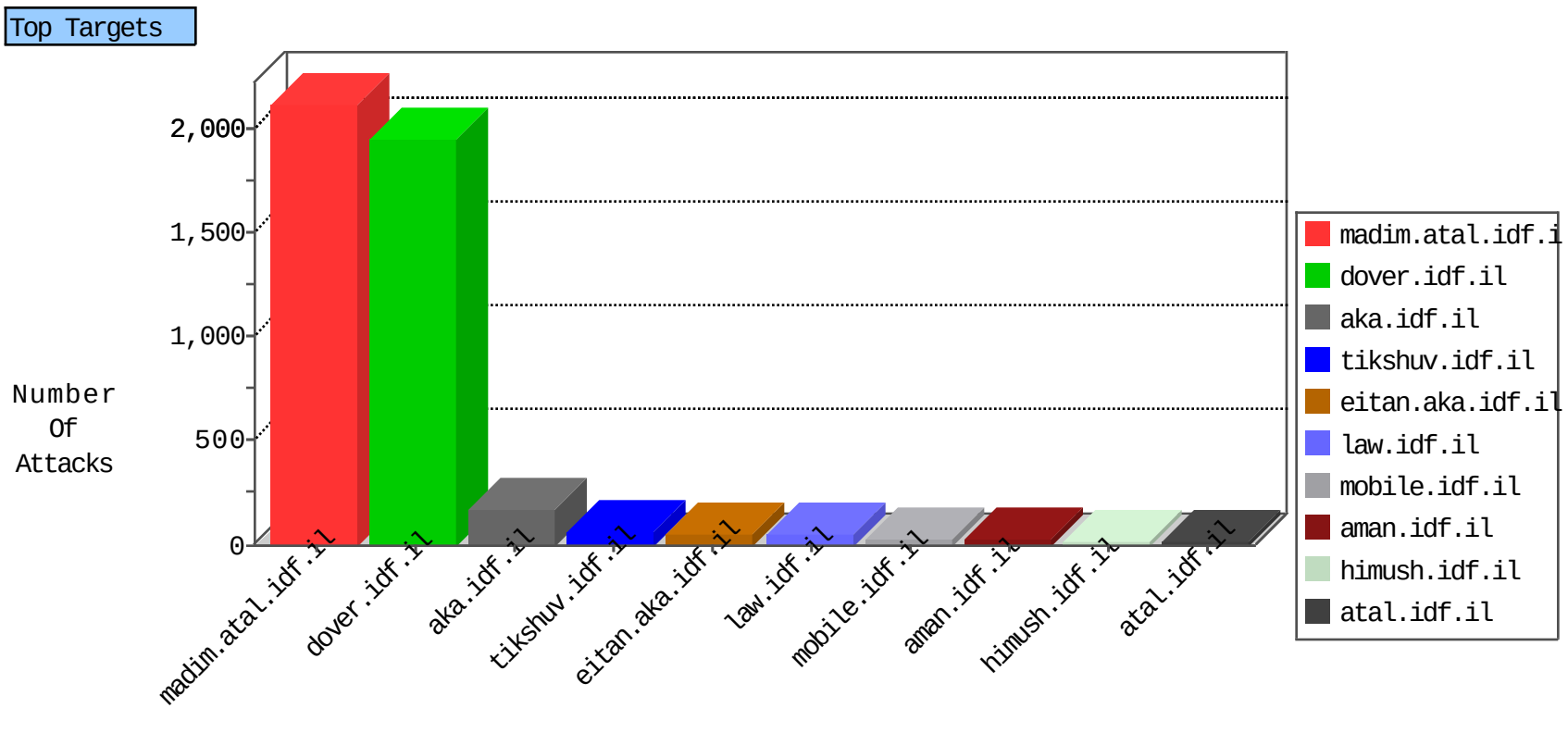
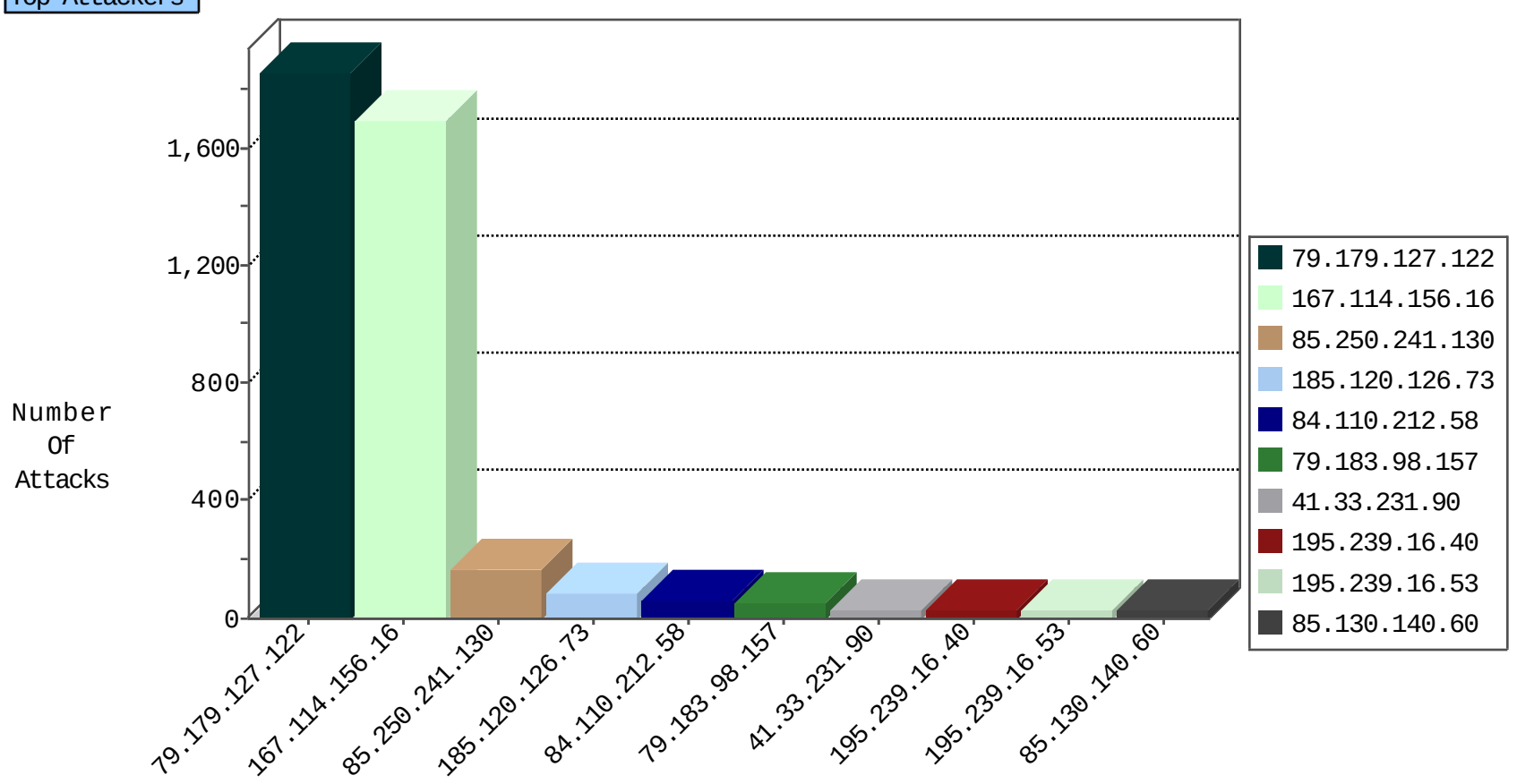
01-05-2016-23:04:02 to 01-06-2016-00:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-05-2016-23:04:02 to 01-06-2016-00:04:02

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	3446
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	78
146.185.57.7	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
45.58.118.218		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
45.58.118.218		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

01-05-2016-23:04:02 to 01-06-2016-00:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-05-2016-23:04:02 to 01-06-2016-00:04:02

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	2
198.20.69.74	147.237.77.61	United States	e.cogat.idf.il	ET DROP Dshield Block Listed Source	1
46.228.207.18	147.237.77.226	Germany	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
180.153.104.125	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
46.228.207.18	147.237.77.205	Germany	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.66	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.198	Germany	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.62.238.153	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.77.243	China	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.8.50	Germany	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
123.20.32.84	147.237.77.235	Vietnam	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	147.237.77.205	China	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.8.28	Germany	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.229.229.112	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.255.65.207	147.237.0.19		madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.113	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
217.12.39.85	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.72.166	China	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.174.71.229	147.237.0.34	Poland	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
209.126.116.147	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
77.109.38.223	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.77.212	Germany	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.66	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.77.121	Germany	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
180.153.104.125	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
123.20.32.84	147.237.77.235	Vietnam	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.64	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.8.46	Germany	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
123.20.32.84	147.237.77.235	Vietnam	sviva.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	147.237.77.176	China	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.0.33	Germany	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.255.65.207	147.237.76.39		mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.162.131	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
77.109.38.223	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN NMAP -sS window 1024	1

01-05-2016-23:04:02 to 01-06-2016-00:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.110.212.58	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	55
79.183.98.157	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	27
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
79.180.181.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
31.154.158.73	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
176.13.20.144	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
157.55.39.75	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	11
41.13.208.142	South Africa	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
176.13.20.144	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
79.183.154.112	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.26.147.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.149.218	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
87.69.119.58	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.120.125.47		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.12	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.235.8.70	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
105.112.41.9	Nigeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
147.235.8.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
5.102.253.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.140.60	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
188.48.2.84	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.13.208.142	South Africa	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.147.229	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
85.130.140.60	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.137.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.135.240	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.130.140.60	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
5.29.254.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
203.133.170.140	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
82.166.247.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.22	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.235.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.137.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.131.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.185.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.206.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.151.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.218.44	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

01-05-2016-23:04:02 to 01-06-2016-00:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.127.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1376
79.179.127.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	267
79.179.127.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	216
85.250.241.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
85.250.241.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	59
109.253.157.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
37.26.149.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
185.32.179.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
85.130.140.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
85.250.241.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	5
2.54.149.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
2.54.34.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.13.14.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.180.181.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.16.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.221.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
5.29.254.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.228.161.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	2
89.139.16.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.86.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
31.154.158.73	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
2.54.175.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.135.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8898-he/refuah.aspx	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2306.jpg	Block	1
213.8.204.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.172.161.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.1	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
182.253.224.110	Indonesia	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
79.170.44.83	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
5.102.253.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.75	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/images/headers/tfasim.gif	Block	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
51.254.131.221	United Kingdom	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
198.71.231.45	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp/wp-admin/	Block	1
37.26.147.170	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
5.28.165.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.140.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-ui.js	Block	1
213.57.108.194	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
104.131.217.156	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 104.131.217.156	Block	1
46.19.85.1	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
184.154.174.162	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp-admin/	Block	1
79.177.53.146	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 79.177.53.146 (Unknown SSL Session)	None	1
5.102.254.140	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1

01-05-2016-23:04:02 to 01-06-2016-00:04:02