WHITE PAPER

Como quebrar a cadeia de destruição do ransomware com o Akamai Enterprise Security Suite

Sumário

Introdução

Elimine o ransomware em várias etapas da cadeia de destruição usando as soluções de segurança corporativa da Akamai

Uma das maiores ameaças de segurança que as organizações enfrentam hoje é o ransomware, uma forma de malware projetada para criptografar arquivos importantes em um dispositivo, tornando-os inutilizáveis. Os operadores de malware exigem um resgate em troca de uma chave de descriptografia ou software que possa restaurar os arquivos para seus dados originais. Nos últimos anos, os grupos de criminosos de ransomware evoluíram suas táticas e começaram a exfiltrar os dados de suas vítimas para serem usados como alavancagem adicional, ameaçando vazá-los publicamente ou vendê-los na dark web.

Para conseguir se defender contra esse tipo de ataque, é importante que os defensores entendam a forma como os grupos de ransomware operam para atingir seus objetivos. Este documento ajudará você a fazer exatamente isso.

Entendendo a cadeia de destruição do ransomware

Os ataques de ransomware são complexos: invadir o sistema é apenas o começo. Para maximizar os danos, um invasor também deve espalhar sua carga mal-intencionada pela rede antes de iniciar a criptografia. Se apenas um único computador for criptografado, o invasor não terá vantagem suficiente para exigir um resgate. Para que o ataque de ransomware seja bem-sucedido, o invasor deve executar várias etapas: descobrir ativos de rede, se mover lateralmente etc. Essas etapas geralmente são chamadas de cadeia de destruição do ransomware.

Cada etapa dessa cadeia abre muitas oportunidades de detecção e mitigação. Preparar sua rede com antecedência com o pacote de segurança empresarial da Akamai pode reduzir sua superfície de ataque e ajudar a mitigar e conter quaisquer possíveis danos causados por ransomware antes mesmo de você estar ciente de que foi atingido. Este documento detalhará como você pode usar a Akamai Guardicore Segmentation, o Enterprise Application Access e o Secure Internet Access para detectar e bloquear atividades de ransomware nas diferentes etapas da cadeia de destruição:

Acesso inicial

A primeira fase do ataque, onde os invasores violam a rede interna pelo lado de fora

Descoberta

Métodos de descoberta que os invasores usam para identificar ativos importantes dentro da rede

Movimento lateral

A fase em que os invasores se espalham pela rede e comprometem ativos adicionais

Comando e controle

As diferentes maneiras pelas quais os invasores mantêm um canal de comunicação na rede para enviar informações e comandos para ativos comprometidos

Exfiltração

Métodos usados por invasores para exfiltrar dados confidenciais roubados de maneira oculta

Acesso inicial

Todas as organizações têm muitas interfaces com a Internet. Os invasores tentarão abusar de cada uma delas para obter acesso à rede. A Akamai permite que você proteja perfeitamente essas interfaces e mantenha os invasores fora de sua rede.

Proteger os servidores voltados para a Internet

Use os recursos de análise de carga útil do Secure Internet Access para proteger os servidores voltados para a Internet contra exploração

De acordo com a Kaspersky, o método mais comum que os invasores usam para obter o acesso inicial é a exploração de aplicações voltadas para a Internet, muitas vezes abusando de vulnerabilidades de dia um em sistemas não corrigidos. Vulnerabilidades como Log4Shell (CVE-2021-44228) e Proxylogon (CVE-2021-26855) ainda estão sendo exploradas no ecossistema hoje para violar redes e implantar ransomware.

O Enterprise Threat Protector pode ser configurado para monitorar todo o tráfego da Web recebido em seus servidores conectados à Internet; esse tráfego é analisado e qualquer atividade mal-intencionada ou irregular pode ser identificada e bloqueada.

Bloquear URLs de phishing

Use os recursos de inspeção de URL do Enterprise Threat Protector para detectar e bloquear tentativas de phishing

Phishing é uma maneira muito comum de violar redes. Os invasores geralmente enviam e-mails contendo links para anexos mal-intencionados ou páginas de login falsas projetadas para roubar credenciais. O uso do cliente do Enterprise Threat Protector em seus endpoints permitirá que você verifique cada um dos URLs em que seus usuários clicam em tempo real, identificando links maliciosos ou anômalos e bloqueando-os.

Reduzir a superfície de ataque VPN

Use o Enterprise Application Access para permitir acesso VPN seguro e específico a aplicações e reduzir a superfície de ataque externo

No ambiente de trabalho híbrido atual, que geralmente inclui trabalho remoto, está se tornando mais comum permitir que os usuários usem uma VPN para fazer login na rede corporativa. Os invasores se adaptaram a isso e começaram a explorar essa oportunidade para obter acesso à rede interna. Os invasores costumam atacar os computadores pessoais dos funcionários, comprometendo suas credenciais de VPN e usando-as para acessar a rede interna. Em alguns casos, os invasores também atacarão servidores vulneráveis para vazar credenciais. Em novembro de 2022, os invasores abusaram de uma vulnerabilidade nos servidores VPN Fortinet para obter acesso inicial e, em seguida, passaram a espalhar ransomware para toda a rede.

O Enterprise Application Access possibilita reduzir esse risco de forma significativa, permitindo o acesso à rede com base em funções e aplicações específicas, ele não concede aos usuários acesso total a toda a rede, como as VPNs tradicionais, mas permite apenas o acesso limitado a aplicações específicas. Dessa forma, mesmo que um invasor comprometa as credenciais do usuário e ignore a proteção MFA, ele ainda não terá acesso à rede, apenas a um conjunto limitado de aplicações.

Comando e controle

Bloquear servidores de comando e controle (C2)

Use o Akamai Secure Internet Access para bloquear servidores de comando e controle de malware conhecidos

O malware em geral e o ransomware em particular exigem a comunicação com servidores externos C2 para enviar comandos e recuperar informações de ativos infectados. Ao analisar os extensos dados de comunicação da Akamai, podemos monitorar os domínios de ransomware e malware C2 e acompanhar as campanhas novas e em evolução. O cliente do Enterprise Threat Protector nos permite monitorar toda a sua comunicação DNS em tempo real e bloquear a comunicação com domínios maliciosos, impedindo que o malware seja executado adequadamente e atinja seus objetivos.

Descoberta

Depois que os invasores violam a rede, eles tentam identificar ativos adicionais para entender sua estrutura antes de começar a se mover lateralmente. Isso muitas vezes resultará em comunicação interna, que pode ser detectada pela Akamai Guardicore Segmentation.

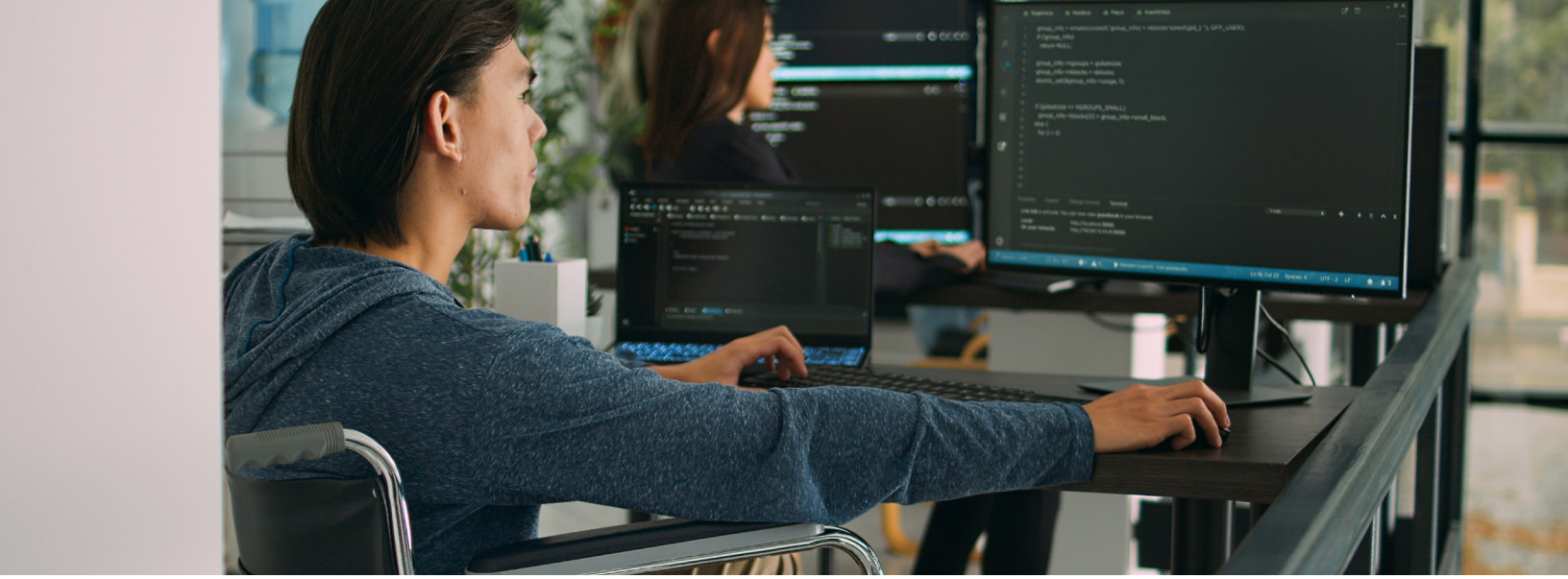
Identificar varreduras de rede

> Use os detectores da Akamai Guardicore Segmentation para identificar varreduras de rede suspeitas

Um dos métodos comuns que os invasores usam para descoberta de rede é o uso da varredura de portas para identificar serviços de rede. Muitos grupos de ransomware são vistos usando varreduras de rede de código aberto. Em um recente comunicado da CISA sobre o ransomware LockBit 3.0, o grupo mostrou estar usando o "SoftPerfect Network Scanner" para realizar a varredura de portas. Outro exemplo é o grupo de ransomware Nokoyawa que foi observado examinando redes em busca de servidores SQL para acessar dados confidenciais neles.

A Akamai Guardicore Segmentation monitora toda a comunicação em sua rede e tem detectores integrados que identificarão e alertarão sobre essas varreduras, permitindo que você interrompa a disseminação do malware antes que ela comece.

Fig. 1: incidentes de varredura de rede na Akamai Guardicore Segmentation



Fraude contra descoberta

Use a Akamai Guardicore Segmentation para identificar tentativas de descoberta

Quando os invasores violam uma rede, eles não têm conhecimento prévio de sua estrutura e dos diferentes ativos nela contidos. Para superar essa lacuna, eles terão que "sondar no escuro" e tentar encontrar o caminho manualmente. A Akamai Guardicore Segmentation permite que você aproveite isso usando o serviço de enganação, atraindo invasores para servidores honeypot, monitorando suas atividades e alertando-o quando anomalias forem detectadas.

Por exemplo, um invasor viola a rede e tenta forçar as credenciais SSH de um servidor Linux. A Akamai Guardicore Segmentation identificará essa anomalia e encaminhará o invasor para um honeypot gerado dinamicamente. Uma vez dentro do honeypot, todas as ações do invasor são registradas e um alerta é gerado.

Veja a seguir um exemplo de um desses alertas:

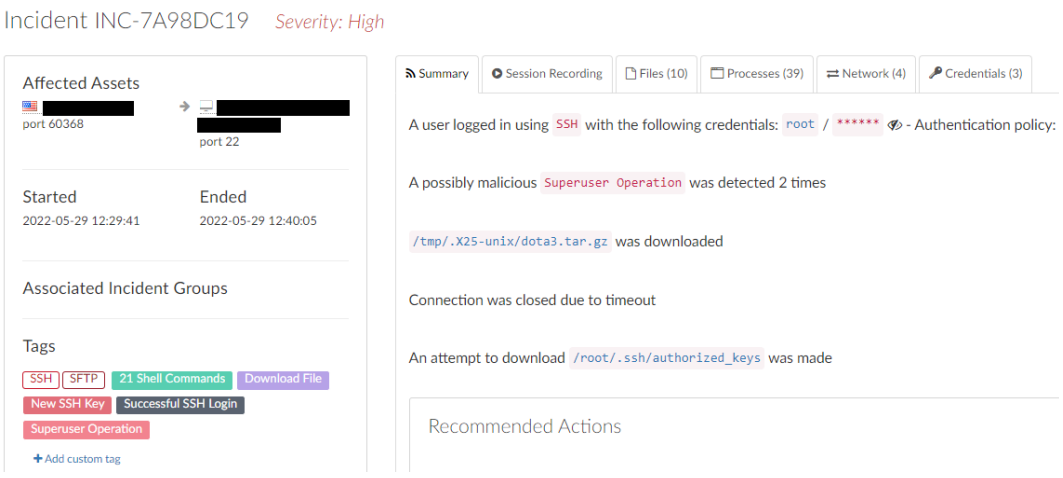


Fig. 2: incidente de enganação na Akamai Guardicore Segmentation

Movimentação lateral

Depois que um invasor obtém acesso à rede e se familiariza com sua topologia, ele deseja usá-la para se deslocar lateralmente. Os grupos de ransomware modernos violarão uma rede e, em seguida, se moverão lateralmente para comprometer o máximo de ativos possível, criptografando todos eles. Os produtos de segurança corporativa da Akamai permitem que você limite as possibilidades de movimento lateral e minimize o escopo da violação.

Identificar indicadores suspeitos do host

> Use o módulo Akamai Guardicore Segmentation Insight para identificar indicadores suspeitos de host de várias maneiras

Os invasores usam as ferramentas PowerShell para atingir uma variedade de metas. Uma delas é realizar movimentos laterais. Os droppers do PowerShell são muito comuns, e os invasores geralmente os usam como a primeira parte do código que executam em um ativo comprometido. As infecções recentes do ransomware Quantum mostraram estar fazendo exatamente isso – executando o código PowerShell em WMI (Windows Management Instrumentation).

Usando o módulo Insight da Akamai Guardicore Segmentation, você pode executar consultas agendadas para verificar o log de eventos do PowerShell em todos os seus ativos, rotulando ativos com indicadores mal-intencionados e colocando-os em quarentena.

Fig 3: criar uma consulta do Insight programada para detectar PowerShell mal-intencionado

Mas o PowerShell é apenas um exemplo. O Insight pode ser aproveitado para examinar uma ampla variedade de indicadores de movimento lateral, usando qualquer uma das tabelas de consulta do osquery existentes, por exemplo:

- Use a tabela de Arquivo para detectar arquivos de malware com base em nomes ou hashes
- Use a tabela de Itens de inicialização para detectar entradas suspeitas de execução automática em seus ativos
- Use a tabela Yara para verificar arquivos em seus ativos usando as regras yara para detectar cepas de malware

Bloquear ataques de LAN

Use a Akamai Guardicore Segmentation para bloquear e detectar ataques em protocolos de rede locais

Depois de violar o paciente zero na rede, os invasores abusam das vulnerabilidades nos protocolos de LAN, como ARP, para comprometer outros ativos. Usando um firewall tradicional, esses ataques podem facilmente ficar fora do âmbito do radar, como são executados na Camada 2 — e esse tipo de comunicação não atinge o firewall.

A abordagem baseada em software da Akamai Guardicore Segmentation permite monitorar e bloquear todo o tráfego que entra ou sai de um ativo, mesmo o tráfego local que normalmente não atingiria o firewall obrigatório.

Restringir portas de gerenciamento

Use a Akamai Guardicore Segmentation para criar uma política de nível de processo para reduzir a superfície de ataque sobre portas sensíveis

Uma vez dentro da rede, os invasores normalmente executarão o escalonamento de privilégios em ativos comprometidos com a finalidade de roubar credenciais. Depois que as credenciais forem obtidas, os invasores geralmente usarão protocolos de gerenciamento como RDP, RPC, SMB e WinRM, para executar uma carga de ransomware em todos os ativos da rede. No entanto, o bloqueio total dessas portas geralmente não é uma opção viável, pois os administradores as exigem para operações regulares.

A Akamai Guardicore Segmentation permite que você aplique a política no nível do processo, permitindo que você determine quais processos devem estar se comunicando por portas de gerenciamento confidenciais. Vamos examinar o WinRM, ele é usado por muitos programas de administração, incluindo o Ansible. No entanto, ele também é frequentemente abusado por invasores com ferramentas como o Evil-WinRM para realizar movimentos laterais. Com a Akamai Guardicore Segmentation, podemos criar uma política para permitir conexões WinRM de entrada somente de processos Ansible, bloqueando outros processos pela mesma porta:

Section	Source	Destination	Ports/Protocols	Action
Allow	ansible-operator	Windows Any	5985 TCP | UDP	Allow
Block	* Any	Windows Any	5985 TCP | UDP	Block

Fig. 4: exemplo da política da Akamai Guardicore Segmentation para limitar a comunicação com o WinRM

Exfiltração

Nos últimos anos, os invasores adaptaram suas táticas de extorsão e começaram a vazar arquivos confidenciais de suas vítimas para serem usados como alavancagem adicional. Os invasores tentarão se misturar com o ruído da rede à medida que eles exfiltram os dados da organização, mas eles muitas vezes ainda podem ser detectados e bloqueados durante essa fase.

Bloquear domínios de exfiltração

Use a Akamai Guardicore Segmentation para limitar o acesso a serviços que podem ser usados para a exfiltração de dados

Os invasores geralmente usam ferramentas públicas para vazar dados da rede, sendo uma opção muito comum os serviços de hospedagem pública, como MEGA, Dropbox e Google Drive. O desafio de monitorar esses domínios é que eles são comumente usados legitimamente dentro da rede. Por exemplo, acessar o domínio MEGA por meio de um navegador pode ser considerado legítimo, mas fazê-lo usando o utilitário rclone, que está sendo usado ativamente por vários grupos de ataque para exfiltrar dados seria considerado mal-intencionado.

Com a Akamai Guardicore Segmentation, podemos minimizar o risco de tais ferramentas bloqueando seus domínios de todos os endpoints que não exigem acesso a eles e permitindo apenas o acesso por meio de aplicações aprovadas, como navegadores.

Defesa multicamadas

Para atingir sua meta mais desejada, os invasores precisam passar por várias fases de ataque diferentes. Cada etapa oferece uma chance para que os defensores bloqueiem e detectem a atividade mal-intencionada associada. Usando os diferentes produtos de segurança da Akamai, os defensores podem empregar mitigações em cada etapa de uma cadeia de destruição de ransomware, impedindo os invasores em seus caminhos e detectando qualquer comportamento irregular.

Para obter mais informações sobre a Akamai Guardicore Segmentation ou para solicitar uma demonstração personalizada do produto, acesse akamai.com/guardicore