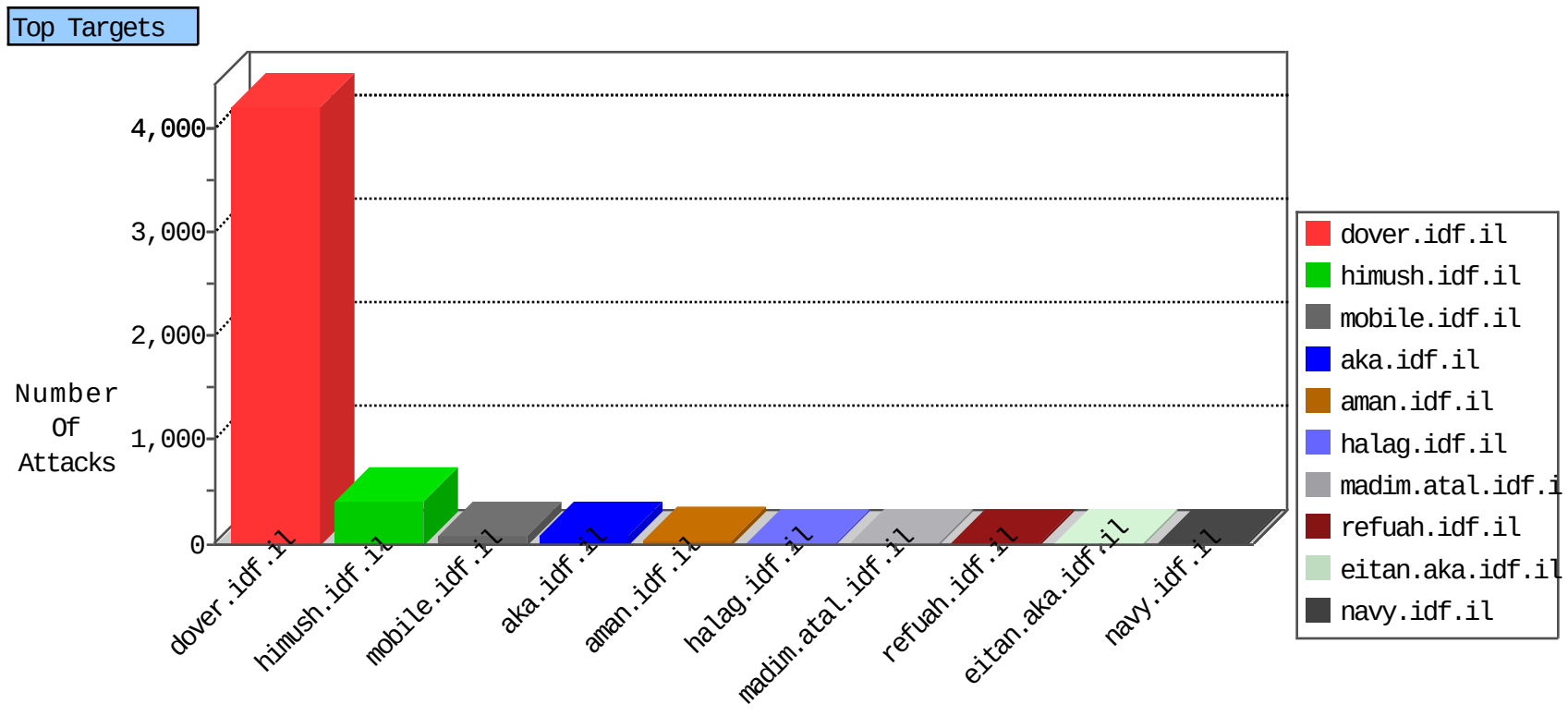
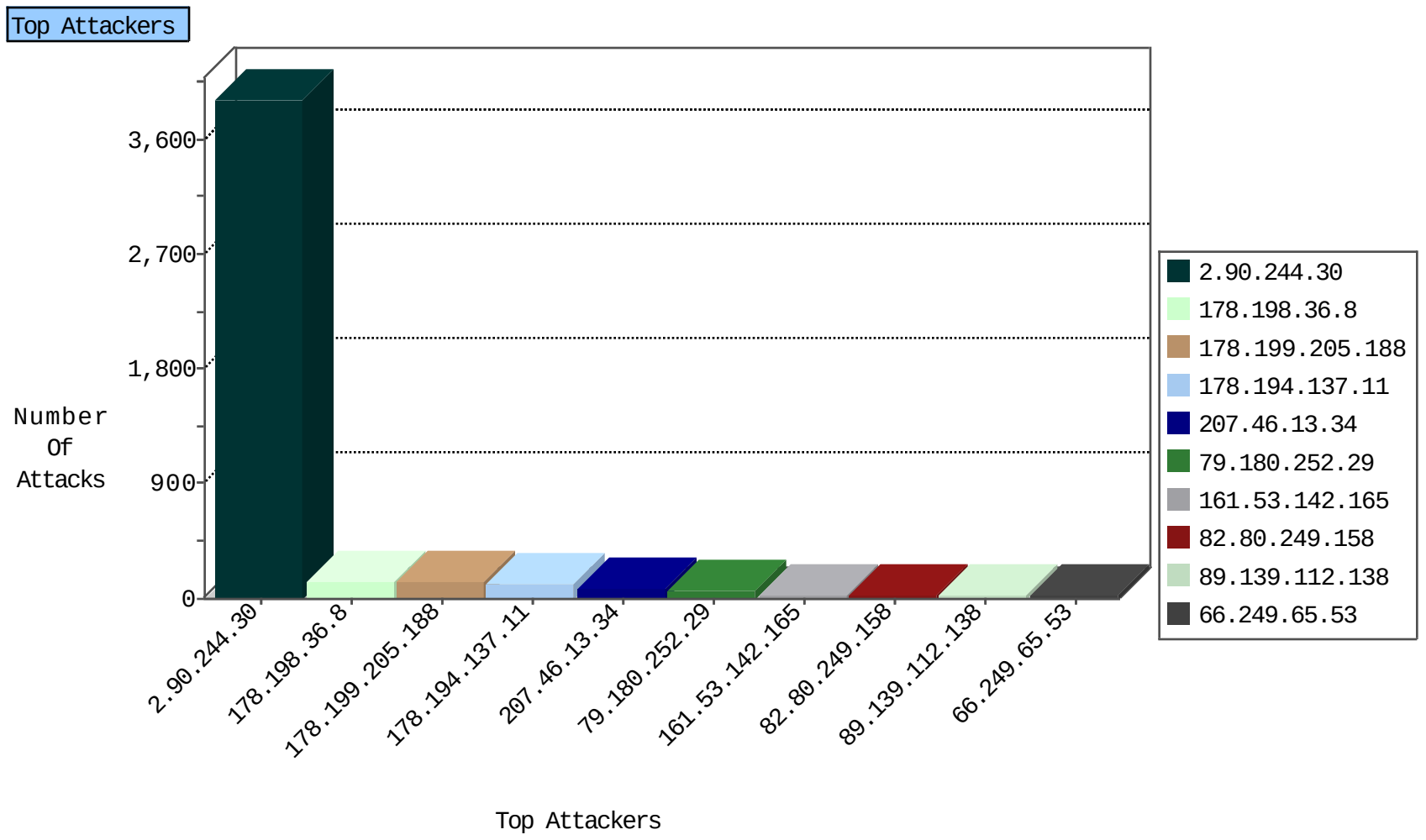
10-03-2016-18:04:04 to 10-03-2016-19:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-03-2016-18:04:04 to 10-03-2016-19:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.90.244.30	Saudi Arabia	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	19
2.90.244.30	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
222.187.220.241	China	147.237.0.33	idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
71.6.216.43	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
182.92.223.10	China	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
14.189.201.41	Vietnam	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
204.155.30.109	United States	147.237.76.86	navy.idf.il	Black List	drop	1
71.6.216.42	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	1

10-03-2016-18:04:04 to 10-03-2016-19:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.113.61.0	Russian Federation	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

10-03-2016-18:04:04 to 10-03-2016-19:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.47	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	3
151.80.41.96	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
219.146.251.139	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
208.100.26.228	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
176.47.3.45	147.237.77.176	Saudi Arabia	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
58.218.200.137	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
52.36.106.136	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
119.29.54.234	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.59.11	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
108.168.178.253	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
108.168.178.253	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
108.168.178.253	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
219.146.251.139	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
183.129.160.229	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
163.172.238.45	147.237.77.178	United Kingdom	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
52.36.106.136	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
125.65.82.44	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
108.168.178.253	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
14.152.59.11	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
108.168.178.253	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
108.168.178.253	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1

10-03-2016-18:04:04 to 10-03-2016-19:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.90.244.30	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3776
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	71
79.180.252.29	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
161.53.142.165	Croatia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	28
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
2.90.244.30	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
178.194.137.11	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	26
178.199.205.188	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	26
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	26
178.199.205.188	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	26
2.90.244.30	Saudi Arabia	147.237.77.216	dover.idf.il	drop		drop	26
178.194.137.11	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
178.199.205.188	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	25
178.199.205.188	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	25
178.194.137.11	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	24
178.194.137.11	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	24
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
178.199.205.188	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
178.194.137.11	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	23
66.249.65.53	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
178.194.137.11	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
107.167.105.168	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
212.106.86.3	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
37.46.41.243	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.32.215.207	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
89.139.112.138	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	9
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.90.244.30	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
37.217.119.192	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.21.104	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.29	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.90.244.30	Saudi Arabia	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	5
46.19.86.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
89.139.112.138	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.102	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
89.139.112.138	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
79.180.189.245	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.102	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
89.139.112.138	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.69.221.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
79.180.139.70	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.230.210.70	Russian Federation	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.121.91.133	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.139.200.123	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.174.52.3	Russian Federation	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
191.82.183.198	Argentina	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4

10-03-2016-18:04:04 to 10-03-2016-19:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.249.158	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.80.249.158	Block	5
185.32.179.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.249.158	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 82.80.249.158	Block	3
185.89.217.234	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.89.217.227	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.249.158	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.80.249.158	Block	3
82.80.249.158	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	3
87.69.87.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.87.20	Block	2
46.116.126.246	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluim/templates/inner.asp	Block	1
109.67.189.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.80.249.158	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 82.80.249.158	Block	1
37.113.61.0	Russian Federation	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
82.80.249.158	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	1
213.8.204.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.73.133	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.133	Block	1
46.116.121.183	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
2.53.55.47	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
77.139.86.153	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
185.89.217.233	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/faq.aspx	None	1
109.253.218.186	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/booklet.aspx	Block	1
82.80.249.158	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 82.80.249.158	Block	1
37.113.61.0	Russian Federation	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
217.132.9.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
82.80.249.158	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 82.80.249.158	Block	1
185.89.217.225	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
71.231.59.157	United States	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
46.116.126.246	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 46.116.126.246	Block	1
87.69.87.20	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/mailbox.aspx	Block	1
2.90.244.30	Saudi Arabia	147.237.77.216	dover.idf.il	Post Request - Missing Content Type	Block	1
82.80.249.158	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 82.80.249.158	Block	1
77.139.223.105	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
173.231.185.150	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/admin/i18n/readme.txt	Block	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/giyus/forum/default.asp	None	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
37.113.61.0	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin.php	Block	1
71.231.59.157	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method i[[#0]][[#0]][[#0]]BÔYÀÛÀm[[#18]]™k‰b=œ[[#19]][[#15]]í[[#27]]S•Ã[[#3]][[#5]][[#6]]¶Á[[#11]]MwÌl"¾[[#20]]TAÎ.ZLÌ[[#5]]É!*k›M"›ºã[[#26]]úÙøÚ{ô;h½örP‡[[#20]]Y,ùÊoõÎ4œ^¾HßØ.Þr¼[[#4]]ÖÙ1ãg{H[•}()	Block	1
94.187.88.57	Lebanon	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/brothers/skira/default.asp	Block	1
2.90.244.30	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized Method POST for 147.237.77.216/	Block	1
77.237.138.202	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
187.253.122.9	Mexico	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
173.231.185.150	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/admin/i18n/readme.txt	Block	1
66.249.65.58	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
84.109.38.47	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
82.80.249.158	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 82.80.249.158	Block	1
185.89.217.230	Netherlands	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
71.231.59.157	United States	147.237.77.216	dover.idf.il	NULL Character in Method i[[#0]][[#0]][[#0]]BÔYÀÛÀm[[#18]]™k‰b=œ[[#19]][[#15]]í[[#27]]S•Ã[[#3]][[#5]][[#6]]¶Á[[#11]]MwÌl"¾[[#20]]TAÎ.ZLÌ[[#5]]É!*k›M"›ºã[[#26]]úÙøÚ{ô;h½örP‡[[#20]]Y,ùÊoõÎ4œ^¾HßØ.Þr¼[[#4]]ÖÙ1ãg{H[•}()	Block	1
46.116.126.246	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/4/	Block	1

10-03-2016-18:04:04 to 10-03-2016-19:04:04