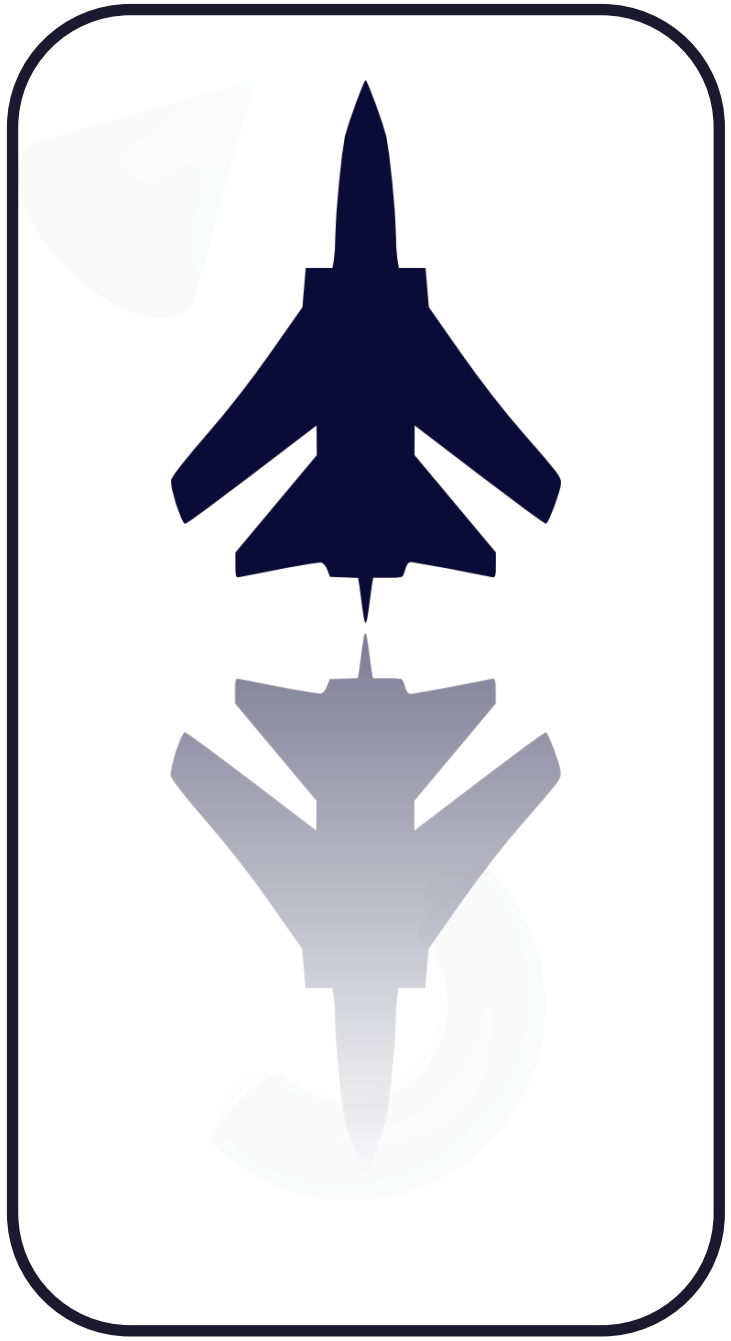


Strafer: A Tool to Detect Infections in Elasticsearch Instances

Aditya K Sood and Rohit Bansal

December 9th, 2020
BlackHat Europe Arsenal 2020

Disclaimer

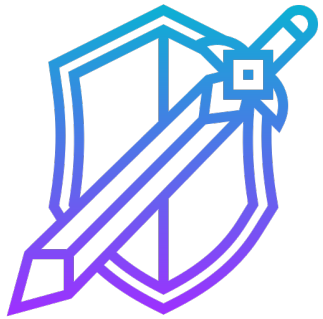
Tool presented in this talk is for sharing research with security community to strengthen the intelligence efforts for enhancing the security of critical services on the internet.

This talk does not relate to any of our previous or present employers.

Strafer Project Team

- Dr. Aditya K Sood
  - Security Practitioner and Researcher
  - Working in the security field for more than 13 years
  - Regular speaker at industry leading security conferences
  - Author of “Targeted Cyber Attacks” Book
  - W: https://www.adityaksood.com
  - T: @adityaksood
  - LinkedIn: https://www.linkedin.com/adityaks

Elasticsearch Threats Research and Tool Development



- Rohit Bansal
  - Principal Researcher, SecNiche Security Labs
  - https://secniche.org/

Elasticsearch Threats Research. And Intelligence Collection

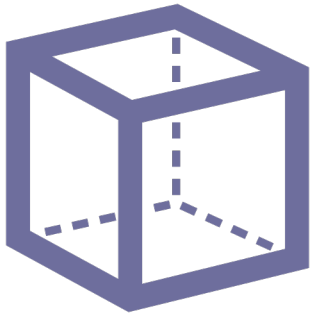
Elasticsearch threats and attacks landscape

Hackers target Elasticsearch clusters in fresh malware campaign

Attack Campaign Targets Exposed Elasticsearch Servers With DDoS Botnet

Attackers Turn Elasticsearch Databases Into DDoS Bots

Beware Of This Internet Cat's Meow—It Destroys Databases



ElasticSearch Ransomware Attacks Highlight Need for Better Security

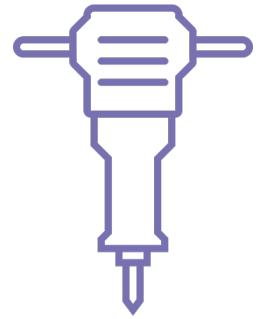
Targeted malware attacks against Elasticsearch servers surge

Old vulnerabilities are proving to be successful.

Dozens of unsecured databases exposed online web wiped by threat actors as part of a campaign tracked as Meow attack.

Introducing Strafer

- Strafer: A tool to detect potential infections in Elasticsearch instances.
- In this version of the tool, the following modules are supported:
  - Elasticsearch instance information gathering and reconnaissance (inline)
  - Elasticsearch instance exposure on the Internet (authentication checks)
  - Detecting potential ransomware infections in the Elasticsearch instances
  - Detecting potential botnet infections such as meow botnet.
  - Detecting infected indices in the Elasticsearch instances
  - Detecting Elasticsearch honeypots



Introducing Strafer

```
$ python strafer.py
        ------------------------------------------------------------


                 _____  __                  ____
                / ___/ / /_ _____ ____ _ / __/___   _____
                \__ \ / __// ___// __ `// /_ / _ \ / ___/
               ___/ // /_ / /   / /_/ // __//  __// /
              /____/ \__//_/    \__,_//_/   \___//_/


        STRAFER : A Tool to Detect Potential Infections in ElasticSearch Deployments !
        Authored by: Aditya K Sood {https://adityaksood.com}

        ------------------------------------------------------------
[-] usage: strafer.py <elasticsearch_host (local or remote)> <elasticsearch service port> <module_name>
[*] modules: [verify_auth] | [ransomware] | [meow_bot] | [eshoney_hp] [espot_hp]
[*]       : verify_auth --> check if elasticsearch interface is <EXPOSED>
[*]       : ransomware --> check potential <RANSOMWARE> infections
[*]       : meow_bot --> check for potential <MEOW BOT> infections
[*]       : eshoney_hp --> check if the elasticsearch instance is <ELASTICHONEY> honeynet
[*]       : espot_hp --> check if the elasticsearch instance is <ELASTICPOT> honeypot

[*] example: strafer.py 127.0.0.1 9200 ransomware
```

Detecting Ransomware Infections

```
$ python strafer.py 94.250.XX.YY 9200 verify_auth
[*] [------------------------------------------------------------]
[*] [     ELASTICSEARCH Infections / Honeypot Detection Tool      ]
[*] [------------------------------------------------------------]


[#] Checking the <GEOIP> status of the Elasticsearch instance ......
[*] Elasticsearch instance is located in <US> | <America/Los_Angeles>

[*] elasticsearch url is constructed as: 94.250.XX.YY:9200

[*] validating authentication: if interface is open to access..

[*] authentication is not in  place for the elasticsearch instance: http://94.250.XX.YY:9200/

[*] security exception occurred: missing authentication credentials

{"error":{"root_cause":[{"type":"security_exception","reason":"missing authentication credentials for REST request [/]","h
ecurity\" charset=\"UTF-8\""}}],"type":"security_exception","reason":"missing authentication credentials for REST request
alm=\"security\" charset=\"UTF-8\""}},"status":401}
[*] ------------------------------------------------------------------------
```

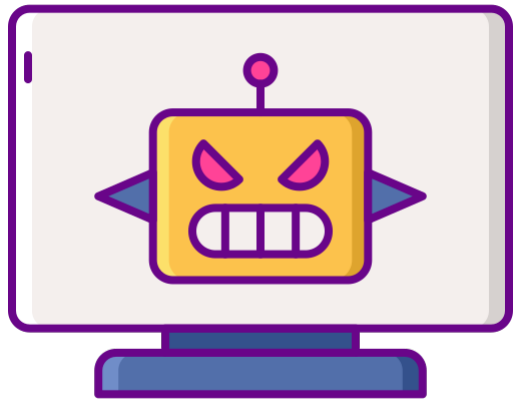
```
$ python strafer.py 121.196.XX.YY 9200 verify_auth
[*] [------------------------------------------------------------]
[*] [     ELASTICSEARCH Infections / Honeypot Detection Tool      ]
[*] [------------------------------------------------------------]


[#] Checking the <GEOIP> status of the Elasticsearch instance ......
[*] Elasticsearch instance is located in <US> | <America/Los_Angeles>

[*] elasticsearch url is constructed as: 121.196.XX.YY:9200

[*] validating authentication: if interface is open to access..

[*] seems like the elasticsearch interface is exposed....

[*] valid URL configuration is: http://121.196.XX.YY:9200/

{
  "name" : "node-1",
  "cluster_name" : "yuanpinhui",
  "cluster_uuid" : "dBVOQcaVSkC7Dh25WB97tw",
  "version" : {
    "number" : "7.10.0",
    "build_flavor" : "default",
    "build_type" : "tar",
    "build_hash" : "51e9d6f22758d0374a0f3f5c6e8f3a7997850f96",
    "build_date" : "2020-11-09T21:30:33.964949Z",
    "build_snapshot" : false,
    "lucene_version" : "8.7.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Detecting Ransomware Infections

```
$ python strafer.py 35.154.XX.YY 9200 ransomware
[*] [------------------------------------------------------------]
[*] [     ELASTICSEARCH Infections / Honeypot Detection Tool      ]
[*] [------------------------------------------------------------]


[#] Checking the <GEOIP> status of the Elasticsearch instance ......
[*] Elasticsearch instance is located in <US> | <America/Los_Angeles>

[*] elasticsearch url is constructed as: 35.154.XX.YY:9200

[*] dumping the search index info to check ransom demand ........
[*] sending request to the source index to analyze the ransomware asks by the malware operator .......
[*] valid URL configuration is: http://35.154.XX.YY:9200/_search?pretty=true

[#] ransomware warning message text pattern matched | pattern - (bitcoin)
[#] ransomware warning message text pattern matched | pattern - (index:read_me)
[#] ransomware warning message text pattern matched | pattern - (data backed up)
[#] ransomware warning message text pattern matched | pattern - (bitcoin_account_identifier)
[#] ---------------------------------------------------------------------
[#] -------- [Elasticsearch Ransomware Infection - Highly Probable] -------
[#] ---------------------------------------------------------------------
[#] Dumping the full data ......................

hits {u'hits': [{u'_score': 1.0, u'_type': u'_doc', u'_id': u'config:7.4.0', u'_source': {u'type': u'config', u'config': {u'buildNum': 26392}, u'updated_at': u'2020-
11-10T18:06:57.633Z'}, u'_index': u'.kibana'}, {u'_score': 1.0, u'_type': u'_doc', u'_id': u'1', u'_source': {u'message': u'All your data is a backed up. You must pa
y 0.04 BTC to 14Ru3Kvvy7G1GSFKS4RXeDKC4KazFDwppy 48 hours for recover it. After 48 hours expiration we will leaked and exposed all your data. In case of refusal to p
ay, we will contact the General Data Protection Regulation, GDPR and notify them that you store user data in an open form and is not safe. Under the rules of the law
, you face a heavy fine or arrest and your base dump will be dropped from our server! You can buy bitcoin here, does not take much time to buy https://localbitcoins.
com with this guide https://localbitcoins.com/guides/how-to-buy-bitcoins After paying write to me in the mail with your DB IP: recoverdb@mailnesia.com and you will r
eceive a link to download your database dump.'}, u'_index': u'read_me'}], u'total': {u'relation': u'eq', u'value': 2}, u'max_score': 1.0}
_shards {u'successful': 2, u'failed': 0, u'skipped': 0, u'total': 2}
took 0
timed_out False

[*] request processed successfully ! exiting !
```

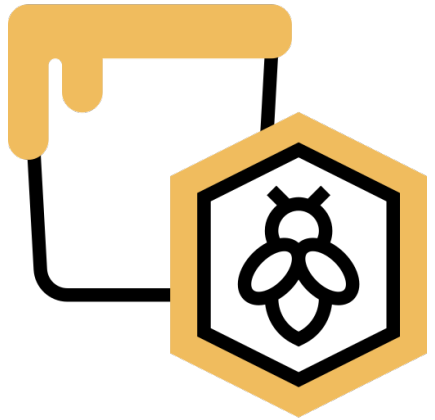
Detecting Botnet Infections

```
$ python strafer.py 47.98.XX.YY 9200 meow_bot
[*] [------------------------------------------------------------]
[*] [     ELASTICSEARCH Infections / Honeypot Detection Tool      ]
[*] [------------------------------------------------------------]


[#] Checking the <GEOIP> status of the Elasticsearch instance ......
[*] Elasticsearch instance is located in <US> | <America/Los_Angeles>

[*] elasticsearch url is constructed as: 47.98.XX.YY:9200
[*] executing detection logic for checking [MEOW Bot]  infections  ..........

[*] valid URL configuration is: http://47.98.XX.YY:9200/_cat/indices?v&health=yellow

[#] detected indices are in yellow state ... potential missing replica shards
[#] despite in yellow state, indices support open operation
[#] detected infection indicator of botnet infection....---- meow botnet
[#] health in yellow detected for indices are in open state with botnet infection signature
[#] Indices are infected. Potential data destruction occured, check your indices and stored data

[#] ----------------------- [MEOW BOTNET INFECTION DETECTED] ---------------------------------


health status index           uuid                   pri rep docs.count docs.deleted store.size pri.store.size
yellow open   .kibana         QD-QeLU7ThKVf9yQphuScg   1   1          1            0       4kb            4kb
yellow open   4fwi9st42u-meow uOuhpgsfRBSUVKr-JtGavA   1   1          0            0      283b           283b
yellow open   wpendns4be-meow 5Ejfpf3xTTO-95CgObYL0A   1   1          0            0      283b           283b
yellow open   b3sxksmbsh-meow vEAalKUdSamQBlqwC_-tYA   1   1          0            0      283b           283b
yellow open   ak3v2d9bva-meow F1HfEa--T9aVacLgJurbWg   1   1          0            0      283b           283b
yellow open   tj1ya6ldph-meow 7gD8GGGVRtuaSWaXKzzYkA   1   1          0            0      283b           283b
yellow open   d83rbdhq6x-meow XPKl4dbCSkmpCgTN2M9LjA   1   1          0            0      283b           283b
yellow open   oigdrgm3tn-meow eu7urXvuQHS9eXMTfle3Ng   1   1          0            0      283b           283b
yellow open   users           S-hY0ioYREGuH10Va8drHw   1   1          2            0      8.4kb          8.4kb
yellow open   nncir8xw0d-meow LlIoNLWYQROxAiwy62Ztbg   1   1          0            0      283b           283b
yellow open   mwiu09xvc0-meow dEvhh7HCS0eUjKe2NxiRjg   1   1          0            0      283b           283b


[*] request processed successfully ! exiting !
```

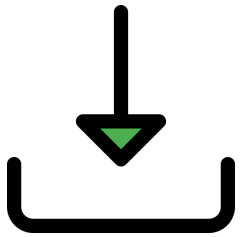


Detecting Elasticsearch honeypots

```
$ python strafer.py 67.205.XX.YY 9200 eshoney_hp
[*] [------------------------------------------------------------]
[*] [     ELASTICSEARCH Infections / Honeypot Detection Tool      ]
[*] [------------------------------------------------------------]


[#] Checking the <GEOIP> status of the Elasticsearch instance ......
[*] Elasticsearch instance is located in <US> | <America/Los_Angeles>

[*] elasticsearch url is constructed as: 67.205.XX.YY:9200

[*] starting ---[ROUND 1]--- detecting indicators for Elastisearch ELASTICHONEY Honeypot.........
[*] valid URL configuration is: http://67.205.XX.YY:9200/

[#] detected buildhash for elastichoney: (build_hash: b88f43fc40b0bcd7f173a1f9ee2e97816de80b19)
[#] detected hardcoded name for elastichoney: (name: USNYES)

[#] ----------------------- [Elasticsearch <ELASTICHONEY> Honeypot Detected] ---------------------------------


[*] starting ---[ROUND 2]--- detecting indicators for Elastisearch ELASTICHONEY Honeypot.........
[*] valid URL configuration is: http://67.205.XX.YY:9200/_security/_authenticate

[#] detected specific indicator for elastichoney <index_not_found_exception> occured for: _security/_authenticate resource -- STRANGE!
[#] detected specific indicator for elastichoney <400> occured for: _security/_authenticate resource -- STRANGE!

[#] ----------------------- [Elasticsearch <ELASTICHONEY> Honeypot Detected] ---------------------------------


[*] starting ---[ROUND 3]--- detecting indicators for Elastisearch ELASTICHONEY Honeypot.........
[*] valid URL configuration is: http://67.205.XX.YY:9200/_cat/indices

[#] detected index for elastichoney: (index_name: 1cf0aa9d61f185b59f643939f862c01f89b21360)
[#] detected index for elastichoney: (index_name: db18744ea5570fa9bf868df44fecd4b58332ff24)

[#] ----------------------- [Elasticsearch <ELASTICHONEY> Honeypot Detected] ---------------------------------


[*] request processed successfully ! exiting !
```



Strafer Tool: Download



https://github.com/adityaks/strafer

Questions and Queries

Aditya K Sood

BlackHat Europe Arsenal 2020