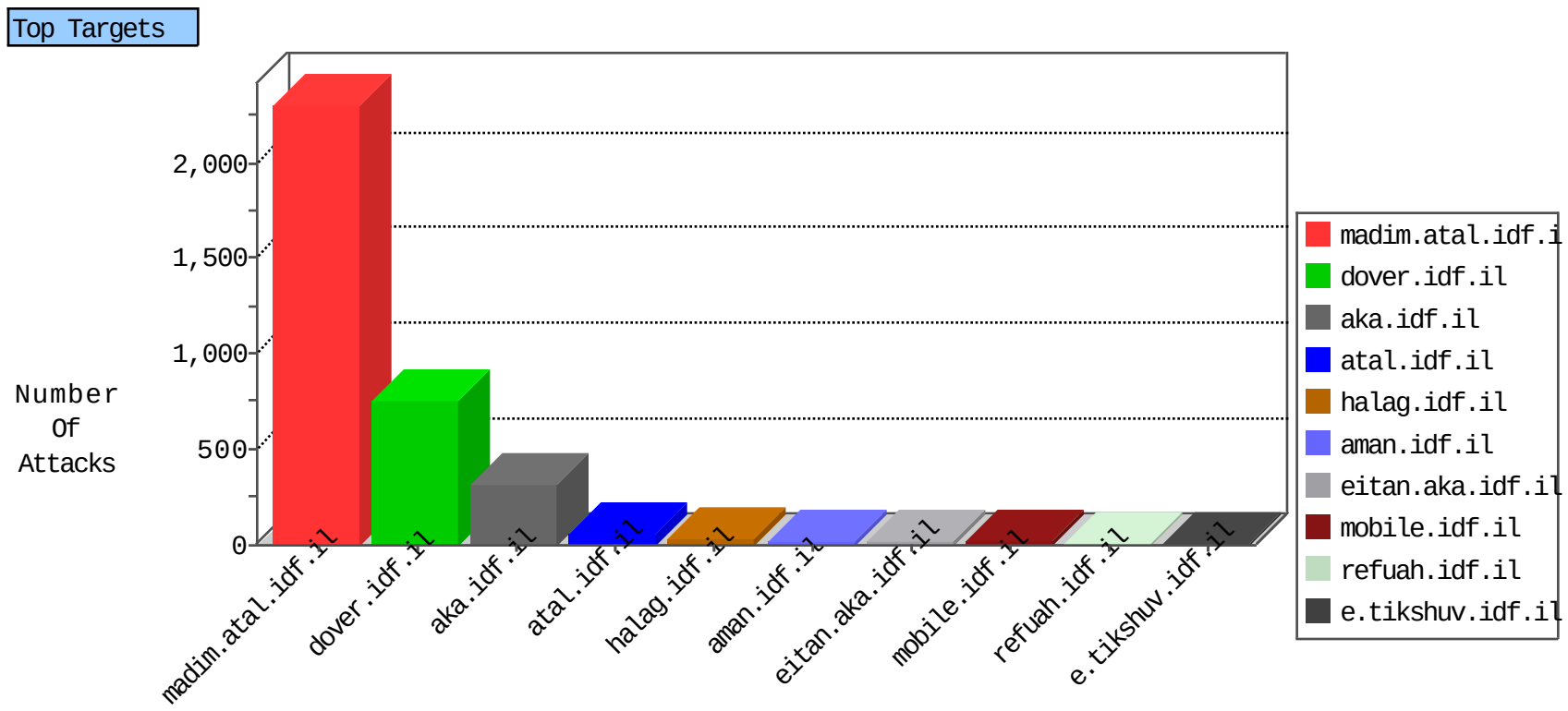
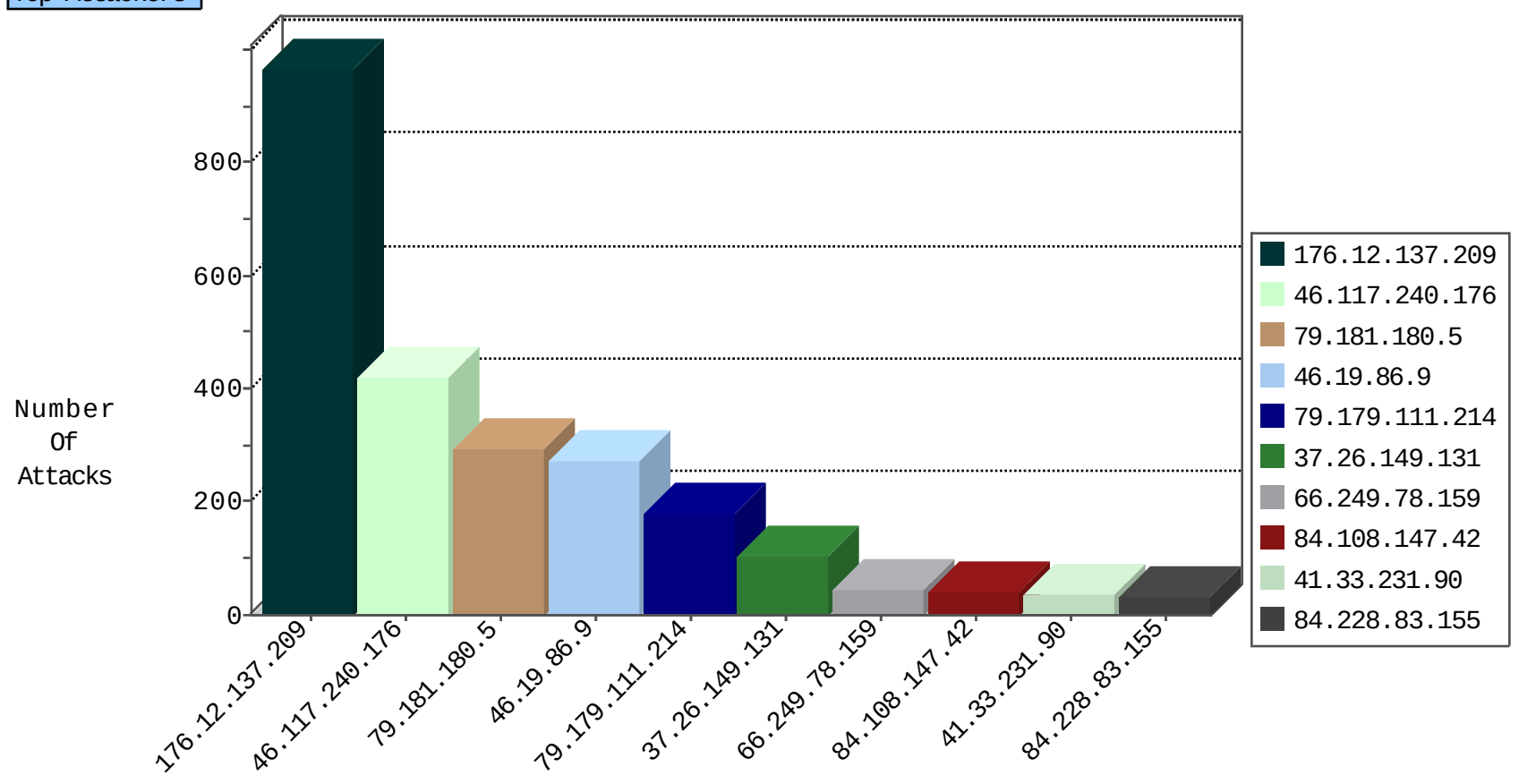
11-21-2015-16:04:04 to 11-21-2015-17:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-21-2015-16:04:04 to 11-21-2015-17:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	23
46.120.132.219	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
10.0.0.10		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
109.160.172.77	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
37.26.149.203	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
80.246.136.204	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
100.100.90.211		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
172.19.238.88		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
217.39.47.53	United Kingdom	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	3
146.185.56.190	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
66.240.192.138	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

11-21-2015-16:04:04 to 11-21-2015-17:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-21-2015-16:04:04 to 11-21-2015-17:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.12.137.209	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	17
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
31.6.71.154	147.237.0.35	Poland	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
176.106.226.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.222.185.165	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	147.237.77.226	Turkey	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
31.6.71.154	147.237.77.234	Poland	halag.idf.il	ET SCAN NMAP -sS window 1024	1
8.37.230.44	147.237.77.216	Anonymous Proxy	dover.idf.il	portscan: TCP Distributed Portscan	1
162.222.185.165	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
58.253.96.122	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
37.26.149.131	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1

11-21-2015-16:04:04 to 11-21-2015-17:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
84.108.147.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
37.142.181.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
192.116.172.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
84.228.83.155	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
46.117.240.176	Israel	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	23
100.100.100.211		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
185.4.252.172	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.249.83.109	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	19
100.100.90.211		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
2.54.21.223	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
131.253.25.224	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.146.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
81.34.222.158	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
81.34.222.158	Spain	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.86.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
73.132.74.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
109.67.153.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.176.178.178	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
100.100.38.208		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.9	Israel	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.9.211		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.9	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
94.159.177.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
8.37.230.44	Anonymous Proxy	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
79.181.191.158	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.146.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.179.111.214	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.54.21.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.177.101.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.125.114.0	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
87.68.44.83	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
217.194.72.98	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.149.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.179.119.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
87.234.40.88	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.181.191.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.178.114.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.9	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
82.166.165.185	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
192.116.142.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.255.253.158	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
82.166.165.185	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
66.249.83.158	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.137.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	693
46.117.240.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	271
176.12.137.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	245
79.181.180.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	186
46.19.86.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	144
46.117.240.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
79.181.180.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
79.179.111.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	104
46.19.86.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	102
79.179.111.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
37.26.149.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
37.26.149.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	39
2.54.28.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
176.12.137.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
2.54.155.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.117.240.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	5
8.37.230.44	Anonymous Proxy	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 8.37.230.44	Block	3
176.13.4.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.147.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.182.219.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
173.252.90.245	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
84.109.127.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.39.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.160.192.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.228.193.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.173.62.123	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
124.73.1.18	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1026-he/shared/usercontrols/headerupper/	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
85.64.99.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.162.161	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
77.127.89.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.161.167	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.110.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.159.226.81	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH)	None	1
66.249.64.200	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/	Block	1
84.109.113.104	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
8.37.230.44	Anonymous Proxy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shael, idfspokeperson	Block	1
132.66.236.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 68.180.228.175	Block	1
192.117.10.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.111.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1