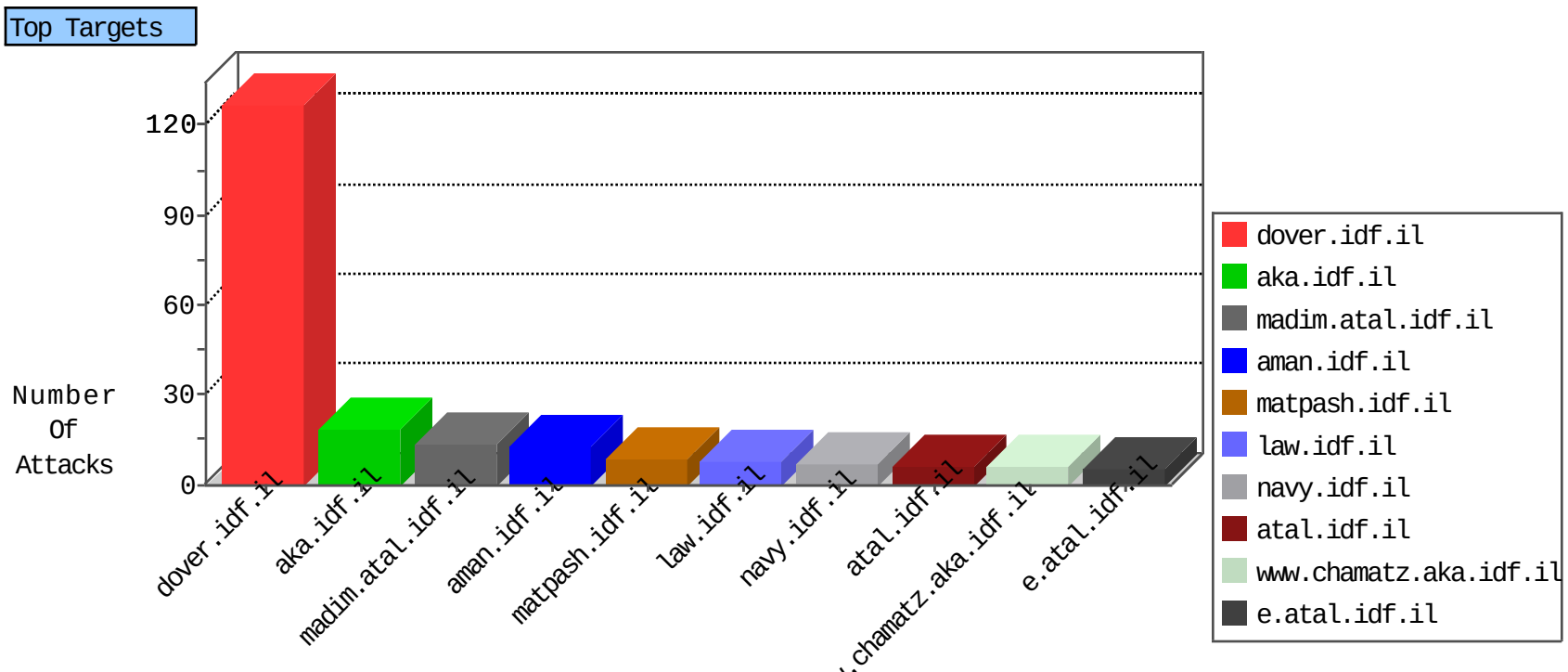
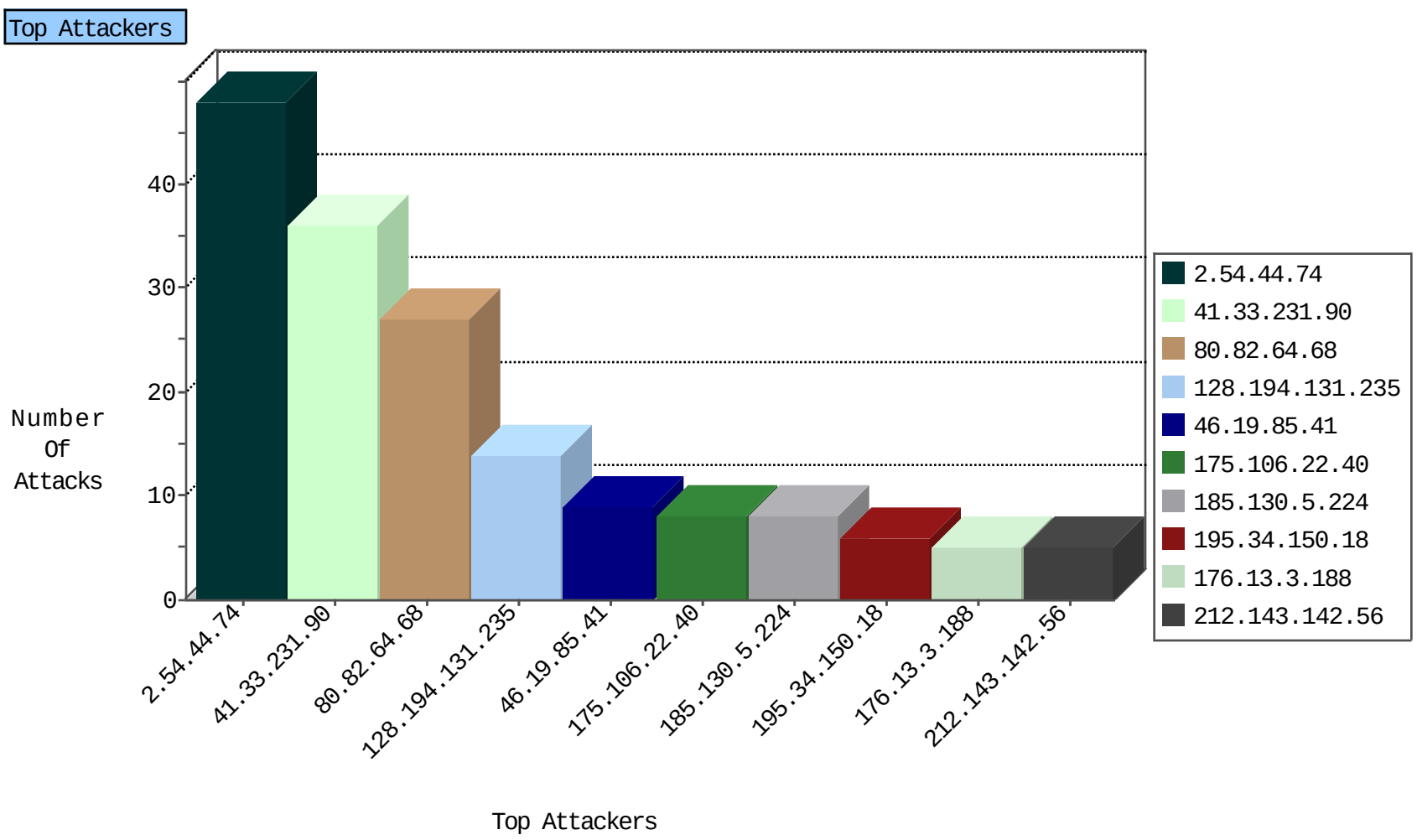
02-11-2016-05:04:05 to 02-11-2016-06:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-11-2016-05:04:05 to 02-11-2016-06:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.224		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.228		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.228		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
114.154.186.88	Japan	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

02-11-2016-05:04:05 to 02-11-2016-06:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-11-2016-05:04:05 to 02-11-2016-06:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.153	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
185.35.62.39	147.237.72.167	Switzerland	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.68	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.77.243	Turkey	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.45.137.67	147.237.77.178	Turkey	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
121.201.27.61	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
108.59.248.198	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
49.236.206.129	147.237.0.17	Malaysia	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.77.216	Turkey	dover.idf.il	ET SCAN NMAP -sS window 1024	1

02-11-2016-05:04:05 to 02-11-2016-06:04:05

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
2.54.44.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
2.54.44.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
175.106.22.40	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.54.44.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.44.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
128.194.131.235	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
128.194.131.235	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
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
79.182.133.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.82.64.68	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
2.52.48.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.82.64.68	Netherlands	147.237.77.233	atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
2.54.44.74	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	3
2.54.44.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
80.82.64.68	Netherlands	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
117.239.56.35	India	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
40.77.167.73	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
54.67.47.113	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
54.193.40.51	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
141.212.122.203	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.24	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.219	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.82.64.68	Netherlands	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
158.130.6.191	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.6	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
81.169.237.146	Germany	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
80.82.64.68	Netherlands	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.82.64.68	Netherlands	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.204	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.47	China	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
80.82.64.68	Netherlands	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.252	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.82.64.68	Netherlands	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
158.130.6.191	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.39	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.232.110.29	United Kingdom	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
95.211.168.182	Netherlands	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.72	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.82.64.68	Netherlands	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.74	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.82.64.68	Netherlands	147.237.76.34	yohalan.idf.il	drop		drop	1
158.130.6.191	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.47	China	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
80.82.64.68	Netherlands	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
80.82.64.68	Netherlands	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
165.91.12.68	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
74.82.47.60	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

02-11-2016-05:04:05 to 02-11-2016-06:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.41	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	9
176.13.3.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	2
165.91.12.68	United States	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 165.91.12.68	Block	2
128.194.131.235	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
80.82.64.68	Netherlands	147.237.77.176	matpash.idf.il	Unauthorized URL Access to iwannaknow.tk/index.php	Block	1
86.123.247.100	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/).html(	Block	1
66.249.78.184	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
142.255.42.29	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
80.82.64.68	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to iwannaknow.tk/index.php	Block	1
197.52.174.155	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
96.244.197.50	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
142.255.42.29	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
80.82.64.68	Netherlands	147.237.77.233	atal.idf.il	Unauthorized URL Access to iwannaknow.tk/index.php	Block	1
2.223.235.190	United Kingdom	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	1
116.39.11.142	Korea, Republic of	147.237.77.74	law.idf.il	PHP Attempt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
86.123.247.100	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
2.223.235.190	United Kingdom	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
116.39.11.142	Korea, Republic of	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
74.82.47.3	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
86.123.247.100	Romania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 86.123.247.100	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1065-he/dover.aspx	Block	1

02-11-2016-05:04:05 to 02-11-2016-06:04:05