Marsh

Estatísticas de ransomware que toda empresa precisa saber

Os ataques de ransomware estão se intensificando em frequência, gravidade e sofisticação –em 2020 aumentaram 148% devido à superfície de ataque mais ampla e aumento do trabalho remoto associado à pandemia.

- Aumento nos ataques de ransomware, impulsionado pela pandemia: **148%**
- A estimativa dos custos globais associados à recuperação de ataques de ransomware em 2021: **US$ 20 bilhões**
- Demanda média de resgate no Q4 2020: **US$ 154.108** (-34% em relação ao Q3 2020)
- Média de dias de inatividade no Q4 2020: **21 dias** (+11% em relação ao Q3 2020)
- Porcentagem de ransomware no Q4 ameaçou vazar dados exfiltrados: **70%** (+43% em relação ao Q3 2020)
- O quão rápido uma nova porta RDP (Remote Desktop Protocol) – um dos três grandes vetores de ataques de ransomware – é descoberta depois de se conectar pela primeira vez à internet: **90 segundos**
- Quantas portas RDP mal configuradas estão abertas para a internet: **4,7 milhões**
- Número médio de ataques de ransomware ocorridos diariamente desde 1º de janeiro de 2016: **4.000**
- Mensagens de e-mail que contêm malwares (phishing de e-mail é outro dos três grandes vetores de ataques de ransomware): **1 em 3.000**

O que tudo isso significa?

A demanda média de resgate caiu no quarto trimestre de 2020. Por quê? Os cibercriminosos estão cada vez mais usando a ameaça de vazamento de dados para encorajar o pagamento de resgate, mas não necessariamente excluindo os dados exfiltrados, mesmo que o resgate seja pago. As vítimas de ransomware estão perdendo a confiança de que seus dados serão excluídos com segurança e, como tal, se recusam a ceder à extorsão cibernética.

Embora a redução dos valores médios de pagamento de resgate seja uma boa notícia para as empresas, o volume de ataques ainda está aumentando e a exfiltração de dados continua sendo uma ameaça séria. Para evitar o pagamento, as organizações devem ser capazes de restaurar e recuperar com eficácia seus dados e arquivos – e suas redes – de seus backups, ou reconstruir do zero.

O que você pode fazer?

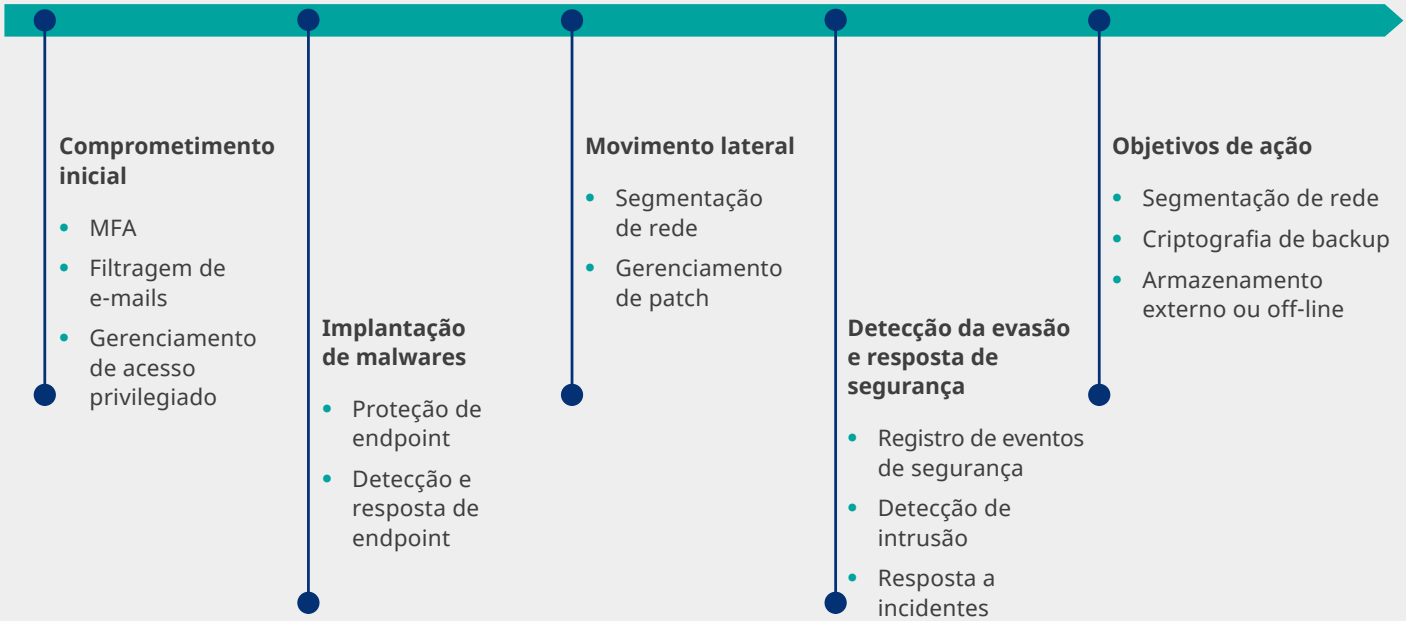
A preparação é a chave. Com a ameaça contínua de exfiltração de dados e o tempo de inatividade prolongado ocorrendo, recomendamos que você analise cuidadosamente sua estratégia de backup. Isso inclui examinar o que contém o backup, onde está hospedado, com que frequência os backups ocorrem e quem é responsável pela execução da estratégia de backup. Finalmente, é importante exercitar e testar os sistemas de backup regularmente. Alternativas de *backup* devem também ser avaliadas, pois em incidentes de maior proporção *backups* podem ser afetados.

> **" O seguro cibernético não deve ser esquecido: ele pode ser uma ferramenta valiosa na luta contra o ransomware"**

O seguro cibernético não deve ser esquecido: ele pode ser uma ferramenta valiosa na luta contra o ransomware. O seguro pode oferecer cobertura abrangente para pagamentos de resgate, custos associados e acesso a fornecedores de incidente e resposta, além de levar as organizações a melhorar seus controles de segurança. Certos controles de segurança estão começando a ser pré-requisitos para cobertura de seguro cibernético, como, autenticação multifator (MFA).

No quarto trimestre, os três principais vetores de ataque para ransomware incluíram phishing de e-mail, comprometimento de RDP e vulnerabilidades de softwares. Os controles podem oferecer alguma proteção contra cada vetor de ataque e em cada estágio de um ataque de ransomware. Abaixo está um exemplo de como um ataque de ransomware pode ser executado, bem como exemplos de apenas alguns dos controles que podem ser úteis em cada estágio do ataque.

Timeline de um ataque de ransomware – e controles compensatórios



QUAIS SERVIÇOS PODEM ME AJUDAR?

Provedores de gerenciamento de risco cibernético, corretores e seguradoras podem frequentemente apoiá-los em buscar proteção de forma econômica, através de uma variedade de recursos e serviços para ajudá-lo a preparar, responder e recuperar perdas de ataques de ransomware. Isso pode incluir:

Preparação:

- Planejamento e atualização de plano de resposta a incidentes cibernéticos
- Avaliação da preparação para evento de ransomware
- Estrutura de segurança cibernética e avaliações de vulnerabilidades
- Treinamento e educação de funcionários em relação a riscos cibernéticos
- Melhores práticas de cibersegurança através da aplicação de *frameworks* conhecidos
- Análise do impacto financeiro
- Identificação de riscos de terceiros

Resposta

- Serviços de gerenciamento de incidentes
- Identificação de fornecedor: incluindo assessoria jurídica, especialistas forenses, suporte de relações públicas e provedores de serviços de restauração de dados
- Serviços de notificação de violação de dados e assessoria especializada
- Suporte para avaliar decisão de pagamento de resgate e compra de criptomoeda
- Suporte com processo de regulação de sinistros para recuperação de perdas através do seguro

Recuperação

- Suporte em incidentes, incluindo suporte com gestão de sinistros
- Seguro cibernético para cobrir perda de receita, despesas extras e outros custos associados ao incidente de ransomware
- Suporte na preparação de prova de perdas e relatórios
- Atualização / reavaliação dos planos de resposta a incidentes

Coberturas

- Lucros Cessantes, diante de um impacto que venha resultar em perda de receita, ou despesas extras para continuar as operações
- Custos para restauração ou recriação de dados corrompidos ou destruídos e outros ativos intangíveis
- Restauração ou reparo de rede ou hardware
- Multas e penalidades regulatórias
- Custos com notificações e obrigações regulatórias diante de um vazamento de dados
- Investigação Forense
- Dano à reputação

A Marsh pode ajudar:

O pacote completo de ofertas de ransomware da Marsh inclui gerenciamento de risco cibernético e seguro. Alguns destaques: podemos ajudar sua organização a se preparar com antecedência para um ataque de ransomware, criando e testando um plano completo de resposta a incidentes cibernéticos. Também podemos projetar e fornecer uma apólice de seguro cibernético com cobertura de ransomware sob medida para sua organização. Saiba mais sobre ransomware e como podemos ajudá-lo.