Ransomware

backup e outras medidas preventivas

GTS–27 Uberlândia, Maio de 2016

Danton Nunes <danton.nunes@inexo.com.br>
Internexo Ltda. São José dos Campos, SP

Do que se trata a encrenca?

Um programa clandestino que cifra os arquivos a que tem acesso.

Do que se trata a encrenca?

Um programa clandestino que cifra os arquivos a que tem acesso.

Normalmente usa criptografia "pesada": AES, com selo cifrado por RSA com chave de 2048+ bits.

Do que se trata a encrenca?

Um programa clandestino que cifra os arquivos a que tem acesso.

Normalmente usa criptografia "pesada": AES, com selo cifrado por RSA com chave de 2048+ bits.

Exige um resgate, normalmente pago em Bitcoins, pela dark–web, para decifrar os arquivos.

Do que se trata a encrenca?

Um programa clandestino que cifra os arquivos a que tem acesso.

Normalmente usa criptografia "pesada": AES, com selo cifrado por RSA com chave de 2048+ bits.

Exige um resgate, normalmente pago em Bitcoins, pela dark–web, para decifrar os arquivos.

Há ataques contra praticamente todos os sistemas operacionais. Você acha que está seguro porque roda Linux, FreeBSD, ou MacOS–X?

Do que se trata a encrenca?

Um programa clandestino que cifra os arquivos a que tem acesso.

Normalmente usa criptografia "pesada": AES, com selo cifrado por RSA com chave de 2048+ bits.

Exige um resgate, normalmente pago em Bitcoins, pela dark–web, para decifrar os arquivos.

Há ataques contra praticamente todos os sistemas operacionais. Você acha que está seguro porque roda Linux, FreeBSD, ou MacOS–X?
– You know nothing, Jon Snow!

Do que se trata a encrenca?

Processo de infecção: por email, links deceptivos, redes sociais (um pouco do de sempre, com a ajuda do usuário!).

Do que se trata a encrenca?

Processo de infecção: por email, links deceptivos, redes sociais (um pouco do de sempre, com a ajuda do usuário!).

Alguns aplicativos de sequestro de dados são altamente sofisticados na arte de enganar detectores de vírus.

Do que se trata a encrenca?

***Processo de infecção*: por email, links deceptivos, redes sociais (um pouco do de sempre, com a ajuda do usuário!).**

Alguns aplicativos de sequestro de dados são altamente sofisticados na arte de enganar detectores de vírus.

Normalmente não se preocupam em escalar privilégios, sequestrar os arquivos a que o usuário tem acesso já faz estrago suficiente.

Do que se trata a encrenca?

***Processo de infecção*: por email, links deceptivos, redes sociais (um pouco do de sempre, com a ajuda do usuário!).**

Alguns aplicativos de sequestro de dados são altamente sofisticados na arte de enganar detectores de vírus.

Normalmente não se preocupam em escalar privilégios, sequestrar os arquivos a que o usuário tem acesso já faz estrago suficiente.

Costumam cifrar tanto arquivos locais quanto em rede, bem como danificar ou remover os backups locais (sombra)

Do que se trata a encrenca?

***Processo de infecção*: por email, links deceptivos, redes sociais (um pouco do de sempre, com a ajuda do usuário!).**

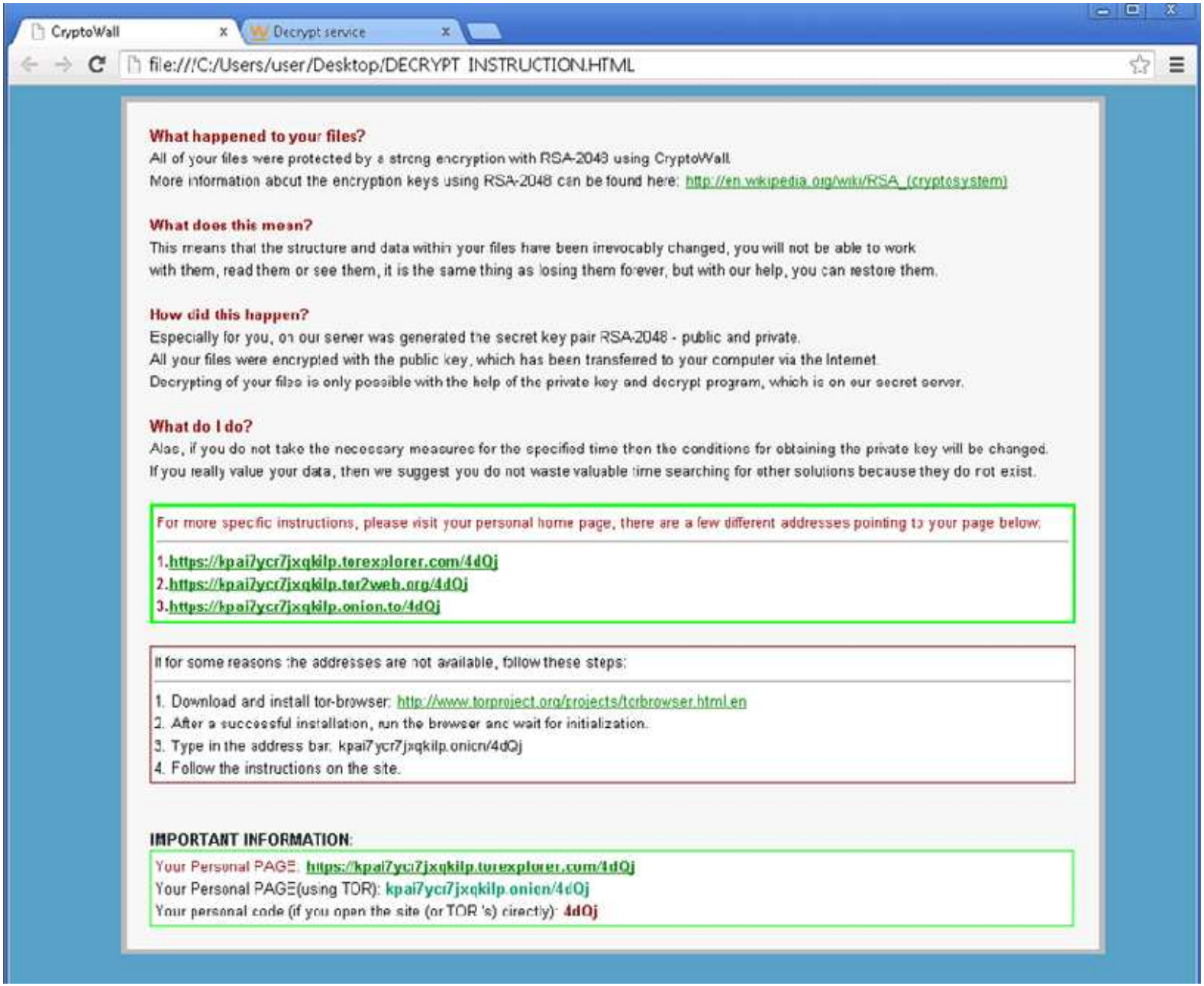
Alguns aplicativos de sequestro de dados são altamente sofisticados na arte de enganar detectores de vírus.

Normalmente não se preocupam em escalar privilégios, sequestrar os arquivos a que o usuário tem acesso já faz estrago suficiente.

Costumam cifrar tanto arquivos locais quanto em rede, bem como danificar ou remover os backups locais (sombra)

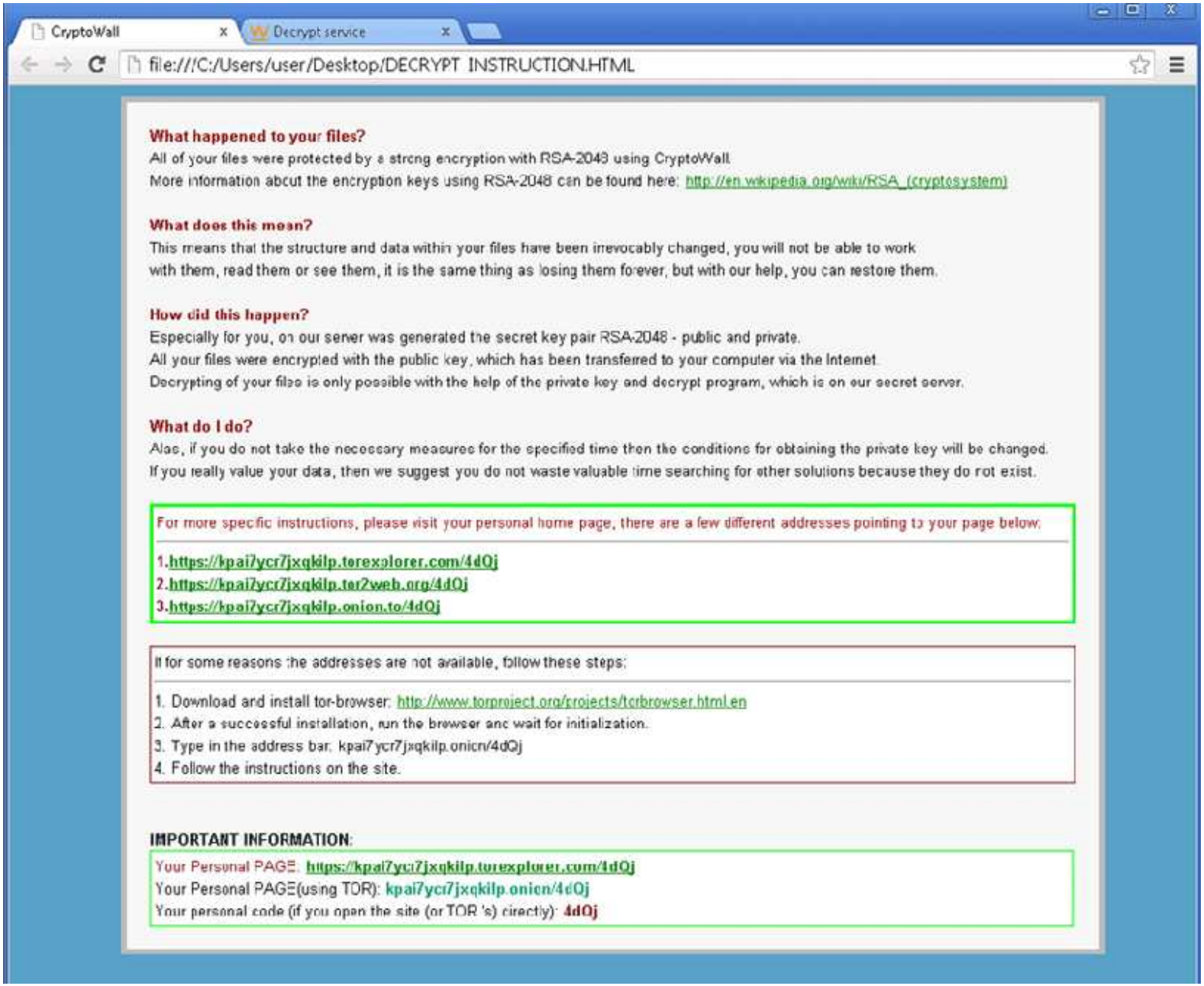
Mais famosos: CryptoLocker, CryptoWall, KeRanger (OS–X), Linux.Encoder.1 (para Linux e alguns sabores de BSD!)

Do que se trata a encrenca?



Do que se trata a encrenca?

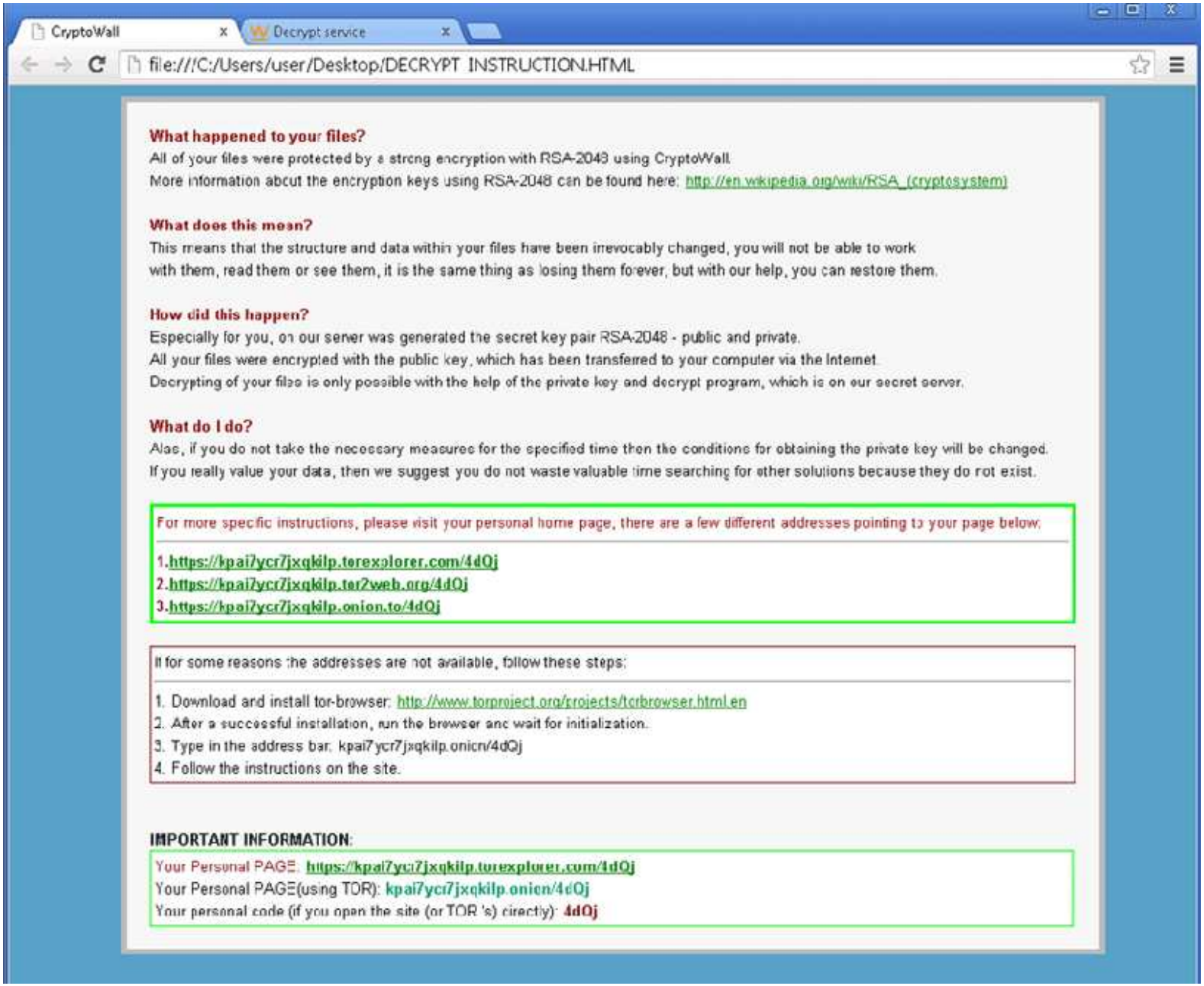
Aviso do CryptoWall sobre o estrago feito aos seus dados.



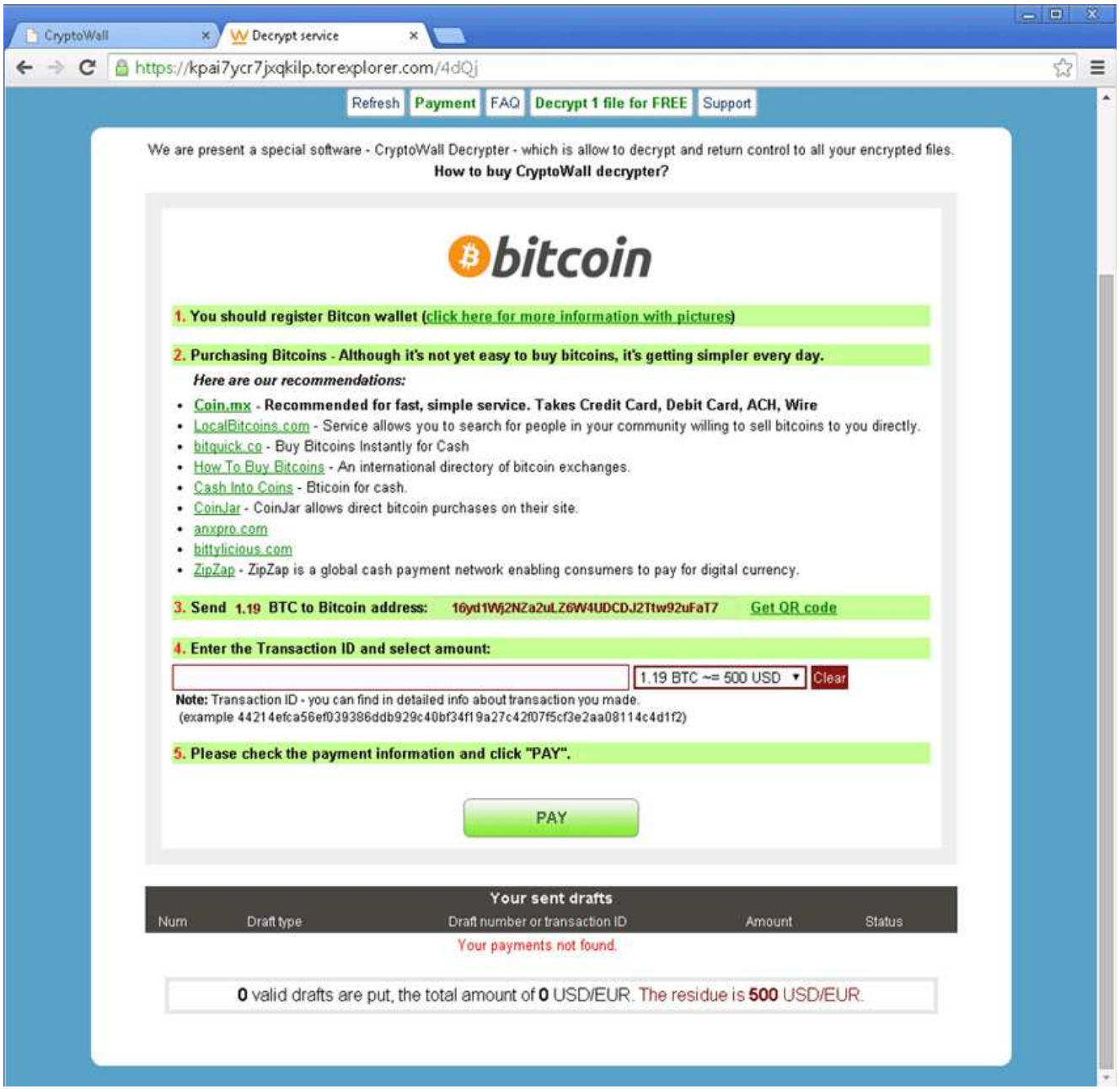
Do que se trata a encrenca?

Aviso do CryptoWall sobre o estrago feito aos seus dados.

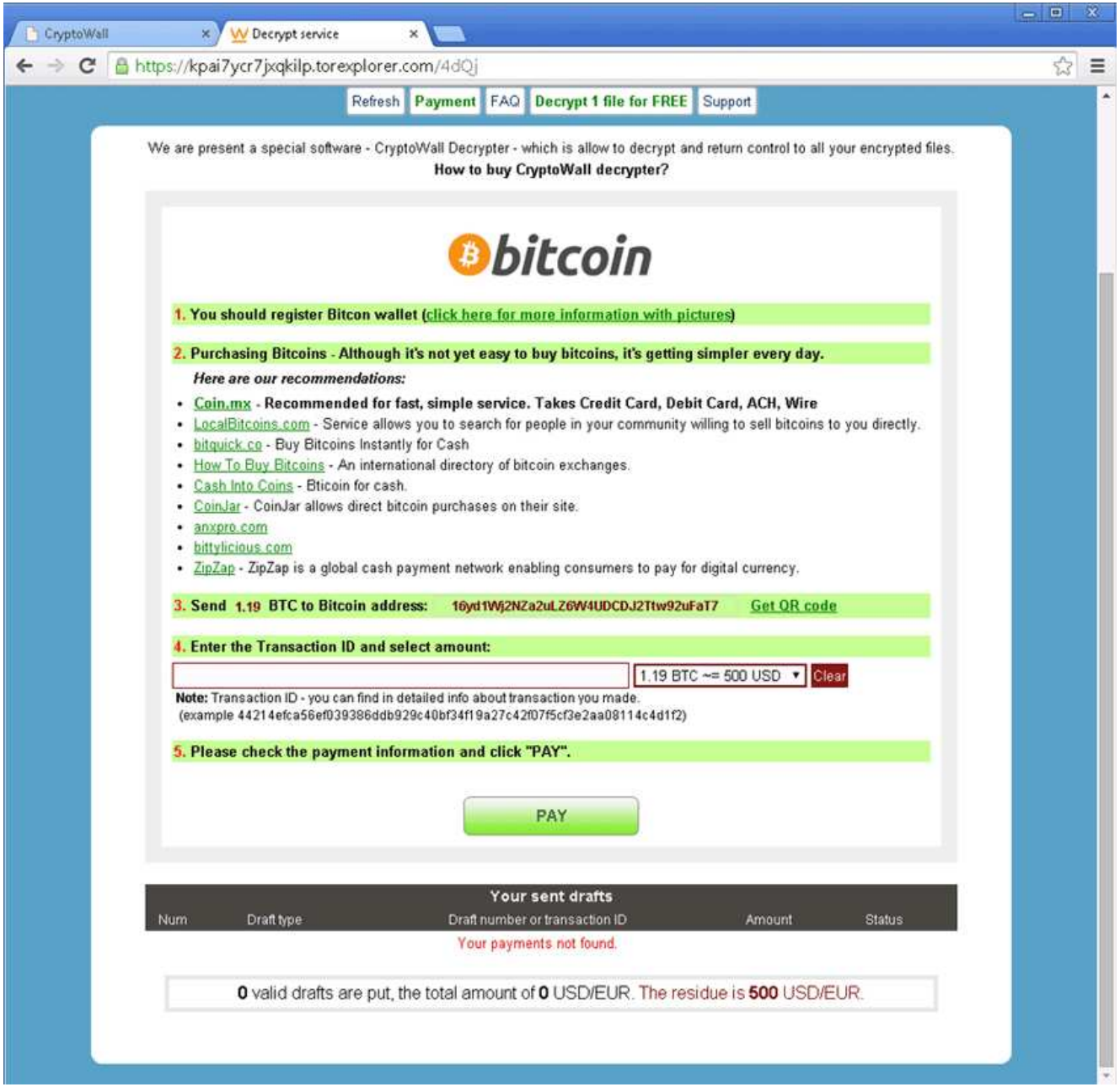
A lingua–gem é até muito bem educada para um bandido!



Do que se trata a encrenca?



Do que se trata a encrenca?



típico pedido de resgate do CryptoWall, com detalhadas instruções sobre como fazer pagamentos com Bitcoin a um sequestrador desconhecido!

O pior aconteceu, e agora?

O pior aconteceu, e agora?

1. Mantenha a calma. Banana opcional.

O pior aconteceu, e agora?

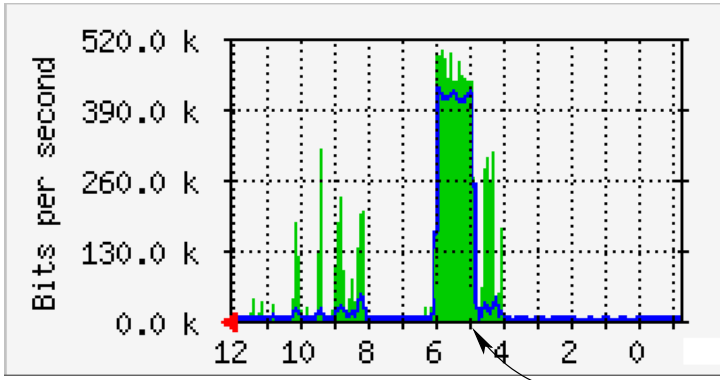
1. Mantenha a calma. Banana opcional.

2. Identifique a fonte do ataque, o que pode ser complicado em rede com muitas estações de trabalho. O MRTG/Nagios/... pode ser útil nesse ponto porque durante o ataque o perfil de tráfego é atípico.

O pior aconteceu, e agora?

1. Mantenha a calma. Banana opcional.

2. Identifique a fonte do ataque, o que pode ser complicado em rede com muitas estações de trabalho. O MRTG/Nagios/... pode ser útil nesse ponto porque durante o ataque o perfil de tráfego é atípico.

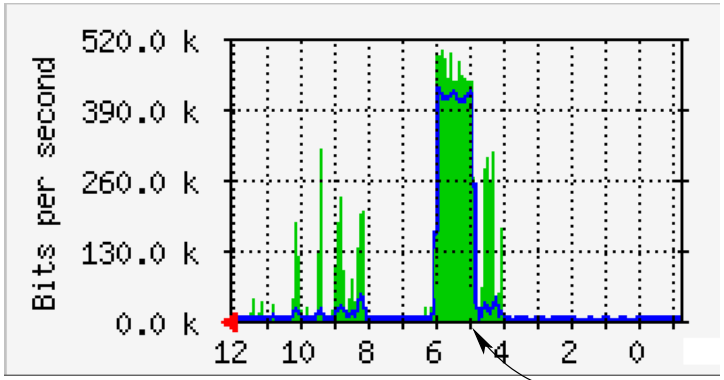


possível início do ataque, marcado por súbito aumento do tráfego na rede local.

O pior aconteceu, e agora?

1. Mantenha a calma. Banana opcional.

2. Identifique a fonte do ataque, o que pode ser complicado em rede com muitas estações de trabalho. O MRTG/Nagios/... pode ser útil nesse ponto porque durante o ataque o perfil de tráfego é atípico.



possível início do ataque, marcado por súbito aumento do tráfego na rede local.

Mas quanta gente monitora TODAS as portas de TODOS os comutadores do tecido de chaveamento?

O pior aconteceu, e agora?

3. Se você tem como recuperar os arquivos de um backup?

O pior aconteceu, e agora?

3. Se você tem como recuperar os arquivos de um backup?
– sim: prossiga;

O pior aconteceu, e agora?

3. Se você tem como recuperar os arquivos de um backup?
– sim: prossiga;
– não: ainda há alguma esperança, mas pode pensar em comprar Bitcoins para pagar o resgate.

O pior aconteceu, e agora?

3. Se você tem como recuperar os arquivos de um backup?

– sim: prossiga;

– não: ainda há alguma esperança, mas pode pensar em comprar Bitcoins para pagar o resgate.

A polícia holandesa possui um conjunto de chaves privadas recuperadas de criminosos que estão presos. Se uma dessas chaves servir, Aleluia!

O pior aconteceu, e agora?

3. Se você tem como recuperar os arquivos de um backup?
– sim: prossiga;
– não: ainda há alguma esperança, mas pode pensar em comprar Bitcoins para pagar o resgate.

> ***A polícia holandesa possui um conjunto de chaves privadas recuperadas de criminosos que estão presos. Se uma dessas chaves servir, Aleluia!***

4. Certifique–se de que o programa sequestrador foi realmente terminado ou a estação contaminada removida da rede.

O pior aconteceu, e agora?

3. Se você tem como recuperar os arquivos de um backup?
– sim: prossiga;
– não: ainda há alguma esperança, mas pode pensar em comprar Bitcoins para pagar o resgate.

> ***A polícia holandesa possui um conjunto de chaves privadas recuperadas de criminosos que estão presos. Se uma dessas chaves servir, Aleluia!***

4. Certifique–se de que o programa sequestrador foi realmente terminado ou a estação contaminada removida da rede.

5. Recupere os arquivos do backup.

O pior aconteceu, e agora?

3. Se você tem como recuperar os arquivos de um backup?
– sim: prossiga;
– não: ainda há alguma esperança, mas pode pensar em comprar Bitcoins para pagar o resgate.

> ***A polícia holandesa possui um conjunto de chaves privadas recuperadas de criminosos que estão presos. Se uma dessas chaves servir, Aleluia!***

4. Certifique–se de que o programa sequestrador foi realmente terminado ou a estação contaminada removida da rede.

5. Recupere os arquivos do backup.

Existe vida além do backup!

Existe vida além do backup!

Backup é aquela coisa que todo o mundo sabe que tem que fazer, mas...

Existe vida além do backup!

Backup é aquela coisa que todo o mundo sabe que tem que fazer, mas...

Há outras formas de proteger os dados contra sequestro, mais automáticas e que permitem recuperação mais rápida e mais recente que os esquemas tradicionais de backup:

Existe vida além do backup!

Backup é aquela coisa que todo o mundo sabe que tem que fazer, mas...

Há outras formas de proteger os dados contra sequestro, mais automáticas e que permitem recuperação mais rápida e mais recente que os esquemas tradicionais de backup:

– Armazenamento em servidores em rede tipo "write–once", de modo que qualquer dado no passado possa ser recuperado. Exemplo: Venti, do Plan9 from Bell Labs

Existe vida além do backup!

Backup é aquela coisa que todo o mundo sabe que tem que fazer, mas...

Há outras formas de proteger os dados contra sequestro, mais automáticas e que permitem recuperação mais rápida e mais recente que os esquemas tradicionais de backup:

– Armazenamento em servidores em rede tipo "write–once", de modo que qualquer dado no passado possa ser recuperado. Exemplo: Venti, do Plan9 from Bell Labs

– Sistemas de arquivos com pontos de controle (checkpoint) A estrutura de arquivos e pastas em cada ponto de controle pode ser recuperada facilmente. Exemplos: Fossil, do Plan9, e nilfs, da NTT.

Sistemas de arquivos com pontos de controle

Sistemas de arquivos com pontos de controle

Operação super simples: qualquer ponto de controle no passado pode ser montado como um sistema de arquivos comum. Normalmente monta–se com a opção "ro".

Sistemas de arquivos com pontos de controle

Operação super simples: qualquer ponto de controle no passado pode ser montado como um sistema de arquivos comum. Normalmente monta–se com a opção "ro".

No caso do Fossil, não há necessidade de ser "root" para montar os pontos de controle do passado.

Sistemas de arquivos com pontos de controle

Operação super simples: qualquer ponto de controle no passado pode ser montado como um sistema de arquivos comum. Normalmente monta–se com a opção "ro".

No caso do Fossil, não há necessidade de ser "root" para montar os pontos de controle do passado.

Uma vez que tenha sido identificado o instante em que o ataque foi iniciado, basta montar o ponto de controle imediatamente anterior para recuperar uma imagem exata do estado dos dados ainda não cifrados.

Sistemas de arquivos com pontos de controle

Operação super simples: qualquer ponto de controle no passado pode ser montado como um sistema de arquivos comum. Normalmente monta–se com a opção "ro".

No caso do Fossil, não há necessidade de ser "root" para montar os pontos de controle do passado.

Uma vez que tenha sido identificado o instante em que o ataque foi iniciado, basta montar o ponto de controle imediatamente anterior para recuperar uma imagem exata do estado dos dados ainda não cifrados.

Resultado: tempo de recuperação mínimo e perda de dados entre mínima e nula!

Sistemas de arquivos com pontos de controle

Por outro lado...

Sistemas de arquivos com pontos de controle

Por outro lado...

Sistemas de arquivos com pontos de controle devoram discos, apesar de contarem com algoritmos para evitar duplicidade de blocos e alguma mágica de compressão de dados.

Sistemas de arquivos com pontos de controle

Por outro lado...

Sistemas de arquivos com pontos de controle devoram discos, apesar de contarem com algoritmos para evitar duplicidade de blocos e alguma mágica de compressão de dados.

Por exemplo, um sistema baseado no nilfs da NTT pode precisar de mais que o dobro do espaço útil para manter poucos meses de pontos de controle no passado.

Sistemas de arquivos com pontos de controle

Por outro lado...

Sistemas de arquivos com pontos de controle devoram discos, apesar de contarem com algoritmos para evitar duplicidade de blocos e alguma mágica de compressão de dados.

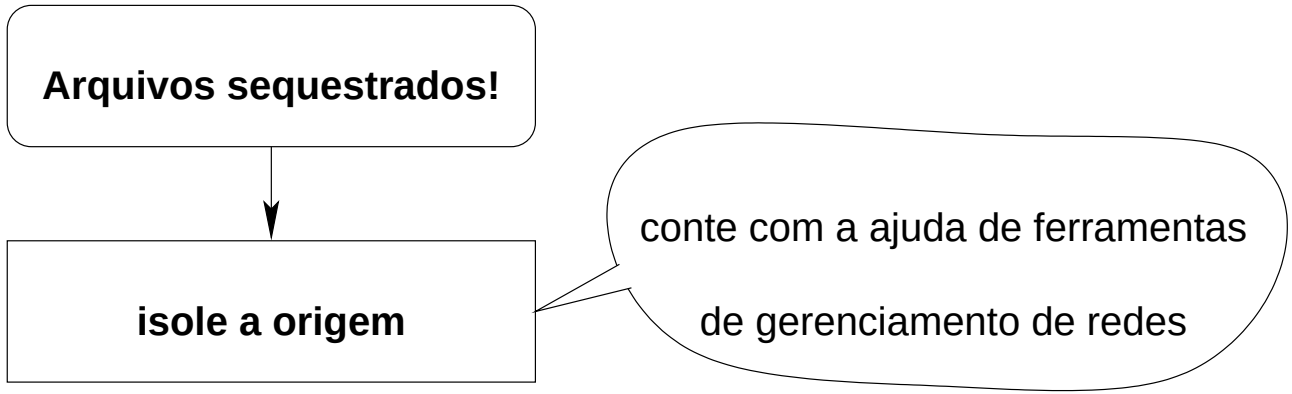
Por exemplo, um sistema baseado no nilfs da NTT pode precisar de mais que o dobro do espaço útil para manter poucos meses de pontos de controle no passado.

O lado bom é que o preço dos discos vem caindo nos últimos anos, tornando tais sistemas cada vez mais viáveis economicamente.

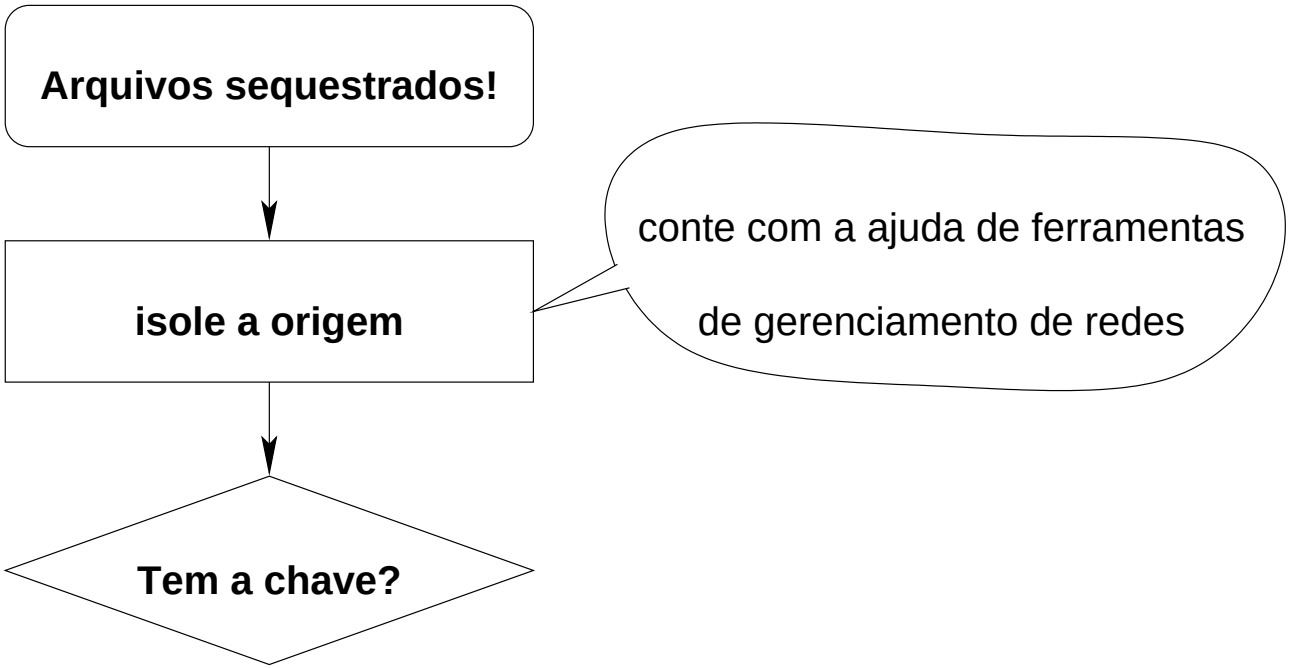
Resumo da novela

Arquivos sequestrados!

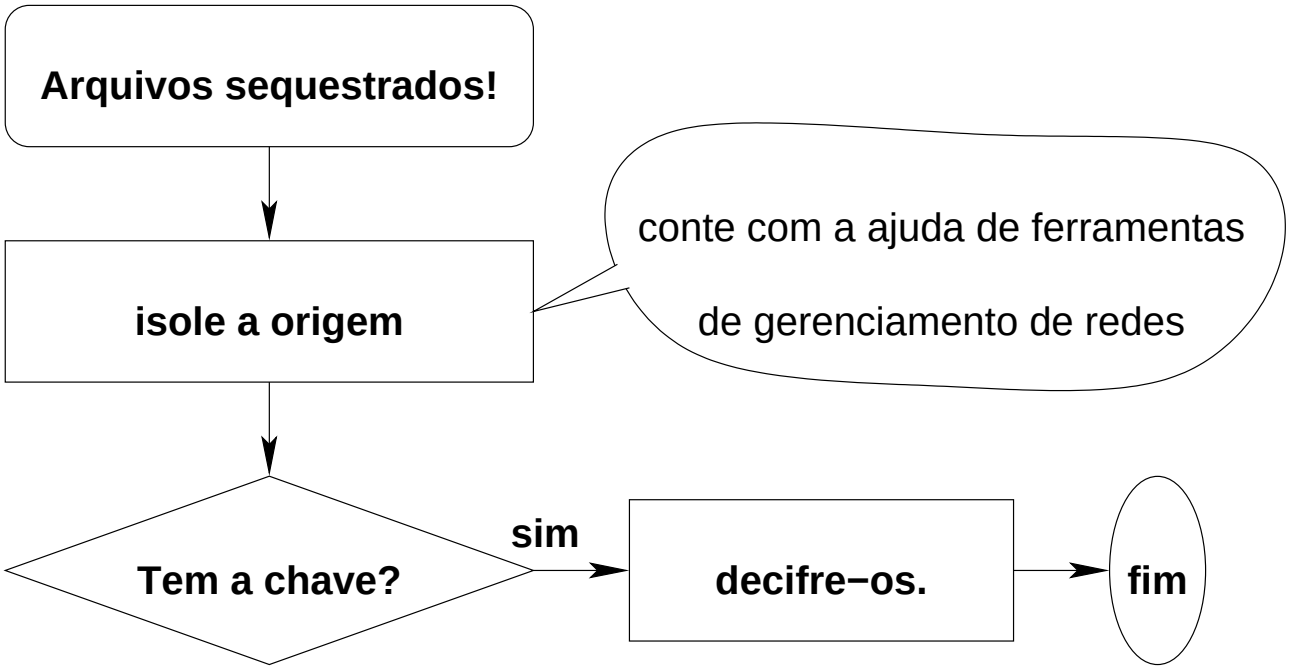
Resumo da novela



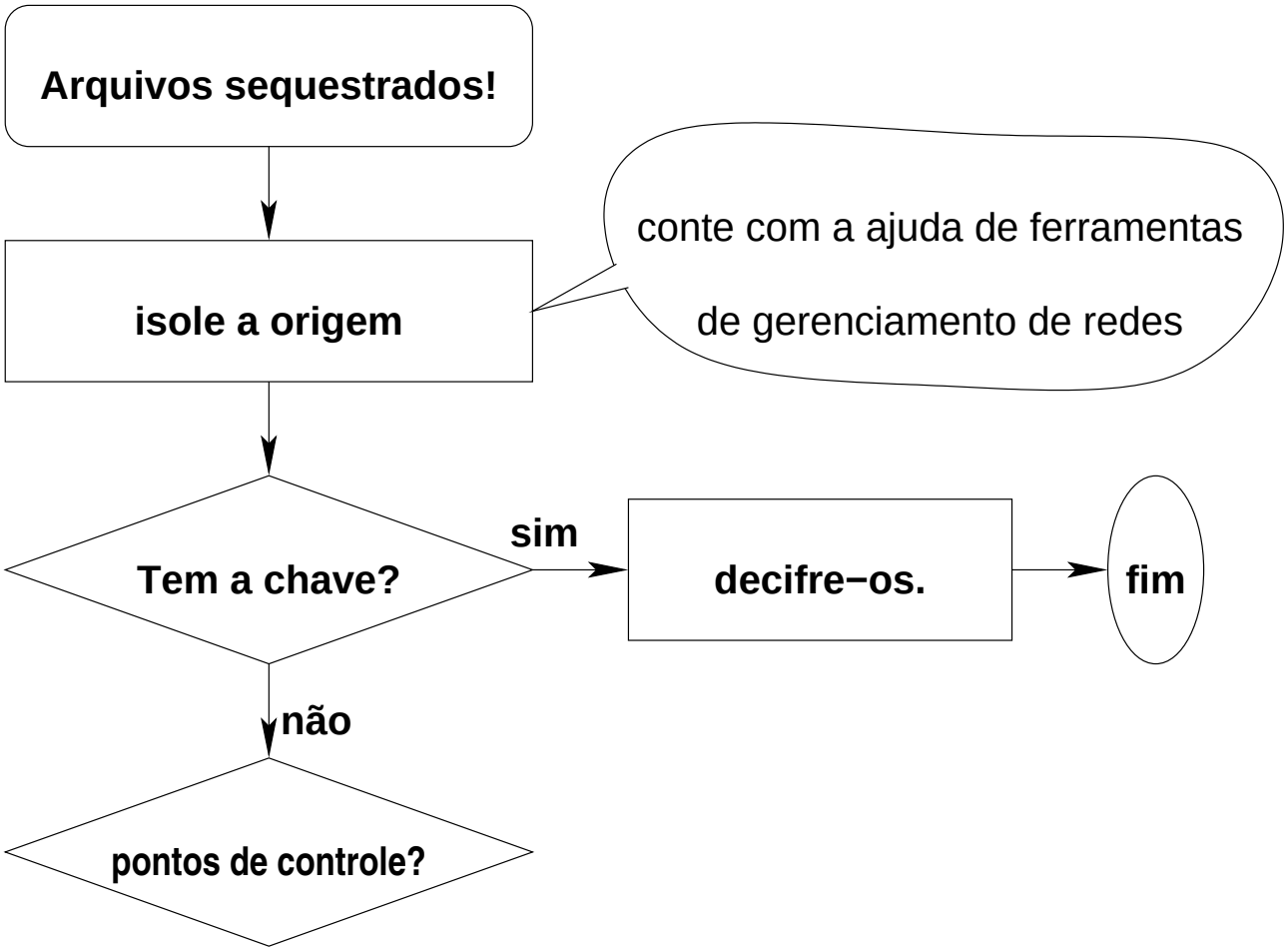
Resumo da novela



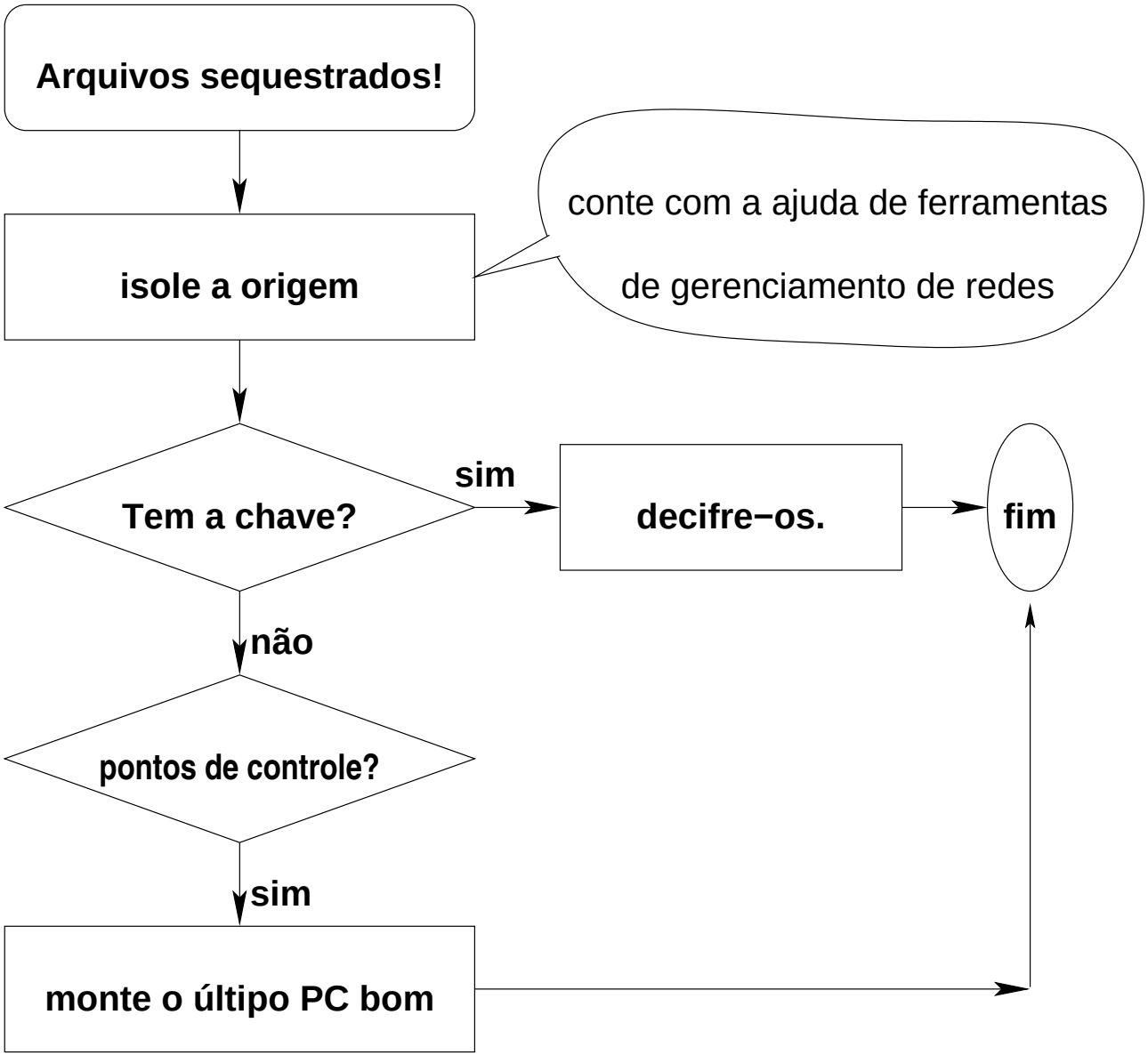
Resumo da novela



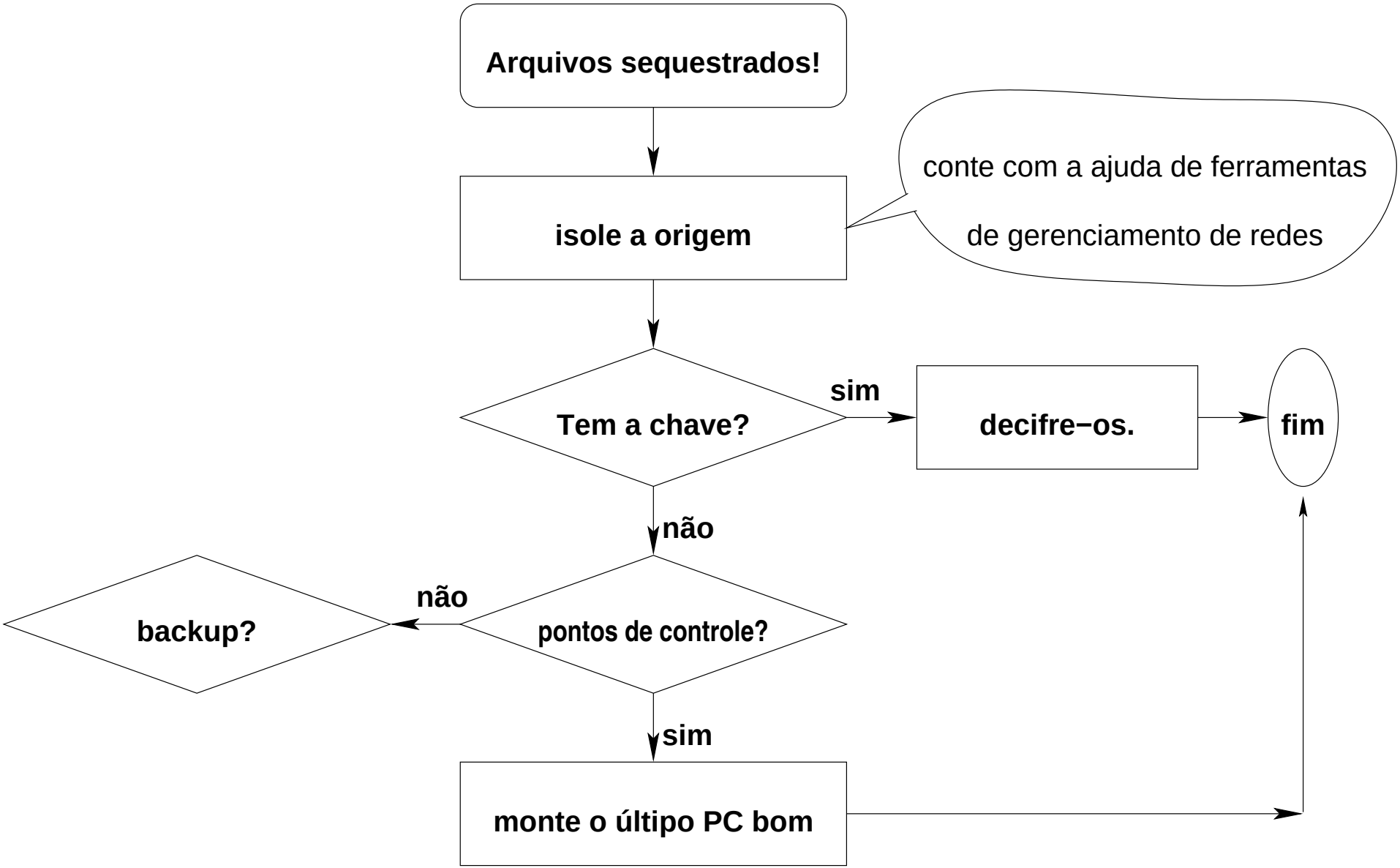
Resumo da novela



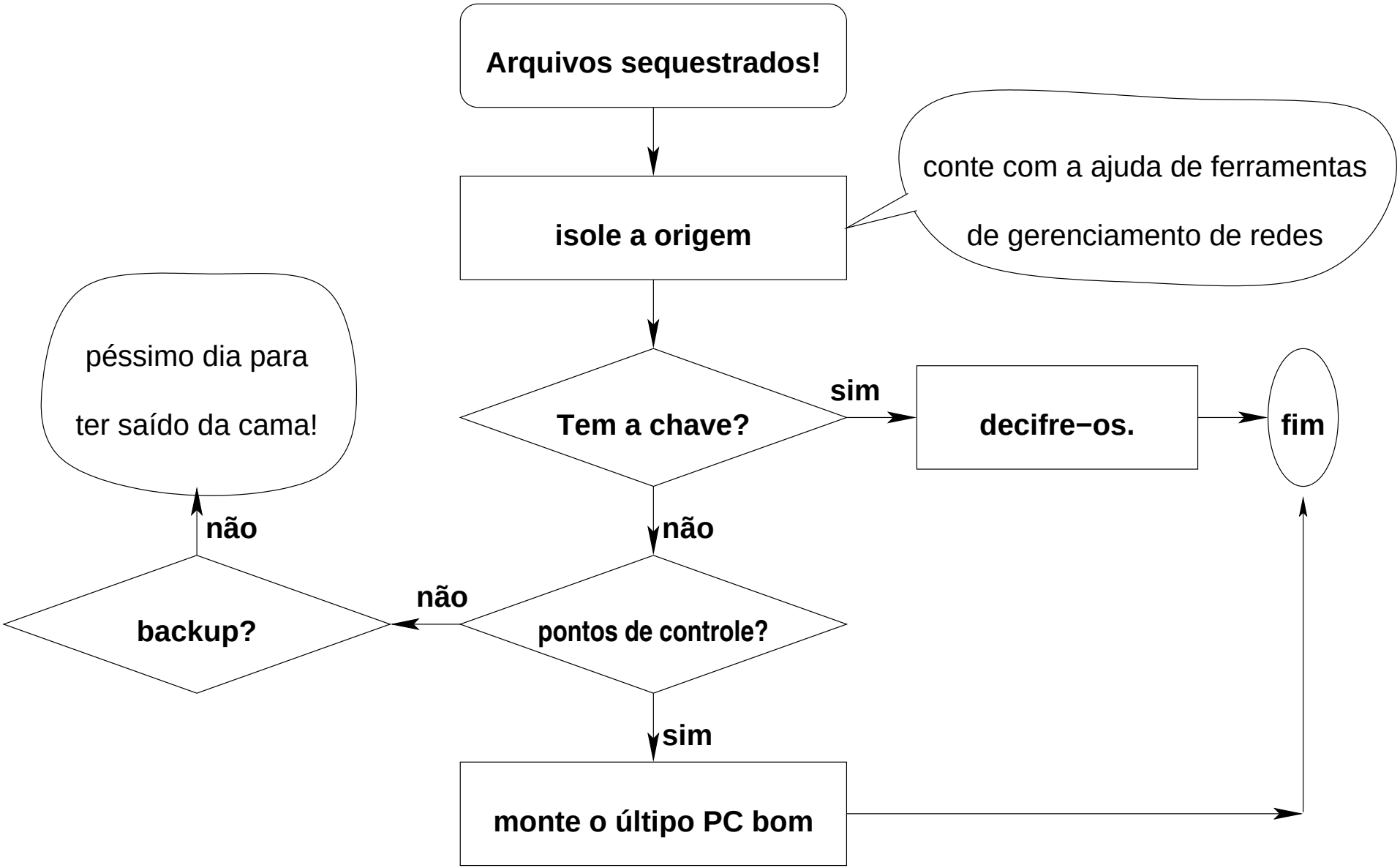
Resumo da novela



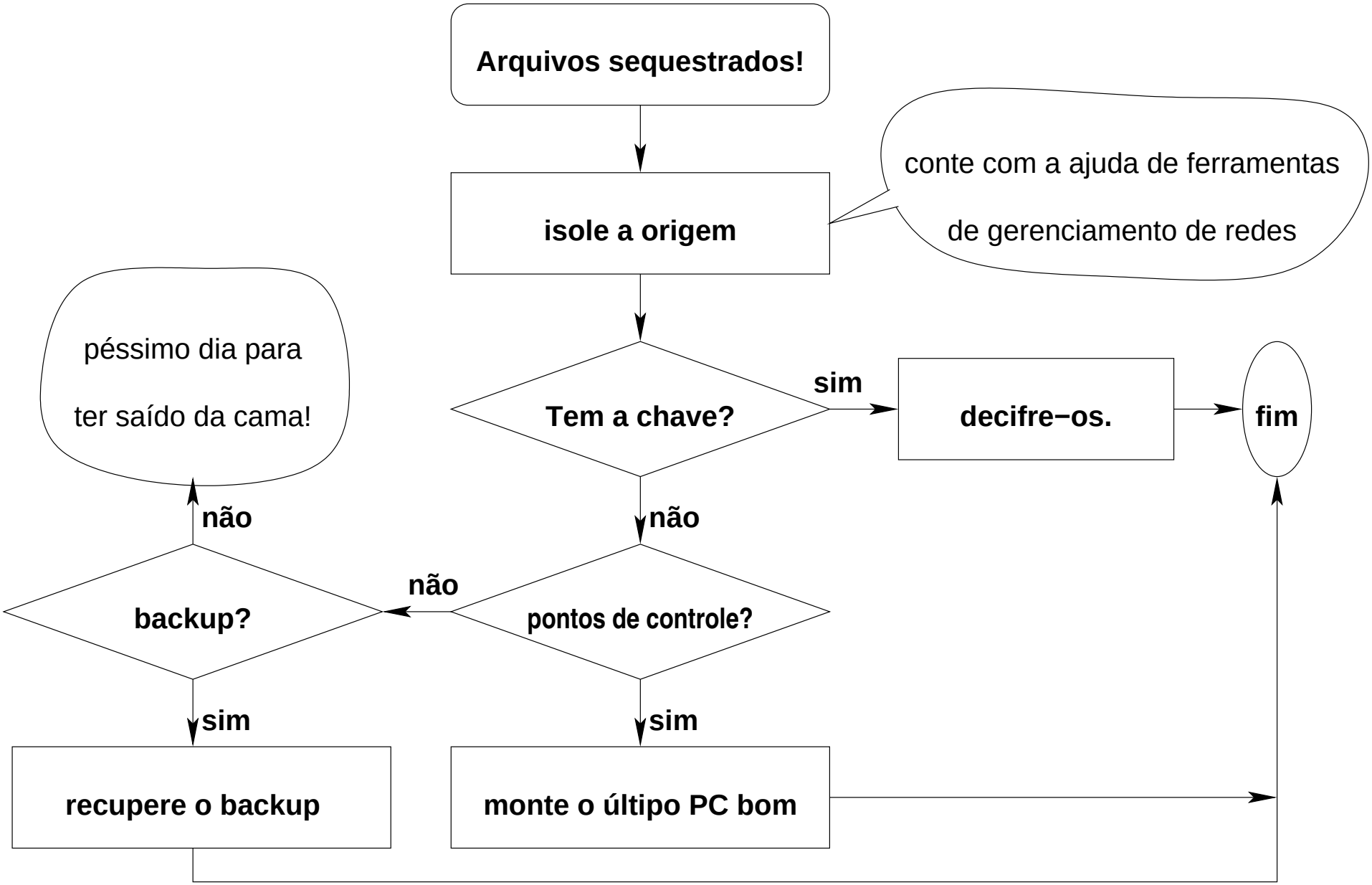
Resumo da novela



Resumo da novela



Resumo da novela



Conclusões

Conclusões

Sequestro de dados está na moda e causa muitos prejuízos.

Conclusões

Sequestro de dados está na moda e causa muitos prejuízos.

Infecção por métodos comuns, com a ajuda do usuário.

Conclusões

Sequestro de dados está na moda e causa muitos prejuízos.

Infecção por métodos comuns, com a ajuda do usuário.

É fundamental isolar a máquina contaminada, pois o bicho pode atacar novamente!

Conclusões

Sequestro de dados está na moda e causa muitos prejuízos.

Infecção por métodos comuns, com a ajuda do usuário.

É fundamental isolar a máquina contaminada, pois o bicho pode atacar novamente!

Somente medidas preventivas funcionam efetivamente, a mais conhecida e que deve ser praticada é o BACKUP!

Conclusões

Sequestro de dados está na moda e causa muitos prejuízos.

Infecção por métodos comuns, com a ajuda do usuário.

É fundamental isolar a máquina contaminada, pois o bicho pode atacar novamente!

Somente medidas preventivas funcionam efetivamente, a mais conhecida e que deve ser praticada é o BACKUP!

Há outros recursos menos conhecidos que o backup e que ajudam na recuperação do desastre: volumes indeléveis e sistemas de arquivos com pontos de controle.

Recursos

Ferramenta da Kasperski usando as chaves recuperadas pela Polícia Holandesa: https://noransom.kaspersky.com/

Recursos

Ferramenta da Kasperski usando as chaves recuperadas pela Polícia Holandesa: https://noransom.kaspersky.com/

Artigo na Wikipedia (muito interessante): https://en.wikipedia.org/wiki/Ransomware

Recursos

Ferramenta da Kasperski usando as chaves recuperadas pela Polícia Holandesa: https://noransom.kaspersky.com/

Artigo na Wikipedia (muito interessante): https://en.wikipedia.org/wiki/Ransomware

Recursos do Plan9 from Bell Labs: https://swtch.com/plan9port/

Recursos

Ferramenta da Kasperski usando as chaves recuperadas pela Polícia Holandesa: https://noransom.kaspersky.com/

Artigo na Wikipedia (muito interessante): https://en.wikipedia.org/wiki/Ransomware

Recursos do Plan9 from Bell Labs: https://swtch.com/plan9port/

Sistema de arquivos com pontos de controle da NTT (Nippon Telephone and Telegraph): http://nilfs.osdn.jp/en/

Recursos

Ferramenta da Kasperski usando as chaves recuperadas pela Polícia Holandesa: https://noransom.kaspersky.com/

Artigo na Wikipedia (muito interessante): https://en.wikipedia.org/wiki/Ransomware

Recursos do Plan9 from Bell Labs: https://swtch.com/plan9port/

Sistema de arquivos com pontos de controle da NTT (Nippon Telephone and Telegraph): http://nilfs.osdn.jp/en/

O site da IBM discute o nilfs, exofs, e menciona outras abordagens ao problema: http://www.ibm.com/developerworks/library/l–nilfs–exofs/

Recursos

Ferramenta da Kasperski usando as chaves recuperadas pela Polícia Holandesa: https://noransom.kaspersky.com/

Artigo na Wikipedia (muito interessante): https://en.wikipedia.org/wiki/Ransomware

Recursos do Plan9 from Bell Labs: https://swtch.com/plan9port/

Sistema de arquivos com pontos de controle da NTT (Nippon Telephone and Telegraph): http://nilfs.osdn.jp/en/

O site da IBM discute o nilfs, exofs, e menciona outras abordagens ao problema: http://www.ibm.com/developerworks/library/l–nilfs–exofs/

E, se você lê japonês, http://nilfs.osdn.jp/ja/

NILFS はオープンソースソフトウェアとして開発・公開しており、現在は Linux カーネルの一機能としてご利用いただくことができます。