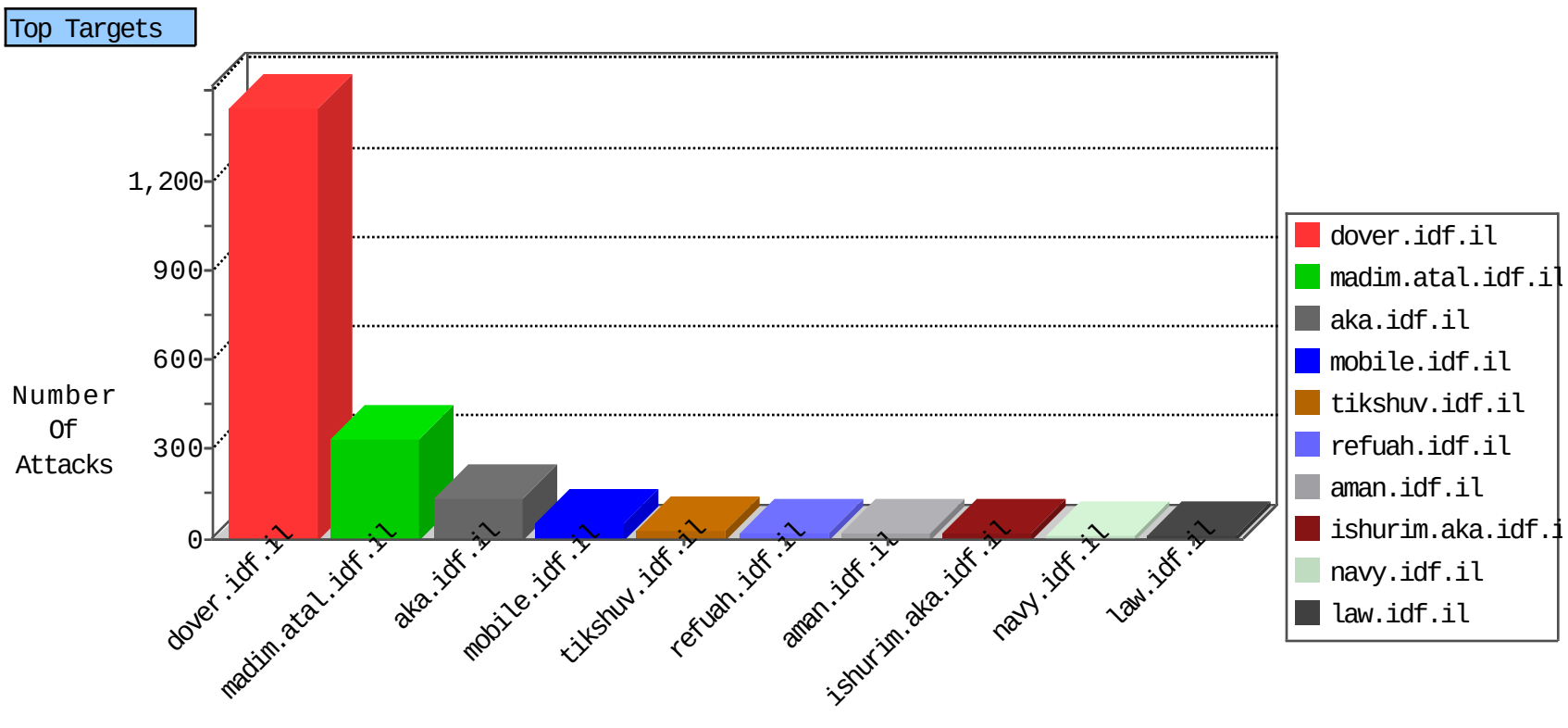
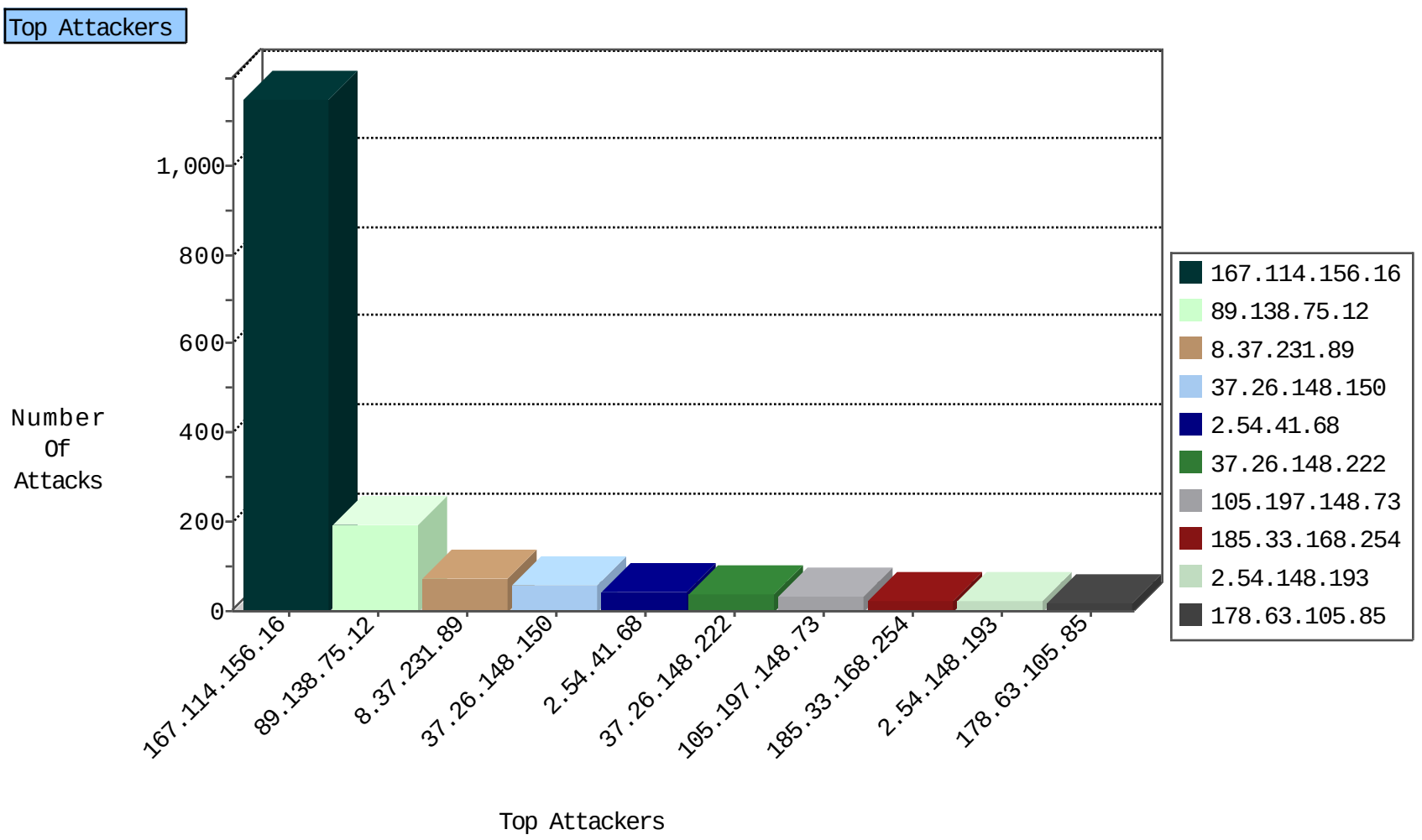
03-12-2016-21:04:06 to 03-12-2016-22:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-12-2016-21:04:06 to 03-12-2016-22:04:06

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	3077
37.26.148.150	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	forward	119
82.145.211.6	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	20
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
8.37.231.89	Anonymous Proxy	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	2
8.37.231.89	Anonymous Proxy	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.94.111.1		147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
85.25.43.94	Germany	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
91.121.39.149	France	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

03-12-2016-21:04:06 to 03-12-2016-22:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.25.198	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
157.55.2.180	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
107.150.56.254	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
46.19.85.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
107.150.56.254	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
79.180.166.63	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-12-2016-21:04:06 to 03-12-2016-22:04:06

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
2.54.161.192	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
66.249.64.9	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
103.9.163.151	147.237.0.19	Australia	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
80.246.133.192	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
185.72.179.221	147.237.76.201		e.atal.idf.il	ET SCAN Potential SSH Scan	1
62.210.24.214	147.237.0.34	France	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.76.196		e.sviva.idf.il	ET SCAN Potential SSH Scan	1
37.139.27.231	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.221	147.237.72.217		e.idf.il	ET SCAN NMAP -sS window 1024	1
173.14.248.34	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
173.14.248.34	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
104.45.210.69	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
103.9.163.151	147.237.0.19	Australia	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
103.9.163.151	147.237.0.19	Australia	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
185.72.179.221	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
62.210.24.214	147.237.0.19	France	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.76.176		test.ncore.idf.il	ET SCAN Potential SSH Scan	1
37.26.148.150	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
178.63.11.208	147.237.77.233	Germany	atal.idf.il	ET SCAN NMAP -sS window 1024	1
173.14.248.34	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
137.226.113.7	147.237.76.86	Germany	navy.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1
104.45.210.69	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1

03-12-2016-21:04:06 to 03-12-2016-22:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.231.89	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	69
105.197.148.73	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
2.54.41.68	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
105.86.124.77	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
2.54.10.135	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.52.163.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.87	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.93	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	7
185.33.168.254	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
185.33.168.254	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	7
105.97.7.220	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
185.33.168.254	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.33.168.254	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.146.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	5
5.22.135.194	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.244	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
5.102.242.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.40	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.149.244	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	4
79.182.216.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.103	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.97.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.107.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.73.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.93.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.248.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.133.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.17.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.127.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.163.116	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.133.192	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.50.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.176.63.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.13.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.5.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	3
5.22.134.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.75.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	192
37.26.148.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
37.26.148.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
2.54.148.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
2.54.41.68	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
109.65.169.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
37.26.148.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.250.180.29	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 85.250.180.29	Block	2
94.230.86.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.179.112.247	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
213.151.35.221	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	2
37.26.146.193	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
92.240.191.208	Czech Republic	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
37.122.210.43	United Kingdom	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/test/wp-admin/	Block	1
8.37.232.233	United States	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.172.133.54	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
185.33.168.254	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
65.55.210.211	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 149.88.71.234 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
94.230.93.80	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
92.240.191.208	Czech Republic	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.mag.idf.il/xmlrpc.php	Block	1
217.78.57.231	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
173.247.228.10	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
68.180.228.151	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/	Block	1
109.253.158.33	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
37.142.250.134	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
31.168.31.178	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
93.173.224.163	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
85.250.180.29	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/6/	Block	1
185.120.125.27		147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20329-he/dover.aspx	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
94.230.93.87	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
92.240.191.208	Czech Republic	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
2.54.17.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
173.247.228.10	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
68.180.230.152	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2065-he/cogat.aspx	Block	1
41.99.67.226	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
149.78.133.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.168.31.178	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
87.69.149.21	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/undefined	Block	1
212.76.122.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
157.55.39.189	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
104.131.147.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
93.172.17.55	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
173.247.228.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
50.63.197.58	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-admin/	Block	1
149.88.59.187	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.88.59.187	Block	1
37.26.146.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1