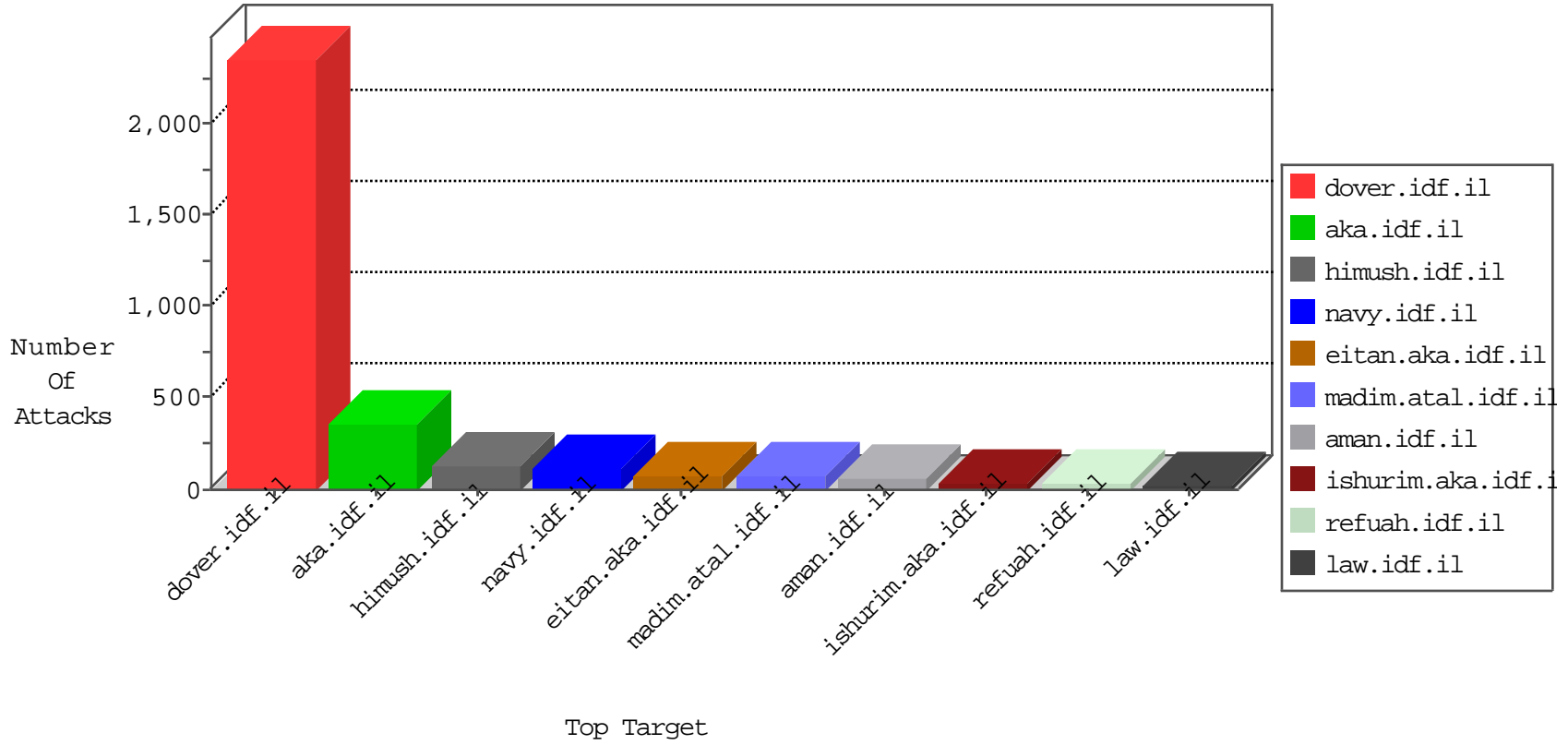


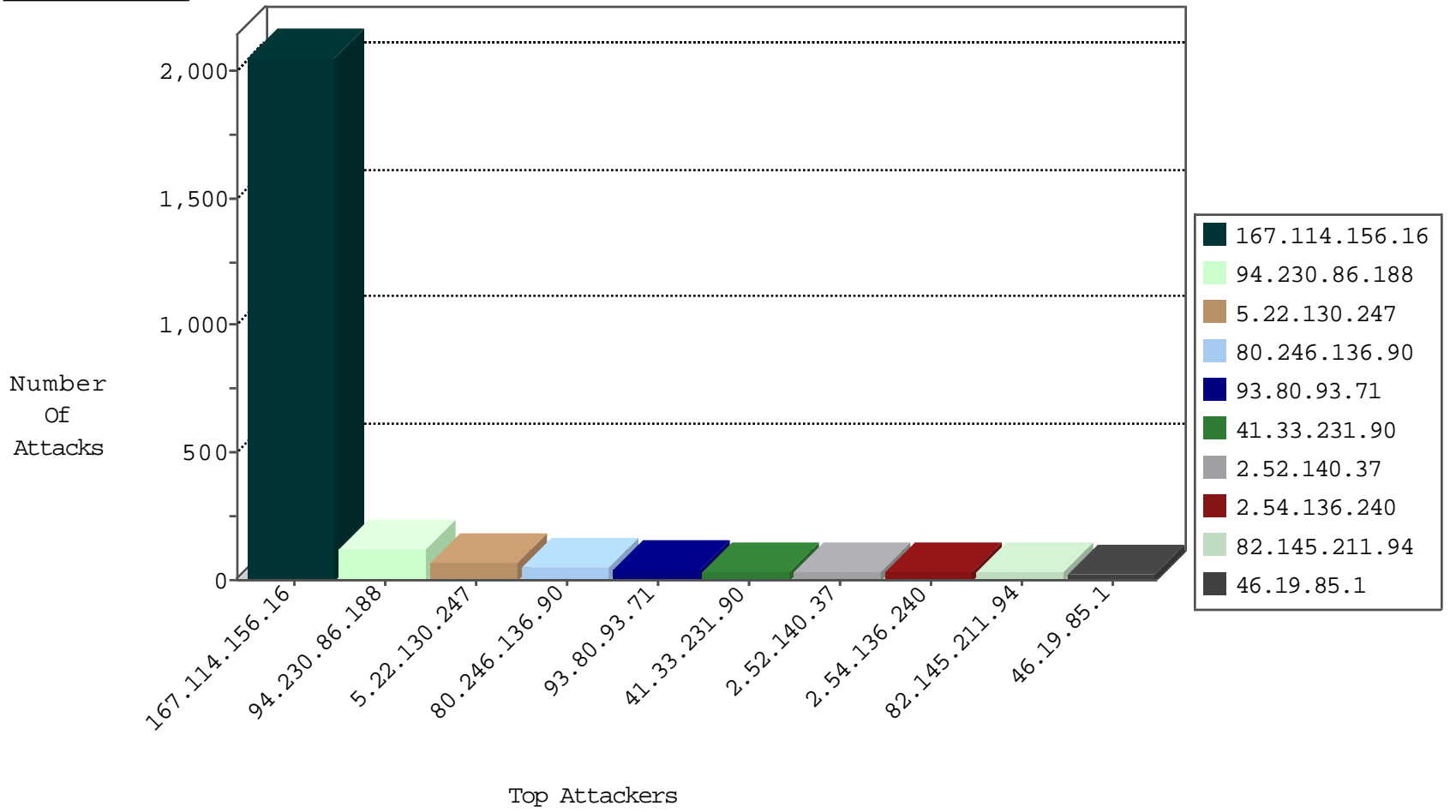
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4030
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3024
66.249.69.34	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	936
82.145.211.94	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	28
95.24.48.96	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
111.121.193.18	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
107.150.55.214	United States	147.237.76.31	nakchal.idf.il	block-sp-trafl	drop	1
66.240.236.119	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
93.80.93.71	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
182.160.107.83	Bangladesh	147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
198.20.69.77	United States	147.237.8.24	e.lifestyle.idf	13840: TLS: OpenSSL Heartbeat Packet	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.230.86.188	147.237.76.30	Israel	himush.idf.il	ET SCAN NMAP -sA (2)	122
84.228.78.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
46.225.127.223	147.237.0.35	Iran, Islamic Republic of	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.242.245.138	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
45.32.36.233	147.237.76.176		test.noore.idf.il	ET SCAN Potential SSH Scan	1
162.242.245.138	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
5.39.222.253	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
123.139.28.144	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
123.139.28.144	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
121.201.27.61	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
109.64.22.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.150.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.230	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
45.32.36.233	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
162.242.245.138	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
5.39.222.253	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
123.139.28.144	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
123.139.28.144	147.237.76.177	China	noore.idf.il	ET SCAN Potential SSH Scan	1
121.201.27.61	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
109.253.209.75	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.173.76	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
96.127.71.88	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.247	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.22.130.247	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
213.8.204.35	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
2.52.140.37	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.86.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.180.51.23	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
80.246.136.55	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.173	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
93.80.93.71	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
5.102.254.25	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.162.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.136.240	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
93.80.93.71	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
79.180.51.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
93.80.93.71	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
93.80.93.71	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
110.168.230.28	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.212	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.1	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.32.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.198.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.148.136	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.96	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.182.172.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.27	Israel	147.237.76.86	navy.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	monitor	6
84.94.174.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
46.19.85.120	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.96	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.111.7.5	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.172.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.63.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.90	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.1	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.173.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.32.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.140.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
81.218.168.131	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
2.54.136.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.27	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
141.105.68.30	Russian Federation	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.52.140.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.136.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
17.138.57.83	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.57.83	Block	10
2.54.188.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
77.125.97.205	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.125.97.205	Block	4
87.69.110.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
80.246.137.205	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
37.26.147.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
178.137.85.67	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.137.85.67	Block	3
141.105.68.30	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 141.105.68.30	Block	2
141.105.68.30	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 141.105.68.30	Block	2
37.26.149.240	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
2.52.37.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.64.129.48	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.13.12.49	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.12.49	None	2
5.29.62.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.49.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.75.77.109	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/30/	Block	1
91.226.212.160	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.111.80.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.236	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
207.46.13.170	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
80.82.64.68	Netherlands	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to habbo.yt/public/css/960_12_col.css	Block	1
37.26.148.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.3.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.164.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.103.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.230.210	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 77.127.230.210	Block	1
87.69.110.137	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.69.110.137	Block	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
46.19.85.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
178.137.85.67	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
80.246.136.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.126.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.135.66.213	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.52.7.113	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
84.111.242.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.84.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
80.246.136.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.11.24	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
2.54.164.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.195.227	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
77.127.242.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/achar	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
46.19.85.119	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
178.255.215.87	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/23709.doc	Block	1
79.182.148.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.32.71	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.97.205	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1