JASK

THREAT ADVISORY

NoSQL-based stacks exposed to the Internet actively exploited

AUTHOR

ROD SOTO / KEVIN STEAR

JASKLABS

TA-00014

TLP

WHITE

RISK FACTOR

MEDIUM

THREAT ADVISORY

NoSQL-based stacks exposed to the Internet actively exploited

AUTHOR
ROD SOTO/
KEVIN STEAR

JASKLABS
TA-00014

TLP
WHITE

RISK FACTOR

MEDIUM

Overview

As reviewed previously by the JASK research team, software frameworks such as LAMP (the Linux operating system, Apache HTTP Server, MySQL relational database management system (RDBMS), and PHP programming language) have become prevalent distributions for hosting content and applications across the internet.

The arrival of Web 2.0 technologies changed this dynamic though, and NoSQL databases (e.g., MongoDB, Redis, HBASE, Cassandra, Neo4j, ElasticSearch) have recently been added to the hosting equation. NoSQL databases provide a mechanism for storage and retrieval of data that is modeled in means other than the tabular relations used in relational databases *. This adoption can be seen in software bundles such as MEAN (MongoDB, Express.js, Angular.js, Node.js), .

However, the addition of new no-sql technologies also brought new risks, vulnerabilities, and subsequent attack vectors. Similar to content management systems, mass exploit campaigns have actively targeted Internet-facing NoSQL distributions for a variety of malicious purposes (e.g., MongoDB, Redis, Elasticsearch). One especially notorious campaign targeting MongoDB distributions even led to the compromise of California's voter database.

Now, recent Imperva research reveals a significant number of Redis hosts have been compromised, adding even more available infrastructure for crime operations such as cryptocurrency mining.

Top NoSQL Attack vectors

- Default/no credentials
- Exposure to the internet
- Remote code execution (I.E CVE-2016-8339, CVE-2016-10572, CVE-2015-5377)
- Combined stack component exploitation (I.E CVE-2017-12629)
- Code injection (I.E. NoSQL injection)

A recent example of how the above attack vectors are quickly modified to turn a profit for criminals is the worm known as RedisWannaMine, a cryptocurrency miner similar to WannaMine. RedisWannaMine exploits a known Apache Struts vulnerability (CVE-2017-9805) to drop a RedisWannaMine cryptocurrency miner payload, which then scans for any other vulnerable Redis and also Windows SMB servers to 'worm' and further propagate infection (and cryptocurrency mining).

AUTHOR
ROD SOTO/
KEVIN STEAR

JASKLABS
TA-00014

TLP
WHITE

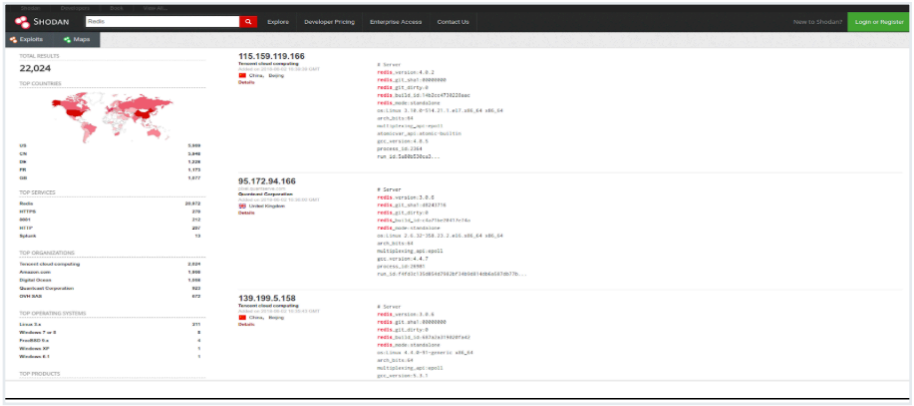
RISK FACTOR

MEDIUM

Lab/Field Study

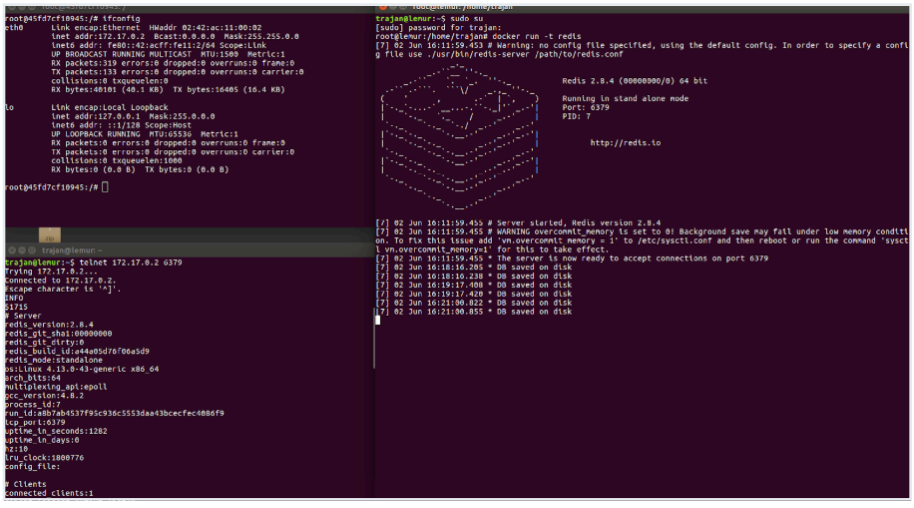
Compromising certain NoSQL distributions can be done with a little work and without much sophistication. The Shodan screenshot below is an example of how easy is to find Redis distributions on the Internet and subsequently access default redis server installs without a password.

Shodan.io Redis results



The following is a proof of concept of simple telnet access and code execution on a default install of a redis server. As can be seen in the screen capture, there is no requirement for a password. This is one method employed by mass exploit campaigns to target default, Internet-facing Redis installs, as well as many MongoDB and Elasticsearch, which have either no authentication requirement or default credentials.

Redis compromise proof of concept



As stated above, malicious actors can and will adapt post-exploitation payloads to perform malicious activities on compromised hosts. An example of this is the RedisWannaMine post exploitation code featured by Imperva research team.

This post-exploitation payload contains code strings that indicate the use of Stratum mining pool protocol. This code indicates that every compromised host has their CPU held hostage as part of a cryptocurrency mining pool. Monero is an example of a popular cryptocurrency that can be mined via CPU cycles.

AUTHOR
ROD SOTO/
KEVIN STEAR

JASKLABS
TA-00014

TLP
WHITE

RISK FACTOR

MEDIUM

RedisWannaMine stratum code from hash
2d89b48ed09e68b1a228e08fd66508d349303f7dc5a0c26aa5144f69c65ce2f2

```
submit_upstream_work stratum_send_line failed
stratum+tcp://
stratum_subscribe send failed
stratum_subscribe timed out
      --no-stratum      disable X-Stratum support
stratum+tcp://%s:%d
stratum thread create failed
no-stratum
stratum_recv_line failed
stratum_recv_line timed out
stratum_recv_line failed to parse a newline-terminated string
stratum_send_line.constprop.27
stratum.lto_priv.37
stratum_handle_method.constprop.16
have_stratum
stratum_thr_id
want_stratum
stratum_thread.lto_priv.57
stratum_thread.part.3.lto_priv.73
stratum_recv_line.constprop.26
```

RedisWannaMine user agent embedded in code
2d89b48ed09e68b1a228e08fd66508d349303f7dc5a0c26aa5144f69c65ce2f2

```
Content-Length: %lu
User-Agent: cpuminer/2.3.3
X-Mining-Extensions: midstate
HTTP request failed: %s
stratum+tcp://
JSON decode failed(%d): %s
JSON protocol response:
error
JSON-RPC call failed: %s
[%d-%02d-%02d %02d:%02d:%02d] %s
Content-Type: application/json
```

JASK Detection

JASK ASOC ingest of relevant log sources and/or the JASK network sensor's deep packet inspection (DPI) can be leveraged to support detection and identification of HTTP traffic of interest. This applies to recent campaigns targeting Redis NoSQL databases and related traffic from malicious cryptocurrency mining.


```
{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"x","pass":"x","agent":"XMRig/2.1.0 (Windows NT 6.1) libuv/1.9.1 gcc/6.3.0"}}
{"id":1,"jsonrpc":"2.0","result":{"id":"486597af-33e5-477f-aa75-c589bcdc4db4","job":
{"blob":"0505a982c6cd057352fedd5f674b745c3a884f7accd08bf7700b63a0077ccb68d3c3548856972900000de635ff0ec584971a02a96305d1c46e2ede7571daee6b8b618e8247dac5620c35709","job_id":"21576de","target":"cf8b0000"},"status":"OK"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0505e582c6cd057352fedd5f674b745c3a884f7accd08bf7700b63a0077ccb68d3c3548856972900000de6d19da2bad4229cd38f30bda78cdfc1cddc422e1ebd0c71587ddb059bee2665c12","job_id":"21577de","target":"cf8b0000"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"05058d83c6cd056a839ec3bb7df66f6d902976645f559c6b900f0986be49d26b196f7aa365a6c3000000def748ab36af5635740a1d988cad0b70c870405afc000432c830b7d40d51fb60950f","job_id":"21578de","target":"cf8b0000"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0505c983c6cd056a839ec3bb7df66f6d902976645f559c6b900f0986be49d26b196f7aa365a6c3000000de801b2eea741eeb0c337a82aa04ccd044c79eb7f334b2597189f897e4923a0ff310","job_id":"21579de","target":"cf8b0000"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"05058584c6cd056a839ec3bb7df66f6d902976645f559c6b900f0986be49d26b196f7aa365a6c3000000dec068f3149c841fc37bf2d2b8e8c7684545d4cef9e59b88402a63e7415edfffe111","job_id":"21580de","target":"cf8b0000"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0505c184c6cd056a839ec3bb7df66f6d902976645f559c6b900f0986be49d26b196f7aa365a6c3000000de4791380796250e4f51d7a3e5d6521e8d6d4973d5662f430ef9ccd8097599a8fb17","job_id":"21581de","target":"cf8b0000"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0505fe84c6cd056a839ec3bb7df66f6d902976645f559c6b900f0986be49d26b196f7aa365a6c3000000de1b71ff7f238388efcac781ff19ec1625e81e9dfd67c16ceb953f1017b84f675717","job_id":"21582de","target":"cf8b0000"}}
```


The example above demonstrates typical 'jsonrpc' traffic being used for Monero mining. ASOC also offers the ability to customize and create patterns for specific header fields (e.g., user agents), strings in URLs, and almost any other feature of the data.

AUTHOR
ROD SOTO/
KEVIN STEAR

JASKLABS
TA-00014

TLP
WHITE

RISK FACTOR

MEDIUM

Mitigation

The following mitigation techniques will work for the most common NoSQL software frameworks. More specific mitigation checks should be applied per use case and per the customization levels of such frameworks.

- Stay up to date on NoSQL updates and security patches. Unless absolutely necessary, do not expose NoSQL databases to the internet.
- Perform assessments against your sites. Make sure there is authentication setup in place and that no default usernames and passwords are used.
- Use complex passwords and multi-factor authentication.
- Use system firewalls and web application firewalls to protect against some attacks.
- Monitor your server for unusual files (webshells, binaries, processes).
- Use Threat Intelligence feeds to monitor for possible NoSQL compromised hosts botnets.
- Monitor your server for unusual traffic. Spikes in traffic to a specific file may indicate the presence of a webshell, cryptocurrency mining traffic or outbound scanning requests.