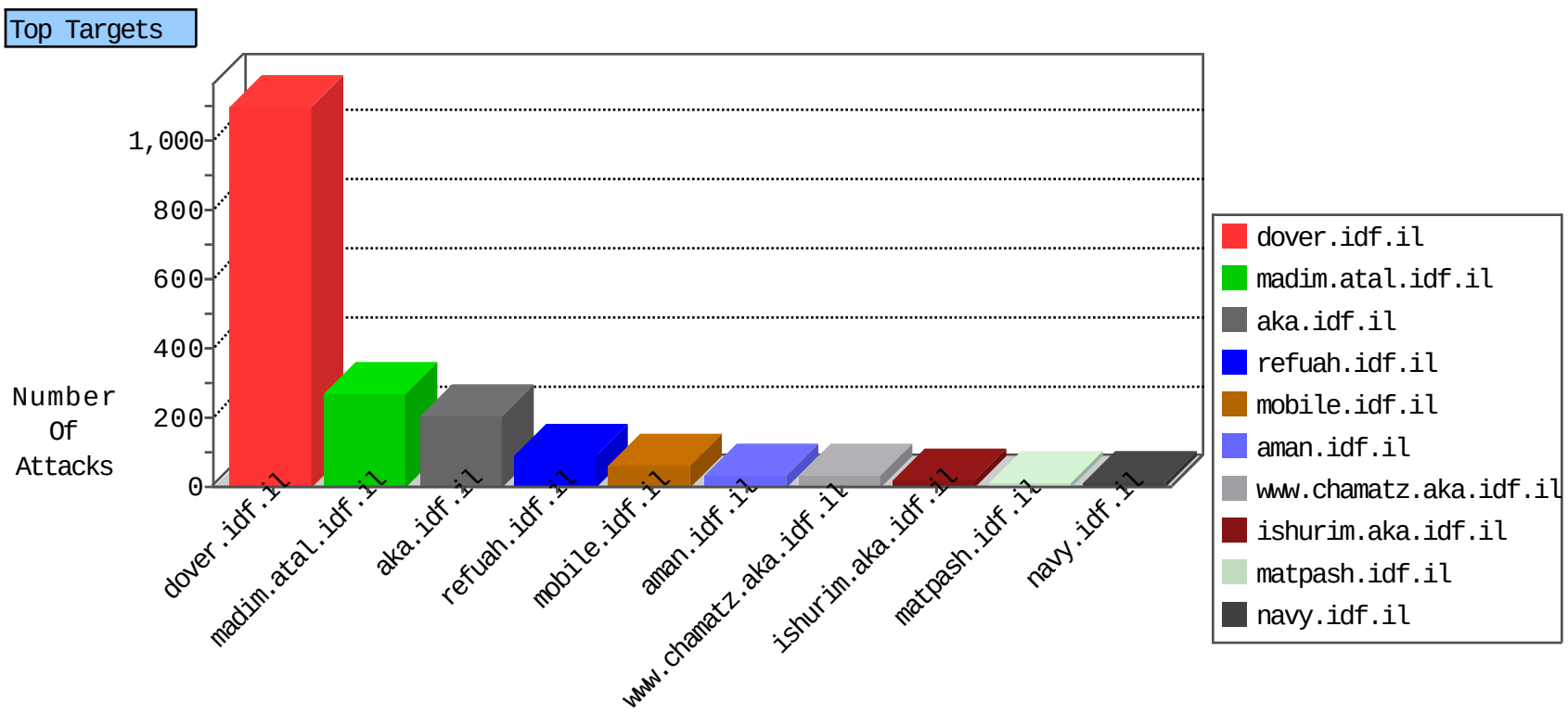
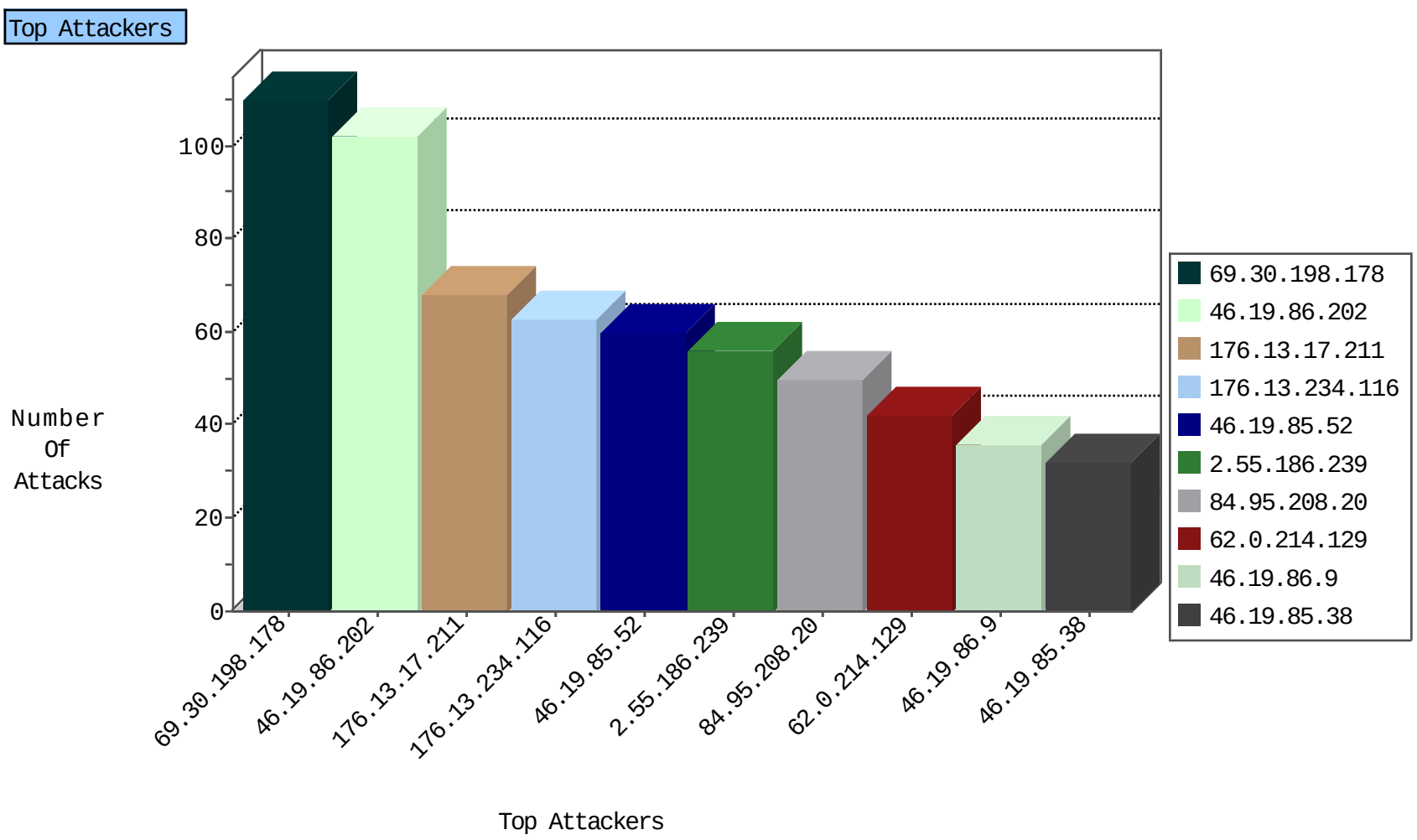
09-20-2016-09:04:01 to 09-20-2016-10:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-20-2016-09:04:01 to 09-20-2016-10:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	7
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
2.53.47.6	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
2.53.187.161	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
212.179.64.162	Israel	147.237.77.216	dover.idf.il	Black List	drop	3
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.37	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
69.30.193.252	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
198.204.224.238	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
142.54.174.83	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.110.84.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
106.186.113.132	Japan	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.12.220.86	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	1

09-20-2016-09:04:01 to 09-20-2016-10:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.198.178	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	110

09-20-2016-09:04:01 to 09-20-2016-10:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.71.30.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.36.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.118.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
67.211.219.120	147.237.76.148	United States	gqcenter.aka.idf.i	ET DROP Spamhaus DROP Listed Traffic Inbound	1
212.33.200.73	147.237.76.30	Iran, Islamic Republic of	himush.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.181.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.117.138.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.213.5.205	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.193.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.138.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.182.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.19.212	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.29.202.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.27.104.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
119.93.77.41	147.237.76.147	Philippines	chinuch.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.237.111.200	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1

09-20-2016-09:04:01 to 09-20-2016-10:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.214.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	42
176.13.17.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	30
2.53.189.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
2.53.147.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
176.13.17.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
176.13.17.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
93.172.154.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.55.186.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
2.55.186.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.55.186.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	14
2.55.186.239	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
46.19.85.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
109.253.137.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.86.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
188.120.154.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.148.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.55.26.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.85.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.236	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.253.130.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.142.144	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.148.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.131.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.117.16.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.176.27.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
213.57.7.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.43.73.50	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
109.253.128.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.157.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
80.246.130.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.47.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.54.84.74	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
176.13.13.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.137	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.215.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.69.120.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.156.143	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

09-20-2016-09:04:01 to 09-20-2016-10:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
176.13.234.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
46.19.86.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
46.210.175.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
109.253.245.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
109.253.192.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
79.181.176.49	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	7
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
2.55.167.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
46.19.86.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
213.57.7.4	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
147.236.50.70	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	3
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
109.253.134.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.14.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.80.196.44	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
77.138.18.174	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	2
2.53.63.178	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.120.203.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
2.55.191.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
37.26.149.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.179.46.189	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/61353.jpg	Block	1
46.19.85.236	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
124.109.61.179	Pakistan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
106.186.113.132	Japan	147.237.76.31	nakchal.idf.il	Multiple Illegal Byte Code Character in Method from 106.186.113.132	Block	1
46.19.86.129	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
2.55.155.233	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
203.45.80.198	Australia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
46.19.85.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
2.53.9.37	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
106.186.113.132	Japan	147.237.76.31	nakchal.idf.il	Multiple NULL Character in Method from 106.186.113.132	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1

09-20-2016-09:04:01 to 09-20-2016-10:04:01