

Old service

Old service

2

Hi, TCC-CSIRT analyst,

rumors are spreading in the ticketing system that an old, unmaintained service is running somewhere in the network, which could be a security risk (even though it's called **3S - Super Secure Service**). Old-timers claim that it had the domain name **supersecureservice.cypherfix.tcc**. This name does not exist in the current DNS, but some information might still be available on the DNS server **ns6-old.tcc**, which will be shut down soon.

Explore the service and gather as much information as possible about 3S.

Querying the nameserver reveals a lot of information.

```
$ dig @ns6-old.tcc any supersecureservice.cypherfix.tcc

; <<>> DiG 9.20.2-1-Debian <<>> @ns6-old.tcc any
supersecureservice.cypherfix.tcc
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9239
;; flags: qr aa rd; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 085527a14ff8672a0100000067237c724a75fb8a342145ef (good)
;; QUESTION SECTION:
;supersecureservice.cypherfix.tcc. IN ANY

;; ANSWER SECTION:
supersecureservice.cypherfix.tcc. 86400 IN TXT "Super secure service in
```

```
testing mode, any records are hipsters friendly!"
supersecureservice.cypherfix.tcc. 86400 IN HINFO "TCC 686" "TCC-OS 20.20"
supersecureservice.cypherfix.tcc. 86400 IN SVCB 2 web3s-
7468656361746368323032342.cypherfix.tcc. alpn="h2,h3,mandatory=alpn"
port=8020
supersecureservice.cypherfix.tcc. 86400 IN SVCB 4 web3s-
7468656361746368323032343.cypherfix.tcc. alpn="h2,h3,mandatory=alpn"
port=8020
supersecureservice.cypherfix.tcc. 86400 IN SVCB 1 web3s-
7468656361746368323032344.cypherfix.tcc. alpn="h2,h3,mandatory=alpn"
port=8020
supersecureservice.cypherfix.tcc. 86400 IN A      10.99.24.21
supersecureservice.cypherfix.tcc. 86400 IN AAAA 2001:db8:7cc::24:21

;; Query time: 4 msec
;; SERVER: 2001:db8:7cc::24:20#53(ns6-old.tcc) (TCP)
;; WHEN: Thu Oct 31 08:47:47 EDT 2024
;; MSG SIZE rcvd: 526
```

The IP address for the "Super secret service" is 10.99.24.21 , port is 8020 and the expected hostname is web3s-746865636174636832303234.cypherfix.tcc . Combining these pieces of information into an HTTP request yields the service's main page.

```
$ curl -H "Host: web3s-746865636174636832303234.cypherfix.tcc"
http://10.99.24.21:8020/
...
    <small>
    You have right to choose password easy to remember and hard to guess.
<br>
    Your security is important for us, do not hesitate to ask for more
security.<br>
    Log in gracefully and purring like a dozen of cats, so no one can you
see you.<br>
    If you fail to login, use your personal identifier FLAG{yNx6-tH9y-hKtB-
20k6} and show it to user support.<br>
...
```

The text on the page contains the flag: FLAG{yNx6-tH9y-hKtB-20k6} .