Zimbra **italovalcy@ufba.br**

[ETIR-UFBA #3438898] Host Realizando Atividade Maliciosa [aberto]

De : ETIR-UFBA - Equipe de Tratamento de Incidentes de Rede <etir@ufba.br> Sex, 30 de Ago de 2019 11:08
Assunto : [ETIR-UFBA #3438898] Host Realizando Atividade Maliciosa [aberto]

Prezados,

O ETIR-UFBA, através de suas soluções de monitoramento, detectou que o host listado abaixo está sendo utilizado para minerar Criptomoedas.

A rede acadêmica brasileira (rede Ipê), provida e mantida pela RNP, tem por objetivo prover serviços avançados de redes para aplicações de ensino e pesquisa.
Segue link da política de uso da rede Ipê: https://www.rnp.br/sites/default/files/politica-uso-rede-ipe.pdf

Solicitamos que o sistema seja verificado para comprovar
a origem de tal atividade e que sejam tomadas as medidas
necessárias para interromper tal ação.

Antes de encerrar este incidente junto ao CAIS, certifique-se que:
1. O incidente foi investigado e identificado:
2. O incidente foi corrigido, garantindo que ele não voltará a acontecer.

Para decodificar o payload e entender melhor os dados do pacote capturado, sugerimos o uso da página abaixo:
https://www.base64decode.org/

O incidente pode ser encerrado mediante resposta dessa mensagem, conforme segue:

Para incidentes tratados e corrigidos, substitua o campo "Assunto"/"Subject" por:
[ETIR-UFBA #3438898] - [RESOLVIDO]

Para incidentes com informações insuficientes ou cujo host denunciado não pertença a Instituição, substitua o campo "Assunto"/"Subject" por:
[ETIR-UFBA #3438898] - [AJUDA]

Atenciosamente,

ETIR-UFBA

IP Conectado ao Minerador, IP Minerador:Porta, DesTimeStamp(GMT-2),Descrição do Incidente, Protocolo,
10.12.27.xx:51559 5.255.86.125:8080, 29/10/2018-21:12:29, ET POLICY Cryptocurrency Miner Checkin, TCP

Payload (Base 64)
eyJpZCI6MSwianNvbnJwYyI6IjIuMCIsIm1ldGhvZCI6ImxvZ2luIiwicGFyYW1zIjp7ImxvZ2luIjoieCIsInBhc3MiOiJ4IiwiYWdlbnQiOiIifX0K