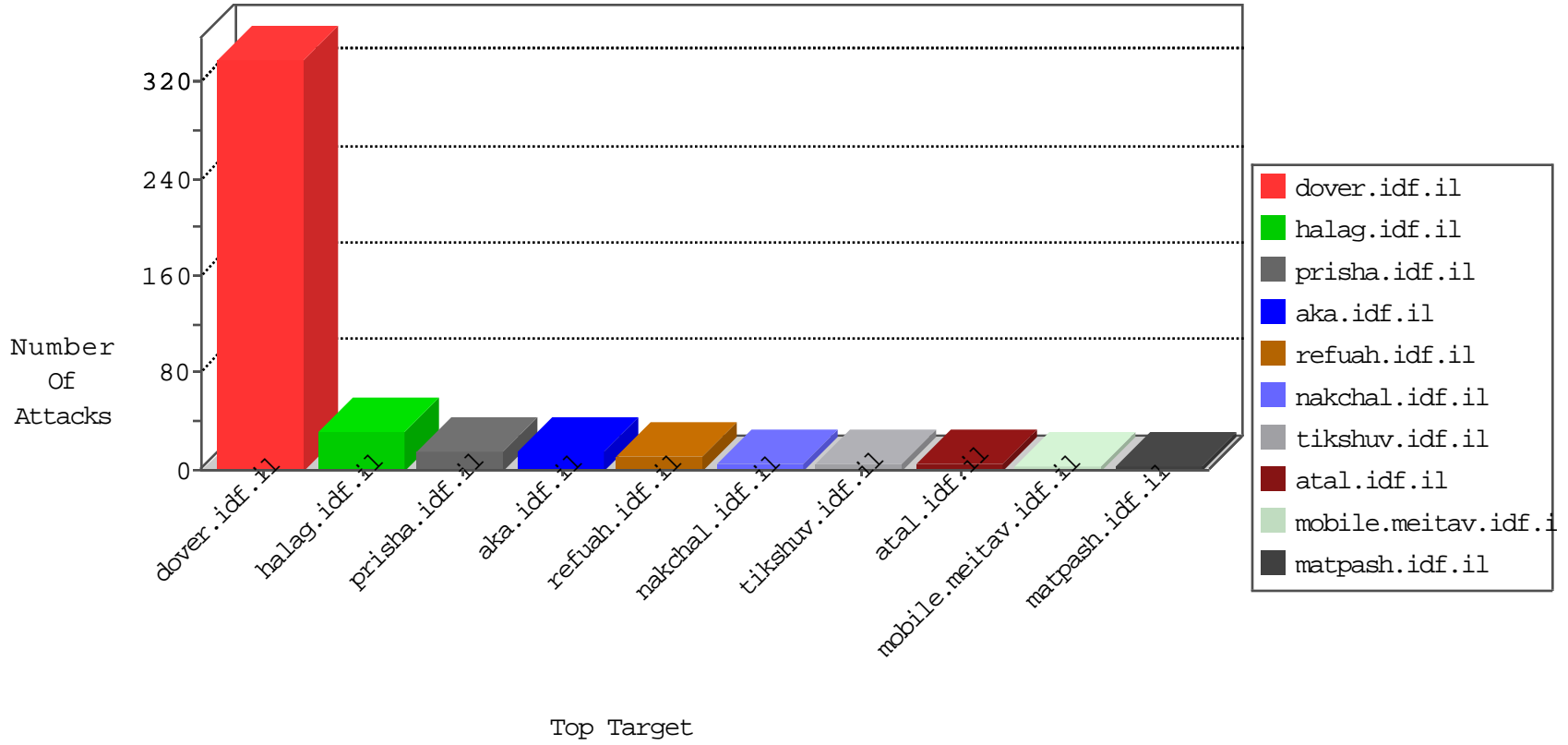


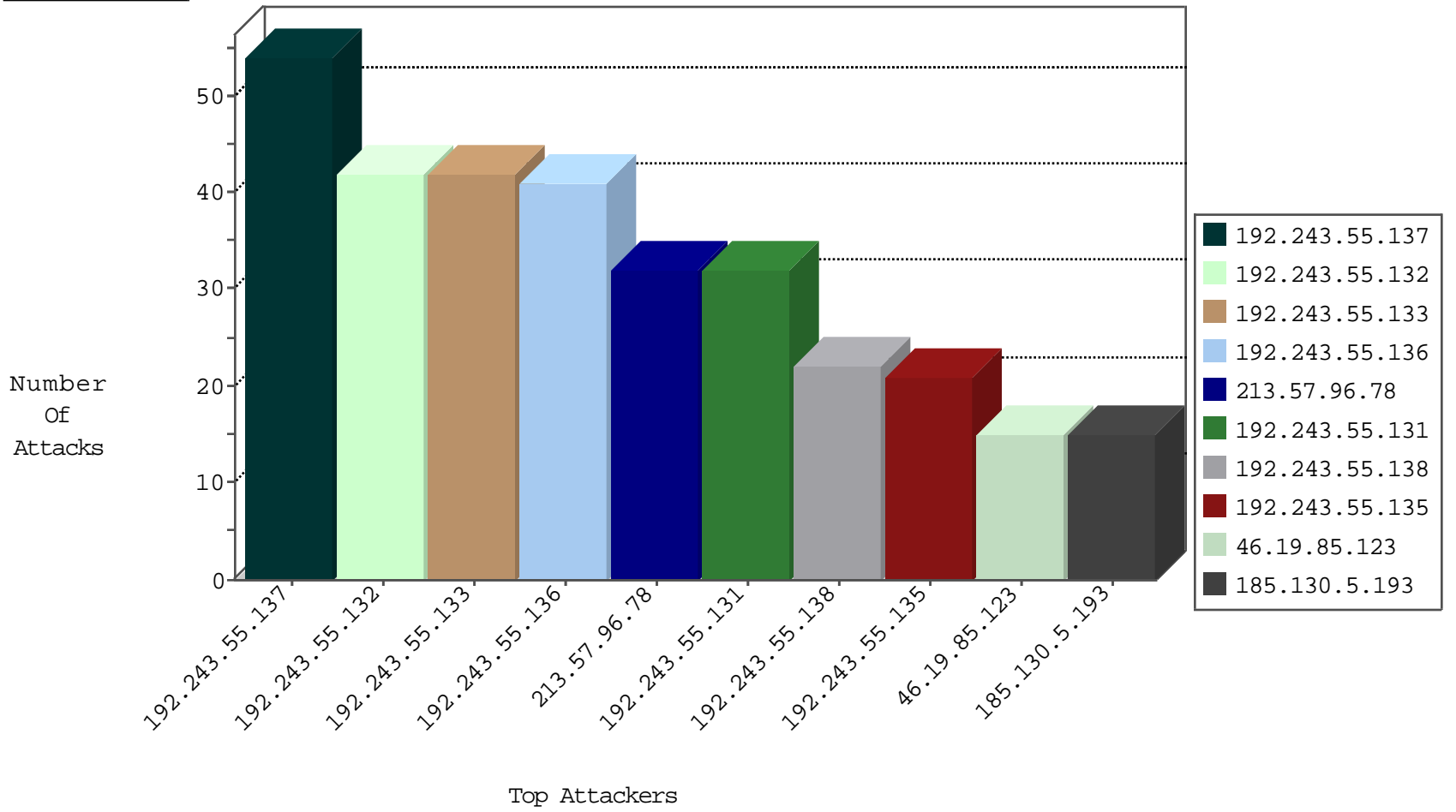
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
104.172.112.17	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	5
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.162	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
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
58.143.17.58	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.246.0.97	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
201.48.50.33	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
201.48.50.33	147.237.0.19	Brazil	madim.atal.idf.i	ET SCAN Potential SSH Scan	1
65.98.59.26	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.0.19	United States	madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
201.48.50.33	147.237.0.33	Brazil	idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.72.156	Latvia	aman.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.76.201	Netherlands	e.atal.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
213.57.96.78	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
185.130.5.193		147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
46.19.85.123	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.44.12	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.64.211.205	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.143	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.64.211.205	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.120.125.5		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.84.32	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.243.55.138	Dominica	147.237.77.216	dover.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
77.126.161.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.64.84.32	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.118.155.216	Ukraine	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
66.249.66.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.241.229.198	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/rabanut/general.aspx	None	1
66.249.64.61	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.equalheights.js	Block	1
40.77.167.20	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
46.118.155.216	Ukraine	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
207.241.237.223	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/iturim/asp/displayonesoldier.asp	None	1
40.77.167.59	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
46.118.155.216	Ukraine	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
213.8.204.50	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation pageNum in www.nakchal.idf.il/1073-he/nakchal.aspx	Block	1
40.77.167.62	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/sip_storage/files/5/size220x0/1655.bmp	Block	1
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.51	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/ui/i18n/jquery-ui-i18n.js	Block	1
213.57.96.78	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
73.23.178.26	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
40.77.167.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in ww.tikshuv.idf.il/site/general.aspx	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.64.56	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/ui/ui.datepicker.js	Block	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1