INTERROMPER ATAQUES DIRIGIDOS SEM FAZER A DECRIPTAÇÃO DO TRÁFEGO

Resumo executivo

Atores de ameaças são astuciosos. Eles usam uma série de técnicas para mascarar seus ataques e evitar a detecção. Com o tráfego HTTPS agora responsável por mais de dois terços de todo o tráfego da Web,[1] a criptografia tornou-se seu método de escolha para contornar as defesas corporativas. A criptografia é apenas uma das muitas táticas evasivas que os invasores têm em suas mangas coletivas; eles também codificam o conteúdo de tráfego, compactam e empacotam arquivos e empregam muitas outras técnicas para passar sorrateiramente pelos controles de segurança.

A análise comportamental do Magnifier™, um aplicativo baseado em nuvem da Palo Alto Networks® Application Framework, capacita as organizações a detectar e interromper ataques ativos. O Magnifier estabelece um perfil comportamental do usuário e do dispositivo analisando os metadados da rede para descobrir os sinais indicadores de intrusões. No entanto, ele não precisa inspecionar o conteúdo do tráfego, por isso é impenetrável pelas técnicas de criptografia e obscurecimento.

Este documento descreve como o Magnifier detecta ataques em andamento e como ele funciona em conjunto com a Security Operating Platform da Palo Alto Networks para erradicar ameaças no tráfego criptografado

1. Façamos a criptografia com a telemetria do Firefox, https://letsencrypt.org/stats

A ascensão da criptografia SSL

Com o uso da Secure Sockets Layer (Camada de Soquetes Seguros) ou SSL, a criptografia[2] explodiu na última década, todo o tráfego da Internet cresceu de aproximadamente 26% em janeiro de 2014 para 69% em fevereiro 2018.[3] As crescentes preocupações com a privacidade e os incentivos do setor para adotar a criptografia motivaram os proprietários de aplicativos de todos os tamanhos a criptografarem o acesso aos sites. Além disso, a rápida proliferação de certificados SSL, gratuitos e de baixo custo, deixou a criptografia ao alcance de praticamente todos os desenvolvedores da web.

Embora a adoção da SSL aumente a privacidade e a segurança, ela também permite que os agentes de ameaças ocultem sua atividade mal-intencionada no tráfego criptografado. Para proteger os ativos corporativos, as organizações precisam de uma maneira robusta de detectar e bloquear ameaças ocultas nas comunicações SSL.

Abordagem da Palo Alto Networks para Proteger o Tráfego Criptografado

Para garantir que nenhum ataque permaneça sem ser detectado, a Palo Alto Networks desenvolveu várias tecnologias para inspecionar e proteger todas as comunicações, incluindo o tráfego criptografado. Essas tecnologias incluem:

Análise comportamental

Depois que os invasores se infiltram em uma rede, eles devem executar uma série de etapas para localizar e roubar ou destruir dados. A análise comportamental do Magnifier monitora a atividade da rede para criar um perfil comportamental e detectar anomalias indicativas de intrusões.

Como o Magnifier analisa os metadados da rede em vez do conteúdo real, ele pode detectar ataques avançados sem precisar da decriptação.

Decriptação SSL de alto desempenho

Para inspecionar cada pacote, os firewalls de última geração podem fazer a decriptação do tráfego HTTPS em altas velocidades. Com suporte de opções flexíveis de implantação, os firewalls de última geração podem fazer a decriptação do tráfego SSL de entrada ou de saída ou atuar como agentes de decriptação SSL.

Com firewalls de última geração, as organizações podem usar a decriptação seletivamente no tráfego por aplicativo, categoria ou usuário.

Proteção avançada de endpoint

Os ataques ocultos no tráfego HTTPS acabam visando os endpoints e seus dados.

A proteção avançada de endpoint Traps™ usa vários métodos de prevenção para interromper explorações e malware, antes que possam comprometer máquinas corporativas. Integra-se à segurança na nuvem e na rede para análise de ameaças, inteligência compartilhada e contenção automatizada.

A Security Operating Platform da Palo Alto Networks fornece proteção máxima contra ataques cibernéticos, enquanto elimina os pontos cegos que o tráfego criptografado pode introduzir.

Detecção de ameaças internas sem fazer a decriptação do tráfego

Quando os invasores obtêm acesso à rede da vítima, eles podem usar várias técnicas evasivas para escapar dos controles de segurança. Em vez de depender de malware, eles podem aproveitar utilitários comuns, como PowerShell® ou ferramentas nativas do sistema, para explorar uma rede comprometida e transferir dados. Os invasores podem roubar credenciais e se movimentar de um endpoint para outro sem necessariamente violar as políticas de segurança ou ativar os alarmes internos.

No entanto, os invasores inevitavelmente se trairão à medida que realizam reconhecimento e ampliam sua presença na rede, porque suas ações se desviarão do comportamento passado e do comportamento de outros usuários ou dispositivos na rede. Na medida em que tentam explorar a rede e controlar outros dispositivos, eles acessam novos destinos, usam novos protocolos, fazem login em sistemas com contas incomuns de usuário e exibem outras mudanças comportamentais que revelam sua má intenção.

A análise comportamental do Magnifier™, um aplicativo baseado em nuvem para o Palo Alto Networks® Application Framework, detecta automaticamente anomalias comportamentais dos ataques ativos. O Magnifier examina os dados qualitativos da rede, endpoint e armazenados na nuvem com o Logging Service da Palo Alto Networks para identificar ataques direcionados, usuários internos mal-intencionados e endpoints comprometidos com uma precisão incomparável (consulte a Figura 1). Ele também simplifica as investigações, fornecendo um pequeno número de alertas acionáveis, num contexto em que os analistas de segurança precisam confirmar e responder aos ataques.

2. Referências neste artigo à criptografia SSL também se aplicam ao Transport Layer Security (Segurança da camada de transporte) ou TLS, o sucessor do SSL.
3. Façamos a criptografia com a telemetria do Firefox, https://letsencrypt.org/stats/

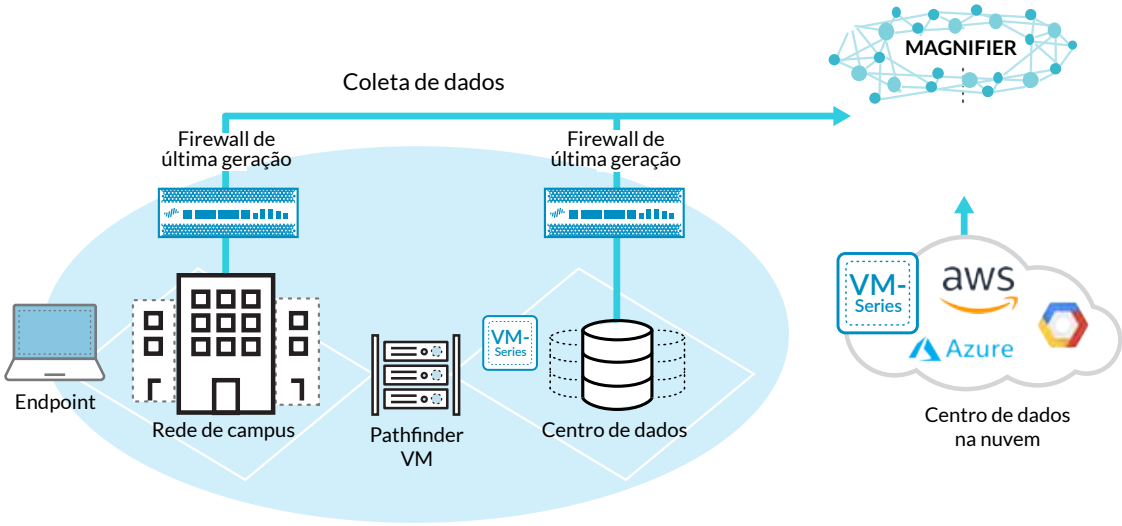

Figura 1: O Magnifier analisa os dados armazenados no Logging Service da Palo Alto Networks a partir do Security Operating Platform para gerar um perfil comportamental e detectar ataques

Projeto à prova de evasão

Em vez de procurar assinaturas do ataque, o Magnifier estabelece um perfil comportamental do usuário e do dispositivo para detectar anomalias indicativas de um ataque. Sua robusta detecção de ataques é baseada não no conteúdo transferido, mas nos atributos da comunicação, incluindo qual usuário e host iniciaram uma conexão, qual destino eles acessaram e qual protocolo eles usaram.

Como o Magnifier não foi projetado para detectar padrões de rede predefinidos, como o comportamento de famílias específicas de malware, os invasores não conseguem contornar facilmente os algoritmos de detecção do Magnifier alterando o tamanho dos pacotes ou explorando o código. Por meio de aprendizagem dinâmica do comportamento de usuários e dispositivos na rede, o Magnifier detecta mudanças comportamentais que os invasores não conseguem mascarar. Por exemplo, se um invasor se movimentar lateralmente de um host para o outro, o invasor não conseguirá evitar a comunicação entre as máquinas.

O Magnifier detecta comportamentos de ataque baseados na rede que são impossíveis de ocultar, mesmo em tráfego criptografado.

Ao caracterizar muitas dimensões diferentes de comportamento, o Magnifier pode detectar irregularidades, como um usuário padrão conectando-se a vários sistemas raramente acessados ou tentando gerenciar computadores remotos, o que indica que um ataque está em andamento.

Como o Magnifier analisa metadados de rede e não transfere conteúdo ou cargas úteis, ele pode descobrir ameaças de rede mesmo em ambientes onde o tráfego está criptografado.

Detecção de um ataque em andamento em qualquer estágio com análise comportamental

Depois que os agentes de ameaças se infiltram em uma rede, eles podem aproveitar seu acesso para explorar o entorno circundante e expandir seu campo de controle até atingir seu objetivo final: roubar, manipular ou destruir dados confidenciais.

O Magnifier detecta cada passo dos agentes de ameaça quando e depois que eles entram na rede:

Movimentação lateral: Para localizar dados confidenciais e manter uma presença persistente na rede, os invasores roubam credenciais, realizam reconhecimento e assumem o controle de vários endpoints. O Magnifier monitora o tráfego de rede para modelar o comportamento esperado e detectar desvios indicativos de ataques. O Magnifier estabelece um perfil comportamental do usuário e do dispositivo analisando os metadados em nível de protocolo, coletados pelos firewalls de última geração da Palo Alto Networks.

Analisando dados de rede coletados de firewalls de última geração, incluindo registros aprimorados de aplicativos e logs de tráfego com dados da tecnologia User-ID™ e App-ID™, o Magnifier pode detectar movimentação lateral e reconhecimento que os invasores não conseguem evitar ou ocultar.

Atividade de comando e controle: O Magnifier reconhece o comportamento de rede associado ao comando e controle, ou C2, como conexões repetidas a sites raramente acessados ou muitas pesquisas de DNS com falha. Consequentemente, o Magnifier pode detectar ataques sem inspecionar o conteúdo transferido.

Além disso, como os firewalls de última geração da Palo Alto Networks podem extrair a indicação de nome de servidor e outros dados pertinentes do tráfego criptografado e apresentar esses dados em logs de aplicativos aprimorados, o Magnifier pode detectar o tráfego C2 mesmo quando as conexões com servidores C2 são criptografadas.

Transferência não autorizada de dados: Depois que os invasores obtêm dados confidenciais, eles precisam transferi-los para fora da rede. O Magnifier examina conexões de saída e detecta grandes uploads para sites raramente acessados ou para aqueles que usam protocolos incomuns.

Como o Magnifier se concentra na quantidade de dados enviados, no número de porta, na popularidade do destino e em outros atributos do site de destino, o Magnifier pode detectar transferência não autorizada, mesmo quando o tráfego carregado é criptografado ou o conteúdo é ofuscado.

Endpoints comprometidos: Usando o serviço de análise de endpoint Pathfinder, o Magnifier pode descobrir malware em execução nos endpoints.

Como o Pathfinder faz a varredura diretamente nos endpoints para verificar os processos em execução e, em seguida, examina-os com o serviço de análise de ameaça baseado na nuvem do WildFire®, ele não é afetado pela criptografia em nível de rede.

Como o Magnifier caracteriza perfis comportamentais quando o tráfego está criptografado

O Magnifier detecta ataques mesmo quando os agentes de ameaças tentam usar criptografia ou obscurecimento para evitar a detecção. A criptografia em nível de aplicativo não afeta a precisão dos algoritmos de detecção de ataque do Magnifier pelas razões que seguem.

Análises de informações em nível de rede

O Magnifier analisa principalmente informações no nível da rede, como fonte de tráfego, destino, domínio, protocolo, número de porta e volume, que podem ser obtidas de cabeçalhos de pacote, mesmo quando o conteúdo no nível do aplicativo é criptografado. Por exemplo, se um invasor tentar mapear a rede para localizar servidores com dados valiosos, o invasor não poderá evitar conexões anormais de rede.

O Magnifier analisa dados coletados por firewalls de última geração para rastrear o comportamento normal de usuários e dispositivos, incluindo os sistemas que eles acessam, os protocolos usados, a quantidade de tráfego que eles enviam e recebem e muitas outras dimensões comportamentais. Se o Magnifier detectar atividade incomum, como solicitações para muitas portas diferentes em um host, incluindo portas que sejam anômalas para um usuário e seus pares – isso gerará um alerta. O Magnifier pode detectar ataques sem inspecionar o conteúdo do aplicativo, portanto, ele não é afetado pela criptografia no nível do aplicativo (veja a Figura 2).

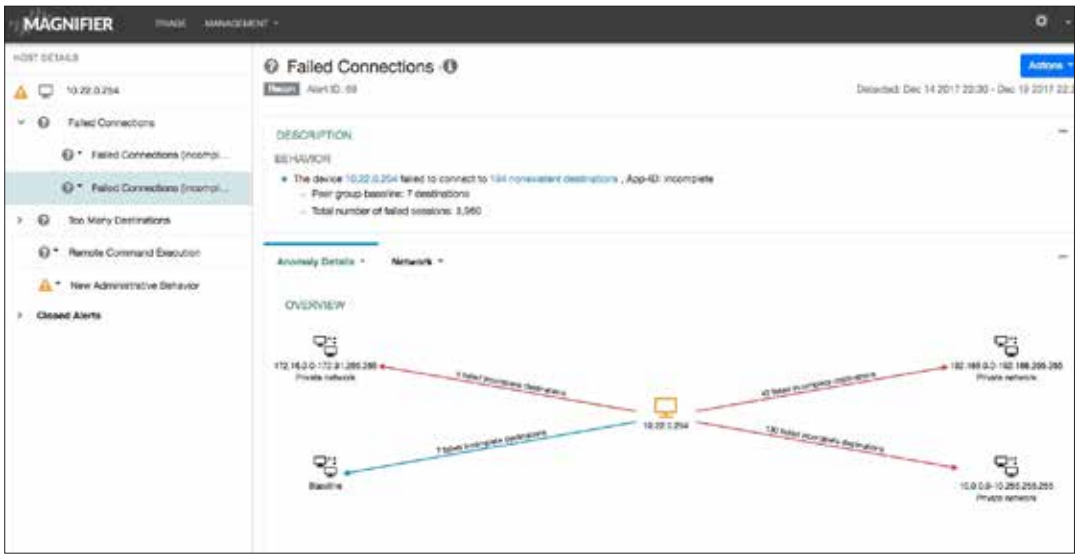

Figura 2: O Magnifier detecta varreduras de porta de rede, mesmo se cada solicitação for criptografada

Simplifica esforços de caça às ameaças

O Magnifier foi totalmente projetado para simplificar os esforços de caça às ameaças. Para esse fim, ele gera um pequeno número de alertas precisos e acionáveis com o contexto do usuário, endpoint e aplicativo. Embora a criptografia não cause impacto nos recursos de detecção do Magnifier, a criptografia pode, em alguns casos, afetar a quantidade de detalhes registrados nos alertas. Quando o tráfego está criptografado, os alertas do Magnifier ainda incluem informações sobre o dispositivo, o usuário, o número de porta e o processo de endpoint ou o arquivo executável associado ao ataque, além de informações sobre o domínio. No entanto, os alertas podem não listar o URL, o agente navegador ou o cabeçalho identificador do endereço da página para ataques baseados em HTTPS. Nesses casos, o Magnifier ainda detectará ataques, mas não fornecerá os dados detalhados do aplicativo que ele normalmente apresenta em alertas.

Apresenta todos os detalhes do aplicativo nos alertas

O Magnifier apresenta detalhes completos do aplicativo nos alertas quando as organizações configuram seus firewalls de última geração para realizar decriptação do tráfego HTTPS. Com a configuração adequada, os firewalls registram metadados completos de rede - incluindo agentes de navegadores, cabeçalhos identificadores do endereço da página e nomes de arquivos - em alertas

para agilizar as investigações. Ao configurar seus firewalls para realizar decriptação do tráfego, as organizações também podem aproveitar seus aplicativos de firewall, as políticas baseadas em usuários e conteúdo e os recursos de prevenção contra ameaças para bloquear o acesso não autorizado, as explorações e malware.

Quando um invasor está dentro de uma rede, a organização visada tem "o mando do jogo". Suas equipes de TI e segurança cibernética controlam os dispositivos, aplicativos e direitos de usuário; elas podem monitorar a atividade da rede para detectar comportamentos anômalos. O Magnifier fornece visibilidade sem precedentes desse tráfego interno da rede e permite que as organizações descubram ameaças internas, mesmo quando o tráfego está criptografado.

Dados de rede inspecionados pelo Magnifier

O Magnifier analisa metadados no nível de protocolo em logs de tráfego, logs aprimorados de aplicativos e logs de ameaças. Não é necessário inspecionar o conteúdo transferido ou as cargas úteis. Construindo um perfil baseado em mais de 1.000 dimensões comportamentais, inclusive com frequência de conexões, fonte e destino do tráfego, protocolos utilizados e muito mais, o Magnifier pode aprender sobre o comportamento esperado de usuários e dispositivos. O Magnifier também monitora tráfego interno, bem como tráfego de saída dos clientes e servidores da Internet.

Dados no nível de sessão

Os firewalls de última geração da Palo Alto Networks extraem os metadados necessários para criar perfil comportamental do usuário e do dispositivo, incluindo:

- IP de origem, IP de destino, porta de origem, porta de destino
- Bytes enviados e recebidos
- Duração da conexão
- Logs aprimorados de aplicativo com dados em nível da transação em DNS, HTTP, DHCP, RPC, ARP, ICMP e mais
- Detalhes sobre o aplicativo de App-ID

Dados do usuário

O Magnifier analisa o tráfego de rede e os dados de endpoint e extrai contexto do usuário, tais como:

- Usuário que fez login
- Usuário típico de uma máquina
- Usuário que cria o processo que iniciou a comunicação

Dados do host

O Magnifier identifica máquinas ao rastrear:

- Nome do host
- Endereço MAC

Encontre ataques em tráfego criptografado com a Palo Alto Networks

Os agentes de ameaças podem desenvolver técnicas nunca vistas antes para enganar usuários e comprometer endpoints. Com a rápida adoção de criptografia SSL, eles podem ocultar seus ataques no tráfego HTTPS para contornar os controles de segurança. Entretanto, depois de infiltrados em uma rede, eles precisam realizar um processo gradual de reconhecimento e movimentação lateral para obter acesso a recursos valiosos.

A Palo Alto Networks fornece defesas poderosas para ataques cibernéticos, especialmente aqueles à espreita em tráfego criptografado. Os firewalls de última geração da Palo Alto Networks podem realizar a decriptação do tráfego para inspecionar e bloquear ataques à rede. A proteção avançada de endpoint Traps protege os destinos finais do ataque, inclusive laptops, computadores pessoais, servidores e dispositivos da IoT contra ameaças sofisticadas.

É possível que adversários humanos, como invasores externos ou fontes internas mal-intencionadas que operam dentro da rede, evitem usar explorações tradicionais para não serem detectados. Com o perfil comportamental de usuário e dispositivo, as organizações podem detectar mudanças comportamentais que revelem ataques ativos. O Magnifier se concentra em metadados da rede, não em conteúdo de aplicativos, isso permite criar perfil comportamental de usuário e dispositivo quando o tráfego está criptografado. Por meio do monitoramento de atividades internas quanto a comportamento anômalo, o Magnifier pode detectar automaticamente os ataques e favorecer as organizações para evitar a onerosa perda de dados.

paloalto NETWORKS®

3000 Tannery Way
Santa Clara, CA 95054

Principal: +1.408.753.4000
Vendas: +1.866.320.4788
Suporte: +1.866.898.9087

www.paloaltonetworks.com