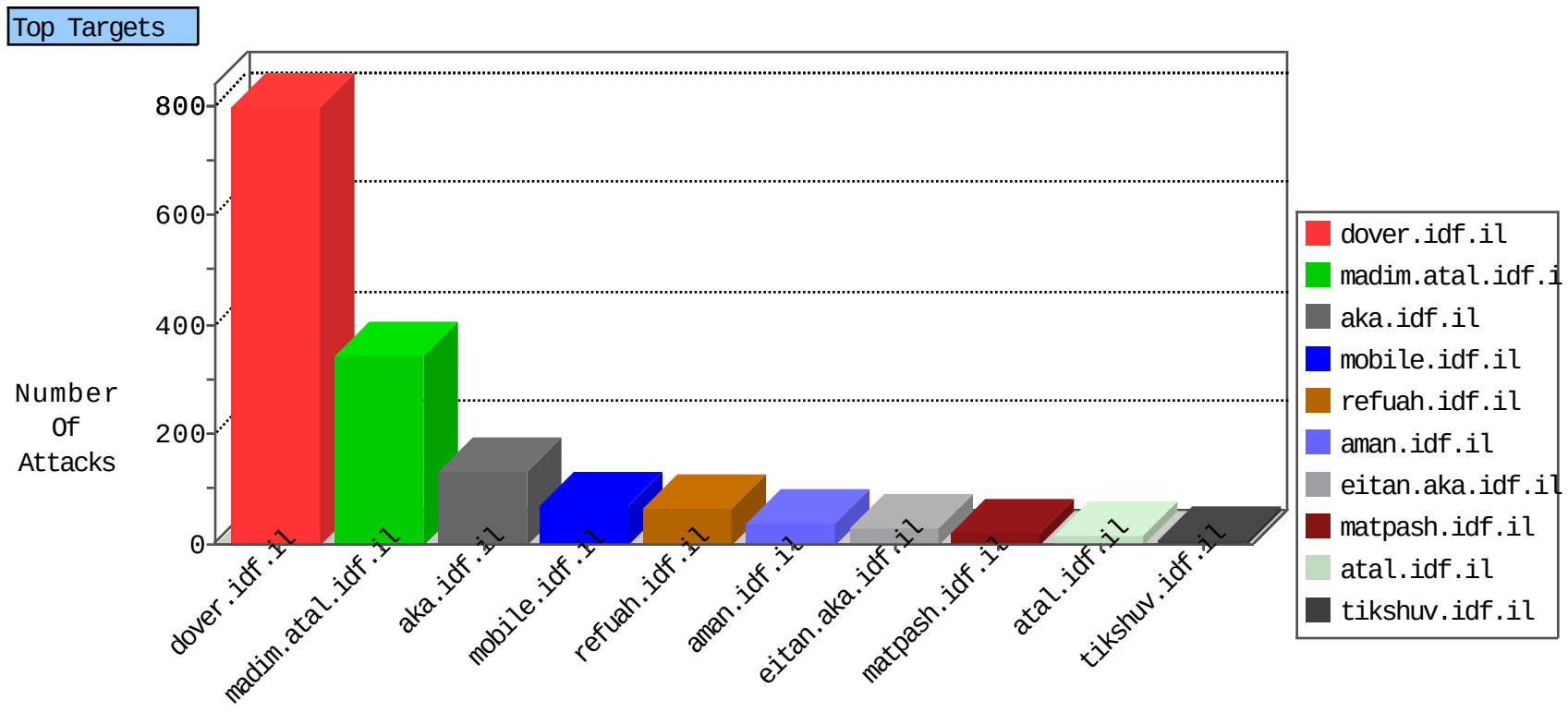
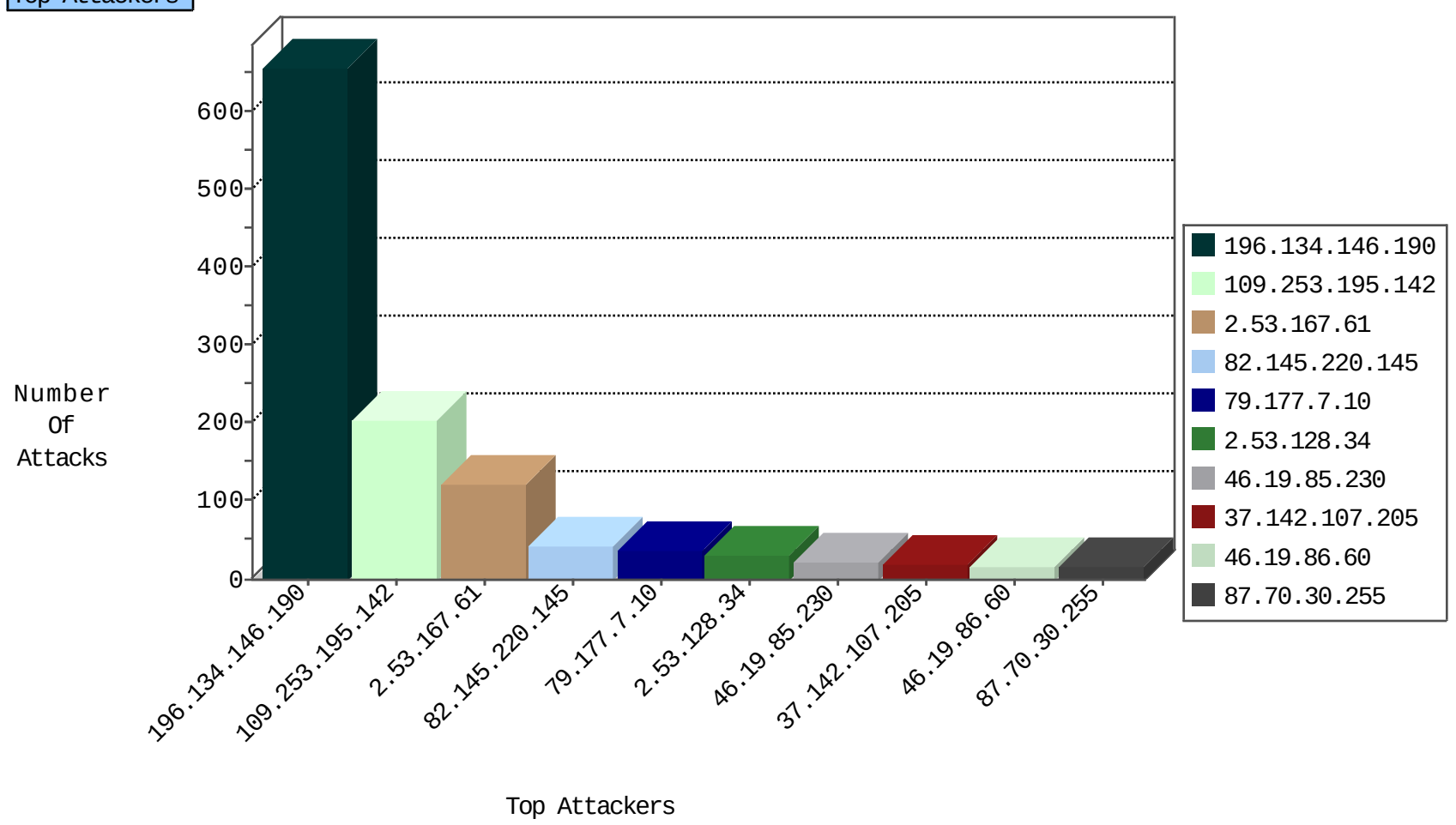
09-15-2016-22:04:06 to 09-15-2016-23:04:06

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-15-2016-22:04:06 to 09-15-2016-23:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
196.134.146.190	Egypt	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	20507
196.134.146.190	Egypt	147.237.77.216	dover.idf.il	Anomaly-IP-bad-frag-bits	drop	2365
95.86.121.155	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	21
196.134.146.190	Egypt	147.237.77.216	dover.idf.il	ICMP-fragmented	drop	21
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.112	United States	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
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.117.226.180	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
176.13.234.29	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
120.132.50.135	China	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
179.99.200.39	Brazil	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
131.179.150.72	United States	147.237.72.156	aman.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
130.194.252.8	Australia	147.237.72.156	aman.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
193.1.13.12	Ireland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.226	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-15-2016-22:04:06 to 09-15-2016-23:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-15-2016-22:04:06 to 09-15-2016-23:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.13.246.0	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	7
142.54.191.210	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
13.75.43.42	147.237.76.42	Hong Kong	refuah.idf.il	ET SCAN Potential SSH Scan	1
116.71.128.85	147.237.76.202	Pakistan	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
116.71.128.85	147.237.76.147	Pakistan	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.167.6.84	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
202.155.58.28	147.237.76.199	Indonesia	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
180.97.106.162	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
180.97.106.37	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
142.54.191.210	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
31.24.228.20	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1
142.54.191.210	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
13.75.43.42	147.237.76.38	Hong Kong	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
116.71.128.85	147.237.76.199	Pakistan	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
116.71.128.85	147.237.76.86	Pakistan	navy.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
79.183.70.254	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
202.155.58.28	147.237.72.156	Indonesia	aman.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
180.97.106.161	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.65	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

09-15-2016-22:04:06 to 09-15-2016-23:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.145.220.145	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	43
2.53.128.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.177.7.10	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
46.19.85.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
37.142.107.205	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
77.127.21.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.177.7.10	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	14
46.19.86.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
188.227.233.73	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
87.70.30.255	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
84.111.124.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
87.70.30.255	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
79.180.137.222	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.111.124.107	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.51	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.183.70.254	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.86.60	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.139.123.177	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.51	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.149.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
185.3.147.78	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
95.86.82.120	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
217.132.155.131	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.60	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.177.153.251	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.176.107.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.60	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
141.226.217.255	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.60.235.58	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
37.26.147.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
66.249.69.81	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.31.57.12	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
79.176.70.118	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.60	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.26.146.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
80.246.140.155	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
141.226.148.52	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
2.53.12.207	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.138.99.27	France	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
91.135.104.252	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.148	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
109.253.135.13	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
82.121.58.24	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
141.226.161.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.53.30.28	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

09-15-2016-22:04:06 to 09-15-2016-23:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.195.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	202
2.53.167.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
77.125.12.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.229.48.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.135.100	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.126.86.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.59.2	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
79.180.3.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method FGDover.aspx in URL	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/forgotpassword.aspx	Block	1
79.183.70.254	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
207.46.13.62	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
5.29.181.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
109.64.82.24	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
77.139.187.72	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1245-he/atal.aspx	Block	1
157.55.39.67	United States	147.237.76.147	chinuch.aka.idf.i	Multiple Unauthorized URL Access from 157.55.39.67	Block	1
80.179.122.185	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/navy/	Block	1
213.57.104.209	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/miluim/	Block	1
31.175.234.125	Poland	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.233.11	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	1
159.220.74.2	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 159.220.74.2	Block	1
84.109.50.189	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
77.138.225.182	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
213.57.184.222	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
141.226.217.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
79.177.7.10	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.76.67	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
176.31.57.12	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.31.57.12	Block	1
217.132.87.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
46.19.85.132	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
157.55.39.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16552-en/dover.aspx-title=for	Block	1
68.180.228.171	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
176.31.57.12	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/dover.aspx'	Block	1
5.28.169.209	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/home/giyus	Block	1
85.64.178.242	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1

09-15-2016-22:04:06 to 09-15-2016-23:04:06