RELATÓRIO

Relatório Global sobre Ransomware de 2023

Resumo executivo

A Fortinet entrevistou recentemente 569 líderes de segurança cibernética e responsáveis pela tomada de decisões de organizações de todos os tamanhos e setores em todo o mundo para entender suas perspectivas sobre ransomware, como isso afetou suas organizações e quais estratégias eles implementaram para mitigar um possível ataque. Na pesquisa deste ano, mais de 80% dos entrevistados dizem que estão "muito" ou "extremamente" preocupados com ameaças de ransomware, mas um número semelhante (78%) das organizações pesquisadas também acredita que estão "muito" ou "extremamente" preparadas para impedir uma violação. Apesar dessas preocupações e sentimentos de preparação, metade das organizações pesquisadas ainda foi vítima de ataques de ransomware no ano passado.

Apesar de 78% das organizações acreditarem que estão "muito" ou "extremamente" preparadas para mitigar um ataque, 50% ainda foram vítimas de ransomware no ano passado.

Das organizações que sofreram um incidente de ransomware, embora 72% tenham indicado que detectaram o incidente em poucas horas (muitas vezes em poucos minutos), 71% disseram que pagaram pelo menos uma parte do resgate exigido. E, embora quase todos os entrevistados tivessem seguro cibernético, isso não garantia que todos os custos fossem cobertos ou que os dados fossem restaurados. Na verdade, apenas 35% dos afetados pelo ransomware recuperaram todos os seus dados após o incidente.

Mas nem tudo são más notícias. De fato, apesar da incerteza econômica, quase todos os líderes pesquisados (91%) esperam aumentar os orçamentos de segurança no próximo ano para investir em tecnologias e serviços que protejam ainda mais suas redes de um potencial ataque de ransomware. Em geral, a principal prioridade dos líderes de segurança é implementar tecnologias avançadas, como inteligência artificial (IA) e aprendizado de máquina (ML), que permitem uma detecção mais rápida de ameaças, seguida de monitoramento central para acelerar a resposta. E especificamente, a segurança da Internet das Coisas (IoT) e os firewalls de próxima geração (NGFWs) lideraram a lista de áreas e produtos em que os líderes planejavam investir, com o maior aumento nos planos para implementar soluções de detecção e resposta a ameaças de endpoints (EDR) e gateway de e-mail seguro (SEG). Esse é um plano promissor, já que os e-mails de phishing foram o método número um que os entrevistados relataram que os agentes de ransomware usaram para obter acesso. E, claro, o endpoint é o destino final do ransomware.

Curiosamente, enquanto muitos líderes de segurança tradicionalmente acreditavam que comprar o melhor produto individual para um projeto renderia o maior nível de segurança cibernética, os dados da pesquisa deste ano indicam que as organizações que relataram adotar uma abordagem de produto pontual eram as mais propensas a se tornarem vítimas de ransomware. No entanto, a tecnologia é apenas parte da solução. A pesquisa constatou que quatro dos cinco principais desafios na prevenção de ransomware estavam relacionados a pessoas e processos.

À medida que o ransomware se prolifera e os métodos de ataque crescem em sofisticação, organizações de todas as formas e tamanhos são um alvo, tornando crucial que os líderes de segurança invistam nas tecnologias, pessoas e processos certos agora para evitar um incidente de ransomware no futuro.

A crescente sofisticação do ransomware torna toda organização um alvo

Embora o ransomware exista há décadas, a ameaça global permanece em níveis máximos. Os ataques estão ficando cada vez mais sofisticados, causando danos crescentes às organizações em todo o mundo. De acordo com observações da equipe de resposta a incidentes do FortiGuard Labs, o cibercrime financeiramente motivado foi responsável pelo maior volume de incidentes (74%) em 2022, com 82% dos cibercrimes financeiramente motivados envolvendo a implantação de ransomware ou scripts maliciosos.[1]

Embora o crescimento do ransomware ano após ano tenha diminuído em 2022 — após a explosão desse método de ataque em 2021 — a frequência dele ainda está aumentando. Por exemplo, no primeiro semestre de 2022, a FortiGuard Labs observou a introdução de 10.666 novas variantes — o dobro do número observado nos seis meses anteriores.[2] A razão provável para a mudança é que as operações de Ransomware-as-a-Service (RaaS) estão amadurecendo, permitindo que os cibercriminosos introduzam com sucesso variantes novas, mais sofisticadas e agressivas do que nunca. E eles também estão sendo mais seletivos, visando especificamente organizações capazes de pagar grandes montantes. Em contraste com o sucesso inicial do RaaS, que inicialmente dependia do volume — mais afiliados significavam mais oportunidades de se infiltrar em redes e lançar ataques — as operadoras de RaaS estão se tornando cada vez mais seletivas em relação aos associados que permitem ingressar em suas operações.

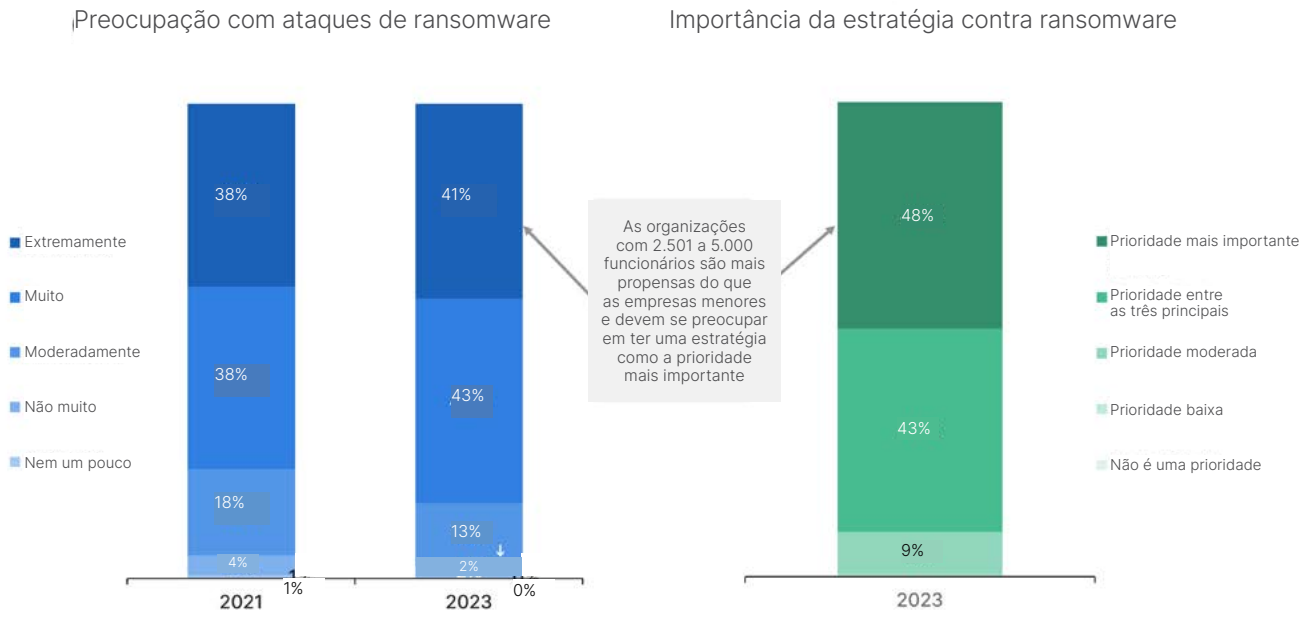
Essa abordagem mais sistemática para executar ataques de ransomware está sendo mais bem-sucedida. Para começar, os invasores estão gastando mais tempo com sondagem para identificar alvos lucrativos, o que significa que muitas demandas de resgate agora chegam a dezenas de milhões de dólares. Além disso, os resgates que esses grupos estão exigindo de seus alvos agora tendem a ser proporcionais

ao tamanho e ao setor da organização. Muitas organizações cibercriminosas usam uma fórmula para determinar o valor a ser solicitado para que a vítima tenha maior probabilidade de pagar.

Essa maturidade crescente das operações de ransomware é esperada, uma vez que o RaaS é um fator significativo do Crime-as-a-Service (CaaS). No entanto, à medida que as operadoras de RaaS se tornam mais agressivas com seus manuais e incorporam elementos cada vez mais destrutivos em ataques, como o uso crescente de wipers, organizações de todas as formas e tamanhos devem implementar estratégias de segurança apropriadas para mitigar possíveis violações.

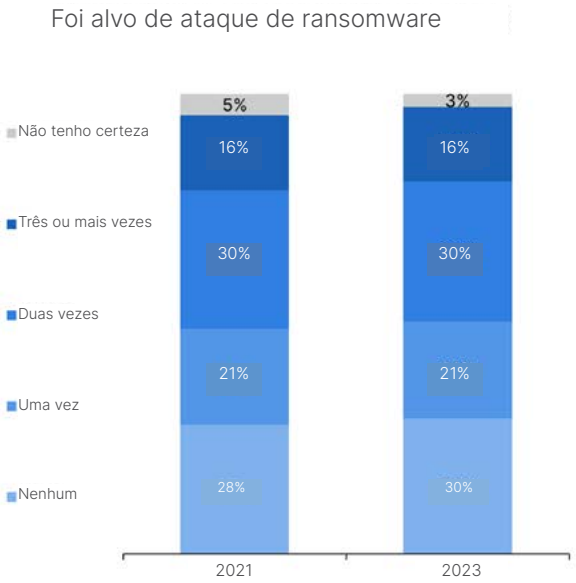
Ataques de ransomware são comuns e caros

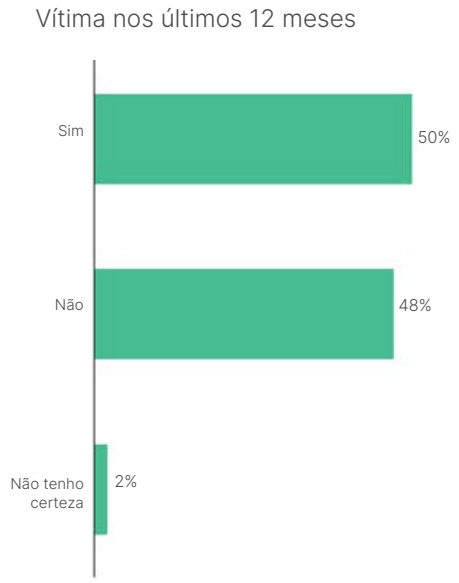
Dada a evolução e a crescente sofisticação das operações de ransomware, não é surpreendente que 84% das organizações representadas na pesquisa deste ano permaneçam "muito" ou "extremamente" preocupadas com essa ameaça, que é ainda maior do que os 76% de entrevistados que expressaram o mesmo nível de preocupação quando perguntados em 2021. No entanto, apesar dessas preocupações, 78% também acreditam que estão "muito" ou "extremamente" preparados para prevenir ou mitigar um ataque de ransomware (um aumento significativo em relação aos 63% que se sentiam assim na pesquisa anterior). De fato, mais de 90% dos entrevistados afirmaram que ter uma estratégia contra ransomware em vigor é a prioridade número um de sua equipe ou uma das três principais. E 88% incluem o seguro cibernético como parte de sua estratégia de preparação.



Infelizmente, a realidade é que permanece uma desconexão entre as percepções dos entrevistados sobre a preparação de sua organização e sua capacidade de evitar um incidente de ransomware. Dos entrevistados este ano, metade das empresas foi vítima de um ataque de ransomware nos últimos 12 meses e 46% foram alvo de ransomware duas ou mais vezes.

Das organizações pesquisadas que foram vítimas de um ataque de ransomware em 2022, o phishing, direcionado a um indivíduo ou grupo por meio de e-mails maliciosos, permaneceu como a principal tática (56%) mais uma vez. Em seguida, vêm o acesso através de portas vulneráveis (54%) e as explorações de protocolo de desktop remoto (51%), ocupando o segundo e terceiro lugares na lista. Com vários métodos relatados por mais de 50% dos entrevistados, parece que os operadores de ransomware buscam várias maneiras como parte dos mesmos ataques ou para ataques subsequentes.





A maioria dos entrevistados cujas empresas sofreram um ataque de ransomware tem uma política que determina que eles paguem o resgate solicitado. É importante notar que, apesar de a maioria (72%) detectar o incidente em poucas horas, às vezes minutos, mais de 70% disseram que pagaram pelo menos uma parte do resgate que os invasores exigiram. Isso mesmo a orientação do FBI sendo de que pagar o resgate só alimenta o problema e não garante que as organizações recuperem seus dados.[3]

Curiosamente, as organizações em certos setores eram mais propensas a pagar o resgate do que outras. Por exemplo, as organizações do setor de manufatura pagaram o resgate solicitado com mais frequência do que as de outras indústrias. E o valor solicitado também era tipicamente maior; na verdade, em 25% das violações entre as empresas de manufatura, o resgate exigido era de US$ 1 milhão ou mais. A disposição da indústria para pagar é compreensível, dado que seu custo de tempo de inatividade é muito elevado. E os invasores exigem mais dessas empresas porque sabem que elas podem pagar.

Dito isso, nem pagar o resgate nem esperar que o seguro cibernético cubra as perdas é uma estratégia eficaz para mitigar um ataque. De fato, 65% dos entrevistados não conseguiram recuperar todos os seus dados após o ataque. Além disso, quase metade (41%) das organizações com seguro cibernético não recebeu tanta cobertura quanto o esperado e, em alguns casos, não recebeu nenhuma por causa de uma exceção da seguradora.

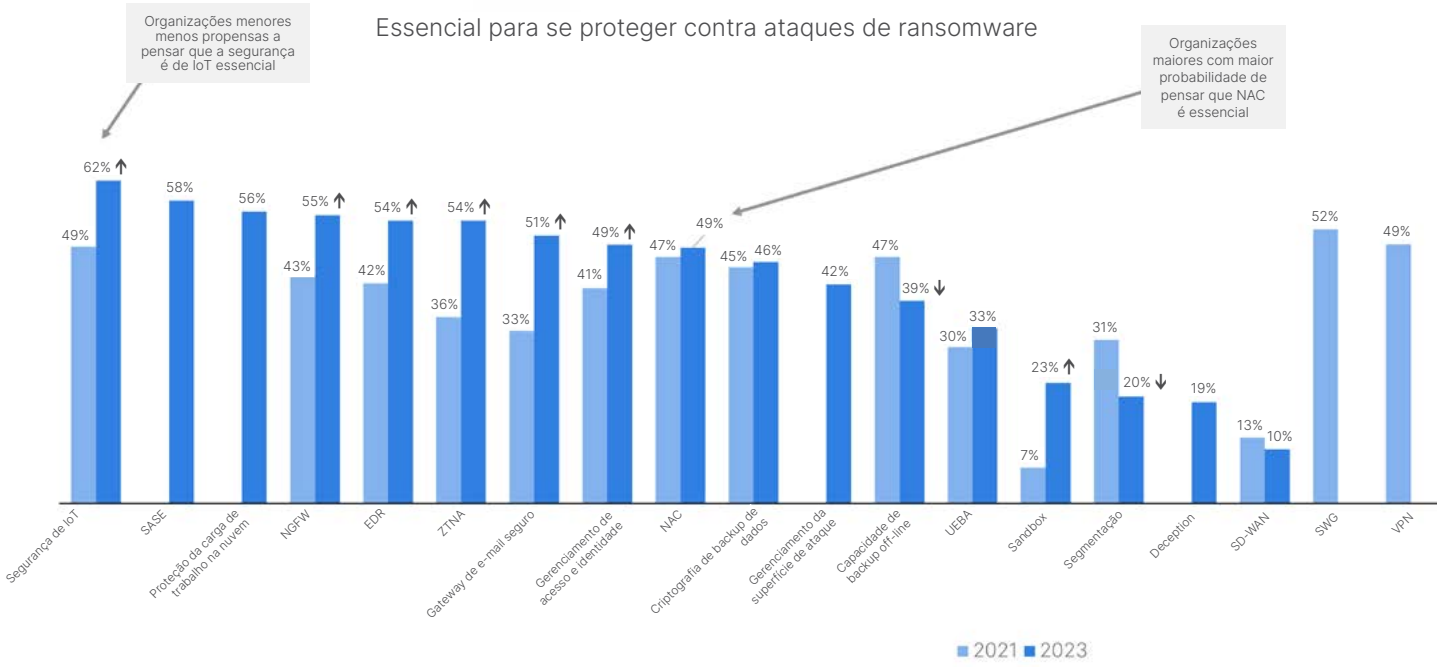
Organizações estão trabalhando ativamente para se proteger contra o ransomware, mas muitas não estão priorizando as proteções essenciais

Pela segunda vez consecutiva, os entrevistados disseram que seu principal desafio na prevenção de ataques foi a crescente sofisticação do cenário de ameaças; algo fora de seu controle. No entanto, os próximos quatro desafios — falta de clareza sobre como proteger adequadamente suas redes contra um ataque de ransomware, falta de conscientização sobre segurança cibernética entre os usuários finais, falta de cadeia de comando clara e dificuldade em impedir que os funcionários sejam enganados pela engenharia social — estavam relacionados a pessoas e processos, o que parece contradizer seu senso de estar preparado para um ataque de ransomware. Pelo lado positivo, é encorajador ver que algumas preocupações que lideraram a lista em 2021 — como as complexidades de garantir uma força de trabalho cada vez mais remota — foram menos preocupantes para os entrevistados este ano.

Também é promissor que, apesar do ambiente econômico geral, 91% das organizações esperam que seus orçamentos de segurança aumentem. Desse grupo, muitos (42%) esperam que seus orçamentos aumentem em mais de 10%, permitindo que, no próximo ano, eles façam investimentos para enfrentar esses desafios relacionados a ransomware. Para proteger suas respectivas empresas, as equipes de segurança também disseram que estão investindo em tecnologia adicional de segurança cibernética, relatando ataques com mais frequência à aplicação da lei e aproveitando seu seguro cibernético quando necessário.

Nenhum investimento único se destacou como a resposta vista como eficaz para mitigar o ransomware, o que é um bom sinal. Emvez disso, uma série de soluções foi citada como essencial para se proteger contra ataques de ransomware. Metade ou mais dos entrevistados citou cada uma das seguintes tecnologias de segurança como cruciais para suas estratégias: segurança de IoT, SASE, proteção de carga de trabalho em nuvem, NGFWs, EDR, acesso de rede de Zero Trust (ZTNA) e SEG. Em comparação com a pesquisa de 2021, o número de entrevistados que citaram as tecnologias ZTNA e SEG como ferramentas críticas aumentou quase 20%. Essa mudança na percepção é uma boa notícia, uma vez que o phishing continua sendo o vetor de ataque mais comum para obter acesso à rede de uma organização, assim, implantar controles granulares para governar o uso de aplicações e dados é uma prática recomendada importante.

No entanto, embora seja ótimo ver as empresas adotando essas tecnologias de segurança, também é interessante notar que elas não estão reconhecendo outras proteções essenciais, como sandboxing, segmentação de rede e armazenamento de dados fora das instalações, que são fundamentais na defesa contra ransomware.



Além do que é visto como importante, também perguntamos no que as organizações planejam investir a seguir. À medida que as equipes avaliam novas ferramentas para se proteger contra ataques de ransomware, entender a postura de segurança atual da empresa e identificar lacunas é um primeiro passo crucial antes de fazer investimentos adicionais. As organizações podem fazer isso mapeando as defesas atuais para a cadeia de ataque usando ferramentas como a estrutura MITRE ATT&CK. Essa abordagem ajudará as equipes a entender se tomaram as medidas mais eficazes para se defender contra ataques de ransomware e quais possíveis lacunas de segurança precisam reparar.

Os três principais investimentos planejados foram em segurança de IoT (57%), NGFWs (53%) e EDR (51%). Uma das descobertas mais surpreendentes da pesquisa anterior da Fortinet foi que o principal método de entrada em 2021 foi o phishing por e-mail, mas apenas um terço das organizações relatou planos para melhorar essa defesa. O phishing por e-mail continuou sendo o método número um de entrada pela segunda vez em 2022, algo que, esperamos, diminuirá se as organizações seguirem seus planos (47% dos entrevistados em 2022, ante aos 31% em 2021) de investimento nessa área.

Necessidade de consolidação e integração

Embora seja encorajador ver empresas investindo em tecnologias adicionais para se proteger contra ransomware, a realidade é que simplesmente adicionar ferramentas a uma caixa de ferramentas já sobrecarregada geralmente não é suficiente para reduzir o risco de uma organização ser atacada. Um número crescente de entrevistados (45%) diz que está usando uma combinação de plataformas de segurança e produtos pontuais, mas 36% continuam comprando apenas os tais produtos pontuais “melhores do mercado”. Como resultado, muitas equipes de segurança acabam gastando muito tempo gerenciando produtos individuais implantados ao longo do tempo e lutando para que sua coleção de tecnologia funcione em conjunto de forma eficaz. E esses processos manuais podem dificultar a capacidade de uma equipe de segurança de coletar os dados certos e responder prontamente a um incidente de ransomware.

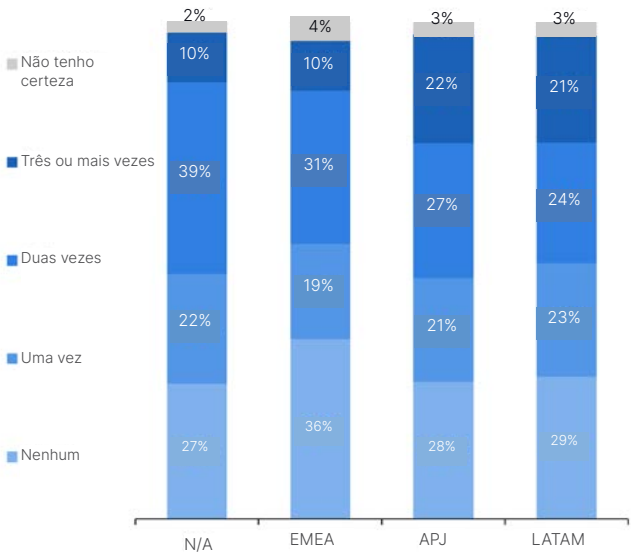
Curiosamente, aqueles que relataram adotar uma abordagem com um produto entre os “melhores do mercado” foram mais propensos (67%) a serem vítimas de um ataque de ransomware, enquanto aqueles que reduziram a sobrecarga do fornecedor consolidando para um pequeno número de plataformas complementadas por produtos pontuais foram os com menor propensão (37%) a serem impactados. Vemos mais e mais organizações consolidando o número de produtos pontuais que usam e, em vez disso, aproveitando um número menor de plataformas estratégicas. Os resultados da nossa pesquisa reforçaram isso, com 99% dos entrevistados vendo soluções integradas ou uma plataforma como essenciais para prevenir ataques de ransomware. E, novamente, não se trata apenas de tecnologia, mas também de pessoas e processos que devem usar essas plataformas corretamente para que sejam eficazes.

Breve análise de ataques de ransomware e preparação organizacional em todo o mundo

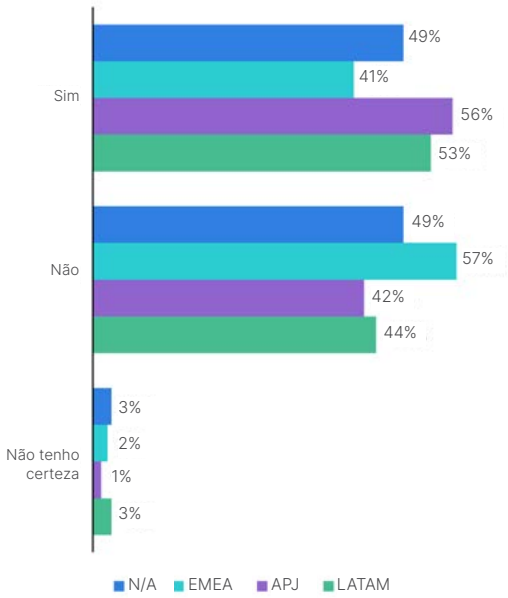
As perspectivas das organizações sobre ransomware e seus respectivos níveis de preocupação, preparação e principais desafios se normalizaram em todas as regiões, com quase todos os entrevistados em todo o mundo indicando que ter uma estratégia de ransomware era a prioridade número um ou uma das mais importantes. Da mesma forma, as regiões implementam consistentemente muitas ferramentas de detecção precoce e resposta, a maioria compra os tais produtos “melhores do mercado” e quase todas têm seguro cibernético.

No entanto, vimos uma variação na porcentagem de empresas em todas as regiões que sofreram um ataque de ransomware nos últimos 12 meses, com o maior número de incidentes de ransomware ocorrendo na Ásia-Pacífico/Japão (APJ) (56%) e o menor número (41%) sendo na Europa, Oriente Médio e África (EMEA).

Foi alvo de ataque de ransomware



Vítima nos últimos 12 meses



Não só isso, mas há diferenças em seus esforços de resposta, como a velocidade de detecção de ataques e se as organizações se sentem compelidas a pagar o resgate solicitado. Por exemplo, a América Latina (LATAM) tendia a detectar ataques mais rapidamente e era menos propensa a táticas de engenharia social do que outras regiões. Em relação à implementação de ferramentas de segurança, os entrevistados da América do Norte (NA) e da EMEA planejam investir mais no ZTNA do que os da APJ e da LATAM. Quanto às demandas de resgate, os entrevistados da EMEA viram valores de resgate menores do que em outras regiões, e quase metade dos entrevistados não pagou o resgate solicitado. As organizações da APJ viram demandas de resgate mais altas e 44% disseram que pagaram o valor total.

Olhando para o futuro: aprimorando as estratégias de segurança

Por fim, perguntamos aos entrevistados sobre os tipos gerais de tecnologias de segurança que eles planejam investir para avançar na proteção contra ataques de ransomware. Vale ressaltar que a área número um, relatada por 50% dos entrevistados, é a adoção de tecnologias avançadas alimentadas por IA e ML, que estava entre suas três principais prioridades. Os líderes de segurança também estão priorizando ferramentas centralizadas de monitoramento, como gerenciamento de informações e eventos de segurança (SIEM) e orquestração, automação e resposta

de segurança (SOAR) para acelerar os esforços de detecção e resposta. Os entrevistados também classificaram os seguintes atributos como "extremamente importantes" ao avaliar novas tecnologias: soluções que incluem inteligência de ameaças acionável (50%), têm recursos de detecção comportamental orientados por IA (48%) e são projetadas para trabalhar em conjunto (45%).

As organizações que relataram adotar uma abordagem de usar um produto pontual dentre os "melhores do mercado" para segurança foram as mais propensas (67%) a serem vítimas de ransomware, enquanto aquelas que consolidaram tecnologias para adotar uma abordagem orientada por plataforma foram as menos propensas (37%) a serem violadas.

Isso nos dá motivos para otimismo, já que as organizações estão reconhecendo que, mesmo com profissionais de segurança experientes na equipe, medidas adicionais são necessárias para impedir que os ecossistemas maduros de cibercrime tenham sucesso. Implantar mais tecnologias de detecção precoce ao longo da cadeia de ataques cibernéticos é fundamental para interromper as tentativas de ransomware.

No entanto, é importante lembrar que "mais" nem sempre significa "melhor" quando o assunto é tecnologia de segurança. As equipes geralmente gastam uma quantidade excessiva de tempo ajustando e remendando produtos pontuais diferentes, o que muitas vezes coloca uma pressão desnecessária sobre os analistas encarregados de proteger a empresa. Ao buscar uma abordagem de arquitetura de malha de segurança — um ecossistema colaborativo de tecnologia de segurança projetado para trabalhar em conjunto, como o Fortinet Security Fabric — as equipes de segurança podem reduzir complexidades, aprimorar os esforços de detecção e reduzir a carga sobre os profissionais do centro de operações de segurança (SOC — Security Operations Center). A adoção de serviços como a detecção e resposta gerenciadas (MDR) e o SOC-as-a-service (SOCaaS) também pode ajudar as equipes de segurança que estão sobrecarregadas a tirar o máximo proveito das tecnologias avançadas que implementaram.

Além da aquisição de tecnologia, preparar seu pessoal e criar processos eficazes é crucial. Você pode fazer isso sozinho ou aproveitar os serviços de prontidão e resposta a incidentes para ajudar a gerar planos novos ou testar planos existentes e identificar áreas para aprimoramento por meio de atividades como a realização de uma análise de lacunas, a execução de exercícios de mesa e o desenvolvimento de manuais e planos de resposta a incidentes.

Embora você e seus analistas sejam responsáveis por proteger sua organização, lembre-se de que todos os funcionários têm um papel a desempenhar na defesa contra os invasores. Os funcionários de uma empresa costumam ser a primeira linha de defesa ao impedir um ataque, tornando os programas contínuos de educação e treinamento em segurança cibernética uma parte crítica de sua estratégia de gerenciamento de riscos.

Os ataques de ransomware não vão diminuir tão cedo. No entanto, os líderes de segurança podem tomar várias ações para proteger melhor os dados e as redes de sua organização. Eles só precisam garantir que essas medidas estejam alinhadas com os riscos e as estratégias empregadas em ataques de ransomware. Adotar uma abordagem de plataforma consolidada para proteger sua empresa, incorporar ferramentas e automação orientadas por IA, testar (e testar novamente) planos e processos, monitorar proativamente vulnerabilidades externas e educar sua base de funcionários mais ampla sobre como detectar um possível ataque cibernético são passos essenciais a serem tomados hoje para diminuir as chances de você ser vítima de um ataque de ransomware amanhã.

[1] "FortiGuard Labs Reports Destructive Wiper Malware Increases Over 50%," Fortinet, 22 de fevereiro de 2023.

[2] "1H 2022 FortiGuard Labs Global Threat Landscape Report," Fortinet, 17 de agosto de 2022.

[3] "How We Can Help You: Common Scams and Crimes," FBI.gov.

maio 3, 2023 12:08 PM

2051666-0-0-PT