Kaspersky APT Intelligence Reporting

kaspersky PREPARADOS PARA O FUTURO

Kaspersky APT Intelligence Reporting

Os clientes do Kaspersky APT Intelligence Reporting recebem acesso contínuo exclusivo às nossas investigações e descobertas, incluindo dados técnicos completos (em vários formatos) sobre cada APT à medida que são descobertos, bem como sobre ameaças que nunca serão divulgadas. Os relatórios contêm um resumo executivo com informações orientadas ao nível C e fáceis de entender que descrevem o APT relacionado, juntamente com uma descrição técnica detalhada do APT com IOCs relacionados e regras YARA para fornecer aos pesquisadores de segurança, analistas de malware, engenheiros de segurança, analistas de segurança de rede e dados acionáveis APT de pesquisadores que permitem uma resposta rápida e precisa à ameaça.

Nossos especialistas também alertam imediatamente sobre qualquer mudança que detectarem nas táticas de grupos de criminosos virtuais. Você também terá acesso ao banco de dados completo de relatórios APT da Kaspersky, outro poderoso componente de pesquisa e análise em suas defesas de segurança.

Benefícios

MITRE ATT&CK
Todos os TTPs descritos nos relatórios são mapeados para o MITRE ATT&CK, permitindo uma melhor detecção e resposta através do desenvolvimento e priorização dos casos de uso de monitoramento de segurança correspondentes, efetuando análises de falhas e testando as defesas atuais contra aos TTPs relevantes.

Informações sobre APTs não públicos
Por várias razões, nem todas as ameaças de alto nível são divulgadas ao público em geral. Mas nós compartilhamos todos eles com nossos clientes

Acesso privilegiado
Receba descrições técnicas sobre as ameaças mais recentes durante as investigações em andamento, antes de serem divulgadas ao público em geral

Análise retrospectiva
É fornecido acesso a todos os relatórios privados disponíveis durante todo o período da assinatura.

Acesso a dados técnicos
Inclui uma lista ampla de IOCs disponíveis nos formatos padrão, que incluem o openIOC ou o STIX, bem como acesso às nossas regras YARA

Perfis de agentes de ameaça
Incluindo o país de origem suspeito e a atividade principal, famílias de malware usadas, setores e regiões visadas e descrições de todos os TTPs usados, com mapeamento para MITRE ATT&CK

Monitoramento contínuo de campanhas de APT.
Acesso a inteligência acionável durante a investigação com informações sobre distribuição de APTs, IOCs, infraestruturas de comando e controle etc.

API RESTful
Integração e automação perfeitas dos seus fluxos de trabalho de segurança

www.kaspersky.com.br