Grupo de crimes cibernéticos de língua chinesa sequestra servidores IIS p

Data: 2025-10-03 15:59:00

Autor: Inteligência Against Invaders

Um grupo de crimes cibernéticos de língua chinesa está sequestrando serviços confiáveis de

informações da Internet (IIS) em todo o mundo para executar golpes de SEO que redirecionam os

usuários para anúncios obscuros e sites de jogos de azar, descobriu o Cisco Talos.

O grupo, rastreado como UAT-8099, explora servidores IIS que têm uma boa reputação para manipular os resultados dos mecanismos de pesquisa para obter ganhos financeiros.

Os servidores IIS comprometidos redirecionam os usuários para anúncios não autorizados ou sites de jogos de azar ilegais.

Os servidores IIS afetados foram identificados na Índia, Tailândia, Vietnã, Canadá e Brasil, visando organizações como universidades, empresas de tecnologia e provedores de telecomunicações. Isso foi baseado no censo de arquivos da Cisco e na análise de tráfego DNS.

A maioria de seus alvos são usuários móveis, abrangendo não apenas dispositivos Android, mas também dispositivos Apple iPhone.

O Cisco Talos detalhou a cadeia de ataque completa e as descobertas adicionais relacionadas à campanha UAT-8099 em um blogue publicado em 2 de outubro de 2025.

A empresa explicou que, quando o grupo descobre uma vulnerabilidade no servidor de destino, ele carrega um shell da web para coletar informações do sistema e realiza o reconhecimento na rede do host.

Quando a coleta de informações for concluída, o UAT-8099 habilitará a conta de convidado, escalonará seus privilégios para o nível de administrador e usará essa conta para habilitar o protocolo de área de trabalho remota (RDP).

Para persistência, os hackers combinam o acesso RDP comSoftEther VPN,Mais fácil(uma ferramenta de rede privada virtual descentralizada) e o PRFVferramenta de proxy reverso.

Em seguida, o grupo executa mais escalonamento de privilégios usando ferramentas compartilhadas para obter permissões no nível do sistema e instalar o BadIIS malware.

Para garantir sua posição, eles implantam mecanismos de defesa para evitar que outros agentes de ameaças comprometam o mesmo servidor ou interrompam sua configuração.

Novas amostras de malware identificadas

O Cisco Talos identificou a atividade do grupo em abril de 2025 e encontrou várias novas amostras de malware BadIIS na campanha.

Em sua análise, a Talos disse que as variantes do BadIIS usadas nesta campanha revelaram semelhanças funcionais e de padrão de URL com uma variante documentada anteriormente em 2021.

Esta versão, no entanto, tinha uma estrutura de código alterada e um fluxo de trabalho funcional para evitar a detecção por produtos antivírus.

O Talos identificou várias instâncias do malware BadIIS no VirusTotal este ano, um cluster com detecção muito baixa e outro contendo strings de depuração em chinês simplificado.