Os invasores abusam do ConnectWise ScreenConnect para descartar o As

Data: 2025-09-11 09:51:15

Autor: Inteligência Against Invaders

Os invasores abusam do ConnectWise ScreenConnect para descartar o AsyncRAT

Os hackers exploram o ConnectWise ScreenConnect para derrubar o AsyncRAT por meio de carregadores de script, roubando dados e persistindo com um atualizador falso do Skype.

Pesquisadores da LevelBlue alertam para uma campanha que abusa ConnectWise ScreenConnect para implantar Classificação AsyncRAT. Os invasores usam carregadores VBScript/PowerShell e obtêm persistência por meio de um atualizador falso do Skype.

O ConnectWise ScreenConnect é um software de desktop remoto e suporte remoto projetado para permitir acesso seguro e em tempo real a computadores e dispositivos de qualquer lugar. Profissionais de TI, provedores de serviços gerenciados (MSPs) e empresas o utilizam amplamente para solucionar problemas, manter e gerenciar endpoints remotamente.

O ataque começou com um cliente ScreenConnect comprometido, os agentes de ameaças iniciaram uma sessão interativa por meio de um domínio malicioso (relay.shipperzone[.]online) vinculados a implantações não autorizadas do ScreenConnect.

Um VBScript disparou comandos do PowerShell que buscaram duas cargas, armazenaram-nas na pasta pública e as executaram diretamente na memória. Os invasores decodificaram e executaram assemblies .NET diretamente na memória em vez de salvar executáveis no disco, usando um truque clássico de malware sem arquivo que torna a detecção e a defesa muito mais difíceis.

“As duas cargas úteis, logs.ldk e logs.ldr, foram baixadas de um servidor remoto. Esses arquivos foram gravados no diretório C:UsersPublic e carregados na memória usando reflexão. O script converteu a carga útil do primeiro estágio (logs.ldk) em uma matriz de bytes e passou a segunda (logs.ldr) diretamente para o método Main(). O script recupera dados codificados da Web, decodifica-os na memória e invoca um método em um assembly .NET carregado dinamicamente.” lê o relatório publicado pela LevelBlue.

“Essa técnica exemplifica o malware sem arquivo: nenhum executável é gravado no disco e toda a lógica maliciosa é executada na memória.”

Obfuscator.dll é o primeiro estágio na memória da cadeia de infecção AsyncRAT. Ele inicia a execução, configura a persistência por meio de um falso “Skype Updater” e desativa defesas como AMSI e ETW. O malware inclui três classes principais para lidar com inicialização, carregamento dinâmico de carga útil e táticas anti-análise, garantindo furtividade e preparando o sistema para a

carga útil principal.

AsyncClient.exe é o mecanismo C2 central da cadeia de ataque AsyncRAT. Ele descriptografa a configuração com AES-256, conecta-se a servidores C2 e analisa comandos por meio de um protocolo personalizado. O malware reúne detalhes do sistema e de segurança, monitora a atividade do usuário com um keylogger e exfiltra dados confidenciais, como extensões de navegador. O malware mantém a persistência por meio de tarefas agendadas usando a função CreateLoginTask() vista em Obfuscator.dll ou recriada de forma redundante a partir de AsyncClient.

"O malware sem arquivo continua a escapar das defesas modernas devido à sua natureza furtiva e dependência de ferramentas legítimas do sistema para execução", conclui o relatório. "Essa abordagem ignora a detecção tradicional baseada em disco operando na memória, tornando essas ameaças mais difíceis de detectar, analisar e erradicar."

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,AsyncRAT)