

Exploração de Compartilhamento CIFS: A maior vulnerabilidade é humana

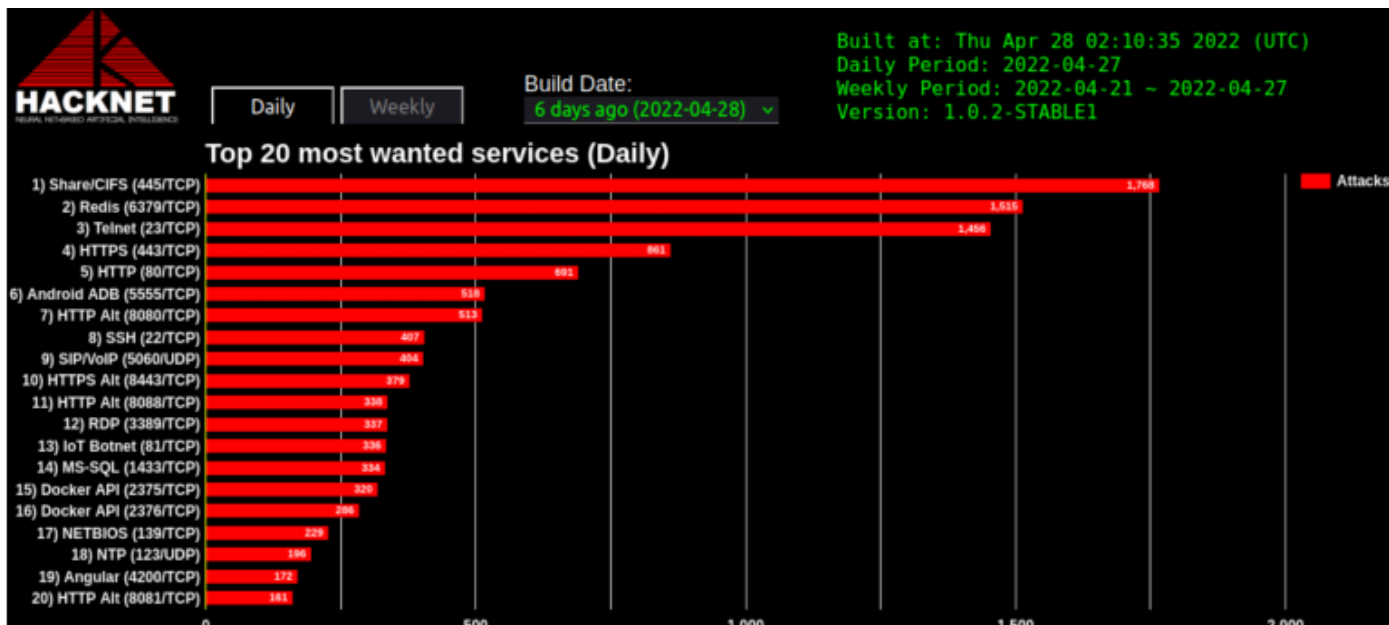
Uma recente vulnerabilidade descoberta no serviço de RPC do Windows, que recebeu a [CVE-2022-26809](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26809), movimentou o mundo do cibercrime na busca por alvos que possam ser explorados, chegando a despontar como serviço mais procurado nos relatórios da Hacknet, um projeto desenvolvido e mantido pela empresa brasileira NetSensor, e que analisa atividades maliciosas em diversos pontos do mundo.

São claros os motivos para toda essa movimentação, afinal, a vulnerabilidade reúne, segundo dados da própria Microsoft, uma conjuntura de características praticamente irresistíveis para qualquer atacante: Ataque via rede, baixa complexidade, sem necessidade de privilégios, sem necessidade de interação do usuário e com alto grau de quebra de confidencialidade, integridade e disponibilidade, ou seja, quebra de “todos” os pilares da Segurança da Informação (CID).

Metric	Value
▼ Métricas de pontuação de base (8)	
▶ Vetor de ataque	▶ Rede
▶ Complexidade do ataque	▶ Baixa
▶ Privilégios necessários	▶ Nenhum
▶ Interação do usuário	▶ Nenhum
▶ Escopo	▶ Inalterado
▶ Confidencialidade	▶ Alta
▶ Integridade	▶ Alta
▶ Disponibilidade	▶ Alta

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26809>

Apesar da procura pelo serviço de compartilhamento CIFS ter chegado ao topo do ranking alguns dias após a divulgação da vulnerabilidade, a HackNet já identificava esse serviço como uma figura constante entre os “top 3” serviços mais procurados em seus relatórios diários.



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

Partindo do pressuposto que um serviço não seria tão procurado, e por tanto tempo, se não houvesse uma grande possibilidade de realizar algum tipo de exploração com alto nível de comprometimento, a NetSensor fez um trabalho de investigação a respeito da exposição e fragilidade desse serviço na Internet, chegando a resultados assustadores, muito embora eles não devam surpreender grande parte dos profissionais de segurança.

Dentre os itens mais críticos e assustadores destacam-se:

- Uma grande quantidade de exposições do serviço, provavelmente sem a real necessidade, seja por descuido durante a implementação, seja por uma má escolha da solução usada para atender uma demanda específica.
- Serviços permitindo a enumeração dos compartilhamentos disponíveis.
- Compartilhamentos com acesso público (guest) contendo dados sensíveis e altamente confidenciais, dentre os quais podemos citar:
 - Dados pessoais de clientes e fornecedores, incluindo dados bancários;
 - Informações corporativas, incluindo detalhes financeiros e de seus produtos;
 - Códigos fonte de sistemas, alguns com permissão de gravação inclusive;
 - Backups de bases de dados inteiras, chegando à exposição de terabytes de dados de uma mesma empresa.
 - As tão desejadas credenciais de acesso à sistemas, diversos portais de gerenciamento de tecnologia e Clouds, entre outros.

Pode até parecer clichê, algo trivial, mas infelizmente não é:

"Revisem exposições desnecessárias dos serviços de compartilhamento CIFS e RPC".

Embora existam diversas vulnerabilidades em serviços e aplicações de mercado, as maiores vulnerabilidades continuam sendo inseridas por pessoas, seja por descuido, falta de conhecimento ou prazos curtos de entrega, o fato é que diante desse cenário vejo uma nova “bolha” se formando no mercado, a qual tenho chamado de “a bolha da segurança”. Mas isso é assunto para um próximo artigo.