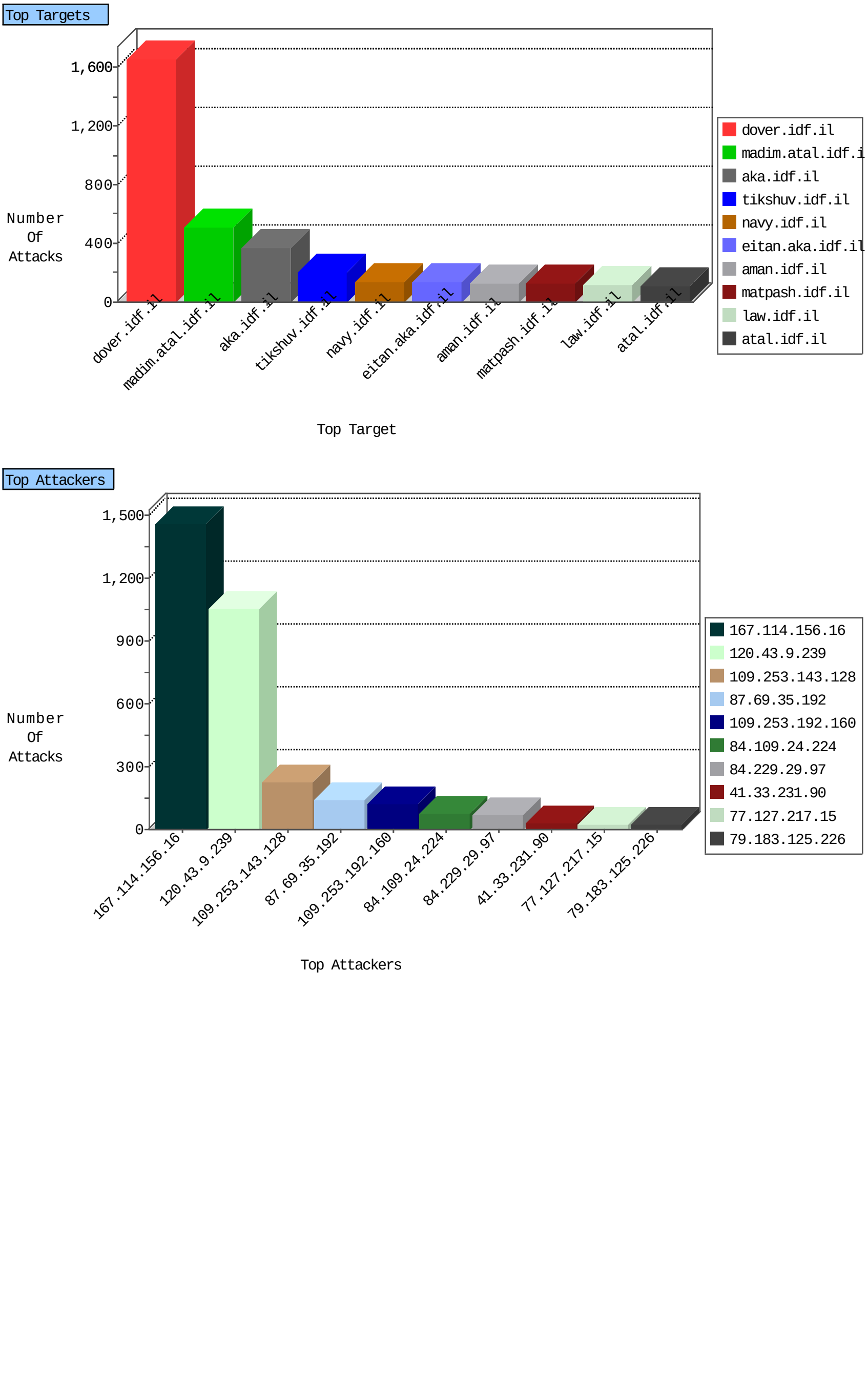
01-08-2016-16:04:09 to 01-08-2016-17:04:09

IDF Under Attack Daily Report



01-08-2016-16:04:09 to 01-08-2016-17:04:09

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	3251
149.88.219.246	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
183.26.118.121	China	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	2
66.249.78.95	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
180.170.186.83	China	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
112.118.173.228	Hong Kong	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
65.181.113.88	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

01-08-2016-16:04:09 to 01-08-2016-17:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
120.43.9.239	China	147.237.77.226	www.chamatz.aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	33
120.43.9.239	China	147.237.0.34	tikshuv.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	32
120.43.9.239	China	147.237.76.86	navy.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	32
120.43.9.239	China	147.237.72.156	aman.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	32
120.43.9.239	China	147.237.77.233	atal.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	32
120.43.9.239	China	147.237.76.200	eitan.aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	32
120.43.9.239	China	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	32
120.43.9.239	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	31
120.43.9.239	China	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	29
120.43.9.239	China	147.237.0.15	kosher-kravi.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	24
120.43.9.239	China	147.237.76.86	navy.idf.il	0854: HTTP: upload* Access	Block	10
120.43.9.239	China	147.237.77.233	atal.idf.il	0854: HTTP: upload* Access	Block	10
120.43.9.239	China	147.237.76.200	eitan.aka.idf.il	0854: HTTP: upload* Access	Block	10
120.43.9.239	China	147.237.72.166	aka.idf.il	0854: HTTP: upload* Access	Block	10
120.43.9.239	China	147.237.77.226	www.chamatz.aka.idf.il	0854: HTTP: upload* Access	Block	10
120.43.9.239	China	147.237.72.156	aman.idf.il	0854: HTTP: upload* Access	Block	9
120.43.9.239	China	147.237.0.34	tikshuv.idf.il	0854: HTTP: upload* Access	Block	9
120.43.9.239	China	147.237.0.15	kosher-kravi.idf.il	0854: HTTP: upload* Access	Block	8
120.43.9.239	China	147.237.77.176	matpash.idf.il	0854: HTTP: upload* Access	Block	8
120.43.9.239	China	147.237.77.74	law.idf.il	0854: HTTP: upload* Access	Block	7

01-08-2016-16:04:09 to 01-08-2016-17:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.236	147.237.76.42	United States	refuah.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
80.82.69.146	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
79.143.181.158	147.237.76.148	Germany	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
203.251.140.72	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
190.252.239.53	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.174.93.203	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.69.146	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential SSH Scan	1
80.82.69.146	147.237.76.148	Netherlands	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
79.143.181.158	147.237.76.148	Germany	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
149.88.86.133	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.203	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.69.146	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1

01-08-2016-16:04:09 to 01-08-2016-17:04:09

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	163
84.229.29.97	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	65
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
120.43.9.239	China	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
120.43.9.239	China	147.237.0.34	tikshuv.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
120.43.9.239	China	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
120.43.9.239	China	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
120.43.9.239	China	147.237.76.200	eitan.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
120.43.9.239	China	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
120.43.9.239	China	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	25
120.43.9.239	China	147.237.72.156	aman.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	25
77.127.217.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
120.43.9.239	China	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	24
79.183.125.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
95.242.212.212	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
120.43.9.239	China	147.237.0.15	kosher-kravi.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	20
85.65.151.161	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
149.78.223.180	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
84.109.232.225	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
85.130.252.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.3.144.21	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
120.43.9.239	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.137	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
84.110.84.61	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
84.110.84.61	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.88.14.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.108.121	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
185.120.125.60		147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.180.171.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.144.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.149.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.168	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.126.91.24	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.250	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.250	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.64.202.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.65.30.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.192	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
109.186.184.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.228.61.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-08-2016-16:04:09 to 01-08-2016-17:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.143.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
109.253.143.128	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.143.128	Block	91
109.253.192.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
87.69.35.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
84.109.24.224	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76
87.69.35.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
120.43.9.239	China	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 120.43.9.239	Block	44
120.43.9.239	China	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 120.43.9.239	Block	43
120.43.9.239	China	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 120.43.9.239	Block	41
120.43.9.239	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 120.43.9.239	Block	41
120.43.9.239	China	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 120.43.9.239	Block	37
109.253.192.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
120.43.9.239	China	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 120.43.9.239	Block	33
120.43.9.239	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 120.43.9.239	Block	29
120.43.9.239	China	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 120.43.9.239	Block	26
120.43.9.239	China	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 120.43.9.239	Block	25
120.43.9.239	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 120.43.9.239	Block	23
170.185.233.107	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/mobilecontroller	Block	18
109.253.143.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
109.253.143.128	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 109.253.143.128	Block	10
84.229.157.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.228.40.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.19.85.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.173.18.237	Israel	147.237.72.166	aka.idf.il	Multiple Redundant HTTP Headers in header Referer	Block	3
37.26.149.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
74.208.16.87	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 74.208.16.87	Block	2
120.43.9.239	China	147.237.72.156	aman.idf.il	Multiple Admin Blocking from 120.43.9.239	Block	2
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	2
149.78.223.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
120.43.9.239	China	147.237.0.15	kosher-kravi.idf.il	Multiple Admin Blocking from 120.43.9.239	Block	2
120.43.9.239	China	147.237.76.200	eitan.aka.idf.il	Multiple Admin Blocking from 120.43.9.239	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
120.43.9.239	China	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 120.43.9.239	Block	2
120.43.9.239	China	147.237.0.34	tikshuv.idf.il	Multiple Admin Blocking from 120.43.9.239	Block	2
120.43.9.239	China	147.237.77.74	law.idf.il	Multiple Admin Blocking from 120.43.9.239	Block	2
46.19.85.44	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
120.43.9.239	China	147.237.76.86	navy.idf.il	Multiple Admin Blocking from 120.43.9.239	Block	2
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/ishurim/cityofficers/	None	1
109.253.143.128	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
91.218.150.140	Netherlands	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
210.5.50.130	New Zealand	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
120.43.9.239	China	147.237.77.226	www.chamatz.aka.idf.il	Admin Blocking	Block	1
5.29.94.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.246.96.128	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
159.203.20.166	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.19.86.92	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

01-08-2016-16:04:09 to 01-08-2016-17:04:09