BOLETIM DE SEGURANÇA

Agências de segurança advertem que hackers norte coreanos estão explorando políticas fracas de DMARC em e-mails

heimdall
security research
A DIVISION OF ISH

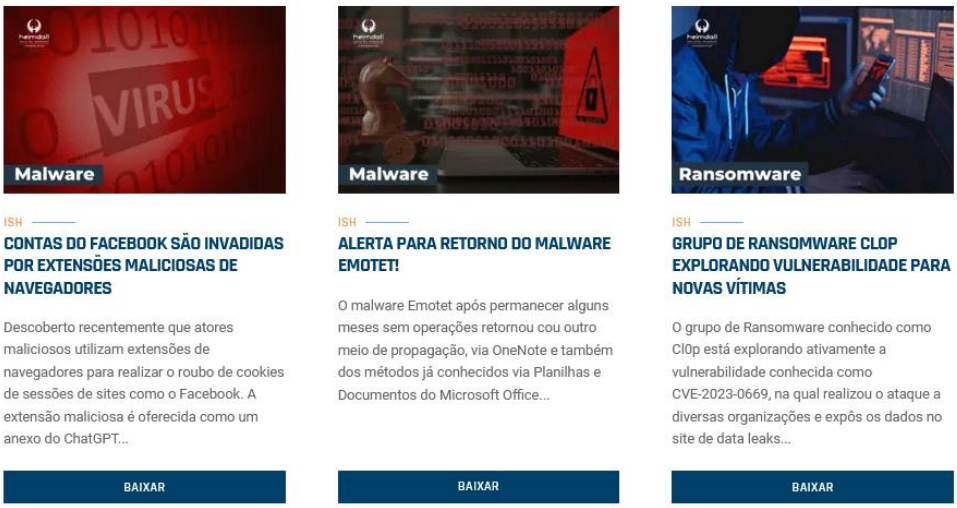
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



SUMÁRIO

1 SUMÁRIO EXECUTIVO

Agências de inteligência dos EUA, divulgaram um comunicado sobre o grupo hacker APT43, vinculado à Coreia do Norte, que está utilizando deficiências nas políticas de DMARC para camuflar ataques de *spearphishing*. Esses ataques são uma forma de phishing altamente direcionada e as falhas nas políticas de DMARC permitem que os hackers escondam suas ações maliciosas, passando por sistemas de segurança de e-mail menos rigorosos.

2 INFORMAÇÕES SOBRE A AMEAÇA

Este ator de ameaça explora vulnerabilidades nas políticas de DMARC para realizar ataques de spearphishing, disfarçando e-mails maliciosos como se fossem de fontes confiáveis, incluindo jornalistas e especialistas em assuntos do Leste Asiático. Segundo a NSA, a Coreia do Norte utiliza essas campanhas para coletar dados sobre a geopolítica e estratégias de política externa que possam influenciar seus interesses, acessando indevidamente documentos e comunicações sigilosas.

O *Reconnaissance General Bureau* (**RGB**), a agência de inteligência militar norte-coreana e sancionada pelos EUA, coordena uma série de operações de espionagem e coleta de inteligência. Essas atividades são executadas pelo grupo APT43, conhecido também por outros nomes como Kimsuky, Emerald Sleet, Velvet Chollima e Black Banshee. Ativo desde 2012, o APT43 é um grupo subordinado ao RGB e está envolvido em uma variedade de ações de espionagem estatal.

O propósito é atualizar continuamente as informações relativas aos Estados Unidos, Coreia do Sul e outras nações relevantes. Isso visa reforçar os objetivos de inteligência nacional da Coreia do Norte e neutralizar quaisquer ameaças percebidas como políticas, militares ou econômicas que possam comprometer a segurança e a estabilidade do governo norte-coreano.

Conforme divulgado pelas agências de seguranças norte americanas, os agentes do APT43 têm se disfarçado de jornalistas e acadêmicos em campanhas de spearphishing. Essas ações têm como alvo, centros de pesquisa, instituições acadêmicas e entidades de mídia nos EUA, Europa, Japão e Coreia do Sul, prática que ocorre desde 2018.

Os atores Kimsuky têm como objetivo principal coletar informações geopolíticas e dados confidenciais para o governo da Coreia do Norte. Eles visam analistas políticos e especialistas, conforme indicado pelas agências em um comunicado conjunto divulgado recentemente em formato PDF. Os êxitos desses atores possibilitam a criação de e-mails de spearphishing mais autênticos e efetivos, que podem ser usados para atacar alvos de maior importância e sensibilidade

3 RECOMENDAÇÕES

Para mitigar esses ataques, o FBI e a NSA recomendam fortalecer as políticas DMARC, adotando configurações como "v=DMARC1; p=quarantine;" ou "v=DMARC1; p=reject;". A primeira opção orienta os servidores a colocarem em quarentena os e-mails suspeitos, potencialmente marcando-os como spam, enquanto a segunda opção bloqueia completamente os e-mails que não passam nas verificações DMARC. Além disso, as agências sugerem a definição de outros campos na política DMARC, como 'rua', que permite às organizações receberem relatórios agregados sobre as tentativas de e-mails fraudulentos que alegam ser do domínio da organização.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **NSA**
- **Bleepingcomputer**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH