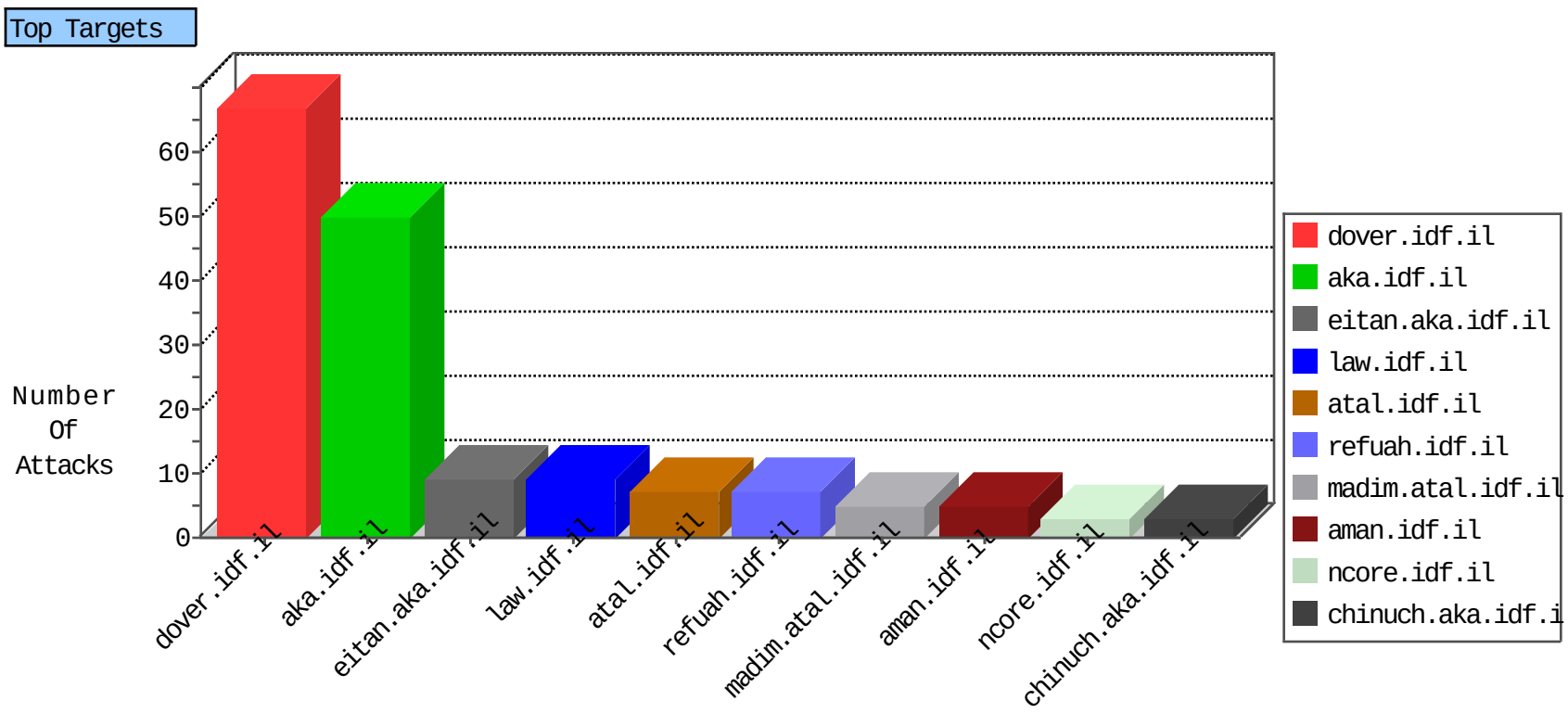
02-06-2016-03:04:01 to 02-06-2016-04:04:01

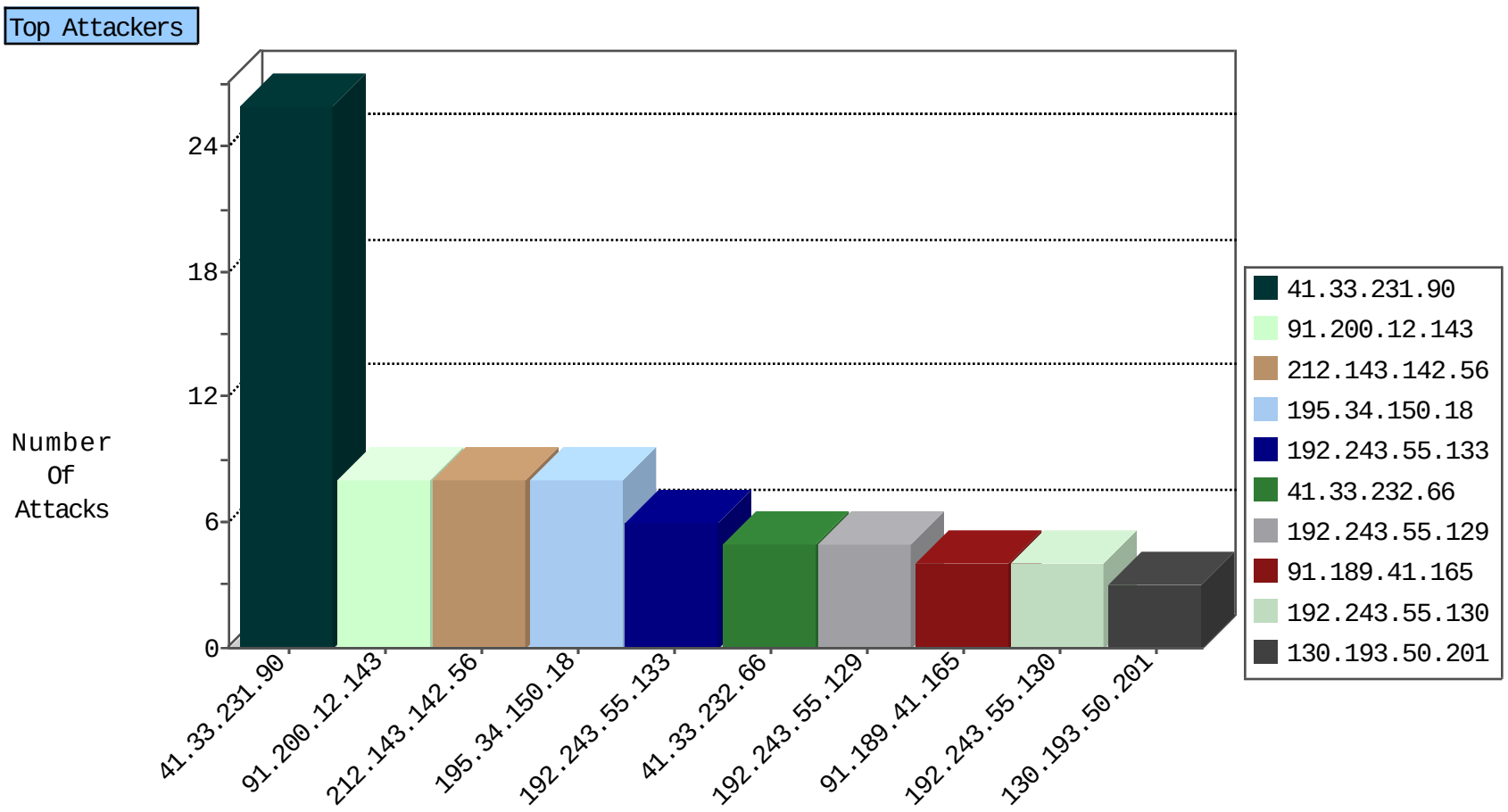
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-06-2016-03:04:01 to 02-06-2016-04:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
219.79.214.170	Hong Kong	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	3
122.190.64.80	China	147.237.72.156	aman.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
188.93.234.208	Portugal	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
198.20.70.114	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

02-06-2016-03:04:01 to 02-06-2016-04:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-06-2016-03:04:01 to 02-06-2016-04:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
187.161.147.150	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.231	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
191.254.241.92	147.237.76.196	Brazil	e.sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.231	147.237.76.34		yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
123.203.18.100	147.237.8.28	Hong Kong	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-06-2016-03:04:01 to 02-06-2016-04:04:01

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	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.143	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
91.200.12.143	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
109.67.184.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.50.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.176.56.176	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
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
46.19.85.41	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
64.12.116.76	United States	147.237.77.216	dover.idf.il	drop		drop	2
173.252.122.116	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
66.249.65.88	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.78.239	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
172.56.36.103	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
188.152.234.175	Italy	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
64.12.116.198	United States	147.237.77.216	dover.idf.il	drop		drop	2
68.180.231.40	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
173.252.115.88	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
105.202.7.205	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.8.132.67	Russian Federation	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.14	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
213.57.218.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.121.86.198	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
146.185.239.102	Russian Federation	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
82.118.236.27	Bulgaria	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
64.12.116.142	United States	147.237.77.216	dover.idf.il	drop		drop	1
185.3.147.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
128.194.135.73	United States	147.237.72.156	aman.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.121.86.198	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.1.101.123	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
64.12.116.144	United States	147.237.77.216	dover.idf.il	drop		drop	1
128.194.135.73	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
68.48.27.242	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.121.96.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.1.101.123	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
5.22.131.72	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
173.252.80.112	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.41	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
188.152.234.175	Italy	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
37.26.149.177	Israel	147.237.72.166	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
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	6
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	5
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.130	Block	4
91.189.41.165	Sweden	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.189.41.165	Block	3
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	3
2.52.182.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.198	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
82.81.39.199	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.65.122	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/news/{"key":"	Block	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	1
98.143.148.107	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/check	Block	1
208.113.160.6	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/test/wp-admin/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/hovot/templates/main.asp	Block	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	1
161.58.148.113	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
66.249.65.152	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
66.249.78.233	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.233	Block	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/klali.aspx	Block	1
180.76.15.153	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/1105-en/contactus.aspx	Block	1
91.189.41.165	Sweden	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1242-he/atal.aspx	Block	1
194.187.168.216	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.80	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/61998	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
184.95.37.155	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/wordpress/wp-admin/	Block	1
91.203.41.15	Sweden	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.69.84	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	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
157.55.39.82	United States	147.237.72.166	aka.idf.il	Unknown Parameter 55bffe68 in www.aka.idf.il/main/home/default.aspx	None	1
74.6.53.161	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/wp-admin/	Block	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	1
95.32.154.11	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/configuration.old	Block	1
198.8.90.65	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	1