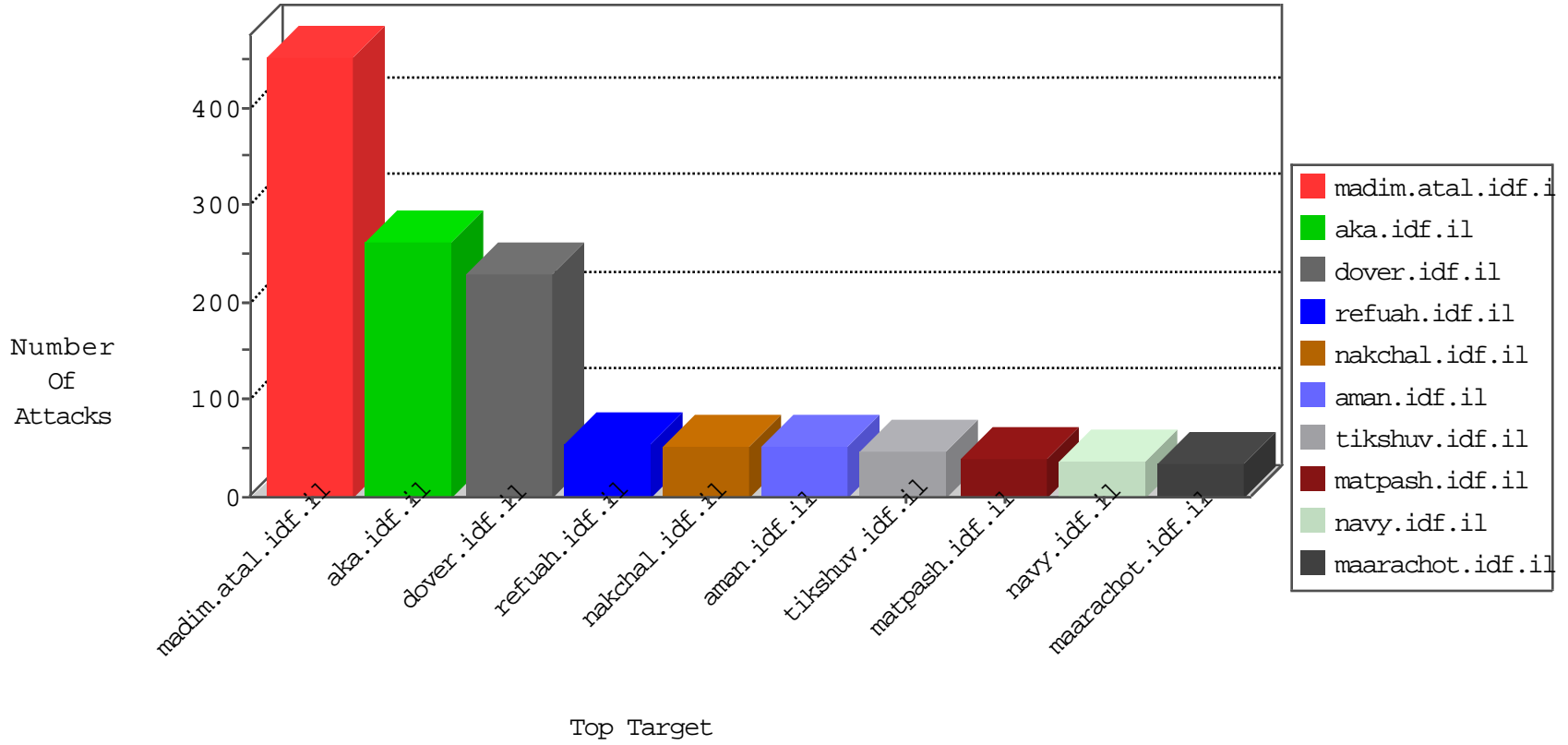


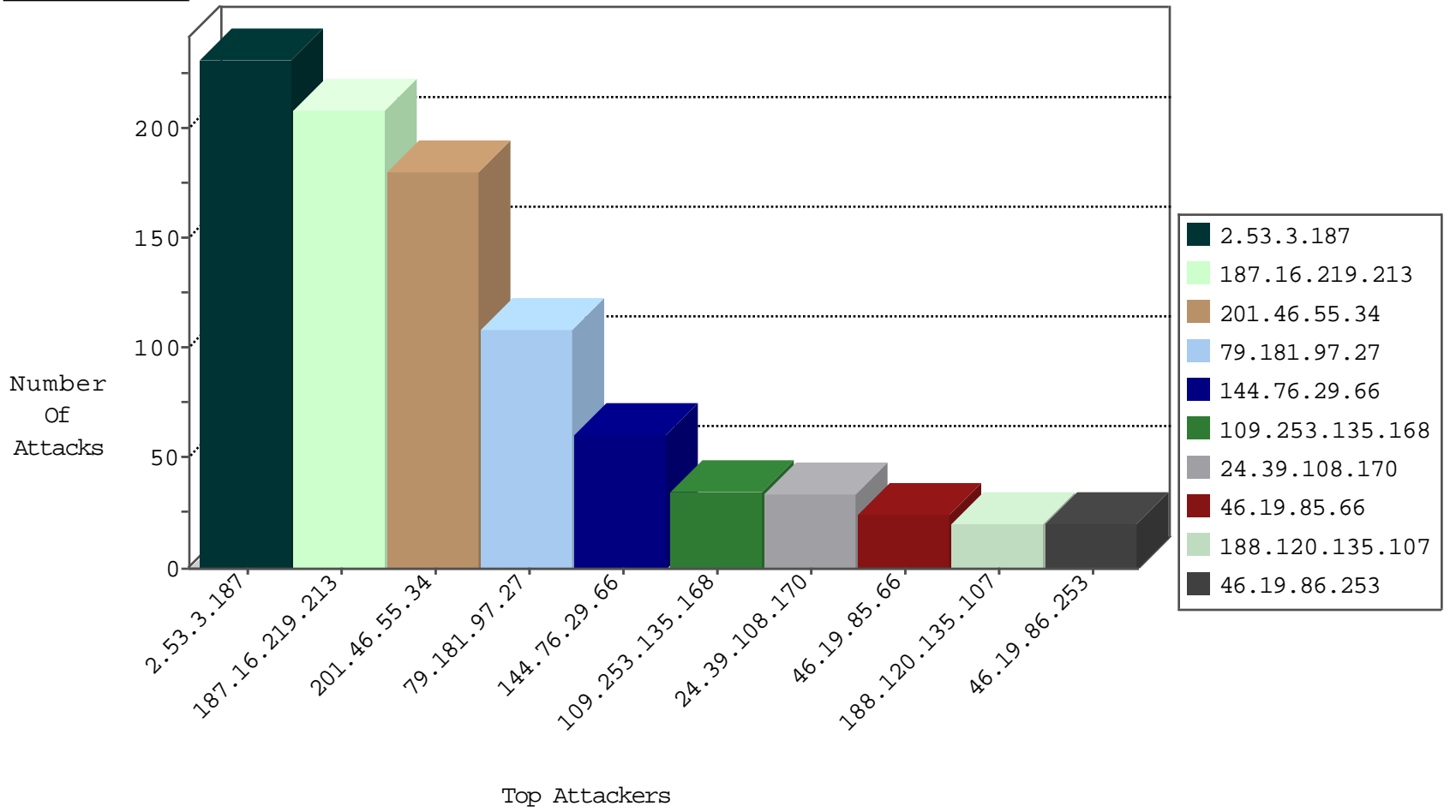
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
2.53.47.187	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
115.210.247.109	China	147.237.72.217	e.idf.il	JLM_Purple_Con_Limit_Tcp	drop	2
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
156.56.250.226	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.29.66	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	27
144.76.29.66	Germany	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	7
144.76.29.66	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	7
144.76.29.66	Germany	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Permit	6
144.76.29.66	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	6
144.76.29.66	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	5
144.76.29.66	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	13
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
188.0.236.165	147.237.77.205	Moldova, Republic of	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.137	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	1
163.172.169.150	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.254.9.91	147.237.0.16	Sweden	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
115.239.248.226	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.52.71	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.158.203.147	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
2.55.153.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
217.132.102.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.255.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.98.45.160	147.237.0.200	France	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
79.177.30.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.149	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.139	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	1
187.79.234.139	147.237.77.216	Brazil	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.100.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
115.239.248.226	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
111.68.107.43	147.237.72.166	Pakistan	aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	1
93.158.203.149	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	147.237.76.197	Indonesia	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
2.53.58.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
213.8.204.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.98.45.160	147.237.0.200	France	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
77.126.65.170	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
24.39.108.170	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
188.120.135.107	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	17
77.138.253.85	France	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
99.122.115.104	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
187.16.219.213	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
187.16.219.213	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
46.19.85.96	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
187.16.219.213	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
187.16.219.213	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
201.46.55.34	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
187.16.219.213	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
187.16.219.213	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
187.16.219.213	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
201.46.55.34	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.19.85.66	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
201.46.55.34	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
109.66.181.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
187.16.219.213	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
201.46.55.34	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
187.16.219.213	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
187.16.219.213	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
187.16.219.213	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
187.16.219.213	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
187.16.219.213	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.34	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
187.16.219.213	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.34	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
185.7.100.98	France	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
201.46.55.34	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.34	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
187.16.219.213	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
108.175.11.17	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
187.16.219.213	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.86.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
201.46.55.34	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.34	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
187.16.219.213	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
187.16.219.213	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
77.92.230.94	Georgia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
5.22.134.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
187.16.219.213	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
185.7.100.98	France	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
187.16.219.213	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.3.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	232
79.181.97.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
185.32.179.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
46.19.86.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
46.19.86.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
79.177.172.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachr/	Block	6
80.246.139.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.55.19.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.181.97.27	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00\$ContentPlaceholder1\$txtLastName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	4
79.180.32.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.11.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.141.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.164.106	France	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
109.253.139.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.17.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.159.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.159.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.7.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.133.80	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
85.65.5.240	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 85.65.5.240 (Unknown SSL Session)	None	2
46.19.85.206	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
213.151.35.216	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	2
109.253.223.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.12	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
113.61.100.242	Australia	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	2
46.19.86.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.132	Israel	147.237.76.42	refuah.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.132	Block	1
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
68.180.229.190	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
113.61.100.242	Australia	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 113.61.100.242	Block	1
87.69.164.38	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.132	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
2.53.16.82	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
46.120.206.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.132	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method ih in URL	Block	1
212.199.118.19	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.199.118.19	Block	1
84.109.126.116	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
31.13.114.82	Ireland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/8/size220x0/1738.jpg	Block	1
114.97.198.63	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 114.97.198.63	Block	1
77.92.230.94	Georgia	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
89.139.139.183	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
46.19.86.26	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.132	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version	Block	1
192.198.151.44	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluum/templates/home.asp	Block	1
82.81.160.69	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.81.160.69	Block	1
157.55.39.254	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in aka.idf.il/main/giyus/	None	1
77.138.165.149	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/kiosk	Block	1
47.54.146.126	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1