The State of SSL in the World

Michael Boman
Omegapoint

OWASP

Who am I?

- Consultant at Omegapoint (Stockholm)
- Penetration Tester
- Incident Handler
- Course Instructor
  - Secure Development
  - Security Testing

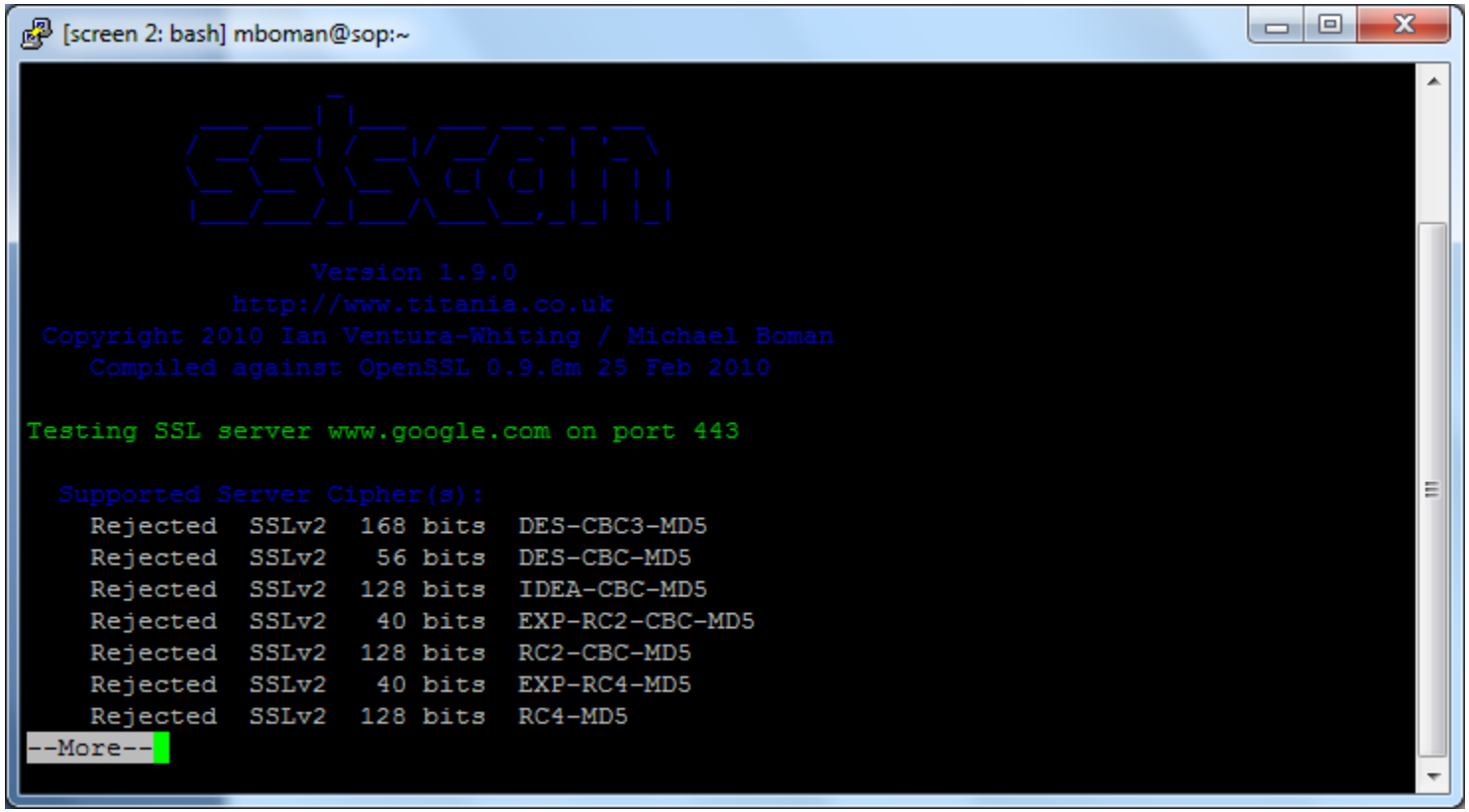
A little background

- Lacked a good tool to perform OWASP-CM-001 tests (Testing for SSL-TLS, OWASP Testing Guide)
  - Couldn't find any that suited my requirements
    - Free, Runs locally, Works on Windows
- Wrote SSLAudit in Perl (GPL)
  - http://code.google.com/p/sslaudit/
  - No longer maintained

A little background (2)

- Re-write SSLAudit or port SSLScan?
  - http://sourceforge.net/projects/sslscan/
- Ported SSLScan to Windows (GPL)
  - http://code.google.com/p/sslscan-win/
- Enhanced SSLScan
  - Renegotiation tests
  - Enhanced XML output format
  - Refactored output code

Demo



SSLSCAN IN ACTION, SINGLE INSTANCE

Why scan a lot of HTTPS servers?

- I noticed that some organizations that you would think would have good security failed miserable on the HTTPS configuration

- Was it a fluke? What differs organizations with good HTTPS settings with those with not-so-good or insecure settings?
  - Money? Popularity? Industry?

First large scan attempt

- Single instance with a large collection of hosts
- Took forever and was not that stable
  - Could not easily resume failed scan process

Second large scan attempt

- Multiple instances with a handful of targets each
- Much better performance, but still takes long time to complete the scan
- Still could not easily resume failed scan process
  - But I didn't need to start from beginning, just the failed batch

Third large scan attempt

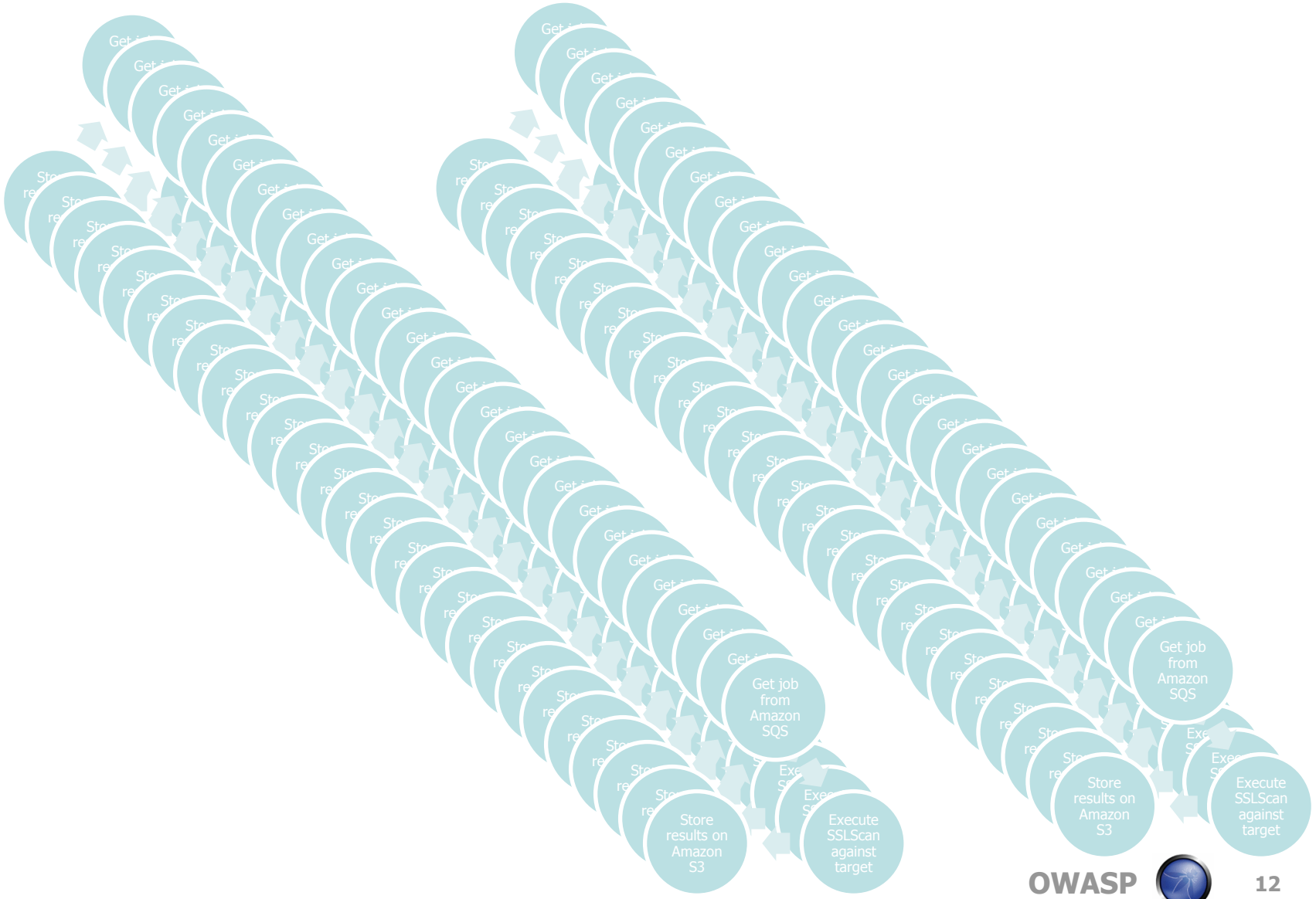
- Using Amazon AWS
  - SQS to keep track of jobs
  - S3 to store results
- Multiple instances scanning one target each
- Easy to resume failed jobs
- Still taking a long time to perform the scan…

Forth large scan attempt

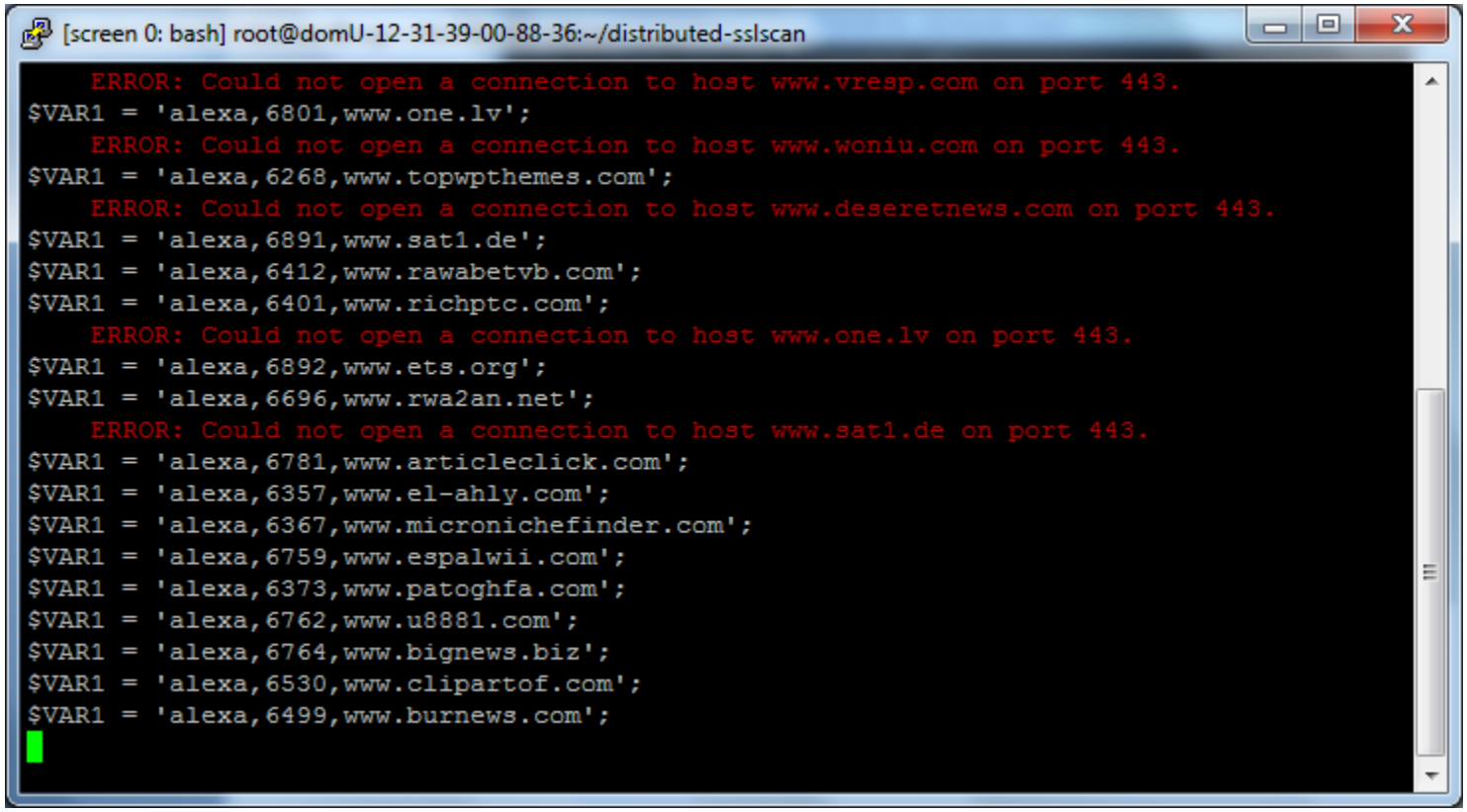
- Added Amazon EC2 to the mix
  - Now I have theoretically unlimited servers to scan from
- Can scan the required dataset within a few days without problem

Forth large scan design

Forth large scan design



Demo



SSLSCAN ON AMAZON EC2

The Question

- What are the key factors for a good HTTPS configuration?
  - Money?
  - Popularity?
  - Industry?

So what did I find?

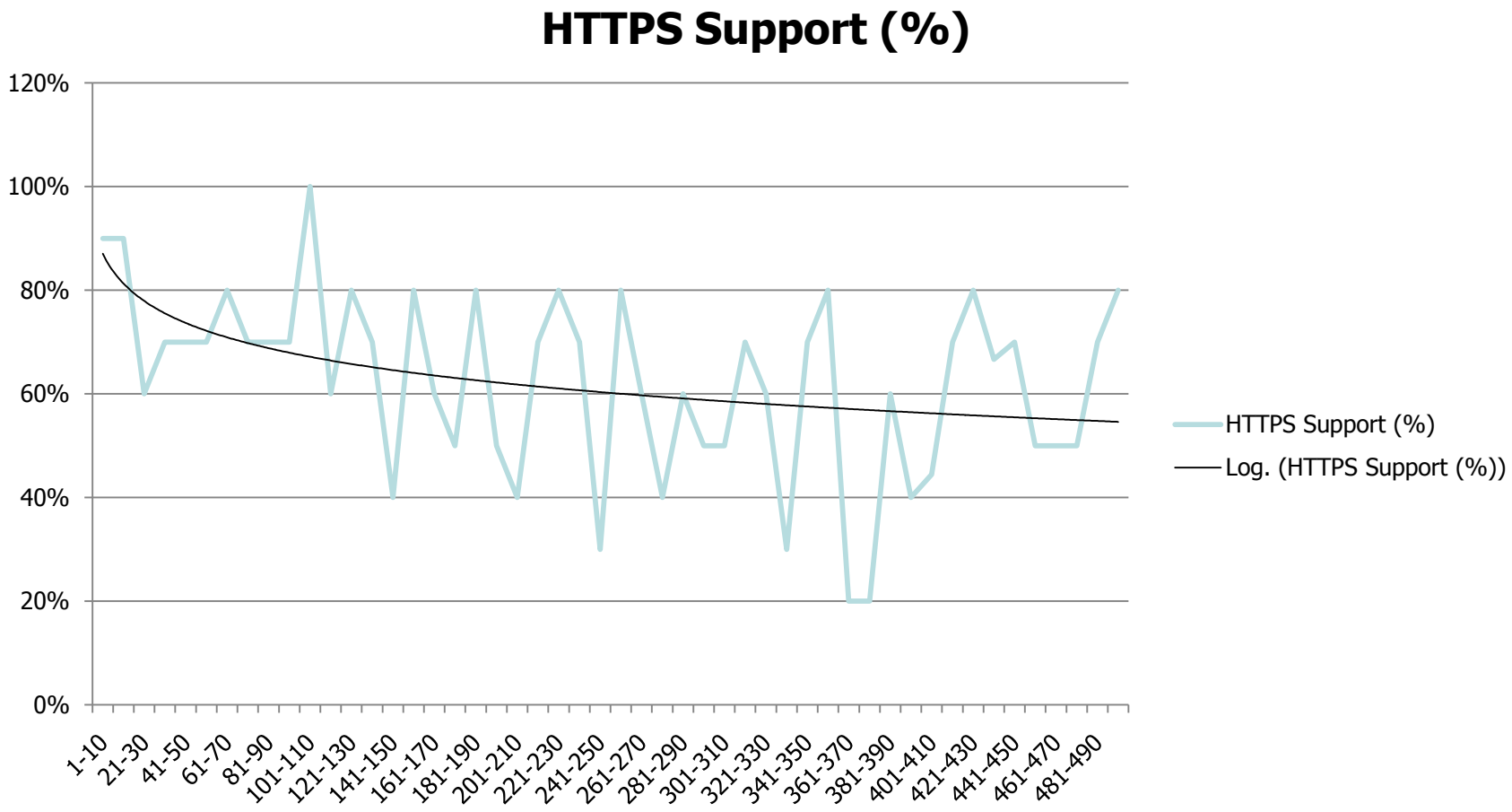
THE NUMBERS...

Data details

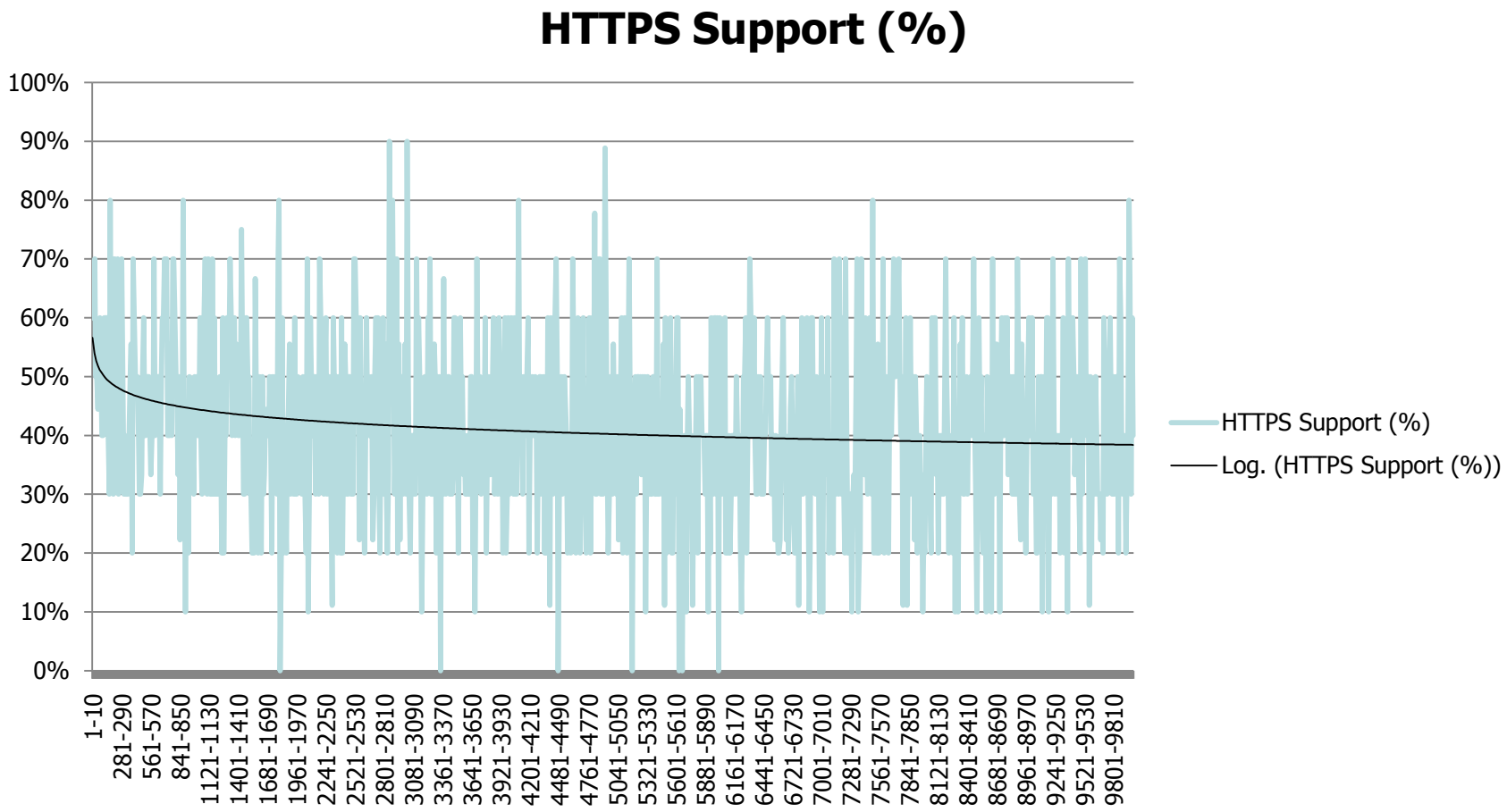
- Alexa list from 18 Apr 2010
- Fortune 500 (2010)
- Data aquired 26 Apr 2010

HOW MANY OF THE TESTED SERVERS SUPPORTS SSL/TLS TO BEGIN WITH?

Fortune 500

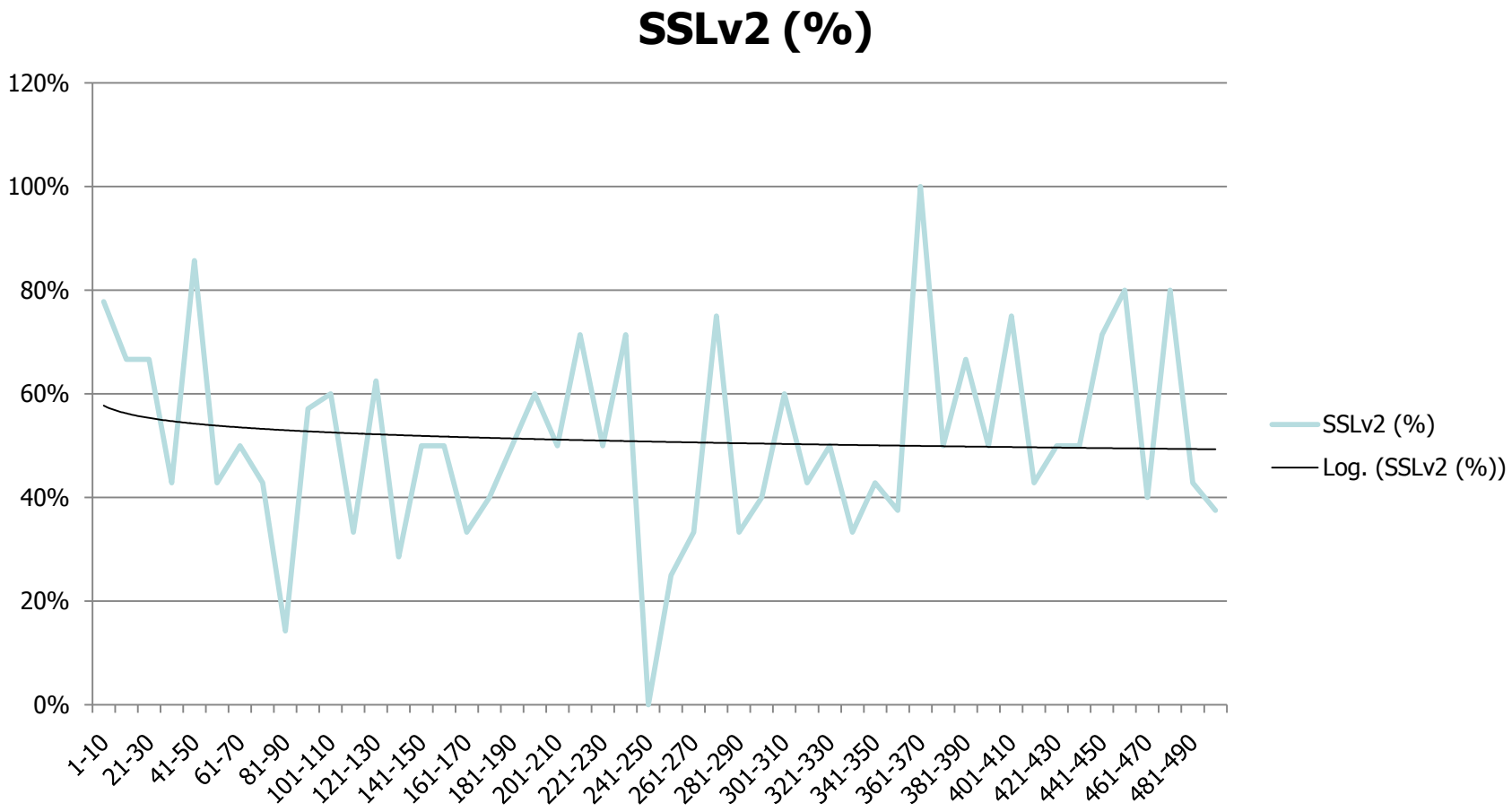

HTTPS Support (%)
120%
100%
80%
60%
40%
20%
0%
1-10
21-30
41-50
61-70
81-90
101-110
121-130
141-150
161-170
181-190
201-210
221-230
241-250
261-270
281-290
301-310
321-330
341-350
361-370
381-390
401-410
421-430
441-450
461-470
481-490
HTTPS Support (%)
Log. (HTTPS Support (%))

Alexa 10k

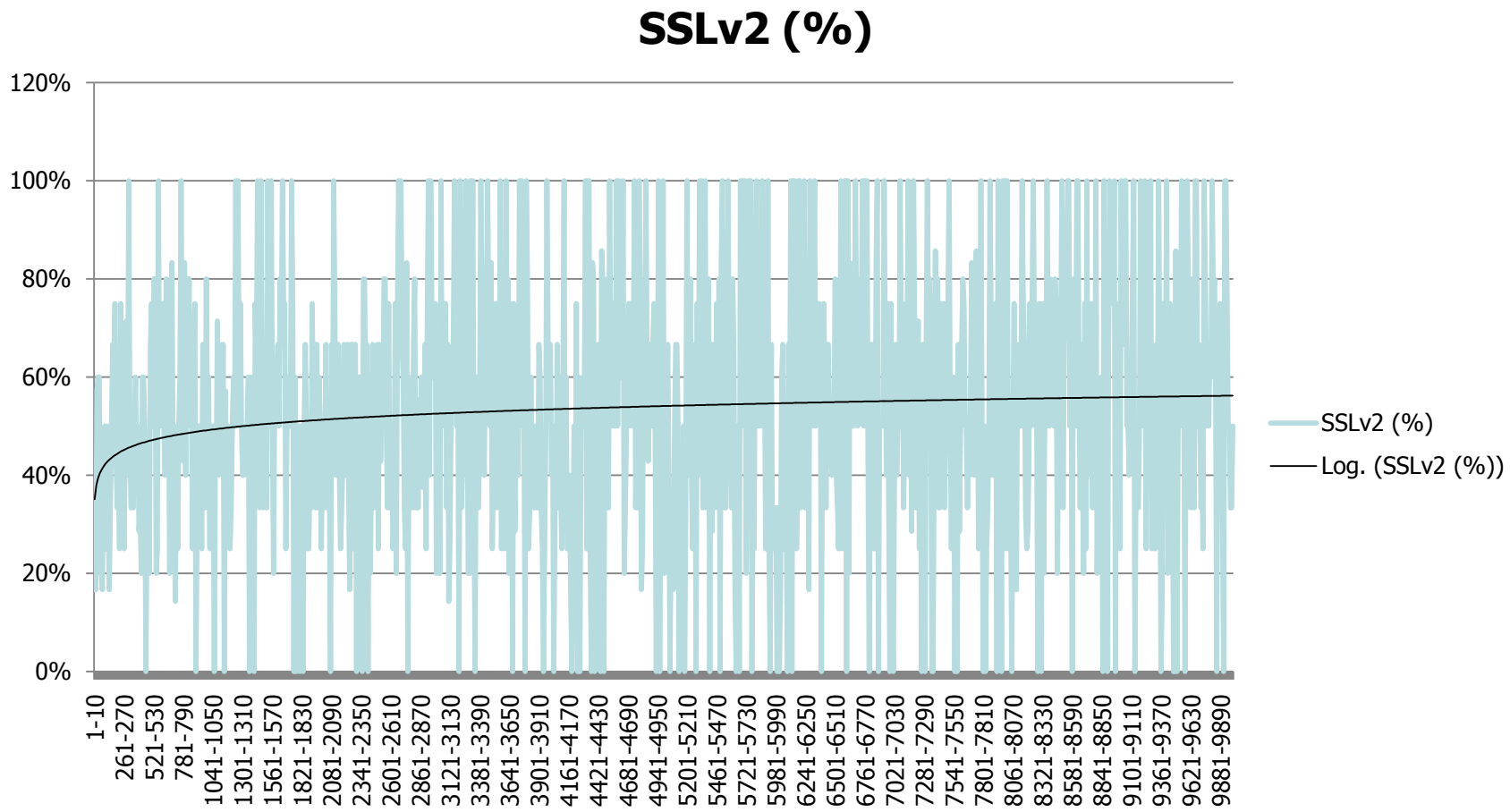

HTTPS Support (%)
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
1-10
281-290
561-570
841-850
1121-1130
1401-1410
1681-1690
1961-1970
2241-2250
2521-2530
2801-2810
3081-3090
3361-3370
3641-3650
3921-3930
4201-4210
4481-4490
4761-4770
5041-5050
5321-5330
5601-5610
5881-5890
6161-6170
6441-6450
6721-6730
7001-7010
7281-7290
7561-7570
7841-7850
8121-8130
8401-8410
8681-8690
8961-8970
9241-9250
9521-9530
9801-9810
HTTPS Support (%)
Log. (HTTPS Support (%))

PROTOCOL SUPPORT

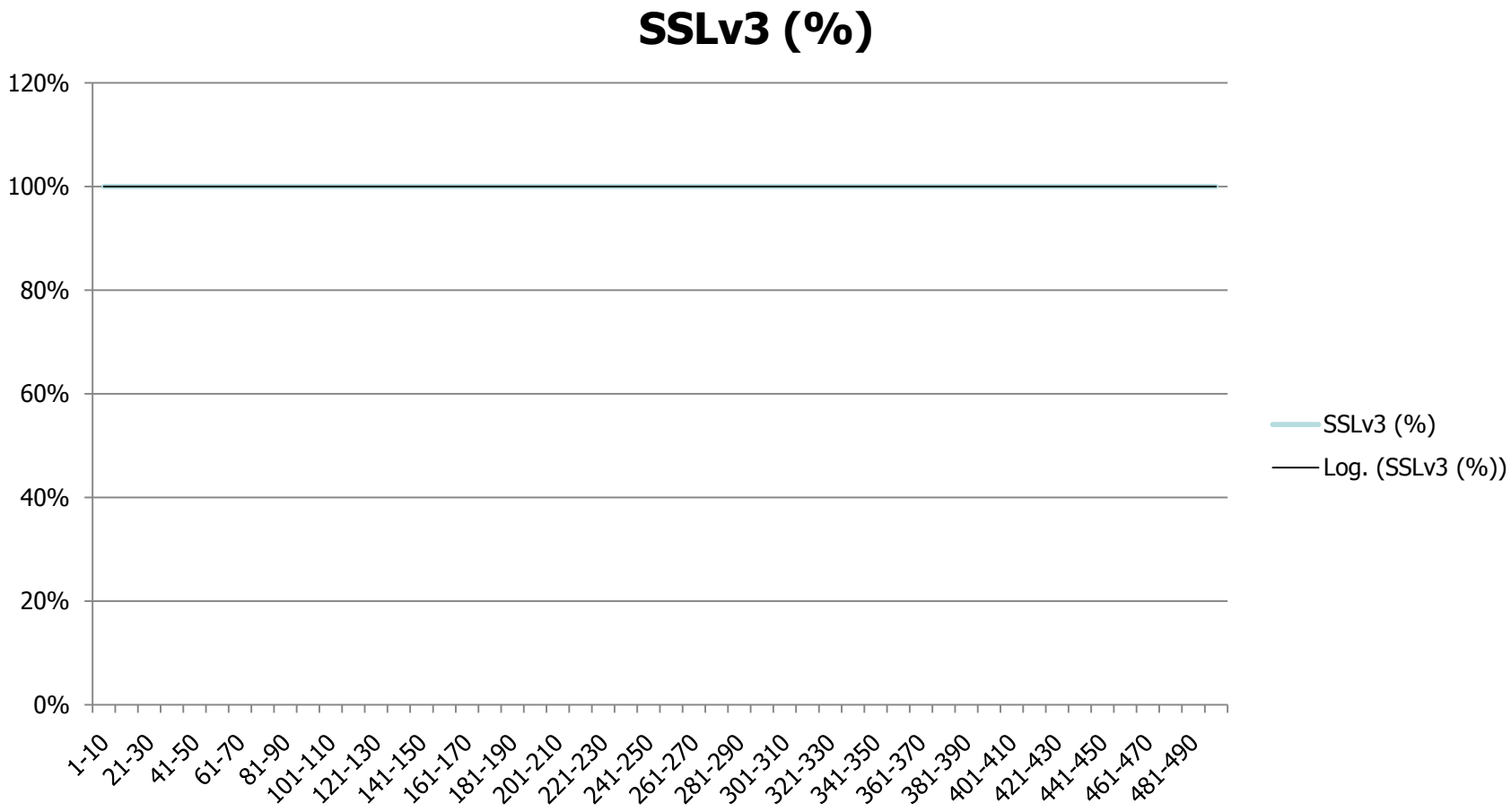
Fortune 500


SSLv2 (%)
120%
100%
80%
60%
40%
20%
0%
1-10
21-30
41-50
61-70
81-90
101-110
121-130
141-150
161-170
181-190
201-210
221-230
241-250
261-270
281-290
301-310
321-330
341-350
361-370
381-390
401-410
421-430
441-450
461-470
481-490
SSLv2 (%)
Log. (SSLv2 (%))

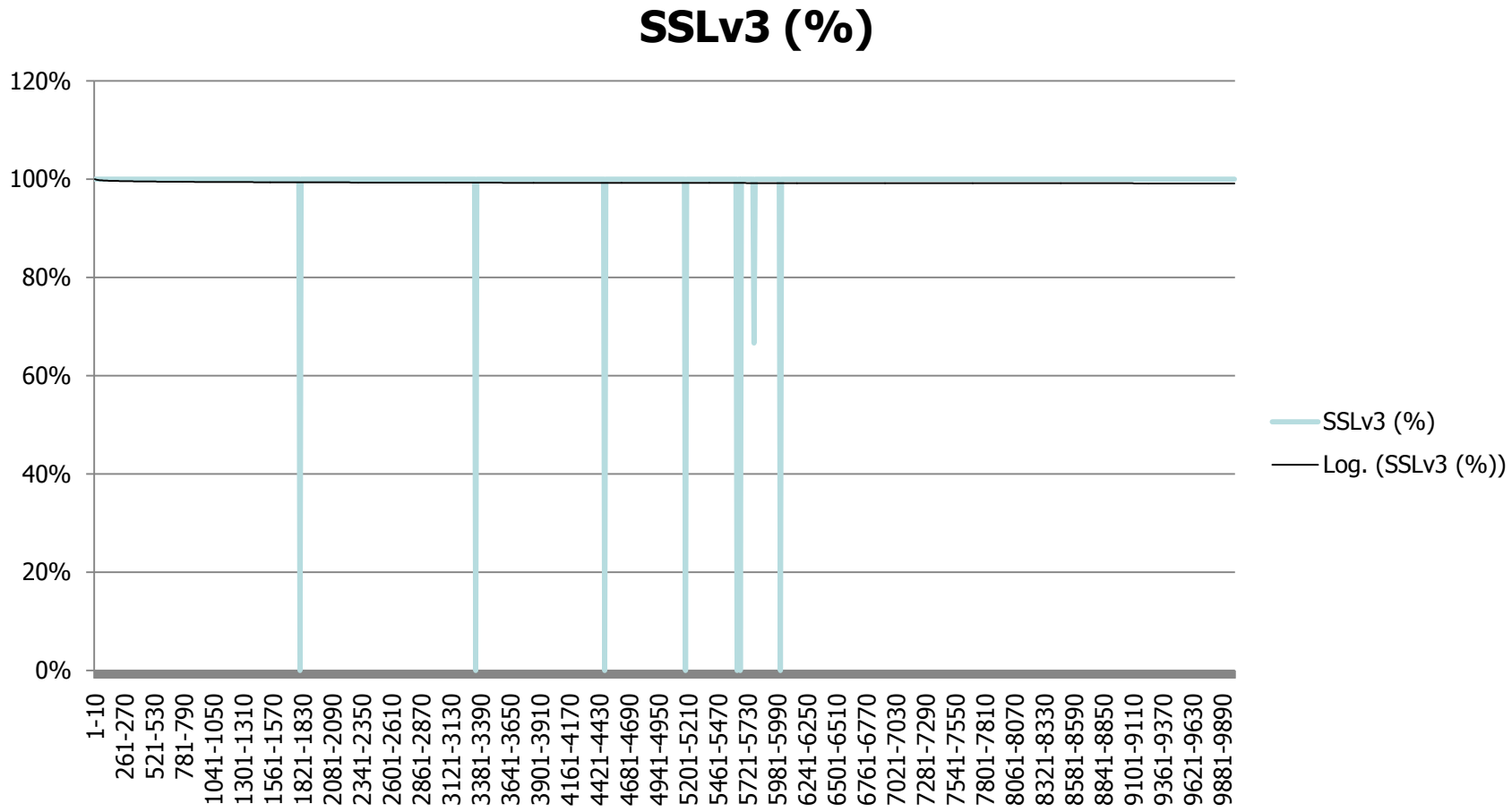
Alexa 10k


SSLv2 (%)
120%
100%
80%
60%
40%
20%
0%
1-10
261-270
521-530
781-790
1041-1050
1301-1310
1561-1570
1821-1830
2081-2090
2341-2350
2601-2610
2861-2870
3121-3130
3381-3390
3641-3650
3901-3910
4161-4170
4421-4430
4681-4690
4941-4950
5201-5210
5461-5470
5721-5730
5981-5990
6241-6250
6501-6510
6761-6770
7021-7030
7281-7290
7541-7550
7801-7810
8061-8070
8321-8330
8581-8590
8841-8850
9101-9110
9361-9370
9621-9630
9881-9890
SSLv2 (%)
Log. (SSLv2 (%))

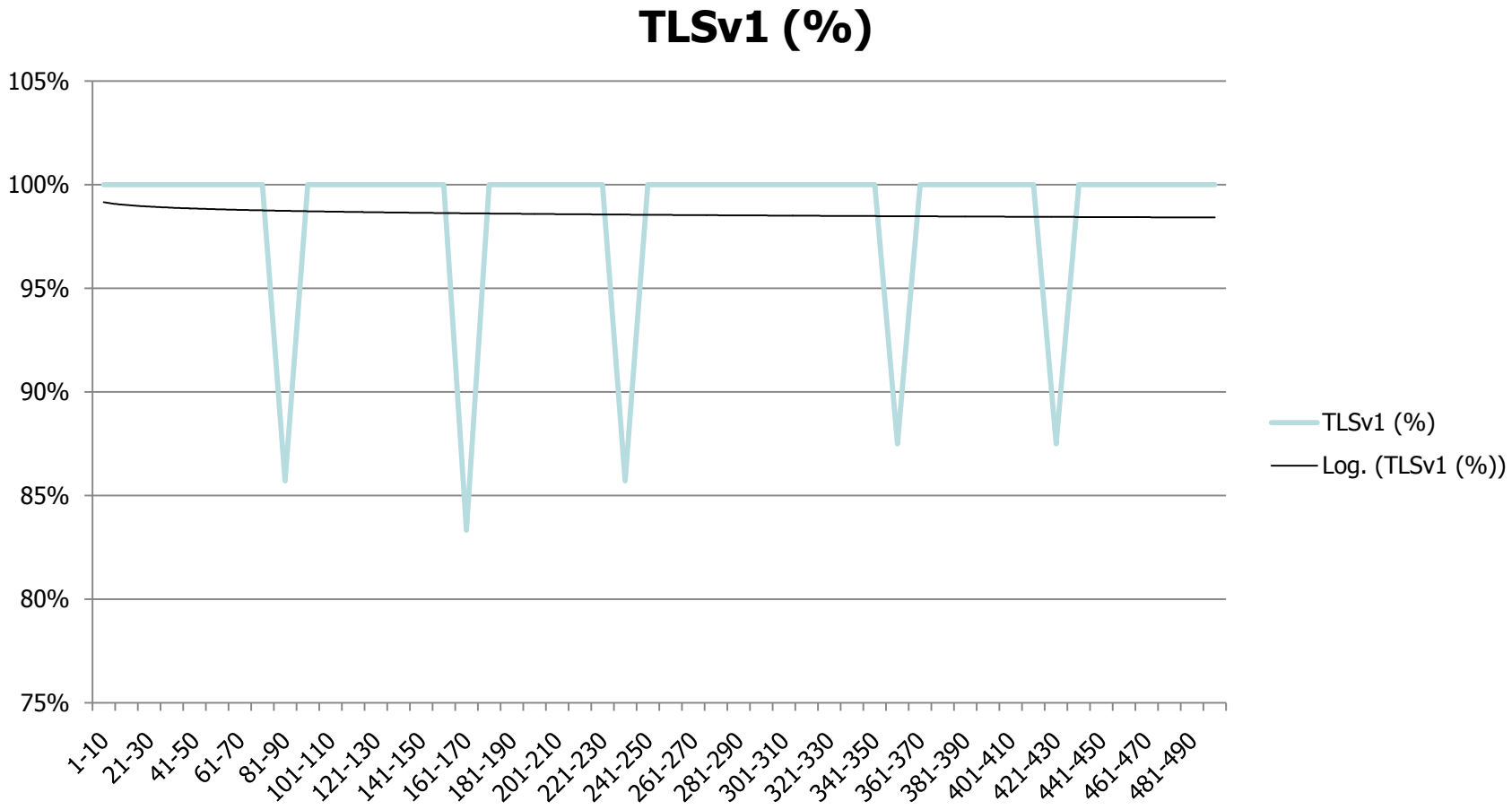
Fortune 500


SSLv3 (%)
120%
100%
80%
60%
40%
20%
0%
1-10
21-30
41-50
61-70
81-90
101-110
121-130
141-150
161-170
181-190
201-210
221-230
241-250
261-270
281-290
301-310
321-330
341-350
361-370
381-390
401-410
421-430
441-450
461-470
481-490
SSLv3 (%)
Log. (SSLv3 (%))

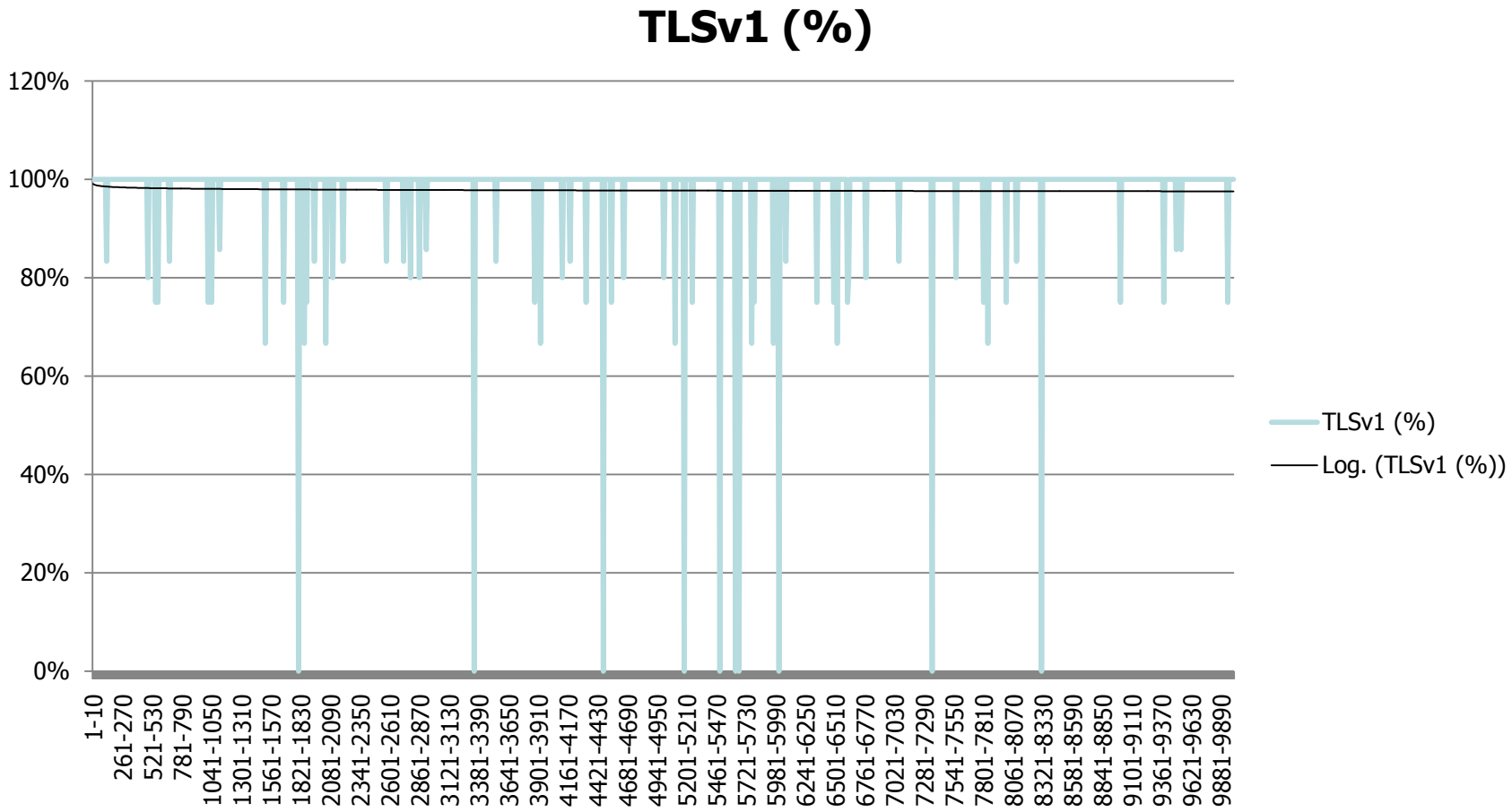
Alexa 10k


SSLv3 (%)
120%
100%
80%
60%
40%
20%
0%
1-10
261-270
521-530
781-790
1041-1050
1301-1310
1561-1570
1821-1830
2081-2090
2341-2350
2601-2610
2861-2870
3121-3130
3381-3390
3641-3650
3901-3910
4161-4170
4421-4430
4681-4690
4941-4950
5201-5210
5461-5470
5721-5730
5981-5990
6241-6250
6501-6510
6761-6770
7021-7030
7281-7290
7541-7550
7801-7810
8061-8070
8321-8330
8581-8590
8841-8850
9101-9110
9361-9370
9621-9630
9881-9890
SSLv3 (%)
Log. (SSLv3 (%))

Fortune 500

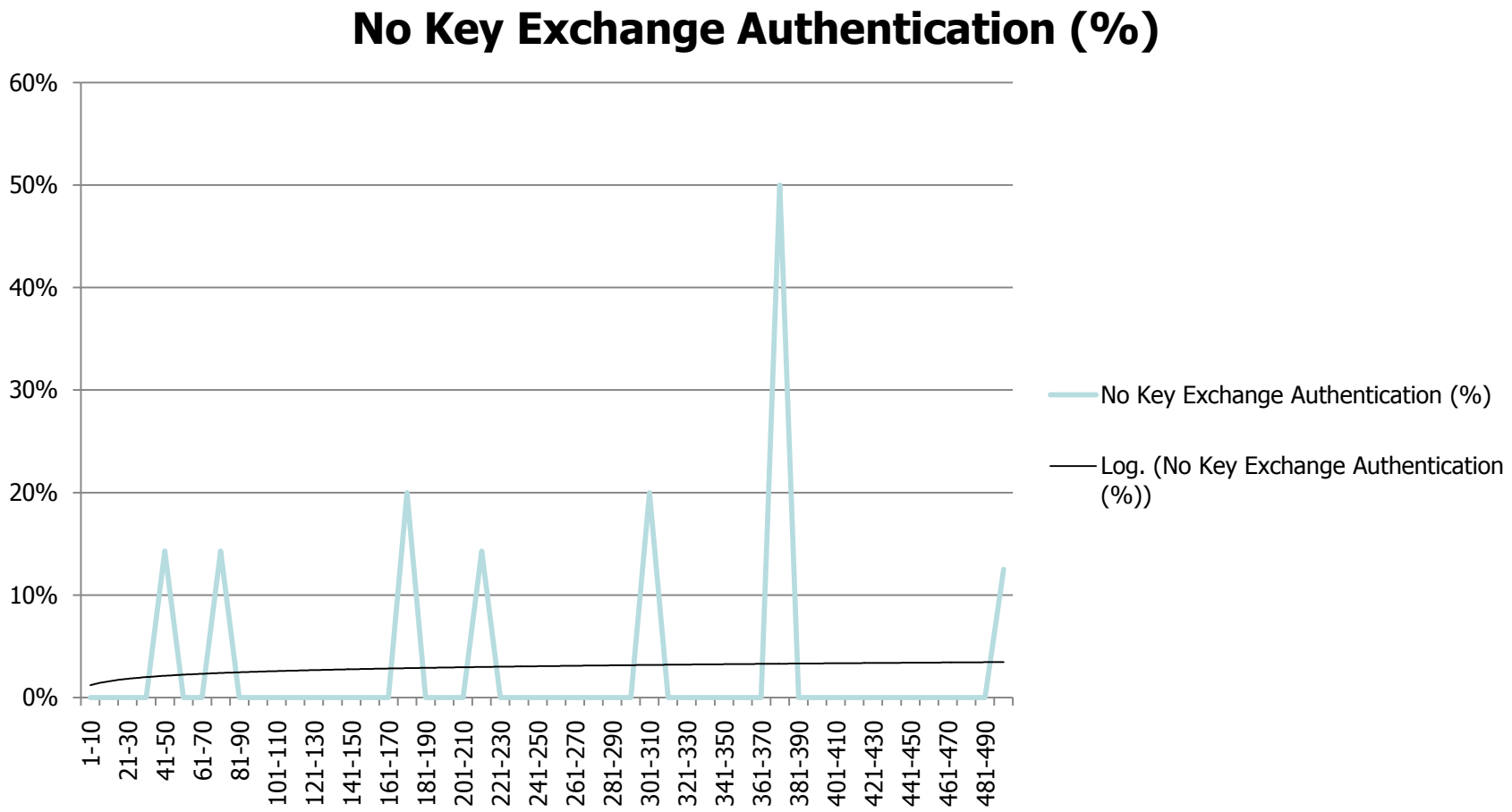

TLSv1 (%)
105%
100%
95%
90%
85%
80%
75%
1-10
21-30
41-50
61-70
81-90
101-110
121-130
141-150
161-170
181-190
201-210
221-230
241-250
261-270
281-290
301-310
321-330
341-350
361-370
381-390
401-410
421-430
441-450
461-470
481-490
TLSv1 (%)
Log. (TLSv1 (%))

Alexa 10k

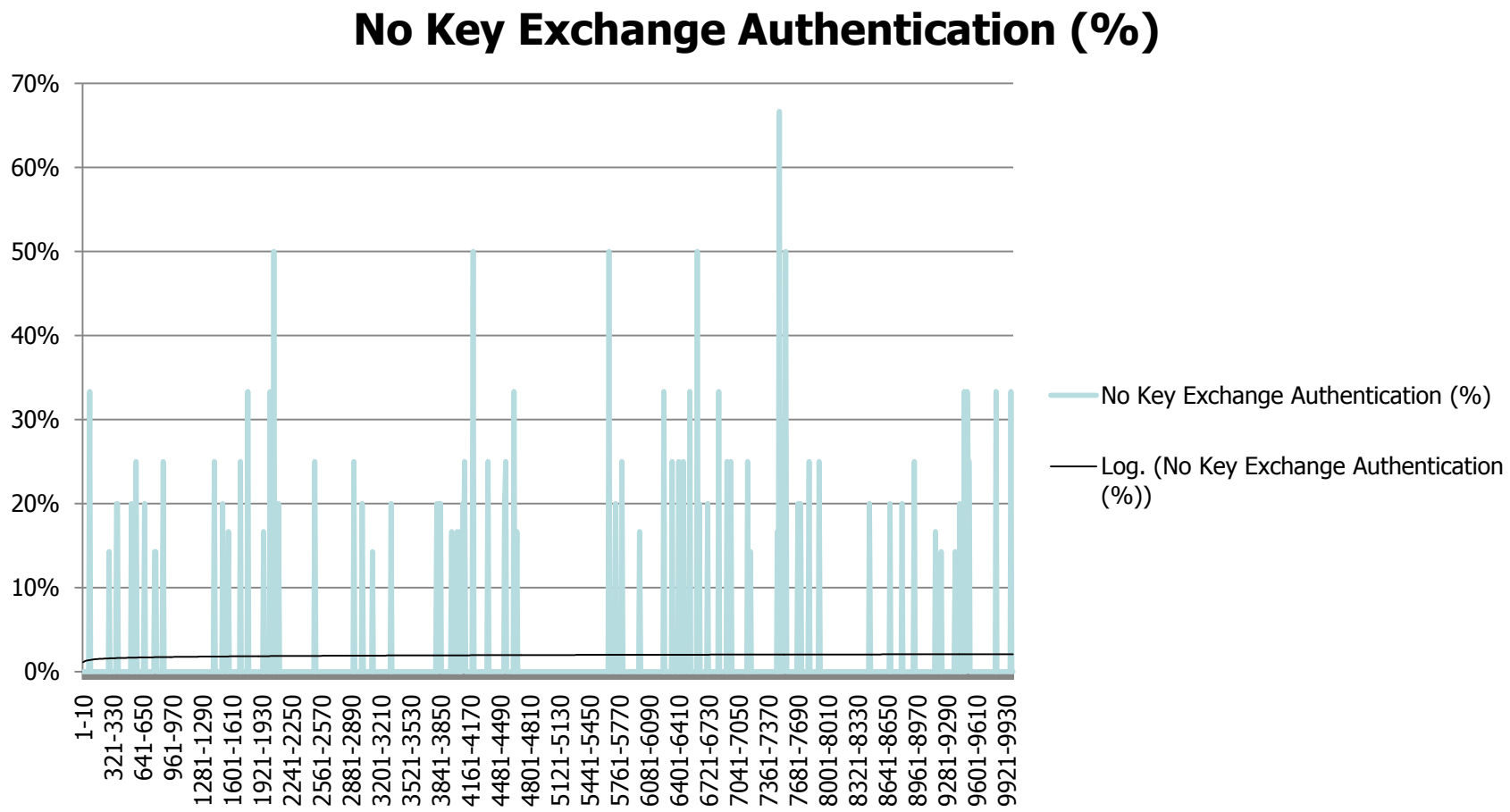

TLSv1 (%)
120%
100%
80%
60%
40%
20%
0%
1-10
261-270
521-530
781-790
1041-1050
1301-1310
1561-1570
1821-1830
2081-2090
2341-2350
2601-2610
2861-2870
3121-3130
3381-3390
3641-3650
3901-3910
4161-4170
4421-4430
4681-4690
4941-4950
5201-5210
5461-5470
5721-5730
5981-5990
6241-6250
6501-6510
6761-6770
7021-7030
7281-7290
7541-7550
7801-7810
8061-8070
8321-8330
8581-8590
8841-8850
9101-9110
9361-9370
9621-9630
9881-9890
TLSv1 (%)
Log. (TLSv1 (%))

INSECURE KEY EXCHANGE

Fortune 500


No Key Exchange Authentication (%)
60%
50%
40%
30%
20%
10%
0%
1-10
21-30
41-50
61-70
81-90
101-110
121-130
141-150
161-170
181-190
201-210
221-230
241-250
261-270
281-290
301-310
321-330
341-350
361-370
381-390
401-410
421-430
441-450
461-470
481-490
No Key Exchange Authentication (%)
Log. (No Key Exchange Authentication (%))

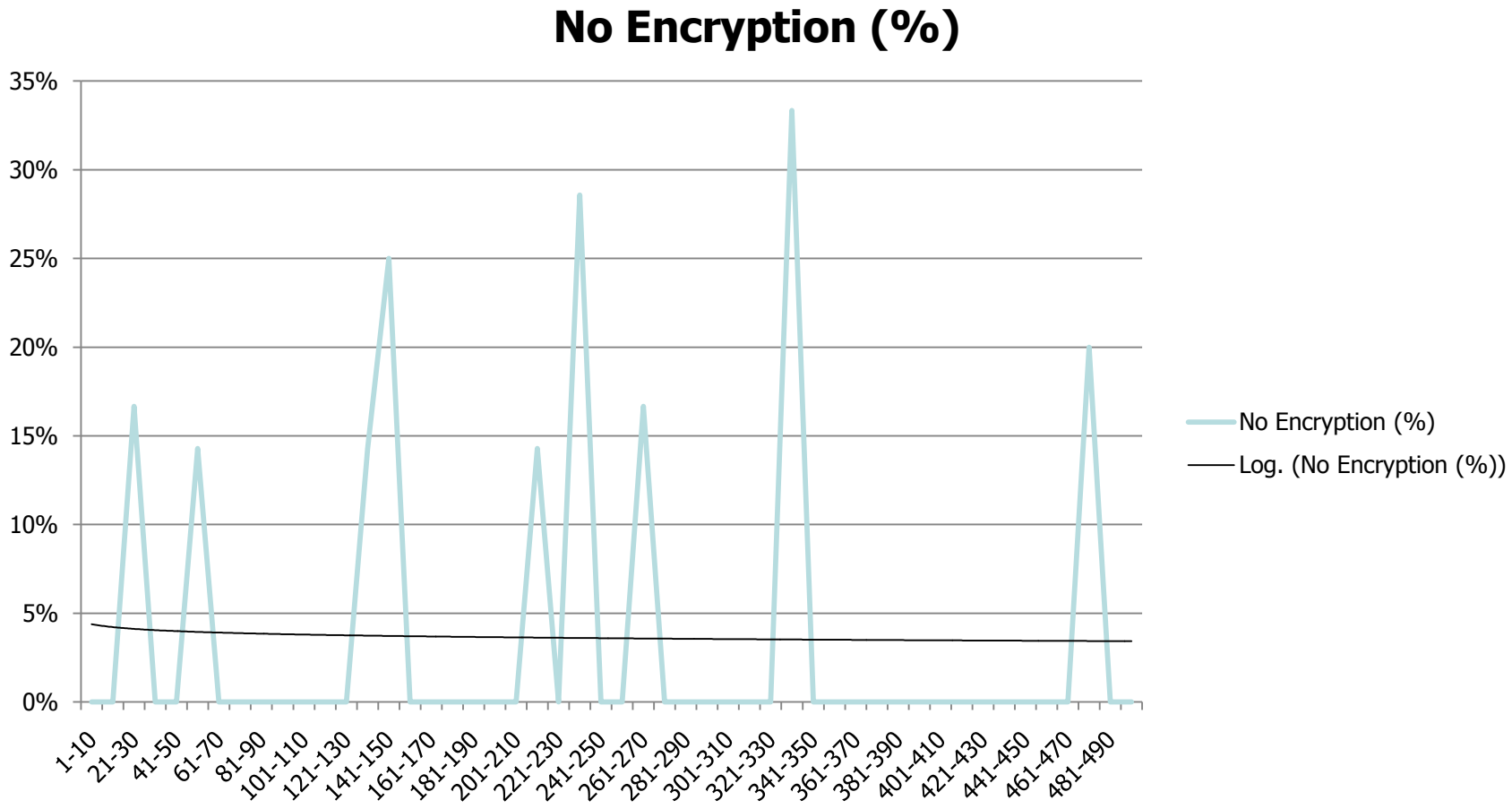
Alexa 10k


No Key Exchange Authentication (%)
70%
60%
50%
40%
30%
20%
10%
0%
1-10
321-330
641-650
961-970
1281-1290
1601-1610
1921-1930
2241-2250
2561-2570
2881-2890
3201-3210
3521-3530
3841-3850
4161-4170
4481-4490
4801-4810
5121-5130
5441-5450
5761-5770
6081-6090
6401-6410
6721-6730
7041-7050
7361-7370
7681-7690
8001-8010
8321-8330
8641-8650
8961-8970
9281-9290
9601-9610
9921-9930
No Key Exchange Authentication (%)
Log. (No Key Exchange Authentication (%))

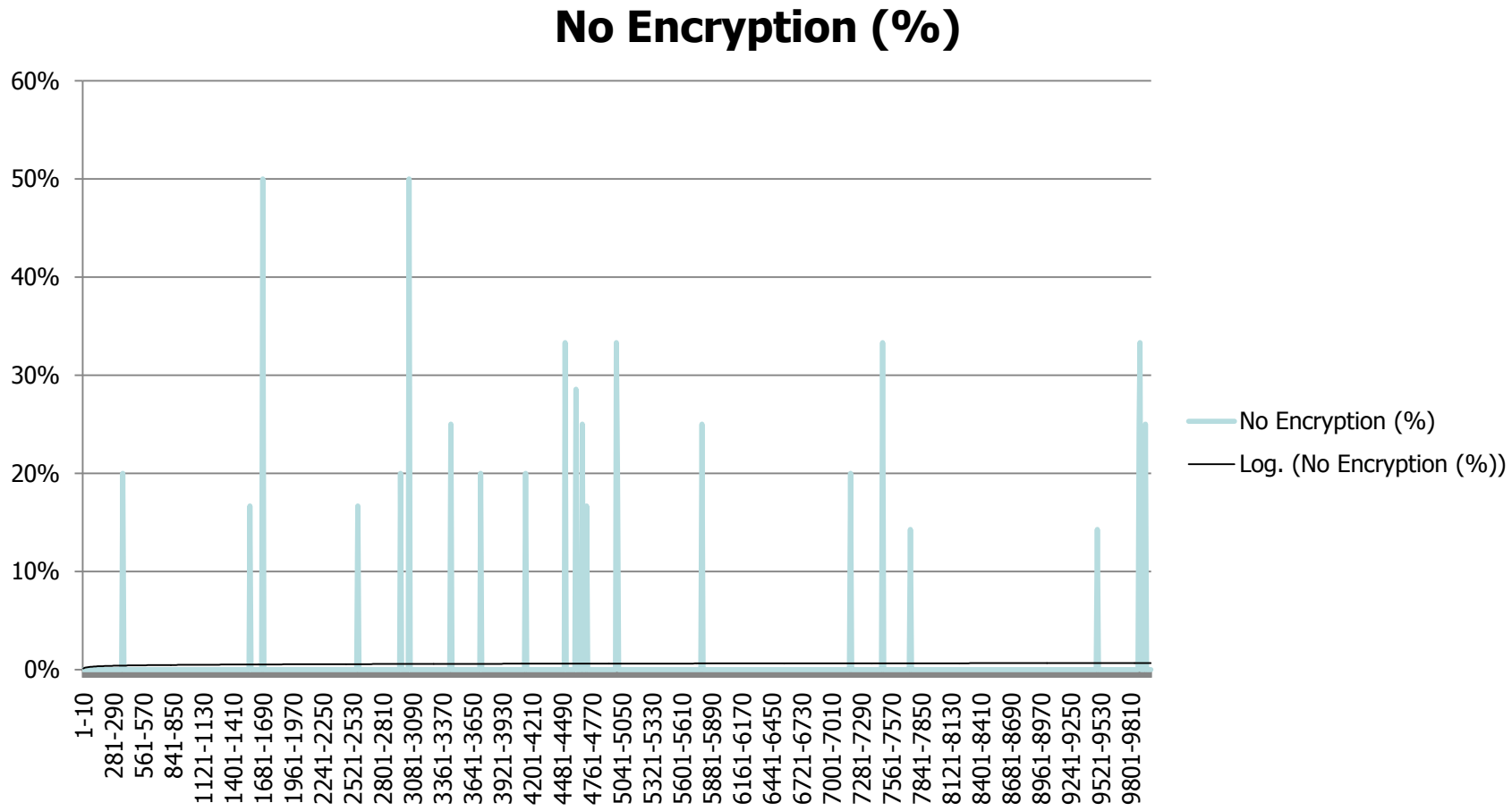
KEY LENGTHS

NO ENCRYPTION (0 BIT KEY)

Fortune 500

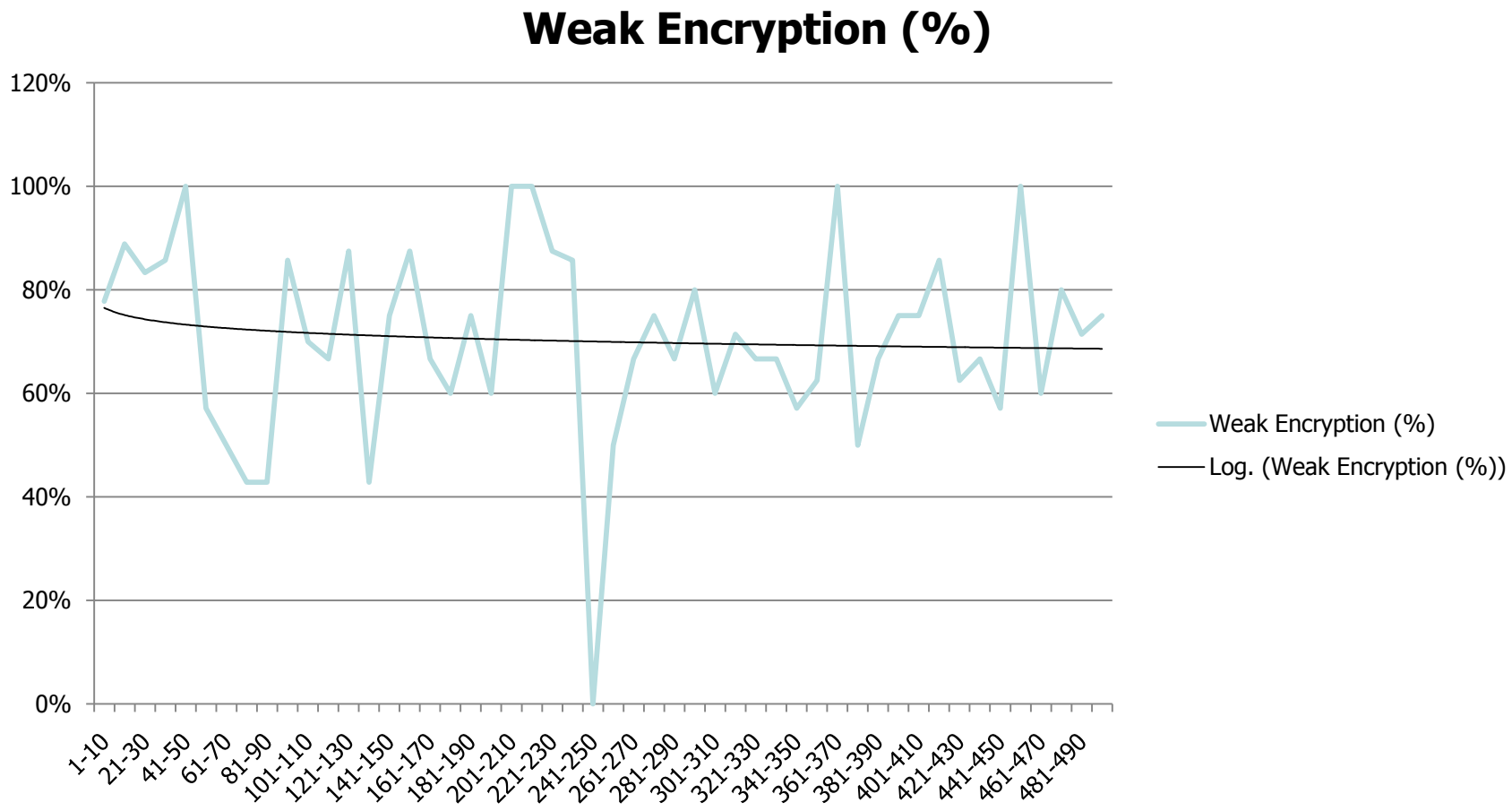

No Encryption (%)
35%
30%
25%
20%
15%
10%
5%
0%
1-10
21-30
41-50
61-70
81-90
101-110
121-130
141-150
161-170
181-190
201-210
221-230
241-250
261-270
281-290
301-310
321-330
341-350
361-370
381-390
401-410
421-430
441-450
461-470
481-490
No Encryption (%)
Log. (No Encryption (%))

Alexa 10k

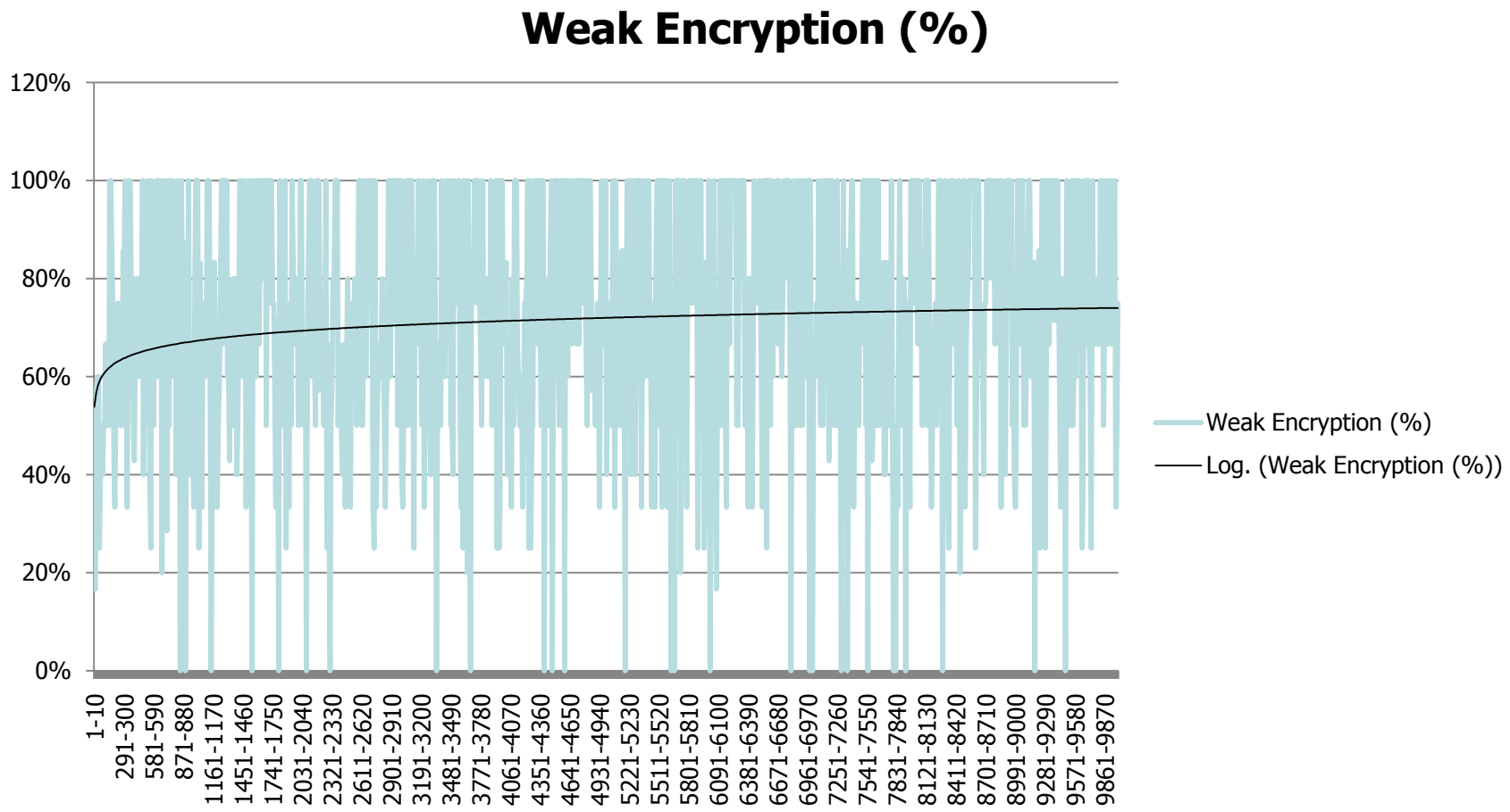

No Encryption (%)
60%
50%
40%
30%
20%
10%
0%
1-10
281-290
561-570
841-850
1121-1130
1401-1410
1681-1690
1961-1970
2241-2250
2521-2530
2801-2810
3081-3090
3361-3370
3641-3650
3921-3930
4201-4210
4481-4490
4761-4770
5041-5050
5321-5330
5601-5610
5881-5890
6161-6170
6441-6450
6721-6730
7001-7010
7281-7290
7561-7570
7841-7850
8121-8130
8401-8410
8681-8690
8961-8970
9241-9250
9521-9530
9801-9810
No Encryption (%)
Log. (No Encryption (%))

WEAK ENCRYPTION (1-127 BIT KEY)

Fortune 500

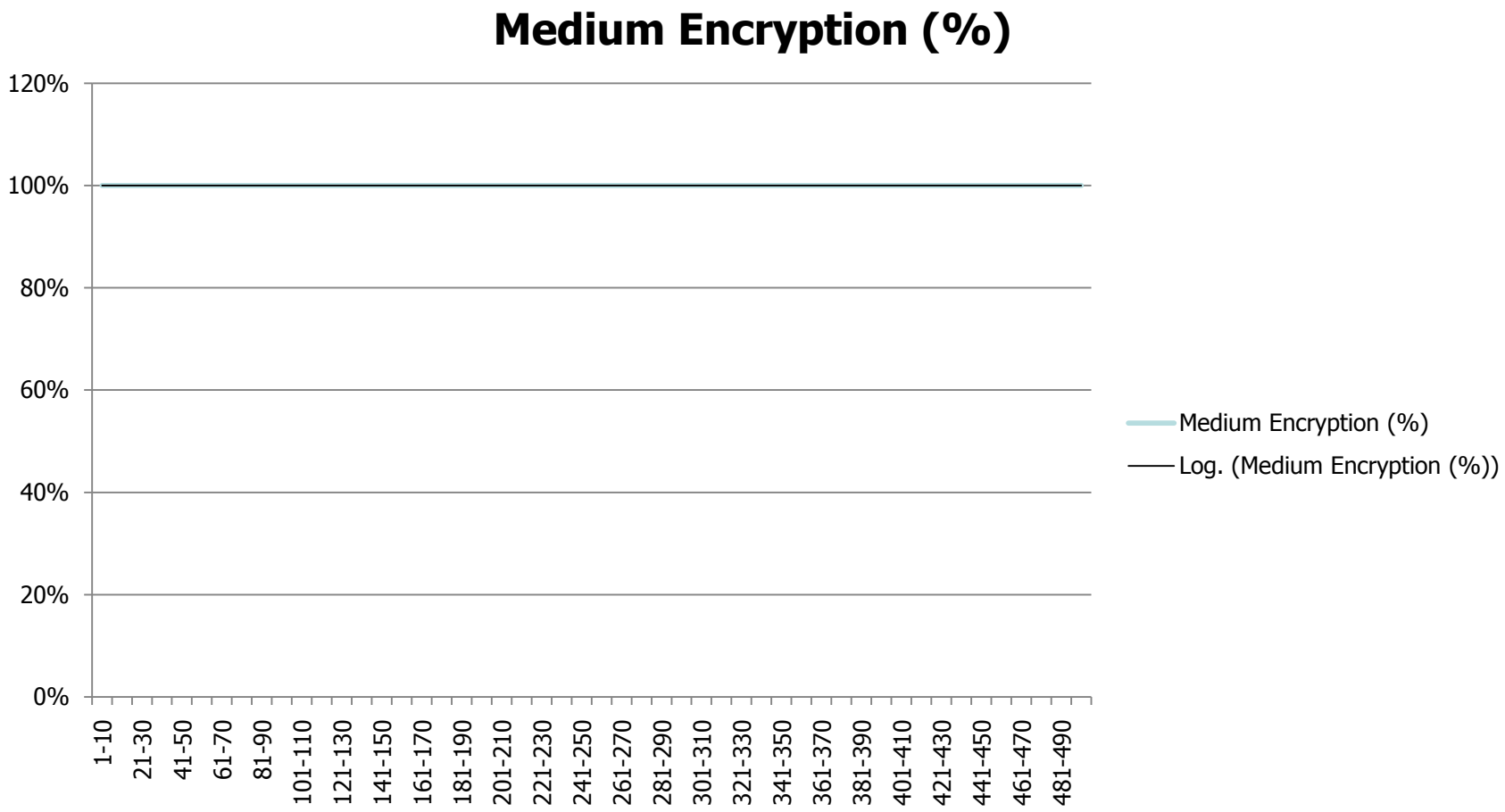

Weak Encryption (%)
120%
100%
80%
60%
40%
20%
0%
1-10
21-30
41-50
61-70
81-90
101-110
121-130
141-150
161-170
181-190
201-210
221-230
241-250
261-270
281-290
301-310
321-330
341-350
361-370
381-390
401-410
421-430
441-450
461-470
481-490
Weak Encryption (%)
Log. (Weak Encryption (%))

Alexa 10k

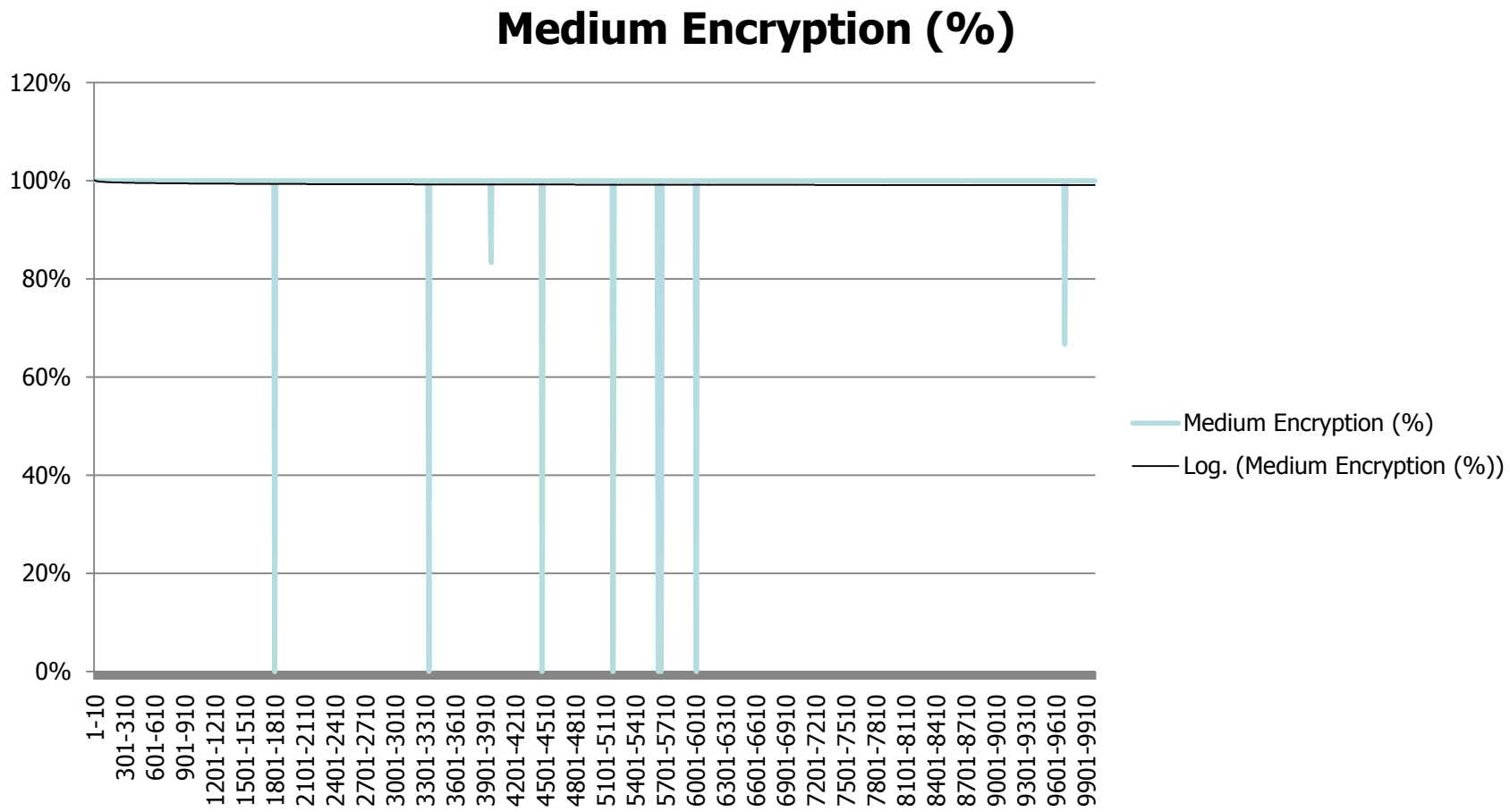

Weak Encryption (%)
120%
100%
80%
60%
40%
20%
0%
1-10
291-300
581-590
871-880
1161-1170
1451-1460
1741-1750
2031-2040
2321-2330
2611-2620
2901-2910
3191-3200
3481-3490
3771-3780
4061-4070
4351-4360
4641-4650
4931-4940
5221-5230
5511-5520
5801-5810
6091-6100
6381-6390
6671-6680
6961-6970
7251-7260
7541-7550
7831-7840
8121-8130
8411-8420
8701-8710
8991-9000
9281-9290
9571-9580
9861-9870
Weak Encryption (%)
Log. (Weak Encryption (%))

MEDIUM ENCRYPTION (128-255 BIT KEY)

Fortune 500

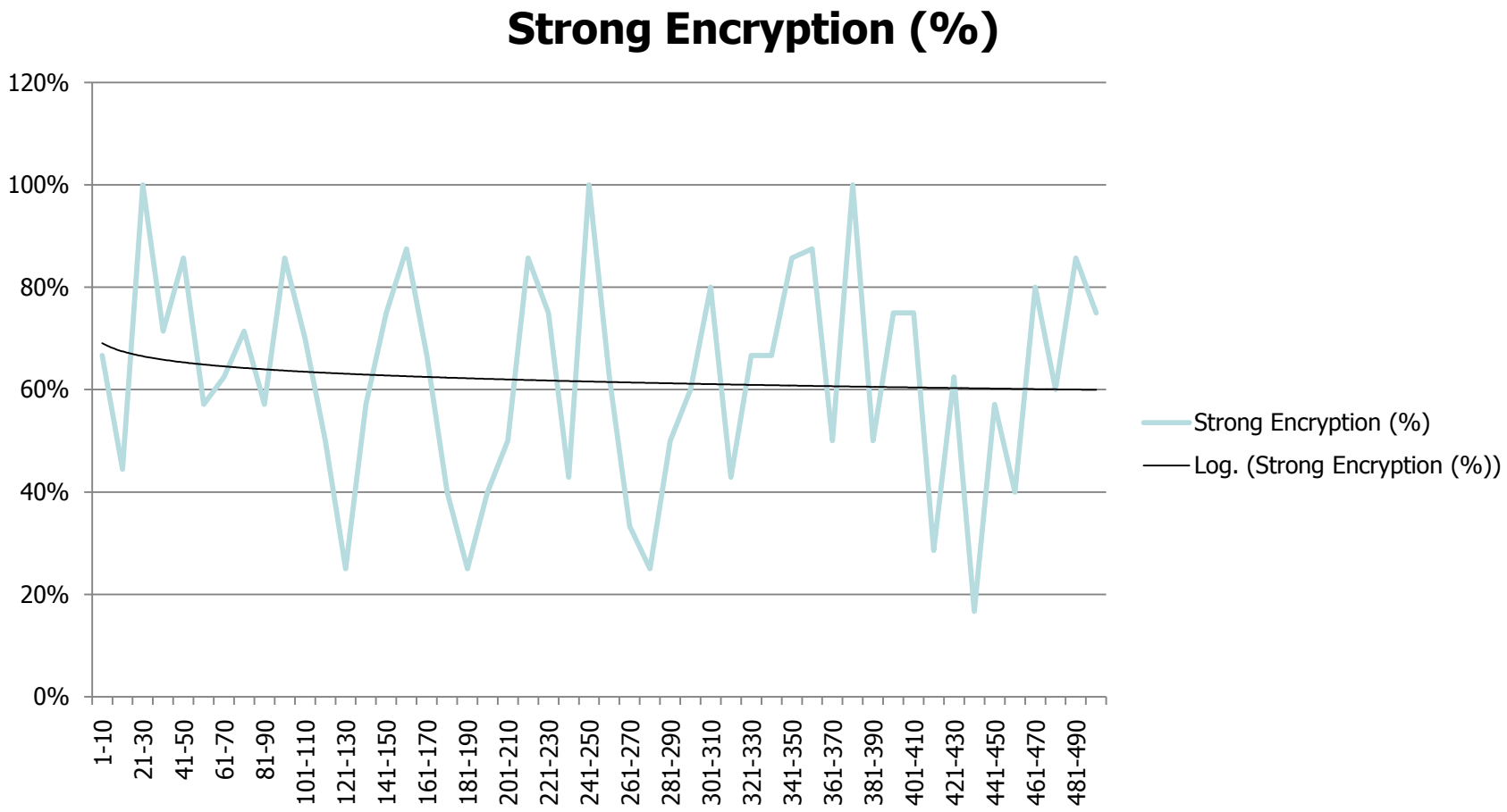

Medium Encryption (%)
120%
100%
80%
60%
40%
20%
0%
1-10
21-30
41-50
61-70
81-90
101-110
121-130
141-150
161-170
181-190
201-210
221-230
241-250
261-270
281-290
301-310
321-330
341-350
361-370
381-390
401-410
421-430
441-450
461-470
481-490
Medium Encryption (%)
Log. (Medium Encryption (%))

Alexa 10k

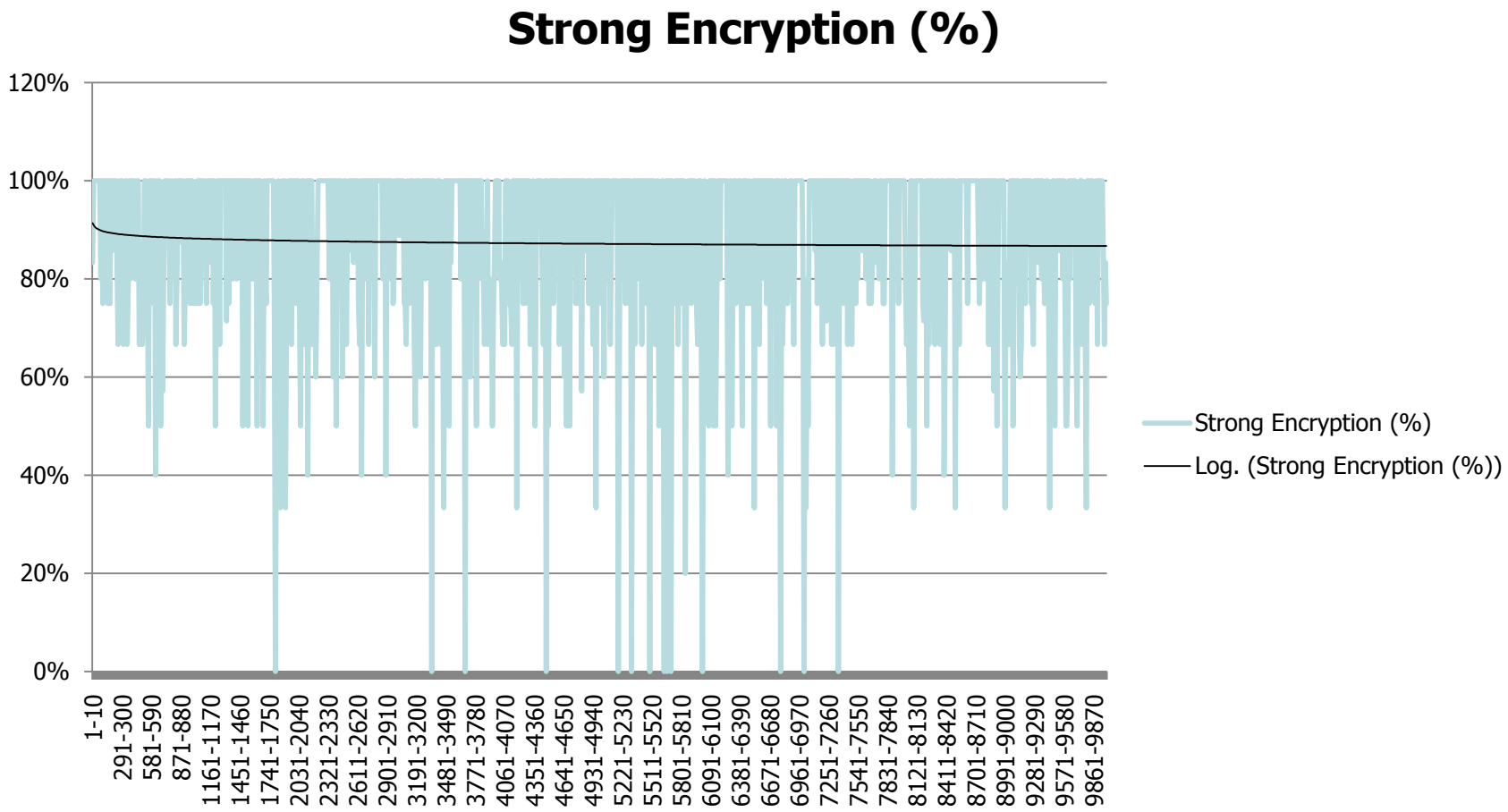

Medium Encryption (%)
120%
100%
80%
60%
40%
20%
0%
1-10
301-310
601-610
901-910
1201-1210
1501-1510
1801-1810
2101-2110
2401-2410
2701-2710
3001-3010
3301-3310
3601-3610
3901-3910
4201-4210
4501-4510
4801-4810
5101-5110
5401-5410
5701-5710
6001-6010
6301-6310
6601-6610
6901-6910
7201-7210
7501-7510
7801-7810
8101-8110
8401-8410
8701-8710
9001-9010
9301-9310
9601-9610
9901-9910
Medium Encryption (%)
Log. (Medium Encryption (%))

STRONG ENCRYPTION (>=256 BIT KEY)

Fortune 500

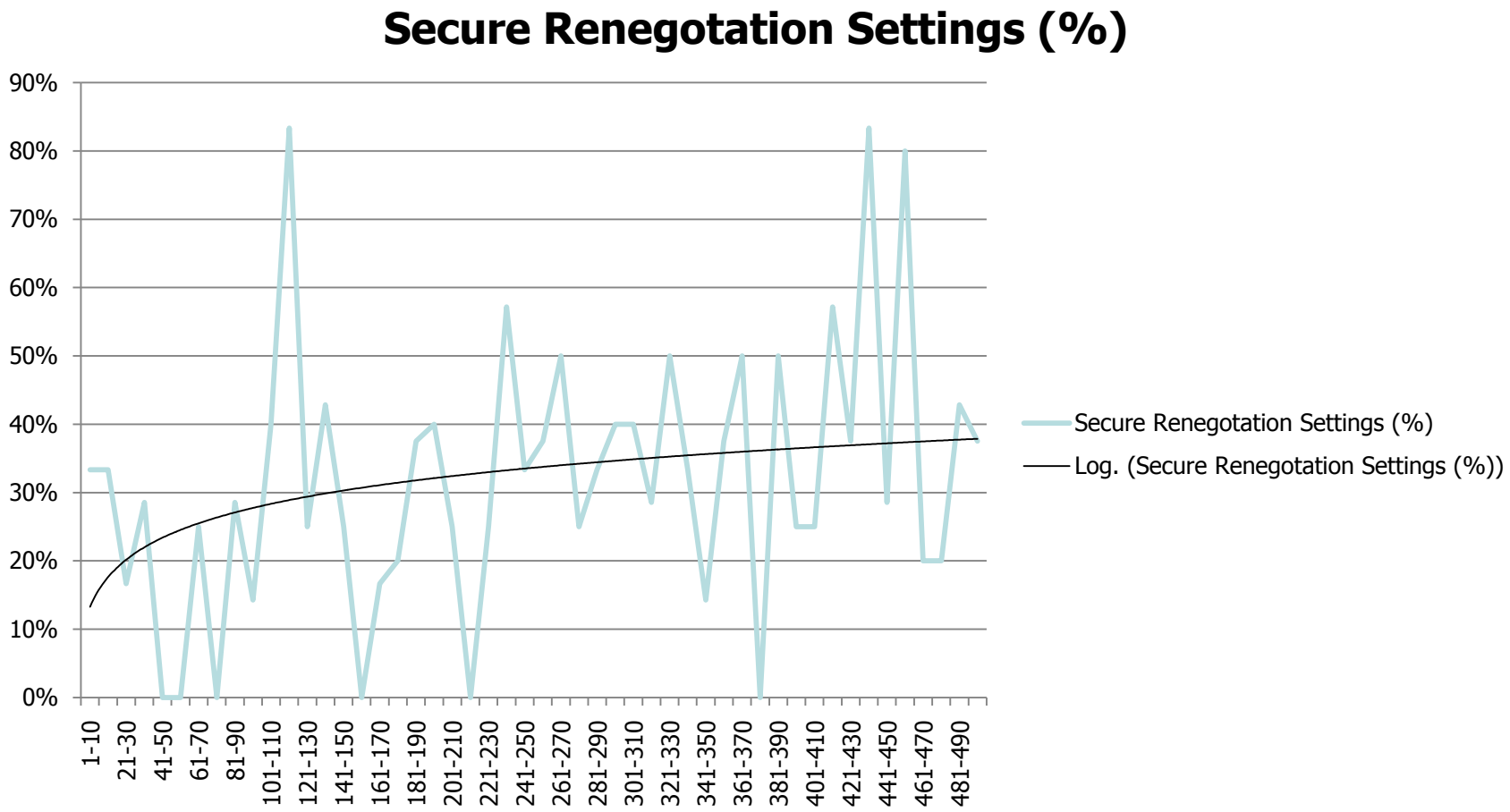

Strong Encryption (%)
120%
100%
80%
60%
40%
20%
0%
1-10
21-30
41-50
61-70
81-90
101-110
121-130
141-150
161-170
181-190
201-210
221-230
241-250
261-270
281-290
301-310
321-330
341-350
361-370
381-390
401-410
421-430
441-450
461-470
481-490
Strong Encryption (%)
Log. (Strong Encryption (%))

Alexa 10k

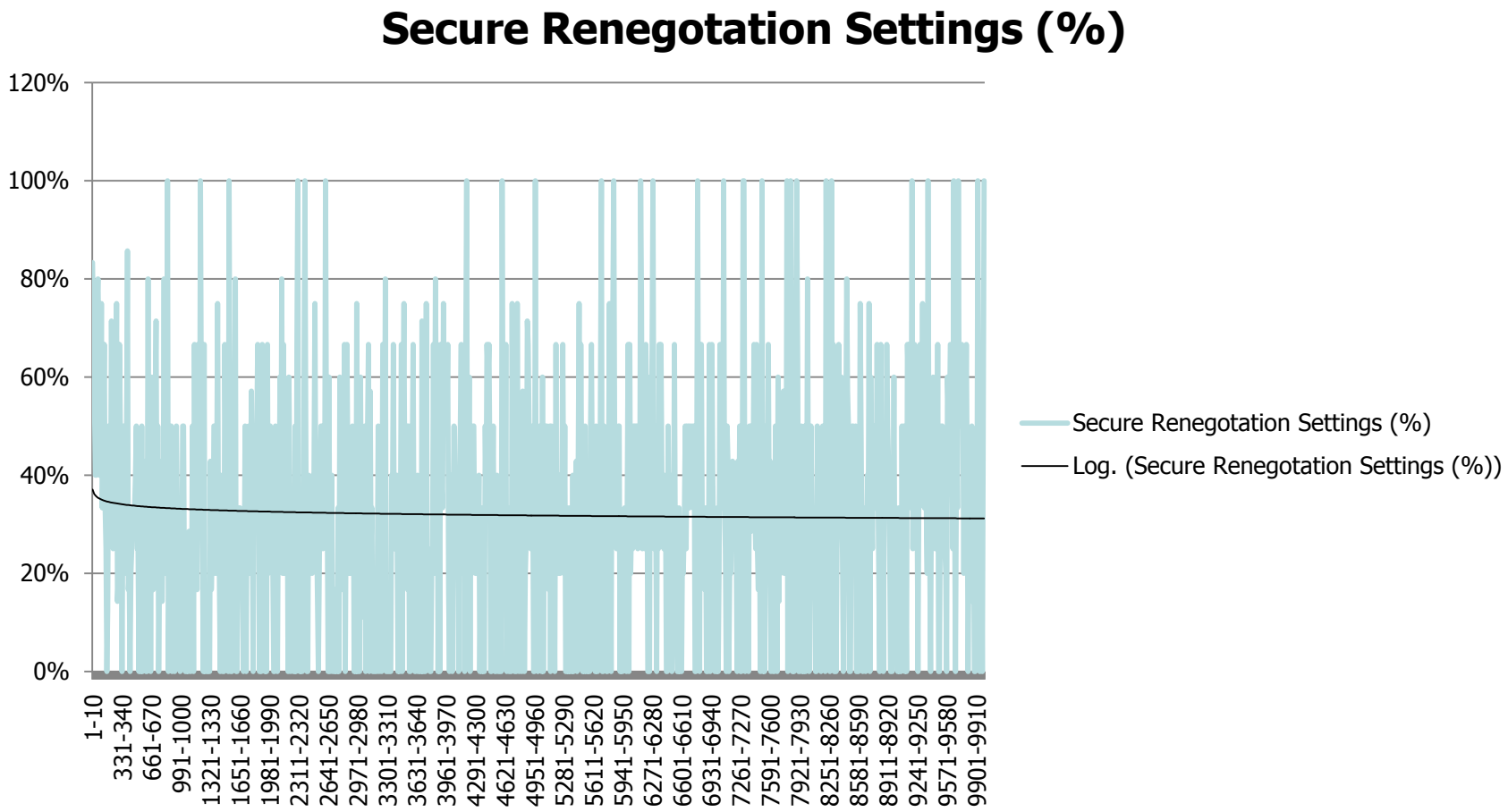

Strong Encryption (%)
120%
100%
80%
60%
40%
20%
0%
1-10
291-300
581-590
871-880
1161-1170
1451-1460
1741-1750
2031-2040
2321-2330
2611-2620
2901-2910
3191-3200
3481-3490
3771-3780
4061-4070
4351-4360
4641-4650
4931-4940
5221-5230
5511-5520
5801-5810
6091-6100
6381-6390
6671-6680
6961-6970
7251-7260
7541-7550
7831-7840
8121-8130
8411-8420
8701-8710
8991-9000
9281-9290
9571-9580
9861-9870
Strong Encryption (%)
Log. (Strong Encryption (%))

SESSION RENEGOTIATION

Fortune 500


Secure Renegotation Settings (%)
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
1-10
21-30
41-50
61-70
81-90
101-110
121-130
141-150
161-170
181-190
201-210
221-230
241-250
261-270
281-290
301-310
321-330
341-350
361-370
381-390
401-410
421-430
441-450
461-470
481-490
Secure Renegotation Settings (%)
Log. (Secure Renegotation Settings (%))

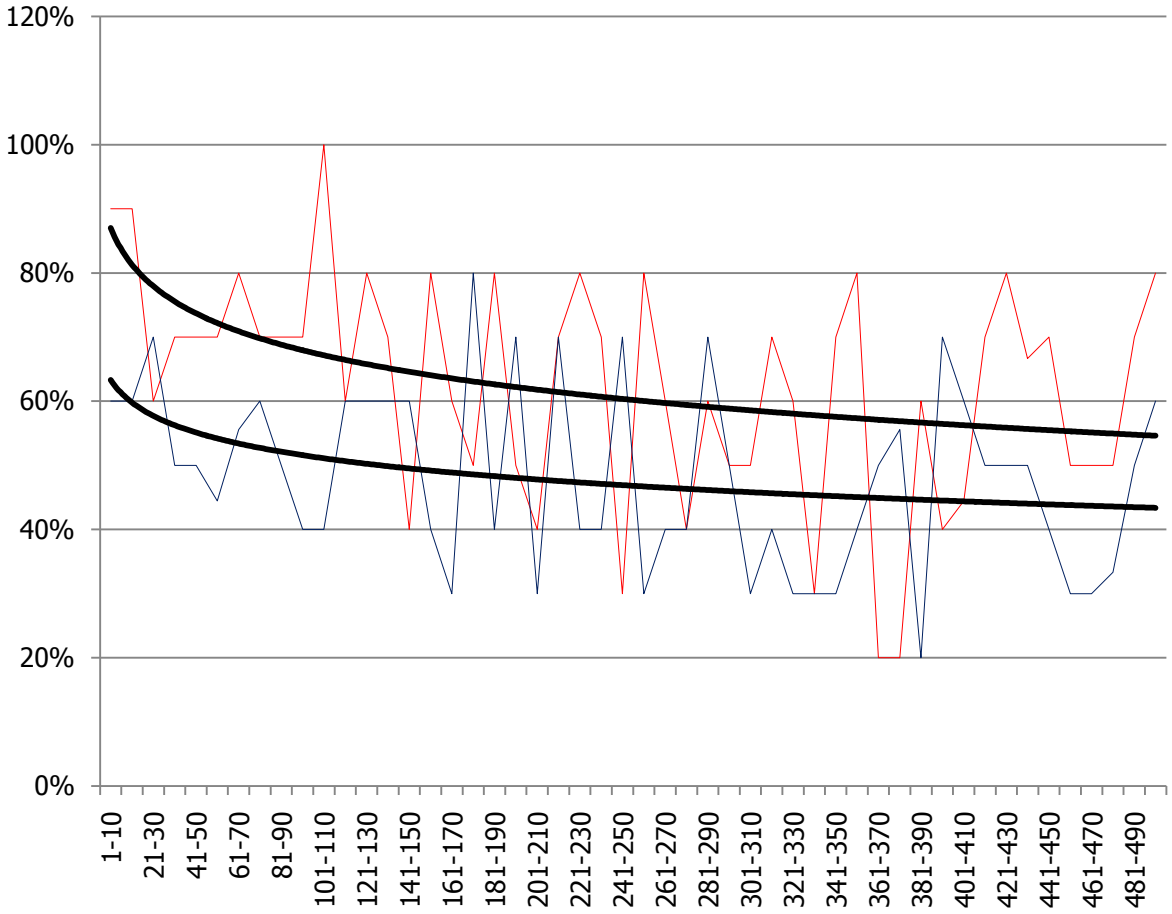
Alexa 10k

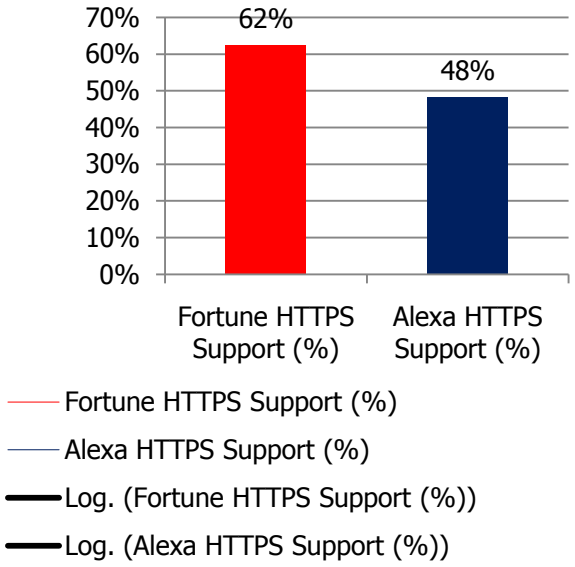

Secure Renegotation Settings (%)
120%
100%
80%
60%
40%
20%
0%
1-10
331-340
661-670
991-1000
1321-1330
1651-1660
1981-1990
2311-2320
2641-2650
2971-2980
3301-3310
3631-3640
3961-3970
4291-4300
4621-4630
4951-4960
5281-5290
5611-5620
5941-5950
6271-6280
6601-6610
6931-6940
7261-7270
7591-7600
7921-7930
8251-8260
8581-8590
8911-8920
9241-9250
9571-9580
9901-9910
Secure Renegotation Settings (%)
Log. (Secure Renegotation Settings (%))

16 Organizations are on both lists

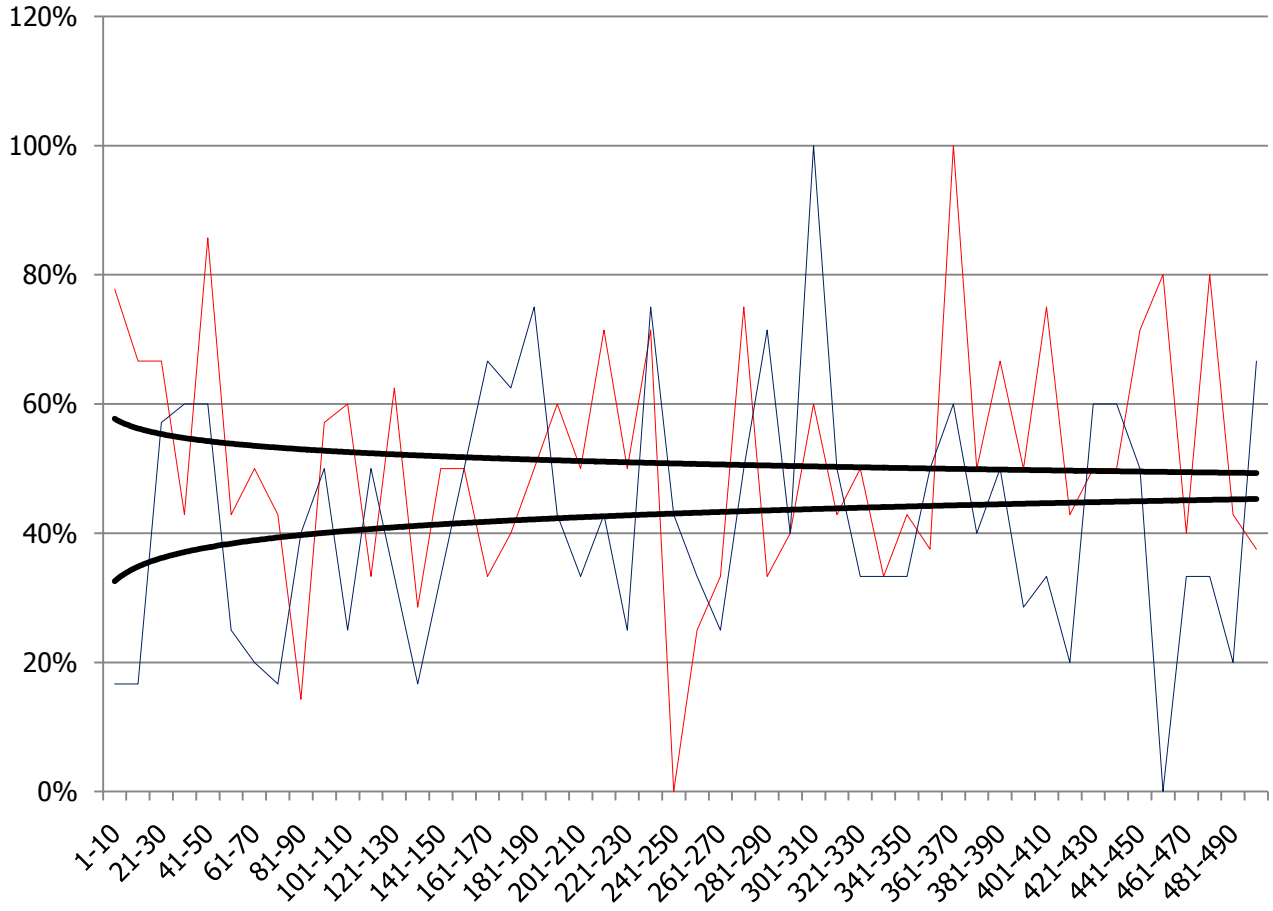
FORTUNE 500 VS ALEXA 500

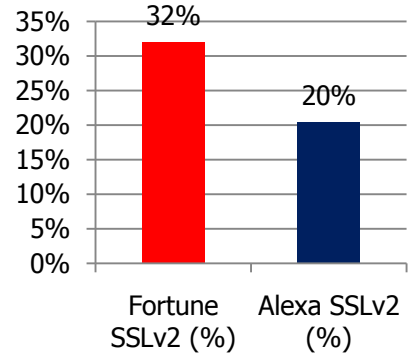
Money vs. Popularity: HTTPS enabled?

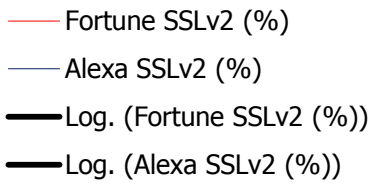




Money vs. Popularity: SSLv2 enabled? (= bad)

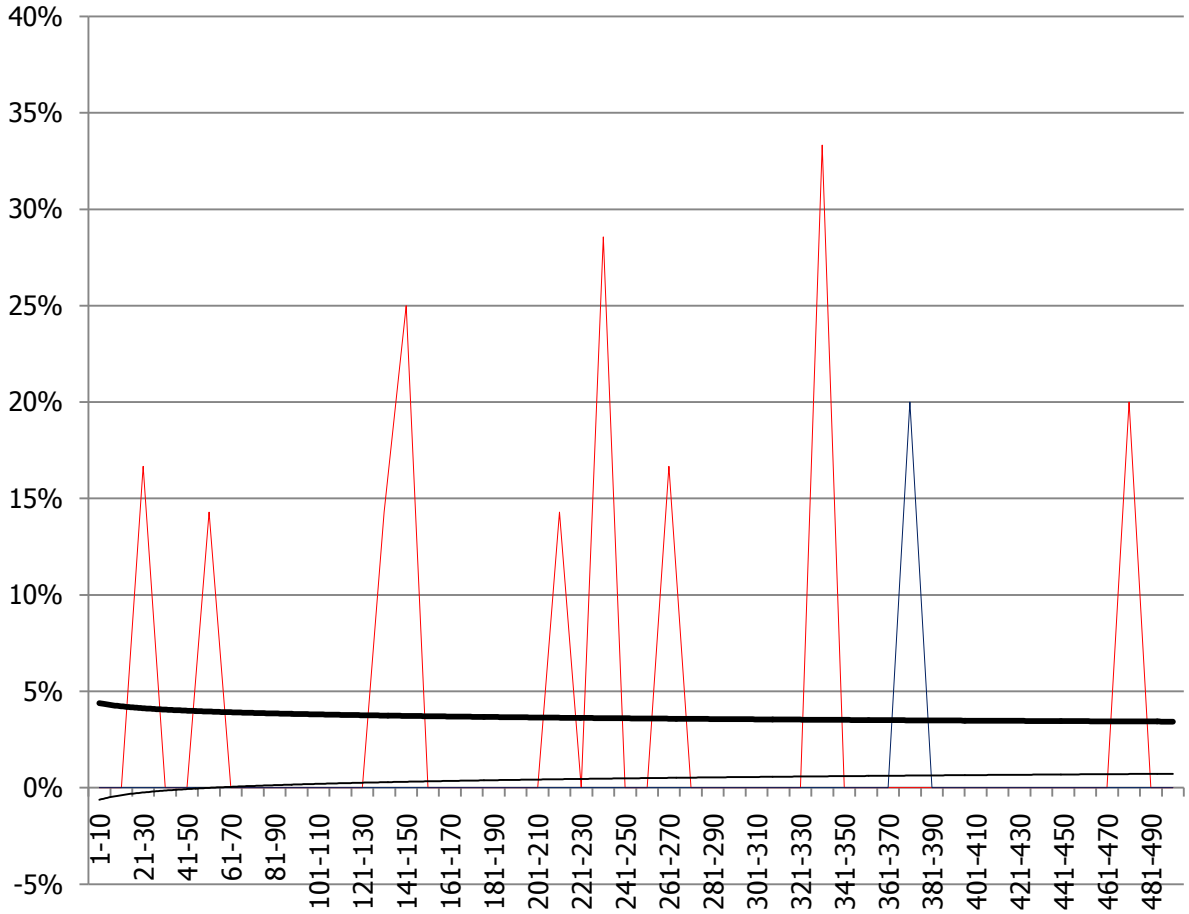


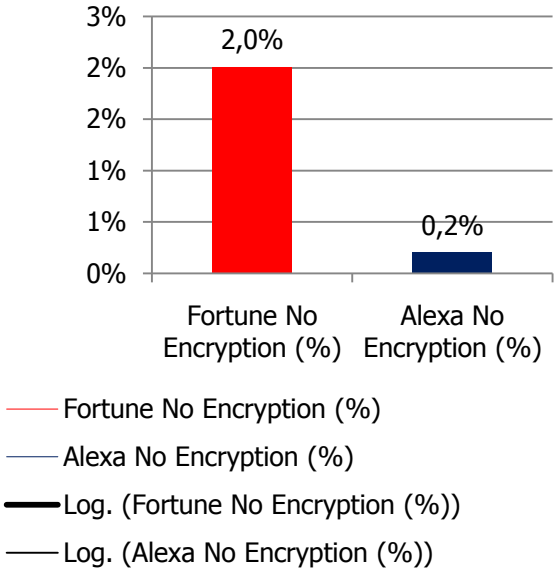




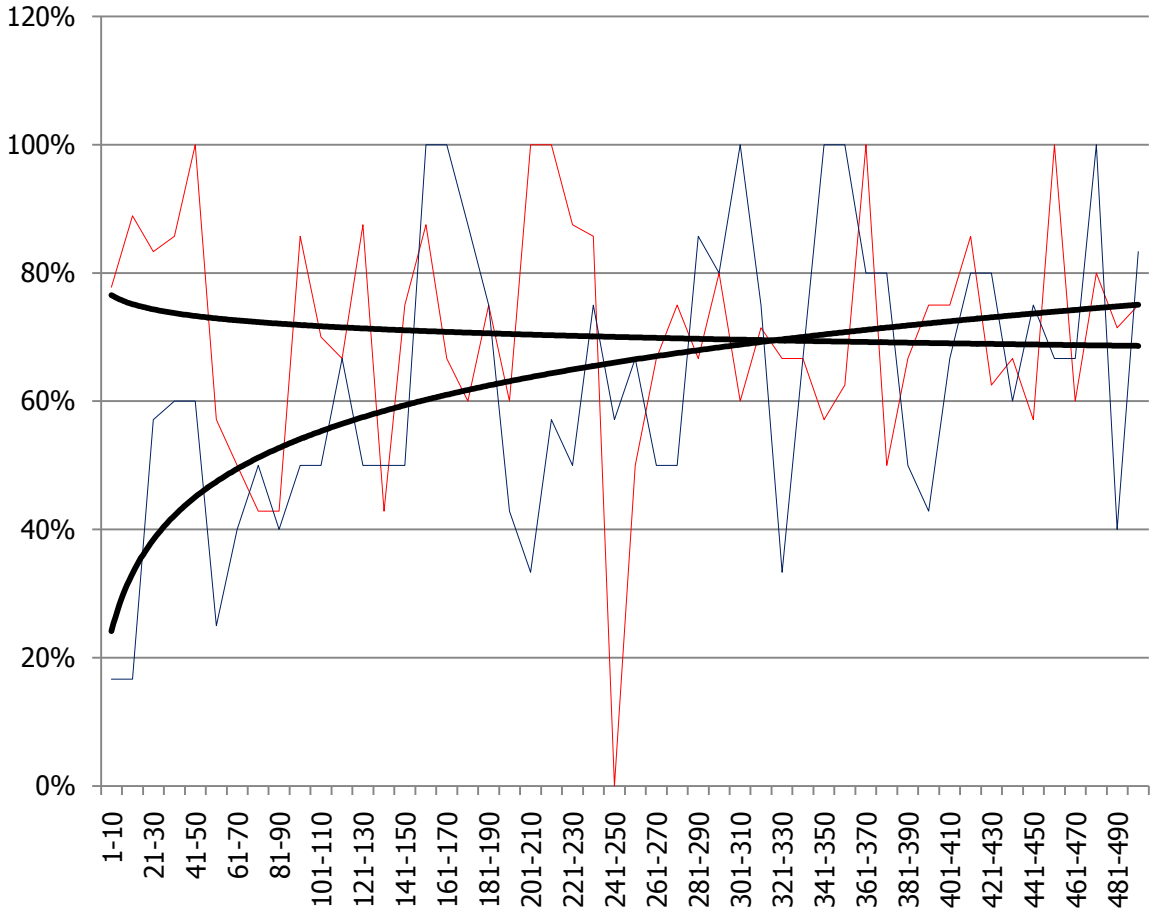
OWASP

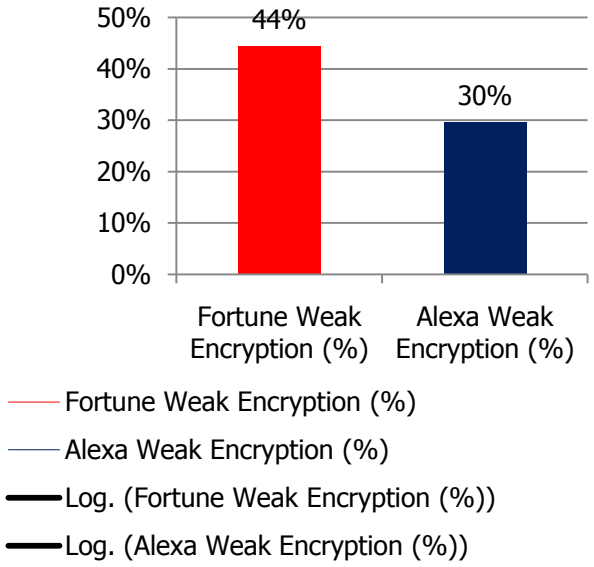
Money vs. Popularity:
0-bit keys being enabled?(=bad)



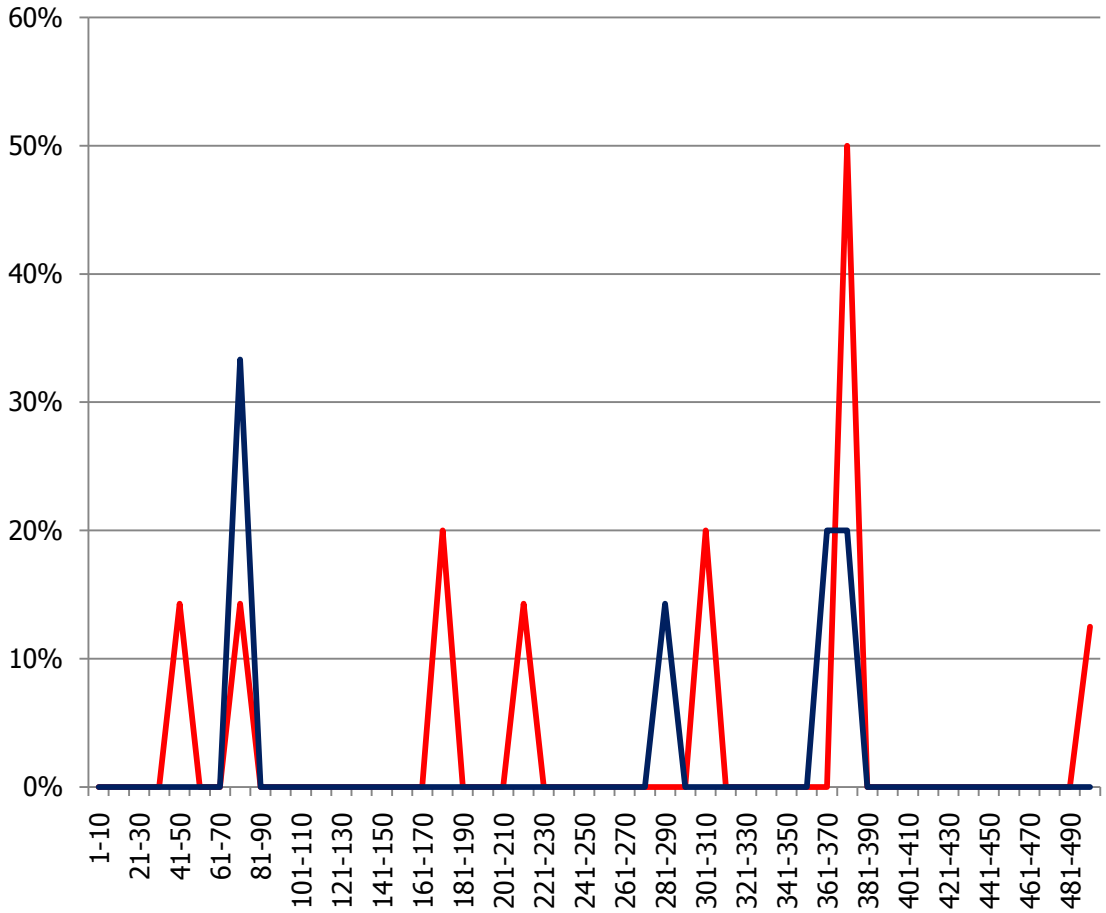


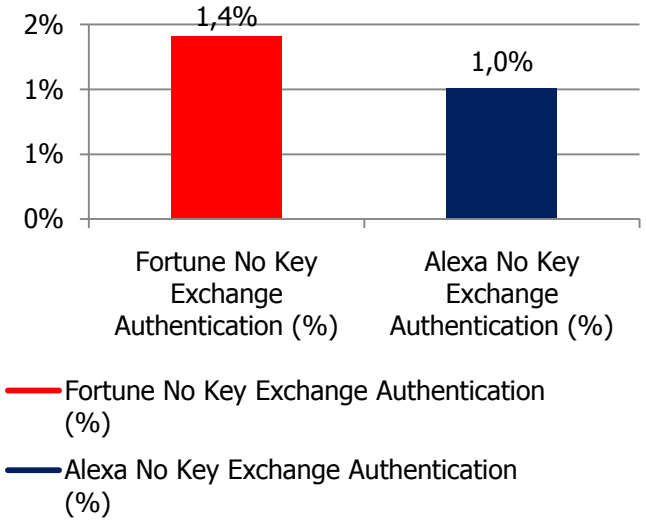
Money vs. Popularity: Weak keys being enabled?(=bad)



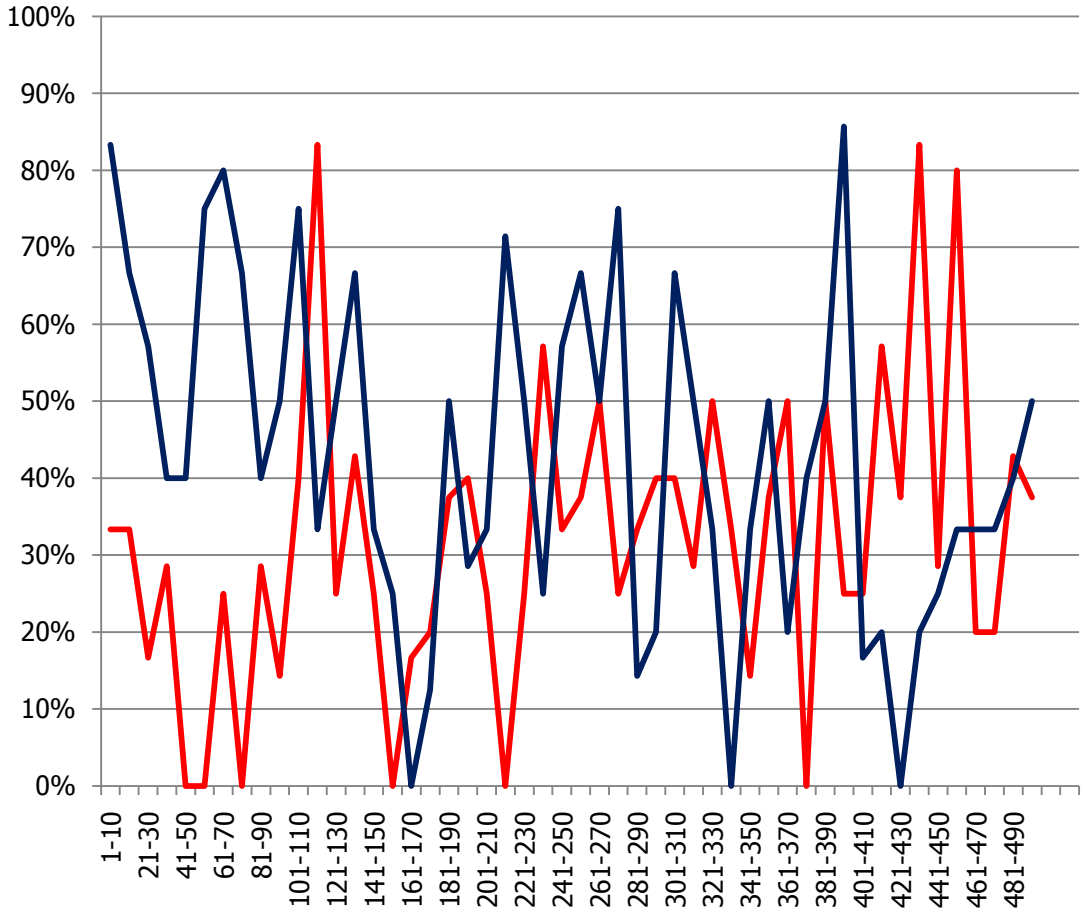


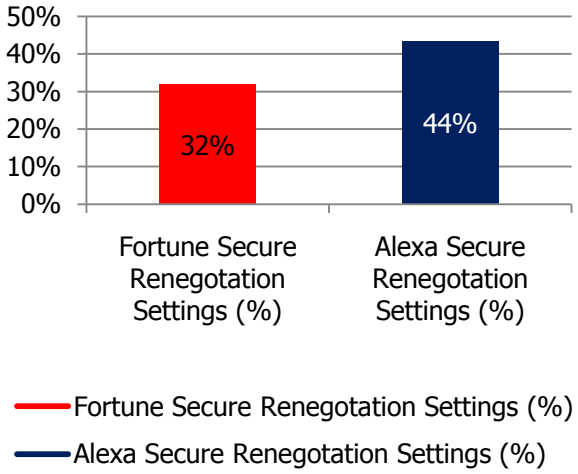
Money vs. Popularity: No auth kx being enabled?(=bad)



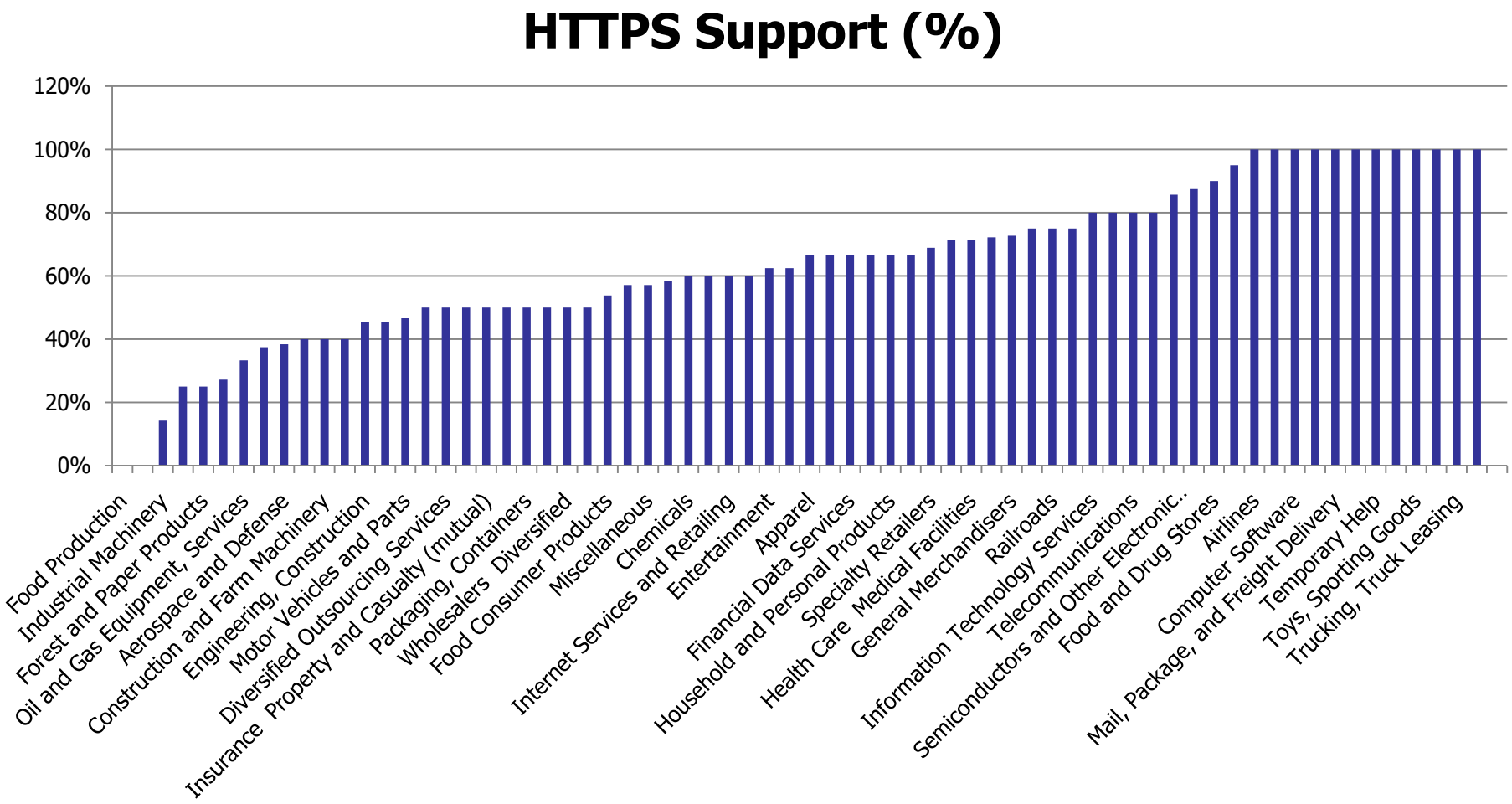


Money vs. Popularity: Secure Session Renegotation?

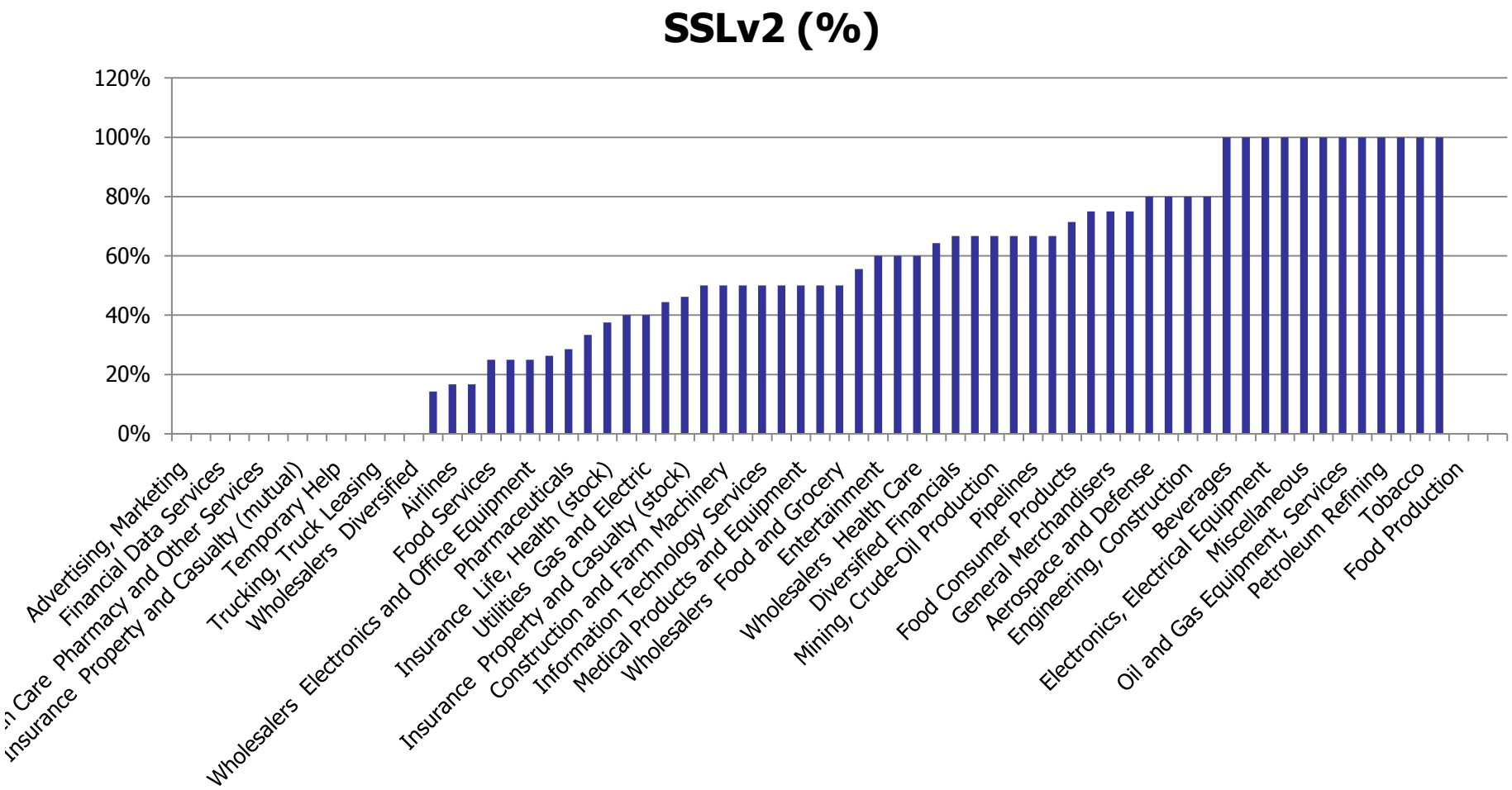




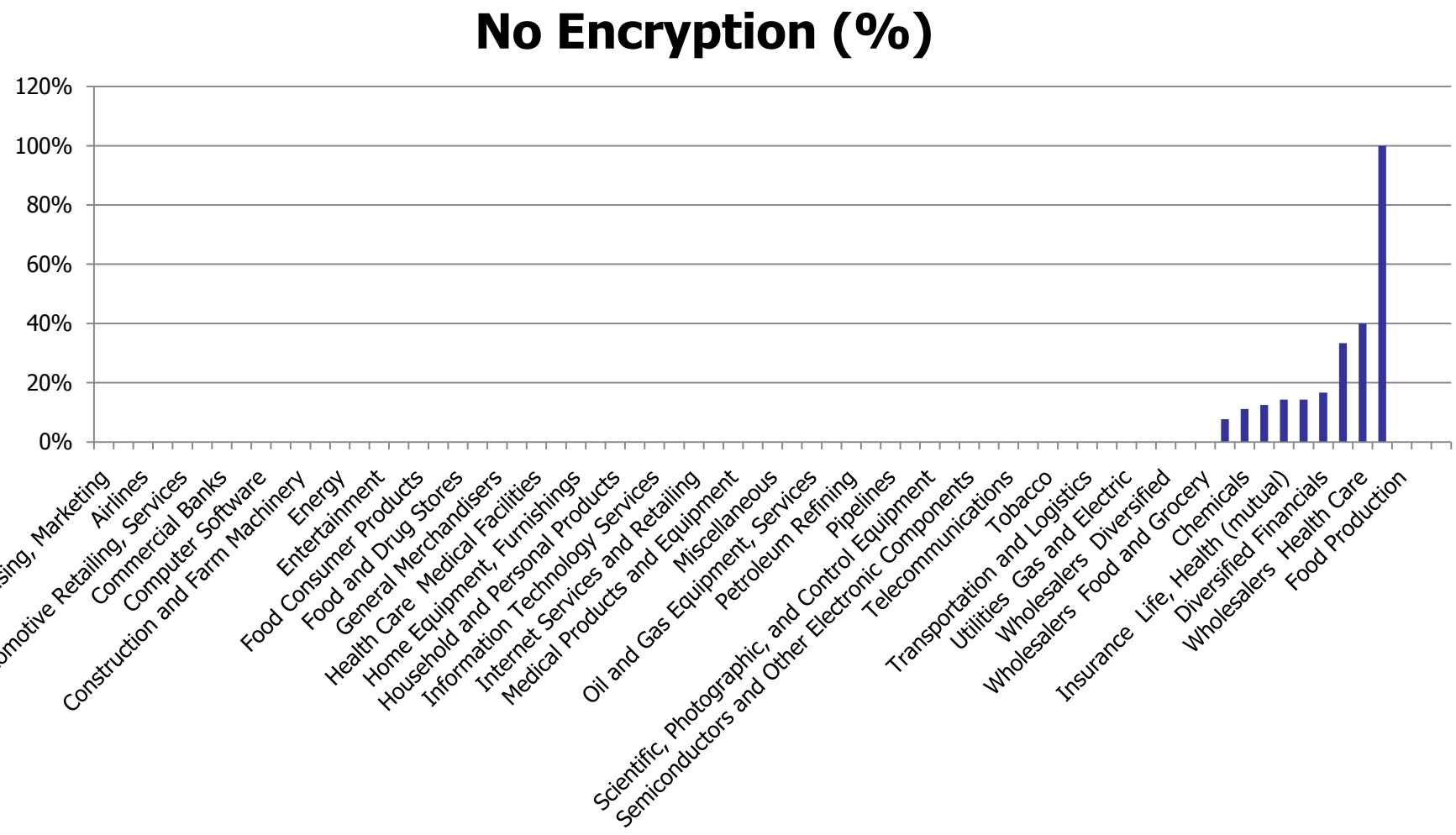
Fortune 500 Industries



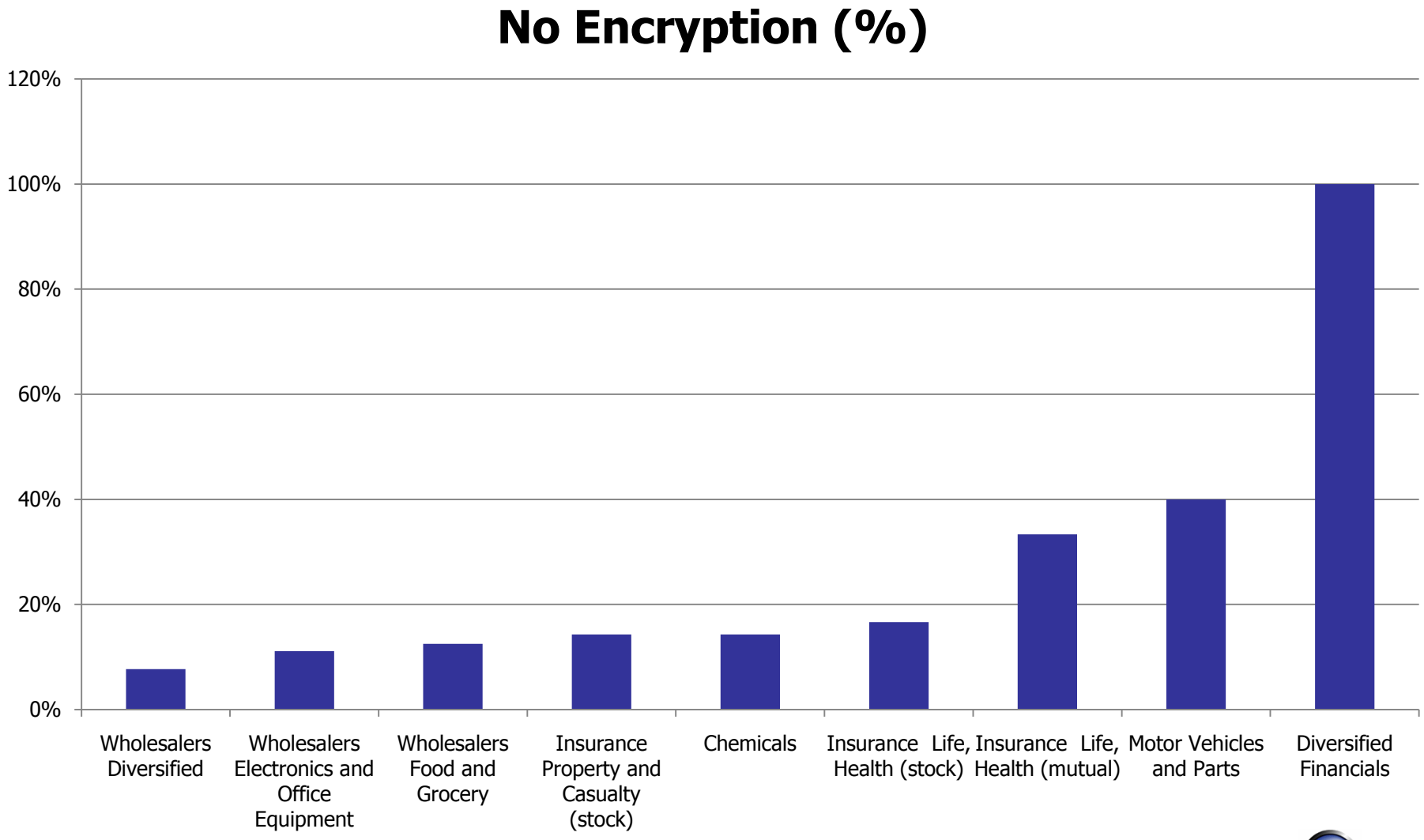
Fortune 500 Industries



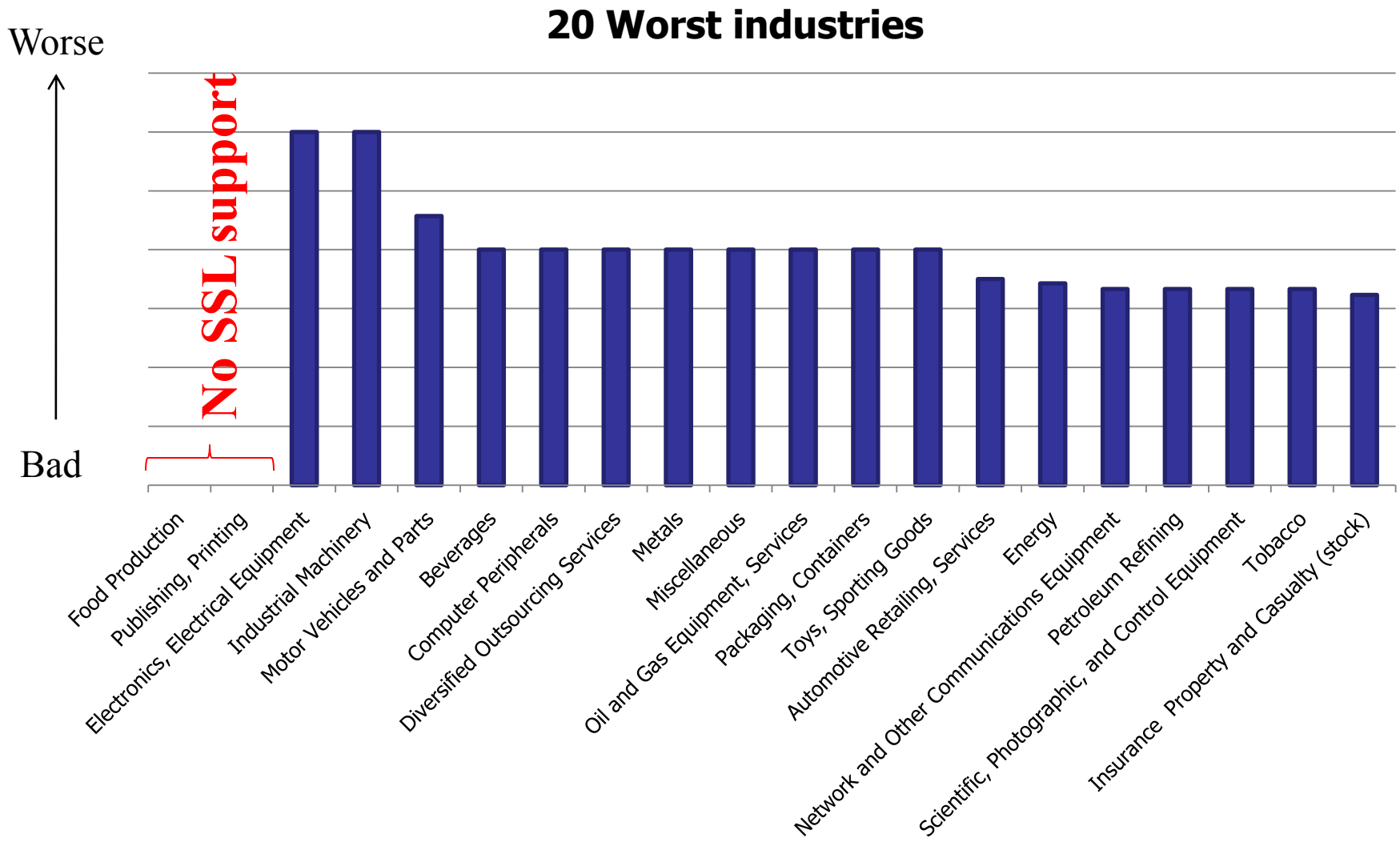
Fortune 500 Industries



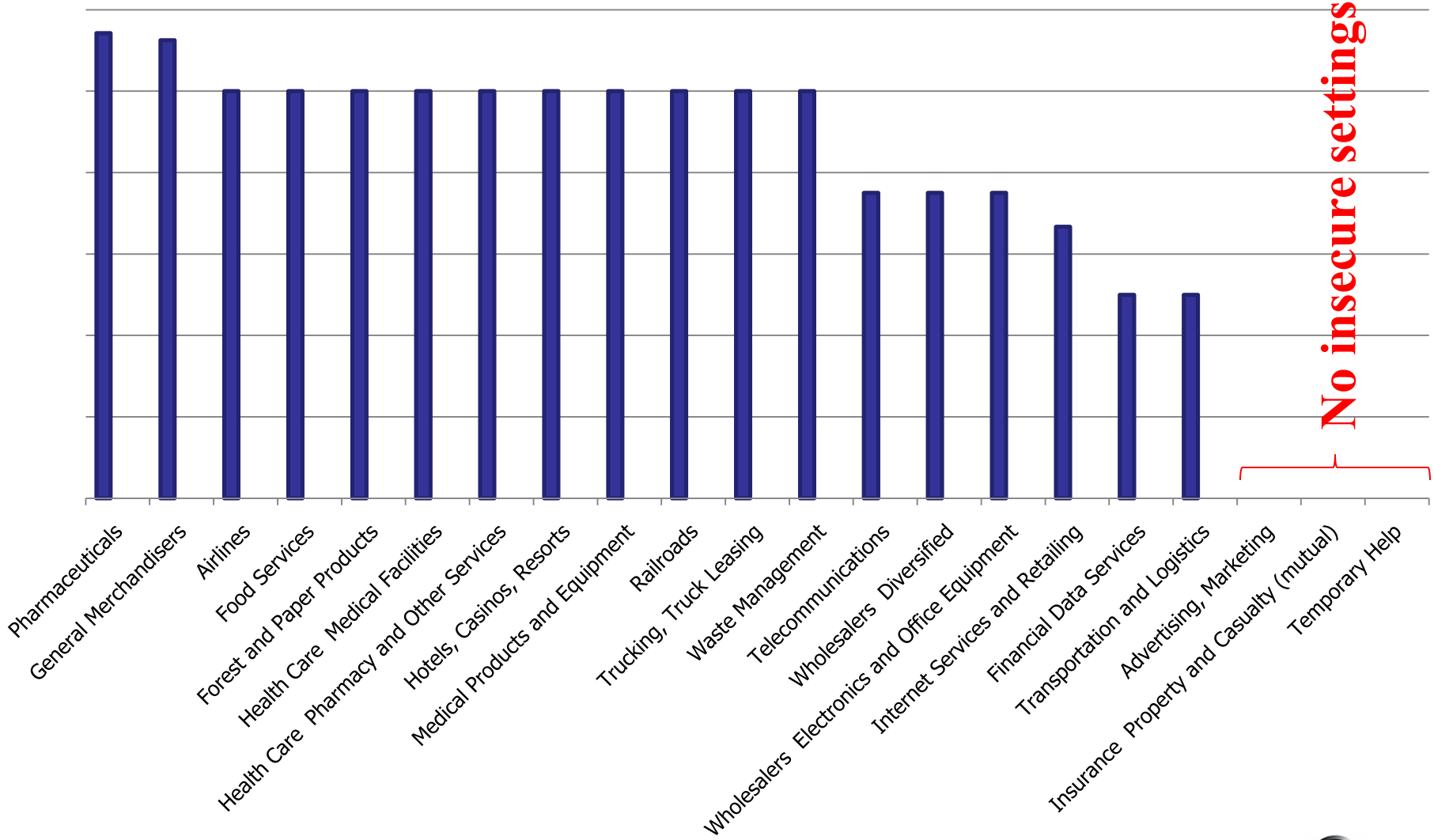
Fortune 500 Industries



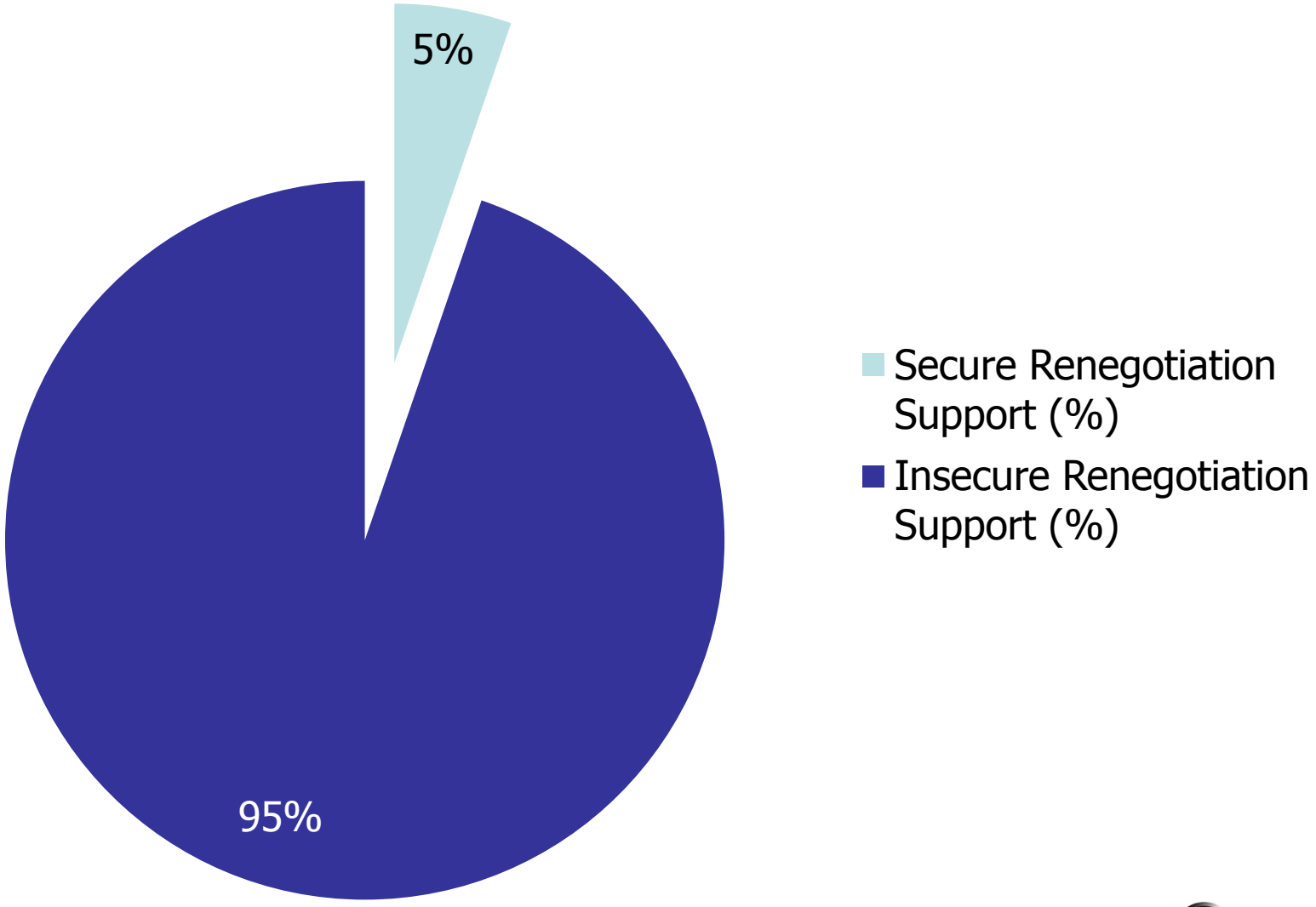
Fortune 500 Industries



Fortune 500 Industries



Commercial Banks



Conclusion

- What the data told me is that
  - Money (Fortune) seems to have something to do with HTTPS being enabled
  - Popularity (Alexa) seems to be they key to enable HTTPS securely
  - There is no obvious real trend in what kind of industry a company is in and their HTTPS security settings, but it seems more likely the company is doing business over the webb the more likely they offer HTTPS on their website

What's next?

- Deeper investigation into the Swedish market in co-operation with .SE (The Internet Infrastructure Foundation – the guys responsible for .SE TLD)

Questions and Answers

- Research website:
  - http://sslresearch.michaelboman.org
    - Raw data, documentation, scripts and tools
- Contact information:
  - owasp2010@michaelboman.org
  - www.michaelboman.org
- References:
  - http://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001)