GhostRedirector surge como novo ator de ameaça alinhado à China

Data: 2025-09-04 16:45:35

Autor: Inteligência Against Invaders

Um grupo de hackers recém-identificado comprometeu pelo menos 65 servidores Windows em todo

o mundo, principalmente no Brasil, Tailândia e Vietnã.

De acordo com os pesquisadores da ESET, o grupo, chamado GhostRedirector, implantou duas ferramentas anteriormente desconhecidas: um backdoor C ++ chamado Rungan e um módulo malicioso de Serviços de Informações da Internet (IIS) conhecido como Gamshen.

O Rungan permite que os invasores executem comandos em servidores comprometidos. Gamshen, por sua vez, manipula os resultados dos mecanismos de pesquisa para inflar artificialmente as classificações de determinados sites, principalmente plataformas de jogos de azar.

Essa tática, descrita como fraude de SEO como serviço, aproveita os servidores comprometidos para melhorar as classificações das páginas sem afetar os visitantes regulares.

“Gamshen […] não veicula conteúdo malicioso ou afeta os visitantes regulares dos sites – a participação no esquema de fraude de SEO pode prejudicar a reputação do site host comprometido, associando-o a técnicas obscuras de SEO e aos sites impulsionados”, explicou a ESET.

Além disso, os pesquisadores observaram que o GhostRedirector também dependia de exploits conhecidos, como BadPotato e EfsPotato, para obter privilégios de administrador. Esses escalonamentos permitiram a criação de novas contas, garantindo que os invasores pudessem manter o acesso mesmo que outro malware fosse removido.

Leia mais sobre malware IIS e esquemas de fraude de SEO: Malware BadIIS explora servidores IIS para fraude de SEO

Os ataques não se limitaram a um setor. A ESET observou vítimas em um amplo conjunto de setores, incluindo saúde, seguros, varejo, transporte, tecnologia e educação.

Os servidores mais afetados estavam localizados no Brasil, Peru, Tailândia, Vietnã e EUA, embora clusters menores tenham sido vistos no Canadá, Finlândia, Índia, Holanda, Filipinas e Cingapura.

Os investigadores concluíram com confiança média que o GhostRedirector está alinhado com a China. Vários indicadores apoiaram isso, incluindo strings chinesas codificadas, um certificado de assinatura de código vinculado a uma empresa chinesa e uma senha contendo a palavra mandarim “huang” – chinês para amarelo.

Essa atividade se assemelha à de outro grupo alinhado à China, o DragonRank, anteriormente ligado à fraude de SEO. Embora haja alguma sobreposição na geografia e nos setores-alvo, a ESET enfatizou que não há evidências de que os dois grupos estejam conectados.

O GhostRedirector está ativo desde pelo menos agosto de 2024, de acordo com a ESET. A campanha destaca como os módulos nativos do IIS podem ser abusados para manipular silenciosamente as classificações de pesquisa.

Ao incorporar código malicioso no software de servidor web da Microsoft, os invasores não apenas obtêm persistência, mas também usam plataformas legítimas para canalizar o tráfego para sites obscuros.

Pesquisadores da ESET alertaram que tais campanhas podem corroer a confiança em organizações comprometidas, mesmo quando os usuários finais não são diretamente prejudicados.

Para se defender contra ameaças semelhantes, os especialistas em segurança aconselham as organizações a monitorar os servidores IIS em busca de módulos incomuns, aplicar patches de segurança oportunos, restringir o uso de contas de alto privilégio e revisar a atividade do PowerShell em busca de downloads suspeitos.

Auditorias regulares de configurações de servidor e contas de usuário também podem ajudar a detectar persistência maliciosa antes que ela cause danos a longo prazo.