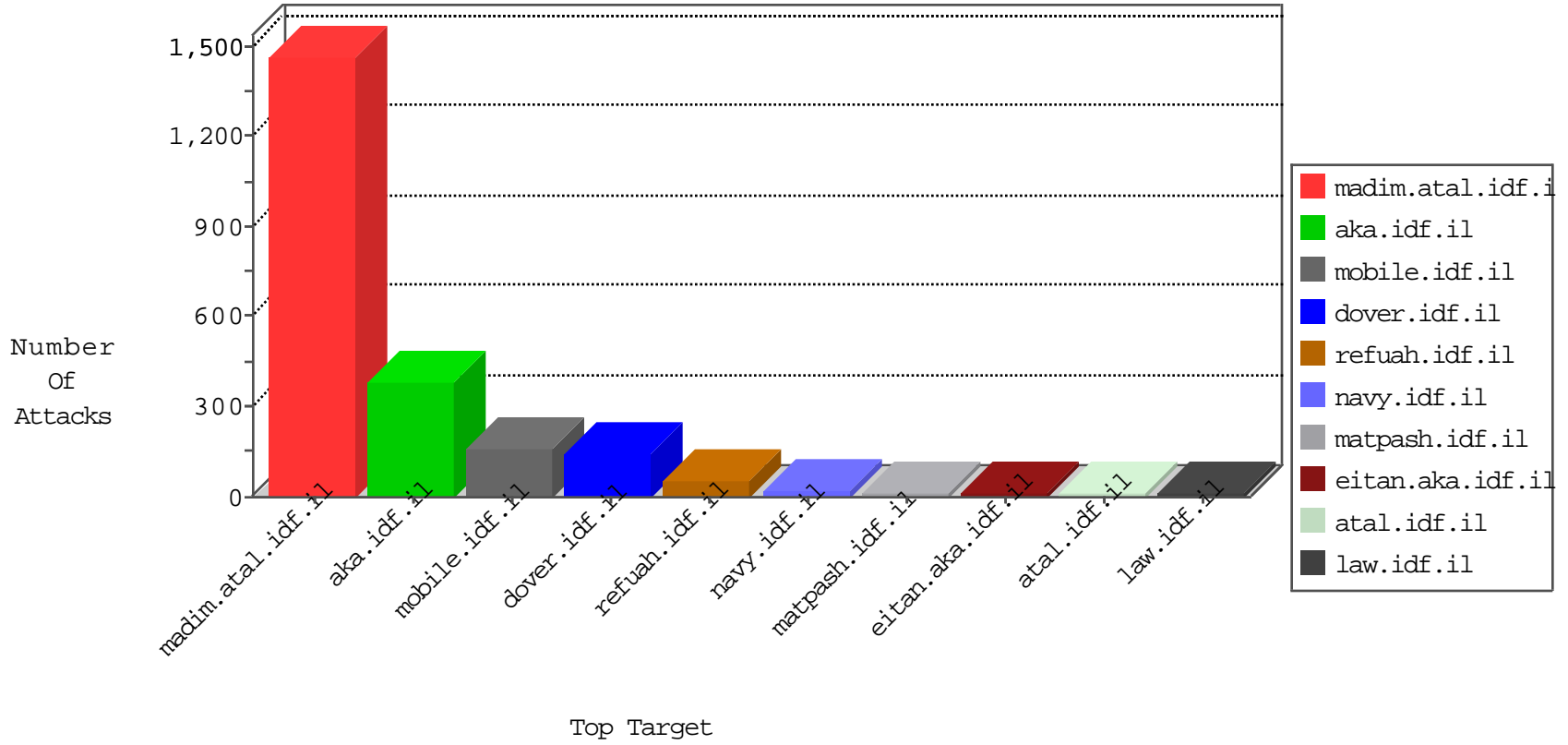


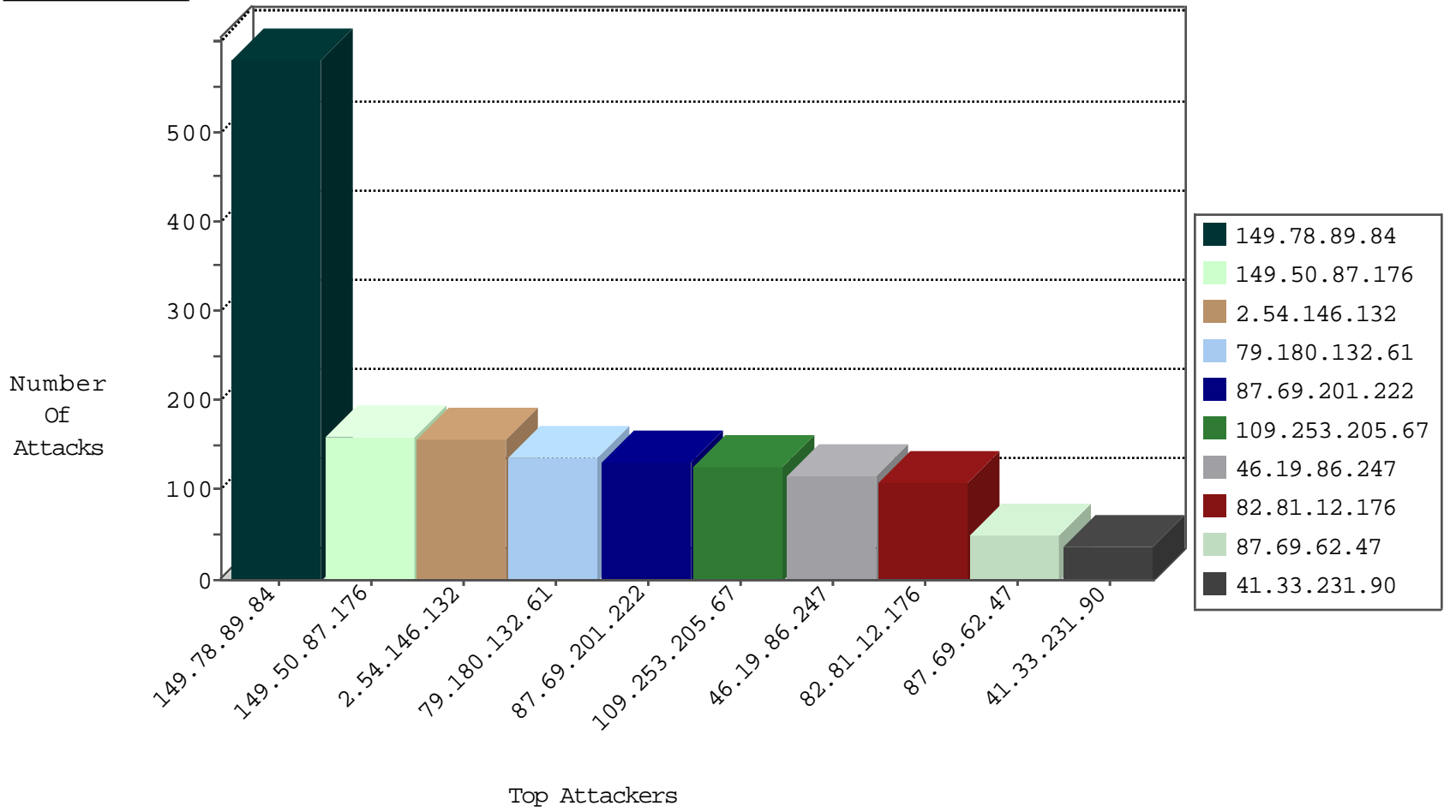
IDF Under Attack Daily Report



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	108
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.198	e.yohanan.idf.il	Block_Udp_All_Nets	drop	1
60.241.21.28	Australia	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

01-30-2016-22:04:05 to 01-30-2016-23:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.76.111.93	147.237.77.74	Israel	law.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.154	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
146.0.75.114	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
46.151.53.217	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
173.55.32.113	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.69.62.47	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
77.127.233.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.180.214.105	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
149.78.89.84	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
66.102.9.54	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	13
79.177.119.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.80.168.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.28.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
93.173.166.203	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.67.180.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.117.25.0	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.138.186.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.224.80	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
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.177.224.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.51.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.24.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.52.62	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
84.108.45.98	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.182.62.251	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
74.6.254.127	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.94.160.150	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.94.185.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.247.36.76	Netherlands	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
199.30.24.142	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.22.129.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
105.191.160.23	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.86.72	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
212.199.156.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.144.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.108.60.144	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.230.86.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
160.160.215.113		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.33.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.177.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.213.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.53.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
160.160.215.113		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3

01-30-2016-22:04:05 to 01-30-2016-23:04:05

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.136.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.38.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.89.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	356
149.78.89.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
149.50.87.176	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
149.78.89.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	105
87.69.201.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
46.19.86.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
79.180.132.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
109.253.205.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
2.54.146.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	80
2.54.146.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
149.50.87.176	United States	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	53
109.253.205.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	44
79.180.132.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
87.69.201.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	26
109.253.210.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
46.19.86.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
46.19.86.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
77.127.233.3	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
79.180.214.105	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
95.86.111.113	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.111.113	Block	5
149.78.202.211	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 149.78.202.211	Block	5
2.54.26.7	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	4
46.19.85.14	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.76.114.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.191.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.142.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.172.135.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.168.122	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.117.24.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.67.52.48	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	2
94.230.86.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
149.78.202.211	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	2
109.67.52.48	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	2
79.183.28.183	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
188.143.232.15	Russian Federation	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 188.143.232.15	Block	2
176.13.19.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
109.64.153.120	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	2
79.181.208.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.198.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
95.86.111.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewiilenvtnlkahulubgkxfuta p4qfggimaa&usg=afqjcnhcvyg7wlcq-yhd5_ammzoyodtwa	Block	2
84.229.82.186	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
46.117.25.0	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.181.229.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.190.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.233.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
185.120.126.14		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/62953.jpg	Block	1
85.95.254.137	Turkey	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1