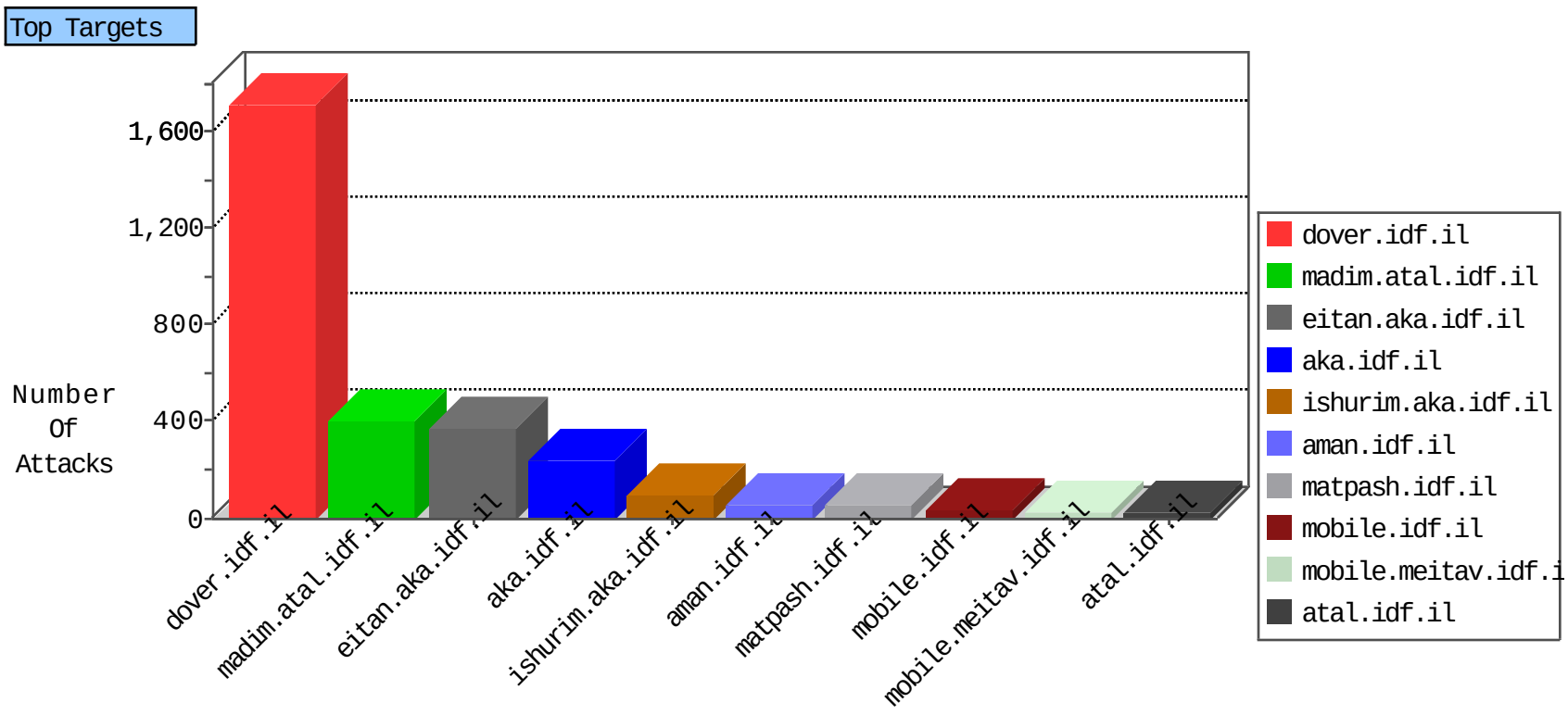
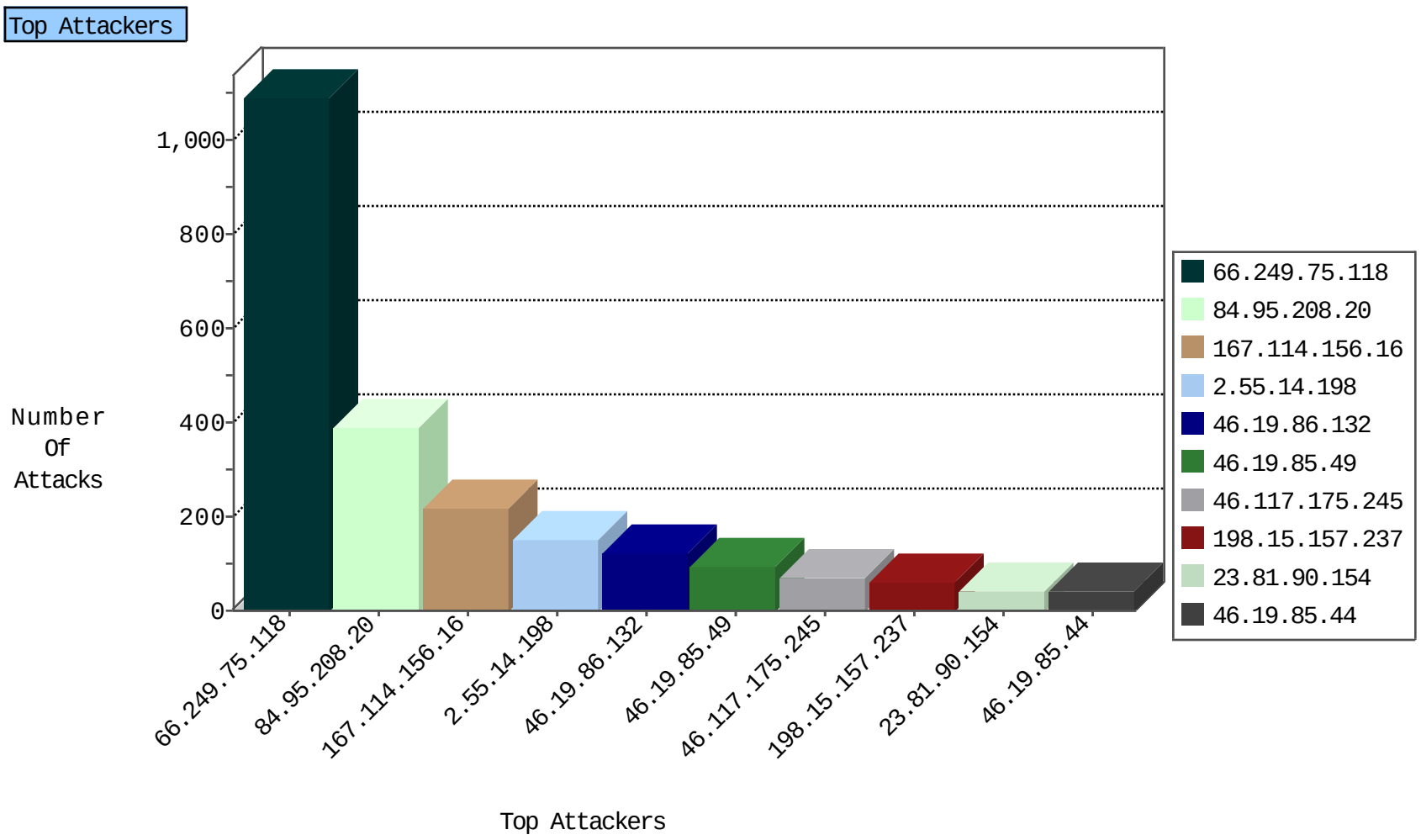
04-20-2016-11:04:00 to 04-20-2016-12:04:00

IDF Under Attack Daily Report





04-20-2016-11:04:00 to 04-20-2016-12:04:00

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	15687
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10646
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	7452
198.15.157.237	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	192
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	80
119.131.139.207	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	6
218.64.77.7	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	6
117.114.147.2	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	5
175.13.116.124	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	4
114.91.134.223	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
180.109.32.165	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
139.129.93.18	China	147.237.76.38	e.e.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
94.102.49.116	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
1.80.115.164	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
113.107.169.132	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
121.141.225.10	Korea, Republic of	147.237.76.196	e.sviva.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
2.53.145.107	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
219.142.187.73	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
223.96.156.160	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
140.250.2.136	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

04-20-2016-11:04:00 to 04-20-2016-12:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-20-2016-11:04:00 to 04-20-2016-12:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.75.118	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1093
40.84.159.128	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
194.56.215.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.172.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
121.141.225.10	147.237.76.199	Korea, Republic of	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
121.141.225.10	147.237.0.15	Korea, Republic of	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
95.9.65.77	147.237.8.14	Turkey	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
88.254.109.108	147.237.77.216	Turkey	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
31.154.161.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
121.141.225.10	147.237.76.202	Korea, Republic of	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.53.1.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
121.141.225.10	147.237.76.177	Korea, Republic of	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.221.135.62	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
95.9.65.77	147.237.8.14	Turkey	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
79.181.51.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.187.44.243	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.19.85.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-20-2016-11:04:00 to 04-20-2016-12:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	177
46.117.175.245	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	70
198.15.157.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
23.81.90.154	United States	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
141.0.14.145	Europe	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	36
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
124.154.227.229	Japan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
5.57.6.39	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.86.198	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.118.30.102	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
46.19.85.44	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
207.241.229.102	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	11
2.55.55.54	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.98	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.109	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.55.14.198	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.26.148.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
62.90.35.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.7.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.160	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.44	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.118.30.102	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.55.14.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
193.186.163.3	Greece	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.160	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.142.64.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
88.254.109.108	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.95.208.20	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.65.170.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.142.64.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
207.232.46.209	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.176.105.33	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
167.114.235.72	France	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.242.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.176.105.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.55.180.81	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

04-20-2016-11:04:00 to 04-20-2016-12:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.14.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	141
46.19.86.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	114
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	98
46.19.85.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	94
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	84
176.13.3.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	10
79.177.145.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/0	Block	9
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	6
46.19.85.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.26.148.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.6.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	3
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	3
37.26.148.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.57.70.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.177.145.2	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.177.145.2	Block	2
37.26.149.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.3.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method ˆE"éwºÝ[[#22]]‹DÒ[[#17]]‰ÊåëÄ•—	Block	1
167.114.235.72	France	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/1093-7963-he/מאיר שחמון/ .aspx	Block	1
213.8.204.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
46.19.86.132	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
81.218.70.243	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	1
2.55.14.198	Israel	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Open Mode	None	1
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Abnormally Long Request method	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Distributed Malformed URL	Block	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	1
46.19.86.192	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
169.229.3.91	United States	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
109.67.5.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.55.189.168	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1824-he/dover.aspx	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Method	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	1
213.211.241.42	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
79.177.145.2	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1038-he/0	Block	1

04-20-2016-11:04:00 to 04-20-2016-12:04:00