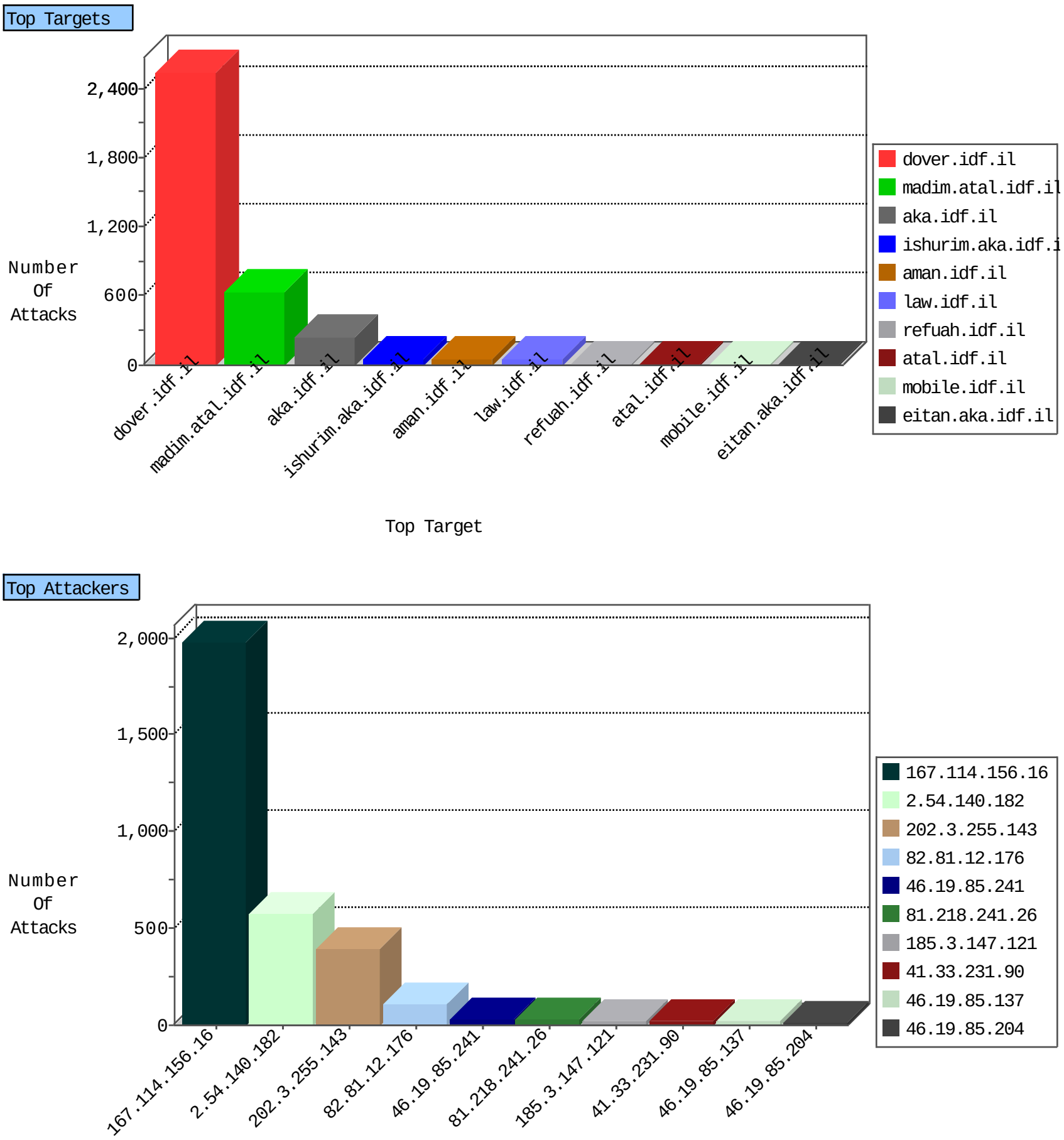
01-19-2016-07:04:00 to 01-19-2016-08:04:00

IDF Under Attack
Daily Report



01-19-2016-07:04:00 to 01-19-2016-08:04:00

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	3215
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	106
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
82.145.45.44	United Kingdom	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	2
107.170.231.174	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
178.62.231.125	United Kingdom	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

01-19-2016-07:04:00 to 01-19-2016-08:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	5
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	4
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	2
178.202.132.160	Germany	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	2
178.202.132.160	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
81.218.33.77	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	2
199.58.86.211	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
162.210.196.130	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
151.80.31.123	Italy	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
157.55.39.150	United States	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	1

01-19-2016-07:04:00 to 01-19-2016-08:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	359
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	11
66.249.64.97	147.237.77.170	United States	maarachot.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
27.251.16.85	147.237.77.216	India	dover.idf.il	GPL SCAN nmap TCP	2
80.246.130.2	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
84.109.73.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.198.0.90	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
133.232.152.43	147.237.8.28	Japan	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
133.232.152.43	147.237.8.28	Japan	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
91.206.201.94	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
163.172.13.173	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
133.232.152.43	147.237.8.28	Japan	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
117.207.253.127	147.237.76.30	India	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

01-19-2016-07:04:00 to 01-19-2016-08:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
46.19.85.241	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	31
46.19.85.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
190.237.24.144	Peru	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
73.133.91.39	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
78.93.118.5	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
94.230.86.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.89.217.230		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.89.217.232		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
62.219.166.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
81.218.241.26	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
80.246.130.2	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
80.246.130.2	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
185.89.217.227		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.177.187.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.187.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.167.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.49.5	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
83.130.116.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.128	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
79.177.62.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.142.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
148.251.6.16	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
185.89.217.234		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
46.117.134.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.89.217.225		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
212.150.222.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
194.177.16.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
157.55.39.67	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.117.232.84	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.89.217.224		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
77.126.18.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
213.204.101.24	Lebanon	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
61.135.190.197	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.140.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	324
2.54.140.182	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.140.182	Block	146
2.54.140.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
185.3.147.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
185.3.147.121	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.3.147.121	Block	10
185.32.179.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
176.13.10.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
37.26.148.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
162.144.93.104	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	2
162.144.93.104	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	2
190.237.24.144	Peru	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.168.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.7.183	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
176.13.3.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.219.166.165	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
81.21.67.195	United Kingdom	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
217.160.130.162	Germany	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
24.226.195.193	Canada	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
72.167.190.172	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
196.11.102.215	South Africa	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
109.253.223.168	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
50.62.208.40	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
188.143.232.21	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
37.26.149.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
186.202.153.17	Brazil	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
89.188.72.212	Denmark	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
184.168.89.215	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
77.101.126.218	United Kingdom	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
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	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
192.232.201.18	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
119.18.63.226	India	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
46.19.86.29	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
187.45.193.167	Brazil	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
93.157.99.179	Poland	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
24.226.195.193	Canada	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
185.61.152.8	United Kingdom	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
2.54.6.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
72.167.190.172	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
198.20.230.169	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
110.4.180.74	Japan	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
50.62.208.146	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
37.142.196.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
186.202.153.29	Brazil	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
89.188.72.212	Denmark	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
184.168.192.107	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
77.101.126.218	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
212.67.214.239	United Kingdom	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1