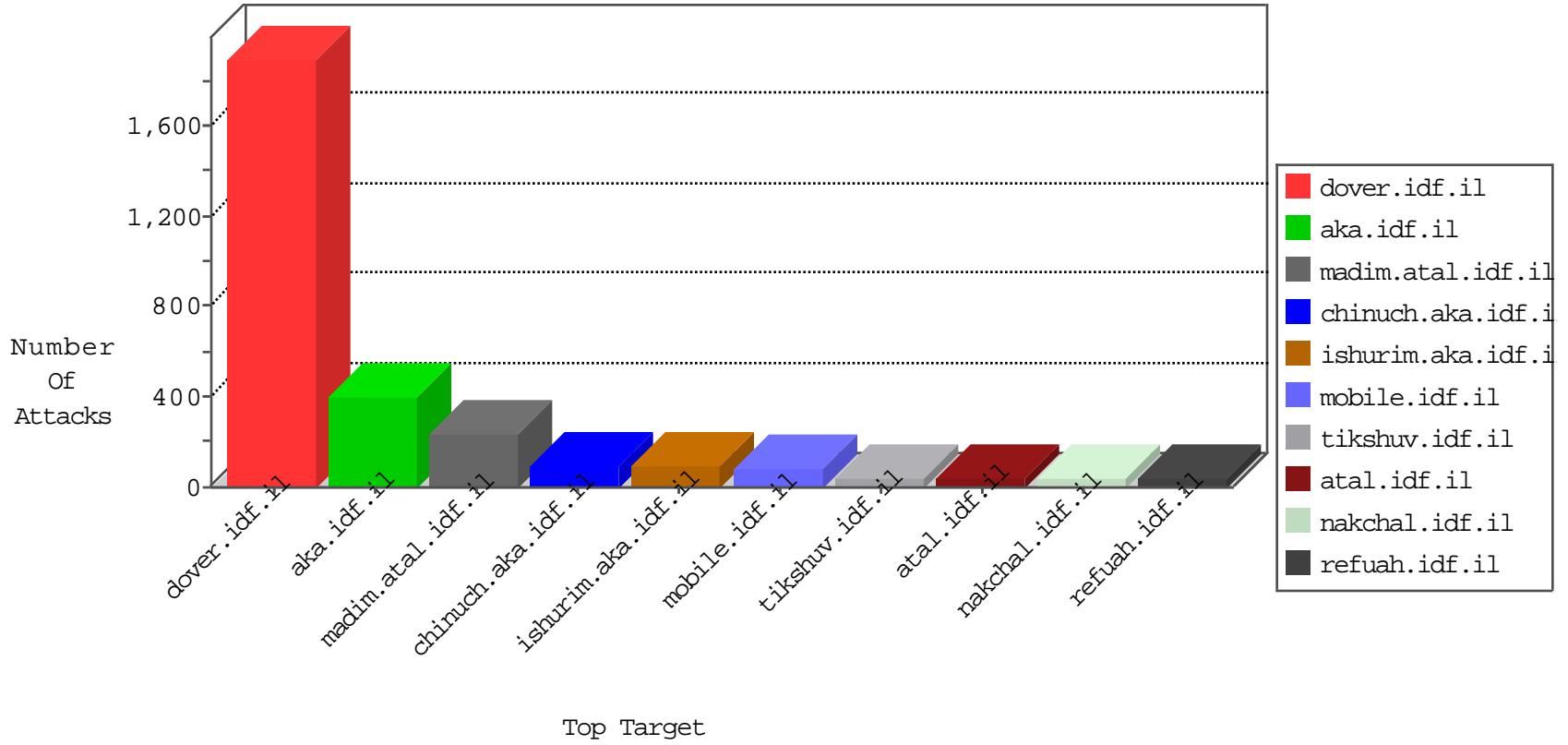


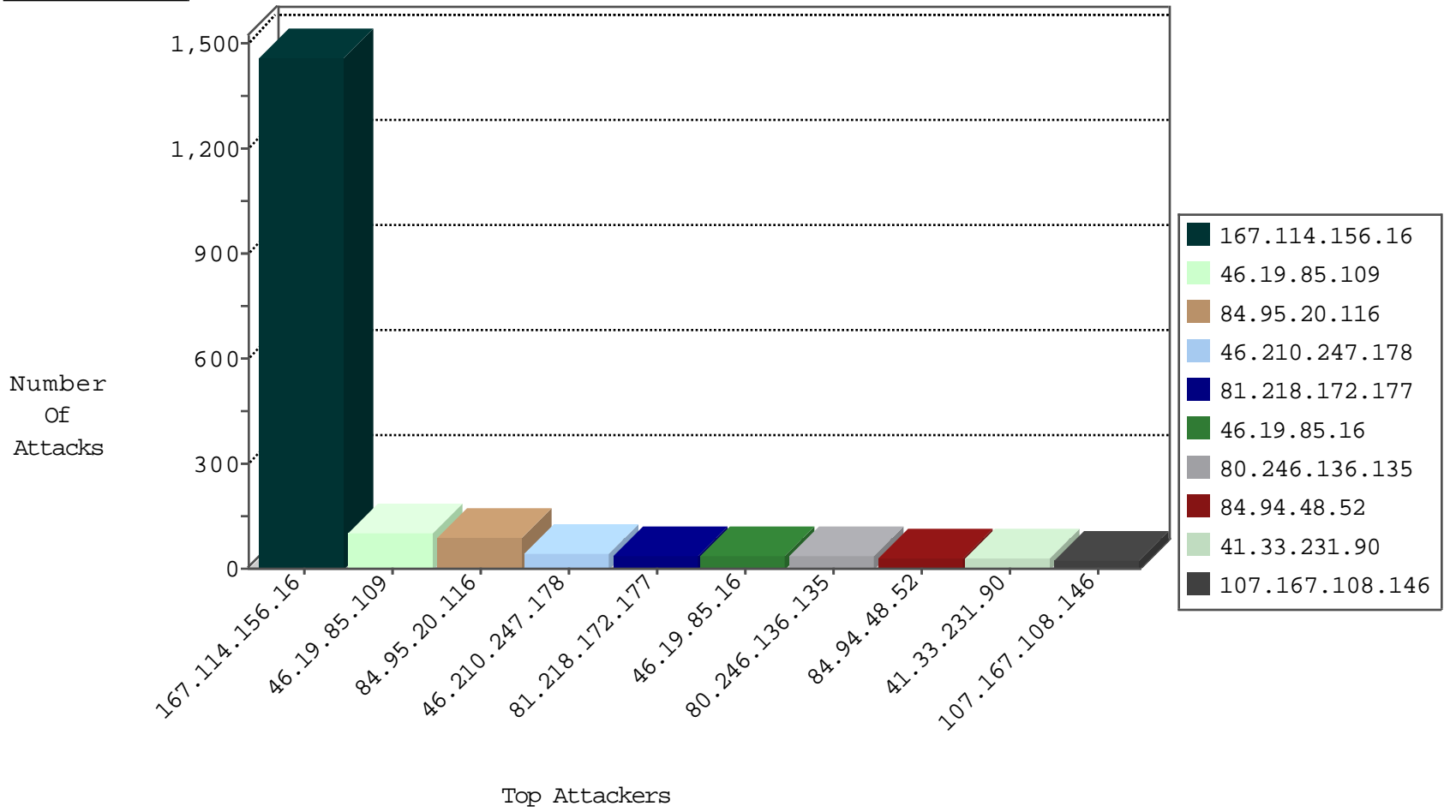
IDF Under Attack Daily Report



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	4008
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3689
66.249.73.214	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3219
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	247
46.210.247.178	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	30
80.178.230.135	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
46.19.86.171	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
37.142.232.101	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
31.168.225.146	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
2.54.142.199	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
109.184.184.214	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
37.26.148.222	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
77.247.178.132	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
193.242.218.6	Switzerland	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
185.130.5.207		147.237.76.31	nakchal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.130.5.207		147.237.76.31	nakchal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
52.1.90.117	United States	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.52.32.193	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
209.126.116.147	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
46.19.86.245	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.191.56.188	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
5.102.254.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.114.146.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.207	147.237.76.31		nakchal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
109.66.121.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.162.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.94.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.48.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.84.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.109	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
209.126.116.147	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.191.56.188	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -f -sS	1
193.47.165.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
119.17.25.137	147.237.77.178	Korea, Republic of	e.matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
95.86.121.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.218.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.101.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.216.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.95.20.116	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
46.19.85.16	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
84.94.48.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
107.167.108.146	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
176.13.14.47	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
79.183.216.41	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
81.218.172.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
81.218.172.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
41.77.138.90	Egypt	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	18
31.168.152.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	17
31.168.149.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	16
37.26.146.183	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.147.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.253.159.182	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
107.6.123.226	Singapore	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	13
2.54.47.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
46.19.85.241	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.52.60.202	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
37.26.149.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
37.26.148.204	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.95.146.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.203	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.148.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.52.32.193	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.50.100.35	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.203	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.6.64.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.23.123	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.146.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.114.105.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.22.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
122.107.224.59	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.253.137.124	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.215.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.166	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.255.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.137.124	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	97
80.246.136.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
176.13.22.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
79.176.118.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
109.186.133.202	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
46.19.86.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
2.54.13.233	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
93.179.68.209	United Kingdom	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
176.13.16.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.14.47	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
93.179.68.209	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.179.68.209	Block	5
176.13.9.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.43.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.207.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.101.3	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 81.218.101.3	Block	3
176.13.21.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.111.229.191	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/1133-22638-he/dover.aspx.	Block	2
109.253.128.247	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
2.54.104.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.17.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.111.9.100	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.73.178	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
37.26.149.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.145.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
2.54.144.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	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
79.178.140.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
50.62.177.8	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
176.13.22.86	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.139.153.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
81.218.101.66	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/booklets.aspx	Block	1
149.78.3.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.154.146.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.34.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
74.82.47.4	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
184.168.200.188	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
84.228.49.191	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.117.123.149	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
37.26.149.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.192.165	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
80.246.140.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.139.19	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1