Microsoft IIS sob ataque de hackers criminosos chineses: como o UAT-809

Data: 2025-10-04 08:35:50

Autor: Inteligência Against Invaders

Redazione RHC**:4 Outubro 2025 09:08**

Um grupo cibercriminoso chinês conhecido como UAT-8099 foi identificado pelo Cisco Talos como responsável por uma campanha de ataque em larga escala. Os ataques, que começaram em abril de 2025, visaram principalmente **Microsoft Internet Information Services (IIS) vulnerável** servidores localizados em vários países, incluindo *Índia, Tailândia, Vietnã, Canadá e Brasil, que foram sistematicamente visados.*

As organizações que gerenciam servidores IIS são aconselhadas a aplicar imediatamente os patches de segurança mais recentes e restringir os tipos de uploads de arquivos permitidos, pois os usuários de dispositivos móveis Android e iOS são particularmente vulneráveis a páginas de download de APK personalizadas e sites de hospedagem de aplicativos iOS disfarçados de recursos oficiais.

Seus focos de atividade ilícita **sobre a alteração dos índices de otimização de mecanismos de pesquisa (SEO)** Para *canalizar tráfego de alto valor para publicidade não autorizada e sites de jogos de azar ilegais,* ao mesmo tempo em que extrai dados confidenciais de instituições de prestígio.

A primeira fase da campanha UAT-8099 envolve **executando verificações automáticas para detectar servidores IIS desatualizados** que permitem *uploads de arquivos irrestritos.* Uma vez que um **servidor mal configurado** for detectado, os operadores implantam um **shell da web ASP.NET de código aberto** , que executa comandos do sistema e coleta informações sobre o ambiente.

A presença desse ponto de suporte permite gerar uma conta de usuário temporária, à qual são atribuídos direitos de administrador, **habilitando o acesso por meio do Remote Desktop Protocol (RDP).** Em seguida, o grupo passa a *instalar web shells adicionais e usa ferramentas públicas de hacking combinadas com o Cobalt Strike para garantir a persistência do sistema.*

Durante esta fase, Pesquisadores do Talos **identificou várias novas versões da família de malware BadIIS.** Essas mesmas variantes mostraram detecção mínima por programas antivírus e incluíram mensagens de depuração em chinês simplificado, sugerindo desenvolvimento contínuo por invasores de língua chinesa.

Para consolidar o controle, o UAT-8099 ativa o RDP, instala **SoftEther VPN e a ferramenta VPN EasyTier não centralizada** e configura túneis de proxy reverso FRP. Segue-se o despejo de credenciais usando Procdump e a compactação de dados com o WinRAR. D_Safe_Manage, uma ferramenta de segurança do IIS usada para fins maliciosos, é instalada para monitorar invasores

concorrentes.

Quando o Googlebot é detectado, *o operador veicula conteúdo e backlinks especialmente criados para rastreadores de mecanismos de pesquisa,* **aumentando artificialmente a reputação do servidor e otimizando as classificações de sites maliciosos.** Caso contrário, os usuários humanos que chegam por meio de mecanismos de pesquisa recebem um código JavaScript que os redireciona automaticamente para sites de jogos de azar ou publicidade.

A implementação de soluções de segurança avançadas, como políticas de senha rigorosas e mecanismos de bloqueio de conta com limites bem definidos, combinados com o monitoramento constante dos logs do servidor web, é uma defesa crucial contra técnicas de ataque como o UAT-8099. A adoção de ferramentas de detecção de endpoint com recursos de análise comportamental também pode ser crucial na identificação do uso anômalo de web shells e beacons específicos como o Cobalt Strike.

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli