**MALWARE OPENING PORTS**

1. A vulnerability in OpenSSL could allow a remote attacker to expose sensitive data, possibly including user authentication credentials and secret keys, through incorrect memory handling in the TLS heartbeat extension [1].
2. The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs) [2].
3. The data obtained by a Heartbleed attack may include unencrypted exchanges between TLS parties likely to be confidential, including any form post data in users' requests. Moreover, the confidential data exposed could include authentication secrets such as session cookies and passwords, which might allow attackers to impersonate a user of the service. An attack may also reveal private keys of compromised parties, which would enable attackers to decrypt communications (future or past stored traffic captured via passive eavesdropping, unless perfect forward secrecy is used, in which case only future traffic can be decrypted if intercepted via man-in-the-middle attacks) [3].

**REFERENCES**

1. <https://www.us-cert.gov/ncas/alerts/TA14-098A>
2. <https://www-304.ibm.com/support/docview.wss?uid=swg21669823>
3. <https://en.wikipedia.org/wiki/Heartbleed>