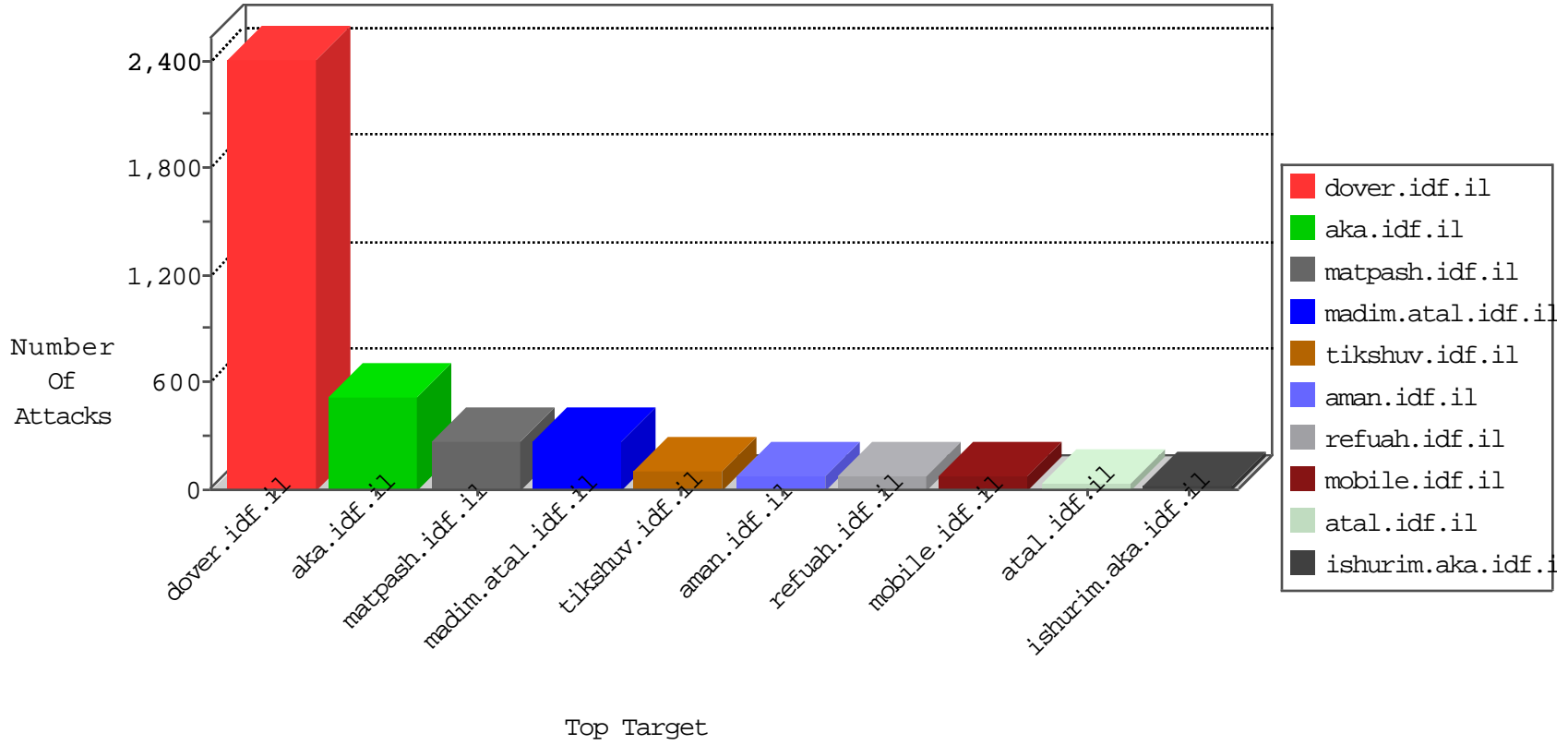


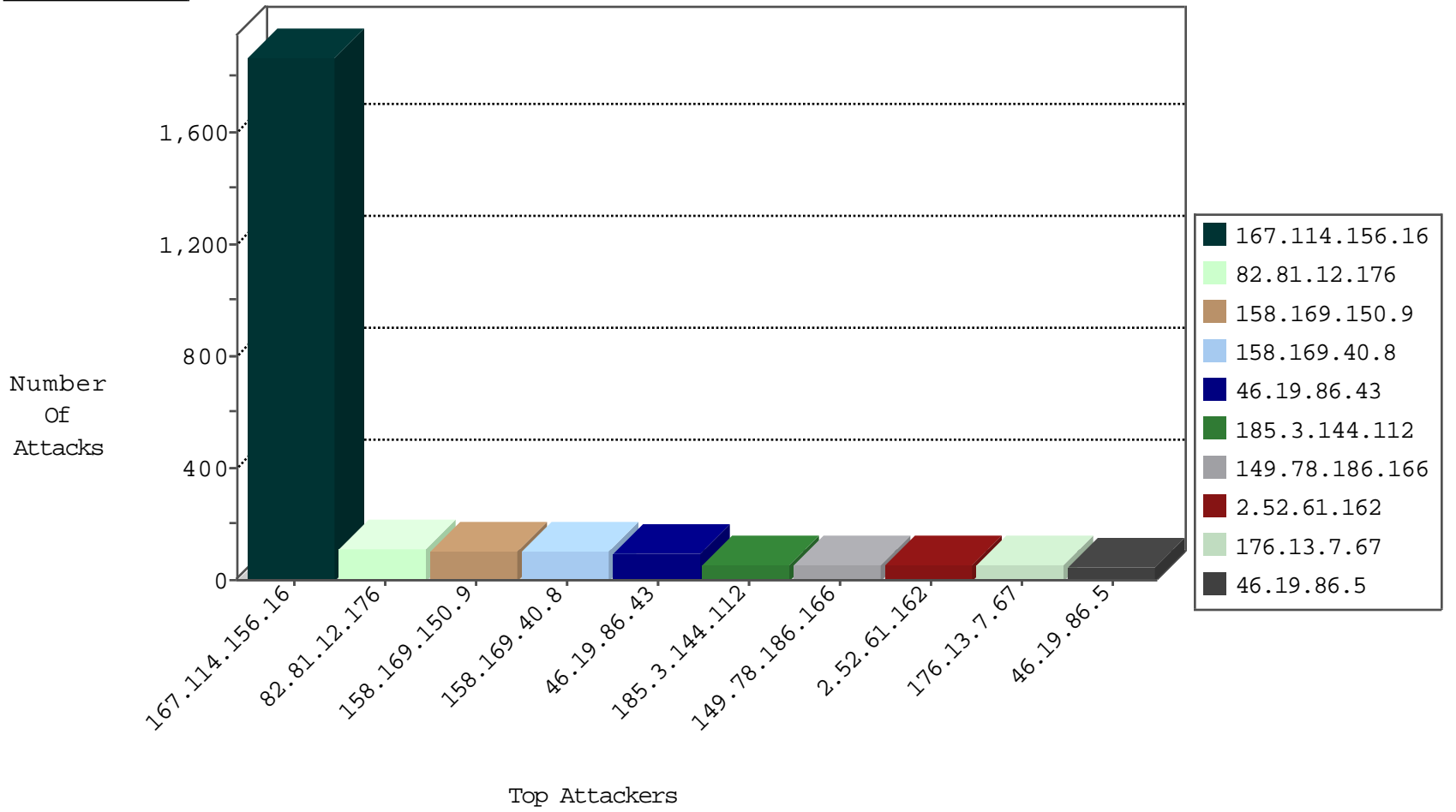
IDF Under Attack Daily Report



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	3073
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	107
79.180.161.175	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
78.188.47.90	Turkey	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
105.107.214.137	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
185.130.5.224		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.143.228	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	14
37.26.146.198	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
199.58.86.209	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
46.121.97.32	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
162.210.196.130	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
177.185.194.138	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
105.107.214.137	Algeria	147.237.77.216	dover.idf.il	10767: HTTP: Acunetix Security Scanner	Block	1

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.i	GPL SCAN nmap TCP	11
81.218.111.210	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
158.169.150.9	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	104
158.169.40.8	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	102
185.3.144.112	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	55
46.19.85.169	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
83.101.10.104	Belgium	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	37
96.95.14.9	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
46.19.86.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
37.26.148.156	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
158.169.40.6	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	16
82.166.57.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	15
41.176.234.30	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
85.130.175.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
158.169.150.6	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
109.160.233.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.183.124.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
158.169.150.8	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
212.29.225.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
149.78.30.154	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
80.246.133.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.178.98.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.147.166	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.89.230.246	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.15.70	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
82.192.95.184	Netherlands	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.52.6.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.228.70.98	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.249.74.249	Algeria	147.237.77.216	dover.idf.il	drop		drop	6
37.26.148.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
31.210.186.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
94.230.86.228	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
31.168.209.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
207.46.13.88	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.66.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.186.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.52.43	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.67.165.155	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
96.95.14.9	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.52.43	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
149.78.186.166	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 149.78.186.166	Block	53
176.13.7.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
2.52.61.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
176.13.19.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
37.26.149.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
2.52.61.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.19.86.5	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
46.19.86.5	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	7
80.246.136.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.30.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
105.107.214.137	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.107.214.137	Block	4
37.26.147.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.68.21.165	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
176.13.3.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.0.28	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	3
85.250.111.191	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtCity in madim.atal.idf.il/1088-he/meretz.aspx	Block	2
176.13.11.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
159.203.83.207	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 159.203.83.207	Block	2
46.19.85.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.178.98.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	2
109.65.54.72	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.126.58.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.172.6	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
66.249.78.130	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
195.154.146.225	France	147.237.72.166	aka.idf.il	Illegal HTTP Version HTTP/	Block	1
66.220.158.100	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.186.157	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
81.218.53.114	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/_vti_bin/owssvr.dll	Block	1
149.78.30.154	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
79.182.174.119	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	1
70.39.157.196	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/71700	Block	1
213.57.140.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
89.138.193.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.102.254.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.176.95	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-9338-he/dover.aspx	Block	1
185.3.147.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.12.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.43	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
54.85.87.184	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/wp-login.php	Block	1
109.253.213.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.20.138	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
207.46.13.36	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/670-2423-he/patzar.asp	Block	1
40.77.167.56	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/sitenap/sitenap.aspx	Block	1
85.250.254.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1