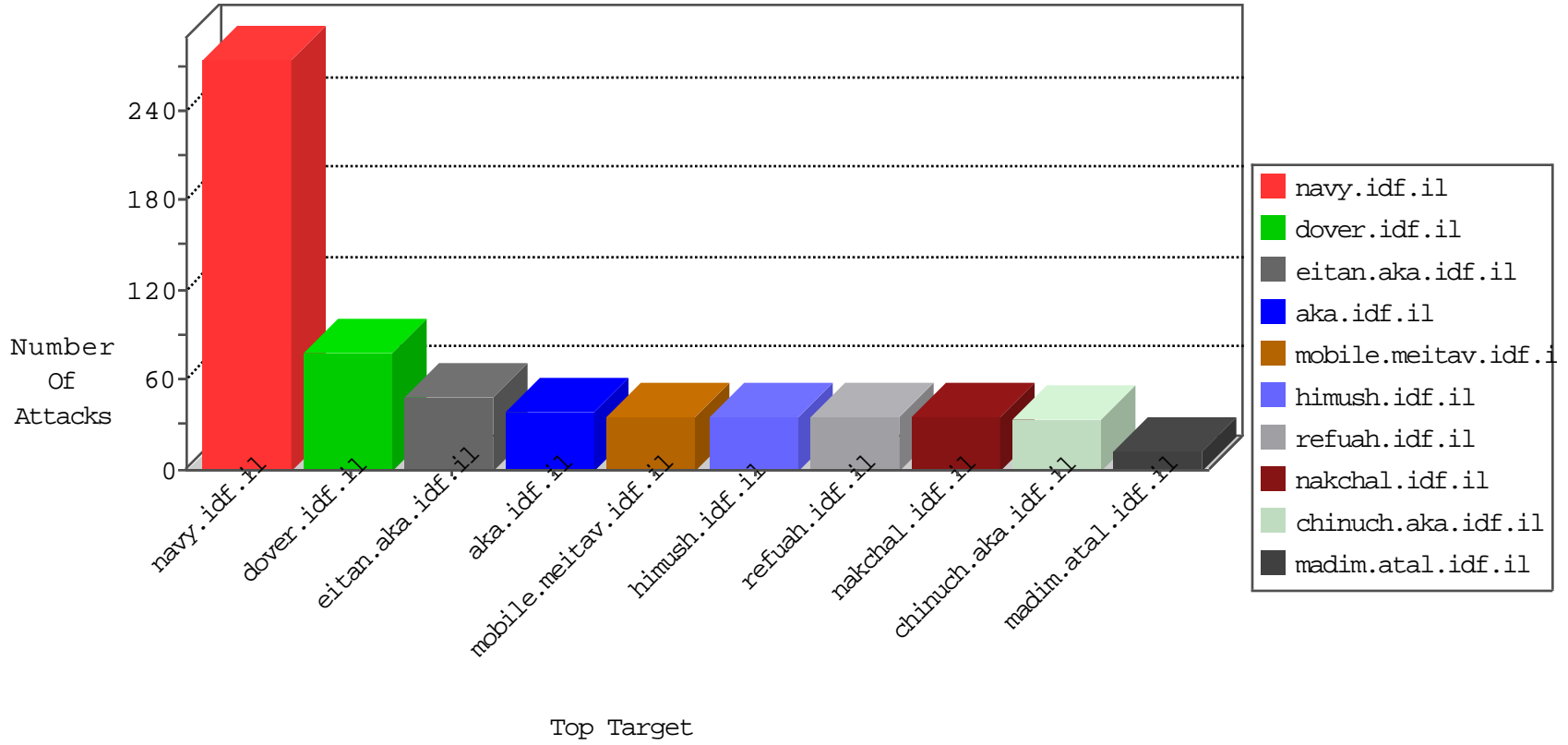


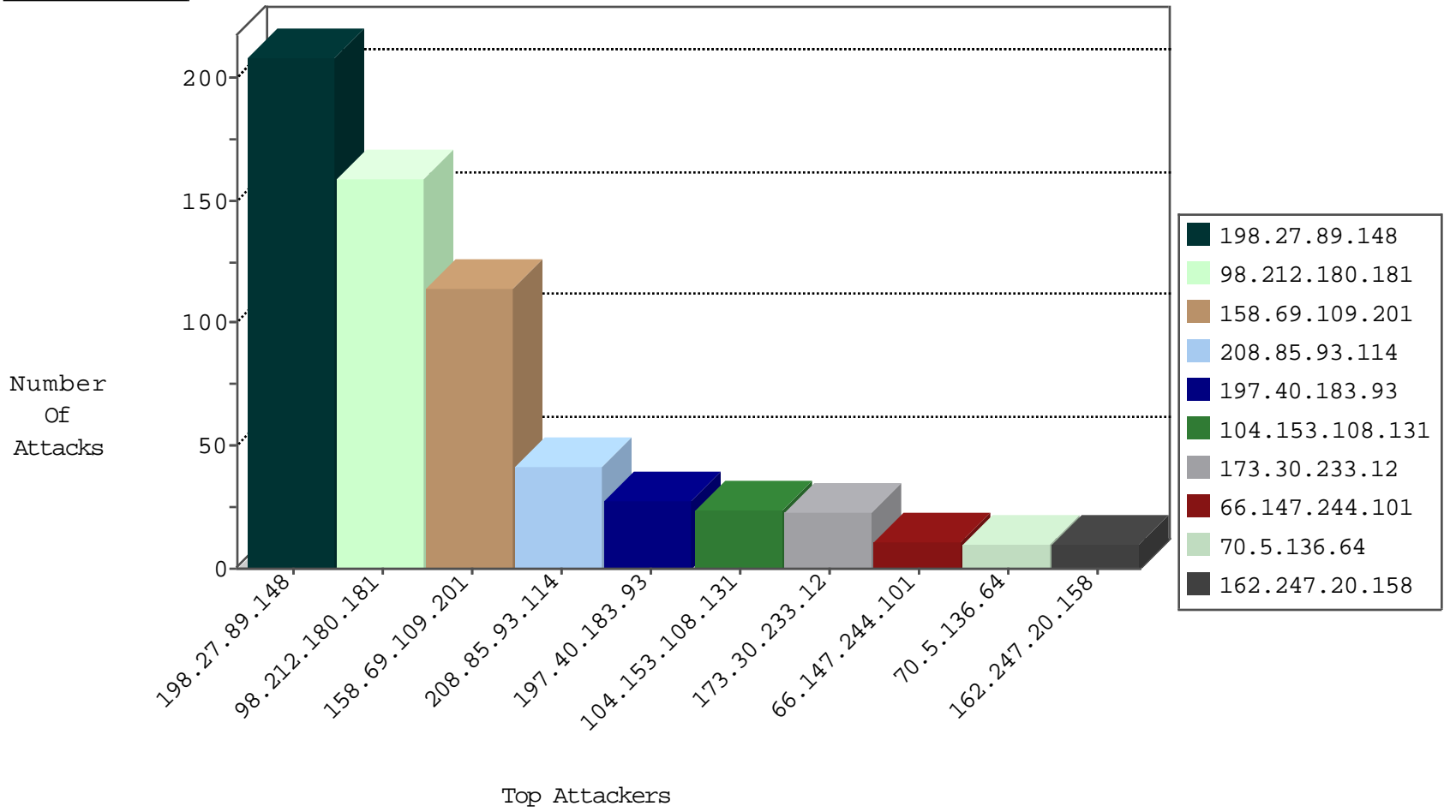
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Black List	drop	2
139.19.117.8	Germany	147.237.76.197	e.himush.idf.il	Black List	drop	2

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.68.128	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
71.6.216.58	147.237.77.243	United States	mobile.idf.il	ET SCAN Potential SSH Scan	1
52.166.130.115	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.76.148	United Kingdom	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.147	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
85.14.42.2	147.237.76.86	Bulgaria	navy.idf.il	ET SCAN NMAP -f -sS	1
69.24.208.162	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
176.58.124.35	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.203.168	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
85.14.42.2	147.237.76.86	Bulgaria	navy.idf.il	ET SCAN NMAP -sS window 2048	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
98.212.180.181	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	159
197.40.183.93	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
198.27.89.148	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
198.27.89.148	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
198.27.89.148	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
198.27.89.148	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
198.27.89.148	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
198.27.89.148	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
198.27.89.148	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
198.27.89.148	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
173.30.233.12	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
104.153.108.131	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
158.69.109.201	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
158.69.109.201	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
158.69.109.201	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
158.69.109.201	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
104.153.108.131	United States	147.237.76.86	navy.idf.il	SYN Attack		monitor	6
158.69.109.201	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
158.69.109.201	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
66.249.64.63	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
158.69.109.201	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
158.69.109.201	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
158.69.109.201	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
158.69.109.201	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
208.85.93.114	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
158.69.109.201	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
158.69.109.201	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
158.69.109.201	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
158.69.109.201	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
158.69.109.201	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
158.69.109.201	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
158.69.109.201	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
158.69.109.201	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
158.69.109.201	United States	147.237.77.170	mearachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
158.69.109.201	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
208.85.93.114	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
158.69.109.201	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
157.55.39.224	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
208.85.93.114	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
208.85.93.114	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
158.69.109.201	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
77.138.246.53	France	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
208.85.93.114	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
208.85.93.114	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
66.249.66.251	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
40.77.167.97	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
104.153.108.131	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
208.85.93.114	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
104.153.108.131	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.147.244.101	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	11
200.181.229.112	Brazil	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/megurim/	Block	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
176.193.108.235	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.64.253	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/piwik.php	Block	1
37.144.50.201	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
188.32.242.20	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.65.156	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
85.64.184.19	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 85.64.184.19 (Open Mode)	None	1
46.19.86.104	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.65.160	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-7237-he/atal.aspx	Block	1
85.64.184.19	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
204.79.180.171	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluum/templates/inner.asp	Block	1
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/120203	Block	1
108.21.193.175	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.144	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/news/news.in.aspx	Block	1