Martin Konov
IT Manager
Data Network Solutions and Support Services Department

INTRACOM
BULGARIA
an Intracom Telecom company

Technology Shaping the Future

Emerging Security Challenges in Cloud Computing

Follow | Link | Watch

Company at Glance

- Founded in 1995, 20th Anniversary of local experience and expertise
- Subsidiary of Intracom Telecom (100%)
- Headquarter, warehouse and 3 regional offices with 54 employees
- Broad portfolio of solutions and services for customers in the sectors of:
  - Telecommunications
  - Public
  - Enterprise & Banking
- Management Systems certified by an independent body:
  - Quality Management (ISO 9001:2008) System
  - Information Security Management (ISO 27001:2005) System
  - Complete technical infrastructure, incl. labs and vehicles
  - Experienced projects managers and engineers

You can avoid this …

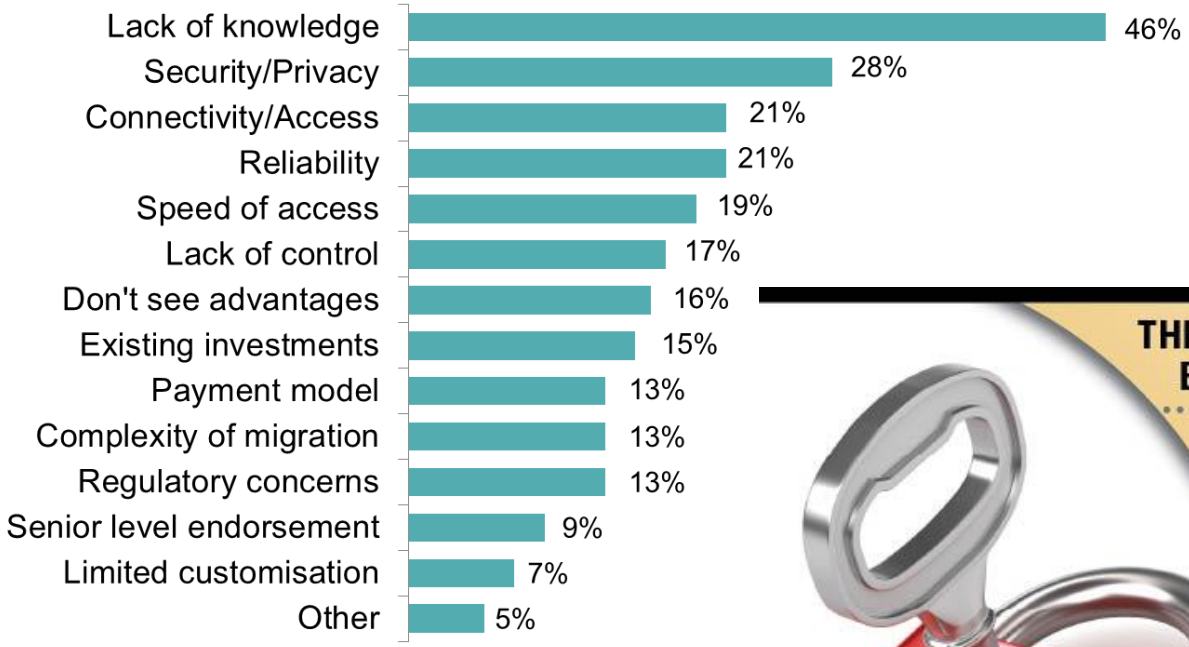
Technology Shaping the Future

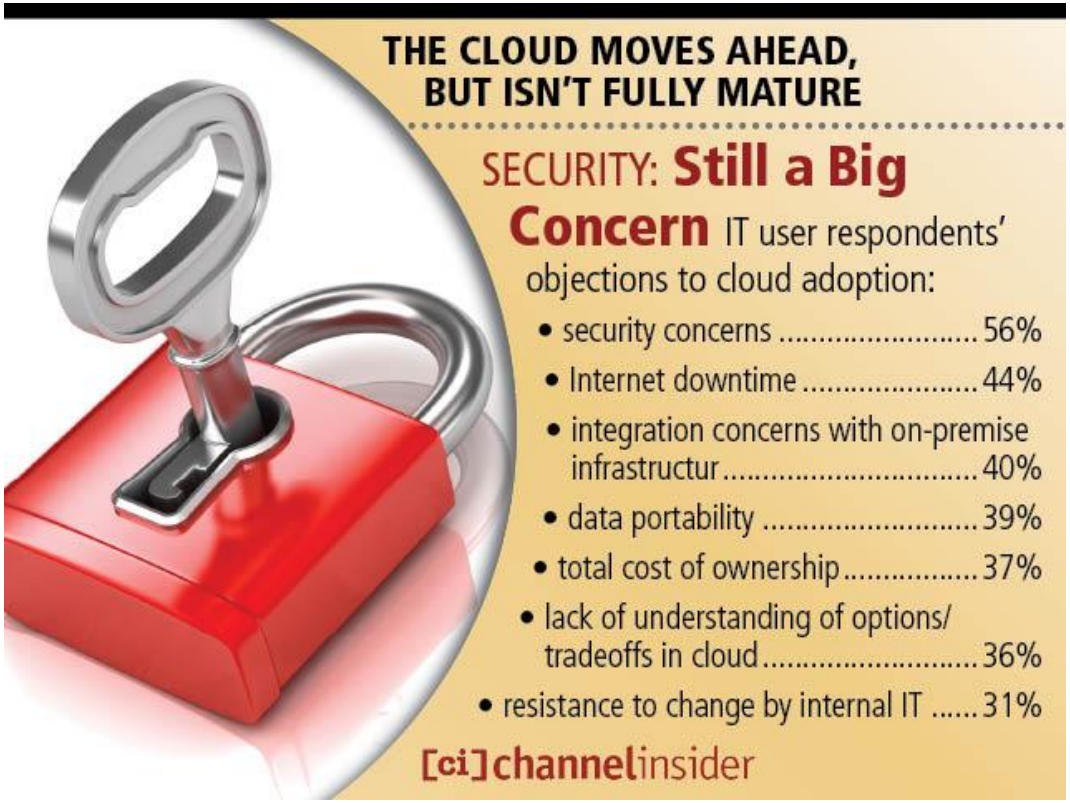
INTRACOM BULGARIA
an Intracom Telecom company

- A symbol of state-of-the-art platforms, new trends in ICT technology and markets
- The strongest Multi-vendor and multi-platform expertise:
  - Vast knowledge on networks and technology convergence
  - Experience on large scale and complex projects delivery
  - International footprint
  - Vertical market's knowledge
- Experienced in delivering turn-key projects On Time, On Budget, On Quality and Beyond Expectations

Cloud Adoption Problems

Challenges to cloud transition





What else as a Service?

INTRACOM BULGARIA
an Intracom Telecom company

- DDoS as a Service
- Software as a Service (PACS)
- Security as a Service
- Storage as a Service
- Backup as a Service

- Hybrid Cloud
- Disaster Recovery
- Virtual Desktop
- Virtual Private Cloud
- Virtual Machines
- Colocation & Managed Hosting
- Data Centre Connectivity

How DDoS Changed in the Last Years?

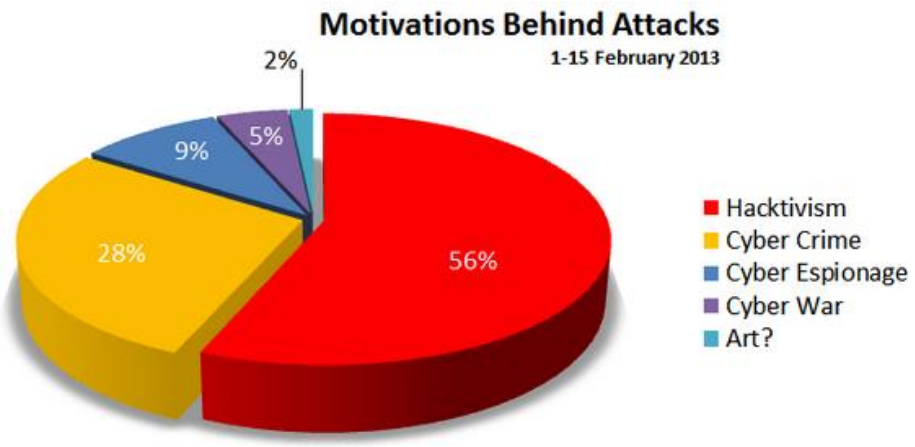
INTRACOM BULGARIA
an Intracom Telecom company

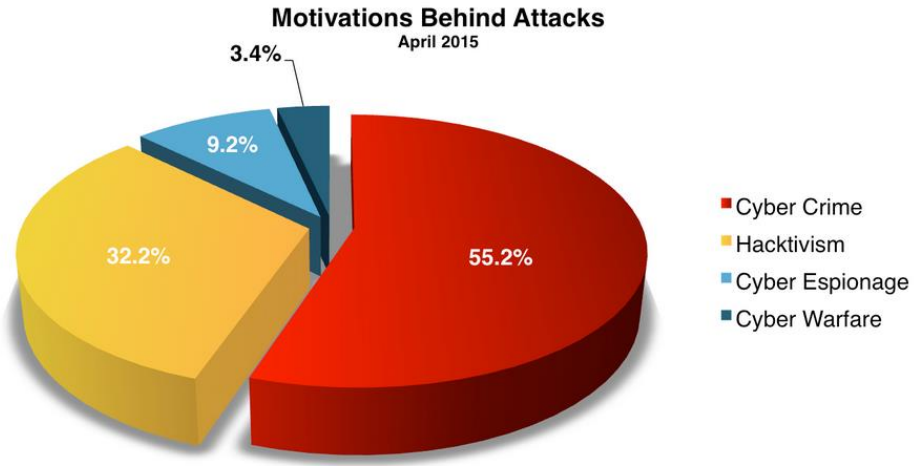
Historically

- Distributed Denial of Service attack
- Lots of small attack points
- Not very organized
- 50 Mbps to 2 Gbps throughput
- Hacktivism rather than stable income

Now

- More widely distributed
- Known good IP addresses
- Lots of large attack points.
- Larger CPU and Bandwidth consumption
- Stable income





DDoS Attack as Easy as Never before

Anonymous : "Volunteer your PC for the Cause"

- Volumetric Attacks – ICMP, UDP, TCP Floods
- Application-Layer Attacks – HTTP, DNS and NTP

Up to Now the World used Firewalls and IPS Devices

- All network devices are in-line, vulnerable and targets of DDoS attacks.
- Affected by large flood and connection attacks
- Build to protect again know attacks
- Don’t check valid (HTTP,DNS, NTP) request rather than invalid one
- All common network solution are in customer premises

How to Stop it?

Trend 1 Volumetric Attacks are Bigger

- Cloud-Based DDoS Mitigation
- Automatic Detection

Trend 2 Sophistication of application attacks

- Visitor Identification and Risk Analysis
- Minimize Disruption to the User Experience

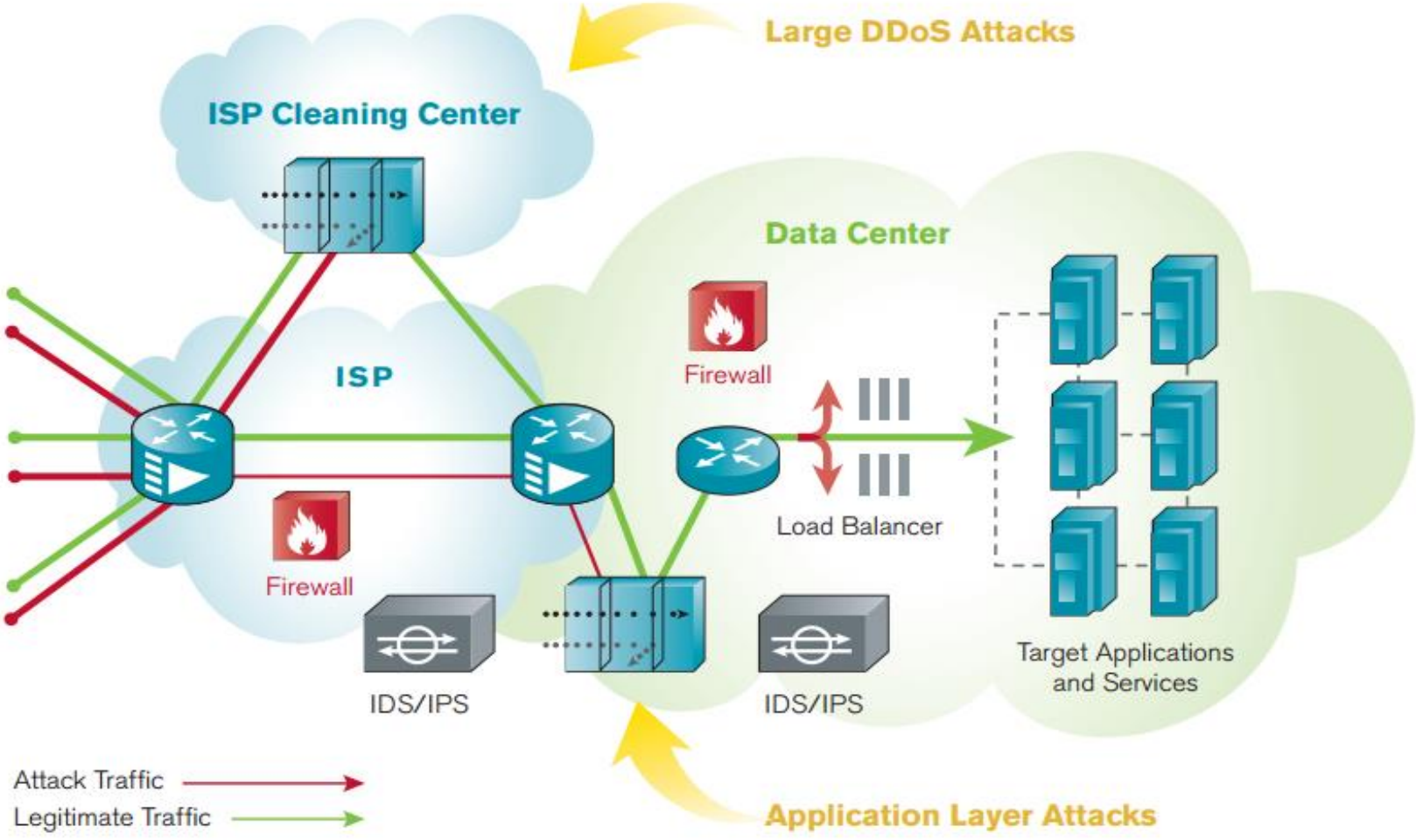
Trend 3 Low-cost attacks

- Always On DDoS protection. Keep your eyes open
- Automatic Detection & Mitigation.

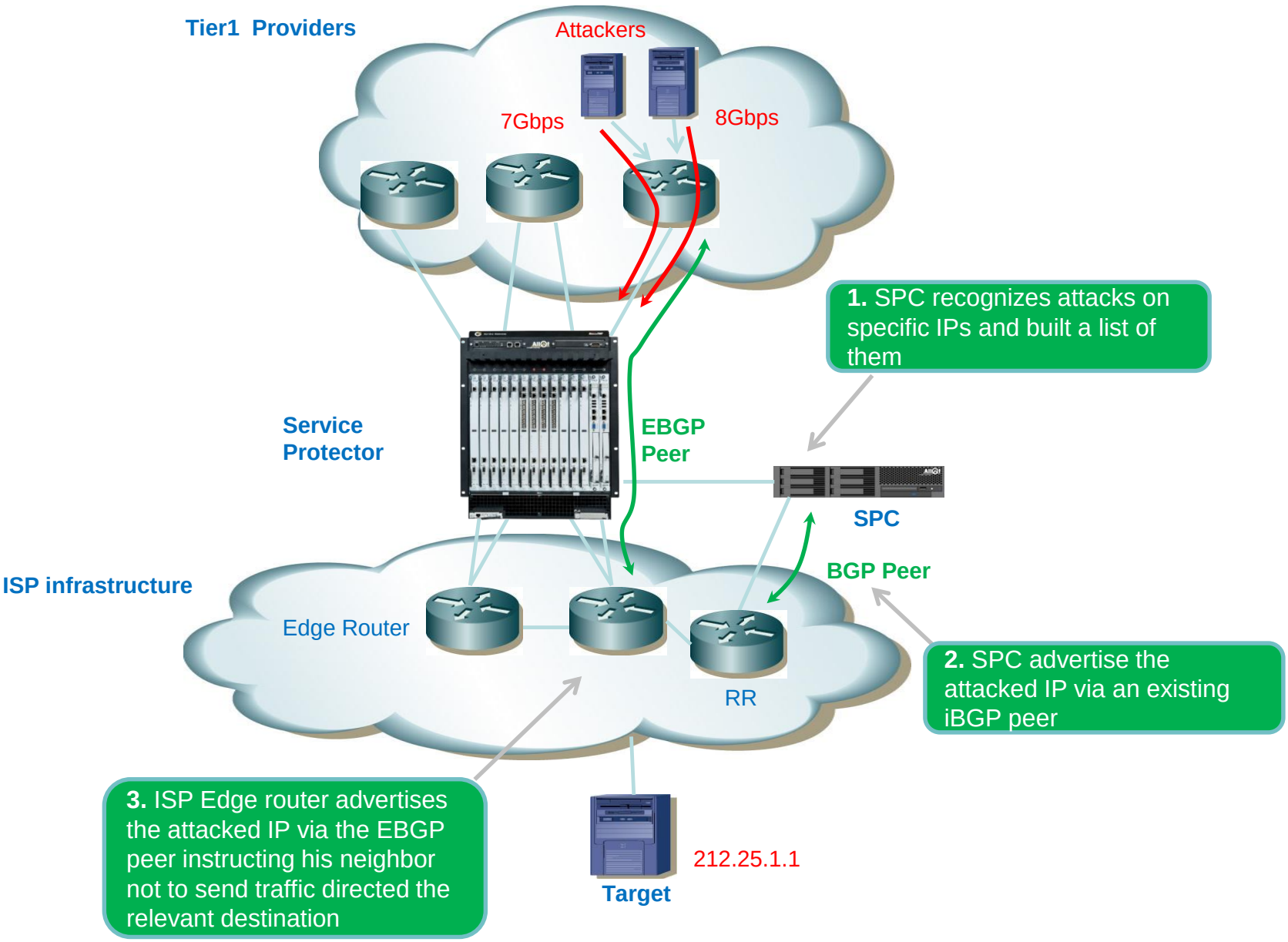
Trend 4 Multi-Vector Attacks

- Security Expertise
- 360˚Security Approach

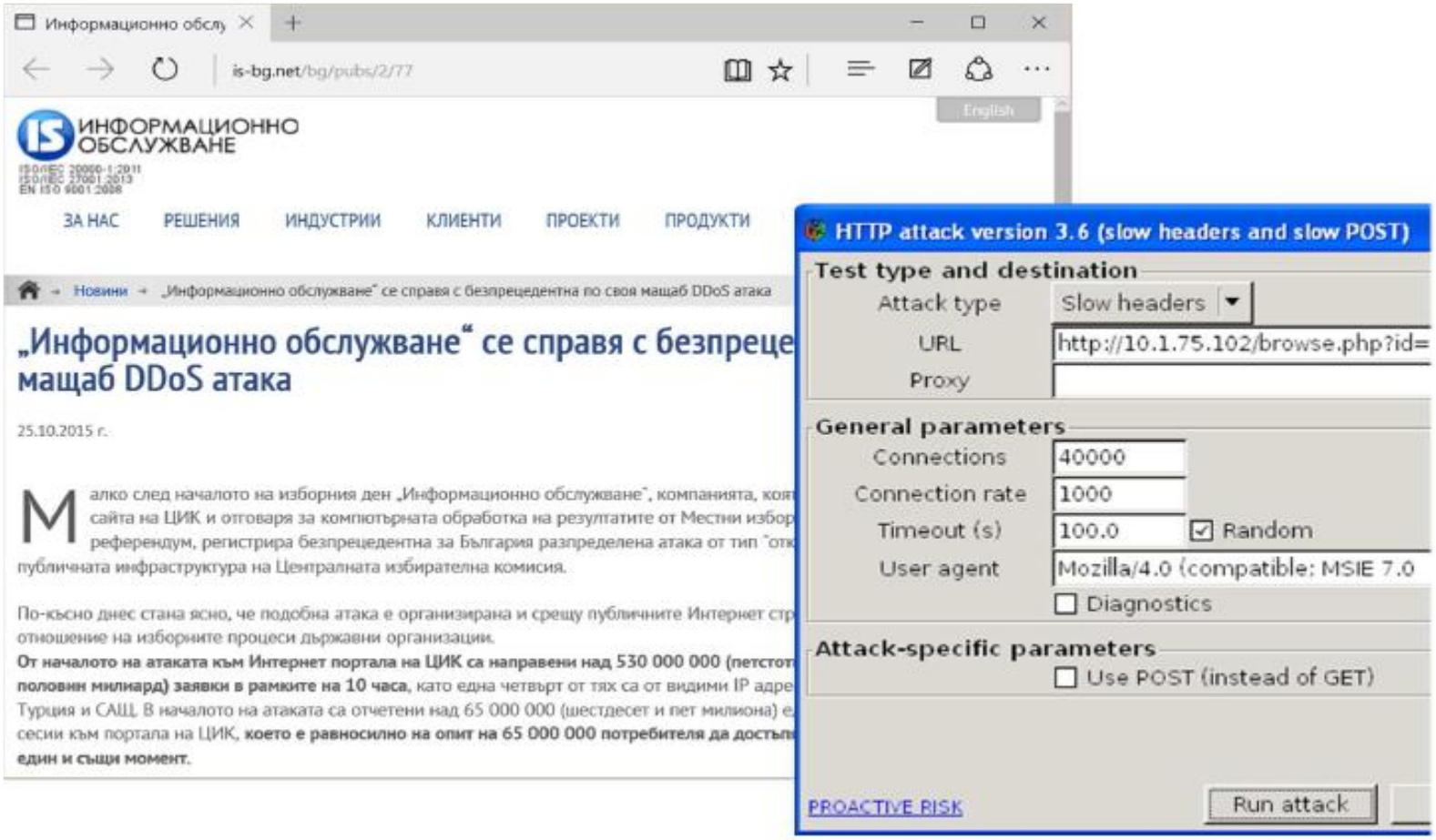
How it Works?


Large DDoS Attacks
ISP Cleaning Center
Data Center
ISP
Firewall
Firewall
Load Balancer
IDS/IPS
IDS/IPS
Target Applications
and Services
Attack Traffic
Legitimate Traffic
Application Layer Attacks

BGP Black Hole Mitigation



Be Aware about the Risk



http://www.is-bg.net/bg/pubs/2/77

Be Aware about the Risk

Хакери са източили от български фирми над 3 млн. евро за седем месеца

Препоръчване (33) G+1 5 От Дневник

Последна промяна в 11:00 на 18 окт 2015, 9929 прочитания, 54 коментара

Фотограф: **Цветелина Белутова**

КАПИТАЛ

по темата

Хакери могат безшумно да командват смартфони чрез Google Now и Siri - 18 окт

Руски хакери са се опитали да откраднат поверителна информация от "Дау Джоунс" - 17 окт

Български компании са били ощетени с над 3 млн. евро от хакери само за последните седем месеца, каза днес по БНТ началникът на отдел "Трансгранична организирана престъпност" в ГДБОП Явор Колев. Той уточни, че това са измамите само чрез прийома Man in the middle.

При него по мейл се изпраща зловреден софтуер като прикачен файл, който заразява компютъра и позволява да се следи кореспонденцията между фирмите. Колев уточни, че само последните две седмица две компании от топ 100 в България са били ощетени, като от едната са откраднати 150 000, а от другата 450 000 евро.

http://www.dnevnik.bg/biznes/finansi/2015/10/18/2631145_hakeri_sa_iztochili_ot_bulgarski_firmi_nad_3_mln_evro/

thank you

For more information, visit
www.intracombg.com

INTRACOM BULGARIA
an Intracom Telecom company

Follow | Link | Watch