DarkBit ransomware da MuddyWater crackeado para recuperação gratuita

Data: 2025-08-11 14:32:23

Autor: Inteligência Against Invaders

A empresa de segurança cibernética Profero quebrou a criptografia dos criptografadores da gangue

de ransomware DarkBit, permitindo que eles recuperassem os arquivos da vítima gratuitamente sem

pagar resgate.

Isso ocorreu em 2023 durante uma resposta a incidentes tratada por especialistas da Profero, que foram trazidos para investigar um ataque de ransomware em um de seus clientes, que criptografou vários servidores VMware ESXi.

O momento do ataque cibernético sugere que foi em retaliação aos ataques de drones de 2023 no Irã que tiveram como alvo uma fábrica de munições pertencente ao Ministério da Defesa iraniano.

No ataque de ransomware, os agentes da ameaça alegaram ser da DarkBit, que anteriormente se passavam por hacktivistas pró-iranianos, visando institutos educacionais em Israel. Os invasores incluíram declarações anti-Israel em suas notas de resgate, exigindo pagamentos de resgate de 80 Bitcoins.

Comando Cibernético Nacional de Israel ataques DarkBit vinculados ao grupo de hackers APT patrocinado pelo Estado iraniano conhecido como Água lamacenta, que têm um histórico de realização de ataques de ciberespionagem.

No caso investigado pela Profero, os invasores não se envolveram em negociações de pagamento de resgate, mas pareciam estar mais interessados em causar interrupções operacionais.

Em vez disso, os invasores lançaram uma campanha de influência para maximizar os danos à reputação da vítima, o que é um tática associada com atores do estado-nação se passando por hacktivistas.

Descriptografando DarkBit

No momento do ataque, não existia nenhum decodificador para o ransomware DarkBit, então os pesquisadores da Profero decidiram analisar o malware em busca de possíveis pontos fracos.

O DarkBit usa uma chave AES-128-CBC exclusiva e um vetor de inicialização (IV) gerado em tempo de execução para cada arquivo, criptografado com RSA-2048 e anexado ao arquivo bloqueado.

[IMAGEM REMOVIDA]

“Os arquivos VMDK são esparsos, o que significa que estão quase vazios e, portanto, os pedaços criptografados pelo ransomware em cada arquivo também estão quase vazios. Estatisticamente, a maioria dos arquivos contidos nos sistemas de arquivos VMDK não será criptografada, e a maioria dos arquivos dentro desses sistemas de arquivos não era relevante para nós / nossa tarefa / nossa investigação.

“Então, percebemos que poderíamos percorrer o sistema de arquivos para extrair o que restava dos sistemas de arquivos internos do VMDK… e funcionou! A maioria dos arquivos de que precisávamos poderia simplesmente ser recuperada sem descriptografia.”

Profero observou que os objetivos do DarkBit teriam sido melhor atendidos com um limpador de dados em vez de ransomware, e que a recusa dos invasores em negociar não os deixou escolha a não ser dissecar a criptografia do malware em busca de um método de recuperação.

Embora a Profero não esteja lançando publicamente o descriptografador DarkBit, eles disseram ao BleepingComputer que futuras vítimas podem contatá-los para obter assistência.

[IMAGEM REMOVIDA]