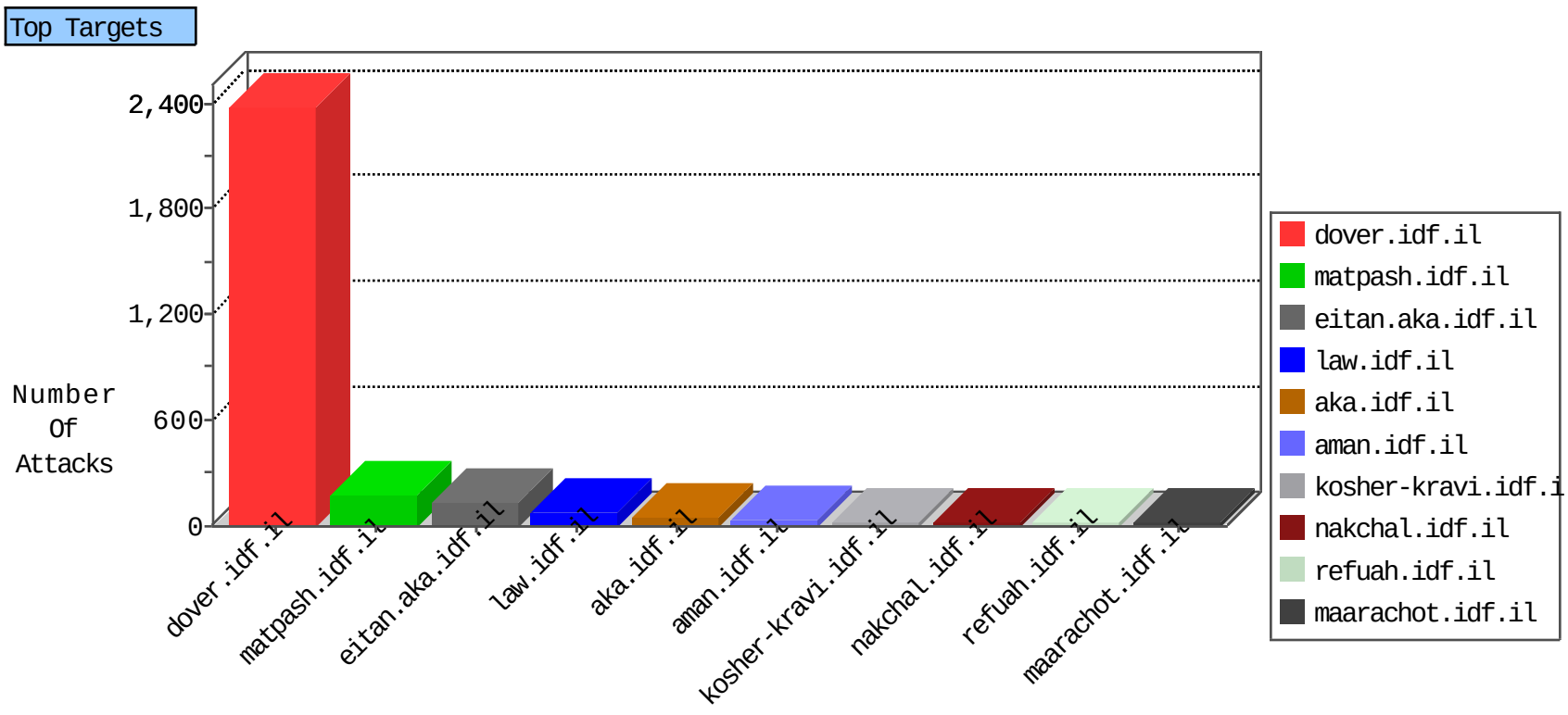
11-28-2015-02:04:01 to 11-28-2015-03:04:01

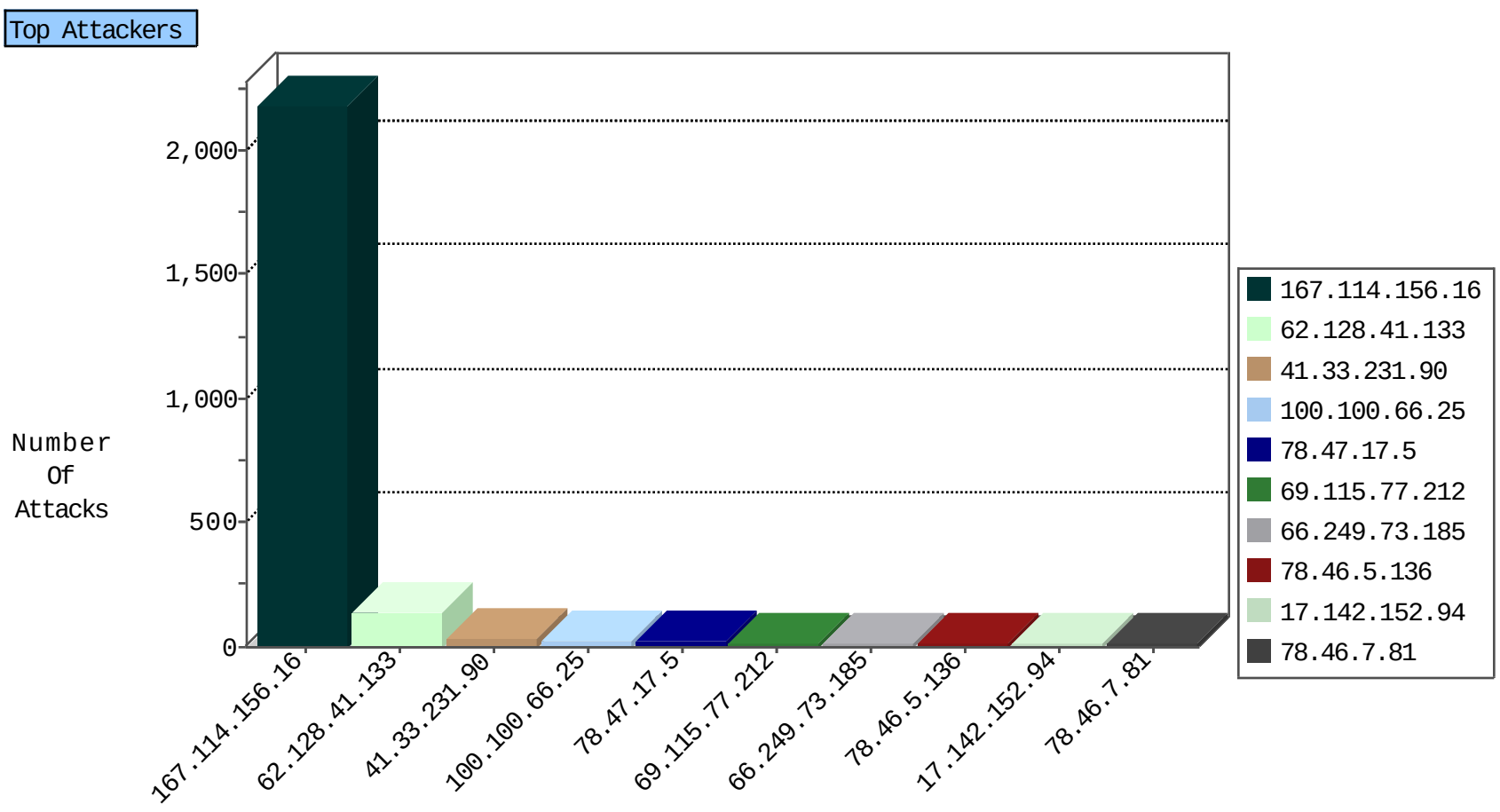
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-28-2015-02:04:01 to 11-28-2015-03:04:01

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	DOS-Tool-SwitchbladG	dest-reset	3325
85.25.43.94	Germany	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

11-28-2015-02:04:01 to 11-28-2015-03:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-28-2015-02:04:01 to 11-28-2015-03:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
46.172.71.252	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
31.6.71.154	147.237.0.17	Poland	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

11-28-2015-02:04:01 to 11-28-2015-03:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
100.100.66.25		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
69.115.77.212	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
17.142.152.94	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
62.128.41.133	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
17.142.152.68	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
17.142.152.85	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
109.65.37.144	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
37.26.147.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
17.142.152.81	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
17.142.145.3	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
17.142.152.86	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
17.142.152.72	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
78.47.17.5	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
17.142.152.110	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
79.54.153.25	Italy	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.103	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.73.201	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
17.142.152.89	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
78.47.17.5	Germany	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
46.19.86.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
87.69.208.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
195.154.226.90	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
40.77.167.91	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
62.128.41.133	Israel	147.237.76.200	eitan.aka.idf.il	drop	First packet isn't SYN	drop	3
78.47.17.5	Germany	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	3
181.117.6.76	Argentina	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
78.47.17.5	Germany	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	3
208.115.113.92	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
79.178.217.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
78.47.17.5	Germany	147.237.77.74	law.idf.il	drop	SAM rule	drop	3
109.64.109.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.232.110.28	United Kingdom	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
199.30.24.201	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
17.142.152.111	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.0.33	idf.il	drop		drop	2
46.19.86.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
40.77.167.35	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
62.128.41.133	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.85.60	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
91.78.193.139	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.125	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
141.212.121.219	United States	147.237.0.33	idf.il	drop		drop	1
84.94.187.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1

11-28-2015-02:04:01 to 11-28-2015-03:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.128.41.133	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 62.128.41.133	Block	117
104.219.52.250		147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
41.42.121.40	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
78.46.7.81	Germany	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	3
64.37.50.82	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
198.20.241.76	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
50.87.43.17	United States	147.237.0.15	kosher-kravi.idf.il	Distributed PHP Attempt	Block	3
175.126.62.59	Korea, Republic of	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
206.167.188.171	Canada	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
221.121.151.95	Australia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
5.9.176.230	Germany	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
78.46.7.81	Germany	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 78.46.7.81	Block	3
192.145.238.195	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
78.46.5.136	Germany	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	3
74.220.207.152	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	3
197.85.182.58	South Africa	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
41.42.121.40	Egypt	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	3
174.136.96.189	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
203.162.53.47	Vietnam	147.237.76.30	himush.idf.il	Distributed PHP Attempt	Block	3
69.27.102.9	Canada	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	3
217.199.164.217	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
103.9.64.178	Australia	147.237.76.30	himush.idf.il	Distributed PHP Attempt	Block	3
192.145.238.195	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
78.46.5.136	Germany	147.237.0.15	kosher-kravi.idf.il	Distributed PHP Attempt	Block	3
196.41.122.249	South Africa	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	3
72.47.234.114	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
173.254.85.31	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
201.175.20.195	Mexico	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
192.145.238.195	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 192.145.238.195	Block	3
213.202.223.160	Germany	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
128.199.139.56	Singapore	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
103.9.64.178	Australia	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	3
186.202.161.36	Brazil	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
208.77.156.165	Canada	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
196.41.122.249	South Africa	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	3
162.144.210.204	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
103.9.64.178	Australia	147.237.76.30	himush.idf.il	Multiple Unauthorized URL Access from 103.9.64.178	Block	3
128.65.127.231	Italy	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
92.53.118.53	Russian Federation	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
194.100.58.154	Finland	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
78.46.157.220	Germany	147.237.0.15	kosher-kravi.idf.il	Distributed PHP Attempt	Block	3
199.103.62.15	Canada	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
119.47.117.196	New Zealand	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
194.100.58.154	Finland	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	3
201.148.104.107	Chile	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	3
198.46.82.33	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
118.127.32.136	Australia	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
192.145.239.21	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
113.23.215.139	Malaysia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
78.46.7.81	Germany	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3

11-28-2015-02:04:01 to 11-28-2015-03:04:01