ini report pokonya.

aditya firman nugroho

trus ini logo.. ( mager )

PT ABC

2024-12-22

ENVIRONMENT:

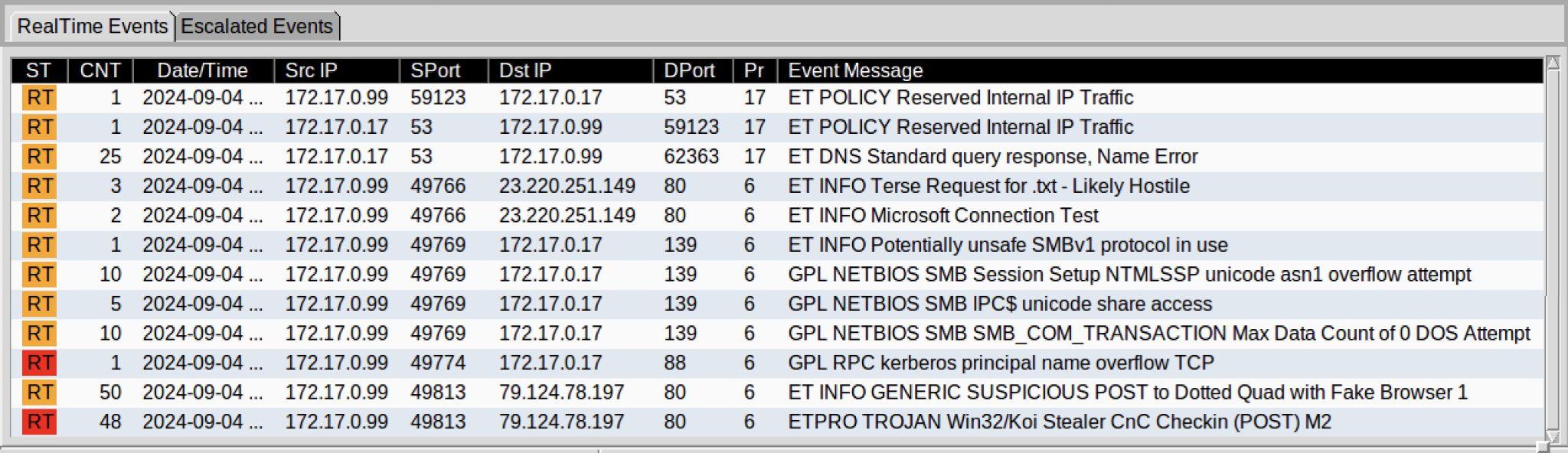
* LAN segment range: 192.168.10.0/24 (192.168.10.0 through 192.168.10.255)
* Domain: example.com
* AD environment name: example
* Domain Controller: 192.168.10.23 - WIN-ABC
* LAN segment gateway: 192.168.10.23
* LAN segment broadcast address: 192.168.10.255

BACKGROUND:

* lihat alert yang ada pada network environment, disitu sudah ada sebuah indikasi malware yang sudah diidentifikasi di laptop

TASK:

* tulislah report terkait dengan incident yang terjadi



# Example Reporting of An Incident Report

Executive Summary :

* pada tanggal 2024 hari jumat di jam 18.42, perusahan PT.ABC terkena malware dimana serangan tersebut dimulai dari komputer yang digunakan oleh username junet. dengan malware

Victim Details :

* Hostname : DESKTOP-KANTOR
* IP Address : 192.168.10.1
* MAC Address : { INI MAC ADDRESS }
* User account name : junet
* name of victim

Indicator of compromise

| SRC IP & PORT | Dest IP:PORT | Alert Name | |
| --- | --- | --- | --- |
| 192.168.10.1:9900 | 172.103.43.211:9980 | Malware Trojan WIN32/ C2 Beaconing | |

URL Generating the alert traffic :

192.168.10.1:9900 – 172.103.43.211:9980 – POST /index.php

192.168.10.1:9900 – 172.103.43.211:9980 – POST /index.php?id&subid=qIOuKk7U 192.168.10.1:9900 – 172.103.43.211:9980 – POST /index.php

Reference

