Abstract (Italian)

Oggigiorno Internet è il fulcro del mondo, e il World Wide Web è la chiave per accedervi. Noi sviluppiamo relazioni personali attraverso i social network e affidiamo informazioni sensibili a servizi online. Le tipiche applicazioni desktop vengono rimpiazzate da applicazioni web perfettamente funzionali, che possono essere utilizzate su qualsiasi dispositivo. Tutto ciò è possibile grazie a nuove tecnologie web che vengono introdotte a ritmo incessante. Tuttavia, il progresso ha un prezzo. Oggi, il web è il principale mezzo utilizzato dal crimine informatico per minacciare individui ed organizzazioni. In un contesto dove l'informazione digitale è estremamente dinamica e volatile, la lotta contro il crimine informatico diventa sempre più difficile.

Questo lavoro di ricerca è diviso in due parti complementari. La prima sezione è focalizzata sullo studio degli aspetti forensi legati al crimine informatico, e mostra alcune limitazioni delle odierne tecniche di analisi delle prove digitali. In primis, viene presentato un nuovo tipo di attacco che sfrutta la disponibilità di generici servizi online al fine di produrre prove digitali false. Le informazioni generate con questa tecnica risultano perfettamente genuine nel contesto di un'indagine forense e possono essere sfruttate per reclamare un alibi. In secundis, viene mostrata una nuova metodologia per l'acquisizione di prove digitali da servizi online. Tale metodo consente di collezionare informazioni in modo robusto ed affidabile anche quando la sorgente remota è estremamente dinamica, come nel caso di un social network.

La seconda parte di questo lavoro si concentra sull'analisi di attività criminali sul web. Il repentino e incessante progresso tecnologico può nascondere delle minacce. La stessa tecnologia utilizzata per sviluppare applicazioni web di ultima generazione può es-

sere sfruttata dal crimine informatico come mezzo d'attacco. In particolare, questo lavoro mostra come alcune funzionalità di HTML5 consentono di offuscare codice web dannoso. Gli attacchi offuscati con queste tecniche sono in grado di evadere i moderni sistemi di analisi malware, che si trovano in affanno rispetto all'incessante progresso tecnologico. Infine, viene presentato uno studio approfondito sul principale mezzo sfruttato oggi dal crimine informatico per attaccare gli utenti del web: gli exploit kit. Il frutto di questo studio è stato lo sviluppo di nuove tecniche e strumenti per supportare i moderni honeyclient nell'indentificazione e nell'analisi di minacce provenienti dal web.