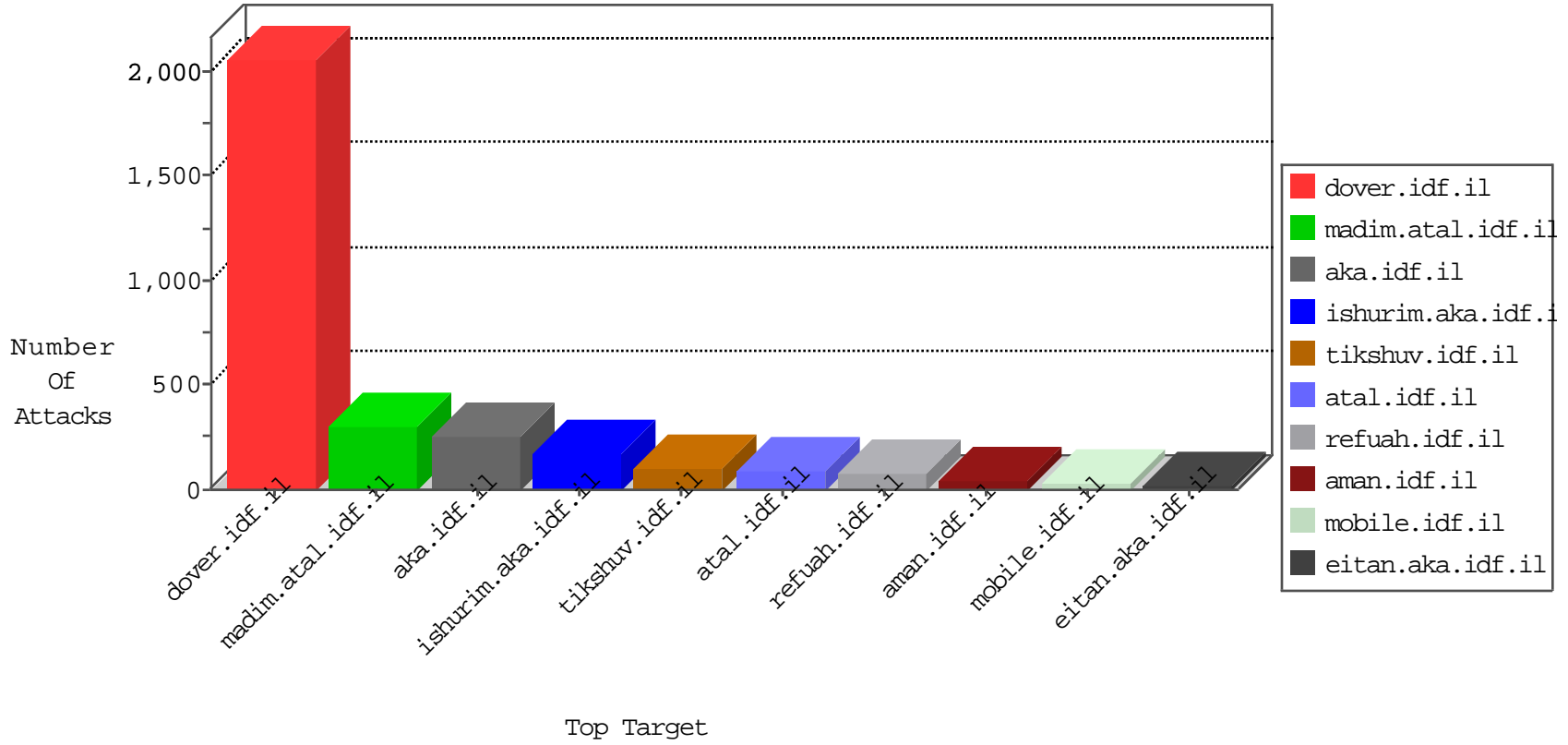


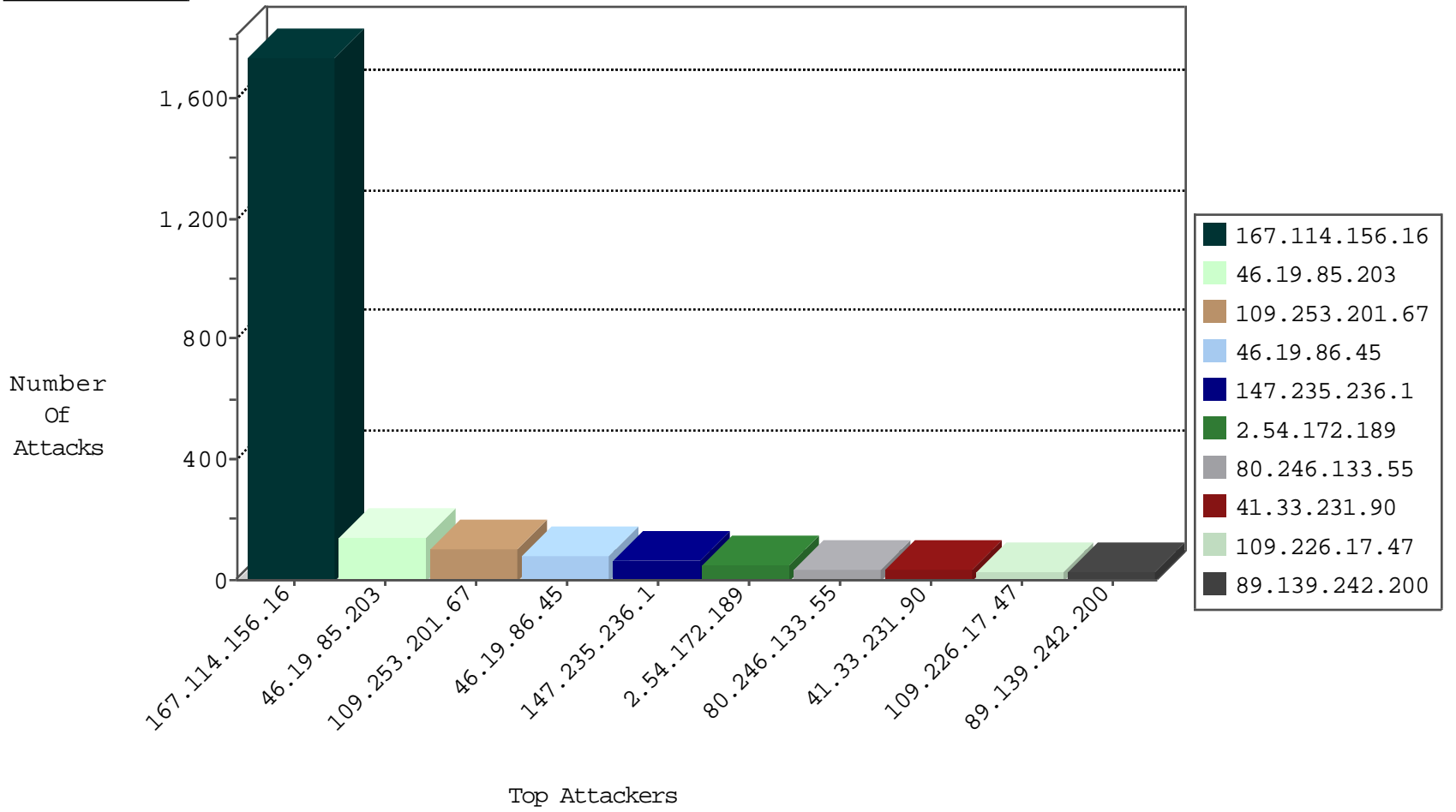
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3039
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	318
147.235.236.1	Israel	147.237.77.233	atal.idf.il	JIM_Purple_Con_Limit_Http	drop	73
147.235.236.1	Israel	147.237.77.233	atal.idf.il	JIM_Purple_Con_Limit_Tcp	drop	23
173.208.136.170	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	3
132.64.31.253	Israel	147.237.77.170	maarachot.idf.il	HTTP-MISC-MS-Windows-HTTP-DOS	dest-reset	3
173.208.136.170	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	2
198.20.70.114	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.199	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
52.53.222.9	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
203.135.142.130	Hong Kong	147.237.8.50	e.tikshuv.idf.il	I4 Source or Dest Port Zero	drop	1
141.212.122.206	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.60	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

01-07-2016-09:04:04 to 01-07-2016-10:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.74	United States	147.237.8.46	e.chinuch.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

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	2
173.199.74.136	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.166.27.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.12.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.18.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.199.74.136	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.59.33.61	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.53.196	147.237.0.33	Ukraine	idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.29.193.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.104.41.54	147.237.76.86	Moldova, Republic of	navy.idf.il	ET SCAN Potential SSH Scan	1
176.13.17.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.199.74.136	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.203	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	142
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
80.246.133.55	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
147.235.236.1	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	33
89.139.242.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.85.187	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
185.89.217.227		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
147.235.236.1	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
212.143.225.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.44.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.89.217.225		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
84.108.236.183	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
217.194.197.98	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.235.124.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
80.246.133.145	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
58.38.250.61	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
80.246.140.105	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
79.178.144.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
80.246.140.105	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
80.246.140.105	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
62.0.251.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.233		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
2.54.165.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.133.30	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.77.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.229	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
37.46.39.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.89.217.226		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.144.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.89.217.232		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
70.211.143.99	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.159	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
2.52.2.135	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
217.194.207.24	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
70.211.143.99	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	5
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.29.243.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.201.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
46.19.86.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
2.54.172.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
109.226.17.47	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.226.17.47	Block	27
46.19.85.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
109.253.201.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
109.253.147.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
46.120.62.127	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	4
46.19.86.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
85.65.62.68	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.62.68	Block	3
176.13.23.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.65.62.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/	Block	3
46.19.85.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.242	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
80.246.137.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.219.174.67	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	2
80.246.136.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
81.218.151.163	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/4/2094.jpg	Block	2
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	2
2.54.58.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
81.218.161.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.16.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
176.13.19.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.128.133	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.54.181.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.0.171	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.0.171	None	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
46.19.85.6	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	1
66.249.78.9	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.9	Block	1
213.8.204.28	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
2.54.131.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.137.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
46.121.14.67	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main.sachar	Block	1
46.19.85.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.120.110	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.36.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	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
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/gyus/general.aspx	Block	1
207.46.13.21	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/out.asp	Block	1
2.54.184.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.166.27.134	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct109 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
2.54.7.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.8.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1