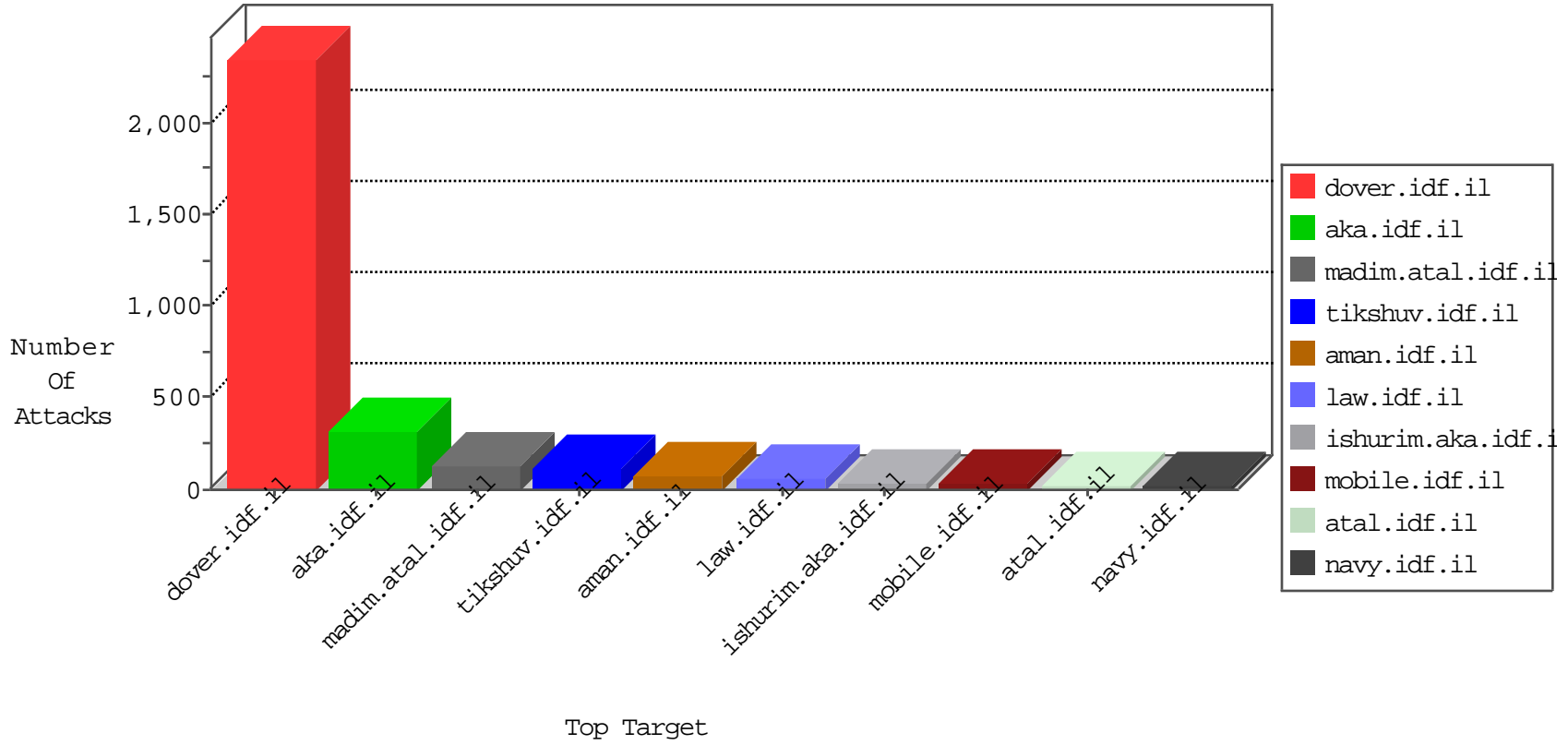


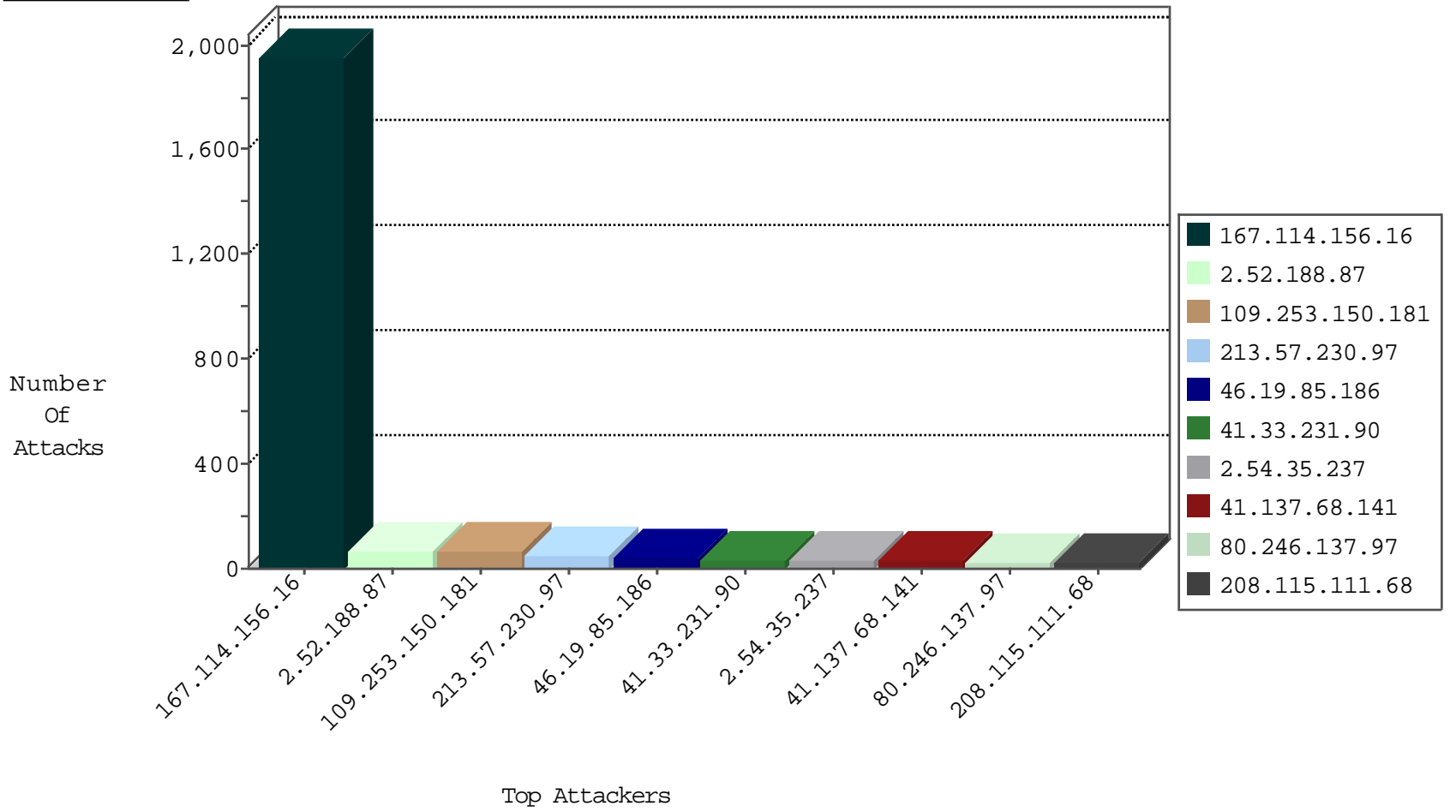
IDF Under Attack Daily Report



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	3001
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	16
82.145.218.194	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
93.174.93.218	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	2
146.185.239.100	Russian Federation	147.237.0.19	madim.atal.idf.il	block-sp-traf1	drop	1
218.103.243.231	Hong Kong	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

01-20-2016-17:04:00 to 01-20-2016-18:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.161.149	Israel	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.81.133	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
125.208.14.181	147.237.72.14	China	dover.idf.il(olc	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.3	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
212.179.245.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.29	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
125.208.14.181	147.237.72.166	China	aka.idf.il	portscan: TCP Distributed Portscan	1
121.201.27.61	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
89.163.145.107	147.237.77.216	Germany	dover.idf.il	ET SCAN Potential SSH Scan	1
66.249.81.218	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
173.163.191.105	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1

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	30
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	25
41.137.68.141	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	24
46.19.85.117	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
212.21.66.6	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
207.195.249.187	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	15
2.52.188.87	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
2.54.47.65	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
109.65.161.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.113	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
185.120.126.122		147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
80.246.136.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.188.87	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.52.188.87	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.52.188.87	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.188.87	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
2.54.170.76	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.35.237	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
109.67.6.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.60.59	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.35.237	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
94.188.248.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.6.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.65.138.89	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.113	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.35.237	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
169.139.224.98	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.75	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.94.56.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
94.188.248.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.250.236.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.35.237	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.6.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.95.214.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.56	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.250.236.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.35.237	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.113	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.22.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.148.150	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.182.148.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.187.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.182.167.164	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
37.46.39.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.22.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.137.68.141	Morocco	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.150.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
213.57.230.97	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 213.57.230.97	Block	48
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
80.246.137.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
81.218.17.4	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	7
176.13.2.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.139.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.67.150.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
95.86.81.97	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
162.243.3.218	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 162.243.3.218	Block	2
93.174.93.218	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Multiple Illegal Byte Code Character in Method from 93.174.93.218	Block	2
195.154.146.225	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
149.78.44.149	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
93.174.93.218	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Multiple NULL Character in Method from 93.174.93.218	Block	2
50.62.161.96	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
46.19.86.79	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	2
173.163.191.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	2
109.65.39.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/gyus/general.aspx	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
31.168.100.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.146	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
5.29.227.158	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
79.182.114.63	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https://www.aman.idf.il/	Block	1
109.160.253.22	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
50.62.161.96	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.mag.idf.il/xmlrpc.php	Block	1
93.174.93.218	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in Method	Block	1
213.151.43.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.178.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.118.87	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
46.19.86.120	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 46.19.86.120 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
84.108.248.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.116.158.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.68.72	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
81.218.207.58	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on www.nakchal.idf.il/xmlrpc.php	Block	1
173.252.74.121	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
75.65.0.252	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
109.65.186.57	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
5.102.254.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/shared/usercontrols/headerupper/	Block	1
109.253.221.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyus/asp/gyus.asp	Block	1
46.117.13.90	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
85.250.18.0	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.148	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
5.29.137.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.176.144	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
109.160.253.22	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1