heimdall

security research

A DIVISION OF ISH

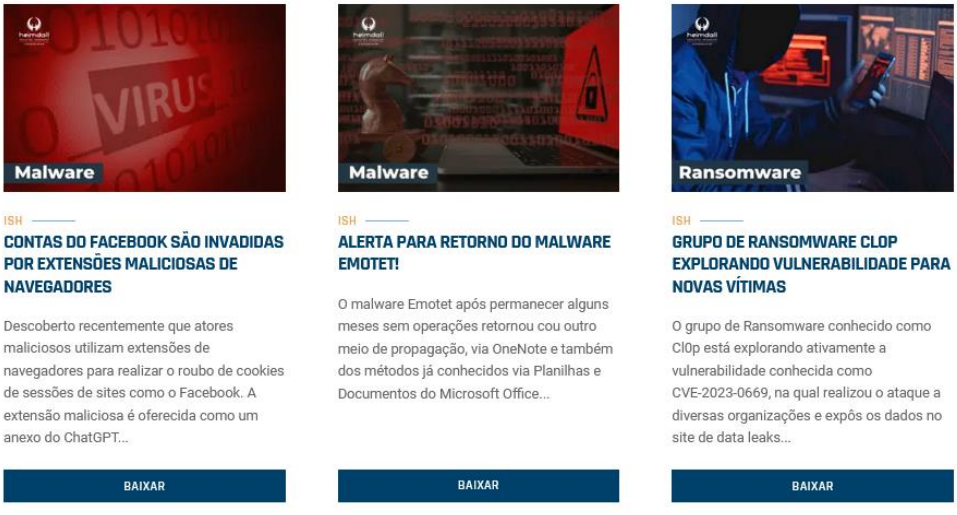
Ataque massivo de DDoS contra serviços do Outlook

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

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

Lista de Figuras

1 OUTLOOK ATINGIDO POR DDOS

No dia 05 de junho, o outlook sofreu uma série de interrupções e esteve por fora do ar várias vezes ontem, cuja autoria teria sido reivindicada por um grupo de hacktivistas conhecidos como **Anonymous Sudan**, alegando que estes realizaram ataques DDoS no serviço.

A interrupção também aconteceu no dia 06 de junho após grandes interrupções, criando interrupções generalizadas para usuários globais do Outlook, impedindo que usuários em todo o mundo acessassem e enviassem e-mails de maneira confiável e utilizassem o aplicativo móvel do Outlook.

As caixas de mensagens apresentavam erros, afirmando que não poderia exibir um e-mail por exemplo.

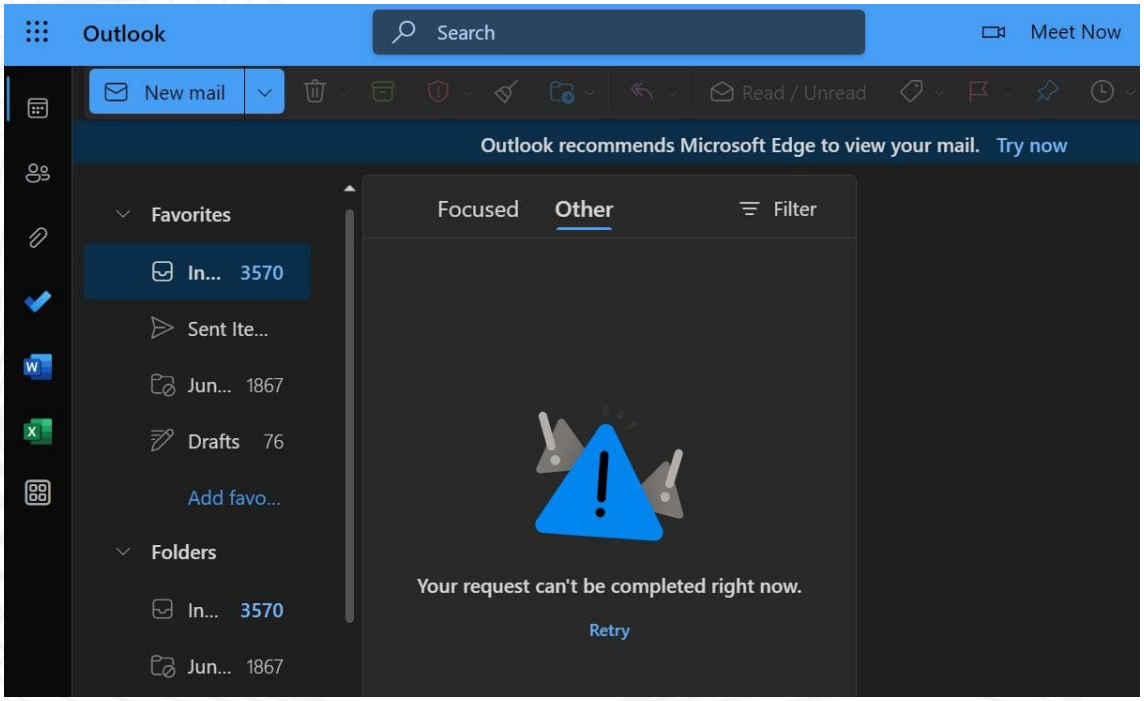


Figura 1 – Exemplo de problemas do Microsoft outlook.

A Microsoft afirmou que as interrupções são causadas por problemas técnicos, cuja mensagem foi postada via Twitter pela própria Microsoft.

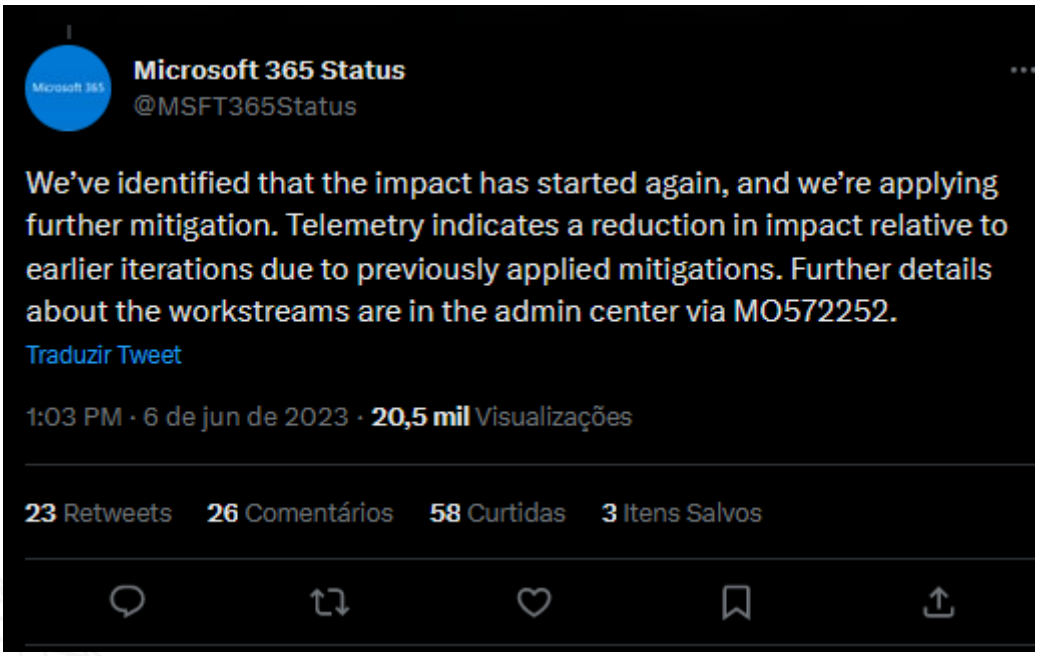


Figura 2 – Publicação da Microsoft via Twitter.

Apesar da Microsoft afirmar que problemas técnicos ocasionaram as interrupções, um grupo conhecido como "Anonymous Sudan" afirmou que estaria por trás destas interrupções, alertando que estão realizando ataques DDoS na Microsoft para protestar contra o envolvimento dos EUA nos assuntos internos do Sudão.

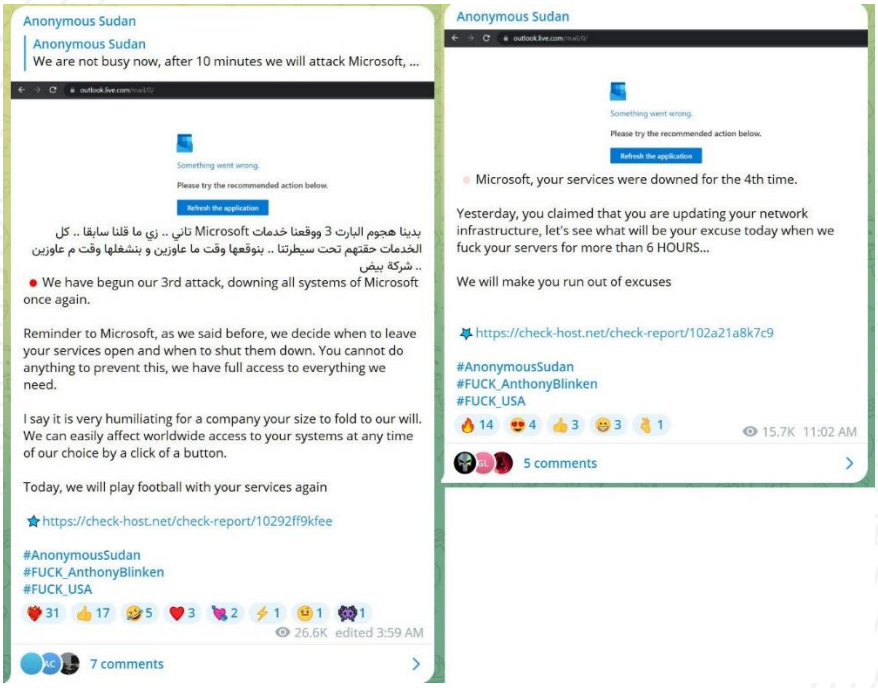


Figura 3 – Anonymous Sudan alegando estar por trás dos ataques na Microsoft.

Segundo as mensagens, o grupo afirmou que:

“Podemos atingir qualquer empresa dos EUA que quisermos. Americanos, não nos culpem, culpem seu governo por pensar em intervir nos assuntos internos sudaneses. Continuaremos a visar grandes empresas, governo e infraestrutura dos EUA”.

“Esperamos que tenha gostado, Microsoft”.

“Microsoft, hoje jogamos futebol com seus serviços. Vamos jogar um jogo divertido. O destino de seus serviços, que é usado por centenas de milhões de pessoas todos os dias, está sob nosso domínio e escolha”.

“Você falhou em repetir o ataque que continuou por horas, então que tal você nos pagar 1.000.000 USD e nós ensinamos seus especialistas em segurança cibernética como repelir o ataque e nós paramos o ataque do nosso lado?”

Sendo que, de acordo com as urls compartilhadas pelo grupo, estes afirmaram que tem como alvo a url https://outlook.live.com/mail/o, ou seja, o principal serviço da Web Outlook.com.

Até a elaboração do boletim, a Microsoft não teria se manifestado quanto as alegações do grupo Anonymous Sudan sobre os ataques.

2 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Publicação Bleeping Computer, Anonymous Sudan – DdoS**

heimdall
security research

A DIVISION OF ISH