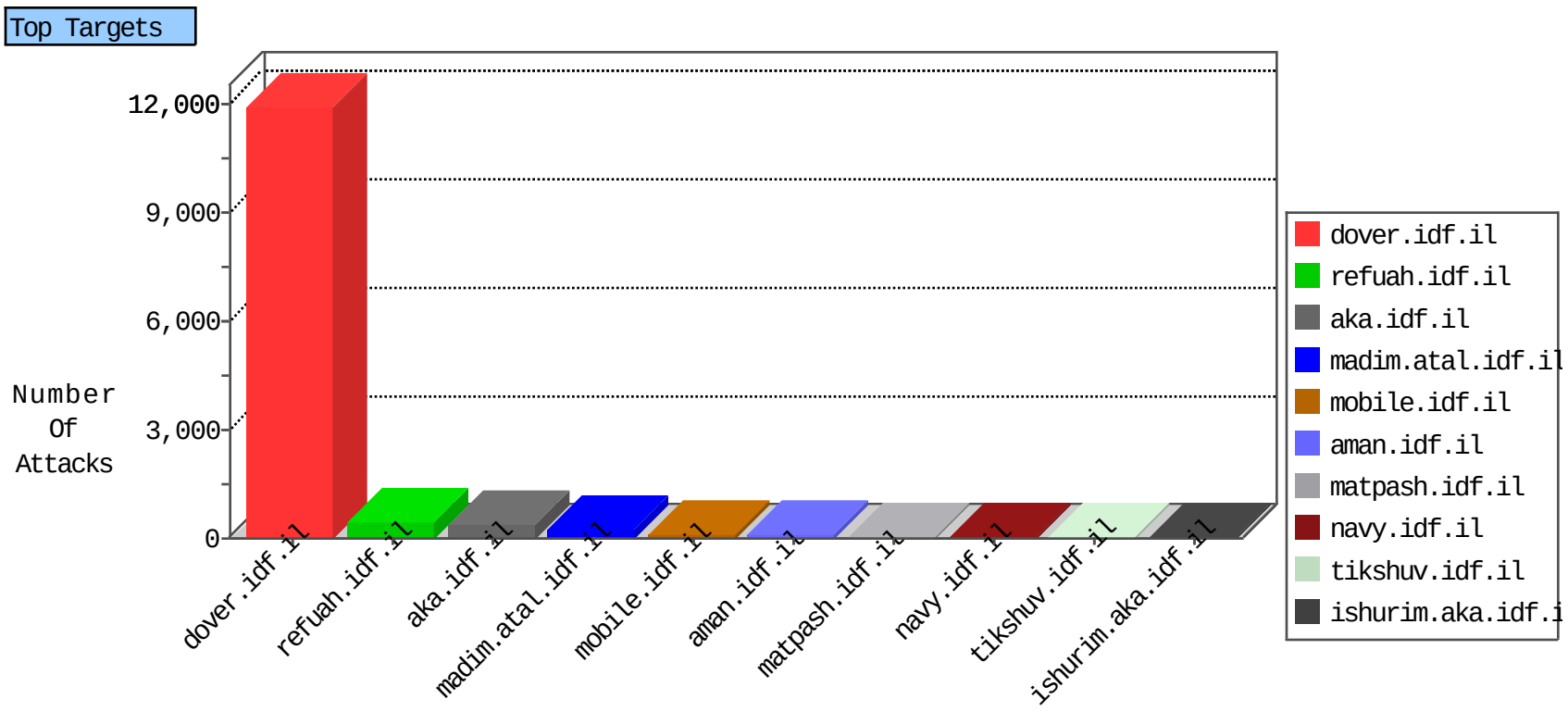
01-06-2016-19:04:09 to 01-06-2016-20:04:09

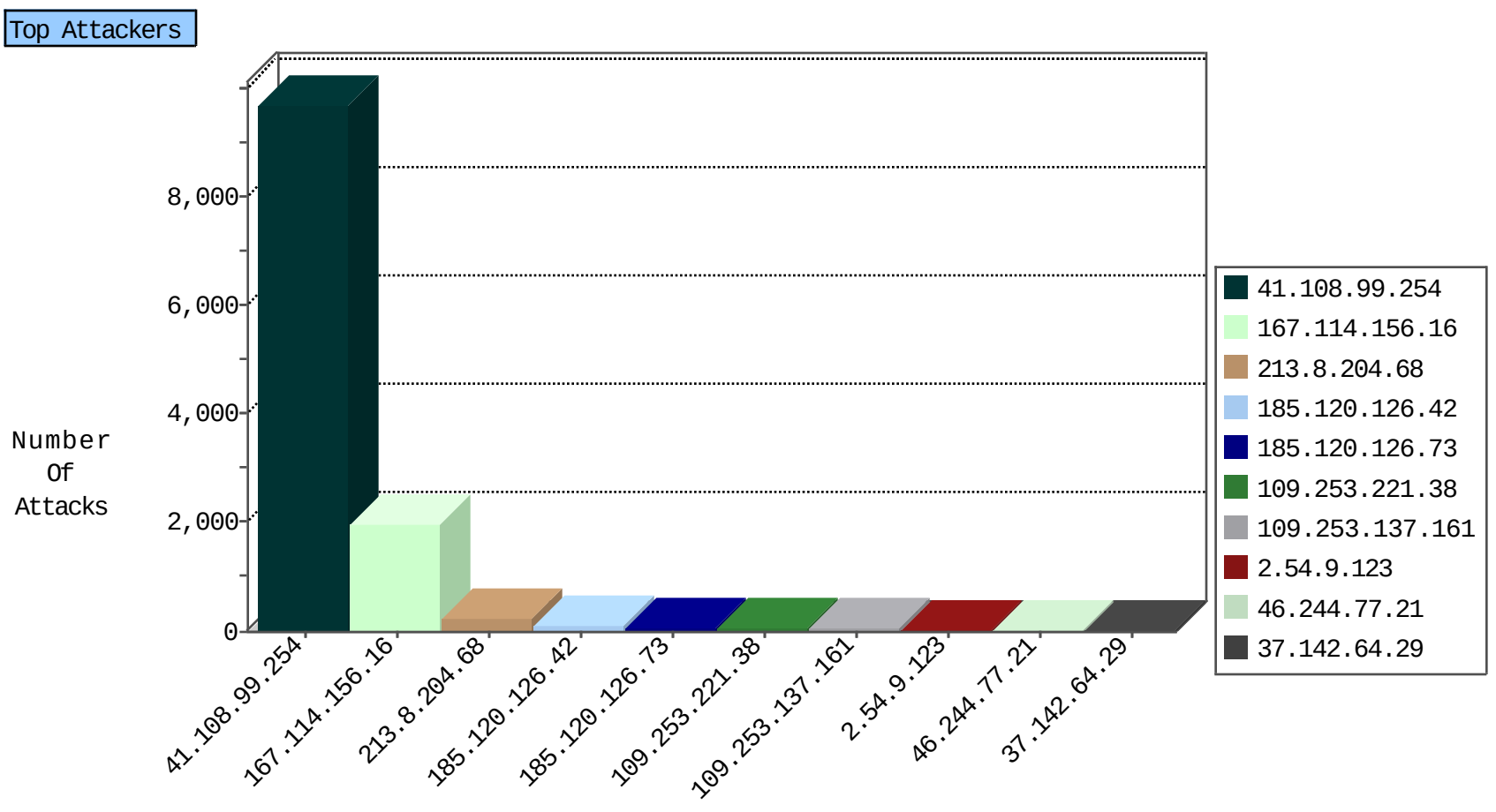
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-06-2016-19:04:09 to 01-06-2016-20:04:09

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	3216
41.108.99.254	Algeria	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	74
79.182.114.82	Israel	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	3
141.212.122.206	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
80.82.64.177	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	drop	1
71.6.135.131	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1

01-06-2016-19:04:09 to 01-06-2016-20:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-06-2016-19:04:09 to 01-06-2016-20:04:09

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	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
49.75.129.202	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	3
49.75.129.202	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
49.75.129.202	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
49.75.129.202	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
195.81.132.99	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN Potential SSH Scan	2
149.78.2.228	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
66.249.64.153	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
193.105.134.220	147.237.0.16	Sweden	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
60.217.72.16	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
115.182.17.13	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.233.53	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
49.75.129.202	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
183.60.233.53	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
49.75.129.202	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
89.248.162.131	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
183.60.233.53	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.25.121.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
49.75.129.202	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
85.64.6.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
176.228.47.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.147.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.81.132.99	147.237.76.148	United Kingdom	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
49.75.129.202	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
131.109.15.15	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
79.177.53.28	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.81.132.99	147.237.8.27	United Kingdom	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
131.109.15.15	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
49.75.129.202	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.160	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
195.81.132.99	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
117.25.155.164	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
62.0.84.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
115.182.17.13	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 3072	1
49.75.129.202	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
190.66.217.5	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
49.75.129.202	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
115.182.17.13	147.237.72.217	China	e.idf.il	ET SCAN NMAP -f -sS	1
183.60.233.53	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
91.98.58.69	147.237.8.46	Iran, Islamic Republic of	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

01-06-2016-19:04:09 to 01-06-2016-20:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.108.99.254	Algeria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4321
41.108.99.254	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	251
41.108.99.254	Algeria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	235
213.8.204.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	225
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	142
185.120.126.42		147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	94
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	78
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
41.108.99.254	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	51
46.244.77.21	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	36
41.108.99.254	Algeria	147.237.77.216	dover.idf.il	drop		drop	33
41.108.99.254	Algeria	147.237.77.216	dover.idf.il	SYN Attack		reject	29
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
213.8.204.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	26
41.108.99.254	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
41.108.99.254	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
41.108.99.254	Algeria	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	19
46.19.86.8	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
185.89.217.233		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	17
84.109.101.91	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	17
41.108.99.254	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
46.19.85.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
79.182.114.44	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.89.217.232		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
37.26.149.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
185.89.217.226		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
66.102.9.107	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	10
185.89.217.224		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
185.89.217.234		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
2.54.189.36	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
185.89.217.235		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
37.26.149.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
185.89.217.228		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
84.228.11.174	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
185.89.217.225		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
109.186.164.109	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
109.186.164.109	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
41.108.99.254	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
185.89.217.227		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
109.253.134.119	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
109.253.144.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.65.148.26	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.52.172.135	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.26.148.161	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		alert	6
199.203.36.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.32.109	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

01-06-2016-19:04:09 to 01-06-2016-20:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.108.99.254	Algeria	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 41.108.99.254	Block	4529
109.253.221.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
109.253.137.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
2.54.9.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
41.108.99.254	Algeria	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 41.108.99.254	Block	36
41.108.99.254	Algeria	147.237.77.216	dover.idf.il	Multiple Malformed URL from 41.108.99.254	Block	36
37.142.64.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
188.143.232.13	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.13	Block	7
46.19.86.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.130.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
193.37.128.168	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	5
46.120.46.55	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.120.46.55	None	5
109.253.221.38	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.221.38	Block	5
176.13.4.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	4
46.19.85.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.27	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
80.74.102.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
79.177.108.56	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
95.86.83.68	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
31.44.136.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.64.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.121.140.220	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.144.14	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
109.253.134.119	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.195.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.18.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
149.88.84.184	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
207.46.13.21	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/img/banner/_banner_1829.pic	Block	1
5.29.165.134	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.253.134.119	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
185.32.179.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.4.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.227.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.2.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.10.210.199	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/size220x0/17882.jpg	Block	1
109.253.217.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.128.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.66.179.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.98.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.120.126.42		147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
46.19.85.171	Israel	147.237.76.31	nakchal.idf.il	Distributed Unknown HTTP Request Method	Block	1
176.13.19.127	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
149.88.122.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.139.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-06-2016-19:04:09 to 01-06-2016-20:04:09