BOLETIM DE SEGURANÇA

Novo recurso de bloqueio de NTLM sobre SMB para evitar ataques.

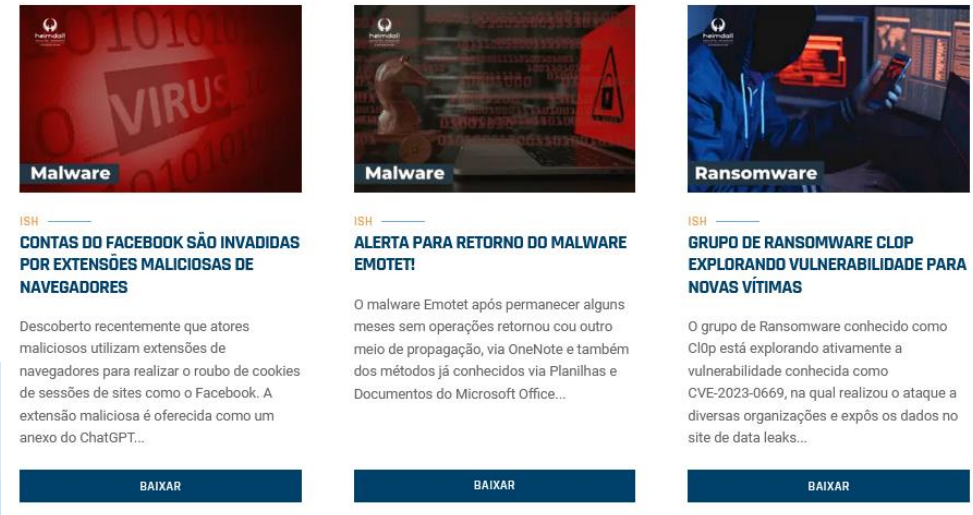
heimdall
security research
A DIVISION OF ISH

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



Sumário

Lista de Figuras

1 NOVO RECURSO DA MICROSOFT

A Microsoft adicionou um novo recurso de segurança ao Windows 11 que permite aos administradores **bloquear NTLM sobre SMB** para fins de evitar ataques de "*pass-the-hash*" (passagem de hash), "*relay*" (retransmissão) de NTML ou quebra de senhas.

Esse recurso modificará a abordagem herdada em que as negociações de autenticação Kerberos e NTLM (ou seja, LM, NTLM e NTLMv2) com servidores de destino seriam alimentadas pelo Windows SPNEGO.

Ao conectar-se a um compartilhamento SMB remoto, o Windows tentará negociar a autenticação com o computador remoto executando uma resposta de desafio NTLM. No entanto, a resposta de desafio NTLM conterá a senha com hash do usuário conectado que está tentando abrir o compartilhamento SMB, que pode então ser capturada pelo servidor que hospeda o compartilhamento.

Vale salientar que estas hashes podem então ser quebrados para recuperar a senha em texto simples ou usando no NTLM Relay e em ataques de pass-the-hash para fazer login como o usuário.

Este novo recurso permite que um administrador bloqueie NTLM de saída por SMB, evitando que a senha com hash de usuário seja enviada para um servidor remoto, evitando efetivamente esses tipos de ataques.

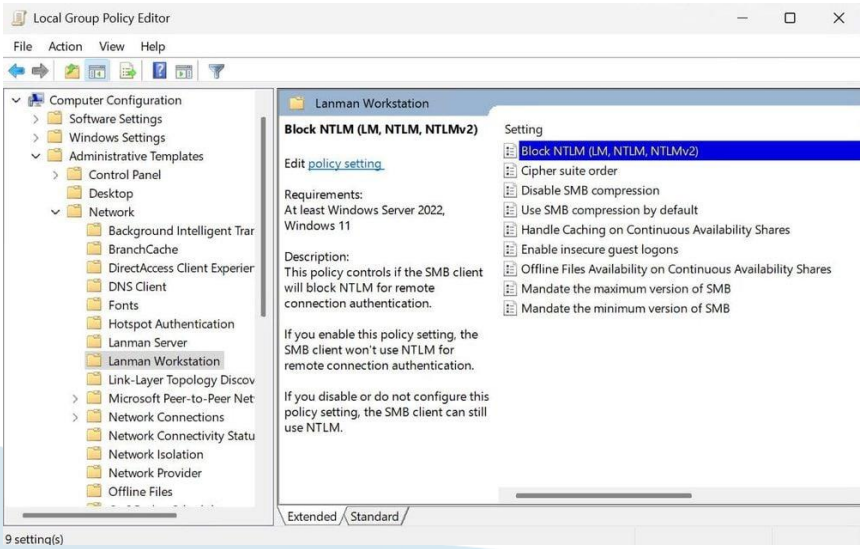


Figura 1 – Política de grupo de bloqueio de SMB NTLM.

De acordo com os engenheiros da Microsoft, esta nova opção poderá fornecer ao administrador o bloqueio intencional do Windows de oferecer NTLM via SMB.

O recurso estará disponível a partir do Windows 11 Insider Preview Build 25951, onde os administradores podem configurar o Windows para bloquear o envio de dados NTLM por SMB em conexões de saídas remotas utilizando a Política de Grupo e o PowerShell.

Além do mencionado, outra opção que está disponível a partir da compilação é o gerenciamento de dialeto SMB, que permite aos administradores bloquear a conexão de dispositivos Windows mais antigos e inseguros, desativando o uso de protocolos SMB mais antigos em sua organização.

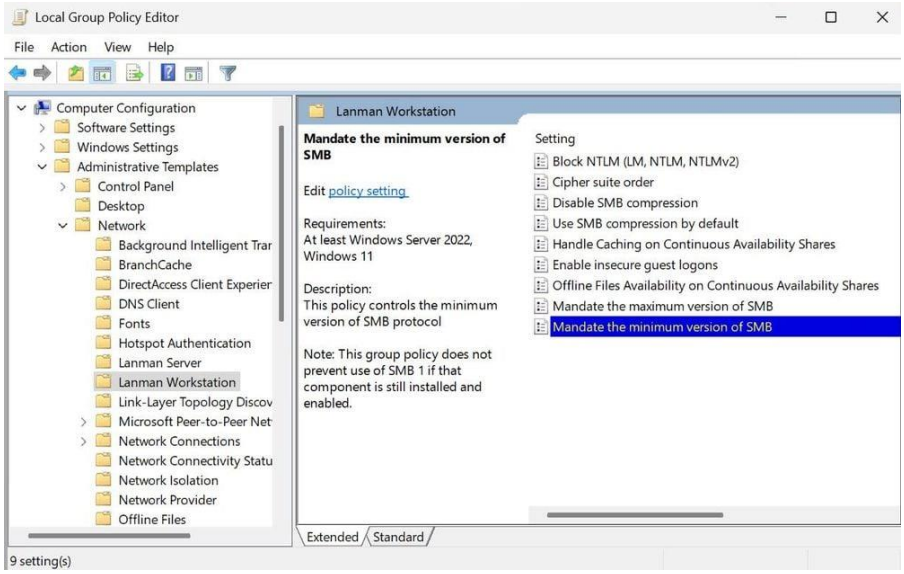


Figura 2 – Gerenciamento de dialeto de SMB.

De acordo com a Microsoft, estas atualizações fazem parte de uma iniciativa mais ampla para melhorar a segurança do Windows e do Windows Server.

2 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Comunicado Microsoft – Novo recurso de bloqueio NTLM**

heimdall
security research
A DIVISION OF ISH