I SEMINARI DEL DII

CYBER master SECURITY

WANNACRY

ANALISI DI UN ATTACCO RANSOMWARE SU SCALA GLOBALE

Mirko Casadei e Matteo Redaelli

Accenture

VENERDÌ 21 SETTEMBRE

H. 11.00 - SALA RIUNIONI DII, VIA CARUSO 16

Abstract

Durante il seminario verrà condotta un'analisi sulle cause e gli effetti della diffusione del ransomware Wannacry. Le diverse fasi dell'attacco saranno commentate ed approfondite sia dal punto di vista del threat actor che dal punto di vista dei difensori. Saranno quindi introdotte le tecnologie impiegate per la diffusione e i processi e gli strumenti utilizzati per la risposta. A conclusione, verrà proposta e commentata con gli studenti la possibile lesson learned. L'intervento inoltre vedrà contestualizzate le diverse figure professionali coinvolte, tra cui Red Team Analyst, Threat Intelligence Analyst, Forensics Analyst e Malware Analyst.

Bio

Mirko Casadei - Security senior consultant, in Accenture è il responsabile Italia per il dominio Malware Analysis ed è coinvolto attivamente negli incidenti informatici ai danni dei Clienti. Si occupa correntemente di differenti aree della sicurezza IT: Threat Intelligence, Incident Response, Digital Forensic and malware analysis, Reverse Engineering, Data Privacy and Compliance, Infrastructure Security, SIEM and Log Management, SOC, CERT, Security Project design and delivery. Precedentemente, membro del Computer Emergency Response Team, all'interno del Centro di Comando e Controllo interforze Nato, e coordinatore tecnico del Blue Team alle esercitazioni internazionali Nato LockedShield. Nell'ambito delle attività forensi e threat hunting ha effettuato il reverse engineering di APT e lo studio di diverse importanti campagne di spionaggio malware. Detiene le certificazioni internazionali GIAC GREM (Reverse Engineering Malware), GCFA(Certified Forensic Analyst) e GCIA (Certified Intrusion Analyst).

Matteo Redaelli - Cyber Security Consultant, ha diversi anni di esperienza in diversi settori relativi alla sicurezza informatica come Cyber Threat Intelligence, Malware Analysis, Web Application Security, Web Application Penetration Testing e SecDevOps. Conduzione operativa di diversi progetti in Italia e in Europa. Certificato SANS GCIH, SANS GCFA, ISO27001.

Laurea Magistrale in Informatica (conseguita lavorando full-time) presso l'Università degli studi di Milano Bicocca con una tesi sulla malware analysis. Laurea Triennale in Informatica presso l'Università degli studi di Milano Bicocca con una tesi sulla sicurezza delle applicazioni web.

Per esigenze logistiche occorre registrarsi inviando una mail a **master-security@iet.unipi.it**

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

In collaborazione con

IIT Istituto di Informatica e Telematica

UNIVERSITÀ DI PISA