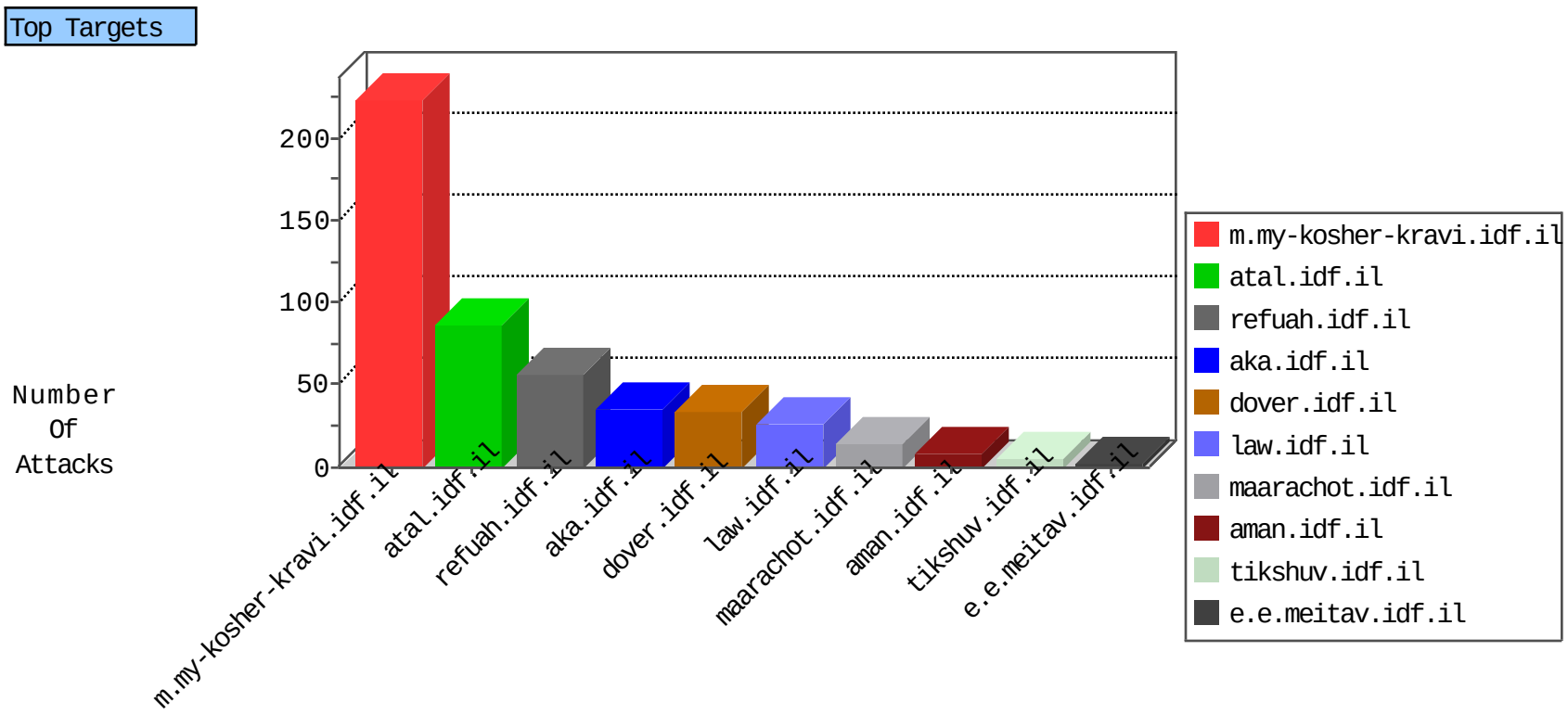
10-01-2016-05:04:09 to 10-01-2016-06:04:09

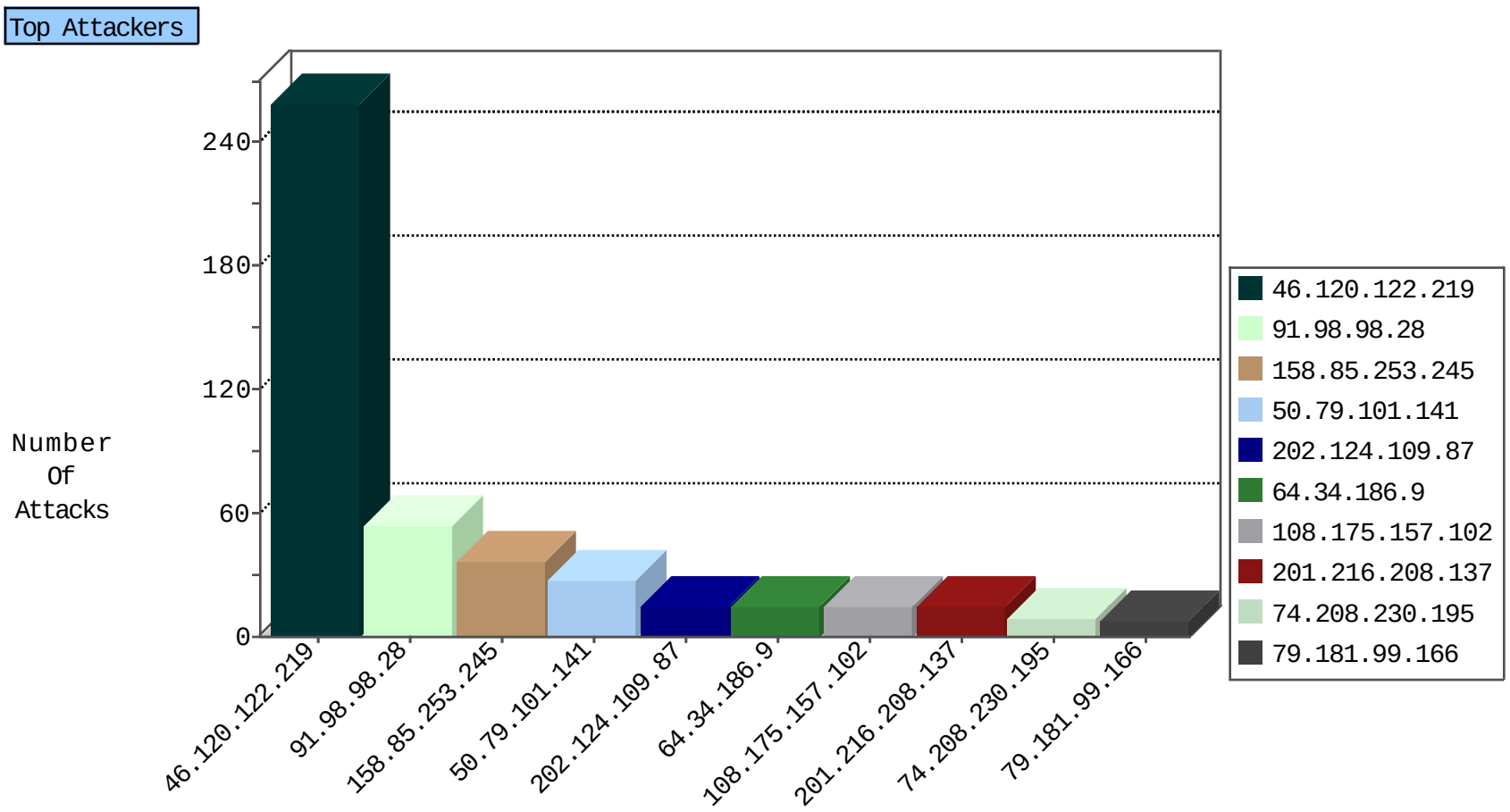
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-01-2016-05:04:09 to 10-01-2016-06:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
96.44.175.185	United States	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2

10-01-2016-05:04:09 to 10-01-2016-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.98.98.28	Iran, Islamic Republic of	147.237.76.42	refuah.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	11
64.34.186.9	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
158.85.253.245	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
158.85.253.245	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
201.216.208.137	Argentina	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
108.175.157.102	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
202.124.109.87	New Zealand	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
158.85.253.245	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
74.208.230.195	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3

10-01-2016-05:04:09 to 10-01-2016-06:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.0.17	Israel	m.my-kosher-kravi.idf.il	Xenu Link Sleuth User Agent	224
91.98.98.28	147.237.76.42	Iran, Islamic Republic of	refuah.idf.il	SQL Injection - Select From	42
158.85.253.245	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	18
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	13
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	11
64.34.186.9	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
201.216.208.137	147.237.77.233	Argentina	atal.idf.il	SQL Injection - Select From	8
108.175.157.102	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
202.124.109.87	147.237.77.74	New Zealand	law.idf.il	SQL Injection - Select From	8
74.208.230.195	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
151.80.41.96	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
183.129.160.229	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
62.150.255.205	147.237.76.31	Kuwait	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
118.175.14.244	147.237.77.19	Thailand	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.240.250.154	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.59.11	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
103.208.244.223	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.59.11	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
103.208.244.223	147.237.0.19		madim.atal.idf.il	ET SCAN Potential SSH Scan	1
183.129.160.229	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
181.143.61.210	147.237.76.196	Colombia	e.sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
62.150.255.205	147.237.76.31	Kuwait	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
62.150.255.205	147.237.76.31	Kuwait	nakchal.idf.il	ET SCAN NMAP -f -sS	1
118.175.14.244	147.237.77.74	Thailand	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.240.250.154	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
40.114.15.49	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
216.81.230.167	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.59.11	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
103.208.244.223	147.237.0.33		idf.il	ET SCAN Potential SSH Scan	1
13.93.120.74	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
103.208.244.223	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.129.160.229	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	147.237.8.46	Turkey	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1

10-01-2016-05:04:09 to 10-01-2016-06:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
50.79.101.141	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	27
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
108.178.44.182	United States	147.237.72.167	ishurim.aka.idf.il	Block HTTP Non Compliant	Response out of state	monitor	3
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	2
90.182.222.82	Czech Republic	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.116.80.67	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
141.212.122.19	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.34	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
68.50.106.107	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.139.91	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.34	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.98	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
79.181.99.166	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
71.6.146.185	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.215	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.232.53.96	Spain	147.237.76.34	yohalan.idf.il	drop		drop	1
74.82.47.56	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.17	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
195.62.53.168	Russian Federation	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
74.82.47.57	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.18	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.27	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
202.124.109.87	New Zealand	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
106.38.241.106	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
78.165.50.203	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1

10-01-2016-05:04:09 to 10-01-2016-06:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.122.219	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.120.122.219	Block	11
99.101.10.94	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.65.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1077-he/atal.aspx	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
157.55.39.128	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-22886-he	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
204.79.180.241	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	1
66.249.65.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8759-he/refuah.aspx	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
216.244.66.236	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/links.aspx	Block	1
68.180.230.186	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
84.108.73.249	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
66.249.64.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1400-he/atal.aspx	Block	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 220.181.125.23	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1

10-01-2016-05:04:09 to 10-01-2016-06:04:09