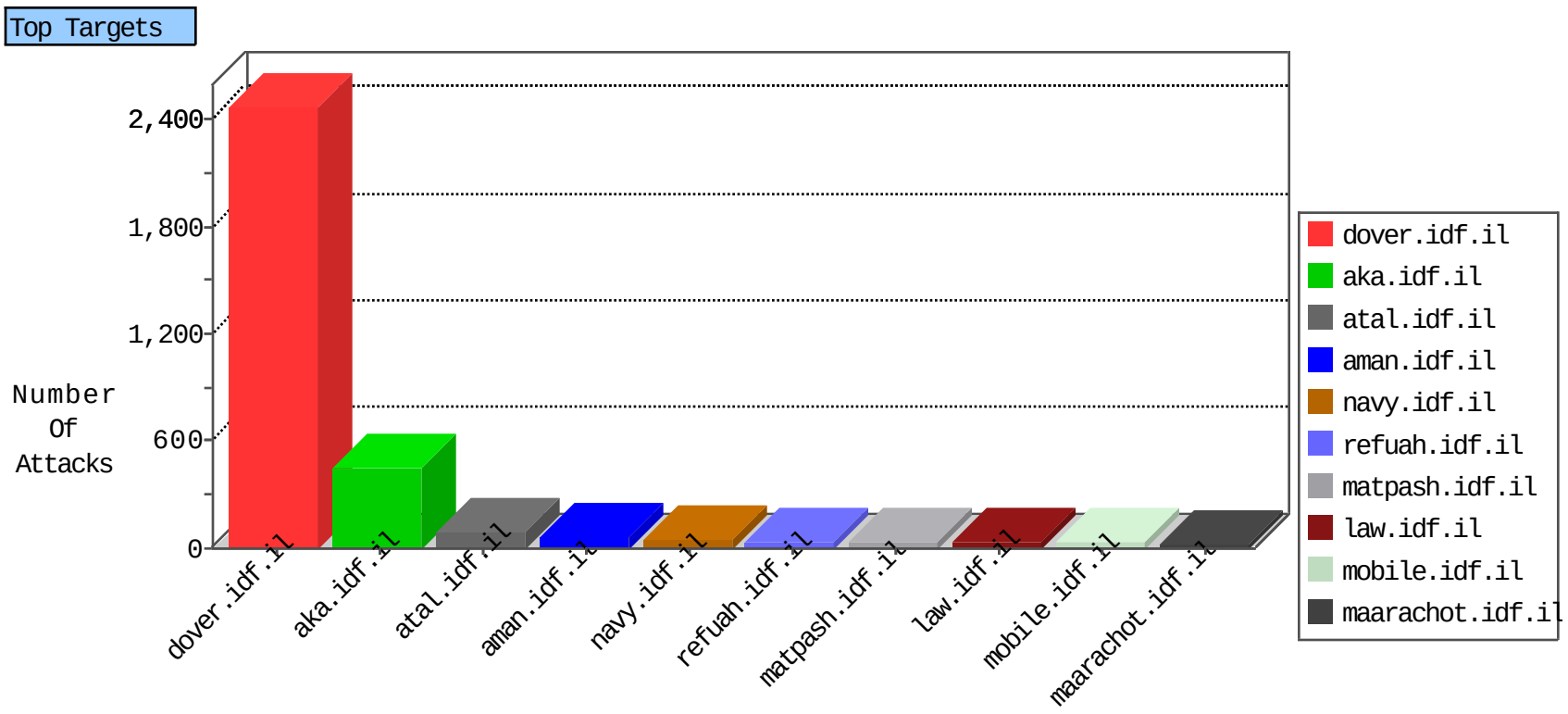
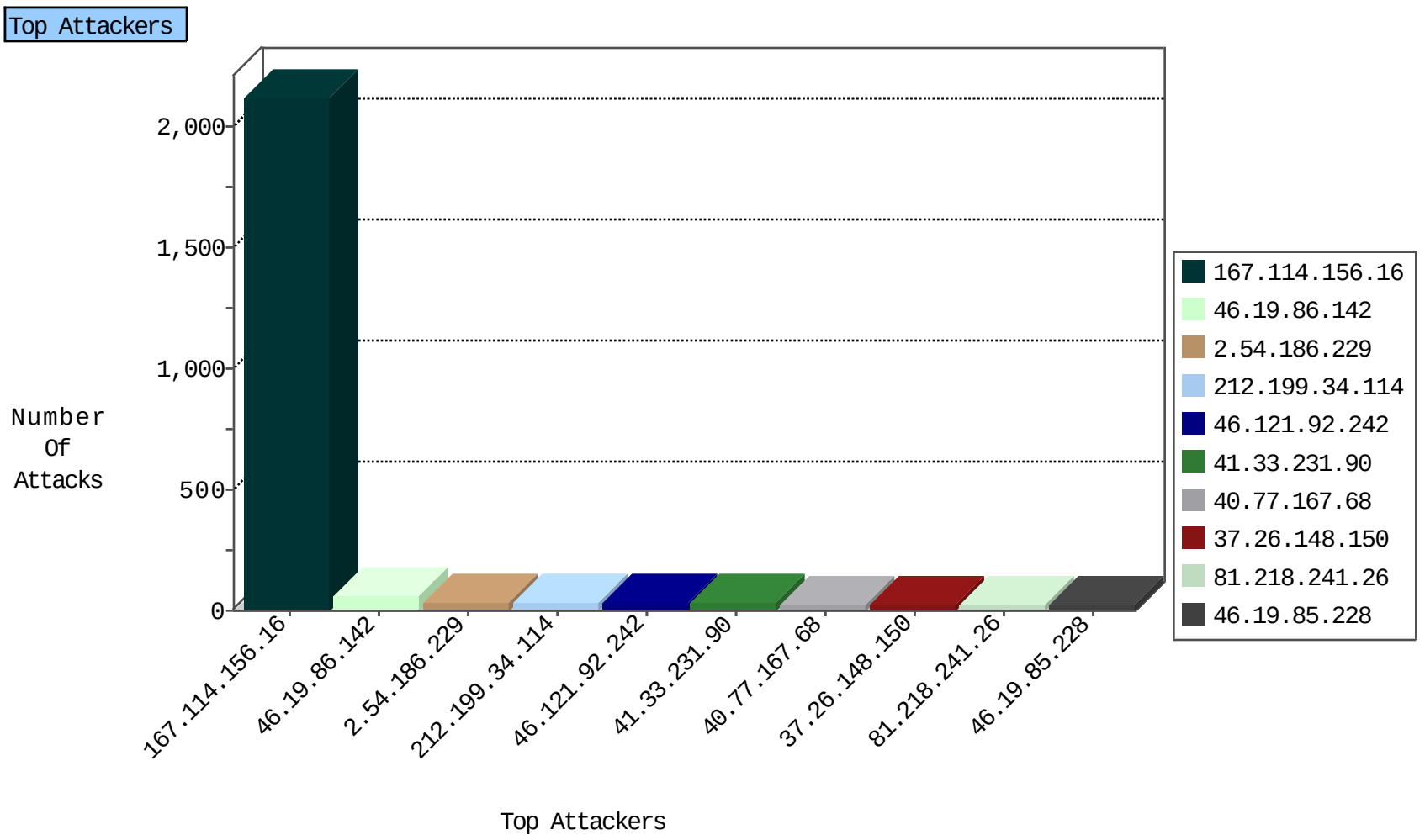
01-12-2016-17:04:04 to 01-12-2016-18:04:04

IDF Under Attack Daily Report





01-12-2016-17:04:04 to 01-12-2016-18:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.81.175	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	5292
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3195
66.249.81.183	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	1153
66.249.73.214	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	242
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
85.130.251.227	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	9
185.130.5.228		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
82.221.105.6	Iceland	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
66.249.81.179	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	1
66.240.236.119	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

01-12-2016-17:04:04 to 01-12-2016-18:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.89.170	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

01-12-2016-17:04:04 to 01-12-2016-18:04:04

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	4
66.249.81.175	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	3
79.179.108.185	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
79.182.21.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.24.122	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.65.201.196	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN NMAP -f -sS	1
46.19.86.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.141.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.32.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.158.236.2	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
85.64.38.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.251.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.165.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.77.79.38	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
185.65.201.196	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
46.19.86.133	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
164.39.11.198	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
5.102.254.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.235.254.181	147.237.77.178	Turkey	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
104.219.238.10	147.237.77.205		prisha.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.236.2	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	1

01-12-2016-17:04:04 to 01-12-2016-18:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.199.34.114	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	33
46.121.92.242	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
40.77.167.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	24
37.26.148.150	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
2.52.172.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
46.19.86.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
188.120.148.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.75	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	14
109.64.64.227	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
149.88.189.109	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
137.95.1.11	United States	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	12
79.177.39.218	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
37.26.148.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
173.203.67.252	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
149.78.188.119	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.54.186.229	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.142	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.86.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.86.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.102	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
46.19.86.142	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.54.186.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
79.182.22.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
2.54.186.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
194.114.62.88	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.54.186.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
85.250.101.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.228	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.250.129.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.3.147.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.2.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.134	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.228	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.250.129.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.111.242.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.149.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.0.1.178	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.178.102.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.55.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.109.85.179	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.22	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
84.111.226.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

01-12-2016-17:04:04 to 01-12-2016-18:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.107.186.233	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.107.186.233	Block	5
109.253.136.182	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	5
176.13.20.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.193.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.108.13.30	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/drushim/<hr><div	Block	3
46.210.209.157	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	3
195.95.183.254	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/6/112466.pdf	Block	3
176.13.6.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.230.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
77.127.126.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.2.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
37.60.42.25	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
195.95.183.254	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 195.95.183.254	Block	2
149.78.63.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.136.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
41.107.81.168	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
2.54.151.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
176.13.7.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
104.194.26.204	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
85.250.129.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
157.55.39.137	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
109.253.219.194	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
212.34.11.85	Jordan	147.237.77.216	dover.idf.il	Malformed URL	Block	1
2.54.163.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.144.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.126.144.182	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
185.120.126.29		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.74.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
173.203.67.252	United States	147.237.72.166	aka.idf.il	Multiple signatures from 173.203.67.252	Block	1
89.138.107.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.0.1.178	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
141.212.122.145	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
84.228.111.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.22.63	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
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	1
46.19.85.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.145.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
104.194.26.204	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
86.121.25.91	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
157.55.39.194	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
46.121.92.242	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1

01-12-2016-17:04:04 to 01-12-2016-18:04:04