Spamhaus

Security Metrics

Felix W. Dekker, Jorai Rijsdijk, Nick Ho Sam Sooi, Jakob S. Kok

Group number
6

GitHub
https://github.com/Erackron/EoC/

Assignment description

During Block 2, you have learnt the importance of measuring cybersecurity and the challenges to create meaningful metric. However, metrics are necessary to show how security activity contributes directly to security goals; measure how changes in a process contribute to security goals; detect significant anomalies in processes and inform decisions to fix or improve processes.

- What security issue does the data speak to?
- What would be the ideal metrics for security decision makers?
- What are the metrics that exist in practice?
- A definition of the metrics you can design from the dataset
- An evaluation of the the metrics you have defined. This should include graphical representations of the metrics (e.g., histograms, scatter plots, time series, bar charts).

Assignment

Security issue

Scenario: We are a company. Have our servers been infected through spam, or is a botnet using is to send spam?

Attackers

1) **(Legitimate) businesses**
   Businesses that try to sell their product through spam. The products may be legitimate, but their methods are questionable.
2) **Cybercriminals**
   Persons or organizations that try to create botnets to send spam, or use spam to

spread the botnet. The spam may be anything, including phishing emails, viruses, and self-replicating botnets.

Threats

1) **Being compromised**
   If the company's machines have been compromised, its servers could be used to facilitate someone else's actions, even though the company will have to pay for the resources (e.g. electricity, bandwidth) used.
2) **Blocklist**
   If the company is infected, its machines may appear on blocklists, which prevents legitimate emails from being received by others.
3) **Terms of Service**
   If the ISP or hosting provider detects that spam is being sent from the company's servers, it may choose to block servers or terminate the contract entirely.
4) **Further threats**
   The botnet could be used to facilitate DDos attacks, or may spread itself through the company's internal network and steal or alter confidential information.

Assets

1) **Servers**
   If servers are infected, they will spend time serving the master of the botnet instead of performing their regular tasks.
2) **Reputation**
   Being marked as a spammer will cause the company to lose reputability, and legitimate emails may be blocked.
3) **Time**
   Removing the botnet and being removed from blocklists costs time (and thus money).

Ideal metrics

	Controls	**Vulnerabilities**	**Incidents**	**Losses**
Physical				
Organizational				
Procedural		Measure vulnerability to known/emerging botnets	Number of your emails marked as spam	
Technical	Having a spam filter on incoming **and** outgoing mail			Number of appearances on block list

Metrics in practice

	Controls	**Vulnerabilities**	**Incidents**	**Losses**
Physical				
Organizational				
Procedural		Measure vulnerability to known/emergin g botnets		
Technical	Having a spam filter on incoming **and** outgoing mail			Number of appearances on block list

Metric design

Based on the dataset we can look at how new botnets emerge and we can look at where the botnets are. The dataset notes the type of the bot, which would allow us to see if our own servers are vulnerable to that infection.

We can also look at how many times our servers appear in the dataset to see if we have (probably) been infected.

More metrics may be derived by looking at the data itself:

- Ranking spam sources by / Mapping types of spam botnet infections by
    - Country

        - Domain
        - ASN
        - IP Range/Network
- Botnet spread through networks
- Appearance of new botnets

Metric evaluation

We'll do this once we have received feedback, to be sure we are on the right track.