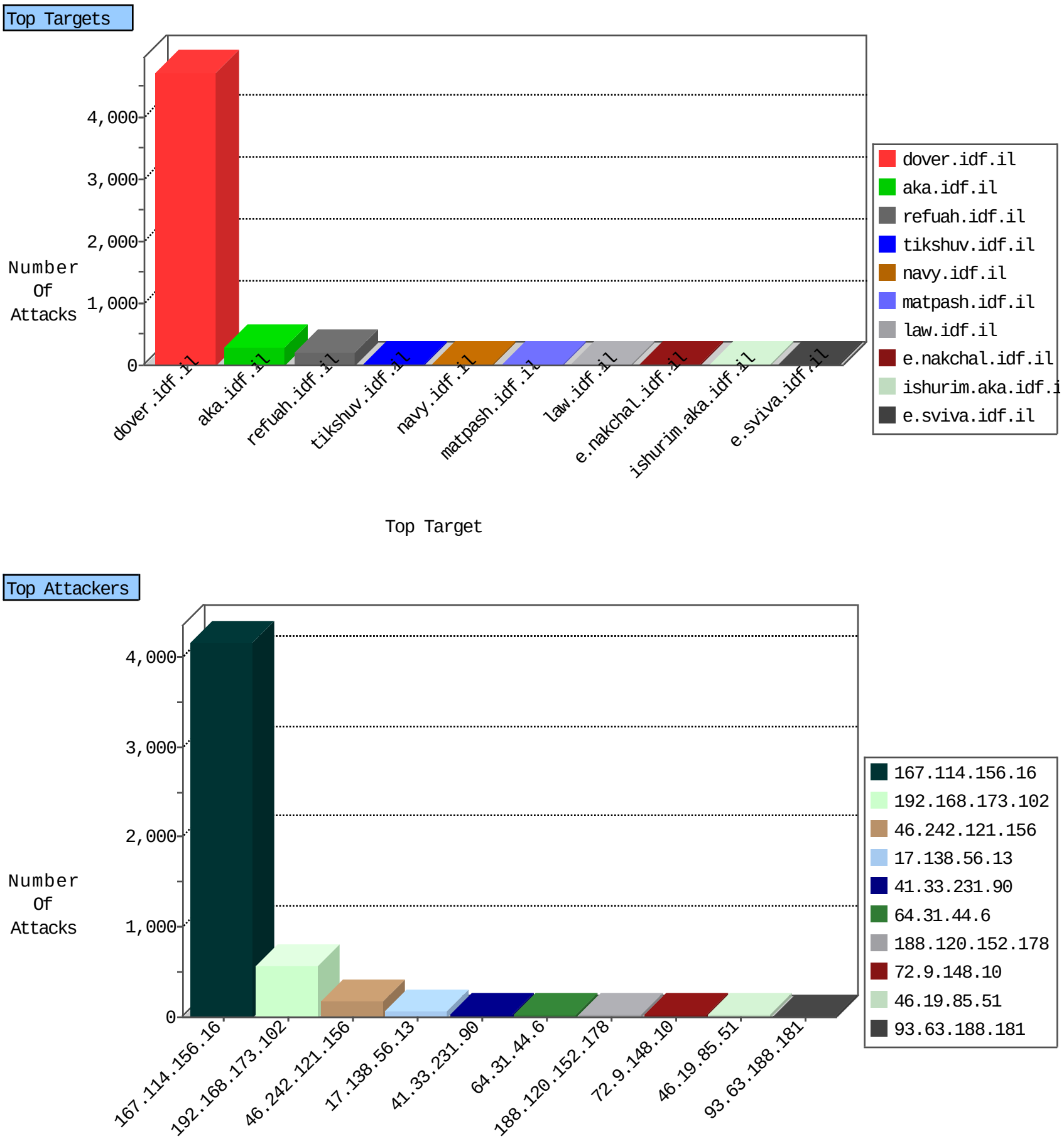
04-09-2016-03:04:03 to 04-09-2016-04:04:03

IDF Under Attack
Daily Report



04-09-2016-03:04:03 to 04-09-2016-04:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4166
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	9
46.242.121.156	Russian Federation	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
120.132.50.135	China	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
192.3.220.210	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
192.3.220.210	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
46.242.121.156	Russian Federation	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	1
52.53.222.9	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1

04-09-2016-03:04:03 to 04-09-2016-04:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
64.31.44.6	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
106.120.173.85	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
61.135.189.99	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
64.31.44.6	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
93.63.188.181	Italy	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
74.208.133.60	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
87.242.112.35	Russian Federation	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
93.63.188.181	Italy	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
70.89.127.77	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
144.76.61.21	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	3
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
70.89.127.78	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-09-2016-03:04:03 to 04-09-2016-04:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
64.31.44.6	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	14
70.89.127.77	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	9
93.63.188.181	147.237.76.42	Italy	refuah.idf.il	SQL Injection - Select From	8
74.208.133.60	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
87.242.112.35	147.237.72.166	Russian Federation	aka.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
70.89.127.78	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	3
66.249.78.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
104.128.144.131	147.237.77.243	Canada	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
93.183.201.2	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
80.82.79.104	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
189.7.174.124	147.237.0.17	Brazil	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.183.201.2	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

04-09-2016-03:04:03 to 04-09-2016-04:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	363
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	205
46.242.121.156	Russian Federation	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	174
17.138.56.13	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	57
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
188.120.152.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
172.56.42.129	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
95.221.200.236	Russian Federation	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.51	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.51	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
123.126.113.109	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
193.9.245.64	Russian Federation	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
130.203.136.75	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
37.205.0.49	Turkey	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
141.0.14.252	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.6.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.242.121.156	Russian Federation	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
107.23.193.247	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
66.87.66.185	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
118.173.140.248	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
2.54.144.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
106.184.3.122	Japan	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.74	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.59.54.182	China	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
77.100.110.170	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.219	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.186.113.132	Japan	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.3.147.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.53.40.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
87.69.255.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
61.135.189.99	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.62.53.168	Russian Federation	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.220	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.53.40.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.90	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
104.148.44.149	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
66.240.219.146	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.74	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
120.132.84.59	China	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

04-09-2016-03:04:03 to 04-09-2016-04:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
78.46.23.198	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
173.252.122.120	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
91.200.12.58	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
31.13.98.115	Ireland	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
198.58.96.215	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
66.249.69.10	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
91.200.12.58	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
37.26.149.158	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
203.127.58.232	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/prisha	Block	1
124.106.155.106	Philippines	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.240.219.146	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/modiin/default.aspx	Block	1
68.180.230.108	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1100-he/nakhal.aspx	Block	1
124.106.155.106	Philippines	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.64.119	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1

04-09-2016-03:04:03 to 04-09-2016-04:04:03