URL Lookup Service

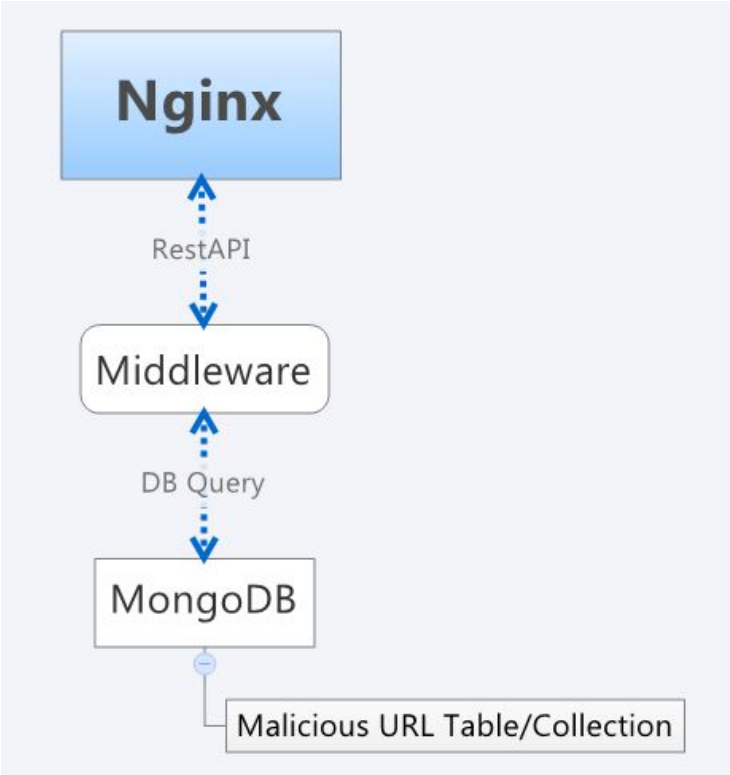
Edward Han
August 17, 2017

Table of Contents

Introduction

- Create an URL lookup Service
- Maintain a list of malicious URLs
- Provide an API that takes URL as an input, and returns whether it’s malicious or not.

Initial Concept



Additional Requirements

- Size of URL list could outgrow the memory capacity of a single server.
- Number of requests/s may exceed initial quota.
- Need to insert/update new malicious URLs every 10 minutes.

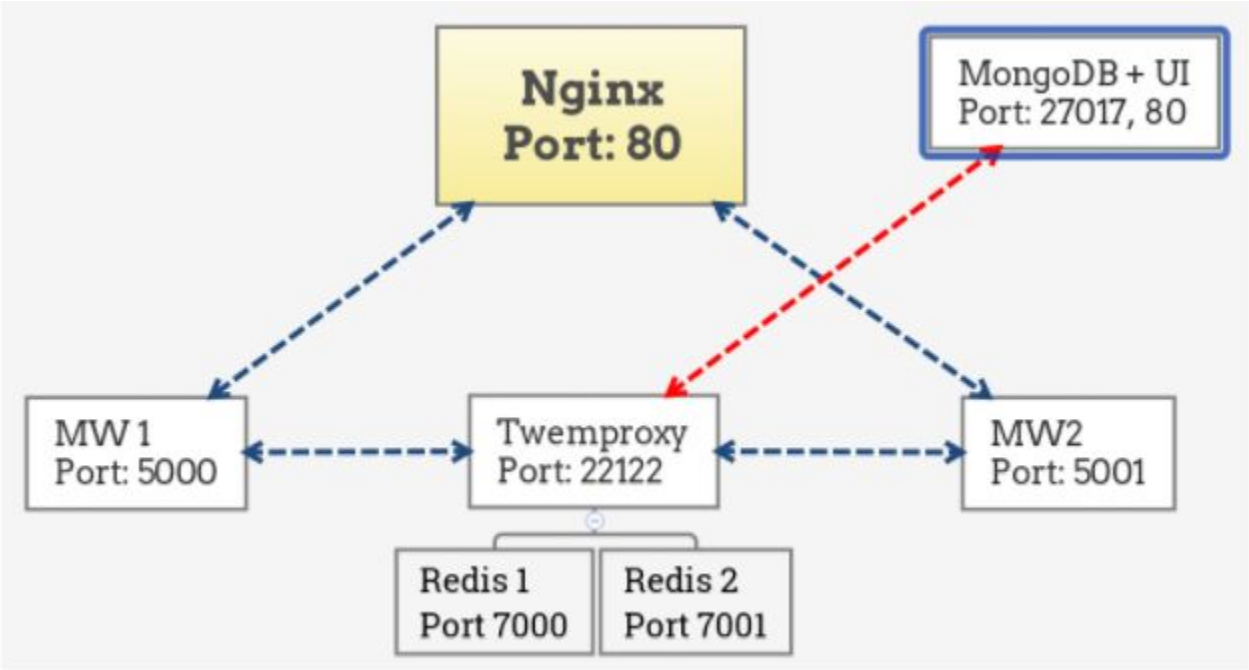
Flaws with Initial Concept

- Too many DB query requests = High disk IO usage.

- Not scalable.
  - Need to shard data across multiple servers.
  - Need to use nginx to load-balance API requests.

- It’s risky to directly write/update production DB every 10 minutes.

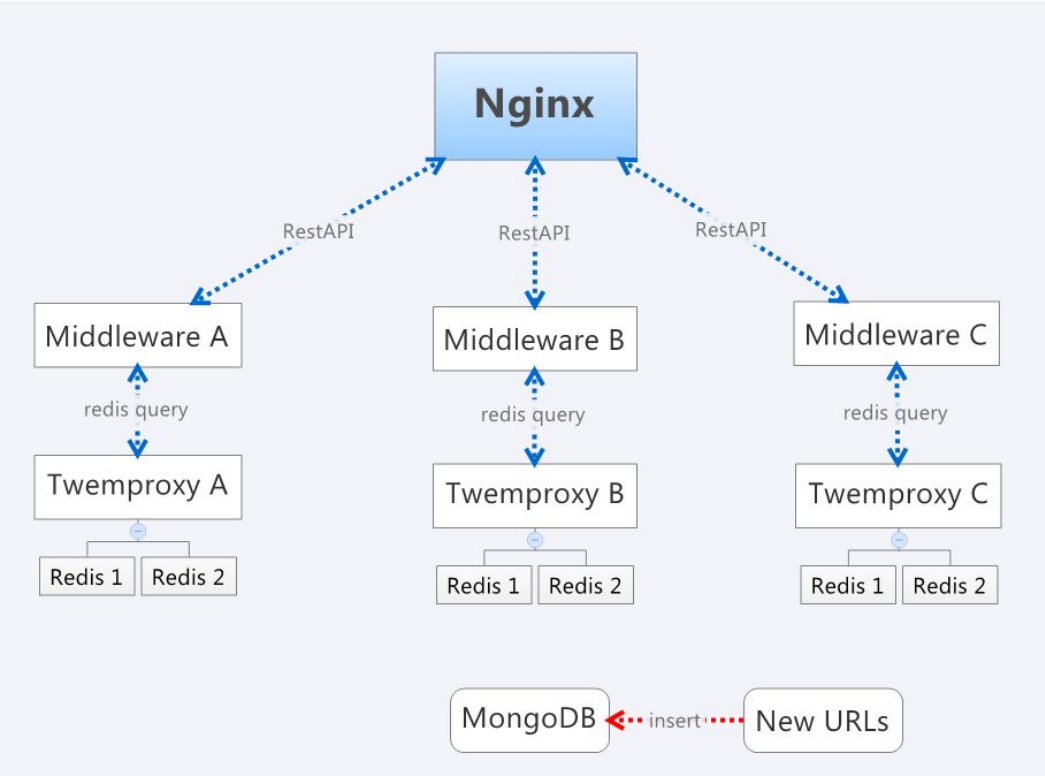
Changes to Initial Concept



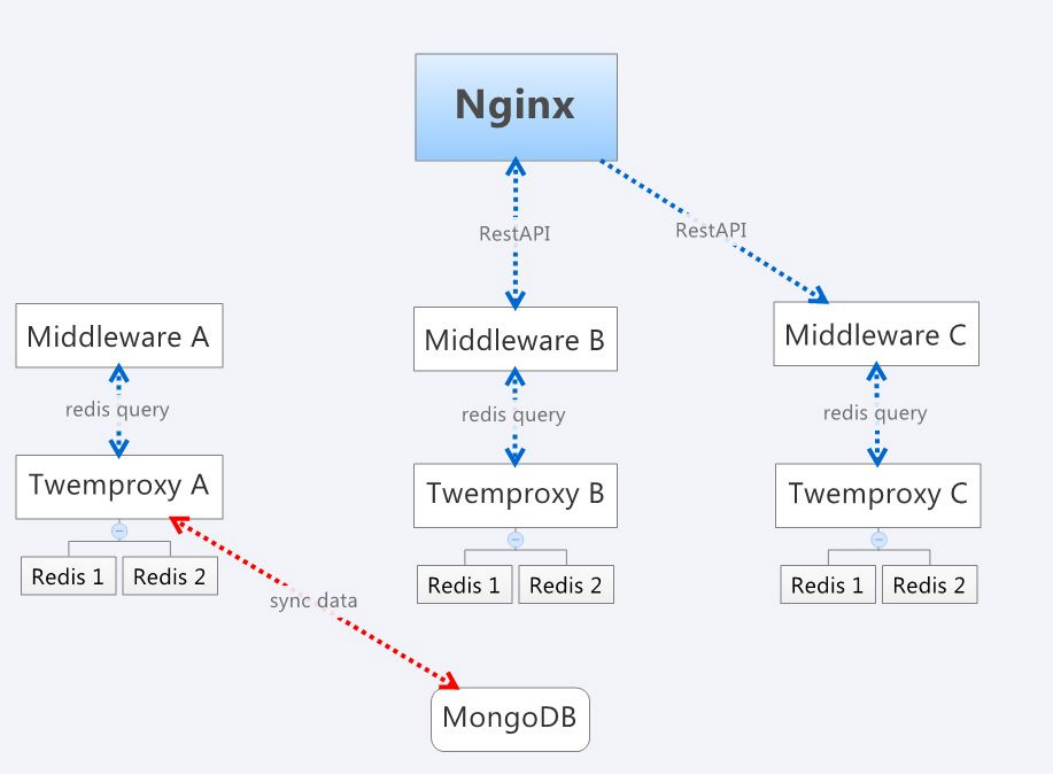
Changes to Initial Concept

- Redis to reduce DB queries, thus reducing disk IO usage.
- Twemproxy/Nutcracker to shard data across multiple redis instances.
- Nginx to load-balance API requests between MW1, MW2, and MW...

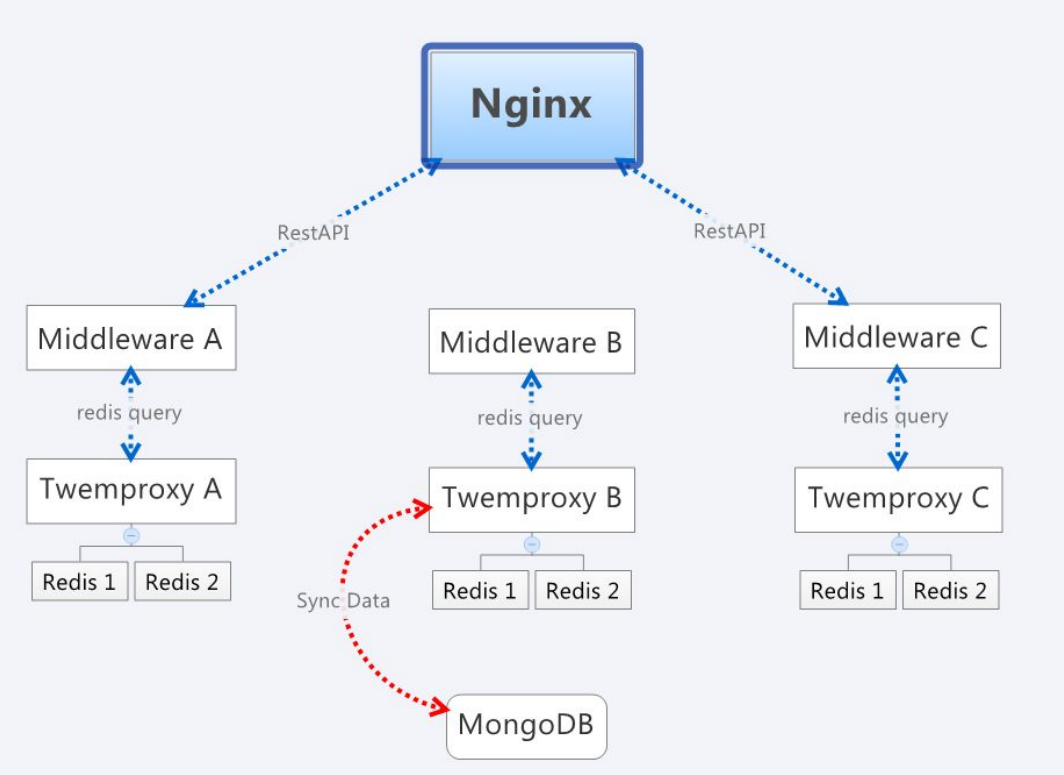
Insert/Update URL List



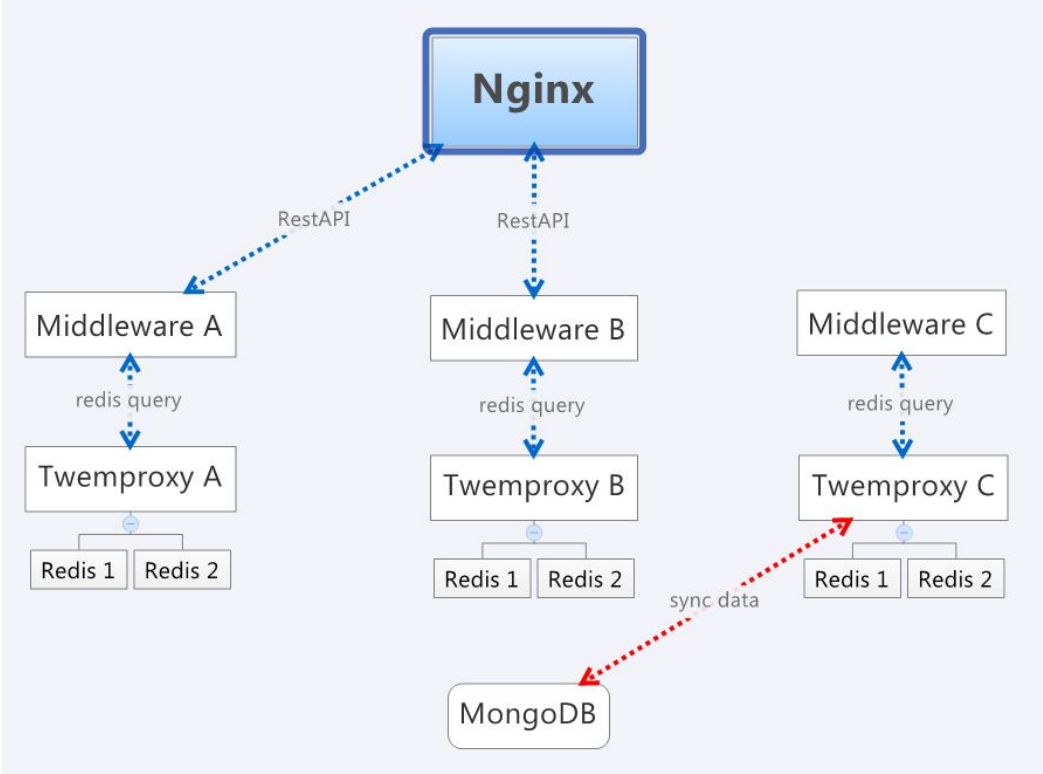
Insert/Update URL List



Insert/Update URL List



Insert/Update URL List

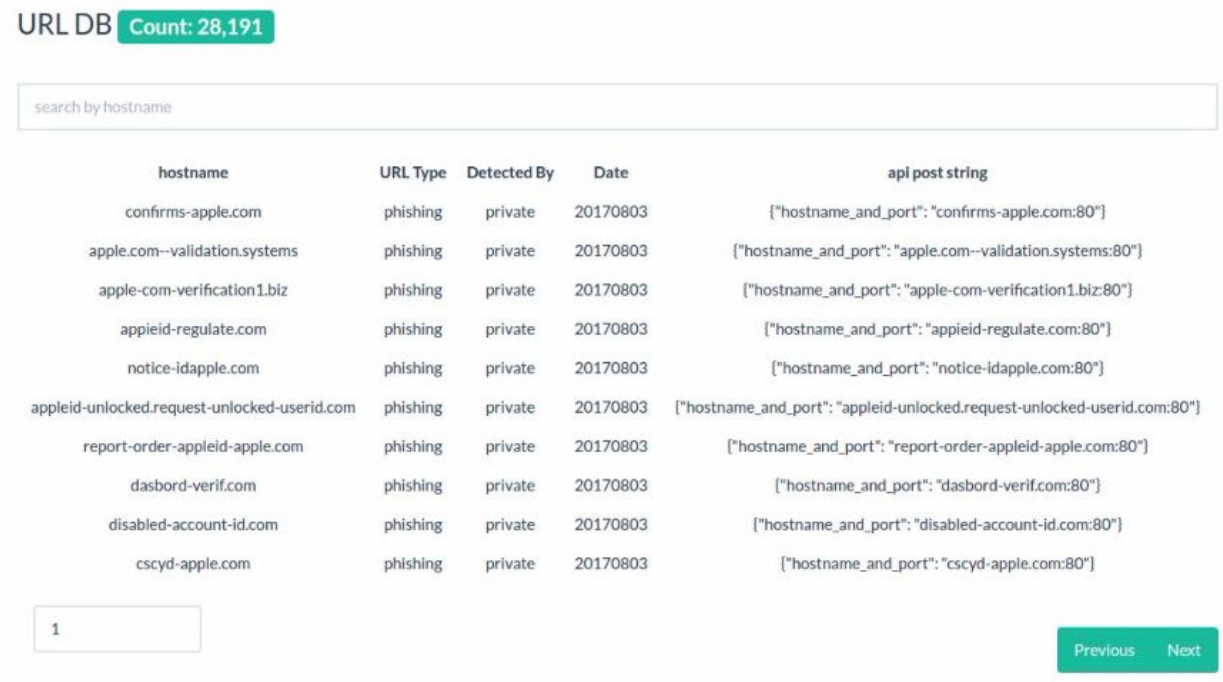


Safe URLs

- youtube.com:80/watch?v=QhcwLyyEjOA
  - Domain name is in the whitelist
  - Query string is not in the blacklist
- Google.com:80
- facebook.com:80

Malicious domain names

A list of URLs in the DB can be viewed at http://45.55.30.245 through google chrome.



URL DB Count: 28,191

search by hostname

hostname	URL Type	Detected By	Date	api post string
confirms-apple.com	phishing	private	20170803	{"hostname_and_port": "confirms-apple.com:80"}
apple.com--validation.systems	phishing	private	20170803	{"hostname_and_port": "apple.com--validation.systems:80"}
apple-com-verification1.biz	phishing	private	20170803	{"hostname_and_port": "apple-com-verification1.biz:80"}
appieid-regulate.com	phishing	private	20170803	{"hostname_and_port": "appieid-regulate.com:80"}
notice-idapple.com	phishing	private	20170803	{"hostname_and_port": "notice-idapple.com:80"}
appleid-unlocked.request-unlocked-userid.com	phishing	private	20170803	{"hostname_and_port": "appleid-unlocked.request-unlocked-userid.com:80"}
report-order-appleid-apple.com	phishing	private	20170803	{"hostname_and_port": "report-order-appleid-apple.com:80"}
dasbord-verif.com	phishing	private	20170803	{"hostname_and_port": "dasbord-verif.com:80"}
disabled-account-id.com	phishing	private	20170803	{"hostname_and_port": "disabled-account-id.com:80"}
cscyd-apple.com	phishing	private	20170803	{"hostname_and_port": "cscyd-apple.com:80"}

1

Previous Next

Malicious URLs

- google.com:80/url/that/is/malware?download=true
  - Sometimes, whitelisted domains can get compromised
    - Whitelisted domain name
    - Blacklisted query string

Neither whitelisted or blacklisted

- fun.amazon.com:/shop/stuff
  - Proceed with caution.