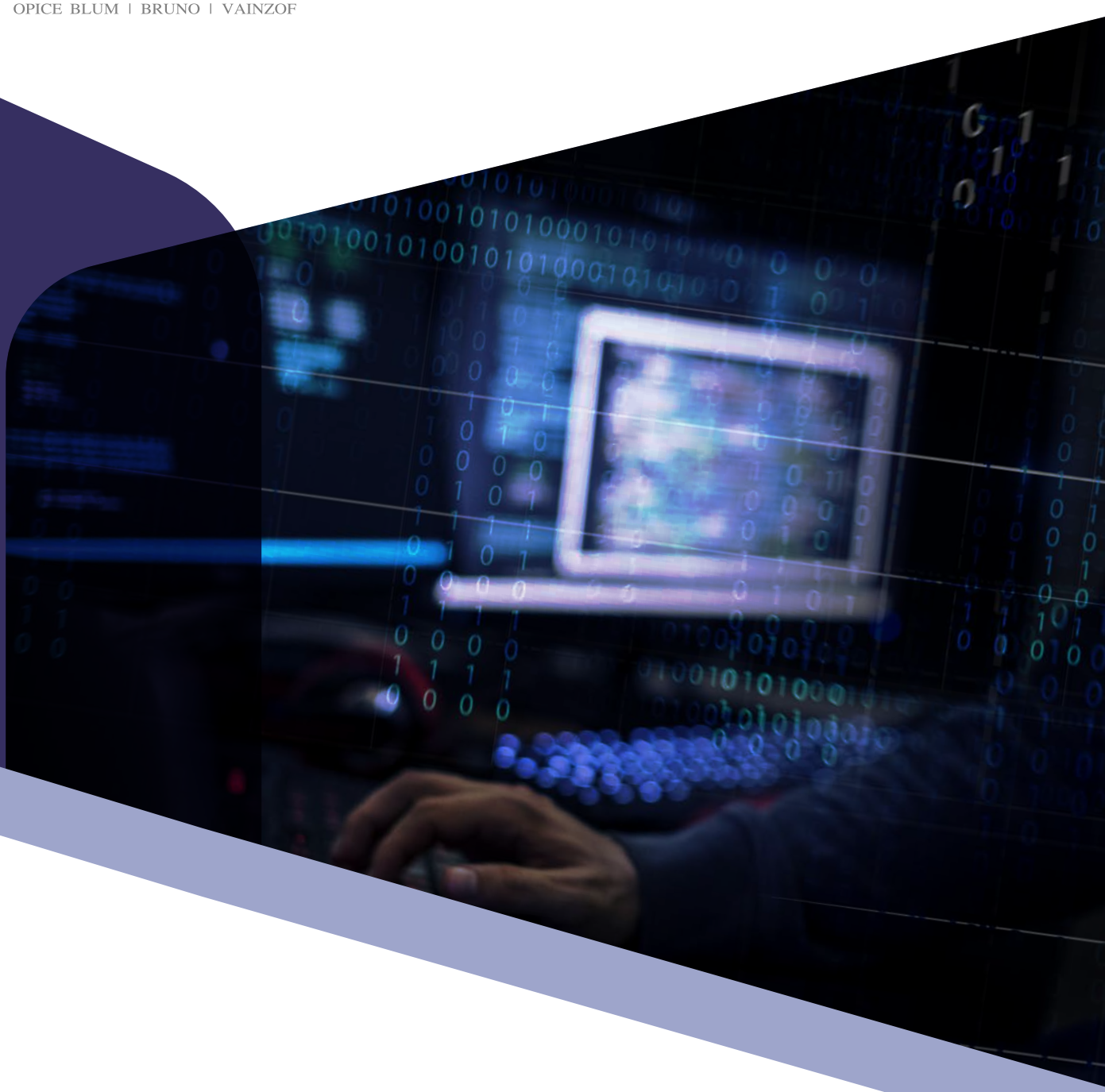
OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

Dezembro 2021



Ransomware

Os impactos para as organizações e as boas práticas de resposta a um ataque

Quem somos?

Fundado em 1997, o Opice Blum, Bruno e Vainzof Advogados Associados é escritório pioneiro em Direito Digital no país. Vimos nascer tendências, participamos delas e nos posicionamos sempre na vanguarda. Inovamos, perseguimos a excelência e ampliamos nossas frentes de atuação para atender de forma, ainda mais completa, nossos clientes.

Nossa atuação é reconhecida no Brasil e no exterior em rankings como Chambers & Partners, Who's Who Legal, The Legal 500, Best Lawyers, Leaders League, Análise Advocacia 500, entre outros.

Resposta a Incidentes de Segurança da Informação

Nossa área de Resposta a Incidentes de Segurança da Informação está preparada para adotar as 15 medidas a seguir:

1 - Preservação das evidências;

2 - Comunicação à seguradora, quando pertinente;

3 - Formação do comitê de crise;

4 - Identificação da causa-raiz do incidente;

5 - Contenção da vulnerabilidade;

6 - Identificação da exposição de dados;

7 - Varredura da *web*: monitoramento da *surface* e *deep web*;

8 - Elaboração de *score* de gravidade do incidente;

9 - Definição sobre a comunicação aos titulares e às autoridades;

10 - Elaboração de *script* para resposta a questionamentos dos consumidores;

11 - Elaboração de Fato Relevante, se cabível;

12 - Elaboração de notas reativas à imprensa;

13 - Relatório forense do incidente;

14 - Estratégia jurídica para contenção;

15 - Medidas jurídicas para identificação do ofensor.

Índice

04 *Ransomware*: Quais os impactos e como as organizações reagem a um ataque?

06 Perfil das organizações

07 Valor de resgate e custos de remediação

09 Como funciona um ataque de *ransomware*?

11 Como reagir a um ataque de *ransomware*?

16 Detecção e Análise

17 Contenção e Erradicação

18 Referências

Ransomware: Quais os impactos e como as organizações reagem a um ataque?

Os custos globais do crime cibernético têm previsão média de crescimento de 15% ao ano nos próximos cinco anos, de acordo com estudo realizado pela *Cybersecurity Ventures*, chegando a US$ 10,5 trilhões anuais até 2025 (em comparação com US$ 3 trilhões em 2015). Os números representam a maior transferência de riqueza econômica da história, o que ameaça os incentivos para inovação e investimento.[1]

Ransomware é uma forma de *malware* (*software* malicioso) que criptografa os arquivos da vítima para que não possam ser acessados. O criminoso, então, exige que a vítima pague um resgate para que seu acesso livre seja restaurado. Os ataques mais recentes incluem a exfiltração de dados de um alvo antes da criptografia, adicionando a liberação pública desses dados como uma segunda camada de extorsão.[2]

É importante ressaltar que os ataques de *ransomware* podem impactar negativamente uma organização de diversas maneiras, com perdas totais atingindo dezenas ou mesmo centenas de milhões de dólares[3].

Os impactos a curto prazo podem incluir:

(i) interrupção de operações críticas de negócios devido à incapacidade de acesso aos dados;
(ii) custos associados à resposta ao incidente e esforços de mitigação;
(iii) perda de produtividade; e
(iv) pagamento do resgate, caso a organização opte por acatar a extorsão.

Já os impactos a longo prazo são:

(i) diminuição de receita;
(ii) danos à reputação da marca;
(iii) demissões de funcionários;
(iv) perda de liderança, clientes e parceiros estratégicos; e
(v) em algumas circunstâncias, comprometimento da viabilidade do negócio como um todo.

Em maio de 2021, por exemplo, a empresa que controla boa parte da rede de dutos dos EUA pagou US$ 4,4 milhões aos criminosos por uma chave de descriptografia para desbloqueio de seus sistemas - um dos ataques de maior impacto até hoje.

A companhia fornece aproximadamente 45% do gás usado ao longo da Costa Leste dos Estados Unidos, sendo que o ataque interrompeu o serviço por seis dias, provocando uma escassez da matéria que elevou os preços do galão acima de US$ 3 pela primeira vez desde 2014[4].

Em outubro deste ano, representantes de 32 países da "Iniciativa Contra *Ransomware*", incluindo o Brasil, reuniram-se para discutir o tema, que culminou com a publicação de um comunicado conjunto cuja proposta é combater a lavagem de dinheiro feita com o uso de criptomoedas. O grupo de países reconhece que o *ransomware* é uma ameaça crescente à segurança global, com graves consequências econômicas e de segurança.[5]

Desse modo, os governos destacaram a necessidade de uma ação urgente, com prioridades e esforços comuns para reduzir o risco desse tipo de ataque, estando entre eles a melhoria da resiliência da rede para evitar incidentes quando possível, bem como resposta com eficácia a eles, e o combate ao ecossistema que promove o ataque por meio da aplicação da lei, investigando e processando os atores envolvidos.

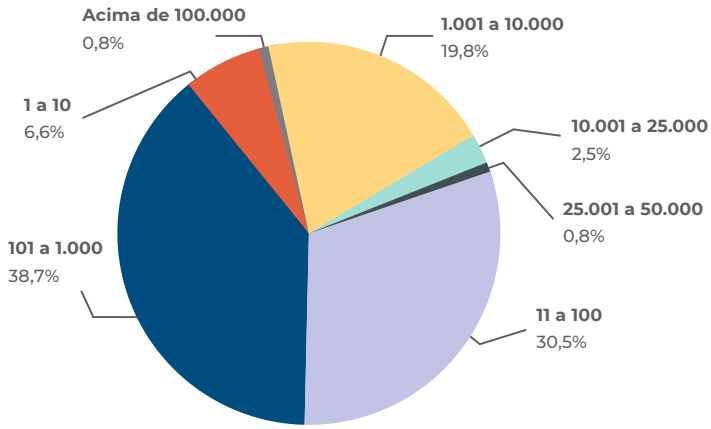
O comunicado aborda, ainda, a importância da cooperação internacional para combater o *ransomware*, de forma a inibir, rastrear e interditar os fluxos de pagamento, de acordo com leis e regulamentações nacionais, reduzindo, assim, os incentivos econômicos da atividade. Essa cooperação pode incluir esforços destinados a facilitar a devida diligência do cliente, relatórios de atividades suspeitas e monitoramento de transações.

Nesse contexto, desenvolvemos este guia porque, embora demandas milionárias cheguem às manchetes, ataques não relatados devastam empresas e organizações de pequeno e médio portes todos os dias. Entender como funciona a economia do *ransomware* ajuda a compreender a extensão da ameaça, bem como a importância de se preparar para um possível ataque.

Perfil das organizações

O ataque sofrido pela operadora de oleodutos norte-americana demonstra que empresas de médio e pequeno portes não estão imunes à ameaça dos *ransomwares*. Pelo contrário, elas constituem o principal alvo desse tipo de ataque. O relatório trimestral do *Coveware Ransomware* (gráfico ao lado) demonstrou que 75% dos ataques visam empresas com menos de mil funcionários.[6]

Distribuição por Tamanho da Empresa (Contagem de Funcionários)

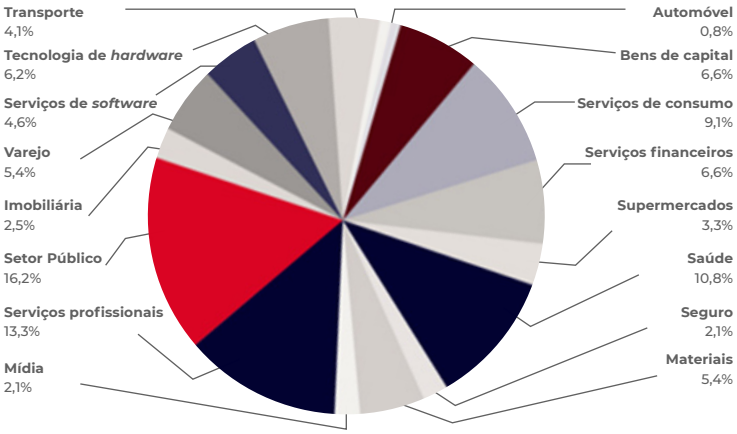


Fonte: Coveware, 2021.

É importante destacar que nenhum setor de negócios está imune a esse tipo de ameaça. Uma pesquisa realizada pela *Cybereason*[7] mostrou que, entre as organizações que relataram perda de receita devido a ataques de *ransomware*, 73% atuavam no setor financeiro, 74% no setor varejista, 64% no setor da saúde, 64% com tecnologia, 58% no setor automobilístico, 51% na manufatura e 50% no setor jurídico. Em 75% dos casos, as vítimas eram entidades governamentais.

A prevalência de ataques no setor público, de serviços profissionais e ao consumidor, bem como financeiro e de saúde, também se manteve no segundo trimestre de 2021, conforme revela o relatório da *Coveware Ransomware*[8].

Indústrias que foram vítimas de ataque *ransomware* em 2021



Fonte: Coveware, 2021.

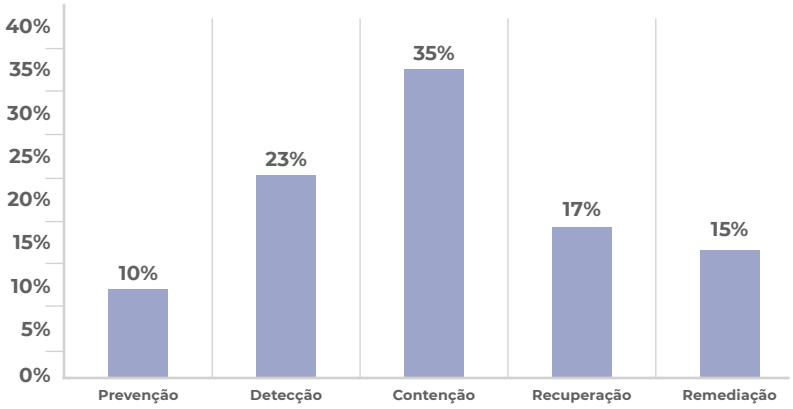
O que acontece é que as organizações pensam que estão totalmente preparadas para lidar com o impacto de um ataque de *ransomware* por terem seguro cibernético, *backups* e serem capazes de concluir os esforços de recuperação em pouco tempo. Mas a realidade é que, independentemente do quão preparada uma organização esteja para responder a um ataque desse tipo, o risco de danos significativos é extremamente alto.

De acordo com **estudo produzido** pela Coalition, uma das maiores seguradoras do ramo na América do Norte[9], os ataques de *ransomware* geraram quase metade de todas as reivindicações de seguro cibernético (41%) nos primeiros seis meses de 2020.

No entanto, a cobertura nem sempre é ampla e garante o custeio dos prejuízos. Além disso, são poucas as organizações capazes de impedir um ataque de *ransomware*.

Entre as organizações entrevistadas que possuíam apólices de seguro em vigor e foram vítimas de um ataque de *ransomware*, 42% relataram que sua seguradora cobriu apenas uma parte das perdas. Já em outra pesquisa, dos 23% dos entrevistados, dos 23% dos entrevistados que relataram ataques à organização, apenas 10% conseguiram se proteger, enquanto outros 35% afirmaram que o problema foi tratado apenas na fase de contenção.

Em qual fase do ciclo de cibersegurança o ataque de *ransomware* foi tratado?



Fonte: Ponemon Institute, 2020.

Valor de resgate e custos de remediação

O pagamento médio de resgate no segundo trimestre de 2021 foi de US$ 136,5 mil, com duração média do incidente e interrupção das atividades de 23 dias. Os números foram divulgados no relatório trimestral do *Coveware Ransomware* e se aproximam dos resultados obtidos em pesquisa realizada por outra empresa de cibersegurança em 2020.

Nesse estudo, dos 357 entrevistados que pagaram o resgate, 282 também compartilharam o valor exato pago, sendo US$ 170,4 mil a média desembolsada. No entanto, o espectro de custeio de resgate era muito amplo, tendo pagamento comum de US$ 10 mil (apontado por 20 entrevistados), sendo o mais alto de US$ 3,2 milhões (apontado por dois entrevistados).

De acordo com a pesquisa, a variação no espectro de valores pagos pode ser explicada pelos seguintes fatores:

Tamanho da organização: as organizações de pequeno e médio portes (entre 100 e 5.000 funcionários) têm, em geral, menos recursos financeiros que empresas maiores. Os criminosos ajustam a demanda de resgate de acordo com a capacidade de pagamento de suas vítimas, normalmente aceitando pagamentos mais baixos de empresas menores. De acordo com o estudo, o pagamento de resgate médio de organizações com 100-1.000 funcionários chegou a US$ 107,6 mil, enquanto o de organizações com 1.000 a 5.000 funcionários teve valor de US$ 225,5 mil;

Natureza do ataque: existem muitos agentes de *ransomware* e muitos tipos de ataque, desde invasores altamente qualificados, que usam táticas, técnicas e procedimentos sofisticados com foco em alvos específicos, a operadores menos qualificados, que usam *malwares* genéricos. Os invasores que investem em um ataque direcionado estão em busca de altos pagamentos de resgate em troca de seus esforços, enquanto os operadores por trás de ataques genéricos geralmente aceitam menor retorno sobre o investimento;

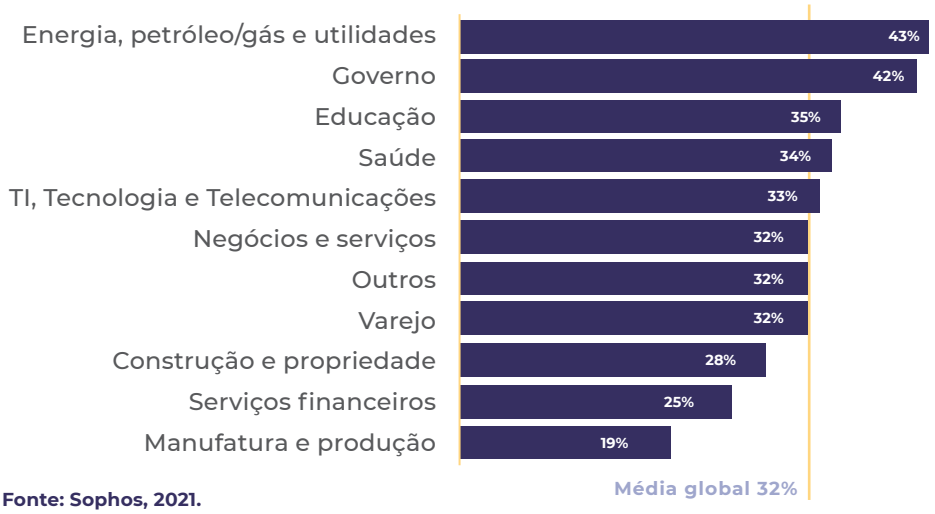
Localização: os atacantes direcionam seus maiores pedidos de resgate para as economias ocidentais desenvolvidas, motivados por sua capacidade de pagar quantias maiores. Os dois maiores pagamentos de resgate foram relatados por entrevistados na Itália. Além disso, o pagamento médio de resgate nos EUA, Canadá, Reino Unido, Alemanha e Austrália foi de US$ 214 mil, número 26% maior que a média global.

Ainda segundo a pesquisa, o percentual de organizações vítimas de *ransomware* que pagaram o resgate aumentou de 26%, em 2020, para 32% neste ano[10]. A propensão para efetuar o pagamento do resgate varia de acordo com o setor de atuação das empresas, a depender do tipo de serviço prestado e da capacidade de restaurar dados afetados a partir de *backups*.

Os setores de gás e energia, por exemplo, têm a maior probabilidade de pagar o resgate, com 43% dos entrevistados reconhecendo que gastaram dinheiro para recuperar a empresa. Esses setores tipicamente possuem muita infraestrutura legada (digital) que não pode ser facilmente atualizada, razão pela qual as vítimas se sentem compelidas a pagar o resgate e, com isso, viabilizar a continuidade dos serviços.

Propensão para pagamento do resgate segundo setor de atuação

Existem diferenças consideráveis no pagamento de resgates entre os setores



Fonte: Sophos, 2021.

Outro fator em destaque refere-se ao aumento do custo de remediação, que foi, no período em questão, de US$ 1,8 milhão, mais do que o dobro do custo relatado em 2020, de US$ 761,1 mil.

Como funciona um ataque de *ransomware*?

Ransomware significa um *software* malicioso que infecta computadores e dispositivos móveis, restringindo o acesso a arquivos, sistemas ou redes, a menos que um resgate seja pago. É possível que usuários façam o *download* acidental do *malware* ao abrir anexos de e-mail, clicar em anúncios, links ou até mesmo ao visitar sites que contêm o *malware*.

Assim que o código é carregado em um computador, ele bloqueia o acesso ao próprio computador ou a dados e arquivos armazenados na máquina. Versões mais ameaçadoras podem criptografar arquivos e pastas em unidades locais, unidades conectadas e até mesmo computadores em rede[11].

As variantes mais comuns de *ransomware* em 2021 foram:

Posição	Tipo - Ransomware	Quota de mercado	Comparativo em relação a 2020
1	Sodinokibi	16,5%	-
2	Conti V2	14,4%	+3
3	Avaddon	5,4%	Novo entre as principais variantes
4	Mespinoza	4,9%	Novo entre as principais variantes
5	Hello Kitty	4,5%	+1
6	Ryuk	3,7%	-3
7	Clop	3,3%	Novo entre as principais variantes
8	THT V2	2,9%	Novo entre as principais variantes
9	LV	2,5%	Novo entre as principais variantes
10	Zeppelin	2,5%	

Fonte: Coveware, 2021.

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

Um típico ataque de *ransomware* segue as seguintes fases:

Infecção: O *ransomware* invade por meio de um vetor, como um e-mail de *phishing* ou anexo, e começa a se instalar nas redes e dispositivos pretendidos ou disponíveis;

Troca de chaves de segurança: O *ransomware* alerta o servidor de comando e o controle do atacante para criar chaves criptográficas para uso na rede local;

Criptografia: O *ransomware* criptografa arquivos nos servidores e rede locais;

Extorsão: O *ransomware* apresenta instruções nas telas de dispositivos locais, demandando que a organização realize o pagamento do resgate, caso contrário os dados serão destruídos;

Pagamento ou recuperação: A organização possui duas escolhas a essa altura:

1. Ela pode realizar o pagamento do resgate e depender dos criminosos para restaurar os arquivos criptografados – o que não é garantido; ou

2. Ela pode apagar os arquivos infectados e restaurar os dados a partir de *backups*[12].

No caso de um ataque de dupla extorsão (*double extortion*), os criminosos ameaçam expor ou vender os dados das vítimas, muitos deles de caráter confidencial ou protegidos por propriedade intelectual. No último ano, o número de ataques nos quais os criminosos conseguiram criptografar com sucesso os dados caiu de 73% para 54%, com muitas organizações conseguindo impedir o ataque antes da criptografia[13].

Entretanto, é possível notar que o percentual de ataques em que dados não foram criptografados, mas a vítima, ainda assim, foi extorquida, mais que dobrou – saltando de 3% para 7%.[14] Isso mostra que alguns criminosos estão mudando o estilo de ataque para, em vez de criptografar arquivos, ameaçar a publicação dos dados roubados caso o resgate não seja pago, o que requer menos esforços por parte deles. Além disso, os valores que as organizações eventualmente terão de pagar como sanção por uma violação de dados pessoais são incluídos pelos criminosos no cálculo do resgate solicitado, aumentando o incentivo das vítimas para realizar o pagamento.

Um processo de exfiltração segue as seguintes etapas:

Atividades pré-exfiltração: os atores de ameaça estabelecem acesso e identificam sistemas que possam conter dados e informações sensíveis;

Coleta de dados e preparação: preparação dos arquivos para serem exfiltrados;

Exfiltração de dados: utilização de um método de transferência de arquivos para exfiltrar os dados;

Execução do *ransomware*: uma vez que os arquivos tenham sido exfiltrados, será executada a criptografia pelo *ransomware*;

Extorsão: os criminosos ou ameaçam vazar os dados, a menos que o resgate seja pago, ou vazam os dados, publicando-os em site de extorsão, sendo requerido pagamento para a remoção das informações.[15]

Como reagir a um ataque de *ransomware*?

Um dos maiores problemas que as organizações enfrentam quando estão sujeitas a um ataque de *ransomware* é se devem ou não realizar o pagamento do resgate exigido. Existem inúmeros fatores a considerar:

(i) deve-se contratar um especialista para negociar os termos do pagamento?;
(ii) após o pagamento, os invasores farão a devolução de todos os dados?;
(iii) como agir em caso de dados corrompidos no processo?;
(iv) como agir se o invasor estiver em país onde o pagamento de resgate é considerado crime?; e
(v) como saber se o pagamento vai encorajar os invasores a realizar novos ataques?.

Infelizmente, diante de um ataque de *ransomware*, se o resgate não for pago, os negócios podem ficar paralisados por dias - ou mesmo semanas - à medida que os dados são restaurados dos *backups*, restabelecendo, assim, os sistemas. No caso de dupla extorsão, não pagar o resgate também significa aceitar o risco de que dados confidenciais ou propriedade intelectual sejam expostos publicamente ou vendidos na *Dark Web*. Novamente, o impacto financeiro da perda de negócios e da produtividade, combinado com o custo dos esforços de recuperação, muitas vezes pode exceder a demanda de resgate.

Por outro lado, a alternativa - pagar o resgate - também traz problemas e riscos. Dos entrevistados ouvidos pela *Cybereason*, cujas organizações realizaram o pagamento, 46% indicaram que conseguiram recuperar o acesso aos dados, porém alguns ou todos os dados estavam corrompidos.

As ferramentas fornecidas pelos invasores para descriptografar os dados costumam ser lentas e inadequadas, o que força as empresas a restaurar seus próprios *backups*, mesmo depois de terem realizado o pagamento do resgate[16].

Da mesma forma, o estudo revelou que 96% das companhias cujos dados foram criptografados obtiveram de volta informações após o ataque - no entanto, apenas 65% desses dados foram efetivamente restaurados[17]. Além disso, das organizações que optaram por pagar o resgate, 80% incorreram em outro ataque, dos quais 46% acreditavam se tratar dos mesmos invasores e 34% de agentes diversos. Ademais, não há garantia de que os dados não serão vendidos ou expostos on-line após o pagamento do resgate[18].

> O *Federal Bureau of Investigation* dos Estados Unidos (FBI) não apoia o pagamento de resgate em resposta a um ataque de *ransomware*, uma vez que a medida não garante o recebimento dos dados de volta. Além disso, o pagamento incentiva os perpetradores a conseguir mais vítimas.[19]

Embora não haja, no ordenamento jurídico brasileiro, sanção penal ou administrativa prevista para organizações ou indivíduos que realizam o pagamento do resgate, é importante se atentar para possível violação à legislação de outros países. Por exemplo, em setembro de 2021, o Departamento de Ativos Estrangeiros do Tesouro Americano (*Department of the Treasury's Office of Foreign Assets Control* - OFAC) emitiu um comunicado descrevendo os riscos envolvidos na facilitação de pagamentos de resgate a agentes mal intencionados que conduzem ataques de *ransomware* a entidades norte-americanas[20].

O documento também orientou sobre as medidas que as empresas ou entidades públicas afetadas por um ataque de *ransomware* podem tomar para mitigar possíveis ações de imposição resultantes de violações inadvertidas dos regulamentos do OFAC. Segundo o Departamento, ao fazer o pagamento de resgate, as vítimas correm o risco de se envolver em transações diretas ou indiretas com indivíduos ou entidades que as colocariam em risco de responsabilidade, bem como com entidades cobertas por embargos abrangentes de país ou região (como Cuba; a região da Crimeia, na Ucrânia; Coreia do Norte; Irã; e Síria).

O envolvimento em transações financeiras com atores sancionatórios é proibido por diversas normas norte-americanas aplicadas pelo OFAC, sendo que as entidades que desrespeitam as regras podem ser consideradas objetivamente responsáveis, estando sujeitas a sanções[21]. A Agência de Segurança Cibernética e de Infraestrutura dos Estados Unidos (*Cybersecurity & Infrastucture Security Agency* - CISO) também corrobora que o pagamento do resgate não garante o processo de descriptografia dos dados ou que os sistemas não estarão comprometidos.[22]

No contexto europeu, a Autoridade de Proteção de Dados italiana (*Garante per la Protezione dei Dati Personale*) ressalta que pagar o resgate é apenas, em tese, a solução mais fácil para o problema. Isso porque, além do prejuízo econômico, há o risco de não receber os códigos de desbloqueio ou acabar em "listas de pagadores" potencialmente sujeitos a ataques periódicos de *ransomware*.[23]

A solução recomendada pela Autoridade é entrar em contato com técnicos especializados capazes de desbloquear o dispositivo, sendo uma alternativa eficaz a formatação da máquina, quando, além de eliminar o *malware*, todos os dados nela contidos serão perdidos, sendo imprescindível que sejam feitos *backups* periódicos. Finalmente, é recomendado sempre relatar o ataque às autoridades policiais competentes, bem como reportar uma possível violação de dados pessoais.

Por sua vez, a Autoridade Espanhola de Proteção de Dados (AEPD) destaca que, das notificações de violação de dados recebidas a partir de 25 de maio de 2018 (data de entrada em vigor do GDPR), 45% resultaram de ataques cibernéticos ocorridos por meio de técnicas de *hacking*, algum tipo de *malware* ou *phishing*[24], enquanto 71% das notificações recebidas indicam que a confidencialidade dos dados pessoais foi afetada, sendo que 36% mostram disponibilidade comprometida.

Ao mesmo tempo, vale ressaltar que mais de 50% das notificações de violação de dados indicam um contexto externo e intencional, enquanto cerca de 10% das notificações demonstram que o motivo por trás da violação foi a criptografia de dados com algum tipo de *ransomware*, e, ocasionalmente, o vetor de ataque é por meio de protocolos de área de trabalho remota.

Apenas nos primeiros cinco meses de 2021, a AEPD recebeu relatos de mais de 700 violações de dados pessoais. A maioria delas foi causada por um ataque externo e intencional, sendo o *ransomware* a ameaça mais frequente, comprometendo não apenas a disponibilidade, mas a confidencialidade dos dados pessoais.

A AEPD destaca que ceder às chantagens dos criminosos não é uma opção e aconselha as empresas a manter as informações que foram criptografadas, caso possam ser desenvolvidas ferramentas no futuro para descriptografá-las.[25]

No mesmo sentido, a Autoridade Francesa de Proteção de Dados (CNIL) recebeu 2.825 notificações de violações de dados pessoais em 2020, 24% a mais do que em 2019. Para mais de 500 delas, a origem foi um ataque de *ransomware*, e a Autoridade relatou aumento para estabelecimentos de saúde.[26] A Agência Nacional de Segurança de Sistemas de Informação Francesa (ANSSI) também não recomenda o pagamento do resgate em caso de ataque, uma vez que ele não garante a obtenção de um meio de descriptografia, além de incentivar os cibercriminosos a continuar suas atividades e, portanto, manter o sistema fraudulento.[27]

Além disso, pagar o resgate não impede que a organização seja alvo de ataque novamente. A experiência mostra que a obtenção da chave de descriptografia nem sempre torna possível reconstituir todos os arquivos comprometidos. Em particular, os arquivos modificados por aplicativo e criptografados ao mesmo tempo por *ransomware* têm grandes chances de serem corrompidos, a exemplo de arquivo de banco de dados. O *Information Commissioner's Office* (ICO), Autoridade de Proteção de Dados do Reino Unido, por sua vez, divulgou números relativos a violações de dados pessoais recebidas no primeiro trimestre de 2021: somente de *ransomware*, foram 219 reclamações.[28]

01 Setor de finanças, seguros e crédito - 57 incidentes relatados

02 Setor de varejo e manufatura - 34 incidentes relatados

03 Setor de governos locais - 32 incidentes relatados

04 Setor de educação e cuidados infantis, além do classificado como "negócios em geral" - ambos com 17 casos de incidentes relatados

É importante destacar que tanto o Regulamento Geral de Proteção de Dados da União Europeia (*General Data Protection Regulation* - GDPR) quanto a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709/2018) exigem que os controladores de dados tomem medidas técnicas e de segurança adequadas para manter os dados protegidos contra, entre outros casos, perda, destruição e/ou acessos indevidos.

Se os dados pessoais pelos quais o controlador é responsável forem criptografados ou expostos como resultado de um ataque de *ransomware*, as autoridades de proteção de dados poderão considerar que ele não tomou as medidas adequadas para mantê-los seguros e, portanto, violou seu dever conforme a lei. Incidentes de segurança, inclusive *ransomware*, envolvendo dados pessoais requerem a notificação à Autoridade de Proteção de Dados competente, a depender do grau de risco (bem como aos titulares afetados).

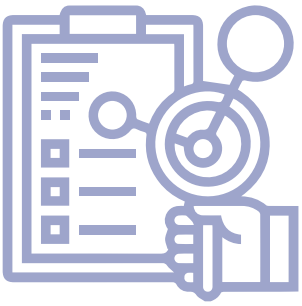
A ANPD (Autoridade Nacional de Proteção de Dados), do Brasil, em seu **Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**, ressalta a importância de cópias de segurança, comumente chamadas de *backups*, serem realizadas regularmente de forma completa e armazenadas em locais seguros e distintos dos dispositivos de armazenamento principais. Também ressalta a importância de cópias não serem sincronizadas on-line (em tempo real), para evitar a perda de dados em casos de infecções por códigos maliciosos (*ransomware*)[29].

Para um passo a passo completo sobre como lidar com incidentes, envolvendo ou não dados pessoais, recomendamos nosso guia sobre **"como identificar e reagir a incidentes de segurança"**.

A Agência de Segurança Cibernética e de Infraestrutura dos Estados Unidos recomenda às organizações responder ao ataque usando a lista de verificação fornecida em seu Guia de *Ransomware*, consistente nas seguintes etapas:

(i) detecção e análise; e
(ii) contenção e erradicação.

Detecção e Análise



Aqui é importante determinar quais sistemas foram afetados e isolá-los imediatamente. Se vários sistemas ou sub-redes forem afetados, é recomendado colocar a rede *off-line* no nível do *switch*. Pode não ser viável desconectar sistemas individuais durante um incidente. Se isso não for possível, o recomendado é localizar o cabo de rede (por exemplo, *Ethernet*) e desconectar os dispositivos afetados da rede, ou removê-los do *Wi-Fi* para conter a infecção.

Após um comprometimento inicial, agentes mal intencionados podem monitorar a atividade ou as comunicações da organização para entender se suas ações foram detectadas. Nesse caso, há duas recomendações: isolar os sistemas de maneira coordenada e usar métodos de comunicação fora da banda, como chamadas telefônicas ou outros meios, para evitar que os atores saibam que foram descobertos, e que ações de mitigação foram realizadas.

Caso isso não seja feito, os criminosos podem se mover lateralmente para preservar seu acesso - que já é uma tática comum - ou implantar *ransomware* amplamente antes de as redes ficarem *off-line*. Somente no caso de impossibilidade de desconectar os dispositivos da rede é que se deve desligá-los para evitar a propagação da infecção por *ransomware*, o que impedirá o armazenamento de artefatos de infecção e possíveis evidências.

Já na análise, deverá ser feita a triagem dos sistemas infectados, identificando e priorizando aqueles em estado crítico, o que confirmará a natureza dos dados armazenados nos sistemas afetados. necessário priorizar restauração e recuperação com base em uma lista predefinida de ativos críticos, incluindo sistemas de informações essenciais para sade e segurança, geração de receita ou outros serviços críticos, bem como sistemas dos quais eles dependem.

É recomendado, ainda, o acompanhamento dos sistemas e dispositivos que não foram percebidos como afetados, para que não sejam priorizados para restauração e recuperação. Isso permite que sua organização volte aos negócios de maneira mais eficiente. Também deve-se consultar a equipe de resposta a incidentes para desenvolver e documentar uma compreensão do que ocorreu com base na análise inicial, além de envolver equipes, internas e externas, e partes interessadas, com o entendimento do que eles podem fornecer para ajudar a mitigar, responder e se recuperar do incidente.

Diante de um incidente, a organização deve sempre compartilhar as informações que ela tem à disposição para receber a assistência mais oportuna e relevante, mantendo a gerência e os líderes sêniores informados por meio de atualizações regulares à medida que a situação avançar para a resolução.

Contenção e Erradicação

Se nenhuma ação de mitigação inicial for possível, deve-se:

- Fazer uma captura de imagem e memória do sistema de uma amostra de dispositivos afetados (por exemplo, estações de trabalho e servidores), coletando todos os *logs* relevantes, bem como amostras de quaisquer binários de *malware* "precursores" e observáveis associados ou indicadores de comprometimento (por exemplo, comandos suspeitos e endereços IP de controle, entradas de registro suspeitas ou outros arquivos relevantes detectados). Atenção para a necessidade de preservação das evidências de natureza altamente volátil - ou de retenção limitada - para evitar perda ou adulteração (por exemplo, memória do sistema, *logs* de segurança, dados em *buffers* de *log* do *firewall*).

- Consultar as autoridades federais sobre os possíveis profissionais de descriptografia disponíveis, uma vez que pesquisadores de segurança já quebraram os algoritmos de criptografia para algumas variantes de *ransomware*.

Referências

[1] MORGAN, Steve. Cybercrime to cost the world $10.5 trillion annually by 2025. Cybersecurity Ventures, nov. 2020. Disponível em: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021. Acesso em: 03 out. 2021.
[2] BLACKBAZE. The Complete Guide to Ransomware, 2021. Disponível em: https://hub.backblaze.com/complete-guide-to-ransomware. Acesso em: 18 out. 2021.
[3] CYBEREASON. Ransomware: The true cost to business, 2021. Disponível em: https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf. Acesso em: 04 out. 2021.
[4] COVEWARE. Q2 Ransom Payment Amount Decline as Ransomware Becomes a National Security Priority, 2021. Disponível em: https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-na-tional-security-priority. Acesso em: 18 out. 2021.
[5] CISO ADVISOR. Combate a Ransomware sufocará finanças do crime, out. 2021. Disponível em: https://www.cisoadvisor.com.br/combate-ao-ransomware-sufocara-financas-do-crime. Acesso em: 18 out. 2021.
[6] Idem.
[7] MORGAN, Steve. Op. cit, 2021.
[8] COVEWARE. Op. cit., 2021.
[9] CIMPANU, Catalin. Ransomware accounted for 41% of all cyber insurance claims in H1 2020. Zero Day, set. 2020. Disponível em: Ransomware accounted for 41% of all cyber insurance claims in H1 2020 | ZDNet. Acesso em: 03 out. 2021.
[10] SOPHOS. The State of Ransomware, 2021. Disponível em: https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx. Acesso em: 18 out. 2021.
[11] ESTADOS UNIDOS. Federal Bureau of Investigation (FBI). Ransomware, 2021. Disponível em: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware. Acesso em: 04 out. 2021.
[12] BLACKBLAZE. Op. cit., 2021.
[13] SOPHOS. Op cit., 2021.
[14] Idem.
[15] BLACKBAZE. Op. cit., 2021.
[16] CYBEREASON. Op. cit., 2021.
[17] SOPHOS. Op. cit., 2021., 2021.
[18] CYBEREASON. Op. cit., 2021.

Referências

[19] ESTADOS UNIDOS. Federal Bureau of Investigation (FBI). Op. cit., 2021.
[20] ESTADOS UNIDOS. Department of Treasury. Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, set. 2021. Disponível em: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf. Acesso em: 02 out. 2021.
[21] UNIÃO EUROPEIA. Conselho da Europa. Cyber Attacks Council prolongs framework for sanctions for another year, 2021. Disponível em: https://www.consilium.europa.eu/en/press/press-releases/2021/05/17/cyber-attacks-council-prolongs-framework-for-sanctions-for-another-year. Acesso em: 18 out. 2021.
[22] ESTADOS UNIDOS. Cybersecurity & Infrastucture Security Agency (CISO). Ransomware Guide, set. 2020. Disponível em: https://www.cisa.gov/stopransomware/ransomware-guide. Acesso em: 04 out. 2021.
[23] ITÁLIA. GARANTE PER LA PRIVACY. Ransomware, 2021. Disponível em: https://www.garanteprivacy.it/temi/cybersecurity/ransomware. Acesso em: 18 out. 2021.
[24] ESPANHA. AEPD. Personal Data Breaches: Protect yourself against ransomware. Disponível em: https://www.aepd.es/en/prensa-y-comunicacion/blog/personal-data-breaches-protect-yourself-against-ransomware. Acesso em: 18 out. 2021.
[25] ESPANHA. AEPD. Personal Data Breaches, 2021. Disponível em: https://www.aepd.es/en/prensa-y-comunicacion/blog/personal-data-breaches. Acesso em: 18 out. 2021.
[26] FRANÇA. CNIL. CNIL publishes its 2020 activity report, 2021. Disponível em: https://www.cnil.fr/en/cnil-publishes-its-2020-activity-report. Acesso em: 18 out. 2021.
[27] FRANÇA. ANSSI. ANSSI Guide Attaques Par Racongiciels, 2021. Disponível em: https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf. Acesso em: 18 out. 2021.
[28] REINO UNIDO. ICO. Data security incident trends, 2021. Disponível em: https://ico.org.uk/action-weve-taken/data-security-incident-trends. Acesso em: 18 out. 2021.
[29] BRASIL. ANPD. Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf/view. Acesso em: 18 out. 2021.

Créditos

Sócios

José Roberto Opice Blum
Renato Opice Blum
Marcos Gomes da Silva Bruno
Rony Vainzof
Camilla Jimene
Caio César Carvalho Lima
Danielle Serafino

Conteúdo jurídico

Giovana Figueiredo Peluso Lopes

Coordenação editorial

Bruno Toranzo

Revisão

Giovana Figueiredo Peluso Lopes
Bruno Toranzo
Yasmin Brandão

Arte e diagramação

Paola Cosentino

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF