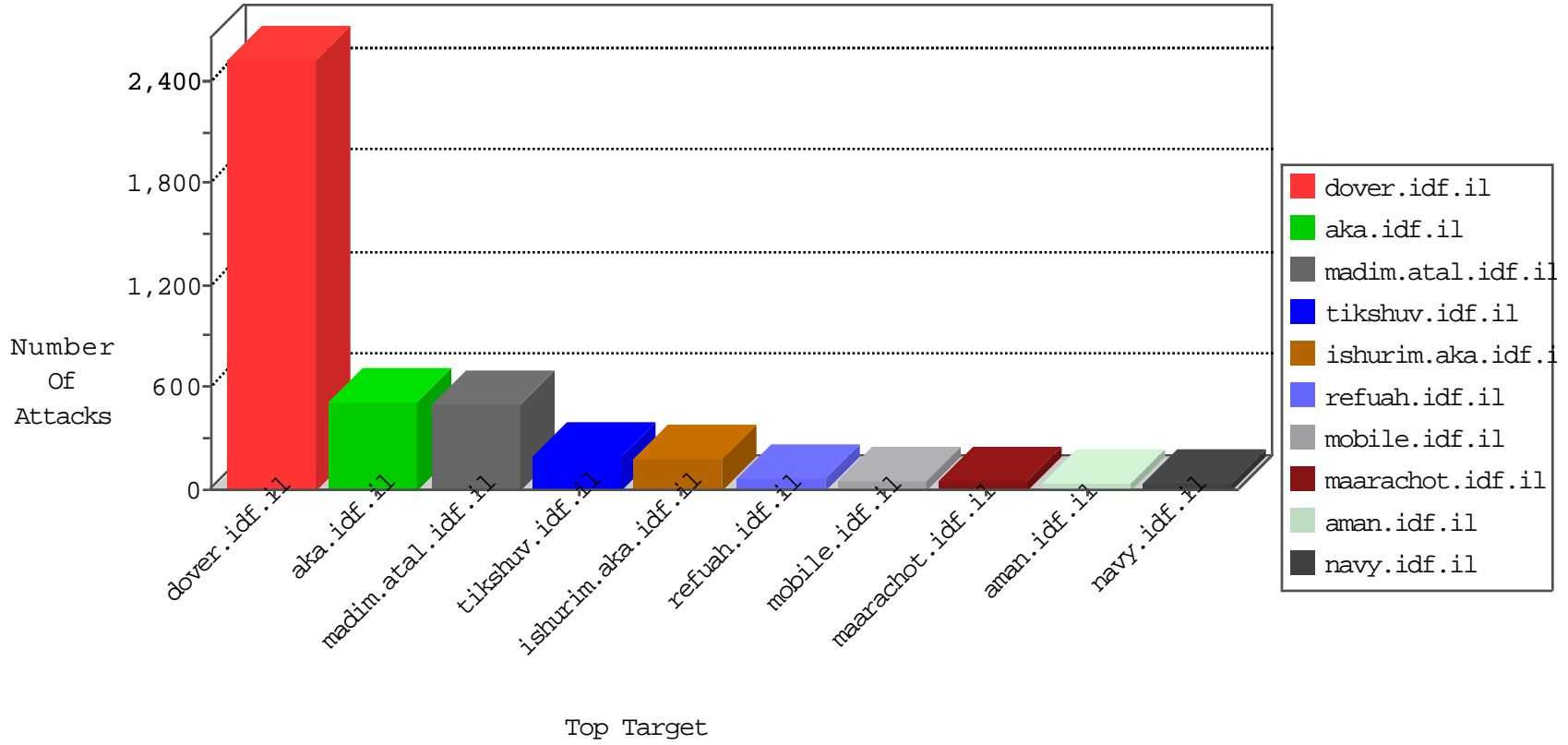


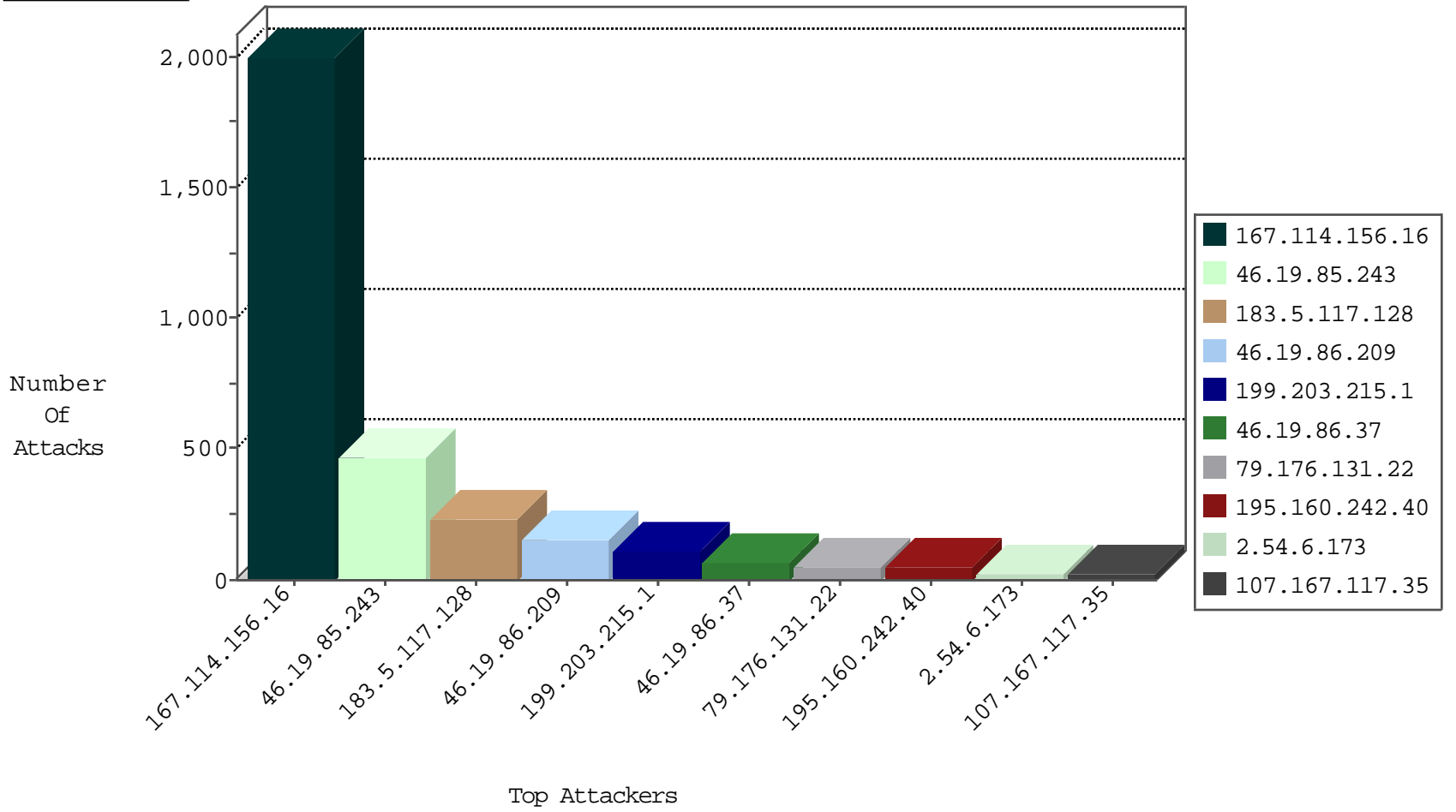
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3005
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	21
46.19.86.37	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
82.145.217.215	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
80.70.128.129	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
46.19.86.249	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
176.106.44.186	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
63.141.227.98	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
107.150.60.245	United States	147.237.77.205	prisha.idf.il	block-sp-trafl	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-trafl	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
142.54.160.212	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-trafl	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.5.117.128	China	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
183.5.117.128	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
183.5.117.128	China	147.237.72.166	aka.idf.il	0854: HTTP: upload* Access	Block	12
183.5.117.128	China	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	12

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
158.255.6.220	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.142.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.63.75	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.3	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1
46.120.144.248	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.32.64.164	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.196	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.231	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
158.255.6.220	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
149.88.139.16	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.232.169	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.73.198	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
62.90.235.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.196	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.130.41	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.231	147.237.0.200		m4u.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.209	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	150
183.5.117.128	China	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	31
183.5.117.128	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	31
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
107.167.117.35	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
80.179.114.27	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
176.13.5.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.0.81.17	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	13
192.0.80.167	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	13
62.0.197.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
213.57.146.178	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
213.57.247.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.86.37	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.19.86.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.86.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
37.26.148.212	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.54.147.177	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.117.58.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
37.26.147.156	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
212.235.124.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
195.160.242.40	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
62.0.200.198	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.37	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
138.134.192.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
84.108.189.31	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.177.237.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.166.140.117	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.188.55	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.114.91.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.85.52	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.178.198.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
80.178.198.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.0.82.17	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
46.19.85.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.0.200.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.52	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.104.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.6.173	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.148.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.21.87	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	6
89.218.71.214	Kazakstan	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
192.0.81.17	United States	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.178.16.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
192.0.80.128	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.178.141.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.7	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
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	262
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
199.203.215.1	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	106
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	80
79.176.131.22	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	52
183.5.117.128	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 183.5.117.128	Block	31
183.5.117.128	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 183.5.117.128	Block	31
81.218.48.37	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
213.57.146.178	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 213.57.146.178	Block	8
109.253.144.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
46.117.164.93	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
183.5.117.128	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	4
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	4
183.5.117.128	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
185.3.147.134	Israel	147.237.77.74	law.idf.il	Parameter Type Violation prefixText in www.law.idf.il/webservices/wscity.aspx/getcities	Block	3
176.13.19.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.49.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.50.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.5.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
185.3.146.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.13.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
17.138.57.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19405-he/dover.aspx)	Block	2
37.26.148.197	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
195.154.227.118	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
212.12.65.154	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationervice.aspx/getauthuser	Block	2
95.25.133.27	Russian Federation	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 95.25.133.27	Block	2
2.54.48.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
46.117.58.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	2
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	2
37.26.149.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
17.138.57.83	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.57.83	Block	2
197.134.238.71	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
37.26.148.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.65.25	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/111092.pdf	Block	1
46.163.68.109	Germany	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/shared/usercontrols/headerupper/	Block	1
2.54.181.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.243.72	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.194.206.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.199.61.93	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.199.61.93	Block	1
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
183.5.117.128	China	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 183.5.117.128	Block	1
77.75.76.166	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/28/	Block	1
207.46.13.10	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
37.142.68.30	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1