WHITE PAPER

Mitigação de riscos, prevenção e redução da cadeia de destruição

Minimize o impacto do ransomware com o Akamai Guardicore Segmentation

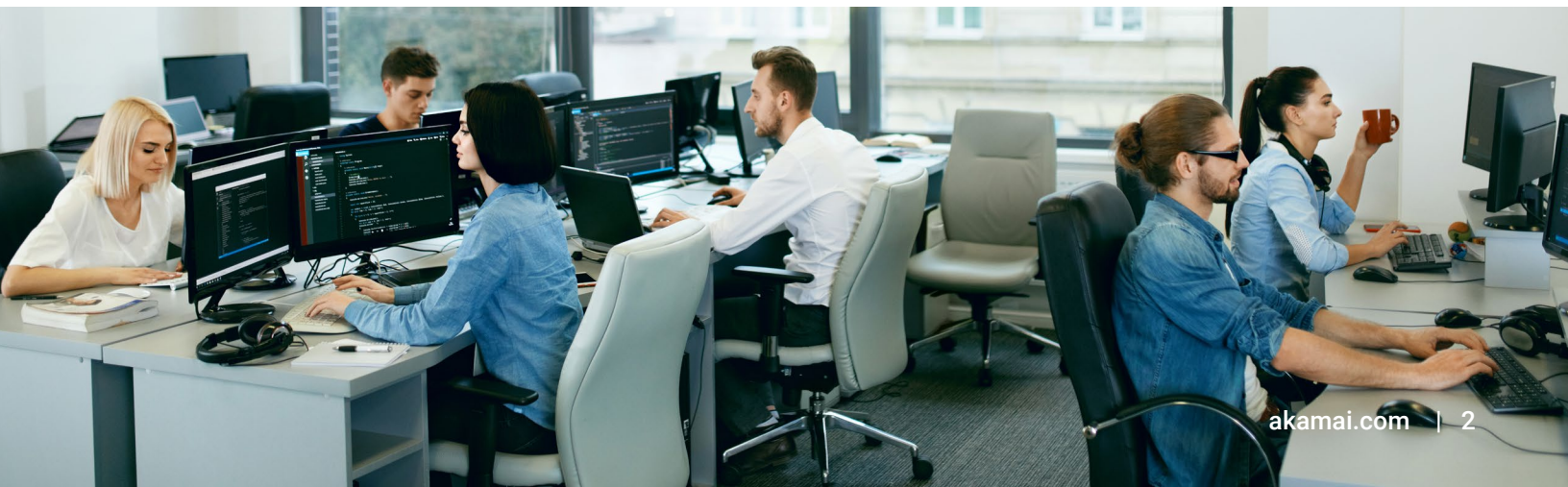
Visão geral

O ransomware, que antes era apenas um tipo incômodo de malware usado por cibercriminosos para restringir o acesso a arquivos e dados por meio de criptografia, se transformou em algo muito pior. Embora a ameaça de perda permanente de dados seja chocante, cibercriminosos e hackers de estado-nação se tornaram sofisticados o suficiente para usar ransomware para penetrar e prejudicar grandes empresas, governos federais, infraestrutura global e organizações de saúde.

O criptoworm WannaCry de 2017, que atingiu 230.000 computadores em todo o mundo ao explorar uma vulnerabilidade no Microsoft Windows, serviu como um marcador de alto perfil das ameaças que o ransomware apresenta. Desde então, os invasores se tornaram cada vez mais sofisticados e os ataques, mais difundidos. Isso inclui o surgimento do ransomware como serviço (RaaS), no qual os hackers vendem seus serviços. O relatório da Akamai sobre ameaças de ransomware, H1 2022, avaliou os padrões de ataque do Conti, um notório grupo RaaS que foi detectado pela primeira vez em 2020 e parece estar baseado na Rússia. A análise indica a necessidade de fortes proteções contra movimentos laterais e o papel crítico que essas proteções podem desempenhar na defesa contra ransomware. Além disso, descobriu que a esmagadora maioria das vítimas do Conti são empresas com receita de US$ 10 milhões a US$ 250 milhões.

> **A microssegmentação reduz a confiança implícita na rede, permitindo apenas a conectividade explicitamente definida pela política, reforçando assim o acesso com privilégios mínimos entre aplicações para tráfego máquina a máquina.**
>
> **— Forrester, Best Practices For Zero Trust Microsegmentation, 27 de junho de 2022**

É um sinal claro de que organizações de todos os tamanhos estão em risco devido a uma mistura de tecnologia desatualizada, estratégias de defesa "boas o suficiente" focadas apenas em perímetros e endpoints, falta de treinamento (e etiqueta de segurança inadequada) e nenhuma solução realmente eficaz conhecida. Na verdade, o relatório Cybersecurity Ventures Who's Who In Ransomware: 2023 Report prevê que até 2031, espera-se que um ransomware ataque uma empresa, consumidor ou dispositivo a cada dois segundos.



Depende do movimento lateral

Um ataque de ransomware começa com uma violação inicial, geralmente ativada por um e-mail de phishing, uma vulnerabilidade no perímetro da rede ou um ataque de força bruta que cria aberturas enquanto desvia as defesas da intenção real do invasor. Depois que o malware chega a um dispositivo ou aplicação. ele prossegue por meio de escalonamento de privilégios e movimento lateral, pela rede e vários endpoints para maximizar os pontos de infecção e criptografia. Os invasores normalmente assumem o controle de um controlador de domínio, comprometem credenciais e, em seguida, encontram e criptografam o backup para impedir que o operador restaure os serviços congelados.

O movimento lateral é fundamental para o sucesso de um ataque. Se o malware não puder se espalhar além de seu ponto de aterrissagem, é inútil; portanto, a prevenção do movimento lateral é essencial. Os recursos de visibilidade e segmentação em uma solução como o Akamai Guardicore Segmentation permitem configurar rapidamente políticas que impedem e contêm uma violação inicial. Você também será alertado sobre movimentos laterais e outros comportamentos suspeitos para ajudar a detectar malware antecipadamente, para que possa reagir imediatamente.

Parte 1: Quebrar a cadeia de destruição do ransomware, mitigação de risco e prevenção

O ransomware não se espalha violando uma única máquina ou dispositivo. Os cibercriminosos usam ransomware para criptografar o maior número possível de sistemas em uma rede para garantir que o resgate seja pago.

Como o ransomware é um ataque multifacetado, a implementação de várias camadas de defesa pode ajudar a evitar danos generalizados, perda de dados e tempo de inatividade. A primeira camada de defesa é tentar evitar a infecção inicial por ransomware.

A cadeia de destruição do ransomware

1. **Posição inicial**
   (Spear) Phishing ou serviços vulneráveis
2. **Movimentação lateral**
   Espalhado pela rede para obter o máximo de impactos
3. **Filtragem**
   Localizar e roubar dados valiosos
4. **Criptografia**
   PKI para criptografia para evitar quebra de código/ decodificação
5. **Nota de resgate**
   Papel de parede, e-mail, arquivo .txt de resgate etc.
6. **Impacto**
   Dados, financeiro, marca etc.

Prevenir infecção inicial

Os primeiros pontos vulneráveis para qualquer rede são seus pontos de contato com a Internet. Embora muitos ataques de ransomware dependam de spear phishing, nada os impede de violar seus serviços expostos à Internet.

Os recursos de visibilidade no Akamai Guardicore Segmentation permitem que você monitore os serviços expostos à Internet e limite sua exposição por meio de políticas para:

- Serviços de acesso remoto (RDP, SSH, TeamViewer, AnyDesk, VPNs)
- Serviços potencialmente vulneráveis (Apache, IIS, Nginx)
- Máquinas potencialmente vulneráveis (detectar máquinas com um sistema operacional não corrigido usando o recurso Insight adicional)
- Serviços expostos indesejados (bancos de dados, controladores de domínio, web internos ou servidores de arquivos)

Quebra da cadeia de destruição com segmentação

É inevitável que uma rede seja violada em algum momento. Isso pode ser causado por coisas como spear phishing, erro humano ou um servidor executando um serviço vulnerável que não foi mitigado adequadamente. É por isso que é fundamental ter estratégias adequadas de mitigação de riscos em vigor.

Depois que uma máquina é violada, você precisa limitar a propagação dentro da rede. Isso pode ser feito de três maneiras:

1. Segmentação por ringfencing de aplicações

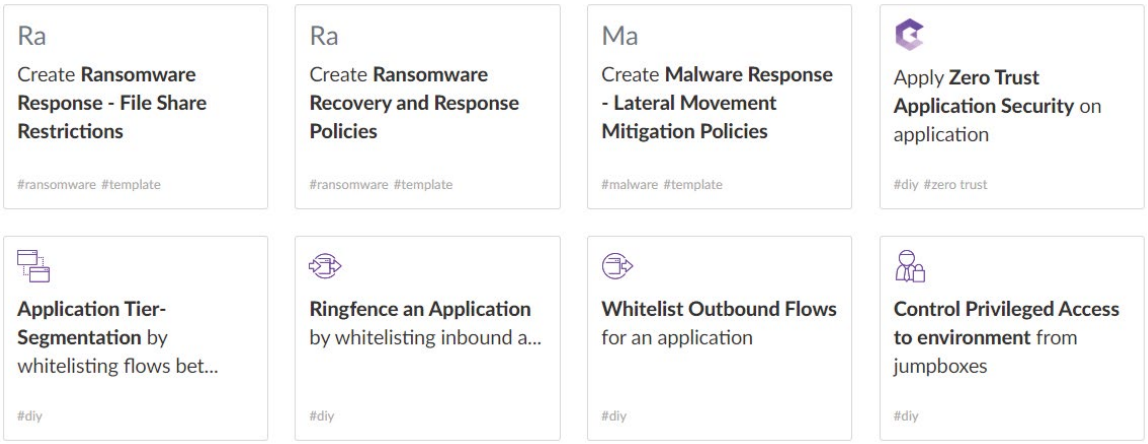
É necessário separar a rede em segmentos operacionais, por aplicação, uso ou ambiente, e impedir conexões desnecessárias entre e dentro desses segmentos.

Eis quatro diretrizes de segmentação a serem consideradas:

- Bloqueie qualquer comunicação entre notebooks/estações de trabalho.
- Bloqueie a comunicação de processos em execução com privilégios "poderosos" de usuários de domínio como administradores de domínio.
- Limite os usuários que podem executar processos nos servidores.
- Limite o acesso de notebooks/estações de trabalho a servidores de data center e instâncias de nuvem.

O Akamai Guardicore Segmentation facilita a proteção de sua rede contra ransomware. Usando modelos pré-construídos, você pode mitigar ataques definindo políticas em três etapas simples:

1. **Selecione sua meta,** como a delimitação de uma aplicação crítica, a criação de políticas de mitigação de ransomware ou a proteção de um diretório ativo.
2. **Identifique os ativos relevantes a proteger,** como os ativos de aplicação de E-commerce que você está buscando delimitar, todas as cargas de trabalho do diretório ativo no data center ou os pontos de extremidade para proteger contra a propagação de ransomware. Essa etapa, em muitos casos, é realizada automaticamente com a rotulagem de IA da Akamai.
3. **Proteger ativos criando políticas.** A IA do Akamai Guardicore Segmentation sugere e recomenda automaticamente políticas com base no tráfego real no ambiente e aprende os padrões de comunicação de aplicações em centenas de redes.

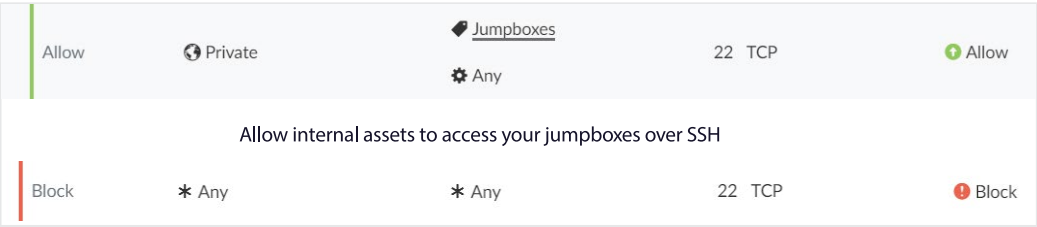


Exemplo: Modelos do Akamai Guardicore Segmentation

2. Prevenir a movimentação lateral com regras de restrição de protocolo

Há diretrizes gerais para protocolos e comportamentos específicos. Devido ao uso inerente de alguns protocolos nas operações diárias normais, eles devem ser restringidos com cuidado. O Akamai Guardicore Segmentation cria uma visualização de todo o tráfego para criar as regras mais precisas para o seu ambiente em torno de protocolos de alto risco, como WinRM, SMB, RPC, RDP, SSH e outros.

Por exemplo, embora o SSH seja útil para a administração remota e também sirva para tornar outros protocolos seguros (como o sFTP), ele também é uma ferramenta usada por invasores para violar máquinas e se propagar pela rede. Você vai querer restringir o SSH de toda a rede o máximo possível, criando jump boxes para usuários autorizados.



Regras criadas no Akamai Guardicore Segmentation

3. Proteger backups e serviços de dados críticos

Para maximizar os danos, os ataques de ransomware geralmente visam os servidores de backup da organização para criptografar os dados armazenados. Da mesma forma, os serviços de dados e os servidores de arquivos são alvos de ransomware.

Use o Akamai Guardicore Segmentation para limitar o acesso aos seus servidores de backup, bancos de dados e servidores de arquivos e para limitar o acesso de fora da rede e de regiões da rede que não precisam de acesso. Para minimizar a comunicação entre os servidores de backup críticos, você pode usar o Akamai Guardicore Segmentation para delimitar as aplicações e bloquear a comunicação entre uma aplicação aos níveis de processo e usuário. Limitar a exposição de seus serviços de dados apenas ao mínimo operacional vai reduzir o fator de risco desses serviços e mitigar a exposição ao ransomware e os caminhos de propagação.

Parte 2: Detecção e resposta de ransomware

Quando se trata de lidar com ciberameaças, como ransomware, o planejamento avançado e a vigilância são essenciais. Ao reagir rapidamente a uma violação, você pode minimizar os danos à sua rede. O Akamai Guardicore Segmentation tem recursos que podem ajudá-lo na detecção e resposta a ameaças.

Detecção de ameaças com o Akamai Guardicore Segmentation

Os incidentes podem incluir:

- **Dissimulação** – detecta e intercepta tentativas suspeitas de movimento lateral e as redireciona para os honeypots dinâmicos para que suas ações possam ser monitoradas e analisadas. Os incidentes de dissimulação são de alta fidelidade, fornecendo dados detalhados sobre atividades maliciosas e a próxima fase de ataque do cibercriminoso.
- **Verificações de rede** – os cibercriminosos reúnem inteligência uma vez que entram em uma rede. Eles usam verificações de rede como um método de reconhecimento para detectar portas abertas ou serviços que outros servidores estão atendendo. O Akamai Guardicore Segmentation detecta automaticamente verificações de rede e alerta os usuários imediatamente.
- **Detecção baseada em políticas** – As políticas de segurança nos níveis de rede e processo permitem o reconhecimento instantâneo de comunicações não autorizadas e tráfego não compatível.

O Akamai Guardicore Segmentation apresenta o recurso Insight

O Akamai Guardicore Segmentation pode fornecer visibilidade em ativos individuais, aproveitando um recurso adicional baseado em osquery. A estrutura de consulta que ele fornece pode detectar rapidamente atividades anômalas, como Volume Shadow Copy, a ação de pré-criptografia mais comum do ransomware. Ele também pode detectar cavalos de Tróia usados para distribuir ransomware, procurando por uma técnica de esvaziamento comum que oculta o malware sob o svchost.exe, um processo legítimo do Windows.

Busca gerenciada de ameaças

O serviço gerenciado de busca de ameaças Akamai Hunt alerta os usuários sobre qualquer comportamento anômalo dentro de sua rede. Isso é feito através de técnicas como analisar as conexões de entrada e saída da Internet e seu GeoIP associado, procurar novos executáveis que tenham presença de rede crescente, que podem indicar propagação, e analisar conexões de ativos para encontrar indicações de movimento lateral através de anomalias na contagem de vizinhos.

Resposta imediata

Depois de detectar uma ameaça como ransomware dentro de sua rede, você pode implantar rapidamente medidas de mitigação aplicando políticas nos níveis de processo e usuário para negar ativamente e isolar a ocorrência de atividades maliciosas.

Visibilidade incremental da infecção

Com seu lead inicial ou indicador de comprometimento (IOC), você pode começar a procurar indicadores adicionais, como padrões de comunicação, processos, portas usadas, ativos infectados e muito mais. O Akamai Guardicore Segmentation pode ajudar a encontrar todos os ativos com esse indicador (todos os ativos que se comunicam com o C2, todos os ativos que se comunicam com uma porta exclusiva ou todos os ativos que executam um processo malicioso). E com um mapa visual do seu ambiente, você pode procurar outras semelhanças em máquinas infectadas ou vestígios de propagação.

Parte 3: Desinfecção e recuperação

Depois de ter uma lista de todas as máquinas e IOCs infectados, você pode começar a desinfetar. Divida suas máquinas em três grupos de rótulos: **Isolado**, **monitorado** e **limpo**.

Isolados

- Ativos **infectados** por malware
- Mantenha esses ativos em **quarentena** até que o malware seja removido

Monitorados

- Ativos que podem ou não estar **infectados**
- **Monitore** até ter certeza de que o malware foi **removido**

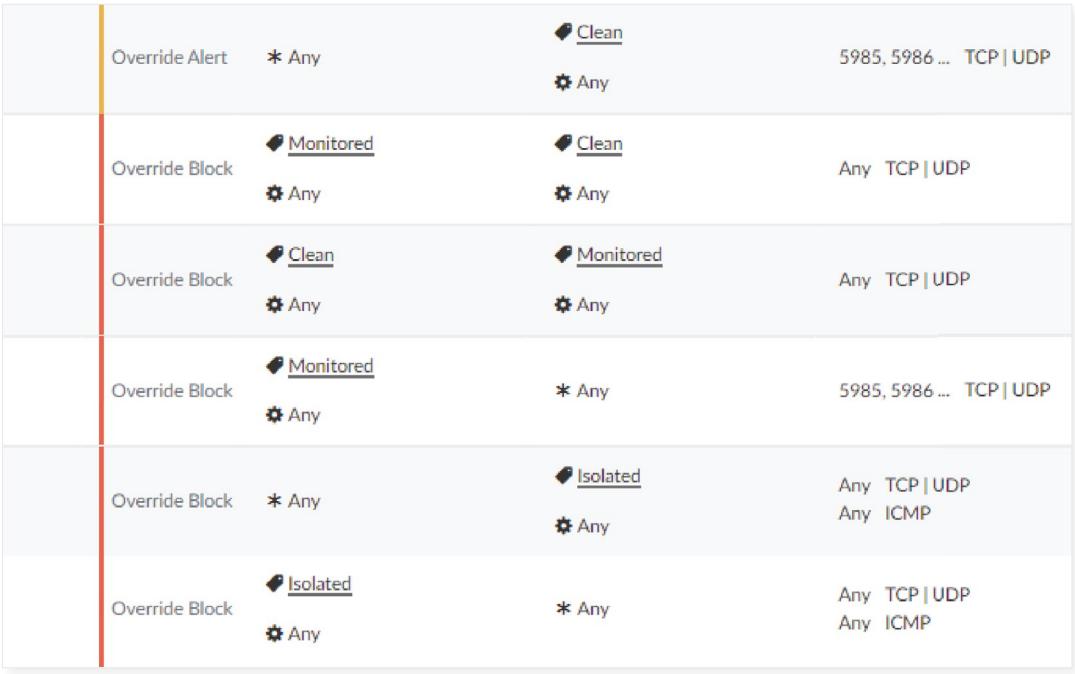
Limpos

- Ativos verificados como **não infectados** e podem **funcionar normalmente**

Diretrizes de segmentação para recuperação

Depois de definir os três grupos de rótulos, você pode começar a adicionar políticas para segmentar sua rede criando quatro níveis de comunicação:

- **Bloquear** todas as comunicações de entrada e saída de máquinas **Isoladas**.
- **Bloquear** a comunicação do protocolo de gerenciamento remoto de e para máquinas **Monitoradas**.
- **Alerta** sobre qualquer comunicação de protocolo de gerenciamento remoto para máquinas **Limpas**.
- **Bloquear** todas as comunicações entre os grupos de rótulos.



Regras de bloqueio e alerta no Akamai Guardicore Segmentation

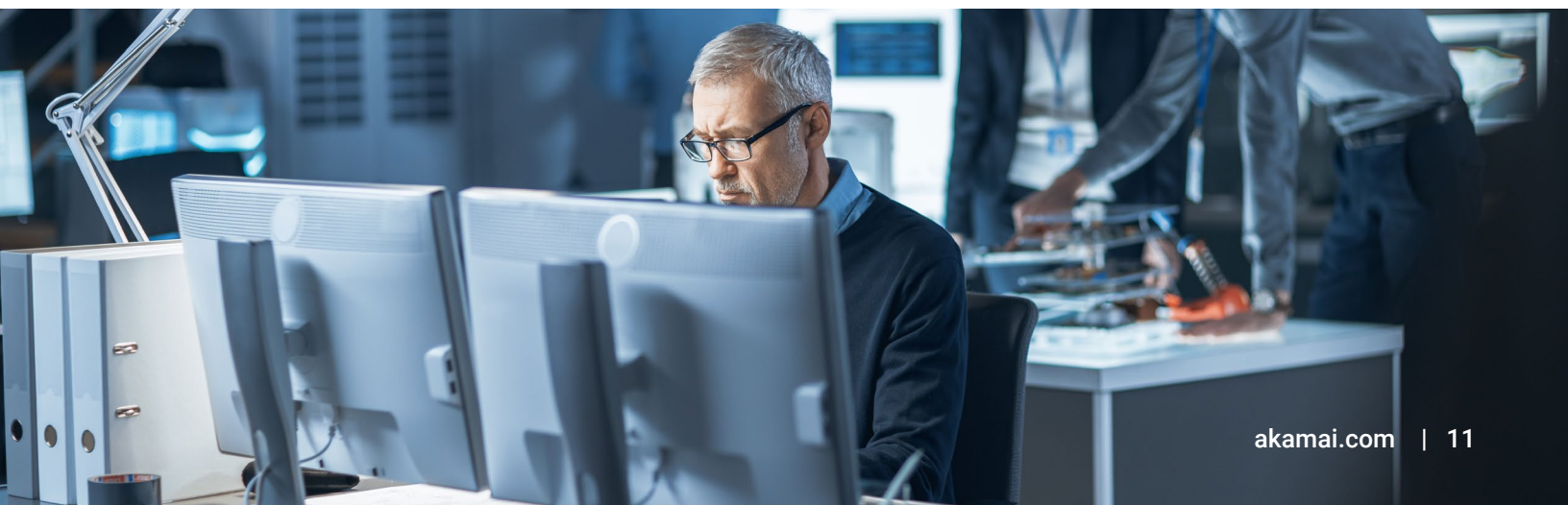
Modelo de recuperação e resposta ao ransomware

O modelo Ransomware Recovery and Response Policies incluído no Akamai Guardicore Segmentation fornece uma política pré-criada e fácil de usar para restringir o acesso nos rótulos **Isolados**, **Monitorados** e **Limpos**.

Este modelo permitirá que você mantenha facilmente a continuidade operacional de máquinas **limpas** sem temer a (re)infecção de máquinas **isoladas**.

Conclusão

Se você ainda confiar em firewalls legados ou em defesa somente de perímetro, talvez não consiga impedir que o ransomware se espalhe pela sua rede e bloqueie aplicações e infraestrutura críticas. A realidade é que as violações são inevitáveis e você precisa estar preparado. O Akamai Guardicore Segmentation pode ajudar você a detectar as ameaças no tráfego leste-oeste do data center e bloquear o movimento lateral do qual o ransomware depende para criptografar e resgatar seus ativos mais críticos.



Cinco etapas para mitigar o impacto de um ataque de ransomware com o Akamai Guardicore Segmentation

Prepare-se identificando cada aplicação e ativo em execução em seu ambiente de TI.

Evite criando regras para bloquear técnicas comuns de propagação de ransomware.

Detecte recebendo alertas para qualquer tentativa de acesso a aplicações segmentadas e backups.

Corrija iniciando medidas de contenção e quarentena de ameaças quando um ataque for detectado.

Recupere com recursos de visualização que suportam estratégias de recuperação em fases.

Interrompa o movimento lateral do ransomware em sua rede. Não acredita em nós? Veja você mesmo. akamai.com/guardicore

A Akamai protege sua experiência do cliente, sua força de trabalho, seus sistemas e seus dados, ajudando a incorporar a segurança em tudo o que você cria, em qualquer lugar que você crie e entregue. A visibilidade da nossa plataforma em relação às ameaças globais nos ajuda a adaptar e desenvolver sua postura de segurança para permitir Zero Trust, interromper ransomware, proteger apps e APIs ou combater ataques DDoS, dando a você a confiança para inovar, expandir e transformar continuamente o que é possível. Saiba mais sobre as soluções de segurança, computação e entrega da Akamai em akamai.com e akamai.com/blog ou Akamai Technologies no Twitter e LinkedIn. Publicado em 05/23.