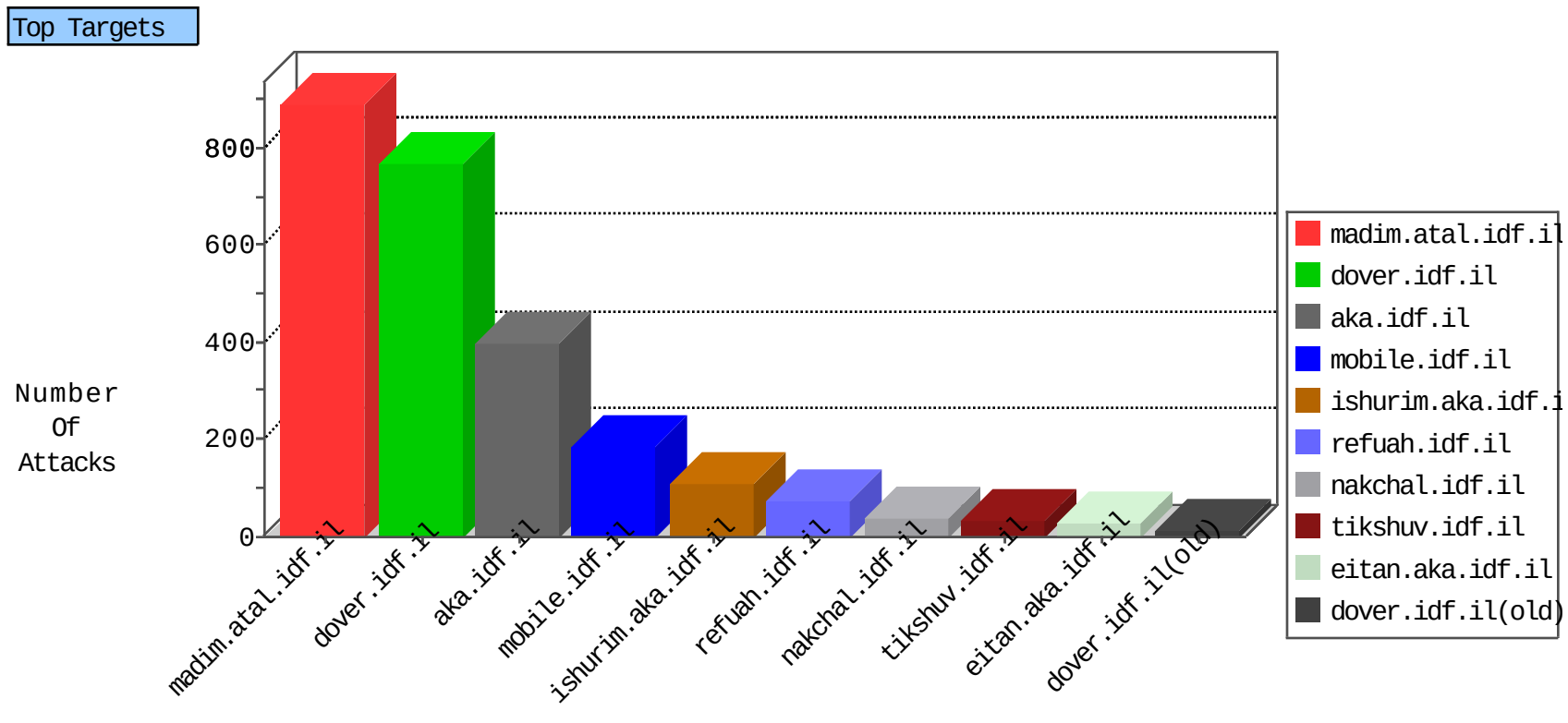
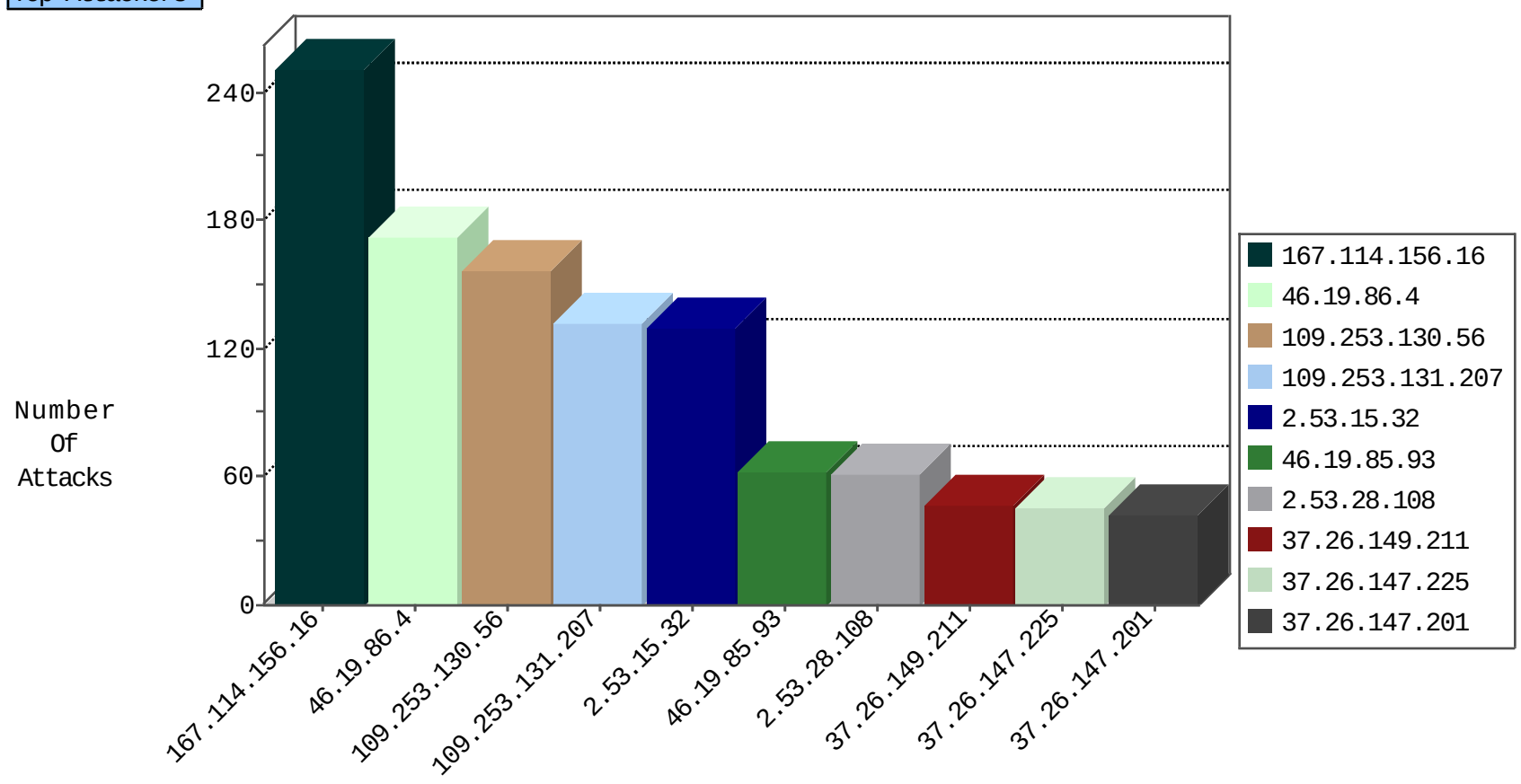
05-01-2016-11:04:02 to 05-01-2016-12:04:02

IDF Under Attack
Daily Report

Top Targets



Top Attackers



05-01-2016-11:04:02 to 05-01-2016-12:04:02

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	HTTP-POST-Segmented-DoS	dest-reset	9858
109.64.172.192	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2550
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2270
66.249.93.115	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	124
66.249.93.111	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	70
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
80.246.136.217	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
192.116.108.242	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3
115.204.91.15	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
60.246.238.177	Macau	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
192.115.177.202	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

05-01-2016-11:04:02 to 05-01-2016-12:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-01-2016-11:04:02 to 05-01-2016-12:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
81.218.251.252	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.116.195.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
37.26.149.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.117.148.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
181.48.132.202	147.237.0.17	Colombia	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.8.19	147.237.77.121	United Kingdom	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
112.198.75.205	147.237.77.216	Philippines	dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.64.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.91.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.46.39.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.242.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.248	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
184.7.206.131	147.237.76.31	United States	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
176.13.12.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.39.184	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.66.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

05-01-2016-11:04:02 to 05-01-2016-12:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
84.95.85.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
176.13.1.183	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
62.219.52.51	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
109.253.137.106	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.149.211	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	16
37.46.39.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
213.57.171.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
89.138.206.111	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
2.53.28.108	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
85.65.111.36	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
2.53.8.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.211	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		alert	12
176.13.15.96	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.55.15.155	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.126.226	Israel	147.237.72.14	dover.idf.il(old)	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
2.53.10.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.102.225.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
199.203.179.99	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
176.13.23.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.212.123.78	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.190	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.190	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.25.107.145	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
2.53.51.54	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.155.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.130.249.145	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
62.90.139.244	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
37.26.149.211	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
194.56.215.218	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
212.179.212.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.93.247	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.156.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.21.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.135.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.251	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.157.244	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.169	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.177.16.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	172
109.253.130.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	157
109.253.131.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	132
2.53.15.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	130
46.19.85.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
37.26.147.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
2.53.28.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
37.26.147.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
46.19.85.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
176.13.3.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
37.26.147.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
81.218.251.252	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	9
109.253.137.106	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
37.26.146.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
109.253.207.141	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
213.57.171.41	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	4
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
77.127.157.244	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.53.10.215	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.53.61.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.46.38.90	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	3
176.13.23.143	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.177	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
178.137.83.178	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	3
46.117.113.137	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.53.2.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	3
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.136.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.224.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.8.97	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.178.168.79	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/homepage/mobile	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
27.255.92.163	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
2.53.28.108	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.211	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	1
77.125.126.27	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
194.90.36.177	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
5.29.169.123	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/	Block	1
52.16.137.212	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
93.172.38.99	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
38.111.147.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1