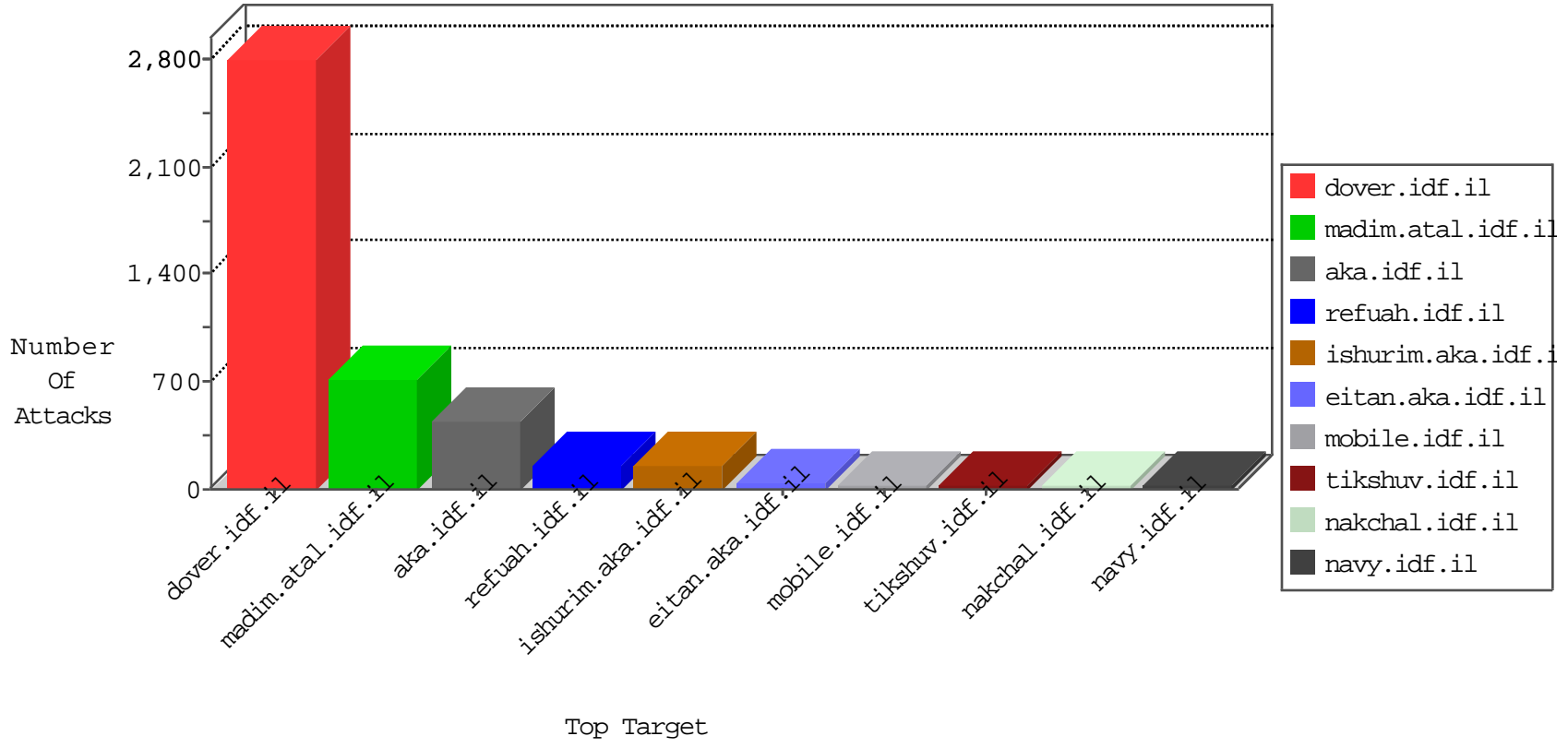


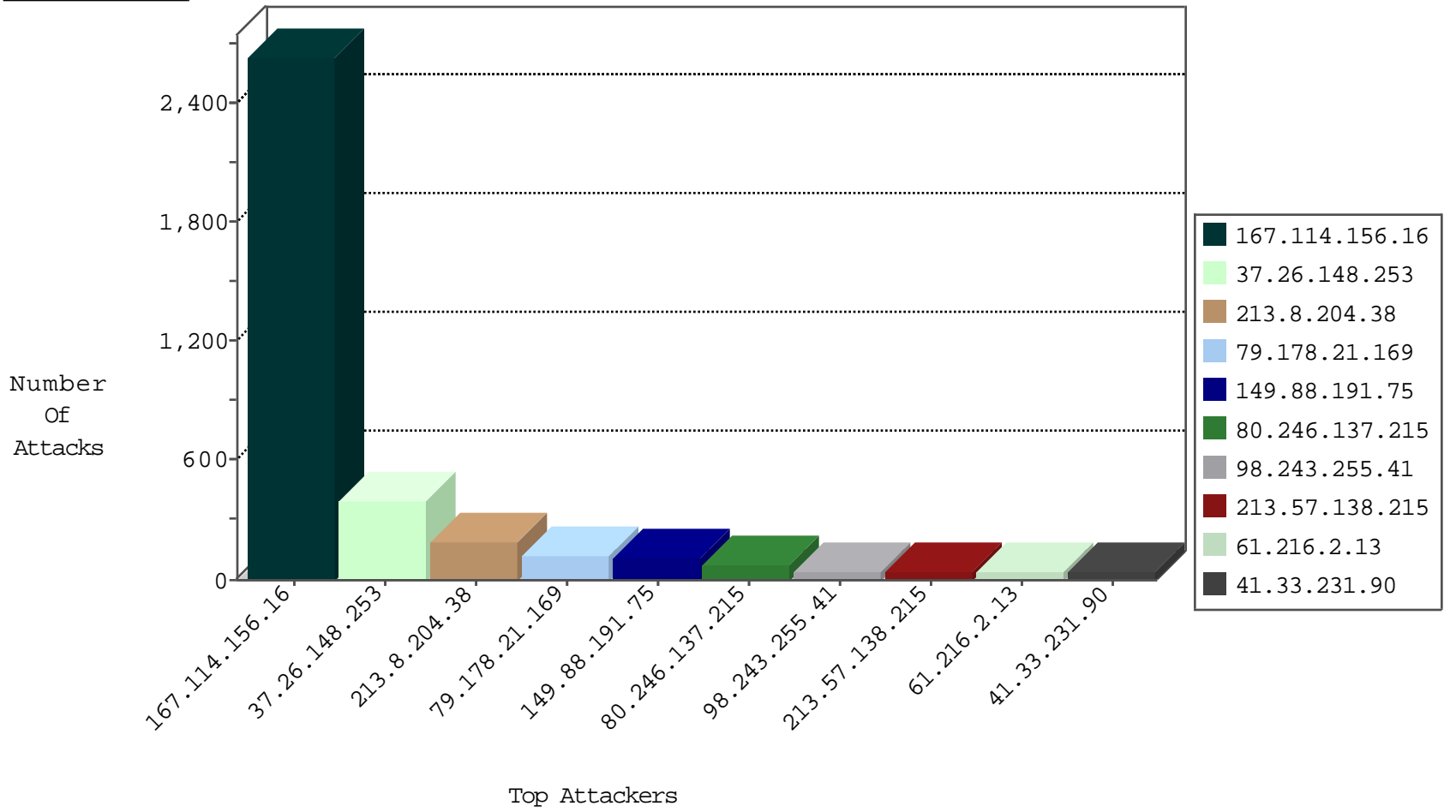
IDF Under Attack Daily Report



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	3608
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
113.36.223.46	Japan	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

12-10-2015-13:04:02 to 12-10-2015-14:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
31.154.33.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
17.142.156.171	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.10.255	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.108.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
24.188.206.110	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.29.220.190	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.56.82.28	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.111.138.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.82	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.178.21.169	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	125
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.120.125.21		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.182.60.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
149.88.191.75	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
149.88.191.75	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
213.57.138.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
213.57.138.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
109.65.135.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.121	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
89.139.35.129	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.116.73.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
213.57.135.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
213.57.135.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
37.26.148.199	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.26.149.221	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
149.88.191.75	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	8
213.57.135.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
213.57.144.100	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	7
82.80.158.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.183.105.129	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.42.70	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.11.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.248.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.52.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.142.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.168.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
61.216.2.13	Taiwan	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	6
37.26.148.253	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.65.142.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
120.36.226.3	China	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
109.64.97.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.36.68	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.106	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
213.57.129.222	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.235.91.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.14.128	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.168.89.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.16.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
61.216.2.13	Taiwan	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	6
79.179.52.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.12.151.89	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.173.190	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.149.221	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.244	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.253	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.148.253	Block	222
37.26.148.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
213.8.204.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	99
213.8.204.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
80.246.137.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
37.26.148.253	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 37.26.148.253	Block	59
98.243.255.41	United States	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
46.19.85.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
2.52.165.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
149.88.191.75	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Malformed URL from 149.88.191.75	Block	7
149.88.191.75	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
149.88.191.75	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Method from 149.88.191.75	Block	7
149.88.191.75	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Unknown HTTP Request Method from 149.88.191.75	Block	7
149.88.191.75	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Abnormally Long Request from 149.88.191.75	Block	6
149.88.191.75	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 149.88.191.75	Block	4
149.88.191.75	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 149.88.191.75	Block	4
212.76.98.118	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.76.98.118	Block	3
37.26.146.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.0.102	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	3
149.88.191.75	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Abnormally Long Header Line from 149.88.191.75	Block	3
149.88.191.75	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal HTTP Version from 149.88.191.75	Block	3
62.219.230.90	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
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
212.179.177.148	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
149.88.191.75	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple NULL Character in Url from 149.88.191.75	Block	2
79.176.21.62	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
5.102.192.138	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
80.246.138.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.116.73.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.142.211.138	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	2
31.154.160.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.178.11.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
84.109.160.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.117.69.237	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
46.19.85.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.88.191.75	Israel	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in Method Ã¿Ã¿[[#25]]-Ã¿pÃ¿-C]QwÃ¿³	Block	1
79.179.52.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
176.12.140.124	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.65.142.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
61.216.2.13	Taiwan	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method	Block	1
149.88.191.75	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Malformed HTTP Header Line from 149.88.191.75	Block	1
89.138.207.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.49	United States	147.237.72.166	aka.idf.il	Unknown Parameter 1225bd80 in www.aka.idf.il/iturim/asp/results.asp	None	1
46.116.67.198	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 46.116.67.198 (Open Mode)	None	1
149.88.191.75	Israel	147.237.72.167	ishurim.aka.idf.il	Malformed HTTP Header Line 1	Block	1
77.125.128.228	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.17.249	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1