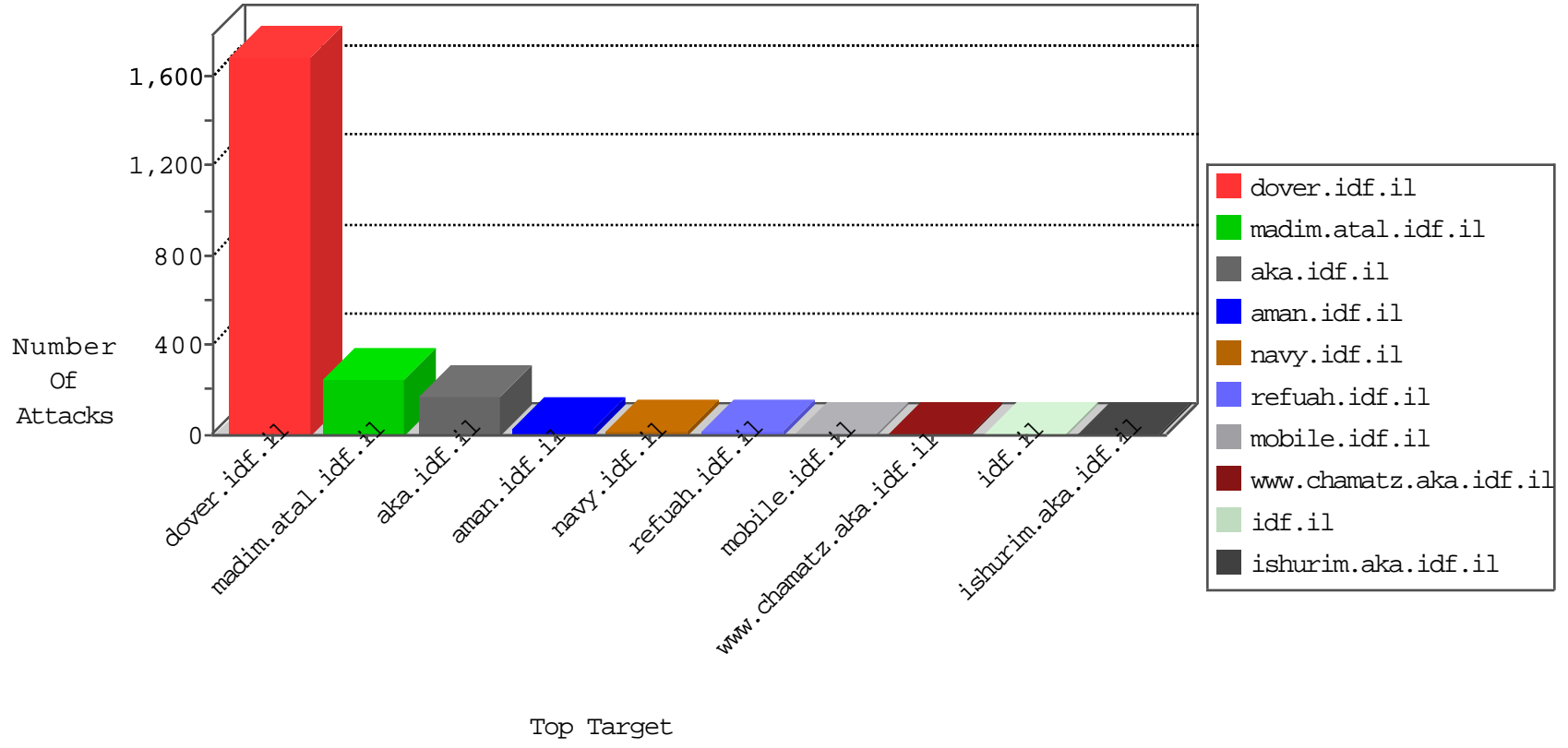


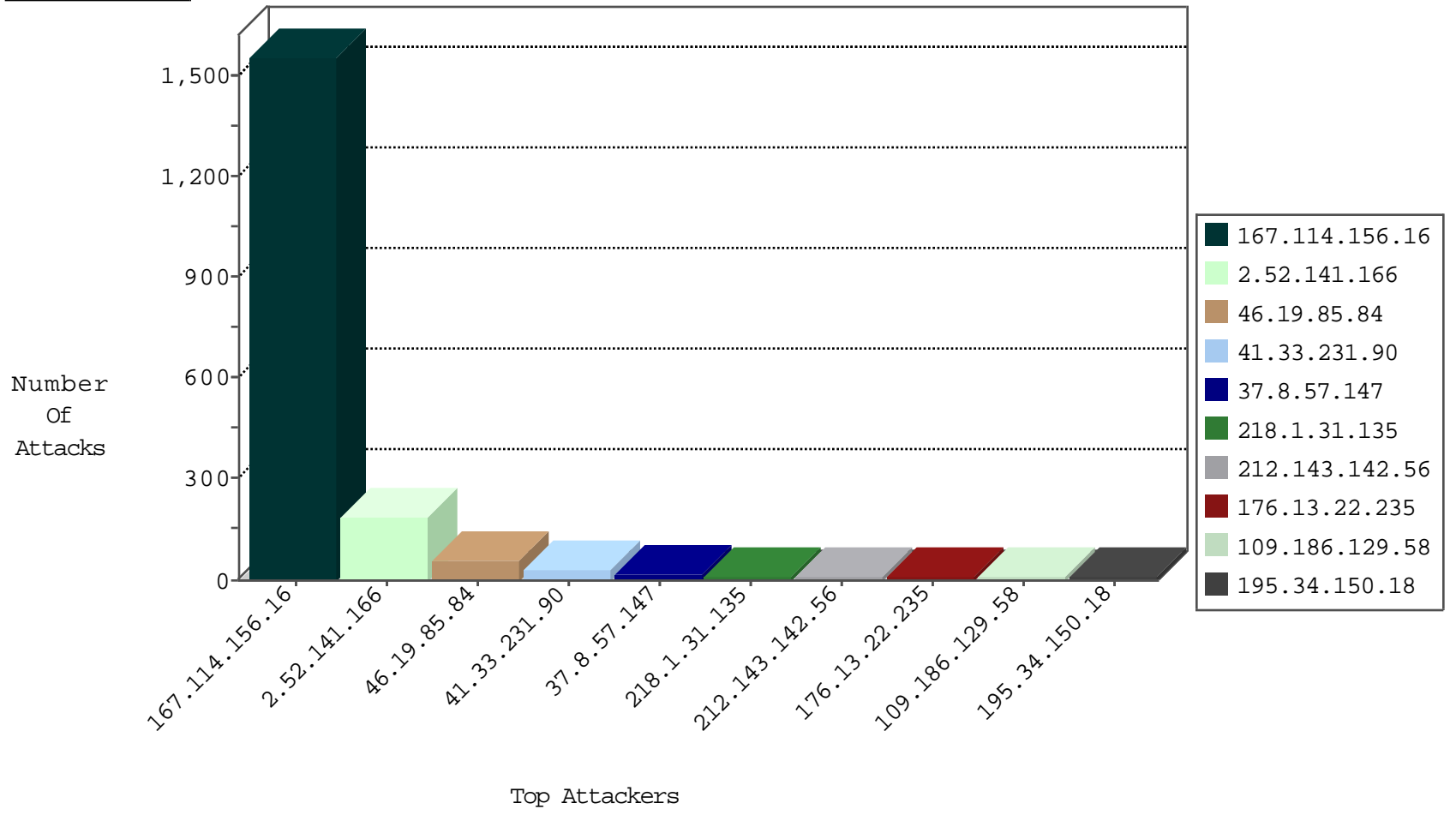
IDF Under Attack Daily Report



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	3140

12-23-2015-22:04:05 to 12-23-2015-23:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.33	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.123	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
218.1.31.135	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
218.1.31.135	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
218.1.31.135	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
218.1.31.135	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
218.1.31.135	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
218.1.31.135	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
86.0.136.197	147.237.0.33	United Kingdom	idf.il	ET SCAN NMAP -sS window 3072	1
218.1.31.135	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
218.1.31.135	147.237.76.198	China	e.yochalan.idf.il	ET SCAN Potential SSH Scan	1
218.1.31.135	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
218.1.31.135	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
218.1.31.135	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
218.1.31.135	147.237.76.34	China	yochalan.idf.il	ET SCAN Potential SSH Scan	1
86.0.136.197	147.237.0.33	United Kingdom	idf.il	ET SCAN NMAP -sS window 1024	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	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.22.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.8.57.147	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.165.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.17.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.186.129.58	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.8.57.147	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	5
213.57.136.246	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.246	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.125.120.128	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	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
37.46.39.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.34.164.200	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.8.57.147	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.46.39.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.186.129.58	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
84.108.56.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.127.215.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.167.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.228.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
62.219.35.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.255	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.182.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.228.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.120.125.63		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.110.26	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.130.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.65.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.157.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.111.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.111.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.0.81.57	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
84.94.80.218	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.64.54.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.198.61	Israel	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.86.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.24.76.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.102.254.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.20.219.76	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.56.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
149.88.40.14	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.141.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
2.52.141.166	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.141.166	Block	64
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
2.52.141.166	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.52.141.166	Block	16
77.125.12.62	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.125.12.62	Block	8
176.12.147.58	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master\$Header1\$ucHeaderSearch\$txtSearch in www.law.idf.il/564-he/patzar.aspx	Block	2
149.88.242.140	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 149.88.242.140 (Unknown SSL Session)	None	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
84.94.209.94	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	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
37.26.146.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
164.138.120.213	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
149.78.12.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
91.196.50.33	Poland	147.237.76.42	refuah.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
50.87.161.155	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
208.90.57.196	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
80.246.137.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.25.151.159	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
2.54.136.112	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.120.115	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.199.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.186	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
46.252.205.134	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
197.221.2.12	South Africa	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
85.250.244.76	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.179.130.114	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
5.29.156.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
2.52.54.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.88.94.109	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
94.185.83.100	Sweden	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on testp4.pospr.waw.pl/testproxy.php	Block	1
50.87.161.155	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
82.80.181.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.35.62.11	Switzerland	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
2.54.138.87	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
173.254.28.70	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
77.125.14.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
109.66.70.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.252.205.134	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
197.221.2.12	South Africa	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
87.68.62.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.180.18.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
8.37.70.123	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1273-he/navy.aspx&usg=alkjrhioblqmhtjo0_-qlh0rxb4a6vutpa	Block	1
176.13.2.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/	Block	1
94.185.83.100	Sweden	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1