

Ethical Hacking e Ransomware

Carlos Eduardo Maciel Rodrigues

E-mail: cadurodrigues@hotmail.com

<https://www.linkedin.com/in/cadurodrigues/>

CEH | ISO27002 | LPI | COBIT | ITIL

MBA – CYBER SECURITY – FORENSICS, ETHICAL
HACKING & DEVSECOPS

CONHECIMENTOS

- 25 anos em TI
- Especialista em Segurança Cibernética
- Red Team | Blue Team
- S.O. Linux | Windows | MAC OS |
- BD MS SQL | MY SQL | ORACLE
- PHP | JAVA | PYTHON
- FIREWALLS | IDS
- SIEM

Experiência

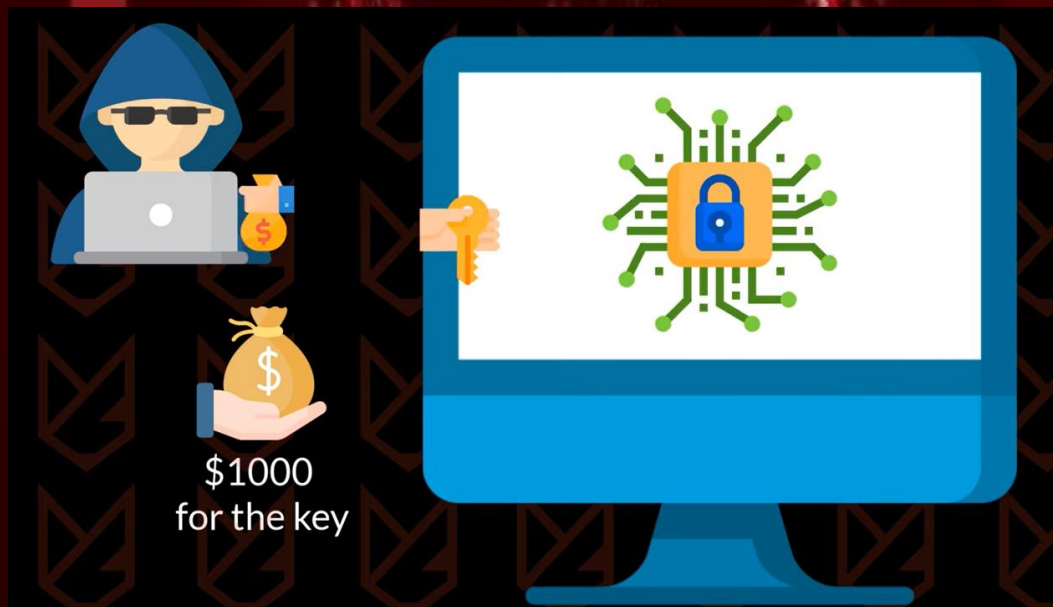
- Consist Business Technology
- Tim Celular
- Banco Safra
- Banco Santander
- Claro Brasil
- Carrefour

Conteúdo:

- Metodologias de análise de vulnerabilidade (NIST 800-155, OSSTMM e OWASP)
- Coleta de informações (footprint and fingerprint) com Google Hacking
- Engenharia Social
- Ransomware
- Análise, exploração e mitigação de vulnerabilidades
- Relatório de Vulnerabilidade

Ransomware?

É um tipo de malware de sequestro de dados, feito por meio de criptografia, que usa como refém arquivos pessoais da própria vítima e cobra resgate pra restabelecer o acesso a estes arquivos.



Impactos causados na TI por Ransomware

A maioria dos primeiros ataques de ransomware se concentrou em indivíduos e alavancou sua crescente dependência de dados pessoais e mídias.

A ideia de perder fotos, vídeos e documentos pessoais gerou pressão suficiente para convencer algumas vítimas a pagar o resgate. mas a cada pagamento de resgate, os invasores se fortalecem cada vez mais e se voltam para alvos maiores.

Impactos causados na TI por Ransomware

Ransomware primeiro ganhou notoriedade como uma ameaça aos dados pessoais.

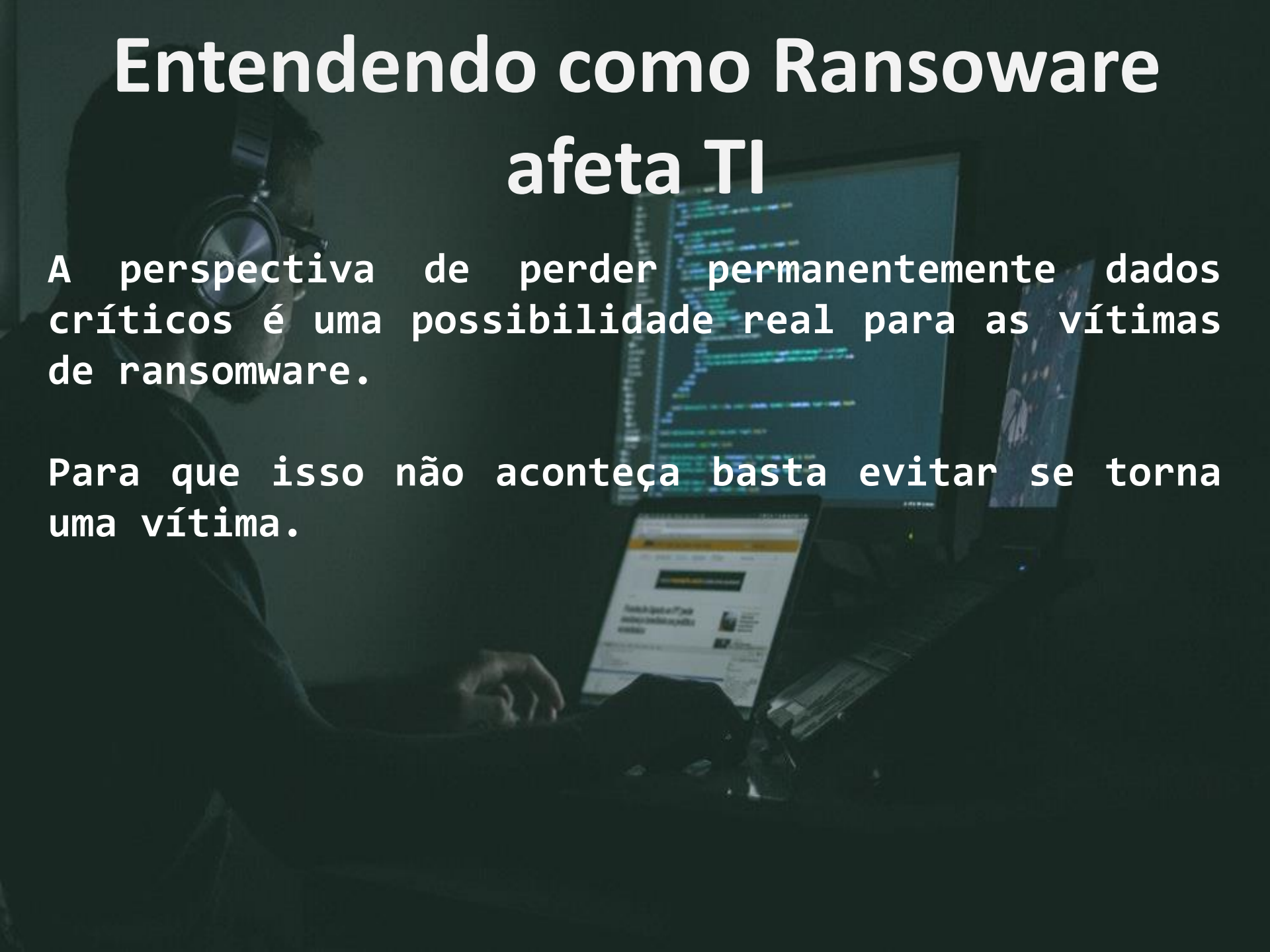
Em 2021, ransomware causaram ao setor público dos Estados Unidos centenas de milhões de dólares em inatividades e danos, segundo o site de segurança da informação:

<https://blog.emsisoft.com/en/41518/ransomware-cost-us-local-governments-623-million-in-2021-but-fewer-incidents-in-2022/>

Entendendo como Ransomware afeta TI

A perspectiva de perder permanentemente dados críticos é uma possibilidade real para as vítimas de ransomware.

Para que isso não aconteça basta evitar se torna uma vítima.



Entendendo como Ransomware afeta TI

Como podemos nos recuperar se algum de nossos controles preventivos falhar em impedir um ataque de ransomware?

Implantar um plano para prevenir, avaliar e recuperar.

Um bom plano de resiliência de ransomware implementa várias camadas de proteção.

Ransomware na vida real

Em 16 de Abril de 2023, a Valid Certificadora, empresa brasileira de certificação digital, sofreu uma tentativa de ataque cibernético. O ataque foi realizado pelo grupo CrossLock, um grupo de ransomware que atua no Brasil.

Após a tentativa de ataque, a Valid Certificadora suspendeu temporariamente os serviços da unidade de certificados digitais, como medida preventiva de segurança. A empresa também informou que todos os protocolos de controle e segurança da informação foram adotados, e que os trabalhos de apuração, documentação e investigação do comprometimento continuam em plena ação.



mccertificado • [Follow](#)



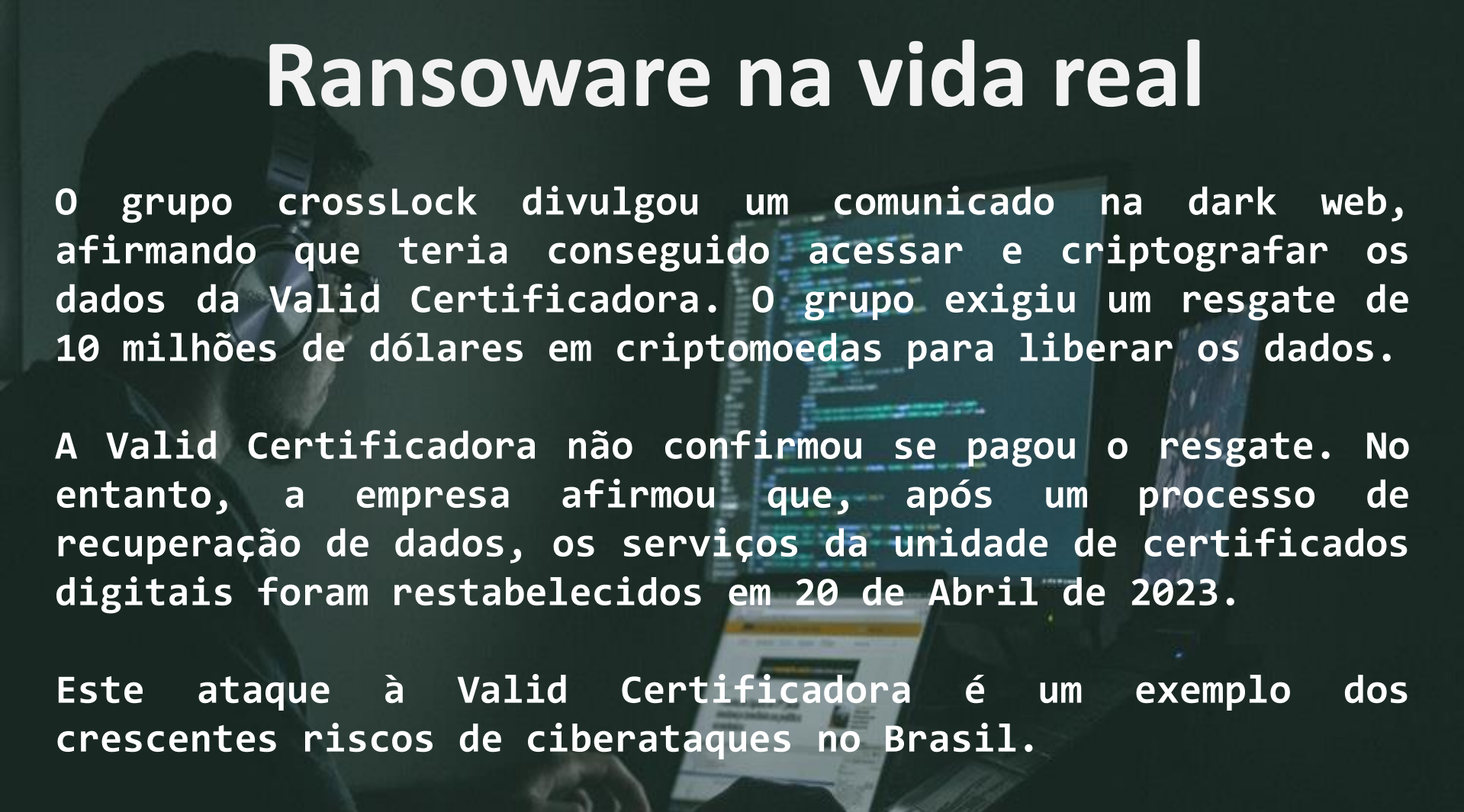
mccertificado Devido a problemas técnicos na VALID CERTIFICADORA, nossos serviços da AR MC CERTIFICADO DIGITAL estão suspensos temporariamente! Agradecemos a compreensão de todos!

Ransomware na vida real

O grupo crossLock divulgou um comunicado na dark web, afirmando que teria conseguido acessar e criptografar os dados da Valid Certificadora. O grupo exigiu um resgate de 10 milhões de dólares em criptomonedas para liberar os dados.

A Valid Certificadora não confirmou se pagou o resgate. No entanto, a empresa afirmou que, após um processo de recuperação de dados, os serviços da unidade de certificados digitais foram restabelecidos em 20 de Abril de 2023.

Este ataque à Valid Certificadora é um exemplo dos crescentes riscos de ciberataques no Brasil.



```
-----!!!!!!ATTENTION!!!!!!-----  
DON'T RENAME, OR TRY TO DECRYPT THE FILES USING A FREE PUBLIC SOFTWARE BECAUSE YOU WILL LOSE ALL YOUR FILES AND DATA  
-----  
Valid certificadora,  
Your entire network has been compromised and completely encrypted and your sensitive data (docs,dbs, customers' info..etc) has been downloaded to our servers.  
To restore your encrypted data and prevent your sensitive data from being leaked you must buy the decryption app.  
Your data will be leaked on:  
Website: [redacted]  
to visit the website you should use tor browser.  
Contact us to get the decryption application:  
tox: [redacted]  
You'll need to download tox client app then add our tox id.  
NOTE: Since tox is peer to peer you'll need to stay online to send the message to us.  
CrossLock
```

0 grupo crossLock divulgou um comunicado na dark web, afirmando que teria conseguido acessar e criptografar os dados da Valid Certificadora. O grupo exigiu um resgate de 10 milhões de dólares em criptomoedas para liberar os dados.

A Valid Certificadora não confirmou se pagou o resgate. No entanto, a empresa afirmou que, após um processo de recuperação de dados, os serviços da unidade de certificados digitais foram restabelecidos em 20 de Abril de 2023.

Este ataque à Valid Certificadora é um exemplo dos crescentes riscos de ciberataques no Brasil.

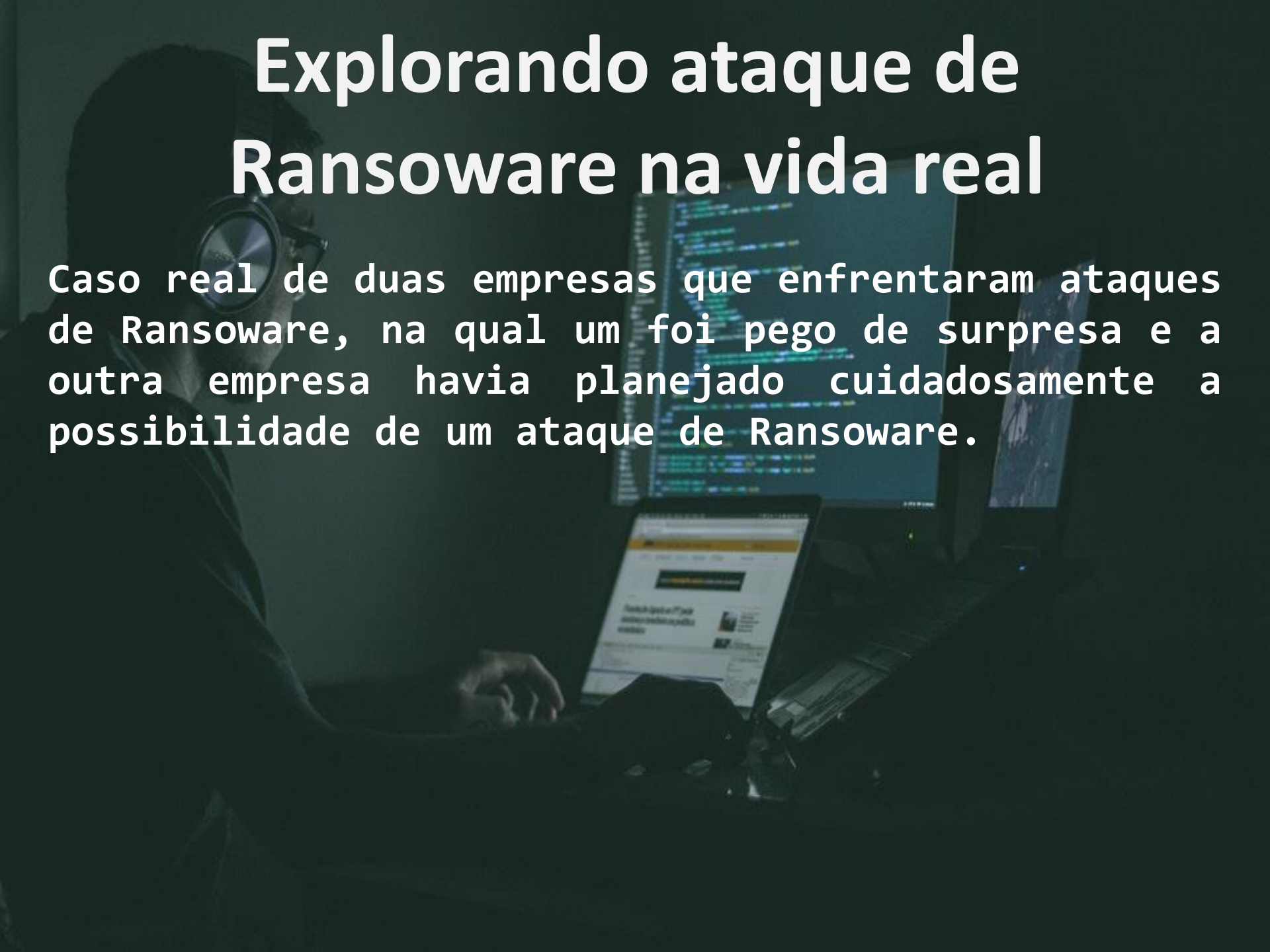
```

-----!!!!!!!!ATTENTION!!!!!!-----
DONT RENAME, OR TRY TO DECRYPT THE FILES USING A FREE PUBLIC SOFTWARE BECAUSE YOU WILL LOSE ALL YOU FILES AND DATA
-----
Valid certificadora,
You entire network has been compromised and completely encrypted and your sensitive data (docs,dbs, customers' info..etc) has been downloaded to our servers.
To restore your encrypted data and prevent your sensitive data from being leaked you must buy the decryption app.
Your data will be leaked on:
Website: http://www.danilov.it/leak/
to visit the website you should use tor browser.
Contact us to get the decryption application:
tox: https://www.torproject.org/
You'll need to download tox client app then add our tox id.
NOTE: Since tox is peer to peer you'll need to stay online to send the message to us.
CrossLock

```

Explorando ataque de Ransomware na vida real

Caso real de duas empresas que enfrentaram ataques de Ransomware, na qual um foi pego de surpresa e a outra empresa havia planejado cuidadosamente a possibilidade de um ataque de Ransomware.



Explorando ataque de Ransomware na vida real

A empresa 1 é a Travelex que é uma empresa de câmbio com sede em Londres e foi vítima de um Ransomware implantado pela gangue sodinokibi, e descobriu que seus principais serviços foram severamente afetados, os backups foram excluídos e 5 GB de dados operacionais foram baixados e criptografados.

A Travelex negociou com os invasores por várias semanas e finalmente concordou em pagar US\$2,3 milhões em criptomoeda para recuperar seus dados e receber garantia de que seus dados não seriam divulgados publicamente. Retomou as operações em 2020.

Explorando ataque de Ransomware na vida real

O caso 2 foi a cidade de Durham, Carolina do Norte, foi vítima pretendida de um ataque de Ransomware em março de 2020. A cidade de Durham havia implementado anteriormente um plano de infraestrutura de monitoramento e backup, baseado em um sistema de backup imutável da Rubrik que garantia que seus backups estivessem protegidos contra comprometimento.

Vários serviços críticos, incluindo o seu servidor 911 foram interrompidos. A equipe conseguiu identificar os arquivos afetados e recuperá-los para restaurar os serviços mais críticos rapidamente.

O que é Backup Imutável?

Backup Imutável possui dados fixos, onde nunca poderão ser excluídos. Por isso recebe o nome de imutável, já que esse tipo de backup torna sua informação permanente.

Atualmente é o tipo de estratégia de nível mais alto de proteção, isso garante 100% a recuperação da cópia de todos os dados.

Segue duas opções com essa solução:

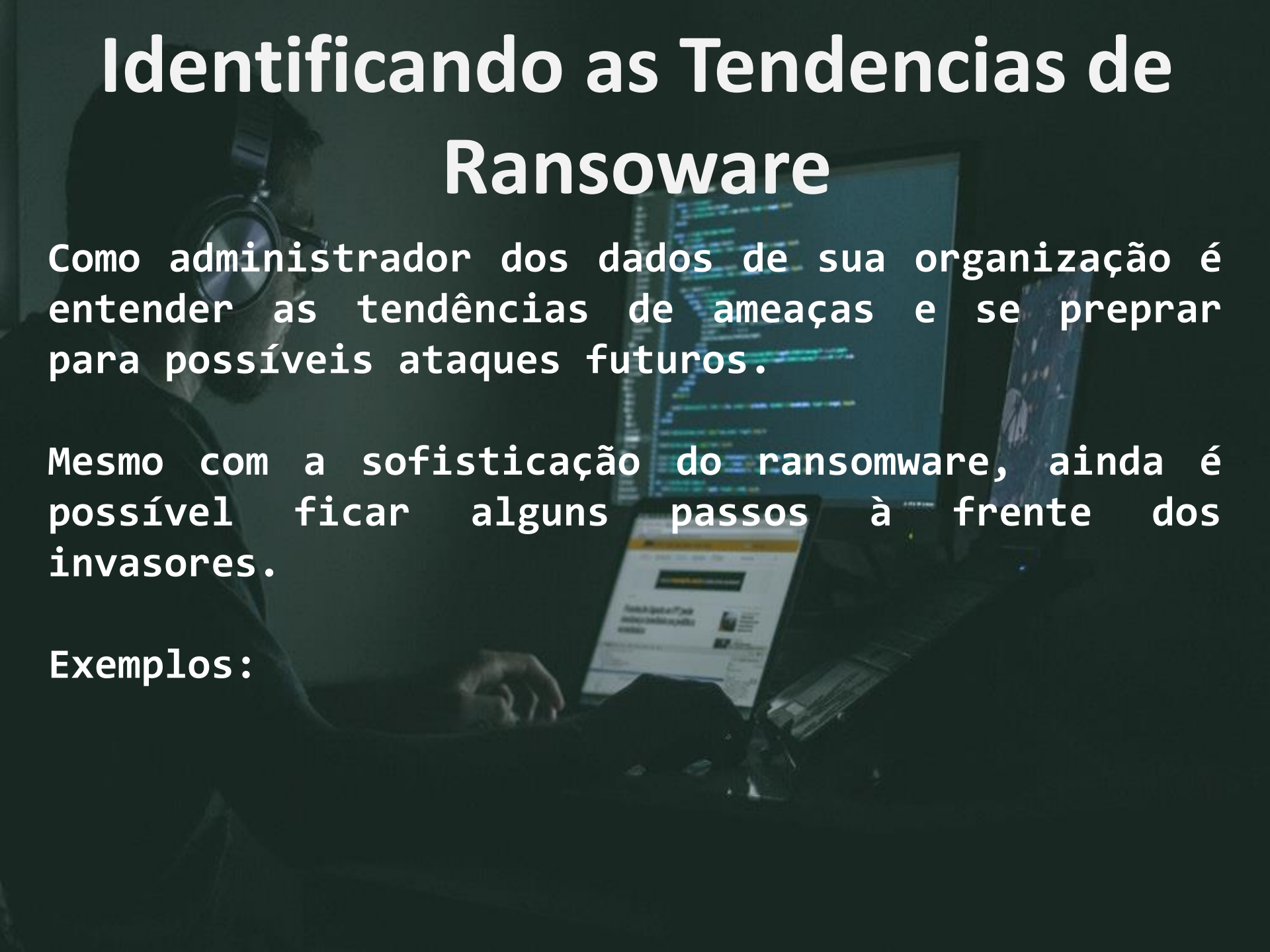
- Rubrik
- Veeam Backup

Identificando as Tendencias de Ransomware

Como administrador dos dados de sua organização é entender as tendências de ameaças e se preparar para possíveis ataques futuros.

Mesmo com a sofisticação do ransomware, ainda é possível ficar alguns passos à frente dos invasores.

Exemplos:



Identificando as Tendencias de Ransomware

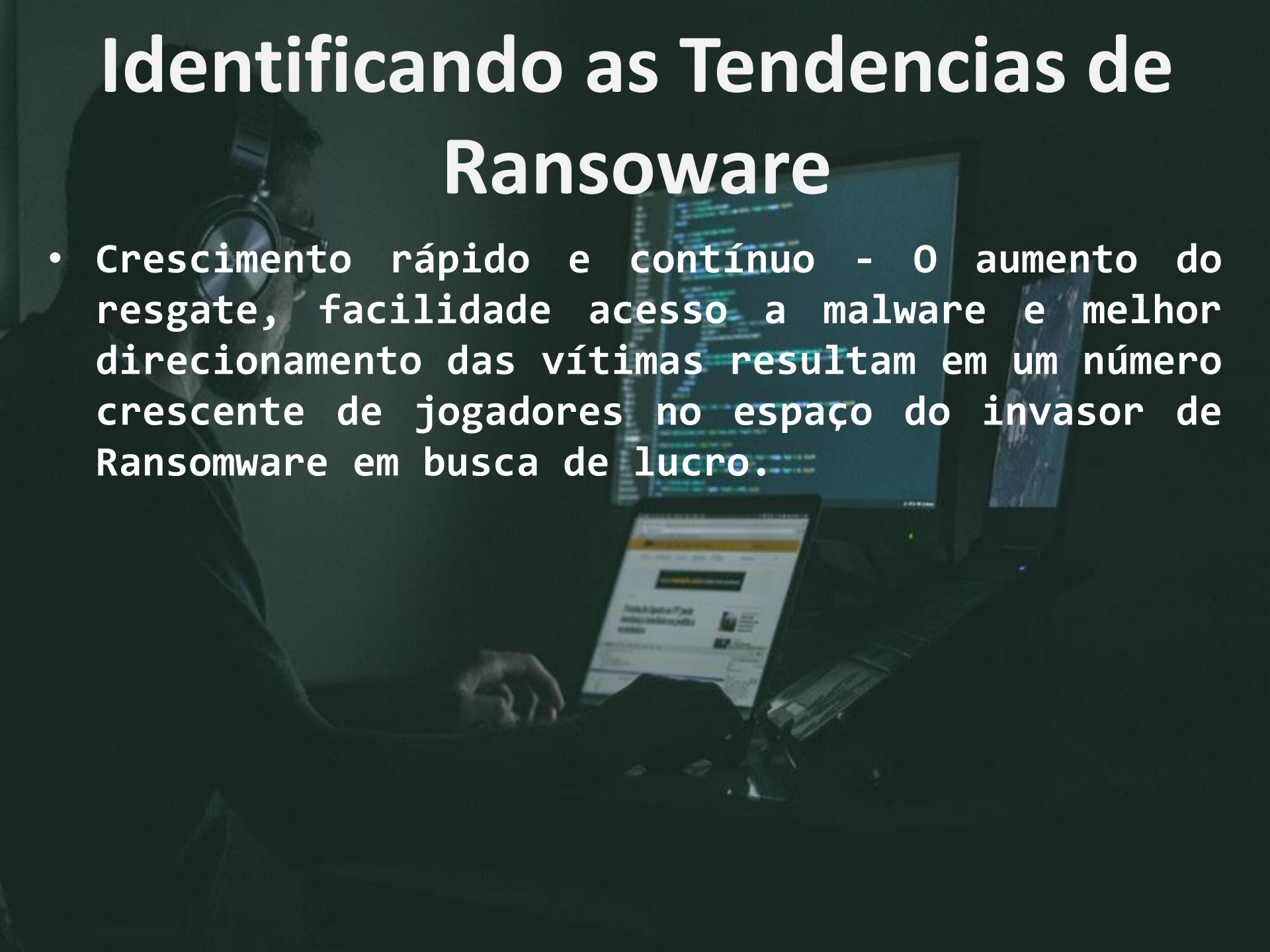
- Aumentar os valores dos resgates - Os invasores concentram seus ataques em menos alvos, mas exigem pagamentos de resgates muito mais altos.
- Malware de commodity emergente - Você não precisa escrever malware para usar Ransomware. (Raas) facilitam tornar-se um invasor de Ransomware.
- Visando situações de trabalho remoto e estudo - COVID-19 resultou em invasores se concentrando em fornecedores de colaboração e educação.

Identificando as Tendencias de Ransoware

- Exfiltração de dados - Bem, além de criptografar dados, alguns ataques agora estão transportando dados para o site do invasor.
- Fazer uma segunda tentativa de extorsão - Dados exfiltrados estão sendo usados para extorquir pagamento adicional de resgate para evitar a liberação de dados confidenciais.
- Procurar e comprometer backups - Muitas variantes de Ransomware atuais vão além de criptografia de dados locais, eles fazem buscas em todas as fontes de dados conectadas.

Identificando as Tendencias de Ransomware

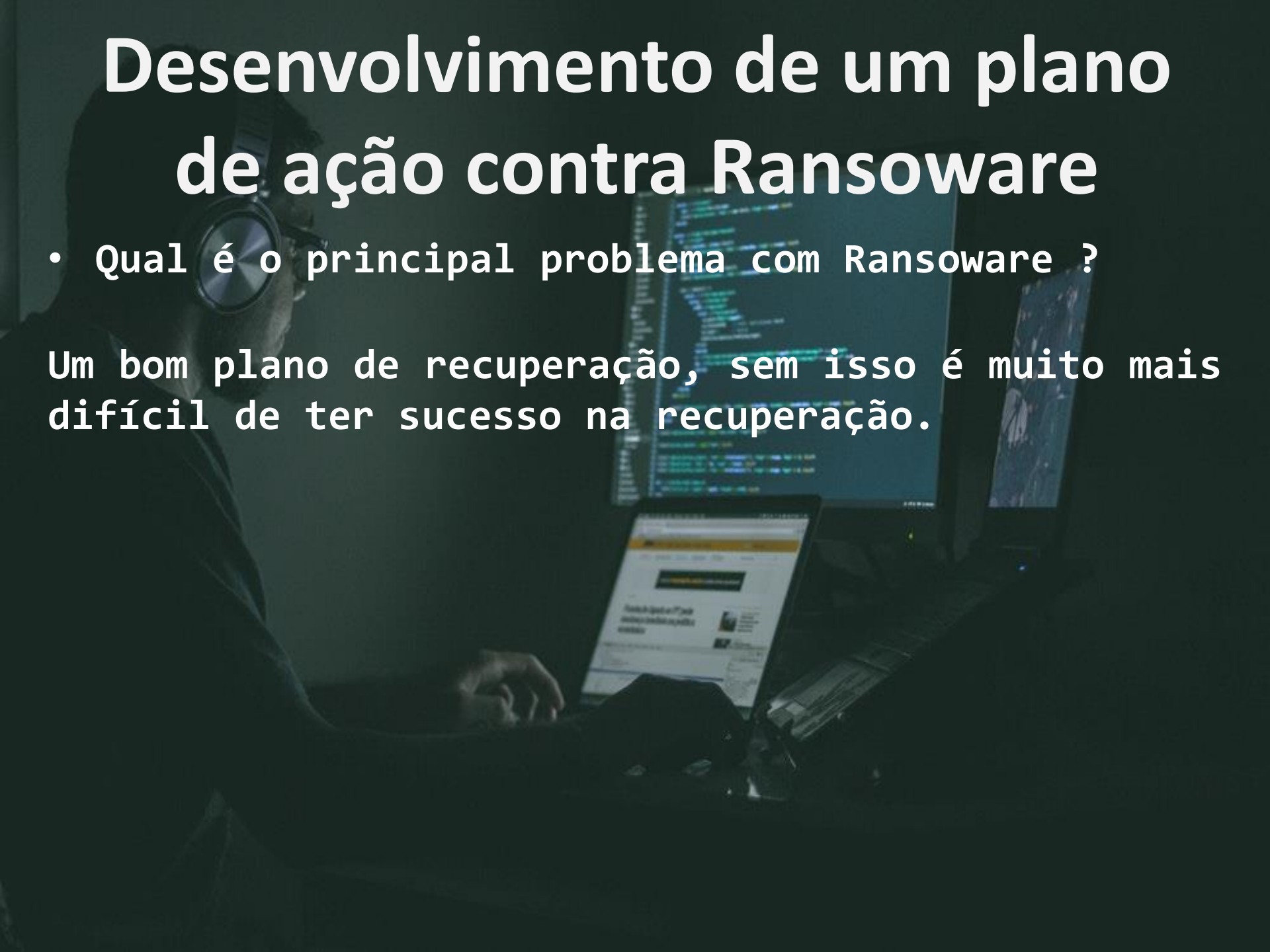
- Crescimento rápido e contínuo - O aumento do resgate, facilidade acesso a malware e melhor direcionamento das vítimas resultam em um número crescente de jogadores no espaço do invasor de Ransomware em busca de lucro.



Desenvolvimento de um plano de ação contra Ransomware

- Qual é o principal problema com Ransomware ?

Um bom plano de recuperação, sem isso é muito mais difícil de ter sucesso na recuperação.



Avaliando suas necessidades

Entender o que é importante para sua organização e o que é importante para os invasores.

Uma avaliação de impacto nos negócios (BIA) é um processo importante para identificar os processos críticos para sua organização.

Exemplo:

Para o varejista online os seus serviços de lojas online, banco de dados de clientes e produtos tem suma importância para o negócio.

Construindo um plano de recuperação

Comece identificando quem são as pessoas chaves que precisam ser envolvidas caso aconteça o incidente com o Ransoware.

Qualquer indivíduo que possa influenciar ou serem afetados pelo plano.

Testando o plano de recuperação

A person wearing headphones and glasses is working on a laptop in a dark room. There are multiple monitors displaying code and data. The person is looking at the laptop screen, which shows a website with a yellow header. The background is dark, and the lighting is focused on the person and the screens.

Melhor que construir é validar se este plano realmente funciona.

Acredito que será frustrante desenvolver um plano de recuperação e na hora da execução, o plano não funcionar.

Protegendo a última linha de defesa

Esta fase é quando o atacante teve sucesso em achar fontes automatizadas para conectar em repositórios de dados e infectar com o Ransoware.

A recuperação sempre deve ser feitas em 3 etapas:

1. Interromper o ataque
2. Identificar os arquivos afetados
3. Recuperar a versão não criptografada dos arquivos de backup

Treinando o usuário para evitar torna-se uma vítima

O melhor investimento para qualquer organização é um treinamento para usuário final.

Além do treinamento do usuário final é essencial recrutar o usuário como um agente de segurança.

A segurança é responsabilidade de todos e não apenas de um pequeno grupo de especialista em segurança da informação.

Deixe todos saber que uma boa segurança é um esforço de equipe e que todos precisam ser diligentes.

Reconhecendo um possível ataque

Uma maneira segura de reduzir o potencial risco de um ataque é ensinar os usuários a estarem atentos a conteúdos suspeitos.

Mostre ao usuários exemplos de e-mails phishing forneça diretrizes como identificar um possível ataque.

Exemplo de Phishing

From: atmcard14@yandex.com
To: cadurodrigues@hotmail.com
Subject: Re: Attention Beneficiary: Carlos Eduardo Maciel Rodriguez
Date: Thu, 30 Oct 2014 11:27:42 +0100

Attention Beneficiary: Carlos Eduardo Maciel Rodriguez

This is to acknowledge the receipt of your email? I am very surprise that you have not receive my email before, which I have instructed my secretary to sent you email two times but you insisted that you have not receive my email before, which I am very sorry if you have not receive it before regarding the name of my country which I from United State Of America, but I was post in Nigeria to come and work as director of ATM-Card Department in which your name and email is among the beneficiaries entitle to receive this fund.

Atenção Beneficiário: Carlos Eduardo Maciel Rodriguez

Isso é para acusar o recebimento do seu e-mail? Estou muito surpreso que você não tenha recebido meu e-mail antes, que instruí minha secretária a lhe enviar e-mail duas vezes, mas você insistiu que não recebeu meu e-mail antes, o que sinto muito se você não o recebeu antes. o nome do meu país que eu sou dos Estados Unidos da América, mas fui postado na Nigéria para vir trabalhar como diretor do Departamento de Cartões ATM em que seu nome e e-mail estão entre os beneficiários com direito a receber este fundo.

Reagindo ao um e-mail suspeito

A person wearing large headphones is sitting at a desk in a dimly lit room. They are looking at a laptop screen which displays a website. In the background, there are two larger monitors. The left monitor shows lines of code in a dark-themed editor, and the right monitor shows a colorful abstract image. The person's hands are on the laptop keyboard.

A sua organização deve ter um local específico para denunciar mensagens de e-mails suspeitos.

- Uma Caixa de e-e-mails que recebem denúncias para ser analisadas.

Seguindo as boas práticas

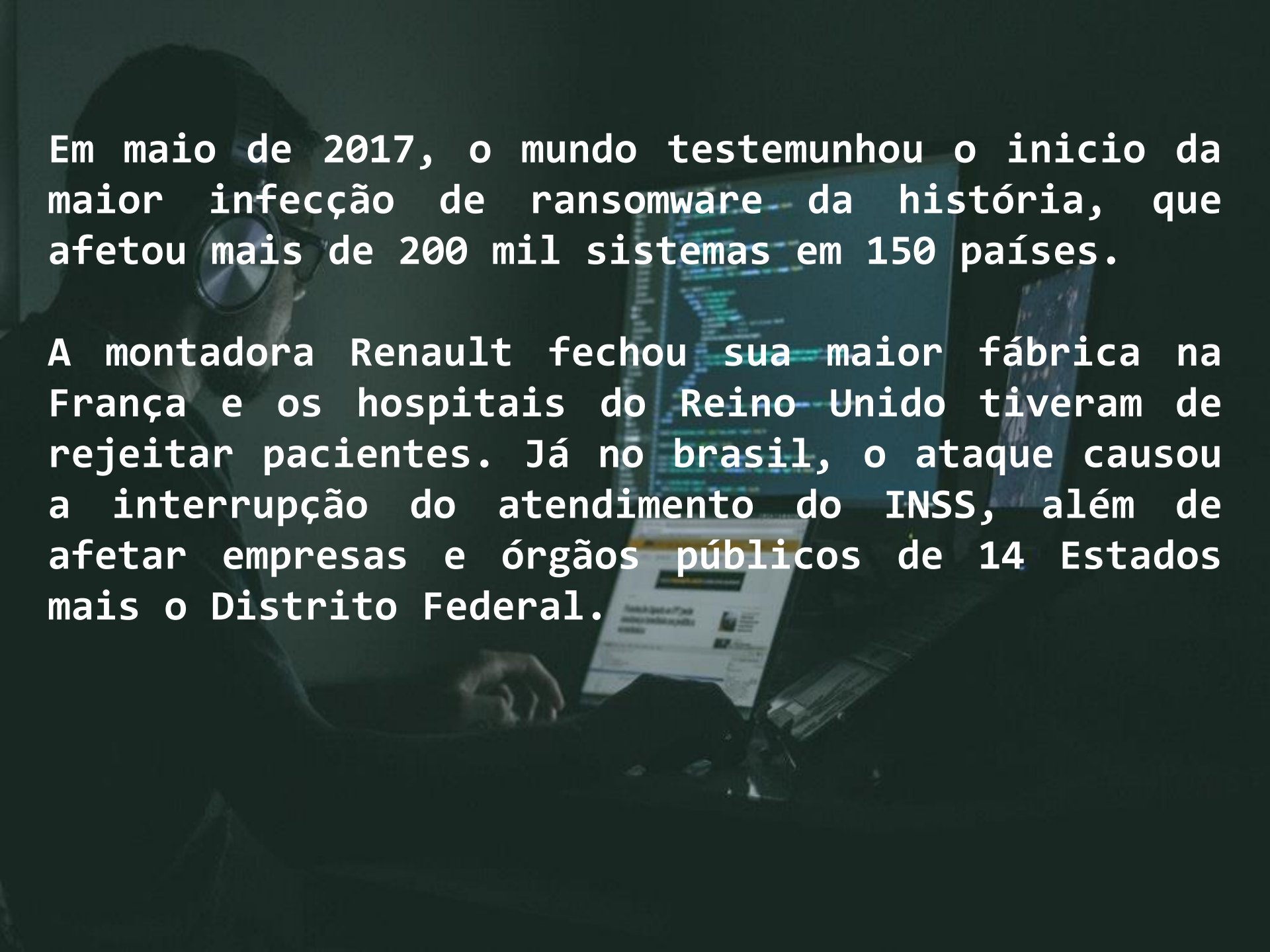
- Verificar os remetentes do e-mail antes de abrir uma mensagem
- Não abra anexos a menos que confie no remetente.
- Não siga links de mensagens de e-mails
- Não responda e-mails com aparência suspeitas
- Encaminhe qualquer mensagem suspeita ao time de Segurança da informação
- Visite apenas sites que você confie
- Não forneça informações pessoais a menos que confie no site
- Não conecte / insira / monte dispositivos externos
- Sempre use um VPN para se conectar a um lugar remoto

Implementar práticas recomendadas de segurança

- Manter seu equipamento, sistemas operacionais e seus pacotes de atualizações
- Repetir o treinamento de conscientização para os usuários periodicamente.
-

Fortalecer a equipe de TI

- Identificar todos os dados críticos
- Criar cópias de backup periódicas de todos os dados críticos
- Desenvolva um plano de teste de recuperação abrangente
- Mantenha todos os equipamentos e softwares atualizados
- Exigir VPN para acesso remoto
- Exigir software antivírus / antimalware para todos os dispositivos
- Implemente uma varredura periódica no seu ambiente de infraestrutura
- Implemente um firewall com regras restritivas
- Realize treinamento periódicos de conscientização
-

A person wearing headphones and glasses is working on a laptop in a dark room. The laptop screen shows a website, and there are other monitors in the background displaying code or data. The text is overlaid on the image.

Em maio de 2017, o mundo testemunhou o início da maior infecção de ransomware da história, que afetou mais de 200 mil sistemas em 150 países.

A montadora Renault fechou sua maior fábrica na França e os hospitais do Reino Unido tiveram de rejeitar pacientes. Já no Brasil, o ataque causou a interrupção do atendimento do INSS, além de afetar empresas e órgãos públicos de 14 Estados mais o Distrito Federal.

Wana Decrypt0r 2.0

OOPS YOUR FILES HAVE BEEN ENCRYPTED!

Payment will be
raised on :

Time left:
02:23:57:37

Your files will be
lost on:

Time left:
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer
accessible because they have been encrypted. Maybe you are busy looking for a way to
recover your files, but do not waste your time. Nobody can recover your files without
our decryption service.

Can I Recover My Files?

Yes. We guarantee that you can recover all your files safely and easily. But you have
not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 7 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 4 months.

How Do I Pay?

But if you want to decrypt all your files, you need to pay.
You only have 7 days to submit the payment. After that the price will be doubled.



Ethical Hacking e Ransomware

Carlos Eduardo Maciel Rodrigues

E-mail: cadurodrigues@hotmail.com

<https://www.linkedin.com/in/cadurodrigues/>

CEH | ISO27002 | LPI | COBIT | ITIL

MBA – CYBER SECURITY – FORENSICS, ETHICAL
HACKING & DEVSECOPS