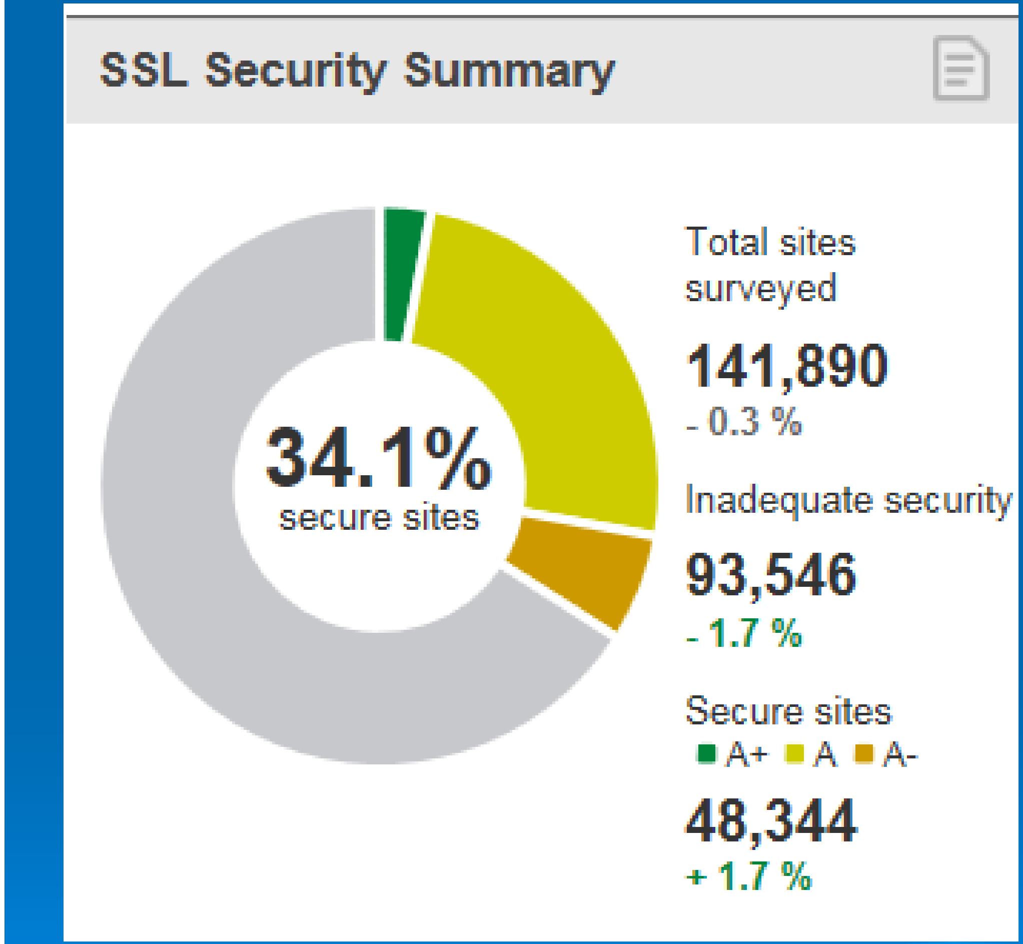
TLS vulnerabilities

- **Heartbleed** (CVE-2014-0160)
- **CCS** (CVE-2014-0224)
- Secure Renegociation (CVE-2009-3555)
- Secure Client-Initiated Renegociation
- **CRIME** (CVE-2012-4929)
- BREACH (CVE-2013-3587)
- **POODLE** (CVE-2014-3566)
- TLS_FALLBACK_SCSV (RFC 7507)
- **FREAK** (CVE-2015-0204)
- **LOGJAM** (CVE-2015-4000)
- **BEAST** (CVE-2011-3389)
- **RC4** (CVE-2013-2566, CVE-2015-2808)

Source: TestSSL- **https://testssl.sh//**

Statistics



SSL Security Summary

Total sites surveyed

141,890

- 0.3 %

Inadequate security

93,546

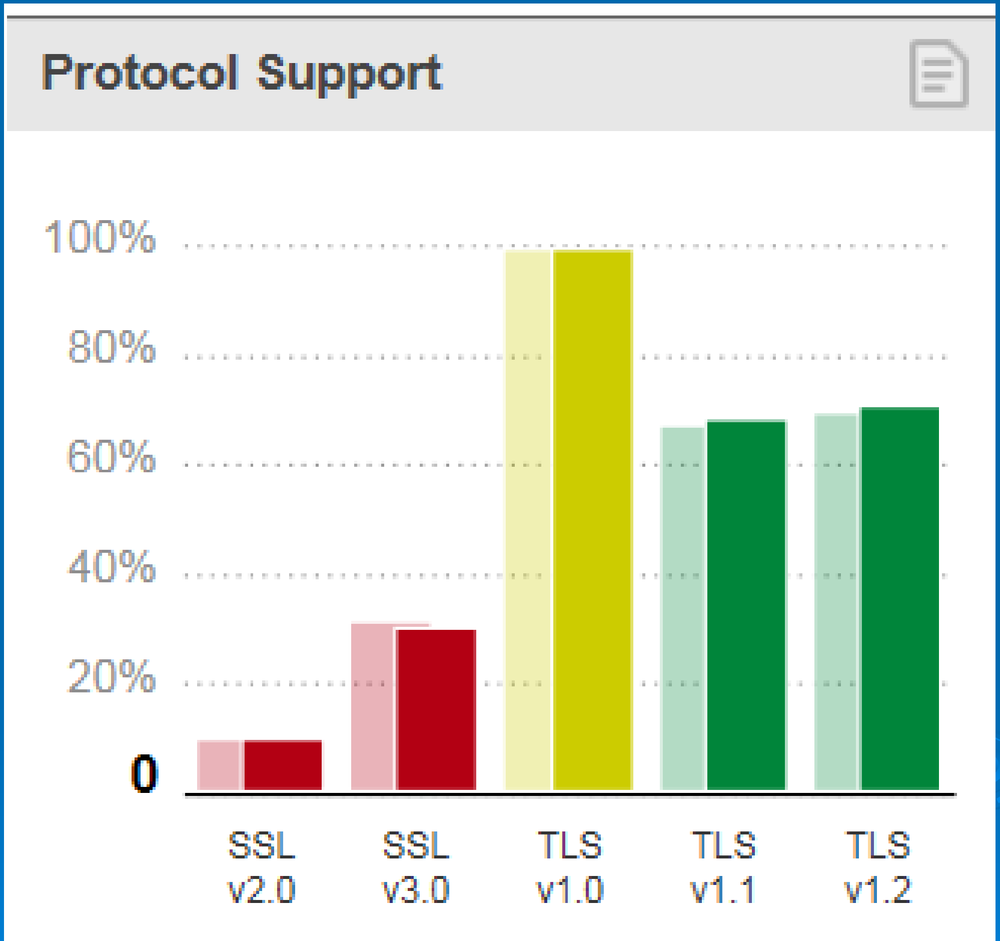
- 1.7 %

Secure sites

🟩 A+ 🟨 A 🟧 A-

48,344

+ 1.7 %



Protocol Support

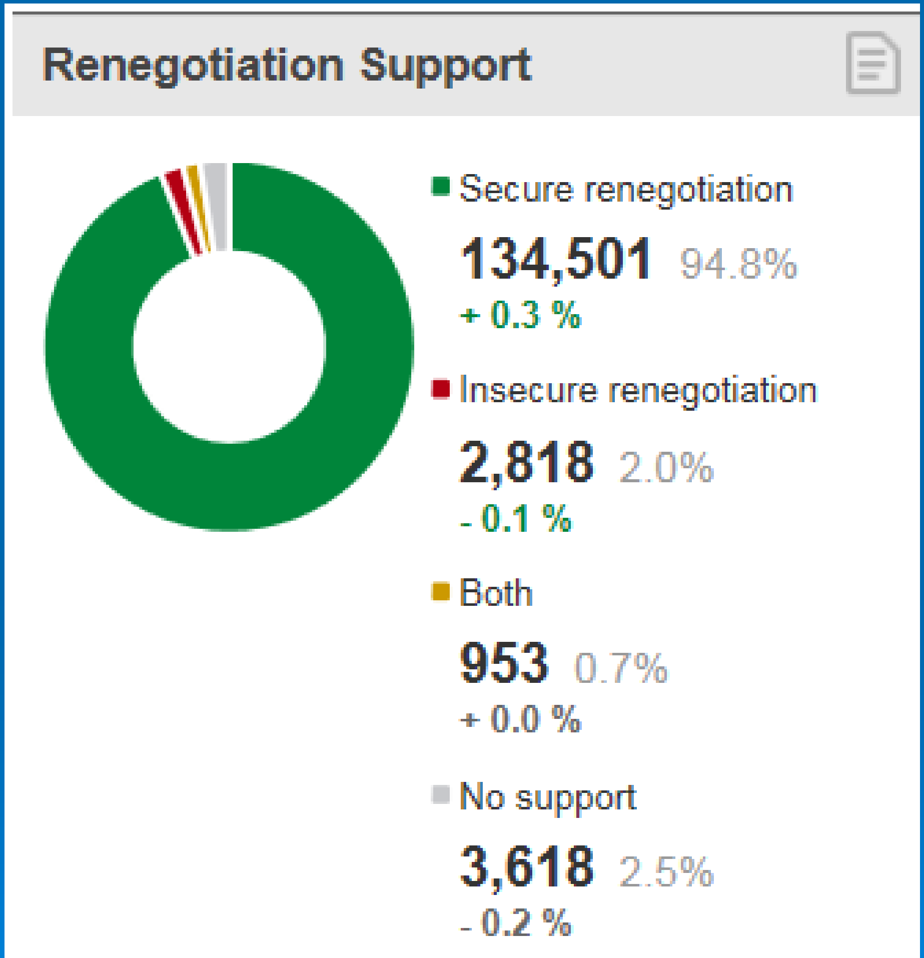
Source: SSL Pulse- **https://www.trustworthyinternet.org/ssl-pulse/**

2009 – SSL Renegotiation

- Vulnerability in block ciphers that use CBC mode
- Allow an **attacker who can highjack an HTTPS connection (MITM)** to inject plaintext into the victim's requests
- The attacker cannot decrypt the client-server communication

Source: SSL Attacks - **http://resources.infosecinstitute.com/ssl-attacks/**

2009 – SSL Renegociation statistics



Renegotiation Support

🟩 Secure renegotiation
134,501 94.8%
+ 0.3 %

🟥 Insecure renegotiation
2,818 2.0%
- 0.1 %

🟨 Both
953 0.7%
+ 0.0 %

⬜ No support
3,618 2.5%
- 0.2 %

Source: SSL Pulse- **https://www.trustworthyinternet.org/ssl-pulse/**

2011 - BEAST

- Vulnerability in block ciphers that use CBC mode: IV used for 1st block and then the ciphertext is used as IV
- Allow an **attacker who can highjack an HTTPS connection (MITM)** to guess the plaintext having the IV and check the ciphertext matches

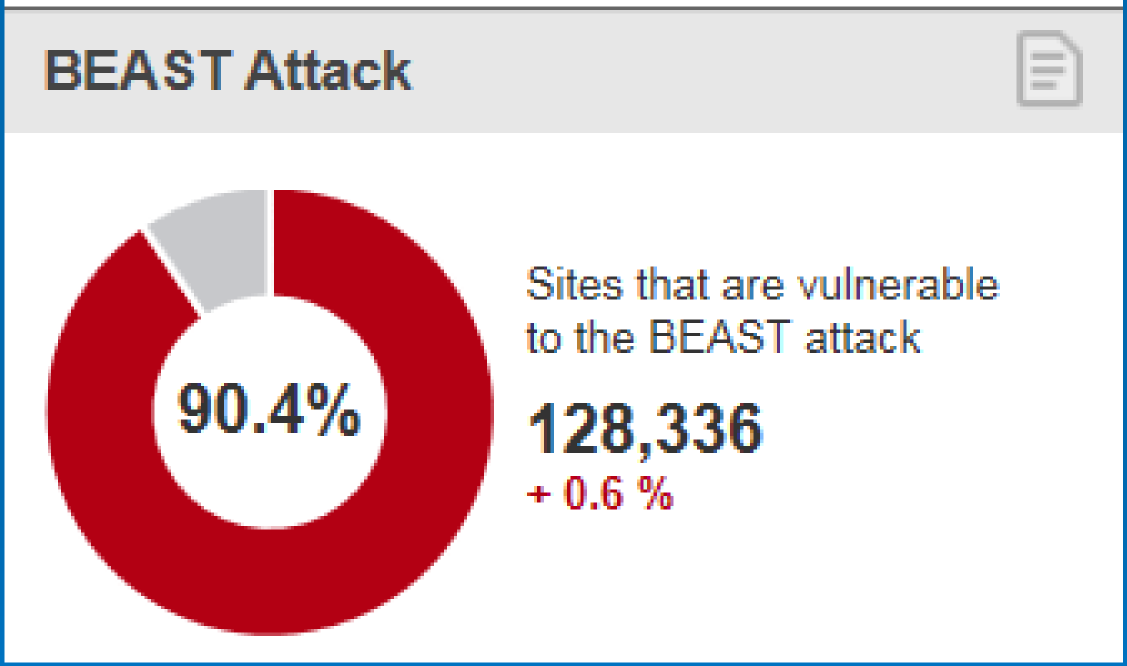
Browser Exploit Against SSL/TLS

- Javascript malware downloaded from an attacker controlled web site
- Send HTTPS requests to the victim web server
- For new SSL connections the attacker can enforce the termination of the SSL session
- Require the same key is used in all encryptions

They said: “Use RC4 to mitigate BEAST attack”

Source: NakedSecurity - **http://nakedsecurity.sophos.com/**

2011 – BEAST statistics



BEAST Attack

90.4%

Sites that are vulnerable to the BEAST attack

128,336

+ 0.6 %

Source: SSL Pulse- **https://www.trustworthyinternet.org/ssl-pulse/**

2012 - CRIME

Compression Ratio Info-leak Made Easy: information leakage resulting from the HTTP request compression usage to defeat SSL's encryption (GZIP combining LZ77: replaces repeated occurrences by a single copy, and Huffman coding)

Control is needed: compression data leaks for known input data (that contains a given character) or for chosen input data (where we added the given character)

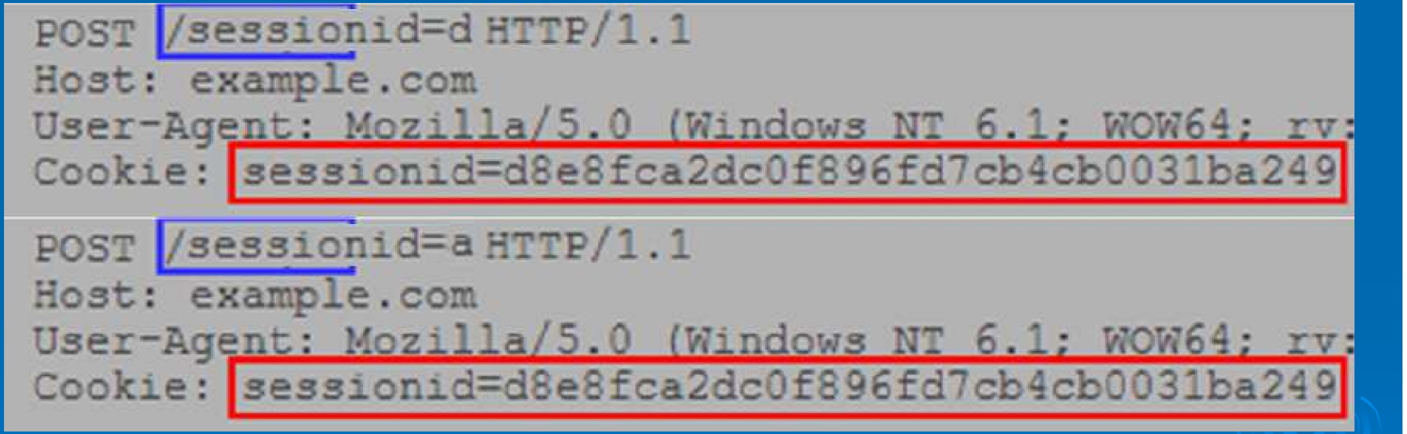
Disable TLS 1.0 compression to avoid CRIME attack

Source: A perfect crime - **https://media.blackhat.com/eu-13/briefings/Beery/bh-eu-13-a-perfect-crime-beery-wp.pdf/**

2012 - CRIME

- CRIME Javascript makes requests to the target server: e.g. to guess the sessionId character by character
- HTTP request compression infoleak:

Attacker makes a guess and can see encrypted packet lengths (if size is reduced then guess ok)



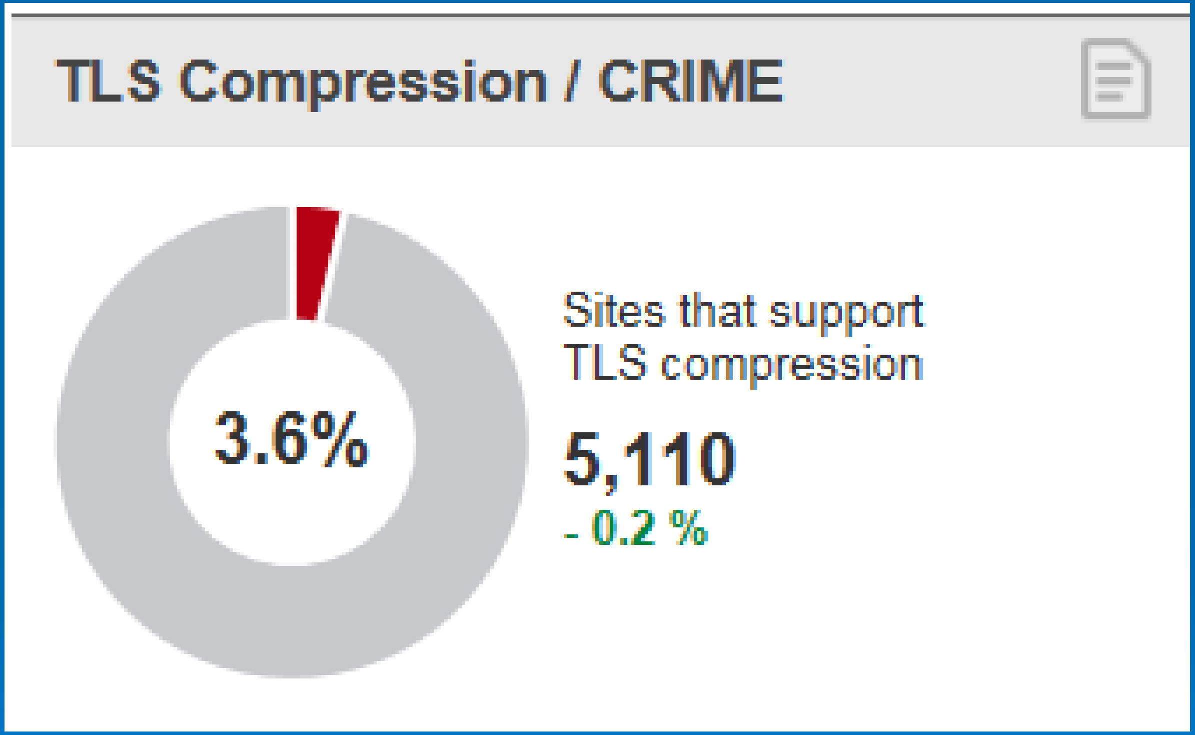
```
POST /sessionid=d HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:
Cookie: sessionid=d8e8fca2dc0f896fd7cb4cb0031ba249
POST /sessionid=a HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:
Cookie: sessionid=d8e8fca2dc0f896fd7cb4cb0031ba249
```

- Time attack (TIME)
- HTTP response compression infoleak:

- **BREACH (2013)** is based on CRIME

Source: A perfect crime - **https://media.blackhat.com/eu-13/briefings/Beery/bh-eu-13-a-perfect-crime-beery-wp.pdf/**

2011 – CRIME statistics



TLS Compression / CRIME

Sites that support TLS compression

5,110

- 0.2 %

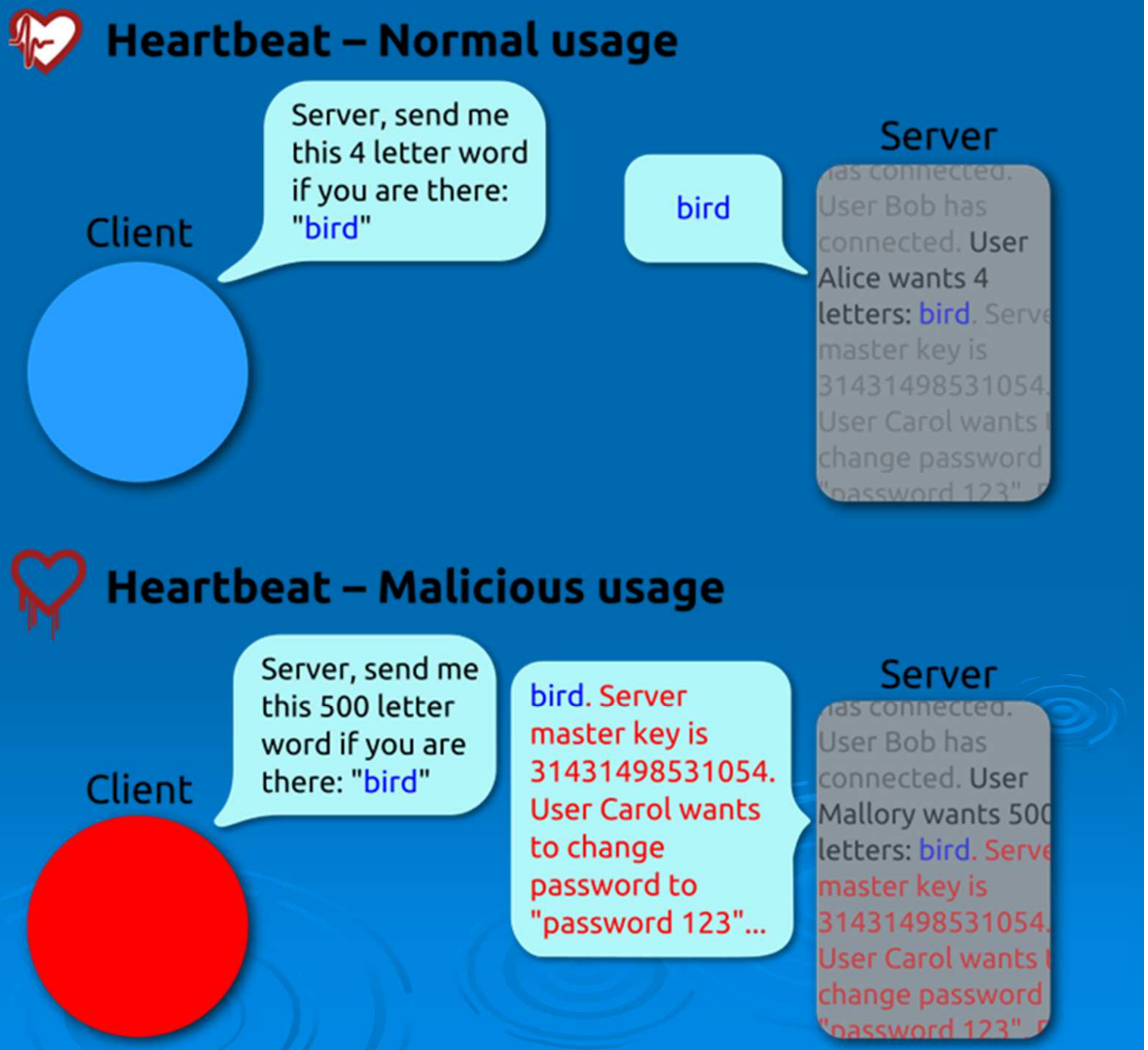
Source: SSL Pulse- **https://www.trustworthyinternet.org/ssl-pulse/**

Prox-IA
Informatique Avancée

http://prox-ia.blogspot.com

2014 - Heartbleed

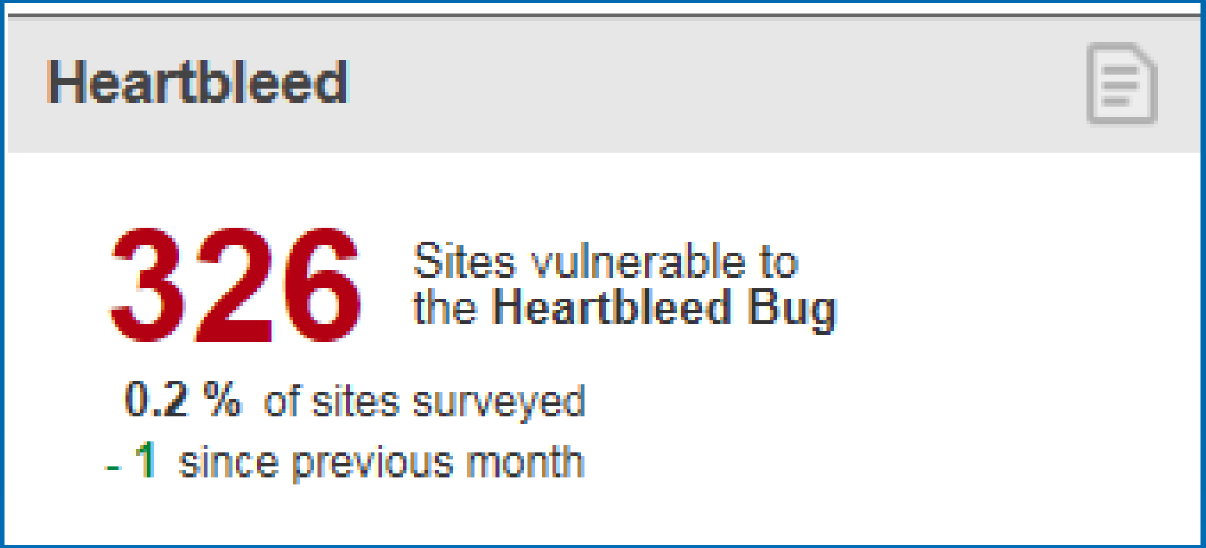
OpenSSL


Heartbeat – Normal usage
Client
Server, send me this 4 letter word if you are there: "bird"
bird
Server
as connected. User Bob has connected. User Alice wants 4 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". P
Heartbeat – Malicious usage
Client
Server, send me this 500 letter word if you are there: "bird"
bird. Server master key is 31431498531054. User Carol wants to change password to "password 123"...
Server
as connected. User Bob has connected. User Mallory wants 500 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". P

Prox-IA
Informatique Avancée

http://prox-ia.blogspot.com

2014 – Heartbleed statistics



Heartbleed

326 Sites vulnerable to the Heartbleed Bug

0.2 % of sites surveyed

- 1 since previous month

Source: SSL Pulse- **https://www.trustworthyinternet.org/ssl-pulse/**

2014 - CCS

- OpenSSL does not properly restrict processing of **ChangeCipherSpec** messages
- It allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications
- Consequently attackers can hijack sessions or obtain sensitive information, via a crafted TLS handshake
- Aka the "CCS Injection" vulnerability.

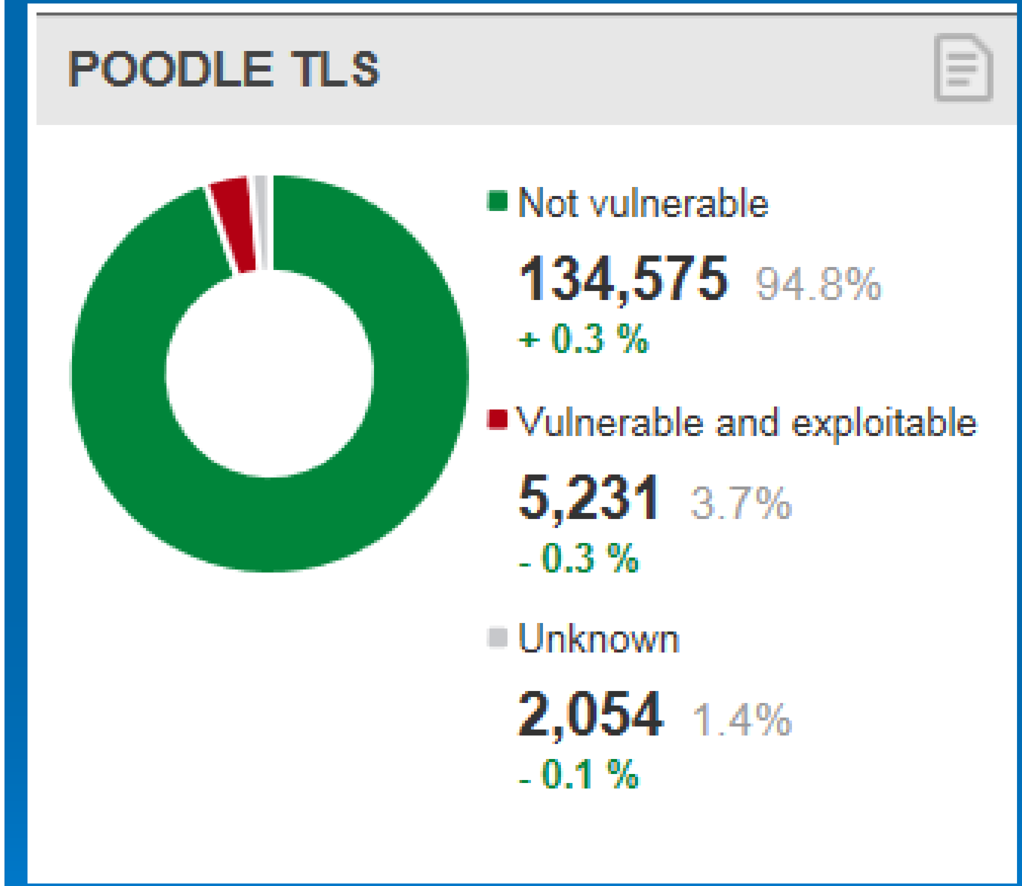
Source: CVE CCS- **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224/**

2014 - POODLE

- Padding Oracle On Downgrading Legacy Encryption
- The downgrade is triggered by active attackers
- Do not use SSL 3.0 or use TLS_FALLBACK_SCSV
- TLS_FALLBACK_SCSV is a signaling suite that can detect protocol downgrade if client also supports this feature

Source: This POODLE bites - **https://www.openssl.org/~bodo/ssl-poodle.pdf/**

2014 – POODLE statistics

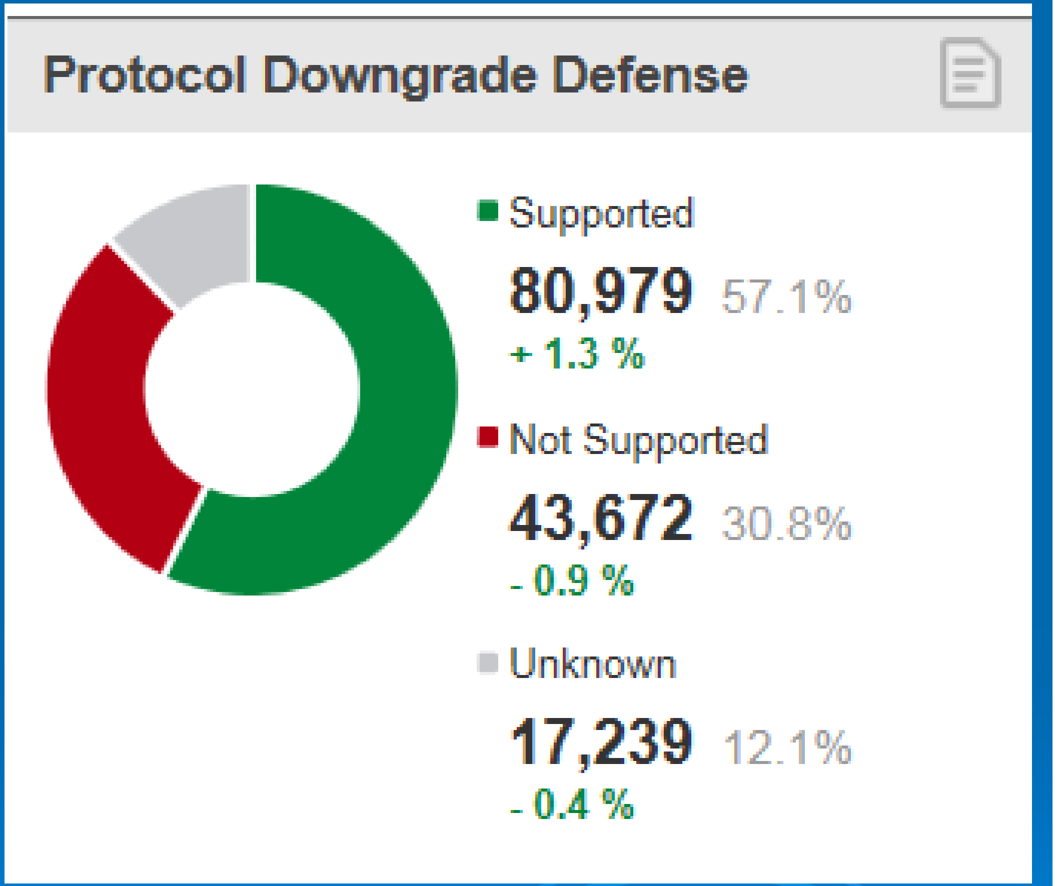


POODLE TLS

🟩 Not vulnerable
134,575 94.8%
+ 0.3 %

🟥 Vulnerable and exploitable
5,231 3.7%
- 0.3 %

⬜ Unknown
2,054 1.4%
- 0.1 %



Protocol Downgrade Defense

🟩 Supported
80,979 57.1%
+ 1.3 %

🟥 Not Supported
43,672 30.8%
- 0.9 %

⬜ Unknown
17,239 12.1%
- 0.4 %

TLS_FALLBACK_SCSV

Source: SSL Pulse- **https://www.trustworthyinternet.org/ssl-pulse/**

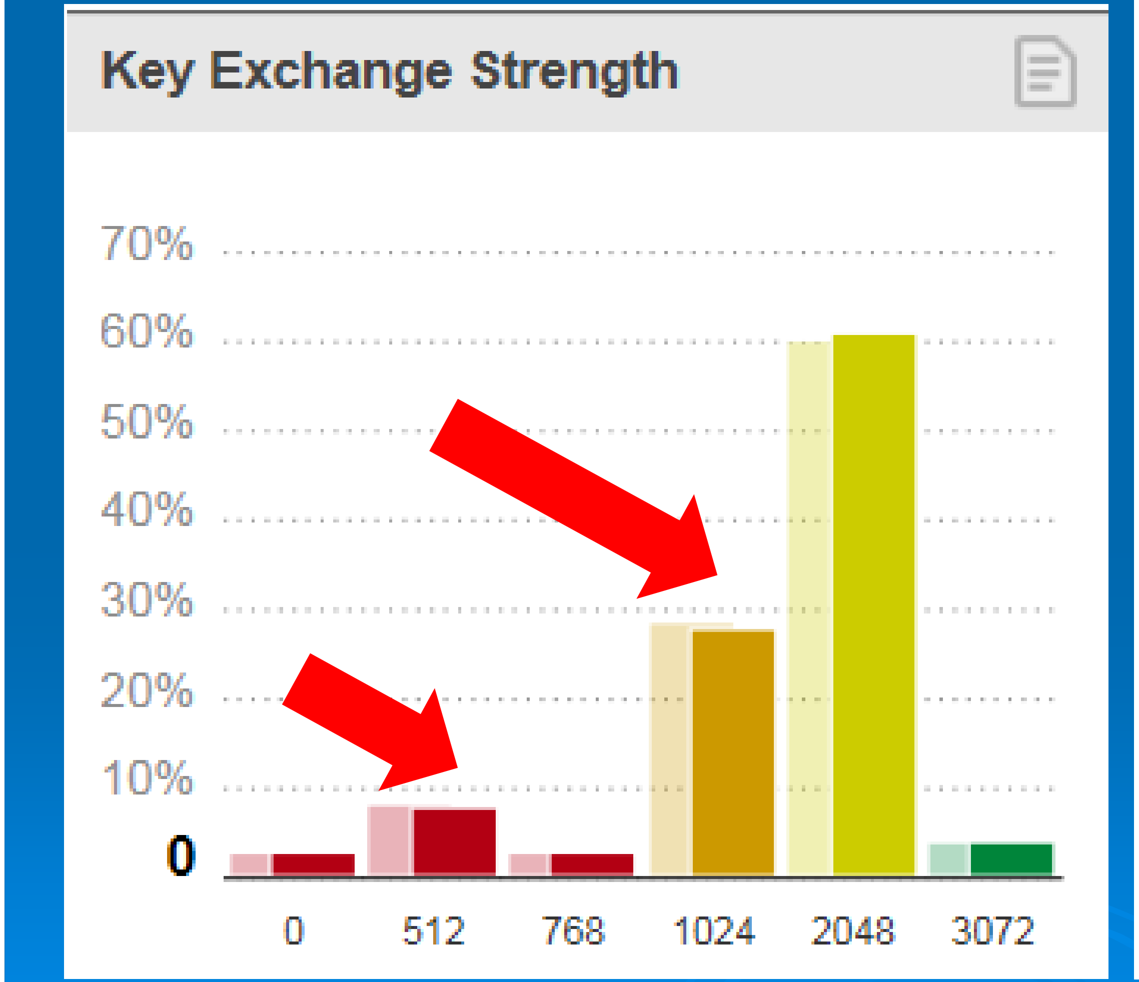
2015 - LOGJAM

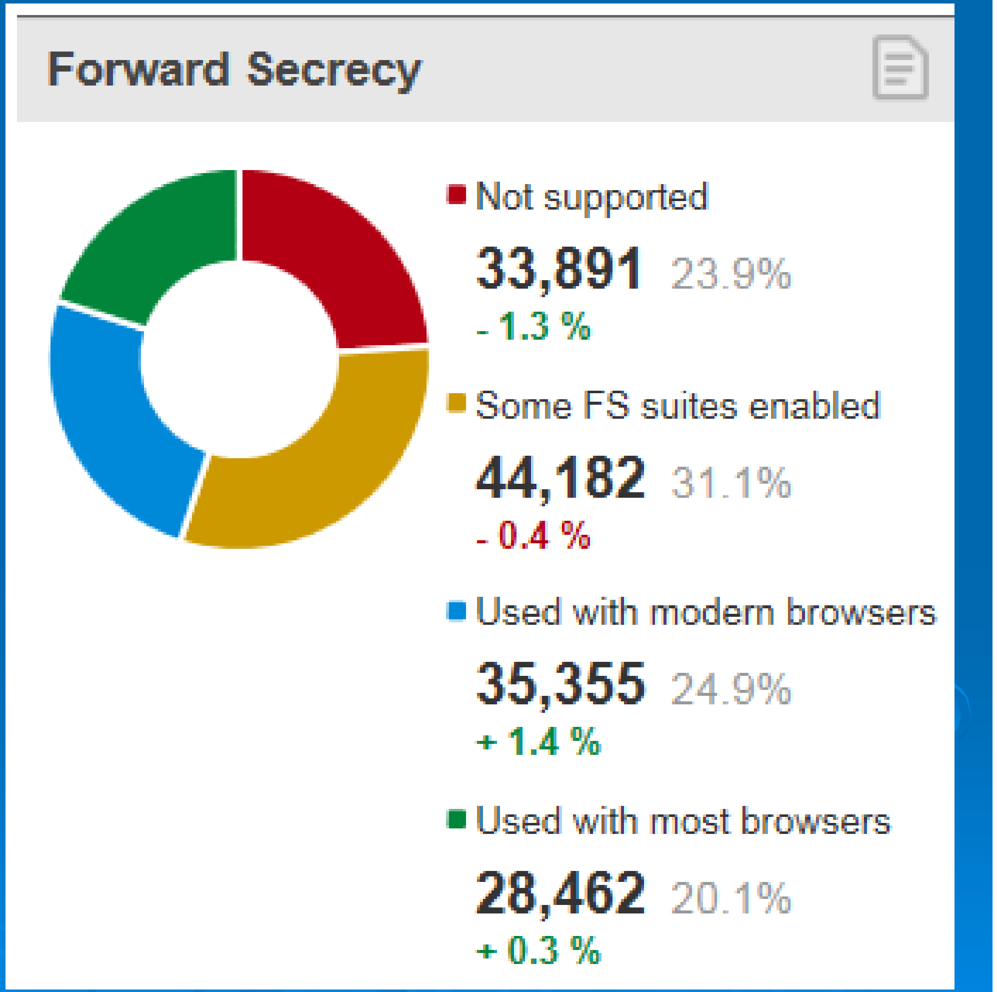
- DHE and ECDHE provides **Forward Secrecy** to protect each protection individually with a fresh key. **Forward Secrecy** property is that even if the server key is compromised it cannot be used to decrypt past connections
- DHE parameters often are fixed and reused: 512/768 bits are weak, 1024 to be breakable by governments and 2048 are safe
- An attacker can perform a bulk computation having only the parameters and break any DHE in minutes

- Due to an TLS protocol vulnerability and exploited by attacking DHE
- Connection can be forced to use “Export Crytography” (DHE_EXPORT). Server does not inform client of this weak choice
- Never the “Client Hello”, “Client Ciphersuites” and chosen “Ciphersuite” are signed by the server

Source: Logjam: the latest TLS vulnerability explained- **https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained//**

2015 – LOGJAM (statistics)





Source: SSL Pulse- **https://www.trustworthyinternet.org/ssl-pulse/**

2015 - FREAK

- Connection can be forced to use “Export Crytography”
- Due to an implementation vulnerability and exploited by attacking RSA key exchange

2015 - RC4

Scenario:

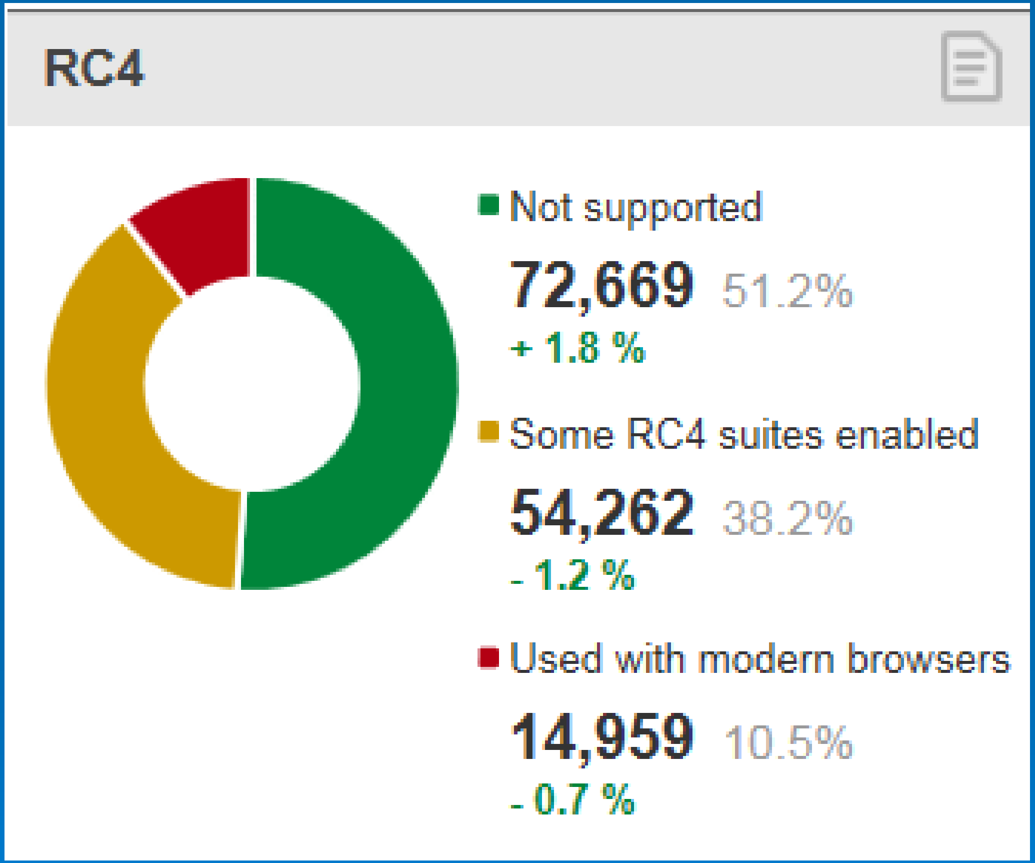
- The attacker sniffs a large number of SSL connections encrypted with RC4 waiting for a weak key
- If weak key, the attacker predicts the LSBs of the keystream and use them to extract the LSBs of the plaintext (**Invariance Weakness**)

- To get a session cookie by bruteforce attack
- To get a n-character password by dictionary attack (accelerate wit a factor 2^n
- To get a credit card number (16 digits = 6 non secrets + **5 entropy** + 4 exposed on receipts + 1 checksum) => 100000 attempts reduced to 1500 and 750 average

- For simplicity we say 1 billion encryptions are seen by the attacker to recover data (e.g. using active generation: BEAST or passive sniff: Facebook) – Note that there is no control on target identity

Source: Attacking SSL when using RC4 - http://www.imperva.com/docs/hii_attacking_ssl_when_using_rc4.pdf/

2015 - RC4



RC4

🟩 Not supported

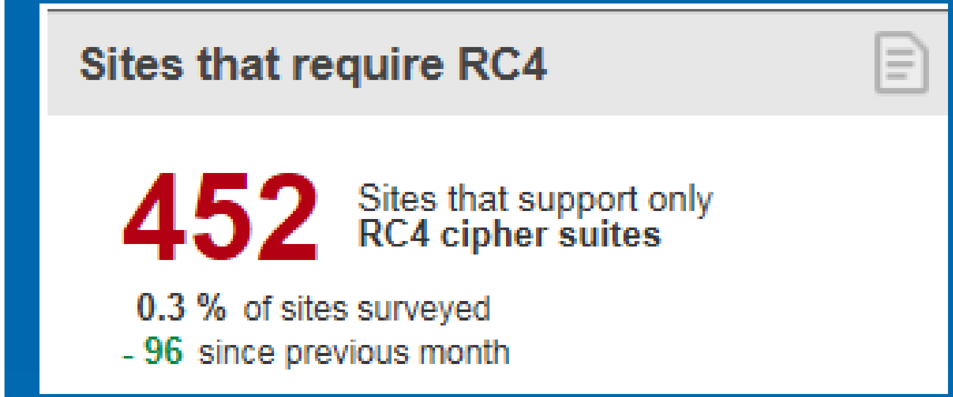
72,669 51.2%
+ 1.8 %

🟨 Some RC4 suites enabled

54,262 38.2%
- 1.2 %

🟥 Used with modern browsers

14,959 10.5%
- 0.7 %



Sites that require RC4

452 Sites that support only RC4 cipher suites

0.3 % of sites surveyed
- 96 since previous month

Source: SSL Pulse- **https://www.trustworthyinternet.org/ssl-pulse/**

2015 - RC4 Likelihood

Server view:

- Daily active users in Facebook is close to 1 billion (4 logins/user)
- In 4 billions logins we have 256 weak keys
- 4 weak key will expose passwords
- RC4 in not anymore in the list of supported ciphersuites

Client view:

- 1 / 64.000.000 to get a weak RC4 key
- 1 / 1.000.000.000 to leak part of secrets
- 1 / 116.531.800 to win at EuroMillions
- 1 / 19.068.840 to win at Loto
- But it can happen to anyone !

Source: Attacking SSL when using RC4 - http://www.imperva.com/docs/hii_attacking_ssl_when_using_rc4.pdf/

Demo I

Go to https://www.ssllabs.com/ssltest/

Test weak web sites with TestSSL on Backtrack

```
> cd /root/Desktop/Repository/TestSSL
> ./testssl.sh https://www.gemalto.com
```