ManageEngine
EventLog Analyzer

Detecção de script malicioso por meio da auditoria do servidor da web

Introdução

No mundo focado digitalmente de hoje, toda empresa possui uma presença online, e muitas delas até mesmo prestam uma boa parte de seus serviços neste formato. Os serviços normalmente envolvem a troca de informações confidenciais de negócios e de usuários finais, como nomes, detalhes de contato ou informações de pagamento. O site e as aplicações da web de uma organização são, portanto, elementos cruciais na construção de relações com seu público-alvo. Um ataque a seus servidores da web causaria graves interrupções na continuidade dos negócios.

Porém, de acordo com o Relatório de Investigações de Violação de Dados de 2018 da Verizon, os ataques a aplicações da web foram a forma mais comum de ataque, pois eles representam 18,5% de todos os incidentes de segurança. Os setores de TI e varejo são particularmente suscetíveis a esses tipos de ataques. Então, por que estamos testemunhando uma tendência tão perturbadora de ataques a aplicações da web?

Isso pode ocorrer porque a segurança geralmente é negligenciada para fornecer aplicações leves, rápidas e fáceis de usar. Brechas de segurança, como proteção de dados insatisfatória e validação de entrada fraca, permitem que hackers recuperem dados confidenciais ou injetem scripts maliciosos em sites ou servidores da web. Neste guia, discutimos a sua execução e como é possível detectá-los usando a auditoria do servidor da web.

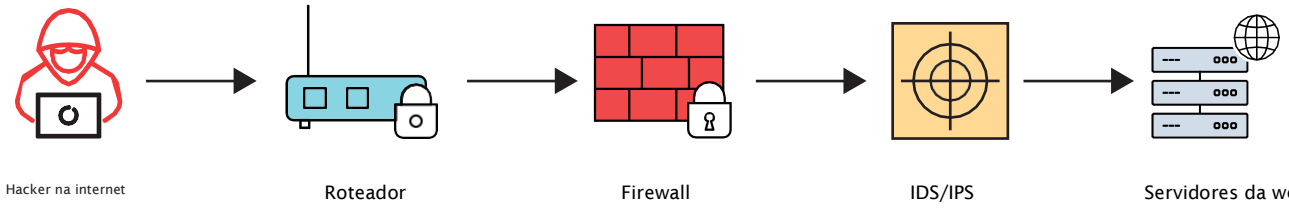
O uso de scripts maliciosos para atacar servidores da web

Um método preferido para violar servidores é injetar código malicioso no site ou no servidor da web. Esse código tem como alvo os sistemas da sua organização ou tenta coletar informações confidenciais dos usuários que acessam seu site, e nenhum deles apresenta uma imagem muito agradável para sua empresa. Scripts maliciosos podem ser usados para diversos objetivos, como:

- Obter controle de um sistema de destino, que pode ser um servidor de arquivos ou banco de dados que contém informações confidenciais.
- Usar sistemas infetados em ataques de botnet.
- Espionar a atividade do usuário.
- Resgatar dados confidenciais.
- Redirecionar usuários para sites maliciosos.
- Hospedar anúncios maliciosos ou indesejados.
- Iniciar malware de mineração de criptografia.

Resumindo, se um invasor for criativo o suficiente, não há limites para como ele pode explorar uma vulnerabilidade do site.

Anatomia de um ataque a servidor da web



Um invasor pode se comunicar com o servidor da web da organização por meio de seu site ou aplicação da web. Ao explorar vulnerabilidades, eles podem incluir conteúdo mal-intencionado em sua comunicação. Como visto acima, o pacote de rede deve passar por algumas camadas de segurança antes de chegar ao servidor da web. Ao auditar sua rede em cada um desses estágios, você pode garantir que seu servidor permaneça protegido contra ataques.

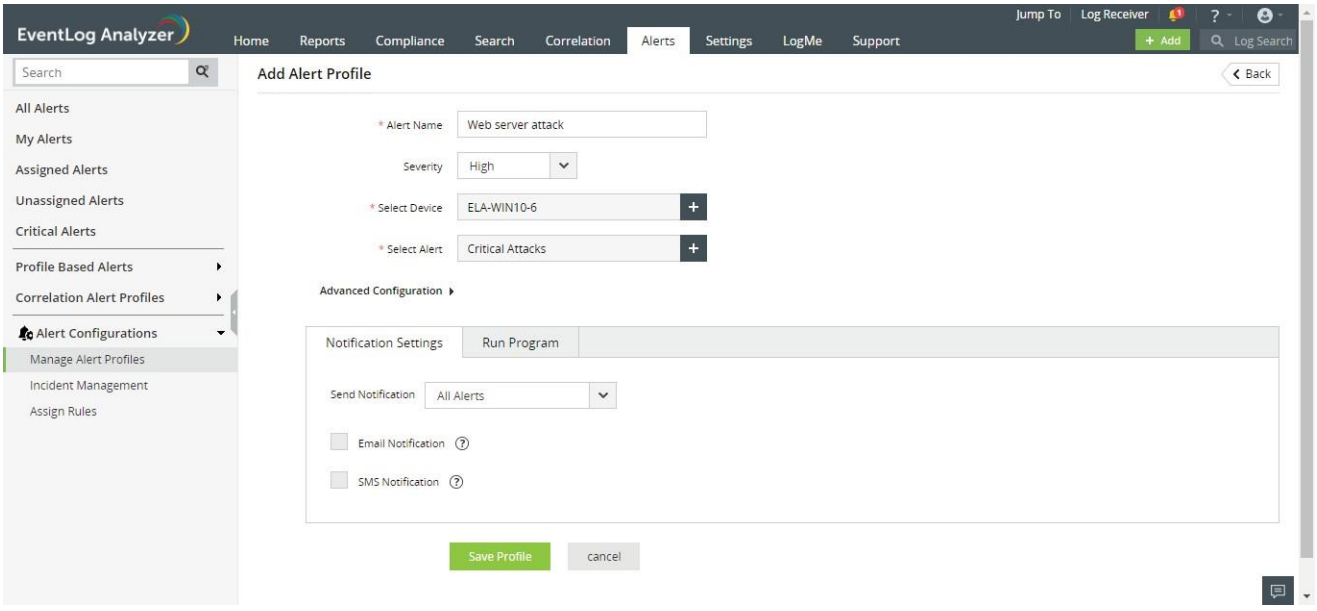
Potencializando o EventLog Analyzer para detectar ataques a servidores da web

O EventLog Analyzer é um software de gerenciamento de logs abrangente que pode rastrear qualquer atividade maliciosa em servidores da web. Ele fornece uma visão geral completa das atividades, incluindo percepções cruciais sobre os padrões de uso. As análises são apresentadas na forma de relatórios abrangentes e intuitivos categorizados em:

- **Relatórios principais:** acompanhe a atividade mais frequente relacionada a usuários, métodos, páginas e muito mais.
- **Relatórios de erro:** monitore os erros que os usuários enfrentam em seu site.
- **Relatórios de ataque:** monitore tentativas de ataques em seu servidor da web.

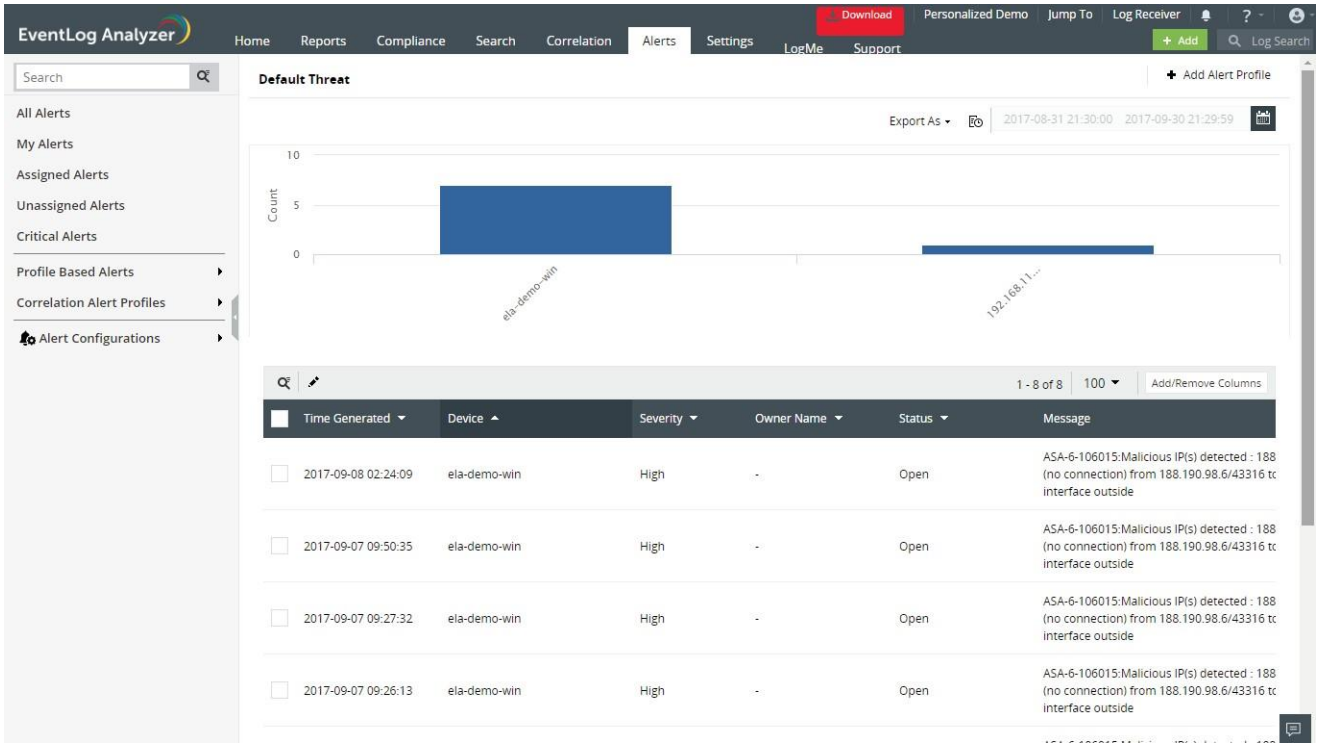
Aqui estão algumas técnicas que podem ser usadas para detectar e investigar ataques direcionados ao seu servidor da web usando o EventLog Analyzer:

1. **Configure alertas para possíveis ataques detectados por seus dispositivos de rede.**



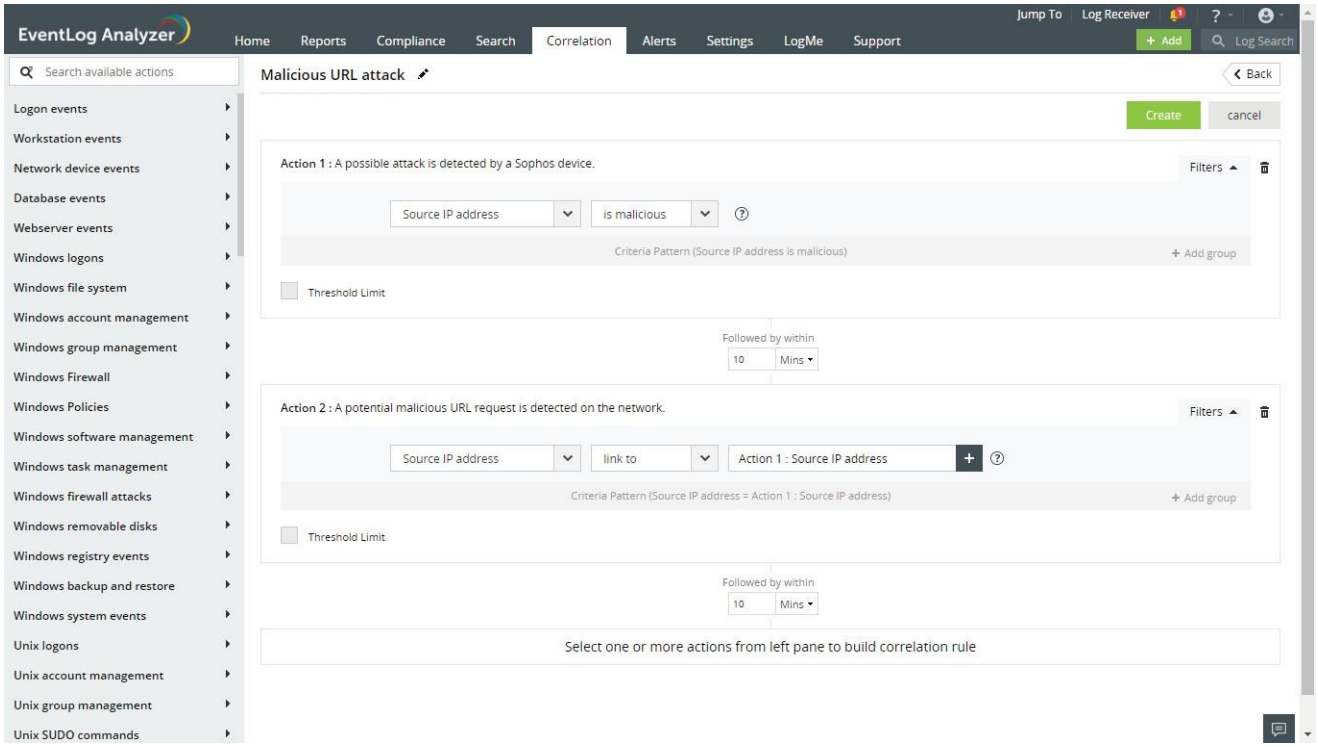
Você pode ser notificado instantaneamente por e-mail ou SMS se possíveis ataques ou tráfego malicioso forem detectados por seu servidor da web. Isso inclui alertas para ataques de negação de serviço (DoS) e solicitações de URL mal-intencionadas. É possível até configurar alertas no sistema de detecção de invasão (IDS) ou no estágio de firewall. Você também pode usar os recursos de emissão de tickets integrados do produto para gerenciar cada alerta como um ticket de incidente, atribuí-lo a um proprietário e rastrear seu status.

2. Sinalize tráfego de fontes maliciosas usando a inteligência contra ameaças.



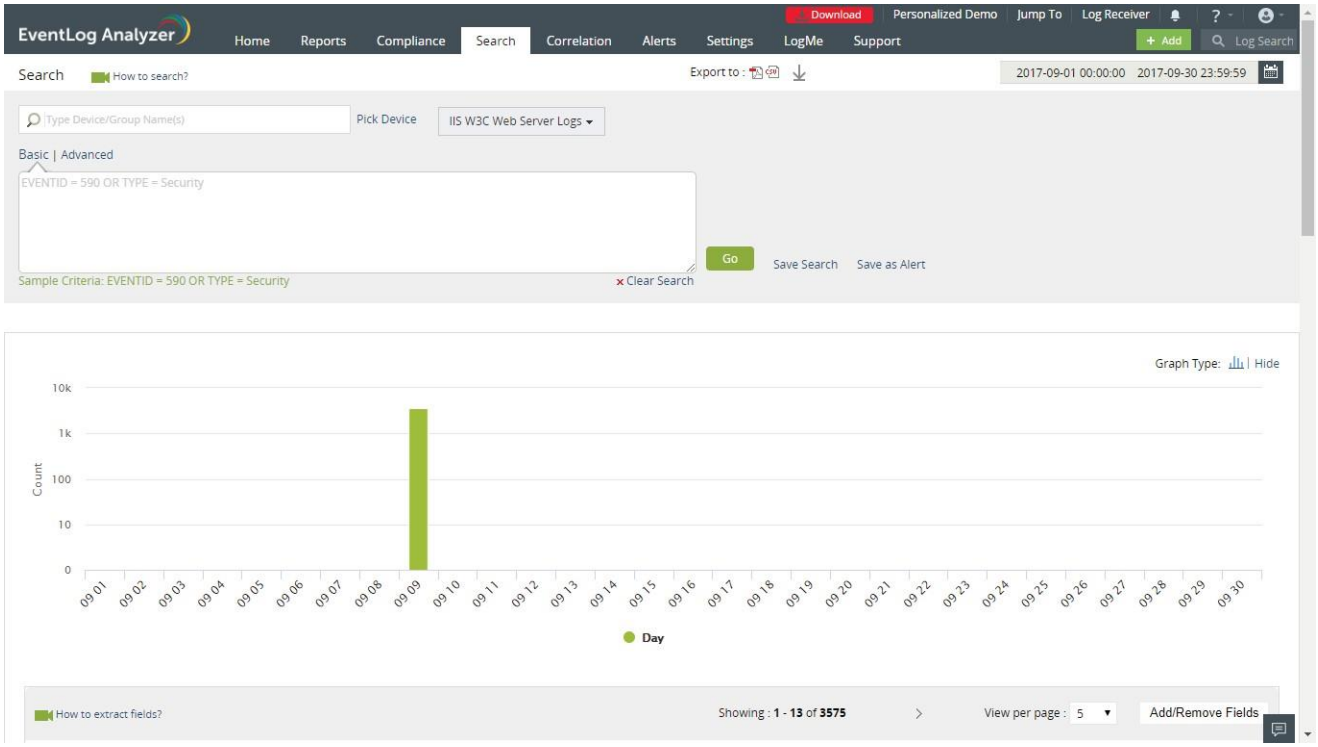
Se um pacote de rede malicioso estiver bem oculto, seus dispositivos da rede podem não percebê-lo. No entanto, a fonte pode ser uma entidade mal-intencionada conhecida. A plataforma de inteligência contra ameaças do EventLog Analyzer processa mais de 600 milhões de fontes de IP/URL mal-intencionadas para ajudá-lo a detectar agentes de ameaça em sua rede. O banco de dados de ameaças é atualizado automaticamente com as informações mais recentes todos os dias. O console de alerta em tempo real da ferramenta está estreitamente vinculado a esse banco de dados. O alerta de ameaça pré-configurado rastreia qualquer tráfego de entrada e saída de fontes mal-intencionadas e emite um alerta em tempo real.

3. Use a correlação de eventos para validar um possível padrão de ataque.



Você pode usar o módulo de correlação de eventos do produto para adicionar mais contexto e validar eventos do seu servidor da web com aqueles de outros dispositivos da rede, como o firewall ou IDS, e gerar um alerta somente se o evento parecer suspeito. Por exemplo, é possível criar uma regra de notificação se um ataque for detectado pelo IDS e seu servidor da web sinaliza uma solicitação de URL potencialmente mal-intencionada do mesmo endereço IP.

4. **Realize investigações forenses usando a pesquisa.**

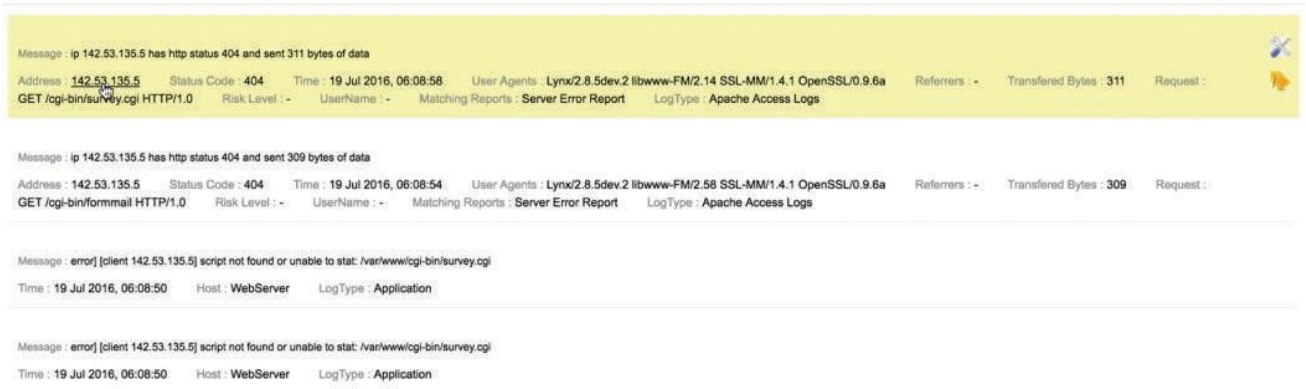


Você também pode usar o mecanismo de pesquisa poderosa do EventLog Analyzer para rastrear qualquer evento e descobrir sua fonte. O procedimento para fazer isso é explicado na próxima seção.

Ataques de backtracking com o EventLog Analyzer

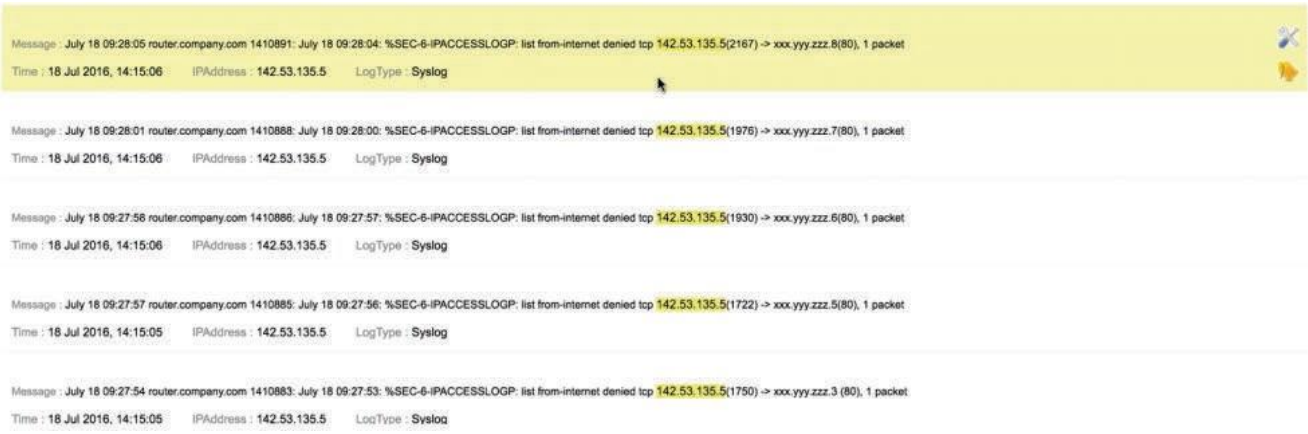
Ao receber um alerta sobre uma possível solicitação mal-intencionada para seu servidor da web, você pode iniciar uma pesquisa nos logs do servidor da web e investigar o padrão de ataque. Um exemplo de investigação é ilustrado abaixo:

- Ao passar pelos logs do seu servidor da web onde o comprometimento foi indicado, há uma entrada para uma solicitação de acesso ao servidor da web por meio de uma conexão SSL aberta.



- Após a solicitação de acesso, haverá uma nova deste mesmo endereço IP para executar um script.
- Clique no campo **Endereço** na mensagem de log para exibir os detalhes de todas as solicitações feitas por esse endereço IP específico para o servidor da web especificado.
- Em seguida, verifique onde mais esse endereço IP atinge sua rede digitando-o no campo de pesquisa. Percorra esses logs e veja se o endereço IP atinge o IDS.

- Você também pode verificar se há entradas de log correspondentes a esse endereço IP do firewall e do roteador.



- Analisar os dados de log de todos esses dispositivos ajudará a reconstruir o ataque.
- Ao examinar os logs, é possível realizar uma análise forense completa do ataque para determinar se ele foi realmente um ataque ou se era um falso positivo. Se for um ataque, você pode bloquear imediatamente o endereço IP para minimizar os danos.

Armado com recursos que ajudam a detectar, investigar e gerenciar incidentes de segurança em seu servidor da web, seu site fica protegido e nem você nem os visitantes dele são afetados negativamente.

ManageEngine

EventLog Analyzer

O EventLog Analyzer é uma solução de gerenciamento de logs e conformidade de TI baseada na web, em tempo real, que combate ataques de segurança de rede. Com capacidades abrangentes de gerenciamento de logs, o EventLog Analyzer ajuda as organizações a atenderem às diversas necessidades de auditoria. Também oferece relatórios e alertas de conformidade prontos para uso que facilmente atendem aos rigorosos requisitos normativos da TI.

$ Obter orçamento

Download

Ligação grátis
+1 844 649 7766

Número de discagem direta
EUA: +1-408-352-9254

eventlog-support@manageengine.com

www.eventloganalyzer.com