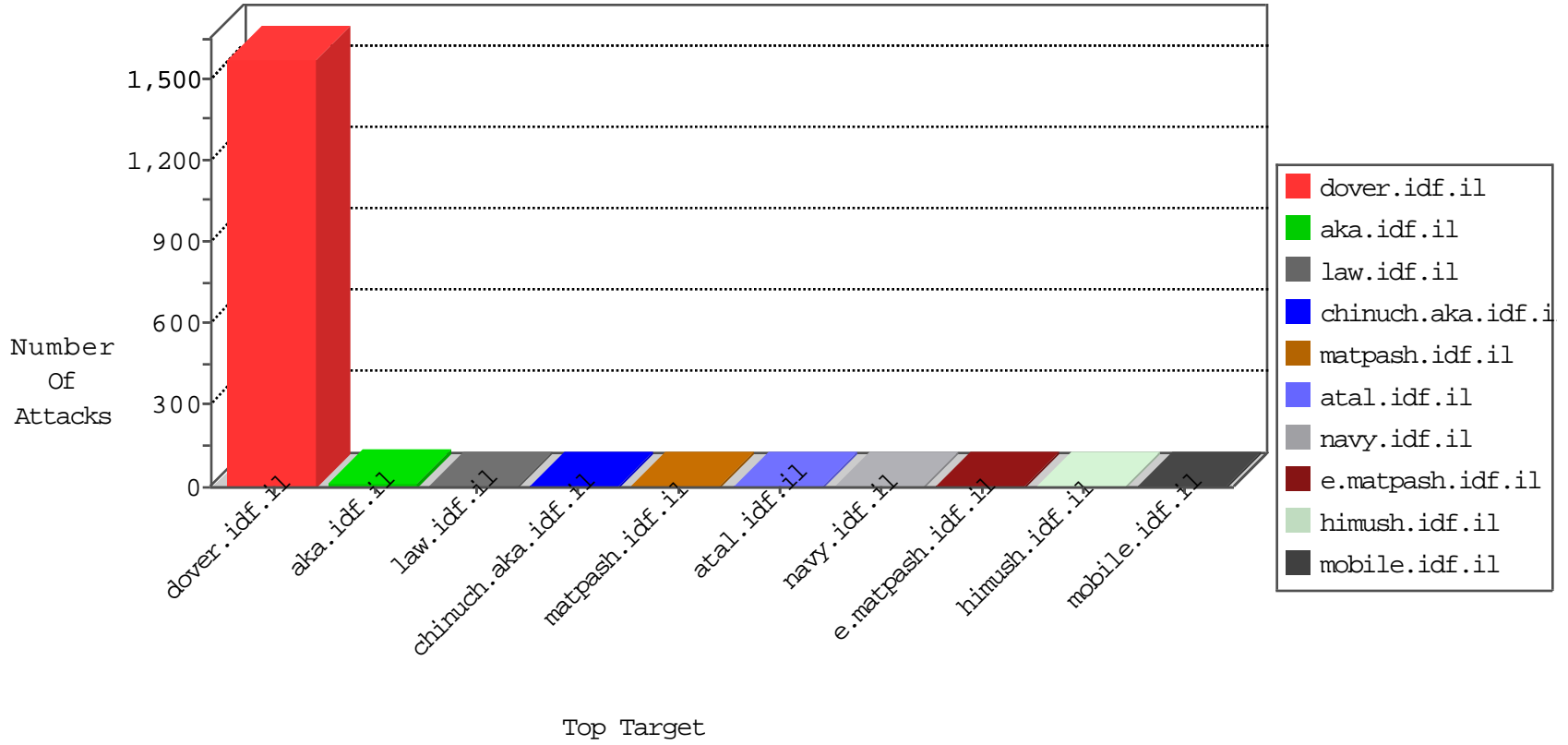


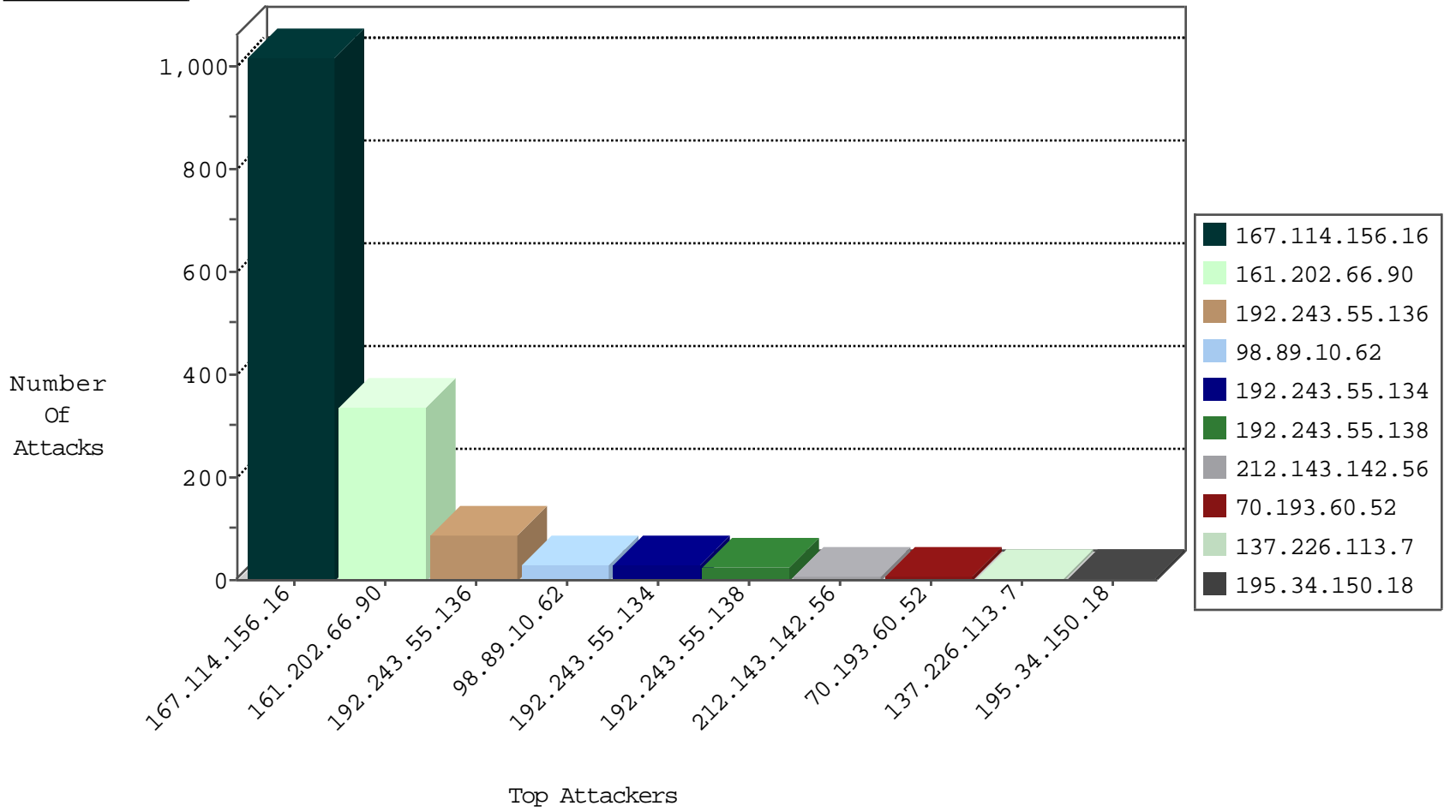
IDF Under Attack Daily Report



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	3158
161.202.66.90	Netherlands	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	1223
5.189.172.102	Germany	147.237.0.33	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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.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
104.128.144.131	147.237.77.178	Canada	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
82.117.208.243	147.237.0.15		kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.77.178	Canada	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
93.113.125.12	147.237.76.38	Romania	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
81.136.134.68	147.237.76.147	United Kingdom	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
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
98.89.10.62	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	12
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
98.89.10.62	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
98.89.10.62	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
98.89.10.62	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
70.193.60.52	United States	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
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
207.46.13.87	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
213.151.44.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.212.122.171	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
70.193.60.52	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.126.252.12	Romania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
216.218.206.102	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
137.226.113.7	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
93.115.95.206	Anonymous Proxy	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
46.166.188.196	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.247.211	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.172	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.87	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
128.232.110.29	United Kingdom	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.79	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.106	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
137.226.113.7	Germany	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
50.93.198.132	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.235	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.88.179.43	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.102	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
128.232.110.29	United Kingdom	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.79	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.164	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.242.161.57	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
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	2
40.77.167.82	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
141.212.122.160	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on 147.237.77.74/	Block	1
66.249.74.107	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
208.80.155.217	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
121.205.231.160	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyus/general.aspx	Block	1
157.55.39.108	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/ishurim	Block	1
38.111.147.83	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/templates/journalview/journalview.aspx	Block	1
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	1
131.253.25.213	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.185	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
161.202.66.90	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
77.75.78.170	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
217.69.133.246	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/kamlar/klali/default.asp	None	1
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1437-he/atal.aspx	Block	1
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
93.115.95.206	Anonymous Proxy	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
50.93.198.132	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
208.80.155.217	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.80.155.217	Block	1
121.205.231.160	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
50.93.198.132	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1