

Already you can something “phishy” is afoot

This is epoch time and it translates to: Wednesday, January 4, 2017 6:37:26 AM

Part 2) Here I pipe from my current search and look for the earliest and latest times using the stats function

Part 1) Here I search for the sender (buttercupgames) and filter out incoming addresses that are local (10.0.0.0/8)

Part 3) Here I pipe from my current search and convert the info into a table where I make what we are looking for easier to find

Part 3.5) Here I took a screenshot of the malware event. You can see the data associated with the attack.

Part 4) Here I created an in app Cron job to inform me every five minutes if another event popped up

Part 4.5) Here Is a list of events that popped up. In order to test the system and save time I made it alert every minute.