Fugitivo de ransomware ucraniano adicionado ao mais procurado da Euro

Data: 2025-09-11 10:15:00

Autor: Inteligência Against Invaders

Um ucraniano de 28 anos foi adicionado a uma lista dos fugitivos mais procurados da Europa por

suposta participação em ataques de ransomware LockerGoga.

Diz-se que Volodymyr Tymoshchuk implantou o ransomware contra centenas de empresas vítimas entre 2018 e 2020, causando mais de US$ 18 bilhões em danos em todo o mundo.

Mais notavelmente, ele está sendo atrelado ao ataque de 2019 à gigante norueguesa de alumínio, Norsk Hydro, que A empresa estimou custou NOK 300-350 milhões (£ 26-40 milhões, US $ 35-41 milhões na época) apenas na primeira semana.

A Europol disse que o desmascaramento de Tymoshchuk ocorreu após uma operação longa, complexa e coordenada envolvendo as autoridades policiais França, Alemanha, Holanda, Noruega, Suíça, Ucrânia, Reino Unido e EUA, juntamente com a Europol e a Eurojust.

Leia mais sobre LockerGoga: Euro Police Swoop em 12 suspeitos de membros de gangues de ransomware

Após prisões anteriores, os investigadores conseguiram mapear a estrutura do grupo e as identidades de vários membros – incluindo desenvolvedores de malware, especialistas em intrusão e lavadores de dinheiro, afirmou a Europol.Cinco pessoas foram presas em abrileste ano em conexão com oVariantes de ransomware LockerGoga, MegaCortex, Hive e Dharma.

EUA oferecem US$ 11 milhões à medida que a rede aperta

O anúncio do grupo policial segue a abertura nos EUA de uma acusação substituta acusando Tymoshchuk (também conhecido como deadforz, Boba, msfv e farnetwork) de servir como administrador não apenas do LockerGoga, mas também dos grupos de ransomware MegaCortex e Nefilim.

“Volodymyr Tymoshchuk é acusado por seu papel em esquemas de ransomware que extorquiram mais de 250 empresas nos Estados Unidos e centenas em todo o mundo”, disse o procurador-geral assistente interino Matthew Galeotti, da Divisão Criminal do Departamento de Justiça.

“Em alguns casos, esses ataques resultaram na interrupção completa das operações comerciais até que os dados criptografados pudessem ser recuperados ou restaurados. Este processo e o anúncio de recompensas de hoje refletem nossa determinação em proteger as empresas contra sabotagem e extorsão digital e perseguir implacavelmente os criminosos responsáveis, não importa onde

estejam localizados.”

O Programa de Recompensas do Crime Organizado Transnacional (TOC) do Departamento de Estado está oferecendo recompensas totalizando US$ 11 milhões por informações que levem à prisão e/ou condenação ou localização de Tymoshchuk ou seus conspiradores.

Ele é acusado de duas acusações de conspiração para cometer fraude e atividades relacionadas em conexão com computadores, três acusações de danos intencionais a um computador protegido, uma acusação de acesso não autorizado a um computador protegido e uma acusação de transmissão de uma ameaça de divulgação de informações confidenciais.

Os esforços do LockerGoga / MegaCortex nem sempre foram bem-sucedidos. Em 2022, Europol e Bitdefender lançou um decodificador para o LockerGoga, permitindo que muitas vítimas recuperem o acesso aos seus dados.