Назив Запосленог: Марко Јовановић
Безбедносна Организација: Национални Центар за Цубер Безбедност
Погођена Организација: Државна Управа за Информационе Технологије
Озбиљност Инцидента: висока
Адреса Погођене Организације: Булевар Краља Александра 15, Београд

Опис инцидента:
Током рутинске провере система у Државној Управи за Информационе Технологије, откривена је
масивна ДДоС (Дистрибутед Дениал оф Сервице) кампања усмерена ка њиховим јавним сервисима. Напад је трајао више од 12 сати, парализујући кључне сервисе и онемогућавајући
грађанима приступ електронским услугама.

Анализа саобраћаја показала је да је напад изведен помоћу великог броја компромитованих
уређаја широм света, што указује на коришћење ботнета. Поред тога, нападачи су користили
софистициране методе за прикривање извора саобраћаја, укључујући ИП споофинг и ротацију проху
Сервера.

Одговорни тим за безбедност је одмах активирао план за ублажавање последица ДДоС напада,
укључујући преусмеравање саобраћаја кроз ЦДН (Цонтент Деливеру Нетwорк) и примену рате-лимитинг техника. Паралелно са тим, спроведене су мере за идентификацију и блокирање
злонамерних ИП адреса на нивоу мреже.
Поред техничких мера, инцидент је послужио као важна лекција за унапређење координације
између различитих државних служби и повећање инвестиција у инфраструктуру отпорну на нападе овог
Типа.