Nimble Development, Inc.
63207 Service Rd., Suite 120
Bend, OR 97703

Security Scan Attestation

To whom it may concern:

On a recurring basis and as recently as January 30, 2022, Nimble Development, Inc. performs a network security scan and security analysis services for Net Worth Strategies, Inc. This assessment inspects all public accessible web-based services for both the stockopter.com and networthstrategies.com top level domains as well as all subdomains (such as app.stockopter.com, testapp.stockopter.com, etc…)

Our review of accessible ports revealed only well known and appropriate access, specifically being for HTTP (port 80) and HTTPS (port 443) services. No other points of access are externally visible. Nimble Development, Inc. has confirmed that the Net Worth Strategies team has developed, deployed, and has been shown to actively maintain effective security practices and controls to provide reasonable assurance to protect against unauthorized access and protect information as required in accordance with their contractual customer agreement and security policies.

The scan results are attached as images and this PDF document is digitally signed and locked to prevent editing.

Jack Robson

Digitally signed by Jack Robson
DN: cn=Jack Robson, o, ou, email=jack@highdesertpure.com, c=US
Date: 2022.01.30 13:37:13 -08'00'

Jack Robson
CEO
Nimble Development, Inc.
January 30, 2022

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-01-30 13:24 Pacific Standard Time
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:24
Completed NSE at 13:24, 0.00s elapsed
Initiating NSE at 13:24
Completed NSE at 13:24, 0.00s elapsed
Initiating Ping Scan at 13:24
Scanning app.stockopter.com (13.67.221.130) [4 ports]
Completed Ping Scan at 13:24, 1.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:24
Completed Parallel DNS resolution of 1 host. at 13:24, 0.10s elapsed
Initiating SYN Stealth Scan at 13:24
Scanning app.stockopter.com (13.67.221.130) [1000 ports]
Discovered open port 80/tcp on 13.67.221.130
Discovered open port 443/tcp on 13.67.221.130
Completed SYN Stealth Scan at 13:24, 6.92s elapsed (1000 total ports)
Initiating Service scan at 13:24
Scanning 2 services on app.stockopter.com (13.67.221.130)
Completed Service scan at 13:25, 7.20s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against app.stockopter.com (13.67.221.130)
Retrying OS detection (try #2) against app.stockopter.com (13.67.221.130)
Initiating Traceroute at 13:25
Completed Traceroute at 13:25, 6.07s elapsed
Initiating Parallel DNS resolution of 12 hosts. at 13:25
Completed Parallel DNS resolution of 12 hosts. at 13:25, 0.12s elapsed
NSE: Script scanning 13.67.221.130.
Initiating NSE at 13:25
Completed NSE at 13:26, 67.66s elapsed
Initiating NSE at 13:26
Completed NSE at 13:26, 0.00s elapsed
Nmap scan report for app.stockopter.com (13.67.221.130)
Host is up (0.11s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE VERSION
80/tcp  open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-server-header:
|   Microsoft-HTTPAPI/2.0
|_  Microsoft-IIS/8.5
443/tcp open  ssl     Microsoft SChannel TLS
| fingerprint-strings:
|   TLSSessionReq:
|     +JrhZ
|     feg[*
|     Greater Manchester1
|     Salford1
|     Sectigo Limited1=0;
|     4Sectigo RSA Organization Validation Secure Server CA0
|     210406000000Z
|     220507235959Z0i1
|     Oregon1
|     Bend1
|     Worth Strategies1
|     www.stockopter.com0
```

(continued on following page)

```
|     t-)y
|     W'1"U
|     \xffHN
|     '2H/
|     F4<q
|     C0A05
|_    0%0#
|_http-favicon: Unknown favicon MD5: DD688A943DAFEC40CC5D9361ADD01A4C
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
| http-server-header:
|   <empty>
|_  Microsoft-HTTPAPI/2.0
|_http-title: StockOpter.com
| ssl-cert: Subject: commonName=www.stockopter.com/organizationName=Net Worth Strategies/
stateOrProvinceName=Oregon/countryName=US
| Subject Alternative Name: DNS:www.stockopter.com, DNS:app.stockopter.com, DNS:testapp.stockopter.com,
DNS:www.networthstrategies.com
| Issuer: commonName=Sectigo RSA Organization Validation Secure Server CA/organizationName=Sectigo
Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-04-06T00:00:00
| Not valid after:  2022-05-07T23:59:59
| MD5:   1c32 7d00 6a4c 6070 2c7a 7bbe 0450 ac22
|_SHA-1: 7c45 e179 32a6 bd0f d3ed 82c3 33e3 6b98 26b5 d767
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port443-TCP:V=7.60%I=7%D=1/30%Time=61F7022E%P=i686-pc-windows-windows%r
SF:(TLSSessionReq,111C,"\x16\x03\x03\x12\xbc\x02\0\0M\x03\x03a\xf7\x021\xa
SF:2\x20\+JrhZ\x8c\xed2\x9fr\xa3N\x05\x8f\xe9A\xe8\xa8\xfd\x13feg\[\*\x8d\
SF:x20-\x01\0\0-\xff\xb4\xbc8\x9e\x16\x89d\x10g\xd4\xf4\xa7<\x08\xfe\x9f\x
SF:d4\x05U\x06Kr\r'\xd5\x0f\0/\0\0\x05\xff\x01\0\x01\0\x0b\0\x12c\0\x12`\0
SF:\x06\xb50\x82\x06\xb10\x82\x05\x99\xa0\x03\x02\x01\x02\x02\x10\^Ip\xb5\
SF:xc4\t\xaa\x7fP\xeb\x97\xa5\xba\+~\x1d0\r\x06\t\*\x86H\x86\xf7\r\x01\x01
SF:\x0b\x05\x000\x81\x951\x0b0\t\x06\x03U\x04\x06\x13\x02GB1\x1b0\x19\x06\
SF:x03U\x04\x08\x13\x12Greater\x20Manchester1\x100\x0e\x06\x03U\x04\x07\x1
SF:3\x07Salford1\x180\x16\x06\x03U\x04\n\x13\x0fSectigo\x20Limited1=0;\x06
SF:\x03U\x04\x03\x134Sectigo\x20RSA\x20Organization\x20Validation\x20Secur
SF:e\x20Server\x20CA0\x1e\x17\r210406000000Z\x17\r220507235959Z0i1\x0b0\t\
SF:x06\x03U\x04\x06\x13\x02US1\x0f0\r\x06\x03U\x04\x08\x13\x06Oregon1\r0\x
SF:0b\x06\x03U\x04\x07\x13\x04Bend1\x1d0\x1b\x06\x03U\x04\n\x13\x14Net\x20
SF:Worth\x20Strategies1\x1b0\x19\x06\x03U\x04\x03\x13\x12www\.stockopter\.
SF:com0\x82\x01\"0\r\x06\t\*\x86H\x86\xf7\r\x01\x01\x01\x05\0\x03\x82\x01\
SF:x0f\x000\x82\x01\n\x02\x82\x01\x01\0\xa2v\+\x11\x0c\xad\[M\xb02\x0b\xbb
SF:<\x8ef!g\x8a\xf9\+\xa6\xe1\.\xd5\xb9\x19\x83\x07\xedq\x01\xf8\xc8\n\xc9
SF:\x1a\xec\xf2\xcf\xdfD\x83K\x81t-\)y\x19\x85\xda\x8aN\xd5\xf0\xfb\x1a\x0
SF:8M\xf9\x10j\xeb\xdf\xd83@\xf7\x11\xc1\xc8\xd1~1\x1a\"rb\xba\xa1\xe5b\x9
SF:0\x05\xd1}\xd4&v\xe8E\xa95\xbartL\xd8\x85\x1ab\xb9\xbb\x12R\x06\xf1Ny\x
SF:f9\xd4f\xe2O\xcd\xbd\xab\x94\)\x95y\x89\[\xde\xc7\xacW'1\"U\xe7\xf5\xf3
SF:\xdcf\x93y\"\xb7\xeaO\x02-4\x03\xd8\xb6RB\x1d\x01N\xb1\xd4\|\xc5\xdd\x1
SF:dk\x97:\xfc;\xa0\x19{3\x06~&y\xf9}Dw\xf3\x1d\x1a\xda\x97s\x97\xf0\\\xff
SF:HN\xe2\x90\x12\xc6fC\$\x9b\xee\xd35\xecy\xd8R6>\x11a\xe1\x05\xeck\x0f6y
SF:\xc2'2H/\x9c\[\x0b\x84F4<q\x15t\xa1\xcd\xc6y\x06i\xcc:,w\x8aVh\xc68\xf0
```

(continued on following page)

```
SF:\xc2'2H/\x9c\[\x0b\x84F4<q\x15t\xa1\xcd\xc6y\x06i\xcc:,w\x8aVh\xc68\xf0
SF:hDe\xde<\x96I\xd6K\xe0\xef\x02\x03\x01\0\x01\xa3\x82\x03&0\x82\x03\"0\x
SF:1f\x06\x03U\x1d#\x04\x180\x16\x80\x14\x17\xd9\xd6%'g\xf91\xc2IC\xd906D\
SF:x8c1\xa9O\xeb0\x1d\x06\x03U\x1d\x0e\x04\x16\x04\x14\xc7O\x1d\x8c\x81\xe
SF:4\x185\xa4-\xb5B\xfc\x8b\xd2\xb5\xf6\xc9\xf0\n0\x0e\x06\x03U\x1d\x0f\x0
SF:1\x01\xff\x04\x04\x03\x02\x05\xa00\x0c\x06\x03U\x1d\x13\x01\x01\xff\x04
SF:\x020\x000\x1d\x06\x03U\x1d%\x04\x160\x14\x06\x08\+\x06\x01\x05\x05\x07
SF:\x03\x01\x06\x08\+\x06\x01\x05\x05\x07\x03\x020J\x06\x03U\x1d\x20\x04C0
SF:A05\x06\x0c\+\x06\x01\x04\x01\xb21\x01\x02\x01\x03\x040%0#\x06\x08\+\x0
SF:6\x01\x05\x05\x07\x02");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012 (89%)
OS CPE: cpe:/o:microsoft:windows_server_2012
Aggressive OS guesses: Microsoft Windows Server 2012 (89%), Microsoft Windows Server 2012 or Windows
Server 2012 R2 (89%), Microsoft Windows Server 2012 R2 (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 18.214 days (since Wed Jan 12 08:17:45 2022)
Network Distance: 24 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   1.00 ms  192.168.1.1
2   9.00 ms  192.168.0.1
3   19.00 ms 10.46.64.1
4   23.00 ms bendor04dst52-bune12-28.network.tds.net (64.50.239.150)
5   26.00 ms sttlwawbdst52-bune110.network.tds.net (64.50.240.211)
6   25.00 ms arvdcolndst51-bune19-9.network.tds.net (64.50.243.229)
7   33.00 ms ae23-0.icr02.mwh01.ntwk.msn.net (104.44.232.150)
8   63.00 ms be-102-0.ibr01.mwh01.ntwk.msn.net (104.44.21.143)
9   59.00 ms be-8-0.ibr01.cys04.ntwk.msn.net (104.44.18.222)
10  60.00 ms be-8-0.ibr02.dsm05.ntwk.msn.net (104.44.18.151)
11  57.00 ms 104.44.32.73
12  ... 23
24  60.00 ms 13.67.221.130

NSE: Script Post-scanning.
Initiating NSE at 13:26
Completed NSE at 13:26, 0.00s elapsed
Initiating NSE at 13:26
Completed NSE at 13:26, 0.00s elapsed
Read data files from: D:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 103.27 seconds
           Raw packets sent: 2146 (99.536KB) | Rcvd: 114 (8.991KB)
```