Naziv Zaposlenog: Marko Jovanović
Bezbednosna Organizacija: Nacionalni Centar za Cyber Bezbednost
Pogodjena Organizacija: Državna Uprava za Informacione Tehnologije
Ozbiljnost Incidenta: visoka
Adresa Pogodjene Organizacije: Bulevar Kralja Aleksandra 15, Beograd

Opis incidenta:
Tokom rutinske provere sistema u Državnoj Upravi za Informacione Tehnologije, otkrivena je masivna DDoS (Distributed Denial of Service) kampanja usmerena ka njihovim javnim servisima. Napad je trajao više od 12 sati, paralizujući ključne servise i onemogućavajući građanima pristup elektronskim uslugama.

Analiza saobraćaja pokazala je da je napad izveden pomoću velikog broja kompromitovanih uređaja širom sveta, što ukazuje na korišćenje botneta. Pored toga, napadači su koristili sofisticirane metode za prikrivanje izvora saobraćaja, uključujući IP spoofing i rotaciju proxy servera.

Odgovorni tim za bezbednost je odmah aktivirao plan za ublažavanje posledica DDoS napada, uključujući preusmeravanje saobraćaja kroz CDN (Content Delivery Network) i primenu rate-limiting tehnika. Paralelno sa tim, sprovedene su mere za identifikaciju i blokiranje zlonamernih IP adresa na nivou mreže.

Pored tehničkih mera, incident je poslužio kao važna lekcija za unapređenje koordinacije između različitih državnih službi i povećanje investicija u infrastrukturu otpornu na napade ovog tipa.

Zaključno, DDoS napad je osnažio svest o značaju kontinuiranog nadzora i pripreme, kao i važnosti međunarodne saradnje u borbi protiv sajber kriminala. Očekuje se uvođenje naprednih sistema za rano upozoravanje i automatizovane protokole reakcije u narednom periodu.