Como “dibrar” a espionagem da Microsoft.

20 de junho de 20156 de setembro de 2015 / Kael

Sempre que ligamos o Windows, um teste de conexão é feito automaticamente através do NCSI (Network Connectivity Status Indicator). O computador faz uma requisição de um arquivo de texto no servidor do NSCI em que o Windows pode identificar quando o computador está conectado em uma rede, quando precisa de senha para alguns tipos de rede sem fio e quanto está conectado à internet.

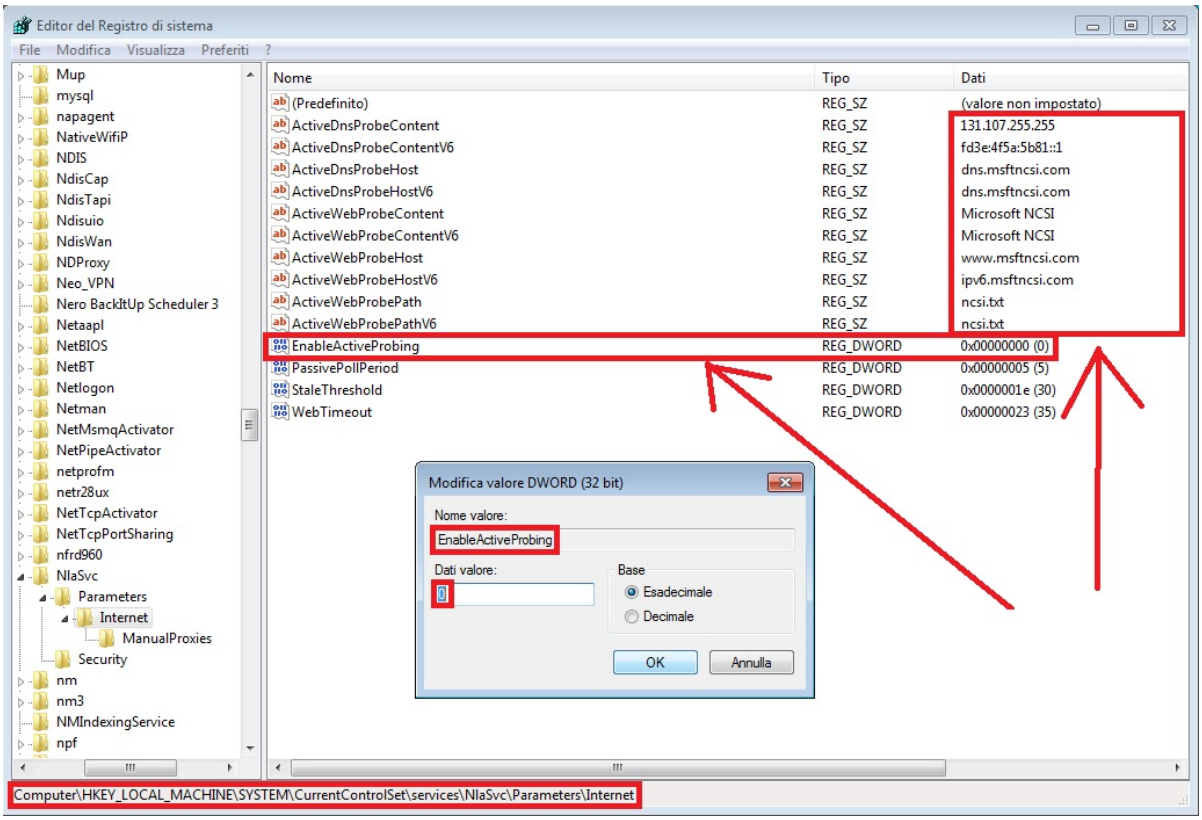
O NCSI facilita a verificação de problemas na conexão, permitindo que uma ajuda mais precisa seja fornecida para usuários básicos. O Windows tenta resolver o domínio www.msftncsi.com e ler o arquivo http://www.msftncsi.com/ncsi.txt, que é um arquivo de texto puro com o texto “Microsoft NCSI”. Numa outra verificação ele faz um dns lookup no dns.msftncsi.com e compara com o IP previamente armazenado nele. Se as coisas não baterem, sinal de que há algum problema na conexão então aparece a mensagem “sem acesso a internet” ou algo parecido.

Ou seja, sempre que o Windows tenta se conectar a um servidor da Microsoft, seu IP fica armazenado nos logs da Microsoft em uma conexão descriptografada.

A microsoft explica que esses IPs não são usados para identificar os usuários, em muitos casos, eles são os endereços de um NAT (network address translation) ou um servidor proxy e não o cliente por trás disso tudo.

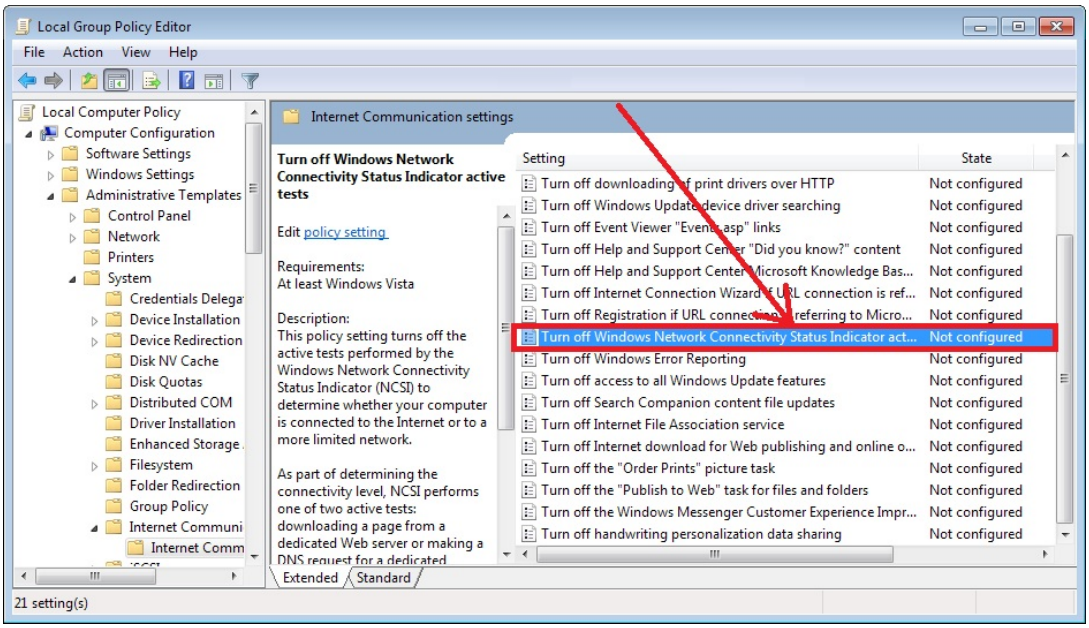
Caso queira bloquear isso:

1. Abra o Regedit (Iniciar > regedit)
2. Vá até HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > NLaSvc > Paramenters > Internet
3. A direita procure por EnableActiveProibing e altere o valor para 0



Caso queira ter mais certeza:

1. Abra gpedit.msc (Iniciar + R > gpedit.msc)
2. Vá até: Local Computer Policy > Computer Configuration > Administrative Templates > System > Internet Communication Management > Internet Communication Settings



Se você tiver paranoia e ainda quiser ter mais certeza:

1. Vá até C:WindowsSystem32driversetc
2. Abra o arquivo hosts
3. Cole as seguintes linhas:
   127.0.0.1 186.215.111.82
   127.0.0.1 www.msftncsi.com
   127.0.0.1 dns.msftncsi.com
4. Salve o arquivo

Ainda com paranoia? Use linux!

Fontes: Hackers Online Club, Hardware.com (antigo Guia do Hardware) e Microsoft

, ,