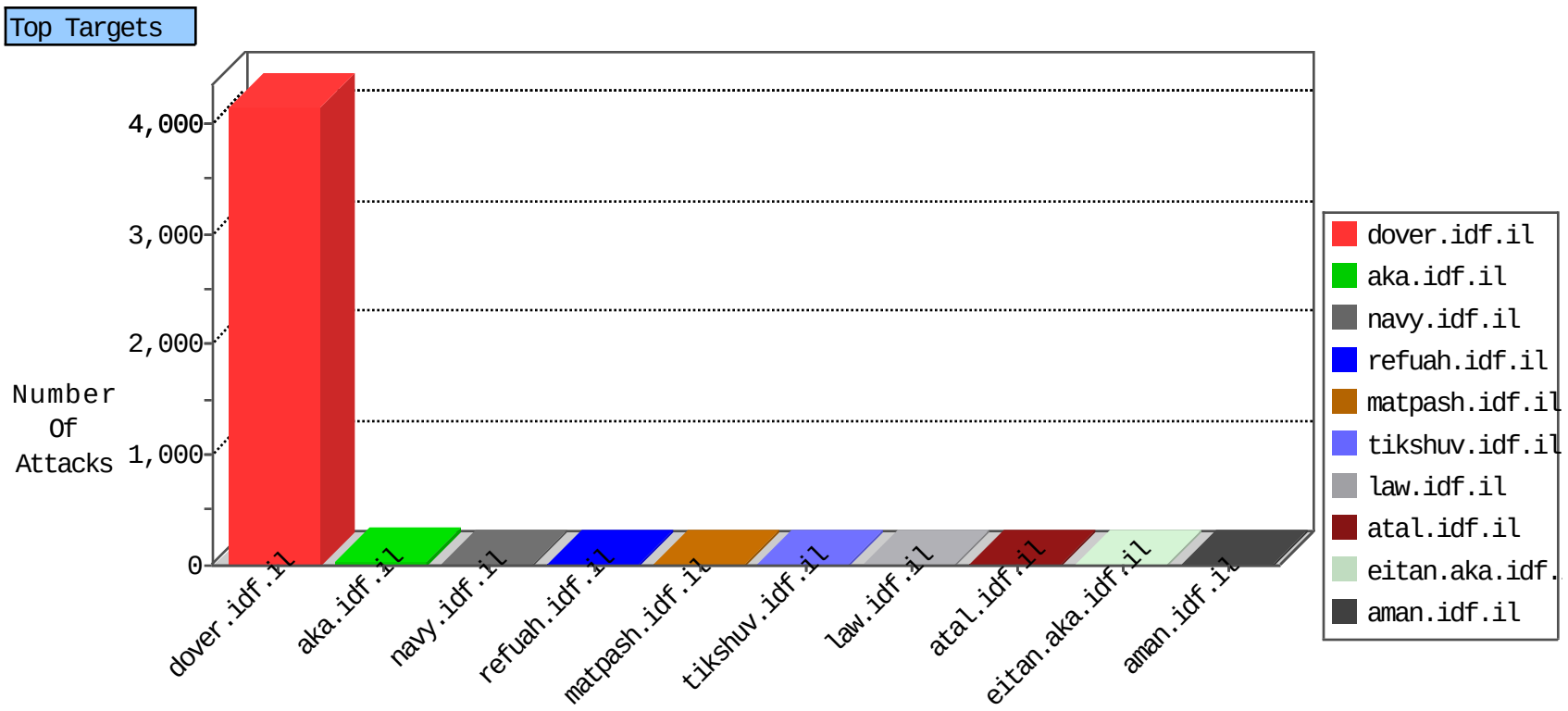
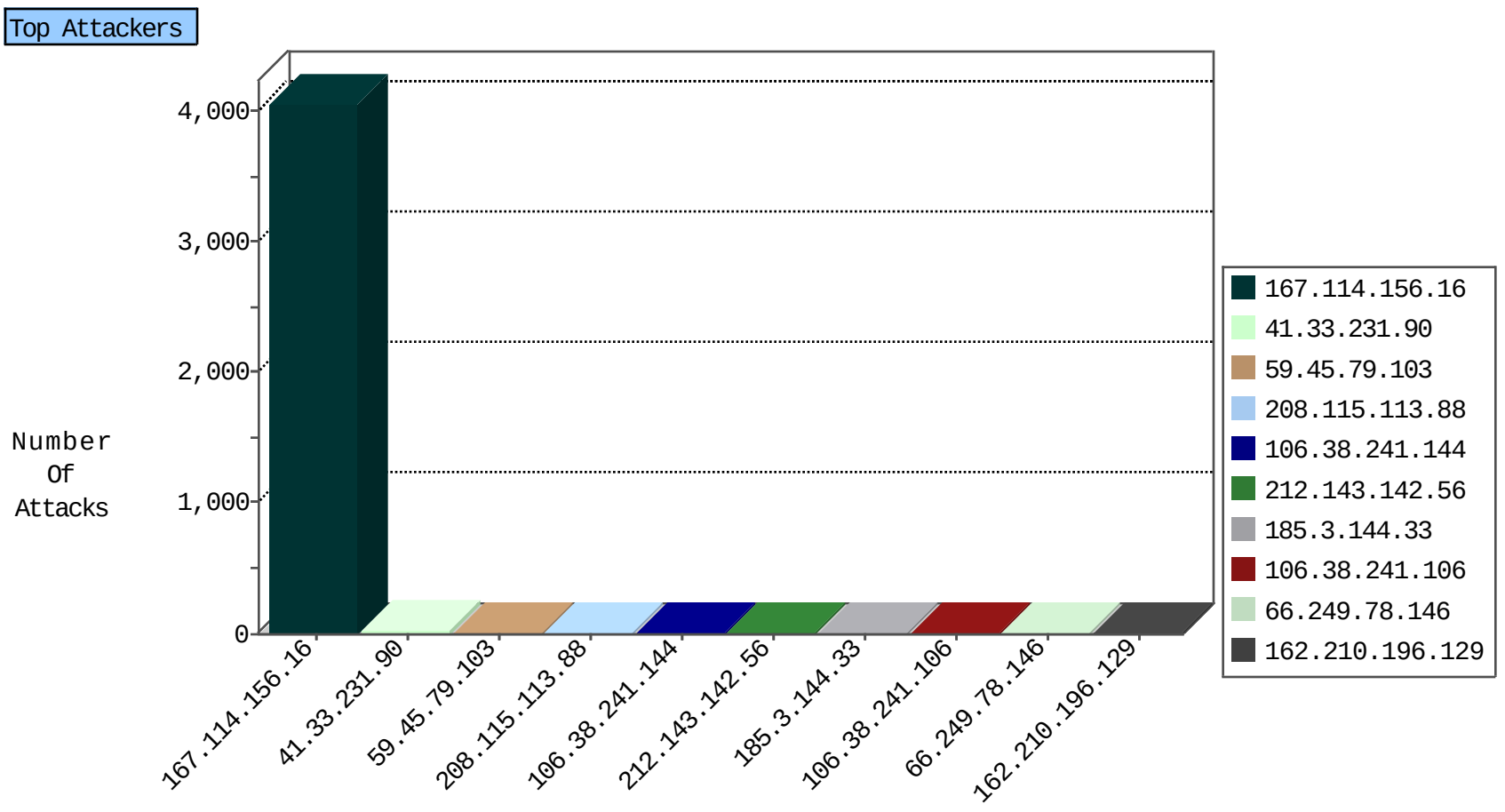
04-16-2016-07:04:03 to 04-16-2016-08:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-16-2016-07:04:03 to 04-16-2016-08:04:03

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	Block_Ip_Web_In	drop	4050
188.138.17.205	France	147.237.77.74	law.idf.il	Block_Udp_All_Nets_Con_Limit	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
184.105.139.67	United States	147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	1
216.218.206.107	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1

04-16-2016-07:04:03 to 04-16-2016-08:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
84.228.19.26	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
162.210.196.129	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
69.197.169.202	United States	147.237.77.233	atal.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
109.66.23.97	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-16-2016-07:04:03 to 04-16-2016-08:04:03

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
59.45.79.103	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
218.194.224.49	147.237.77.176	China	matpash.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
59.45.79.103	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
13.92.246.145	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
124.83.33.93	147.237.76.30	Philippines	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.103	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.76.202	Latvia	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.4.79.76	147.237.77.235	Germany	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
185.112.248.50	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.8.27		e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.103	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

04-16-2016-07:04:03 to 04-16-2016-08:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.6.151.254	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
99.238.125.103	Canada	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
178.154.189.8	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.83.142	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
36.80.0.207	Indonesia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.158.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
157.55.39.44	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
176.58.74.72	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.184.3.122	Japan	147.237.0.35	akaws.idf.il	drop		drop	1
77.125.1.92	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
182.75.169.10	India	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.214	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.32	United States	147.237.0.33	idf.il	drop		drop	1
184.105.247.251	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.184.3.122	Japan	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
77.125.1.92	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
50.117.87.151	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.84	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.215	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
99.238.125.103	Canada	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.32	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.251	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.53.175.52	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.184.3.122	Japan	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.207	United States	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
100.72.224.48		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.32	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
182.75.169.10	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
5.22.130.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
120.132.84.137	China	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.82.64.37	Netherlands	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.212	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
159.226.95.66	China	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
104.148.44.145	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.52	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
182.75.169.10	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
94.102.49.54	Netherlands	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.7	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.214	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

04-16-2016-07:04:03 to 04-16-2016-08:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	6
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/yoman.asp	Block	2
2.53.13.236	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	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
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
180.76.15.145	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9710-he/refuah.aspx	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18457-he/dover.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/unitfs.asp	Block	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 185.3.144.33	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/937-he/refuah.aspx	Block	1
2.53.151.194	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover	Block	1
207.46.13.57	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/scripts/generalfunctions.js	Block	1
95.35.66.147	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
2.55.129.213	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/scripts/site.js	Block	1
141.212.122.209	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
46.1.89.22	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/huhu123	Block	1

04-16-2016-07:04:03 to 04-16-2016-08:04:03