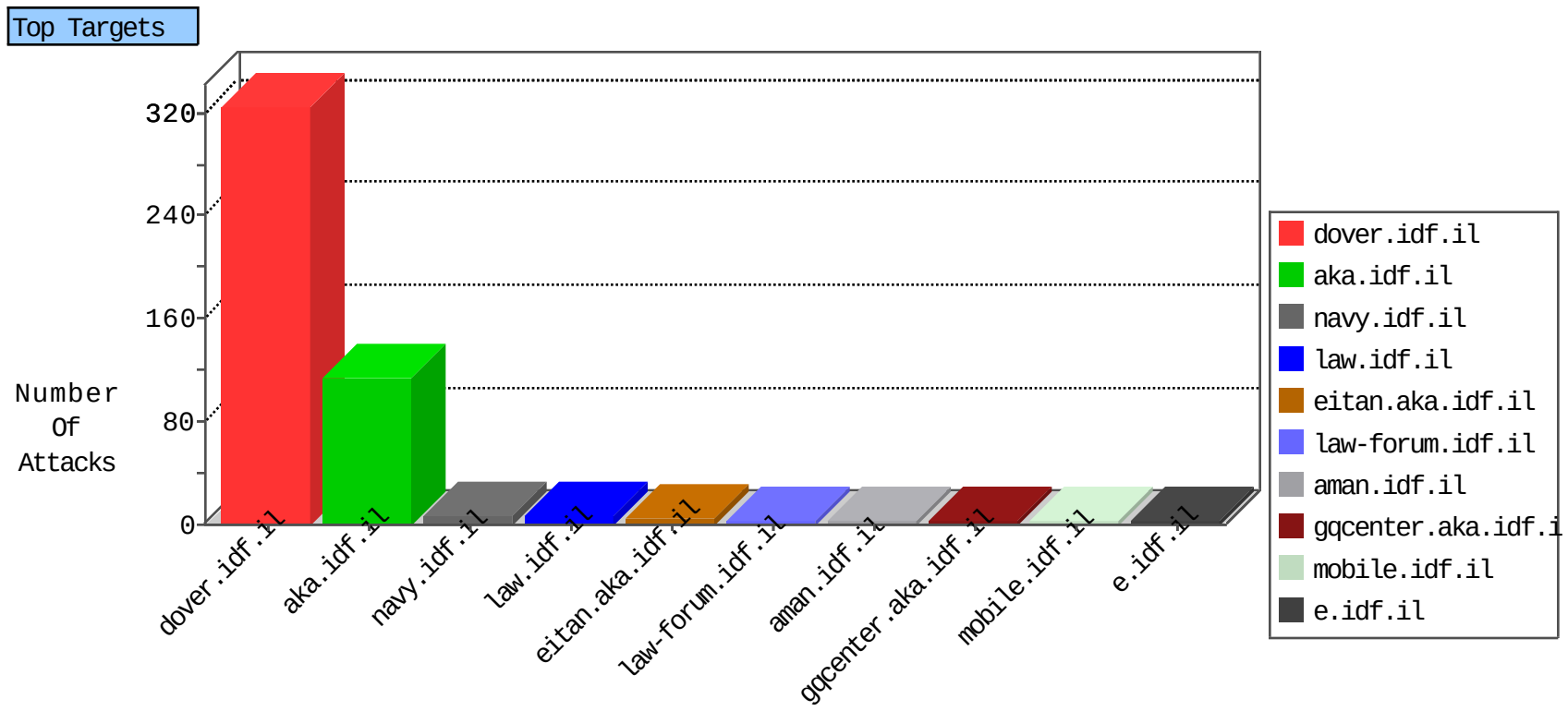
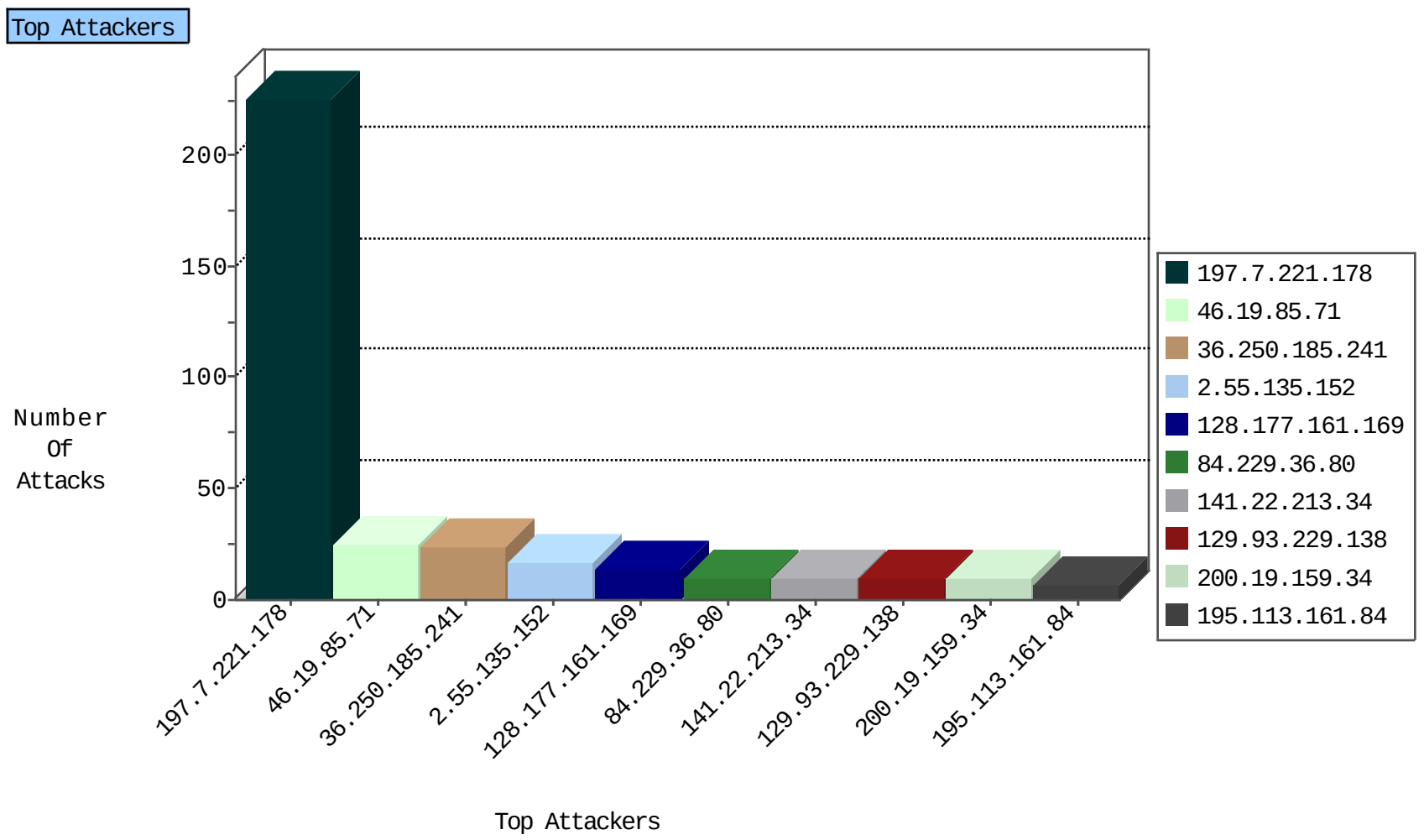
09-18-2016-05:04:04 to 09-18-2016-06:04:04

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-18-2016-05:04:04 to 09-18-2016-06:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	10
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	10
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	10
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	7
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.84	Czech Republic	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	2
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.133.224.147	United States	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
130.217.77.4	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.194.252.8	Australia	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.113	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
218.93.206.21	China	147.237.0.34	tikshuv.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
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-18-2016-05:04:04 to 09-18-2016-06:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.209	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-18-2016-05:04:04 to 09-18-2016-06:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.129.148.230	147.237.76.86	Latvia	navy.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
109.236.80.12	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.80.12	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
104.232.98.3	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 4096	1
104.232.98.3	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -f -sS	1
91.201.236.50	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
84.93.84.77	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	1
31.24.228.20	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
216.81.230.167	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
113.85.79.187	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.236.80.12	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
109.236.80.12	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.3	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 2048	1
91.201.236.50	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.77.19	Ukraine	law-forum.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.185.0.148	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1

09-18-2016-05:04:04 to 09-18-2016-06:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	217
128.177.161.169	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
84.229.36.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.135.152	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
197.7.221.178	Tunisia	147.237.77.216	dover.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	5
2.55.135.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
199.30.25.76	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.75.145	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.55.135.152	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.55.135.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.179.2.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
84.229.36.80	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
139.162.37.147	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.26.147.247	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
108.26.193.39	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.249	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
212.179.20.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.20	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.21	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
188.120.154.68	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
139.162.37.147	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.120.244.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.147.247	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
189.249.145.182	Mexico	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
85.250.214.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.246	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.55.135.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

09-18-2016-05:04:04 to 09-18-2016-06:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
36.250.185.241	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 36.250.185.241	Block	17
36.250.185.241	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	3
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.183	Block	2
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
36.250.185.241	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
217.69.133.220	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
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
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmiluim/templates/home.asp_blank	Block	1
109.253.157.135	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
66.249.64.184	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
77.138.22.198	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
157.55.39.57	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/apple-app-site-association	Block	1
216.244.66.236	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1

09-18-2016-05:04:04 to 09-18-2016-06:04:04