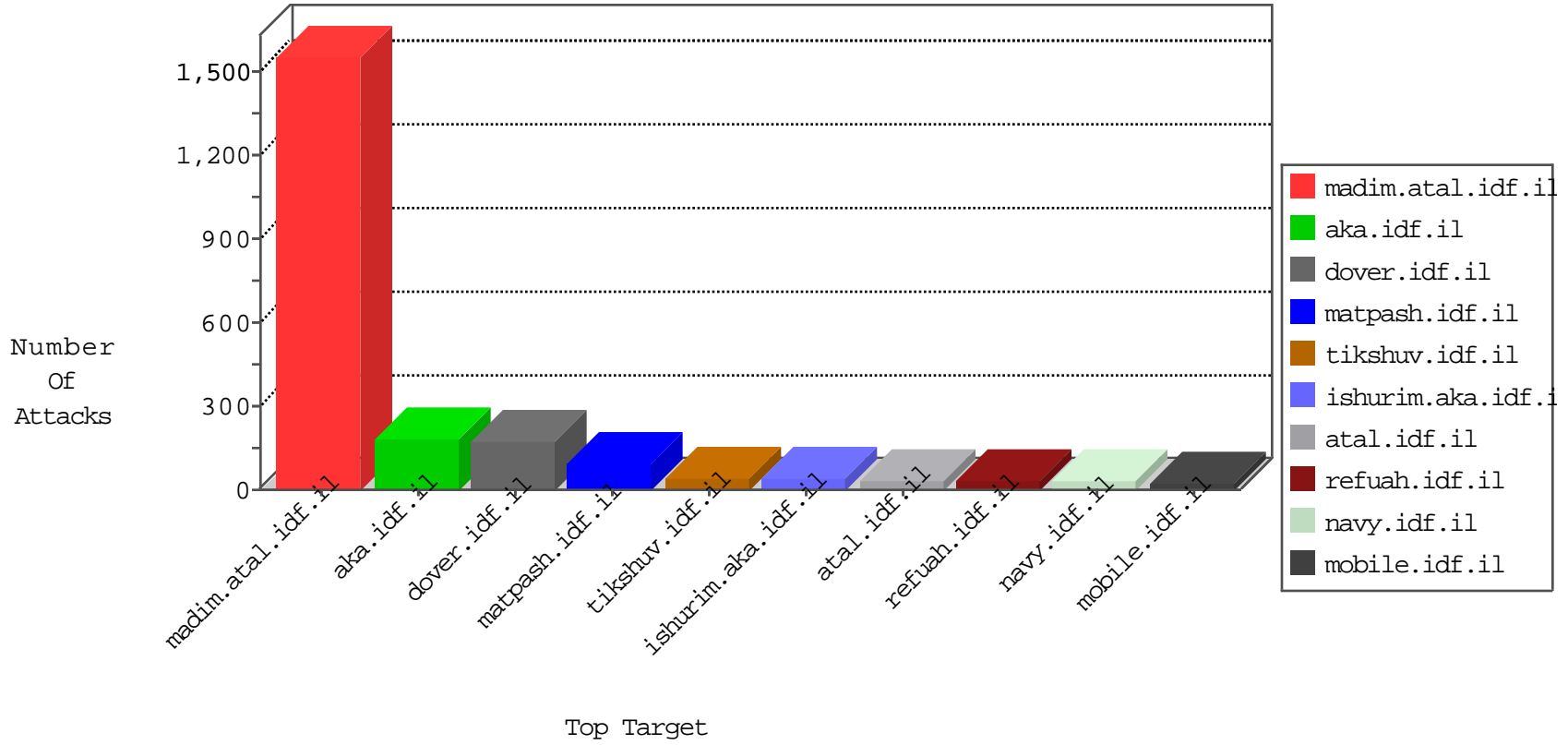


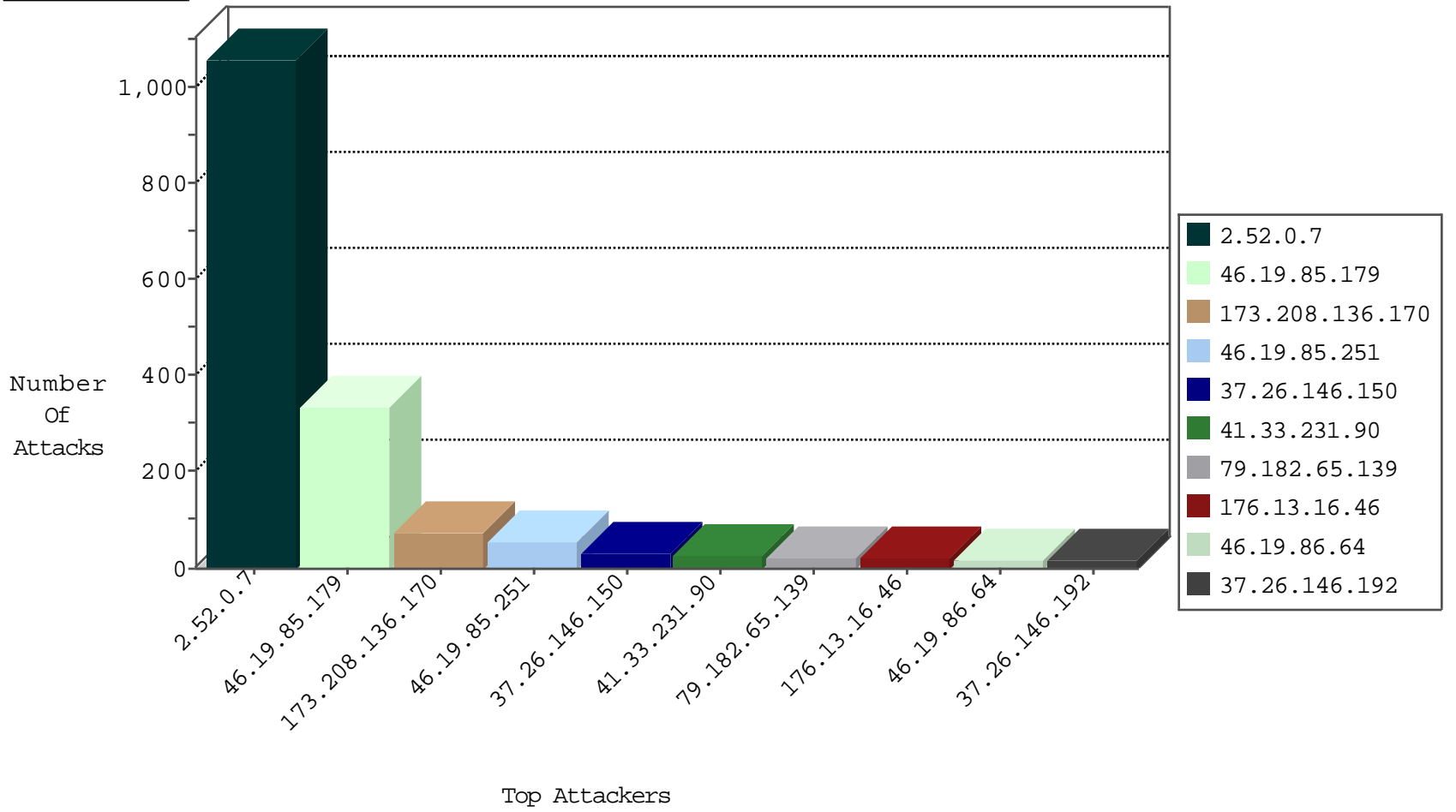
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.192	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
91.221.58.27	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
185.130.5.224		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.199	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
185.103.252.17		147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
198.23.112.119	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.56.215.218	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	5
109.253.142.159	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
151.80.31.152	Italy	147.237.76.86	navy.idf.il	C1000228: HTTP: AhrefBot crawler	Block	2
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
77.125.160.66	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
79.181.107.183	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
72.27.221.77	147.237.76.44	Jamaica	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
72.27.221.77	147.237.77.170	Jamaica	maarachot.idf.il	ET SCAN Potential SSH Scan	1
69.160.35.132	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.242.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.28.165.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.113.125.11	147.237.0.17	Romania	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
82.81.27.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.115.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
72.27.221.77	147.237.76.197	Jamaica	e.himush.idf.il	ET SCAN Potential SSH Scan	1
72.27.221.77	147.237.76.30	Jamaica	himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
202.159.189.109	147.237.77.216	Australia	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
194.114.146.227	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
31.168.83.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.113.125.11	147.237.0.34	Romania	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
82.81.86.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.112	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
173.208.136.170	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	25
46.19.86.64	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
84.94.198.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.219.24.52	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
2.52.32.79	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.17	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
37.26.147.255	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
217.194.203.52	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
80.246.130.112	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.200.205.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.10	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.93	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.193	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.32.79	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.46	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.60.38.99	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	6
46.19.85.179	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.189	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.148.193	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.167.176	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.53.177	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.22.130.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.130.112	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
81.218.68.234	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.143.124.116	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.17	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
122.172.244.82	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.210.187.129	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.144	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.124.116	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.52.32.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.189	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.178.152.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.54.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
194.50.98.12	Ukraine	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.22.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.193.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.34.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.205.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.141.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.85.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.218.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.8.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.26	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
2.52.0.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	675
2.52.0.7	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.52.0.7	Block	217
46.19.85.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	175
2.52.0.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	167
46.19.85.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	150
46.19.85.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
173.208.136.170	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 173.208.136.170	Block	37
37.26.146.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
176.13.16.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
79.182.65.139	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.182.65.139	Block	20
93.172.55.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
46.19.85.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
173.208.136.170	United States	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 173.208.136.170	Block	5
46.19.85.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.157.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.52.170.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.201.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.38.222	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
176.13.0.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.210.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.168.23.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.59	Block	3
2.54.24.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.216.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.169.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
182.75.125.66	India	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	2
79.177.28.62	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/gyus/controls/atuda/Å	Block	2
80.178.227.165	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
85.65.26.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/controls/atuda/Å	Block	2
109.242.102.73	Greece	147.237.77.74	law.idf.il	PHP Attempt	Block	2
109.242.102.73	Greece	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	2
182.75.125.66	India	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
74.6.254.122	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyus/general.aspx	Block	1
208.115.113.84	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/æ××ª××" ×" xž×æ×?×"	Block	1
94.205.92.144	United Arab Emirates	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
85.64.153.70	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
37.26.146.203	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
46.116.114.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
216.218.206.68	United States	147.237.0.16	ny-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
46.19.85.62	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
192.117.113.18	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	1
10.145.40.16		147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	1
180.76.15.149	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
79.175.96.147		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
147.235.236.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
212.76.113.72	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.76.113.72	Block	1
94.205.92.144	United Arab Emirates	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
37.26.149.144	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
182.75.125.66	India	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1