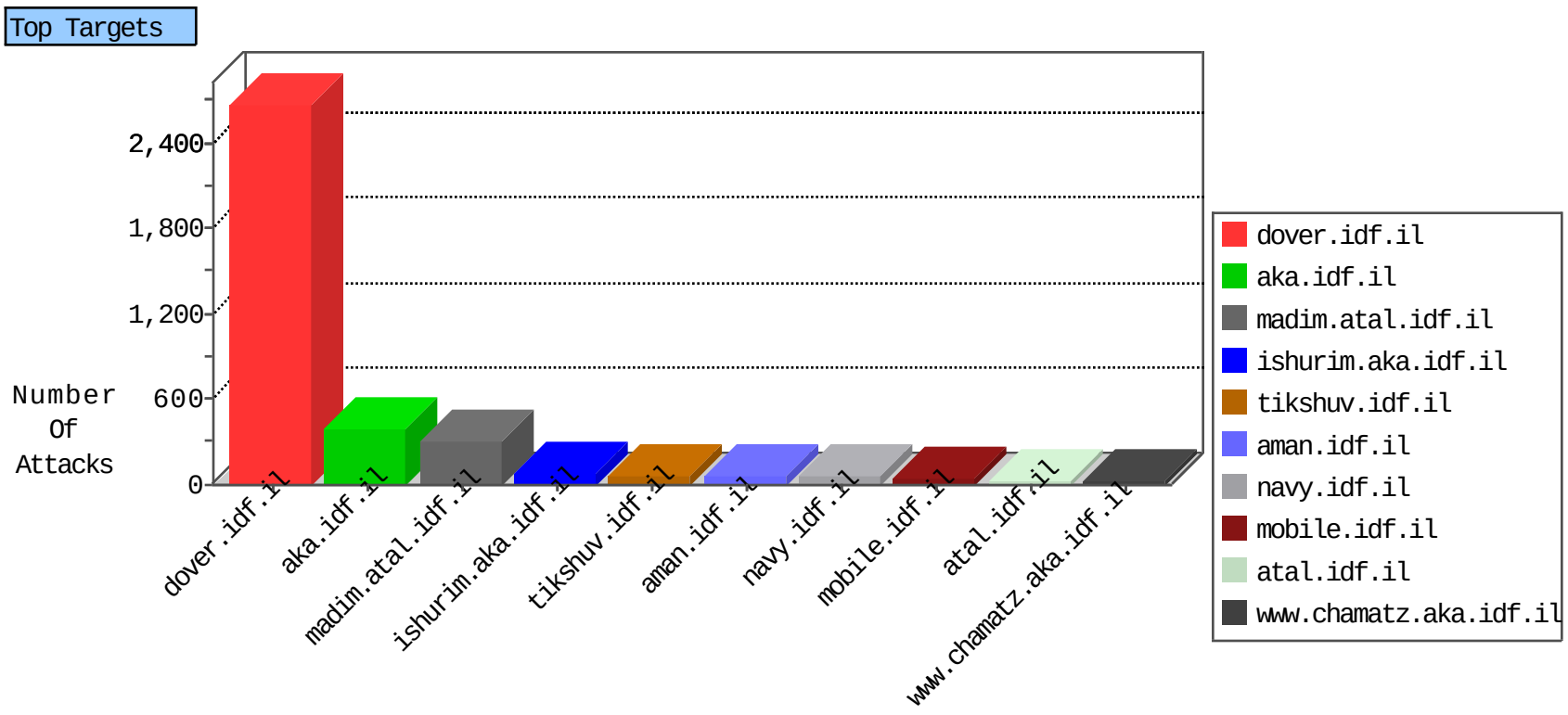
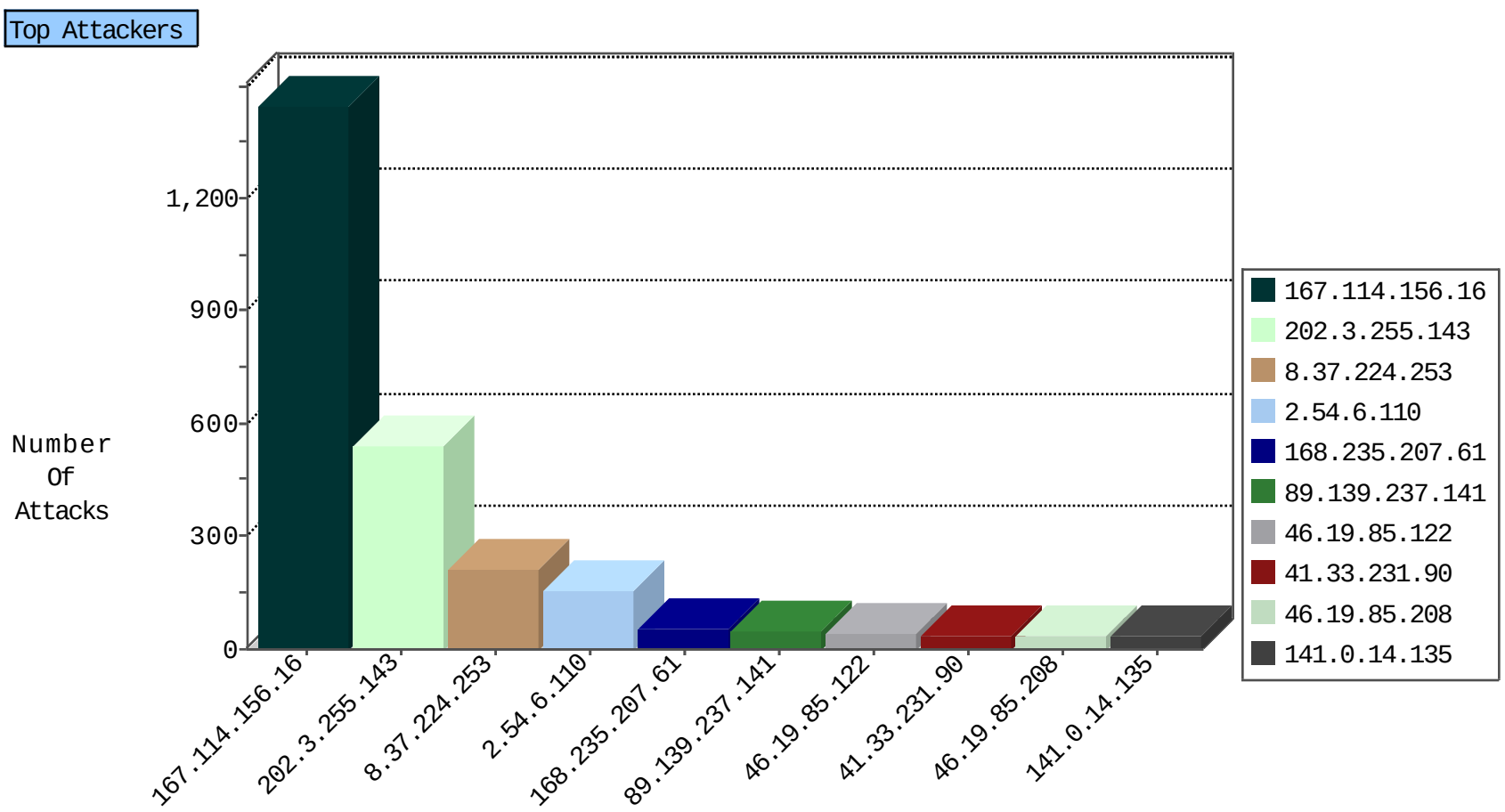
01-17-2016-21:04:05 to 01-17-2016-22:04:05

IDF Under Attack Daily Report





01-17-2016-21:04:05 to 01-17-2016-22:04:05

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	DOS-Tool-SwitchbladG	dest-reset	3062
217.132.37.25	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.177.151.68	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
213.57.153.47	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
79.181.13.165	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
206.191.151.226	United States	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
42.112.10.74	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
42.112.10.87	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
42.112.10.68	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
42.112.10.75	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
8.37.224.253	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1
168.235.207.61	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1
42.112.10.92	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
42.112.10.70	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
89.248.174.4	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
42.112.10.80	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
42.112.10.65	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
202.116.234.16	China	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
60.160.133.176	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
42.112.10.73	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
89.248.174.4	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
42.112.10.81	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
42.112.10.66	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1

01-17-2016-21:04:05 to 01-17-2016-22:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-17-2016-21:04:05 to 01-17-2016-22:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	500
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
212.143.124.223	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
206.191.151.226	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.237	147.237.77.178		e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
199.191.56.188	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 2048	1
160.176.173.39	147.237.77.216		dover.idf.il	Tehila - Perl LWP with fake user agent	1
109.64.31.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.0.35	Sweden	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.143	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	1
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.48.25	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
206.191.151.226	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.237	147.237.77.178		e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
206.191.151.226	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.237	147.237.77.178		e.matpash.idf.il	ET SCAN NMAP -f -sS	1
199.191.56.188	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 4096	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
199.191.56.188	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -f -sS	1
149.78.172.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.8.28	Sweden	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.77.216	Kazakstan	dover.idf.il	ET SCAN NMAP -sS window 4096	1
191.240.136.5	147.237.77.61	Brazil	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.54.146.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 4096	1
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -f -sS	1
183.60.48.25	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
208.80.155.211	147.237.76.86	United States	navy.idf.il	Tehila - Perl LWP with fake user agent	1
176.13.1.158	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

01-17-2016-21:04:05 to 01-17-2016-22:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.224.253	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	117
8.37.224.253	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	95
168.235.207.61	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	50
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.208	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
141.0.14.135	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	33
79.179.121.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.86.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
2.54.133.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.33.226.98	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
162.254.149.198	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
2.54.47.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.147.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.67.203.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.147.170	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.6.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.13.56	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.86.190.247	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
66.249.93.140	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	11
149.86.191.95	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
87.68.51.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
87.69.29.140	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
80.179.9.115	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	8
80.246.136.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
5.29.241.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
80.246.138.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
82.102.169.113	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	8
80.179.9.7	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	8
37.26.149.242	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
80.246.138.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.54.146.196	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
217.132.37.25	Israel	147.237.77.216	dover.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	monitor	6
2.54.146.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.28.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.37.25	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.127.169.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.146.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.60.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.124.223	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.146.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
109.253.146.39	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.146.196	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.6.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	79
2.54.6.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
89.139.237.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
84.228.15.210	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
2.52.160.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
149.88.6.12	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
46.19.86.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
84.108.45.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.13.56	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
93.173.23.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.241.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.68.54	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 37.142.68.54	Block	3
109.253.198.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
72.167.190.37	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
80.246.136.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.228.240.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.228.240.41	Block	2
79.180.220.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
79.172.252.42	Hungary	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
5.29.61.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.143.124.223	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/	Block	2
37.142.68.54	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
5.29.241.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.213.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.170.116.69	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 107.170.116.69	Block	2
173.252.81.119	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
27.50.89.230	Australia	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
89.161.169.148	Poland	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
207.46.13.105	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
149.88.225.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.152.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.228.243.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.53.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
188.128.189.57	Poland	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
46.117.137.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
78.129.234.106	United Kingdom	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
176.13.18.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.88.8.64	France	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 89.88.8.64	Block	1
213.8.204.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
160.176.173.39		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-admin/admin-ajax.php	Block	1
62.0.75.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
119.18.157.130	Indonesia	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
84.228.37.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
203.124.120.63	Singapore	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1