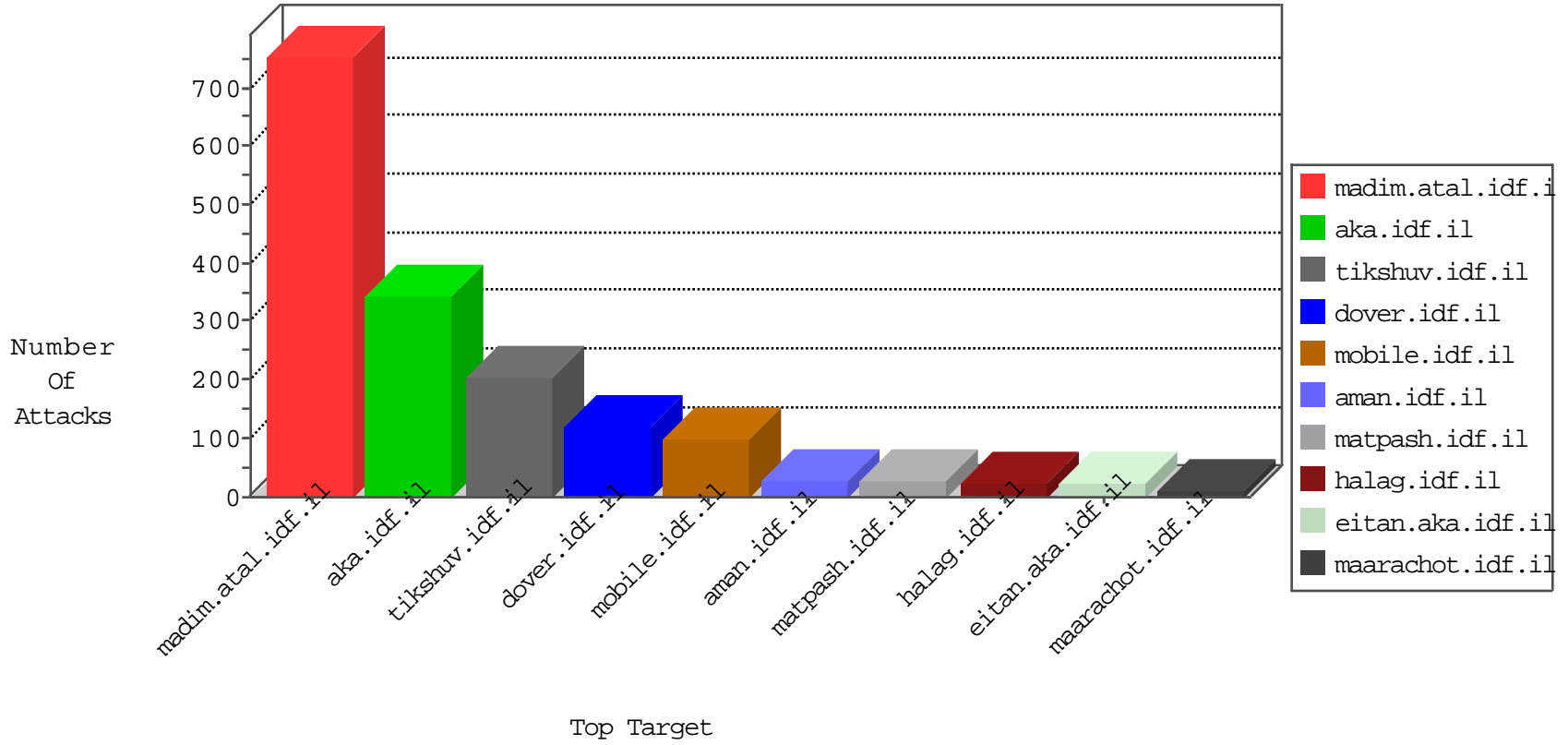


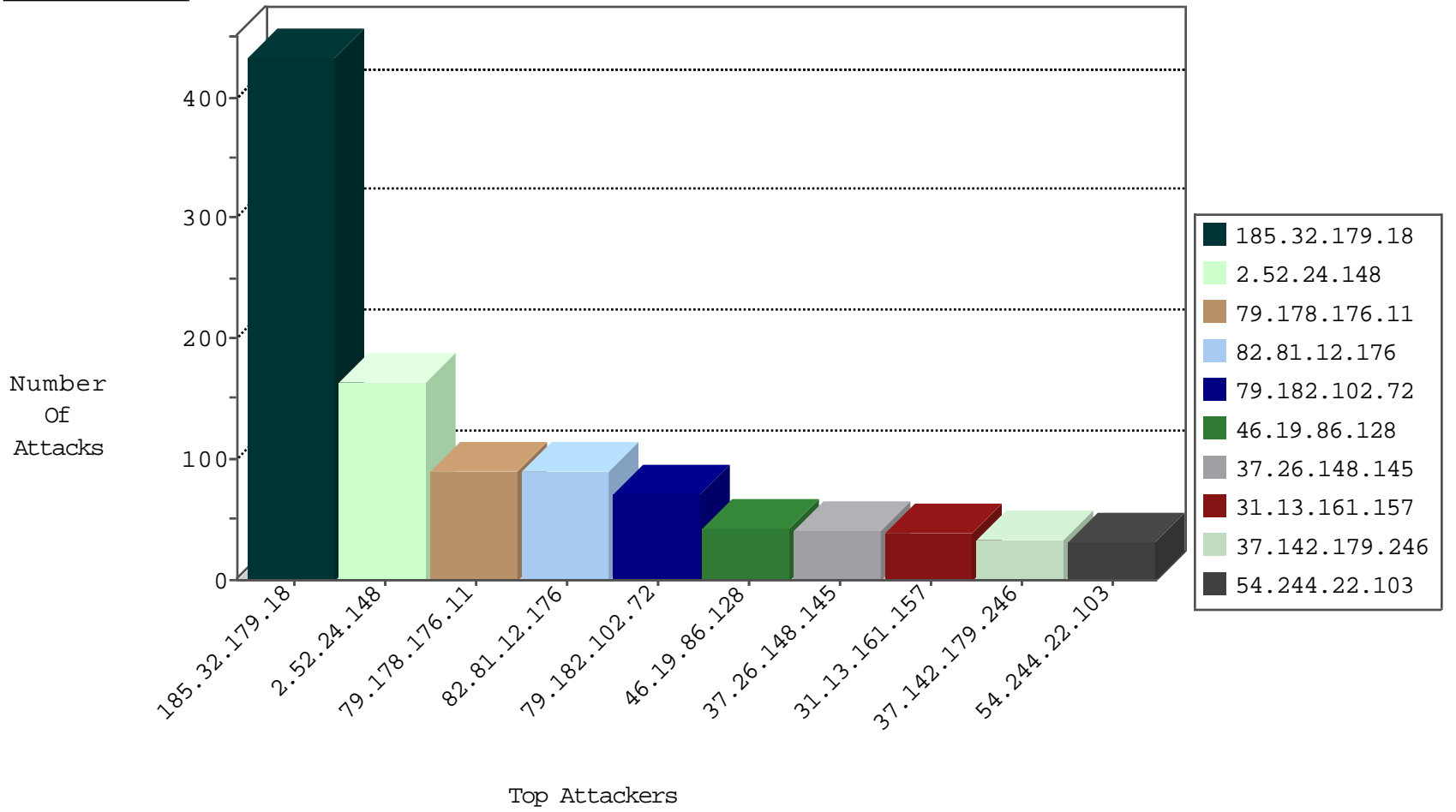
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	90
109.64.3.34	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2

01-30-2016-14:04:05 to 01-30-2016-15:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.63.195.10	Italy	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	12
185.32.179.18	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.93.189	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
46.148.22.26	147.237.77.216	Lithuania	dover.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.76.44	Lithuania	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.0.34	Lithuania	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
24.205.237.219	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.222.185.165	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
1.2.235.10	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.182.170.38	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
61.182.170.38	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
208.80.155.224	147.237.76.86	United States	navy.idf.il	Tehila - Perl LWP with fake user agent	1
61.182.170.38	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
182.254.149.138	147.237.76.198	China	e.yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.148.22.26	147.237.77.74	Lithuania	law.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.76.34	Lithuania	yochalan.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.34	United States	yochalan.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
2.54.177.231	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
61.182.170.38	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
61.182.170.38	147.237.76.34	China	yochalan.idf.il	ET SCAN Potential SSH Scan	1
208.80.155.224	147.237.72.166	United States	aka.idf.il	Tehila - Perl LWP with fake user agent	1
50.204.188.142	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.142.179.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	32
89.138.189.105	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
79.179.39.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.116.190.190	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
31.13.161.157	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	15
79.181.48.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
109.65.1.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
79.181.149.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.177.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
31.13.161.157	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
188.120.148.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.33	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
77.127.56.61	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
84.111.170.164	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
109.65.72.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.65.72.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.12.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.199.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.180.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
188.120.148.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.118	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
185.32.179.251	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
31.13.161.157	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.13.161.157	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.102.254.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.16.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.157.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
208.80.155.224	United States	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
85.65.139.157	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
31.154.35.244	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
65.55.210.185	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.177.14.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.45.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.164.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.145.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.213.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.180.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.236.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.177.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
31.13.161.157	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
31.210.186.255	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-30-2016-14:04:05 to 01-30-2016-15:04:05

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.214.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.57.116	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
185.32.179.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	221
185.32.179.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
185.32.179.18	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 185.32.179.18	Block	95
79.178.176.11	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.178.176.11	Block	91
2.52.24.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
2.52.24.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	74
79.182.102.72	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	71
46.19.86.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
37.26.148.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
80.246.136.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
87.69.127.143	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	12
87.69.127.143	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 87.69.127.143	Block	7
62.219.193.62	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 62.219.193.62	Block	7
80.246.137.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
5.22.134.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
93.173.55.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.167.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.4.206.38	Spain	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
176.13.5.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.97.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.134.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.94.33.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.181.48.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.28.132.84	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
46.116.63.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.181.149.231	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.66.181.73	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.66.181.73	Block	2
82.166.245.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.236.150	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	2
109.253.206.158	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
80.246.136.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.64.38.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.8.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.9.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.136.119	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.186.186.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.85.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.94.165.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.43.182	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	PHP Attempt	Block	1
157.55.39.113	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/page.asp	Block	1
66.249.79.108	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
87.68.74.85	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/http://websearch.searchere.info/	Block	1
46.116.81.112	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.34.63.20	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
37.26.149.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.10.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.152.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.202.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1