Whom do we trust - Booters and SSL/TLS certificates

Jessica Steinberger*†, Benjamin Kuhnert*, Saed Alavi*, José Jair Santanna†, Anna Sperotto†, Harald Baier* and Aiko Pras†

* da/sec - Biometrics and Internet Security Research Group
University of Applied Sciences Darmstadt
Darmstadt, Germany
Email:{Jessica.Steinberger, Benjamin.Kuhnert, Saed.Alavi, Harald.Baier}@crisp-da.de

† Design and Analysis of Communication Systems (DACS)
University of Twente
Enschede, The Netherlands
Email:{J.Steinberger, J.J.Santanna, A.Sperotto, A.Pras}@utwente.nl

Nowadays, DDoS attacks still remain the top cause of network and service outages. The reason is that these attacks are getting more sophisticated and frequent whereas the required technial skills to perform these attack are not required anymore [**JS15**]. Currently, DDoS attacks are offered as a service, namely Booters, for less than 10 US dollars [**JS16**]. As Booters offer a service that a customer is required to pay for, Booters make use of SSL/TLS certificates. The use of SSL/TLS certificates is used to ensure secure credit card transactions, data transfer and logins.

In this talk, we present the early-stage results of the analysis of the used certificate chains of Booter websites. In particular, we present the common used certificate chains, the used cryptography and cipher suites, protocol use within SSL/TLS for purpose of security parameters negotiation, the issuer and the validity of the certificate. Our analysis revealed that there is a tyical certificate chain used by Booter websites. In our future work, we investigate if the SSL/TLS certificates and their certificate chains could be used to mitigate DDoS attacks performed by Booter websites.

References

[JS15] J.J. Santanna, R. van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, L. Zambenedetti Granville, and A. Pras. Booters - an analysis of DDoS-as-a-service attacks. In *Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on*, pages 243–251, May 2015. DOI: 10.1109/INM.2015.7140298.

[JS16] J. Steinberger, J.J. Santanna, E. Spatharas, H. Amler, N. Breuer, K. Graul, B. Kuhnert, U. Piontek, A. Sperotto, H. Baier and A. Pras. "Ludo" - kids playing Distributed Denial of Service In *Proceedings of TERENA Networking Conference (TNC16), Prague (Czech Republic), June 2016, to appear.*