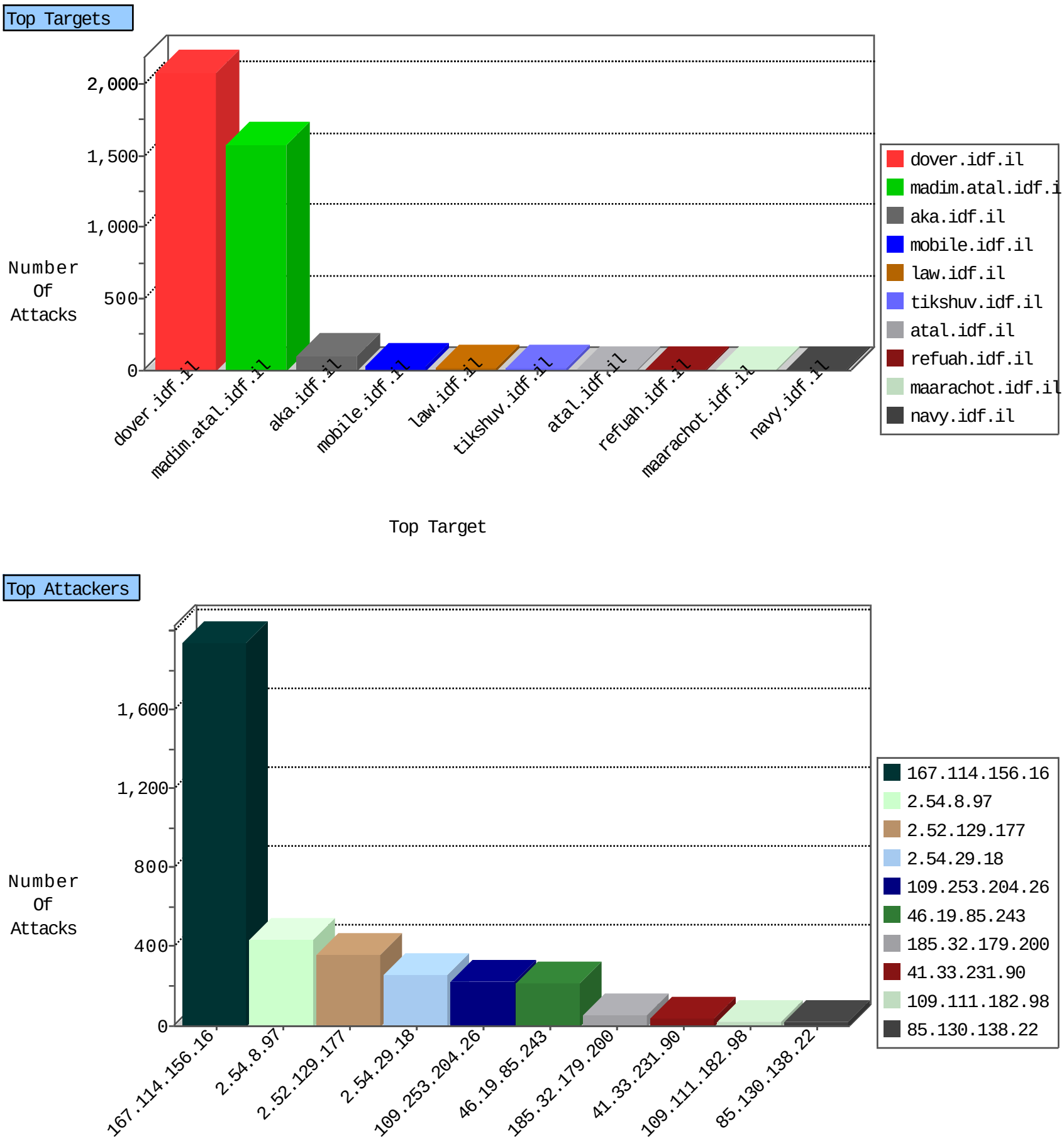
01-08-2016-08:04:00 to 01-08-2016-09:04:00

IDF Under Attack
Daily Report



01-08-2016-08:04:00 to 01-08-2016-09:04:00

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	3222
65.181.113.88	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.162	China	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
107.150.60.246	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1
180.97.106.162	China	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.228		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.162	China	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

01-08-2016-08:04:00 to 01-08-2016-09:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-08-2016-08:04:00 to 01-08-2016-09:04:00

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
109.111.182.98	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN Potential SSH Scan	3
109.111.182.98	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Potential SSH Scan	2
109.111.182.98	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.73.214	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
208.100.26.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
109.111.182.98	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential SSH Scan	1
187.160.18.148	147.237.76.198	Mexico	e.yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.111.182.98	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
183.60.252.84	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
109.111.182.98	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
109.111.182.98	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN Potential SSH Scan	1
109.111.182.98	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
109.111.182.98	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN Potential SSH Scan	1
109.65.190.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.111.182.98	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
1.93.129.5	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
109.111.182.98	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
1.93.129.5	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
109.111.182.98	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN Potential SSH Scan	1
217.12.39.85	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN NMAP -sS window 1024	1
109.111.182.98	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
109.111.182.98	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
187.160.18.148	147.237.76.176	Mexico	test.ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.252.84	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
109.111.182.98	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN Potential SSH Scan	1
109.111.182.98	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN Potential SSH Scan	1
109.67.52.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.111.182.98	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential SSH Scan	1
1.93.129.5	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
109.111.182.98	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN Potential SSH Scan	1
1.93.129.5	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1

01-08-2016-08:04:00 to 01-08-2016-09:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
72.9.148.10	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
72.9.148.10	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
37.26.148.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
49.199.22.146	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.167.8	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.37.11	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
49.199.22.146	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.64.146.246	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.102.254.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.212.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.102.254.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.250.77.153	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.219.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.168.51.250	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.225	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.168.200.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
172.56.38.226	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.197	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.102.221.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
208.100.26.233	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
62.219.235.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.11.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.65.172.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.251	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence		monitor	3
185.27.105.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.145.95.42	United Kingdom	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.246.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
208.100.26.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.54.8.97	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
134.159.176.242	Australia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.225	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
176.13.11.225	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
193.33.2.114	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
49.199.22.146	Australia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
64.233.172.206	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
176.13.11.225	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.131.31	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.252	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.147.251	Israel	147.237.77.243	mobile.idf.il	SYN Attack		reject	2
49.199.22.146	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.86.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.38.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
72.9.148.10	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.129.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.8.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	243
2.52.129.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	233
2.54.29.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	142
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	130
2.52.129.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	125
109.253.204.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	119
109.253.204.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
2.54.8.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
2.54.29.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	96
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	87
2.54.8.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	85
185.32.179.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
85.130.138.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
2.54.29.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	17
79.178.3.127	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.178.3.127	Block	11
2.52.129.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	7
109.253.219.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.19.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.104.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
40.77.167.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
85.250.77.153	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	3
109.253.212.219	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.250.77.153	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 85.250.77.153	Block	2
62.90.184.163	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl17 in www.aka.idf.il/main/sachar/payslips.aspx	None	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/international_training	Block	1
2.52.8.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.65.34.177	Moldova, Republic of	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /	Block	1
37.26.146.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
216.189.152.170	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp>israeli	Block	1
79.178.216.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcdhphdmltxdewmtguzg9j&infocenteritem=true	Block	1
162.247.73.206	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.230.230.230	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
40.77.167.95	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chinuch/miktzoa/default.asp	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation docId in tikshuv.idf.il/site/story.aspx	Block	1
84.111.196.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
69.171.228.117	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.219.37	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
95.86.93.53	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
37.26.147.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
216.218.206.68	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
194.187.168.208	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.181.212.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.0.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
40.77.167.95	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/giyus/qanda/default.asp	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
74.82.47.3	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1