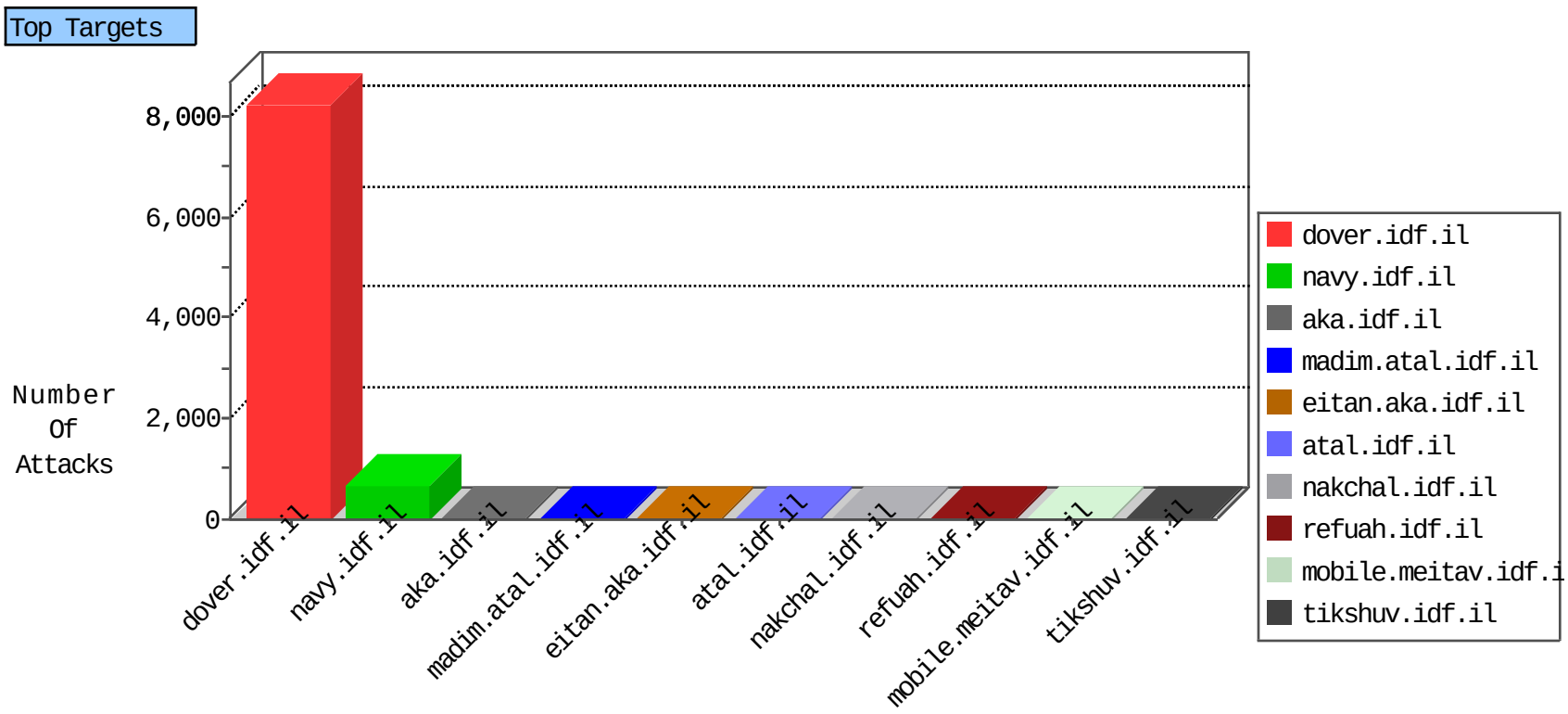
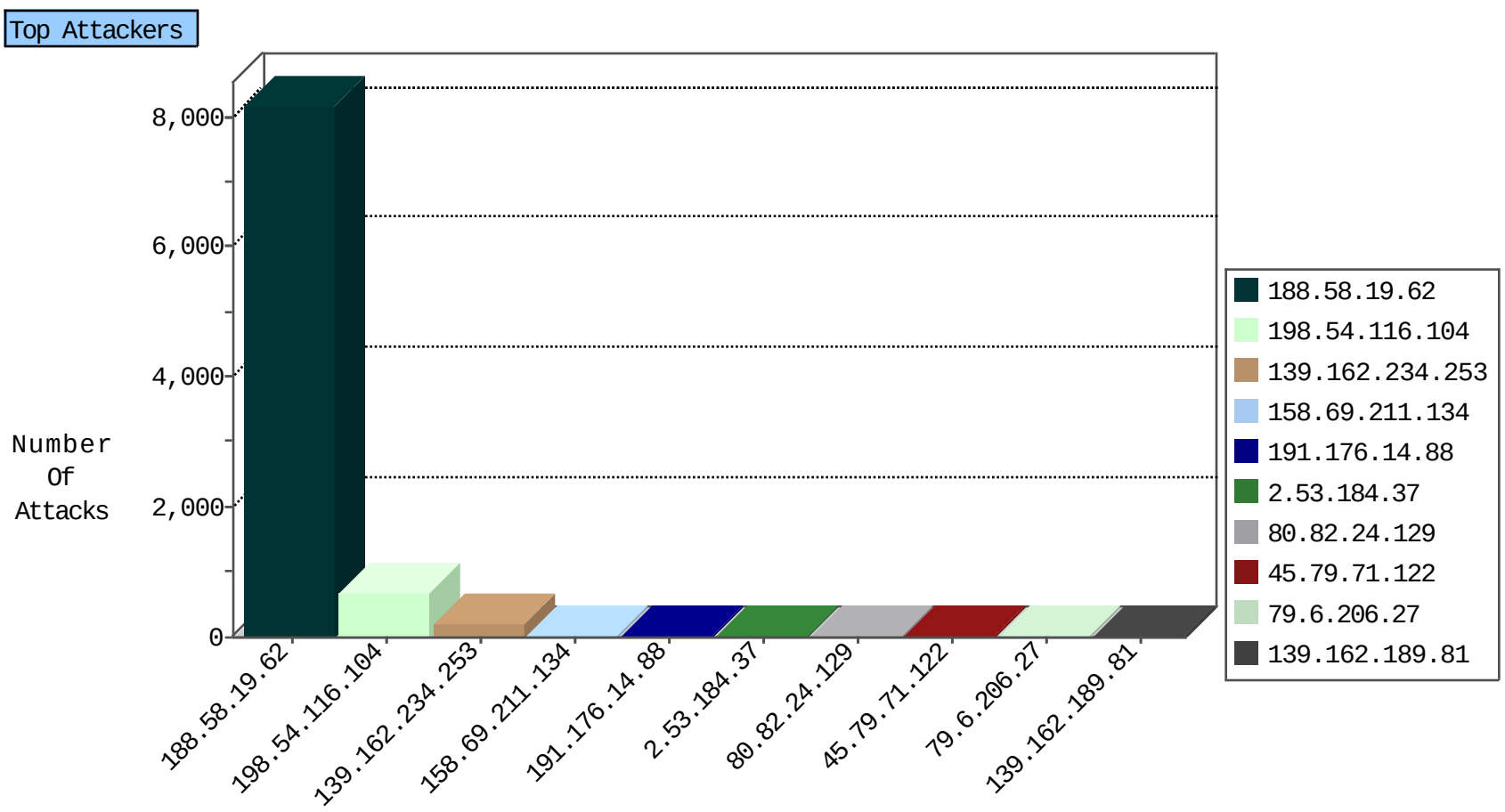
09-07-2016-01:10:20 to 09-07-2016-02:10:20

IDF Under Attack Daily Report





09-07-2016-01:10:20 to 09-07-2016-02:10:20

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
218.92.147.81	China	147.237.77.227	e.hamaz.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
94.102.56.181	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1

09-07-2016-01:10:20 to 09-07-2016-02:10:20

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.148.247	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-07-2016-01:10:20 to 09-07-2016-02:10:20

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
139.162.189.81	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
91.121.184.8	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
45.79.71.122	147.237.0.34	United States	tikshuv.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
66.249.64.8	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
195.16.127.148	147.237.76.148	Russian Federation	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
195.16.127.148	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
191.109.107.236	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.232.98.38	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
104.232.98.38	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -f -sS	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
58.140.165.41	147.237.76.34	Korea, Republic of	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.16.127.148	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
195.16.127.148	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
178.220.165.231	147.237.76.199		e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
139.59.4.16	147.237.76.86	Singapore	navy.idf.il	ET SCAN Potential SSH Scan	1
104.232.98.38	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

09-07-2016-01:10:20 to 09-07-2016-02:10:20

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.58.19.62	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8175
198.54.116.104	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	654
139.162.234.253	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
139.162.234.253	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
139.162.234.253	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
139.162.234.253	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
139.162.234.253	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
139.162.234.253	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
139.162.234.253	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
139.162.234.253	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
79.6.206.27	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
139.162.234.253	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
139.162.234.253	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
80.82.24.129	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
139.162.234.253	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
191.176.14.88	Brazil	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	7
139.162.234.253	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
139.162.234.253	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
139.162.234.253	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
139.162.234.253	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
139.162.234.253	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
185.32.179.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
139.162.236.251	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
139.162.234.253	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
139.162.234.253	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
139.162.234.253	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
139.162.234.253	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
139.162.234.253	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
139.162.234.253	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
158.69.211.134	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
158.69.211.134	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
185.120.124.49	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
158.69.211.134	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
68.33.90.133	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
191.176.14.88	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
158.69.211.134	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.26.148.160	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
191.176.14.88	Brazil	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
185.32.179.70	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
158.69.211.134	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
158.69.211.134	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
192.169.7.223	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
187.61.110.201	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
86.90.205.80	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
24.0.111.69	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
157.55.12.74	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
158.69.211.134	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
158.69.211.134	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.178.208.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

09-07-2016-01:10:20 to 09-07-2016-02:10:20

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.184.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Distributed Unknown HTTP Request Method	Block	2
207.46.13.93	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
176.13.238.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Distributed Malformed URL	Block	2
80.82.24.129	Poland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/edim/theproj/theproj.asp	Block	1
46.19.86.44	Israel	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method akpotnt1yugp5 in URL	Block	1
196.207.44.209	South Africa	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
139.162.189.81	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 139.162.189.81 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/kapatz/contactus.aspx	Block	1
207.46.13.57	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	1
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Malformed HTTP Header Line 1	Block	1
139.162.189.81	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.116	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/agrigats.aspx	Block	1
71.86.197.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
45.79.71.122	United States	147.237.0.34	tikshuv.idf.il	Multiple Malformed HTTP Header Line from 45.79.71.122	Block	1
139.162.189.81	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
66.249.65.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar/dover.aspx/	Block	1
77.139.100.37	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
46.19.86.44	Israel	147.237.0.34	tikshuv.idf.il	Malformed URL	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/	Block	1

09-07-2016-01:10:20 to 09-07-2016-02:10:20