Gangue de Ransomware de Embargo Acumula US$34,2 Milhões em Receit

Data: 2025-08-13 02:38:52

Autor: Inteligência Against Invaders

A gangue de ransomware Embargo gerou aproximadamente US$ 34,2 milhões em receitas de

ataques desde que surgiu em abril de 2024, de acordo com uma nova análise da TRM Labs.

A plataforma de inteligência blockchain rastreou pagamentos criptográficos de endereços de vítimas para uma variedade de destinos provavelmente associados ao grupo de ransomware.

Isso incluiu centenas de depósitos no valor de aproximadamente US$ 13,5 milhões distribuídos em vários provedores globais de serviços de ativos virtuais.

Outros fundos foram lavados por meio de carteiras intermediárias, exchanges de alto risco e plataformas sancionadas, como Cryptex.net.

No total, aproximadamente US$ 18,8 milhões em fundos de vítimas permanecem em endereços não atribuídos.

A vasta distribuição dos lucros do resgate é provavelmente uma tática deliberada para evitar a detecção pelas autoridades, de acordo com os pesquisadores.

Isso inclui interromper padrões comportamentais ou atrasar a movimentação de fundos até que as condições externas sejam mais favoráveis, como atenção da mídia, taxas de rede ou liquidez.

O TRM Labs também observou que os endereços de criptomoeda historicamente vinculados à agora extinta gangue BlackCat canalizaram fundos para clusters de carteiras associados às vítimas do Embargo.

Essa sobreposição on-chain reforça a avaliação de que o Embargo pode ser uma versão renomeada do BlackCat, que Desligamento em um aparente golpe de saída em março de 2024.

Embargo adota recursos técnicos avançados

Os Laboratórios TRM relatório, publicado em 8 de agosto, observou que o Embargo pode estar adotando IA e aprendizado de máquina (ML) para escalar ataques, criar iscas de phishing mais convincentes, adaptar malware e acelerar as operações.

Essa avaliação é baseada nas capacidades técnicas do ator ransomware-as-as-service (RaaS), permitindo que ele implante ransomware altamente avançado e agressivo.

O embargo normalmente obtém acesso inicial explorando vulnerabilidades de software não corrigidas ou por meio de engenharia social. Este último inclui e-mails de phishing e downloads drive-by entregues por meio de sites maliciosos.

Uma vez dentro de uma rede, o grupo demonstra um foco claro na evasão da defesa e na maximização do impacto. Ele implanta um kit de ferramentas de duas partes para desativar as ferramentas de segurança e remover as opções de recuperação antes de criptografar arquivos.

Leia agora: Embargo Ransomware Gang Implanta Ferramentas Personalizadas de Evasão de Defesa

Após a criptografia, as vítimas são direcionadas a se comunicar por meio da infraestrutura controlada pelo Embargo. Isso permite que o grupo mantenha o controle sobre as negociações e reduza a exposição.

Ele usa dupla extorsão táticas em negociações, ameaçando vazar ou vender dados exfiltrados se a vítima se recusar a pagar.

O Embargo mantém um site de vazamento de dados onde lista organizações e, às vezes, os nomes de executivos individuais, que se recusam a pagar.

O embargo também evita marcas abertas e táticas de alta visibilidade de outros grupos de ransomware mais proeminentes, como LockBit e Akira.

“Essa restrição operacional provavelmente ajudou o Embargo a evitar a detecção da aplicação da lei e reduziu a atenção da mídia”, observaram os pesquisadores do TRM Labs.

O modelo RaaS do grupo permite que os afiliados usem suas ferramentas para realizar ataques em troca de uma participação nos lucros. No entanto, o Embargo mantém o controle sobre as operações principais, incluindo infraestrutura técnica e negociações de pagamento.

Assim como o BlackCat, o ransomware implantado pelo Embargo está na linguagem de programação Rust, permitindo compatibilidade entre plataformas e ofuscação aprimorada.

Além disso, o site de vazamento de dados do Embargo se assemelha muito ao do BlackCat tanto no design visual quanto na funcionalidade subjacente e na estrutura de conteúdo, observaram os pesquisadores.

Possível alinhamento do estado-nação

Embora o Embargo seja principalmente motivado financeiramente, vários incidentes apresentaram mensagens politicamente carregadas e referências ideológicas, sugerindo um possível alinhamento entre o estado-nação.

“Essa sobreposição potencial complica a atribuição e reflete uma tendência mais ampla de atores motivados financeiramente envolvidos em campanhas com temas políticos. Além disso, os atores do estado-nação quase certamente Aproveite os grupos cibercriminosos como proxies para promover objetivos estratégicos ou financeiros, mantendo a negação plausível”, escreveram os pesquisadores.

O grupo visa desproporcionalmente organizações sediadas nos EUA, com foco particular em Saúde, serviços às empresas e setores da indústria transformadora.

Isso provavelmente se deve à sensibilidade à interrupção operacional nesses setores.

Pedidos de resgate emitidos pelo grupo foram observados em até US $ 1,3 milhão.