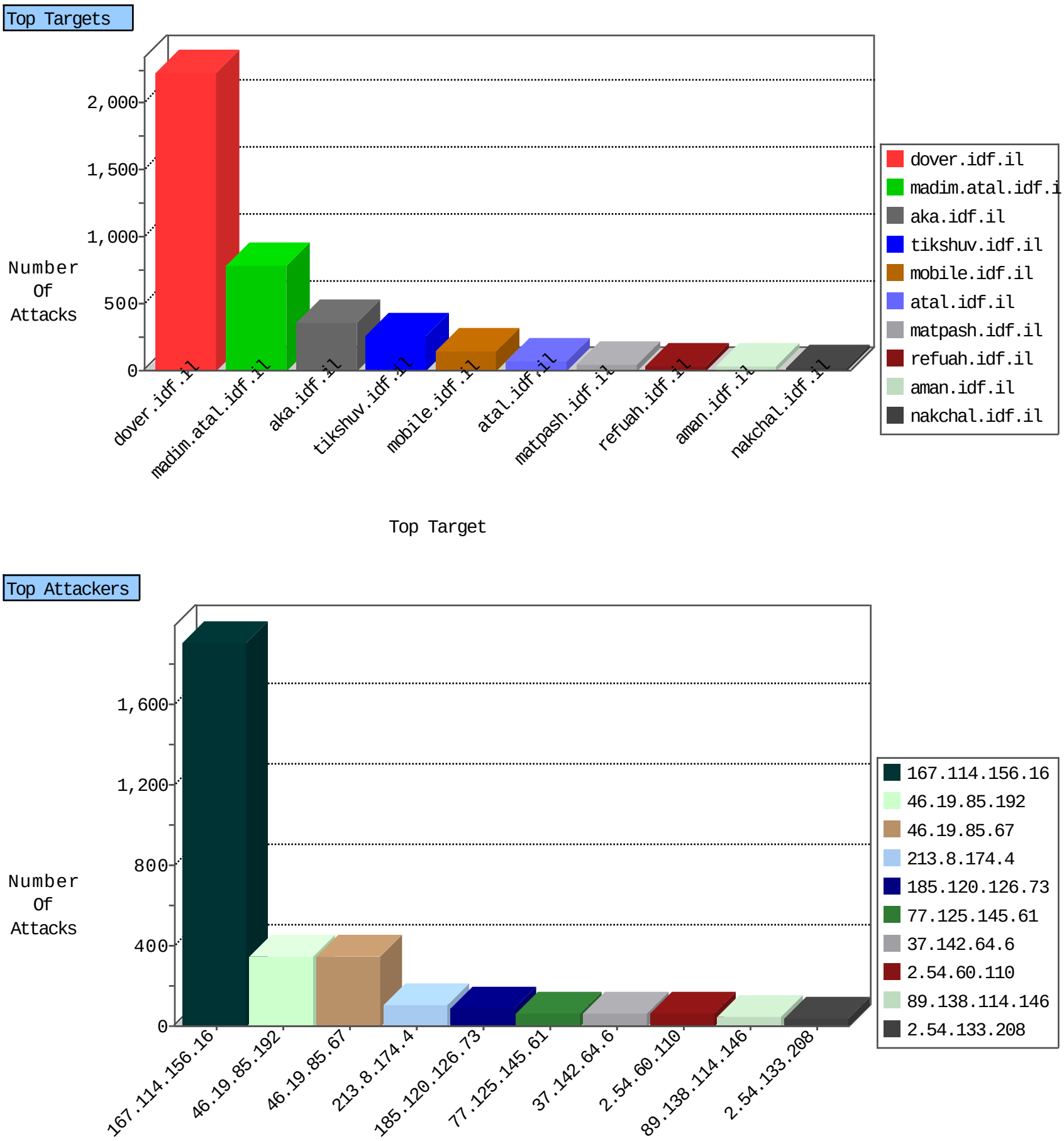
01-05-2016-19:04:08 to 01-05-2016-20:04:08

IDF Under Attack Daily Report



01-05-2016-19:04:08 to 01-05-2016-20:04:08

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	3529
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	342
71.6.216.42	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

01-05-2016-19:04:08 to 01-05-2016-20:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-05-2016-19:04:08 to 01-05-2016-20:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
46.228.207.18	147.237.76.197	Germany	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.147	Germany	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.172.159	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.76.44	Germany	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.68.41.9	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.228.207.18	147.237.72.166	Germany	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.177.192.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.210.188.101	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
52.90.147.148	147.237.77.216	United States	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
183.251.219.189	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.22.129.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
52.90.147.148	147.237.76.42	United States	refuah.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
149.88.136.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
52.90.147.148	147.237.0.16	United States	my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
109.65.29.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.228.207.18	147.237.77.227	Germany	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
106.75.199.201	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.228.207.18	147.237.76.148	Germany	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.86	Germany	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.172.159	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.76.34	Germany	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.178.141.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.228.207.18	147.237.0.34	Germany	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.150.214.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.140.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
52.90.147.148	147.237.76.86	United States	navy.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
52.90.147.148	147.237.0.17	United States	m.my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
109.186.166.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.228.207.18	147.237.77.243	Germany	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
106.75.199.201	147.237.76.31	China	nakchal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

01-05-2016-19:04:08 to 01-05-2016-20:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	55
89.138.114.146	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
2.54.133.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
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	29
46.60.28.145	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	29
2.54.23.225	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.67.145.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
80.246.136.193	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.181.206.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.109.146.148	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
79.182.203.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.179.241.55	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
2.52.168.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
80.178.157.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
80.178.157.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
93.172.168.192	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
80.246.133.83	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
85.250.44.189	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
212.34.12.8	Jordan	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	7
46.120.57.244	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.102.253.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.66.119.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.150.203.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.9.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.80.146.24	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.166.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.50.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
109.253.209.62	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.170	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.65.28.222	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
93.172.166.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.66.96.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.170	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
40.77.167.16	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.50.245	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.80	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.22.129.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
89.138.114.146	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
5.22.130.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.211.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
85.250.44.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
2.54.52.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.188.98	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

01-05-2016-19:04:08 to 01-05-2016-20:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	209
46.19.85.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	149
46.19.85.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	124
46.19.85.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	112
213.8.174.4	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	102
46.19.85.192	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.85.192	Block	63
77.125.145.61	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	60
2.54.60.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	59
37.142.64.6	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
46.19.85.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	25
37.142.64.6	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 37.142.64.6	Block	19
5.29.9.131	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
46.19.85.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	13
2.52.20.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 2.52.20.26	Block	10
2.54.133.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
2.54.23.225	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.13.2.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
80.246.136.193	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
2.54.150.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
77.125.79.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
37.26.149.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.57.109.10	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.57.109.10	Block	3
46.19.86.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.121.89.4	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.121.89.4	Block	3
109.253.144.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
217.132.105.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
80.178.157.42	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
109.65.23.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
94.230.86.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.57.72.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
31.168.66.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	2
212.143.134.129	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/589-he/patzar.aspx=	Block	2
79.178.2.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.187.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.21.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
82.166.81.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.108.145.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.116.86.123	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	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
31.210.188.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.64.51.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage	Block	2
46.121.89.4	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giy.us	Block	2
176.13.9.72	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
178.137.85.67	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 178.137.85.67	Block	2
89.138.105.88	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
105.107.115.131	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1154-ar/	Block	2
52.90.147.148	United States	147.237.76.86	navy.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.114	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
84.108.220.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.34.12.8	Jordan	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1

01-05-2016-19:04:08 to 01-05-2016-20:04:08