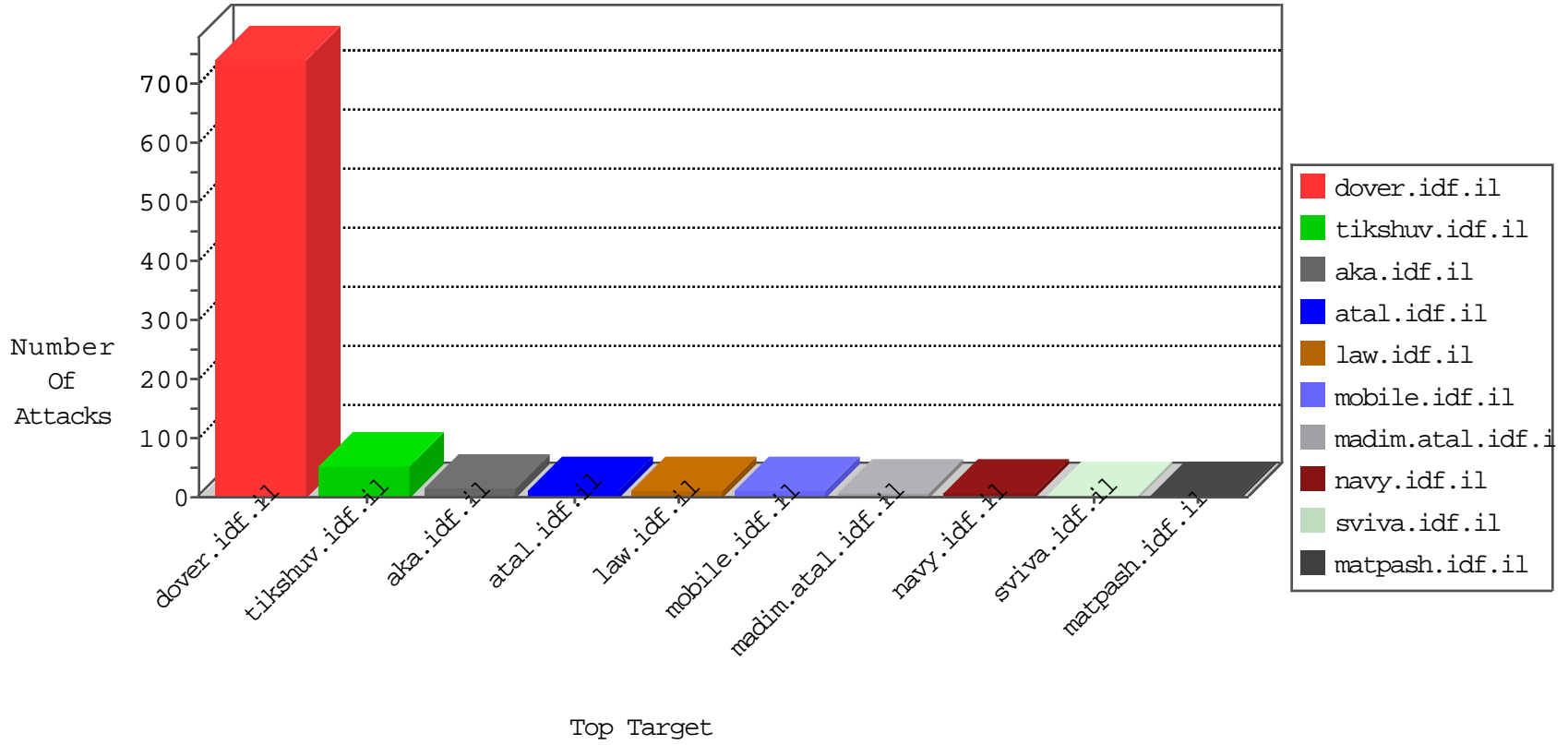


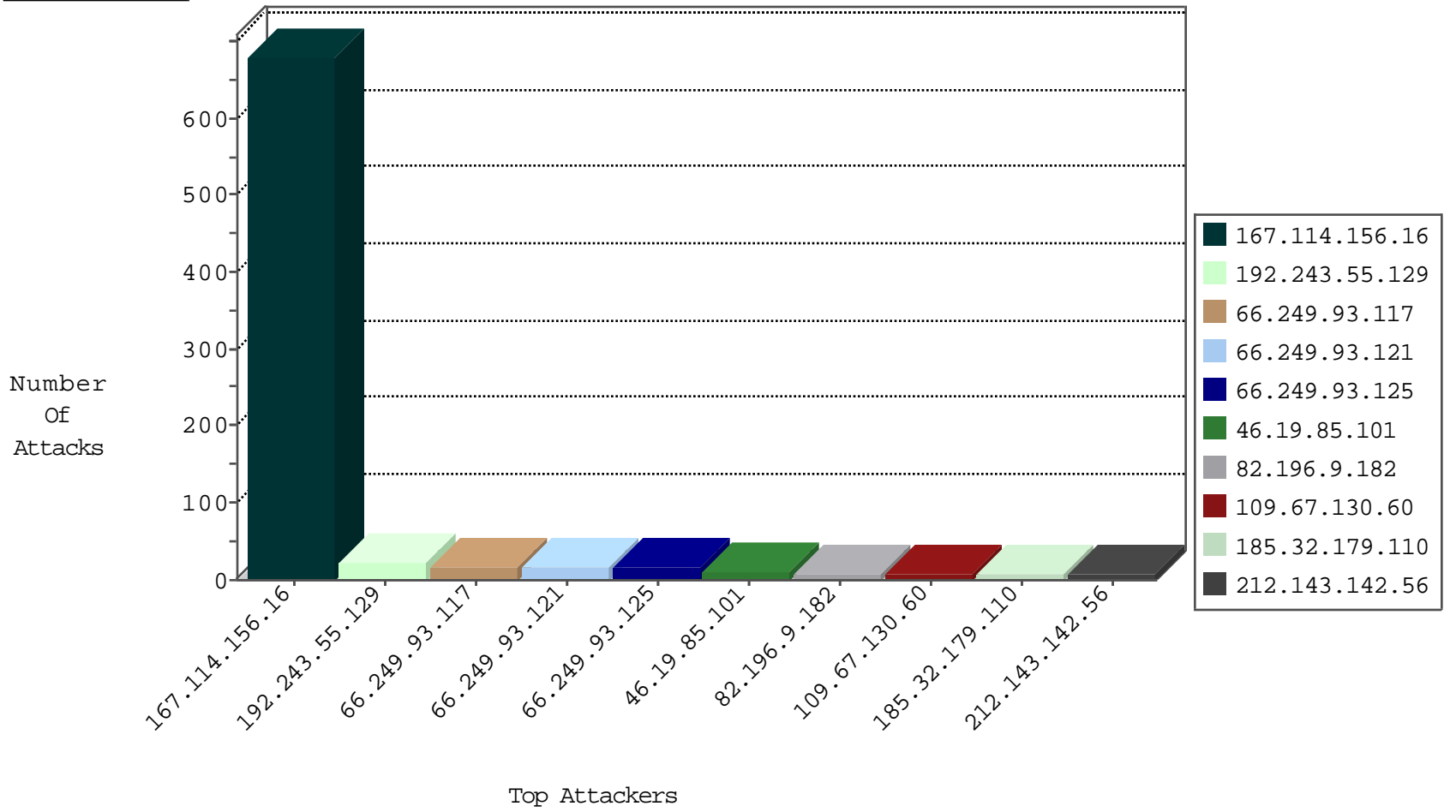
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3011
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
184.105.139.88	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.206	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.100	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
185.56.28.67	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
71.6.165.200	United States	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
180.175.229.69	China	147.237.8.14	e.ordhot.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
93.219.123.228	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

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
167.114.172.229	147.237.77.216	Canada	dover.idf.il	SERVER-APACHE Apache mod_proxy reverse proxy information disclosure attempt	2
185.130.5.179	147.237.76.202		e.halag.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.179	147.237.76.197		e.himush.idf.il	ET SCAN Potential SSH Scan	1
180.97.81.71	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
205.200.120.138	147.237.0.34	Canada	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.76.30	Sweden	himush.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.179	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.179	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
174.44.245.112	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
82.196.9.182	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
66.249.93.125	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
66.249.93.121	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	14
185.32.179.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
64.246.165.50	United States	147.237.0.34	tikshuv.idf.il	Header Rejection	header rejection pattern found in request	monitor	4
79.183.99.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.129	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.67.130.60	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	3
109.67.130.60	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
46.19.85.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.109.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.156.0	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.138.197.18	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
77.125.108.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
144.76.93.46	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.125.108.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
82.196.9.182	Netherlands	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.15	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.227	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
159.226.95.66	China	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.122	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.119.167.19		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.98	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.16	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.62.53.168	Russian Federation	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
82.196.9.182	Netherlands	147.237.77.19	law-forum.idf.il	Web Server Enforcement Violation	Masscan Port Scanner	reject	1
74.82.47.48	United States	147.237.76.176	test.ncoore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.228	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
159.226.95.66	China	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
220.181.108.92	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.120.173.159	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
82.196.9.182	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	Web Server Enforcement Violation	Masscan Port Scanner	reject	1
185.119.167.19		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
66.249.93.121	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.112	United States	147.237.8.46	e.chiruch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.72	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
82.196.9.182	Netherlands	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.243	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.114.146.227	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	4
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19015-en/dover.aspx89/dont-you-wish-this-was-waiting-for-you-at-home-i-doeathhowcomment=1367249835647	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakchal.idf.il/1111-he/nakhal.aspx	Block	1
157.55.39.12	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
167.114.172.229	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.19	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
194.114.146.227	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/1/size338x0/1651.jpg	Block	1
109.67.130.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
167.114.172.229	Canada	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 167.114.172.229	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
217.69.133.246	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/schar	Block	1
121.169.10.226	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
184.105.247.196	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
121.169.10.226	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.102.9.101	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1