Grupo de hackers iraniano Nimbus Manticore expande direcionamento eu

Data: 2025-09-24 12:03:11

Autor: Inteligência Against Invaders

Uma longa campanha de espionagem cibernética ligada ao Irã intensificou suas operações na

Europa.

O grupo, conhecido como Nimbus Manticore, tem um histórico de visar as indústrias aeroespacial, de telecomunicações e de defesa em linha com Prioridades do Corpo de Guardas da Revolução Iraniana (IRGC).

Spear Phishing Surge na Europa

De acordo com novas descobertas da Check Point Research (CPR), a última onda de atividades do grupo mostra uma mudança em direção à Europa Ocidental, com organizações na Dinamarca, Suécia e Portugal enfrentando riscos elevados.

Os invasores se passam por recrutadores de empresas aeroespaciais e de telecomunicações conhecidas, direcionando as vítimas para portais de carreira convincentes, mas fraudulentos. Cada alvo recebe credenciais de login personalizadas, uma tática que permite o rastreamento próximo das vítimas e um controle rígido de acesso.

A partir daí, os invasores distribuem arquivos maliciosos que iniciam um processo de infecção sofisticado e em vários estágios. Isso envolve o sideload de arquivos DLL maliciosos em executáveis legítimos do Windows, incluindo componentes do Microsoft Defender, para evitar a detecção.

Leia mais sobre operações cibernéticas iranianas: MPs alertam sobre ameaça cibernética iraniana “significativa” ao Reino Unido

Kit de ferramentas de malware em evolução

No centro dessas campanhas está uma família de backdoors personalizados. Primeira identificação como *‘Minibike’* em 2022, o malware evoluiu para novas cepas, principalmente ‘MiniJunk’ e ‘MiniBrowse’. Essas ferramentas permitem que os invasores exfiltrem arquivos, roubem credenciais do navegador e emitam comandos remotos, empregando ofuscação pesada para resistir à análise.

O malware mostra técnicas avançadas, como:

- Sideload de DLL em vários estágios para evitar verificações de segurança normais

- Tamanhos binários inflados para ignorar verificações antivírus
- Uso de certificados de assinatura de código válidos de provedores confiáveis
- Ofuscação no nível do compilador que insere código indesejado e cadeias de caracteres criptografadas

“A campanha reflete um ator maduro e com bons recursos, priorizando furtividade, resiliência e segurança operacional”, disse a CPR.

Infraestrutura de nuvem para resiliência

A Nimbus Manticore depende muito de serviços de nuvem para hospedar sua infraestrutura, incluindo domínios registrados no Serviço de Aplicativo do Azure e protegidos pela Cloudflare. Essa configuração fornece redundância, permitindo que os invasores restabeleçam rapidamente os servidores de comando e controle (C2) se um for desativado.

O direcionamento da campanha é consistente com operações anteriores contra Israel e os estados do Golfo.

No entanto, como mencionado acima, os pesquisadores da CPR observaram recentemente uma clara expansão em direção à Europa, com ataques recentes vinculados a portais de carreira falsos que se passam por empresas aeroespaciais e de telecomunicações. Os setores de maior risco incluem:

- Telecomunicações, particularmente provedores de satélite
- Empresas aeroespaciais e de aviação
- Empreiteiros de defesa

A análise da CPR sugere que a campanha permaneceu ativa mesmo durante o conflito de 12 dias entre Israel e Irã em meados de 2025.

A capacidade de operar sem ser detectada por meio de ofuscação pesada e uso de infraestrutura legítima destaca a crescente sofisticação do grupo.