Kaspersky Network Security Threat Data Feeds

kaspersky BRING ON THE FUTURE

A proteção do endpoint sozinha não é suficiente.

A proteção em nível de rede também é necessária.

Veja aqui o porquê:

- A proteção contra diferentes tipos de ataques deve consistir em várias camadas.
- Nem todos os hosts em seu ambiente terão proteção de segurança de endpoint, por exemplo, nem todos os servidores críticos para o negócio ou hosts em uma rede industrial.
- Alguns hosts "protegidos" podem não estar atualizados com assinaturas / hashes / regras de detecção.

Feed de Dados de Ameaças da Kaspersky Network Security

Quase toda empresa hoje em dia tem um Firewall de Próxima Geração (NGFW). É um dos controles de segurança de rede modernos mais eficazes, aumentando os níveis de proteção das redes corporativas contra ciberataques.

A maioria dos NGFW não apenas é capaz de utilizar conhecimento interno sobre ameaças cibernéticas, mas também oferece funcionalidades que permitem o uso de listas dinâmicas de indicadores de comprometimento (IoCs) de fontes externas para bloquear ameaças cibernéticas em tempo real.

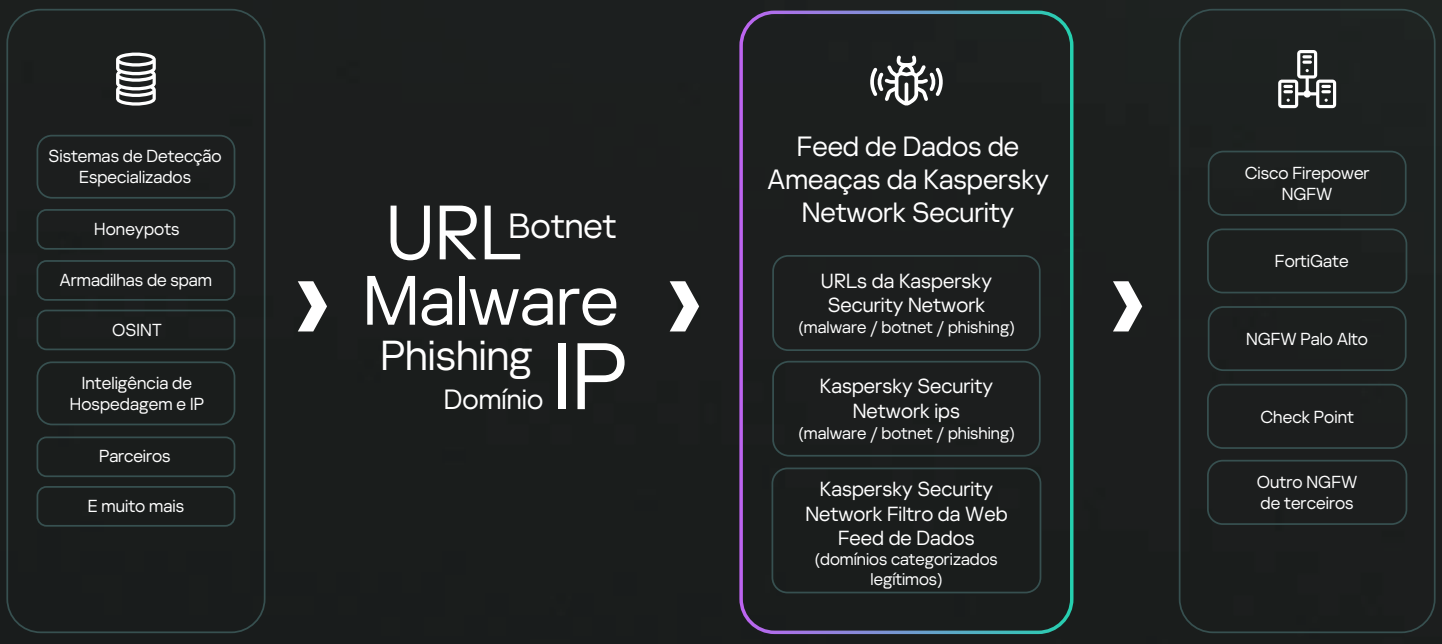
Ter que configurar rapidamente as regras de detecção NGFW para sempre estar à frente dos adversários é quase impossível. Por isso é essencial ter conhecimento em inteligência de ameaças externas. Isso traz um elemento crítico adicional de proteção para o seu ambiente, que de outra forma poderia passar despercebido.

A Kaspersky oferece coleções especialmente criadas de IoCs que, quando importadas para um NGFW, melhoram significativamente o nível de proteção de segurança da rede corporativa contra as ameaças mais prevalentes, sem integração ou configuração complicadas, e mantendo a topologia de rede atual.

Os feeds de dados de ameaças de segurança da rede Kaspersky são baseados nos feeds de dados de inteligência de ameaças da Kaspersky e contêm listas regularmente atualizadas de vários tipos de IoCs (endereços IP e domínios). Usar essas informações permite que você monitore/bloqueie o acesso do usuário a recursos de rede perigosos.

Saiba mais

Feed de Dados de Ameaças da Kaspersky Network Security



Coleta de dados e armazenamento

Os feeds de dados da Kaspersky Security Network são compostos por várias listas, cada uma focada em um tipo específico de ameaça cibernética. Os feeds contêm listas de endereços IP com a pontuação de ameaça mais alta e domínios de nível superior e de segundo nível de recursos conhecidos por distribuir malware, atuar como centros de comando e controle de botnets (C&C) ou hospedar recursos de phishing.

Os Feeds de Dados são montados a partir de fontes integradas, heterogêneas e altamente confiáveis, tal como o Kaspersky Security Network e os nossos próprios Web Crawlers, o serviço de Botnet Monitoring (monitoramento de botnets, seus alvos e atividades, 24 horas por dia, 7 dias da semana), armadilhas de spam, equipes de pesquisa e parceiros.

Em seguida, em tempo real, todos os dados agregados são analisados detalhadamente e refinados utilizando técnicas de pré-processamento, como critérios estatísticos, sandboxes, análises investigativas, ferramentas de semelhança, profiling comportamental, validação por analistas e verificação de listas de permissões.

Destaques

Monitoramento em tempo real

Todos os feeds são automaticamente gerados em tempo real com base em descobertas em todo o mundo, fornecendo altos índices de detecção e precisão.

O Kaspersky Security Network fornece visibilidade em uma porcentagem significativa de todo o tráfego da internet, abrangendo dezenas de milhões de usuários finais em mais de 213 países.

Suporte nativo

Suporte nativo para os NGFWs mais populares:

- Cisco
- FortiGate
- Palo Alto
- Outros NGFWs de terceiros (com funcionalidade de listas dinâmicas externas com suporte de autenticação básica)

Autenticação segura

Os Feeds de Dados oferecem uma variedade de métodos de autenticação adaptados para atender a diferentes necessidades de segurança e preferências de integração.

Fácil integração

Guias de configuração suplementares passo a passo para cada NGFW suportado e suporte técnico da Kaspersky permitem uma configuração fácil e entregam valor imediato.

Disponibilidade contínua

Todos os feeds são gerados e monitorados por uma infraestrutura altamente tolerante a falhas, assegurando disponibilidade contínua

100% de dados verificados

Os feeds de dados cheios de falsos positivos são prejudiciais, pois podem bloquear recursos legítimos.

Os feeds de dados da Kaspersky Security Network aplicam extensos testes e filtros antes de liberar os feeds, garantindo que os dados verificados em 100% sejam entregues.

Benefícios

Reforce suas soluções de defesa de rede

com indicadores de comprometimento continuamente atualizados para bloquear automaticamente as ameaças cibernéticas mais prevalentes

Prevenir a exfiltração de ativos sensíveis.

e propriedade intelectual de máquinas infectadas para fora da sua organização

Bloqueie rapidamente as ameaças cibernéticas para se proteger.

Proteja sua organização contra ameaças cibernéticas e mantenha a continuidade dos negócios.

Kaspersky Threat Data Feeds

Saiba mais

www.kaspersky.com.br

#kaspersky
#bringonthefuture