Allegato 1) Elenco dei progetti di ricerca

Titolo: SPAAM - Sicurezza e Prevenzione di Attacchi in Ambito Mobile (Codice pratica: 88bab806)

Soggetto proponente
Denominazione: Università del Salento
Dipartimento/Istituto/Unità: Dipartimento di Ingegneria dell'Innovazione
Sede di svolgimento del progetto: Campus Ecotekne, via per Monteroni s.n.c. Lecce

Impresa privata
Denominazione: Deep Consulting Srl
Sede di svolgimento del progetto: Via Stradella Barone, 9, Bari

Ambito di ricerca dell'European Research Council (Livello 1):	Physical Sciences and Engineering
Ambito di ricerca dell'European Research Council (Livello 2):	Physical Sciences and Engineering
Filiera produttiva regionale:	03 - INFORMATICA

Descrizione del progetto di ricerca
Lo scopo del progetto è la definizione di nuove procedure per la protezione da malware in contesto mobile, con il fine di supportare la difesa pro-attiva di reti di dispositivi (device) connessi all'interno di reti aziendali e private. La difesa di dispositivi mobili da attacchi di tipo malware è importante per garantire sia la protezione dei dati personali degli utenti privati che la protezione dal punto di vista aziendale, in cui la difesa delle reti riguarda sia la sicurezza dei segreti industriali e degli asset appartenenti all'azienda, ma anche servizi essenziali come trasporti pubblici, sanità, etc. La crescente diffusione del lavoro agile, insieme a tendenze già conosciute come BYOD (bring your own device), rendono difficoltosa la protezione interna. Infatti, se da una parte questi approcci semplificano la comunicazione e la flessibilità per l'utente, dall'altra questo si traduce in una più ampia superficie di attacco, data appunto da un sistema eterogeneo di sistemi di comunicazione utilizzati nello stesso contesto lavorativo, in cui la protezione del sistema mobile è, spesso, responsabilità dell'utilizzatore. Inoltre, nuove tipologie di malware potrebbero emergere come risultato di nuovi componenti digitali, ognuna delle quali può essere individualmente classificata come "sicura". Tale criticità è trasversale alle diverse filiere produttive, a partire da quella informatica, cui si rivolge la presente proposta, e conseguentemente quelle che fruiscono di servizi IT in diversi ambiti, fino ad arrivare agli utenti finali (si pensi, ad esempio, alle applicazioni m-health). Le diverse scale sulle quali le reti di dispositivi mobile possono avere effetti, a livello di infrastrutture, enti o persone, richiedono quindi adeguate contromisure che non valutino un device solo localmente, ma come un nodo immerso in un network complesso (caratterizzato da interdipendenze su molteplici livelli) e aperto (in cui i dispositivi connessi a una rete e le loro connessioni con altre reti possano aggiungersi o essere rimossi nel tempo). possano potenziali fonti di acquisizione di informazione o di attacco) sono complesse e, spesso, non visibili all'utente e al gestore della rete. A tal fine, il progetto porrà le basi per la definizione di framework di strumenti e

metodologie che valuti la propagazione delle vulnerabilità all'interno di reti IT attraverso dispositivi mobile, con particolare attenzione all'analisi di malware e all'esfiltrazione di dati. Le attività su cui sarà coinvolto l'assegnista si innesteranno nell'attuale ricerca di strumenti a supporto di Network Intrusion Detection Systems (NIDS), focalizzandosi su potenziali vulnerabilità difficilmente tracciabili a causa di fattori ambientali o di limitazioni tecnologiche. Tali aspetti si traducono nei seguenti obiettivi realizzativi: OR1. Definizione di un approccio di valutazione delle limitazioni delle attuali tecniche di analisi dei malware e dei NIDS OR2. Definizione di un prototipo di protocollo per supportare le tecniche di malware analysis e intrusion detection in condizioni di limitata tracciabilità dei dispositivi mobile e delle loro connessioni con altre reti.