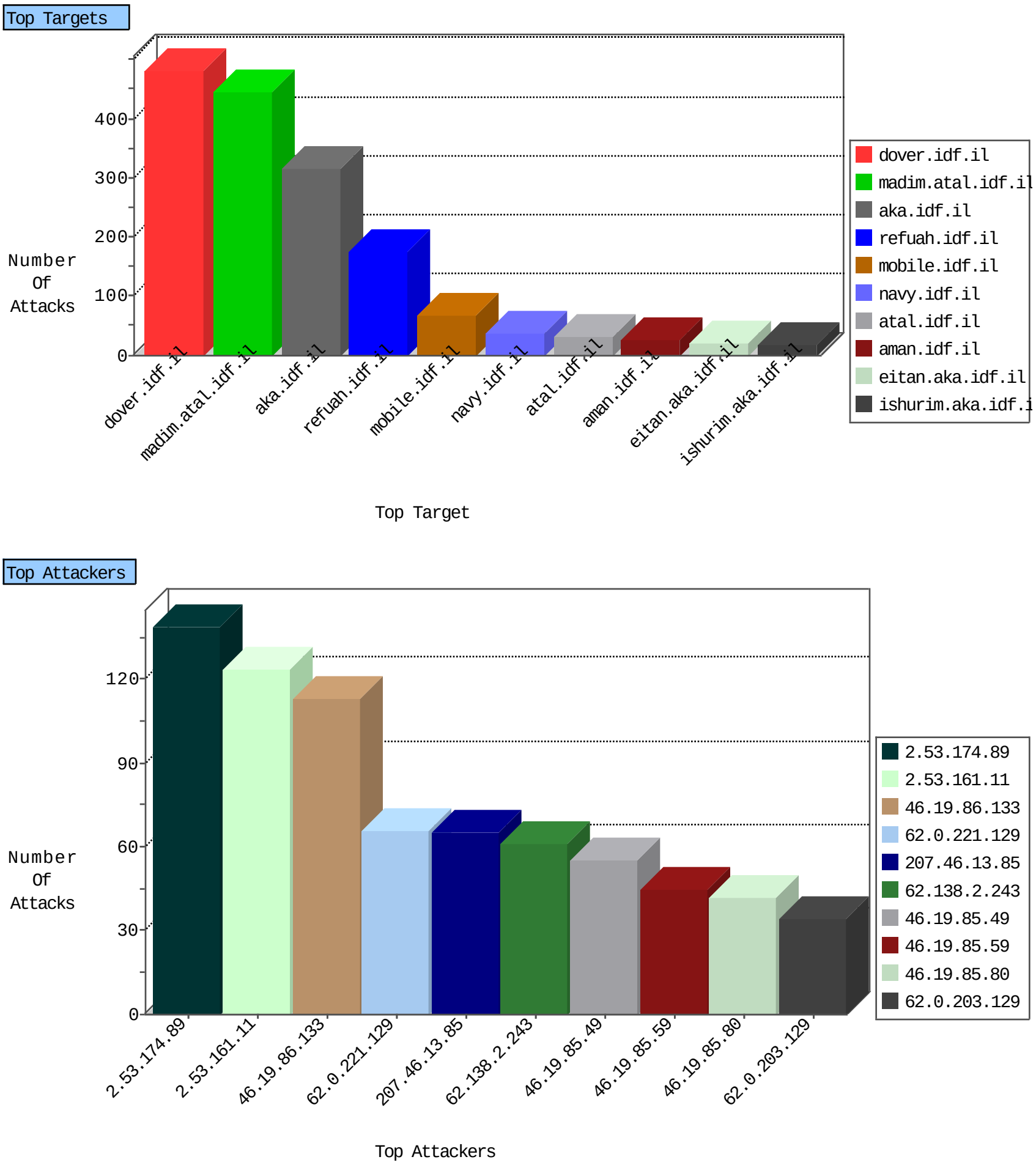
10-05-2016-11:04:05 to 10-05-2016-12:04:05

IDF Under Attack Daily Report



10-05-2016-11:04:05 to 10-05-2016-12:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.90.25.90	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
84.109.4.76	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
82.145.208.51	Europe	147.237.76.42	refuah.idf.il	Black List	drop	5
77.138.15.134	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
2.53.189.254	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
2.53.38.97	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
71.6.146.186	United States	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1
192.187.118.69	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
2.53.150.63	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
2.55.41.120	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-05-2016-11:04:05 to 10-05-2016-12:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.138.2.243	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	60
69.30.198.178	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.138.2.243	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

10-05-2016-11:04:05 to 10-05-2016-12:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.86.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
217.23.6.58	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
77.127.11.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.23.6.58	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
54.90.189.128	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.83.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.229.223.8	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
212.25.83.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.130.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.236.132.115	147.237.77.216	Iraq	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.76.148	United Kingdom	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
31.154.81.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.236.86.32	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
92.247.34.203	147.237.77.170	Bulgaria	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
217.23.6.58	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.26.168	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.23.6.58	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
77.125.37.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.23.6.58	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.229.223.8	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.204.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.161.40.17	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
208.100.26.228	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.136.237.251	147.237.76.147	Iran, Islamic Republic of	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
31.168.2.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
119.147.84.8	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.130.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.230.86.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.183.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

10-05-2016-11:04:05 to 10-05-2016-12:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.46.13.85	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	65
62.0.203.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	34
62.0.221.129	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	33
62.0.221.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
62.0.200.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
2.53.184.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.49	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
62.0.205.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
46.120.47.186	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.85.80	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.85.80	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
46.19.85.49	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
46.19.85.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.59	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
176.13.238.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.159	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
46.19.86.212	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.59	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
62.90.167.68	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
194.90.25.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
194.90.25.90	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
79.177.161.207	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
2.55.49.30	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
176.13.246.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
62.90.161.203	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
62.0.197.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
62.0.229.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.246.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
185.32.179.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.32.179.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.32.179.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.152	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.152	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
1.47.36.144	Thailand	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.55.56.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.55.130.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
185.32.179.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.55.130.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.55.130.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.32.179.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.174.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	139
2.53.161.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
46.19.86.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
2.53.130.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
2.53.14.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
109.253.145.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
109.253.214.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
213.151.56.143	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.151.56.143	Block	4
79.180.183.24	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.180.183.24	Block	4
193.105.199.65	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
37.26.146.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
193.105.199.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
77.139.85.161	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	3
37.26.149.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.133.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.238.74	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.66.57.63	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	3
212.235.49.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	3
109.66.57.63	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	3
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
47.88.0.90	Canada	147.237.77.233	atal.idf.il	Multiple Admin Blocking from 47.88.0.90	Block	2
84.95.149.196	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
176.13.251.70	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
47.88.0.90	Canada	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 47.88.0.90	Block	2
185.32.179.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	2
81.218.163.134	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.121.79.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
31.168.240.238	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	2
176.13.246.117	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.180.183.24	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
2.53.5.99	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
157.55.39.208	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
46.210.133.254	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
87.71.28.104	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.81.214.73	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
176.13.247.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.93.251	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Unknown HTTP Request Method TÀ`Q[[#28]]%•Òy&K½«?Ÿ®jcf[[#3]]‰5/UV±&i‹rÁ€€Á¢¨&Òl[[#14]] in URL	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.19.86.212	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
10.100.35.38		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
80.178.101.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.12	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Method	Block	1
213.57.70.4	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.56.239	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1