MostereRAT tem como alvo usuários do Windows com táticas furtivas - Ag

Data: 2025-09-09 07:43:34

Autor: Inteligência Against Invaders

Uma campanha de phishing que oferece uma nova variedade de malware, o MostereRAT, foi descoberta por pesquisadores de segurança cibernética. O Trojan de Acesso Remoto (RAT) tem como alvo os sistemas Microsoft Windows e dá aos invasores controle total sobre as máquinas comprometidas.

De acordo com o FortiGuard Labs, que descobriu a ameaça, o que diferencia essa campanha é o uso em camadas de técnicas avançadas de evasão. O malware é escrito em Easy Programming Language (EPL), uma linguagem de codificação baseada em chinês raramente usada em ataques cibernéticos, e depende de vários estágios para ocultar o comportamento malicioso.

Ele pode desativar ferramentas de segurança, bloquear o tráfego antivírus e estabelecer comunicações seguras com seu servidor de comando e controle (C2) usando TLS mútuo (mTLS).

Cadeia de ataque e entrega

A campanha começa com e-mails de phishing que parecem ser consultas comerciais legítimas, visando principalmente usuários japoneses. Depois que a vítima clica em um link, um documento do Word contendo um arquivo oculto é baixado. Esse arquivo direciona o usuário a abrir um executável incorporado, que inicia o malware.

O executável descriptografa seus componentes e os instala no diretório do sistema. Os serviços são então criados para garantir a persistência, com alguns sendo executados sob privilégios de nível SYSTEM para acesso máximo. Antes de fechar, o programa exibe uma mensagem falsa em chinês simplificado sugerindo que o arquivo é incompatível, uma tática destinada a incentivar a disseminação adicional.

Leia mais sobre campanhas de phishing direcionadas aos mercados asiáticos: Campanha ShadowSilk tem como alvo governos da Ásia Central

Lauren Rucker, analista sênior de inteligência de ameaças cibernéticas da Deepwatch, disse: “Dado que o vetor de ataque inicial são os e-mails de phishing que levam a links maliciosos e downloads de sites, a segurança do navegador é uma área crítica para a defesa”.

Ela acrescentou que a aplicação de políticas que restringem downloads automáticos e limitam os privilégios do usuário pode ajudar a evitar o escalonamento para SYSTEM ou TrustedInstaller.

O MostereRAT usa vários métodos para interferir nas proteções de segurança. Ele pode desativar o Windows Update, encerrar processos antivírus e impedir que as ferramentas de segurança se comuniquem com seus servidores.

O malware também aumenta os privilégios imitando a conta TrustedInstaller, uma das mais poderosas em sistemas Windows.

“Embora esse malware use algumas técnicas criativas para evitar a detecção, encadeando novas linguagens de script com ferramentas confiáveis de acesso remoto, ele ainda segue um padrão comum de exploração de usuários e endpoints superprivilegiados sem controle de aplicativos”, explicou James Maude, CTO de campo da BeyondTrust.

Recursos e ferramentas de acesso remoto

Uma vez estabelecido, o RAT suporta uma ampla gama de funções, incluindo:

- Keylogging e coleta de informações do sistema
- Baixando e executando cargas nos formatos EXE, DLL, EPK ou shellcode
- Criando contas de administrador ocultas para persistência
- Execução de ferramentas de acesso remoto como AnyDesk, TightVNC e RDP Wrapper

Laboratórios FortiGuard Observou que partes da infraestrutura do malware estavam anteriormente vinculadas a um trojan bancário relatado em 2020. Sua evolução para *MostereRAT* destaca como os agentes de ameaças continuam a refinar técnicas para escapar dos sistemas de detecção modernos.

Maude enfatizou a importância de reduzir privilégios e controlar aplicativos. “Se você remover o privilégio de administrador local, reduzirá muito a superfície de ataque e limitará o impacto de uma infecção por malware”, concluiu.