SOC168 - Whoami Command Detected in Request Body

Caso conduzido individualmente no simulador SOC da plataforma LetsDefend. Atuei como analista SOC N1, realizando todas as etapas de triagem, investigação, contenção e relatório.

Descrição:

Recebido alerta SOC168 referente à detecção do comando `whoami` dentro de uma requisição HTTP enviada ao servidor "172.16.17.16", identificado pelo SIEM como um possível ataque de Command Injection.

Análise:

Em 28 de fevereiro de 2022, às 04h12, nosso SOC emitiu o alerta SOC168 após detectar o comando whoami no corpo de uma requisição HTTP direcionada ao servidor 172.16.17.16. Esse padrão é típico de uma tentativa de **Command Injection**.

A investigação apontou o IP de origem 61.177.172.87 cuja reputação foi verificada em **VirusTotal**, **AbuseIPDB** e **Cisco Talos** como malicioso e com origem na **China**.

Com base na análise dos logs e na linha de comando executada no servidor WebServer1004, foi possível confirmar a execução dos seguintes comandos remotos:

- Whoami
- hostname
- ipconfig
- net user

Todas as requisições responderam com HTTP 200, confirmando que os comandos foram aceitos e executados com sucesso.

Ação tomada:

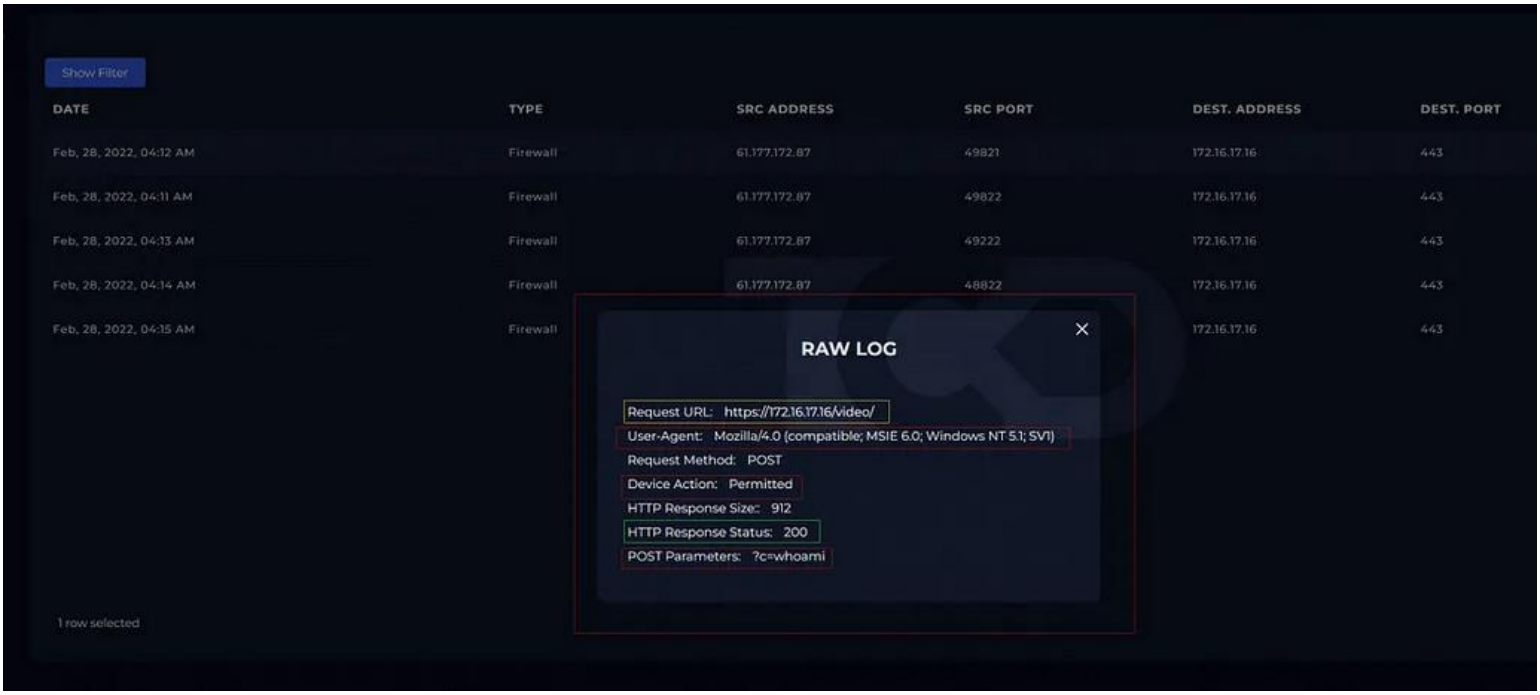
- Alerta classificado como **True Positive**, confirmando exploração real.
- O servidor comprometido foi isolado para contenção e encaminhado para análise e remediação adicional, conforme o playbook da LetsDefend.

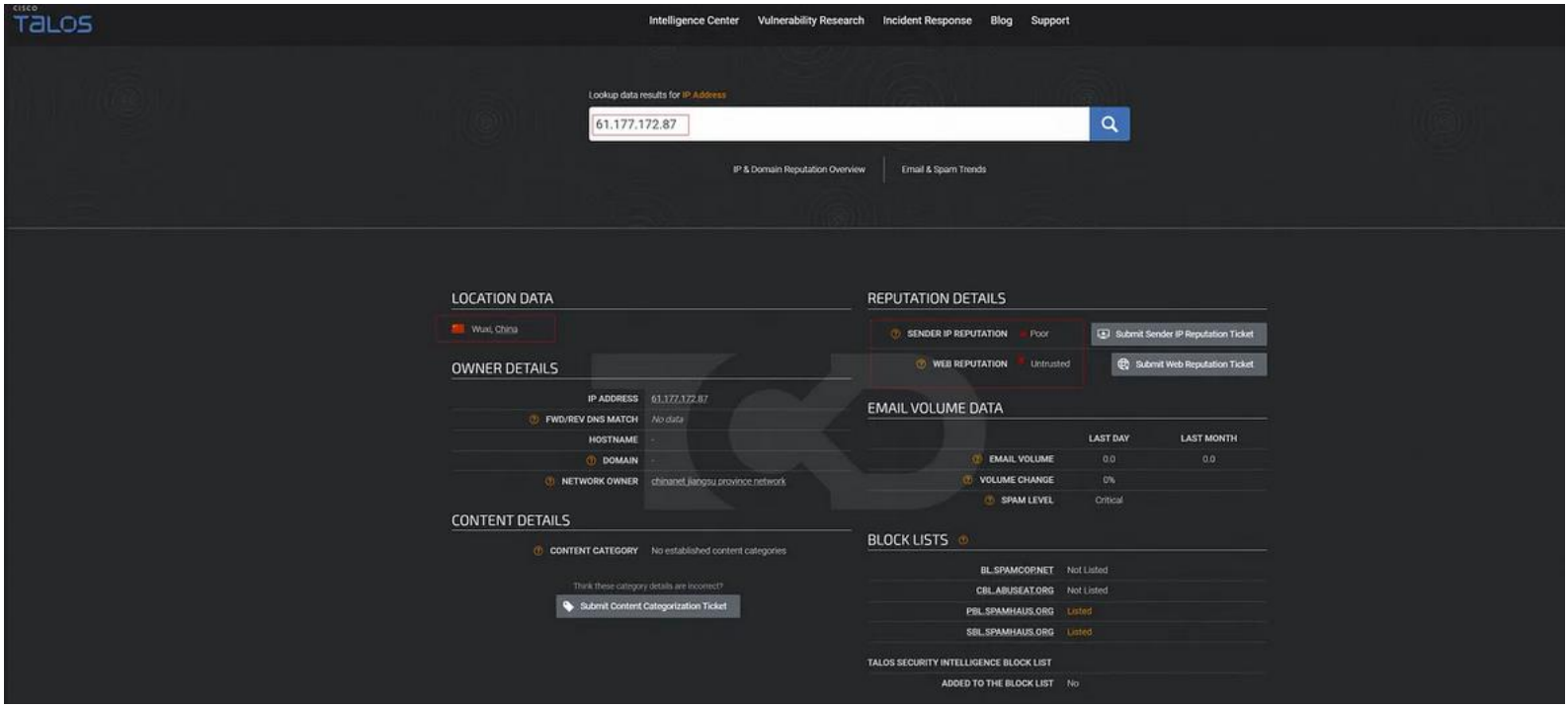
Escalonamento:

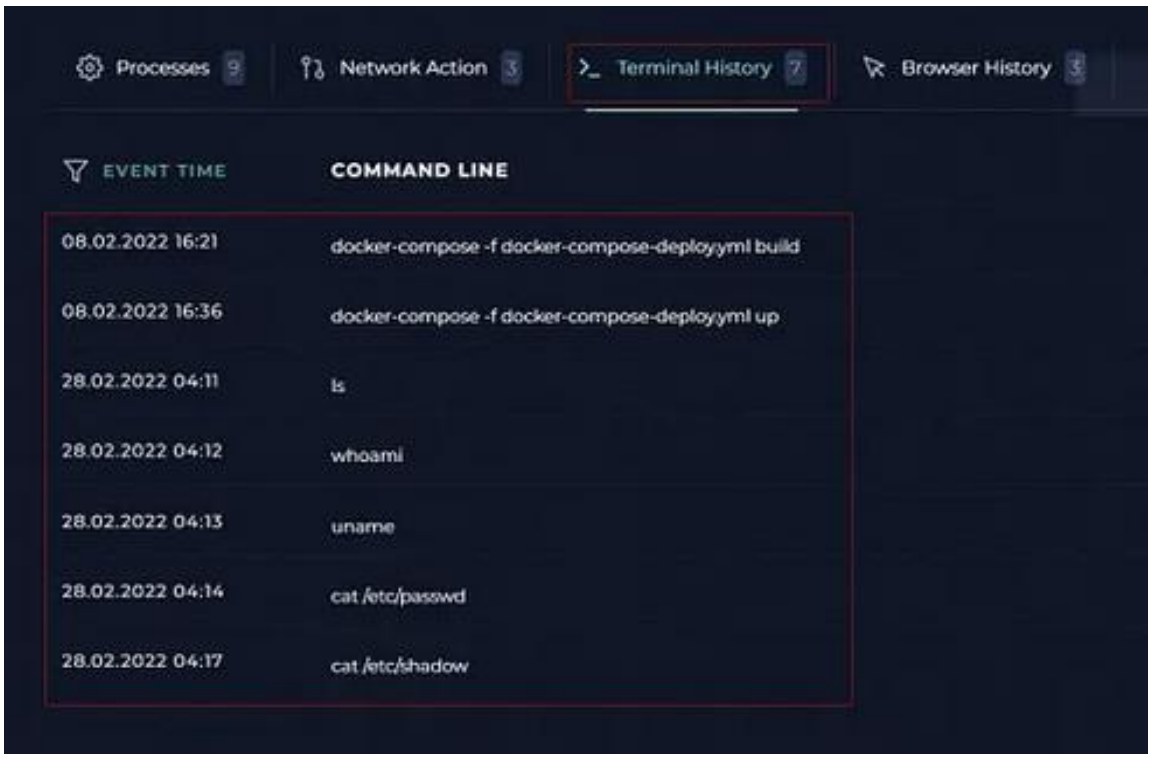
As evidências foram coletadas e o incidente foi escalado ao time N2 para análise aprofundada e ações corretivas.

Evidências/IOC:

Indicador	Tipo	Descrição
jsipmanager@163[.]com	E-mail	Possível origem do ataque
163.com	Domínio	Domínio vinculado ao e-mail de origem
61.177.172[.]87	IP externo	IP de origem das requisições
hxxps://172.16.17.16/victim	URL interna	Requisição que executou o comando
172.16.17[.]16	IP interno	Servidor comprometido (WebServer1004)




Intelligence Center
Vulnerability Research
Incident Response
Blog
Support
Lookup data results for IP Address
61.177.172.87
IP & Domain Reputation Overview
Email & Spam Trends
LOCATION DATA
Wuxi, China
OWNER DETAILS
IP ADDRESS 61.177.172.87
FWD/REV DNS MATCH No data
HOSTNAME -
DOMAIN -
NETWORK OWNER chinanet jiangsu province network
CONTENT DETAILS
CONTENT CATEGORY No established content categories
Think these category details are incorrect?
Submit Content Categorization Ticket
REPUTATION DETAILS
SENDER IP REPUTATION Poor
WEB REPUTATION Untrusted
Submit Sender IP Reputation Ticket
Submit Web Reputation Ticket
EMAIL VOLUME DATA
LAST DAY
LAST MONTH
EMAIL VOLUME 0.0 0.0
VOLUME CHANGE 0%
SPAM LEVEL Critical
BLOCK LISTS
BL.SPAMCOP.NET Not Listed
CBL.ABUSEAT.ORG Not Listed
PBL.SPAMHAUS.ORG Listed
SBL.SPAMHAUS.ORG Listed
TALOS SECURITY INTELLIGENCE BLOCK LIST
ADDED TO THE BLOCK LIST No


Processes 9
Network Action 3
Terminal History 7
Browser History 3
EVENT TIME
COMMAND LINE
08.02.2022 16:21 docker-compose -f docker-compose-deploy.yml build
08.02.2022 16:36 docker-compose -f docker-compose-deploy.yml up
28.02.2022 04:11 ls
28.02.2022 04:12 whoami
28.02.2022 04:13 uname
28.02.2022 04:14 cat /etc/passwd
28.02.2022 04:17 cat /etc/shadow