# Accepted Manuscript


Title: A survey on technical threat intelligence in the age of sophisticated cyber attacks

Author: Wiem Tounsi, Helmi Rais

PII: S0167-4048(17)30183-9
DOI: https://doi.org/doi:10.1016/j.cose.2017.09.001
Reference: COSE 1197

To appear in: *Computers & Security*

Received date: 24-4-2017
Revised date: 24-7-2017
Accepted date: 5-9-2017

Please cite this article as: Wiem Tounsi, Helmi Rais, A survey on technical threat intelligence in the age of sophisticated cyber attacks, *Computers & Security* (2017), https://doi.org/doi:10.1016/j.cose.2017.09.001.

# A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attacks

Wiem Tounsi, Helmi Rais

*Managed Security Services Division, AlliaCERT Team, Alliacom, France*

{FirstName.SurName}@alliacom.com

Short Biography of authors

**Wiem Tounsi** is a cyber security scientist and a R&D Professional. She obtained her Ph.D. degree in January 2014 from TELECOM Bretagne (Rennes, France) of Mines-TELECOM Institute. She received the Engineering degree in computer networks and telecommunications from INSA.T and the M.S. degree in electronic systems and communication networks from the Polytechnic School (EPT) in 2008 and 2009, respectively. Her research interests include cyber threat intelligence generation, reverse engineering, formal verification/analysis of security properties and management of security and privacy policies. She has authored several research papers in selective and high level international journals and conferences.

**Helmi Rais** is a senior professional in charge of security services, business development and R&D. He received the Engineering degree in computer networks and telecommunications from INSA.T in 2004. Reaching 15 years of Expertise in cyber security, his main interests include data protection, risk assessment and cyber defense strategies building. He is a member of founding team of ANSI, AlliaCERT, TUNCERT, OIC-CERT, AfricaCERT, DevTeam and a speaker and panelist in different IT security events (TedX, ITU, FIRST, Alliacom Events, CNIS Mag, OIC-CERT, TF-CSIRT and Securiday).

**Abstract**

Today's cyber attacks require a new line of security defenses. The static approach of traditional security based on heuristic and signature does not match the dynamic nature of new generation of threats that are known to be evasive, resilient and complex. Organizations need to gather and share real-time cyber threat information in order to prevent attacks or at least execute timely disaster recovery. Threat Intelligence (TI) means evidence-based knowledge representing threats that can inform decisions. There is a general awareness for the need of threat intelligence while