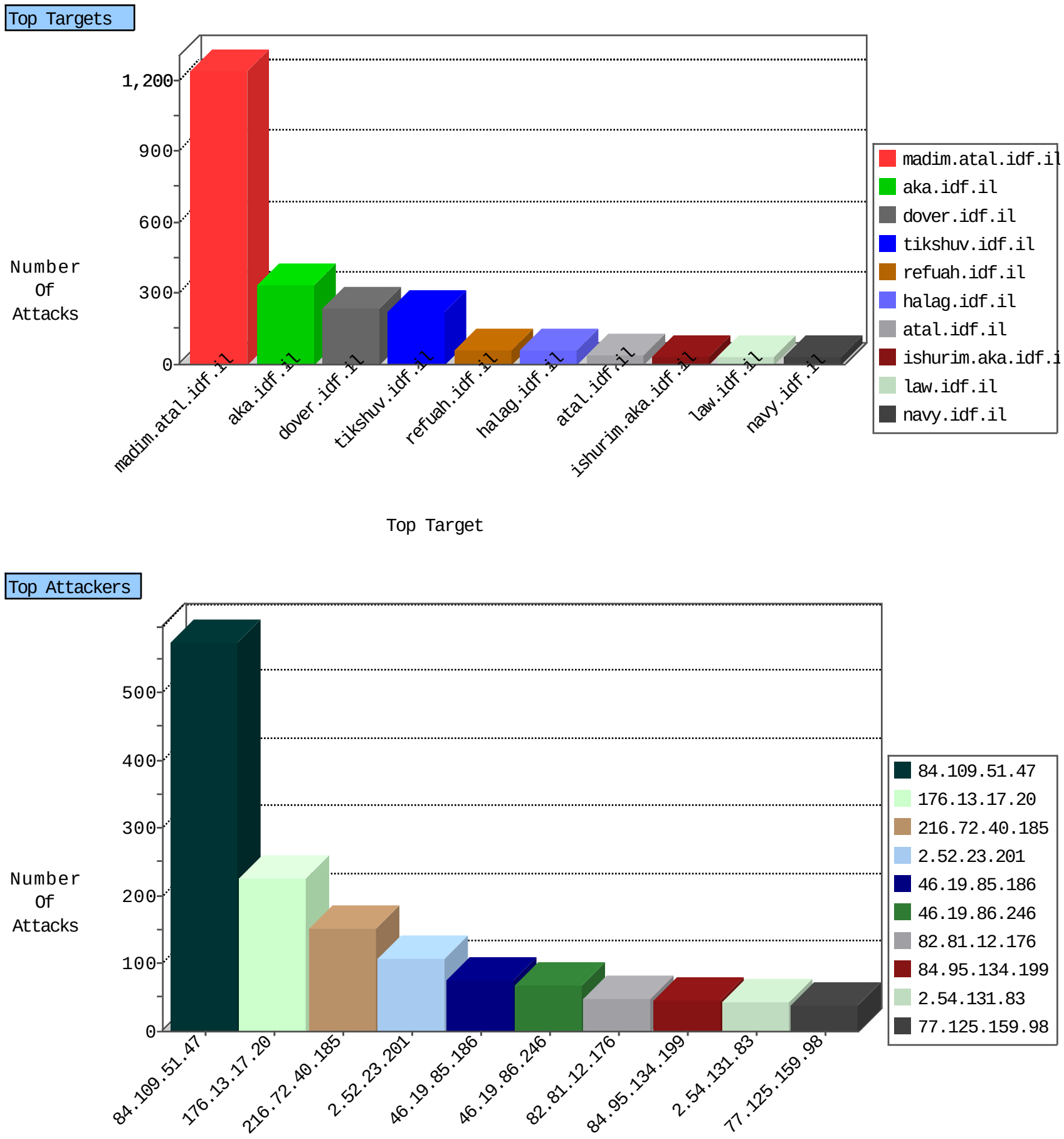
01-28-2016-15:04:01 to 01-28-2016-16:04:01

IDF Under Attack Daily Report



01-28-2016-15:04:01 to 01-28-2016-16:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	48
2.54.135.246	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
87.68.154.207	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
212.199.182.150	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
192.118.132.185	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Http	drop	2
85.105.123.40	Turkey	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
114.93.2.242	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
114.93.2.242	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
79.181.70.85	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
114.93.2.242	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
114.93.2.242	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

01-28-2016-15:04:01 to 01-28-2016-16:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-28-2016-15:04:01 to 01-28-2016-16:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.81.198	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
62.90.147.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
137.117.168.203	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.100.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.216.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.154.94.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.189.191	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.183.201.2	147.237.77.233	Ukraine	atal.idf.il	ET SCAN Potential SSH Scan	1
85.64.15.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.76.201		e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.23.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.214.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
203.156.189.226	147.237.0.16	Thailand	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
66.240.219.146	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
137.117.168.203	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.210.227.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
137.117.168.203	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.67.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.202.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.3.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.130.171.84	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.31.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.194.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.6.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.249.162	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-28-2016-15:04:01 to 01-28-2016-16:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.95.134.199	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.64.71.176	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
66.102.9.119	United States	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	15
176.13.18.5	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
176.13.18.5	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.52.23.201	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.138	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.210.147.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.74	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.199.196.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
147.235.8.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
147.235.8.38	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.126.118.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.80.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.80.135.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.145.43.166	United Kingdom	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.230.20.52	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.193.120	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.219	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.136.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
109.64.71.176	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
50.62.208.40	United States	147.237.77.234	halag.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
192.232.237.124	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
216.172.189.93	United States	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.54.142.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
143.95.197.199	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
149.78.10.22	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
187.45.193.167	Brazil	147.237.77.74	law.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
2.54.142.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
109.199.124.52	Bulgaria	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
72.55.168.69	Canada	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
187.45.195.13	Brazil	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
74.208.77.114	United States	147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
50.116.75.183	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.54.142.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.142.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5

01-28-2016-15:04:01 to 01-28-2016-16:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.109.51.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	297
84.109.51.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	270
176.13.17.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	225
216.72.40.185	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	152
2.52.23.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	95
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
46.19.86.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
2.54.131.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
77.125.159.98	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	39
213.57.135.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
109.253.206.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
46.19.85.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
93.173.4.141	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
2.54.12.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
46.19.86.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	10
84.109.51.47	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 84.109.51.47	Block	7
176.13.12.20	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	6
2.54.142.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
185.32.179.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.175.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.150.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
217.165.93.177	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
2.54.35.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.179.134.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.136.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.213.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
36.232.57.67	Taiwan	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	2
185.89.217.231		147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
194.208.45.10	Austria	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
185.89.217.232		147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
69.171.231.225	United States	147.237.72.166	aka.idf.il	Post Request - Missing Content Type	Block	2
37.26.148.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.136.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed 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
185.89.217.227		147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.148.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.160.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
192.232.201.18	United States	147.237.72.166	aka.idf.il	Unknown Parameter author in www.aka.idf.il/	None	2
176.13.20.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
36.232.57.67	Taiwan	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
79.179.188.146	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/home.aspx	Block	1
2.54.25.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.186.173.3	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
192.232.201.18	United States	147.237.72.166	aka.idf.il	Unknown Parameter author in www.aka.idf.il/main/home/default.aspx	None	1
179.53.147.21	Dominican Republic	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.50.100.110	United States	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
80.246.136.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.150.220	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1

01-28-2016-15:04:01 to 01-28-2016-16:04:01