SOPHOS

Melhores práticas de proteção de endpoint para bloquear ransomware

Guia prático para configurar sua solução de endpoint para oferecer a proteção ideal.

Documento técnico Sophos. Outubro, 2024

Introdução

O ransomware está entre as ameaças cibernéticas mais intensas, com uma extensa projeção e consequências que chegam a ser catastróficas. Dos entrevistados na pesquisa O Estado do Ransomware 2024 da Sophos, 59% deles responderam que suas organizações foram atingidas por ransomware no ano anterior. Em 70% desses incidentes, os dados foram criptografados pelo invasor.

No geral, o custo médio para remediar um ataque de ransomware chegou aos exorbitantes US$ 2,73 milhões — um aumento de 50% em comparação ao ano anterior. Além disso, mais de um terço (34%) das organizações levou mais de um mês para se recuperar dos ataques, ressaltando a maior complexidade e severidade desses incidentes.

Os tempos de recuperação mais longos destacam a necessidade de dedicar mais esforços de resposta. Essa complexidade extenua consideravelmente as equipes de segurança internas, com 95% das organizações relatando dificuldades na efetivação de tarefas operacionais de segurança essenciais[1].

Essas revelações enfatizam a urgência das organizações reforçarem suas defesas contra ransomwares e estratégias de recuperação, já que os custos crescentes, tempos de recuperação prolongados e maior pressão nas equipes de segurança faz do ransomware uma ameaça descomunal para a continuidade dos negócios. Uma solução de proteção de endpoint bem configurada é uma das defesas mais eficazes contra ransomwares. Este documento técnico aprofunda-se no mecanismo de ataque do ransomware, nas estratégias para preveni-lo e nas melhores práticas para otimizar a sua proteção de endpoint e assegurar segurança máxima.

Como os ataques de ransomware são lançados

Existem muitos agentes de ameaças e muitos tipos de ataque de ransomware. Alguns são altamente direcionados, outros são mais oportunistas. É frequente ver adversários (chamados também de criminosos cibernéticos ou invasores) varrendo as redes em busca de pontos fracos ou vulnerabilidades que lhes darão acesso ao seu ambiente. Veja o texto a seguir de uma gangue de ransomware que atacou uma organização de educação canadense:

> *"Vocês têm uma antiga vulnerabilidade Log4j crítica que não foi corrigida no Horizon; foi assim que conseguimos fazer nossa primeira investida de acesso. Fizemos uma varredura em massa e vocês apareceram. Não foi intencional."*

Essa referência também destaca os caminhos comuns que os adversários seguem para explorar vulnerabilidades sem patches, que foi a causa primária mais utilizada nos ataques de ransomware em 2024.[2]

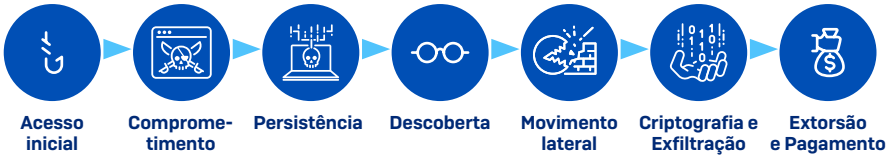
Grande parte do aumento em ataques de ransomware nos últimos anos pode ser atribuída ao crescimento do modelo RaaS de ransomware como serviço. Seguindo o modelo RaaS, um grupo de criminosos cibernéticos desenvolve um ransomware e o aluga a outros adversários. Essa abordagem enfraquece as barreiras de defesa, facilitando o acesso a ransomwares a mais agentes de ameaças novatos.

Uma vez que os adversários consigam atingir o ambiente de trabalho das vítimas, eles geralmente passam vários dias, semanas ou meses explorando a rede, escalando privilégios, exfiltrando dados e instalando malwares. Em 2023, o tempo médio de permanência em ataques de ransomware era de seis dias[3]. Isso dá à defesa uma janela para identificar e bloquear os invasores antes de um ataque.

1 A carência de qualificação em segurança virtual em PMEs — Sophos

2 O Estado do Ransomware 2024 – Sophos
3 Tudo muito quieto(?): Relatório Sophos de Adversários Ativos do 1S de 2024 – Sophos

Um ataque típico de ransomware apresenta uma estrutura semelhante a esta:



É importante ressaltar que os adversários são estratégicos na sua forma de ação, direcionando seus ataques às organizações em períodos menos propícios de serem detectados. Os ataques de ransomware normalmente ocorrem às sextas e sábados, na intenção de explorar a provável diminuição no monitoramento pela TI durante o fim de semana.

Análises feitas pela equipe de resposta a incidentes do Sophos X-Ops mostraram que 43% dos ataques de ransomware em 2023 foram realizados nesses dias, e 91% dos ataques começaram fora do horário de expediente normal (de segunda a sexta, das 8h às 18h) no fuso horário da vítima, aproveitando-se assim dos períodos em que a possibilidade de detecção e resposta era menor[4].

Ransomware remoto

O Relatório de Defesa Digital da Microsoft de 2023 declara que cerca de 60% dos ataques de ransomware operados por humanos envolvem a criptografia remota. Também conhecida como ransomware remoto, a criptografia remota ocorre quando um endpoint comprometido é usado para criptografar dados em outros dispositivos na mesma rede.

Um fator-chave que leva ao uso cada vez maior dessa abordagem é a sua escalabilidade: um endpoint não gerenciado ou mal protegido pode expor toda a sua organização à criptografia remota maliciosa, mesmo se outros dispositivos tiverem soluções de segurança avançada instaladas.

As organizações devem ficar extremamente atentas à ameaça de um ataque de ransomware remoto, porque nem todas as soluções de segurança de endpoint podem protegê-las contra esse tipo de ataque de modo eficaz.

Remote Desktop Protocol ou protocolo de implantação de ransomware?

Em 2023, o protocolo RDP (Remote Desktop Protocol) desempenhou seu papel em 90% dos ataques cibernéticos investigados pelo pessoal de resposta a incidentes da Sophos — um aumento em comparação aos 83% do ano anterior[5].

O RDP e as ferramentas de compartilhamento de desktop, como a VNC (Virtual Network Computing), são úteis no gerenciamento de sistemas remotos, mas, sem as defesas apropriadas, os agentes de ransomware as exploram para elevar privilégios, roubar credenciais, mover-se lateralmente, instalar backdoors, criar contas falsas e evadir-se da detecção.

É essencial impedir que os adversários usem o protocolo RDP para o acesso externo, acesso interno e movimentos laterais de exploração. Mesmo com o progresso das organizações em assegurar que o protocolo RDP não fique exposto externamente, os adversários o utilizam amplamente para mover-se lateralmente dentro de uma organização.

4 Detendo adversários ativos: Lições da linha de frente para a defesa cibernética – Sophos

5 Tudo muito quieto(?): Relatório Sophos de Adversários Ativos do 1S de 2024 – Sophos

As melhores práticas de TI para se proteger contra ransomware

Manter-se seguro contra ransomware e outras ameaças exige mais do que ter as mais modernas soluções de segurança. Boas práticas de segurança em TI, incluindo treinamento regular para os funcionários, são essenciais. Ainda que esta lista não abranja tudo, assegure-se de que estas práticas sejam seguidas.

1. Aplique patches cedo, e sempre

Você sabia?
Embora os ataques de ransomware sempre resultem em impactos negativos, os ataques que começam pela exploração de vulnerabilidades sem patches são especialmente cruéis. As organizações atingidas por ataques que começaram dessa forma relataram custos de recuperação quatro vezes mais altos e tempos de recuperação mais longos em comparação com os ataques que começaram com credenciais comprometidas.

A exploração de vulnerabilidades sem patches foi a principal causa primária dos ataques de ransomware em 2024[6]. Em geral, malwares e adversários exploram as vulnerabilidades de segurança em aplicativos populares. Quanto mais cedo você instalar patches em seus endpoints, servidores, dispositivos móveis e aplicativos, menos vulnerabilidades haverá para os adversários explorarem.[7]

2. Use senhas fortes

Pode soar banal, mas não é. Uma senha fraca e previsível pode dar aos hackers o acesso à sua rede em segundos. Recomendamos que as senhas sejam exclusivas e com, no mínimo, 12 caracteres, usando uma combinação de letras maiúsculas e minúsculas e incluindo um caractere especial: Bem.De5SEJe1to!

3. Habilite a autenticação multifator (MFA)

A autenticação MFA oferece uma camada extra de proteção após o primeiro fator, que é, em geral, uma senha. Habilitar a MFA em todos os aplicativos e serviços que aceitam essa autenticação é essencial. Os adversários geralmente adquirem credenciais válidas na dark web ou tentam obtê-las com afinco após entrarem no seu ambiente.

A MFA é um obstáculo adicional para parar um adversário e impedir que se autentique como um usuário válido sem ser interpelado. Para finalizar, sempre que os aplicativos permitirem, use passkeys que resistem ao phishing.

4. Regularize o acesso interno e externo à rede

Não deixe as portas da rede expostas. Bloqueie o acesso RDP na sua organização e outros protocolos de gerenciamento remoto. Garanta aos usuários remotos o uso de uma solução Zero-Trust Network Access (ZTNA) para acessar aplicativos, serviços e outros recursos empresariais.

5. Monitore os direitos de administrador

Examine constantemente os direitos de admin locais e no domínio. Saiba quem os têm e remova-os daqueles que não necessitam deles. Não fique conectado usando suas credenciais de administrador por mais tempo do que o necessário.

6. Faça backup regular dos dados em vários locais e pratique os procedimentos de restauração com frequência.

Em nossa pesquisa de 2024, O Estado do Ransomware, 68% dos gerentes de TI que tiveram seus dados criptografados conseguiram reavê-los através de backups. Faça o backup regular dos seus dados em vários locais, usando a MFA para proteger os backups na nuvem. Pratique a restauração de backups para garantir um processo coerente. Monitore a ocorrência de atividades suspeitas para proteger os backups de possíveis ameaças.

7. Remova aplicativos desnecessários

Os adversários usam aplicativos comuns instalados com propósitos maliciosos. Essa abordagem, chamada de "living-off-the-land", ou LOL, dificulta diferenciar o uso legítimo de uma atividade mal-intencionada. Se um usuário não precisa de um determinado aplicativo para desempenhar seu trabalho, reconsidere se ele deveria ser realmente instalado. No caso de dúvida, deixe o arquivo de lado.

8. Encontre dispositivos sem proteção na sua rede

Os adversários usam dispositivos sem proteção de endpoint para permanecerem ocultos no seu ambiente e não serem interpelados. Esses dispositivos sem proteção podem ser usados em ataques de ransomware remoto.

6 O Estado do Ransomware de 2024 – Sophos
7 Vulnerabilidades sem patches: o vetor de ataque de ransomware mais cruel – Sophos

Melhores práticas para a sua solução de proteção de endpoint

Um método eficiente de proteger-se contra ataques de ransomware é ter uma solução de proteção de endpoint, detecção e resposta de endpoint (EDR) ou detecção e resposta estendidas (XDR) que inclua tecnologias avançadas de prevenção e capacidade de caça a ameaças.

A configuração incorreta da ferramenta de segurança é considerada o maior risco à segurança cibernética das organizações[8]. Políticas com parâmetros mal configurados, exclusões e outros fatores podem comprometer a postura de segurança. Assegure que a sua proteção de endpoint esteja configurada corretamente para oferecer proteção máxima.

Portanto, recomendamos que você siga estas práticas para proteger seus dispositivos de endpoint contra ransomware:

1. Ative todas as políticas e recursos recomendados

Parece óbvio, mas essa é uma maneira infalível de obter a melhor proteção da sua solução de segurança de endpoint.

As políticas e configurações são criadas para bloquear ameaças específicas, e verificá-las regularmente para confirmar que todas as opções de proteção estão ativas garante a proteção de seus endpoints contra ransomwares correntes e inéditos. Confirme que os recursos de detecção de técnicas de ataque sem arquivo e as tecnologias de comportamento estejam habilitados. Recomendamos também que você:

A) Habilite a proteção contra adulterações

Isso previne a modificação ou remoção não autorizada do software de proteção de endpoint. Uma das primeiras ações que os adversários executam após acessarem um sistema é tentar desativar ou remover a proteção do endpoint.

B) Habilite o log forense (especialmente na nuvem)

Se você for comprometido, vai querer saber o que aconteceu, para que possa evitar a reincidência. Contudo, os adversários geralmente eliminam os logs do sistema para acobertar seus passos, removendo os indícios forenses que contribuiriam para entender o ataque. Você também poderá perder o acesso ao seu dispositivo. Ter um registro das atividades na nuvem garante que você mantenha o acesso a informações cruciais.

C) Confirme que as atualizações de produtos e conteúdo da proteção de endpoint estejam habilitadas

Para se manter em dia com a constante evolução no cenário de ameaças e proteger-se contra ameaças emergentes, é de vital importância que você atualize seus produtos de segurança regularmente com dados novos. Desabilitar as atualizações de produtos e conteúdo deteriorará a sua proteção pouco a pouco.

2. Revise regularmente suas exclusões

As exclusões previnem a varredura por malware de diretórios e tipos de arquivo confiáveis. Por vezes, elas são usadas para reduzir atrasos do sistema e minimizar o risco de alertas falsos positivos de segurança.

Com o tempo, uma lista crescente de exclusões cria lacunas na sua segurança e que os adversários podem tentar se aproveitar. O malware que conseguir se embrenhar nos diretórios excluídos — talvez movido acidentalmente por um usuário — pode ter êxito em suas peripécias.

Verifique a lista de exclusões regularmente nas configurações da sua política e remova o máximo de exclusões que puder. Aquelas que você não puder remover devem ser o mais específicas possível. Por exemplo, em lugar de excluir uma unidade de disco ou um diretório de banco de dados, exclua apenas os arquivos específicos usando o seu caminho completo. Isso evita que o malware transponha o seu sistema de segurança e seja executado na mesma pasta.

3. Ative a MFA no seu painel de segurança

Assim, você garante o acesso seguro à plataforma que gerencia sua proteção de endpoint e outros controles de segurança. Isso impede que os adversários alterem deliberadamente suas configurações ou desativem ou removam a proteção, o que pode deixar seus endpoints e servidores vulneráveis ao ataque.

4. Mantenha a boa higiene de TI e siga as práticas recomendadas

Avaliar sua higiene de TI regularmente assegura que seus endpoints e os softwares instalados sejam executados com eficiência máxima. Isso alivia os riscos à sua segurança cibernética e pode economizar tempo quando você remediar incidentes futuros.

Implementar um programa para manter a higiene de TI é crucial para salvaguardar-se contra ataques de ransomware e outras ameaças virtuais. Por exemplo: assegurar que o RDP seja executado apenas onde necessário e esperado; verificar regularmente questões de configuração; monitorar o desempenho do dispositivo, e remover programas indesejados e desnecessários. Uma verificação de higiene de TI poderá destacar a necessidade de atualizar softwares. É também uma forma infalível de assegurar que o backup dos seus dados seja feito regularmente.

8 A carência de qualificação em segurança virtual em PMEs — Sophos

5. Saia no encalço de adversários ativos no seu ambiente
No atual cenário de ameaças, os adversários estão cada vez mais astutos, implantando, com frequência, ferramentas legítimas e roubando credenciais para evitar serem detectados. A busca proativa por ameaças avançadas e adversários ativos é essencial para identificar e bloquear esses ataques "living-off-the-land". Uma vez encontrados, você precisa estar preparado para tomar as ações devidas para interrompê-los rapidamente.

Tecnologias como a detecção e resposta de endpoint (EDR) e a detecção e resposta estendidas (XDR) oferecem as funcionalidades de caça a ameaças, investigação e neutralização para a sua equipe interna de segurança. Contudo, como os adversários geralmente dão início a seus ataques fora do horário de expediente, talvez a sua equipe de segurança não esteja por perto para bloqueá-los. Muitas organizações têm dificuldades em manter uma defesa 24 horas contra ataques avançados de ransomware — por isso os serviços MDR de detecção e resposta gerenciadas são essenciais para várias organizações.

Tecnologias de segurança em camadas para proteger contra ransomware

O conhecido ditado "Melhor prevenir do que remediar" enfatiza o já dito: bloquear um problema no início é mais fácil do que corrigi-lo mais tarde. A proteção da sua organização contra ransomwares vai se beneficiar da abordagem de segurança de TI em camadas, com várias tecnologias trabalhando em conjunto para criar defesa e visibilidade. A começar pela proteção de endpoint, as organizações podem adicionar mais camadas conforme suas necessidades mudam, aprimorando a proteção e visibilidade com o passar do tempo.

Exemplos:

- **Um firewall** para identificar e bloquear o tráfego de rede suspeito e impedir que ameaças entrem no seu ambiente. Um firewall tem visibilidade do tráfego que entra e sai da rede da sua organização. Porém, ele não tem visibilidade do tráfego de rede dentro do seu ambiente.
- O produto **NDR de detecção e resposta de rede** pode detectar dispositivos sem proteção e identificar adversários movendo-se lateralmente na sua rede. O NDR oferece visibilidade ao tráfego de rede interno que o firewall não consegue ver.
- **Uma plataforma XDR** pode fornecer recursos de caça a ameaças, investigação e neutralização. Ela também pode integrar-se a outras soluções de segurança de TI, oferecendo visibilidade entre todos os controles de segurança a partir de uma mesma plataforma.
- **Um serviço MDR** oferece monitoramento e caça a ameaças 24 horas por dia, sete dias por semana, realizada por peritos especializados em detectar e responder a ataques cibernéticos que as soluções tecnológicas por si só não conseguem evitar. O seu serviço MDR deve oferecer resposta a incidentes de grande escala para interromper, conter e eliminar completamente um adversário sem custos adicionais. Um serviço MDR deve integrar-se às suas ferramentas de segurança cibernética existentes para proporcionar visibilidade completa de todo o seu ambiente. O MDR oferece o mais alto nível de proteção contra ataques avançados de ransomware coordenados por humanos.
- **Uma solução de gerenciamento da superfície externa de ataque (EASM) ou gerenciamento de vulnerabilidades (VM)** pode ser usada para identificar e priorizar vulnerabilidades. Isso permite que você identifique e aplique os patches que faltam antes que os adversários possam explorá-las.

A Sophos protege contra ransomware

O **Sophos Endpoint** adota uma abordagem de prevenção em primeiro lugar abrangente à segurança, bloqueando ameaças sem se basear em uma técnica só. Ele usa tecnologias sofisticadas que bloqueiam a mais ampla variedade de ataques, incluindo:

- **Proteção hermética contra ransomware** que protege contra ataques de ransomware locais e remotos, incluindo as novas variantes. Ela bloqueia a criptografia maliciosa em tempo real e reverte os arquivos afetados automaticamente para o seu estado original, minimizando o impacto nos negócios.
- A **tecnologia anti-exploit** protege contra ataques sem arquivo e explorações de dia zero ao bloquear as técnicas usadas pelos adversários em toda a cadeia de ataque.
- A **proteção adaptável contra ataques** é a primeira defesa dinâmica do setor que se adapta para responder a adversários ativos e ataques executados por humanos. Defesas reforçadas e habilitadas dinamicamente previnem que os adversários avancem suas ações ao minimizar a superfície de ataque e interromper o ataque.

O Sophos Endpoint é fácil de configurar e gerenciar. Instale o Sophos Endpoint e pronto! As tecnologias recomendadas de proteção são ativadas por padrão, para que você tenha as configurações de proteção mais reforçadas imediatamente em ação, sem necessidade de ajustes. O controle granular também está disponível se solicitado.

Você gerencia o Sophos Endpoint através do **Sophos Central,** a plataforma de segurança cibernética mais confiável do mundo. Essa poderosa plataforma de gerenciamento de segurança cibernética baseada na nuvem unifica todas as soluções de segurança Sophos Next-Gen e força o acesso por MFA.

Os clientes Sophos gerenciam a proteção de seus endpoints através do Sophos Central, beneficiando-se do recurso de verificação de integridade da conta. Ele identifica desvios da postura de segurança em políticas e exclusões e outras configurações incorretas de alto risco, permitindo que os administradores resolvam problemas com um clique.

Sophos XDR – ferramentas proativas de caça a ameaças e higiene de TI

O **Sophos XDR** é uma plataforma de detecção e resposta unificada desenvolvida com base no princípio da proteção em primeiro lugar do Sophos Endpoint. Ele permite detectar, investigar e responder rapidamente a ameaças multiestágio em todos os principais vetores de ataque.

Totalmente integradas à sua plataforma Sophos XDR, as tecnologias Sophos trabalham juntas para oferecer os melhores resultados de segurança possíveis. Além disso, aumente o retorno de investimento de seus produtos existentes de segurança cibernética usando integrações prontas para usar com um extenso ecossistema de soluções externas de endpoint, firewall, rede, e-mail, identidade, produtividade, segurança da nuvem, e backup e recuperação.

O Sophos XDR oferece ferramentas e funcionalidades projetadas para maximizar a eficiência dos analistas de segurança e administradores de TI.

- Detecções priorizadas por IA nas principais superfícies de ataque ajudam a identificar atividades suspeitas que exigem atenção imediata.
- Detecções e casos são automaticamente mapeados para as táticas MITRE ATT&CK, para você poder identificar facilmente as possíveis lacunas em suas defesas.
- Ações automatizadas, como encerramento de processo, reversão de ransomware e isolamento de rede, contêm as ameaças rapidamente, poupando um tempo valioso. As funcionalidades de IA generativa direcionadas a resultados capacitam analistas de segurança para neutralizar os adversários mais rapidamente, aumentando a eficiência dos analistas e a confiança nos negócios.

Sophos MDR – resposta e detecção gerenciadas 24/7

O **Sophos MDR** é um serviço de segurança gerenciada 24 horas executado por peritos altamente capacitados que trabalham por você, defendendo-o contra novas ameaças e adversários avançados ativos. O serviço Sophos MDR oferece proteção máxima contra ransomware.

Com o nível de atendimento Sophos MDR Complete, você se beneficia de resposta a incidentes completa e ilimitada, sem taxas extras. Nossos peritos podem executar um extenso conjunto de ações de resposta por você, remotamente, para interromper, conter e eliminar completamente um adversário.

Como o Sophos XDR, o Sophos MDR integra e coleta dados de telemetria de todos os produtos Sophos e os integra a uma extensa linha de produtos de segurança de terceiros para aumentar a visibilidade e proteção de todo o seu ambiente.

Serviço por Honorários do Sophos Incident Response – um serviço de resposta em standby

Ter uma equipe de resposta a incidentes a postos antes de os adversários atacarem é a única forma de economizar tempo, reduzir custos e mitigar o impacto de uma violação (por exemplo, quando um adversário lança um ransomware).

O **Serviço por Honorários do Sophos Incident Response** é uma assinatura anual a um time de elite com peritos em resposta a acidentes por demanda que se embrenham em seu ambiente de operação para conter, reter e eliminar adversários ativos com rapidez. Inclui também o planejamento e aplicação de recursos críticos contra incidentes para melhorar a postura de segurança da sua organização e diminuir a probabilidade de uma violação.

Observação: o Serviço por Honorários do Sophos Incident Response não é necessário se você tiver uma assinatura de nível de atendimento Sophos MDR Complete, que inclui resposta a incidentes de grande escala em seus serviços básicos.

Sophos Managed Risk — serviço de gerenciamento da superfície externa de ataque e vulnerabilidade

Vulnerabilidades sem patches são a principal causa primária de ataques de ransomware, tornando essencial identificar, investigar e priorizar as exposições de alto risco em todo o seu ambiente antes que se tornem um problema. O Sophos Managed Risk, alimentado pela tecnologia Tenable líder do setor, ajuda a fazer exatamente isso.

Com o **Sophos Managed Risk,** nossos analistas experientes identificam vulnerabilidades de segurança cibernética de alta prioridade e possíveis vetores de ataque em seu ambiente para que possam agir a fim de prevenir ataques antes que eles interrompam os seus negócios.

Conclusão

O ransomware continua evoluindo, mantendo grande pressão e força sobre as organizações vitimadas, o que incentiva a continuidade do pagamento de resgates. O seu objetivo é bloquear a entrada desses adversários na sua organização e detectá-los e ejetá-los rapidamente caso consigam ter acesso. Assegure-se de seguir as práticas recomendadas de TI e segurança de endpoint, continuar instruindo os usuários finais e permanecer atento a ameaças e adversários no seu ambiente. A abordagem em camadas e prevenção em primeiro lugar da segurança cibernética com detecção e resposta 24/7 dá à sua organização uma chance maior de proteger-se contra ransomwares e as últimas ameaças.

Para explorar as formas como a Sophos pode ajudar você a otimizar suas defesas contra ransomware, fale com um consultor ou acesse www.sophos.com

2024-10-01 (WP-NP)

SOPHOS