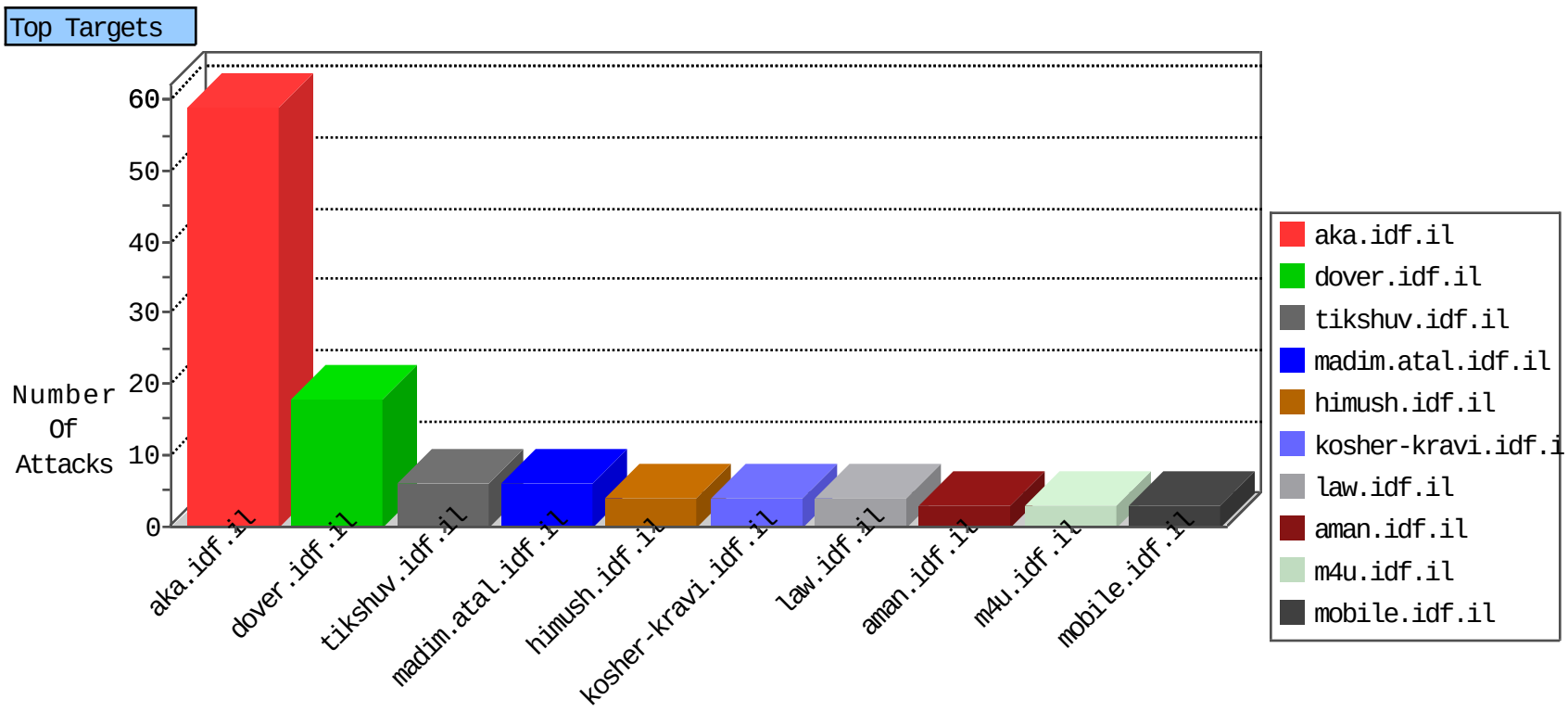
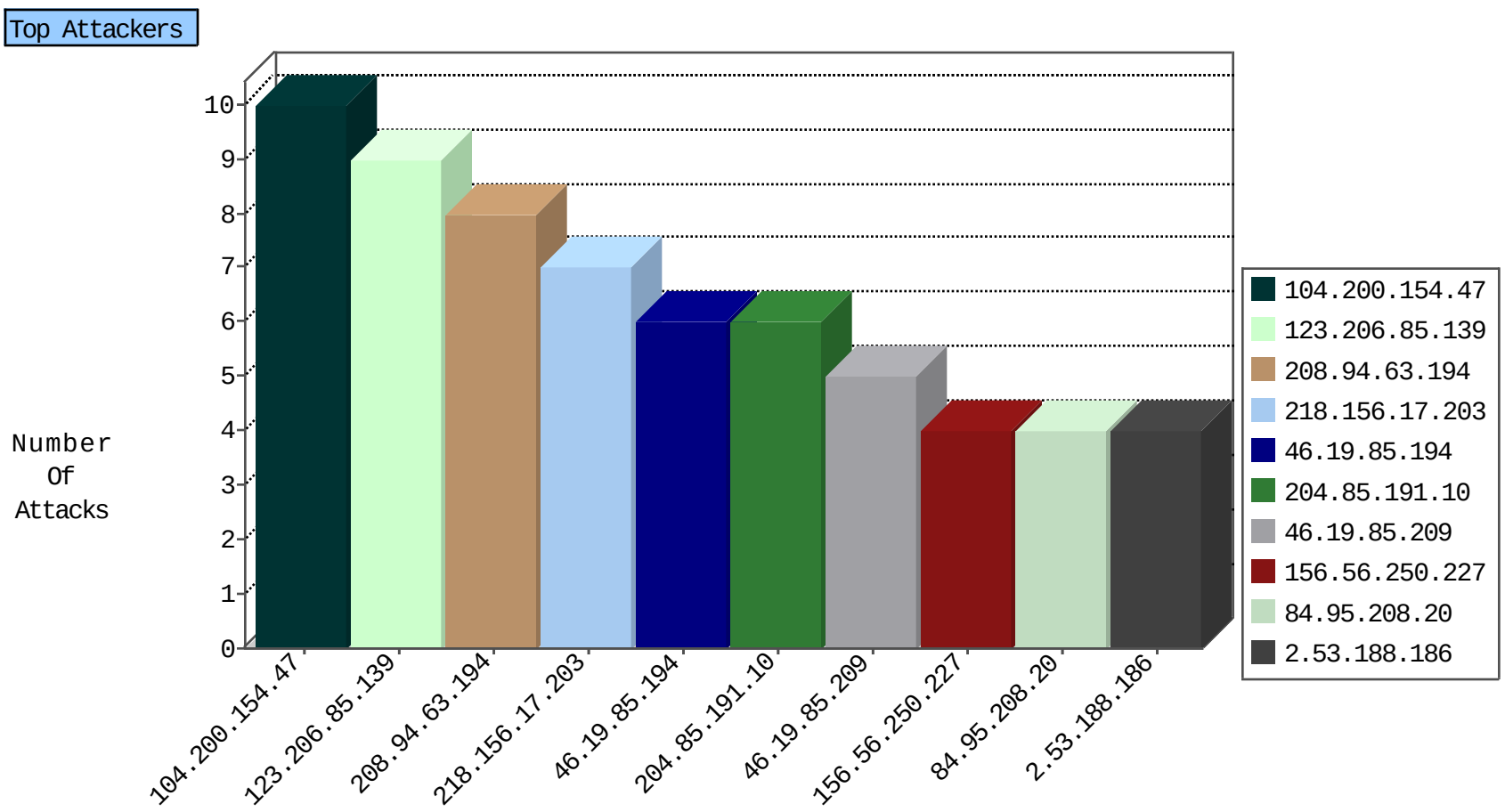
09-17-2016-05:04:08 to 09-17-2016-06:04:08

IDF Under Attack
Daily Report





09-17-2016-05:04:08 to 09-17-2016-06:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	8
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.221	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	2
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.226	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
218.156.17.203	Korea, Republic of	147.237.72.217	e.idf.il	JLM_Purple_Con_Limit_Http	drop	1
192.33.90.69	Switzerland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
218.156.17.203	Korea, Republic of	147.237.77.19	law-forum.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-17-2016-05:04:08 to 09-17-2016-06:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.68.105	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-17-2016-05:04:08 to 09-17-2016-06:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.255.90.133	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
212.116.72.226	147.237.0.200	Sweden	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
202.155.58.28	147.237.72.217	Indonesia	e.idf.il	ET SCAN NMAP -sS window 1024	1
201.73.83.242	147.237.76.30	Brazil	himush.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
104.245.99.228	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
5.255.90.133	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
220.162.98.24	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.116.72.226	147.237.0.200	Sweden	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
201.73.83.242	147.237.76.30	Brazil	himush.idf.il	ET SCAN NMAP -sS window 2048	1
201.73.83.242	147.237.76.30	Brazil	himush.idf.il	ET SCAN NMAP -f -sS	1
123.206.85.139	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
104.245.99.228	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1

09-17-2016-05:04:08 to 09-17-2016-06:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
104.200.154.47	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	10
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.209	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.64.169	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.24.149	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
84.108.70.15	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
218.156.17.203	Korea, Republic of	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
139.162.37.147	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.206.85.139	China	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
84.108.232.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
1.144.96.4	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
218.156.17.203	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
177.69.235.90	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
106.186.113.169	Japan	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
218.156.17.203	Korea, Republic of	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
123.206.85.139	China	147.237.0.33	idf.il	drop		drop	1
84.108.232.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.29.182.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.247.223	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
123.30.135.177	Vietnam	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
218.156.17.203	Korea, Republic of	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
123.206.85.139	China	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
89.248.167.131	Netherlands	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.247.231	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.206.85.139	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
218.156.17.203	Korea, Republic of	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
139.162.37.147	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
95.90.228.52	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.252	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
123.206.85.139	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-17-2016-05:04:08 to 09-17-2016-06:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.188.186	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	4
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	2
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/piwik.php	Block	1
84.108.70.15	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-9070-he/atal.aspx	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1

09-17-2016-05:04:08 to 09-17-2016-06:04:08