Servidores IIS comprometidos por hackers chineses para manipulação de

Data: 2025-10-03 08:05:31

Autor: Inteligência Against Invaders

A Cisco Talos revelou que o UAT-8099, um grupo de crime cibernético de língua chinesa, vem explorando servidores vulneráveis ??de serviços de informação na Internet (IIS) em vários países para conduzir Otimização do mecanismo de pesquisa (SEO) Fraude e roubar dados de alto valor.

Identificada em abril de 2025, este grupo tem como alvo servidores respeitáveis ??do IIS na Índia, Tailândia, Vietnã, Canadá e Brasil, com foco em organizações como universidades, empresas de tecnologia e fornecedores de telecomunicações.

Seu principal objetivo é aumentar o ranking de pesquisa de sites maliciosos e redirecionar o tráfego legítimo para anúncios não autorizados e plataformas ilegais de jogo.

Visão geral da campanha

A campanha UAT-8099 começa com o reconhecimento em servidores IIS não patches que permitem uploads de arquivos irrestritos.

Depois que uma vulnerabilidade é encontrada, os atores de ameaças carregam um shell da web ASP.NET de código aberto para executar comandos e reunir informações do sistema.

Esse acesso inicial permite que eles criem e elevem uma conta de usuário convidado aos privilégios do administrador, permitindo o acesso ao RDP (Remote Desktop Protocol).

O grupo então implanta conchas da Web e usa ferramentas de hackers de código aberto ao lado do ataque de cobalto para estabelecer e manter a persistência.

Cisco Talos descoberto Várias novas variantes de malware Badiis nesta campanha, incluindo clusters com detecção de antivírus mínima e aqueles que contêm mensagens de depuração chinesa simplificadas.

Após obter acesso inicial, o UAT-8099 assegura o controle de longo prazo, ativando o RDP, instalando o Softether VPN, usando a ferramenta VPN descentralizada easyTier e a configuração do proxy reverso do FRP.

Eles escalam privilégios com ferramentas públicas, dump credenciais usando o ProcDump e compactam dados roubados com Winrar. Para bloquear outros atacantes, eles instalam o D_SAFE_MANAGE, uma ferramenta conhecida de segurança do Windows IIS.

Os scripts de automação do grupo otimizam tarefas como instalação de módulos, configuração de

RDP e criação de tarefas programadas para margar um berçal de cobalto sob o disfarce de um provedor de código WMI legítimo.

As defesas em camadas e os scripts personalizados os ajudam a evitar a detecção e a manter o acesso ininterrupto a servidores comprometidos.

Manipulação e impacto de SEO

Depois que a persistência é estabelecida, o malware badiis é usado para manipular rastreadores de mecanismos de busca e visitantes humanos.

O manipulador OnBeginRequest verifica os cabeçalhos HTTP quanto aos valores do agente de usuário e do referente para determinar se atuam como proxy ou injetar javascript malicioso.

Quando o Googlebot é detectado, o malware serve conteúdo ou backlinks criados para inflar rankings de pesquisa. Para usuários humanos referidos nos mecanismos de pesquisa, ele injeta JavaScript que redireciona os navegadores para sites de jogos de azar ou anúncio.

O manipulador OnsendResponse aprimora ainda mais a fraude, fornecendo conteúdo focado em SEO projetado especificamente para rastreadores, seguido de redirecionamentos direcionados para os usuários que encontram páginas de erro.

Ao comprometer vários servidores do IIS em todo o mundo, o UAT-8099 cria uma rede de sites de alta realização que aumentam coletivamente a visibilidade de seus destinos maliciosos.

Os usuários móveis nos dispositivos Android e iOS são particularmente afetados, pois os servidores comprometidos servem páginas de download de aplicativos APK e iOS personalizados.

A Cisco Talos continua monitorando esta campanha, pedindo às organizações que protejam seus servidores do IIS aplicando os patches mais recentes, restringindo os tipos de upload de arquivos, aplicando políticas de contas fortes e implantando soluções robustas de monitoramento.

A falha em abordar essas vulnerabilidades não apenas corre o risco de interrupção operacional, mas também facilita a fraude de SEO em larga escala e o roubo de credenciais.