A ameaça de ataques Ransomware com inteligência AI

Juntamente com seus muitos benefícios, a AI também capacitou agentes maliciosos a lançar ataques cibernéticos cada vez mais sofisticados, com o ransomware surgindo como uma ameaça particularmente potente.

Um relatório recente do National Cyber Security Centre (NCSC) do Reino Unido alertou que invasores maliciosos já estão aproveitando a AI para desenvolver ataques ransomware, criando riscos significativos para indivíduos, empresas e até mesmo infraestrutura crítica. Agentes de ameaças como o APT28 têm estado ocupados usando modelos de linguagem grande (LLMs, large language models) em movimentos elaborados para evitar a detecção e executar reconhecimento avançado.

Veja mais detalhes sobre essas ameaças e como se manter resiliente contra elas.

Como a AI adiciona sofisticação e expansão aos ataques

Ransomware têm sido uma ameaça persistente há anos, e a integração de técnicas de AI está elevando esses ataques a um novo nível de sofisticação, velocidade e escala.

Adaptação e personalização em tempo real. O ransomware com inteligência AI é capaz de adaptar suas táticas em tempo real e modificar o código de malware para evitar a detecção. Os LLMs podem ser usados para alterar o código-fonte de um malware para evitar regras de acionamento, como regras YARA, que identificam padrões em famílias de malware para alertar um possível ataque.

Automatização de ataques. A AI pode automatizar vários estágios do processo de ataque, aumentando a eficiência dos ataques e reduzindo a necessidade de intervenção humana.

Fraquezas direcionadas à precisão. Ao aproveitar a AI para reconhecimento e avaliação de vulnerabilidade, o ransomware com inteligência AI pode explorar os pontos fracos nas defesas de cibersegurança existentes com precisão alarmante. Os invasores podem identificar e explorar pontos de entrada que as defesas tradicionais podem ignorar. Isso inclui vulnerabilidades de dia zero e configurações incorretas em software e sistemas, complicando ainda mais a tarefa de defesa contra esses ataques. Algoritmos de aprendizado de máquina (ML, Machine Learning) podem analisar grandes quantidades de dados para identificar possíveis alvos, criar e-mails de phishing convincentes e até mesmo personalizar demandas de resgate com base no perfil da vítima.

Ataques de acompanhamento bem informados. Modelos de linguagem multimodal (MMLMs, Multimodal Language Models) que podem analisar vídeos e fotos de instalações, equipamentos e outras informações publicamente disponíveis podem ajudar os invasores a obter metadados, versões de software e dados de geolocalização para entender especificações técnicas para aprofundar ataques.

O deep fakes e o “brandjacking” com AI generativa também podem ser usados para atrair as vítimas a fornecer credenciais com sites realistas e legítimos, “influenciando as operações”, com artigos de notícias gerados por AI ou vídeos falsos.

Mais riscos exigem mais resiliência

As consequências dos ataques ransomware com inteligência AI podem ser devastadoras: perdas financeiras significativas, danos à reputação e até mesmo interrupções operacionais. Em alguns casos, o pagamento pode ser a única opção para recuperar dados criptografados, perpetuar o ciclo do cibercrime e incentivar ataques futuros.

Para combater a onda crescente de ataques ransomware com inteligência AI, é necessária uma arquitetura de segurança em camadas e resiliente a dados. Isso inclui investir em defesas robustas de cibersegurança que aproveitam a AI e o aprendizado de máquina para detecção e resposta a ameaças. Ao analisar o tráfego de rede, o comportamento do usuário e a atividade do endpoint em tempo real, as soluções com inteligência AI podem ajudar as organizações a identificar e mitigar ameaças de ransomware antes que elas causem danos.

Mas nem todas as arquiteturas de segurança são criadas da mesma forma, e isso pode ser a diferença entre voltar a ficar online em horas ou dias. Em um blog anterior, dissipamos alguns mitos sobre lacunas de ar. Também discutimos a análise de segurança e os sistemas SIEM e analisamos detalhadamente os benefícios dos bunkers de dados, incluindo uma arquitetura de exemplo para você começar.

Além disso, as organizações devem priorizar a conscientização e a educação sobre cibersegurança para capacitar os funcionários a reconhecer e relatar atividades suspeitas. O phishing continua sendo um vetor comum para ataques de ransomware, e as pessoas desempenham um papel crucial para impedir essas tentativas ao exercer cautela e vigilância on-line.

A colaboração entre partes interessadas do setor, agências de aplicação da lei e especialistas em cibersegurança é essencial para compartilhar inteligência contra

ameaças, desenvolver práticas recomendadas e coordenar respostas a ataques ransomware. Ao trabalharmos juntos, podemos melhorar nossa resiliência coletiva e nos defender melhor contra o cenário de ameaças em evolução. Agora é a hora de dar o próximo passo na modernização de suas soluções de proteção de dados. Saiba mais sobre o risco de um ataque ransomware e comece a proteger sua empresa contra ataques ransomware.

Escrito por:

Roger Boss