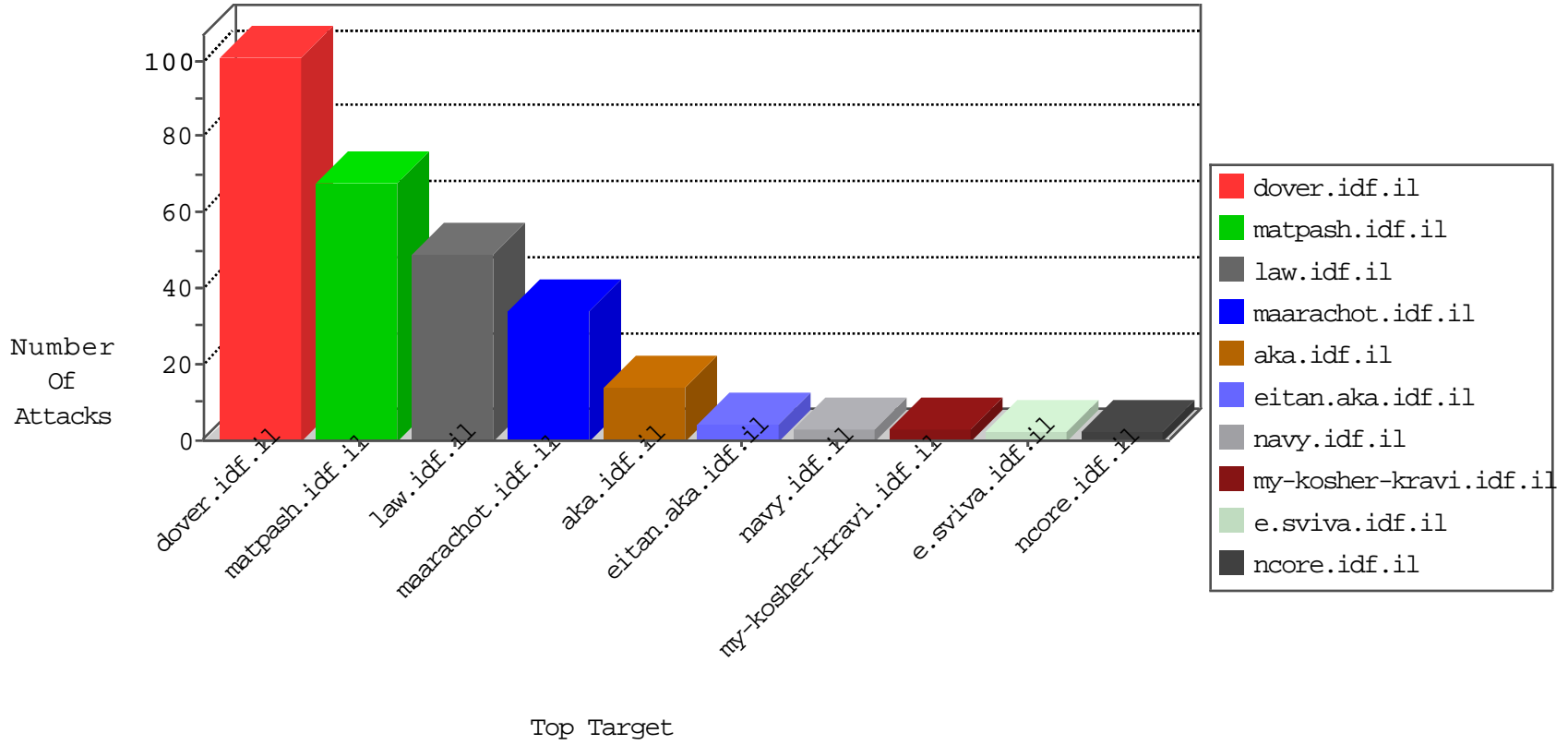


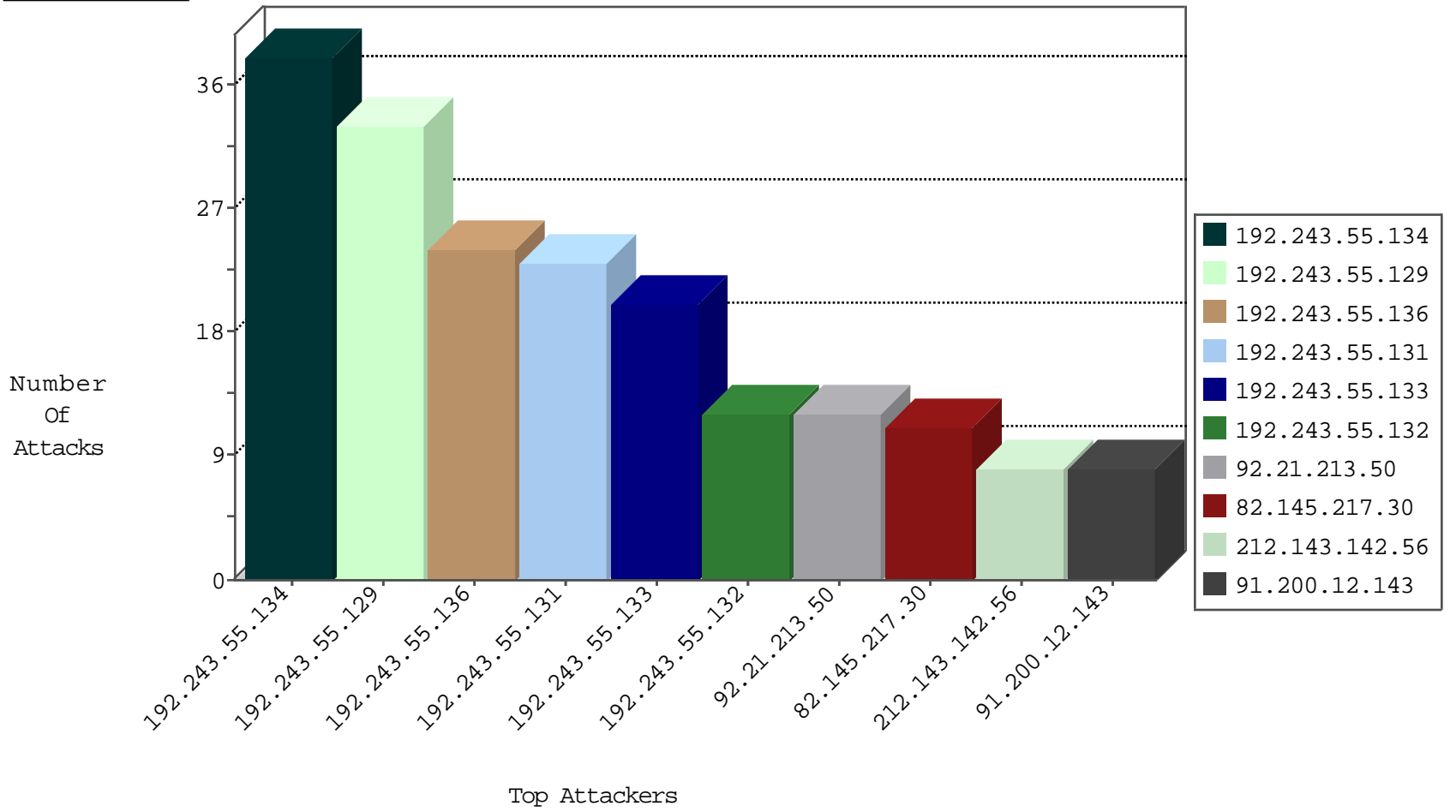
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.217.30	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	11
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	6
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.143.254.66	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
141.255.164.234	Switzerland	147.237.77.226	www.chanatz.aka.idf.il	Block_Ntp_All_Net	drop	1
104.156.246.165	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
61.239.211.122	Hong Kong	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
141.255.164.234	Switzerland	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
23.228.107.104	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.2	United States	147.237.0.16	ny-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
104.156.246.165	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
61.239.211.122	Hong Kong	147.237.0.16	ny-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
141.255.164.234	Switzerland	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
23.228.107.104	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
104.156.246.165	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
61.239.211.122	Hong Kong	147.237.0.17	m.ny-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
141.255.164.234	Switzerland	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
104.156.246.165	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
104.156.246.165	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.57	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.69	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
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
123.126.113.80	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
209.126.116.147	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.76.39	Austria	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.72.166	Ukraine	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
218.246.0.97	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
91.200.12.143	Ukraine	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence		monitor	4
92.21.213.50	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
100.38.255.165	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
92.21.213.50	United Kingdom	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.129	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.131	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
84.229.34.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.136	Dominica	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
68.197.56.236	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.129	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence		monitor	2
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.131	Dominica	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.136	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence		monitor	2
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.136	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
68.197.56.236	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.136	Dominica	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence		monitor	2
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
70.210.152.171	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.129	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
147.235.8.64	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
92.21.213.50	United Kingdom	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.131	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xhlytalltawmy5kb2m=&infocenteritem=true	Block	1
40.77.167.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
99.238.9.59	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
192.243.55.133	Dominica	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112745.pdf	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/	Block	1
131.253.25.214	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
203.127.96.245	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/undefined/	Block	1
149.125.24.107	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/gyus/authenticationservice.aspx/getauthuser	Block	1
207.46.13.68	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/page.asp	Block	1
87.139.80.210	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
172.56.19.63	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/gyus/authenticationservice.aspx/getauthuser	Block	1
37.47.41.216	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
87.139.94.177	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1