

ANALISE SEMANAL · SEMANA DE 6 A 13 DE OUTUBRO DE 2026

Dezessete técnicas, uma mediana de onze horas: o Active Directory é o segundo passo de quase todo ataque

A orientação conjunta de agências sobre comprometimento de Active Directory ganhou versão atualizada em setembro, com dezessete técnicas catalogadas. A leitura que a Sophos publicou em 7 de outubro acrescenta o número que falta no documento oficial: entre a primeira ação do atacante e a primeira tentativa contra o diretório, a mediana observada é de onze horas. Esta análise organiza as dezessete em quatro blocos, mostra o que cada bloco deixa em log e separa o que se resolve com configuração do que exige projeto.

ORIENTAÇÃO
ATUALIZADA EM
SETEMBRO DE 2026

17 TÉCNICAS
CATALOGADAS

MEDIANA DE 11
HORAS

67% DAS INTRUSÕES
POR IDENTIDADE

LEITURA LGPD

O que esta análise mostra: a orientação conjunta de agências sobre detecção e mitigação de comprometimento de Active Directory recebeu versão atualizada em setembro de 2026 e catalogou dezessete técnicas. Lidas em bloco, elas não descrevem dezessete problemas: descrevem quatro. Quatro técnicas pegam credencial a partir de posição comum no domínio. Cinco convertem credencial comum em privilégio alto e em movimento lateral. Três usam a infraestrutura que emite confiança, certificado e tiquete, para fabricar autenticação. Cinco mantêm acesso depois da resposta a incidente, inclusive atravessando para o ambiente de nuvem. A leitura da Sophos publicada em 7 de outubro acrescenta a dimensão de tempo que o documento oficial não traz: a mediana entre a primeira ação do atacante e a primeira tentativa contra o diretório é de onze horas, e 67% das intrusões estudadas em 2026 começaram por credencial comprometida ou por outra tática de identidade, incluindo roubo de token e abuso de relação de confiança. A consequência prática inverte a ordem usual dos projetos: o controle que paga mais rápido não é o de detecção avançada no diretório, é reduzir o que uma credencial comum alcança nas primeiras horas.

Quase nenhum ataque começa no Active Directory. Quase todo ataque passa por ele. Essa diferença é a razão pela qual o diretório raramente aparece no relatório de incidente como causa e quase sempre aparece como meio.

A orientação conjunta de agências sobre o tema foi atualizada em setembro e traz dezessete técnicas. É uma lista boa e difícil de usar, porque dezessete itens não cabem em uma reunião e não produzem ordem de prioridade. O que segue é uma tentativa de tornar a lista operável: quatro blocos, o que cada bloco exige do atacante, o que ele deixa em registro e qual controle corta mais.

A dimensão que falta no documento oficial

O relatório de adversário ativo da Sophos, citado na leitura que a empresa publicou em 7 de outubro, dá a mediana de onze horas entre a primeira ação observada e a primeira tentativa de alcançar o Active Directory. Onze horas é menos que um turno de plantão e muito menos que o tempo médio de escalada de um alerta de prioridade média em boa parte das operações.

O segundo número ajuda a fechar a conta: 67% das intrusões estudadas pela empresa em 2026 começaram por credencial comprometida ou por tática relacionada a identidade, como roubo de token e abuso de relação de confiança. Juntos, os dois dizem a mesma coisa de dois jeitos. A entrada é identidade, o destino é o diretório, e o intervalo é curto.

Isso muda a pergunta de orçamento. Investir primeiro em correlação sofisticada de evento de diretório só faz sentido se a equipe estiver de pé para agir dentro daquelas onze horas. Quando não está, o dinheiro rende mais em reduzir alcance: menos conta com privilégio, menos delegação, menos permissão de replicação.

Bloco 1. Acesso a credencial, a partir de posição comum

Quatro técnicas, e a característica comum é que nenhuma delas exige privilégio para começar. Qualquer conta de domínio serve.

- Pulverização de senha. Poucas tentativas por conta, muitas contas, para não disparar bloqueio. Aparece como volume anômalo de falha de autenticação distribuída, e não como ataque a uma conta.
- Kerberoasting. Pede tiquete de serviço para conta com SPN registrado e quebra a senha fora do ambiente. O insumo é a lista de SPN, que qualquer usuário autenticado pode consultar.
- AS-REP roasting. Mesma ideia contra conta que tem pré-autenticação Kerberos desabilitada. É configuração legada que sobrevive por compatibilidade.
- Senha em preferência de diretiva de grupo. Credencial gravada em GPP, legível por quem lê o volume de sistema do domínio. Antigo, conhecido, e ainda encontrado.

O que corta: MFA resistente a phishing para usuário privilegiado, remoção de conta de serviço desnecessária e de credencial legada, uso de conta de serviço gerenciada de grupo onde a aplicação permitir, e registro centralizado de autenticação. Em Kerberoasting, o controle que realmente resolve é tirar a senha humana do caminho, e não aumentar o comprimento dela.

Bloco 2. Escalada e movimento lateral

Cinco técnicas. Aqui o atacante já tem credencial e está convertendo alcance.

- Abuso de MachineAccountQuota. O valor padrão permite que usuário comum crie objeto de computador, e esse objeto é a base de vários caminhos de escalada.
- Delegação não restrita. Servidor com delegação irrestrita guarda tiquete de quem se autentica nele. Comprometer o servidor é colher credencial de quem passou por ali.
- DCSync. Pede replicação de diretório como se fosse controlador de domínio, e extrai material de credencial sem tocar no controlador.
- Extração do ntds.dit. A base do diretório inteira, geralmente via cópia de sombra de volume.
- Shadow Credentials. Escreve material de chave em atributo da conta alvo e passa a autenticar como ela, sem trocar senha e sem deixar o rastro de uma troca.

O que corta: restringir quem cria conta de computador, eliminar delegação que não tem justificativa, minimizar quem tem permissão de replicação, tratar controlador de domínio como sistema de camada zero e revisar acesso a atributo sensível do diretório. Shadow Credentials é o item que mais escapa de revisão, porque a alteração parece administrativa.

Bloco 3. Certificado e autenticação fabricada

Três técnicas, e é o bloco com a pior relação entre impacto e visibilidade.

- Abuso de AD CS, incluindo certificado dourado. Modelo de certificado mal configurado permite que a requisição informe o próprio nome de sujeito. O resultado é um certificado válido para autenticar como outra pessoa, emitido pela autoridade legítima da casa.
- Tíquete dourado. Com o segredo da conta krbtgt, o atacante emite tíquete de concessão arbitrário. O domínio aceita porque a assinatura é boa.
- Tíquete de prata. Mesma lógica em escopo de um serviço, com o segredo da conta daquele serviço. Mais discreto, porque não passa pelo controlador na hora do uso.

O que corta: endurecer modelo de certificado, restringir acesso à autoridade certificadora e aos controladores, proteger chave privada e backup dela, remover permissão de autenticação desnecessária e manter procedimento de rotação e de recuperação para os segredos críticos de Kerberos e de conta de computador. A recomendação de detecção mais útil deste bloco é monitorar quem emite confiança, ou seja, requisição de certificado, alteração de modelo e administração da autoridade, e não apenas a autenticação que vem depois.

Bloco 4. Persistência e travessia para a nuvem

Cinco técnicas. Este é o bloco que decide se a resposta a incidente funcionou.

- Golden SAML. Com a chave de assinatura da federação, o atacante forja asserção e entra na aplicação em nuvem sem passar pelo diretório local.
- Comprometimento do Entra Connect. O servidor de sincronização é ponte entre os dois mundos e costuma ter privilégio nos dois.
- Contorno de confiança unidirecional. A relação de confiança de mão única não é a fronteira que o desenho sugere.
- Abuso de SID History. Atributo pensado para migração que carrega privilégio de um domínio para outro.
- Skeleton Key. Altera o processo de autenticação na memória do controlador para aceitar uma senha mestra, mantendo as senhas legítimas funcionando.

O que corta: tratar Entra Connect, AD FS e controladores como camada zero, separar conta privilegiada local de conta privilegiada em nuvem, restringir relação de confiança, revisar SID History, endurecer LSASS e centralizar log de sincronização, de federação, de autenticação e de atividade administrativa. E uma regra de recuperação que quase nunca está no plano: validar credencial, token, confiança e sistema de autenticação, e não apenas o artefato inicial que abriu o caso.

O que a detecção precisa correlacionar

SINAL	POR QUE ELE IMPORTA
Requisição de tíquete de serviço em volume por uma conta	Insumo de Kerberoasting. Tíquete isolado é rotina; sequência é padrão.
Criação de objeto de computador por conta não administrativa	MachineAccountQuota em valor padrão, base de escalada.
Atividade de replicação fora de controlador de domínio	Assinatura de DCSync.

Alteração de modelo de certificado e requisição com nome de sujeito informado	Caminho de AD CS, o mais silencioso dos quatro blocos.
Logon com credencial explícita e mudança em atributo sensível	Shadow Credentials e preparação de persistência.
PowerShell e criação de processo em autoridade certificadora e em controlador	Execução onde não deveria haver execução interativa.

Nada disso funciona isolado. O ponto repetido na orientação e na leitura da Sophos é o mesmo: tratar cada requisição Kerberos como maliciosa produz ruído, e o que identifica ataque é a sequência. Quando a atividade de identidade parece suspeita, a revisão precisa olhar sessão, endpoint, alteração no diretório e atividade associada em nuvem antes de fechar o caso.

O que muda para quem opera no Brasil

- A migração para nuvem não aposentou o diretório, duplicou a fronteira. A maioria das operações de porte médio aqui está em modelo híbrido, com sincronização de identidade e federação. Isso significa que o bloco 4 é o mais relevante e o menos monitorado, porque o log de sincronização raramente chega ao SIEM.
- Conta de serviço com senha de anos é a regra, não a exceção. Sistema de ERP, de folha e de integração costuma rodar com conta nomeada criada por alguém que já saiu. Essa é a conta que o Kerberoasting procura, e a troca dela é projeto de aplicação, não de segurança.
- Controle de certificado está com outra equipe. Em muita empresa, a autoridade certificadora interna é operada pela infraestrutura e nunca foi tratada como sistema de identidade. O bloco 3 só melhora quando essa fronteira organizacional é resolvida.
- O artigo 46 da LGPD volta aqui, e é leitura nossa e não decisão publicada. Comprometimento de diretório costuma alcançar todo repositório de dado pessoal da organização de uma vez. Valor padrão de MachineAccountQuota, delegação irrestrita sem justificativa e senha em GPP são difíceis de sustentar como medida de segurança adequada diante de um incidente.
- Onze horas é o número que define a escala do plantão. Operação que detecta bem e escala em um dia útil não chega a tempo. Antes de comprar mais detecção, vale responder quem age às duas da manhã de domingo, e com qual autoridade para desconectar conta.

Leitura LATAMSEC

Há uma coisa curiosa nas dezessete técnicas: nenhuma é falha de software com CVE para corrigir. Todas são uso previsto de recurso previsto, em configuração que a instalação entrega por padrão ou que alguém escolheu por conveniência operacional. Delegação irrestrita existe para resolver um problema real. MachineAccountQuota com valor aberto existe para facilitar ingresso de máquina. Modelo de certificado permissivo existe porque alguém precisava emitir certificado rápido.

Isso tem uma consequência desconfortável para o ciclo de gestão de vulnerabilidade: o scanner não vai achar. Não há versão para subir, não há pacote para instalar. O trabalho é revisão de configuração e de permissão, que não gera número para o painel e não fecha ticket com satisfação.

Também explica por que esse conjunto de problemas sobrevive a trocas de fornecedor e de CISO. Ele não é uma dívida técnica que alguém contraiu em um projeto. É o acúmulo de vinte anos de decisões razoáveis, cada uma defensável no dia em que foi tomada, que juntas transformaram o diretório no ponto onde todo acesso se

encontra.

Quatro perguntas para levar à próxima reunião de arquitetura.

Para quem opera o diretório: quantas contas podem replicar o diretório hoje, e quantas delas são controladores?

Para quem responde pela identidade: qual é a senha de conta de serviço com SPN mais antiga ainda em uso, e qual aplicação depende dela?

Para quem responde pela nuvem: o log do servidor de sincronização e o da federação chegam ao mesmo lugar que o log do controlador de domínio?

Para o comitê de risco: o plano de recuperação prevê rotação de krbtgt e revalidação de confiança, ou termina na restauração do servidor comprometido?

Três evidências que um conselho pode exigir

EVIDÊNCIA 1

Lista de contas de serviço com SPN registrado, com data da última troca de senha

É o insumo exato do Kerberoasting. Conta de serviço com SPN, senha antiga e algoritmo fraco é o alvo de menor custo dentro do domínio. Se a lista não existe, a superfície é desconhecida.

EVIDÊNCIA 2

Relação de quem pode replicar o diretório e de quem pode criar objeto de computador

O primeiro conjunto define quem consegue DCSync. O segundo define se MachineAccountQuota ainda está no valor padrão. As duas respostas são consultas simples e quase nunca estão documentadas.

EVIDÊNCIA 3

Inventário de modelo de certificado que permite informar o próprio nome de sujeito

É o caminho de abuso de AD CS que transforma um usuário comum em administrador de domínio sem tocar em senha. Controle de certificado é controle de identidade, e costuma estar com outra equipe.

Fontes

- ASD's ACSC · Detecting and mitigating Active Directory compromises. orientação conjunta de agências, com as dezessete técnicas e as mitigações recomendadas, em versão atualizada de setembro de 2026.
<https://www.cyber.gov.au/business-government/detecting-responding-to-threats/detecting-and-mitigating-active-directory-compromises>
- Sophos · CISA's 17 Common Active Directory Compromise Techniques: A Sophos MDR Perspective. com a mediana de onze horas até a primeira tentativa, a proporção de intrusões iniciadas por identidade e casos de resposta.
<https://www.sophos.com/en-us/blog/cisa-active-directory-compromise-techniques>
- NCSC Nova Zelândia · Detecting and mitigating Active Directory compromises. com a adoção nacional da mesma orientação e o recorte para organizações menores.
<https://www.ncsc.govt.nz/protect-your-organisation/detecting-and-mitigating-active-directory-compromises/>
- GovTech Review · New guidance on detecting and mitigating AD compromises released. com o contexto de publicação e o alcance pretendido da orientação.
<https://www.govtechreview.com.au/content/gov-security/news/new-guidance-on-detecting-and-mitigating-ad-compromises-released-100932599>

Análise semanal publicada em 13 de outubro de 2026 em latamsec.com.br/recursos/active-directory-dezessete-tecnicas/.

Reprodução permitida com crédito e link. As leituras marcadas como nossas são opinião editorial da LATAMSEC e não decisão de autoridade.