elastic security labs

2024

Relatório Global de Ameaças da Elastic

Tendências de ameaças SOC o que os líderes precisam saber

Criado para oferecer insights acionáveis para equipes de segurança e CISOs, o Relatório Global de Ameaças da Elastic 2024 apresenta as principais descobertas de meses de análise em mais de 1 bilhão de pontos de dados, cortesia da telemetria pública e específica da Elastic. Essas conclusões foram organizadas em insights dos dados e ações sugeridas para a sua organização.

Principais insights

01 Ambientes de nuvem estão sendo mal configurados pelas empresas

Nossa nova seção sobre gerenciamento de postura de segurança na nuvem (CSPM) comparou ambientes com os benchmarks do Center for Internet Security (CIS) e descobriu que, em média, cerca de 50% dos ambientes falharam nas verificações, independentemente do provedor de serviços de nuvem (CSP).

02 A evasão de defesas continua sendo a tática de endpoint mais vista

A Evasão de Defesas foi responsável por 38% dos comportamentos dos endpoints, sugerindo que os adversários se sentem à vontade para navegar pelos sistemas de segurança. Esse número diminuiu 6% em relação ao ano passado, destacando que as ferramentas de defesa estão funcionando de forma eficaz.

03 Os alertas de acesso a credenciais continuam a aumentar, principalmente na nuvem

Em ambientes de nuvem, o acesso às credenciais foi responsável por 23% da atividade. Além disso, os ambientes de endpoint revelaram um aumento de 3% nessas técnicas ano após ano. Isso pode ser atribuído à crescente prevalência de ladrões de informações e brokers de credenciais, bem como ao fato de que as ferramentas de segurança têm crescido em visibilidade.

04 Os adversários estão abusando das ferramentas de defesa para entrar nos sistemas com eficiência

Cerca de 53% dos arquivos maliciosos observados foram identificados como ferramentas de segurança ofensivas, usadas pelas empresas para descobrir pontos fracos e pontos que podem ser abusados por adversários. Essas ferramentas de segurança ofensiva (OSTs) têm grandes equipes de pesquisa e desenvolvimento para criar novos recursos, como Injeção de Processo — uma forma de evasão de defesa que foi responsável por 53% dos eventos de alerta do Windows neste ano.

05 A IA generativa não aumentou a quantidade ou o impacto dos ataques que observamos

As equipes de segurança estão preocupadas com um ataque iminente de GenAI. Embora tenhamos visto um pequeno aumento no volume de ameaças, a GenAI reforçou amplamente as tecnologias de defesa com recursos como resumo de alertas e automação de tarefas.

 |

Principais sugestões

01 Audite seu ambiente com frequência

Os adversários confiam em controles de segurança permissivos ou mal configurados para se infiltrar nos ambientes e, depois de conseguirem invadir, se concentram em adulterar sensores e dados. Avaliações comparativas e de risco podem ajudar a identificar se você está utilizando as práticas recomendadas e os padrões do setor para controlar efetivamente o acesso em sua empresa.

02 Prepare-se para a IA generativa ajustando seus controles de segurança

O aumento da GenAI resultará em um aumento nas tentativas de engenharia social. Embora seja sempre uma boa ideia treinar sua base de usuários para identificar essas e outras tentativas, as equipes de segurança também devem verificar os controles e permissões para garantir que uma tentativa bem-sucedida de phishing não cause danos perenes.

03 Implemente agentes de endpoint interativos para neutralizar ataques de evasão de defesa

Ataques de Evasão de Defesa têm sido a principal tática usada por alguns anos. Embora esteja diminuindo, os adversários ainda estão utilizando esses métodos para se infiltrar e navegar nos ambientes. Tecnologias de endpoint como Elastic Agent oferecem visibilidade e capacidade, ao mesmo tempo em que reduzem a quantidade de ferramentas necessárias.

04 Crie um plano de resposta robusto para credenciais expostas

Observamos que técnicas como força bruta e acesso às credenciais do navegador a partir de memória suspeita são utilizadas de forma regular. A rotação de credenciais expostas e a organização de fluxos de trabalho rápidos para resposta a violações farão uma grande diferença. As equipes de segurança devem exigir a autenticação multifator.

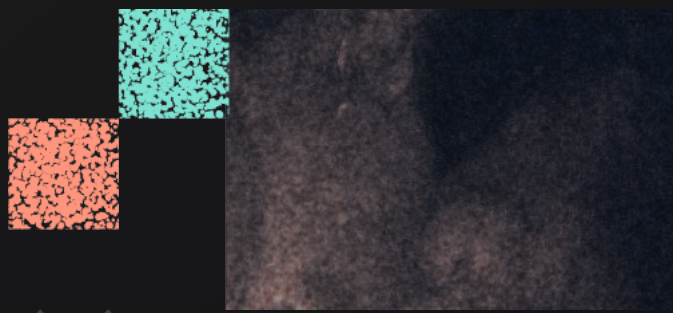
05 Compare seu ambiente de nuvem com os benchmarks do CIS

Os benchmarks CIS são um padrão do setor e ajudarão a identificar de forma rápida quais áreas precisam de atenção. Sua equipe deve desenvolver um plano para monitorar e aumentar a pontuação, o que melhorará a detecção de ameaças e reduzirá o risco a longo prazo.

Domine o cenário das ameaças

Prepare-se para a evolução dessas ameaças e muito mais. Receba todas as nossas sugestões e veja a análise completa do cenário de ameaças atual no Relatório Global de Ameaças da Elastic de 2024. Você também pode seguir nossos especialistas em @ElasticSecLabs.

Veja como o Elastic Security pode modernizar suas operações de segurança.



 |

elastic security labs