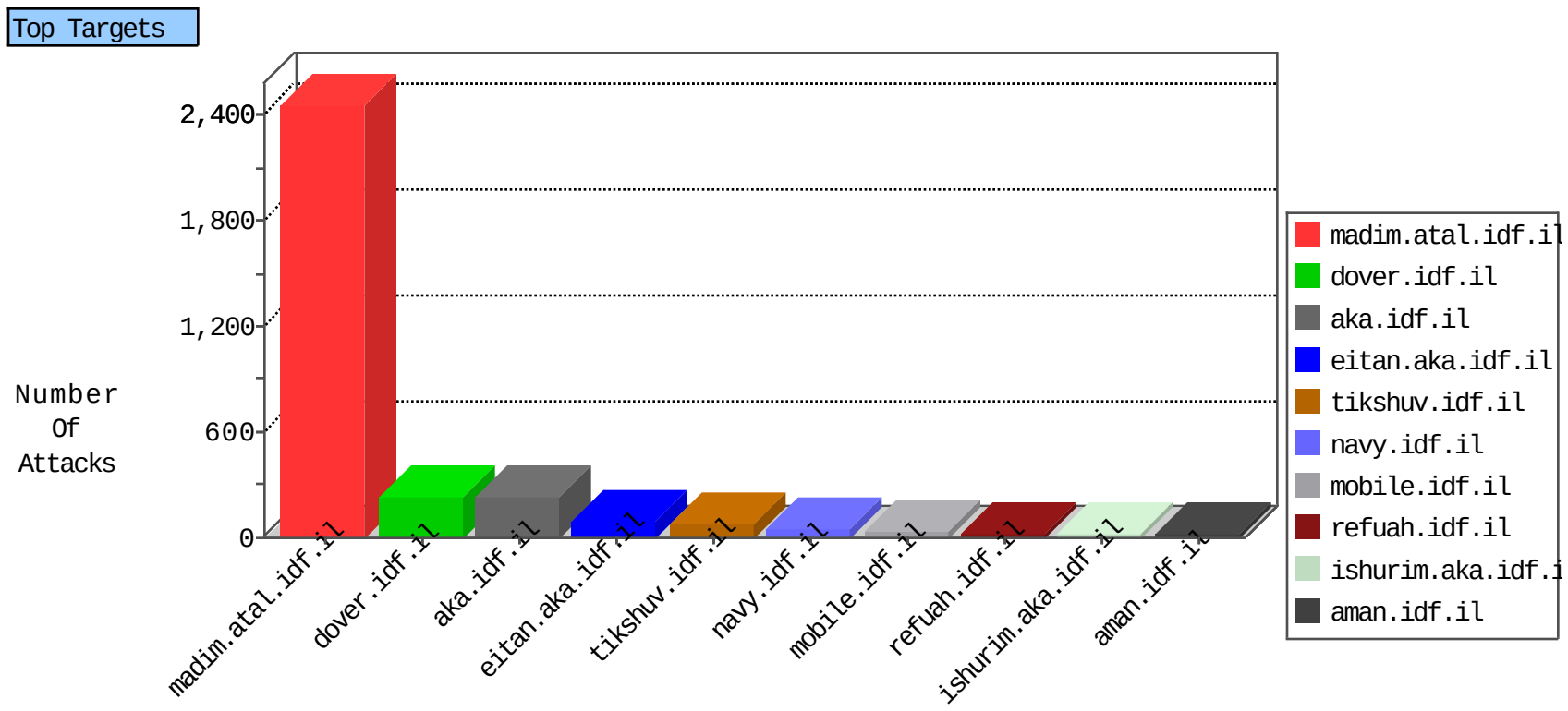
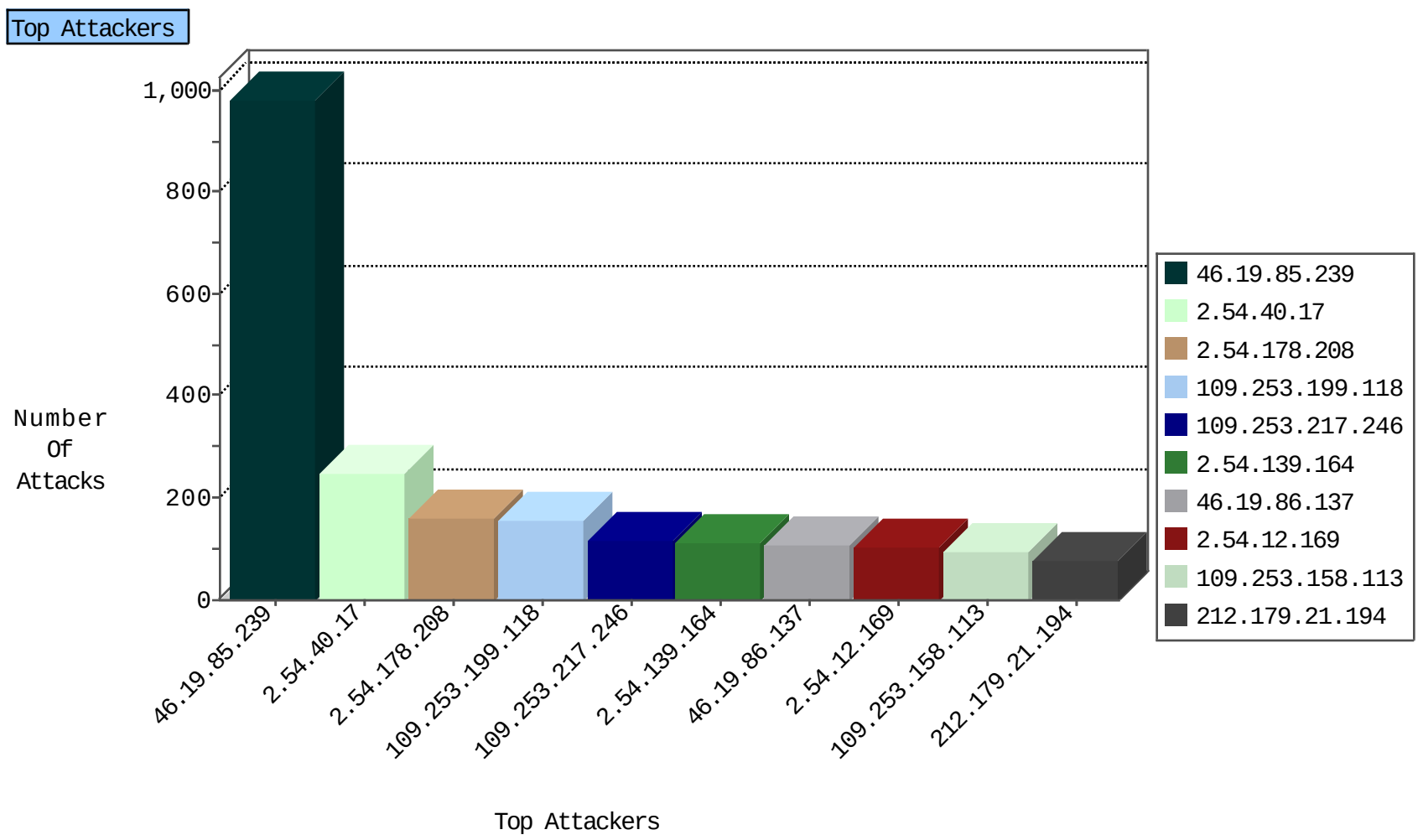
01-26-2016-08:04:04 to 01-26-2016-09:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-26-2016-08:04:04 to 01-26-2016-09:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
94.76.9.116	Bahrain	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Tcp	drop	2
1.222.105.130	Korea, Republic of	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
66.240.236.119	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.36	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
142.54.169.162	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1

01-26-2016-08:04:04 to 01-26-2016-09:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.248.12.153	Netherlands	147.237.76.42	refuah.idf.i	14331: HTTP: Suspicious User-Agent (My Session)	Block	2
46.19.86.137	Israel	147.237.77.216	dover.idf.il	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	1
198.20.69.74	United States	147.237.76.202	e.halag.idf.i	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-26-2016-08:04:04 to 01-26-2016-09:04:04

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	3
94.76.3.178	147.237.76.177	Bahrain	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.2.26	147.237.72.217	Bahrain	e.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.252.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.193.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
121.201.27.61	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
109.253.201.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.76.21.144	147.237.76.201	Bahrain	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.3.178	147.237.76.147	Bahrain	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.77.121		e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.193.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.43.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.196.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.161.4.141	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
121.40.195.144	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.255.65.207	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

01-26-2016-08:04:04 to 01-26-2016-09:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	76
84.94.158.140	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
217.194.193.5	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.200	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
207.241.231.227	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	11
2.52.141.1	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.184	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.52.169.196	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.183.52.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.0.211.71	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	9
157.55.39.237	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.179.218.166	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	7
80.246.136.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.17.111	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.145.185	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.218.166	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
174.127.66.147	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
80.246.136.98	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.179.162.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.107	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
157.55.39.198	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.204.128.94	Netherlands	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.29.58	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
80.246.136.98	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
176.13.7.251	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
212.179.218.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.179.218.166	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
217.194.198.109	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
217.194.198.109	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.140.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
62.0.211.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.179.218.166	Israel	147.237.76.86	navy.idf.il	SYN Attack		reject	4
2.52.0.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.189	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.24.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.173.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.70.243	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
5.22.130.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.219.125.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.78		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.241.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.82	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
46.19.85.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	587
46.19.85.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	257
2.54.40.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	164
46.19.85.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	138
2.54.139.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
2.54.178.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
46.19.86.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
109.253.199.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
2.54.12.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
109.253.217.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
109.253.158.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	83
2.54.40.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	76
176.13.6.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
80.178.157.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
109.253.199.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	49
2.54.178.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	45
109.253.132.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
176.13.7.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
109.253.217.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	30
80.246.136.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
176.13.10.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	28
176.13.17.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
80.178.239.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
109.253.158.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	12
2.52.173.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
2.54.40.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	10
80.246.139.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.213.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.139.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
5.29.151.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
2.54.178.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	5
109.253.207.221	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	4
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/main/home/default.aspx	Block	4
46.19.85.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.182.96.48	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	3
109.65.50.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.147.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.136.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.182.96.48	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
2.54.23.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
31.168.164.126	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	2
2.54.165.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.0.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.233.76.49	Russian Federation	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/wp-admin/admin-ajax.php	Block	2
89.139.155.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.148.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
95.35.75.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2

01-26-2016-08:04:04 to 01-26-2016-09:04:04