Labris NETWORKS

Company Presentation
2014

Labris Networks | Company Profile

Industry	NETWORK SECURITY
Founded	2002
Verticals Served	ALL VERTICAL MARKETS From 5 users to 1 Million users
Area Served	EMEA (20+ countries)
Products	NETWORK SECURITY SOFTWARE UTM APPLIANCES DDOS MITIGATION APPLIANCES

Deloitte. Technology Fast 500 EMEA 2013
WINNER

EAL4+ Common Criteria CERTIFIED

2013	İstanbul Export Office	DDoS Mitigator – Cyber Warfare App.
2012	*10th year*	LBRMNG Series Appliances
2011	Enterprise References in 15 countries	Labris Cloud Security (IBM Smartcloud)
2010		LBRLOG Series Appliances
2009		LBRUTM Series Appliances
2008		
2007		L Series Appliances
2006		
2005	Turkey Sales	Security Gateway Software
2004		
2003	ODTÜ Teknokent R&D Office	
2002	Founded	

Deloitte.
Technology Fast50
Turkey 2012 Winner

EAL4+
Common Criteria
CERTIFIED

TÜBİTAK

Product & Services

Labris UTM

MNG

LOG

Database Updates
Firmware Updates
Technical Support
Network Security Trainings

HARPP
ddos mitigator

Database Updates
Firmware Updates
Technical Support
Specific DDoS Trainings
DDoS Mitigation Consultancy
DDoS CERT Service

Unified Threat Management

Features

- Firewall
- Web Filtering
- Application Control/IM/p2p
- VPN
- AntiSpam, Antivirus,
- IPS (Intrusion Prevention System)
- Traffic Shaping
- High Availability
- Network Visibility
- Logging

Technical Background

Products	Network security software and hardware
Software and Hardware	C, C++, Java, J2EE Web Applications, Reporting Unix Bash, Python Big data, data mining, NoSQL, SSL decryption X86 platforms, embedded platforms(MIPS, RISC, FPGA)
OS	Linux FreeBSD
Network Topologies	Over 2000 different network topologies are built or analyzed. Extensive knowledge about network security.
Threats and Security	Spam, Virus, APT, Scans, DoS/DDoS, L7 Attacks, Web Vulnerabilities
Employees	40 (Electronics, Computer Science, Mathematics)
R&D Investment	3,5 million TL / year (2013)


cyber warfare lab
Product
Information
Research
Algorithms and Method Development
Development for Performance
Performance testing and testing automation
Network Threat Analysis
Malware Analysis
Signature and Database Production
Research Projects
Information Disseminati on

cyber warfare lab

Information Dissemination

- Papers
- Turkish Cyber Security Council and working groups
- Turkish Informatics Assoc. And working groups
- Information Security Assoc. And working groups
- Government Institutions and Exercises

R&D Interests

cyber warfare lab

Network Security

- Managing protocol vulnerabilities
- Sensor Networks
- Anomaly detection and machine learning
- Traffic shaping and routing

High Performance Applications

- Software and Hardware based optimizations
- Research of new methods and creation of research projects

Security Analysis and Testing

- Development of traffic simulation tools
- Development of traffic analysis tools
- Automation of security function testing

Malware, Attack and Vulnerability research

- Malware detection

Sample Security Domain: DoS/DDoS

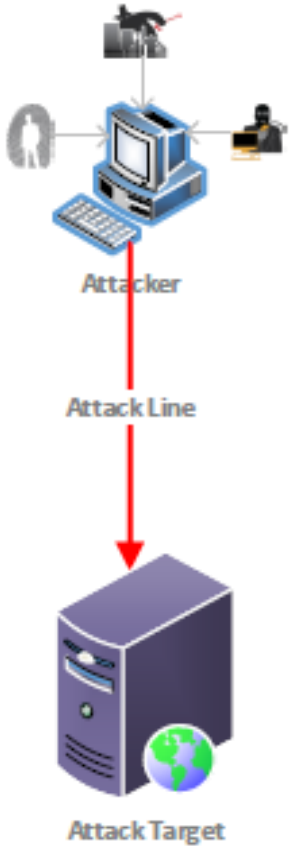
- DoS/DDoS attacks target the «Availability» of C.I.A. triple.

Definition of DoS/DDoS

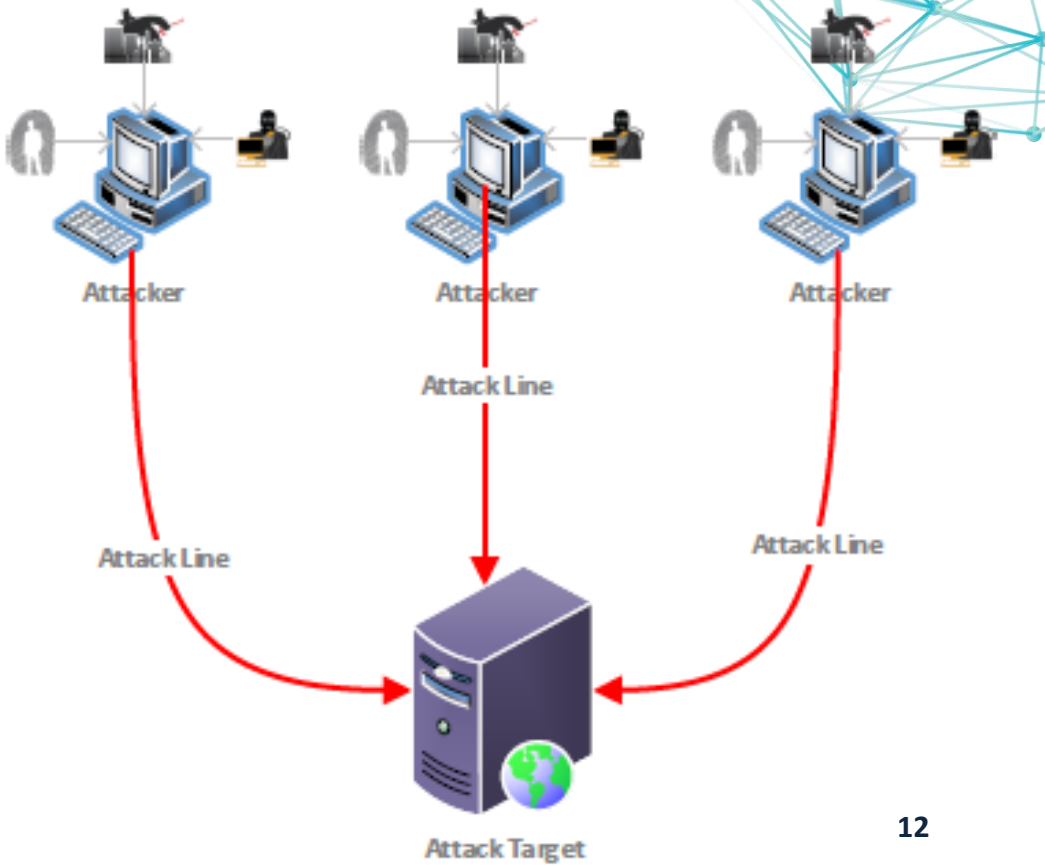
cyber warfare lab

Making the IT services unavailable for its end users and applications

DoS : Denial of Service

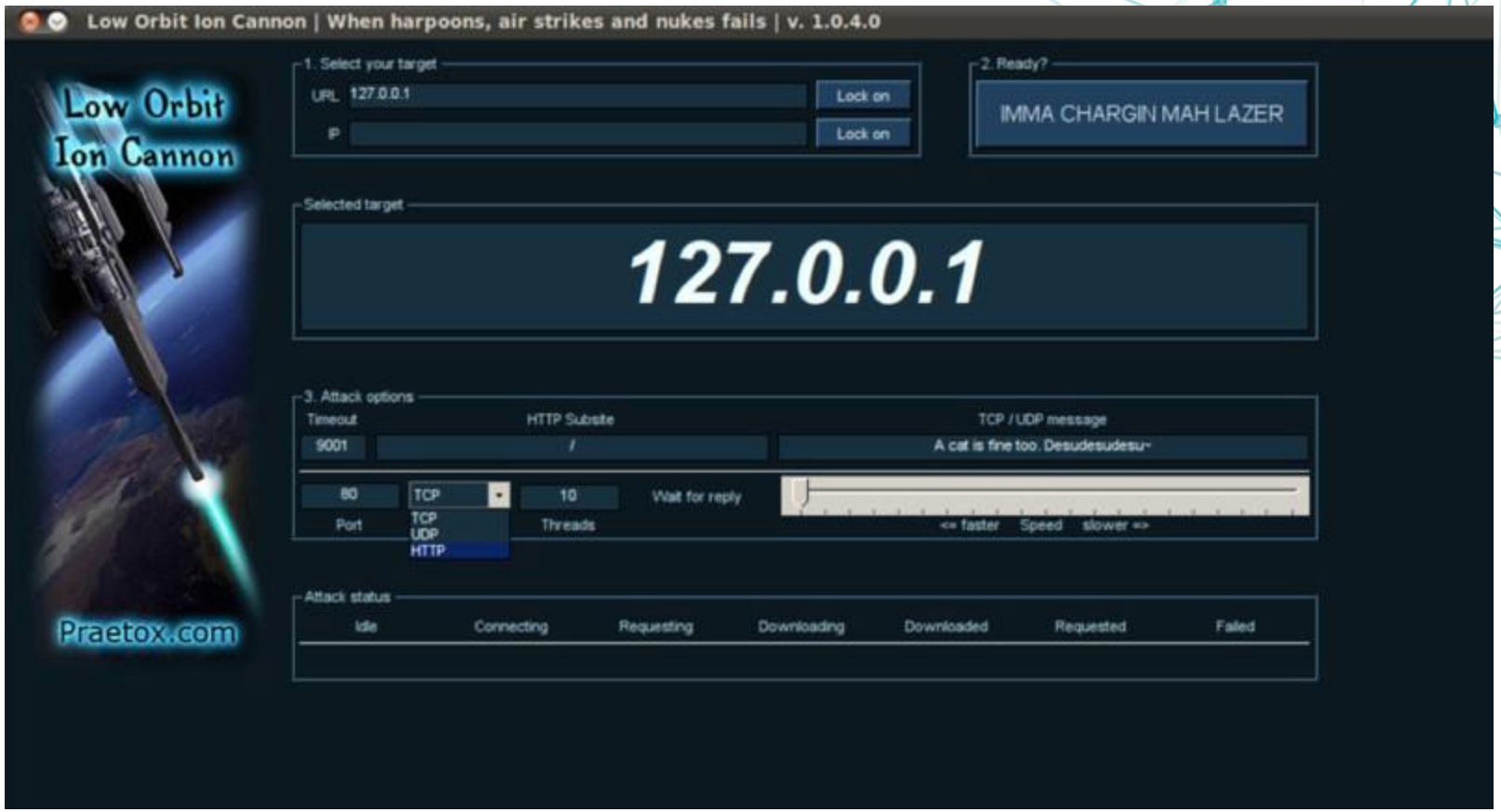


DDoS: Distributed Denial of Service



Less attack knowledge

cyber warfare lab



Main Types of DDoS Attacks

TCP Connection Flood: Aim is to exploit the session capacities of the network systems. Many sessions are opened without closing, trying to stay in the session table to prevent the users from opening a session.

TCP SYN Flood: Sending SYN packets, this attack exploits the session tables, allowed concurrent sessions, bandwidth, also increasing the latency.

UDP Flood: UDP is easy to spoof protocol. This kind of attack targets to occupy the network devices and the bandwidth.

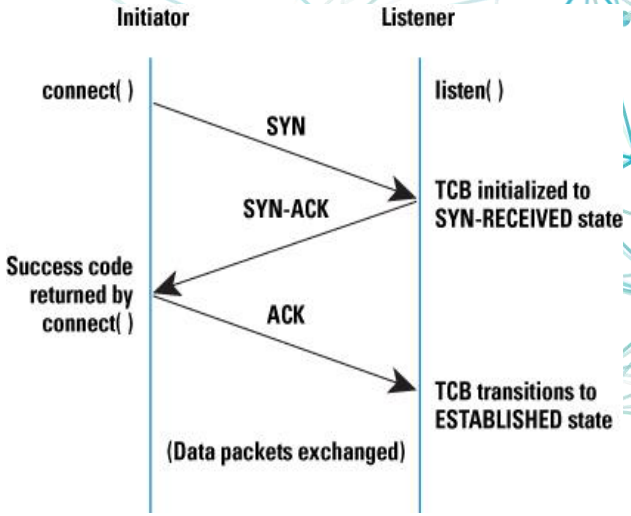
HTTP GET Flood: Targets the webservers' maximum concurrent session limits. Send HTTP GET packets. It can not be spoofed since TCP session is needed.

HTTP POST Flood: Similar to the mechanism of HTTP GET flood, it works with POST packets. It can result in a excessive usage of server sources.

DNS Flood: To make the DNS server out-of-service, the DNS packets are sent. It can be regarded as asymmetric attack since it can be spoofed and can be done with small request packets for larger reply packets.

TCP/IP

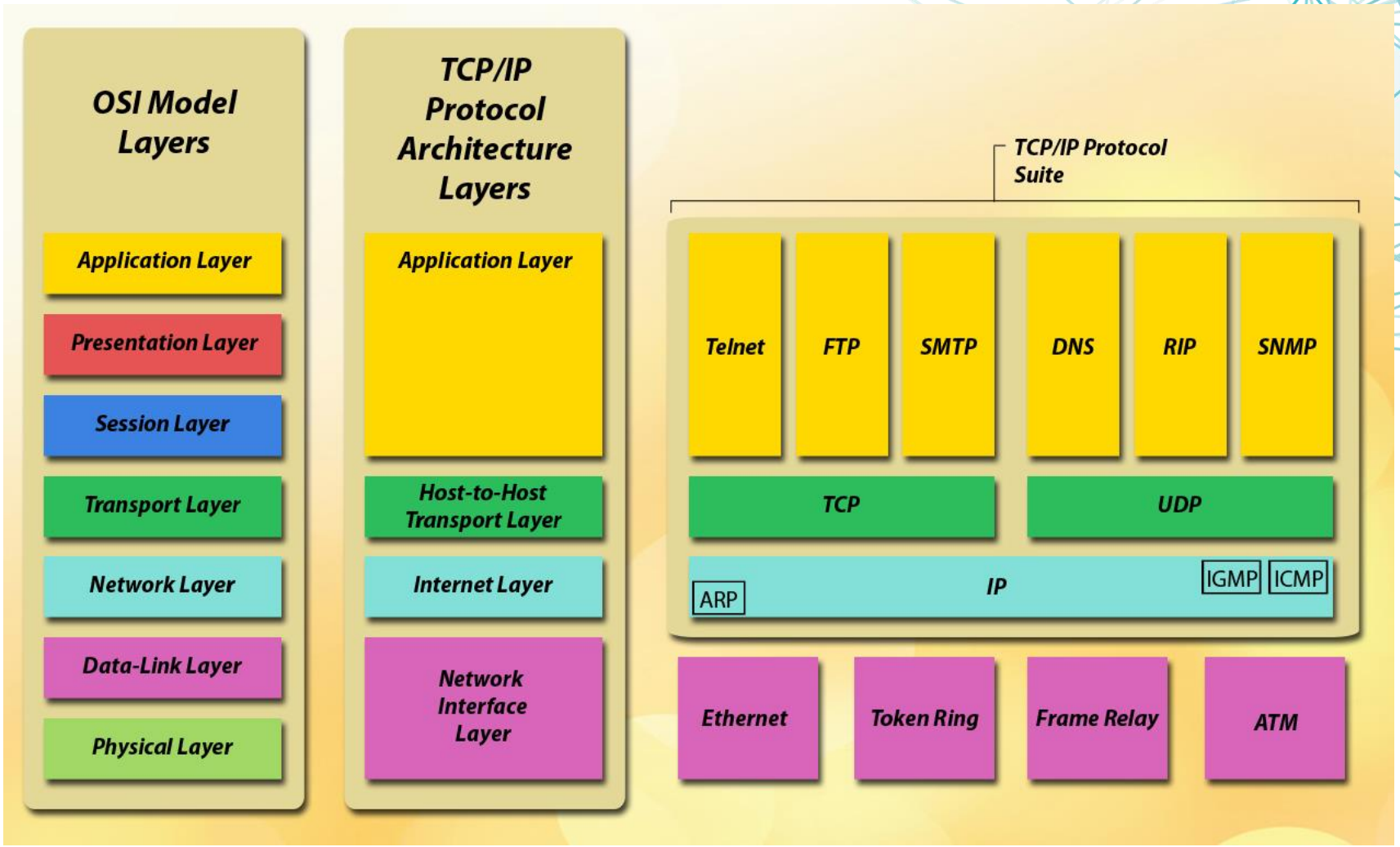
- **TCP (**Transmission Control Protocol**)**
  - 3 way handshake
- **UDP (** User Datagram Protocol **)**
  - No error detection
  - No spoof detection



TCP/IP

* Anonim

TCP/IP

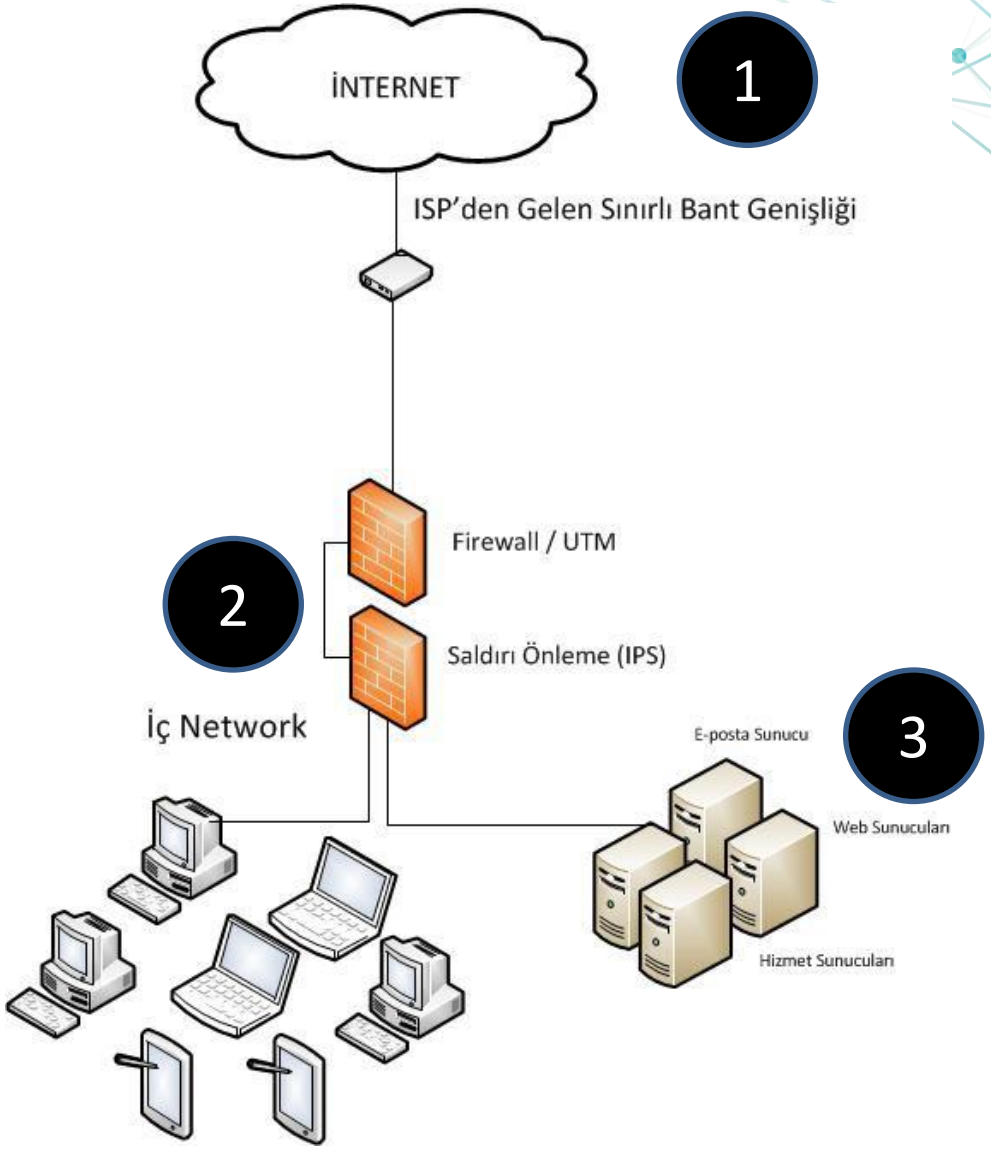


* Anonim

Session Table

tcp	6	57599	ESTABLISHED	src=192.168.0.23	dst=74.125.136.125	sport=59686	dport=5222	packets=4128	bytes=423046
tcp	6	16611	ESTABLISHED	src=192.168.2.130	dst=95.9.177.199	sport=37378	dport=993	packets=99	bytes=10081
tcp	6	29454	ESTABLISHED	src=192.168.2.1	dst=192.168.2.130	sport=8080	dport=54775	packets=1	bytes=1500
tcp	6	16613	ESTABLISHED	src=192.168.2.130	dst=95.9.177.199	sport=37395	dport=993	packets=19	bytes=2394
tcp	6	6933	ESTABLISHED	src=192.168.2.182	dst=173.194.70.125	sport=41610	dport=5222	packets=28	bytes=3711
tcp	6	34135	ESTABLISHED	src=192.168.2.139	dst=157.55.236.132	sport=64029	dport=443	packets=14	bytes=2580
tcp	6	29200	ESTABLISHED	src=192.168.2.174	dst=95.9.177.199	sport=43955	dport=993	packets=1316	bytes=131132
tcp	6	31816	ESTABLISHED	src=192.168.0.170	dst=91.93.128.195	sport=52794	dport=5222	packets=415	bytes=40632
tcp	6	30566	ESTABLISHED	src=192.168.0.153	dst=23.51.112.60	sport=56486	dport=443	packets=7	bytes=727
tcp	6	34927	ESTABLISHED	src=192.168.2.139	dst=74.125.136.125	sport=63966	dport=5222	packets=92	bytes=7268
tcp	6	13293	ESTABLISHED	src=192.168.2.142	dst=23.52.48.60	sport=49446	dport=443	packets=14	bytes=1276
tcp	6	39409	ESTABLISHED	src=192.168.0.152	dst=74.125.136.16	sport=60192	dport=993	packets=39451	bytes=2300577
tcp	6	57598	ESTABLISHED	src=192.168.0.23	dst=91.93.128.195	sport=41754	dport=5222	packets=760	bytes=158639
tcp	6	13291	ESTABLISHED	src=192.168.2.142	dst=23.52.48.60	sport=49442	dport=443	packets=16	bytes=1368
tcp	6	39397	ESTABLISHED	src=192.168.0.152	dst=95.9.177.199	sport=52329	dport=993	packets=47	bytes=4903
tcp	6	57599	ESTABLISHED	src=172.16.1.2	dst=204.89.241.6	sport=50714	dport=80	packets=45	bytes=2466
tcp	6	36989	ESTABLISHED	src=192.168.2.155	dst=91.190.216.52	sport=50078	dport=12350	packets=131	bytes=6344
tcp	6	16151	ESTABLISHED	src=192.168.2.130	dst=95.9.177.199	sport=37377	dport=993	packets=40	bytes=4611

Main Problems in DDoS Attacks



Future DDOS Trends

Today:
About 30 types of attacks

Future:
APT characteristics in DDOS attacks

Shift to L7

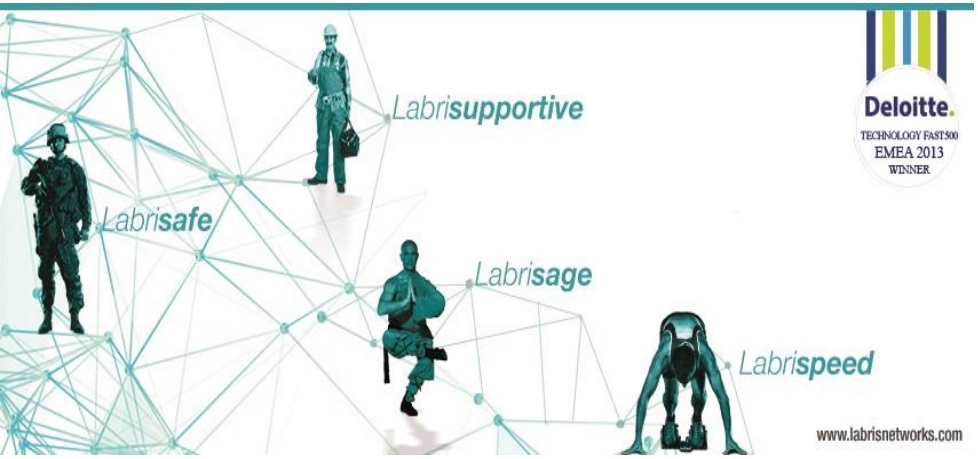
High Loads of UDP floods

Real User Mimicking

Mobile Driven Attacks

IoT Attacks

R&D


Labrisupportive
Labrisafe
Labrisage
Labrispeed
Deloitte.
TECHNOLOGY FAST 500
EMEA 2013
WINNER
www.labrisnetworks.com

Agile Manifesto

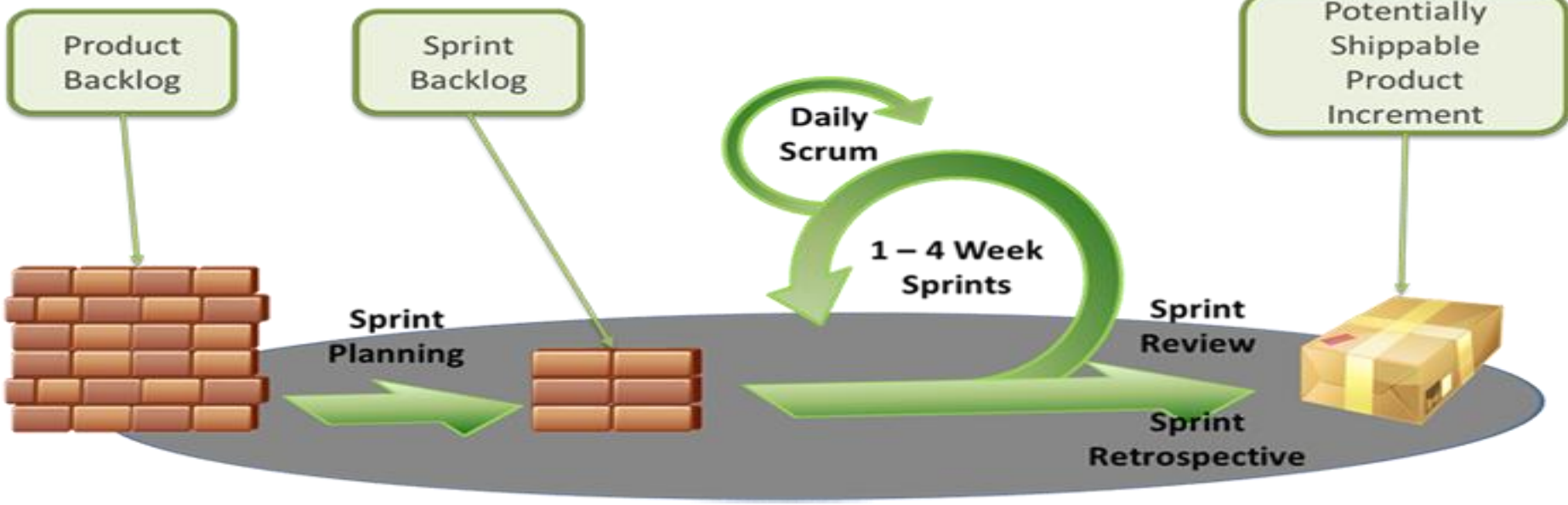
Individuals and interactions over processes and tools

Working software over comprehensive documentation

Customer collaboration over contract negotiation

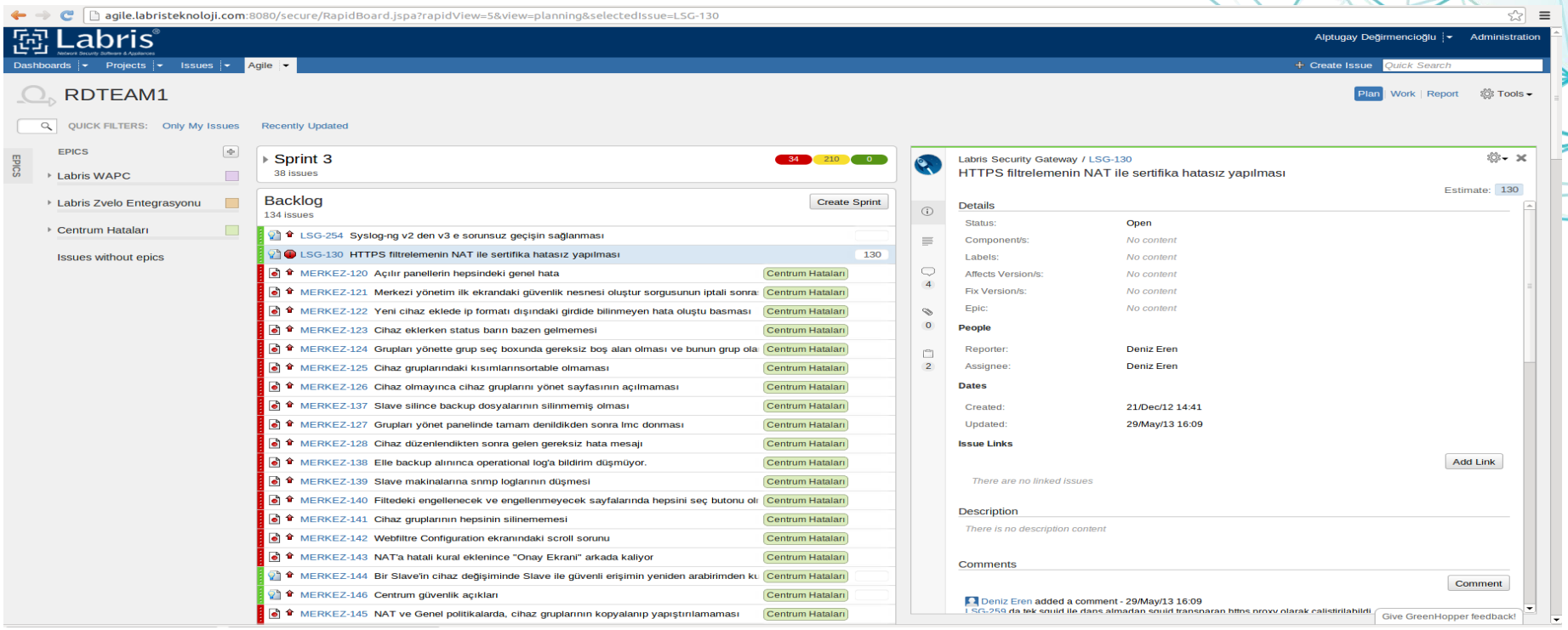
Responding to change over following a plan

Scrum Cycle

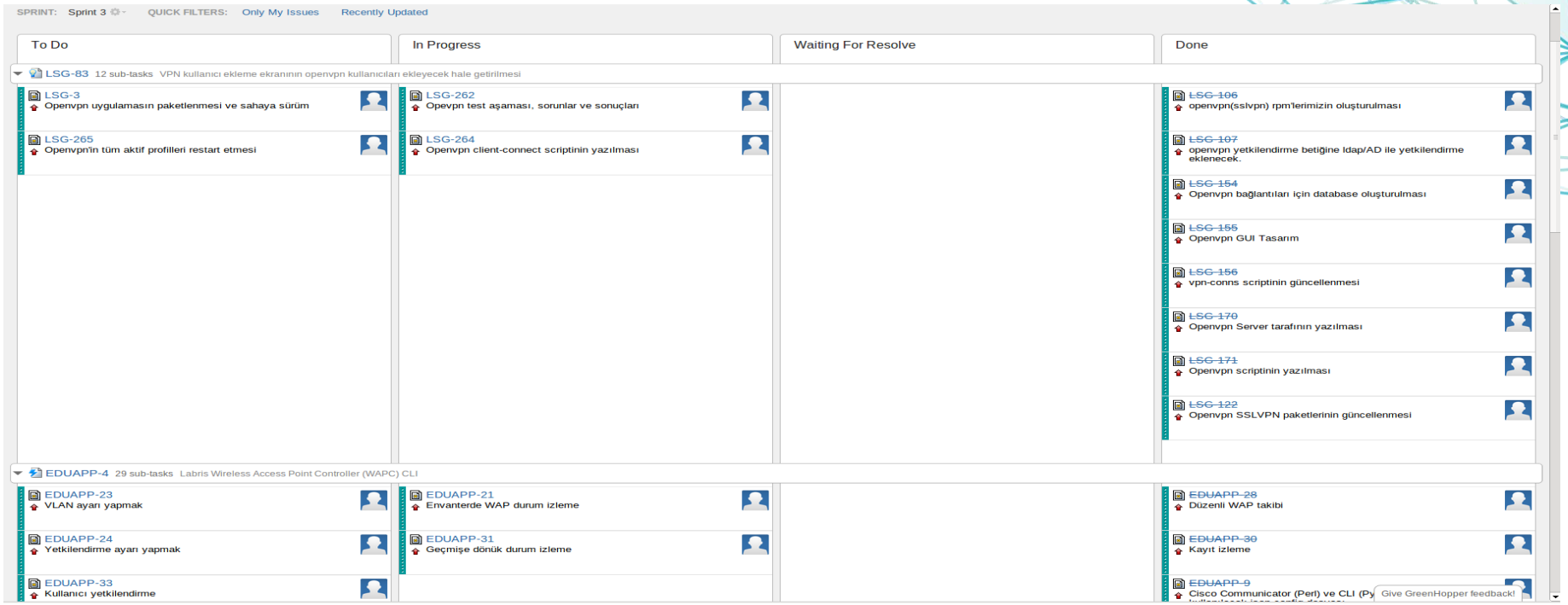

Product Backlog
Sprint Backlog
Daily Scrum
1 – 4 Week Sprints
Potentially Shippable Product Increment
Sprint Planning
Sprint Review
Sprint Retrospective

Scrum Team

Product Backlog

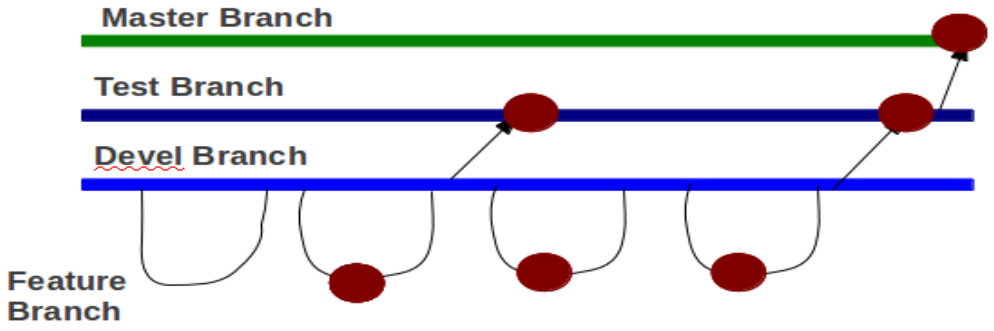


Scrum Board


SPRINT: Sprint 3
QUICK FILTERS: Only My Issues Recently Updated
To Do
In Progress
Waiting For Resolve
Done
LSG-83 12 sub-tasks VPN kullanıcı ekleme ekranının openvpn kullanıcıları ekleyecek hale getirilmesi
LSG-3 Openvpn uygulamasın paketlenmesi ve sahaya sürüm
LSG-265 Openvpn'in tüm aktif profilleri restart etmesi
LSG-262 Opevpn test aşaması, sorunlar ve sonuçları
LSG-264 Openvpn client-connect scriptinin yazılması
LSG-106 openvpn(sslvpn) rpm'lerimizin oluşturulması
LSG-107 openvpn yetkilendirme betiğine ldap/AD ile yetkilendirme eklenecek.
LSG-154 Openvpn bağlantıları için database oluşturulması
LSG-155 Openvpn GUI Tasarım
LSG-156 vpn-conns scriptinin güncellenmesi
LSG-170 Openvpn Server tarafının yazılması
LSG-171 Openvpn scriptinin yazılması
LSG-122 Openvpn SSLVPN paketlerinin güncellenmesi
EDUAPP-4 29 sub-tasks Labris Wireless Access Point Controller (WAPC) CLI
EDUAPP-23 VLAN ayarı yapmak
EDUAPP-24 Yetkilendirme ayarı yapmak
EDUAPP-33 Kullanıcı yetkilendirme
EDUAPP-21 Envanterde WAP durum izleme
EDUAPP-31 Geçmişe dönük durum izleme
EDUAPP-28 Düzenli WAP takibi
EDUAPP-30 Kayıt izleme
EDUAPP-9
Give GreenHopper feedback!

Revision Control

- Before work on an issue is started, a feature branch is created from devel branch.
- When the work on an issue is completed (meets the criteria for definition of done) the code is merged into the devel branch.
- Prior to a major release the code on devel branch is merged into the test branch and sent to the test team for extensive testing.
- When the testing is completed successfully the code is merged into the master branch and ready to be shipped.



References

Having operations in a rapidly growing global network of more than 20 countries, Labris® products protect enterprises, brands, government entities, service providers and mission-critical infrastructures.

Military

Turkish Air Force
Turkish Naval Forces
Turkish Land Forces
Ministry of National Defence
Turkish Military Academies
General Command Of Mapping
Military Hospital Networks

Government

Turkish Prime Ministry
Ministry of T. and Communications
Ministry of Health Hospitals
Ministry of Interior (911 Infra., Police)
Ministry of Finance

Education

Ministry of Education FATİH Project PoC
Turkish Universities
Kyrgyzstan Manas University
Turkmen Polytechnical University

Private

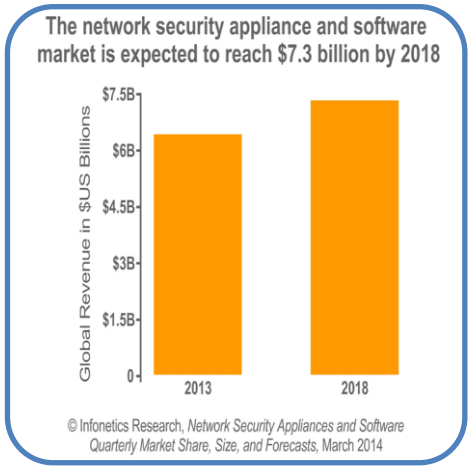
SHOW TV, Ajans Press
Global Construction Companies/Contractors (Renaissance, IC, Yuksel)
PALMALI Group
Bureau Veritas, TR

Security (Growth & Threats)

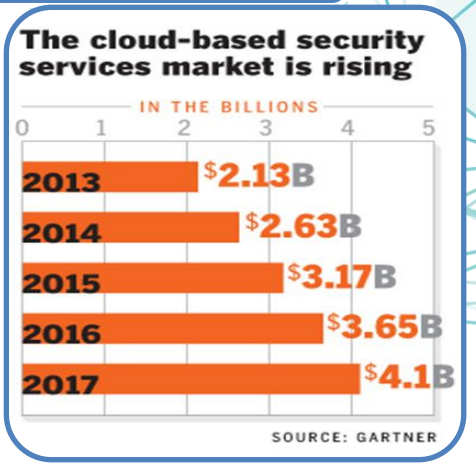
WORLDWIDE SECURITY MARKET GROWTH

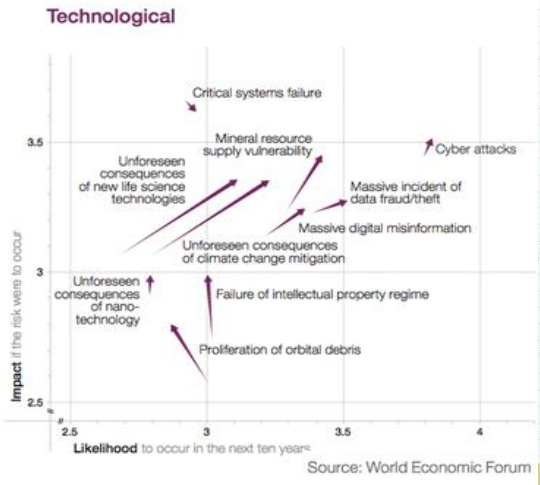
- The worldwide security technology and services market is forecast to reach **$67.2** billion in 2013, **up 8.7** percent **from $61.8** billion in 2012.
- **The market is expected to grow to more than $86 billion in 2016**. (Gartner, Inc.)

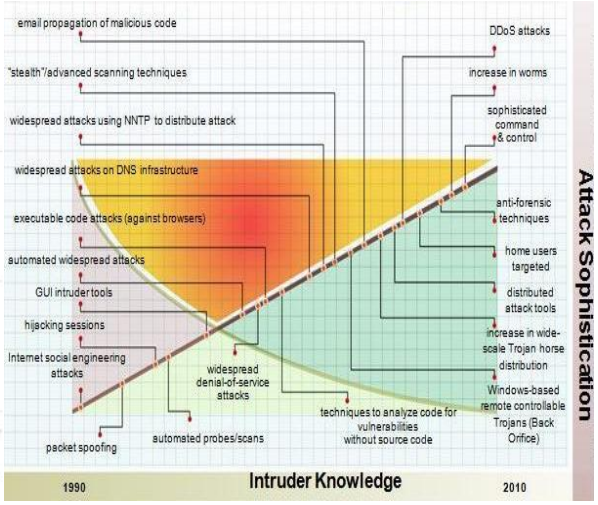
NETWORK SECURITY MARKET GROWTH

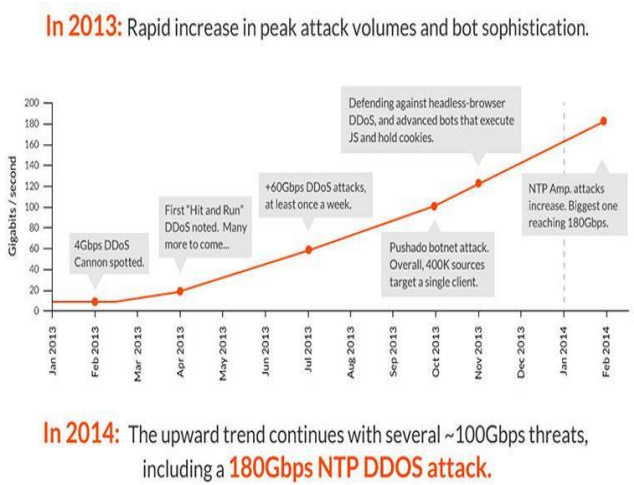


CLOUD-BASED SECURITY MARKET GROWTH









Technical Qualification

Labris NETWORKS

Get in touch..

Labris Networks R&D Headquarters
T: +90 312 210 1491
info@labrisnetworks.com

Eastern Europe Sales Offices – Prague&Warsaw
T: +420 220 994 422
ee-sales@labrisnetworks.com

UK Sales Office
T: +44 7703 503242
eu-sales@labrisnetworks.com