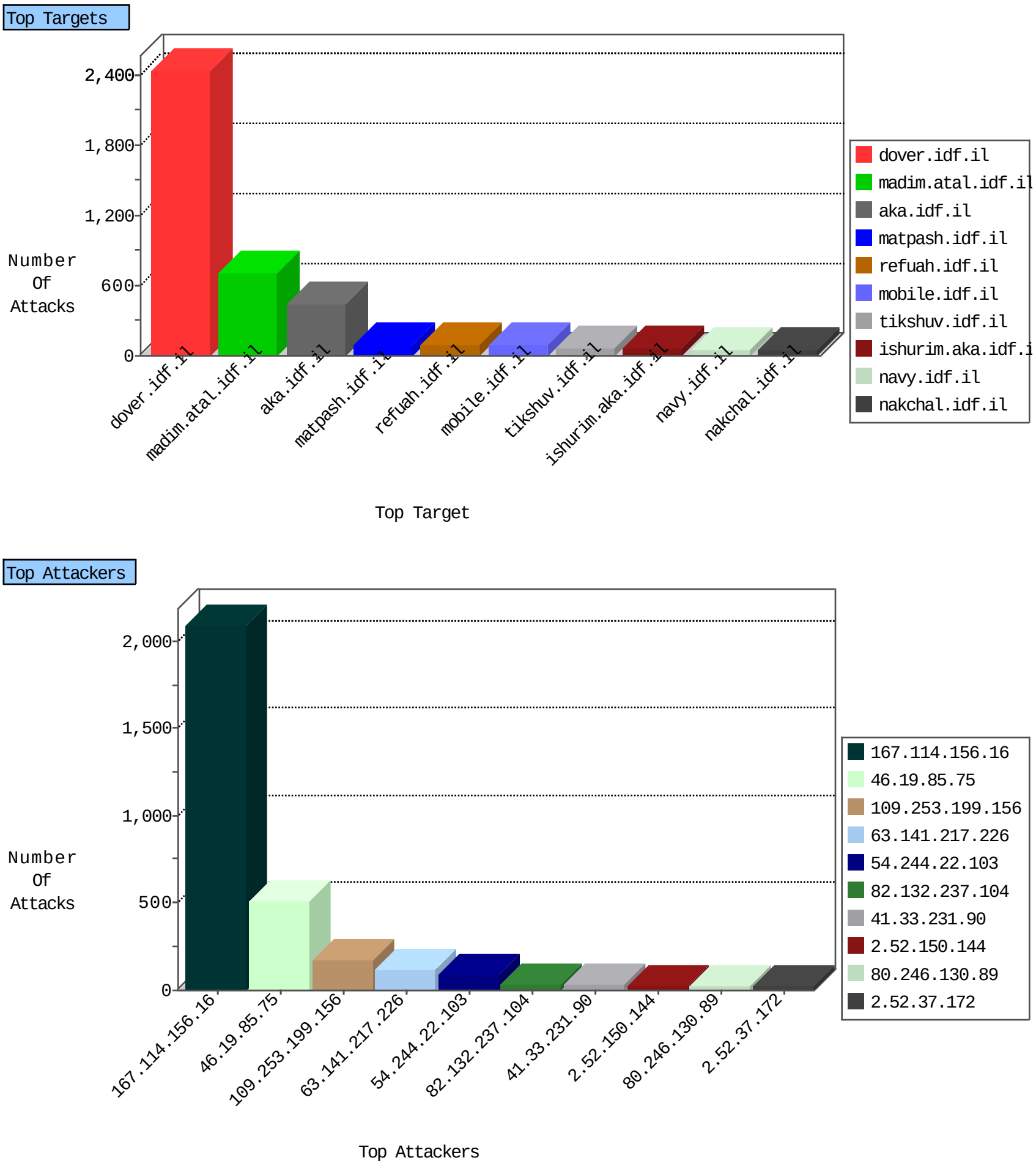
01-13-2016-14:04:05 to 01-13-2016-15:04:05

IDF Under Attack
Daily Report



01-13-2016-14:04:05 to 01-13-2016-15:04:05

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	DOS-Tool-SwitchbladG	dest-reset	3020
80.179.92.46	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	30
194.90.217.36	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
79.177.11.229	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.177.11.229	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	6
46.19.86.15	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
84.94.43.81	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
192.118.78.200	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
192.117.134.156	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
107.150.55.214	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
142.54.160.210	United States	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
149.88.229.119	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
107.150.60.246	United States	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
63.141.227.98	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
142.54.169.162	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
107.150.60.246	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
199.203.215.1	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
142.54.169.165	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
107.150.55.212	United States	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
113.254.233.249	Hong Kong	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

01-13-2016-14:04:05 to 01-13-2016-15:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
175.9.139.89	China	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

01-13-2016-14:04:05 to 01-13-2016-15:04:05

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	2
117.25.155.164	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
85.250.199.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.89.41	147.237.0.34	Israel	tikshuv.idf.il	GPL SCAN nmap TCP	1
207.232.27.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.59.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.151.53.196	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.247	147.237.76.201		e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.68.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.14.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
24.153.158.106	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.136.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
117.25.155.164	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -f -sS	1
84.94.59.38	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.200.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.68	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
199.203.196.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
68.180.229.239	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
188.161.107.114	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.247.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.216	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
24.153.158.106	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -f -sS	1
158.255.6.220	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

01-13-2016-14:04:05 to 01-13-2016-15:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
63.141.217.226	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	120
82.132.237.104	United Kingdom	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	27
80.246.130.89	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
2.52.150.144	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	18
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
46.19.86.214	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
54.244.22.103	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
212.179.28.215	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
82.166.140.117	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
109.253.202.21	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
2.54.10.186	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.61.226	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.102.9.107	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	10
2.52.37.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
82.166.219.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.228.230.48	Bulgaria	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.19.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.14.153	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.109.125.50	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
176.13.22.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.117.135.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
54.244.22.103	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.73	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.49.152	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
62.219.46.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.54.31.7	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.171.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.129.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.188.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.149.220	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.139.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
173.208.136.170	United States	147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
89.139.140.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
85.250.187.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.73	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.182.82	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.18.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.118.78.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
185.32.179.94	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.154	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

01-13-2016-14:04:05 to 01-13-2016-15:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	299
46.19.85.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
109.253.199.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	104
46.19.85.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	100
109.253.199.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
109.66.58.124	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
17.138.57.83	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.57.83	Block	10
197.134.238.71	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	8
197.134.238.71	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	8
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
212.199.224.24	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 212.199.224.24	Block	7
62.219.119.136	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	5
109.65.178.221	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
79.177.60.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	4
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	3
176.13.19.37	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.171.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.147	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
176.13.14.153	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.143.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	3
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
213.151.48.39	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.151.48.39	Block	2
212.117.143.250	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	2
84.228.230.48	Bulgaria	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
84.94.38.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	2
46.19.85.147	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.85.147	Block	2
85.65.22.88	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
95.25.133.27	Russian Federation	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 95.25.133.27	Block	2
176.13.2.94	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/forgotpassword.aspx parameter	None	2
46.19.86.10	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
212.76.99.52	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.76.99.52	Block	2
62.219.119.136	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.219.119.136	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
62.219.119.136	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	2
46.19.86.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.25.133.27	Russian Federation	147.237.76.86	navy.idf.il	WEB MISC Unauthorized File Access	None	1
212.199.224.24	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/general/general_title_r.gif	Block	1
2.54.169.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.133.93	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	1
176.13.7.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
162.209.102.100	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.19.85.172	Israel	147.237.76.31	nakchal.idf.il	Illegal HTTP Version ASP.NET_SessionId=bm31gd45r15l1n45tsqwtxzp; __atuvc=2%7C52%2C1%7C2; __atuvs=569644db22defb18000	Block	1
93.125.99.34	Belarus	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
2.54.3.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
74.82.47.4	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.65.23	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1

01-13-2016-14:04:05 to 01-13-2016-15:04:05