Kaspersky®
Threat Intelligence

Casos de uso estratégico da inteligência de ameaças

Nossas vidas dependem muito da Internet. O baixo custo e a alta velocidade da comunicação que ela fornece a tornam um componente integral e essencial da base de empresas e governos bem-sucedidos. Os ambientes dinâmicos e interconectados oferecem várias funções importantes, com capacidade para melhorar as comunicações, proteger dados pessoais, confidenciais e outros, além de permitir a supervisão e o controle de sistemas e processos de negócios críticos, tudo isso ao mesmo tempo que estimulam a competitividade. No entanto, a crescente interconectividade está expandindo a superfície de ataque, e os adversários estão prontos para explorar todas as vulnerabilidades possíveis, em todos os níveis.

Nos últimos anos, temos observado que os limites entre diferentes tipos de ameaças e diferentes tipos de agentes de ameaças estão se desfazendo. Um exemplo disso é o despejo de código pelo grupo Shadow Brokers, que colocou exploits avançadas (supostamente desenvolvidas pela NSA) à disposição de grupos criminosos que, de outra forma, não teriam acesso a esse tipo de código sofisticado. Um outro exemplo é o surgimento de campanhas de ameaças direcionadas avançadas (APTs) não focadas na espionagem cibernética, mas no roubo de recursos para financiar outras atividades em que o grupo da APT está envolvido.

As motivações dos agentes de ameaças variam muito, do roubo de valores à derrubada de concorrentes, roubo de identidades e fraude. Além disso, cada setor e cada organização tem seus dados exclusivos para proteger, um conjunto único de aplicativos, tecnologias que usam, etc. Tudo isso confere uma tremenda variabilidade nas maneiras como os ataques são executados, e novos métodos surgem todos os dias.

Nesse cenário de ameaças que muda rapidamente, promover o crescimento da empresa por meio da transformação digital pode ser um desafio excepcional, e os administradores precisam adotar uma abordagem estratégica, examinando continuamente os riscos cibernéticos em relação às metas e prioridades gerais da empresa.

A compreensão dos riscos permite tomar decisões mais inteligentes, por exemplo, ao lançar uma nova iniciativa, abrir um novo escritório regional ou planejar o investimento em uma tecnologia. E também ajuda a desenvolver estratégias de atenuação proativa e a justificar as necessidades associadas de orçamento e pessoal.

A inteligência de ameaças estratégica apresenta uma visão geral das tendências dos ataques, das técnicas e métodos usados pelos invasores, incluindo suas motivações e atribuições, e ajuda a responder a uma série de perguntas específicas:

- Quem são seus adversários? O que eles querem?
- Quais grupos de ameaças estão ativos em seu setor ou sua região?
- Quais são os vetores de ataques usados?
- Qual é a melhor maneira de montar um ataque contra a sua organização?
- Quais rotas e informações estão disponíveis para um invasor que tem você como alvo específico?
- Já foi montado algum ataque? Você está prestes a ser ameaçado?
- Quais ações são necessárias para reduzir seu perfil de risco?

Ao entender essas perguntas e mapear as respostas para seus ativos, sistemas e processos de negócios críticos, você pode realizar uma análise de riscos completa e apresentar cenários de riscos claros e relevantes para sua equipe executiva e, assim, justificar o investimento em determinados programas, tecnologias e pessoal. De posse dessas informações, a empresa pode concentrar sua estratégia de segurança de informações nas áreas apontadas como alvos principais dos cibercriminosos e agir rapidamente e com precisão para repelir invasores e minimizar o risco de um ataque bem-sucedido.

A Kaspersky Lab oferece:

Tipo de relatório	Inteligência fornecida	Caso de uso
Relatórios de inteligência de APTs	• Descrições de táticas e métodos usados por invasores em campanhas de espionagem cibernética direcionadas a vários setores • Perfis de agentes de ameaças com as táticas, técnicas e procedimentos (TTPs, Tactics, Techniques and Procedures) que eles usam • Mapeamento das TTPs para o MITRE ATT&CK – uma base de conhecimento de TTPs de adversários baseados na experiência do mundo real.	• Entender os agentes de ameaças que visam seu setor ou sua região e quais TTPs eles usam • Identificar quais recursos de informações e sistemas estão em risco, o impacto potencial do comprometimento e como estabelecer uma priorização adequada • Ajustar as estratégias de segurança de informações, planejar e justificar os investimentos em certas tecnologias, equipes e programas para cobrir possíveis vetores de ataques.
Relatórios de inteligência de ameaças financeiras	• Descrições de táticas e métodos usados por invasores que visam o setor financeiro • Informações sobre ataques a infraestruturas específicas, como caixas eletrônicos ou dispositivos de pontos de venda • Informações sobre ferramentas específicas adaptadas para atacar redes financeiras usadas, desenvolvidas e vendidas por cibercriminosos em comunidades e fóruns da Darknet em diversas regiões.	• Identificar os adversários que visam instituições financeiras em todo o mundo e as TTPs que eles usam • Identificar quais recursos de informações e sistemas estão em risco, o impacto potencial do comprometimento e como estabelecer uma priorização adequada • Ajustar as estratégias de segurança de informações, planejar e justificar os investimentos em certas tecnologias, equipes e programas para cobrir possíveis vetores de ataques.
Relatórios de inteligência de ameaças específicos para o cliente	• Identificação passiva do perímetro da rede, dos serviços disponíveis e das vulnerabilidades existentes • Análise de vulnerabilidades e exploits personalizadas • Identificação, monitoramento e análise de todas as amostras de malware ativas ou inativas que visam sua organização • Vazamentos de dados e credenciais • Ameaças de phishing direcionadas às marcas dos clientes • Evidências de ameaças e atividades de botnets que visam especificamente os clientes, parceiros e fornecedores de uma empresa • Análises específicas do setor, incluindo TTPs de cibercriminosos relevantes.	• Garantir a disponibilidade e a alocação correta de recursos para atenuar as falhas de segurança identificadas • Fornecer informações aos projetos complexos de devida diligência de terceiros para combater ataques à cadeia de fornecimento • Ajustar políticas e controles para atenuar possíveis ameaças internas • Melhorar a conscientização sobre segurança das equipes internas, desenvolvendo um programa específico baseado em constatações (por exemplo, credenciais corporativas comprometidas por meio de serviços de terceiros) • Atenuar possíveis danos à reputação com o monitoramento do uso não autorizado de marcas da empresa para fins de phishing • Planejar e justificar os investimentos em certas tecnologias, equipes e programas para cobrir vetores de ataques relevantes.

Kaspersky Lab
Cibersegurança para empresas: **www.kaspersky.com.br/enterprise**
Notícias sobre ameaças cibernéticas: **www.securelist.com**
Notícias sobre segurança de TI: **www.kaspersky.com.br/blog**

#truecybersecurity
#HuMachine

www.kaspersky.com.br