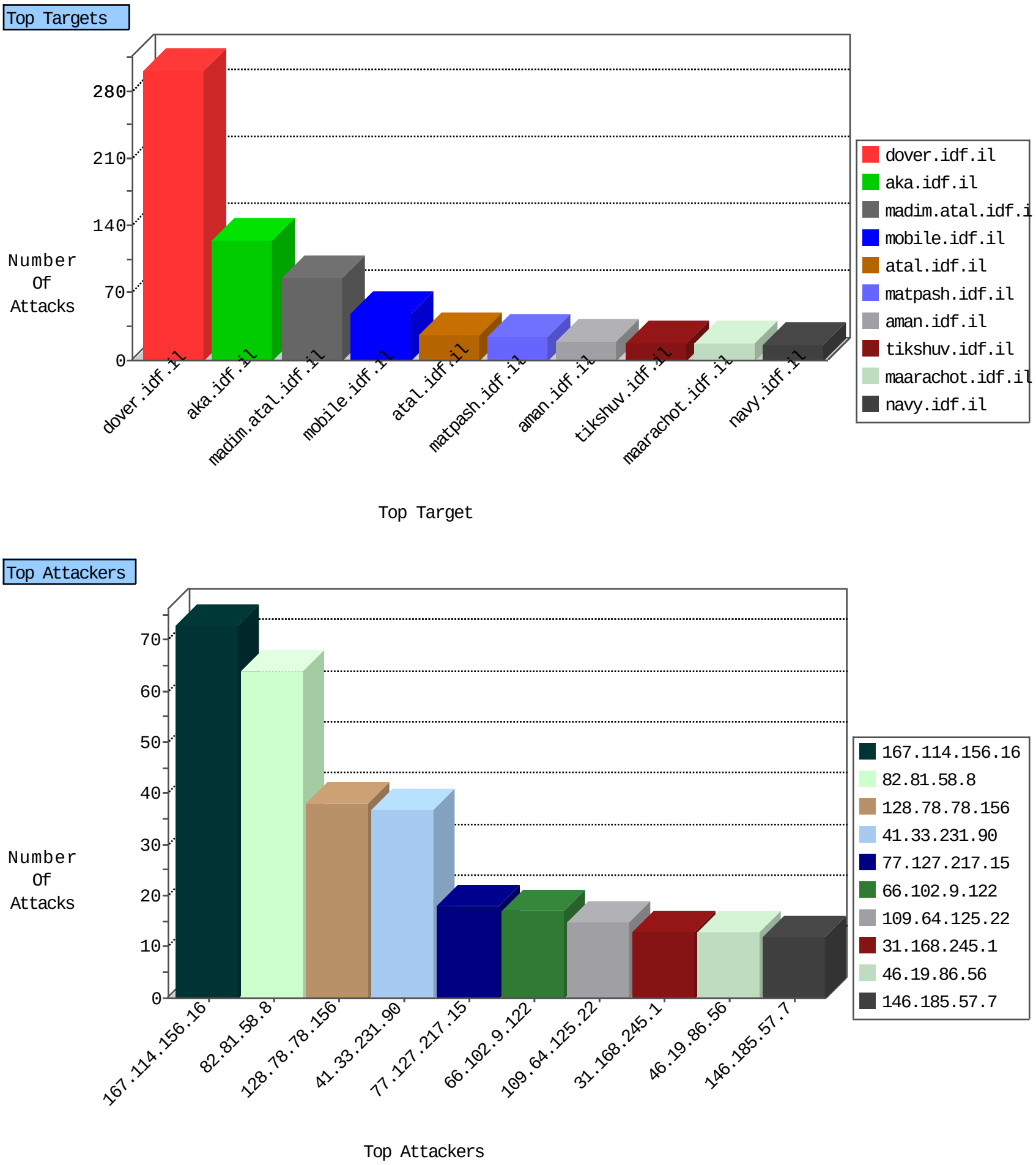
01-09-2016-14:04:09 to 01-09-2016-15:04:09

IDF Under Attack
Daily Report



01-09-2016-14:04:09 to 01-09-2016-15:04:09

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	1401
128.78.78.156	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
208.54.37.255	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
78.21.25.198	Belgium	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
146.185.57.7	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	6
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
146.185.57.7	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
109.64.3.34	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
178.151.196.124	Ukraine	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
79.178.138.67	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
89.248.174.4	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
146.185.239.100	Russian Federation	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
107.150.60.245	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
128.78.78.156	France	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
107.150.55.214	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.130.5.224		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
107.150.60.77	United States	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
107.150.60.242	United States	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1

01-09-2016-14:04:09 to 01-09-2016-15:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.145	Italy	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1

01-09-2016-14:04:09 to 01-09-2016-15:04:09

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
192.198.151.43	147.237.72.166	Europe	aka.idf.il	ET SCAN NMAP -sA (2)	2
183.60.252.84	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 2048	1
52.90.147.148	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
212.129.55.113	147.237.0.200	France	m4u.idf.il	ET SCAN Potential SSH Scan	1
212.129.55.113	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 4096	1
98.119.105.221	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -f -sS	1
212.129.55.113	147.237.8.28	France	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
212.129.55.113	147.237.0.35	France	akaws.idf.il	ET SCAN Potential SSH Scan	1

01-09-2016-14:04:09 to 01-09-2016-15:04:09

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
77.127.217.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.102.9.122	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	17
109.64.125.22	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
43.255.176.89	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.148.186	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
31.168.245.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.182.187.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.51		147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.65.50.15	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
31.168.245.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
128.78.78.156	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
109.67.205.199	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
128.78.78.156	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.64.154.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
128.78.78.156	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
85.65.89.177	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	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
146.185.56.178	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
84.229.35.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.147.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.54.48.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.59.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.182.160.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
208.54.37.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.177.187.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.143.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
37.26.147.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
85.130.216.252	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
84.108.87.88	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.224.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.183.108.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.48.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.175.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.72.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
78.21.25.198	Belgium	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.148.200	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
157.55.39.2	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.22.130.117	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
149.78.165.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.102.253.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
78.21.25.198	Belgium	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
37.46.39.240	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.130.121	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

01-09-2016-14:04:09 to 01-09-2016-15:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.58.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
46.19.86.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
46.19.86.239	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.239	Block	6
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	4
176.13.6.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.65.230.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
109.253.198.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
93.45.50.229	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	3
37.142.228.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.54.50.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
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
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	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
185.58.73.50	Croatia	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
50.87.12.21	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
216.218.207.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
109.186.4.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.162	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/links.aspx	Block	1
91.185.208.141	Slovenia	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
79.182.187.70	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2351.jpg	Block	1
46.117.255.189	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
216.194.173.26	United States	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
31.168.23.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.75	Block	1
85.65.54.28	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
188.143.232.21	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
51.255.202.66	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.201.154.175	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
40.77.167.3	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/×³×ŸÂ¿Â½×³×ŸÂ¿Â½×³×ŸÂ¿Â½×³×ŸÂ¿Â½×³Â ×³×ŸÂ¿Â½×³Ã—	Block	1
207.232.21.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/aschar	Block	1
91.185.208.141	Slovenia	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.mag.idf.il/xmlrpc.php	Block	1
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	1
176.13.13.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1882	Block	1
50.62.176.181	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
216.194.173.26	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/xmlrpc.php	Block	1
31.168.245.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.75	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1391-12626-e n/dover.aspx	Block	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/general.aspx?catid=61550	Block	1
78.46.4.54	Germany	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
62.128.48.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
84.109.94.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.154.41	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58625&docid=72420	Block	1

01-09-2016-14:04:09 to 01-09-2016-15:04:09