Michal Wozniak 21941097
Sebastian Proctor-Shah 29649727

WEB QUERIES STATISTIC

BASIC STASTISTIC

INFORMATION	VALUE
# TIMEOUT	4014
# unknownHost	923
# total error (timeout+unknownHost)	4937
# use HTTPS	7323
# HTTPS not supported	8740

SSL VERSION STATISTIC

# TLSV1.2	5988
# TLSv1.1	33
# TLSv1.0	1302

RESPECTION OF MINIMUM KEY SIZE FOR KEY TYPE

# RSA KEY RESPECTED (>= 1024)	6833
# RSA KEY NOT RESPECTED MIN	0
# EC KEY RESPECTED (>= 256)	490
# EC KEY NOT RESPECTED MIN	0

SIGNATURE- ALGORITHM

# SHA1	1054
# SHA256	6269
# PERCENT OF SHA1 ON TOTAL OF HTTPS	14.40%
# PERCENT OF SHA256 ON TOTAL OF HTTPS	85.60%

STRICT-TRANSPORT-SECURITY STATISTIC

# Strict-transport-security supported	352
# strict-transport-security not supported	3983
Percentage strict-security supported	8.84%
# HTTPS WITH HSTS > 1 MONTH	295
# HTTPS WITH HSTS < 1 MONTH	57

HTTPS SUPPORT

# HTTPS SUPPORTED *	45.59%
# HTTPS NOT SUPPORTED*	54.41%

*we ignored the unknown host and timeout connection in our calculation

All statistic values were provided by excel equations using the csv file

RESULTS

For my queries, I used a 2 second time out. Usually if you are browsing the internet and it take you more than 2 second to get to a webpage then you aren't satisfied with your experience. I wanted to try with a smaller one to save time but I realized after some testing that I was getting too many time out.

The statistic showed us that more than 54.41% of our queried websites aren't even using HTTPS. Out of the one are supporting https, 14.4% of them are using a hash function that is currently being deprecated (SHA1). Therefore we have even less website that using optional security parameters.

The only thing that is good is that they are all using the minimum required size key for their key type. The most used algorithm is sha256 with 86.6%. We didn't detect any other algorithm beside SHA1 and SHA256. The Strict-Transport-Security header isn't used a lot in https connection with only 8.84% using them.