Atores de ameaças explorando máquinas das vítimas para monetização de

Data: 2025-08-21 20:41:10

Autor: Inteligência Against Invaders

Os pesquisadores de segurança cibernética descobriram uma campanha em andamento em que os atores de ameaças exploram a vulnerabilidade crítica do CVE-2024-36401 no Geoserver, um banco de dados geoespacial, para executar remotamente o código e monetizar a largura de banda das vítimas.

Essa falha de execução remota de código, classificada em uma pontuação CVSS de 9,8, permite que os invasores implantem kits legítimos de desenvolvimento de software (SDKs) ou aplicativos modificados que geram renda passiva por meio de compartilhamento de rede ou proxies residenciais.

A abordagem imita estratégias de monetização benigna usadas pelos desenvolvedores de aplicativos, evitando anúncios tradicionais para manter a experiência do usuário e a retenção de aplicativos.

Essas aplicações maliciosas operam silenciosamente, consumindo recursos mínimos enquanto lucra com a largura de banda não utilizada, sem distribuir malware evidente.

Vulnerabilidade geoserver alvo

Desde o início de março de 2025, os atacantes digitalizaram instâncias geoserver expostas à Internet, com o Cortex Xpanse identificando 3.706 servidores acessíveis ao público no início de maio de 2025, destacando uma vasta superfície de ataque principalmente na China e em outras regiões.

A campanha evoluiu em fases, começando com explorações iniciais do IP 108.251.152.209 em 8 de março de 2025, buscando executáveis ??personalizados de 37.187.74.75.

De acordo com a Unidade42 relatórioestes incluíram variantes de um aplicativo mal utilizado (por exemplo, A193, D193, E193) e SDK (por exemplo, A593, C593).

No final de março, as táticas mudaram depois que o IP da distribuição foi sinalizado malicioso, interrompendo novas amostras de aplicativos e passando para um novo IP, 185.246.84.189, até 1º de abril.

A infraestrutura expandiu-se ainda mais em meados de abril, com outro host de distribuição em 64.226.112.52, mantendo a persistência até junho de 2025.

A exploração aproveita as funções de extensão de JXPath em geotools, permitindo Código arbitrário

injeção por meio de expressões como getRuntime (). Exec (), facilitando a execução do comando por meio de solicitações como GetPropertyValue em serviços WFS, WMS ou WPS.

Táticas de monetização

A análise aprofundada revela que a cadeia de exploração começa com o CVE-2024-36401 para baixar uma carga útil em segunda etapa, como a variante SDK Z593, de hosts controlados por atacantes usando servidores transfer.sh nas portas 8080.

Esse estoque busca scripts adicionais (por exemplo, Z401, Z402) que criam diretórios ocultos, configuram ambientes e iniciam executáveis ??secretamente.

Os binários, construídos com Dart para plataforma cruzada Compatibilidade do Linuxintegre os SDKs legítimos para compartilhar largura de banda para renda passiva, evitando a detecção imitando serviços de baixo perfil em vez de criptominos com intensidade de recursos.

A comparação confirma que os SDKs são versões oficiais não modificadas, potencialmente ignorando as proteções do terminal.

A telemetria de março a abril de 2025 mostra 7.126 instâncias geoserver expostas em 99 países, com a China hospedando a maioria.

Para mitigar, as organizações devem corrigir prontamente. As ferramentas da Palo Alto Networks, como prevenção avançada de ameaças (assinatura 95463), incêndio avançado e córtex XDR, fornecem defesas contra essas explorações e cargas úteis.

Indicadores de compromisso

Tipo	Valores
Endereços IP	37.187.74.75:8080, 64.226.112.52:8080, 108.251.152.209, 185.246.84.189
Amostra SHA256 Hashes	89F5E7D66098E736C39EB36123ADCF55851268973E6614C67E3589E73451B24 (A101), 4E4A467ABE1478240CD34A1DEAEF019172B7834AD57D46F89A7C6C357F066FDB (A193), 7C18FE9DA63C86F696F9AD7B5FCC8292CAC9D49973BA12050C0A3A18B7BD1CC9 (A593), 915D1BB1000A8726DF87E0B15BEA77C5476E3EC13C8765B43781D5935F1D2609 (Z593)

Encontre esta notícia interessante! Siga -nosGoogle News Assim,LinkedIn eX Para obter atualizações instantâneas!