

Atualmente, um dos temas mais relevantes e de maior interesse geral em cibersegurança é o aumento dos ataques ransomware (“ransom” significa “resgate” em inglês), um tipo de malware que criptografa os dados da vítima e exige um resgate em criptomoedas (geralmente BitCoin) para liberá-los. Pouco importa se os dados estão na nuvem ou em computadores e servidores locais - uma vez que o programa malicioso obteve acesso, o efeito será o mesmo.

Este tema tem ganhado destaque devido aos recentes ataques de alto nível de sofisticação contra empresas, governos, hospitais e até mesmo oleodutos, causando graves perturbações econômicas e sociais.

Entre os aspectos que tornam este tema particularmente importante estão:

- ◆ Aumento sensível na frequência e sofisticação dos ataques
- ◆ Impacto em infraestruturas críticas e grandes organizações
- ◆ Evolução para um modelo de “Ransomware as a Service” (RaaS)
- ◆ Implicações geopolíticas e até de segurança nacional
- ◆ Desafios para empresas e governos na prevenção e resposta
- ◆ Despreparo de instituições quanto à prevenção e recuperação dos dados sequestrados



RaaS (“Ransomware as a Service”) é um modelo de negócio onde desenvolvedores de *malware* “alugam” seu *ransomware*, permitindo que indivíduos com pouca habilidade técnica realizem ataques sofisticados. O modelo geralmente opera com divisão de lucros, aumentando muito a frequência e o alcance dos ataques.

### **Todo cuidado é pouco! Observe alguns cuidados básicos:**

- Mantenha todo software atualizado, de preferência com atualizações automáticas ativadas.
- Utilize um antivírus confiável e sempre atualizado. Opções gratuitas nem sempre oferecem a melhor proteção.
- Seja cauteloso ao navegar ou ler qualquer tipo de mensagem (e-mail, WhatsApp, SMS etc.), evite sites suspeitos/desconhecidos e não clique em links, pop-ups ou anúncios suspeitos.

- Eduque-se sobre engenharia social para facilitar a identificação de tentativas de manipulação. NUNCA forneça informações pessoais ou sensíveis a fontes não verificadas.
- Fique atento a comportamentos incomuns nos seus dispositivos, tais como lentidão ou travamento inexplicáveis e arquivos com extensões ou nomes desconhecidos.

---

At.,

**Nilton Teixeira**

<https://www.advancegroup.com.br>

Microsoft Partner ID 3288934

**Segurança nunca é demais!**

