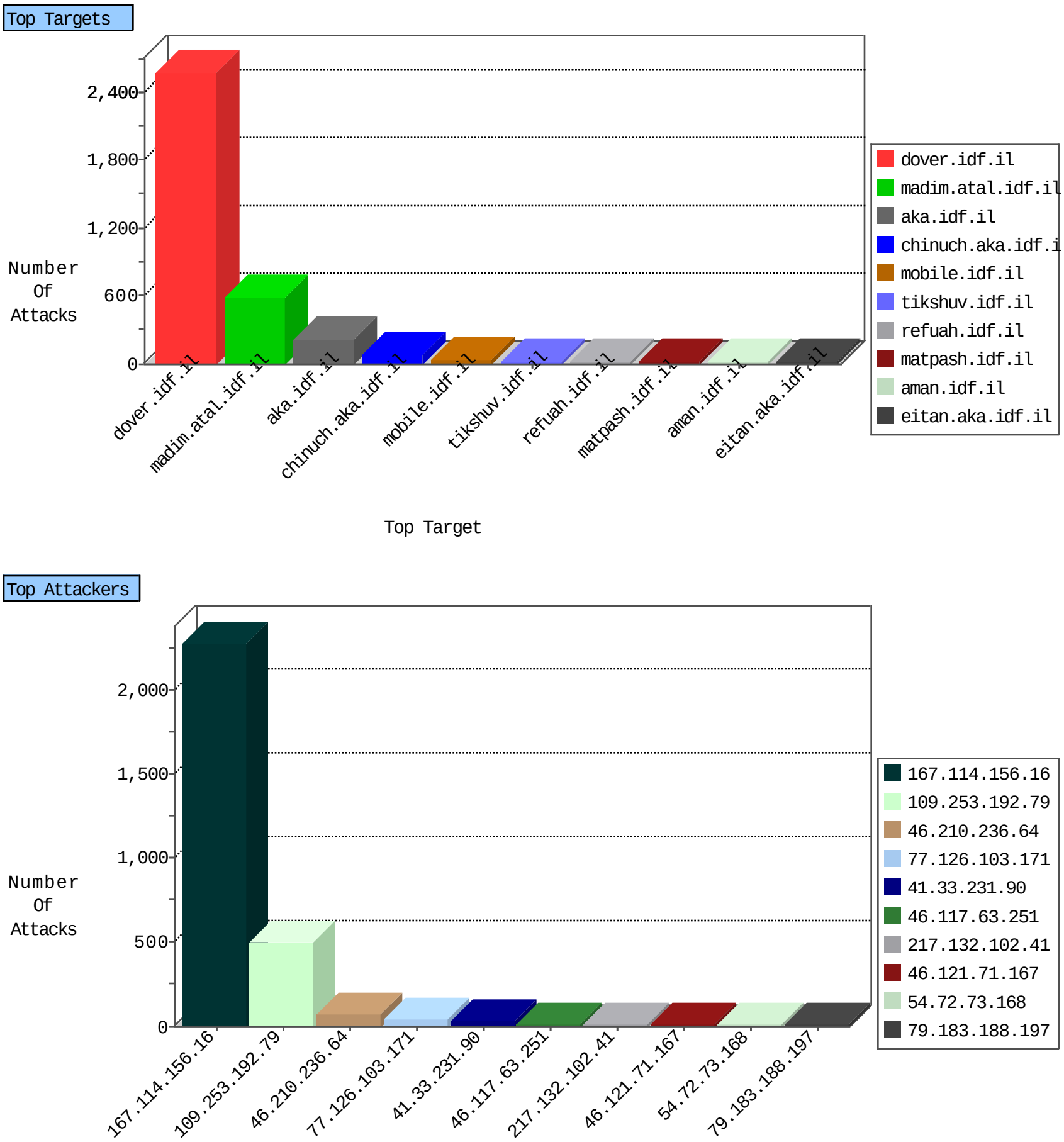
01-09-2016-17:04:08 to 01-09-2016-18:04:08

IDF Under Attack Daily Report



01-09-2016-17:04:08 to 01-09-2016-18:04:08

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	3738
66.249.66.31	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
40.77.167.42	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
207.46.13.75	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
45.35.64.142		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
157.55.2.150	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
120.89.105.229	Nepal	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.66.204.68	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
173.252.90.228	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
107.170.119.178	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
41.33.231.90	Egypt	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	F_Dover_Under_Attack_Con_Http	drop	2
207.46.13.123	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
89.108.144.114	Lebanon	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
173.252.90.228	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
65.55.213.25	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
107.150.55.210	United States	147.237.76.31	nakchal.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
107.150.60.78	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
142.54.160.213	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
43.255.176.89	Japan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

01-09-2016-17:04:08 to 01-09-2016-18:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-09-2016-17:04:08 to 01-09-2016-18:04:08

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
27.189.88.81	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
158.255.2.52	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
131.100.80.110	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
106.75.199.201	147.237.77.226	China	www.chamatz.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
103.6.223.61	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
200.203.100.12	147.237.76.176	Brazil	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.247	147.237.77.170		maarachot.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.22.84	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
131.100.80.110	147.237.0.19	Brazil	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
117.25.155.164	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
103.6.223.61	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
101.18.131.174	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.195	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.77.176	Ukraine	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
185.130.5.247	147.237.0.19		madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
168.62.238.153	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1

01-09-2016-17:04:08 to 01-09-2016-18:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2063
46.210.236.64	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
46.121.71.167	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
79.183.188.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
89.108.144.114	Lebanon	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
77.126.220.30	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
8.37.224.23	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.54.60.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.179.194.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.228.197.183	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.66.17.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.106.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.215.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.20.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
120.89.105.229	Nepal	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.127.148.178	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	5
2.52.58.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
93.172.166.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.62.27	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.166	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.121	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.180.106.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.109.13.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.180.102.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.177	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.102.253.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.68.146.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.88.53.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.97.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.253.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.68.240.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.75	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.176.164.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.170.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
43.255.176.89	Japan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
85.64.67.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
149.78.58.129	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	3

01-09-2016-17:04:08 to 01-09-2016-18:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.192.79	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.192.79	Block	295
109.253.192.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
109.253.192.79	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 109.253.192.79	Block	103
77.126.103.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
46.117.63.251	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 46.117.63.251	Block	17
217.132.102.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 217.132.102.41	Block	15
79.182.57.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
79.176.54.164	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	5
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	4
79.179.56.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.160.181.6	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	3
2.54.31.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.156.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.11.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
207.46.13.123	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
207.46.13.123	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/w/load.php	Block	2
109.253.201.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.169.42	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1437-he/atal.aspx	Block	2
79.182.213.175	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.182.213.175	Block	2
2.54.48.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.171.115	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.176.54.164	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.176.54.164	Block	1
66.249.64.185	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx	Block	1
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	1
88.235.100.72	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
185.32.179.84	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.183.134.48	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
79.178.30.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.168.67.217	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
2.52.62.117	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
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	1
77.126.92.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.69.216	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.166.186.198	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.161.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.194.166	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sip_storage/files/9/1849.pdf.	Block	1
2.54.154.41	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2278.jpg	Block	1
89.138.161.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.134.48	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
46.117.163.129	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.117.163.129	Block	1
185.32.179.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.75.213.91	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	1
2.52.174.237	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.115.168	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	1
217.132.102.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/default.asp	Block	1
84.228.78.60	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
46.166.186.206	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcdhphdmltxdezmzquzg9j&infocenteritem=true	Block	1

01-09-2016-17:04:08 to 01-09-2016-18:04:08