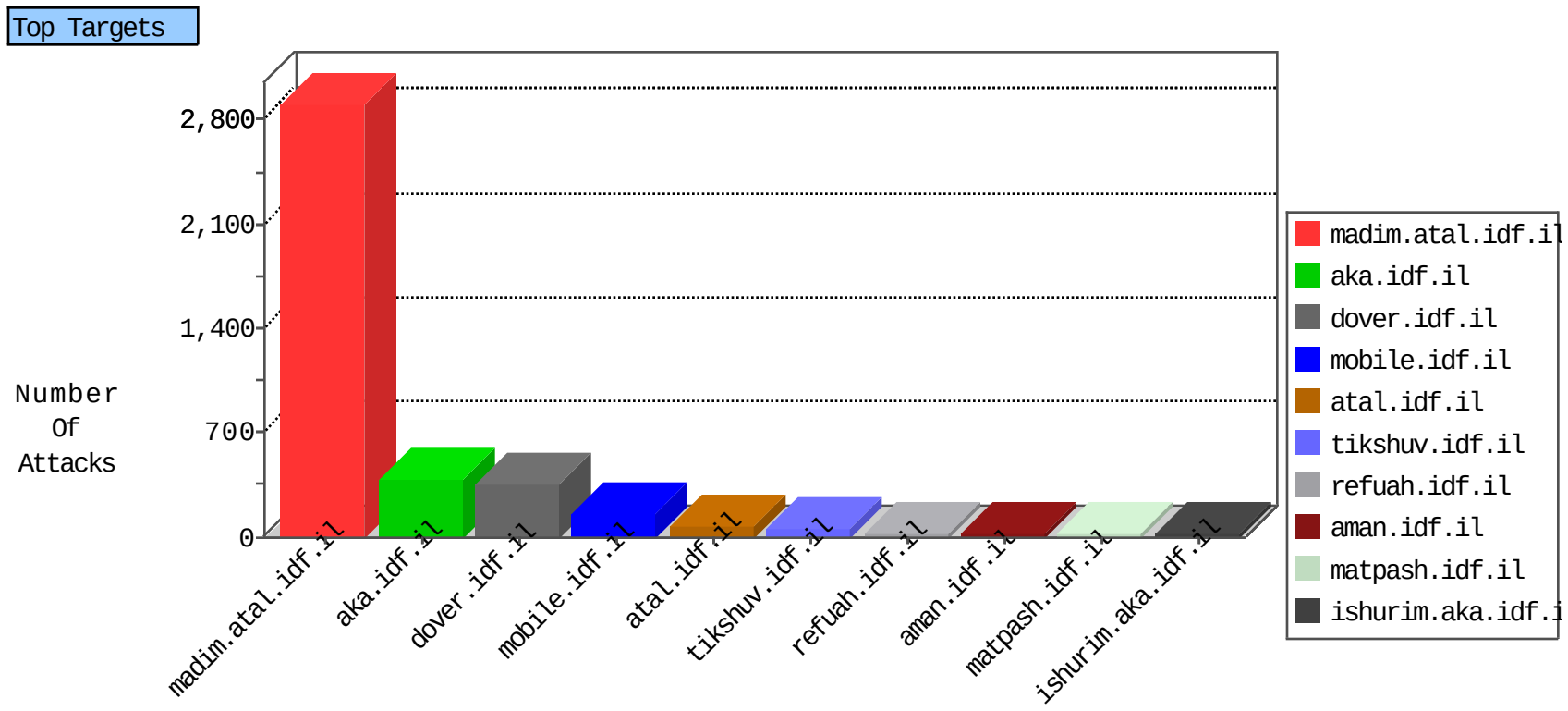
01-26-2016-20:04:08 to 01-26-2016-21:04:08

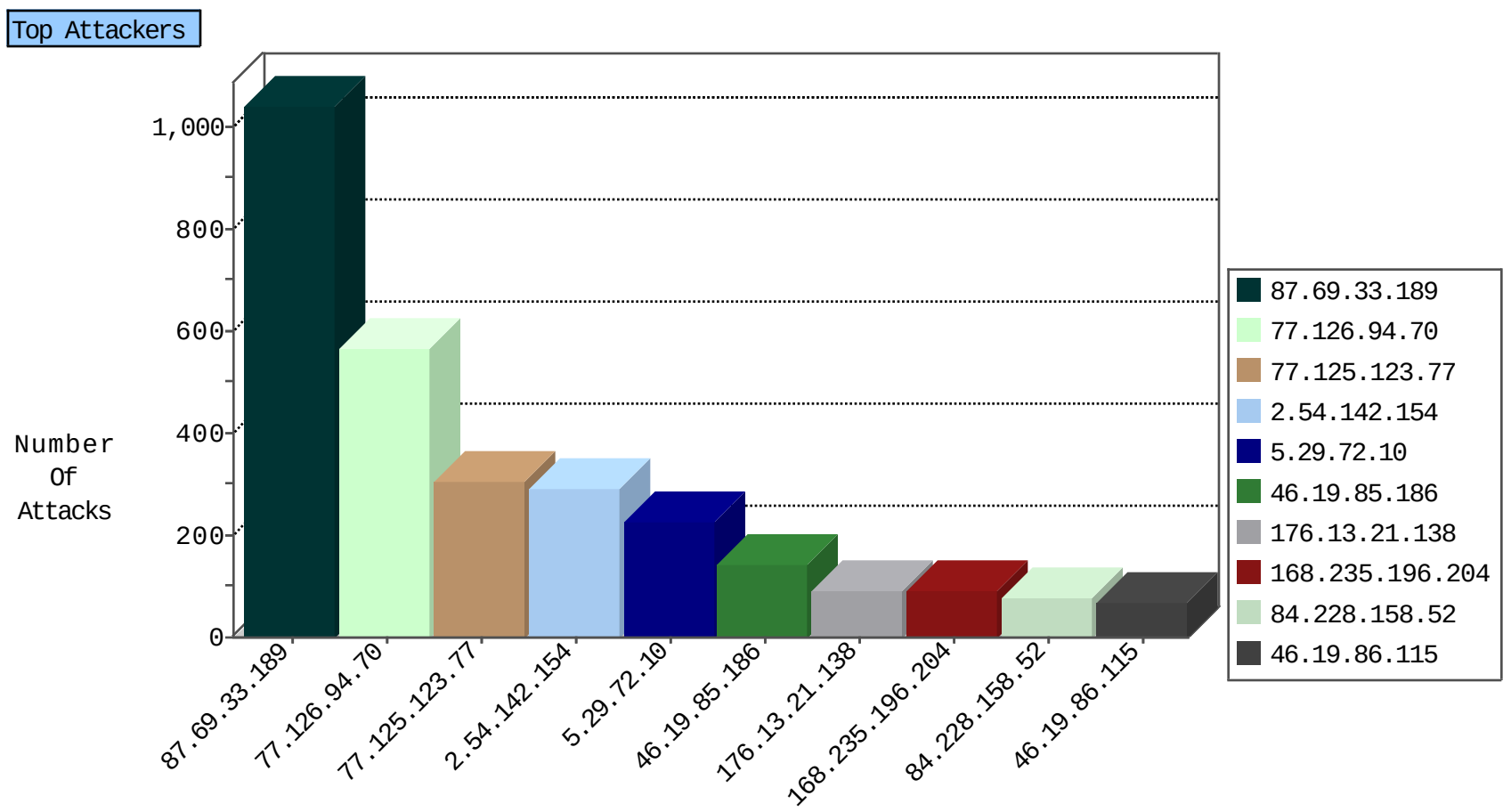
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-26-2016-20:04:08 to 01-26-2016-21:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.147.158	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
198.58.102.158	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.181.147.158	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
168.235.196.204	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
82.166.184.140	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	2
23.239.64.15	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
81.218.56.125	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
180.180.99.26	Thailand	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
185.11.146.169	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
122.0.26.36	Malaysia	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

01-26-2016-20:04:08 to 01-26-2016-21:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-26-2016-20:04:08 to 01-26-2016-21:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.199.57.192	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	16
213.204.101.24	147.237.76.30	Lebanon	himush.idf.il	ET SCAN NMAP -sA (2)	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
208.80.155.224	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2
87.68.73.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.79.104	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.224.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.216.176.244	147.237.8.28	Latvia	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
62.219.160.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.193.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
137.117.168.203	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
93.172.157.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.139.128.68	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.17.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.252.193.52	147.237.77.61	Turkey	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.11.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.87.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.216.176.244	147.237.0.19	Latvia	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.216.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.150.177.188	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
37.210.152.69	147.237.0.17	Qatar	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
151.250.144.242	147.237.77.216	Turkey	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.62.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.186.130.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

01-26-2016-20:04:08 to 01-26-2016-21:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
168.235.196.204	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	87
84.228.158.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	35
2.54.170.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
89.138.66.58	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	15
109.253.206.135	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
109.253.156.80	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.206.135	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
2.54.163.125	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
185.120.125.2		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.179.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
185.32.179.220	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
5.102.254.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.86	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.214	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
5.102.254.147	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
82.102.169.113	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.116.187.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.26.144.143	Turkey	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	6
109.253.133.101	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.197.234	Israel	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.89	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.64.217.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.117.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.65.22.167	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.181.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
172.56.35.50	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.110	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.29.195.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.44.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
79.177.202.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
149.88.82.67	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.163.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.254.65.114	Romania	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
206.217.69.114	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.163.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.99	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
206.217.69.114	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.163.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
79.178.195.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.93.99	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

01-26-2016-20:04:08 to 01-26-2016-21:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.33.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	524
87.69.33.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	447
77.126.94.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	307
2.54.142.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	161
77.126.94.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	158
77.125.123.77	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.125.123.77	Block	142
5.29.72.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	120
2.54.142.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
77.125.123.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
5.29.72.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
77.126.94.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	100
176.13.21.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
46.19.86.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
87.69.33.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	65
109.253.147.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
77.125.123.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	55
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
176.13.16.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
185.3.147.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
46.120.193.175	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.120.193.175	Block	17
2.54.142.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	16
5.22.130.139	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	11
50.28.145.181	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	8
2.54.170.181	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
31.154.176.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
89.138.66.58	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
208.80.155.224	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
176.61.137.36	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/yassin7.	Block	4
79.182.197.234	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	4
87.69.33.189	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtFirstName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	3
84.109.9.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.184.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.3.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.11.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.149.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.196.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.142.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.182.197.234	Israel	147.237.76.39	mobile.meitav.idf.il	Untraceable SSL Sessions: Open Mode	None	2
195.175.43.250	Turkey	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	2
178.241.92.232	Turkey	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	2
79.180.98.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.64.110.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.69.33.189	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
79.179.108.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
213.57.179.150	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2

01-26-2016-20:04:08 to 01-26-2016-21:04:08