Warlock Ransomware explora falhas do SharePoint para acesso inicial e r

Data: 2025-08-21 23:45:05

Autor: Inteligência Against Invaders

O Warlock Ransomware Group intensificou suas operações, direcionando os servidores não

atingidos no Microsoft SharePoint, alavancando vulnerabilidades críticas para obter execução de

código remoto e acesso inicial à rede.

Esta campanha, observada em meados de 2025, envolve o envio de solicitações de postagem HTTP criadas para fazer upload de conchas da web, facilitando o reconhecimento, Escalada de privilégiose roubo de credenciais.

Exploração inicial

Os invasores exploram falhas como CVE-2023-27532 em software de backup de Veeam desatualizados e recentemente divulgou problemas de desserialização do SharePoint, permitindo que eles ignorem a autenticação e a entrada em ambientes corporativos.

As vítimas abrangem vários continentes, incluindo América do Norte, Europa, Ásia e África, com setores como governo, finanças, fabricação, tecnologia e infraestrutura crítica afetadas fortemente.

As táticas de Warlock ecoam as de grupos como Black Basta, sugerindo possíveis afiliações ou rebranding, e demonstram uma rápida evolução de anúncios do fórum em junho de 2025 a ataques globais sofisticados.

Ao abusar de objetos de política de grupo para escalada de privilégios, os invasores criam novos GPOs, ativam contas de convidados e os adicionam aos grupos de administradores, concedendo acesso elevado para um compromisso adicional.

Uma vez lá dentro, os operadores de warlock empregam uma cadeia de ataque de várias etapas que inclui evasão de defesa, descoberta, Acesso à credenciale exfiltração.

Eles usam ferramentas Windows embutidas como CMD.EXE e NLTEST para enumeração de confiança do domínio, coleta de informações do sistema via ipconfig e lista de tarefas e descoberta de contas por meio de comandos de grupo líquido.

Cadeia de ataque

O dumping de credenciais é alcançado com o Mimikatz para extrair senhas de texto simples da memória e despejando colméias de Sam e Registro de Segurança, geralmente por meio de ferramentas como o CrackMapexec.

O movimento lateral ocorre sobre ações da SMB para copiar cargas úteis, incluindo binários renomeados como vmtools.exe (detectados como Trojan.win64.killav.i), que encerra os processos de segurança instalando um driver malicioso chamado Googleapiutil64.sys e matar repetidamente alvos listados em arquivos Log.txt.

A implantação do ransomware anexa a extensão .x2anylock a arquivos criptografados, solta as notas de resgate e exfiltrações de dados usando rclone disfarçado como tendrection.exe em contas de unidade de prótons.

O malware, um derivado Lockbit 3.0, evita criptografar extensões de permissões, diretórios e nomes de sistemas específicos para manter a furtividade operacional.

Nas cadeias anteriores, os atacantes usaram a DLL lateral com executáveis ??legítimos como mpcmdrun.exe e jcef_helper.exe para carregar cargas úteis maliciosas, substituindo discos com writenull.exe para impedir a recuperação.

Esse ataque ressalta os riscos de remendos atrasados ??e a necessidade de defesas em camadas. As organizações devem aplicar patches da Microsoft para vulnerabilidades do SharePoint imediatamente e monitorar indicadores, como modificações suspeitas de GPO, RDP não autorizado, ou o tunelamento de protocolo por meio de binários renomeados em nuvem.

De acordo com o relatórioA plataforma Vision One da Trend Micro fornece a detecção de IOCs de Warlock através de consultas de caça de ameaças, atualizações de inteligência e regras proativas que bloqueiam tentativas de exploração, terminações de processo e exfiltração.

É essencial o monitoramento contínuo de dumping de credenciais, movimento lateral e execuções de comando anormais, além de restringir as ações administrativas e a manutenção de assinaturas de segurança atualizadas para combater variantes de ransomware em evolução como a Warlock.

Indicadores de compromisso (IOCs)

SHA-1 HASH	Nome da detecção
0BBBF2A9D49152AC6AD755167CCB0F2B4F00B976	Ransom.win32.warlock.a.note
CF0DA7F6450F09C8958E253BD606B83AA8058F2	Ransom.win32.warlock.a
8B13118B378293B9DC891B57121113D0AEA3AC8A	Ransom.win32.warlock.a
0488509B4DBC16DCB6D5F531E3C8B9A59B69E522	Trojan.win64.killav.i

Encontre esta notícia interessante! Siga -nosGoogle News Assim,LinkedIn eX Para obter atualizações instantâneas!