Abuso de acesso remoto é o maior indicador pré-ransomware - Against In

Data: 2025-09-09 10:44:45

Autor: Inteligência Against Invaders

Abusos de Software de acesso remoto e os serviços são os indicadores ‘pré-ransomware’ mais comuns, de acordo com uma nova pesquisa da Cisco Talos.

Os adversários frequentemente utilizam serviços remotos legítimos, como RDP, PsExec e PowerShell, observaram os pesquisadores. Além disso, softwares de acesso remoto como AnyDesk, Atera e Microsoft Quick Assist eram frequentemente explorados.

A Cisco identificou essas táticas, técnicas e procedimentos (TTPs) como parte dos esforços dos cibercriminosos para obter acesso de administrador de domínio de nível empresarial em sistemas comprometidos.

Pré-ransomwarerefere-se ao estágio de um ataque em que os adversários realizam atividades como escalonamento de privilégios, coleta de credenciais e implantação de acesso remoto sem ainda executar criptografia em grande escala.

As mitigações sugeridas contra o abuso de tal software e serviços de acesso remoto incluem:

- Configure soluções de segurança para permitir que apenas aplicativos benignos comprovados sejam iniciados e impedir a instalação de software inesperado
- Exigir MFA em todos os serviços críticos, incluindo acesso remoto e serviços de gerenciamento de acesso de identidade (IAM), e monitorar o uso indevido de MFA
- Implantar ferramentas como o Monitor do Sistema no Windows para visibilidade e registro em log do ponto de extremidade

Leia agora: Como as ferramentas de acesso remoto esquecidas estão colocando as organizações em risco

Outro TTP comum pré-ransomware era o despejo de credenciais do sistema operacional. Essa técnica está relacionada aos esforços para extrair credenciais de conta de um sistema comprometido para permitir o movimento lateral.

Os pesquisadores observaram que as principais técnicas/locais de despejo de credenciais incluíam o registro do controlador de domínio, a seção de registro SAM, o AD Explorer, o LSASS e o NTDS. DIT.

O código aberto Mimikatz também é frequentemente usada para extrair credenciais.

A descoberta de serviços de rede também foi destacada como uma tática pré-ransomware

significativa. As principais ferramentas e comandos observados usados para descoberta de serviços de rede incluíram netscan, nltest e netview.

“Priorizar a moderação do uso de serviços remotos e software de acesso remoto e/ou proteger os armazenamentos de credenciais mencionados acima pode ajudar a limitar a maioria dos adversários vistos nesses compromissos pré-ransomware”, observaram os pesquisadores.

Os pesquisadores disseram ter grande confiança de que todos os incidentes incluídos no estudo envolveram táticas consistentemente vistas como precedendo a implantação do ransomware.

Chave de resposta rápida para evitar a implantação de ransomware

O Cisco Talos estudar, publicado em 8 de setembro, destacou a resposta rápida como fundamental para evitar a ocorrência de incidentes graves de ransomware.

Quando o Talos Incident Response (IR) foi acionado dentro de um a dois dias após a primeira atividade observada, a execução do ransomware foi impedida em um terço (32%) dos casos em que os ataques foram impedidos com sucesso.

Um alerta EDR/MDR que levou à contenção das equipes de segurança em duas horas foi identificado como um fator que contribuiu para o impedimento de 32% dos ataques.

Uma notificação de parceiros do governo dos EUA e representantes de seu provedor de serviços gerenciados (MSP) sobre uma possível preparação de ransomware em seu ambiente impediu a execução de ransomware em 14% dos casos.

Isso inclui alertas da Agência de Segurança Cibernética e Infraestrutura (CISA) Iniciativa de notificação pré-ransomware, lançado em março de 2023.

As restrições de segurança das organizações foram fundamentais para impedir as cadeias de ataque em 9% dos compromissos bem-sucedidos. Em um exemplo, os agentes de ameaças comprometeram uma conta de serviço na organização de destino, mas as restrições de privilégio apropriadas na conta impediram suas tentativas de acessar sistemas importantes, como controladores de domínio.