Napadení UBNT v síti

Eurosignal

eurosignal

O síti

- ISP od roku 2002
- pokrytí - Praha, Praha-západ, Berounsko
- od roku 2009 bezdráty na Ubiquiti
- přes 7000 aktivních zařízení Ubiquiti, AP i klienti

Jak to všechno začalo

- napadení přes klientské zařízení s veřejnou ip
- rozšíření do našich AP i přes oddělený dohled
- chyba ve viru připravuje vlnu resetování
- zvláštní chování sítě v pátek večer

Nepříjemné probuzení

- mizející AP ze sítě
- hledání problému, fóra ještě spí
- rychlá analýza viru a napsání antiviru
- obnovování vyresetovaných AP na dálku z denních záloh
- průběžné vylepšování a rozšiřování možností antiviru a obslužných skriptů

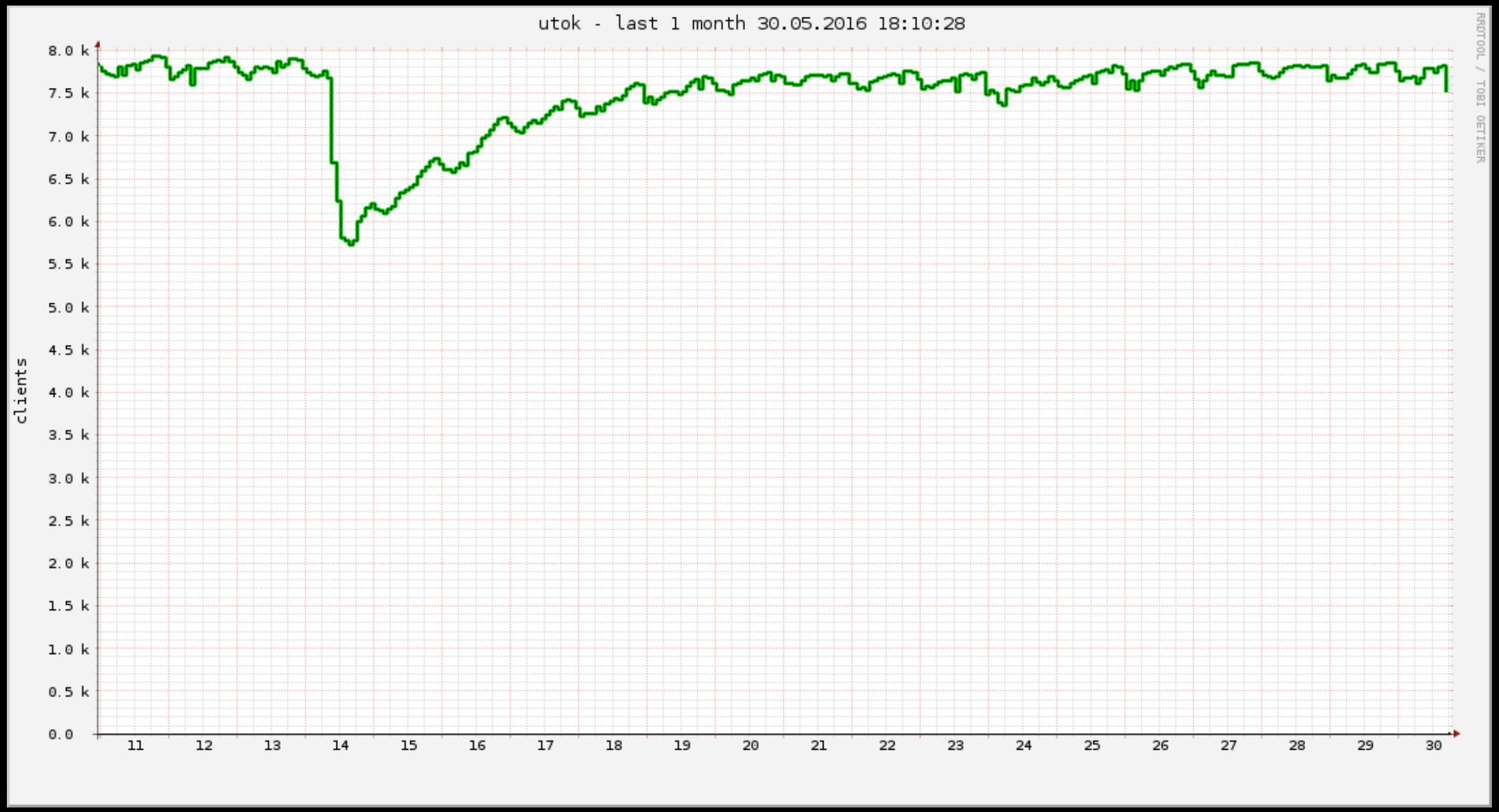
A klienti?

- spousta telefonů od sobotního rána
- antivir se snažil léčit i klienty
- oživování klientů na dálku přes výchozí essid
- obnova z denních záloh
- možnost obnovy ze zálohy klientem
- problém s vlastními hesly

Jak to dopadlo

- naše AP v provozu během sobotního dopoledne, téměř bez nutnosti výjezdu
- námi spravovaní klienti v provozu do tří dnů
- nutnost objet “resetovače”
- zvýšení zabezpečení všech zařízení, nejen AP

Jak to dopadlo



eurosignal

Co útok přinesl

- otestování krizové situace
- zlepšení zabezpečení
- rozšíření a vylepšení utilit pro správu
- zálohování se vyplácí
- podrobná dokumentace se vyplácí

Děkuji za pozornost.

eurosignal