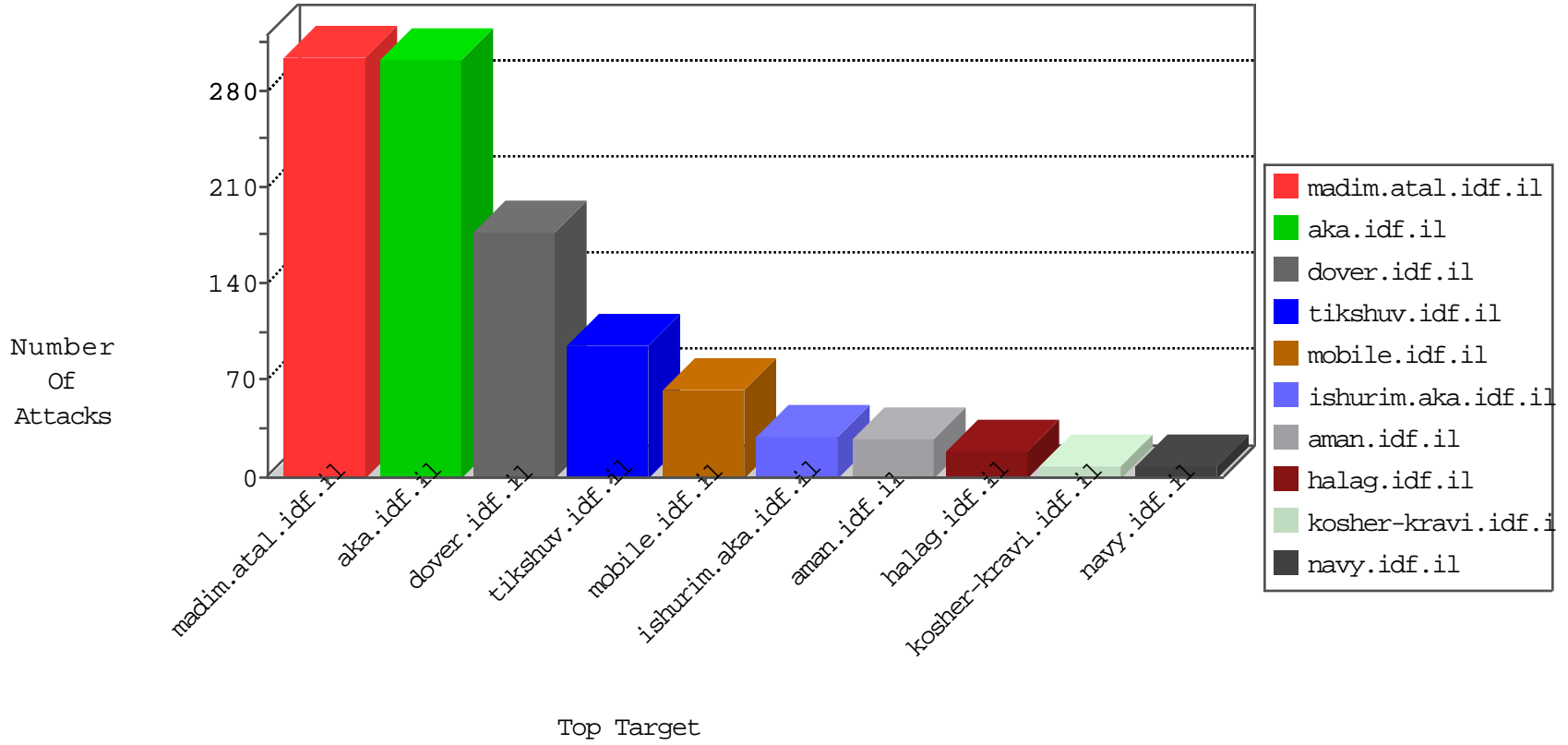


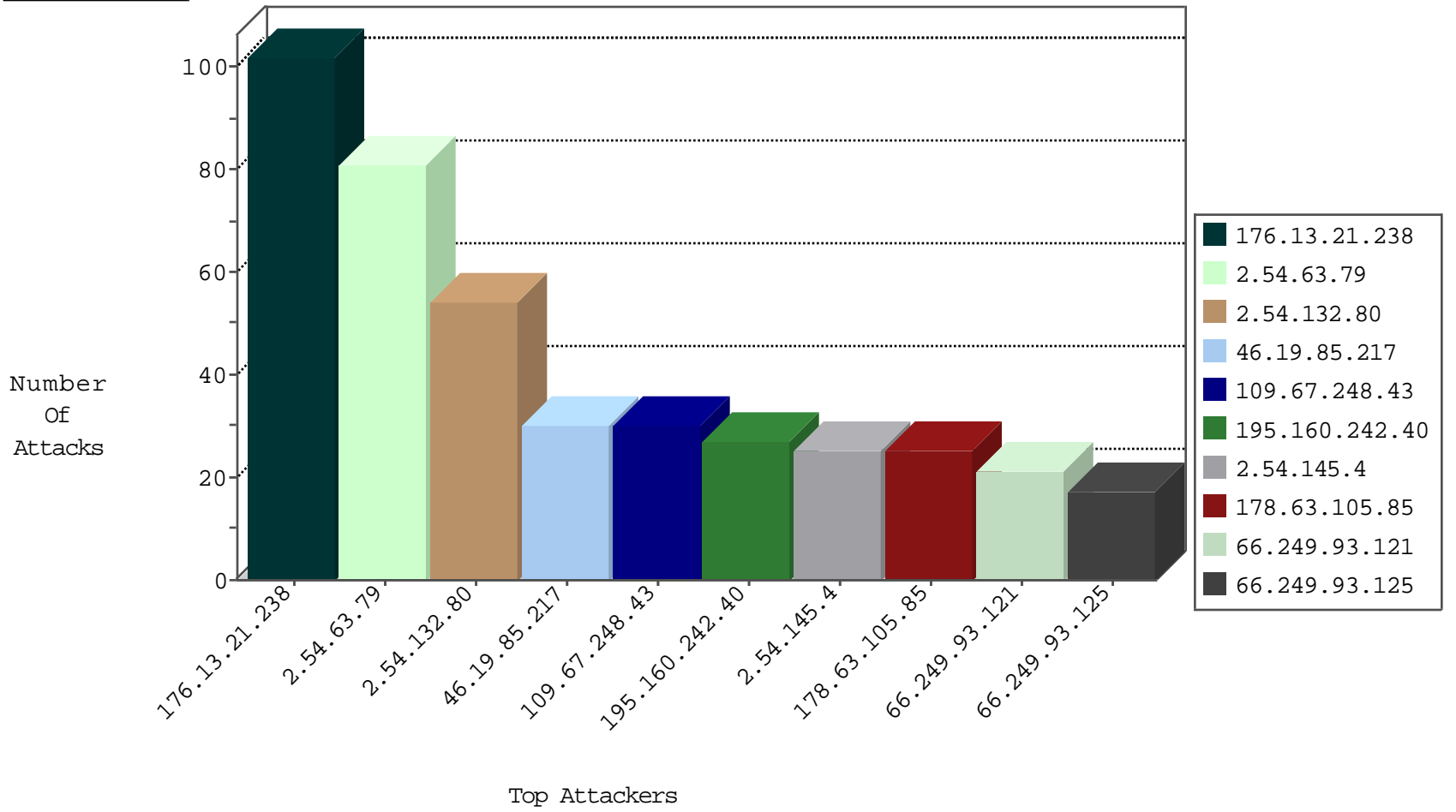
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
82.81.54.21	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
89.248.174.4	Netherlands	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.106	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
64.246.161.190	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-trafl	drop	1
89.248.174.4	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.74	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.120.176	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
83.130.108.116	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
5.29.150.215	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
85.65.111.36	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.183.29.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
46.117.7.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.198.151.45	147.237.72.166	Europe	aka.idf.il	ET SCAN NMAP -sA (2)	1
5.29.185.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.73.194.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.164.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.77.216	Canada	dover.idf.il	ET SCAN NMAP -f -sS	1
2.52.23.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.184.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.184.187	147.237.72.217	Israel	e.idf.il	ET SCAN NMAP -sS window 3072	1
79.183.186.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.141.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
216.223.27.55	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.45.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.175.119	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.77.216	Canada	dover.idf.il	ET SCAN NMAP -sS window 2048	1
2.54.160.136	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.71.68.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
83.130.108.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.229.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
216.72.40.186	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
109.67.248.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.93.121	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	21
66.249.93.125	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
2.54.145.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
176.13.20.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.57.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	11
176.13.10.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.0.244.129	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	8
80.74.100.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.108	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
62.0.197.201	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
176.13.2.230	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.26.149.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.74.105.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
195.160.242.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
188.120.132.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.251	Israel	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	6
2.54.171.28	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	5
46.19.86.186	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	4
91.199.69.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.26.146.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	4
82.80.196.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	4
2.54.29.199	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	4
46.19.85.114	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.0.212.201	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
77.126.237.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.182.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.132.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.29.197.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.29.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.54.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.194.207.24	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
31.168.123.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.48.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.231.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.23.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.160.242.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.54.44.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.109.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.21.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
2.54.63.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
2.54.132.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
46.19.85.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
80.246.139.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 195.160.242.40	Block	10
176.13.10.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	4
46.19.86.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.184	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
46.19.86.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.20.85	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.204.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.54.247	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
89.235.207.220	Estonia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	2
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	2
37.26.146.251	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.147.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.8.10.16	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/himush	Block	2
84.109.89.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.51.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	2
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 195.160.242.40	Block	2
212.76.107.108	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/&sa=u&ved=0ahukewjk47tpoq7lahwbvbokhdjyd54qf ggumae&usg=afqjcnexum5xtap6fajrxy3kwnzuyhjgig	Block	2
89.235.207.220	Estonia	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
2.54.173.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.136.252	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	2
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
37.26.146.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.126.128	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
212.179.21.194	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
151.252.97.208	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	1
2.54.184.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.194.207.24	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.52.24.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
79.182.116.217	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Unknown HTTP Request Method oà±@•^ù[[#16]]E>i in URL	Block	1
37.26.146.249	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.145.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
2.54.57.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
212.179.218.166	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.108.67.76	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/new	Block	1
192.116.248.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in Header Name •[[#31]]Nç^îá•Ø[[#25]]€€0#[[#19]]9{!ÊÂc•Ê^s¼	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
5.164.94.62	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx	Block	1