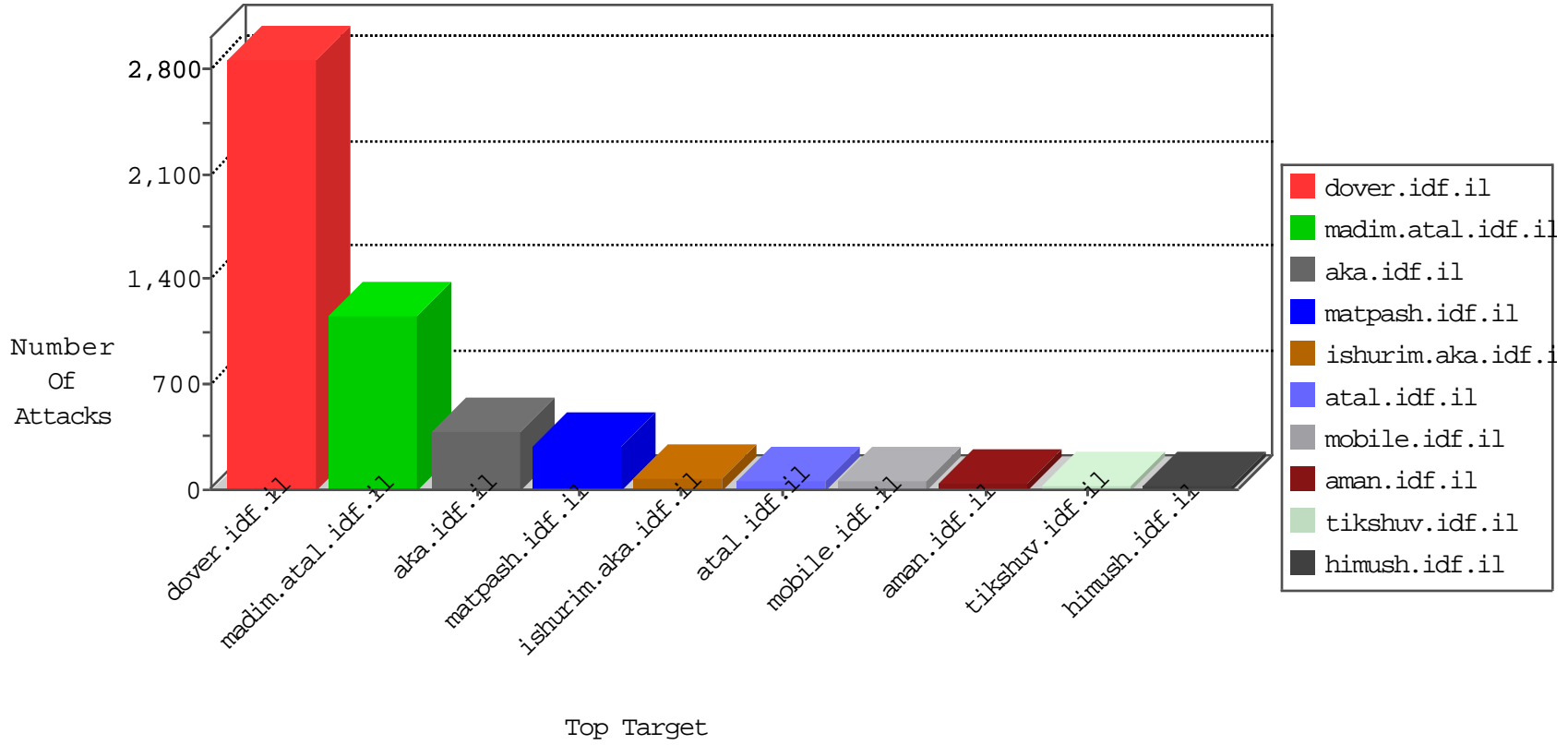


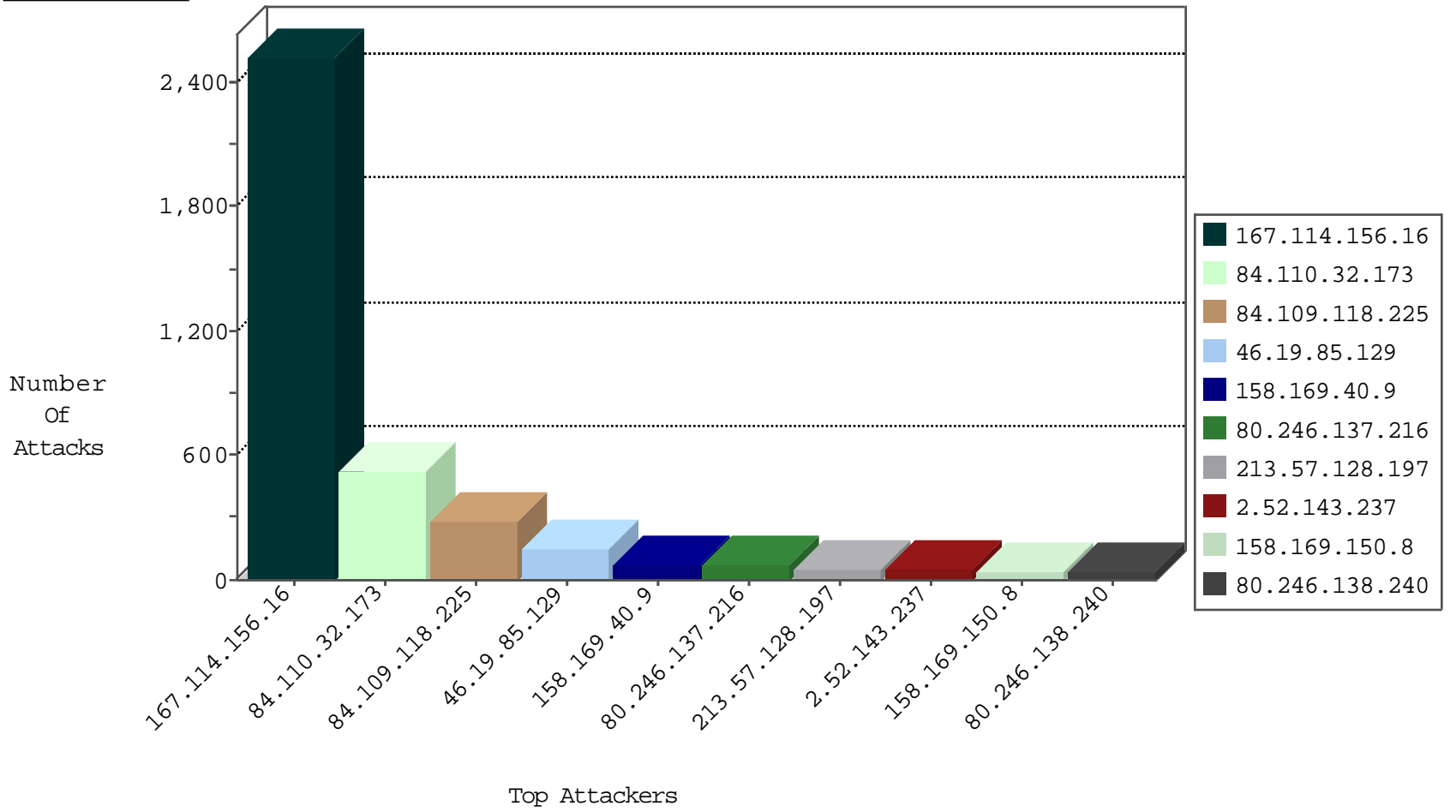
IDF Under Attack Daily Report



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	3311
84.110.32.173	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	534
66.249.64.190	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	107
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
203.238.52.170	Korea, Republic of	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.72.167	ishurim.aka.idf.il	block-sp-trafl	drop	1

12-10-2015-15:04:08 to 12-10-2015-16:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.52.7.119	147.237.72.167	Israel	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	12
217.77.220.195	147.237.77.216	Ukraine	dover.idf.il	Tehila - Perl LWP with fake user agent	4
77.126.66.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.76.200	United States	eitan.aka.idf.il	ET DROP Dshield Block Listed Source	1
128.30.52.96	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
79.178.12.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.55	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
218.108.132.58	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
212.235.60.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
91.201.236.113	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
158.169.40.9	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	73
213.57.128.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	55
2.52.143.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
158.169.150.8	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
80.246.130.10	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
62.207.60.231	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	32
158.169.150.10	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	29
80.179.9.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
176.12.151.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
100.100.17.80		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
158.169.40.7	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	24
37.140.141.31	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	22
80.179.9.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.86.121	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
212.235.67.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.19	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
37.26.147.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
82.102.169.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
100.100.17.80		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
2.52.7.119	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	9
2.54.155.15	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.109	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
148.177.129.212	Europe	147.237.72.166	aka.idf.il	drop	SAM rule	drop	9
158.169.150.5	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
79.183.239.81	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
137.95.1.11	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
213.229.101.119	United Kingdom	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.238	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
158.169.40.6	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.19	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.109.160.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.19	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
158.169.40.10	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
109.64.101.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.129.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.23.64	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.86.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.186.190.253	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
149.78.85.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.7.119	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.239.81	Israel	147.237.76.30	himush.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.16.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.243	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.64	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
180.191.79.221	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.110.32.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	237
84.109.118.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	203
84.110.32.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
84.110.32.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	122
46.19.85.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
80.246.137.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
84.109.118.225	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 84.109.118.225	Block	41
84.109.118.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
80.246.138.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
46.19.85.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	33
80.246.136.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
80.246.136.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
217.77.220.195	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	8
80.246.137.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
80.246.137.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
80.246.137.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
149.88.80.245	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
217.77.220.195	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 217.77.220.195	Block	4
80.246.137.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.109.132.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.39.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.41.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
217.77.220.195	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/zboard.php	Block	3
176.12.151.101	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	3
109.67.8.223	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 109.67.8.223	Block	3
46.19.85.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.22.185	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
213.8.204.38	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatenakatgauntity.aspx	Block	2
93.13.181.194	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.13.181.194	Block	2
180.191.79.221	Philippines	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 180.191.79.221	Block	2
2.54.37.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.79.25	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
84.109.160.248	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.182.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.69.119.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.173.149.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.179.177.148	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
46.19.85.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.137.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
92.211.0.222	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	2
79.181.173.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1133-he/dover.aspx	Block	2
46.116.116.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.8.223	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/7/size338x0/1877.jpg	Block	1
80.246.137.173	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
192.114.23.208	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
37.142.64.73	Israel	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	1
108.35.32.9	United States	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$ct100\$cphMain\$contentMainArea\$contentDetailsArea\$ctlFactoryMananagerDetails\$ctlMobilePhone2\$txtPh in www.aka.idf.il/homas/site/homasformphase2.aspx	None	1