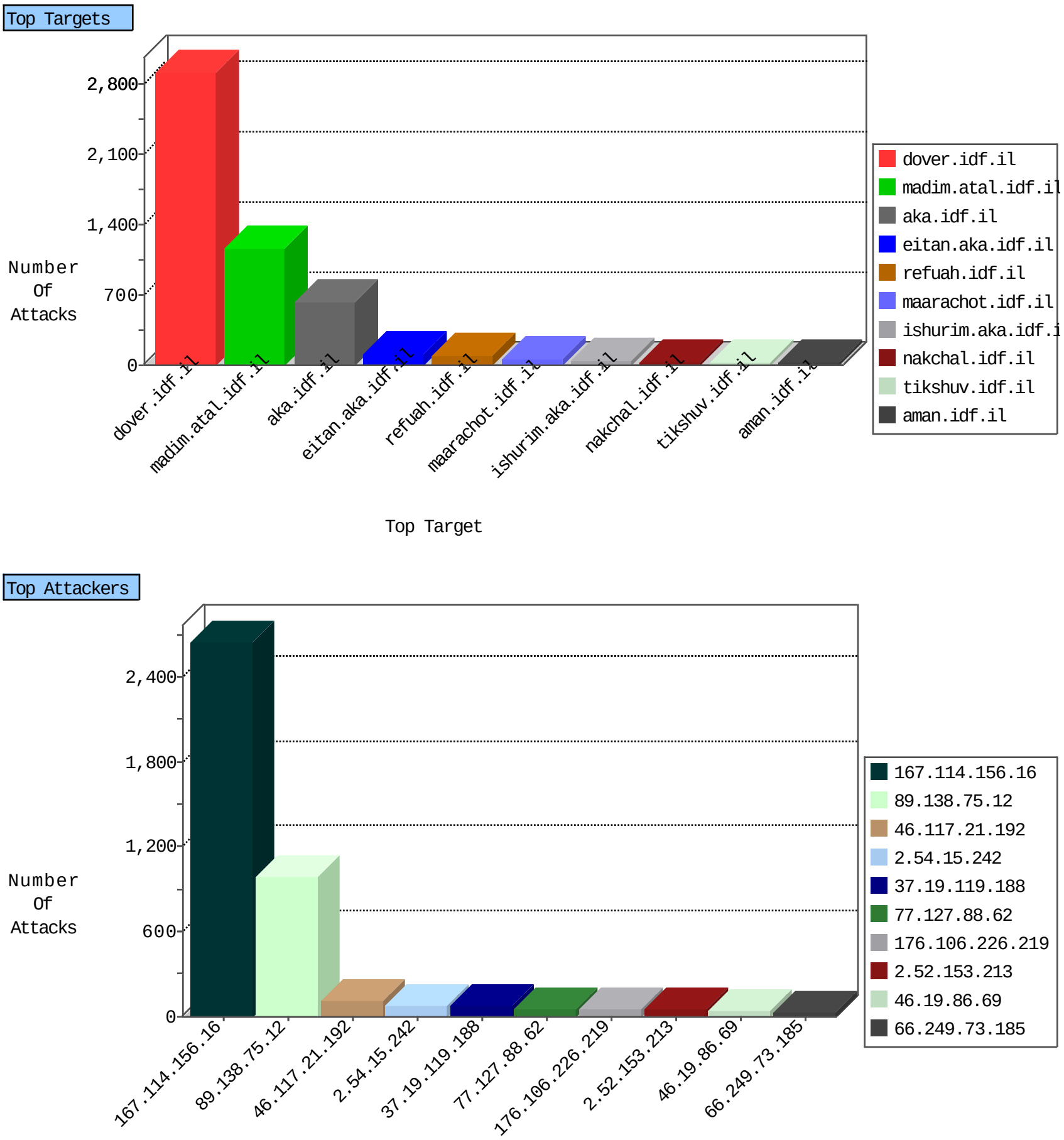
11-25-2015-22:04:05 to 11-25-2015-23:04:05

IDF Under Attack
Daily Report



11-25-2015-22:04:05 to 11-25-2015-23:04:05

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	3325
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
178.163.122.46	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
52.27.97.133	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
167.114.95.199	Canada	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
61.182.170.38	China	147.237.76.30	himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
61.182.170.38	China	147.237.76.177	ncore.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

11-25-2015-22:04:05 to 11-25-2015-23:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.146	Italy	147.237.72.167	ishurim.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-25-2015-22:04:05 to 11-25-2015-23:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
61.182.170.38	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
109.74.226.90	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Potential SSH Scan	1
61.182.170.38	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
109.74.226.90	147.237.77.121	Iran, Islamic Republic of	e.navy.idf.il	ET SCAN Potential SSH Scan	1
61.182.170.38	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
109.74.226.90	147.237.76.198	Iran, Islamic Republic of	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
109.74.226.90	147.237.76.39	Iran, Islamic Republic of	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
109.74.226.90	147.237.72.217	Iran, Islamic Republic of	e.idf.il	ET SCAN Potential SSH Scan	1
109.74.226.90	147.237.0.33	Iran, Islamic Republic of	idf.il	ET SCAN Potential SSH Scan	1
151.11.201.3	147.237.0.35	Italy	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
93.113.125.11	147.237.8.27	Romania	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
109.74.226.90	147.237.77.235	Iran, Islamic Republic of	sviva.idf.il	ET SCAN Potential SSH Scan	1
86.74.211.239	147.237.72.14	France	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
109.74.226.90	147.237.77.226	Iran, Islamic Republic of	www.chamatz.aka.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
109.74.226.90	147.237.77.178	Iran, Islamic Republic of	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
61.182.170.38	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
109.74.226.90	147.237.76.202	Iran, Islamic Republic of	e.halag.idf.il	ET SCAN Potential SSH Scan	1
109.74.226.90	147.237.76.86	Iran, Islamic Republic of	navy.idf.il	ET SCAN Potential SSH Scan	1
109.74.226.90	147.237.76.38	Iran, Islamic Republic of	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.76.39	United States	mobile.meitav.idf.il	ET DROP Dshield Block Listed Source	1
109.74.226.90	147.237.72.156	Iran, Islamic Republic of	aman.idf.il	ET SCAN Potential SSH Scan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
109.74.226.90	147.237.0.16	Iran, Islamic Republic of	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.74.226.90	147.237.77.243	Iran, Islamic Republic of	mobile.idf.il	ET SCAN Potential SSH Scan	1
92.52.188.198	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.74.226.90	147.237.77.227	Iran, Islamic Republic of	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1

11-25-2015-22:04:05 to 11-25-2015-23:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.19.119.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	72
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.86.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
176.106.226.219	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
176.106.226.219	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
213.57.130.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	26
46.19.85.31	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
100.100.55.208		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
100.100.108.53		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
100.100.68.69		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
2.52.153.213	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
100.100.45.140		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
46.19.86.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
100.100.91.162		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
46.117.21.192	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.102.140		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
66.249.73.201	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
93.173.169.90	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.232	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.52.16.237	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
212.117.140.158	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.232	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.52.153.213	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	9
213.57.130.70	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.85.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
213.57.130.70	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
37.26.149.170	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.54.144.146	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
188.161.9.100	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	8
46.19.85.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
2.52.153.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.232	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.189.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.153.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.105	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.73.193	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.15.242	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.189.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.246	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
100.100.56.200		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
79.181.124.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.146.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.153.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.116.208.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.146.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.110.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.146.230	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
185.3.146.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.75.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	480
89.138.75.12	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 89.138.75.12	Block	273
89.138.75.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	239
46.117.21.192	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	97
77.127.88.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
2.54.15.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
2.54.15.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
77.127.88.62	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.127.88.62	Block	4
2.54.173.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.197.151	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
2.54.24.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.17.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.133.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.176.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.21.194	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	3
80.246.137.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.114.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.80	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
46.19.85.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.2.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
93.173.150.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.116.120.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.228.19.224	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH)	None	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/miluim.jpg	Block	1
109.160.147.148	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
46.117.42.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.82.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.105.174	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
176.12.149.163	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 176.12.149.163	Block	1
46.19.86.6	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
67.215.4.73	Canada	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
149.88.109.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.68.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.215.116	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.138.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.235.8.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
54.183.117.152	United States	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/	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
185.3.146.244	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
46.116.208.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
93.219.7.180	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/german	Block	1
87.69.191.130	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pniasubmittedsuccessfully.aspx	None	1
157.55.39.169	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
5.22.134.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.43.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim.	Block	1
141.212.122.112	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Malformed URL proxytest.zmap.io:80	Block	1