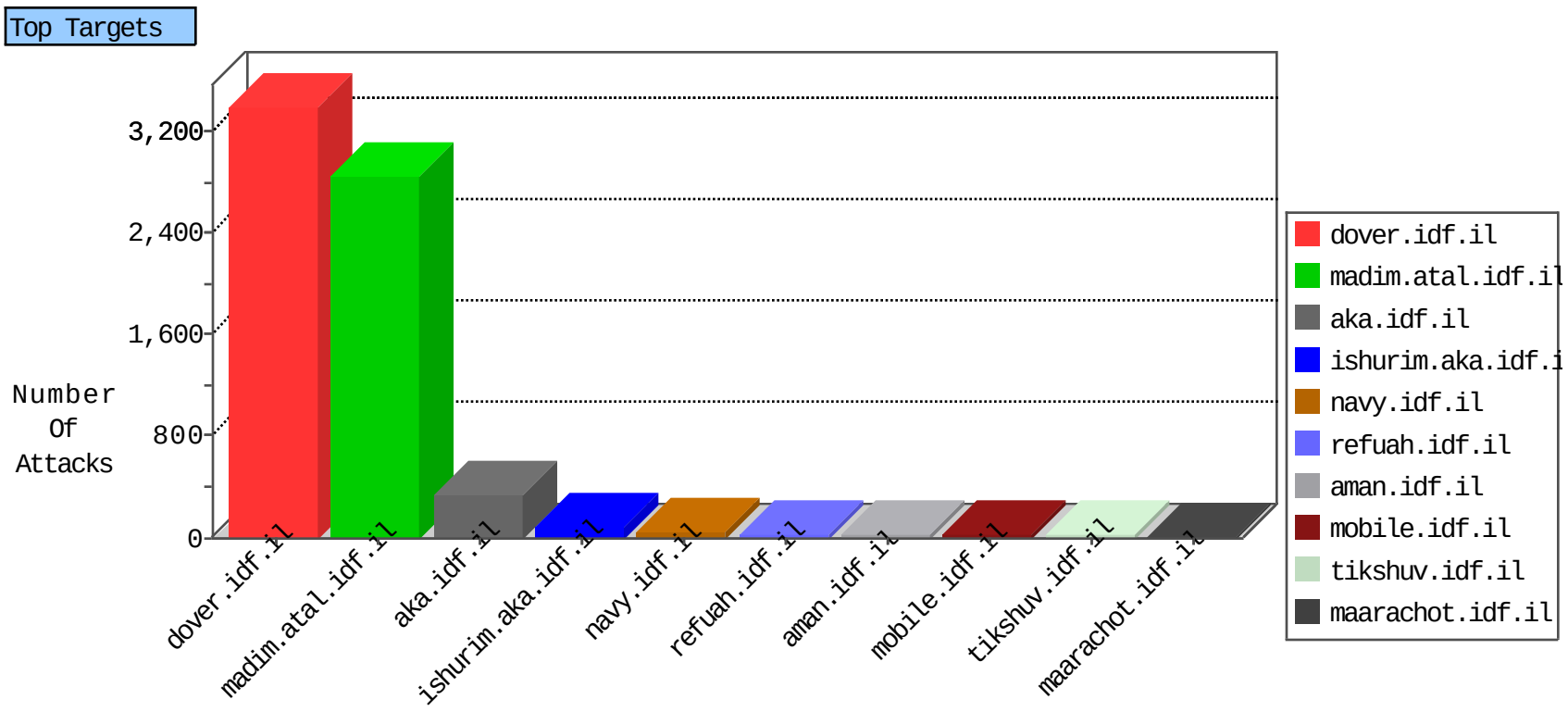
01-05-2016-10:04:06 to 01-05-2016-11:04:06

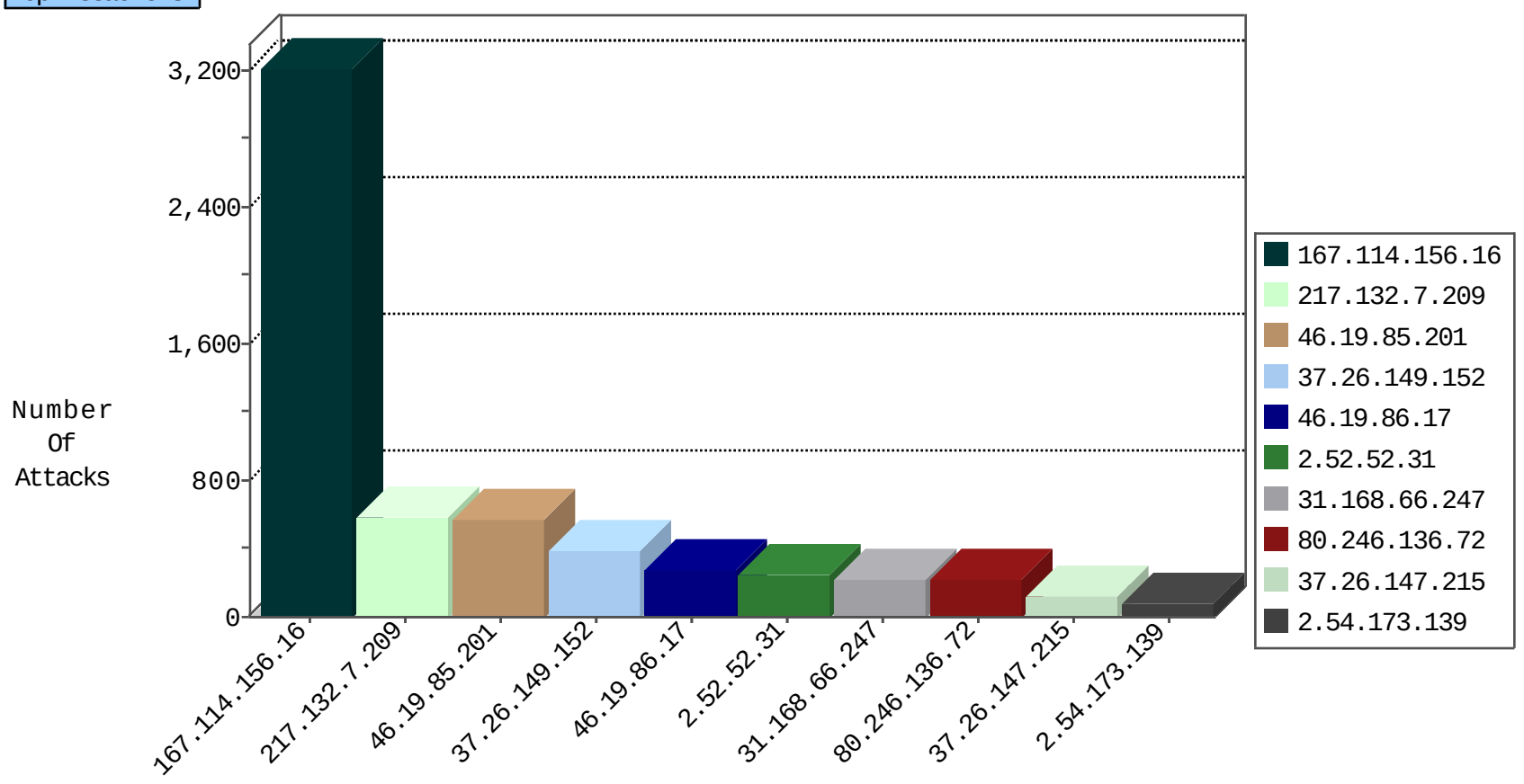
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-05-2016-10:04:06 to 01-05-2016-11:04:06

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	4886
66.249.75.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	745
204.93.154.212	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	204
204.42.253.130	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	2
31.168.178.197	Israel	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	1
109.66.10.228	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.216.55	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.62	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

01-05-2016-10:04:06 to 01-05-2016-11:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

01-05-2016-10:04:06 to 01-05-2016-11:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
85.130.244.240	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
117.21.248.87	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
213.57.180.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
67.207.202.9	147.237.72.156	United States	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
209.126.116.147	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
66.206.15.100	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
199.203.215.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.206.15.100	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
185.27.105.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.255.233.124	147.237.72.166	United States	aka.idf.il	GPL WEB_SERVER TRACE attempt	1
117.21.248.87	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
109.65.72.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.75.198	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
200.63.163.131	147.237.8.27	Argentina	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
66.206.15.100	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.54.8.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
173.255.233.124	147.237.72.166	United States	aka.idf.il	SERVER-WEBAPP TRACE attempt	1

01-05-2016-10:04:06 to 01-05-2016-11:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1040
2.54.173.139	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
46.19.85.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
2.54.188.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
188.120.159.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.250	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	9
109.66.177.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.179.183.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.32	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.183.128.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.181	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.173.181	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.48.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.120.28.83	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
157.55.39.224	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.244.240	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
84.94.124.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.20.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.111.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.28.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.243.152	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.1	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
91.195.163.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.14	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
31.210.187.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.95	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.130.227.133	United Kingdom	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
130.193.51.64	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.173	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
176.13.14.72	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.168.181	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.80	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.221.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
43.255.176.89	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.66.150.21	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
157.55.39.180	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
147.235.8.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.86.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
1.2.235.179	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
81.218.71.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.169.117	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.24.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

01-05-2016-10:04:06 to 01-05-2016-11:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.132.7.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	348
46.19.85.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	336
37.26.149.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	234
46.19.86.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	165
37.26.149.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	127
80.246.136.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	126
217.132.7.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	125
2.52.52.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	124
46.19.85.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	122
217.132.7.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	113
46.19.85.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.86.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
31.168.66.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	100
31.168.66.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
2.52.52.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	91
80.246.136.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
37.26.147.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	70
2.52.52.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	35
176.13.17.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	34
2.54.167.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
46.19.86.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	32
37.26.149.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	32
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
37.26.147.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
80.246.130.195	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.130.195	Block	15
176.13.17.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
2.54.189.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
2.52.14.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
46.19.86.127	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	4
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	4
108.203.48.137	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
95.86.98.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.11.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
216.72.40.185	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
46.19.86.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.17.75	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.17.75	Block	3
80.246.136.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
176.13.2.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
149.78.169.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.30.14	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	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
176.13.7.125	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
27.115.41.130	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	2
207.46.13.75	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	2
46.19.85.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2

01-05-2016-10:04:06 to 01-05-2016-11:04:06