Zmap

We performed four zmap internet scans, one from an AWS instance, one from an Azure instance, and two more from different Internet connections.

```
sudo zmap -n 429496729 -B 20M -p 80 -o out.txt -b /etc/zmap/blacklist.conf
```

We combined the scans (see combine.sh) into a single IP list resulting in a combined list of approximately 526,885 unique IP addresses that expose TCP/80 to the Internet. Next, we fed that combined list into zgrab to make HTTP requests for the URL for the unauthenticated settings export.

```
cat ~/combined_deduped.txt | ./zgrab2 --output-file test.json http
↪  --endpoint="/cgi-bin/ExportAllSettings.sh"

grep 'backupsettings.dat' test.json
```

We only found one instance of the HTTP interface exposed on the WAN side.


```
{
  "ip": "REDACTED",
  "data": {
    "http": {
      "status": "success",
      "protocol": "http",
      "result": {
        "response": {
          "status_line": "200 OK",
          "status_code": 200,
          "protocol": {
            "name": "HTTP/1.1",
            "major": 1,
            "minor": 1
          },
          "headers": {
            "content_length": [
              "83"
            ],
            "date": [
              "Fri, 06 May 2022 17:46:00 GMT"
            ],
            "server": [
              "lighttpd"
            ]
          },
          "body": "\n<HTML>\n\n<meta http-equiv=\"Refresh\" content=\"1;
          ↪  url=/backupsettings.dat\">\n\n</HTML>\n",
          "body_sha256": "f37f89bd853d09a5f794981f3e057be57e853d874acd53ecc992c76dd716389a",
```

```
          "content_length": 83,
          "request": {
            "url": {
              "scheme": "http",
              "host": "REDACTED",
              "path": "/cgi-bin/ExportAllSettings.sh"
            },
            "method": "GET",
            "headers": {
              "accept": [
                "*/*"
              ],
              "user_agent": [
                "Mozilla/5.0 zgrab/0.x"
              ]
            },
            "host": "REDACTED"
          }
        }
      },
      "timestamp": "2022-05-06T17:46:00Z"
    }
  }
}
```


The original zmap paper (https://zmap.io/paper.pdf) got a ~1.77% HTTP hit rate, while we got 0.02 - 0.04%. This suggests we may have had issues with how we performed the initial zmap scans. Assuming the actual rate is about 1.7%, we'd expect to see ~73 million hosts exposing HTTP to the Internet. We saw only one WavLink in ~527,000 HTTP hosts. Extrapolating that rate, we would only expect to see less than 140 Wavlinks with web interfaces exposed to the Internet. Thus, it is unlikely any unpatched RCE in the web interface will pose a serious risk of creating a botnet.

This makes sense as, by default, the web interface is not exposed on the WAN side.