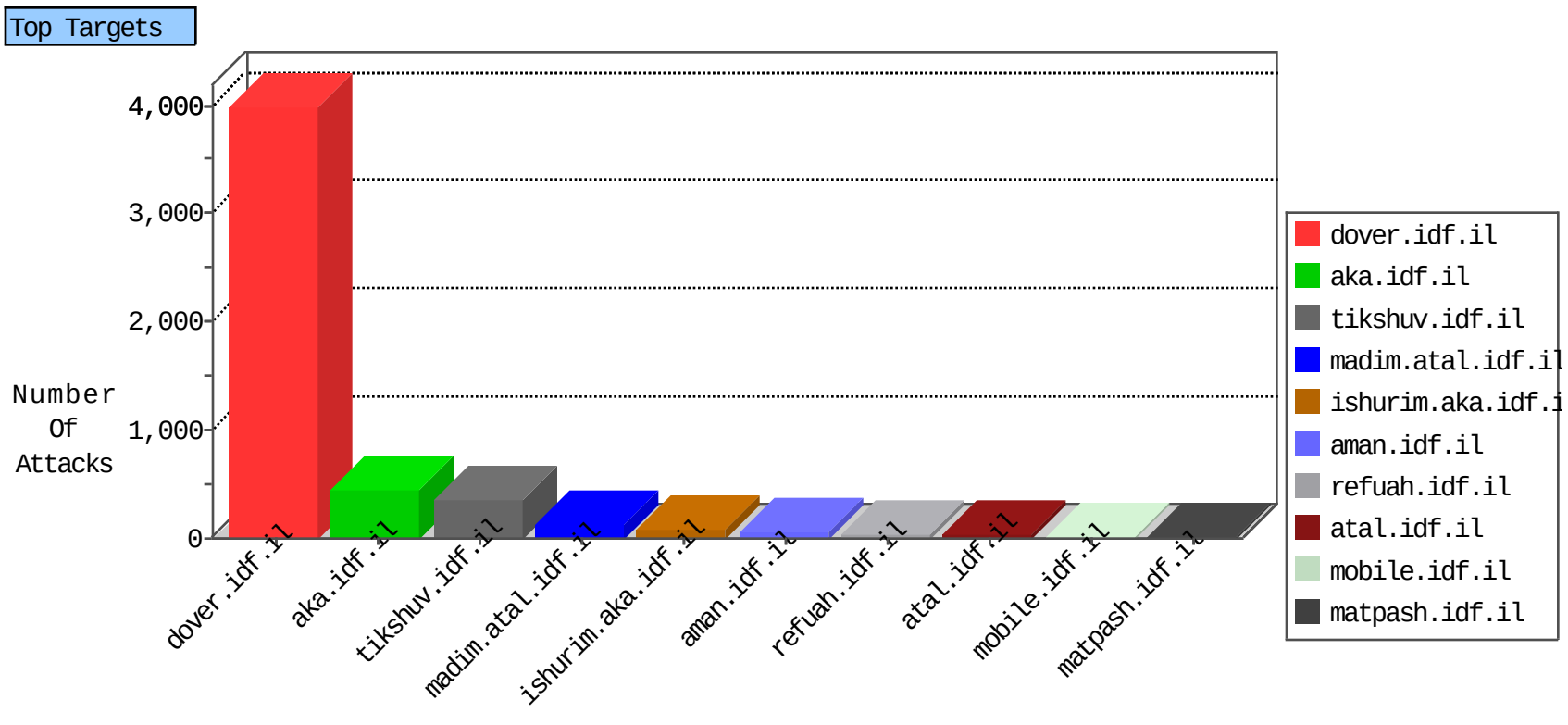
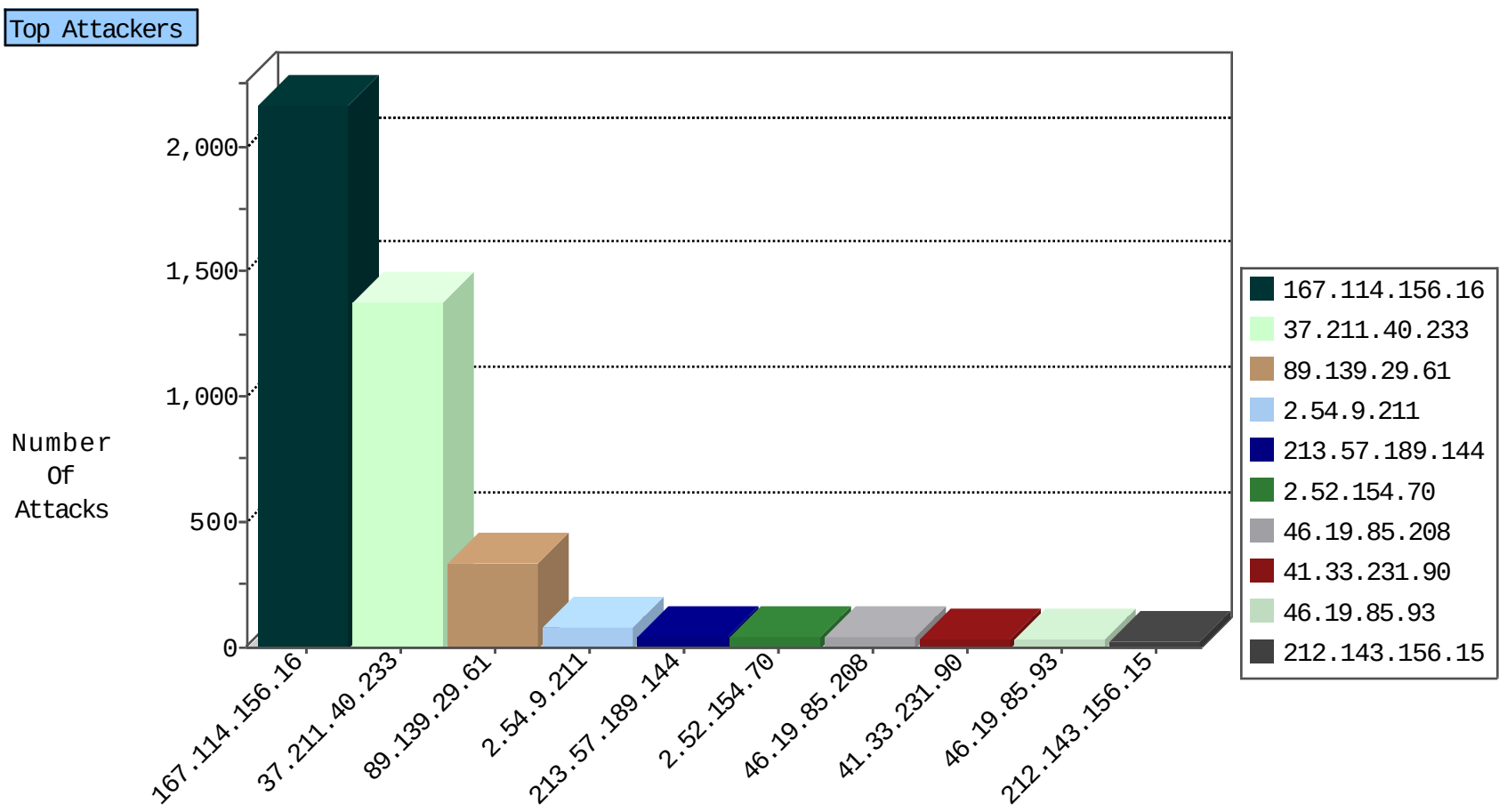
01-14-2016-11:04:04 to 01-14-2016-12:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-14-2016-11:04:04 to 01-14-2016-12:04:04

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	3146
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	553
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	333
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	261
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	52
2.54.9.211	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	50
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	19
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	19
46.19.85.93	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
109.226.26.218	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
2.54.140.130	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.183.33.131	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
176.13.14.1	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
198.27.117.202	Canada	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
130.25.67.207	Italy	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
37.26.148.141	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

01-14-2016-11:04:04 to 01-14-2016-12:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-14-2016-11:04:04 to 01-14-2016-12:04:04

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	2
104.192.0.20	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.19	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.77.212	Ukraine	e.dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
81.144.170.190	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
80.246.130.39	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
66.249.93.113	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
217.194.207.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.5.34	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.16.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.20	147.237.72.167	United States	ishurim.aka.idf.i	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.77.216		dover.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.137.132	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.182.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.54.199	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.154.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1

01-14-2016-11:04:04 to 01-14-2016-12:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	445
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	154
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	29
46.19.85.12	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	21
46.19.86.173	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	20
2.52.146.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	17
80.246.133.111	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.85.163	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
2.54.9.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
176.13.22.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
212.143.156.15	Israel	147.237.72.167	ishurim.aka.idf.i	drop	SAM rule	drop	13
46.19.85.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.52.154.70	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
46.19.85.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.49	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
82.80.137.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.9.211	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
213.8.204.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
212.143.156.15	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
37.26.148.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.114.23.209	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.115	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.154.70	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
213.140.59.146	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.52.154.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.154.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
192.114.23.209	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.54.9.211	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
46.19.86.142	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.52.188.93	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.250.208.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
213.8.204.48	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.176.14.156	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.66.2.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.226.26.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.250.236.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.8.204.48	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.26.146.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.226.26.218	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
85.250.236.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	SYN Attack		reject	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.139.29.61	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	336
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 37.211.40.233	Block	80
46.19.85.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
213.57.189.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
176.13.21.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
2.54.24.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
80.246.137.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.94.90.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.21.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	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
176.13.23.29	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
212.199.71.118	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 212.199.71.118	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	2
2.54.158.151	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
109.253.222.76	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
5.175.13.138	Germany	147.237.72.166	aka.idf.il	Unknown Parameter amp;moduletogoto in www.aka.idf.il/giyus/login/	None	1
94.230.93.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.54.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.208.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
80.246.133.111	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
130.193.51.51	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.146.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
213.8.204.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.175.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.187.142.208	Czech Republic	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.86.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
185.32.179.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.18.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.47.57	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 2.52.47.57 (Open Mode)	None	1
37.142.170.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.201.138.237	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.181.17.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.189.144	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/login.aspx	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
31.154.32.81	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
101.65.110.228	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/5/3785.pdf/rk=0/rs=s9jekpouhgmh3sqp0entghbrbw4-	Block	1
85.250.236.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.228.63.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.131.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1