EUA acusam administrador de LockerGoga, MegaCortex, Nefilim ransomw

Data: 2025-09-09 21:01:39

Autor: Inteligência Against Invaders

O Departamento de Justiça dos EUA acusou o cidadão ucraniano Volodymyr Viktorovich

Tymoshchuk por seu papel como administrador das operações de ransomware LockerGoga,

MegaCortex e Nefilim.

Também conhecido online como deadforz, Boba, msfv e farnetwork, o Tymoshchuk esteve envolvido em ataques de ransomware que levaram à violação de centenas de empresas, resultando em milhões de dólares em danos, de acordo com um Acusação substituta revelada hoje.

Entre julho de 2019 e junho de 2020, Tymoshchuk e seus cúmplices supostamente violaram as redes de mais de 250 empresas nos Estados Unidos e muitas outras em todo o mundo em ataques de ransomware LockerGoga e MegaCortex.

No entanto, em muitos desses incidentes, eles não conseguiram implantar o ransomware nas redes das vítimas devido aos primeiros alertas de aplicação da lei.

De julho de 2020 a outubro de 2021, Tymoshchuk supostamente atuou como administrador da operação de ransomware Nefilim, fornecendo acesso a afiliados, incluindo o co-réu Artem Aleksandrovych Stryzhak, que foi extraditado da Espanha em abril de 2025, em troca de 20% do produto do resgate.

Em novembro de 2023, empresa de cibersegurança O Grupo-IB também ligou Tymoshchuk para as gangues de ransomware JSWORM, Karma, Nokoyawa e Nemty, ajudando-os a recrutar afiliados em vários fóruns de hackers de língua russa desde abril de 2019.

[IMAGEM REMOVIDA]disse o procurador dos EUA Joseph Nocella Jr.

“Em alguns casos, esses ataques resultaram na interrupção completa das operações comerciais até que os dados criptografados pudessem ser recuperados ou restaurados”, acrescentou o procurador-geral adjunto interino Matthew R. Galeotti.

Em setembro de 2022, como parte de um esforço global direcionado a essas redes de crimes cibernéticos, decodificadores para LockerGoga e Megacórtex ransomware foram lançados por meio da iniciativa “No More Ransomware Project” para ajudar as vítimas a recuperar seus arquivos criptografados sem pagar resgate.

Tymoshchuk enfrenta duas acusações de conspiração por fraude de computador, três acusações por danificar um computador protegido e acusações de acesso não autorizado e ameaça de divulgar

informações confidenciais.

O Programa de Recompensas contra o Crime Organizado Transnacional (TOC) do Departamento de Estado dos EUA também está oferecendo uma recompensa de até US$ 11 milhões por qualquer informação que possa levar à localização, prisão ou condenação de Tymoshchuk ou seus cúmplices.

[IMAGEM REMOVIDA]