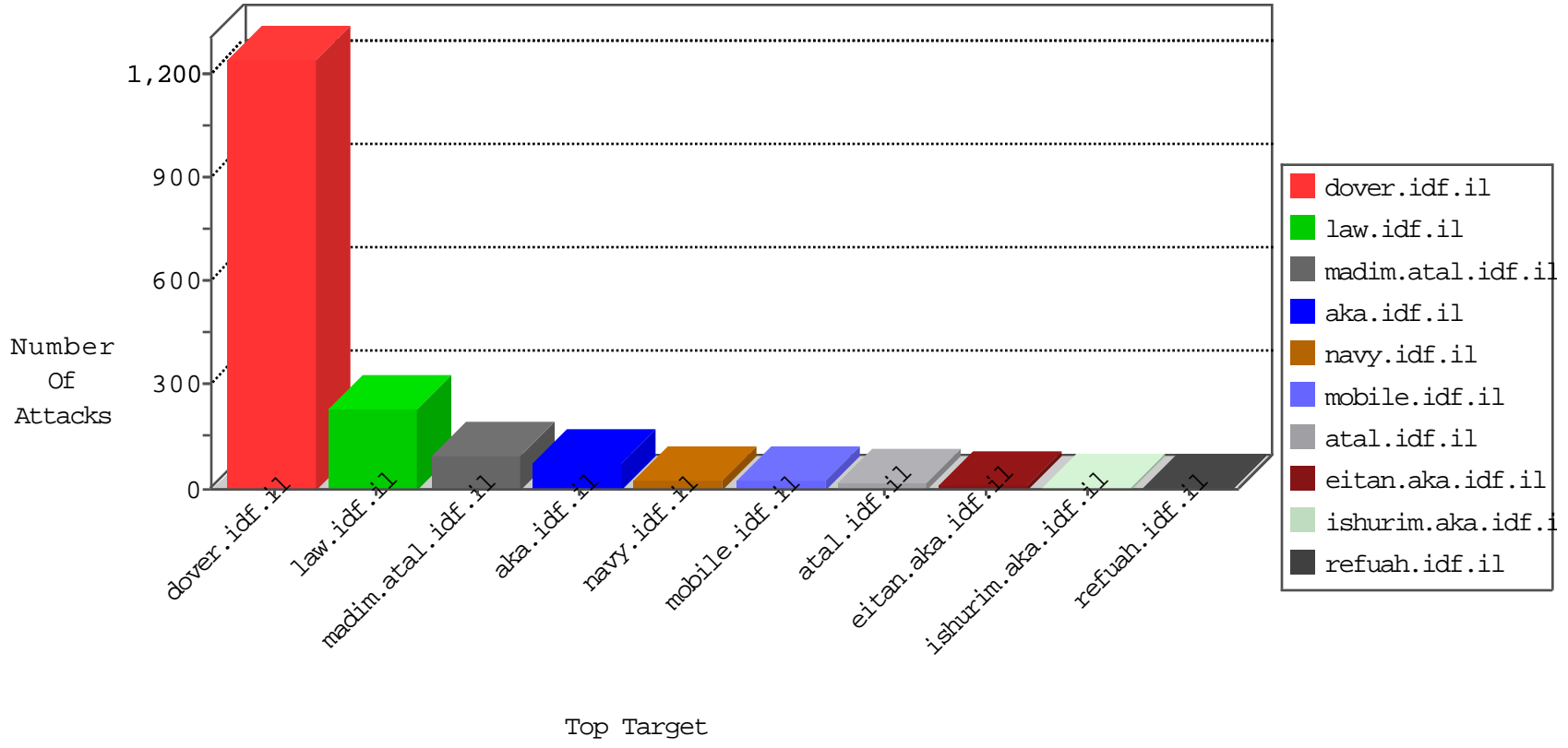


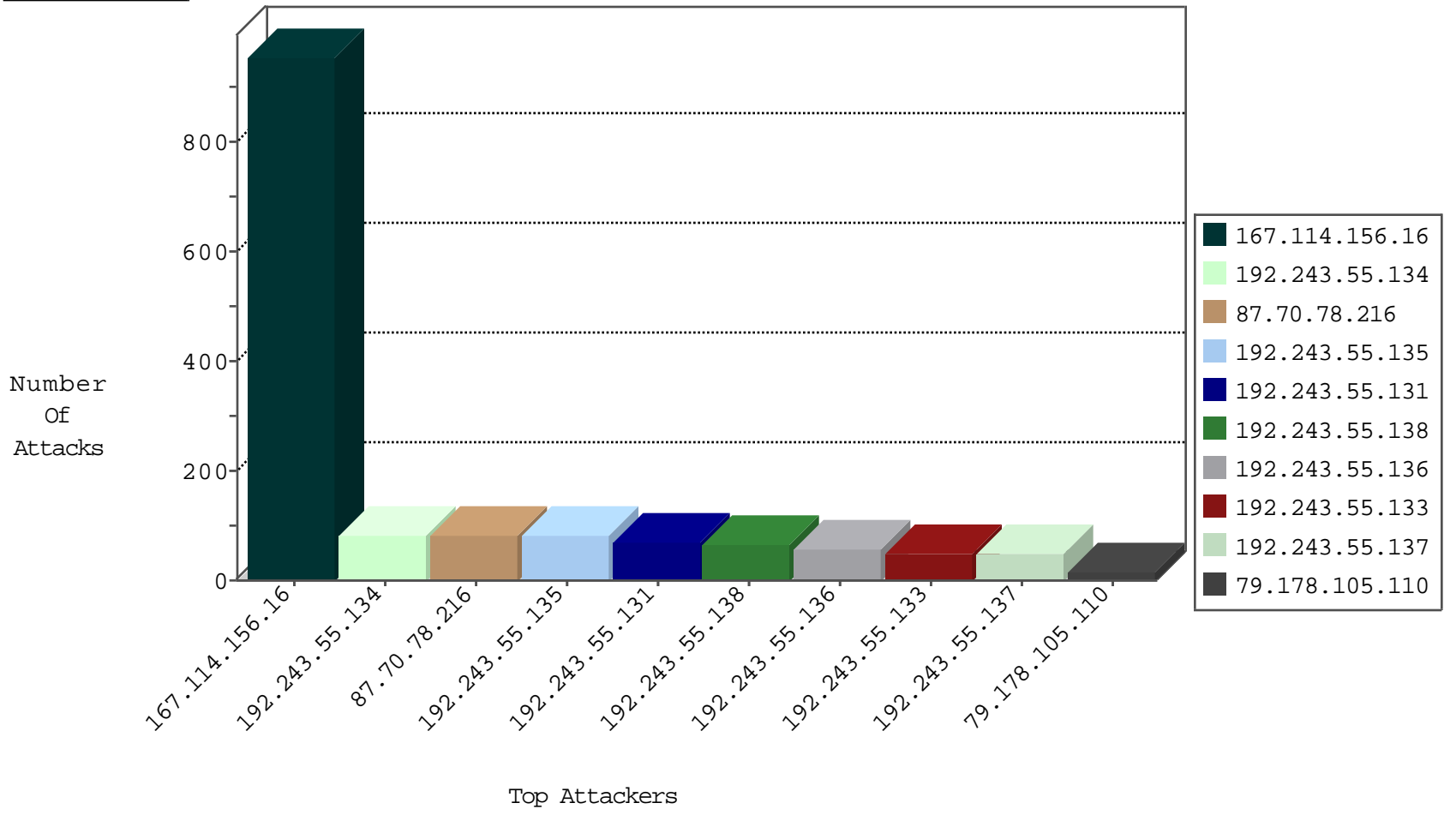
# IDF Under Attack Daily Report



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	4000
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
216.218.206.95	United States	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.67	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.83	United States	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.77.61	e.cogat.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
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
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

## 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
104.232.98.38	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 1024	1
192.243.55.136	147.237.77.216	Dominica	dover.idf.il	GPL WEB_SERVER ISAPI .printer access	1
104.232.98.38	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 3072	1
192.243.55.136	147.237.77.216	Dominica	dover.idf.il	SERVER-IIS ISAPI .printer access	1
147.175.16.71	147.237.8.24	Slovakia	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
79.178.105.110	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
2.54.186.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.117.97.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
66.249.64.124	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.64.3	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.243.55.134	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
192.243.55.133	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
185.120.125.88		147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.131	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.135	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
87.69.26.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.137	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.70.78.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
5.29.87.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
93.173.34.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.246	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
37.237.240.29	Iraq	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.237.240.29	Block	2
79.183.147.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.120.125.88		147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
40.77.167.82	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 40.77.167.82	Block	2
37.26.147.222	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
203.127.96.228	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
54.193.67.45	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
157.55.39.65	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.178.105.110	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1486-he/atal.aspx	Block	1
213.254.241.4	United Kingdom	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$btnSearch in www.aka.idf.il/main/sachar/default.aspx	None	1
105.196.230.201	Egypt	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
66.249.64.119	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
184.105.139.67	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
37.237.240.29	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/css/icons/icons.woff	Block	1
217.194.197.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
105.196.230.201	Egypt	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
37.26.147.222	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.147.222	Block	1
84.111.52.31	Israel	147.237.72.166	aka.idf.il	Unknown Parameter moduleTo tqGoTo in www.aka.idf.il/main/giyus/login.aspx	None	1
220.255.97.58	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
131.253.25.221	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
70.27.253.214	Canada	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19121-en/dover.aspx http://www.printerdustcovers.net/speck-kindle-dustjacket-red-fits-6-display-latest-generation-kindle	Block	1
46.60.16.117	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
220.255.145.186	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
132.74.95.19	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/8/108808.pdf	Block	1
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1