Configuração de estratégias, processos e tecnologia de endpoints para lidar com ransomware

Índice

Resumo executivo

O cenário de ameaças continua evoluindo com ataques mais sofisticados e técnicas evasivas. O ransomware é uma das formas mais assustadoras de crime cibernético que as organizações enfrentam atualmente, e não dá sinais de que vai desaparecer. O FortiGuard Labs relata que houve um aumento de sete vezes na atividade de ransomware em dezembro em comparação com julho de 2020.[1] Uma pesquisa global de ransomware também mostrou que 67% das organizações foram alvos de ransomware, com quase metade dizendo que foram alvos mais de uma vez.[2]

O ransomware pode obter acesso a um sistema de várias maneiras, geralmente com um simples clique ou até mesmo sem clique nenhum. E como o ransomware é tão predominante, as organizações precisam estar preparadas. Elas precisam ter estratégias para que estejam prontas antes, durante e depois de um ataque de ransomware. Muitas empresas desenvolvidas já têm planos de resposta a incidentes prontos para uso. Mas, para reduzir o risco e o escopo de possíveis incidentes, muitas coisas também devem ser feitas com antecedência para diminuir o risco de um incidente e para entender o que fazer quando no meio de um ataque.

A evolução contínua do Ransomware como Serviço (RaaS), a ênfase na “caça grande” (grandes resgates para grandes alvos) e a ameaça de divulgação de dados comprometidos se as demandas não fossem atendidas criaram um mercado com crescimento massivo que os cibercriminosos transformaram em algo altamente lucrativo.[3]

Introdução

Os ataques de ransomware estão aumentando e tendem a ser extremamente meticulosos. Os invasores estão levando algum tempo para fazer o reconhecimento a fim de atingir vítimas específicas e podem permanecer no ambiente por semanas a fio, mapeando e contornando os controles de segurança. Quanto mais tempo os invasores estiverem à espreita, mais danos eles podem causar. Desta vez, eles têm a oportunidade não apenas de descartar a carga útil do ransomware, mas também de descobrir maneiras de exfiltrar seus dados e, em seguida, manter essas informações como reféns. As organizações precisam de estratégias abrangentes de prevenção, detecção, resposta e remediação para que os sistemas críticos possam ser restaurados o mais rápido possível.

Estratégia pré-incidente

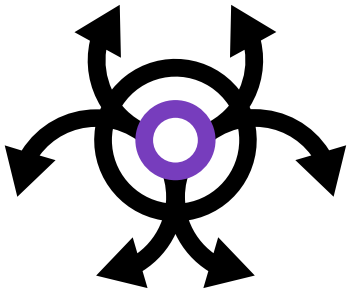
As organizações geralmente precisam fazer mudanças fundamentais na frequência, localização e segurança de seus backups de dados. Quando combinado com o comprometimento da cadeia de suprimentos digital e uma força de trabalho atuando à distância para a rede, existe um risco real de que os ataques possam vir de qualquer lugar. Soluções de segurança baseadas na nuvem, como serviço de acesso seguro de borda (SASE), para proteger dispositivos fora da rede; segurança de endpoints avançada, incluindo soluções de detecção e resposta de endpoint (EDR), que podem interromper o ataque de malware; e acesso Zero Trust e estratégias de segmentação de rede que restringem o acesso a aplicações e recursos com base na política e no contexto, devem ser consideradas para minimizar o risco e reduzir o impacto de um ataque de ransomware bem-sucedido. Por fim, o elemento humano continua tão importante quanto a tecnologia. É importante fornecer aos funcionários atualizações contínuas sobre novas metodologias de ataque de engenharia social para que eles saibam o que devem e o que não devem fazer.

Dito isso, como os endpoints são o destino final do ransomware, você precisa se concentrar na segurança de endpoints sólida. Este processo começa com a redução da superfície de ataque de cada endpoint ao fechar portas e periféricos desnecessários, controlar as aplicações instaladas no sistema, proteger vulnerabilidades de exploração e manter essa configuração segura. A partir daí, é fundamental usar uma análise estática robusta que combine threat intelligence com aprendizado de máquina. A análise deve ser realizada em todo o código que está sendo adicionado aos dispositivos e complementada pela inspeção baseada em comportamento dinâmico de todas as atividades de tempo de execução para detectar ameaças. É essencial ter a capacidade de agir em tempo real e conter ataques em andamento sem esperar a triagem manual de alerta e a resposta.

Estratégia de monitoramento contínuo

Um relatório recente da Aberdeen estabeleceu uma linha de base da eficácia de segurança da proteção de endpoint baseada em assinatura tradicional em 92,5% (deixando 7,5% de risco de comprometimento). O relatório também estabeleceu o valor incremental da redução da superfície de ataque em 3,5%, levando a eficácia para 97%. Ele calculou que a segurança de endpoints baseada em comportamento pode realmente aumentar a eficácia para 99,6% (ou apenas 0,4% de exposição ao risco).[4]

Para todas as medidas de prevenção, é importante que as organizações com um centro de operações de segurança (Security Operations Center — SOC) com cobertura 8 horas por dia, 5 dias por semana ou 24 horas por dia, 7 dias por semana, tenham um acordo de serviço com seu fornecedor de segurança de endpoints ou parceiro de serviços de segurança gerenciados para cobertura após o expediente e suporte de escalonamento. Esses serviços se concentram no monitoramento de alertas e ameaças suspeitas, fornecendo orientação e as próximas etapas aos responsáveis pela resposta a incidentes, o que pode incluir a busca proativa de ameaças, abrangendo a busca por Indicadores de compromisso (Indicators of Compromise — IOCs), identificação de possíveis programas vulneráveis e não autorizados, e recuperação e análise de artefatos forenses. Depois que o evento é analisado, uma notificação de incidente explica a ameaça e as recomendações para as etapas de revisão e/ou remediação.



O ransomware está envolvido em 27% dos incidentes de segurança de malware.[5]

Estratégia de resposta

Quando um incidente de segurança é descoberto, é imperativo responder de imediato para minimizar danos potenciais, mesmo com contenção no local. Habilidades especializadas, ferramentas e processos repetíveis são necessários para a mitigação de ameaças eficaz. Eles podem ser usados para avaliar a situação e determinar como conter a ameaça e recuperar as operações.

Mesmo com as ferramentas e processos de pessoal implantados, a preparação e a prática adicionais continuam sendo essenciais para suavizar as ações de resposta em meio a um incidente cibernético emergente. Essas atividades incluem:

- Avaliação da prontidão de resposta a incidentes para avaliar a postura de segurança atual de uma organização por meio da revisão da arquitetura de rede, controles de segurança e funções e responsabilidades da equipe. O objetivo é identificar tecnologia, pessoas e processos
- Revisão do manual de resposta a incidentes para determinar a suficiência e áreas para melhoria do processo passo a passo no caso de um grande incidente de segurança cibernética, como um ataque de ransomware
- Exercícios de simulação de resposta a incidentes para simular tipos de incidentes e testar o plano de resposta a incidentes e execução reais da organização, com o objetivo de praticar e melhorar os processos de resposta

Resumo

Quando uma organização está no meio de um ataque de ransomware, é tarde demais para implementar as estratégias, processos e tecnologia para impedir o dano. O planejamento e a preparação antes que ocorra um ataque são essenciais. Para ajudar as equipes de segurança a mitigar os danos das ameaças e minimizar o tempo de resposta, as organizações devem investir em soluções que cubram todos os estágios de redução da superfície de ataque, prevenção e detecção de ameaças, contenção e resposta.

[1] "Global Threat Landscape Report: A Semiannual Report", FortiGuard Labs, fevereiro de 2021.

[2] "The 2021 Ransomware Survey Report", Fortinet, 3 de novembro de 2021.

[3] "Global Threat Landscape Report: A Semiannual Report", FortiGuard Labs, fevereiro de 2021.

[4] "Quantifying the Risk Reduction of Evolving Endpoint Security Technologies", Aberdeen Strategy and Research, julho de 2021.

[5] "2020 Data Breach Investigations Report," Verizon, 2020.

FORTINET®

www.fortinet.com

dezembro 17, 2021 11:48 AM

983114-A-0-PT