Seminar announcement

November 26, 2021, Time: 9:00-11:00am
Online (Microsoft Teams)
Seminar Series on Data Security (MSc Degree in Data Science)
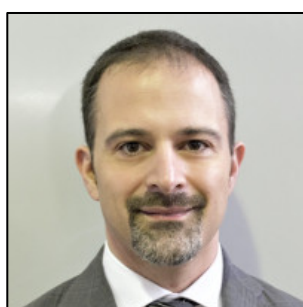
Dr. Antonio Forzieri

EMEA Cyber Security Specialization and Advisory

Splunk Inc.

Connecting the dots: Investigating an APT campaign using Splunk

Abstract: Frothly is a small home brewing startup company out of San Francisco. Last year, the company got hacked by Taedonggang APT. Since then, Frothly hired Bud Stoll as head of IT and he has taken Frothly to the cloud, both Azure and AWS. During this workshop you will be assuming the role of Alice Bluebird, Frothly's security analyst.

On August 20th, 2018, during lunch, you see your CEO calling you on your mobile, but you decide not to pick it up. A bit later, while at the bar, the CEO calls again. The news is not good. You run to the office, log into Splunk Enterprise Security, and see plenty of triggered incidents. Based on threat intelligence gathered, it appears that Taedonggang APT is back at it with Frothly. Are you ready to investigate?

Lecturer short bio: *At Splunk, Ing. Antonio Forzieri is responsible for the Cyber Security offering for EMEA. Previously Antonio worked in Symantec as a Global Cyber Security Practice Lead supporting customers in complex Cyber Security Initiatives ranging from building/evolving Cyber Defense Centers to supporting customers in Cyber Security Intelligence Programs. Antonio Forzieri holds a degree in Telecommunication Engineering from Politecnico di Milano where he is also a lecturer for the course "Internet: Mobility and Security".*

Microsoft Teams link:
https://teams.microsoft.com/l/meetup-join/19%3aaKasC8I_4_Ag4wV0L9eQO-QPmSgy1NAPDdxBFTjz44g1%40thread.tacv2/1636982471433?context=%7b%22Tid%22%3a%222fcfe26a-bb62-46b0-b1e3-28f9da0c45fd%22%2c%22Oid%22%3a%22e7d8babb-0ea0-45c6-91ac-82940c3f1edf%22%7d

Organizers: Dr. R. Natella (contact for info: roberto.natella@unina.it), Proff. D. Cotroneo, S.P. Romano