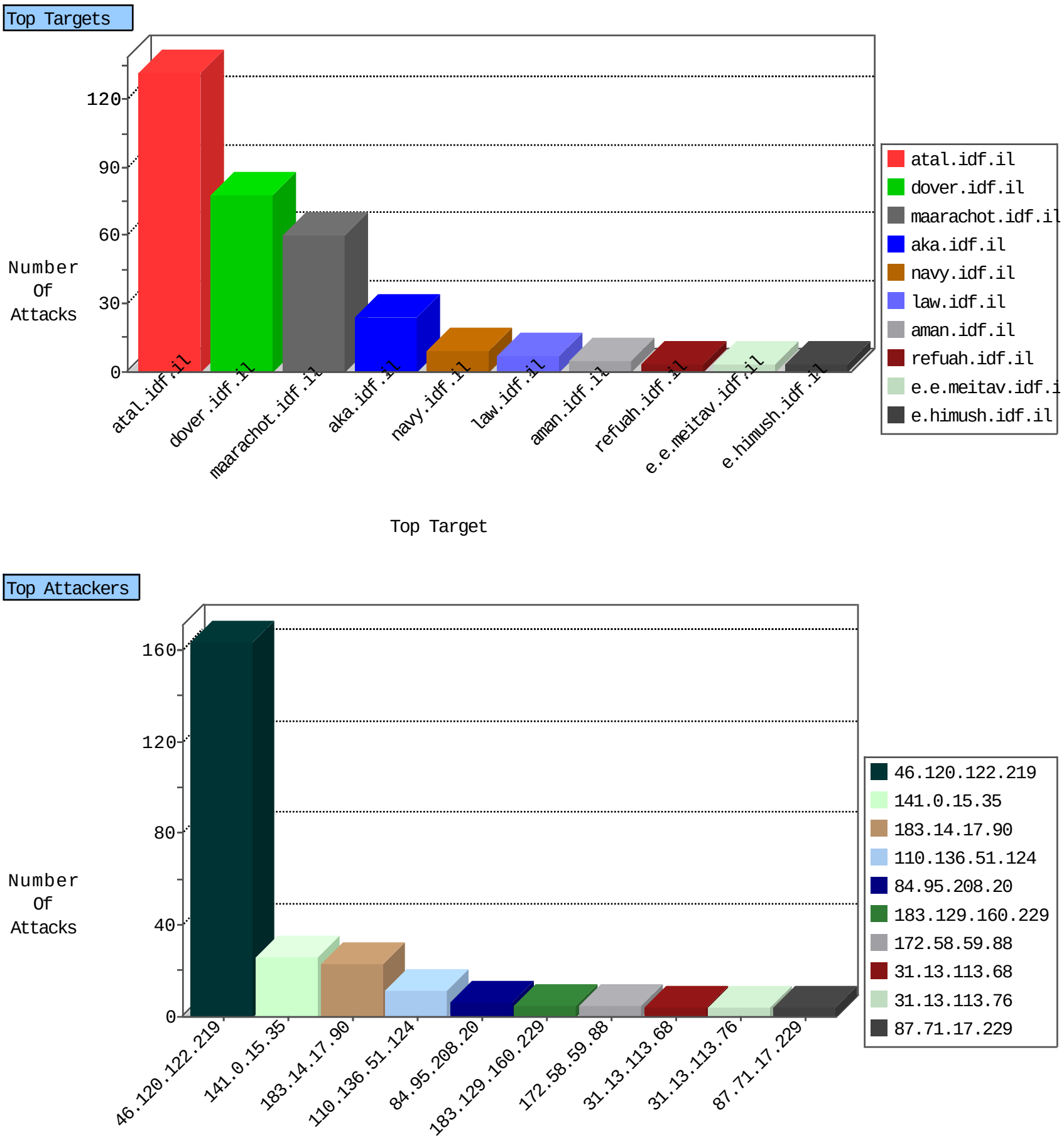
09-30-2016-05:04:03 to 09-30-2016-06:04:03

IDF Under Attack Daily Report



09-30-2016-05:04:03 to 09-30-2016-06:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.128.43.98	Switzerland	147.237.76.197	e.himush.idf.il	Black List	drop	1
38.229.1.13	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
71.6.158.166	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
173.0.52.105	United States	147.237.76.177	ncore.idf.il	Black List	drop	1

09-30-2016-05:04:03 to 09-30-2016-06:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-30-2016-05:04:03 to 09-30-2016-06:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.233	Israel	atal.idf.il	Xenu Link Sleuth User Agent	118
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	31
14.182.97.71	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
116.105.52.150	147.237.8.27	Vietnam	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
46.120.122.219	147.237.77.234	Israel	halag.idf.il	Xenu Link Sleuth User Agent	1
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	1
46.120.122.219	147.237.76.86	Israel	navy.idf.il	Xenu Link Sleuth User Agent	1
188.136.237.251	147.237.8.46	Iran, Islamic Republic of	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
46.120.122.219	147.237.0.17	Israel	m.my-kosher-kravi.idf.il	Xenu Link Sleuth User Agent	1
188.136.237.251	147.237.8.46	Iran, Islamic Republic of	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
163.172.169.150	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
123.59.173.17	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
86.125.216.254	147.237.77.170	Romania	maarachot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.172.91.20	147.237.0.33	Ukraine	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.120.122.219	147.237.76.42	Israel	refuah.idf.il	Xenu Link Sleuth User Agent	1
188.136.237.251	147.237.8.46	Iran, Islamic Republic of	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1

09-30-2016-05:04:03 to 09-30-2016-06:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
141.0.15.35	Norway	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	26
46.120.122.219	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
172.58.59.88	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
31.13.113.76	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.81	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
87.71.17.229	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
31.13.113.68	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.246.139.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
188.120.156.228	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
172.58.43.206	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
136.243.150.138	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
31.13.113.92	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.2.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
31.13.113.65	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
217.132.11.125	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
31.13.100.117	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
183.129.160.229	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
31.13.100.118	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.44	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
93.174.93.164	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.15	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.70	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
31.13.113.78	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
139.162.37.147	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
84.109.70.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.150	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
192.243.55.132	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.44	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
125.77.28.26	China	147.237.76.34	yohalan.idf.il	drop		drop	1
74.82.47.29	United States	147.237.0.35	akaws.idf.il	drop		drop	1
216.218.206.86	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
31.13.113.81	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.205	prisha.idf.il	drop	SAM rule	drop	1
2.53.179.78	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
84.109.70.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
31.13.113.66	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
125.77.28.26	China	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.49	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
31.13.113.89	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
5.9.17.118	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.43	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.7	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.54.5.175	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
131.253.24.140	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
76.109.53.177	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
31.13.113.91	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1

09-30-2016-05:04:03 to 09-30-2016-06:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.14.17.90	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 183.14.17.90	Block	17
110.136.51.124	Indonesia	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	6
183.14.17.90	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
110.136.51.124	Indonesia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	5
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	3
1.10.170.149	Thailand	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	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
66.249.64.187	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
192.243.55.134	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58623&docid=77019	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
180.76.15.32	China	147.237.76.42	refuah.idf.i	Unauthorized URL Access to 147.237.76.42/994-9740-he/refuah.aspx	Block	1
66.249.79.169	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
193.252.118.176	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
46.120.122.219	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
75.112.24.234	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.48	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.102.6.3	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
157.55.39.4	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.183	Block	1
192.243.55.130	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chinuch/klali/default.asp?catid=42817&docid=46708	Block	1
157.55.39.177	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1

09-30-2016-05:04:03 to 09-30-2016-06:04:03