHHCCDUGPde8WNL within 2 weeks from now to
retrieve your files and prevent them from being leaked!
We are the only ones in the world that can provide your files for you!
When your server was hacked, the files were encrypted and sent to a server we control!
You can e-mail fairware@sigaint.org for support, but please no stupid questions or
time
wasting! Only e-mail if you are prepared to pay or have sent payment! Questions such
as:
"can i see files first?" will be ignored.
We are business people and treat customers well if you follow what we ask.
FBI ADVISE FOR YOU TO PAY: https://www.tripwire.com/state-of-security/latest-security-
news/ransomware-victims-should-just-pay-the-ransom-says-the-fbi/
HOW TO PAY:
You can purchase BITCOINS from many exchanges such as:
http://okcoin.com
http://coinbase.com
http://localbitcoins.com
http://kraken.com
When you have sent payment, please send e-mail to fairware@sigaint.org with:
1) SERVER IP ADDRESS
2) BTC TRANSACTION ID
and we will then give you access to files, you can delete files from us when done
Goodbye!
```

Ransomware: Novidade no Combate

Detectando em "tempo real" novos CryptoRansonware

- CryptoDrop
  - Apresentado na 2016 IEEE 36th International Conference on Distributed Computing Systems
    - **http://www.cise.ufl.edu/~traynor/papers/scaife-icdcs16.pdf**
  - Sistema de "detecção precoce" que alerta usuário sobre atividade "suspeita"
    - Uso de "indicadores de comportamento"
      - Aumento nas operações envolvendo criptografia;
      - Alterações em determinados tipos de arquivos (principais arquivos de usuários);
    - Pode interromper processo que começa a alterar dados do usuário (criptografia!?);
    - Testes → Perda de 10 arquivos em média (até detecção e parada do processo).
    - Testado com 492 variantes de ransomware → detecção e bloqueio em 100% dos casos;
    - Falso-positivos com uso normal de PGP/GPG e aplicativos de compressão (aplicação em muitos arquivos)



http://news.softpedia.com/news/cryptodrop-gives-users-hope-to-prevent-ransomware-infections-in-the-future-506187.shtml

Ransomware: Novidade no Combate

Detectando em "tempo real" novos CryptoRansonware

- CryptoStalker
  - Ferramenta que monitora/detecta Ransomware em sistemas Linux
    - **http://github.com/unixist/cryptostalker**
  - Precursor do CryptoDrop (CryptoStalker → Março/2016 | CryptoDrop → Julho/2016)

Branch: master ▾ randumb / cryptostalker.py

Executable File | 76 lines (64 sloc) | 2.3 KB | Raw | Blan

```
1  import argparse
2  import inotify.adapters
3  import os
4  import sys
5  import time
6
7  from randumb import Random
8
9  class Stalk(object):
10   def __init__(self, path, count, window):
11     self.path = path
12     self.count = count
13     self.window = window
14     self.files = []
15     self.last = time.time()
16
```

http://news.softpedia.com/news/cryptostalker-a-tool-to-detect-crypto-ransomware-on-linux-502002.shtml

Ransomware: Novidade no Combate

Detectando em "tempo real" novos CryptoRansonware

- Solução semelhante Kaspersky (distribuição gratuita)
  - Anti-Ransomware Tool for Business
  - **http://go.kaspersky.com/Anti-ransomware-tool.html**
  - Módulos Utilizados:
    - Kaspersky Security Network: Anti-ransomware com base na nuvem
    - Inspetor do Sistema: Monitora eventos do sistema proativamente
      - Criação/modificação de arquivos e configurações do sistema operacional
      - Execução de programas e troca de dados pela rede
      - Bloqueio e reversão de processos com uso de criptografia

Projeto Ransomware (Open Source)

Hidden-Tear

- **http://github.com/utkusen/hidden-tear**

  - Open Source Ransomware Honeypot
    - Busca e encripta arquivos ".txt", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".odt", ".jpg", ".png", ".csv", ".sql", ".mdb", ".sln", ".php", ".asp", ".aspx", ".html", ".xml", ".psd";
    - Utiliza, por padrão, AES 256;
    - Facilmente customizável (alterar tipos de arquivos e método de criptografia p.ex.);
  - Projeto abandonado :(
  - Contato para interessados:

    http://utkusen.com/en/contact.html

Projeto Anti-Ransomware (Open Source)
C0p3rnic0/Protein

- http://github.com/c0p3rnic0/PROTEIN

- Powershell Anti-Ransomware
  - Script para monitoramento ativo de arquivos em servidores de arquivos em busca de ransomware conhecidos ou desconhecidos.
- Além dos códigos-fonte vídeos demonstrativos;
- Identifica e analisa a criação de novos arquivos;
- Uso de blacklists (ameaças potenciais) e whitelists (arquivos conhecidos);
- Envio de alertas por e-mail para administradores quando novos ransomware forem detectados;
- Exibição de mensagem no computador do usuário, quando um novo ransomware for detectado;
- Desativa o usuário afetado no domínio, impedindo o acesso ao sistema pelo ransomware;
- Bloqueia o acesso a rede (via MAC Address) pelo computador do usuário afetado pelo ransomware.

Sugestão de Leitura (site em constante atualização)

Ransomware Overview

- Planilha com informações sobre Ransomwares:
  - Nome (identificação);
  - Extensões utilizadas;
  - Algoritmos (criptografia) utilizados;
  - Outros nomes pelos quais são conhecidos;
  - Decryptor (se disponível): URL para download;
  - Informações complementares.
- Versão Web (HTML):
  - **http://www.nyxbone.com/malware/RansomwareOverview.html**
- Google Docs (shortcode):
  - **http://goo.gl/b9R8DE**

https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdjWdCEsGIM0Y0Hvmc5g/pubhtml

Ransomware Overview

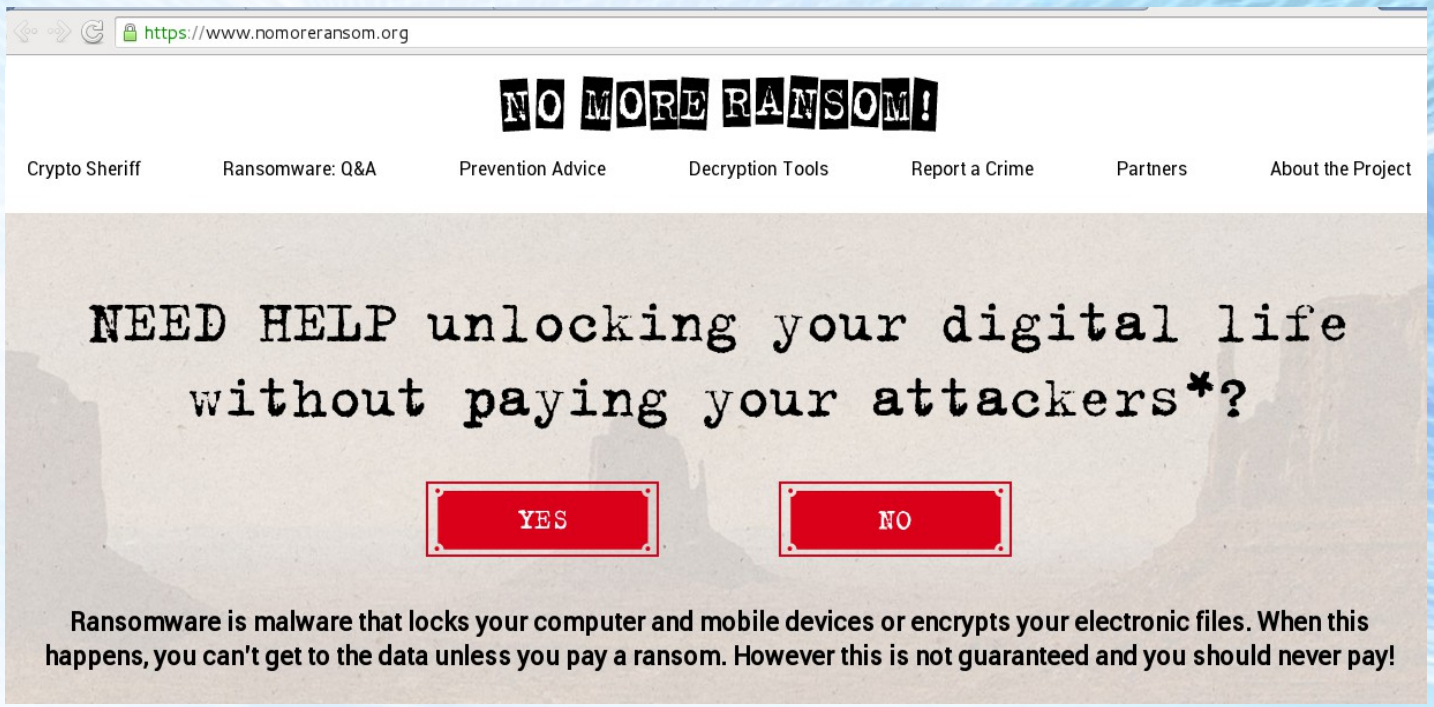
Ransomware | Unidentified | Detection | Prevention | Infographics | Download | Sources and Contributors

Name	Extensions	Extension Pattern	Ransom Note Filename(s)	Comment	Encryption Algorithm
.CryptoHasYou.	.enc		YOUR_FILES_ARE_LOCKED.txt		AES(256)
777	.777	_[timestamp]_$[email]$.777 e.g. ._14-05-2016-11-59-36_$ni	read_this_file.txt		XOR
7ev3n	.R4A .R5A		FILES_BACK.txt		
7h9r	.7h9r		README_.TXT		AES
8lock8	.8lock8		READ_IT.txt	Based on HiddenTear	AES (256)
Alfa Ransomware	.bin		README HOW TO DECRYPT YOUR F	Made by creators of Cerber	
Alma Ransomware	random	random(x5)			AES(128)
Alpha Ransomware	.encrypt		Read Me (How Decrypt) !!!!.txt		AES(256)
AMBA	.amba		ПРОЧТИ_МЕНЯ.txt READ_ME.txt	Websites only amba@riseup.net	
Angry Duck	.adk			Demands 10 BTC	
Apocalypse	.encrypted .SecureCrypted .FuckYourData .unavailable .bleepYourFiles .Where_my_files.txt		*.How_To_Decrypt.txt *.Contact_Here_To_Recover_Your_ *.Where_my_files.txt *.Read_Me.Txt	decryptionservice@mail.ru recoveryhelp@bk.ru ransomware.attack@list.ru esmeraldaencryption@mail.ru dr.compress@bk.ru	
ApocalypseVM	.encrypted .locked		*.How_To_Get_Back.txt	Apocalypse ransomware version which uses VMprotect	
AutoLocky	.locky		info.txt info.html		
BadBlock			Help Decrypt.html		

Sugestão de Leitura (site em constante atualização)

No More Ransom!

- **http://www.nomoreransom.org**



- Parceria: Europol / Polícia da Holanda / EUA (ic3.gov) / Kaspersky / Intel
- Dicas de prevenção / Perguntas frequentes;
- Denúncia (Report a Crime);
- Análise de arquivos criptografados (upload).

Sugestão de Leitura (sites em constante atualização)

Melhores Sites com Fóruns sobre o Assunto

- Malwaresbytes
  - `http://forums.malwarebytes.org`
- Bleeping Computer
  - `http://www.bleepingcomputer.com/forums/f/239/ransomware-help-tech-support`

Malwarebytes

bleepingcomputer
From a bleeping computer to a working computer

Sugestão de Leitura (complementar)

Guia OWASP

OWASP – Open Web Application Security Project

- Anti-Ransomware Guide
  - Versão 1.2 (11/10/2016)
  - Medidas para proteção de perímetro, mitigação e endpoints
  - **http://www.owasp.org/index.php/OWASP_Anti-Ransomware_Guide_Project**

OWASP
Open Web Application Security Project

Sugestão de Leitura (complementar)

Links Relacionados

- Security Response: Evolution of Ransomware (Symantec)
  - **http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf**
- Report Ransomware 2014-2016 (Kaspersky)
  - **httpKSN://securelist.com/files/2016/06/KSN_Report_Ransomware_2014-2016_final_ENG**.pdf
- Threats Predictions 2016 (McAfee)
  - **http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf**

RANSOMWARE

(Sequestro de Dados)

GTER 42 | GTS 28

07 a 09 de Dezembro de 2016, São Paulo

O que fazer?

Perguntas !?

Informações Complementares !?

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Ransonware (Sequestro de Dados): O que fazer?

ricardokleber@ricardokleber.com

www.segurancaderedes.com.br

www.youtube.com/segurancaderedes