Acesse os informativos anteriores

Ataques com malware dão lugar ao uso de credenciais válidas roubadas

Ameaças mais rápidas e inteligentes

O recém lançado Relatório Global de Ameaças da CrowdStrike acende um alerta para todas as organizações: os criminosos estão mais rápidos, sofisticados e usando táticas alternativas para contornar as defesas tradicionais.

🎯 A PRINCIPAL AMEAÇA: O FOCO NA IDENTIDADE

Confirmando o alerta dado em nosso último informativo, a maior mudança no cenário de ameaças não é um novo malware, mas o foco em **roubar credenciais válidas**. *Hackers* estão deixando de lado as invasões com código malicioso e estão simplesmente "logando" nos sistemas com contas legítimas.

- **IA Generativa:** ataques de phishing e engenharia social aprimorados com IA para criar e-mails, mensagens e até mesmo ligações com vídeo e voz extremamente convincentes, personalizados e muito difíceis de diferenciar.

⏱️ UM DADO ALARMANTE: A NOVA CORRIDA CONTRA O TEMPO

O tempo médio que um invasor leva para se mover lateralmente na rede após obter o acesso inicial ("breakout time") atingiu um novo recorde.

- **Apenas 62 minutos.** Esse é o tempo mínimo que um ataque leva para se espalhar pela rede, comprometer outros sistemas e extrair dados.

☁️ O ALVO EM EXPANSÃO: AMBIENTES EM NUVEM

A infraestrutura em nuvem continua sendo um alvo prioritário. Os atacantes exploram ativamente configurações incorretas, APIs expostas e credenciais de nuvem fracas para obter acesso rápido a dados críticos e escalar privilégios.

RECOMENDAÇÕES ESTRATÉGICAS

- A defesa precisa ser tão rápida e inteligente quanto o ataque. Alertas em tempo real precisam complementar as abordagens tradicionais.
- A segurança cibernética não é mais apenas sobre prevenir a entrada de malware: é uma batalha pela segurança das identidades!
- A proteção das contas de usuários e senhas é prioridade máxima. Monitorar o uso de credenciais em tempo real e impor políticas de segurança é fundamental.

Nosso foco é a segurança!

A metodologia da Advance destaca-se por identificar rapidamente comprometimentos na cibersegurança com a abordagem Zero Trust, minimizando riscos e restringindo acesso às informações críticas. Implementamos backups 100% seguros e imutáveis, garantindo a salvaguarda e recuperação dos dados em qualquer cenário.

At.,
Nilton Teixeira
https://www.advancegroup.com.br
Microsoft Partner ID 3288934
Segurança nunca é demais!

ADVANCE GROUP
BECAUSE IT MUST BE A SOLUTION

Acesse os informativos anteriores