ENTENDENDO O INIMIGO

Um guia rápido sobre ransomware, o sequestro de dados, e porque as empresas estão em risco

#1

Onde estão meus dados?

A história se repete

OS RELATOS DE EMPRESÁRIOS QUE TIVERAM DADOS SEQUESTRADOS SÃO SEMPRE PARECIDOS. O QUE ERA PARA SER UM DIA NORMAL DE TRABALHO, COMEÇOU COM PROBLEMAS PARA ACESSAR SISTEMAS. EM TODAS AS TELAS DE COMPUTADORES CORPORATIVOS, MENSAGENS DE "SERVIDOR NÃO ENCONTRADO" APARECIAM A QUEM TENTAVA ABRIR ARQUIVOS OU ACESSAR E-MAILS.

Não demorava até que alguém da área de tecnologia aparecesse, relatando que um vírus havia infectado o ambiente da empresa e que todas as informações que faziam o negócio funcionar, como cadastro de clientes, arquivos financeiros e de projetos, estavam inacessíveis.

Em alguns computadores, uma mensagem na área de trabalho informava que os dados haviam sido sequestrados, que o preço do resgate era de milhares de dólares e que o valor deveria ser pago em bitcoin, o que impediria o rastreamento do receptor após o pagamento. O empresário, desesperado para obter os dados, pagava. Porém, nada era devolvido.

O que vem em seguida é um acúmulo de prejuízos, em que a empresa tem que lidar com clientes insatisfeitos pelas entregas não realizadas, pagamentos de fornecedores em aberto, catálogo de produtos que não existe mais.

“Isso está mesmo acontecendo?”

Todos os dias, empresas sofrem sequestro de dados. Para se ter uma ideia, o Brasil é o segundo colocado em número de ataques mundiais de ransomware. Isso quer dizer que o nosso país representa 10,75% desse tipo de ameaça em todo o mundo. Outro dado que impressiona e serve de alerta é esse:

Mais da metade das empresas que foram atacadas, não tinham tecnologia para monitoramento e detecção de comportamento suspeito no ambiente.

Por isso, criamos esse e-book. Queremos apresentar uma visão clara do que é o ransomware e de como ele ameaça os negócios, para que você consiga identificar vulnerabilidades na sua empresa e se estruturar para proteger seus dados.

Ransomwares podem fechar uma empresa

Você já se perguntou quanto vale, em dinheiro, as suas informações? As lançadas no ERP da sua empresa, ou em uma planilha de fluxo de caixa, talvez o conteúdo de vários e-mails que guardam os históricos de negociações.

Quanto tudo isso vale?

- US$ 1 bilhão é o valor que foi pago em resgate por dados sequestrados por ransomware em 2016;
- Em 2017, o número saltou para US$ 5 bilhões;
- US$ 500 é o valor médio de um resgate pago pelo usuário final vítima de ransomware;
- US$ 30 mil é a média que as empresas se dizem dispostas a pagar por dados sequestrados;
- 65% das empresas optam por pagar o resgate quando são vítimas de ransomware.

Fonte: CIO/IDG

TODA INFORMAÇÃO TEM VALOR PARA ALGUÉM, PORTANTO, NO QUE DEPENDER DOS HACKERS, OS ATAQUES DE RANSOMWARE SEMPRE VÃO EVOLUIR.

Conhecendo o inimigo

O que é ransomware

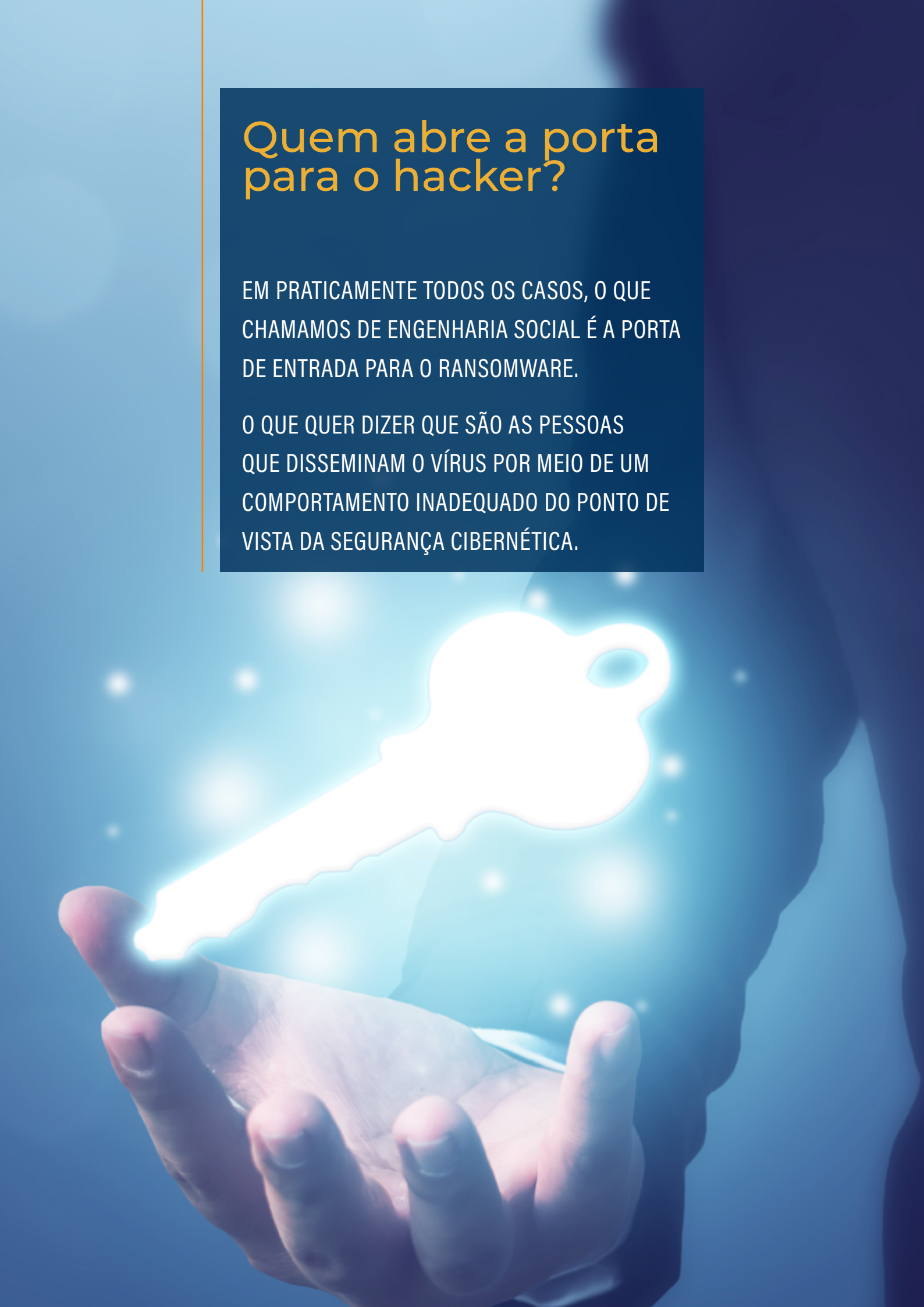
É uma família de vírus de computador, criado com intuito de bloquear o acesso do usuário a arquivos e sistemas por meio de criptografia. Se o dono das informações as quiser novamente, precisa pagar um resgate (ransom, em inglês) em criptomoeda, que são moedas digitais baseadas em criptografia. Elas não são rastreáveis em transações financeiras, o que protege a identidade do sequestrador.

O primeiro registro de ransomware é de 1980. De lá para cá, já foram registradas pelo menos 34 mil variações do vírus. Esse número cresce na mesma velocidade que a internet evolui. Por outro lado, o que mantém essa ameaça tão presente não mudou em anos de história da tecnologia.

Quem abre a porta para o hacker?

EM PRATICAMENTE TODOS OS CASOS, O QUE CHAMAMOS DE ENGENHARIA SOCIAL É A PORTA DE ENTRADA PARA O RANSOMWARE.

O QUE QUER DIZER QUE SÃO AS PESSOAS QUE DISSEMINAM O VÍRUS POR MEIO DE UM COMPORTAMENTO INADEQUADO DO PONTO DE VISTA DA SEGURANÇA CIBERNÉTICA.



Para ficar mais claro, o caminho percorrido pelo ransomware costuma seguir as seguintes etapas:

1. Instalação

Tudo começa com o recebimento de um e-mail, ou mensagem em uma rede social, tentando convencer o usuário a clicar em um link. O texto pode sugerir, por exemplo, que há uma pendência com a justiça. Também é comum um ransomware se passar por um antivírus ou um jogo. O usuário faz o download e, ao instalar, contamina o computador.

2. Identificação

O malware instalado inicia o mapeamento de arquivos elegíveis a serem criptografados. Fotos, vídeos, planilhas, documentos, tudo o que está em pastas acessadas pela vítima.

3. Criptografia

O malware faz o download de chaves de criptografias fortes (RSA de 2048 bits) de vários servidores do hacker. Essa movimentação apenas o atacante pode visualizar. A criptografia dos arquivos elegíveis inicia e, em poucos minutos, todos os dados são sequestrados.

4. Notificação

Quando o usuário do computador é avisado pelo hacker de que foi infectado, os dados já estão bloqueados. Na maioria das vezes, a vítima é informada por e-mail. Dependendo da variante, este comunicado aparece como um simples pop-up, ou no fundo de tela do usuário.

5. Pagamento

Na notificação, o hacker também exige um preço para liberação dos arquivos capturados. Normalmente, a transação financeira precisa ser feita por bitcoins, para manter o anonimato. Em uma guerra psicológica, há variantes que impõem que, se o pagamento não for realizado até uma determina hora, todos os arquivos serão deletados. Um ransomware chamado Jigsaw, identificado em 2016, agia assim: o usuário tinha 72 horas para efetuar o pagamento e a cada hora, uma parte dos dados era deletada para aumentar o senso de urgência.

6. Recuperação

Se o empresário decide pagar o resgate, não há garantias de que os dados serão recuperados. Nos casos em que o hacker devolve os arquivos, ele pede que a vítima envie o que está criptografado por meio de algum serviço de armazenamento em nuvem, como Dropbox. Então descriptografa os dados e os envia de volta. Também pode acontecer de o atacante entregar parte das chaves de criptografia.

Mas, a realidade é que menos da metade das pessoas conseguem reaver os dados após a realização do pagamento. E mesmo que eles sejam devolvidos, não há como ter certeza de que estarão íntegros, ou que não serão vendidos clandestinamente mais tarde.

Para responder adequadamente a uma interrupção nos negócios depois de um ataque cibernético agressivo, é preciso preparação. E a estratégia começa com conhecimento e informação.

Agora que você já sabe um pouco o que é ransomware e como ele pode prejudicar seus negócios, entenda quais estratégias adotar para prevenir ataques e responder da forma certa a incidentes. Você também pode conversar com um dos nossos especialistas, é só enviar um email para **contato@ish.com.br**

ISH

www.ish.com.br