Explicações em vídeo

Artigos explicativos originais extraídos da biblioteca de vídeos da Cyber Crucible — ransomware, roubo de dados, roubo de identidade, segurança autônoma e FortressAI — cada um com o respetivo vídeo.

- As empresas estão exagerando em relação ao risco de IA, ou é um problema de visibilidade?
- Por que os modelos tradicionais de SOC têm dificuldade contra ciberataques em velocidade de máquina?
- Como é, no dia a dia, uma cibersegurança verdadeiramente autônoma?
- As ferramentas de IA, como o ChatGPT, podem substituir uma equipe humana de cibersegurança?
- O ransomware ainda consegue atingir dados armazenados em serviços de nuvem como OneDrive ou Google Drive?
- Se o ransomware se autoapaga, isso significa que o ataque terminou?
- A segurança cibernética deve focar-se na resiliência ou na prevenção de ataques antes que ocorram?
- Como a Cyber Crucible me ajuda a gerenciar fornecedores e resultados de cibersegurança?
- Como a Cyber Crucible me ajuda a controlar os gastos com segurança cibernética e os contratos com fornecedores?
- A Cyber Crucible funciona em conjunto com outras ferramentas de cibersegurança e EDR?
- Por que a IA é um risco de negócio, e não apenas uma ferramenta de produtividade, para os executivos da empresa?
- Os funcionários já estão usando ferramentas de IA antes de a nossa empresa ter uma política oficial de IA?
- Quais são os sinais de alerta de que um ataque de ransomware está acontecendo?
- O que realmente acontece nos momentos durante um ataque de ransomware?
- O que realmente acontece quando o ransomware atinge um servidor de empresa?
- Por que o ransomware ataca arquivos compartilhados antes de atingir meu desktop?
- O que inspirou o fundador a criar a Cyber Crucible?

- De onde realmente vêm os ataques de ransomware?
- Quem os atacantes de ransomware realmente visam hoje?
- Quem Corre Maior Risco de um Ataque de Ransomware e Por Que São Alvos?
- Quem Realmente Executa os Ataques de Ransomware e Como Eles Operam?
- Quem é o cliente ideal para a proteção contra ransomware da Cyber Crucible?
- Por que os ataques de ransomware estão se tornando mais comuns a cada ano?
- Por que a Cyber Crucible utiliza IA em vez de uma equipe humana de SOC para conter ransomware?
- Por que as equipas de segurança recebem milhares de alertas por dia e como podem lidar com isso?
- Por que o roubo de credenciais e de identidade é mais perigoso do que a criptografia de ransomware?
- Por que o ransomware se tornou tão difícil de impedir e de recuperar?
- Por que o antivírus tradicional não consegue impedir ataques de ransomware zero-day e sem arquivo (fileless)?
- Os hackers usarão mais IA em ataques de ransomware em 2025?
- O uso da Cyber Crucible reduz o orçamento geral de segurança de uma empresa?

As empresas estão exagerando em relação ao risco de IA, ou é um problema de visibilidade?

Resposta curta: A maioria das organizações não está exagerando em relação ao risco de IA — elas simplesmente não têm visibilidade real sobre como as ferramentas de IA estão sendo efetivamente utilizadas em seu ambiente. Sem essa visibilidade, a suposição mais segura é a de que o risco atual está sendo subestimado, e não exagerado.

Saiba mais: impeça que os dados sensíveis cheguem ao ChatGPT e a outras ferramentas de IA (FortressAI)

Por que o "risco de IA" costuma se resumir a pontos cegos

Quando as empresas avaliam sua exposição ao risco relacionado à IA, um padrão comum se destaca: algumas organizações admitem abertamente que não têm uma visão clara de como as ferramentas de IA estão sendo usadas internamente. Outras acreditam ter essa visibilidade, apenas para descobrir o contrário assim que o monitoramento é efetivamente implementado. Na prática, uma vez que o rastreamento é ativado, o volume e a variedade de uso de ferramentas de IA que aparecem costumam ser surpreendentes, a ponto de os recursos de visibilidade, às vezes, precisarem ser executados em modo controlado ou simulado apenas para acompanhar a quantidade de atividade que surge quase imediatamente.

Essa lacuna sugere que as preocupações com o risco de IA raramente são exageradas. Na maioria das vezes, a preocupação é subestimada, porque os líderes estão trabalhando sem os dados necessários para avaliar a situação com precisão.

Por que o risco desconhecido deve ser tratado como alto risco

Uma forma útil de pensar sobre isso é semelhante às finanças pessoais: se você nunca verifica o saldo da sua conta bancária, a suposição responsável é a de que você não tem fundos significativos disponíveis, e não o contrário. A mesma lógica se aplica ao uso de IA dentro de uma empresa. Sem variáveis concretas, como quais ferramentas estão em uso, com que frequência e por quem, as organizações não têm base confiável para presumir que o risco é baixo. O padrão responsável é assumir a pior exposição possível até que os dados reais de uso comprovem o contrário.

O padrão mais amplo por trás da adoção de IA

Entre usuários, unidades de negócio e as próprias ferramentas de IA, novos casos de uso — frequentemente não sancionados — continuam surgindo mais rápido do que a governança consegue acompanhar. Esse padrão consistente indica que a maioria das organizações, independentemente do porte ou do setor, ainda está se atualizando sobre como a IA está realmente sendo usada em seu ambiente. Estabelecer uma visibilidade clara é o primeiro passo necessário antes que o risco de IA possa ser avaliado ou gerenciado com precisão.

https://player.vimeo.com/video/1176539821?texttrack=pt

Assistir no Vimeo · Legendas: English, Français, Español, العربية

Por que os modelos tradicionais de SOC têm dificuldade contra ciberataques em velocidade de máquina?

Resposta curta: Os centros de operações de segurança tradicionais foram projetados para uma era de hacking mais lenta e previsível, dependendo de assinaturas e de análise humana para detectar ameaças após o fato. Os atacantes de hoje utilizam ferramentas automatizadas que sofrem mutação constantemente, portanto as defesas precisam migrar para abordagens preventivas e sem assinaturas, que operem mais rápido do que o próprio ataque.

Saiba mais: prevenção de ransomware e de roubo de credenciais ao nível do kernel (Cyber Crucible Core)

Como o cenário de ameaças mudou

Anos atrás, as ferramentas maliciosas se comportavam de maneiras bastante consistentes e identificáveis. As equipes de segurança conseguiam criar métodos de detecção com base em padrões conhecidos, pois os atacantes ainda não dependiam fortemente da automação para alterar constantemente suas técnicas. Essa abordagem funcionava bem o suficiente para capturar algumas das ameaças mais sofisticadas daquela época, incluindo ataques altamente direcionados descobertos há mais de uma década.

Esse cenário não existe mais. Os atacantes modernos utilizam automação para gerar variações rápidas de suas ferramentas, dificultando que a detecção baseada em assinaturas consiga acompanhar o ritmo. Quando uma nova assinatura é identificada, catalogada e implantada em toda a pilha de segurança, o atacante muitas vezes já avançou para uma nova variante.

Por que os modelos legados de SOC ficam para trás

Os fluxos de trabalho tradicionais de SOC dependem da identificação de indicadores conhecidos, seguida de investigação e resposta por meio de processos majoritariamente manuais ou semiautomatizados. Esse modelo pressupõe que os atacantes se movem em um ritmo que dá tempo aos defensores para analisar e reagir. Quando os ataques são automatizados e podem sofrer mutação em tempo real, essa premissa deixa de se sustentar, deixando uma lacuna persistente entre o surgimento de uma ameaça e o momento em que ela é tratada.

O que as defesas modernas precisam fazer em vez disso

As ferramentas de segurança agora precisam operar sem depender exclusivamente de assinaturas previamente conhecidas. Em vez disso, precisam detectar e prevenir comportamentos maliciosos diretamente, agindo em velocidade de máquina em vez de esperar por ciclos de análise conduzidos por humanos. A tecnologia FortressAI da Cyber Crucible foi construída com base nesse princípio, com foco em interromper tentativas de ransomware, roubo de dados e roubo de identidade por meio de ação preventiva e automatizada, em vez de correspondência de assinaturas após o fato.

https://player.vimeo.com/video/1182235055?texttrack=pt

Assista no Vimeo · Legendas: English, Français, Español, العربية

Como é, no dia a dia, uma cibersegurança verdadeiramente autônoma?

Resposta curta: A segurança autônoma genuína deve parecer rotineira e de baixo esforço, e não uma fonte constante de alertas ou ansiedade. Se uma ferramenta de segurança exige atenção contínua, ajustes ou preocupação, ela não está funcionando de forma autônoma.

Por que "monótono" é o objetivo

As equipes de segurança e o pessoal de TI já lidam com mais tarefas do que conseguem realisticamente concluir. Adicionar uma ferramenta que exige verificações regulares, revisão manual de alertas ou resolução de problemas de madrugada anula o propósito da automação. Uma proteção autônoma eficaz deve operar silenciosamente em segundo plano, muito como um extintor de incêndio montado na parede. A maioria das pessoas não pensa no seu extintor de incêndio até que um inspetor apareça uma vez por ano para confirmar que ele está carregado e pronto. No restante do tempo, ele simplesmente permanece ali, cumprindo sua função sem exigir atenção.

Esse é o padrão que a segurança autônoma deve atender. Ela deve lidar com ameaças por conta própria, sem afastar a equipe de outras prioridades ou se tornar mais um item em uma lista de tarefas já longa.

O que isso significa na prática

Se um produto de segurança faz você verificar painéis constantemente, questionar se ele detectou algo ou perder o sono se perguntando se está realmente funcionando, ele não é verdadeiramente autônomo — é apenas mais uma tarefa manual com outro rótulo. O FortressAI, da Cyber Crucible, foi construído com base nessa ideia: detectar e interromper atividades de ransomware, roubo de dados e roubo de identidade sem precisar de supervisão humana constante para funcionar corretamente.

A medida de sucesso não é a quantidade de atividade que uma ferramenta de segurança gera ou a frequência com que precisa de ajustes. É o quão pouco ela precisa ser lembrada. Quando a segurança autônoma funciona como deveria, ela deve ser discreta — presente, confiável e praticamente invisível até o momento em que for necessária.

https://player.vimeo.com/video/1190816235?texttrack=pt

Assista no Vimeo · Legendas: English, Français, Español, العربية

As ferramentas de IA, como o ChatGPT, podem substituir uma equipe humana de cibersegurança?

Resposta curta: Não. Ferramentas de IA de uso geral podem apoiar o trabalho de segurança ao resumir informações ou responder a perguntas básicas, mas não são suficientemente confiáveis para substituir uma equipe de segurança treinada quando decisões reais de risco estão em jogo.

Saiba mais: impeça que os dados sensíveis cheguem ao ChatGPT e a outras ferramentas de IA (FortressAI)

Por que a confiança da IA pode ser enganosa

Ferramentas como o ChatGPT costumam apresentar respostas com um tom de certeza, mesmo quando as informações subjacentes estão incompletas ou incorretas. Isso pode criar uma falsa sensação de autoridade, semelhante a uma pessoa persuasiva que afirma algo com tanta confiança que os outros aceitam como fato sem verificar mais a fundo. Na conversa cotidiana, esse tipo de confiança equivocada é um problema menor. Na cibersegurança, onde as decisões afetam a forma como uma organização identifica e responde a ameaças, aceitar resultados imprecisos sem questionamento pode causar danos reais. A análise de segurança depende de contexto, verificação e julgamento que os modelos de IA de uso geral atuais não estão totalmente equipados para reproduzir.

Onde a IA ainda pode ajudar

Apesar dessas limitações, as ferramentas de IA não deixam de ter valor em um contexto de segurança. Elas podem servir como ponto de partida para pesquisas, ajudar a explicar conceitos ou auxiliar na redação e organização de informações. Usada dessa forma, a IA funciona como uma ferramenta de apoio, e não como uma tomadora de decisões. O ponto-chave é reconhecer a diferença entre a IA auxiliando um analista experiente e a IA tentando avaliar e mitigar riscos de

forma independente, o que exige uma expertise mais profunda do que essas ferramentas oferecem atualmente.

O caso a favor de expectativas honestas

Fornecedores e profissionais de IA que estabelecem expectativas realistas, em vez de exagerar o que essas ferramentas podem fazer, têm mais chances de construir uma confiança duradoura. Superestimar as capacidades da IA em segurança corre o risco de corroer a confiança assim que as limitações se tornarem evidentes. Uma comunicação clara e ponderada sobre o que a IA pode e não pode fazer ajuda as organizações a tomar decisões informadas sobre como incorporá-la de forma responsável. A abordagem da Cyber Crucible reflete esse mesmo princípio: em vez de posicionar a IA como substituta de defensores qualificados, tecnologias de proteção autônoma como a FortressAI são projetadas para atuar em conjunto com a expertise humana, fortalecendo a capacidade de uma organização de prevenir ransomware, roubo de dados e roubo de identidade, sem fingir eliminar a necessidade de supervisão informada.

https://player.vimeo.com/video/1134578207?texttrack=pt

Assistir no Vimeo · Legendas: English, Français, Español, العربية

O ransomware ainda consegue atingir dados armazenados em serviços de nuvem como OneDrive ou Google Drive?

Resposta curta: Sim. Embora o armazenamento em nuvem já tenha estado fora do alcance do ransomware, os atacantes adaptaram os seus métodos e agora conseguem visar dados armazenados na nuvem através de técnicas como o mapeamento de unidades e, mais comummente hoje em dia, o roubo de chaves de API e tokens de sessão.

Saiba mais: prevenção de ransomware e de roubo de credenciais ao nível do kernel (Cyber Crucible Core)

Como a abordagem do ransomware aos dados na nuvem mudou

Quando o trabalho remoto impulsionou uma rápida mudança para o armazenamento em nuvem, tanto as empresas como os cibercriminosos estavam a adaptar-se simultaneamente ao novo ambiente. Nas fases iniciais desta mudança, o ransomware normalmente não conseguia tocar em ficheiros armazenados em plataformas na nuvem — se os dados estivessem na nuvem em vez de num servidor local, os atacantes geralmente deixavam-nos em paz, pois não tinham um caminho direto até eles.

Isso mudou à medida que os atacantes aprenderam a ligar manualmente o armazenamento na nuvem, como uma conta da Amazon, OneDrive ou Google Drive, a um sistema infetado. Fizeram isto ao montar o armazenamento na nuvem como uma letra de unidade local, de forma semelhante a como um dispositivo USB aparece como a sua própria unidade num computador. Uma vez montados desta forma, os ficheiros baseados na nuvem tornavam-se tão expostos à encriptação quanto os ficheiros num disco rígido local.

A maior ameaça de hoje: chaves e tokens roubados

À medida que a utilização da nuvem amadureceu, as táticas dos atacantes voltaram a mudar. Em vez de montar unidades manualmente, muitos vão agora atrás de chaves de API e tokens de sessão — credenciais que concedem acesso direto, a nível de programa, a contas e dados na nuvem. Obter uma destas é comparável a roubar uma palavra-passe, exceto que frequentemente proporciona um acesso mais amplo e rápido aos recursos na nuvem do que apenas uma palavra-passe roubada.

Esta mudança é importante porque a mesma velocidade e escalabilidade que tornam a computação em nuvem valiosa para equipas de TI legítimas estão agora também disponíveis para os atacantes. Entre os clientes da Cyber Crucible no último ano, mais de metade sofreu uma tentativa de roubo de um token de sessão na nuvem com o objetivo de sequestrar a sessão ativa de um utilizador, enquanto menos de 9% sofreram algum comprometimento real de dados. Isto sugere que os atacantes estão a priorizar o roubo de credenciais e tokens como o seu principal ponto de entrada, sendo o roubo de dados um objetivo secundário.

Os dados na nuvem estão automaticamente seguros?

O armazenamento na nuvem não garante proteção contra ransomware ou roubo de dados. Simplesmente altera o método que os atacantes têm de usar para chegar a esses dados — deslocando o risco principal para o comprometimento de credenciais e tokens de sessão em vez da encriptação direta de ficheiros.

https://player.vimeo.com/video/1047006345?texttrack=pt

Ver no Vimeo · Legendas: Inglês, Francês, Espanhol, Árabe

Se o ransomware se autoapaga, isso significa que o ataque terminou?

Resposta curta: Não. O ransomware moderno é frequentemente projetado para se apagar assim que termina de criptografar os arquivos, mas essa autoexclusão não tem nenhuma relação com a real segurança dos seus sistemas ou dados—ela apenas remove evidências da ferramenta que causou o dano.

Por Que o Ransomware "Desaparecer" Não Significa Recuperação

Os atacantes de hoje raramente dependem de um único malware para toda a intrusão. Em vez disso, costumam utilizar uma sequência de ferramentas separadas: uma para coletar credenciais, outra para localizar e exfiltrar dados valiosos, e uma final para criptografar arquivos e obter o máximo de vantagem. Assim que essa última ferramenta de criptografia conclui sua tarefa, ela comumente se apaga do sistema. O que resta são notas de resgate com instruções de contato e, mais importante, arquivos que permanecem bloqueados. A ausência do malware em si não é um sinal de resolução—significa apenas que o trabalho do atacante foi concluído do ponto de vista dele.

O Que Realmente Acontece com Seus Dados

No momento em que a criptografia ocorre, qualquer roubo de dados geralmente já aconteceu, e essas informações estão perdidas independentemente do que acontecer a seguir. Os arquivos criptografados que restam podem, em alguns casos, ser resolvidos por meio de negociação com o atacante ou por meio de ferramentas de descriptografia, mas não há garantia de sucesso. Técnicas que antes permitiam a descriptografia automatizada sem pagar aos atacantes tornaram-se muito menos eficazes à medida que os operadores de ransomware adaptaram seus métodos. Não existe uma ação simples de recuperação, como reiniciar um dispositivo, que reverta a criptografia.

A Escolha Real Após um Ataque

Depois que o ransomware segue seu curso e se autoapaga, as organizações geralmente ficam com dois caminhos: reconstruir os sistemas e dados afetados a partir de backups limpos, ou tentar a descriptografia por meio de pagamento e negociação com o atacante. Nenhuma das opções é rápida ou garantida, razão pela qual a prevenção—impedir o ransomware antes que a criptografia e o roubo de dados ocorram—continua sendo muito mais eficaz do que tentar reagir depois do fato.

https://player.vimeo.com/video/1043482941?texttrack=pt

Assista no Vimeo · Legendas: English, Français, Español, العربية

A segurança cibernética deve focar-se na resiliência ou na prevenção de ataques antes que ocorram?

Resposta rápida: A resiliência—recuperar-se após um ataque—é importante, mas o objetivo mais relevante é prevenir ransomware, roubo de dados e roubo de identidade antes que o dano ocorra, uma vez que os ataques automatizados são incessantes e cada vez mais bem informados sobre o momento certo para atacar.

Dois Significados de "Resiliência"

O termo "resiliência" em segurança cibernética tem-se desviado para duas ideias diferentes. Uma é se as próprias ferramentas de segurança conseguem continuar a funcionar sob ataque—essencialmente, se o software destinado a proteger consegue sobreviver a ser diretamente alvo ou adulterado, de forma semelhante a perguntar se uma câmara de segurança consegue continuar a gravar depois de alguém tentar desativá-la. O outro significado, mais tradicional, é se a empresa consegue recuperar e retomar a normalidade depois de uma violação já ter ocorrido.

Ambos são importantes, mas nenhum deles deve ser a estratégia principal. Os ataques modernos são automatizados e constantes. A principal razão pela qual as organizações não são atacadas continuamente é que os atacantes se tornaram hábeis em interpretar sinais sobre quais são os alvos que valem o seu tempo—por exemplo, evitando empresas que claramente não têm os recursos financeiros que tornem um ataque rentável. Este nível de segmentação automatizada significa que a resiliência, por si só, é uma postura reativa contra um adversário que está sempre a sondar.

Por Que a Prevenção Deve Vir Primeiro

Ser resiliente após uma violação é comparável a ter uma boa oficina de reparação de automóveis já identificada depois de um acidente de carro. É útil, mas é muito melhor evitar completamente o acidente. Ninguém quer testar o quão bem funciona o processo de reparação se puder, em vez disso, evitar a colisão em primeiro lugar.

Aplicado à segurança empresarial, isto significa que a prioridade deve ser impedir os ataques antes que sejam bem-sucedidos—o equivalente a ter travões fiáveis em vez de apenas um bom plano de reparação para depois de um acidente. A Cyber Crucible trabalha nesse sentido, concentrando-se na prevenção autónoma, com o objetivo de deter tentativas de ransomware, roubo de dados e roubo de identidade antes que possam causar danos, em vez de depender apenas da recuperação e da limpeza após o facto.

https://player.vimeo.com/video/1194994916?texttrack=pt

Ver no Vimeo · Legendas: English, Français, Español, العربية

Como a Cyber Crucible me ajuda a gerenciar fornecedores e resultados de cibersegurança?

Resposta curta: A Cyber Crucible cuida da prevenção automatizada no endpoint, o que libera você para selecionar e responsabilizar seu próprio provedor de monitoramento ou resposta — em vez de ficar preso a um serviço empacotado e difícil de avaliar, vinculado a um único fornecedor de EDR ou XDR.

O Problema Oculto dos Serviços de Segurança Empacotados

Muitas organizações pagam quantias significativas por um centro de operações de segurança hospedado que vem vinculado a um produto específico de detecção de endpoint ou de detecção e resposta estendida. O problema é que esse arranjo frequentemente deixa o cliente com pouca visibilidade sobre quão atento ou eficaz esse serviço de monitoramento realmente é. Você pode não saber o quão de perto seu ambiente está sendo observado, com que rapidez os problemas são escalados, ou se sua conta é prioritária para esse provedor. Como o monitoramento está atrelado à tecnologia subjacente, há pouco espaço para negociar, medir ou substituir o serviço caso ele não atenda às expectativas.

Separar a Prevenção do Monitoramento Restaura o Controle

A Cyber Crucible foca na camada de prevenção da proteção de endpoint, interrompendo automaticamente tentativas de ransomware, roubo de dados e roubo de identidade. Como a prevenção é tratada de forma independente, as organizações deixam de ser obrigadas a adquirir um único pacote combinado de detecção e resposta. Em vez disso, você ganha a liberdade de escolher qualquer parceiro de detecção e resposta gerenciadas (MDR) ou serviços de segurança gerenciados (MSSP) que atenda às suas necessidades, seja sua própria equipe interna, um MSSP especializado, ou outro provedor de MDR totalmente diferente.

Por Que a Escolha Importa

Essa separação lhe dá a capacidade de definir seus próprios acordos de nível de serviço, medir a qualidade e a capacidade de resposta da equipe que monitora seu ambiente, e responsabilizar esse provedor por meio de uma relação contratual real. Em vez de esperar que um fornecedor empacotado esteja lhe dando atenção adequada, você pode avaliar e impor padrões de desempenho de acordo com seus próprios termos. Em última análise, a abordagem da Cyber Crucible visa oferecer às organizações um controle genuíno — controle contra atacantes e, igualmente importante, controle sobre os relacionamentos e contratos com fornecedores que sustentam seu programa de segurança.

https://player.vimeo.com/video/1046829518?texttrack=pt

Assistir no Vimeo · Legendas: English, Français, Español, العربية

Como a Cyber Crucible me ajuda a controlar os gastos com segurança cibernética e os contratos com fornecedores?

Resposta curta: A Cyber Crucible não reduz necessariamente o seu orçamento total de segurança, mas oferece mais controle sobre como esse orçamento é gasto, permitindo separar a prevenção contra ransomware e roubo de dados dos serviços de monitoramento e resposta — para que você possa escolher e responsabilizar o fornecedor que cuida desse último.

O Custo Oculto dos Serviços de SOC Empacotados

Muitas organizações pagam somas significativas a um centro de operações de segurança (SOC) hospedado, que vem empacotado com uma plataforma EDR ou XDR. O desafio desse arranjo é que o cliente geralmente tem pouca visibilidade sobre o quanto essa equipe de monitoramento é atenta ou eficaz. Não há uma maneira fácil de medir a qualidade da resposta, o engajamento da equipe ou o quão seriamente sua conta é priorizada. Você está essencialmente confiando que o serviço nos bastidores está funcionando bem, sem uma forma prática de verificar isso.

Separando a Prevenção do Monitoramento

A Cyber Crucible se concentra especificamente no lado da prevenção da proteção de endpoints — impedindo ransomware, roubo de dados e roubo de identidade antes que o dano ocorra. Como a prevenção é tratada de forma independente, as organizações deixam de estar presas a um único fornecedor empacotado para prevenção e monitoramento. Isso significa que você pode selecionar seu próprio provedor de detecção e resposta gerenciadas (MDR), MSSP, ou até mesmo contar com sua equipe interna para o monitoramento e a resposta contínuos.

Recuperando o Controle sobre a Responsabilização dos Fornecedores

Essa separação importa porque restaura sua capacidade de negociar e fazer cumprir acordos de nível de serviço claros com os fornecedores que você escolher. Você pode avaliar a capacidade de resposta, medir o desempenho e responsabilizar os fornecedores de maneiras que não são possíveis quando prevenção e monitoramento estão vinculados sob um único contrato. Em resumo, o valor não está apenas na defesa técnica contra invasores — está em recuperar a supervisão e o controle sobre seus próprios relacionamentos com fornecedores, contratos e a qualidade do serviço pelo qual você está pagando.

https://player.vimeo.com/video/1046667196?texttrack=pt

Assistir no Vimeo · Legendas: English, Français, Español, العربية

A Cyber Crucible funciona em conjunto com outras ferramentas de cibersegurança e EDR?

Resposta curta: Sim. A Cyber Crucible é construída sobre sensores proprietários próprios e tecnologia de monitorização comportamental, pelo que funciona em conjunto com praticamente qualquer outro produto de segurança sem interferir com as ferramentas existentes.

Por Que a Compatibilidade Não É um Problema

A Cyber Crucible não depende de hooks de EDR partilhados ou de integrações a nível de sistema das quais outros fornecedores de segurança também dependem. Como a sua abordagem de deteção e monitorização, incluindo os métodos de recolha comportamental que estão por trás do FortressAI, é construída de raiz de forma personalizada, não compete pelos mesmos recursos do sistema nem interfere com os hooks utilizados por outras ferramentas de proteção de endpoints. Este design permite que a Cyber Crucible funcione como uma camada de proteção adicional, em vez de um substituto ou de uma sobreposição conflituante. Já foi implementada em conjunto com produtos de uma vasta gama de fornecedores de segurança estabelecidos e, na prática, a maioria dos ambientes não apresenta quaisquer problemas de compatibilidade.

Quando São Necessários Ajustes

A rara situação que exige configuração adicional envolve software personalizado, desenvolvido internamente, que uma empresa tenha criado por conta própria. Ocasionalmente, essas ferramentas desenvolvidas internamente exibem padrões de comportamento que se assemelham ao tipo de atividade que a Cyber Crucible foi concebida para detetar, como alterações rápidas de ficheiros ou interações incomuns com o sistema. Quando isto acontece, a solução é simples: pode ser adicionada uma regra de exclusão para que a Cyber Crucible reconheça a ferramenta interna como legítima. Esta exclusão mantém-se fiável enquanto o software interno permanecer devidamente assinado e inalterado, ou seja, continuar a corresponder ao seu estado esperado e verificado. Se essas condições se mantiverem, a ferramenta funciona normalmente em conjunto com a Cyber Crucible, sem qualquer atrito contínuo.

O Que Isto Significa para as Equipas de Segurança

As organizações não precisam de remover ou reconfigurar a sua atual pilha de segurança para adotar a Cyber Crucible. Foi concebida para complementar as defesas existentes, adicionando uma camada dedicada, focada na prevenção de ransomware, roubo de dados e roubo de identidade, sem perturbar as ferramentas que já protegem o ambiente.

https://player.vimeo.com/video/1043463490?texttrack=pt

Assistir no Vimeo · Legendas: Inglês, Francês, Espanhol, Árabe

Por que a IA é um risco de negócio, e não apenas uma ferramenta de produtividade, para os executivos da empresa?

Resposta curta: As equipes executivas frequentemente veem a IA puramente como um impulsionador de produtividade, mas o uso não gerenciado da IA pode expor segredos essenciais do negócio — planos de produtos, dados de receita e estratégia de vendas — diretamente a partes externas. Este é um risco estratégico e financeiro que deve estar na mesa do CEO, do CFO, do COO e da liderança de vendas, não apenas do departamento de TI.

Um Tipo Diferente de Exposição

Os incidentes tradicionais de cibersegurança, como uma violação de dados que faz registros de clientes parar na dark web, seguem um padrão conhecido: a liderança responde, os reguladores podem se envolver, multas às vezes são pagas e o conselho recebe um briefing. As empresas já lidaram com esse cenário antes, e existem processos para geri-lo.

A IA introduz uma nova categoria de exposição, ainda pouco compreendida. Quando os funcionários usam ferramentas de IA sem as devidas salvaguardas, podem estar alimentando informações confidenciais do negócio — planos futuros de produtos, previsões de lucro, pipelines de vendas — em sistemas que nunca foram projetados para manter essas informações contidas. Ao contrário de um incidente de invasão, isso não é necessariamente resultado de um ataque. Pode acontecer simplesmente através do uso normal e bem-intencionado da IA pelos colaboradores.

O Problema das Consultas Internas

Um risco frequentemente negligenciado é o que acontece internamente na empresa quando uma ferramenta de IA tem amplo acesso a documentos e dados internos. Se os controles de acesso não forem cuidadosamente projetados, um funcionário pode fazer uma simples pergunta a um assistente de IA e receber uma resposta detalhada contendo planos sensíveis que nunca deveriam circular livremente, mesmo internamente. Isso é uma falha de governança, não uma falha técnica, e pode ser tão prejudicial quanto um vazamento externo.

Por Que Isso Deve Estar no Nível da Liderança

Optar por não investir em um ambiente interno de IA devidamente controlado não elimina essa categoria de risco; simplesmente a transfere para fora da supervisão direta da organização. Os líderes empresariais jamais considerariam publicar demonstrativos de lucros e perdas ou pipelines de vendas em um site público. O uso não gerenciado da IA pode criar um resultado semelhante sem que ninguém tenha essa intenção. Tratar isso como um risco central de negócio, e não apenas como uma questão puramente técnica, é essencial para proteger as vantagens competitivas que a liderança trabalhou para construir.

https://player.vimeo.com/video/1211538534?texttrack=pt

Assista no Vimeo · Legendas: English, Français, Español, العربية

Os funcionários já estão usando ferramentas de IA antes de a nossa empresa ter uma política oficial de IA?

Resposta curta: Sim. A maioria das organizações descobre que funcionários, contratados, consultores e fornecedores já estão usando ferramentas de IA de formas criativas e inesperadas muito antes de qualquer política ou projeto formal de governança de IA ser finalizado. Esperar por uma política "perfeita" antes de abordar o uso de IA deixa a empresa cega quanto ao que já está acontecendo.

Saiba mais: impeça que os dados sensíveis cheguem ao ChatGPT e a outras ferramentas de IA (FortressAI)

A suposição comum

Muitos líderes presumem que a adoção de IA dentro da organização está suspensa até que uma política oficial seja escrita, aprovada e implementada. O raciocínio é que os funcionários aguardarão pacientemente por regras claras antes de experimentar novas ferramentas. Na prática, essa suposição raramente se confirma. As pessoas tendem a procurar formas de trabalhar de maneira mais eficiente, independentemente de já existir ou não uma orientação formal.

O que as organizações realmente encontram

Quando as empresas implementam ferramentas de monitoramento ou aplicação de políticas, como o FortressAI da Cyber Crucible, frequentemente descobrem que o uso de IA é muito mais difundido e variado do que o esperado. Os colaboradores são, por natureza, engenhosos; a mesma criatividade e capacidade de resolução de problemas que os tornam funcionários valiosos também os leva a encontrar novas formas, não autorizadas, de usar ferramentas de IA para economizar tempo ou melhorar seus resultados. Isso não é um sinal de má intenção, mas sim da natureza humana: as pessoas usarão as ferramentas disponíveis para facilitar o seu trabalho, quer uma

política o permita oficialmente ou não.

Por que a visibilidade importa mais do que uma política perfeita

O verdadeiro risco não é o fato de uma política ainda não ter sido finalizada. É que as organizações frequentemente carecem de visibilidade sobre como a IA já está sendo usada em todo o seu ambiente. Sem essa visibilidade, as equipes de segurança e conformidade não conseguem avaliar a exposição a vazamentos de dados, uso não autorizado de ferramentas ou outros riscos associados à adoção de IA. Em vez de esperar que uma estrutura abrangente de governança de IA seja concluída, as organizações beneficiam-se ao obter, primeiro, uma visão sobre os padrões de uso atuais. Compreender o que realmente está acontecendo na prática permite que as políticas sejam fundamentadas na realidade, e não em suposições sobre o comportamento dos funcionários.

https://player.vimeo.com/video/1176537677?texttrack=pt

Assista no Vimeo · Legendas: English, Français, Español, العربية

Quais são os sinais de alerta de que um ataque de ransomware está acontecendo?

Resposta curta: Uma vez acionado, o ransomware pode paralisar uma empresa em apenas 60 a 90 segundos, portanto os sinais de alerta visíveis tendem a aparecer apenas quando o ataque já está em andamento, sem antecedência suficiente para interrompê-lo manualmente. A defesa real está em identificar o trabalho de preparação que os atacantes realizam previamente, antes mesmo de acionarem o gatilho final.

Por que o ransomware parece repentino

Os ataques de ransomware costumam ser descritos como instantâneos, mas isso é enganoso. Os atacantes normalmente passam um tempo dentro da rede antes de agir, mapeando silenciosamente os sistemas, obtendo acesso e se posicionando para causar o máximo de dano. Esse trabalho preparatório é semelhante ao de uma equipe militar preparando um campo de batalha antes do início de uma operação. Depois que tudo está em posição, o evento real de criptografia ou bloqueio pode ocorrer em menos de dois minutos. No momento em que os funcionários percebem que algo está errado, o dano já está, em grande parte, em curso.

Como é o momento do ataque

Quando um ataque é executado, as empresas costumam notar uma mudança súbita e perturbadora: determinados aplicativos ou serviços param de responder, as conexões de rede ficam instáveis, os sistemas telefônicos podem cair, e as operações normais parecem ser interrompidas quase simultaneamente. Igualmente inquietante é o fato de que alguns sistemas continuam funcionando normalmente durante essa janela. Essa aparente normalidade não é um bom sinal. Frequentemente, isso significa que os atacantes estão usando esses sistemas não afetados como disfarce enquanto o restante do ambiente está sendo comprometido.

Por que a detecção precoce importa mais do que a reação

Como os sinais visíveis de ransomware só aparecem nos segundos finais e acelerados de um ataque, esperar para reagir a esses sinais não é uma estratégia confiável. Uma proteção significativa depende de identificar e interromper a atividade maliciosa durante a etapa de preparação, antes que os atacantes estejam prontos para agir. É nessa camada que ferramentas de detecção autônoma como o FortressAI, da Cyber Crucible, são projetadas para atuar, com o objetivo de interromper o comportamento do atacante antes que ele chegue ao ponto sem retorno, em vez de esperar pelos sintomas externos que surgem quando o ataque já está em andamento.

https://player.vimeo.com/video/1043488930?texttrack=pt

Assistir no Vimeo · Legendas: English, Français, Español, العربية

O que realmente acontece nos momentos durante um ataque de ransomware?

Resposta curta: A fase real de encriptação de um ataque de ransomware é notavelmente rápida, muitas vezes concluída em cerca de 60 a 90 segundos após ser desencadeada, embora os atacantes passem um tempo significativo e não observado antecipadamente, posicionando-se dentro de uma rede. No momento em que sintomas visíveis surgem, o dano já está a desenrolar-se em tempo real, razão pela qual a deteção tem de ocorrer antes do desencadeamento final, e não depois.

A Calmaria Antes do Ataque

Antes de o ransomware ser ativado, os atacantes normalmente passam tempo a mover-se silenciosamente pelos sistemas de uma empresa, identificando dados valiosos, desativando cópias de segurança e criando as condições necessárias para um ataque bem-sucedido. Este trabalho preparatório pode passar despercebido porque as operações normais da empresa continuam como habitual. A rede pode parecer estável e saudável até ao momento em que o atacante decide lançar a fase final. Tal como um silêncio inquietante mesmo antes de algo catastrófico acontecer, este período de calma pode ser enganador, uma vez que não reflete a disrupção prestes a ocorrer.

O Início Rápido dos Danos

Uma vez lançado, um incidente de ransomware pode desenrolar-se em menos de dois minutos. Nesse curto período, os colaboradores podem notar quebras súbitas: o e-mail deixa de funcionar, os sistemas telefónicos ficam silenciosos, as aplicações comportam-se de forma errática ou as ligações de rede tornam-se instáveis. Estes são sintomas de encriptação e comprometimento do sistema a acontecer simultaneamente em todo o ambiente. Como o processo se move tão rapidamente, tipicamente não há tempo suficiente para uma intervenção manual depois de este começar.

Por Que Razão Alguns Sistemas Continuam a Funcionar

Um pormenor inquietante de muitos incidentes de ransomware é que nem tudo falha ao mesmo tempo. Alguns serviços podem continuar a funcionar normalmente mesmo enquanto outros colapsam. Isto acontece frequentemente porque esses sistemas não afetados são exatamente onde o atacante ainda está a operar, usando-os como ponto de apoio ou área de preparação. Reconhecer este padrão é importante, uma vez que assumir que um problema é "apenas parcial" pode criar uma falsa sensação de segurança enquanto o comprometimento está ativamente em curso. A prevenção eficaz depende da identificação e paragem da atividade maliciosa antes de a fase destrutiva final começar, uma vez que, uma vez desencadeada, a janela para agir é extremamente curta.

https://player.vimeo.com/video/1046658956?texttrack=pt

Ver no Vimeo · Legendas: English, Français, Español, العربية

O que realmente acontece quando o ransomware atinge um servidor de empresa?

Resposta curta: Quando o ransomware atinge um servidor, os invasores normalmente desativam primeiro os seus serviços e, em seguida, encriptam os seus dados enquanto cortam o acesso das equipas de TI e de segurança, impedindo qualquer intervenção — por vezes utilizando dezenas ou mesmo centenas de estações de trabalho comprometidas para executar a encriptação remotamente.

Os Primeiros Sinais de um Ataque

Um dos primeiros indicadores de que um servidor foi comprometido é a perda súbita de serviço. Como os invasores sabem que o ransomware pode corromper acidentalmente ficheiros durante o processo de encriptação, muitos optam por desligar deliberadamente as aplicações em execução num servidor antes de iniciar a encriptação. Isto significa que os funcionários ou clientes que dependem desse sistema — seja uma plataforma de processamento salarial, uma aplicação web ou outro serviço crítico para o negócio — podem notar uma interrupção antes de alguém perceber que um incidente de segurança está em curso.

Bloquear os Defensores Enquanto a Encriptação se Propaga

Assim que o ataque está em curso, o ransomware começa a encriptar os dados armazenados no servidor. Para impedir que as equipas de segurança ou os administradores intervenham, os invasores bloqueiam frequentemente o acesso à rede do servidor, isolando-o das pessoas que normalmente responderiam à ameaça. Esta tática dá ao invasor tempo para concluir a encriptação dos ficheiros antes que os defensores possam agir.

As Estações de Trabalho Podem Ser o Verdadeiro Ponto Fraco

Curiosamente, o servidor em si nem sempre é a origem do perigo. Em muitos casos, os invasores comprometem um grande número de estações de trabalho de funcionários — por vezes 50, 70 ou mais — que já têm acesso legítimo ao servidor. Estas estações de trabalho são depois utilizadas simultaneamente para encriptar remotamente os dados do servidor. Como o ataque é lançado a partir de múltiplos pontos finais em simultâneo, as estações de trabalho ligadas ao servidor representam muitas vezes uma vulnerabilidade maior do que a própria infraestrutura do servidor.

Este padrão evidencia por que razão a defesa contra ransomware não pode centrar-se apenas nos servidores. A segurança de terminais em todos os dispositivos com acesso ao servidor desempenha um papel fundamental para impedir os ataques antes que a encriptação se propague. O FortressAI da Cyber Crucible foi concebido para identificar e interromper estes comportamentos nas fases mais iniciais, quer a ameaça se origine num servidor, quer se propague a partir de estações de trabalho ligadas.

https://player.vimeo.com/video/1041172405?texttrack=pt

Ver no Vimeo · Legendas: Inglês, Français, Español, العربية

Por que o ransomware ataca arquivos compartilhados antes de atingir meu desktop?

Resposta rápida: Quando um ransomware infecta uma estação de trabalho individual, essa máquina raramente é o alvo real. Os atacantes usam a infecção inicial como ponto de lançamento para alcançar recursos de rede compartilhados, e só criptografam ou danificam o desktop local depois de já terem atacado dados de maior valor em outros locais.

Por que o desktop é a última parada, não a primeira

Um equívoco comum é achar que, se o ransomware chega ao computador de um funcionário específico, os arquivos desse funcionário são o que os atacantes desejam. Na realidade, o malware é programado para olhar além da máquina local quase imediatamente. Uma vez que consegue se estabelecer, ele começa a escanear a rede em busca de recursos acessíveis com maior valor, como servidores de arquivos, wikis internas ou bancos de dados contendo informações de clientes. Criptografar ou exfiltrar esses dados centralizados é o verdadeiro objetivo, pois isso afeta muito mais a organização do que a pasta de um único usuário.

A nota de resgate chega por último, não primeiro

Como os atacantes priorizam os dados de toda a rede antes de tocar no dispositivo de origem, o funcionário que foi infectado costuma ser a última pessoa a perceber que algo está errado. Quando uma nota de resgate aparece na tela dessa pessoa, os atacantes normalmente já terminaram de criptografar ou roubar dados em grande parte da infraestrutura da empresa. Essa sequência é intencional. Ela permite que os atacantes causem o máximo de dano operacional antes que alguém na organização tenha a chance de detectar a intrusão ou responder a ela. A nota de resgate visível é essencialmente um sinal de que o dano mais sério já ocorreu nos bastidores.

O que isso significa para a defesa

Fotos ou documentos pessoais armazenados localmente em um desktop costumam ser o alvo menos importante em um ataque de ransomware, mesmo que possam ser o sinal mais visível de que ele ocorreu. Uma defesa eficaz precisa levar esse padrão em conta, concentrando-se em detectar e interromper atividades maliciosas o mais cedo possível, antes que possam alcançar sistemas compartilhados. O FortressAI da Cyber Crucible foi desenvolvido levando em conta essa sequência de ataque, com o objetivo de intervir nos estágios iniciais de uma intrusão, em vez de apenas reagir quando a criptografia se torna visível em máquinas individuais.

https://player.vimeo.com/video/1043466243?texttrack=pt

Assistir no Vimeo · Legendas: English, Français, Español, العربية

O que inspirou o fundador a criar a Cyber Crucible?

Resposta breve: A Cyber Crucible surgiu de uma carreira dedicada à construção de soluções pontuais para missões governamentais classificadas, e do desejo de aplicar essa mesma capacidade de resolver problemas para ajudar muito mais pessoas a combater o ransomware e o cibercrime em todo o mundo.

De Missões Classificadas a um Problema Global

Muito antes de a Cyber Crucible existir como empresa, seu fundador já resolvia problemas de segurança complexos, incluindo a identificação de uma forma de assumir o controle de uma botnet para proteger as pessoas contra ela. Esse padrão de decompor desafios técnicos difíceis e projetar soluções práticas se estendeu por uma carreira na National Security Agency e em outras organizações governamentais. Repetidas vezes, uma nova ferramenta ou técnica era criada para resolver uma necessidade específica de uma missão, apenas para ser usada uma única vez, transferida para uma equipe aliada ou arquivada após cumprir seu propósito restrito. Cada invenção tinha importância, mas o impacto se limitava aos contornos de uma única missão classificada.

Transformando Soluções Individuais em Algo que Todos Podem Usar

Esse ciclo de resolver um problema e depois ver sua utilidade permanecer restrita a uma única equipe ou operação, eventualmente, tornou-se frustrante, mesmo que o trabalho em si fosse significativo. Quando o ransomware surgiu como uma ameaça generalizada, ele apresentou um tipo diferente de oportunidade: a chance de aplicar a mesma abordagem inventiva, mas voltada para um problema que afeta organizações e indivíduos em todos os lugares, não apenas uma unidade especializada isolada. A percepção foi de que ajudar uma população mais ampla de pessoas exigia mais do que outra ferramenta personalizada para um caso de uso restrito. Exigia um produto comercial que pudesse ser implantado de forma fácil e confiável em larga escala.

Por Que Isso Molda a Cyber Crucible Hoje

Essa mudança de pensamento é a base da abordagem da Cyber Crucible. Em vez de construir uma solução para uma única equipe ou missão, o objetivo é criar uma tecnologia, impulsionada pela FortressAI, que funcione de forma automática e consistente para organizações em qualquer lugar, para que menos pessoas precisem sofrer os danos e as interrupções causados por ransomware, roubo de dados e roubo de identidade. O trabalho focado em missões do passado ainda tem importância, mas o propósito que impulsiona a Cyber Crucible é alcançar e proteger o maior número possível de pessoas.

https://player.vimeo.com/video/1046673820?texttrack=pt

Assista no Vimeo · Legendas: English, Français, Español, العربية

De onde realmente vêm os ataques de ransomware?

Resposta curta: Os operadores de ransomware não estão confinados a um punhado de países bem conhecidos; a automação e as ferramentas criminosas baratas agora permitem que os atacantes operem a partir de praticamente qualquer lugar do mundo.

A história simplista da mídia não corresponde às evidências

A cobertura noticiosa frequentemente aponta para um único país ou região como a origem dos ataques de ransomware, pois isso resulta em uma manchete rápida e fácil de assimilar. Na prática, a experiência direta na resposta a incidentes ativos conta uma história mais complexa. Quando a Cyber Crucible começou a lidar com casos ativos de ransomware, nossa equipe recebeu uma ampla variedade de chamadas telefônicas relacionadas aos ataques—muitas originadas de telefones pré-pagos ou descartáveis ("burner phones") sem histórico de propriedade rastreável. Essas chamadas vinham de diversas regiões diferentes, incluindo o Sul da Ásia, o Oriente Médio, partes da Europa, a América do Sul e até mesmo a América do Norte. Alguns interlocutores eram operadores de baixo nível, enquanto outros pareciam ser os verdadeiros desenvolvedores do malware, ocasionalmente participando de conversas surpreendentemente profissionais, entre pares, sobre os detalhes técnicos de seus ataques.

A automação reduziu a barreira de entrada

Embora certas regiões do mundo ainda possam produzir uma parcela desproporcional de desenvolvedores de ransomware habilidosos, o surgimento de kits de ransomware como serviço, ferramentas de automação e alcance básico assistido por IA tornou muito mais fácil a participação de agentes menos sofisticados. Alguém com habilidade técnica limitada agora pode alugar infraestrutura de ataque, comprar acesso roubado à rede de corretores de acesso inicial e conduzir uma campanha de extorsão com investimento inicial mínimo. Isso efetivamente abriu as portas para que criminosos oportunistas localizados em qualquer lugar possam participar, em vez de restringir a atividade de ransomware a um pequeno grupo de agentes vinculados a estados-nação.

Por que isso importa para a defesa

A gíria regional, os padrões linguísticos e o comportamento de chamadas observados durante esses incidentes reforçam que os atacantes são geograficamente diversos, não limitados a uma única nação "agente malicioso". Compreender o ransomware como uma empresa criminosa globalmente distribuída e impulsionada pela automação—em vez de uma narrativa geopolítica simplista—leva a estratégias de defesa mais bem informadas e a uma visão mais clara do risco real que as organizações enfrentam.

https://player.vimeo.com/video/1047715735?texttrack=pt

Assistir no Vimeo · Legendas: Inglês, Francês, Espanhol, Árabe

Quem os atacantes de ransomware realmente visam hoje?

Resposta curta: Os operadores de ransomware já não se concentram apenas em organizações grandes e de alto perfil. A automação e as ferramentas orientadas por IA tornaram lucrativo visar empresas de praticamente qualquer dimensão, o que significa que a maioria das organizações deve presumir que é um alvo potencial.

Como a seleção de alvos mudou desde 2020

Nos primeiros dias do ransomware moderno, executar um ataque desde o acesso inicial até à extorsão exigia hackers experientes e qualificados, trabalhando em grande parte manualmente. Isso limitava o número de atacantes capazes e mantinha o foco em alvos grandes e de elevado valor, onde o retorno justificava o esforço.

À medida que a procura crescia, grupos de hackers estabelecidos começaram a operar mais como negócios em expansão. Em vez de depender apenas de um pequeno número de operadores de elite, começaram a criar programas de ransomware-as-a-service que empacotam métodos de ataque comprovados em manuais repetíveis e automatizados. Isto permitiu que operadores menos experientes conduzissem campanhas eficazes, de forma semelhante a um vendedor júnior que consegue ter sucesso utilizando um guião criado a partir dos métodos de um vendedor de topo.

Por que razão as organizações mais pequenas estão agora em risco

A automação, a aprendizagem automática (machine learning) e a automação robótica de processos permitem que estes operadores executem múltiplos ataques em simultâneo, geram negociações de resgate e gerem o apoio ao pagamento ou à recuperação em grande escala. Assim que estas funções se tornaram largamente automatizadas, atacar empresas mais pequenas também passou a ser lucrativo, uma vez que são máquinas — e não pessoas — que tratam da maior parte do contacto e do acompanhamento.

Esta mudança significa que os atacantes são menos seletivos. Os grandes alvos ("big game") continuam a atrair atenção devido à dimensão do potencial retorno, mas a atividade quotidiana destas operações criminosas assemelha-se cada vez mais à prospeção comercial de rotina: sistemas automatizados procuram continuamente qualquer organização que possa pagar. Os sistemas responsáveis pela seleção de alvos normalmente não têm qualquer conhecimento sobre quem ou o que o alvo realmente é, seja este uma grande empresa ou uma pequena organização sem fins lucrativos.

O que isto significa para as organizações

Uma vez que a seleção de alvos é largamente automatizada e indiscriminada, a questão mais relevante para a maioria das organizações não é se poderão ser especificamente escolhidas, mas sim o quão preparadas estão para uma eventual tentativa. Soluções como a Cyber Crucible, construídas sobre a FortressAI, foram concebidas para ajudar as organizações a detetar e travar o ransomware e ameaças relacionadas, independentemente da dimensão ou do perfil do alvo.

https://player.vimeo.com/video/1047715793?texttrack=pt

Ver no Vimeo · Legendas: English, Français, Español, العربية

Quem Corre Maior Risco de um Ataque de Ransomware e Por Que São Alvos?

Resposta curta: O risco de ransomware muitas vezes se resume a quem os "corretores de acesso" criminosos consideram mais fácil de invadir ou são especificamente pagos para invadir, o que significa que escolas, hospitais e fornecedores de infraestrutura com defesas mais fracas ou dados valiosos frequentemente estão no topo da lista.

Saiba mais: prevenção de ransomware e de roubo de credenciais ao nível do kernel (Cyber Crucible Core)

Como os Alvos São Escolhidos, Antes de Mais Nada

Por trás da maioria dos incidentes de ransomware existe um mercado que a maioria das pessoas nunca vê. Um grupo, frequentemente chamado de corretores de acesso inicial, passa seu tempo invadindo redes sem nenhum plano específico para o que acontece a seguir. Assim que conseguem se estabelecer, eles anunciam esse acesso para venda, descrevendo exatamente o que controlam, como direitos administrativos sobre ferramentas de segurança, a capacidade de desativar proteções antivírus, ou acesso a uma grande parcela dos dispositivos de uma organização. Eles podem descrever, por exemplo, ter comprometido a frota de dispositivos de um distrito escolar ou as ferramentas de acesso remoto de um fornecedor de TI. Compradores, que vão desde grupos de roubo de dados até operadores de ransomware e agentes patrocinados por estados, então fazem lances por esse acesso com base em quão valioso e completo ele parece.

Quando os Ataques São Encomendados, Não Apenas Oportunistas

Existe também um segundo padrão, mais direcionado. Aqui, um comprador, como um grupo de ransomware ou um agente estatal, faz um pedido específico: encontrar e comprometer um determinado número de organizações que atendam a certos critérios, como hospitais de um determinado porte em uma determinada região, ou fornecedores de serviços públicos como estações de tratamento de água. Os corretores de acesso então tratam isso como uma tarefa de vendas, caçando ativamente organizações que se encaixem no perfil. Assim que conseguem, vendem esse acesso ao solicitante original, mesmo que os dois lados normalmente nunca interajam diretamente nem saibam a identidade um do outro. É por isso que agrupamentos repentinos de ataques contra organizações semelhantes, como vários hospitais em uma mesma região, frequentemente refletem uma ordem de compra coordenada, e não uma coincidência.

Por Que Isso Importa para a Defesa

Como o direcionamento de alvos pode ser tanto oportunista quanto especificamente encomendado, qualquer organização com controles de segurança fracos, dados sensíveis ou serviços críticos pode se tornar um alvo, independentemente do porte ou do setor. Compreender essa dinâmica entre compradores e vendedores reforça por que defesas proativas e sempre ativas importam mais do que reagir depois que uma violação já foi vendida ao maior lance.

https://player.vimeo.com/video/1047715835?texttrack=pt

Assistir no Vimeo · Legendas: English, Français, Español, العربية

Quem Realmente Executa os Ataques de Ransomware e Como Eles Operam?

Resposta curta: Os ataques de ransomware são realizados por uma rede vagamente organizada de desenvolvedores, revendedores e operadores que funcionam de forma semelhante a uma cadeia de suprimentos empresarial, e os mais eficazes tratam a extorsão como um ofício profissional, e não como uma vingança pessoal.

Saiba mais: prevenção de ransomware e de roubo de credenciais ao nível do kernel (Cyber Crucible Core)

Ransomware como uma Cadeia de Suprimentos Organizada

O ransomware raramente é obra de um único hacker atuando sozinho. Em vez disso, opera mais como uma indústria distribuída composta por desenvolvedores de malware que criam as ferramentas, revendedores ou afiliados que distribuem o acesso a esse malware, e operadores que executam os ataques propriamente ditos contra as vítimas. Cada grupo desempenha um papel distinto, semelhante a como um fornecedor de software legítimo pode depender de fabricantes, distribuidores e equipes de vendas. Essa estrutura em camadas é parte do que torna o ransomware resiliente: interromper um elo da cadeia não necessariamente interrompe a operação mais ampla.

Os Profissionais vs. os Atacantes Emocionais

Nem todos os atacantes se comportam da mesma forma quando suas tentativas são bloqueadas. A Cyber Crucible vivenciou diretamente esse contraste. Em um caso, um atacante ligado ao Leste Europeu ligou depois de ser impedido, tratando o encontro como um quebra-cabeça técnico a ser resolvido, e não como um insulto pessoal. Esse indivíduo chegou a mencionar detalhes internos do software para provar que havia feito engenharia reversa do produto, e continuou entrando em contato periodicamente depois disso, discutindo suas operações quase como um colega faria.

Em contraste, outro atacante ligado a Bangladesh reagiu com raiva e hostilidade após ser frustrado, recorrendo a insultos em vez de buscar soluções. Esse contato não continuou a se comunicar ao longo do tempo.

Por Que Isso Importa para a Defesa

Essas experiências sugerem que os agentes de ameaça mais "bem-sucedidos" e persistentes tendem a ser aqueles que abordam o ransomware como um desafio de negócios—metódicos, pacientes e focados em encontrar soluções alternativas. Compreender os atacantes como adversários que agem de forma empresarial, em vez de criminosos puramente caóticos, ajuda a orientar como a tecnologia defensiva, como o FortressAI da Cyber Crucible, é projetada: para antecipar tentativas calculadas de burlar as proteções, e não apenas ataques isolados ou motivados emocionalmente.

https://player.vimeo.com/video/1047715866?texttrack=pt

Assistir no Vimeo · Legendas: English, Français, Español, العربية

Quem é o cliente ideal para a proteção contra ransomware da Cyber Crucible?

Resposta curta: A Cyber Crucible é a solução ideal para pessoas que pensam em termos de impacto para o negócio, e não apenas em recursos técnicos. Isso inclui líderes de TI com recursos limitados e executivos que compreendem o que mesmo uma breve interrupção pode custar à empresa.

Saiba mais: prevenção de ransomware e de roubo de credenciais ao nível do kernel (Cyber Crucible Core)

Por que o pensamento voltado para o negócio importa mais do que o cargo

Não existe um único cargo que defina o cliente ideal da Cyber Crucible. O que importa é se a pessoa compreende as consequências reais de um incidente de ransomware ou de roubo de dados: perda de receita, interrupção das operações e o tipo de dano financeiro que pode persistir por meses ou anos depois. Alguém com essa mentalidade não precisa ser convencido de que a prevenção automatizada vale a pena; essa pessoa já entende que evitar o tempo de inatividade está diretamente ligado à proteção do lucro e à manutenção do funcionamento do negócio.

Isso é diferente de uma conversa de vendas puramente técnica, na qual o valor de um produto se perde em jargões que só especialistas conseguem acompanhar. A abordagem da Cyber Crucible, impulsionada pela FortressAI, foi moldada em torno de um resultado simples e prático para os clientes em primeiro lugar, com a tecnologia subjacente construída para sustentar esse resultado. Por isso, as conversas mais claras costumam acontecer com pessoas que se importam com o que uma falha de segurança significa para o negócio, e não apenas com o funcionamento interno do software.

Exemplos dos interlocutores certos

Um diretor de TI que gerencia uma equipe e um orçamento limitados, e que é pessoalmente responsável pela disponibilidade e pela confiabilidade dos sistemas, geralmente percebe o valor

rapidamente, pois o tempo de inatividade afeta sua carga de trabalho diária e seu desempenho. Por outro lado, um CEO ou CFO pode insistir em uma proteção automatizada mesmo quando a equipe de segurança se sente satisfeita com as medidas existentes, simplesmente porque reconhece que uma breve interrupção, às vezes de apenas uma hora, pode gerar um dano financeiro que leva bem mais de um ano para ser recuperado.

O elo em comum

Seja a conversa iniciada por um líder de TI focado em operações ou por um executivo com foco financeiro, o encaixe mais forte para a Cyber Crucible é qualquer pessoa que avalie a segurança cibernética sob a ótica da continuidade dos negócios e do risco financeiro, e não apenas sob a ótica dos detalhes técnicos.

https://player.vimeo.com/video/1046877762?texttrack=pt

Assistir no Vimeo · Legendas: English, Français, Español, العربية

Por que os ataques de ransomware estão se tornando mais comuns a cada ano?

Resposta rápida: Os ataques de ransomware estão aumentando porque os grupos cibercriminosos evoluíram de agentes desorganizados e oportunistas para operações disciplinadas que usam automação para atacar muitas vítimas com eficiência e extrair pagamento rapidamente.

Saiba mais: prevenção de ransomware e de roubo de credenciais ao nível do kernel (Cyber Crucible Core)

De startups caóticas a operações organizadas

Quando o ransomware se tornou pela primeira vez uma ameaça generalizada, muitos atacantes eram inexperientes. Uma onda de indivíduos recém-desempregados durante a era da pandemia tentou a sorte no cibercrime, muitas vezes com resultados inconsistentes. Como em qualquer setor emergente, apenas os operadores mais organizados e capazes sobreviveram àquele período inicial de seleção. Com o tempo, esses grupos passaram a funcionar menos como oportunistas dispersos e mais como empresas estruturadas focadas em receita consistente.

Até 2024, essa maturidade se traduziu em forte dependência da automação. Operações de ransomware já estabelecidas agora usam ferramentas automatizadas para incorporar participantes menos experientes aos seus ataques, mantendo ainda assim processos eficientes e repetíveis. Isso permitiu que escalassem sua atividade muito além do que uma pequena equipe de hackers habilidosos conseguiria realizar manualmente.

Calibrando o ataque para o máximo retorno financeiro

Uma parte fundamental dessa evolução é aprender a dimensionar corretamente um ataque. Se uma invasão for muito pequena, uma equipe de TI bem preparada pode simplesmente restaurar os

sistemas e evitar qualquer pagamento. Se um ataque for muito abrangente, eliminando toda a infraestrutura da empresa, pode não haver nenhum negócio viável restante para efetuar o pagamento do resgate. Os grupos modernos de ransomware buscam um meio-termo: disrupção suficiente para pressionar a empresa a pagar rapidamente, sem causar tantos danos a ponto de tornar a recuperação ou a negociação irrelevantes.

Por que a automação impulsiona esse aumento

Uma vez que o processo de ataque pode ser automatizado, os cibercriminosos deixam de se contentar em perseguir uma única vítima por vez. Usando ferramentas que se assemelham a inteligência artificial, aprendizado de máquina e automação robótica de processos, eles conseguem atingir dezenas ou centenas de organizações em paralelo. Muitas vítimas optam por não divulgar publicamente os incidentes, permitindo que os atacantes concluam um ciclo de extorsão e passem para novos alvos. Esse modelo de negócio escalável e repetível — e não qualquer tecnologia nova isolada — é o principal motivo pelo qual os ataques de ransomware continuam a aumentar.

https://player.vimeo.com/video/1043463561?texttrack=pt

Assistir no Vimeo · Legendas: English, Français, Español, العربية

Por que a Cyber Crucible utiliza IA em vez de uma equipe humana de SOC para conter ransomware?

Resposta curta: A Cyber Crucible foi construída como um sistema totalmente automatizado desde o primeiro dia, porque os ataques de ransomware se desenrolam muito mais rápido do que qualquer equipe de segurança humana consegue reagir, e a inteligência artificial é a única forma prática de modelar e agir sobre o comportamento de ataque em tempo real.

Saiba mais: prevenção de ransomware e de roubo de credenciais ao nível do kernel (Cyber Crucible Core)

O Problema de Depender dos Tempos de Resposta Humanos

Quando a Cyber Crucible foi desenvolvida pela primeira vez, por volta de 2019, o ransomware já estava superando a capacidade de resposta das equipes de operações de segurança. Mesmo as primeiras variantes de ransomware conseguiam bloquear todos os sistemas de uma organização em poucos minutos. Isso não deixava nenhuma janela realista para que uma pessoa percebesse os sinais de alerta, avaliasse o que estava acontecendo e intervisse antes que ocorressem danos sérios. Desde então, os ataques só se tornaram mais rápidos—alguns relatórios sugerem que a rede de uma empresa de médio porte pode ser totalmente comprometida em apenas 90 segundos. Nessa velocidade, esperar que um analista humano detecte e interrompa um ataque em andamento simplesmente não é viável, independentemente de quão habilidosa ou bem equipada seja a equipe.

Por Que a Modelagem Comportamental Requer IA

Interromper um ataque tão rápido exige mais do que alertas velozes—exige um software capaz de reconhecer padrões de comportamento malicioso e tomar uma decisão de contenção instantaneamente, sem esperar que uma pessoa interprete os dados. Construir manualmente esse tipo de modelagem comportamental detalhada, cobrindo as diversas formas pelas quais um ataque pode se desenrolar, levaria muito mais tempo do que qualquer defensor tem disponível. A inteligência artificial se tornou a ferramenta necessária para construir esses modelos comportamentais com eficiência suficiente para serem incorporados diretamente ao software de segurança, permitindo que as decisões ocorram no exato momento em que um ataque começa, em vez de depois do fato consumado.

IA Como Necessidade Prática, Não Como Tendência

A adoção de uma defesa orientada por IA não teve relação com o acompanhamento de uma tendência do setor—foi uma resposta prática a um problema de tempo que o monitoramento baseado em humanos não conseguia resolver. A abordagem da Cyber Crucible reflete a ideia de combinar a ferramenta certa com a tarefa certa: quando os ataques se comprimem em segundos, a defesa precisa operar na mesma escala de tempo, o que significa tomada de decisão automatizada e baseada em IA, em vez de revisão manual.

https://player.vimeo.com/video/1046871333?texttrack=pt

Assista no Vimeo · Legendas: English, Français, Español, العربية

Por que as equipas de segurança recebem milhares de alertas por dia e como podem lidar com isso?

Resposta breve: A sobrecarga de alertas não surgiu da noite para o dia — acumulou-se gradualmente à medida que os atacantes se tornaram mais automatizados e evasivos, transformando sinais de alerta antes claros em indícios ténues e ambíguos que exigem um profundo conhecimento especializado para serem interpretados. O Cyber Crucible foi criado para romper este ciclo, tratando a deteção e a resposta de forma automática, em vez de exigir que equipas humanas filtrem intermináveis sinais de baixa confiança.

Saiba mais: prevenção de ransomware e de roubo de credenciais ao nível do kernel (Cyber Crucible Core)

Como a Fadiga de Alertas Se Tornou a Norma

A deteção de segurança não se degradou porque os fornecedores decidiram transferir o fardo para os clientes. Aconteceu lentamente, à medida que os atacantes refinaram as suas técnicas para mutarem e se automatizarem mais rapidamente do que as ferramentas defensivas conseguiam classificar de forma definitiva um evento como malicioso. O que antes era um indicador claro de comprometimento tornou-se um indício ténue perdido entre inúmeros outros indícios igualmente ténues. Analisá-los devidamente exige tempo considerável de analistas seniores, e muitas vezes aquilo que parece suspeito não é mais do que um controlador de impressora com mau funcionamento. Entretanto, um único alerta de baixa confiança que passe despercebido pode ser o único vestígio visível de uma intrusão grave e ativa.

Por Que Mais Alertas Não Significaram Melhor Segurança

À medida que as ferramentas de deteção tentavam acompanhar a evolução das ameaças, compensaram sinalizando qualquer coisa ligeiramente fora do comum. Isto criou uma torrente de alertas que, tecnicamente, cumpria o requisito de avisar os clientes, mas deixava as equipas de segurança incapazes de investigar cada um de forma realista. O resultado natural é um de dois cenários: as equipas começam a ignorar alertas de baixa confiança — exatamente onde os atacantes mais sofisticados tendem a esconder-se — ou ficam sobrecarregadas, e o trabalho crítico simplesmente não é feito, independentemente do esforço ou da intenção.

Um Ponto de Partida Diferente

Reconhecendo que soluções incrementais não resolveriam um problema enraizado em anos de complexidade acumulada, a Cyber Crucible abordou a questão a partir de um ângulo totalmente diferente. Em vez de gerar mais alertas para os humanos analisarem, a nossa tecnologia FortressAI foi concebida para detetar e responder de forma autónoma, em tempo real, a ameaças de ransomware, roubo de dados e roubo de identidade. Utilizando abordagens modernas como a IA generativa, a Cyber Crucible visa reduzir a dependência da revisão manual de alertas e resolver o desequilíbrio subjacente entre a automatização dos atacantes e a capacidade dos defensores.

https://player.vimeo.com/video/1186492629?texttrack=pt

Ver no Vimeo · Legendas: English, Français, Español, العربية

Por que o roubo de credenciais e de identidade é mais perigoso do que a criptografia de ransomware?

Resposta curta: A criptografia de ransomware é a etapa visível e final de um ataque, mas o dano real muitas vezes ocorre antes e passa despercebido, quando os atacantes coletam automaticamente senhas, tokens de sessão, chaves e carteiras de criptomoedas. A Cyber Crucible concentra-se em detectar e interromper essa fase inicial e oculta, em vez de esperar pelo momento em que os dados são bloqueados.

Por que as ferramentas de segurança muitas vezes não percebem a ameaça maior

Muitos produtos de segurança são desenvolvidos para reagir à criptografia, pois essa é a parte do ataque que uma empresa realmente percebe—os sistemas param de funcionar, os arquivos ficam ilegíveis e as operações são interrompidas. Essa interrupção visível naturalmente atrai mais atenção e investimento. No entanto, a criptografia costuma ser a última ação tomada pelo atacante, não a primeira. Quando a empresa percebe os efeitos do ransomware, o atacante geralmente já concluiu a parte mais importante da invasão: coletar silenciosamente dados relacionados à identidade, como credenciais, tokens de autenticação, chaves de criptografia e acesso a carteiras digitais. Essa fase inicial não causa nenhuma interrupção visível, por isso tende a ser subestimada, mesmo proporcionando aos atacantes acesso duradouro e repetível à rede.

O primeiro estágio silencioso de um ataque

Os ataques modernos são amplamente automatizados, e a fase de roubo de identidade pode ser concluída em apenas alguns segundos em toda a organização. Como não há interrupção imediata

dos negócios, essa etapa carece da urgência e da visibilidade que a criptografia de ransomware gera, tornando-a fácil de ser ignorada. No entanto, é essa etapa que dá aos atacantes a capacidade de retornar quando quiserem e causar mais danos, incluindo a implantação de ransomware posteriormente.

Como a Cyber Crucible aborda essa lacuna

A Cyber Crucible foi projetada para detectar acessos não autorizados a dados de identidade no exato momento em que ocorrem, em vez de esperar que a criptografia comece. Como essa atividade acontece de forma tão rápida e silenciosa, um esforço significativo de engenharia foi dedicado a tornar a detecção rápida e precisa—identificando quem está acessando dados sensíveis de identidade sem retardar as operações comerciais cotidianas ou a atividade dos usuários.

https://player.vimeo.com/video/1141670023?texttrack=pt

Assistir no Vimeo · Legendas: English, Français, Español, العربية

Por que o ransomware se tornou tão difícil de impedir e de recuperar?

Resposta curta: O ransomware evoluiu de um simples truque de hacking para uma operação criminosa madura e semelhante a um negócio, que utiliza criptografia em camadas e chaves que desaparecem para tornar a recuperação quase impossível sem pagamento. Compreender como a criptografia e o tratamento de chaves realmente funcionam explica por que backups, apreensões por parte das autoridades e soluções rápidas costumam ser insuficientes.

Como o Ransomware Difere de uma Violação de Dados

Uma violação de dados consiste em roubar informações discretamente para vendê-las mais tarde, enquanto os operadores de ransomware têm um objetivo diferente: permanecer dentro de uma rede apenas o tempo suficiente para causar o máximo de disrupção e, então, se revelar. Uma vez causado o dano, esconder-se deixa de importar para eles. Essa operação está cada vez mais automatizada e é conduzida como um negócio, completa com processamento de pagamentos e "atendimento ao cliente" de descriptografia, pois os atacantes precisam de uma forma confiável de coletar dinheiro em escala.

O Truque de Criptografia por Trás do Ataque

O ransomware normalmente depende de dois tipos de criptografia funcionando em conjunto. A criptografia simétrica rápida (como o AES) bloqueia os arquivos propriamente ditos, enquanto a criptografia assimétrica, mais lenta — o mesmo método usado para proteger o tráfego da web —, protege a própria chave simétrica. Essa é uma técnica criptográfica bem estabelecida, tomada de empréstimo de sistemas de segurança legítimos, mas no ransomware ela significa que, mesmo que a chave de um único arquivo fosse de alguma forma recuperada, os atacantes adicionaram complexidade extra para que a descriptografia de um arquivo dependa, muitas vezes, da geração de uma nova chave para o próximo, tornando os atalhos muito mais difíceis do que parecem.

Por Que as Opções de Recuperação Continuam Enfraquecendo

Os primeiros ransomwares reutilizavam uma única chave em muitas vítimas, o que permitia que os defensores, ocasionalmente, extraíssem e compartilhassem uma ferramenta de descriptografia. Os atacantes responderam gerando chaves únicas e de uso exclusivo, que nunca são armazenadas em nenhum lugar recuperável. Isso elimina a opção de qu

https://player.vimeo.com/video/1065143398?texttrack=pt

Assista no Vimeo · Legendas: English, Français, Español, العربية

Por que o antivírus tradicional não consegue impedir ataques de ransomware zero-day e sem arquivo (fileless)?

Resposta curta: As ferramentas de segurança baseadas em assinaturas dependem do reconhecimento de padrões de ataque conhecidos, mas os atacantes modernos testam deliberadamente suas ferramentas contra essas mesmas defesas antes de implantá-las e, cada vez mais, evitam completamente a criação de arquivos detectáveis. Essa combinação de ameaças mutantes e não reconhecidas com técnicas que operam apenas na memória tornou os métodos tradicionais de detecção muito menos confiáveis.

O Problema de Depender de Assinaturas Conhecidas

Os ataques zero-day são, por definição, novos ou alterados o suficiente para ficarem fora do que as ferramentas de segurança existentes já reconhecem. Os fornecedores há muito prometem melhorias na detecção dessas ameaças, mas os atacantes têm uma vantagem inerente: eles têm acesso aos mesmos produtos comerciais de segurança que os defensores utilizam. Antes de lançar uma campanha, os atacantes costumam testar seu malware contra ferramentas de detecção populares, refinando-o até que consiga passar despercebido. Isso transforma a detecção em um alvo em constante movimento, em vez de uma defesa fixa.

Técnicas Sem Arquivo (Fileless) Comprometem o Whitelisting

Os atacantes também deixaram de inserir executáveis maliciosos óbvios em um sistema. Em vez disso, eles sequestram aplicativos legítimos e confiáveis, já aprovados por ferramentas de whitelisting de aplicativos, executando atividades maliciosas por meio de processos que o software de segurança presume serem seguros. Quando essa abordagem sem arquivo é combinada com código que muta rapidamente, os ataques podem ser concluídos em uma janela de tempo muito

curta — às vezes dentro de meia hora — muito antes que uma equipe humana de resposta a incidentes possa realisticamente investigar.

Os Atacantes Apagam Seus Próprios Rastros

Em muitos casos, como o ataque ocorre na memória em vez de no disco, os atacantes eliminam registros, evidências e até sensores de segurança antes de finalizar sua operação. Isso é semelhante a um assaltante desativar câmeras de segurança e alarmes antes de cometer um crime: quando alguém procura por evidências, a visibilidade mais útil já foi destruída. Essa combinação de métodos de ataque imprevisíveis com evidências que se autoapagam é o motivo pelo qual a Cyber Crucible investiu esforços significativos na construção de uma abordagem automatizada e escalável — projetada para capturar os dados críticos necessários para tomar decisões precisas antes que os atacantes possam apagar os rastros, em vez de depender do reconhecimento de ameaças após o fato.

https://player.vimeo.com/video/1164197533?texttrack=pt

Assistir no Vimeo · Legendas: English, Français, Español, العربية

Os hackers usarão mais IA em ataques de ransomware em 2025?

Resposta curta: Sim. Espera-se que os invasores continuem a expandir o uso de inteligência artificial, especialmente modelos de linguagem de grande escala, para se passar por indivíduos confiáveis e manipular vítimas a conceder acesso ou confiança.

Saiba mais: prevenção de ransomware e de roubo de credenciais ao nível do kernel (Cyber Crucible Core)

Por Que a IA Se Tornou a Favorita dos Hackers

Resultados de pesquisa, feeds de notícias e conversas cotidianas estão agora saturados de referências à IA, e esse mesmo entusiasmo se instalou entre os cibercriminosos. Quando a maioria das pessoas menciona IA, normalmente está se referindo a modelos de linguagem de grande escala, como aqueles por trás do ChatGPT e de ferramentas semelhantes, capazes de imitar a comunicação humana de forma convincente. Os invasores reconheceram que essa capacidade é extremamente útil para a engenharia social. Em vez de depender de e-mails de phishing genéricos, eles podem gerar mensagens, vozes ou conversas que se assemelham muito a um colega, fornecedor ou figura de autoridade real, tornando muito mais fácil conquistar a confiança de um alvo antes de atacar.

Espere Táticas de Personificação Mais Refinadas

A tendência para 2025 não é que os ataques baseados em IA sejam algo totalmente novo, mas sim que estão se tornando mais sofisticados e profissionais. Da mesma forma que empresas legítimas estão implementando agentes de vendas com IA e ferramentas automatizadas de prospecção, os invasores estão refinando suas próprias técnicas de personificação baseadas em IA. Isso significa mensagens mais convincentes que imitam chefes, colegas de trabalho ou parceiros confiáveis,

todas projetadas para explorar as relações de trabalho nas quais as pessoas confiam diariamente. O perigo é que uma conversa que pareça pessoal e legítima pode, na verdade, estar vindo de um sistema de IA altamente capaz, construído para manipular, não para ajudar.

O Que Isso Significa para a Defesa

À medida que essas táticas de personificação amadurecem, as organizações devem presumir que os ataques baseados em confiança se tornarão mais difíceis de identificar apenas por instinto. Verificar solicitações por meio de canais independentes, em vez de confiar em uma mensagem ou chamada à primeira vista, torna-se cada vez mais importante. Como esses ataques são projetados para contornar o julgamento humano, contar com capacidades automatizadas de detecção e resposta, como as incorporadas ao FortressAI da Cyber Crucible, oferece uma camada adicional de proteção quando a engenharia social consegue ultrapassar as defesas de uma pessoa.

https://player.vimeo.com/video/1046827321?texttrack=pt

Assistir no Vimeo · Legendas: English, Français, Español, العربية

O uso da Cyber Crucible reduz o orçamento geral de segurança de uma empresa?

Resposta curta: a Cyber Crucible não foi projetada para reduzir diretamente o seu orçamento de segurança; em vez disso, ela libera o tempo e os recursos de equipe que antes eram gastos com monitoramento manual e com a análise de falsos positivos, permitindo redirecionar essa capacidade para lacunas de segurança que antes você não conseguia custear.

Por que a automação não significa automaticamente economia

É tentador presumir que substituir processos manuais de segurança por uma ferramenta automatizada como a Cyber Crucible reduziria imediatamente os custos. Na prática, não é assim que costuma acontecer. Muitos programas de segurança dependem de um conjunto heterogêneo de ferramentas que exigem ajustes constantes, supervisão e revisão manual de alertas. Quando você introduz uma automação que reduz essa carga operacional, o valor não está principalmente em uma fatura menor — está no tempo e na atenção recuperados pela sua equipe. Essa capacidade recuperada tende a ser reinvestida em outras prioridades de segurança, em vez de ser contabilizada como economia pura.

Onde o verdadeiro valor aparece

A maioria dos líderes de TI e segurança já sabe que sua lista de tarefas supera as pessoas e ferramentas disponíveis. A equipe limitada e as restrições técnicas fazem com que muitos riscos conhecidos simplesmente não sejam tratados. Ao reduzir o esforço manual gasto em separar falsos positivos e supervisionar sistemas de detecção, a Cyber Crucible dá às equipes espaço para finalmente enfrentar esses problemas negligenciados. Nesse sentido, o benefício está relacionado à flexibilidade e ao controle orçamentário, não necessariamente a um orçamento menor. Os líderes podem escolher se querem reduzir gastos, realocá-los ou expandir a cobertura para áreas que antes eram inacessíveis devido a limitações de recursos.

O que a Cyber Crucible pode e não pode prometer

A Cyber Crucible não pode resolver todas as restrições orçamentárias que uma organização enfrenta. O que ela pode fazer é dar aos líderes de segurança mais controle sobre como seus gastos se traduzem em proteção real. Ao substituir o monitoramento manual e trabalhoso por uma defesa automatizada, as equipes ganham a capacidade de direcionar o orçamento existente para fortalecer a eficácia geral do programa de segurança que construíram — em vez de gastá-lo mantendo ferramentas que exigem atenção constante.

https://player.vimeo.com/video/1043470826?texttrack=pt

Assistir no Vimeo · Legendas: English, Français, Español, العربية