Cyber Security Intelligence & Threat Mitigation

Adi Mendel

May 13, 2015

Network Trends and their security aspects

- NFV and SDN is here in more than just lab trials
  - NFV's Security is still a challenge but also an opportunity
- Analytics is becoming a critical tool for all departments in the organization
  - Security Analytics is gaining momentum in order to have visibility into the threats and their impact
- Enterprise AUP & BYOD – it's here and it's growing
  - Endpoint and Mobile security is a huge challenge\headache for SP and Enterprises and great opportunity for innovative solutions
- Encrypted Traffic is growing
  - The inability to decrypt and analyze SSL\TLS traffic for threats coming along side leaves a big hole uncovered

Interesting Inputs

- 71% of represented organizations experienced at least one successful cyberattack in the last year

Figure 2: Frequency of successful attacks in the past 12 months

- For the 2nd consecutive year, **mobile devices** are perceived as IT security weakest link
- Security analytics is the top-ranked network security technology planned for acquisition in 2015
- Phishing, malware, and zero-days give IT security the most headaches
- More than 2/3 are looking to replace or augment current endpoint protection tools

Source: 2015 CyberThreat Defense Report, by CYBEREDGE GROUP

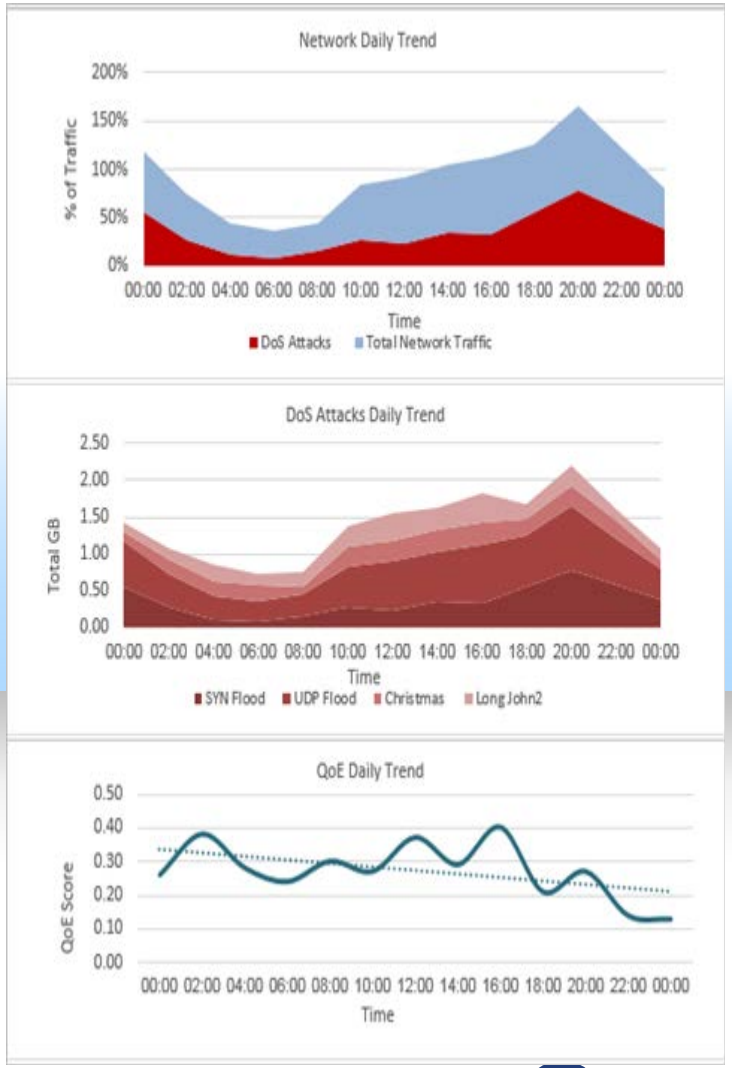
Survey Demographics: 814 qualified IT security decision makers

NFV and Cloud – New Threats

- **No more clear boundaries to the perimeter we need to secure**
- **Services can be distributed across many locations – no single point of defense**
  - Open for Multiple DDoS attacks simultaneously
  - Services hosts by different cloud ISP – who really protects my assets and what control\visibility do I have
- **The use of open source …**
- **Cybercriminals themselves are taking full advantage of cloud resources to boost up their efficiency**

Security Analytics – key factor

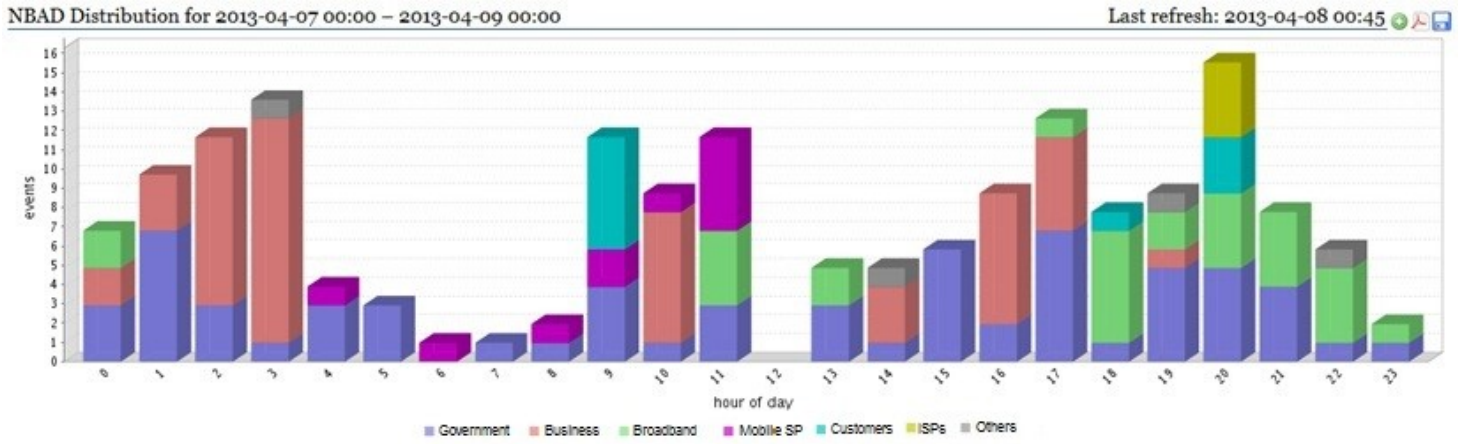
- We saw clear correlation between QoE and security threats
- The need to have the ability to correlate between network analytics and security analytics is becoming mandatory
- Security analytics should includes the ability to handle encrypted traffic and also deal with anonymizers



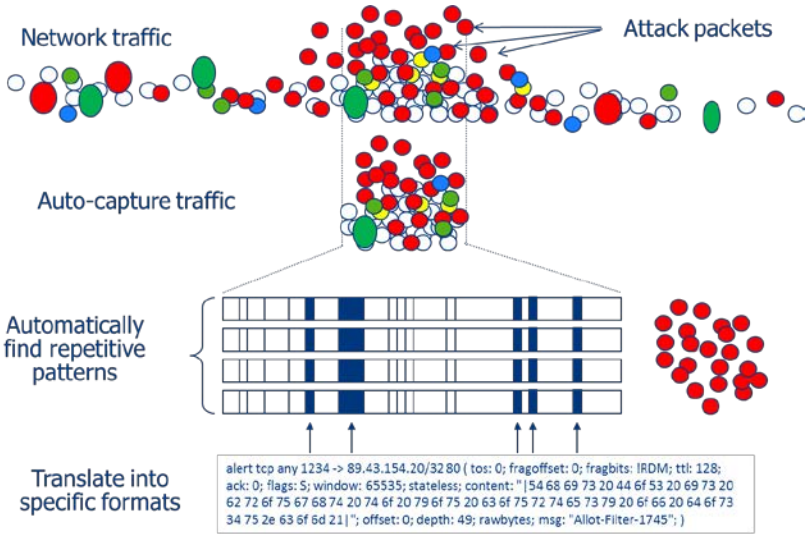
Mobile Devices – the new attack tool

- The processing power has grown and enable the devices to become an attacking device same as any PC
- The “openness” of the majority of the devices makes it very easy to install malwares viruses etc
- The Corporate Acceptable Use Policy (AUP) needs to be updated to cope with web and cloud applications
- The use of personal devices on corporate infrastructure (BYOD) is opening a back door into the organization for internal threats
- Maintaining a security solution updated on end user device is almost mission impossible

Actionable Security – DDoS Protection



DDoS/DoS/Scan attacks per Day



Anti-DDoS as a Service

Audit User Activity

Automatic/on-demand Mitigation action

Allot communications

Actionable Security – Network based Web Security