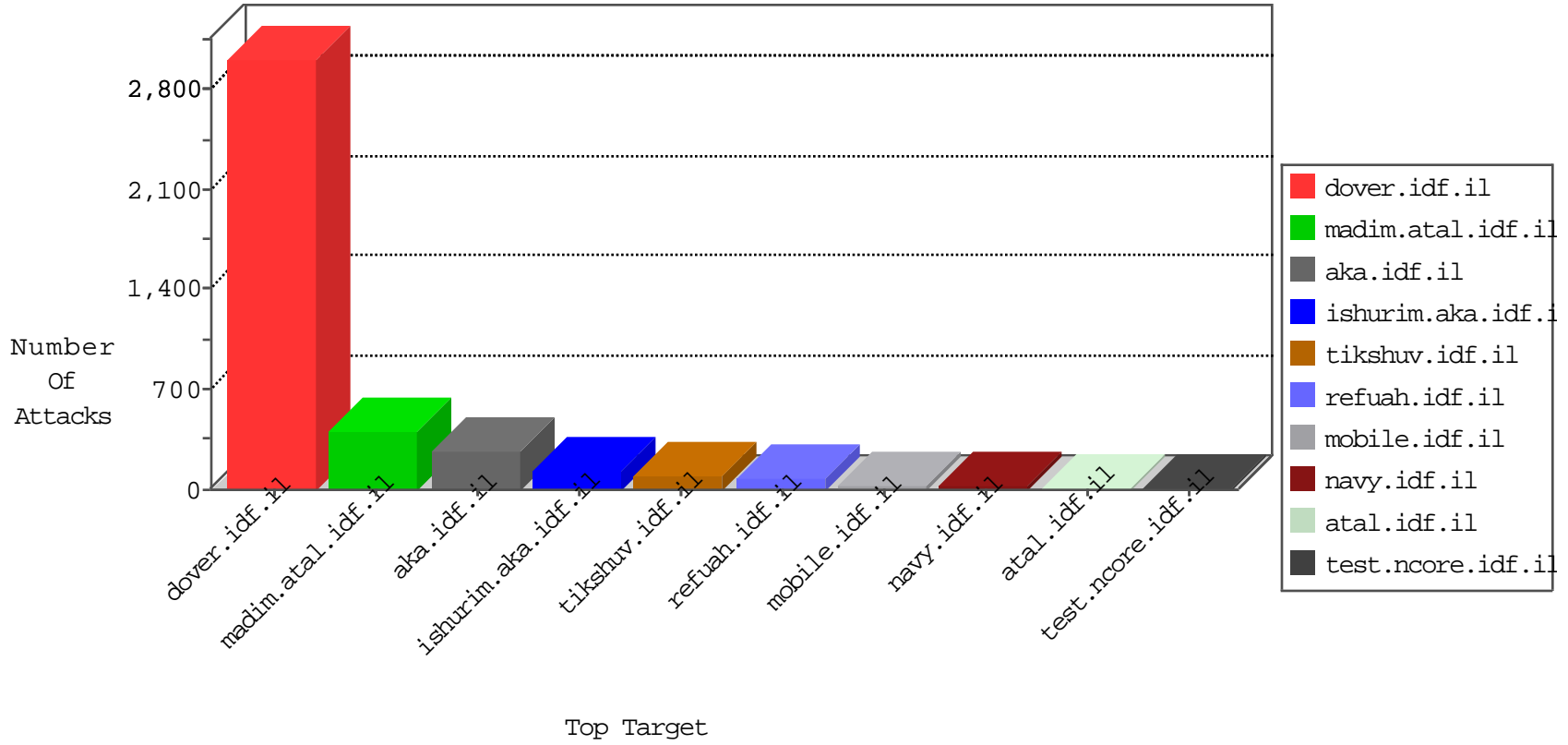


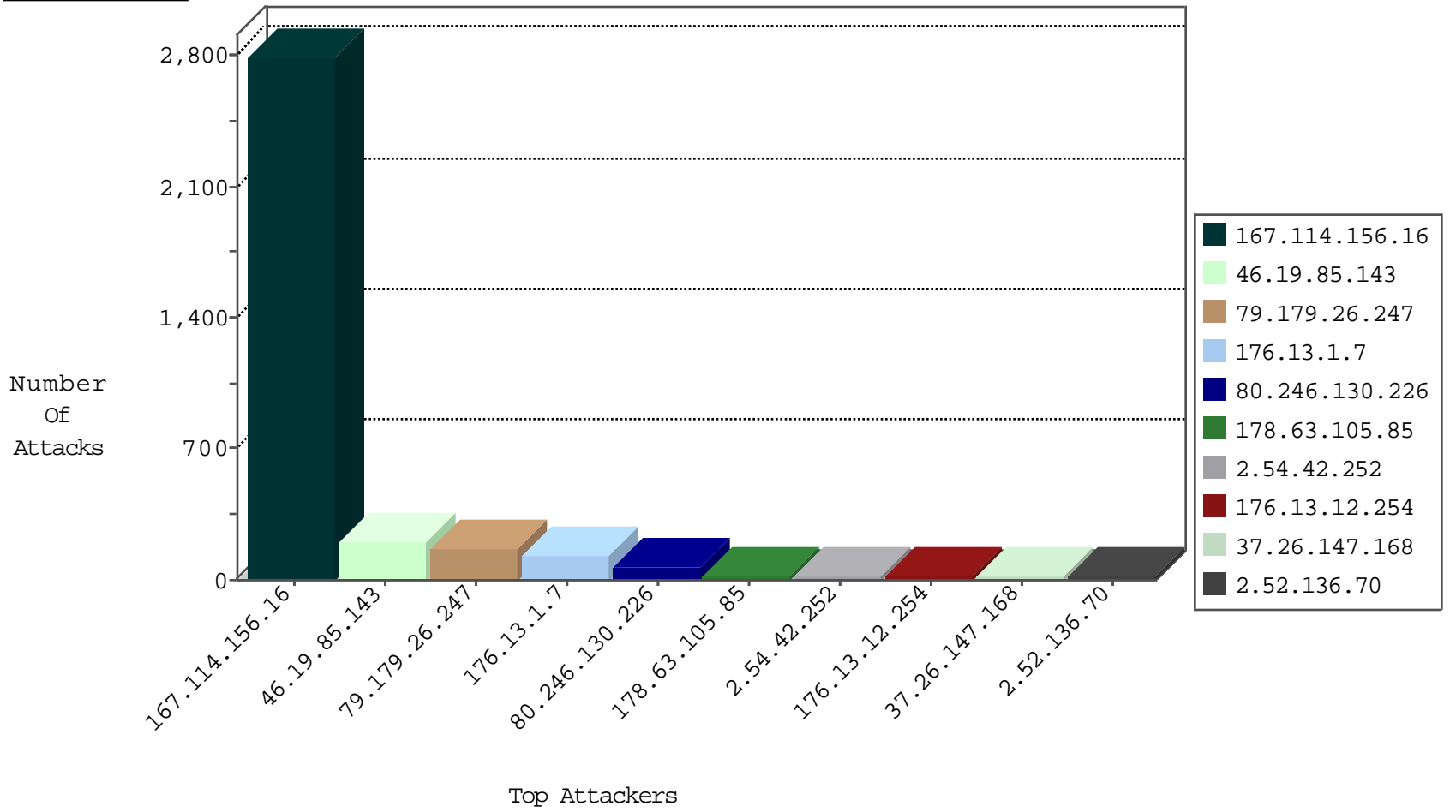
IDF Under Attack Daily Report



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	3817
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
180.97.31.70	China	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid I4 Header Length	drop	1
109.22.97.63	France	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1		147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
109.239.58.41	Germany	147.237.8.14	e.orchot.idf.il	Invalid TCP Flags	drop	1
185.94.111.1		147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.149.38	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
66.249.93.121	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.22.130.253	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
37.46.39.122	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
66.249.93.125	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.249.93.125	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
66.249.93.117	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
37.26.149.232	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
213.57.231.142	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.93.121	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
217.132.38.183	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.253.159.40	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.254.131.243	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
149.50.90.223	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
188.165.15.202	France	147.237.77.216	dover.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	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	4
82.230.117.182	147.237.76.39	France	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
82.230.117.182	147.237.76.38	France	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
149.78.140.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.190.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.214.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.204.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
31.210.177.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.131.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.230.117.182	147.237.76.201	France	e.atal.idf.il	ET SCAN Potential SSH Scan	1
82.230.117.182	147.237.76.197	France	e.himush.idf.il	ET SCAN Potential SSH Scan	1
82.230.117.182	147.237.76.176	France	test.noore.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
82.230.117.182	147.237.76.31	France	nakchal.idf.il	ET SCAN Potential SSH Scan	1
132.74.14.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.111.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.173.248.88	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.77.205	Ukraine	prisha.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
2.54.168.101	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.95.86.27	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.230.117.182	147.237.76.200	France	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
82.230.117.182	147.237.76.177	France	ncore.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
82.230.117.182	147.237.76.42	France	refuah.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.8.45	China	e.eitan.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
176.13.1.7	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
80.246.130.226	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	63
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	29
37.26.147.168	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.13.12.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
176.13.22.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
84.95.86.27	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	9
79.178.223.75	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.66.153.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.129.221	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.183	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
5.22.135.178	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
79.181.25.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.97.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.1.7	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.236.211	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
109.253.145.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.144.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	5
80.246.140.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.254.94	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.154.42.111	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	5
46.19.85.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.120.154.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
173.13.253.73	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
185.3.146.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	4
46.19.85.98	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	4
46.19.85.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
149.78.192.70	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
5.22.131.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.46.39.254	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.135.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.8.204.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.46.39.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.149.240	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
37.26.146.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.127.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
165.51.191.195		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
5.102.195.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.208.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.177.138.120	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.46.39.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.166.112.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	199
79.179.26.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	158
2.52.136.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
2.54.42.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
184.168.193.33	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 184.168.193.33	Block	5
2.54.187.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
132.74.165.90	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/	Block	3
2.54.0.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.84.251	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.86.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.172.5	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
46.19.86.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
64.1.16.66	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.25.201	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.86.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.140.102.59	Russian Federation	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.180.34.127	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
2.53.9.106	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
188.165.15.202	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
89.138.102.163	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
41.40.229.104	Egypt	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	1
68.180.228.167	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
2.54.137.95	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
213.254.241.4	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.145.150	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method If-Modified-Since: in URL tue,	Block	1
5.140.102.59	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
79.180.34.127	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.180.34.127	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
2.53.9.106	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
189.218.72.251	Mexico	147.237.77.74	law.idf.il	Suspicious Response Code	Block	1
89.138.228.189	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
41.40.229.104	Egypt	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php	Block	1
68.180.230.189	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.149.159	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	1
66.249.84.195	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.126	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
89.138.228.189	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
77.237.138.202	Czech Republic	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	1
5.22.135.102	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
46.19.85.143	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
149.88.54.154	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
37.46.38.99	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatenakatgauntity.aspx	Block	1
80.246.130.226	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
2.54.40.222	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1