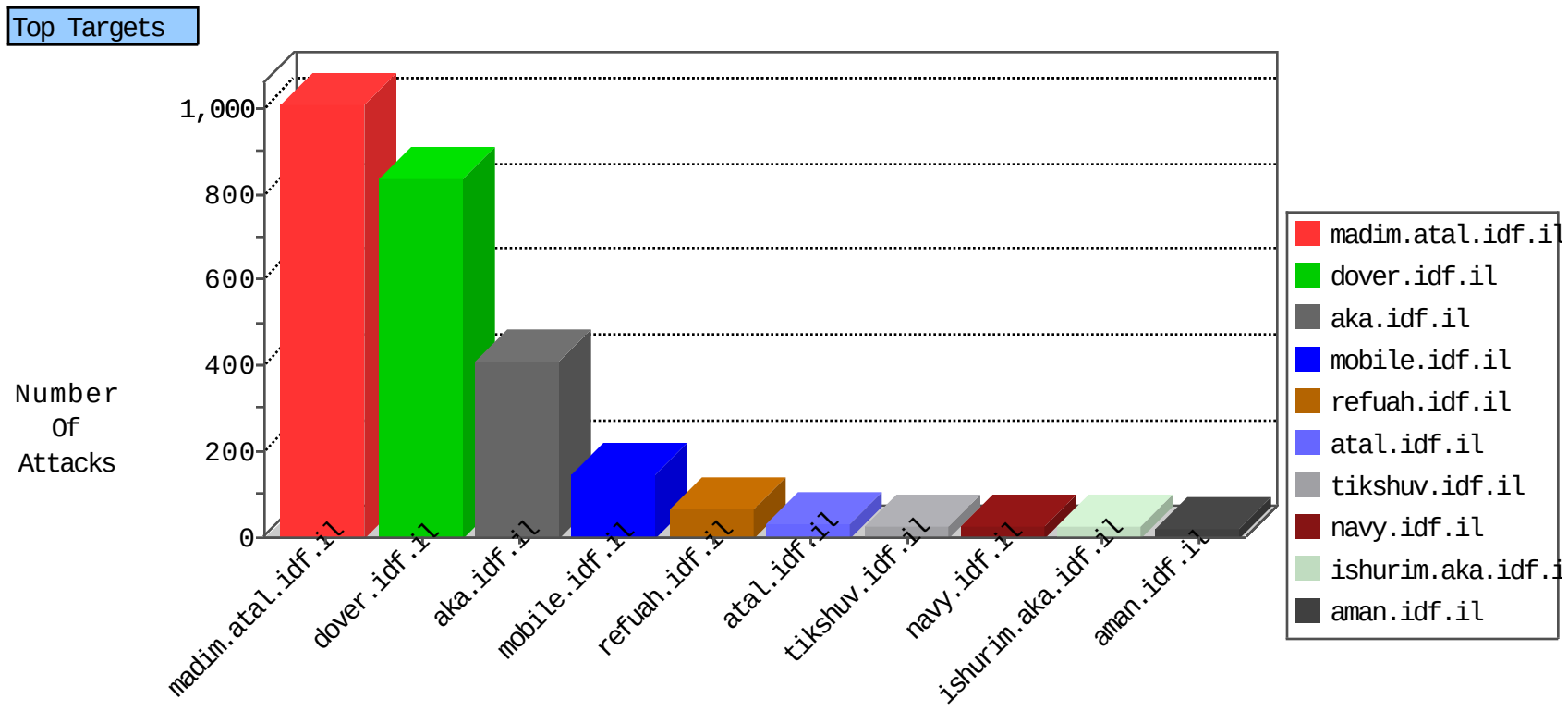
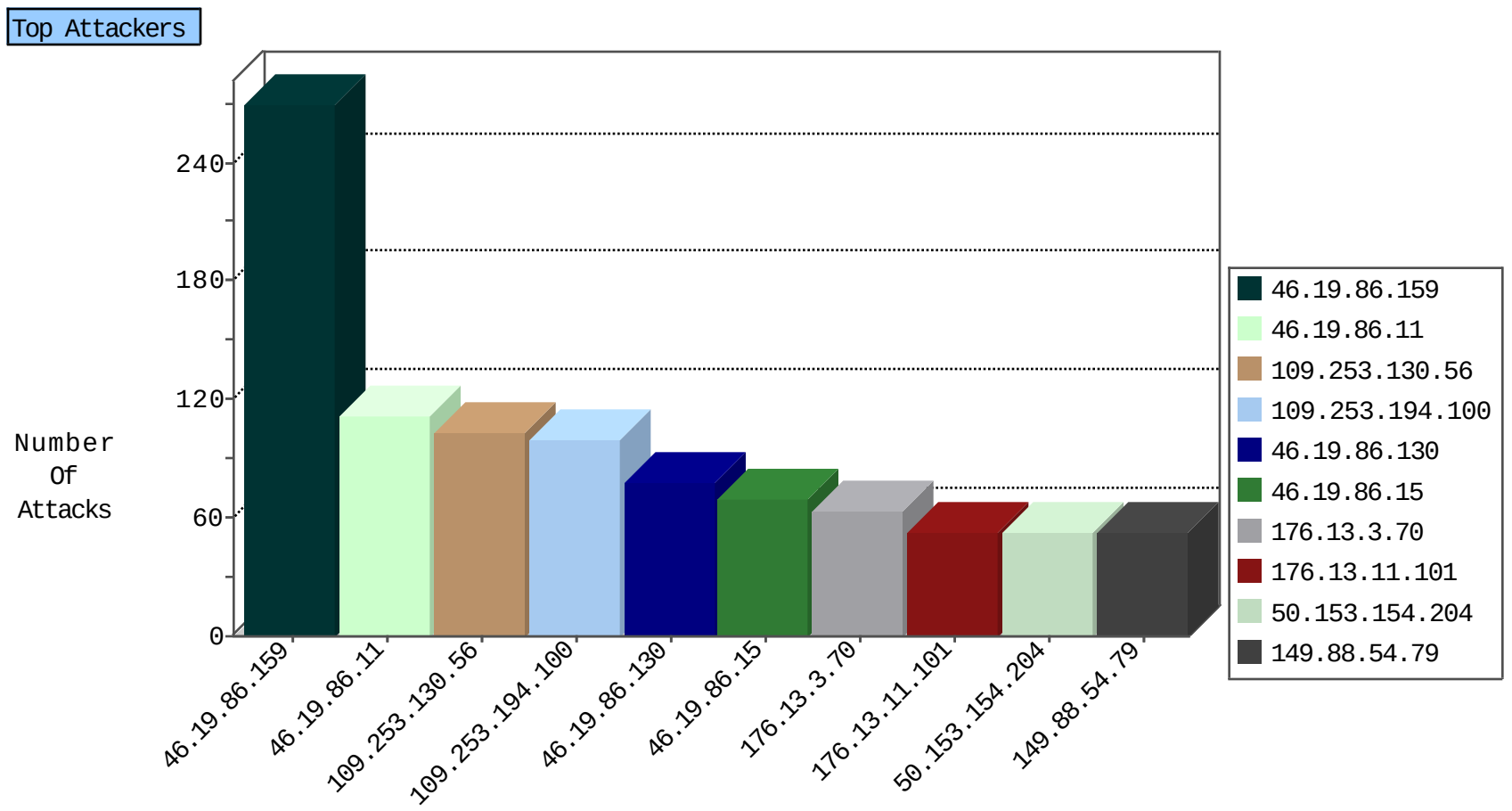
05-01-2016-09:04:08 to 05-01-2016-10:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



05-01-2016-09:04:08 to 05-01-2016-10:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.133	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2509
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1816
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	464
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	326
89.138.62.157	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	102
192.115.248.2	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
46.19.86.14	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
149.78.154.69	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
213.8.204.61	Israel	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	DOS-Tool-SwitchbladG	dest-reset	2
185.94.111.1	Russian Federation	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

05-01-2016-09:04:08 to 05-01-2016-10:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-01-2016-09:04:08 to 05-01-2016-10:04:08

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	3
66.249.64.186	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
109.253.207.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.216.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.157.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.238.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.102.216.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.232.98.3	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
2.53.21.242	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.165.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.214.29.239	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -f -sS	1
208.100.26.228	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.21.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
176.228.190.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.240.250.154	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.211	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
109.253.135.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.61.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.128.236	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.165.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.184.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.214.29.239	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
2.53.11.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.76.112.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.197.103.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.181.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.5.220.79	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.125.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
172.93.98.2	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.248.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

05-01-2016-09:04:08 to 05-01-2016-10:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
50.153.154.204	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
37.187.157.108	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
149.88.54.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
212.179.71.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
198.100.144.55	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
37.26.146.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
213.57.119.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
192.114.23.18	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
216.75.214.5	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.86.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
212.143.40.145	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
162.243.99.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.149.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
162.245.222.20	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.115.248.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
84.110.110.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.13.1.252	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
191.96.65.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
81.218.251.252	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.253.138.25	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
213.57.119.122	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	7
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.13.1.252	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.0.112.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.146.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.136.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.221.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.99.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.55.11.133	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.138.25	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

05-01-2016-09:04:08 to 05-01-2016-10:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	270
46.19.86.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	112
109.253.130.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
109.253.194.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	100
46.19.86.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
46.19.86.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	69
176.13.3.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
176.13.11.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
176.13.3.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
2.53.181.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
176.13.10.81	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	30
46.19.85.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
109.253.156.161	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	12
2.53.8.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
192.116.232.69	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	9
109.253.201.70	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	6
176.13.21.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.1.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.2.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.134.76	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	5
80.246.133.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
109.253.156.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
195.160.242.40	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	4
195.160.242.40	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 195.160.242.40	Block	3
2.53.155.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.142.65	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	3
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	3
80.246.137.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.129.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
151.31.8.223	Italy	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 151.31.8.223	Block	3
109.253.144.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.194.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	2
2.53.152.133	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
131.253.25.184	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
109.253.138.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.111	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
54.241.242.243	United States	147.237.76.42	refuah.idf.il	NULL Character in Header Name at [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
95.86.87.163	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.55.34.177	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
157.55.39.53	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17607-en/dover.aspx-title=over	Block	1
2.53.13.106	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
109.253.144.25	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
203.127.96.248	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.241.242.243	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in URL ‚'©bÜz“[[#25]][[ɔ#0[[]#0[[]#28¸+¸/¸]]0¸[[#19]]¸	Block	1
109.67.110.225	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
78.177.225.44	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1

05-01-2016-09:04:08 to 05-01-2016-10:04:08