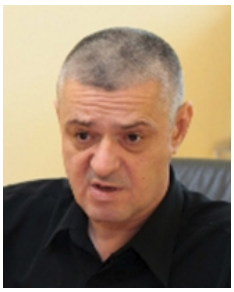

Саша Живановић

Начелник Одељења за борбу против високотехнолошког криминала МУП-а Републике Србије

Изазови заштите приватности: Искуства МУП-а Републике Србије у борби против високотехнолошког криминала

Резиме: Иако је настао пре готово педесет година, Интернет је постао глобална рачунарска мрежа тек почетком деведесетих година прошлог века. Захваљујући њему данас нам је омогућено да обављамо некад незамисливе процесе, животне и пословне активности. Без сумње, Интернет већ данас на планетарном нивоу има све разноврснију примену кроз велики број сервиса, а своју експанзију нарочито је доживео кроз примену електронске трговине и банкарства. Нажалост, као и већина других достигнућа, и Интернет има тамнију страну, односно може да се злоупотреби. Сведоци смо да се ова глобална мрежа неретко користи и за разне врсте превара, дистрибуције педофилског материјала и других облика високотехнолошког криминала. Материјалне штете које проузрокује финансијски сајбер криминал на глобалном нивоу већ се мере у милијардама америчких долара. Погодности Интернета, пре свега могућност да делују скривено и анонимно, неретко кроз коришћење рањивости нултог дана (**zero day** vulnerability) све чешће користе и организоване криминалне групе приликом вршења финансијског сајбер криминала, где циљани (spear phishing) напади у последње време нису усмерени само на мултинационалне и велике корпорације, већ су мете напада постале мала и средња предузећа са мањим бројем рачунара који им превасходно служе за обављање услуге електронског банкарства и електронске трговине. Такође, велики удео у данашњем финансијским сајбер криминалу представља и инфекција са злонамерним програмом тј. ransomware инфекција која кодира практично све корисничке податке на рачунару и тражи откуп у криптовалутама за одговарајући кључ како би се декодирали подаци. По правилу, сем ransomware инфекција, жртве сазнају да су мете финансијског сајбер криминала тек када се изврши новчана трансакција са њихових пословних рачуна, а приликом извршења компромитовања пословне електронске поште или тзв. ''директорске преваре'' (Business Email Compromise) жртве сазнају за превару тек након неколико дана тј. када контактирају инопартнера, најчешће телефонским позивом. Аутор ће у раду објаснити феномен финансијског сајбер криминала, организацију и методологију деловања организованих криминалних група, векторе напада финансијског сајбер криминала, као и проактивни приступ супростављања финансијском сајбер криминалу.